QUẢN LÝ VÀ DUY TRÌ HỆ ĐIỀU HÀNH MICROSOFT WINDOWS SERVER 2003

MỤC LỤC

PHẦN 1
QUẢN LÝ VÀ DUY TRÌ HỆ ĐIỀU HÀNH

CHƯƠNG 1: GIỚI THIỆU HỆ ĐIỀU HÀNH WINDOWS SERVER 2003 CỦA MICROSOFT

Mục đích của khóa học này là hướng dẫn bạn cách quản trị và duy trì một môi trường mạng dựa trên nền Microsoft Windows Server 2003 và chuẩn bị cho môn thi 70-290 trong hệ thống chứng chỉ của Microsoft. Khóa này giả định rằng bạn đã có một chút ít kinh nghiệm với các sản phẩm Microsoft Windows nhưng lại khá mới với họ sản phẩm Windows Server 2003. Do đó, mục tiêu của chương này là giới thiệu với bạn các phiên bản khác nhau của hệ điều hành Windows Server 2003 để bạn có thể nhận biết các điểm khác nhau cơ bản giữa chúng và lựa chọn sản phẩm phù hợp, đáp ứng được nhu cầu của hệ thống của bạn.

Chương 1 sẽ hướng dẫn bạn qua các bước cài đặt Windows Server 2003 trên một máy tính và cấu hình nó thành một Active Directory Domain Controller (Máy chủ quản trị miền sử dụng Active Directory). Giảng viên có thể không yêu cầu bạn cài đặt hệ điều hành trên máy tính của bạn tại lớp học, nhưng nếu bạn muốn làm việc với hệ điều hành Windows Server 2003 tại nhà hoặc nơi nào khác ngoài lớp học, bạn phải làm quen với quá trình cài đặt và các bước cấu hình hệ thống này.

Sau khi kết thúc chương này, bạn có khả năng:

- **Nhận biết các khác nhau cơ bản giữa các phiên bản của hệ điều hành Windows Server 2003**
- **Cài đặt Windows Server 2003**
- **Tạo một máy chủ quản trị miền (domain controller)**
- **Nhận biết các thành phần logic và các khái niệm về Active Directory**

HỌ HỆ ĐIỀU HÀNH WINDOWS SERVER 2003

Windows Server 2003 là sản phẩm mới nhất trong các hệ điều hành Windows Server và được cải tiến rất nhiều so với các phiên bản trước đó: bảo mật tốt hơn, độ tin cậy cao hơn và dễ dàng quản trị. Phần sau đây sẽ trình bày tổng quan về họ sản phẩm Windows Server 2003, tập trung vào các điểm giống và khác nhau giữa 4 phiên bản: Web Edition, Standard Edition, Enterprise Edition và Datacenter Edition

Các phiên bản của họ Windows Server 2003

Windows Server 2003 là một phiên bản cập nhật cho nền tảng và các công nghệ đã giới thiệu trong Windows 2000. Nếu bạn nghiên cứu Windows Server 2003 trên cơ sở đã có kinh nghiệm về Windows 2000, bạn sẽ thấy việc chuyển đổi tương đối dễ dàng. Nếu bạn chỉ có kinh nghiệm với Windows NT 4, quá trình học của bạn có thể sẽ khó khăn hơn một chút.

Mặc dù giao diện cơ bản của Windows Server 2003 khá giống với Windows 2000 nhưng hệ điều hành này có rất nhiều cải tiến và tính năng mới nhằm bổ sung khả năng bảo mật, độ tin cậy và tăng cường nhiều công cụ quản trị. Khi bạn cân nhắc đến việc nâng cấp hay chuyển đổi sang hệ điều hành Windows Server 2003, bạn sẽ phải chỉ ra các tính năng và sự cải tiến đáng kể trong Active Directory, các công cụ mới hỗ trợ cho các đối tượng chính sách nhóm (GPO - Group Policy Object), sự tăng cường khả năng bảo mật cho hệ thống, sự cải tiến của Terminal Services hay hàng loạt các tính năng tiên tiên của hệ điều hành mới này.

> ***THÔNG TIN THÊM: Các tính năng mới trong Windows Server 2003****:Để tham khảo thêm đầy đủ các tính năng mới và khả năng hoàn hảo của Windows Server 2003, bạn có thể truy nhập vào Web site của Microsoft theo địa chỉ: http://www.microsoft.com/windowsserver2003*

Các phiên bản khác nhau của Windows Server 2003 được thiết kế để hỗ trợ các nền tảng thiết bị phần cứng và vai trò máy chủ khác nhau. Bên cạnh 4 phiên bản cơ bản của Windows Server 2003 - Web, Standard (Tiêu chuẩn), Enterprise (Doanh nghiệp) và Datacenter (Trung tâm dữ liệu) – hệ điều hành này còn có thêm các phiên bản hỗ trợ phần cứng 64 bit và các hệ thống nhúng. Phần tiếp theo sẽ trình bày chi tiết hơn về các phiên bản này.

Các yêu cầu hệ thống

Bốn phiên bản hệ điều hành khác nhau trong việc hỗ trợ các phần cứng. Bảng 1.1 liệt kê các yêu cầu hệ thống đối với từng phiên bản, đồng thời kèm theo phần cứng mà Microsoft khuyến nghị sử dụng.

Bảng 1-1: Các yêu cầu hệ thống của Windows Server 2003

	Web Edition	**Standard Edition**	**Enterprise Edition**	**Datacenter Edition**
Tốc độ CPU tối thiểu	133 MHz	133 MHz	133 MHz	400 MHz
Tốc độ CPU nên dùng	550 MHz	550 MHz	733 MHz	733 MHz
RAM tối thiểu	128 MB	128 MB	128 MB	512 MB
RAM nên dùng	256 MB	256 MB	256 MB	1 GB
RAM tối đa	2 GB	4 GB	32 GB	64 GB
Số bộ vi xử lí SMP (Symmetric MultiProcessing)	2	4	8	32
Khoảng trống đĩa tối thiểu	1.5 GB	1.5 GB	1.5 GB	1.5 GB

Phiên bản Web (Web Edition)

Để tăng tính cạnh tranh của Windows Server 2003 so với các máy chủ Web khác, Microsoft đã cho ra một phiên bản đặc biệt của Windows Server 2003, được thiết kế chuyên dụng cho chức năng của một máy chủ Web. Phiên bản Web là một phần của hệ điều hành chuẩn cho phép người quản trị có thể triển khai các Web site, các ứng dụng Web và các dịch vụ Web mà không tốn nhiều chi phí và công sức quản trị. Hệ điều hành này hỗ trợ tối đa 2GB bộ nhớ RAM và 2 bộ vi xử lí – chỉ bằng một nửa so với khả năng hỗ trợ của bản Standard Edition.

Phiên bản Web không có nhiều tính năng như các phiên bản Windows Server 2003 khác, tuy nhiên nó vẫn tích hợp một số thành phần có thể không cần thiết cho một Web Server điển hình, đó là:

- Một máy chủ chạy phiên bản Web có thể là thành viên của một miền sử dụng Active Directory nhưng nó không thể trở thành một máy chủ quản trị miền

- Mô hình ***Client Access License*** - CAL (*giấy phép truy nhập từ máy trạm*) chuẩn không được áp dụng cho các máy chủ chạy hệ điều hành Web Edition. Hệ điều hành này hỗ trợ một số lượng không giới hạn các kết nối Web, nhưng nó lại giới hạn tối đa 10 kết nối ***Server Message Block*** (SMB) đồng thời. Điều này có nghĩa là không thể có nhiều hơn 10 người dùng mạng nội bộ có thể truy nhập các tài nguyên file và máy in tại một thời điểm bất kì
- Các tính năng Tường lửa Bảo vệ Kết nối Internet (***Internet Connection Firewall*** -ICF) và Chia sẻ Kết nối Internet (***Internet Connection Sharing*** - ICS) sẽ không có trong phiên bản Web, điều này sẽ không cho phép máy chủ thực hiện chức năng của một cổng kết nối Internet.
- Một máy chủ chạy hệ điều hành Web Edition không thể thực hiện chức năng của một máy chủ DHCP, máy chủ fax, máy chủ Microsoft SQL hay một Máy chủ Dịch vụ Dầu cuối mặc dù chức năng ***Remote Desktop*** (*Truy nhập toàn màn hình từ xa*) dành cho quản trị vẫn được hỗ trợ.
- Phiên bản Web sẽ không cho phép chạy các ứng dụng không phải dịch vụ Web

Tuy nhiên, phiên bản Web lại bao gồm đầy đủ các thành phần chuẩn mà một máy chủ Web cần, bao gồm ***Microsoft Internet Information Services (IIS) 6, Network Load Balancing (NLB),*** và ***Microsoft ASP.NET***.

Do vậy, hiển nhiên là phiên bản Web không phải là một nền tảng thích hợp cho các máy chủ mạng thông thường. Nó cho phép các cơ quan hay tổ chức triển khai các máy chủ Web chuyên dụng, không hỗ trợ các thành phần khác mà máy chủ web này không cần thiết sử dụng trong vai trò của nó.

> ***LƯU Ý: Mua phiên bản Web***. *Bản Web Edition không được bán thông qua các kênh phân phối lẻ, sản phẩm này chỉ được cung cấp cho các khách hàng của Microsoft chấp nhận kí kết các văn bản thỏa thuận bản quyền riêng cho doanh nghiệp (Enterprise and Select licensing agreements), các nhà cung cấp dịch vụ kí kết văn bản thỏa thuận bản quyền riêng cho nhà cung cấp dịch vụ (service provider licensing agreement - SPLA) thông qua các Nhà Sản xuất Thiết bị gốc của Microsoft (Microsoft original equipment manufacturers - OEMs) hoặc các Đối tác Xây dựng Hệ thống (System Builder partners)*

Phiên bản Tiêu chuẩn (Standard Edition)

Phiên bản Standard sử dụng cho nền tảng máy chủ đa chức năng trong đó có thể cung cấp các dịch vụ thư mục (Directory), file, in ấn, ứng dụng, multimedia và dịch vụ Internet cho các doanh nghiệp cỡ vừa và nhỏ. Sau đây là một vài trong rất nhiều tính năng có trong phiên bản này của hệ điều hành :

- **Directory services (Dịch vụ Thư mục)**: Phiên bản Standard có khả năng hỗ trợ đầy đủ đối với Active Directory cho phép các máy chủ có thể đóng vai trò là máy chủ thành viên hoặc các máy chủ quản trị miền. Người quản trị mạng có thể sử dụng các công cụ kèm theo hệ điều hành để triển khai và quản trị các đối tượng Active Directory, các chính sách nhóm (GP – Group Policy) và các dịch vụ khác dựa trên nền Active Directory.
- **Dịch vụ Internet:** Phiên bản Standard bao gồm IIS 6.0 cung cấp các dịch vụ Web và FTP cũng như các thành phần khác sử dụng trong quá trình triển khai máy chủ Web như dịch vụ Cân bằng Tải (NLB – Network Load Balancing). Chức năng NLB cho phép nhiều máy chủ Web có thể cùng duy trì (host) một Web site đơn, chia sẻ các yêu cầu kết nối của client trong tối đa 32 máy chủ đồng thời cung cấp khả năng chống lỗi cho hệ thống.
- **Các dịch vụ cơ sở hạ tầng:** Phiên bản Standard bao gồm các dịch vụ Microsoft DHCP Server, Domain Name System (DNS) Server, và Windows Internet Name Service (WINS) Server, cung cấp các dịch vụ cơ bản cho mạng nội bộ và các máy khách trên Internet.
- **Định tuyến TCP/IP** (TCP/IP Routing): Một máy chủ chạy phiên bản Standard có thể thực thi như một router với rất nhiều cấu hình bao gồm định tuyến LAN và WAN, định tuyến truy nhập Internet và định tuyến truy nhập từ xa. Để thực hiện các chức năng này, dịch vụ Định tuyến và Truy nhập Từ xa (Routing and Remote Access Service - RRAS) có hỗ trợ cho các tính năng Chuyển đổi Địa chỉ Mạng (Network Address Translation – NAT), Dịch vụ Xác thực Internet (Internet Authentication Service – IAS), các giao thức định tuyến như Giao thức Thông tin Định tuyến (Routing Information Protocol – RIP) và Ưu tiên Đường Ngắn nhất (Open Shortest Path First – OSPF).
- **Dịch vụ File và In ấn**: Người dùng trong mạng có thể truy nhập các ổ đĩa, thư mục và máy in chia sẻ trên một máy chủ chạy phiên bản Standard của hệ điều hành . Mỗi máy khách (client) khi muốn truy nhập đến các tài nguyên đã chia sẻ trên máy chủ sẽ phải có một Giấy

phép Truy nhập (Client Access License - CAL). Phiên bản Standard thông thường được bán thành một gói gồm 5, 10 Giấy phép Truy nhập (CAL) hoặc nhiều hơn, và khi muốn thêm nhiều người dùng truy nhập, bạn sẽ phải mua bổ sung các Giấy phép Truy nhập (CAL) này.

- **Máy chủ Terminal (đầu cuối):** Một máy chủ chạy Phiên bản Standard có thể thực hiện chức năng một Máy chủ Dịch vụ Dầu cuối, cho phép các máy tính và các thiết bị khác có thể truy nhập màn hình Windows và các ứng dụng đang chạy trên máy chủ này. Máy chủ Dịch vụ Dầu cuối bản chất là một kĩ thuật điều khiển từ xa cho phép các máy khách (client) truy nhập đến một phiên làm việc Windows trên máy chủ. Mọi ứng dụng được thực thi trên máy chủ và chỉ bàn phím, màn hình và các thông tin hiển thị được truyền qua mạng. Các máy khách của Máy chủ Dịch vụ Dầu cuối được yêu cầu Giấy phép Truy nhập khác so với Giấy phép Truy nhập chuẩn CAL mặc dù Phiên bản Standard đã cung cấp sẵn một Giấy phép Truy nhập cho 2 người dùng sử dụng dịch vụ Remote Desktop for Administration (Dịch vụ truy nhập toàn màn hình từ xa dành cho các tác vụ quản trị), một công cụ quản trị từ xa dựa trên dịch vụ Terminal
- **Các dịch vụ bảo mật:** Phiên bản Standard còn có rất nhiều các tính năng bảo mật mà một người quản trị có thể triển khai nếu cần, bao gồm khả năng Mã hóa Hệ thống File (EFS) – bảo vệ các file trên các ổ cứng máy chủ bằng cách lưu trữ chúng trong một định dạng đã được mã hóa, tính năng bảo mật IP (IP Security - IPsec) mở rộng, - sử dụng chữ kí số để mã hóa dữ liệu trước khi truyền đi trên mạng, tính năng tường lửa ICF – qui định các luật đối với các luồng dữ liệu đi từ Internet vào trong mạng và tính năng sử dụng Public Key Infrastructure (PKI) – cung cấp khả năng bảo mật dựa trên mã hóa bằng khóa công khai và các chứng nhận số hóa.

Phiên bản Doanh nghiệp (Enterprise Edition)

Phiên bản Enterprise được thiết kế hoạt động trên các máy chủ cấu hình mạnh của các tổ chức doanh nghiệp cỡ vừa và lớn. Phiên bản này khác phiên bản Standard chủ yếu ở mức độ hỗ trợ phần cứng. ví dụ: Bản Enterprise hỗ trợ tối đa 8 bộ vi xử lí so với 4 bộ của bản Standard và tối đa 32GB bộ nhớ RAM so với khả năng của bản Standard chỉ là 4GB.

Phiên bản Enterprise còn bổ sung thêm một số tính năng quan trọng mà không có trong bản Standard, bao gồm các thành phần sau:

- **Microsoft Metadirectory Services - MMS (Dịch vụ Siêu Thư mục Microsoft)**: *Metadirectory* bản chất là thư mục của các thư mục – một

phương tiện tích hợp nhiều nguồn thông tin vào một thư mục đơn, thống nhất. MMS cho phép chúng ta có thể kết hợp các thông tin trong Active Directory với các dịch vụ thư mục khác, để tạo ra một cách nhìn tổng thể tất cả các thông tin về một tài nguyên nào đó. Phiên bản Enterprise chỉ cung cấp hỗ trợ cho MMS mà không phải là phần mềm MMS thực sự, phần mềm này bạn phải lấy từ Microsoft Consulting Service (Dịch vụ tư vấn Microsoft - MCS) hoặc thông qua một thỏa thuận với đối tác MMS.

- **Server Clustering (Chuỗi Máy chủ)**: Chuỗi máy chủ là một nhóm các máy chủ nhưng lại đóng vai trò như một máy chủ đơn cung cấp khả năng sẵn sàng cao cho một nhóm các ứng dụng. Tính sẵn sàng trong trường hợp này có nghĩa là các chu trình hoạt động của ứng dụng đó được phân bố đều trong các máy chủ trong chuỗi, giảm tải trên mỗi máy chủ và cung cấp khả năng chịu lỗi nếu bất kì máy chủ nào bị sự cố. Các máy chủ trong chuỗi, được gọi là các nút, đều có khả năng truy nhập đến một nguồn dữ liệu chung, thông thường là một mạng lưu trữ lớn (Storage Area Network - SAN), cho phép các nút luôn được duy trì cùng một nguồn thông tin dữ liệu cơ sở. Phiên bản Enterprise hỗ trợ máy chủ cluster có tối đa 8 nút
- **Bộ nhớ RAM Cắm nóng (Hot Add Memory):** Phiên bản Enterprise bao gồm phần mềm hỗ trợ một đặc tính của phần cứng gọi là Bộ nhớ Cắm nóng, cho phép người quản trị mạng có thể thêm hoặc thay thế bộ nhớ RAM trong máy chủ mà không cần tắt máy hoặc khởi động lại. Để sử dụng tính năng này, máy tính phải có phần cứng hỗ trợ tương ứng.
- **Quản trị Tài nguyên Hệ thống của Windows (Windows System Resource Manager - WSRM):** Tính năng này cho phép người quản trị mạng có thể phân bố tài nguyên hệ thống cho các ứng dụng hoặc chu trình dựa trên nhu cầu của các người dùng, đồng thời duy trì các bản báo cáo về tài nguyên do các ứng dụng hay chu trình trong hệ thống sử dụng. Điều này cho phép các tổ chức doanh nghiệp có thể thiết lập giới hạn sử dụng tài nguyên cho một ứng dụng xác định hoặc tính chi phí cho khách hàng dựa trên các tài nguyên họ sử dụng.

Phiên bản Trung tâm Dữ liệu (Datacenter Edition)

Phiên bản Datacenterđược thiết kế cho các máy chủ ứng dụng cao cấp, lưu lượng truy nhập lớn, yêu cầu sử dụng rất nhiều tài nguyên hệ thống. Phiên bản này cũng gần giống Phiên bản Enterprise khi so sánh các tính năng, tuy nhiên nó hỗ trợ tốt hơn cho việc mở rộng phần cứng, có thể hỗ trợ tối đa

64GB bộ nhớ và 32 bộ vi xử lí. Phiên bản này không tích hợp một số tính năng có trong bản Enterprise, ví dụ như tính năng ICS và ICF bởi vì các máy chủ cao cấp chạy bản Datacenter thông thường không được gán các vai trò cần sử dụng đến các chức năng này.

> ***LƯU Ý: Mua phiên bản Datacenter***. *Việc mua các phiên bản Datacenter, cũng giống như đối với phiên bản Web, không được thực hiện thông qua các kênh phân phối lẻ. Bạn có thể mua các hệ điều hành này thông qua một OEM như là sản phẩm kèm theo trong một bộ phần cứng máy chủ cao cấp.*

Các phiên bản 64-Bit

Cả hai Phiên bản Enterprise và Datacenter đều có các phiên bản riêng hỗ trợ các máy tính trang bị bộ vi xử lí Intel Itanium. Itanium là một bộ vi xử lí hỗ trợ việc đánh địa chỉ 64-bit (trong khi các bộ vi xử lý Intel x86 tiêu chuẩn chỉ hỗ trợ 32-bit), cho phép mở rộng không gian bộ nhớ ảo và vùng bộ nhớ phân trang đồng thời cải tiến hiệu năng xử lý dấu phẩy động. Nó được thiết kế đặc biệt cho các tác vụ yêu cầu năng suất bộ xử lý cực lớn, ví dụ như các ứng dụng cơ sở dữ liệu khổng lồ, các phân tích khoa học và các máy chủ Web có lượng truy nhập rất lớn.

Các yêu cầu hệ thống cho các phiên bản Itanium chạy các phiên bản Enterprise và Datacenter của hệ điều hành Windows 2003 Server về cơ bản rất khác so với các yêu cầu của các phiên bản này đối với các phần cứng x86 (được tổng kết trong Bảng 1-2). Đồng thời, một số tính năng trong các phiên bản dành cho hệ thống x86 sẽ không có trong Itanium, ví dụ các chip Itanium sẽ không hỗ trợ các ứng dụng Windows 16-bit, các ứng dụng chế độ thực, các ứng dụng POSIX (Portable Operating System Interface for UNIX) hoặc các dịch vụ in ấn cho các máy trạm Apple Macintosh.

Bảng 1-2: Các yêu cầu hệ thống đặc biệt cho bản Windows Server 2003 trên Itanium:

	Enterprise Edition	Datacenter Edition
Tốc độ tối thiểu của CPU	733 MHz	733 MHz
RAM tối đa	64 GB	512 GB
Khoảng trống đĩa tối thiểu	2 GB	2 GB

CÀI ĐẶT WINDOWS SERVER 2003

Trước khi bạn có thể học cách quản trị và duy trì một hệ thống Windows Server 2003, bạn phải có khả năng cài đặt hệ điều hành này và cấu hình nó để thực hiện các tác vụ theo yêu cầu. Mặc dù khóa này không giới thiệu về các chủ đề nâng cao như thiết kế Active Directory, tuy nhiên sẽ đề cập đến việc quản trị các đối tượng Active Directory ví dụ như các người dùng, máy tính và các nhóm. Trước khi bạn có thể thực hành một số các bài tập thực hành trong cuốn sách này và trong cuốn Lab Manual, bạn phải có một máy tính cài đặt hệ điều hành Windows Server 2003 và được cấu hình thành một máy chủ quản trị miền sử dụng Active Directory

Các giai đoạn cài đặt:

Nếu bạn đã có kinh nghiệm cài đặt Windows Server 2000, bạn sẽ thấy quá trình cài đặt Windows Server 2003 rất thân thiện. Nó được chia thành 2 giai đoạn riêng biệt:

Chế độ text:

Giai đoạn khởi tạo quá trình cài đặt bắt đầu khi máy tính khởi động từ đĩa CD chứa bộ cài Windows Server 2003 và chạy chương trình Winnt.exe. Không giống như Windows 2000 và các phiên bản trước đó, Windows Server 2003 không hỗ trợ việc bắt đầu cài đặt từ đĩa mềm. Chương trình Winnt.exe nạp các file của hệ điều hành Windows Server 2003 từ đĩa CD. Đây là phiên bản hạn chế, thực thi trong chế độ văn bản của hệ điều hành bởi vì các file cần thiết cho Giao diện Đồ họa người dùng (***Graphical User Interface - GUI***) chưa được cài đặt. Chương trình này sẽ định dạng phân vùng mà sẽ sử dụng để làm đĩa hệ thống, Tạo cấu trúc thư mục gốc của hệ thống và chép các file của hệ điều hành từ các thư mục tạm vào đúng vị trí. Tiếp theo chương trình cài đặt bắt đầu xây dựng ***registry***, tạo các khóa chứa các thông tin cơ bản về hệ điều hành, cũng như các thông tin về phần cứng được phát hiện trong quá trình cài đặt. Sau đó máy tính khởi động lại.

Chế độ đồ họa:

Khi hệ thống khởi động lại lần hai, nó sử dụng các file khởi động và các file của hệ điều hành, hiện đã nằm cố định trên đĩa hệ thống. Giao diện Windows thân thiện xuất hiện lần đầu tiên, sử dụng trình điều khiển hiển thị VGA với độ phân giải thấp. Sau khi hệ thống khởi động xong, quá trình đồ họa bắt đầu bằng chu trình phát hiện phần cứng. Khi các phần cứng mới được phát hiện, và trình điều khiển đã được cài đặt, chương trình bắt đầu thu thập thông tin từ người dùng mà nó cần để hoàn thành quá trình cài đặt, đồng thời nó sẽ cài đặt rất nhiều thành phần không thiết yếu khác của hệ thống. Nếu

như card mạng được phát hiện, chương trình cài đặt sẽ cài các thành phần mạng cần thiết và kết buộc chúng với trình điều khiển thiết bị mạng. Cuối cùng, chương trình xây dựng Thực đơn Khởi động (***Start Menu***), thiết lập các tham số bảo mật hệ thống, xóa các file tạm tạo ra trong quá trình cài đặt và lưu cấu hình hệ thống lại trước khi khởi động lại lần cuối cùng.

Các thao tác cài đặt:

Phần này sẽ trình bày các bước chi tiết của quá trình cài đặt Windows Server 2003 với giả định rằng bạn sử dụng một máy tính thỏa mãn các yêu cầu hệ thống của Windows Server 2003, đồng thời bạn cài đặt hệ điều hành từ một đĩa CD nguyên gốc và các đĩa cứng của hệ thống là hoàn toàn trống.

> ***LƯU Ý: Các thay đổi trong quá trình cài đặt.*** *Các thao tác cài đặt ở đây giả định rằng bạn sử dụng một máy tính có cấu hình phần cứng cơ bản. Sự có mặt của các thiết bị phần cứng nhất định nào đó khác trong máy tính có thể gây ra các thay đổi trong quá trình cài đặt (ví dụ như các bước cấu hình bổ sung) không được đề cập ở đây.*

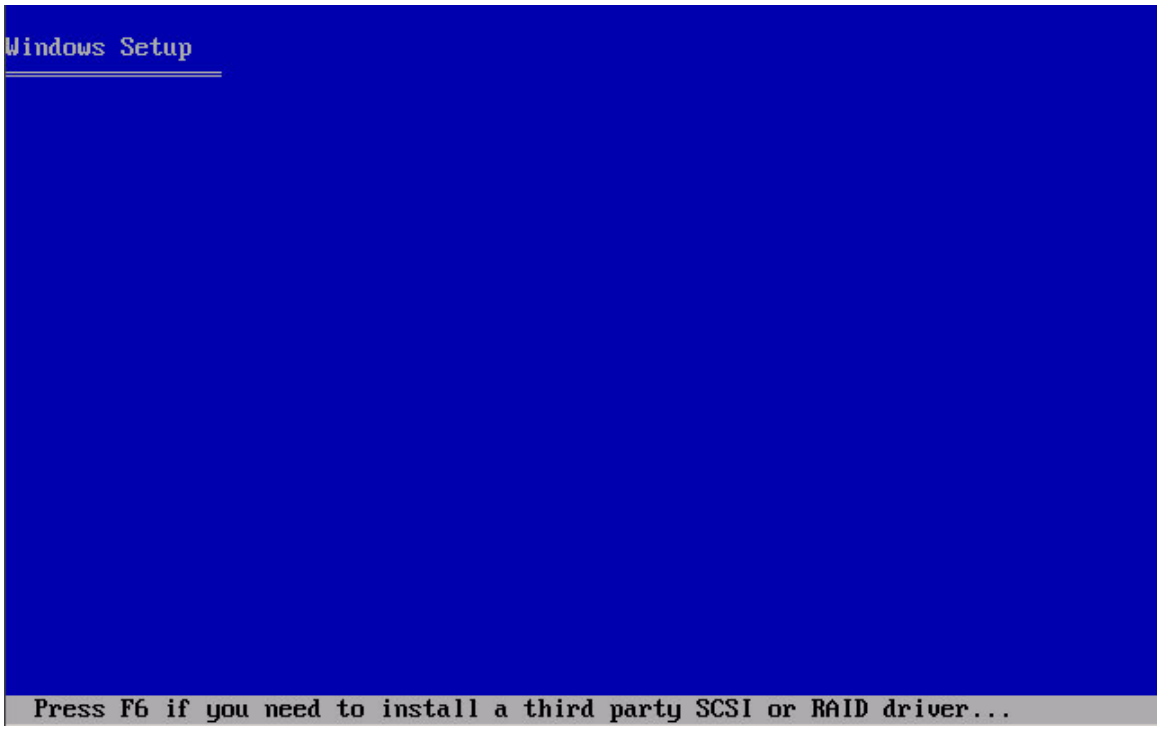
Cài đặt Windows Server 2003:

Để cài đặt Windows Server 2003, sử dụng các thao tác sau đây:

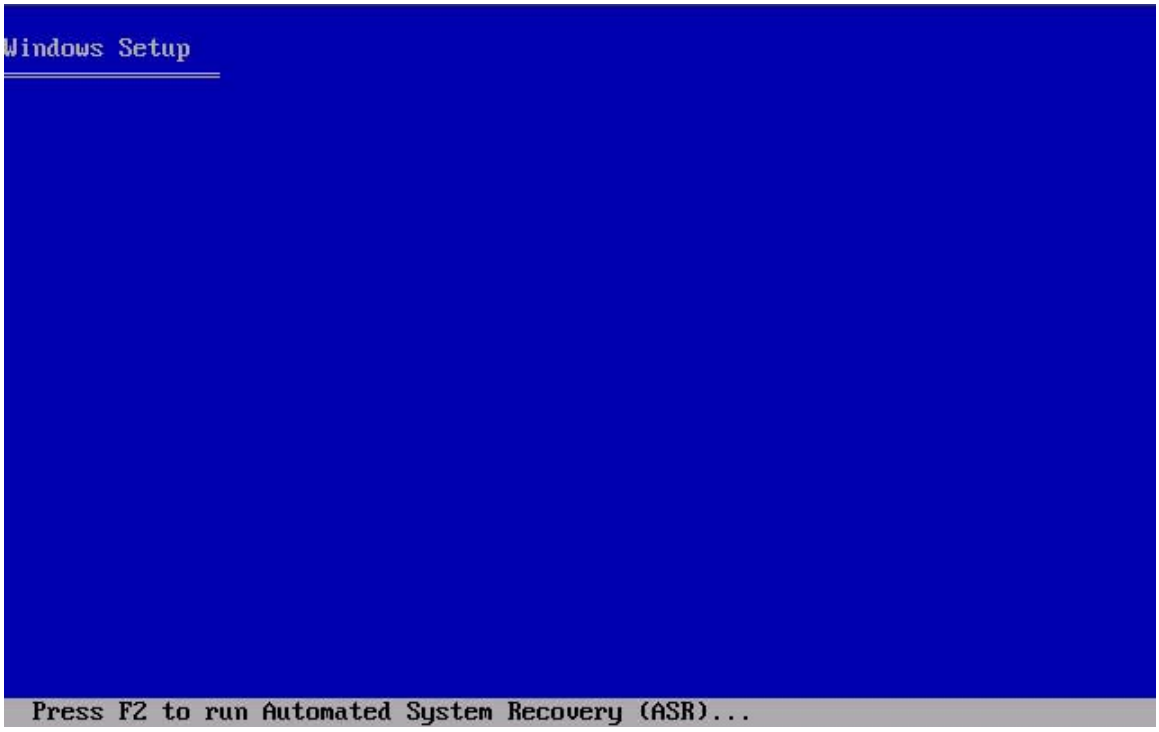
1. Đưa đĩa CD có bộ cài Windows Server 2003 vào trong ổ CD-ROM và khởi động lại máy. Nếu bạn nhận được thông báo "***press a key to boot from CD.***." – (nhấn phím bất kỳ để khởi động từ CD). nhấn một phím bất kỳ

2. Sau khi máy tính khởi động, một chuỗi các thông báo hiện ra nói rằng trình cài đặt đang xem xét các cấu hình phần cứng của máy tính. Sau đó màn hình Windows Setup xuất hiện

3. Nếu máy tính của bạn cần có các trình điều khiển thiết bị lưu trữ đặc biệt không có trong bộ cài của Windows Server 2003, nhấn F6 khi được nhắc và cung cấp các trình điều khiển thiết bị phù hợp.



4. Hệ thống sẽ nhắc bạn nhấn F2 nếu bạn muốn thực hiện thao tác Khôi phục Hệ thống Tự động (***Automated System Recovery - ASR***). Không nhấn F2 lúc này và quá trình cài đặt tiếp tục



LƯU Ý: Thủ tục Khôi phục hệ thống tự động (Automated System Recovery – ASR): *Là một tính năng mới trong Windows Server 2003 thay thế tính năng Đĩa Sửa chữa Khẩn cấp (Emergency Repair Disk)*

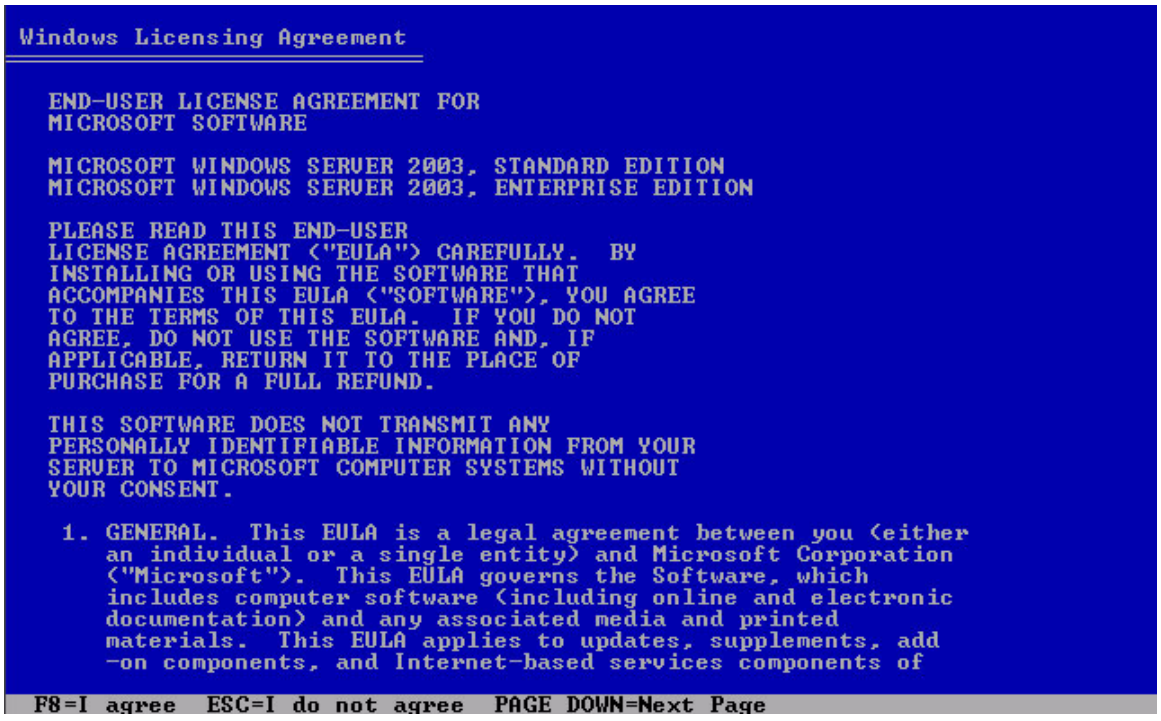
có trong các phiên bản trước của Windows. Muốn tìm thêm thông tin về ASR, xem Chương 4 của cuốn sách này.

Một thanh trạng thái ở phía dưới màn hình chỉ ra trình cài đặt đang nạp các file. Điều này là cần thiết để khởi động phiên bản tối giản của hệ điều hành. Vào lúc này, phần cứng của hệ thống chưa được nhận dạng chính xác, do đó sau khi nạp lớp nhân của hệ điều hành, trình cài đặt sẽ nạp một danh sách các trình điều khiển thiết bị hỗ trợ cho một lượng lớn các thiết bị lưu trữ, bàn phím, con trỏ chuột và thiết bị video, tất cả để tạo ra một cấu hình vào/ra chuẩn cho phép quá trình cài đặt có thể tiếp tục được.

LƯU Ý: Định vị các Trình điều khiển Thiết bị Lưu trữ. *Nếu một trình điều khiển của một thiết bị lưu trữ nào đó không nằm trong Windows Server 2003, bạn phải chuẩn bị nó, khởi động lại quá trình cài đặt và nhấn F6 để cung cấp chúng cho chương trình cài đặt.*

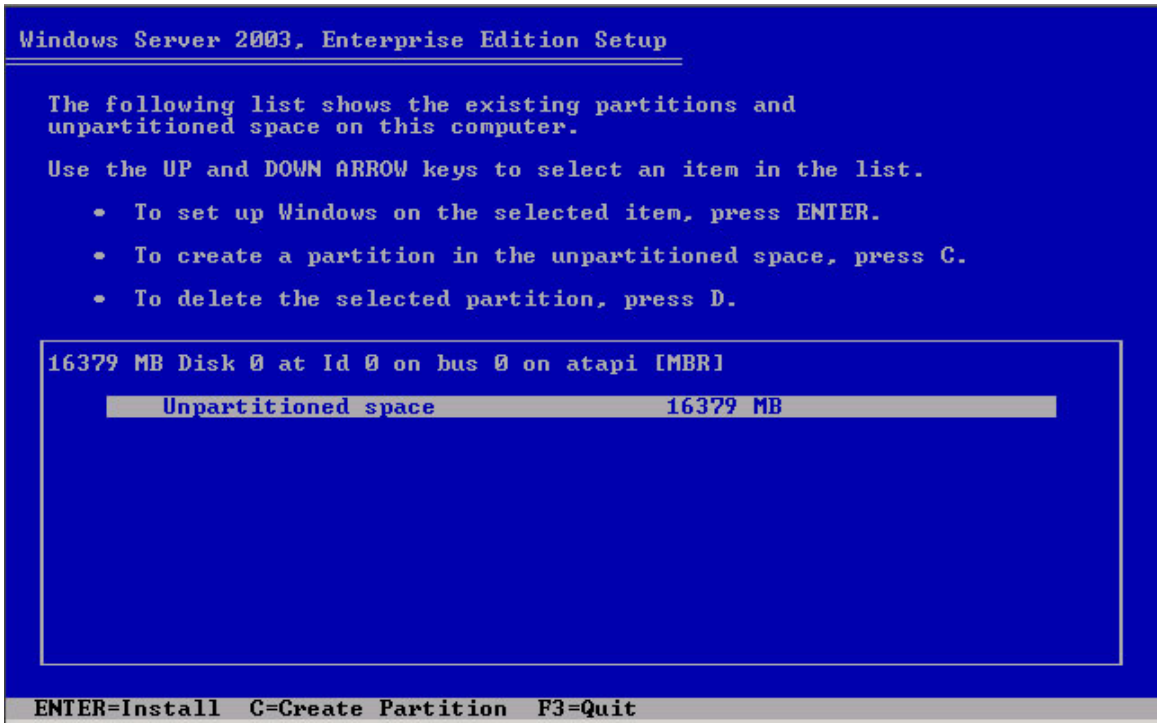
5. Nếu bạn đang cài đặt phiên bản thử nghiệm của Windows Server 2003, một màn hình nhắc nhở cài đặt (***Setup Notification***) sẽ thông báo cho bạn biết điều đó. Đọc thông báo này và nhấn ***Enter*** để tiếp tục. Màn hình ***Welcome To Setup*** (*Chào mừng bạn đên với trình cài đặt*) sẽ xuất hiện.

6. Đọc thông báo "***Welcome To Setup***" và nhấn ***Enter*** để tiếp tục, Màn hình ***License Agreement*** (*Thỏa thuận Bản quyền*) xuất hiện.



7. Đọc thỏa thuận về bản quyền và nhấn **F8** để chấp nhận. Một màn hình xuất hiện liệt kê một danh sách các phân vùng trên các ổ cứng trong máy tính cùng với các vùng không gian đĩa trống. Từ màn hình này, bạn có thể tạo và xóa các phân vùng trên các đĩa cứng nếu cần. Nếu bạn trỏ vào lựa

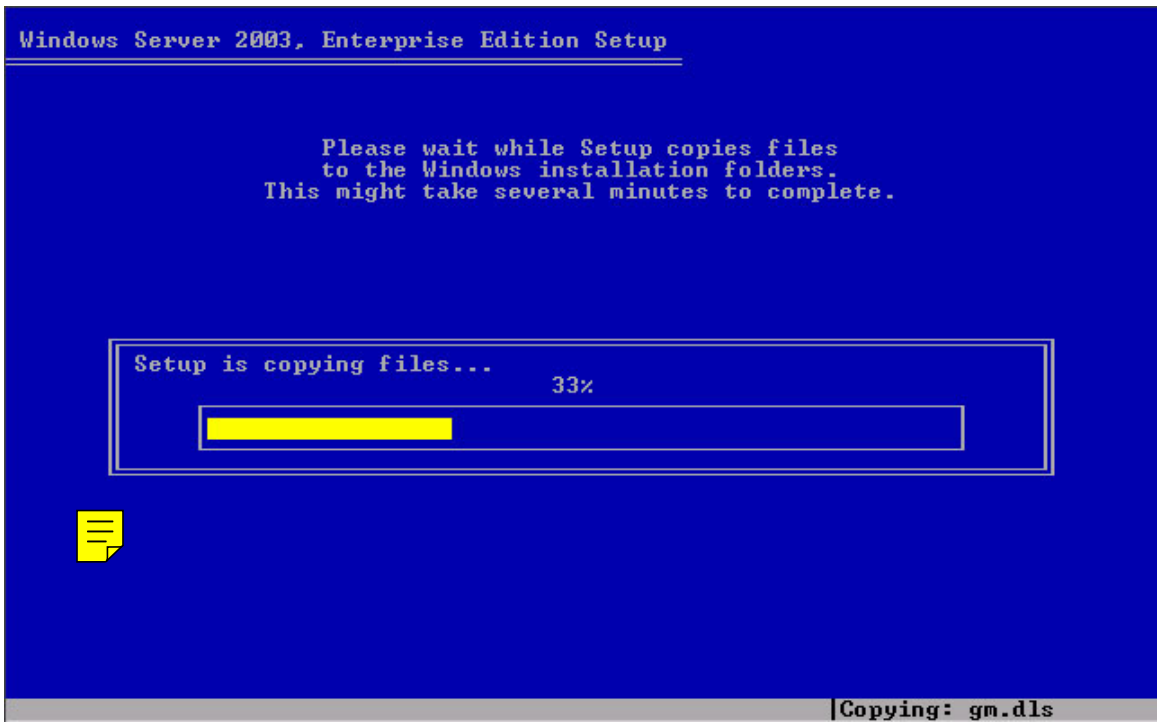
chọn "***Unpartitioned Space***" (*Không gian đĩa chưa phân vùng*), bạn có thể tạo một phân vùng trên toàn bộ không gian đĩa đó. Nếu bạn muốn tạo một phân vùng sử dụng một phần của không gian đĩa cứng chưa phân vùng đó, bạn nhấn phím C và nhập vào kích thước của phân vùng mà bạn muốn tạo. Để hoàn thành bài tập thực hành trong cuốn sách này, đề xuất nên sử dụng một phân vùng tối thiểu 3GB. Bên cạnh đó, bạn phải dành ra ít nhất 1GB không gian chưa phân vùng trên đĩa cứng để chuẩn bị cho các bài tập thực hành về việc tạo các phân vùng mới trong Windows 2003 sau này.



8. Lựa chọn một không gian đĩa chưa phân vùng có dung lượng tối thiểu 4GB và nhấn C, đồng thời nhập vào kích thước phân vùng định tạo là 3072. Sau đó nhấn ***Enter***

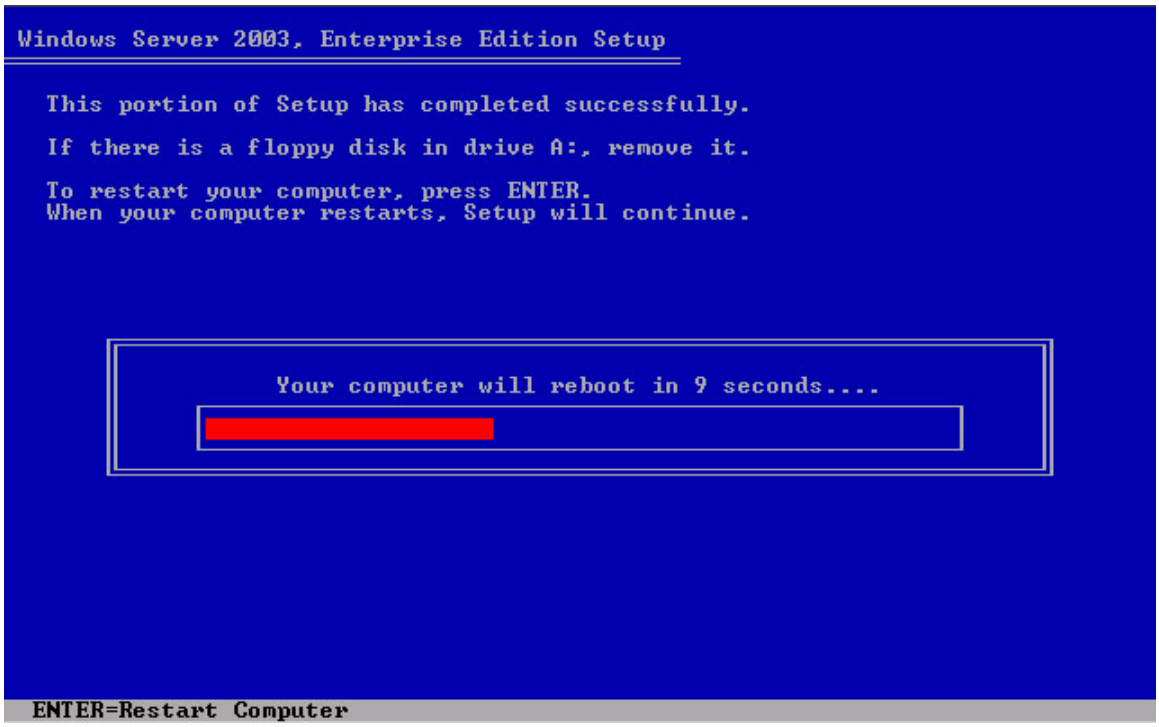
9. Một màn hình xuất hiện, nhắc bạn lựa chọn hệ thống file sử dụng khi định dạng phân vùng đã lựa chọn. Lựa chọn "***Format The Partition Using The NTFS File System***" (*Định dạng phân vùng sử dung hệ thống file NTFS*) và nhấn ***Enter***.

Trình cài đặt sẽ định dạng phân vùng sử dụng NTFS, kiểm tra các lỗi vật lý của đĩa cứng mà có thể gây ra sự cố khi cài đặt và bắt đầu chép các file từ đĩa CD vào trong đĩa cứng. Quá trình này có thể chiếm của bạn vài phút.



10.Trình cài đặt sẽ khởi tạo cấu hình của Windows và sau đó hiển thị lên màn hình một thanh trạng thái màu đỏ thể hiện số đếm giảm dần trong 15

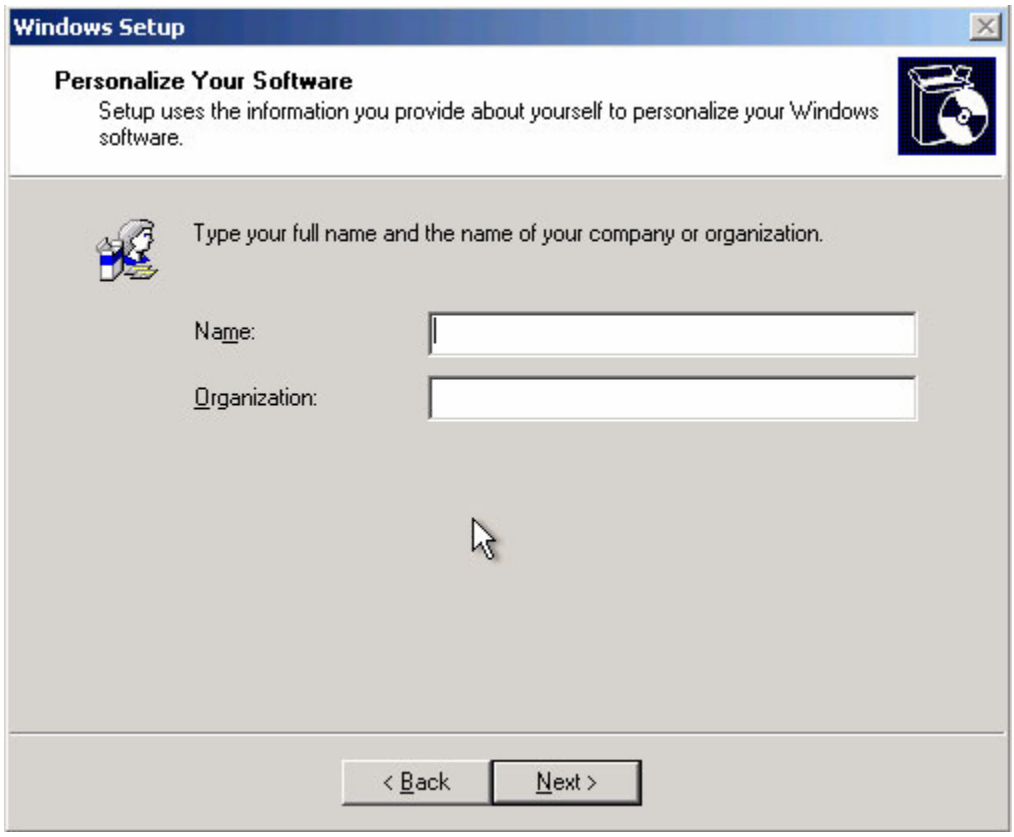
giây trước khi máy tính khởi động lại và chuyển sang chế độ đồ họa của quá trình cài đặt.



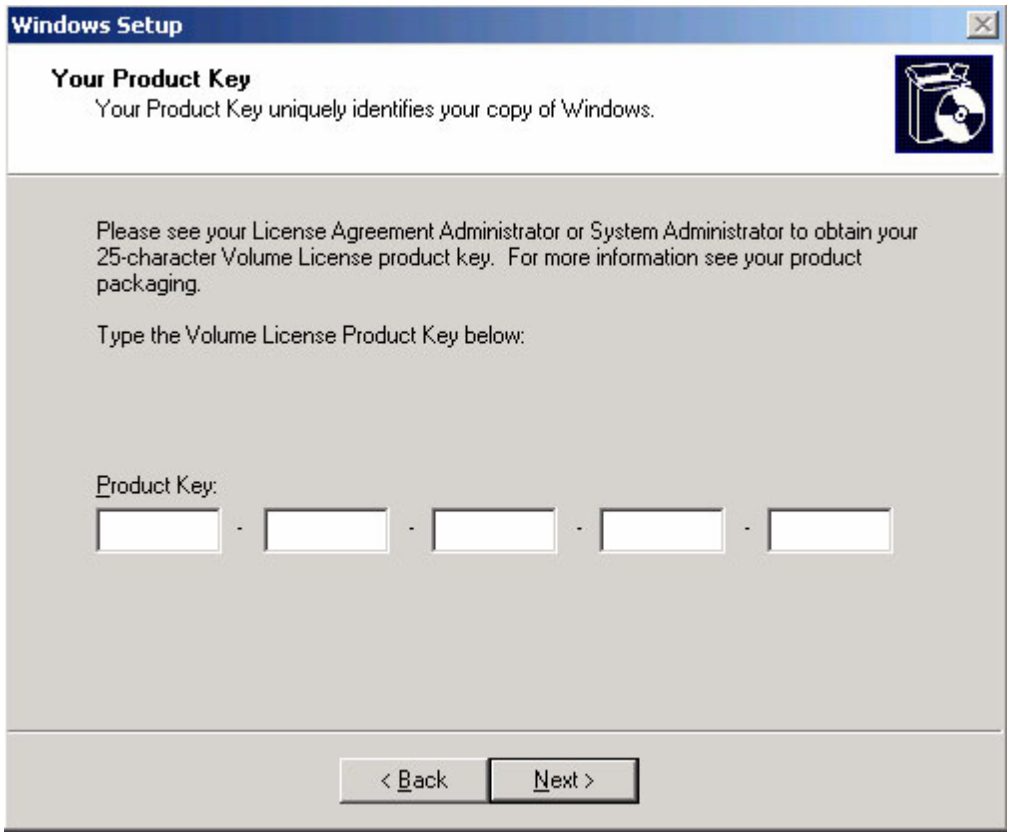
Trình cài đặt Windows sẽ nạp và hiển thị một giao diện đồ họa cho phép theo dõi các tiến trình cài đặt ở khung bên trái. Khi các tiến trình ***Collecting Information*** (*Thu thập thông tin*), ***Dynamic Update*** (*Cập nhật động*) và ***Preparing Installation*** (*Chuẩn bị cài đặt*) đều được lựa chọn, thể hiện rằng các bước này đã hoàn thành. Tiến trình ***Collecting Information*** (*Thu thập thông tin*) đã được hoàn thành trước khi giao diện đồ họa này xuất hiện và tiến trình ***Dynamic Update*** (*Cập nhật động*) không được thực hiện khi chúng ta cài đặt từ đĩa CD.

Tiến trình ***Preparing Installation*** (*Chuẩn bị cài đặt*) được thực hiện khi mà trình cài đặt đã chép xong các file vào đĩa cứng. Bước cài đặt Windows bắt đầu với quá trình phát hiện các phần cứng, quá trình này có thể diễn ra trong vài phút. Không giống như chu trình phát hiện phần cứng khi ở chế độ văn bản, trong đó nó nhận biết phần cứng bằng việc nạp các trình điều khiển và sử dụng thử rồi phát hiện lỗi, quá trình này nhận biết chính xác các thành phần trong máy tính, ghi thông tin về chúng vào ***registry***, đồng thời cấu hình sao cho hệ điều hành nạp các trình điều khiển chuẩn cho phần cứng đó. Sau cùng ***Windows Setup Wizard*** (*Trình Hướng dẫn Cài đặt Windows*) sẽ được nạp và trang "***Regional And Language Options***" (*Tùy chọn vùng và ngôn ngữ*) xuất hiện.

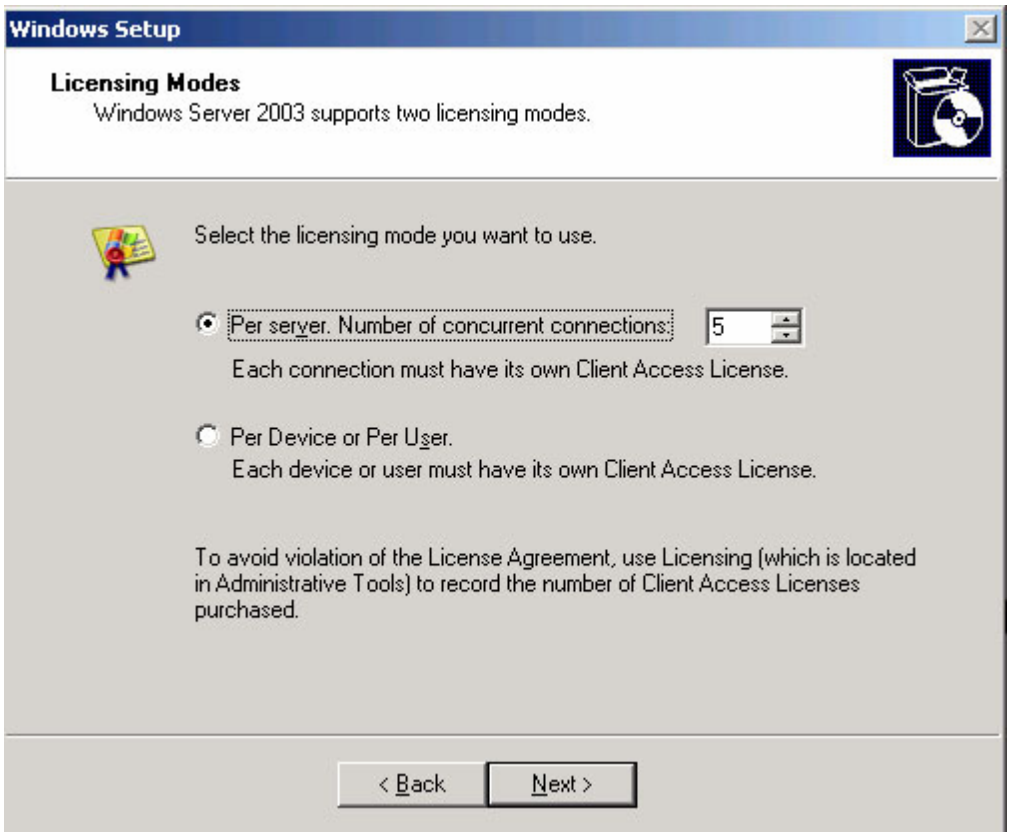
11. Chỉnh sửa các thiết lập mặc định về vùng và ngôn ngữ nếu cần thiết, bằng cách nhấn chuột vào phím ***Customize*** hoặc ***Details***. Sau đó nhấn ***Next***. Trang ***Personalize Your Software*** (*Tùy biến phần mềm của bạn*) xuất hiện.



12. Trong hộp thoại ***Name***, nhập vào tên của bạn và trong hộp thoại ***Organization***, nhập vào tên của cơ quan rồi nhấn ***Next***. Trang "***Your Product Key***" (*Khóa sản phẩm của bạn*) xuất hiện.

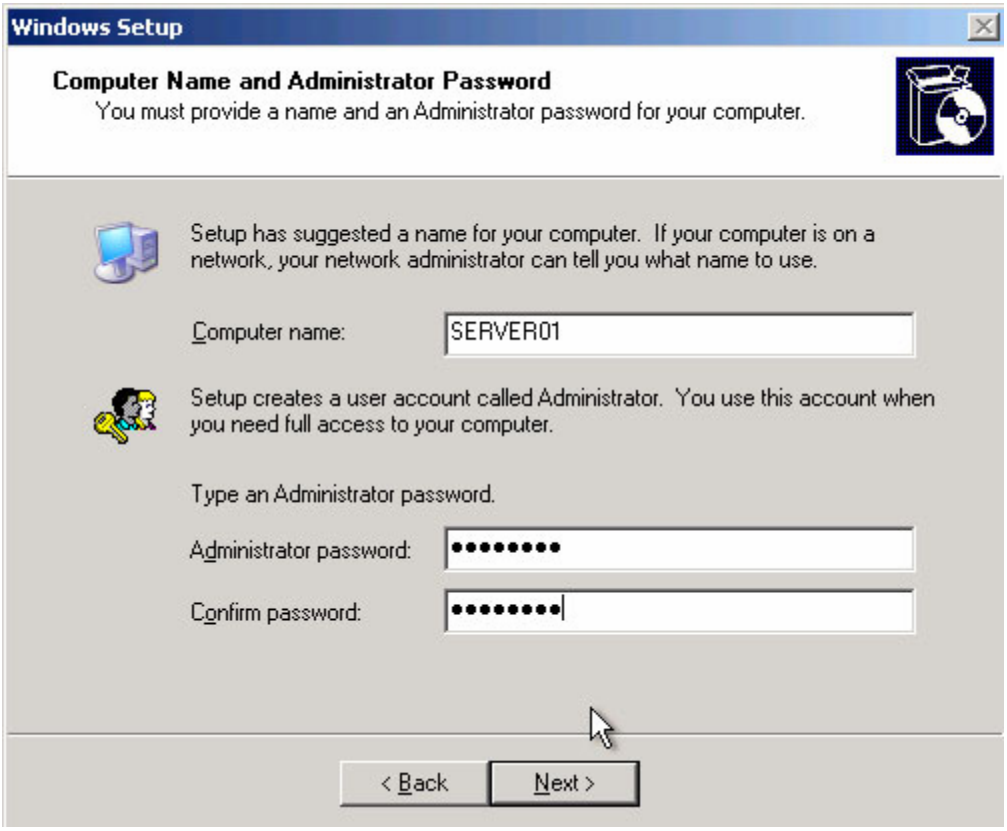


13. Nhập vào các hộp thoại ***Product Key*** các thông số khóa của sản phẩm đi kèm trong đĩa CD Windows Server 2003 và nhấn ***Next***. Trang "***Licensing Modes***" - (*Các chế độ giấy phép*) xuất hiện



14.Giữ nguyên giá trị mặc định là 5 ở trong mục "***Per Server Number Of Concurrent Connections***" (*Số lượng các kết nối đồng thời trên 1 máy chủ*) và nhấn ***Next.*** Trang "***Computer Name And Administrator Password***" - (*Tên máy tính và mật khẩu quản trị*) xuất hiện.

> ***LƯU Ý: Bản quyền Windows Server 2003.*** *Nếu bạn sử dụng phiên bản thử nghiệm của Windows Server 2003, giá trị mặc định 5 kết nối đồng thời tới máy chủ là đủ để hoàn thành khóa học này. Tuy nhiên, nếu bạn sử dụng một bản Windows Server 2003 có bản quyền, bạn nên nhập vào một số lượng hợp lệ các kết nối đồng thời dựa trên Giấy phép (**license**) mà bạn có.*

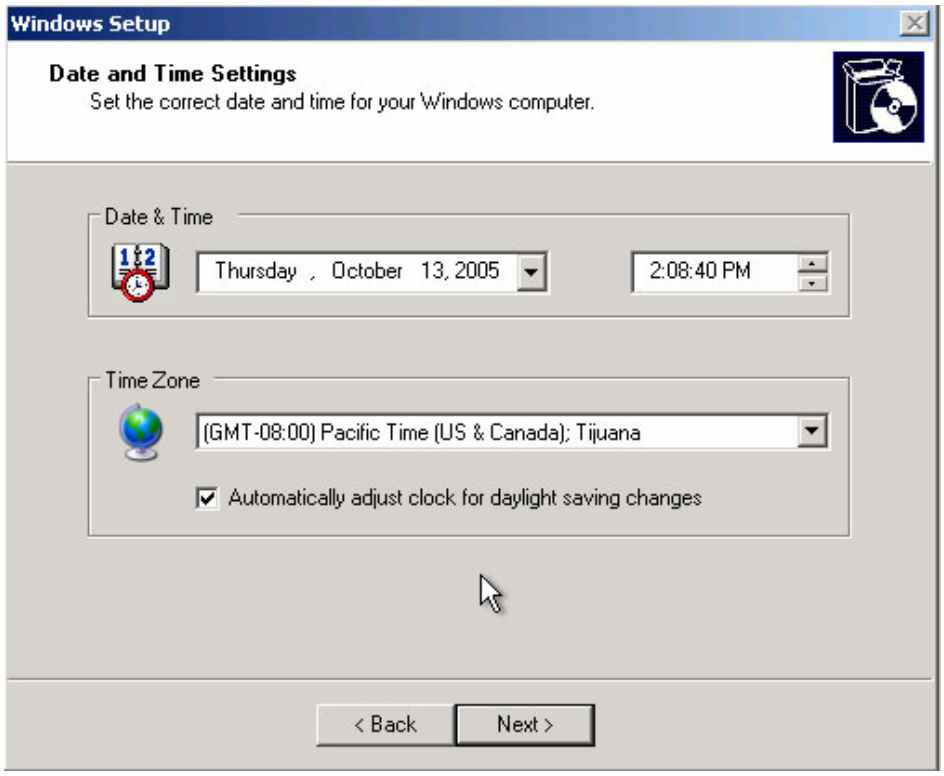


15.Trong hộp thoại ***Computer Name***, nhập vào ***Serverxx*** trong đó ***xx*** là số thứ tự duy nhất mà giảng viên cung cấp cho bạn.

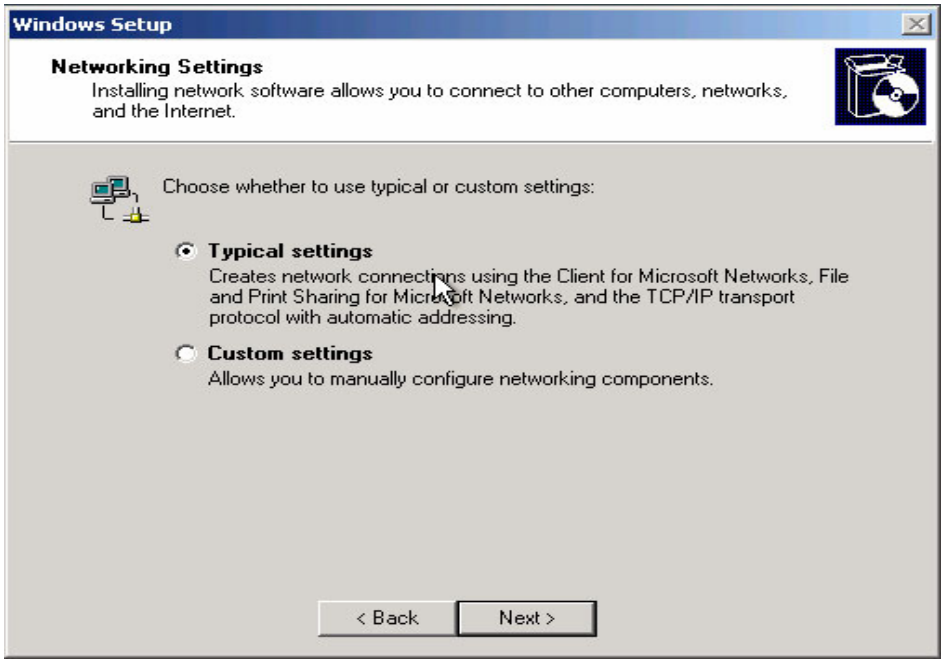
> ***CẢNH BÁO: Tránh tình trạng trùng tên***. *Nếu máy tính của bạn kết nối vào mạng LAN, kiểm tra với quản trị mạng trước khi nhập vào tên cho máy tính của bạn*

16.Trong hộp thoại "***Administrator Password và Confirm Password***", nhập mật khẩu cho tài khoản ***Administrator*** và sau đó nhấn ***Next***. Trang "***Date And Time Settings***" (*Thiết lập ngày giờ*) xuất hiện.

> ***QUAN TRỌNG: Xác định mật khẩu***. *Đối với phương thức cài đặt thủ công, Windows Server 2003 sẽ không cho phép bạn chuyển tới bước tiếp theo cho đến khi bạn nhập vào mật khẩu cho tài khoản* ***Administrator*** *thỏa mãn các yêu cầu phức hợp. Theo mặc định, Windows Server 2003 yêu cầu một mật khẩu phức hợp phải có độ dài tối thiểu 7 ký tự, đồng thời chứa tối thiểu 3 trong 4 thành phần sau: ký tự hoa, ký tự thường, chữ số và ký tự đặc biệt. Bạn được phép sử dụng mật khẩu trống, tuy nhiên việc sử dụng mật khẩu trống là không được khuyến khích*

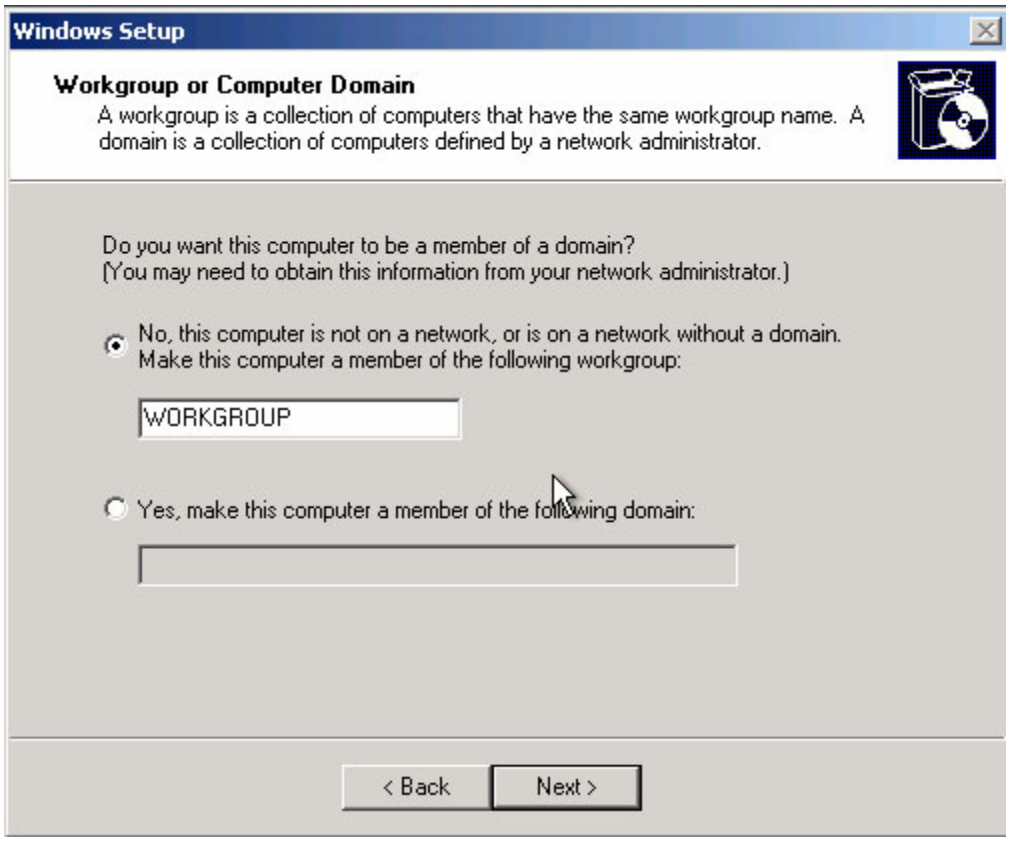


17.Nhập vào thời gian và ngày tháng chính xác đồng thời lựa chọn múi giờ chuẩn cho khu vực của bạn. Sau đó nhận ***Next***, màn hình "***Network Settings***" (*Thiết lập mạng*) xuất hiện



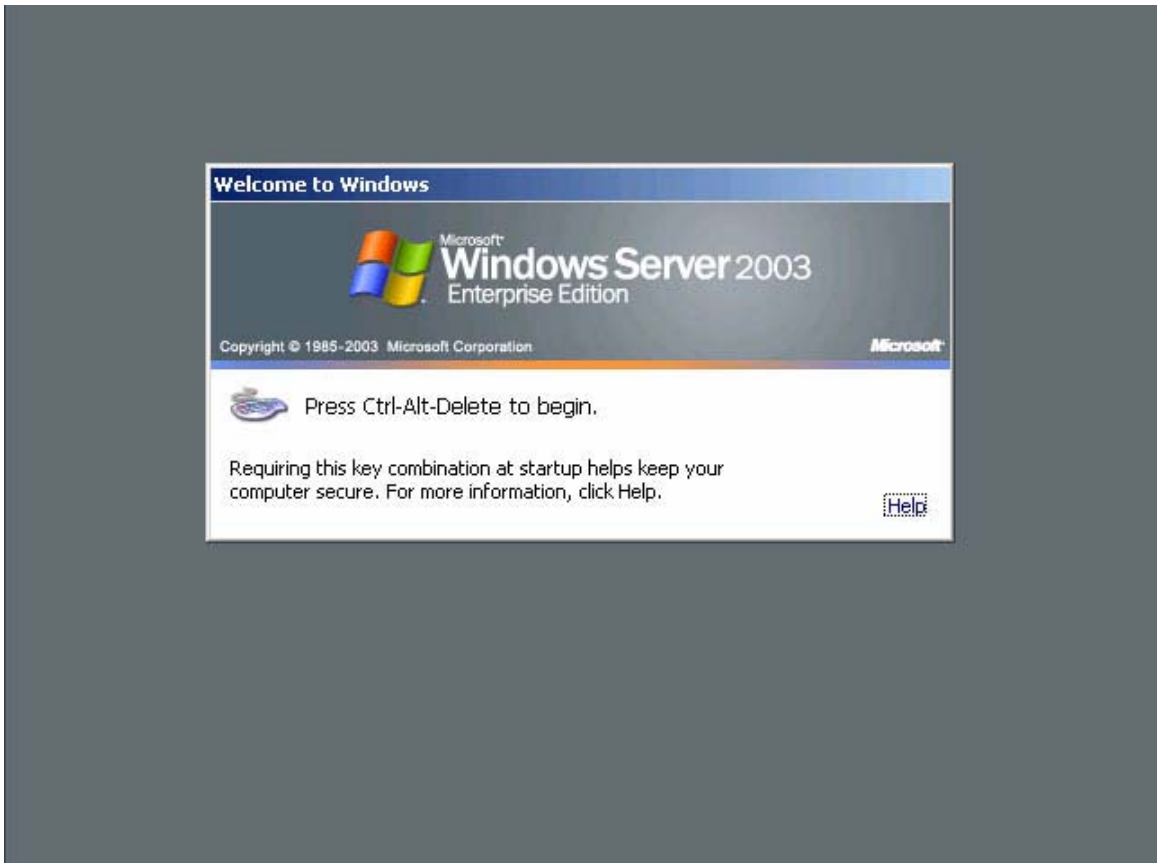
18.Giữ nguyên lựa chọn mặc định "***Typical Settings***" và sau đó nhấn ***Next***. Trang "***Workgroup Or Computer Domain***" (*Gia nhập miền hoặc nhóm*) xuất hiện.

LƯU Ý: Các thiết lập mạng điển hình. *Lựa chọn "Typical Settings" trong trang "Network Settings" sẽ cho phép trình cài đặt thực hiện cài đặt các thành phần sau: "Client for Microsoft Networks", "Network Load Balancing", "File and Printer Sharing for Microsoft Networks" và "Internet Protocol (TCP/IP)" (mặc dù module "Network Load Balancing" bị vô hiệu hóa) đồng thời cấu hình TCP/IP cho phép nhận địa chỉ IP từ một máy chủ DHCP. Nếu bạn kết nối với một hệ thống mạng không có máy chủ DHCP, bạn phải xác định địa chỉ IP và các thiết lập cấu hình TCP/IP khác thông qua người quản trị mạng, đồng thời lựa chọn "Custom Settings" và nhập các tham số này vào để cho máy tính của bạn có khả năng kết nối với các máy khác trong mạng LAN.*



19.Giữ nguyên lựa chọn mặc định "***No***" và tên nhóm mặc định là "***WORKGROUP***" và nhấn ***Next***.

Trình cài đặt sẽ cài và thiết lập các thành phần còn lại của hệ điều hành bằng cách chép các file, cài đặt thực đơn ***Start***, đăng kí các thành phần, lưu các thiết lập và xóa các file tạm. Sau đó quá trình cài đặt kết thúc, máy tính tự khởi động và màn hình "***Welcome To Windows***" (*Chào mừng bạn đến với Windows*) xuất hiện.



Trong môi trường kinh doanh, ví dụ như một mạng doanh nghiệp lớn, quá trình cài đặt hệ điều hành thường sẽ được thục hiện khác so với các thao tác ở trên. Người quản trị mạng của một công ty lớn với rất nhiều máy tính thường không có thời gian để thực hiện quá trình cài đặt thủ công và kéo dài như trên đối với từng máy tính. Họ có thể sử dụng rất nhiều phương án để thực hiện theo phương thức dây chuyền hoặc tự động hóa quá trình cài đặt Windows Server 2003, bao gồm các phương pháp sau đây:

- ***File trả lời:***

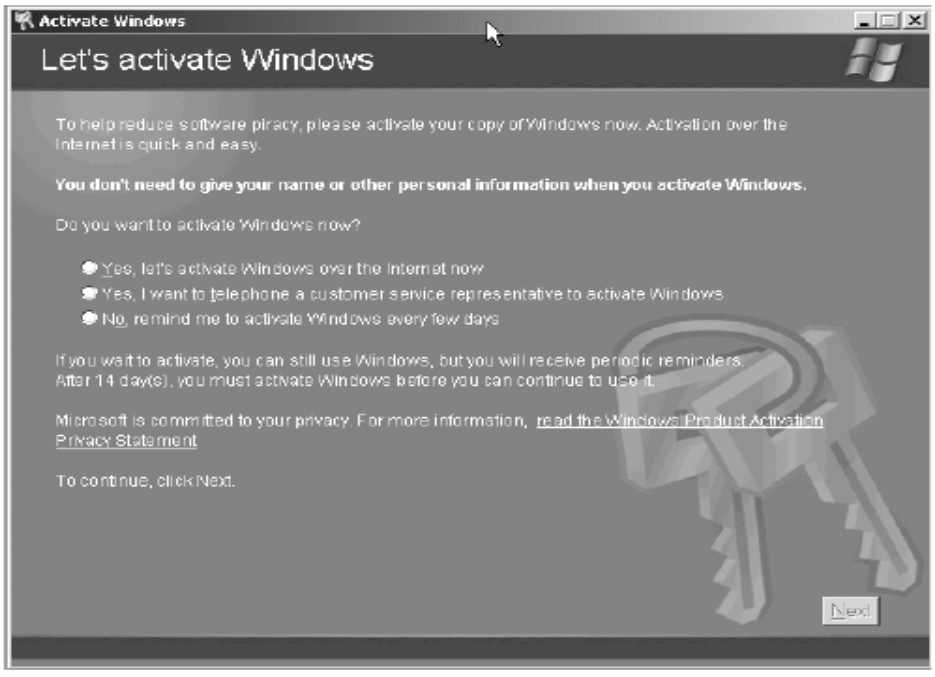
Một file trả lời là một ***script*** (kịch bản) chứa các giá trị thiết lập của tất cả các tùy chọn hiển thị cho người dùng trong quá trình cài đặt Windows như ở trên. Với một file trả lời được cấu hình tốt, ta có thể bắt đầu quá trình cài đặt hệ thống và để nó chạy mà không cần phải tác động gì bởi các tham số trả lời cho các câu hỏi trong quá trình cài đặt đã có trong file trả lời. Điều hạn chế lớn nhất của phương pháp triển khai cài đặt hệ điều hành sử dụng file trả lời là mỗi máy tính cần một file trả lời riêng. Một số giá trị thiết lập trong quá trình cài đặt phải là duy nhất, ví dụ như tên máy tính hoặc địa chỉ IP.

- ***Nhân ảnh đĩa.***

Khi bạn triển khai cài đặt một số lượng lớn các máy tính giống nhau, bạn có thể bỏ qua các quá trình cài đặt này bằng cách sử dụng ảnh đĩa. Một ảnh đĩa là một bản sao bit-to-bit của đĩa cứng trong máy tính mà đã được cài đặt hệ điều hành. Việc chuyển ảnh đĩa này sang một máy tính khác có cấu hình phần cứng tương tự cho phép hệ điều hành có thể chạy trên máy tính đó mà không phải cài đặt lại. Windows Server 2003 có cung cấp kèm theo một công cụ gọi là ***Remote Installation Services*** (*Dịch vụ cài đặt từ xa*) cho phép người quản trị mạng có thể sử dụng để triển khai các ảnh đĩa đến các máy tính qua đường truyền mạng.

Kích hoạt (Activate) Windows Server:

Một số phiên bản của Windows Server 2003, bao gồm cả bản thử nghiệm cung cấp kèm theo trong cuốn sách này, yêu cầu bạn phải kích hoạt (***activate***) hệ điều hành sau khi cài đặt. Tùy thuộc vào phiên bản mà bạn đang sử dụng, bạn có thể có 14 hoặc 30 ngày để kích hoạt Windows Server 2003. Kích hoạt là một quá trình rất đơn giản, chỉ thực hiện 1 lần bằng cách nhấn ***Start***, chọn ***All Programs*** và nhấn vào ***Activate Windows***. Trang màn hình "***Let's Activate Windows***" (*Hãy kích hoạt Windows*) trong Trình Hướng dẫn Kích hoạt Windows – "***Activate Windows Wizard***" xuất hiện (như trong Hình 1-1)



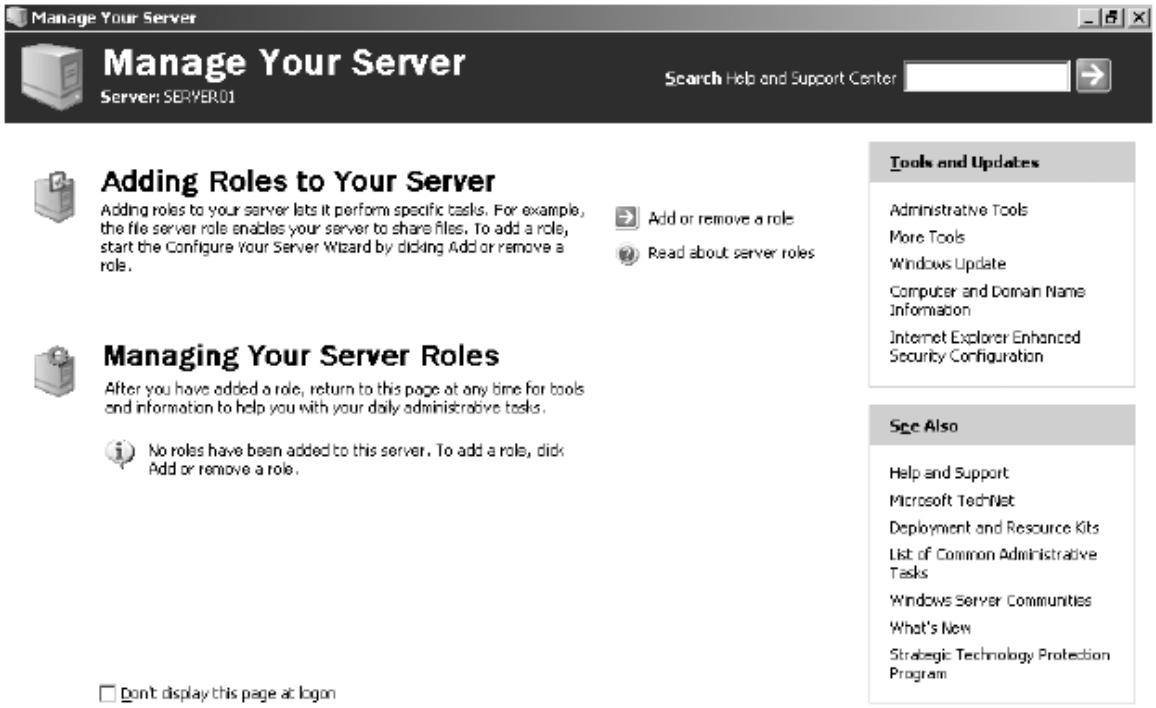
Hình 1-1: Trang *Let's Activate Windows* trong Trình Hướng dẫn Kích hoạt Windows

> ***LƯU Ý: Volume Licensing (Giấy phép khối)***. *Nếu bạn có được bản quyền Windows Server 2003 thông qua một chương trình Microsoft volume licensing nào đó, bạn sẽ không phải kích hoạt bản quyền này.*

Để kích hoạt Windows qua Internet, bạn phải kết nối máy tính với Internet trước khi bạn có thể bắt đầu quá trình kích hoạt. Điều này có nghĩa là máy tính được trang bị một modem và cấu hình để kết nối đến một nhà cung cấp dịch vụ (ISP) hoặc cấu hình với một vài tham số TCP/IP (bao gồm địa chỉ IP, Mặt nạ mạng con (***Subnet Mask***), máy chủ DNS và cổng ra (***gateway)*** mặc định) rồi kết nối đến mạng LAN mà có đường ra Internet. Nếu máy tính không thể truy nhập Internet, bạn phải kích hoạt Windows bằng điện thoại

CẤU HÌNH WINDOWS SERVER 2003

Sau khi cài đặt và kích hoạt Windows, bạn có thể cấu hình máy chủ bằng cách sử dụng trang ***Manage Your Server*** (*Cấu hình Máy chủ Của bạn*), như trong Hình 1-2. Trang này được nạp sau khi bạn đăng nhập, hoặc bạn có thể nạp nó bất kì lúc nào bằng cách lựa chọn ***Manage Your Server*** trong thực đơn ***Start***. Trang này cho phép bạn cài đặt một số dịch vụ, công cụ đặc biệt và cấu hình dựa vào vai trò mà máy chủ này thực hiện.



Hình 1-2: Trang Manage Your Server

Khi bạn nhấn vào liên kết "***Add Or Remove A Role***" (*Thêm hoặc bớt vai trò*), trình hướng dẫn cấu hình máy chủ ("***Configure Your Server Wizard***")

hiện ra. Sau khi quét tìm kiếm thông tin về các kết nối mạng, trình hướng dẫn này cho phép bạn có thể lựa chọn một trong những vai trò sau:

- **Máy chủ File:** Cung cấp khả năng truy nhập đến file và thư mục một cách tập trung cho từng người dùng, phòng ban và toàn bộ tổ chức. Lựa chọn vai trò này cho phép bạn quản lý không gian đĩa cứng bằng cách kích hoạt và cấu hình ***disk quota*** (*Hạn ngạch đĩa cứng*) và nâng cao hiệu quả tìm kiếm hệ thống file bằng cách sử dụng ***Indexing Services*** (*Dịch vụ chỉ mục*)
- **Máy chủ in ấn:** Cung cấp khả năng truy nhập đến các thiết bị in ấn một cách tập trung và có quản lý. Máy chủ in ấn sẽ sử dụng một máy in chung và trình điều khiển thiết bị in để phục vụ cho người dùng trên các máy trạm. Lựa chọn vai trò này sẽ khởi động ***Add Printer Wizard*** (*Trình hướng dẫn cài đặt máy in*), cho phép bạn có thể cài đặt các máy in và các trình điều khiển thiết bị in tương ứng của Windows. Lựa chọn vai trò máy chủ in ấn sẽ đồng thời cài đặt IIS 6, cấu hình ***Internet Printing Protocol*** (*Giao thức in ấn qua Internet* – IPP) và cài đặt các công cụ quản trị máy in trên nền Web
- **Máy chủ ứng dụng (IIS, ASP.NET):** Cung cấp các thành phần cơ bản để có thể hỗ trợ các ứng dụng Web. Việc lựa chọn thực hiện vai trò này sẽ cài đặt và cấu hình IIS 6 cùng với Microsoft ASP.NET và COM+ lên máy chủ.
- **Máy chủ thư điện tử (POP3, SMTP):** Cài đặt các giao thức ***Post Office Protocol version 3 -*** **(POP3)** và ***Simple Mail Transfer Protocol*** - (**SMTP**) cho phép máy chủ có thể thực hiện chức năng của một máy chủ quản lý thư điện tử vào và ra cho các người dùng trên mạng.
- **Máy chủ Terminal:** Cung cấp cho các máy khách khả năng truy nhập đến các ứng dụng và tài nguyên trên máy chủ như là các ứng dụng và tài nguyên này được cài đặt trên chính các máy trạm. Người dùng kết nối đến máy chủ này bằng cách sử dụng các chương trình ***Terminal Services client*** (*Máy khách Chạy dịch vụ Đầu cuối truy nhập từ xa*) hoặc ***Remote Desktop client (****Máy khách Truy nhập toàn màn hình từ xa****)***
- **Máy chủ VPN/Truy nhập từ xa:** Cung cấp các dịch vụ truy nhập từ xa và định tuyến đa giao thức cho các kết nối quay số, LAN và WAN. Kết nối ***Virtual private network*** (*Mạng riêng ảo* - VPN) cho phép người dùng và các chi nhánh ở xa có thể kết nối đến một cách bảo mật

mà không tốn nhiều chi phí, sử dụng Internet như là phương thức truyền thông.

- **Máy chủ quản trị miền** - Máy chủ quản trị miền sử dụng ***Active Directory*** cung cấp dịch vụ thư mục cho các máy khách trong mạng. Lựa chọn này sẽ khởi động "***Active Directory Installation Wizard***" (*Trình hướng dẫn cài đặt Active Directory*) và cho phép bạn cấu hình máy chủ thực hiện chức năng của một máy chủ quản trị miền cho một miền mới hoặc miền sẵn có và nếu như chưa có máy chủ DNS nào trong mạng, trình cài đặt này sẽ cài đặt dịch vụ ***Microsoft DNS Server***
- **Máy chủ DNS:** Cung cấp khả năng phân giải tên bằng cách phân giải từ tên máy sang địa chỉ IP (phân giải xuôi - ***forward lookups***) và từ địa chỉ IP sang tên máy chủ (phân giải ngược - ***reverse lookups***). Việc lựa chọn vài trò này sẽ cài đặt dịch vụ ***Microsoft DNS Server*** và sau đó khởi động ***Configure A DNS Server Wizard*** (*Trình hướng dẫn cấu hình máy chủ DNS*)
- **Máy chủ DHCP:** Cung cấp dịch vụ cấp địa chỉ IP tự động cho các máy trạm (Các máy trạm này phải cấu hình sử dụng IP động). Việc lựa chọn vai trò này sẽ cài đặt dịch vụ ***DHCP Server*** và khởi động trình hướng dẫn "***New Scope Wizard***" (*Trình Hướng dẫn tạo Phạm vi DHCP mới*) cho phép bạn có thể định nghĩa một hoặc nhiều dải địa chỉ IP trong mạng
- **Máy chủ Streaming Media.** Việc lựa chọn vai trò này sẽ cài đặt dịch vụ ***Windows Media Services*** – WMS, cho phép máy chủ có thể cung cấp các dữ liệu nội dung phim ảnh đa phương tiện (***stream multimedia content***) qua kết nối mạng nội bộ hoặc Internet. Nội dung này có thể được lưu trữ và cung cấp cho người dùng theo yêu cầu hoặc truyền theo thời gian thực.
- **Máy chủ WINS:** Cung cấp khả năng phân giải tên máy tính bằng cách phân giải các tên NetBIOS sang địa chỉ IP. Không cần thiết phải cài đặt dịch vụ WINS trừ khi bạn muốn hỗ trợ các hệ điều hành trước đây như Windows 95 và Windows NT, các hệ điều hành này dựa trên cách sử dụng tên máy kiểu NetBIOS. Các hệ điều hành mới như Windows Server 2003, Windows 2000 và Windows XP không yêu cầu dịch vụ WINS mặc dù các các ứng dụng kiểu cũ trên các hệ điều hành này có thể yêu cầu việc phân giải tên NetBIOS. Việc lựa chọn vai trò này sẽ cài đặt dịch vụ WINS.

TẠO MÁY CHỦ QUẢN TRỊ MIỀN

Để hoàn thành bài tập thực hành trong sách này và trong cuốn Lab Manual, bạn phải có một máy tính cài đặt Windows Server 2003 và được cấu hình như một máy chủ quản trị miền.

Cài đặt Active Directory:

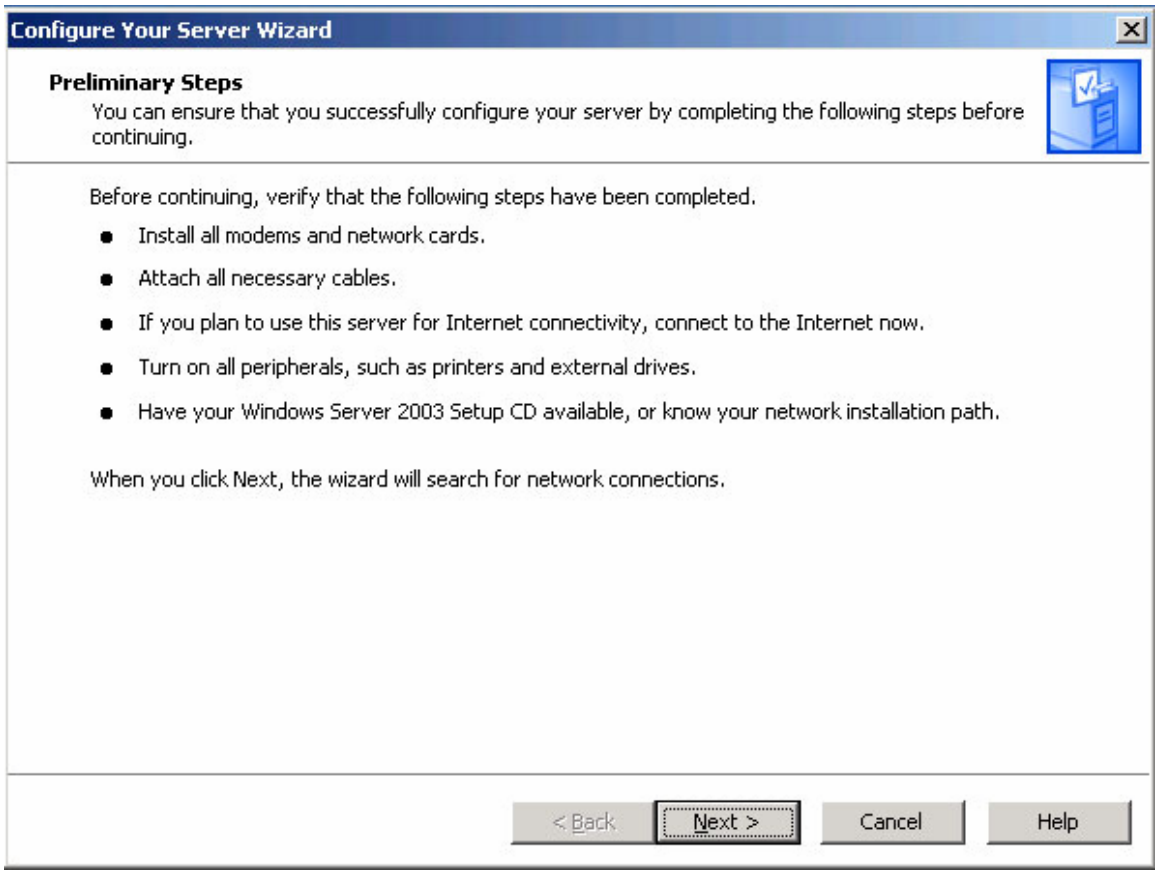
Để cấu hình máy ***Serverxx*** của bạn thực hiện chức năng của một máy chủ quản trị miền, sử dụng các thao tác sau đây:

> ***LƯU Ý: Các lựa chọn khi cài đặt Active Directory.*** *Khi trình hướng dẫn cài đặt Active Directory chạy, các lời nhắc hiện ra có thể khác nhau tùy vào việc nó phát hiện trong hệ thống mạng đã có máy chủ quản trị miền nào hay không. Nếu bạn kết nối máy tính đến một mạng có một miền khác, các bước có thể thay đổi và bạn có thể phải điều chỉnh lại các lựa chọn hoặc ngắt kết nối ra khỏi mạng trước khi làm bài tập thực hành này.*

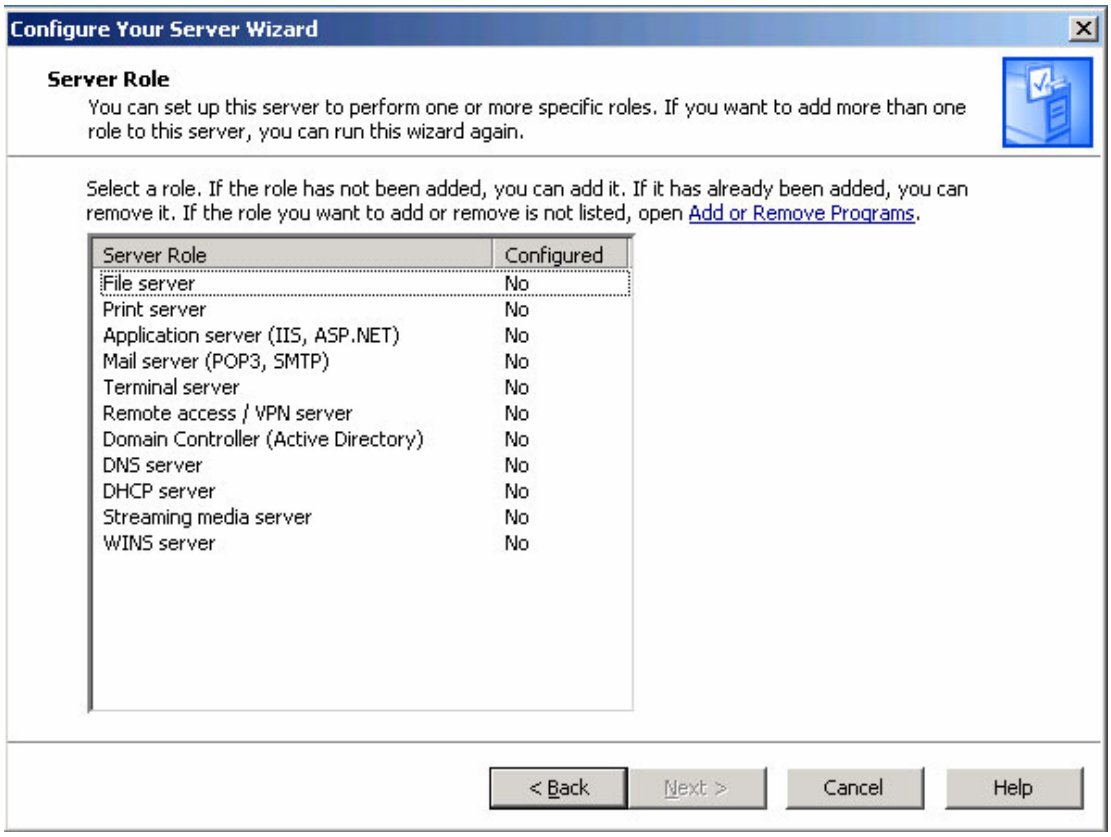
1. Đăng nhập vào máy tính Windows Server 2003 bằng tài khoản ***Administrator***

2. Nếu trang "***Manage Your Server***" (*Quản trị máy chủ của bạn*) không mở, bạn có thể mở nó từ thực đơn nhóm chương trình ***Administrative Tools***

3. Nhấn vào liên kết "***Add Or Remove A Role***" (*Thêm hoặc bớt vai trò*). Trình hướng dẫn cấu hình máy chủ ("***Configure Your Server Wizard***") được nạp và trang ***Preliminary Steps*** (*Các bước khởi đầu*) xuất hiện.



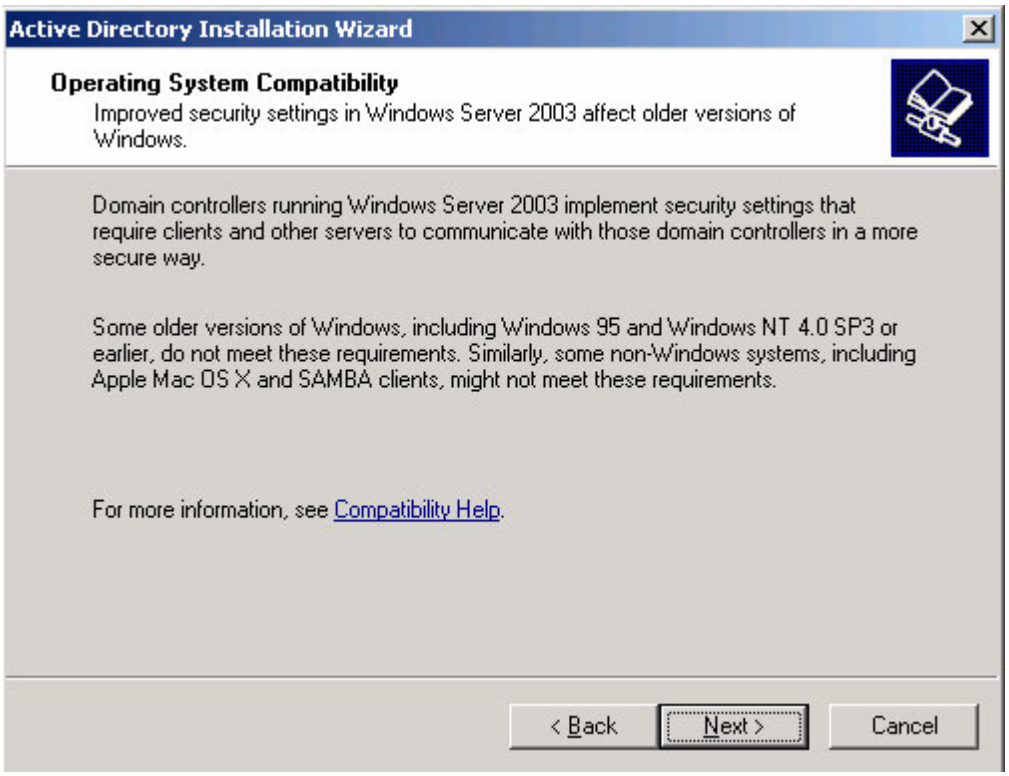
4. Xác nhận rằng các bước liệt kê trong trang này đã được hoàn thành và sau đó nhấn ***Next.*** Sau một khoảng thời gian chờ khi trình này quét và kiểm tra trên mạng, trang ***Server Role*** (*Vai trò máy chủ*) xuất hiện.



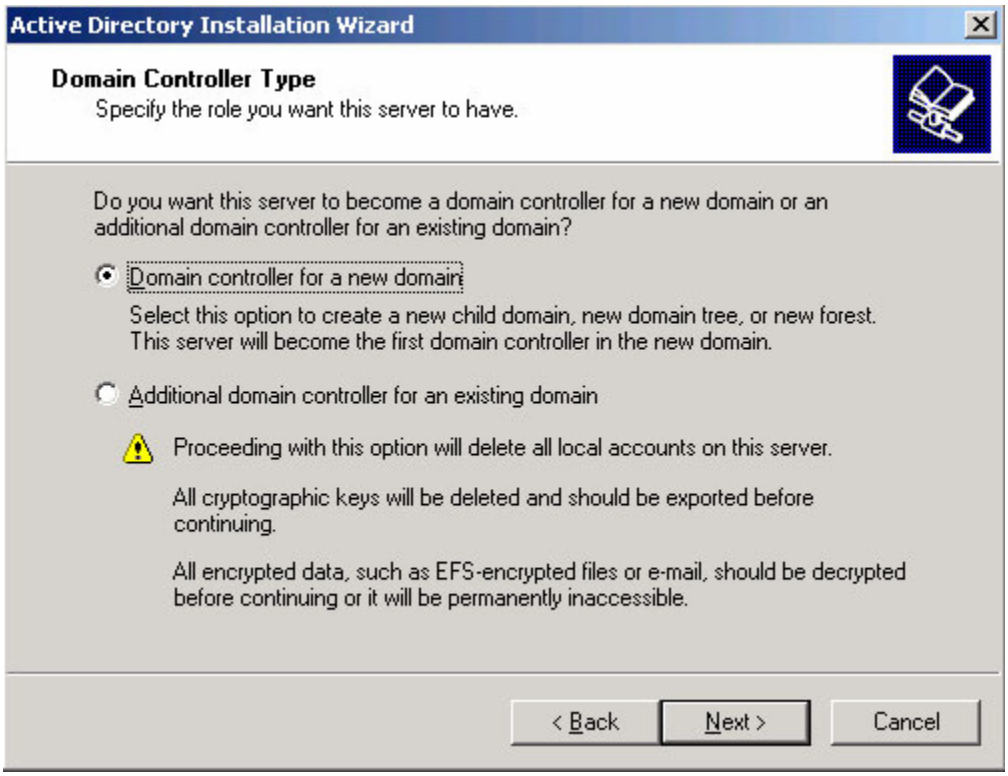
5. Lựa chọn ***Domain Controller (Active Directory)*** từ danh sách các vai trò máy chủ và nhấn ***Next***. Trang ***Summary Of Selections*** hiện ra.

6. Nhấn ***Next.*** Trình hướng dẫn cài đặt "***Active Directory Installation Wizard***" được nạp.

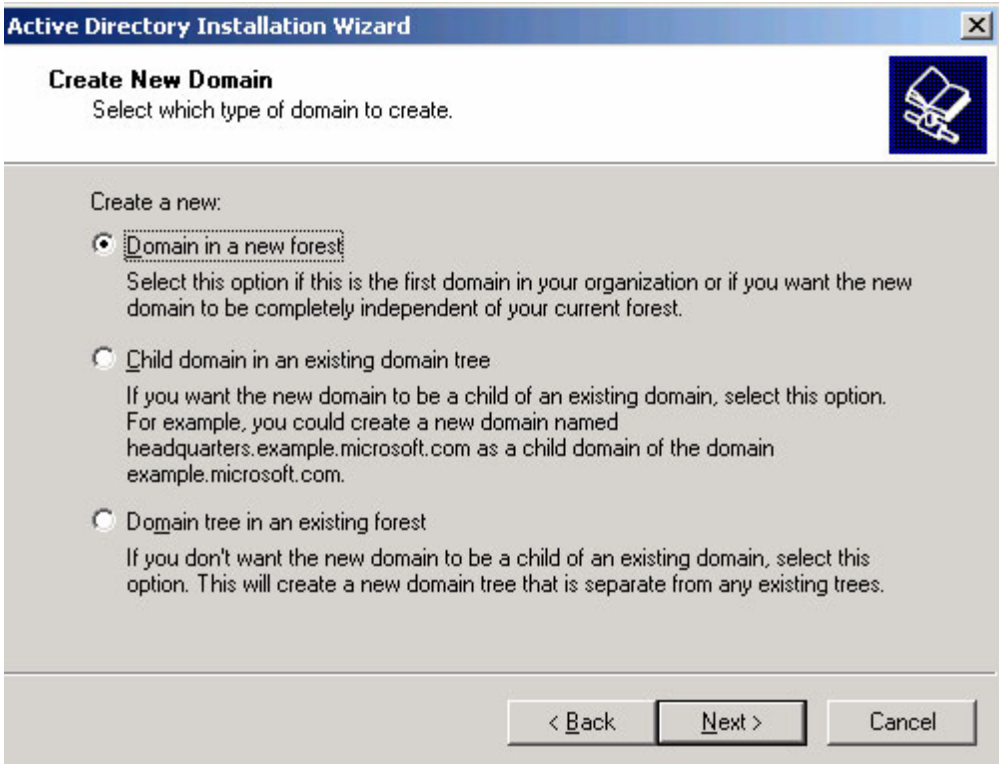
7. Nhấn ***Next*** để bỏ qua trang ***Welcome***. Trang ***System Compatibility*** (*Tính tương thích hệ thống*) xuất hiện



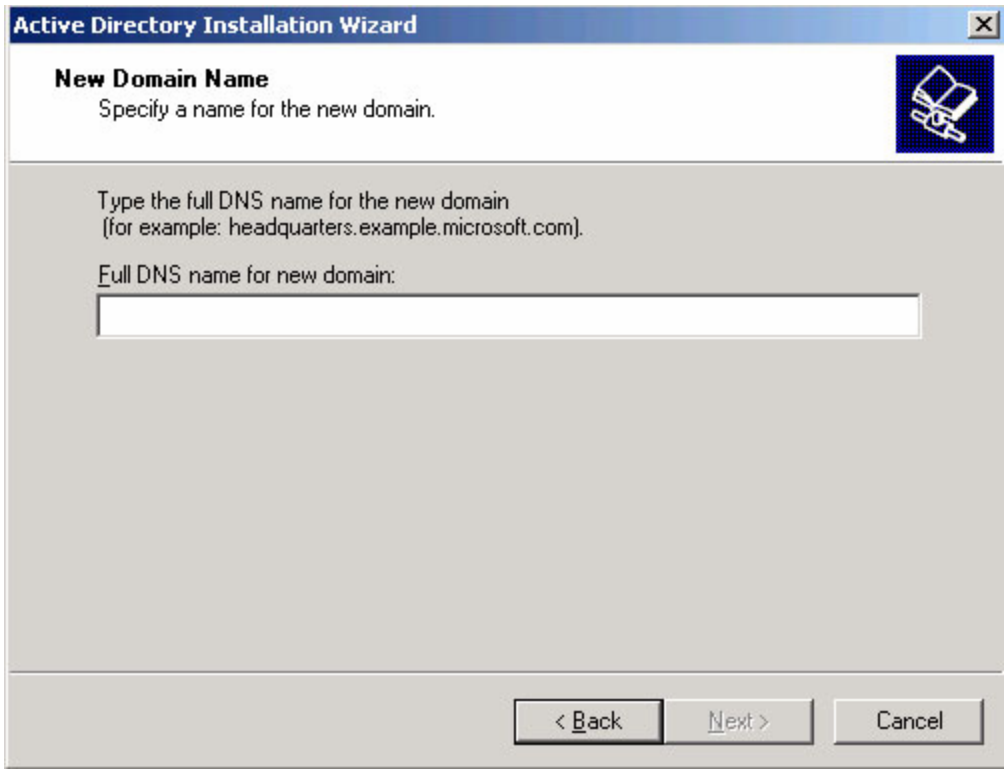
8. Đọc các thông tin trong trang này và nhấn ***Next***. Trang ***Domain Controller Type*** (Kiểu máy chủ quản trị miền) hiện ra.



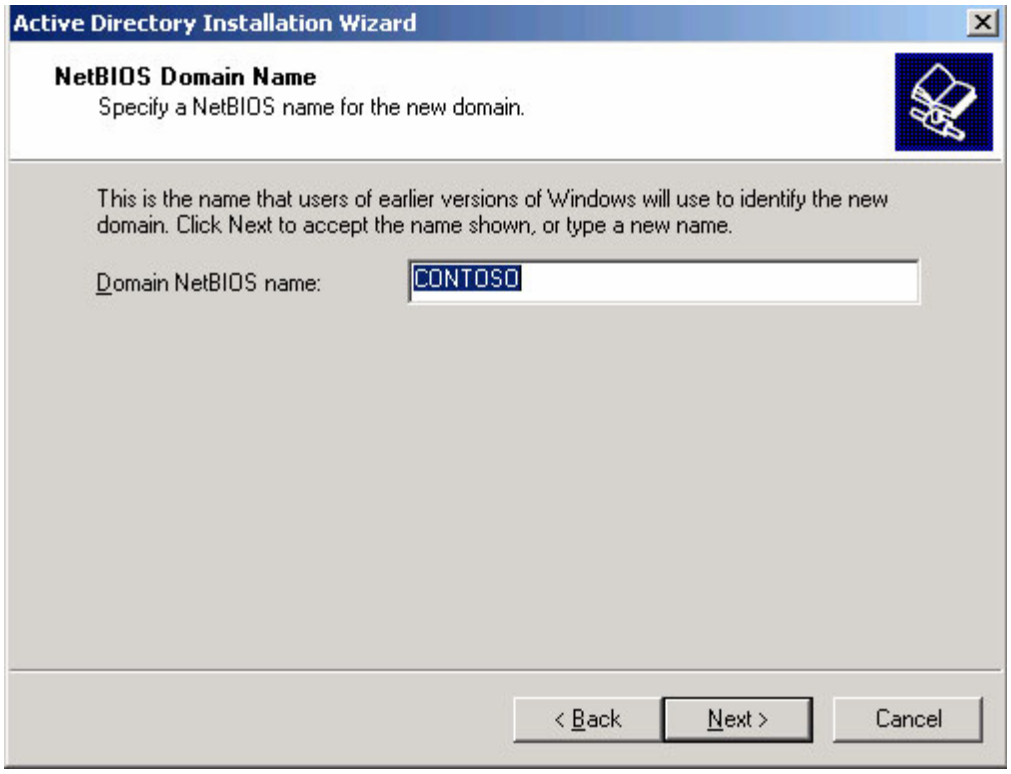
9. Giữ nguyên giá trị mặc định "***Domain Controller For A New Domain***" (Máy chủ quản trị miền cho một miền mới) được lựa chọn và nhấn ***Next***. Trang ***Create New Domain*** (Tạo miền mới) xuất hiện



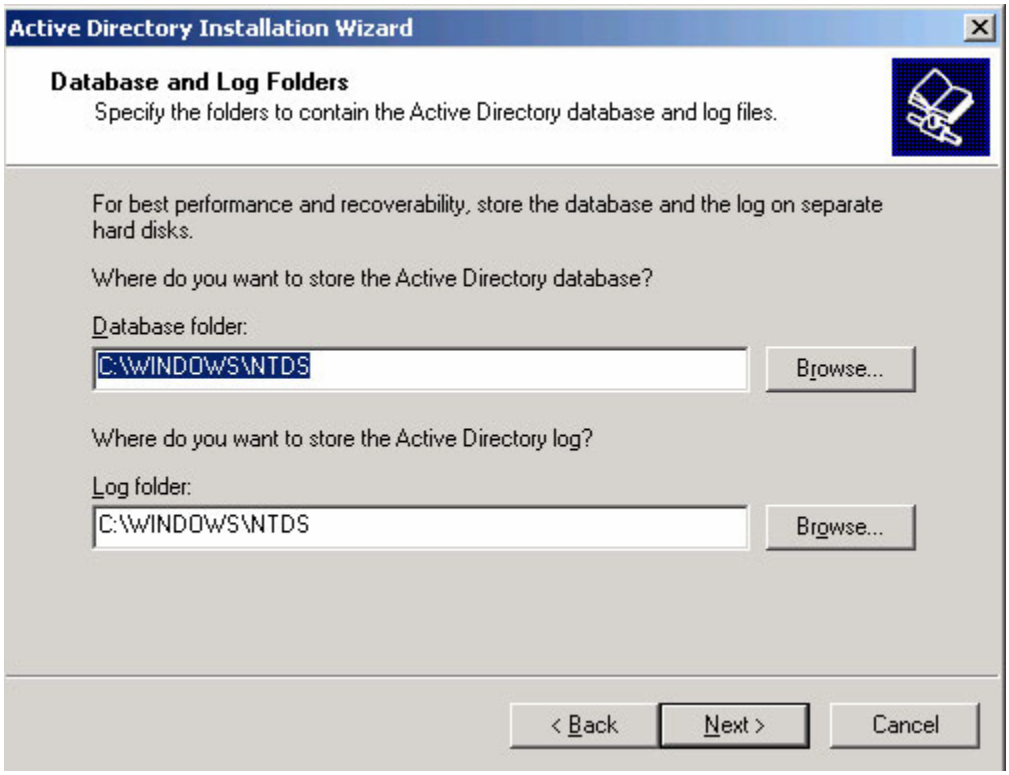
10.Giữ nguyên giá trị mặc định "***Domain In A New Forest***" (Miền trong một rừng mới) được lựa chọn và nhấn ***Next***. Trang ***New Domain Name*** (Tên miền mới) xuất hiện.



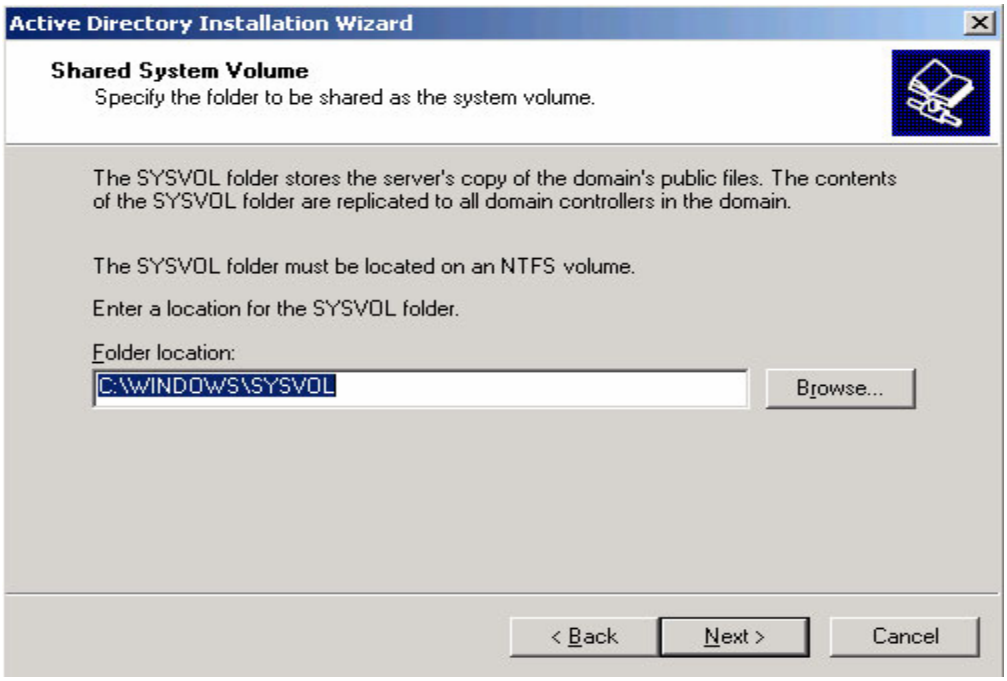
11.Trong hộp thoại "***Full DNS Name For New Domain***" (*Tên DNS đầy đủ của miền mới*), nhập vào đó: ***ACNAxx.com***, trong đó ***xx*** là số mà giảng viên cấp cho bạn, sau đó nhấn ***Next***. Trang ***NetBIOS Domain Name*** (*Tên miền NetBIOS*) xuất hiện.



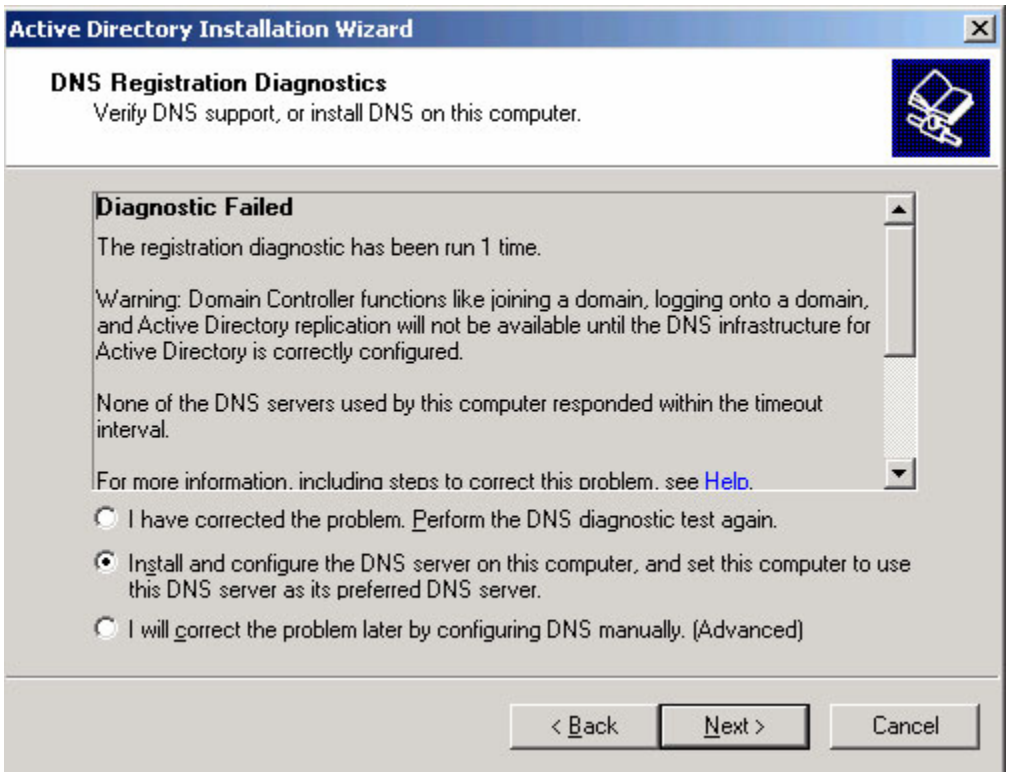
12.Xác nhận rằng tên xuất hiện trong hộp thoại "***Domain NetBIOS Name***" là ***ACNAXX*** và nhận ***Next***. Trang "***Database And Log Folders***" (*Thư mục chứa CSDL và nhật ký*) xuất hiện.



13.Nhấn ***Next*** để chấp nhận vị trí mặc định của các thư mục chứa log và CSDL. Trang "***Shared System Volume***" (*Thư mục hệ thống được chia sẻ*) xuất hiện.

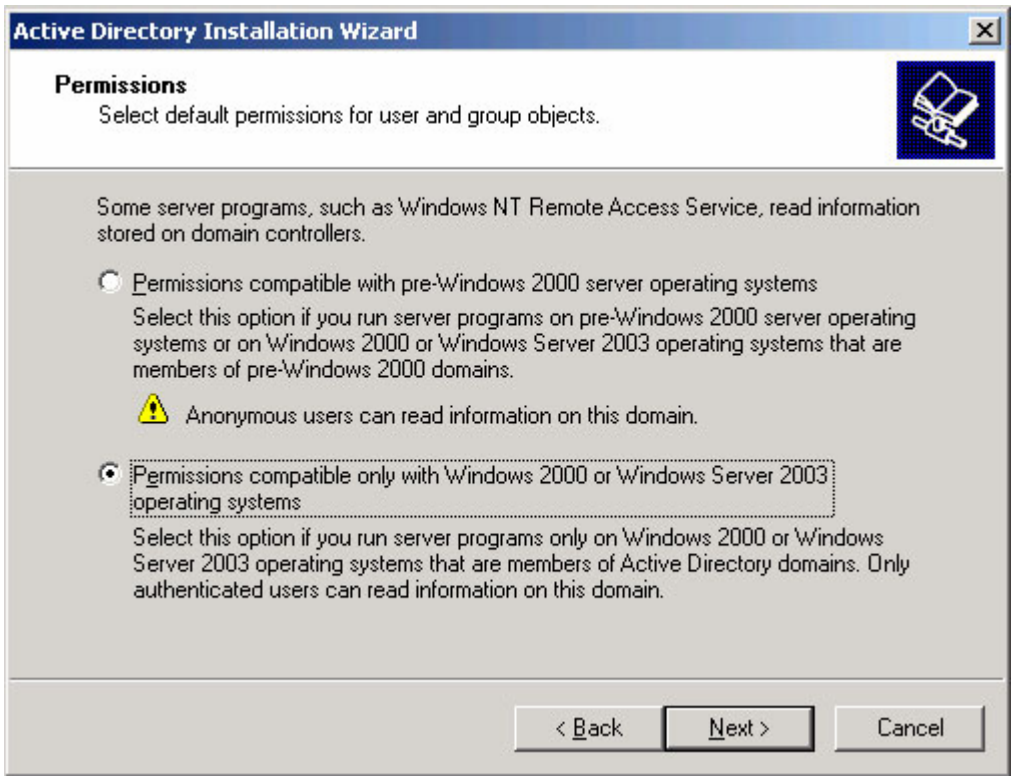


14.Nhấn ***Next*** để chập nhận vị trí mặc định của thư mục hệ thống chia sẻ. Trang ***DNS Registration Diagnostics*** (*Chẩn đoán đăng ký DNS*) xuất hiện

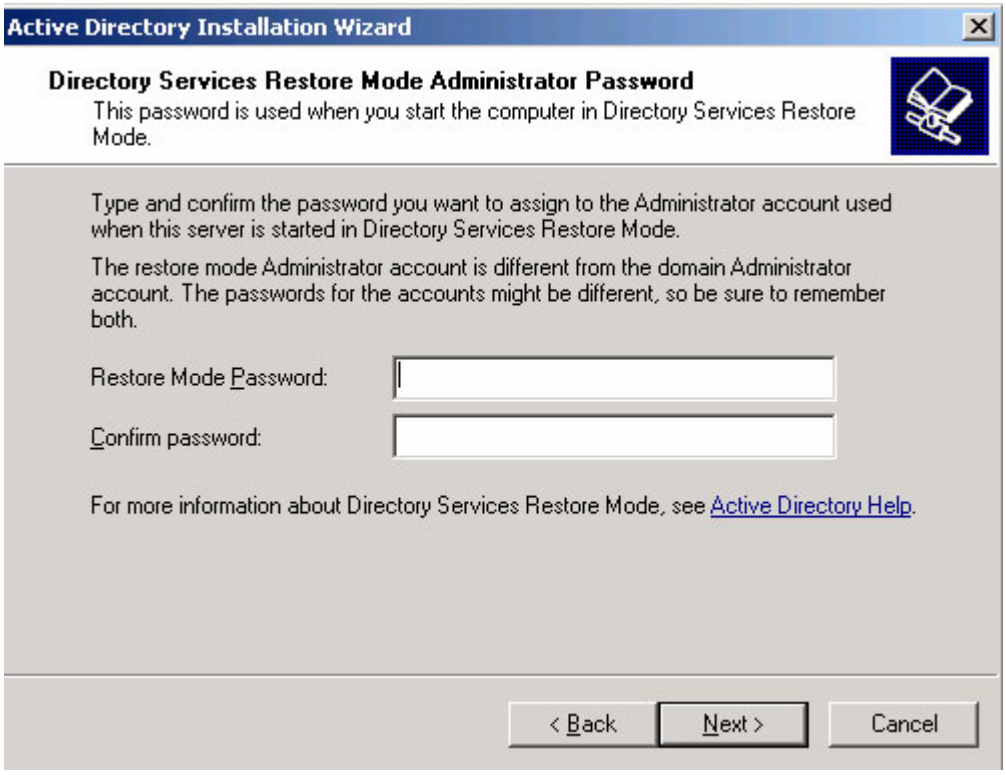


Tại thời điểm này, trình hướng dẫn sẽ thử kết nối đến các máy chủ DNS được chỉ định trong phần cấu hình TCP/IP, để xác định liệu các máy chủ DNS đó có chứa các bản ghi cần thiết cho quá trình cài đặt Miền sử dụng ***Active Directory*** hay không.

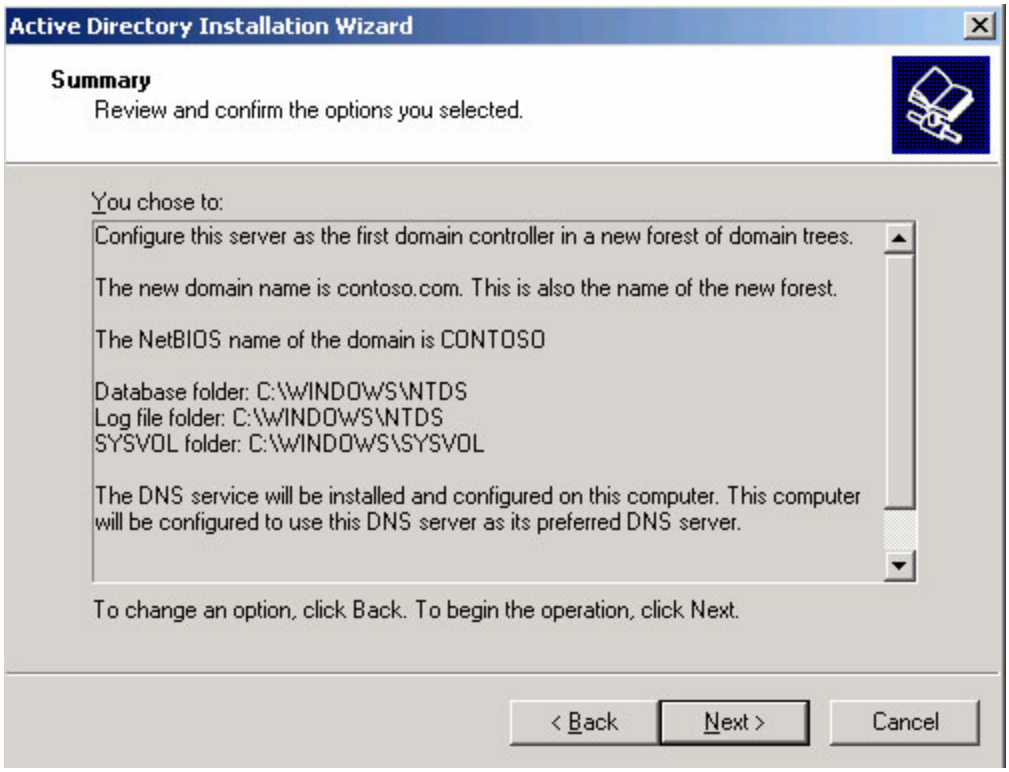
15.Lựa chọn "***Install And Configure The DNS Server On This Computer***" (*Cài đặt và cấu hình máy chủ DNS trên máy tính này*) và sau đó nhấn ***Next***. Trang ***Permissions*** (*Cấp phép*) xuất hiện



16.Nhấn ***Next*** để chấp nhận lựa chọn mặc định về quyền cấp phép và sau đó nhấn ***Next***. Trang "***Directory Services Restore Mode Administrator Password***" (*Mật khẩu tài khoản quản trị trong chế độ khôi phục dịch vụ thư mục*) xuất hiện



17.Nhập mật khẩu tương ứng vào các hộp thoại ***Restore Mode Password*** và ***Confirm Password*** và sau đó nhấn ***Next***. Trang "***Summary***" (*Tổng kết*) xuất hiện

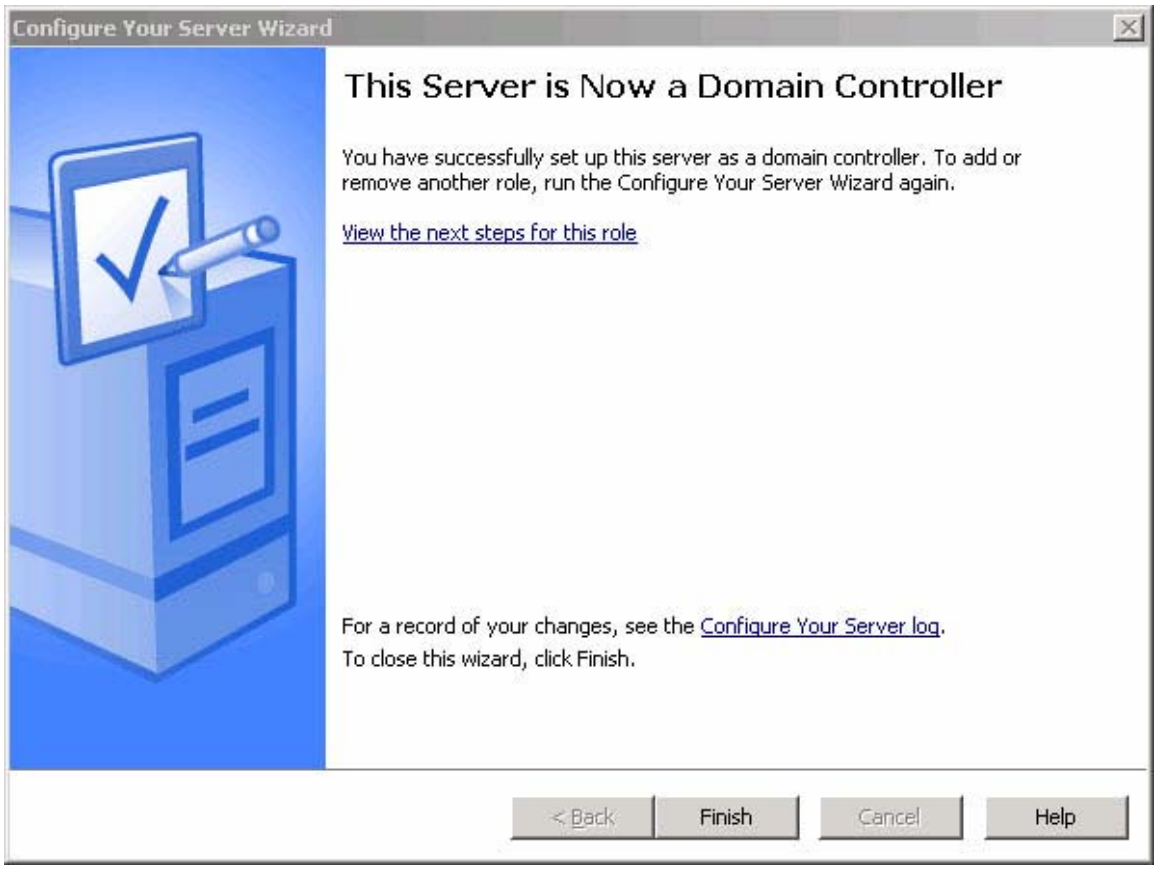


18.Xem lại toàn bộ các thông số mà bạn đã chọn và nhấn ***Next.*** Trình cài đặt sẽ bắt đầu cài đặt các dịch vụ ***Active Directory*** và ***DNS Server***.

19.Khi quá trình cấu hình hoàn thành xong, trang "***Completing The Active Directory Installation Wizard***" (*Hoàn thành quá trình cài đặt Active Directory*) xuất hiện. Nhấn ***Finish***.

20.Một hộp thoại thông báo của trình cài đặt ***Active Directory Installation Wizard*** xuất hiện, nhắc bạn khởi động lại máy tính. Nhấn ***Restart Now***

21.Sau khi máy tính khởi động lại, bạn đăng nhập bằng tài khoản ***Administrator***. Trình hướng dẫn ***Configure Your Server Wizard*** lại xuất hiện, hiển thị trang ***This Server Is Now A Domain Controller*** (*Máy chủ này bây giờ là một máy chủ quản trị miền*).



22.Nhấn ***Finish***

CÁC KHÁI NIỆM CƠ BẢN VỀ ACTIVE DIRECTORY

Mặc dù dịch vụ thư mục ***Active Directory*** không phải là chủ đề chính trong khóa học này, tuy nhiên một số khái niệm cơ bản về ***Active Directory*** là luôn luôn cần thiết cho mọi cán bộ quản trị mạng Window Server 2003. Các chương sau đây sẽ không bàn bạc về các chủ đề nâng cao như thiết kế ***Active Directory*** hay quản trị ***schema***, nhưng bạn sẽ sử dụng các công cụ quản trị ***Active Directory*** cung cấp trong Windows Server 2003 và sẽ học cách thao tác với các đặc tính của các đối tượng trong ***Active Directory***, ví dụ như người dùng, nhóm và máy tính.

> ***LƯU Ý: Active Directory***. *Để học thêm về các chủ đề nâng cao trong Active Directory, bạn có thể tham dự khóa học cho kỳ thi 70-294:* ***Planning, Implementing, and Maintaining a Microsoft Windows Server 2003 Active Directory Infrastructure*** *(Lập kế hoạch, triển khai và duy trì một hệ thống Microsoft Windows Server 2003 Active Directory)*

Dịch vụ thư mục (Directory Service) là gì ?

Hệ thống mạng nội bộ đầu tiên xuất hiện trong những năm đầu 1990 được tổ chức thành một nhóm các máy tính và được gọi là ***workgroup (****Nhóm làm việc****)***. Một ***workgroup*** máy tính cho phép người dùng có thể phối hợp tốt hơn trong cùng một dự án khi cần chia sẻ các tài nguyên như các văn bản và máy in. Và vì giá trị của việc sử dụng các hệ thống mạng dữ liệu ngày càng được khẳng định trong thế giới kinh doanh, các hệ thống mạng cũng trở nên lớn dần. Ngày nay một hệ thống mạng của các tổ chức doanh nghiệp thường có hàng ngàn nút mạng.

Khi các hệ thống mạng ngày càng lớn dần, số lượng tài nguyên chia sẻ cũng nhiều hơn, và do đó ngày càng khó khăn trong việc định vị và tìm kiếm các tài nguyên. Khi bạn làm việc cho một công ty với 12 nhân viên, bạn không khó khăn gì trong việc nhớ số điện thoại bàn của mỗi người, tuy nhiên khi công ty bạn có đến 1200 nhân viên, việc nhớ hết các số này là điều không tưởng. Để tìm ra một số của người bạn muốn liên lạc, phần lớn các công ty lớn đều sử dụng một danh bạ bao gồm tên và số liên lạc của mỗi người trong tổ chức, người ta gọi đó là ***directory*** (*Thư mục*). Một **dịch vụ thư mục** là một nguồn tài nguyên số hóa, mặc dù có thể thực hiện các chức năng không

giống nhau nhưng đều chứa một danh sách các tài nguyên có thể sử dụng trong một hệ thống mạng dữ liệu.

Một dịch vụ thư mục có thể chứa các thông tin về các máy tính trong mạng, các người dùng mạng và cả các thiết bị phần cứng, phần mềm ví dụ như các máy in và ứng dụng. Bằng cách lưu trữ thông tin trong một thư mục trung tâm, các tài nguyên này có thể được sử dụng đối với tất cả mọi người tại mọi thời điểm.

Miền và máy chủ quản trị miền:

Hệ thống mạng Windows hỗ trợ 02 mô hình dịch vụ thư mục: workgroup và domain, trong đó Mô hình Miền được ứng dụng trong các tổ chức triển khai Windows Server 2003. Mô hình dịch vụ thư mục ***workgroup*** là một CSDL phẳng bao gồm tên các máy tính và được thiết kế cho các mạng nhỏ. Đây là hình thức dịch vụ thư mục sơ khai được giới thiệu trong hệ điều hành Windows NT 3.1 những năm 1990.

Mô hình Miền là một kiến trúc thư mục có phân cấp của các tài nguyên - ***Active Directory*** – và được sử dụng bởi tất cả các hệ thống là thành viên của miền. Các hệ thống này có thể sử dụng các tài khoản người dùng, nhóm và máy tính trong thư mục để bảo mật các tài nguyên của chúng. ***Active Directory*** do đó đóng vai trò như một trung tâm lưu trữ nhận thực, cung cấp một danh sách tin cậy chỉ ra "Ai là ai" trong miền.

Bản thân ***Active Directory*** còn hơn là một CSDL, nó chứa một danh sách các thành phần hỗ trợ, bao gồm cả các ***transaction logs*** (nhật ký giao dịch) và dữ liệu hệ thống - còn gọi là ***Sysvol*** – nơi đây chứa các thông tin về các kịch bản đăng nhập và chính sách nhóm. Nó là một dịch vụ hỗ trợ và sử dụng các CSDL này, bao gồm giao thức ***Lightweight Directory Access Protocol*** (LDAP – *Giao thức truy nhập thư mục hạng nhẹ*), ***giao thức bảo mật Kerberos***, các ***chu trình đồng bộ dữ liệu*** và ***dịch vụ đồng bộ file*** (***File Replication Service*** - FRS). Cuối cùng, ***Active Directory*** là một bộ sưu tập các công cụ mà người quản trị mạng có thể sử dụng để quản lý dịch vụ thư mục.

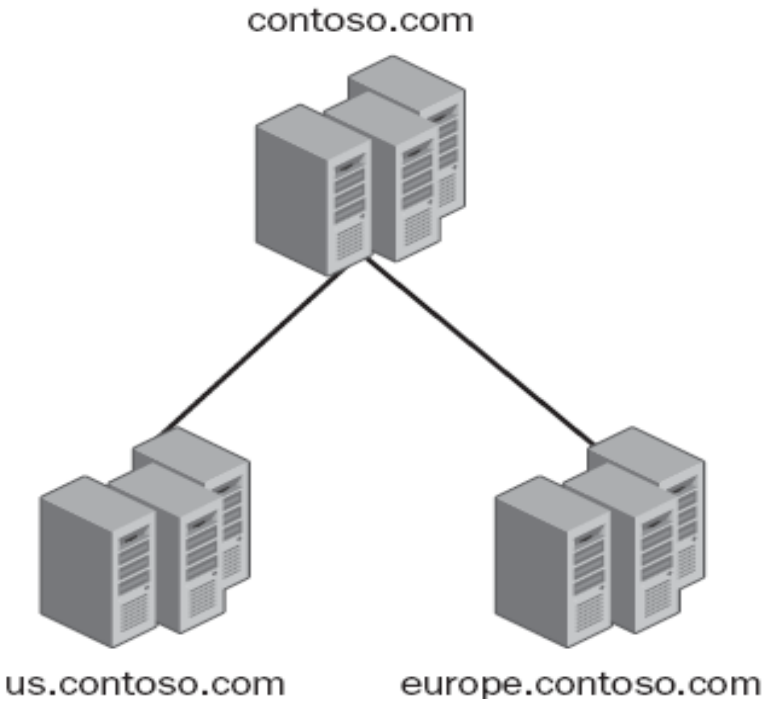
Cơ sở dữ liệu của ***Active Directory*** và các dịch vụ của nó được cài đặt trên một hay nhiều **máy chủ quản trị miền**. Một máy chủ quản trị miền là một máy chủ đã được thăng cấp bằng cách chạy trình cài đặt ***Active Directory*** (***Active Directory Installation Wizard***) như đã mô tả trong phần trước thuộc chương "Khởi tạo máy chủ quản trị miền". Khi máy chủ được thăng cấp thành một máy chủ quản trị miền, nó chứa một bản (hay một bản sao) của CSDL ***Active Directory***.

Bởi vì ***Active Directory*** là một tài nguyên cơ sở và rất quan trọng của hệ thống, nó phải luôn sẵn sàng với mọi người dùng trong mọi thời điểm. Vì lí do này, miền ***Active Directory*** thông thường có ít nhất 2 máy chủ quản trị miền để nếu một máy chủ bị sự cố, máy chủ còn lại vẫn có thể phục vụ người dùng. Các máy chủ quản trị miền luôn luôn đồng bộ dữ liệu với nhau nên mỗi máy chủ này đều chứa các thông tin hiện tại của miền hệ thống. Khi một người quản trị mạng thay đổi một bản ghi trong CSDL của ***Active Directory*** trên bất kì một máy chủ quản trị miền nào, sự thay đổi này được đồng bộ với tất cả các máy chủ quản trị miền trong miền đó. Điều này được gọi là **đồng bộ đa chủ** (***multiple-master***) bởi vì chúng ta có thể thay đổi trên bất kì một máy chủ quản trị miền nào.

> ***LƯU Ý: Đồng bộ đơn chủ (Single-Master)****. Mô hình miền dựa trên nền Windows NT sử dụng một kĩ thuật được gọi là đồng bộ đơn chủ (**single-master**) trong đó mọi thay đổi đối với các bản ghi của miền phải được thực hiện trên một máy chủ quản trị miền chính (**primary domain controller - PDC**) và các thông tin này sau đó được đồng bộ với một hay nhiều máy chủ quản trị miền dự phòng (**Backup Domain Controller - BDC**). Việc đồng bộ đa chủ (**Multiple-master**) là tốt hơn cho một hệ thống mạng lớn bởi vì người quản trị có thể cập nhận các thông tin cho CSDL Active Directory trên bất kì một máy chủ quản trị miền nào, không nhất thiết phải trên máy chủ PDC.*

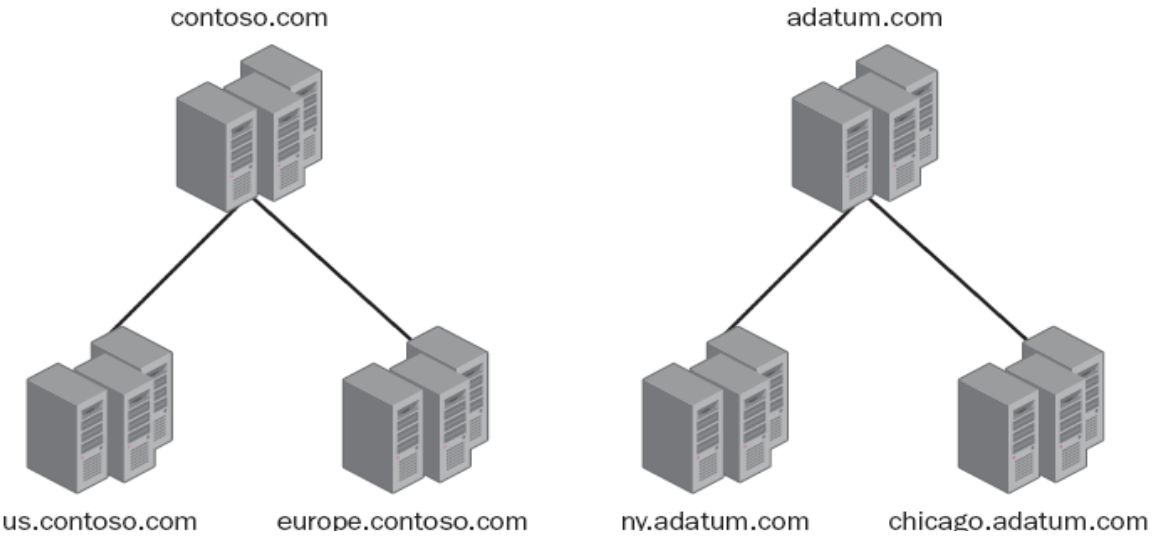
Domain, Tree và Forest (Miền, Cây và Rừng)

Một miền là một đơn vị quản trị cơ bản của dịch vụ thư mục trong Windows Server 2003. Hơn nữa một hệ thống mạng lớn có thể có nhiều hơn một miền trong ***Active Directory*** của nó. Mô hình nhiều Miền sẽ tạo ra một cấu trúc logic được gọi là các cây (***Tree***) nếu như chúng chung nhau một không gian tên miền DNS. ví dụ: ***ACNA.com, us.ACNA.com*** và ***europe.ACNA.com*** cùng chung một không gian tên miền DNS và được coi là một cây (***tree***) như chỉ ra trên Hình 1-3. Miền ***ACNA.com*** là miền cha trong đó hai miền còn lại được gọi là miền con và do đó ***ACNA.com*** cũng được gọi là miền gốc (***root domain***)



***Hình 1-3*: Cây sử dụng Active Directory**

Nếu các miền trong một ***Active Directory*** không chia sẻ một miền gốc chung, hệ thống sẽ có nhiều cây. Một ***Active Directory*** chứa nhiều cây sẽ được gọi là một rừng (***forest***) như chỉ ra trên Hình 1-4. Rừng là một kiến trúc lớn nhất trong ***Active Directory***. Khi bạn thăng cấp máy chủ quản trị miền đầu tiên trong một hệ thống mạng Windows Server 2003, bạn đã đồng thời tạo ra một rừng, một cây trong rừng đó và một miền trong cây đó. Một rừng có thể chứa rất nhiều miền trong nhiều cây, hoặc có thể chỉ có một miền.



Hình 1-4: Rừng sử dụng *Active Directory*

Khi quá trình cài đặt ***Active Directory*** có nhiều hơn một miền, một thành phần của ***Active Directory*** gọi là **Global Catalog** cho phép các máy trạm trong một miền có thể tìm kiếm thông tin trong một miền khác. ***Global catalog*** bản chất là một tập hợp bao gồm các thông tin dữ liệu của tất cả các miền kết hợp lại. Khi bạn tìm kiếm một người dùng trong một miền khác, ***global catalog*** có thể không chứa tất cả các thông tin về người dùng đó, tuy nhiên nó đủ dữ liệu để trả lời cho biết bạn có thể tìm kiếm các thông tin chi tiết hơn ở đâu.

Các đối tượng và thuộc tính:

Mọi CSDL đều được tạo nên bởi các bản ghi và trong ***Active Directory***, các bản ghi này được gọi là các đối tượng. Một đối tượng là một phần tử thể hiện một tài nguyên mạng xác định. Một ***Active Directory*** có thể chứa các đối tượng thể hiện các tài nguyên vật lý, ví dụ như các máy tính và máy in, hoặc các tài nguyên nhân sự, ví dụ như các người dùng và nhóm, hoặc các tài nguyên phần mềm, ví dụ như ứng dụng và vùng DNS, hoặc các tài nguyên quản trị, ví dụ như các OU và site. Sau khi thăng cấp một máy tính thành máy chủ quản trị miền, người quản trị có thể tạo các đối tượng trong miền đó.

Các đối tượng ***Active Directory*** được sử dụng thông dụng nhất là:

- **Domain (Miền):** Là một đối tượng gốc có chứa các đối tượng khác trong miền
- **Organizational Unit (Đơn vị tổ chức):** Là một đối tượng chứa (***container object***) được sử dụng để tạo ra các nhóm logic bao gồm các đối tượng như máy tính, người dùng và nhóm.
- **Người dùng:** Thể hiện một người dùng mạng và thực hiện chức năng là dữ liệu để nhận dạng và xác thực.
- **Máy tính:** Thể hiện một máy tính trong mạng và cung cấp tài khoản máy tính cần thiết cho hệ thống để đăng nhập vào Miền
- **Nhóm:** Một đối tượng chứa thể hiện một nhóm logic các người dùng, máy tính hoặc các nhóm khác, độc lập trongcấu trúc của ***Active Directory***. Các nhóm có thể chứa các đối tượng từ các OU và các Miền.
- **Thư mục chia sẻ:** Cung cấp các truy nhập mạng dựa trên ***Active Directory*** đến một thư mục chia sẻ trong một máy tính Windows.
- **Máy in:** Cung cấp các truy nhập mạng dựa trên ***Active Directory*** đến một máy in trong một máy tính Windows

Mỗi đối tượng ***Active Directory*** có chứa một tập hợp **các thuộc tính**, chính là các thông tin về đối tượng đó. Một đối tượng người dùng, sẽ có các thuộc tính mô tả tên tài khoản người dùng đó, mật khẩu, địa chỉ, số điện thoại và các thông tin nhận dạng khác. Một đối tượng nhóm sẽ có một thuộc tính cho biết danh sách các người dùng là thành viên của nhóm đó. Người quản trị mạng có thể sử dụng ***Active Directory*** để chứa bất kì thông tin nào về các người dùng trong tổ chức và các tài nguyên khác.

Bên cạnh các thuộc tính thuần túy thông tin, các đối tượng còn có các thuộc tính thực hiện các chức năng quản trị, ví dụ như một Danh sách Kiểm soát Truy nhập (***Access Control List*** - ACL) chỉ định ai có các Cấp phép truy nhập đến đối tượng đó.

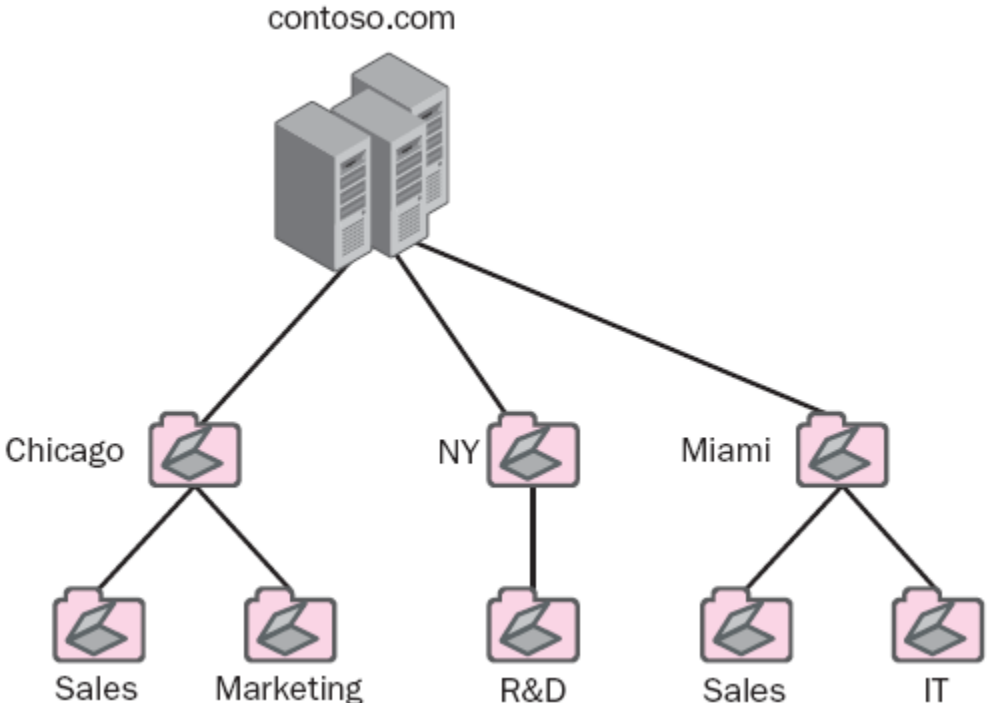
Các phần tử trong ***Active Directory*** chỉ ra kiểu đối tượng nào mà người quản trị có thể tạo ra và thuộc tính nào mỗi đối tượng có thể có, được gọi là ***schema*** *(lược đồ)*. Theo mặc định, ***Active Directory schema*** chứa một bộ danh sách các kiểu đối tượng và các thuộc tính, nhưng đôi khi chúng ta cần thêm vào ***Active Directory*** các kiểu đối tượng khác hoặc các thuộc tính khác cho các kiểu đối tượng sẵn có. Điều này là hoàn toàn có thể bởi vì ***Active Directory schema*** là có thể mở rộng. Người quản trị có thể mở rộng ***schema*** thủ công bằng cách sử dụng snap-in "***Active Directory Schema***" hoặc các ứng dụng có thể tự động mở rộng ***schema*** để tạo các kiểu đối tượng mới hoặc các thuộc tính mới cần thiết. ví dụ khi bạn cài đặt Microsoft Exchange, ứng dụng này sẽ chỉnh sửa ***schema*** để thêm vào các thuộc tính mới cho mọi đối tượng người dùng trong CSDL của ***Active Directory***.

Các containers và leaves (Đối tượng Chứa và Đối tượng Lá)

Active Directory có khả năng chứa hàng triệu đối tượng và do đó phải có một phương thức tổ chức các đối tượng đó thành các đơn vị nhỏ hơn ở trong miền. Để tổ chức quản lý các đối tượng như vậy, ***Active Directory*** sử dụng kiến trúc phân cấp. Một miền được gọi là một đối tượng chứa bởi vì các đối tượng khác có thể được tạo ra và phân cấp trong miền. OU là một dạng khác của đối tượng chứa mà người quản trị có thể tạo ra các đối tượng phân cấp trong nội bộ miền. Một đối tượng không thể chứa các đối tượng khác, ví dụ như một người dùng hoặc máy tính, được gọi là ***leaf object*** (*đối tượng lá*)

Một trong các tác vụ khó khăn và phức tạp trong việc quản trị ***Active Directory*** là tạo ra một kiến trúc phân cấp các OU sao cho hiệu quả nhất. Người quản trị có thể sử dụng rất nhiều cách để thiết kế cấu trúc phân cấp OU, ví dụ như thiết kế theo vị trí địa lý, theo phòng ban hoặc kết hợp cả hai. Hình 1-5 là một ví dụ cho thấy cấu trúc phân cấp của ***Active Directory*** trong đó lớp OU đầu tiên thể hiện các thành phố của một tổ chức có rất nhiều chi

nhánh, và lớp thứ hai thể hiện các phòng ban trong mỗi chi nhánh. Bằng cách tạo ra cấu trúc phân cấp ***Active Directory*** một cách logic, người dùng và người quản trị mạng có thể dễ dàng xác định và tìm kiếm các đối tượng khi cần.



Hình 1-5: Một cấu trúc phân cấp OU trong *Active Directory*

Nhóm cũng là một đối tượng chứa, nhưng **nó không phải là thành phần của cấu trúc phân cấp** bởi vì các thành viên của nhóm có thể nằm ở bất kì đâu trong miền. Để thực hiện đúng chức năng tổ chức, các đối tượng chứa đồng thời phải đóng vai trò quan trọng trong việc quản trị các đối tượng. Trong một hệ thống file, các Cấp phép được áp dụng trên các đối tượng được truyền từ trên xuống dưới trong cấu trúc phân cấp. ví dụ nếu bạn gán cho một đối tượng OU có Cấp phép truy nhập một thư mục chia sẻ nào đó, thì các đối tượng nằm trong OU đó sẽ được thừa hưởng các Cấp phép truy nhập này. Đây là một trong những tính năng cơ bản trong cấu trúc phân cấp mà người quản trị có thể áp dụng một cách hiệu quả. Thay vì gán các quyền và cấp phép cho từng người dùng, người quản trị có thể gán các quyền và cấp phép này cho các đối tượng chứa và các đối tượng người dùng trong nó sẽ được thừa hưởng các Quyền và Cấp phép cần thiết.

Các chính sách nhóm:

Do cách thức thừa hưởng các thiết lập từ đối tượng mức cha truyền xuống mức con, người quản trị có thể sử dụng các OU để gom các đối tượng cần cấu hình tương tự nhau. Các thiết lập cấu hình mà bạn áp dụng đến từng máy

tính chạy Windows cũng có thể quản trị một cách tập trung nhờ sử dụng một tính năng của ***Active Directory*** gọi là **chính sách nhóm** (***Group Policy*** – GP). Các chính sách nhóm cho phép bạn xác định các thiết lập bảo mật, triển khai phần mềm, cấu hình hệ điều hành và cách thức hoạt động của các ứng dụng trên một máy tính mà không cần thiết phải thực hiện trực tiếp trên máy tính đó. Bạn có thể thiết lập các tùy chọn cấu hình trên một đối tượng đặc biệt của ***Active Directory*** gọi là **Đối tượng Chính sách Nhóm (Group Policy Object - GPO)** sau đó kết nối các GPO này vào các đối tượng trong ***Active Directory*** chứa các máy tính hoặc người dùng mà bạn muốn cấu hình.

GPO là một tập hợp của rất nhiều các thiết lập cấu hình, từ các quyền đăng nhập của người dùng đến các phần mềm được cho phép hoạt động trong hệ thống. Bạn có thể gắn các GPO này với mọi đối tượng chứa trong ***Active Directory*** như ***Miền, site*** hoặc ***OU*** và các máy tính và người dùng trong các đối tượng chứa đó sẽ nhận được các thiết lập cấu hình trong GPO. Trong hầu hết các trường hợp, người quản trị mạng thiết kế cấu trúc phân cấp sao cho có thể áp dụng các GPO một cách hiệu quả nhất. Bằng cách đặt các máy tính có các vai trò xác định vào trong cùng một OU, bạn có thể gán một GPO có các thiết lập đặc biệt dựa trên vai trò của các máy tính đó vào OU này và như vậy bạn đã cấu hình một lúc được nhiều máy tính.

TỔNG KẾT

- Windows Server 2003 có 4 phiên bản chính—***Web Edition, Standard Edition, Enterprise Edition*** và ***Datacenter Edition***—chúng khác nhau trong cách hỗ trợ phần cứng và các tính năng mà chúng cung cấp.
- Phiên bản ***Enterprise*** và ***Datacenter*** có các phiên bản riêng có thể sử dụng với các nền phần cứng 64 bit cũng như 32 bit.
- Windows Server 2003 bản thương mại hay bản dùng thử đều yêu cầu có khóa sản phẩm và bạn phải kích hoạt sản phẩm trong vòng 14 hoặc 30 ngày sau khi cài đặt.
- Trang "***Manage Your Server***" và Trình Hướng dẫn Cấu hình Máy chủ (***Configure Your Server Wizard***) cho phép bạn có thể cấu hình máy tính chạy Windows Server 2003 thực hiện các chức năng khác nhau.
- ***Active Directory*** là dịch vụ thư mục dựa trên miền, chứa các Đối tượng mà bản thân các đối tượng này lại có một tập các thuộc tính của chúng.
- Cấu trúc phân cấp của ***Active Directory*** được tạo bởi rừng, cây, miền và OU. Quyền, Cấp phép và các Chính sách Nhóm sẽ được truyền xuống theo cấu trúc phân cấp đó.
- Để cài đặt ***Active Directory***, bạn thăng cấp một hay nhiều máy tính chạy Windows Server 2003 thành máy chủ quản trị miền bằng cách sử dụng trình cài đặt "***Active Directory Installation Wizard***". Một máy chủ quản trị miền sẽ chứa một bản của CSDL ***Active Directory*** và nó sẽ chịu trách nhiệm cung cấp thông tin ***Active Directory*** đáp ứng các yêu cầu của người dùng.

BÀI TẬP THỰC HÀNH

Bài tập thực hành 1-1: Lựa chọn hệ điều hành

Đối với mỗi phiên bản hệ điều hành của Windows Server 2003 trong cột bên trái, hãy chỉ ra các mô tả tương ứng trong cột bên phải.

1. Web Edition	a. Hỗ trợ 512 GB bộ nhớ
2. Standard Edition	b. Hỗ trợ chuỗi máy chủ có 8 nút
3. Enterprise Edition	c. Không chạy được các ứng dụng 16 bit
4. Datacenter Edition	d. Hỗ trợ chuỗi máy chủ 32 nút, có cân bằng tải (NBL)

5. Datacenter Edition (64-bit)	e. Hỗ trợ máy tính có 4 CPU

Bài tập thực hành 1-2: Đăng nhập vào Windows

Khi bạn đã hoàn thành việc cài đặt hệ điều hành Windows Server 2003, máy tính khởi động lại và hiển trị hộp thoại "***Welcome To Windows***" Để đăng nhập vào máy tính lần đầu tiên, bạn thực hiện các thao tác sau:

1. Trong màn hình ***Welcome To Windows***, bạn nhấn đồng thời 3 phím ***CTRL+ALT+DELETE***. Hộp thoại "***Log On To Windows***" (*Đăng nhập vào Windows*) xuất hiện.
2. Trong hộp thoại ***Password***, nhập vào mật khẩu mà bạn đã thiết lập cho tài khoản ***Administrator*** trong quá trình cài đặt hệ điều hành. Màn hình nền Windows xuất hiện.

Bài tập thực hành 1-3: Xem các đối tượng Active Directory

Khi bạn tạo ra một ***Miền Active Directory***, theo mặc định hệ điều hành sẽ tạo ra một số đối tượng chứa và đối tượng lá (***container*** và ***leaf objects***). Để xem thông tin về các đối tượng này, sử dụng các thao tác sau:

1. Đăng nhập vào máy chủ quản trị Miền bằng tài khoản ***Administrator***
2. Nhấn ***Start,*** trỏ đến ***Administrative Tools*** và nhấn vào "***Active Directory Users And Computers***" (*Quản trị máy tính và người dùng trong Active Directory*). Cửa sổ "***Active Directory Users And Computers"*** xuất hiện.
3. Mở rộng biểu tượng miền ***ACNAxx.com*** trong ô bên trái và lựa chọn OU ***Users*** bên trong domain đó. Các đối tượng người dùng và nhóm trong OU ***Users*** xuất hiện trong ô bên phải.

CÁC CÂU HỎI ÔN TẬP

1) Bạn đang có kế hoạch triển khai các máy tính chạy Windows Server 2003 cho một phòng ban gồm 250 người. Máy chủ sẽ chứa các thư mục gốc và các thư mục chia sẻ cho phòng ban này, đồng thời nó sẽ chứa một số máy in để các tài liệu của phòng ban này có thể gửi đến in ấn. Phiên bản nào của Windows Server 2003 sẽ cung cấp giải pháp hiệu quả nhất cho phòng ban này. Giải thích về câu trả lời của bạn.
2) Phiên bản nào sau đây của Windows Server 2003 yêu cầu kích hoạt sản phẩm:

a) Phiên bản bán lẻ Standard

b) Phiên bản thử nghiệm Enterprise

c) Phiên bản Enterprise, Giấy phép mở (Open License)

d) Phiên bản Standard, Giấy phép theo dung lượng (Volume License)

3) Chỉ ra sự khác biệt cơ bản giữa cây ***Active Directory*** và rừng ***Active Directory***?

4) Kiểu đối tượng ***Active Directory*** nào sau đây không phải là đối tượng chứa?

a) Người dùng

b) Nhóm

c) Máy tính

d) ***Organizational unit***

5) Mệnh đề nào sau đây là đúng khi nói về quá trình cài đặt trong Windows Server 2003 ? (Lựa chọn tất cả các mệnh đề có thể)

a) Trình cài đặt có thể được nạp bằng cách khởi động từ đĩa CD.

b) Trình cài đặt có thể được nạp bằng cách khởi động từ các đĩa mềm

c) Trình cài đặt yêu cầu mật khẩu của tài khoản ***Administrator*** không phải là trống để đáp ứng các yêu cầu về tính phức hợp.

d) Trình cài đặt yêu cầu bạn phải kích hoạt bản quyền sản phẩm trước khi cài đặt hệ điều hành

CÁC KỊCH BẢN TÌNH HUỐNG

Kịch bản 1-1: Các tính năng của Windows Server 2003, phiên bản Web

Bạn là người quản trị mạng và được giao nhiệm vụ triển khai các máy chủ Windows Server 2003 cho Web-site thương mại mới của công ty. Web-site này do một nhà tư vấn thuê ngoài thiết kế. ***Site*** này yêu cầu 4 máy chủ Web, cấu hình thành một chuỗi máy chủ 4 trạm (***Clusters***) hoạt động theo chế độ ***Load-balancing (****cân bằng tải****)*** đồng thời phải có 1 máy chủ CSDL đơn chạy trên nền SQL Server. Kế hoạch triển khai của cán bộ tư vấn yêu cầu sử dụng Windows Server 2003 Web Edition trên cả 5 máy chủ. Trong các mệnh đề sau đây, mệnh đề nào là đúng khi nói về đề xuất triển khai này?

1. Phiên bản Web là hệ điều hành phù hợp với 5 máy chủ này
2. Phiên bản Web là hệ điều hành phù hợp với máy chủ CSDL nhưng không phù hợp với các máy chủ Web bởi vì nó không hỗ trợ chuỗi máy chủ ở chế độ cân bằng tải (NLB)
3. Phiên bản Web là hệ điều hành phù hợp với các máy chủ Web nhưng không phù hợp với máy chủ CSDL vì nó không thể chạy SQL Server
4. Phiên bản WebEdition không phải là hệ điều hành phù hợp với cả máy chủ Web và máy chủ CSDL

Kịch bản 1-2: Lựa chọn phiên bản Windows Server 2003

Bạn đang có kế hoạch triển khai các máy tính Windows Server 2003 cho một miền ***Active Directory*** mới trong một Tổng công ty lớn bao gồm rất nhiều ***Active Directory*** tách biệt được các công ty con duy trì. Tổng công ty quyết định sử dụng Exchange Server 2003 để xây dựng hệ thống truyền tin thống nhất cho toàn bộ các chi nhánh và dự định sử dụng ***Microsoft Metadirectory Services*** (MMS – *Dịch vụ Siêu thư mục Microsoft*) để đồng bộ các thuộc tính của các đối tượng trên toàn hệ thống. Phiên bản Windows Server 2003 nào sẽ cung cấp phương án hiệu quả nhất cho việc triển khai này. Giải thích câu trả lời.

CHƯƠNG 2: QUẢN TRỊ HỆ ĐIỀU HÀNH MICROSOFT WINDOWS SERVER 2003

Công việc hàng ngày của người quản trị hệ thống Windows Server 2003 phần lớn bao gồm các nhiệm vụ cấu hình các đối tượng ***Active Directory***, chỉnh sửa các phần mềm và các dịch vụ thiết lập trên máy tính, cài đặt các phần cứng và phần mềm mới, sử dụng các công cụ mà hệ điều hành cung cấp để thực hiện rất nhiều nhiệm vụ khác. Khi hệ thống mở rộng thêm nhiều máy tính, các nhiệm vụ phải làm cũng tăng dần theo. ***Microsoft Management Console*** (MMC – *Bảng Điều khiển Quản trị Microsoft*) là công cụ quản trị chủ yếu của hệ thống Windows Server 2003. MMC cho phép người quản trị có thể tích hợp các công cụ thông dụng vào trong một giao diện đơn và sử dụng chúng để quản trị các máy tính Windows ở mọi nơi trong mạng. Hiểu biết về các tính năng của MMC là điều rất quan trọng giúp cho việc quản trị hệ thống một cách hiệu quả hơn.

Khi các yêu cầu điều khiển máy tính ở xa trở nên phức tạp hơn ngoài khả năng của các tác vụ được thực hiện bởi MMC, chúng ta có thể sử dụng hai công cụ quan trọng khác để quản trị từ xa: ***Remote Desktop for Administration*** (*Màn hình Quản trị Từ xa*) và ***Remote Assistance*** (*Trợ giúp Từ xa*). ***Remote Desktop for Administration*** là một ứng dụng theo kiểu máy chủ/máy khách trong đó màn hình điều khiển của máy chủ ở xa được hiển thị trên màn hình của máy trạm tại chỗ, cho phép bạn có thể điều khiển chức năng của chuột và bàn phím như là bạn đăng nhập tại chỗ vào máy tính ở xa đó. ***Remote Assistance*** có chức năng tương tự tuy nhiên nó được thiết kế cho phép một người sử dụng Windows Server 2003 hay Windows XP có thể yêu cầu sự trợ giúp từ người dùng khác trong mạng. Khi một người dùng đưa ra một yêu cầu hỗ trợ, một chuyên gia nào đó trong mạng có thể thiết lập một kết nối từ xa đến màn hình của người dùng đó.

Sau khi kết thúc chương này, bạn có thể:

- **Sử dụng các bảng điều khiển MMC cấu hình sẵn.**
- **Tạo một bảng điều khiển MMC mới.**
- **Quản trị cả máy tính tại chỗ và ở xa bằng bảng điều khiển MMC**

- **Xử lý các sự cố của Dịch vụ đầu cuối**
- **Cấu hình máy chủ cho phép sử dụng *Remote Desktop for Administration***
- **Cho phép máy tính có khả năng chấp nhận các yêu cầu *Remote Assistance***
- **Sử dụng một trong các phương pháp để yêu cầu và thiết lập một phiên làm việc *Remote Assistance*.**

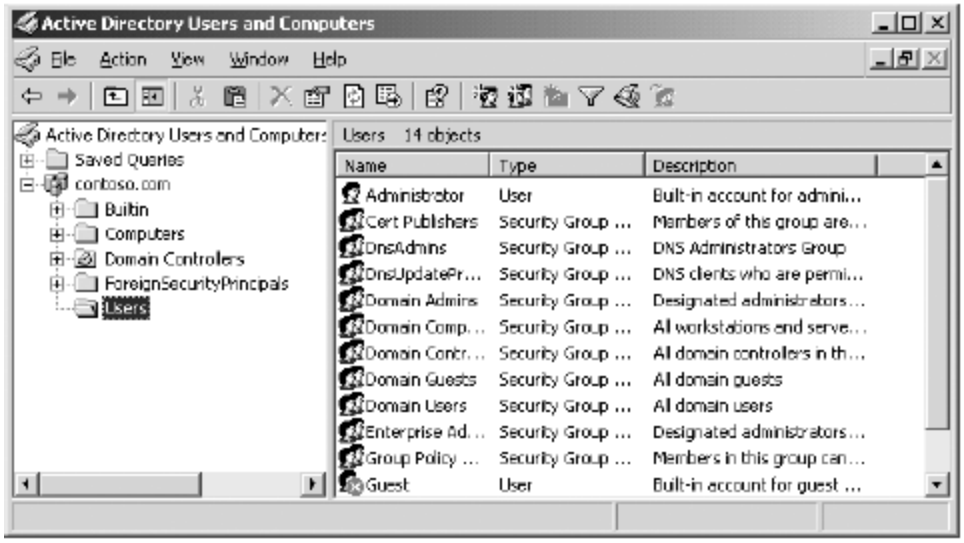
SỬ DỤNG MICROSOFT MANAGEMENT CONSOLE (MMC)

MMC là một ứng dụng lớp vỏ (***shell application***) mà Windows Server 2003 sử dụng để cung cấp các truy cập đến phần lớn các công cụ quản trị mạng và hệ thống. MMC cung cấp một giao diện chuẩn thông dụng cho một hoặc nhiều các module ứng dụng (được gọi là các **snap-in**) được sử dụng để cấu hình môi trường hệ thống. Các snap-in này được trao các nhiệm vụ khác nhau và cũng có thể kết hợp, sắp xếp theo thứ tự, hoặc nhóm lại với nhau trong một lớp vỏ MMC tùy theo sở thích của người quản trị. Một MMC với một hoặc nhiều snap-in đã cài đặt sẽ được gọi là một ***Console*** *(Bảng điều khiển)*. Phần lớn các công cụ quản trị chủ yếu trong Windows Server 2003 là các bảng điều khiển MMC với một danh sách các snap-in được cài đặt phù hợp cho một ứng dụng nào đó. Ngoài trừ một số trường hợp, còn lại hầu hết mọi ***shortcut*** (liên kết tắt) trong nhóm chương trình ***Administrative Tools*** (*Các công cụ quản trị*) trên một máy tính Windows Server 2003 đều được liên kết đến các bảng điều khiển MMC đã cấu hình sẵn.

Ví dụ, khi bạn thăng cấp một máy tính Windows Server 2003 thành một máy chủ quản trị domain, trình hướng dẫn cài đặt "***Active Directory Installation Wizard***" sẽ tạo ra các ***shortcut*** đến ba công cụ quản trị chủ yếu cho ***Active Directory***:

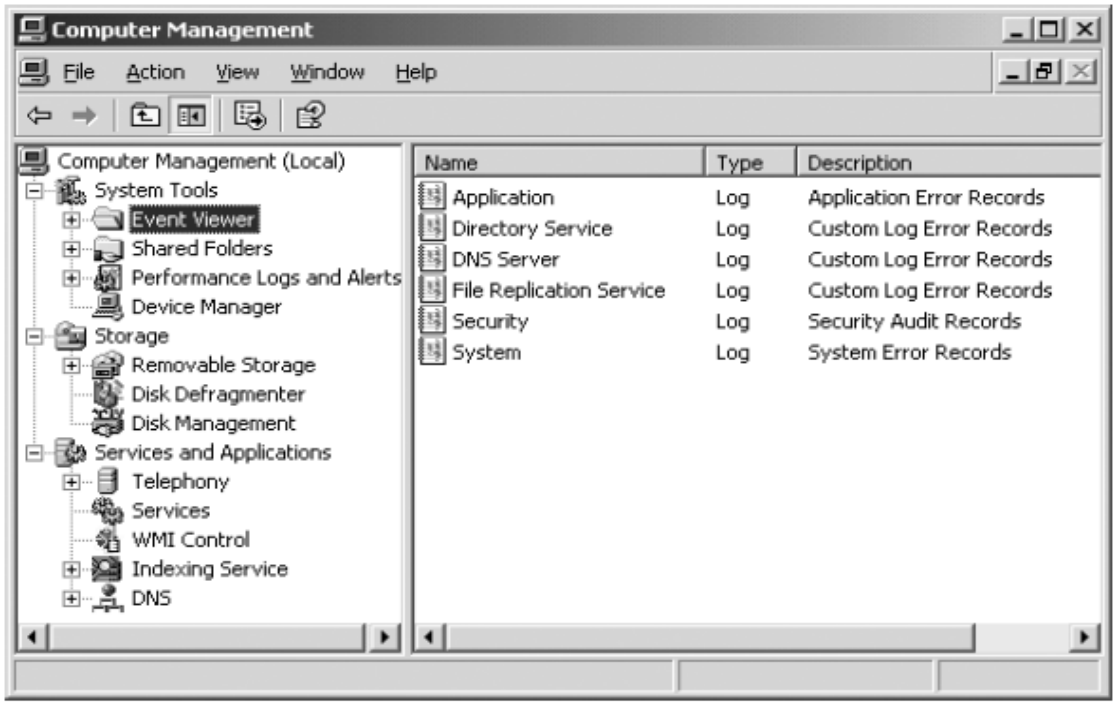
- ***Active Directory Domains and Trusts*** (Miền và Quan hệ tin cậy trong Active Directory)
- ***Active Directory Sites and Services*** (Dịch vụ và Vị trí trong Active Directory)
- ***Active Directory Users and Computers*** (Người dùng và Nhóm trong Active Directory)

Mỗi ***shortcut*** sẽ mở ra một Bảng điều khiển MMC chứa một snap-in đơn như trên Hình 2-1. Ví dụ snap-in "***Active Directory Users and Computers***" được thiết kế sẵn cho việc quản trị các đối tượng người dùng, nhóm và máy tính trong miền. Đó là các snap-in nằm trong lớp vỏ MMC, chứ không phải là bản thân các MMC cung cấp các công cụ quản trị mà bạn đang sử dụng.



***Hình 2-1*: Bảng điều khiển "Active Directory Users and Computers"**

Ba bảng điều khiển ***Active Directory*** liệt kê ở trên đều chứa các snap-in đơn lẻ, nhưng một bảng điều khiển MMC không chỉ giới hạn sử dụng một snap-in tại một thời điểm. Khi bạn mở bảng điều khiển "***Computer Management***" (Quản trị Máy tính) trong nhóm chương trình ***Administrative Tools*** trên bất cứ một máy tính Windows Server 2003 nào, bạn có thể thấy một bảng điều khiển chứa rất nhiều snap-in, tất cả kết hợp trong một giao diện đơn, thuận tiện như trong Hình 2-2



***Hình 2-2*: Bảng điều khiển "Computer Management"**

***LƯU Ý: Tính tương thích của MMC**. Bảng điều khiển MMC có thể chạy trên các hệ điều hành Windows Server 2003, Windows XP, Windows 2000, Windows NT 4 và Windows 98.*

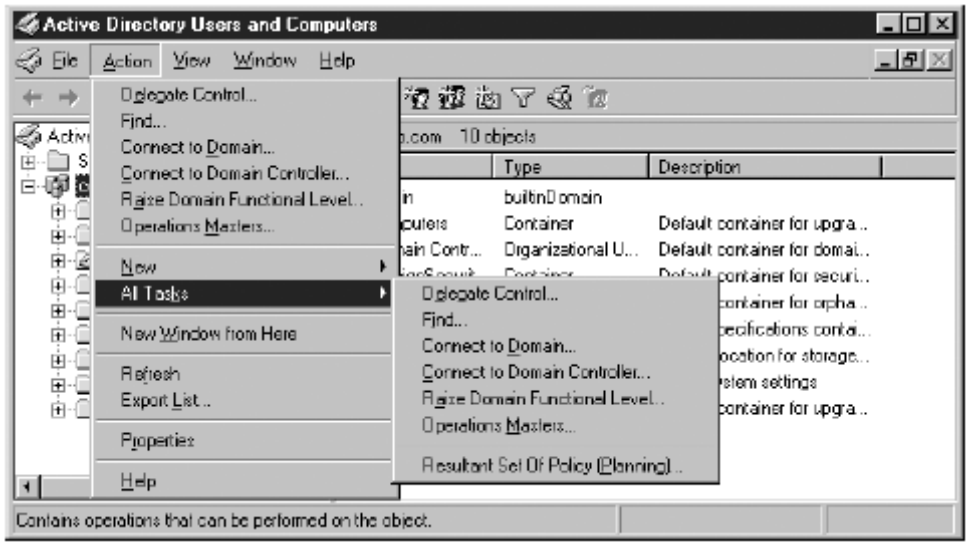
Sử dụng giao diện MMC

MMC sử dụng kiểu thiết kế 2 ô, giống như Windows Explorer (*Trình duyệt Windows*). Ô bên trái, được gọi là **scope pane** (khung phạm vi), chứa một danh sách phân cấp các snap-in cài đặt trong bảng điều khiển này và các tiêu đề mà bảng điều khiển này cung cấp. Cấu trúc phân cấp này đôi lúc còn được gọi là **console tree** (*Cây điều khiển*). Bạn có thể mở rộng và thu nhỏ các phần tử thuộc ***khung phạm vi*** để hiển thị nhiều hoặc ít các thông tin, giống như khi bạn mở rộng và thu nhỏ các thư mục bên trong Windows Explorer. Lựa chọn một phần tử trong khung phạm vi sẽ hiển thị nội dung của nó trong ô bên phải của bảng điều khiển, được gọi là **details pane** (Khung chi tiết). Các thành phần mà bạn nhìn thấy trong ***khung chi tiết*** sẽ hoàn toàn phụ thuộc vào chức năng của các snap-in mà bạn đang sử dụng.

Sử dụng các Thực đơn trong MMC

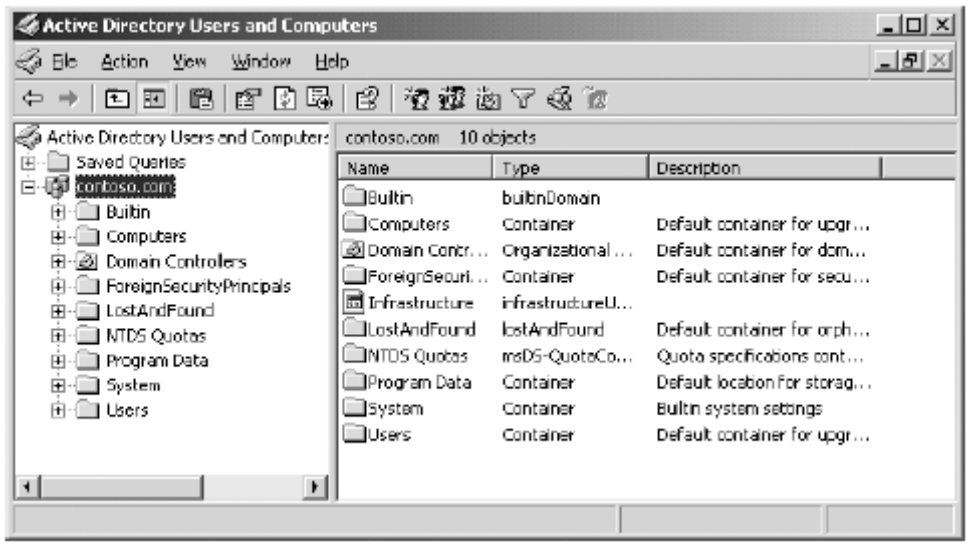
Phía trên hai ô nói trên, MMC có một thực đơn và thanh công cụ chuẩn của Windows. Các lệnh trên các thực đơn và các công cụ trên thanh công cụ sẽ thay đổi tùy theo snap-in nào bạn đang lựa chọn trong khung phạm vi. Ví dụ khi bạn mở bảng điều khiển "***Computer Management***" và lần lượt nhấn vào mỗi snap-in trong ***khung phạm vi***, bạn sẽ thấy nội dung của thanh công cụ thay đổi theo các snap-in này, đồng thời thay đổi cả một số nội dung của thực đơn .

Thực đơn chính cho các chức năng theo ngữ cảnh trong một bảng điều khiển MMC là thực đơn ***Action*** (*Hành động*). Khi bạn lựa chọn một phần tử của snap-in trong cả ***scope pane*** hay ***details pane***, thực đơn ***Action*** sẽ thay đổi các lệnh áp dụng với phần tử đó. Phần lớn các thực đơn ***Action*** chứa một thực đơn con "***All tasks***" –(*tất cả các tác vụ*) cho phép bạn lựa chọn các tác vụ có thể thực hiện trên phần tử mà bạn đang chọn. (Như chỉ ra trên hình 2-3). Thông thường ta có thể thấy một thực đơn con ***New*** (*mới*) dưới thực đơn ***Action*** cho phép bạn có thể tạo các phần tử con trong phần tử bạn đang chọn. Trong hầu hết các trường hợp, các lệnh trong thực đơn ***Action*** đối với một phần tử lựa chọn cũng sẽ xuất hiện trong thực đơn ngữ cảnh, sẽ hiện ra khi bạn nhấn chuột phải vào phần tử đó.



Hình 2-3: Thực đơn *Action* trong một bảng điều khiển MMC

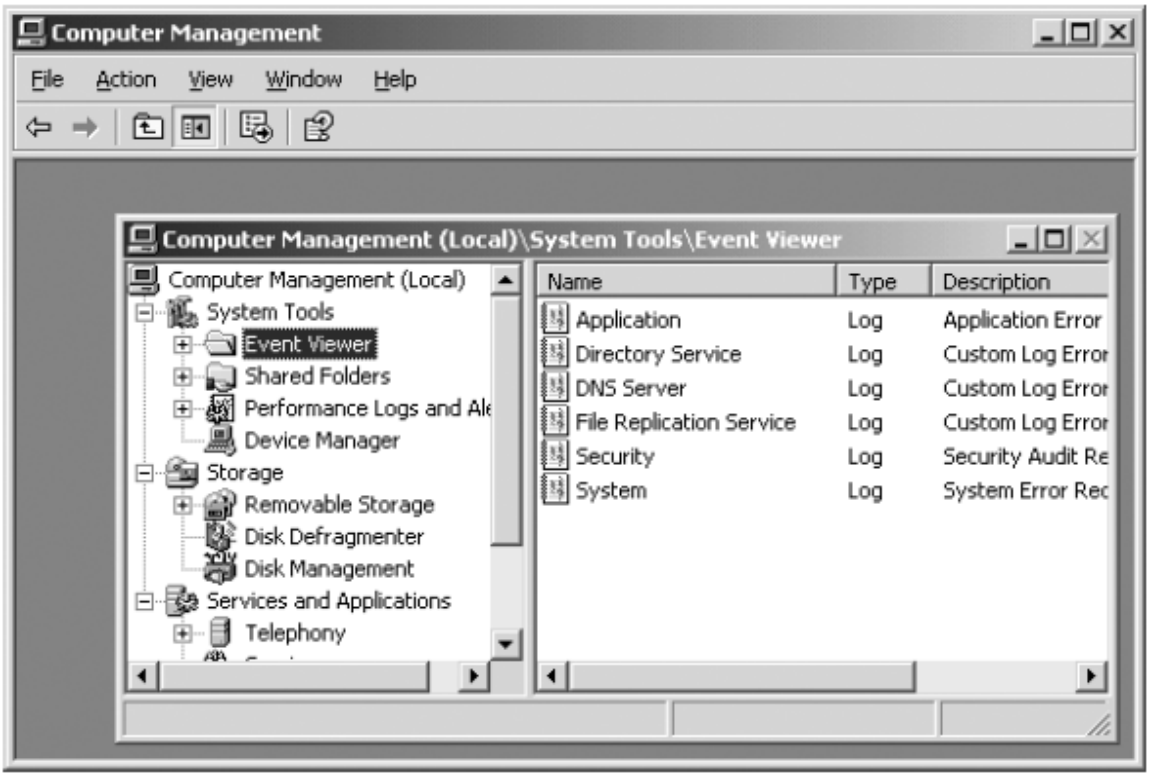
Mặc dù thực đơn ***Action*** thay đổi thường xuyên, các thực đơn khác trong MMC có thể chứa các thành phần ngữ cảnh xác định, điển hình là thực đơn ***View***, chứa các lệnh điều khiển cách thức snap-in hiển thị thông tin. Ví dụ một số snap-in trong MMC theo mặc định chỉ hiển thị một phần các thông tin có thể, tuy nhiên khi dòng lệnh ***Advanced Features*** (Các tính năng tiên tiến) xuất hiện trên thực đơn ***View***, việc lựa chọn lệnh này sẽ cho phép bảng điều khiển hiển thị đầy đủ các thông tin (Như thể hiện trong Hình 2-4)



Hình 2-4*: Bảng điều khiển "*Active Directory Users and Computers*" hiển trị khi chọn *Advanced Features

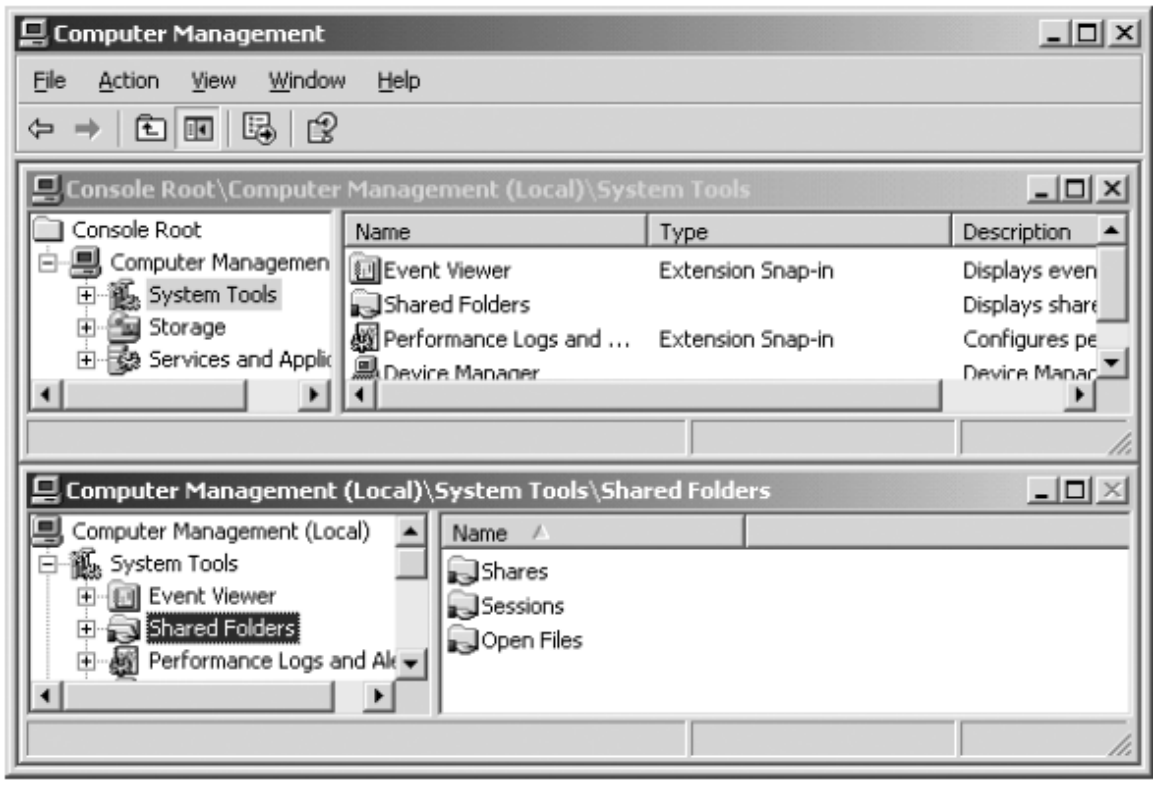
Sử dụng nhiều cửa sổ Windows.

Nếu bạn quan sát cẩn thận trong phần phía trên bên phải của một trong các bảng điều khiển MMC định nghĩa sẵn, bạn có thể thấy hai tổ hợp phím thao tác Windows bởi vì các snap-in cài đặt trong bảng điều khiển này thực ra nằm trong một cửa sổ riêng và đã ở trong trạng thái cực đại (***maximize***) theo mặc định. Khi bạn nhấn vào phím ***Restore Down*** (*"thu nhỏ" - phím ở giữa trong 3 phím*) các snap-in này sẽ thu về trạng thái cửa sổ nổi như trong Hình 2-5.



Hình 2-5: Một bảng điều khiển MMC với cửa sổ nổi

Bạn có thể tạo thêm các cửa sổ trong bảng điều khiển này bằng cách lựa chọn ***New Window*** từ thực đơn Window. Điều này cho phép bạn tạo ra 2 cách xem khác nhau đối với một snap-in đơn hoặc cùng một lúc có thể làm việc với hai snap-in khác nhau trong một bảng điều khiển (Như hiển thị trong Hình 2-6). Bạn có thể lựa chọn một phần tử trong ***khung phạm vi*** và lựa chọn lệnh ***New Window From Here*** (*Cửa sổ mới từ đây*) từ thực đơn ***Action*** để tạo ra một cửa sổ mới trong đó phần tử vừa lựa chọn sẽ được nằm ở mức gốc của bảng điều khiển.



***Hình 2-6*: Một bảng điều khiển Windows với 2 cửa sổ mở**

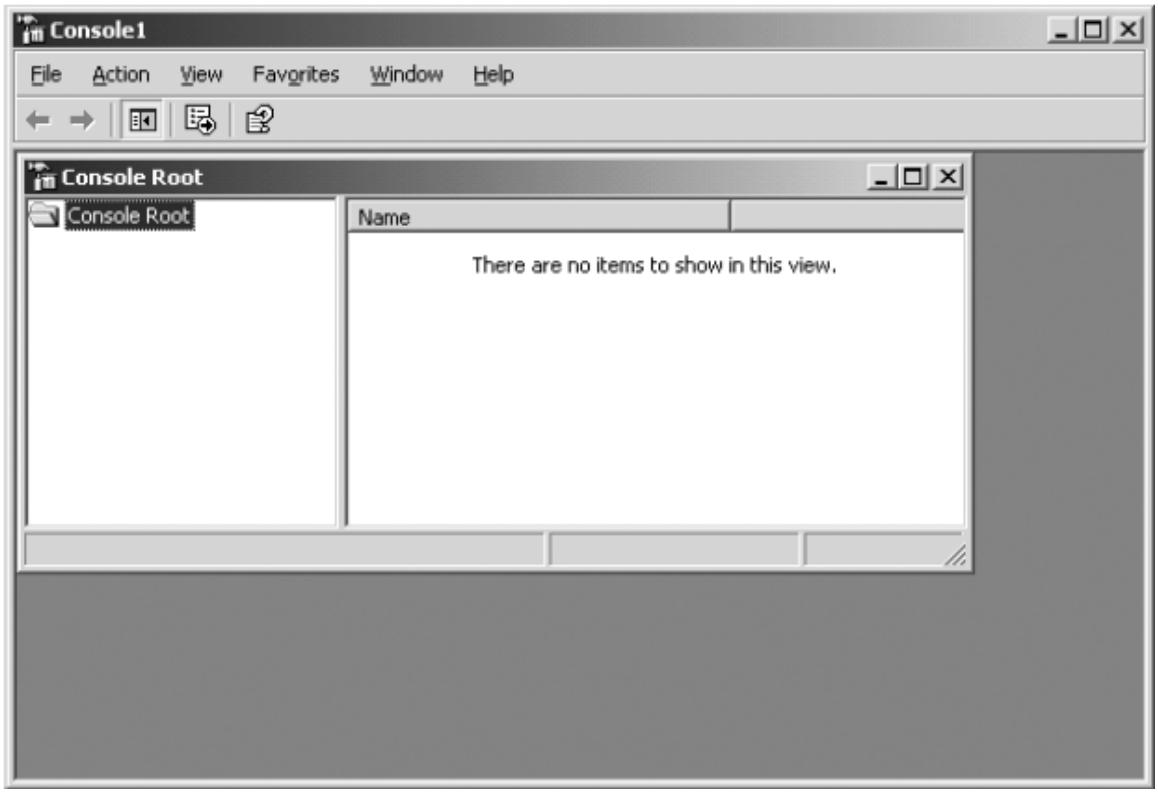
> ***LƯU Ý: Mở nhiều cửa sổ Windows***. *Không phải tất cả các bảng điều khiển MMC đều cho phép bạn có thể mở ra nhiều cửa sổ. Bạn có thể cấu hình một bảng điều khiển hoạt động ở chế độ User mode (chế độ Người dùng) để ngăn ngừa việc tạo ra các cửa sổ mới. Để có thêm thông tin về điều này, xem thêm mục "Các lựa chọn thiết lập Bảng điều khiển" trong phần sau của chương này.*

Tạo các bảng điều khiển MMC tùy chọn.

Windows Server 2003 có một tập hợp rất nhiều các MMC Snap-in, không phải tất cả đều có thể truy cập ngay thông qua các ***shortcut*** mặc định trong thực đơn ***Start*** (*Bắt đầu*). Một số công cụ rất mạnh được trang bị cùng với hệ điều hành bắt bạn phải tự tìm kiếm chúng. Các ***Developer*** (*Lập trình viên phát triển*) của các hãng phần mềm khác cũng có thể tạo ra các MMC snap-in của riêng họ và thêm vào trong các sản phẩm của họ. Điều này dẫn đến một trong những khả năng tốt nhất của MMC, đó là khả năng tạo ra các bảng điều khiển tùy chọn chứa bất kì các snap-in nào mà bạn muốn sử dụng. Bạn có thể kết hợp một hoặc nhiều snap-in hoặc một phần của các snap-in vào trong một bảng điều khiển đơn để tạo nên một giao diện đơn trong đó bạn có thể thực hiện mọi tác vụ quản trị hệ thống. Bằng cách tạo ra các MMC tùy chọn, bạn không phải chuyển giữa các chương trình hoặc các bảng điều

khiển khác nhau. Các bảng điều khiển tùy chọn có thể chứa mọi snap-in của Windows Server 2003, cho dù chúng đã được đưa vào hay không trong các bảng điều khiển cấu hình sẵn, hay các snap-in của các phần mềm khác mà bạn có.

File thực thi của MMC là ***mmc.exe***. Khi bạn chạy file này từ hộp thoại ***Run*** hoặc từ dấu nhắc dòng lệnh, một bảng điều khiển trống được tạo ra như thể hiện trong hình 2-7. Đây là một bảng điều khiển không có snap-in nào cả và khi đó các thực đơn và thanh công cụ sẽ có các chức năng mặc định của MMC. Phần tử duy nhất trong cửa sổ bảng điều khiển là ***console root object*** (*đối tượng gốc của bảng điều khiển*) nằm trong ***khung phạm vi***, nó là một khung chứa, thể hiện mức trên cùng của cấu trúc phân cấp trong bảng điều khiển. Trước khi bạn có thể thực hiện bất kì một tác vụ quản trị nào bằng bảng điều khiển này, bạn phải thêm một hoặc nhiều các snap-in vào trong đó.



Hình 2-7: Một bảng điều khiển MMC trống

Thêm các snap-in

Có hai loại snap-in như sau:

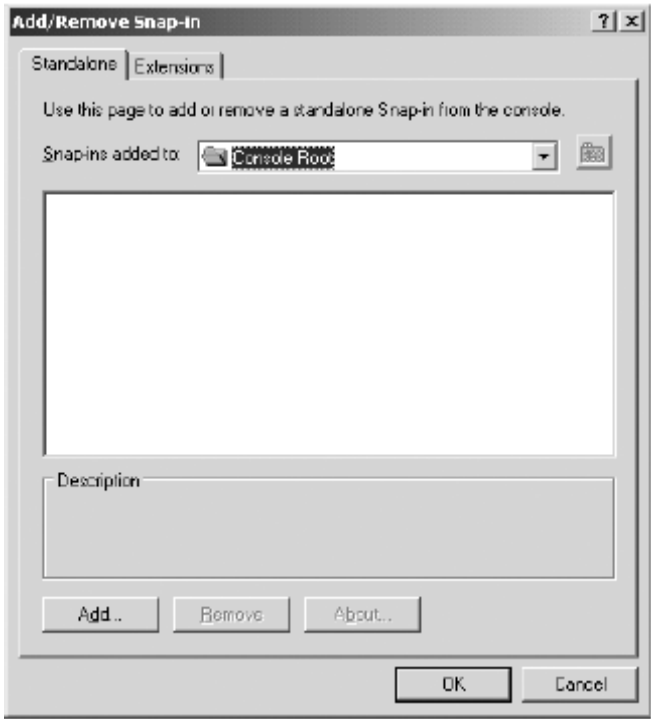
- **Đơn lẻ (StandAlone)**: Một snap-in đơn lẻ là một công cụ đơn mà bạn có thể cài đặt trực tiếp vào trong một MMC trống. Các snap-in đơn lẻ

xuất hiện trong lớp đầu tiên, nằm trực tiếp dưới gốc của bảng điều khiển trong ***khung phạm vi***.

- **Mở rộng (Extension)**: Các snap-in mở rộng cung cấp thêm tính năng cho các snap-in đơn lẻ. Bạn không thể thêm một snap-in mở rộng vào một bảng điều khiển mà trước đó chưa thêm snap-in đơn lẻ tương ứng. Các snap-in mở rộng có thể xuất hiện ở dưới các snap-in đơn lẻ tương ứng trong ***khung phạm vi*** của bảng điều khiển.

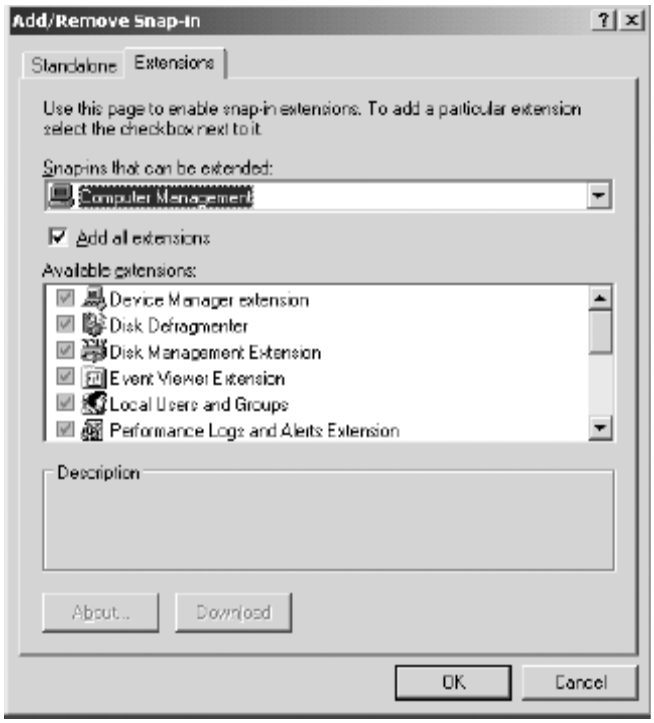
Một số snap-in sẽ cung cấp cho ta cả chức năng của một snap-in đơn lẻ và mở rộng. Ví dụ snap-in ***Event Viewer*** (*Xem sự kiện*) được sử dụng để hiển thị nội dung của các nhật kí sự kiện trong máy tính. Trong bảng điều khiển ***Computer Management***, snap-in ***Event Viewer*** xuất hiện như là một snap-in mở rộng, nằm dưới đối tượng ***System Tools*** trong khung phạm vi, tuy nhiên bạn có thể thêm snap-in ***Event Viewer*** vào một bảng điều khiển nào đó như là một snap-in đơn lẻ và khi đó nó sẽ nằm ngay dưới gốc của bảng điều khiển.

Để thêm các snap-in vào một bảng điều khiển tùy chọn, bạn lựa chọn ***Add/Remove Snap-in*** (thêm/bớt Snap-in) từ thực đơn File để hiển thị hộp thoại ***Add/Remove Snap-in*** (như thể hiện trong Hinh 2-8). Theo mặc định, thẻ ***Standalone*** trong hộp thoại này được lựa chọn, bạn nhấn ***Add*** (thêm) để hiển thị một danh sách các snap-in đơn lẻ có sẵn trong máy tính.



Hình 2-8: Hộp thoại *Add/Remove Snap-in*

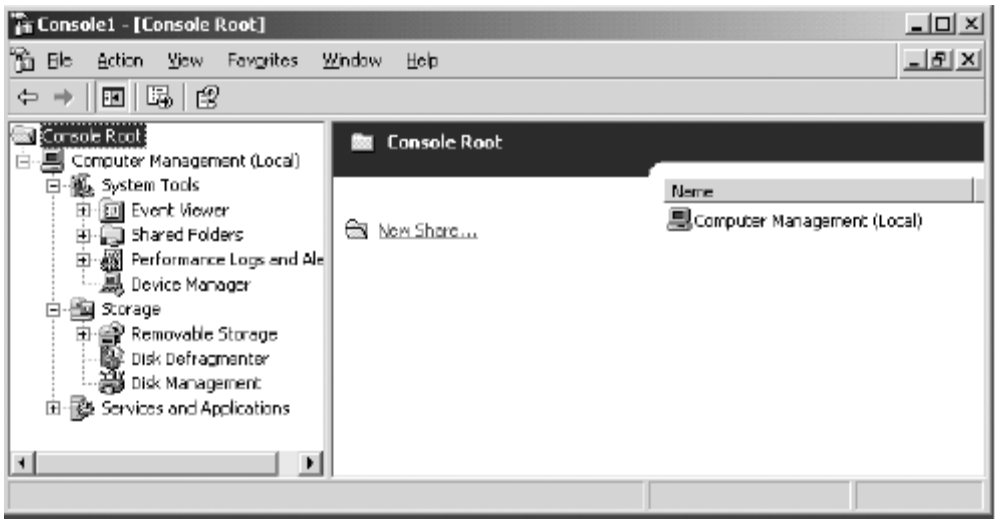
Bạn có thể lựa chọn và thêm vào bảng điều khiển bao nhiêu snap-in đơn lẻ tùy thích. Sau khi bạn thêm các snap-in đơn lẻ vào, bạn có thể trỏ vào snap-in đơn lẻ đó, lựa chọn thẻ ***Extensions*** để hiển thị một danh sách các snap-in mở rộng gắn kèm với snap-in đơn lẻ mà bạn đã chọn (Thể hiện trong hình 2-9). Sau khi bỏ đi dấu chọn trong ô "***Add All Extensions***", bạn có thể lựa chọn từng snap-in mở rộng mà bạn muốn thêm vào bảng điều khiển này. Sử dụng danh sách xổ xuống trong mục "***Snap-in Added To***", bạn có thể chỉ định snap-in mở rộng được thêm này sẽ nằm ngay dưới gốc của bảng điều khiển hay ở dưới các phần tử khác trong cây.



Hình 2-9: Thẻ *Extension* trong hộp thoại *Add/Remove Snap-in*

Tạo các Taskpad (Bảng Tác vụ)

Khi bạn đã nhập xong các snap-in vào trong bảng điều khiển tùy chọn của mình, bán có thể tạo thêm các ***taskpad*** tùy chọn. ***Taskpad*** là một vùng nằm trong ***khung chi tiết***, dành cho một số snap-in nhất định, chứa các liên kết đến các chức năng thường xuyên được snap-in này sử dụng (Thể hiện trong hình 2-10). Để tạo ra một ***taskpad***, bạn chọn một snap-in trong "***khung phạm vi***" và lựa chọn "***New Taskpad View***" từ thực đơn ***Action***. Trình hướng dẫn "***New Taskpad View Wizard***" sẽ hướng dẫn bạn các thao tác để xác định vị trí và cách thức xuất hiện của ***taskpad.*** Sau khi tạo ra ***taskpad***, bạn có thể chạy trình hướng dẫn "***New Task Wizard***" để tạo ra các kết nối trong ***taskpad*** này.



Hình 2-10: Một bảng điều khiển MMC với *taskpad*

Các tùy chọn thiết lập bảng điều khiển.

Khi bạn đã thêm các snap-in bạn muốn vào trong các bảng điều khiển MMC, bạn có thể thiết lập các lựa chọn chỉ định người dùng khác có thể thay đổi cái gì trong cấu hình của bảng điều khiển này. Chọn ***Options*** từ thực đơn ***File*** để hiện thị hộp thoại ***Options***, trong đó bạn có thể chỉ định tên hiển thị trên thanh tiêu đề của bảng điều khiển, và lựa chọn chế độ cho bảng điều khiển.

Theo mặc định, mọi bảng điều khiển mới bạn tạo ra đều được cấu hình sử dụng chế độ ***Author mode*** (*Chế độ tác giả*) cho phép toàn quyền truy cập đến đến mọi chức năng của bảng điều khiển. Các chế độ mà bạn có thể lựa chọn như sau:

- **Author Mode**: Cung cấp toàn quyền truy cập bảng điều khiển, bao gồm khả năng thêm hoặc bớt các snap-in, tạo thêm cửa sổ, tạo các taskpad view và các tác vụ, xem toàn bộ thông tin trong cây bảng điều khiển, thay đổi các lựa chọn và lưu cấu hình của bảng điều khiển.
- **User Mode: Full Access (Chế độ người dùng - Toàn quyền truy cập):** Cho phép người dùng có quyền duyệt qua các snap-in và các cửa sổ để truy cập đến mọi thành phần của cây bảng điều khiển. Cấm người dùng thêm/bớt các snap-in hoặc thay đổi các thuộc tính của bảng điều khiển.
- **User Mode: Limited Access, Multiple Windows (Chế độ người dùng – Hạn chế truy cập, nhiều cửa sổ):** Cho phép ngườidùng tạo cửa sổ mới và xem nhiều cửa sổ trong bảng điều khiển nhưng không cho phép đóng bớt các cửa sổ sẵn có.

- **User Mode: Limited Access, Single Window: (Chế độ người dùng – Hạn chế truy cập, một cửa sổ):** Không cho phép người dùng mở thêm cửa sổ mới và chỉ cho phép xem một cửa sổ trong bảng điều khiển

Các chế độ trong bảng điều khiển cho phép bạn tạo ra các bảng điều khiển cho những người dùng có khả năng hạn chế và những người dùng không được phép thay đổi bảng điều khiển. Các thiết lập chế độ trong bảng điều khiển chính là lí do tại sao bạn không thể thêm các snap-in vào trong các bảng điều khiển được cấu hình sẵn do Windows Server 2003 cung cấp.

Lưu các bảng điều khiển MMC.

Khi bạn cấu hình xong một bảng điều khiển tùy chọn đúng như bạn mong muốn, bạn phải lưu nó lại thành một file để sau đó bạn có thể tiếp tục sử dụng. File bảng điều khiển MMC có phần mở rộng .msc và sẽ được gắn với ứng dụng ***mmc.exe***, do đó khi mở một file bảng điều khiển, hệ thống sẽ nạp chương trình ***mmc.exe*** và mở file đó. Theo mặc định, các bảng điều khiển được lưu trong thư mục "***Administrative Tools***" trong "***User profile***" (Khái lược người dùng) và do đó nó sẽ xuất hiện như một ***shortcut*** trong nhóm chương trình ***Administrative Tools*** của thực đơn ***Start*** .

> ***LƯU Ý: shortcut Bảng điều khiển***. ***Shortcut*** *cho bảng điều khiển tùy chọn của bạn chỉ xuất hiện trong nhóm chương trình* ***All Programs/Administrative Tools,*** *không phải trong nhóm* ***Administrative Tools*** *của bản thân thực đơn* ***Start***

Kết nối đến các máy tính ở xa

Các bảng điều khiển MMC xuất hiện trong thực đơn Start của một máy tính chạy Windows Server 2003 đều được cấu hình để quản lý các tài nguyên trong nội bộ máy tính đó. Tuy nhiên, với hầu hết các snap-in được cung cấp trong Windows Server 2003, bạn cũng có thể quản lý các máy tính khác qua mạng. Đây là một trong những tính năng hữu ích nhất của MMC bởi vì nó cho phép các nhà quản trị mạng có thể quản trị các máy tính ở bất kì đâu trong mạng từ màn hình máy trạm của mình.

> ***LƯU Ý: Mục đích của kỳ thi***. *Mục đích của kỳ thi 70-290 là học viên có khả năng "quản trị máy chủ từ xa" và "quản trị máy chủ bằng cách sử dụng các công cụ hỗ trợ sẵn có"*

Bạn có thể truy cập vào một máy tính ở xa sử dụng một MMC snap-in bằng hai cách:

- Hướng các snap-in có sẵn vào máy tính khác
- Tạo một bảng điều khiển tùy chọn với các snap-in trỏ đến các hệ thống khác.

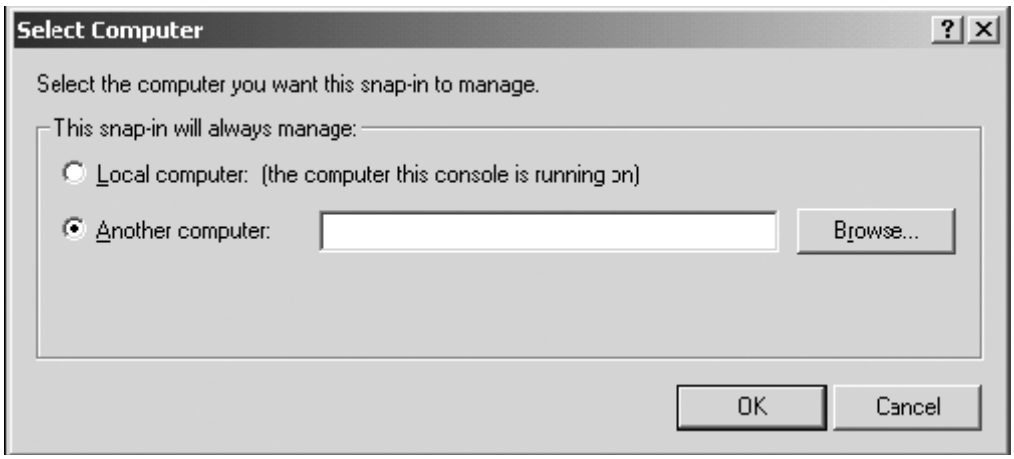
Để kết nối và quản trị hệ thống khác sử dụng MMC snap-in, bạn phải nạp bảng điều khiển đó bằng một tài khoản có quyền quản trị trên máy tính ở xa.

Cấp phép cần thiết chính xác tùy thuộc vào chức năng mà snap-in thực hiện. Nếu tài khoản sử dụng không có đủ quyền trên máy tính ở xa, bạn sẽ có khả năng nạp snap-in nhưng không thể đọc thông tin hoặc chỉnh sửa các thiết lập cấu hình trên máy tính đó.

> ***LƯU Ý: Sử dung "Run as"****. Nếu bạn biết tài khoản bạn đang sử dụng không có đủ các cấp phép cần thiết để quản lý máy tính ở xa, bạn có thể sử dụng tính năng "Run as" - còn gọi là đăng nhập thứ cấp – để chạy bảng điều khiển với tài khoản khác có các quyền thích hợp với các tác vụ mà bạn muốn thực hiện.*

Định hướng cho snap-in.

Một snap-in sẽ được hướng đến một hệ thống xác định bằng cách sử dụng lệnh "***Connect To Another Computer***" trong thực đơn ***Action***. Lựa chọn lệnh này sẽ mở ra một hộp thoại "***Select Computer***" (Như thể hiện trên Hình 2-11), trong đó bạn có thể nhập vào tên của máy tính bạn muốn quản trị và nhấn ***OK***, các phần tử của snap-in trong khung phạm vi sẽ thay đổi thể hiện tên của máy tính mà bạn vừa lựa chọn.



Hình 2-11: Hộp thoại *Select Computer*

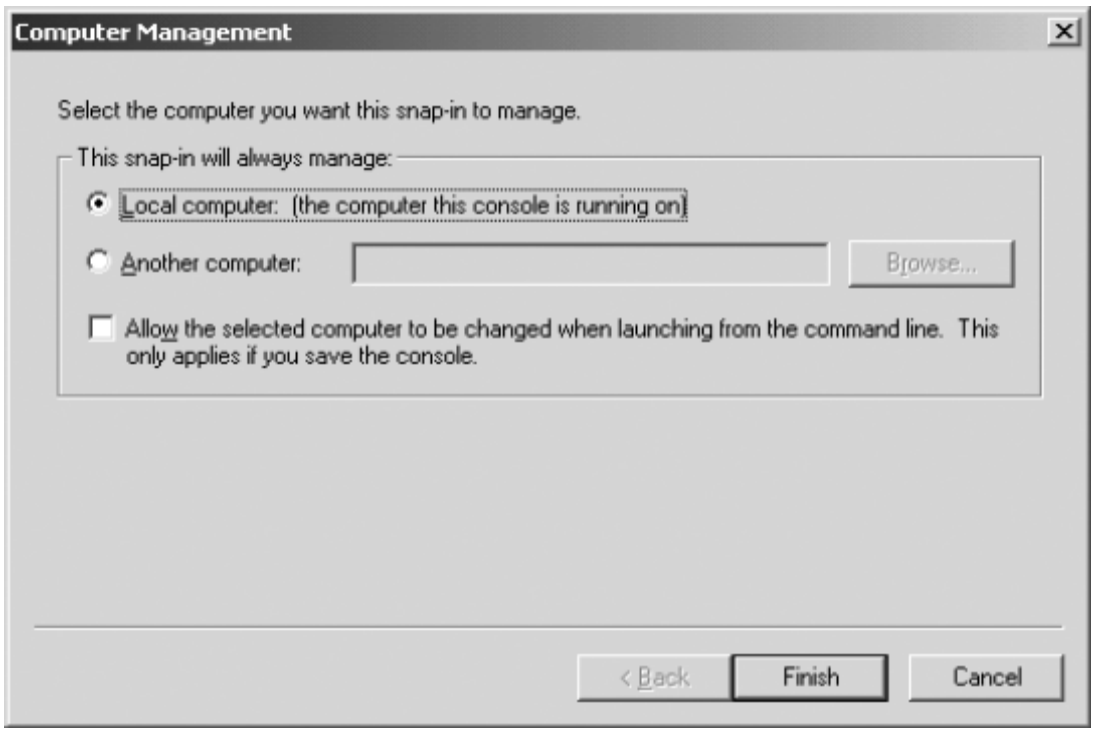
Không phải tất cả các snap-in đều có khả năng kết nối đến các máy tính ở xa bởi vì một số snap-in không cần điều này. Ví dụ bảng điều khiển quản trị ***Active Directory*** sẽ tự động tìm đến máy chủ quản trị miền trong mạng và

truy cập vào CSDL ***Active Directory*** tại đó, do đó không cần phải nhập vào tên máy tính.

Tạo một bảng điều khiển kết nối từ xa.

Kết nối đến một máy tính ở xa bằng cách định hướng một bảng điều khiển sẵn có là cách rất tiện dụng để thực hiện các tác vụ quản trị, nhưng nó lại bị giới hạn bởi thực tế là bạn có thể chỉ được truy cập đến một máy tính trong một thời điểm. Bạn có thể mở một bảng điều khiển và định hướng mỗi khi bạn muốn truy cập đến hệ thống ở xa. Một phương pháp cố định hơn là tạo ra một bảng điều khiển tùy chọn với các snap-in đã được định hướng sẵn đến các hệ thống khác.

Khi bạn thêm một snap-in vào một bảng điều khiển tùy chọn bằng cách chọn nó trong danh sách các snap-in và nhấn nút Add, bạn có thể thấy một hộp thoại trong đó bạn có thể lựa chọn snap-in này sẽ quản lý máy tính nào, như thể hiện trong Hình 2-12. Điều này sẽ làm tăng khả năng của quản trị của các MMC, bạn không chỉ tạo ra các bảng điều khiển với rất nhiều công cụ trong đó mà bạn còn có thể sử dụng các công cụ đó với nhiều máy tính trong hệ thống. Ví dụ, bạn có thể tạo ra một bảng điều khiển đơn chứa rất nhiều snap-in "***Computer Management***" trong đó mỗi snap-in trỏ đến một máy tính khác nhau. Điều này cho phép bạn có thể quản trị các máy tính Windows Server 2003, Windows XP và Windows 2000 trên toàn mạng từ một bảng điều khiển đơn duy nhất.



Hình 2-12*: Hộp thoại *Computer Management

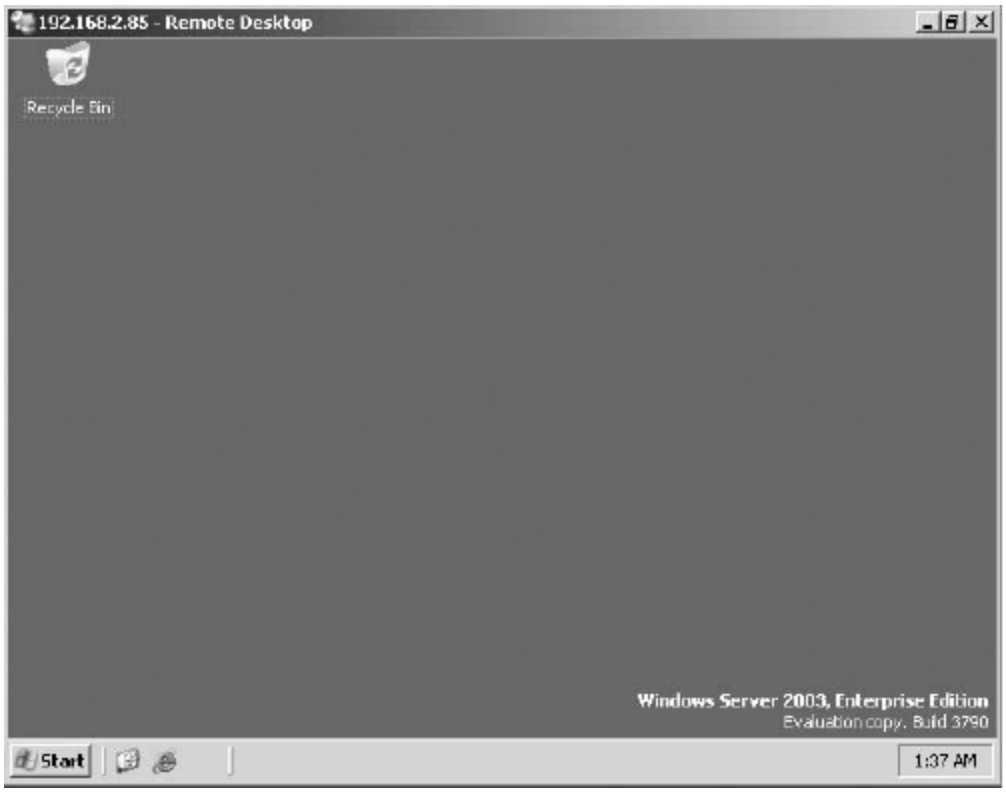
QUẢN TRỊ MÁY CHỦ BẰNG "REMOTE DESKTOP FOR ADMINISTRATION" (MÀN HÌNH QUẢN TRỊ TỪ XA)

Trong Windows 2000, ***Terminal Services*** (Dịch vụ đầu cuối) là một thành phần phải cài đặt riêng, còn với Windows Server 2003 nó được cài đặt mặc định bởi hệ điều hành coi dịch vụ này như là một thành phần được tíchh hợp sẵn của chúng. Bằng cách mua và cấu hình giấy phép hợp lý, bạn có thể cấu hình một máy tính chạy Windows Server 2003 để phục vụ các máy khách ***Terminal Services***, cung cấp khả năng truy cập màn hình Windows và các ứng dụng trên máy chủ này.

Tuy nhiên, ***Terminal Services*** không chỉ có chức năng hỗ trợ các máy khách ***Terminal Services***. Bạn có thể sử dụng ***Terminal Services*** truy cập đến các máy tính ở xa để thực hiện các tác vụ quản trị mà không cần khả năng chia sẻ ứng dụng. Windows Server 2003 gọi đó là tính năng "***Remote Desktop for Administration***" (Màn hình Quản trị Từ xa). Hệ điều hành cho phép tối đa 02 kết nối "***Remote Desktop for Administration***" đồng thời mà không yêu cầu bất kì giấy phép nào và sử dụng rất ít tài nguyên hệ thống.

> ***LƯU Ý: Mục đích của kỳ thi.*** *Mục đích của kỳ thi 70-290 là học viên có khả năng "quản trị máy chủ bằng cách sử dụng Terminal Services theo chế độ quản trị từ xa"*

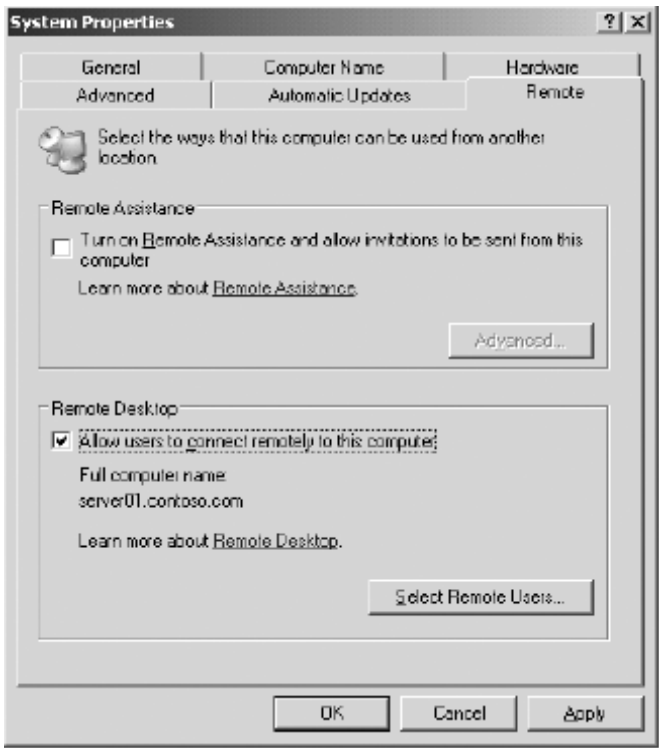
Sử dụng bảng điều khiển MMC, bạn có thể kết nối đến một máy tính ở xa và thực hiện rất nhiều tác vụ quản trị, tuy nhiên một quản trị mạng đôi khi cần truy cập một cách toàn phần đến máy tính đó. ***Terminal Services*** trong Windows Server 2003 cho phép một phần mềm máy khách có tên "***Remote Desktop Connection***" (Kết nối Màn hình Từ xa) chạy trên một máy tính khác để kết nối đến máy chủ và truy cập đến mọi thành phần trong máy chủ này. Cửa sổ màn hình của máy khách hiển thị màn hình của máy chủ, cho phép người dùng có thể truy cập đến mọi công cụ và điều khiển tiêu chuẩn trên máy chủ và thậm chí còn có thể chạy các ứng dụng trên máy chủ này. (Thể hiện trong Hình 2-13)



Hình 1-13*: Một phiên làm việc *Remote Desktop

Kích hoạt và Cấu hình Máy chủ Remote Desktop

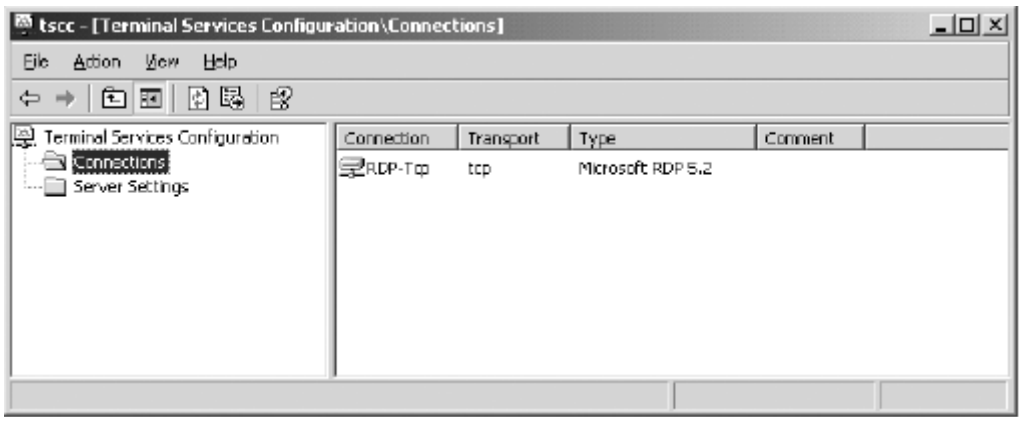
Bởi vì mọi thành phần cần thiết để thực hiện kết nối "***Remote Desktop for Administration***" đều đã được cài đặt mặc định trong hệ điều hành Windows Server 2003, do đó việc kích hoạt ứng dụng ở phía máy chủ là công việc đơn giản. Trong thẻ ***Remote*** của hộp thoại "***System Properties***" – Các thuộc tính Hệ thống - (Truy cập đến hộp thoại này bằng cách chọn biểu tượng System trong bảng điều khiển ***Control Panel***), lựa chọn "***Allow Users To Connect Remotely To This Computer***" (Cho phép người dùng kết nối từ xa đến máy tính này) (Như hiển thị trong hình 2-14). Theo mặc định, thành viên của nhóm ***Administrators*** cục bộ của máy tính có quyền truy cập từ xa đến máy tính này. Để cho phép người dùng khác có thể truy cập đến máy tính bằng ***Remote Desktop***, bạn phải chọn mục "***Select Remote Users***" và thêm tài khoản của người dùng này vào danh sách cho phép.



Hình 1-14: Thẻ Remote trong hộp thoại System Properties

Việc chọn lựa chọn này là tất cả các việc bạn phải làm để kích hoạt máy chủ ***Remote Desktop*** trong Windows Server 2003. Tuy nhiên, bạn cũng có thể cấu hình các thuộc tính của máy chủ ***Remote Desktop*** bằng cách sử dụng snap-in ***Terminal Services Configuration*** trong MMC (Như thể hiện trong Hình 2-15).

> ***LƯU Ý: Terminal Services và Máy chủ quản trị miền (DC)****. Theo mặc định, máy chủ quản trị miền được cấu hình chấp nhận các kết nối* ***Terminal Services*** *chỉ từ các thành viên trong nhóm* ***Administrators****. Thậm chí những người dùng mà bạn đã tự tay thêm vào nhóm* ***Remote Desktop Users*** *cũng không thể truy cập được. Để loại bỏ hạn chế này, bạn phải thay đổi giá trị hiệu lực của khóa "****Allow Log On Through Terminal Services****" (Cho phép đăng nhập từ* ***Terminal Service****s) trong chính sách nhóm, mà theo mặc định danh sách liệt kê trong khóa này chỉ có nhóm Administrators. Để làm điều này, bạn có thể chỉnh sửa chính sách nội bộ (****Local computer policy****) của máy chủ quản trị miền hoặc định nghĩa các thiết lập tương tự trong đối tượng chính sách nhóm (GPO) mà gắn với các đối tượng* ***Active Directory*** *chứa các máy chủ này, Ví dụ như "****Default Domain Controller Policy*** *– GPO". (Chính sách Mặc định cho Máy chủ Quản trị Miền)*

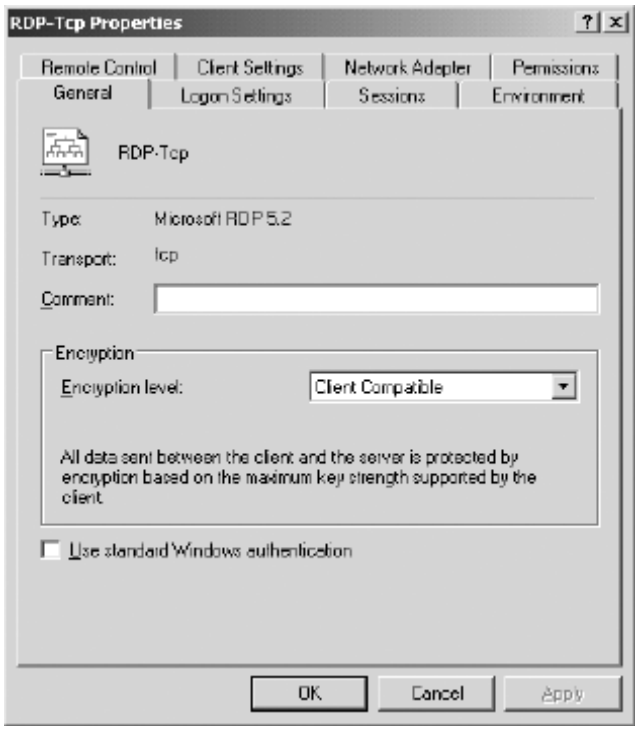


***Hình 2-15*: Snap-in "*Terminal Services Configuration*"**

Để cấu hình các thuộc tính của máy chủ ***Remote Desktop***, ta thêm snap-in có tên "***Terminal Services Configuration***" vào bảng điều khiển MMC. Nhấn vào thư mục ***Connnections*** trong khung phạm vi, lựa chọn kết nối ***RDP-Tcp*** liệt kê trong khung chi tiết và từ thực đơn ***Action***, lựa chọn ***Properties***. Hộp thoại ***RDP-Tcp Properties*** xuất hiện.

Sử dụng các thẻ trong hộp thoại này, bạn có thể cấu hình rất nhiều thuộc tính của máy chủ như sau:

- **General (Tổng quan):** Thiết lập mức mã hóa và kĩ thuật xác thực cho kết nối đến máy chủ.



- **"Logon setting" (Thiết lập đăng nhập):** Cho phép bạn xác định các thông số đăng nhập được sử dụng trong các kết nối đến máy chủ thay cho các thông số đăng nhập do máy khách cung cấp.
- **Sessions (Phiên làm việc):** Chứa các thiết lập có quyền ưu tiên hơn các thiết lập của máy khách, chỉ ra khi nào kết thúc một phiên kết nối, giới hạn thời gian kết nối và thời gian nghỉ cho phép của phiên, đồng thời chỉ ra có cho phép kết nối lại hay không.
- **Environment (Môi trường):** Phủ nhận các thiết lập của máy khách và cấu hình trong ***User profile*** (Khái lược người dùng) để chạy một chương trình nào đó khi kết nối đến máy chủ.
- **Remote Control (Điều khiển từ xa)**: Chỉ ra khả năng điều khiển từ xa của phiên làm việc "***Remote Desktop Connection***" có thực hiện được hay không và nếu được thì liệu người dùng có bắt buộc phải gán các quyền khi khởi tạo một phiên làm việc từ xa hay không. Các thiết lập phụ thêm có thể hạn chế phiên làm việc từ xa chỉ cho phép xem hoặc cho phép toàn quyền tương tác với hệ thống.
- **Client Setting (Các thiết lập với máy khách)**: Phủ nhận các thiết lập trên máy khách về căn chỉnh độ sâu màu sắc và việc ánh xạ các tài nguyên.
- **Network Adapter (card mạng):** Xác định card mạng nào trên máy chủ có thể tiếp nhận các kết nối "***Remote Desktop for Administration***"
- **Permissions (Cấp phép)**: Xác định các quyền được cấp của các kết nối ***Remote Desktop***.

Cài đặt và Cấu hình Remote Desktop Connection (Kết nối tới Màn hình Từ xa)

Một máy tính khi tạo kết nối đến máy chủ Remote Desktop, nó phải chạy một chương trình có tên "***Remote Desktop Connection***". Chương trình máy khách này được cài đặt theo mặc định trong hệ điều hành Windows Server 2003 và Windows XP, tuy nhiên nó còn có thể chạy trên bất kì phiên bản Windows 32 bit nào. Windows Server 2003 có các file cài đặt của Remote Desktop Connection trong đĩa CD cài đặt đồng thời nó còn được chép vào trong thư mục ***Systemroot\System32\Clients\Tsclient\Win32***. Bạn có thể cài đặt phần mềm máy khách này trên bất kì một máy tính nào từ cả hai bộ cài này bằng cách sử dụng các thao tác sau:

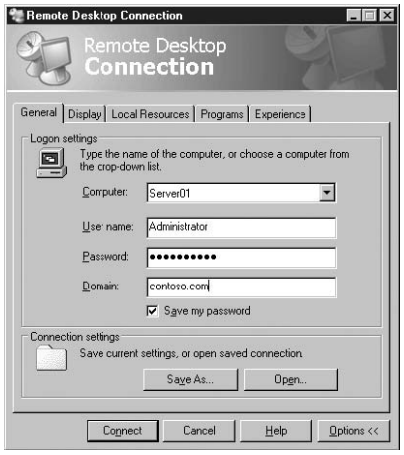
- **Từ đĩa CD**: Cho đĩa CD cài đặt Windows Server 2003 vào trong ổ. Khi màn hình Welcome to Microsoft Windows Server 2003 xuất hiện, nhấn vào liên kết "***Perform Additional Tasks***" (thực hiện các tác vụ khác) và chọn "***Set Up Remote Desktop Connection***" (Cài đặt Kết nối Màn hình Từ xa". Làm theo các chỉ thị hiển thị trên màn hình của Trình Hướng dẫn Cài đặt Kết nối Màn hình Từ xa (***Remote Desktop Connection" – InstallShield Wizard***)
- **Từ trên mạng**: Tạo một thư mục chia sẻ từ thư mục ***Systemroot\System32\Clients\Tsclient\Win32***. Kết nối đến thư mục chia sẻ này từ máy tính khách và chạy file ***Setup.exe***. Làm theo các chỉ thị hiển thị trên màn hình của trình hướng dẫn "***Remote Desktop Connection – InstallShield Wizard***"

  HƯỚNG DẪN NHANH Cập nhật Máy khách: *Bạn nên nâng cấp các máy tính chạy các phiên bản trước của dịch vụ Terminal máy khách bằng phiên bản mới nhất của "**Remote Destop Connection**" để nhận được các tính năng ưu việt của nó như: Giao diện người dùng được sửa lại, Mã hóa 128 bit, và Lựa chọn Cổng Thay thế,*

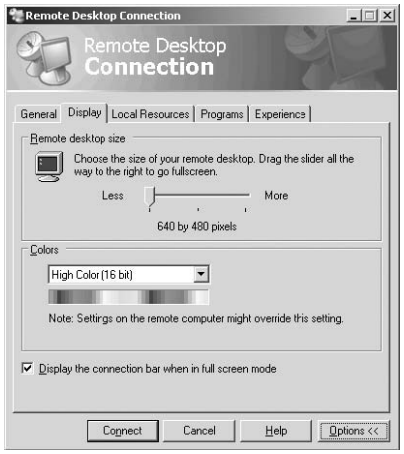
Khi chương trình đã được cài đặt, bạn có thể kết nối đến máy chủ bằng cách chạy chương trình thông qua ***shortcut "Remote Desktop Connection***" trong thực đơn ***Start*** và cấu hình máy khách thông qua hộp thoại "***Remote Desktop Connection***". Các thẻ trong hộp thoại này cho phép bạn cấu hình các tham số máy khách như sau:

> ***LƯU Ý: Xem các lựa chọn máy khách****: Nhấn chuột vào nút Options (các lựa chọn)để hiển thị toàn bộ hộp thoại "**Remote Desktop Connection**"*

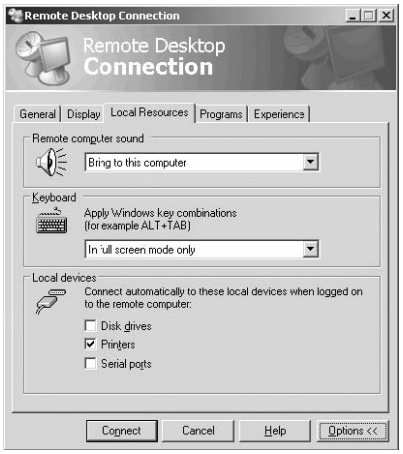
- **General (Tổng quan)**: Cho phép bạn xác định máy khách này kết nối đến máy chủ nào, các thông số mà máy khách sử dụng để đăng nhập và liệu có lưu các thiết lập cấu hình cho kết nối này hay không.



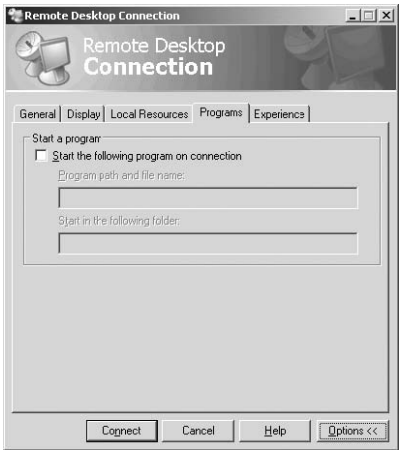
- **Display (Hiển thị):** Cho phép bạn xác định kích thước của cửa sổ Remote Desktop, độ sâu màu và liệu các thanh kết nối có xuất hiện hay không trong chế độ toàn màn hình.



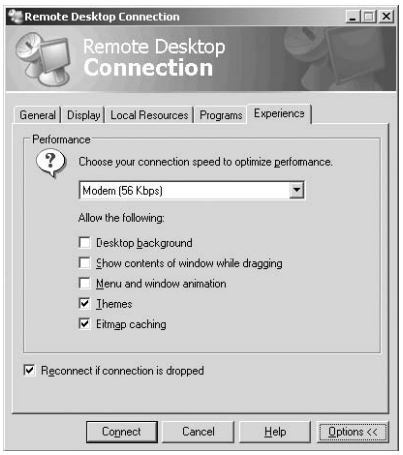
- **Local Resource (Tài nguyên nội bộ):** Cho phép bạn cấu hình liệu có truyền các tín hiệu âm thanh trên máy chủ đến máy khách hay không, cách thức kết hợp phím của Windows thể hiện trên máy ở xa như thế nào và liệu đĩa cứng, máy in và kết nối bằng cổng serial có gắn vào phiên làm việc từ xa này không. Ví dụ lựa chọn ***Disk Drives*** sẽ cho phép các đĩa cứng trên máy khách sẽ xuất hiện trong phiên kết nối Remote Desktop như là các đĩa cứng cục bộ của máy chủ



- **Programs (Chương trình):** Cho phép bạn xác định tên và thư mục khởi đầu cho một ứng dụng sẽ được nạp ngay khi kết nối từ xa được thiết lập.



- **Experience (Kinh nghiệm):** Cho phép bạn xác định tốc độ của kết nôi giữa máy khách và máy chủ và vô hiệu hóa một số thuộc tính của màn hình hiển thị để tăng băng thông kết nối và tăng khả năng giao tiếp giữa máy khách và máy chủ.



> ***LƯU Ý: "Remote Desktop" và "Terminal Services"****."Remote Desktop for Administration" và "Terminal Services" sử dụng chung rất nhiều thành phần. Với một giấy phép thích hợp, người dùng mạng có thể sử dụng cùng máy khách truy cập một máy chủ terminal để chạy một ứng dụng chia sẻ nào đó hoặc sử dụng "Remote Desktop for Administration".*

Khắc phục các sự cố của Terminal Services

Khi bạn sử dụng "***Remote Desktop for Administration***", bạn tạo ra một kết nối giữa chương trình máy khách và một máy chủ. "***Remote Desktop for Administration***" sử dụng cùng kiểu kết nối giống như ***Terminal Services*** sử dụng để chạy các ứng dụng chia sẻ, và do đó các nguyên nhân của các sự cố kết nối cũng sẽ giống nhau. Trong trường hợp một kết nối bị đứt hoặc phiên làm việc không thể sử dụng vì lý do nào đó, nguyên nhân có thể xác định theo các phán đoán sau:

> ***LƯU Ý: Mục đích của kỳ thi.*** *Mục đích của kỳ thi 70-290 là học viên phải có khả năng "Xử lý các Sự cố của Terminal Services", "Chẩn đoán và Giải quyết các vấn đề liên quan đến Bảo mật Terminal Services" và "Chẩn đoán và Giải quyết các vấn đề liên quan đến các Truy cập của Máy khách đến Máy chủ Terminal Services"*

- **Kết nối mạng hỏng**: Với bất kì ứng dụng nào dựa trên kết nối máy chủ/máy khách, các sự cố thường do trục trặc đường kết nối mạng, ví dụ như các thiết lập cấu hình của TCP/IP không đúng, trục trặc trong vấn đề phân giải tên DNS, vấn đề định tuyến hoặc phần cứng mạng hoạt động không tốt. Bạn có thể kiểm tra các kết nối mạng bằng cách xem các ứng dụng mạng khác có hoạt động tốt hay không, thử kết nối sử dụng IP thay vì dùng tên DNS và xem các người dùng khác có bị hiện tượng tương tự hay không. Kiểm tra các thiết lập TCP/IP trên các máy chủ và máy khách xem có chính xác chưa, kiểm tra máy chủ DNS có hoạt động tốt không và các phần cứng mạng có trục trặc gì không.
- **Các thiết lập cổng**: ***Terminal Services*** sử dụng cổng TCP và UDP 3389 cho tất cả các kết nối giữa máy chủ và máy khách theo mặc định. Nếu hoặc máy chủ hay máy khách được cấu hình sử dụng các cổng khác nhau hoặc nếu vì một lý do nào đó cổng này bị chặn lại (Ví dụ như Tường lửa), kết nối giữa máy chủ và máy khách sẽ không thực hiện được.

- **Các thông số cấp phép (Credential):** người dùng phải thuộc nhóm ***Administrators*** hoặc "***Remote Desktop Users***" để có thể kết nối đến các máy chủ bằng "***Remote Desktop for Administration***". Hơn nữa, bạn có thể chặn các kết nối từ một người dùng xác định bằng cách kích hoạt quyền người dùng "***Deny Logon Through Terminal Services***" (Từ chối Truy cập thông qua Dịch vụ Dầu cuối) trong chính sách bảo mật nội bộ hoặc sử dung chính sách nhóm (GP).
- **Số lượng các kết nối**: Nếu phiên làm việc người dùng bị ngắt khi người dùng chưa log off, máy chủ có thể coi kết nối đó vẫn mở và điều này có thể dẫn tới việc đạt đến giới hạn kết nối mặc dù có không quá hai người đang kết nối tại thời điểm đó. "***Remote Desktop for Administration***" cho phép tối đa hai kết nối tại cùng một thời điểm.

SỬ DỤNG REMOTE ASSISTANCE

Remote Desktop được thiết kế để cung cấp các truy cập quản trị từ xa đến máy tính, tuy nhiên các người dùng cuối đôi khi cũng có thể tận dụng khả năng này. Rất nhiều người dùng, nhất là những người không có khả năng kĩ thuật tốt, hay có các vấn dề về cấu hình và có cách đặt các câu hỏi mà các chuyên gia hỗ trợ (thậm chí là bạn bè, người thân) khó có thể giải quyết hoặc trả lời thông qua điện thoại. "***Remote Assistance***" là một biến thể khác của "***Terminal Services***" cho phép người dùng có thể yêu cầu sự giúp đỡ từ một người dùng khác ở xa và nhận sự giúp đỡ này thống qua các hướng dẫn hoặc làm mẫu ngay trên màn hình của họ mà không cần phải đến tận nơi. "***Remote Assistance***" cho phép người giúp đỡ (hoặc chuyên gia theo cách mà các ứng dụng vẫn đề cập đến) có thể hỗ trợ, giải quyết sự cố và thậm chí đào tạo người dùng khi họ cần, với chi phí thấp và thời gian trễ rất nhỏ.

> ***LƯU Ý: Mục dích của kỳ thi***. *Mục đích của kỳ thi 70-290 là học viên có thể "Quản trị Máy chủ Từ xa Sử dụng Remote Assistance"*

Kích hoạt Remote Assistance

Trước khi bạn có thể nhận được các trợ giúp từ xa, bạn phải kích hoạt chức năng này bằng một trong các cách sau:

- **Sử dụng Control Panel**: Mở "***System Properties***" trong "***Control Panel***" và lựa chọn thẻ ***Remote***. Đánh dầu chọn "***Turn On Remote Assistance And Allow Invitations To Be Sent From This Computer***" (Bật chức năng hỗ trợ từ xa và cho phép các đề nghị có thể gửi đi từ máy tính này). Nhấn vào phím ***Advance***, bạn có thể cấu hình cho phép chuyên gia nắm toàn quyền điều khiển máy tính hoặc chỉ cho phép

xem các hoạt động trên máy tính, đồng thời xác định thời gian có hiệu lực của lời đề nghị giúp đỡ từ xa.

- **Sử dụng Chính sách nhóm**: Sử dụng bảng điều khiển "***Group Policy Object Editor***" (***gpedit.msc***) để mở một GPO của một miền hoặc một OU chứa các máy khách. Duyệt đến mục ***Computer Configuration\Administrative Templates\System\Remote Assistance*** và kích hoạt chính sách "***Solicited Remote Assistance***" (Thu hút các hỗ trợ từ xa). Chính sách này sẽ cho phép bạn có thể xác định mức độ điều khiển của chuyên gia trên máy khách, khoảng thời gian hiệu lực của lời đề nghị giúp đỡ và phương pháp gửi thư đề nghị. Chính sách "***Offer Remote Assistance***" (Đề xuất Hỗ trợ Từ xa) cho phép bạn xác định tên người dùng hoặc nhóm được gọi là chuyên gia và liệu các chuyên gia này có thể thực hiện các tác vụ trên máy khách hay chỉ quan sát theo dõi máy khách mà thôi.

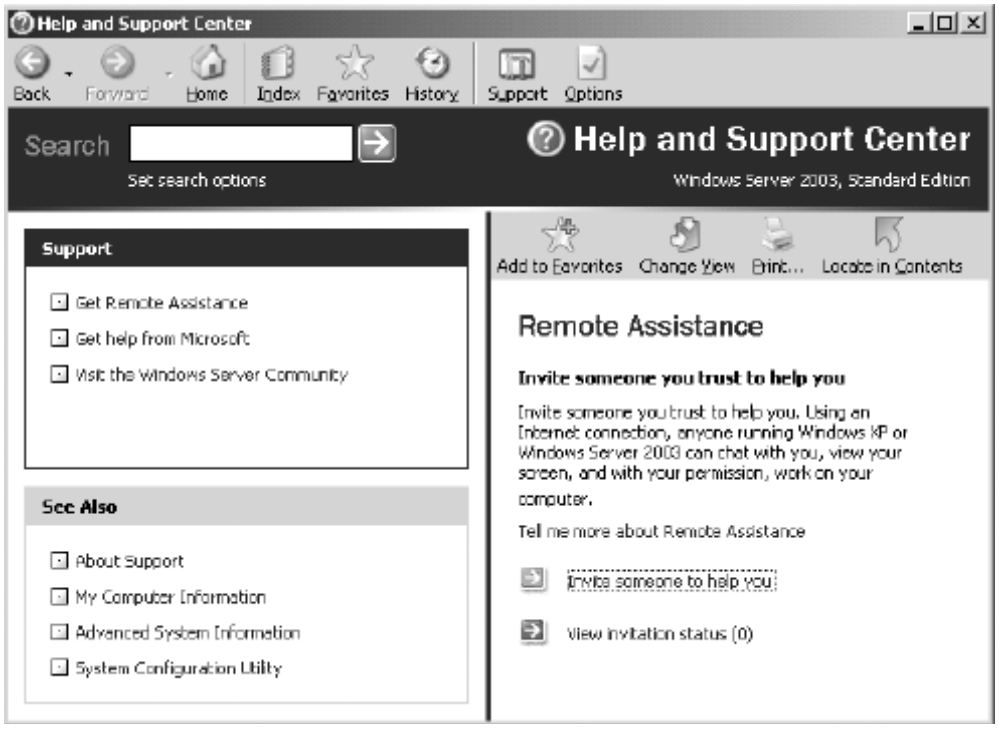
Tạo lời đề nghị

Để nhận được các trợ giúp từ xa, một máy khách phải đưa ra lời đề nghị và gửi nó đến một chuyên gia nào đó. Máy khách có thể gửi lời đề nghị này sử dụng một trong các phương pháp sau đây.

- **Microsoft Windows Messenger (Dịch vụ Truyền thông điệp của Windows)**: Để sử dụng dịch vụ Windows Messenger cho kết nối ***Remote Assistance***, bạn phải có tên tài khoản Windows Messenger của chuyên gia trong danh sách liên lạc và gửi yêu cầu trực tiếp từ Windows Messenger trên máy khách. ***Remote Assistance*** chỉ được phép yêu cầu trực tiếp khi chuyên gia đang trực tuyến trên mạng (***online***)
- **Thư điện tử**: Để gửi một lời đề nghị bằng thư điện tử, cả hai máy tính đều phải là các máy trạm tương thích và có khả năng truyền/nhận thư điện tử bằng giao thức MAPI (***Messaging Application Programming Interface*** – Giao diện Lập trình Ứng dụng Truyền thông điệp)
- **File**: Khi bạn lưu lời đề nghị vào một file, bạn có thể sử dụng bất kì phương thức nào để gửi file đó đến chuyên gia,có thể bằng thư điện tử (không cần thiết phải sử dụng giao thức MAPI), bằng một giao dịch FTP (***File Tranfer Protocol*** – Giao thức Truyền File trên Internet) hay sử dụng đĩa mềm.

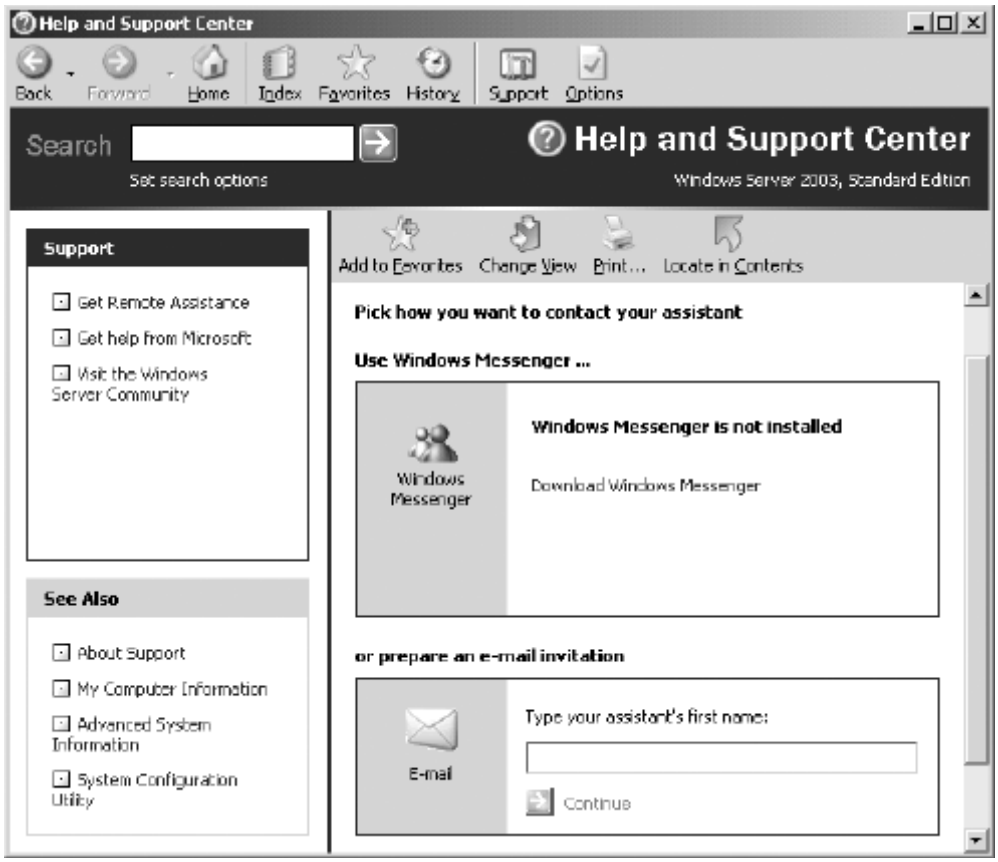
Để tạo ra một đề nghị, bạn lựa chọn "***Help And Support***" (Trợ giúp và hỗ trợ) từ thực đơn ***Start*** để mở màn hình "***Help And Support Cente***r" (Trung

tâm trợ giúp và hỗ trợ) và nhấn vào liên kết "***Remote Assistance***" để hiển thị màn hình như Hình 2-16:



***Hình 2-16*: Màn hình Remote Assistance**

Khi bạn nhấn vào liên kết "***Invite Someone To Help You***" (Đề nghị ai đó giúp bạn), bạn sẽ thấy một giao diện như Hình 2-17. Sau đó bạn làm theo các hướng dẫn để lựa chọn phương thức liên lạc



Hình 1-17: Trang *Remote Assistance trong Help And Support Center*

> ***HƯỚNG DẪN NHANH Sử dụng mật khẩu.*** *Khi người dùng tạo ra một lời đề nghị, họ có thể chỉ định mật khẩu mà chuyên gia sẽ phải sử dụng để kết nối đến máy tính của họ. Bạn nên yêu cầu người dùng luôn luôn sử dụng mật khẩu trong các kết nối Remote Assistance và hướng dẫn họ cách cung cấp mật khẩu này cho các chuyên gia sử dụng một phương thức truyền thông khác với phương thức họ sử dụng khi gửi lời đề nghị này đi.*

Chuyên gia khi nhận được lời đề nghị có thể tham gia vào việc trợ giúp bằng cách chạy ứng dụng ***Remote Assistance***, ứng dụng này cho phép chuyên gia kết nối đến máy tính ở xa như hình 2-18. Sử dụng giao diện này, người dùng và chuyên gia có thể nói chuyện hoặc nhắn tin cho nhau và theo mặc định, chuyên gia có thể nhìn thấy mọi thứ, mọi cử chỉ của người dùng đang thực hiện trên máy tính của họ. Nếu máy trạm ở xa được cấu hình cho phép điều khiển từ xa, chuyên gia có thể nhấn vào nút "***Take Control***" và thực hiện các thao tác điều khiển máy tính này.

Hình 1-18: **Giao diện *Remote Assistance* của chuyên gia**

Bảo mật Remote Assistance

Bởi vì một chuyên gia khi sử dụng khả năng điều khiển từ xa một máy khách sẽ có thể thực hiện tất cả các tác vụ trên máy tính đó như một người dùng tại đó nên tính năng này có thể gây ra vấn đề về bảo mật. Khi một người dùng chưa được xác thực có thể nắm quyền điều khiển một máy tính bằng ***Remote Assistance*** thì hoàn toàn có thể gây nên các phá hoại không giới hạn. Tuy nhiên, ***Remote Assistance*** được thiết kế để giảm thiểu các nguy cơ này bằng cách sử dụng một số tính năng sau:

- **Invitations (Đề nghị):** Không ai có thể kết nối đến một máy tính khác bằng ***Remote Assistance*** trừ khi người đó nhận được lời đề nghị từ máy khách. Máy khách có thể cấu hình khoảng thời gian hiệu lực của lời mời tính bằng phút, giờ, hoặc ngày để hạn chế không cho các chuyên gia đã được mời kết nối đến máy tính của mình sau đó.
- **Interactive connectivity (Các kết nối tương tác)**: Khi một chuyên gia chấp nhận lời mời từ một máy khách và kết nối đến máy tính đó, một người dùng phải ngồi tại máy khách đó và cho phép chuyên gia

quyền truy cập. Bạn không thể sử dụng ***Remote Assistance*** để kết nối đến một máy tính mà không có ai cho phép.

- **Client-site Control (Điều khiển tại máy khách)**: Các máy khách luôn là người có quyền quyết định cuối cùng trên một kết nối ***Remote Assistance***. Máy khách hoàn toàn có thể ngắt kết nối bất kì lúc nào bằng cách nhấn phím ESC hoặc nhấn vào ***Stop Control*** (ESC) trong trang ***Remote Assistance*** hiển thị trên máy khách.
- **Remote Control Configuration (Cấu hình điều khiển từ xa)**: Sử dụng hộp thoại ***System Properties*** hoặc các chính sách nhóm trợ giúp từ xa (***Remote Assistance Group Policy***), người dùng và người quản trị có thể xác định liệu chuyên gia có được phép điều khiển máy khách hay không. Một chuyên gia khi chỉ có quyền đọc sẽ không có khả năng chỉnh sửa cấu hình máy tính khi sử dụng ***Remote Assistance.*** Các chính sách nhóm cũng có thể cho phép người quản trị có quyền chỉ định người dùng nào được coi là chuyên gia và không một người dùng nào khác có thể sử dụng ***Remote Assistanc***e để kết nối đến máy khách mặc dù có đủ quyền trên máy đó.
- **Firewalls (Tường lửa)**: ***Remote Assistance*** sử dụng cổng 3389 trong giao thức TCP khi truyền thông trên mạng. Khi các hệ thống mạng sử dụng ***Remote Assistance*** nội bộ và có kết nối đến Internet, người quản trị mạng nên chặn cổng này trên tường lửa để ngăn cản người dùng bên ngoài mạng có thể nắm quyền điều khiển máy tính thông qua các đề nghị hỗ trợ từ xa bằng ***Remote Assistance***. Tuy vậy, chúng ta hoàn toàn có thể cung cấp khả năng hỗ trợ từ xa đến các máy khách thông qua Internet khi mở cổng 3389 này.

  LƯU Ý: Sử dụng Windows Messenger. *Nếu bạn muốn sử dụng Windows Messenger để gửi lời đề nghị Remote Assistance, bạn phải mở cổng 1863 để cho phép ứng dụng Windows Messenger có thể truyền thông.*

TỔNG KẾT

- "***Microsoft Management Console***" là công cụ quản trị hệ thống chính dành cho Windows Server 2003
- MMC là một ứng dụng lớp vỏ mà bạn sử dụng để chạy các snap-in, đó là các công cụ riêng biệt được nạp vào trong MMC
- Có hai loại snap-in: ***Stand-Alone*** (Đơn lẻ) và ***Extention*** (Mở rộng) trong đó cách thức hiển thị và chức năng của loại mở rộng trong MMC sẽ tùy thuộc vào ngữ cảnh.
- Một số snap-in có thể sử dụng với cả máy tính tại chỗ và ở xa, một số thì chỉ giới hạn trong các máy tính tại chỗ.
- Bảng điều khiển MMC có thể lưu ở chế độ Tác giả (***Author Mode***), cho phép người dùng có toàn quyền với cấu hình của bảng điều khiển hoặc Chế độ Người dùng (***User Mode***), cho phép giới hạn các quyền truy cập.
- "***Remote Desktop for Administration***" cho phép bạn quản trị một máy chủ ở xa như là bạn đăng nhập vào máy chủ đó tại chỗ đó với vai trò quản trị.
- ***Remote Assistance*** là một sự trợ giúp có tính chất thỏa thuận: Người dùng đề nghị chuyên gia giúp đỡ hoặc chuyên gia, nếu được cấu hình thông qua chính sách nhóm, có thể khởi tạo một phiên hỗ trợ. Trong các trường hợp khác, người sử dụng phải chấp nhận thiết lập kết nối và luôn luôn ở trong trạng thái điều khiển phiên hỗ trợ này. Không bao giờ chuyên gia có thể nắm quyền điều khiển máy tính mà người dùng không được thông báo.
- "***Remote Desktop Connection***" là thành phần mặc định của Windows XP và Windows Server 2003, có thể cài đặt trên bất kì hệ điều hành Windows 32 bit nào từ đĩa CD cài đặt Windows Server 2003 (hoặc sau khi chia sẻ thư mục) hoặc từ bất kỳ máy tính Windows Server 2003 nào.
- Cả hai tính năng "***Remote Desktop for Administration***" và ***Remote Assistance*** đều sử dụng Dịch vụ Đầu cuối (***Terminal Services***) để truyền thông, nhưng không bao giờ yêu cầu một giấy phép ***Terminal Services*** đặc biệt nào.

BÀI TẬP THỰC HÀNH

Bài tập thực hành 2-1: Mở một cửa sổ MMC

Trong bài tập thực hành này, bạn mở một cửa số thứ hai trong một bảng điều khiển MMC.

1. Nhấn ***Start,*** trỏ vào "***Administrative Tools***" và nhấn "***Computer Management***". Bảng điều khiển "***Computer Management***" xuất hiện
2. Từ thực đơn Window, chọn "***New Window***". Một cửa sổ thứ hai xuất hiện bên trên cửa sổ thứ nhất.
3. Từ thực đơn ***Window***, lựa chọn "***Tile Horizontally***" (xếp theo hang ngang). Bảng điều khiển thay đổi và hiển thị 2 cửa sổ cùng một lúc. Lưu ý rằng bạn có thể thao tác trên hai cửa sổ hoàn toàn độc lập nhau.

Bài tập thực hành 2-2: Tạo một bảng điều khiển MMC tùy chọn

Trong bài tập thực hành này, bạn sẽ tạo một bảng điều khiển MMC tùy chọn mới

1. Nhấn ***Start*** và sau đó chọn ***Run***. Hộp thoại ***Run*** xuất hiện
2. Trong hộp văn bản ***Open***, nhập vào ***mmc*** và nhấn ***OK***. Một cửa sổ có tên ***Console1*** xuất hiện
3. Từ thực đơn File, lựa chọn "***Add/Remove Snap-in***". Hộp thoại "***Add/Remove Snap-in***" xuất hiện
4. Nhấn ***Add***. Hộp thoại "***Standalone Snap-in***" xuất hiện
5. Trong danh sách "***Available Standalone Snap-in***", lựa chọn "***Device Manager***" và nhấn ***Add***. Hộp thoại "***Device Manager***" xuất hiện
6. Nhấn ***Finish*** để chấp nhận các thiết lập mặc định và nhấn ***Close*** sau đó nhấn ***OK***. ***S***nap-in "***Device Manager***" xuất hiện trong ô phạm vi (scope pane) của bảng điều khiển
7. Từ thực đơn ***File***, lựa chọn "***Save a***s" và sau đó lưu bảng điều khiển trong thư mục mặc định "***Administrative Tools***" với tên là ***DevMgr.msc***.

Bài tập thực hành 2-3: Kích hoạt Remote Desktop for Administration

Trong bài tập thực hành này, bạn cấu hình máy khách chấp nhận các kết nối ***Remote Desktop***

1. Nhấn ***Start,*** trỏ vào "***Control Panel***" và lựa chọn ***System***. Hộp thoại "***System Properties***" xuất hiện
2. Lựa chọn thẻ ***Remote*** và sau đó chọn "***Allow Users To Connect Remotely To This Computer***"
3. Nhấn ***OK***

CÁC CÂU HỎI ÔN TẬP

1. Chế độ mặc định khi bạn tạo một Bảng điều khiển MMC là gì ?
2. Liệu một snap-in có thể hướng vào cả máy tính tại chỗ và máy tính ở xa cùng lúc được không ?
3. Nêu các thông số cấp phép cần thiết để quản trị một máy tính ở xa sử dụng MMC ?
4. Liệu một MMC có sẵn có thể thay đổi ngữ cảnh từ Tại chỗ sang Từ xa hay phải nạp một snap-in kiểu tương tự vào trong bảng điều khiển để thực hiện kết nối từ xa?
5. Liệu mọi chức năng của snap-in có luôn luôn sẵn sàng để sử dụng khi bạn kết nối đến một máy tính ở xa?
6. Bao nhiêu kết nối đồng thời có khả năng thực hiện đến một máy chủ Terminal chạy ở chế độ ***Remote Administration?*** Tại sao ?
7. Công cụ nào được sử dụng để kích hoạt ***Remote Desktop*** trên một máy chủ ?
    a. Terminal Services Manager
    b. Terminal Services Configuration
    c. System Properties trong Control Panel
    d. Terminal Services Licensing

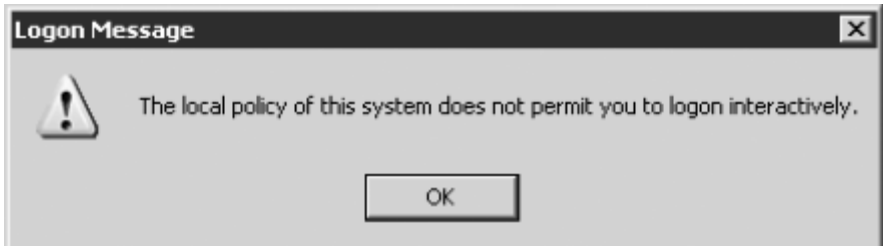
CÁC KỊCH BẢN TÌNH HUỐNG

Tình huống 2-1: Sử dụng Remote Assistance

Công ty của bạn đã kích hoạt Remote Assistance trong mỗi máy tính trong hệ thống. Nhân viên kinh doanh thường xuyên đi công tác và sử dụng máy xách tay để thực hiện công việc khi họ đang trên đường. Trong hệ thống mạng nội bộ, bạn sử dụng Windows Messenger để liên lạc với các máy trạm và để sử dụng ***Remote Assistance***. Tuy nhiên, bạn đã cấm các dữ liệu kiểu Instant Messenger với Internet bằng cách đóng cổng TCP 1863 tại tường lửa. Bạn muốn thực hiện tác vụ ***Remote Assistance*** đối với các máy khách ở xa nhưng bạn không thể kết nối đến họ bằng Windows Messenger để xem họ có online hay không. Mô tả hai phương pháp thay thế để cho các nhân viên kinh doanh có thể gửi các đề nghị ***Remote Assistance*** đến các chuyên gia trong văn phòng công ty?

Tình huống 2-2: Sử dụng kết nối Remote Desktop

Bạn đang cố gắng kết nối đến một máy chủ Windows Server 2003 trong mạng của bạn bằng ***Remote Desktop Connection***, tuy nhiên bạn luôn nhận được thông báo sau khi bạn cố gắng kết nối:



Bạn đã kiểm tra thiết lập trên máy chủ và xác nhận các điều sau đây:

1. Bạn là thành viên của nhóm ***Remote Desktop Users***
2. Bạn không phải là thành viên của nhóm ***Administrators***
3. Bạn có khả năng kết nối đến một thư mục chia sẻ trên máy chủ Terminal và máy tính này có phản hồi với lệnh ping.

Thiết lập nào mà bạn phải kiểm tra trên máy chủ Terminal để giải quyết sự cố này ?

CHƯƠNG 3: GIÁM SÁT HỆ ĐIỀU HÀNH MICROSOFT WINDOWS SERVER 2003

Một trong những nhiệm vụ chính của người quản trị hệ thống là đảm bảo cho hệ thống mạng chạy trơn tru và hiệu quả và Windows Server 2003, với một bộ sưu tập các công cụ cho phép bạn thực hiện điều này. Một máy chủ có thể hoạt động với khả năng cao nhất ngay sau khi cài đặt, tuy nhiên hiệu năng của nó có thể giảm dần theo thời gian vì rất nhiều lí do. Một người quản trị hệ thống tốt phải giám sát hiệu năng của máy chủ thường xuyên đều đặn để nhận biết chiều hướng và phát hiện các sự cố có thể ảnh hưởng đến hiệu năng. Học cách sử dụng các công cụ quản trị của Windows Server 2003 một cách đúng đắn là một kĩ năng cơ bản để bạn có thể nhận biết các thay đổi hiệu năng hệ thống trước khi rơi vào tình trạng thảm họa.

Sau khi hoàn thành chương này, bạn có khả năng:

- **Sử dụng *Event Viewer* để giám sát nhật kí hệ thống**
- **Cấu hình *Task Manager* để hiển thị các dữ liệu hiệu năng**
- **Sử dụng *System Monitor* để hiển thị các dữ liệu hiệu năng thời gian thực**
- **Tạo các *counter log* (*Nhật ký của các biến đếm*) và các *Alert (Cảnh báo*)**

CÁC KỸ NĂNG GIÁM SÁT MÁY CHỦ

Các công cụ giám sát hiệu năng máy chủ có trong Windows Server 2003 cho phép người quản trị có thể kiểm tra rất nhiều các tham số hệ thống theo rất nhiều cách khác nhau. Cách thức bạn sử dụng các công cụ phụ thuộc vào các tài nguyên mà bạn muốn giám sát cũng như các sở thích cá nhân của bạn. Có hai kiểu giám sát hệ thống cơ bản như sau:

- **Giám sát theo thời gian thực:** Giám sát thời gian thực sử dụng các công cụ hiển thị chuỗi liên tục các thông số, mô tả hệ thống đang làm gì tại thời điểm hiện tại. Các thông số này có thể hiển thị bằng số liệu hoặc dưới dạng đồ thị. Hiển nhiên, phương pháp này cung cấp các thông tin gần với hiện tại nhất, tuy nhiên chỉ có một số ít quản trị hệ thống có đủ thời gian và sở thích ngồi xem đồ thị các tham số hiệu năng hệ thống suốt cả ngày dài.
- **Giám sát bằng nhật ký**: Giám sát nhật ký thông thường cung cấp các thông tin tương tự như giám sát thời gian thực tuy nhiên các thông tin này được lưu trong một thiết bị lưu trữ cố định thay vì (hoặc thêm vào) hiển thị chúng ngay lập tức. Phương pháp này cho phép người quản trị có thể quan sát xu hướng phát triển qua thời gian dài hơn là theo dõi trong một phiên giám sát thời gian thực. Khi sử dụng giám sát bằng nhật ký, các quản trị hệ thống phải đảm bảo cung cấp đủ không gian lưu trữ để lưu các dữ liệu chụp được và đương nhiên, họ phải kiểm tra các thông tin này đều đặn

Cách thức sử dụng của việc giám sát thời gian thực và giám sát bằng nhật ký không

có tính chất loại trừ nhau. Mỗi phương pháp có giá trị riêng của nó và một số công cụ giám sát của Windows Server 2003 hỗ trợ cả hai.

Giám sát các phân hệ

Hiệu năng hệ thống Windows Server 2003 có thể chia thành 4 phân hệ cơ bản, mỗi phân hệ này phải hoạt động tốt để máy tính có thể vận hành được một cách hoàn hảo. Bốn phân hệ này là:

- **Bộ vi xử lý**: Một bộ vi xử lý trong máy tính thực hiện hàng triệu phép tính sử dụng các chu kì đồng hồ (***Clock Cycles***) của bộ vi xử lý, với mỗi phép tính toán dành cho một tác vụ đặc biệt. Các chu kì đồng hồ trong bộ vi xử lý được phân chia cho rất nhiều các tiến trình chạy trong máy tính. Bộ vi xử lý càng nhanh thì càng có nhiều chu kì đồng

hồ trong một khoảng thời gian nhất định. Giám sát hiệu năng bộ vi xử lý thông thường sẽ kiểm tra mức độ hoạt động của bộ vi xử lý khi nó thực hiện các tác vụ thường lệ. Nếu việc sử dụng chu kì đồng hồ của bộ vi xử lý luôn đạt đến 100%, hiệu năng hệ thống có thể đang quá tải do không đủ năng lực xử lý.

- **Bộ nhớ**: Bộ nhớ truy cập ngẫu nhiên (RAM) là một không gian lưu trữ tạm thời mà một máy tính sử dụng như một vùng đệm cho dữ liệu đi từ và đến bộ vi xử lý. Khi không đủ bộ nhớ RAM sẵn sàng để hoàn thành các tác vụ cụ thể nào đó, Windows sử dụng không gian đĩa cứng thay cho RAM trong một tiến trình gọi là ***paging*** (*phân trang*). Bởi vì truy cập các đĩa cứng chậm hơn rất nhiều so với truy cập RAM nên hiệu năng hệ thống sẽ giảm khi có quá nhiều việc phân trang diễn ra. Giám sát hiệu năng bộ nhớ là một công việc quan trọng đảm bảo máy tính có đủ bộ nhớ để hoàn thành các tác vụ chuyên biệt của nó.
- **Đĩa cứng**: Các đĩa cứng trong máy tính cung cấp khả năng lưu trữ lâu dài cho hệ điều hành và các file ứng dụng, cũng như các dữ liệu sử dụng và tạo ra bởi các ứng dụng. Giám sát hiệu năng của phân hệ đĩa cứng thông thường sẽ phải kiểm tra số lượng các yêu cầu truy cập đĩa cứng đang đợi để xử lý tại một thời điểm cụ thể. Nếu một lượng lớn các dữ liệu đang đợi để đọc hoặc ghi vào đĩa, hiệu năng nói chung của máy tính có thể là đang quá tải.
- **Mạng:** Giám sát phân hệ mạng có sự khác biệt đôi chút so với 3 phân hệ trên bởi vì hiệu năng của mạng có thể bị ảnh hưởng bởi các yếu tố bên ngoài cũng như bên trong. Một lượng lớn các yêu cầu truyền thông qua mạng được xếp hàng có thể làm giảm hiệu năng hệ thống, điều này có thể được các người dùng trên mạng cảm nhận, mặc dù bản thân máy tính vẫn hoạt động hoàn hảo.

Xác định phân hệ nào trong máy tính yêu cầu giám sát kĩ càng hơn phụ thuộc vào các ứng dụng mà máy tính này đang chạy. Các ứng dụng khác nhau yêu cầu hiệu năng của các phân hệ ở các mức khác nhau và một sự cố với một phân hệ nhất định nào đó có thể có các tác động khác nhau đối với các ứng dụng khác nhau.

Thiết lập một Baseline (Đường cơ sở)

Khi bạn giám sát các đặc tính của hiệu năng hệ thống, giá trị hiệu năng thực của các phân hệ là không quan trọng bằng sự thay đổi của các giá trị này theo thời gian. Ví dụ nếu bạn kiểm tra hiệu năng của bộ vi xử lý của một máy chủ mà được cài đặt lần đầu cách đây một năm và phát hiện ra mức sử

dụng của bộ vi xử lý là 100%, bạn không có cách nào biết được liệu nó đã luôn như vậy hay là có sự thay đổi nào gần đây tác động đến hiệu năng của bộ vi xử lý này.

Do các nguyên nhân trên, một trong những phần quan trọng nhất trong việc giám sát hiệu năng máy chủ là thiết lập **đường cơ sở** cho các mức hiệu năng hệ thống mà bạn có thể tham khảo sau này. Đó là lý do tại sao phần giới thiệu của chương này chỉ ra rằng bạn nên học cách sử dụng các công cụ giám sát trước khi mọi thứ có thể hư hỏng. Một **đường cơ sở** là một tập hợp của các mức hiệu năng khi máy tính hoạt động một cách bình thường, tốt nhất là ngay sau khi nó được cài đặt và cấu hình đầy đủ. Bằng cách so sánh các mức sau này với đường cơ sở, bạn có thể xác định liệu hiệu năng của các phân hệ này đang bị suy giảm hay không. Bạn sẽ học thêm về cách tạo các đường cơ sở trong phần sau của chương này và thảo luận về rất nhiều công cụ giám sát có trong Windows Server 2003.

SỬ DỤNG EVENT VIEWER

Windows Server 2003 duy trì rất nhiều nhật ký chứa các thông tin về các tiến trình đang chạy. Để xem các nhật ký này, bạn có thể sử dụng snap-in Event Viewer (Trình xem sự kiện) trong MMC. Event Viewer có thể hoạt động như một snap-in đơn lẻ hoặc mở rộng. Nhóm chương trình Administrative Tools trong Windows Server 2003 có một shortcut dẫn đến bảng điều khiển chứa Event Viewer, đồng thời snap-in này cũng đi kèm với rất nhiều các công cụ khác trong bảng điều khiển Computer Management.

> ***LƯU Ý: Mục đích của kỳ thi.*** *Mục đích của kỳ thi 70-290 là học viên có khả năng "giám sát và phân tích sự kiện. Các công cụ có thể bao gồm Event Viewer và System Monitor"*

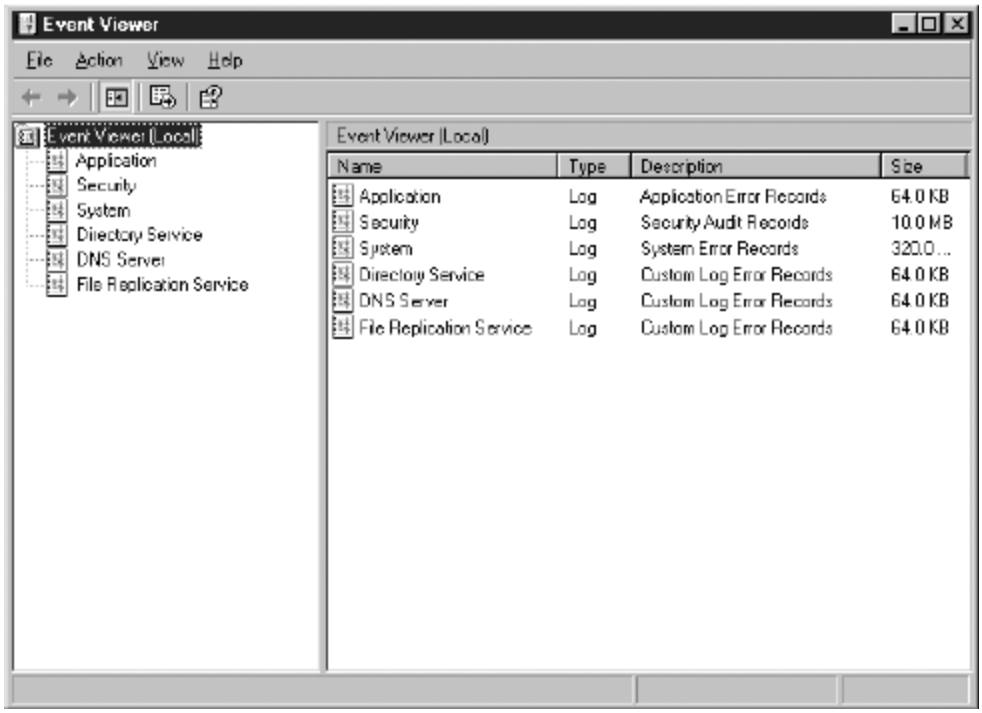
Các nhật ký trong Event Viewer

Khi bạn nạp ứng dụng Event Viewer (Thể hiện trong Hình 3-1), khung Phạm vi chứa một danh sách các nhật ký duy trì trong hệ thống. Ba nhật ký cơ bản xuất hiện trong tất cả các máy tính chạy Windows Server 2003 là:

- **Ứng dụng:** Chứa các thông tin về các chương trình chạy trong máy tính, được xác định bởi các nhà phát triển ứng dụng
- **Hệ thống:** Chứa các thông tin về các sự kiện do các cấu thành của Windows Server 2003 sinh ra, ví dụ như các dịch vụ hoặc trình điều khiển thiết bị. Ví dụ, một dịch vụ không khởi động được hoặc một trình điều khiển không thể nạp trong quá trình khởi động hệ thống sẽ

được ghi lại trong nhật ký Hệ thống. Các kiểu sự kiện ghi được trong nhật ký này được hệ điều hành cấu hình trước và không thể thay đổi được. Đây là các nhật ký cơ bản của Windows Server 2003 và bạn nên luôn luôn xem các nhật ký này đầu tiên khi bạn tìm kiếm thông tin về một sự cố hệ thống nào đó.

- **Bảo mật:** Có thể chứa các thông tin về các sự kiện liên quan đến bảo mật, ví dụ như không đăng nhập thành công, các truy cập đến các tài nguyên được bảo vệ (Ví dụ như các thư mục chia sẻ hoặc file hệ thống) và sự thành công hoặc thất bại của các sự kiện được kiểm định (audit). Windows Server 2003, trong cấu hình mặc định của nó, không ghi thông tin trong nhật ký Bảo mật. Các sự kiện ghi lại trong nhật ký này được xác định bởi các chính sách kiểm định mà bạn có thể kích hoạt bằng các Chính sách Cục bộ của Máy tính (***Local Computer Policy***) hoặc các Chính sách Nhóm (***Group Policy***). Theo mặc định, chỉ có các thành viên của nhóm ***Administrators*** mới có khả năng xem các nhật ký này.



Hình 3-1: Bảng điều khiển *Event Viewer*

Khi một máy tính được thăng cấp thành một máy chủ quản trị miền, hai nhật ký sau đây được thêm vào ***Event Viewer***:

- **Dịch vụ thư mục (*Dircetory Service*)**: Chứa các thông tin về dịch vụ thư mục sử dụng ***Active Directory***, ví dụ như việc đồng bộ các đối

tượng không thể cùng tồn tại hoặc các sự kiện quan trọng trong thư mục.

- **Dịch vụ đồng bộ file (*File Replication Service*)**: Chứa các thông tin về sự thành công hoặc thất bại của các hoạt động đồng bộ xảy ra giữa các máy chủ quản trị miền.

Cuối cùng, khi máy tính được cài đặt dịch vụ Microsoft DNS Server, ***Event Viewer*** có chứa thêm nhật ký:

- **DNS Server:** Chứa các thông tin về tình trạng và hoạt động của dịch vụ DNS Server

Mặc dù ***Event Viewer*** chứa các nhật ký quan trọng nhất của Windows Server 2003 nhưng nó không chứa tất cả. Một số lượng lớn các dịch vụ có trong hệ điều hành sẽ duy trì các nhật ký riêng của nó. Trong hầu hết các trường hợp, các nhật ký này là các file văn bản đơn giản mà bạn có thể mở bằng bất kì trình soạn thảo văn bản nào, ví dụ như ứng dụng ***Windows Notepad.***

Một số các nhật ký riêng lẻ bạn có thể tim thấy trên máy tính chạy hệ điều hành Windows Server 2003 như sau:

- Kiểm định DHCP
- ***Dr. Watson*** (*Các lỗi của chương trình*)
- Các hoạt động Fax
- ***Internet Connection Firewall*** (ICF – Tường lửa cho các Kết nối Internet)
- ***Microsoft Internet Information Services*** (IIS – Dịch vụ Thông tin Internet của Microsoft)
- Các máy khách của ***Windows Media Services***
- Các giao dịch CSDL trong WINS (Dịch vụ Chuyển đổi Tên Internet)

Hiểu các kiểu sự kiện

Khi bạn lựa chọn một trong các nhật ký liệt kê trong khung Phạm vi của snap-in ***Event Viewer***, bạn sẽ thấy một danh sách các sự kiện riêng biệt trong khung Chi tiết. Kiểu của mỗi sự kiện sẽ được hiển thị ngay bên cạnh nó bằng các biểu tượng. Kiểu của sự kiện thể hiện tầm quan trọng của nó và cho biết nó là kết quả của một quá trình thông thường hay một sự cố nào đó. Các kiểu sự kiện sử dụng trong snap-in ***Event Viewer*** được liệt kê trong

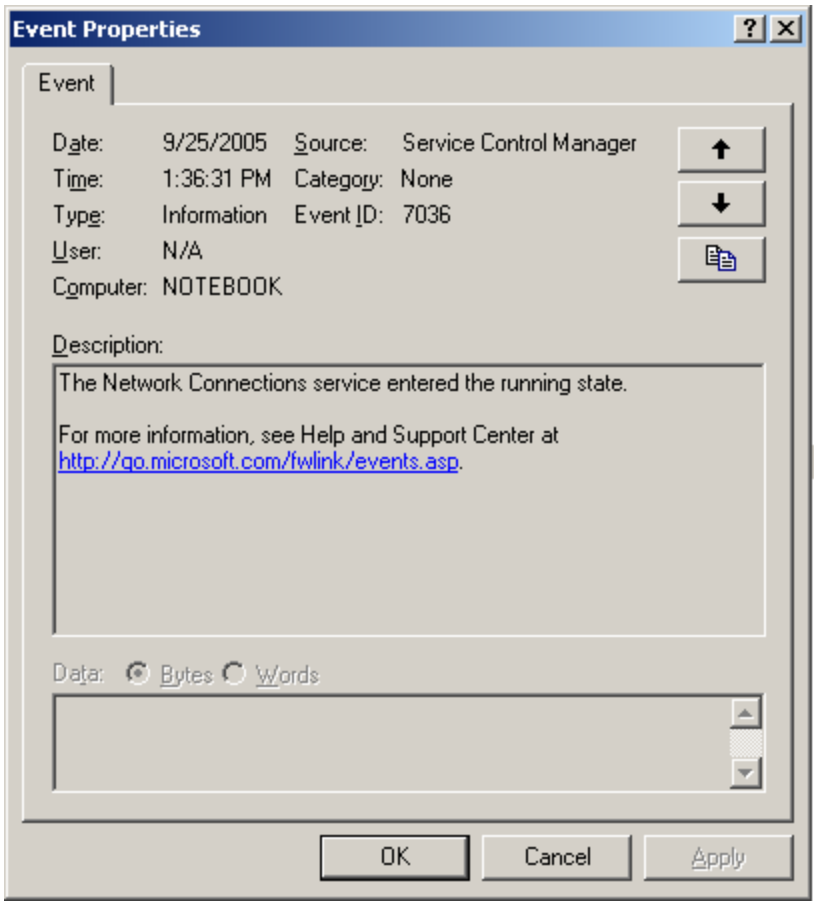
Bảng 3-1. Hiển nhiên, các báo lỗi và các cảnh báo là những kiểu sự kiện có ý nghĩa nhất đối với một người quản trị mạng bởi vì chúng thể hiện rằng các sự cố quan trọng đang xảy ra.

Bảng 3-1: Các kiểu sự kiện trong Windows 2000

Kiểu sự kiện	Biểu tượng	Mô tả
Lỗi		Một sự cố có ý nghĩa quan trọng, ví dụ như mất dữ liệu hoặc sai chức năng
Cảnh báo		Một sự kiện có thể không có ý nghĩa nhưng có thể thể hiện một sự cố trong tương lai
Thông tin		Một sự kiện mô tả hoạt động thành công của một ứng dụng, trình điều khiển hoặc dịch vụ
Kiểm định thành công		Một truy cập bảo mật thành công được kiểm định
Kiểm định thất bại		Một truy cập bảo mật thất bại được kiểm định

Nhấn đúp vào một sự kiện trong khung khung Chi tiết của Event Viewer sẽ hiển thị hộp thoại thuộc tính của sự kiện đó. Như thể hiện trong Hình 3-2. Hộp thoại này chứa một hoặc nhiều thông tin về sự kiện, bao gồm:

- **Date (Ngày):** Ngày sự kiện đó diễn ra
- **Time (Thời gian):** Thời gian sự kiện đó diễn ra
- **Type (Kiểu):** Kiểu sự kiện diễn ra (Lỗi, cảnh báo, thông tin, kiểm định thành công hoặc kiểm định thất bại)
- **User (Người dùng):** Tên của người dùng liên quan đến tiến trình sinh ra sự kiện này
- **Computer (Máy tính)**: Tên của máy tính trên đó sự kiện này xảy ra.
- **Source (Nguồn):** Module phần mềm sinh ra sự kiện này
- **Category (Hạng mục):** Sự phân loại của sự kiện này, được định nghĩa bởi tiến trình nguồn
- **Event ID (Mã số của sự kiện):** Một giá trị đơn nhất để nhận biết sự kiện cụ thể này.
- **Description (Mô tả):** Một thông báo văn bản mô tả bản chất của sự kiện, được tạo ra bởi tiến trình nguồn
- **Data (Dữ liệu):** Dữ liệu nhị phân sinh ra bởi sự kiện



Hình 3-2: Hộp thoại *Event Properties*

Cấu hình nhật ký trong Event Viewer

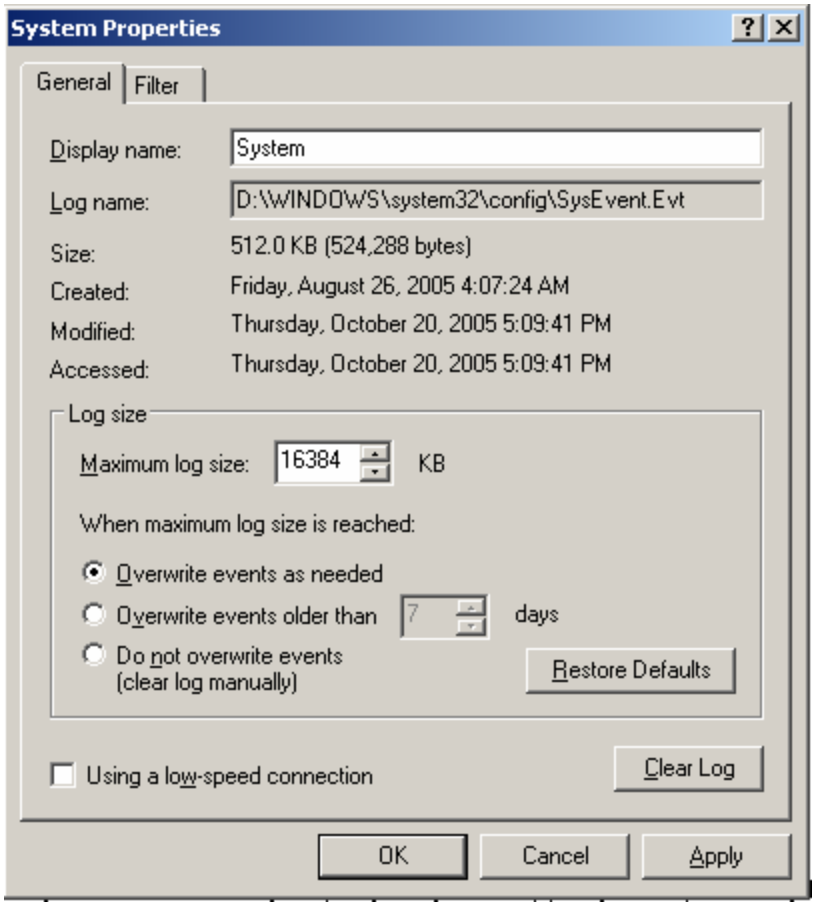
Mỗi nhật ký trong snap-in Event Viewer có hộp thoại thuộc tính riêng của nó mà bạn có thể sử dụng để cấu hình các tham số duy trì nhật ký và điều khiển thông tin nào được hiển thị trong nhật ký. Các thiết lập này được nói đến trong phần tiếp sau đây của chương trình

Các thiết lập duy trì nhật ký sự kiện

Trên thẻ ***General*** của mỗi hộp thoại ***Properties*** của nhật ký (như chỉ ra trên Hình 3-3), bạn có thể chỉ định kích thước tối đa của nhật ký và cách xử lý của nó khi các nhật ký này đạt đến kích thước tối đa. Các lựa chọn duy trì nhật ký có thể là:

- **Overwrite Events As Needed (***Ghi đè các sự kiện khi cần***):** Nhật ký sẽ xóa từng mục cũ nhất nếu cần khi file nhật ký đã đạt đến kích thước tối đa xác định

- **Overwrite Events Older Than X Days (***Ghi đè sự kiện cũ hơn X ngày***)**: Nhật ký sẽ duy trì các mục trong một số ngày (1 đến 365) xác định bởi lựa chọn này và ghi đè các mục cũ hơn nếu cần. Nếu nhật ký đạt đến giá trị tối đa xác định và không có mục nào cũ hơn số ngày chỉ định, hệ thống ngừng ghi sự kiện mới vào nhật ký.
- **Do Not Overwrite Events (Clear Log Manually) (***Không ghi đè nhật ký (Xóa nhật ký thủ công***)):** Hệ thống duy trì mọi mục của nhật ký cho tới khi chúng được xóa đi một cách thủ công bởi người quản trị. Khi nhật ký đạt đến kích thước tối đa xác định, hệ thống sẽ ngừng ghi các sự kiện vào nhật ký.



Hình 3-3: Thẻ *General* trong hộp thoại *Properties* của nhật ký sự kiện Hệ thống

Các thiết lập mặc định cho các nhật ký sự kiện trong một máy chủ quản trị miền Windows Server 2003 chạy dịch vụ Microsoft DNS Server thể hiện trong Bảng 3-2. Các nhật ký của dịch vụ thư mục và đồng bộ file có kích thước tối đa rất nhỏ (512K) bởi vì các mục vào của nhật ký này là tương đối hiếm. Nhật ký Hệ thống, tuy vậy, lại có kích thước tối đa vô cùng lớn (128

MB). Điều này xảy ra khi máy tính được thăng cấp thành một máy chủ quản trị miền và một phần của việc cấu hình mặc định cho máy chủ quản trị miền Windows Server 2003 là kích hoạt một số chính sách kiểm định, điều này gây ra một số lượng lớn các sự kiện được ghi vào trong nhật ký Hệ thống. Trong khi đó, giá trị tối đa mặc định cho nhật ký Bảo mật trong một máy tính Windows Server 2003 mà không phải máy chủ quản trị miền là 16MB

Bảng 3-2: Các thiết lập mặc định duy trì nhật ký sự kiện

Event Log	Maximum Log Size	Log Retention Setting
Application	16,384 KB (16 MB)	Overwrite events as needed (Ghi đè khi cần)
Directory Service	512 KB	Overwrite events as needed
DNS Server	16,384 KB (16 MB)	Overwrite events older than 7 days (Ghi đè các sự kiện cũ hơn 7 ngày)
File Replication Service	512 KB	Overwrite events as needed
Security	131,072 KB (128 MB)	Overwrite events as needed
System	16,384 KB (16 MB)	Overwrite events as needed

> ***LƯU Ý: Cấu hình các thiết lập duy trì sử dụng các chính sách nhóm.*** *Ngoài cách cấu hình các thiết lập duy trì cho các nhật ký sự kiện một cách thủ công bằng cách sử dụng snap-in* ***Event Viewer****, bạn còn có thể cấu hình các tham số tương tự cho các nhật ký Ứng dụng, Hệ thống và Bảo mật bằng cách kích hoạt các chính sách nhóm Event Log trong đối tượng chính sách nhóm (GPO) và áp dụng nó vào các máy tính riêng lẻ hoặc vào một đối tượng chứa trong Active Directory.*

Trên một máy chủ quản trị miền, việc để thiết lập mặc định ***Overwrite Events As Needed*** trong nhật ký Bảo mật có thể dẫn đến việc các dữ liệu liên quan đến vấn đề bảo mật hoặc các truy cập tài nguyên quan trọng sẽ bị ghi đè nếu người quản trị không thường xuyên lưu các mục trong nhật ký lại. Để đảm bảo các nhật ký Bảo mật không bị mất, Windows Server 2003 có

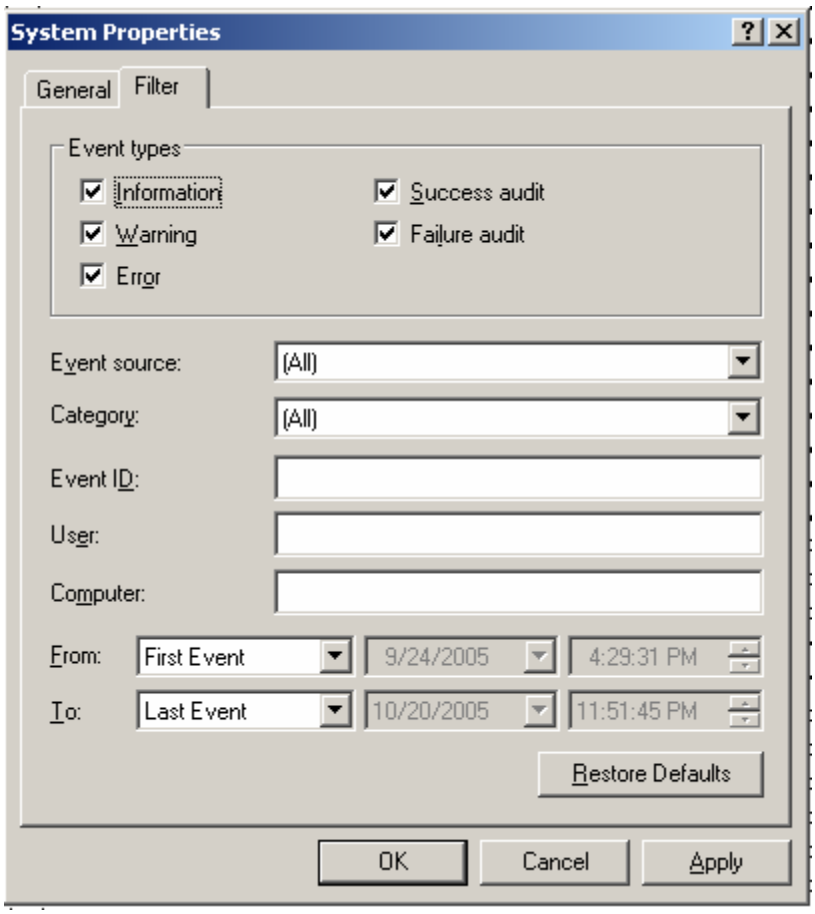
một biện pháp mạnh dưới hình thức một chính sách nhóm cho lựa chọn bảo mật gọi là ***Audit: Shut Down System Immediately If Unable To Log Security Audits*** (*Kiểm định: Tắt hệ thống ngay lập tức nếu không thể ghi nhật ký kiểm định Bảo mật*).

Sử dụng các bộ lọc

Khi bạn sử dụng ***Event Viewer*** lần đầu tiên, snap-in này hiển thị mọi sự kiện được ghi lại trong nhật ký lựa chọn đó theo thứ tự thời gian. Tùy vào kích thước của nhật ký và các thiết lập duy trì, danh sách này có thể rất dài. Tuy nhiên, nhiều mục trong nhật ký là thuộc kiểu Thông tin, đó là các kết quả của các hoạt động thông thường hàng ngày.

Để định vị các mục đặc biệt trong danh sách này, bạn có thể chỉnh sửa thứ tự sắp xếp của nó bằng cách nhấn vào một trong các tiêu đề của cột hoặc bạn có thể giới hạn hiển thị các thông tin xuất hiện trong nhật ký tập trung vào các sự kiện quan trọng, bằng cách sử dụng ***Filter*** (*Bộ lọc*) hoặc dùng lệnh ***Find*** (*Tìm kiếm*)

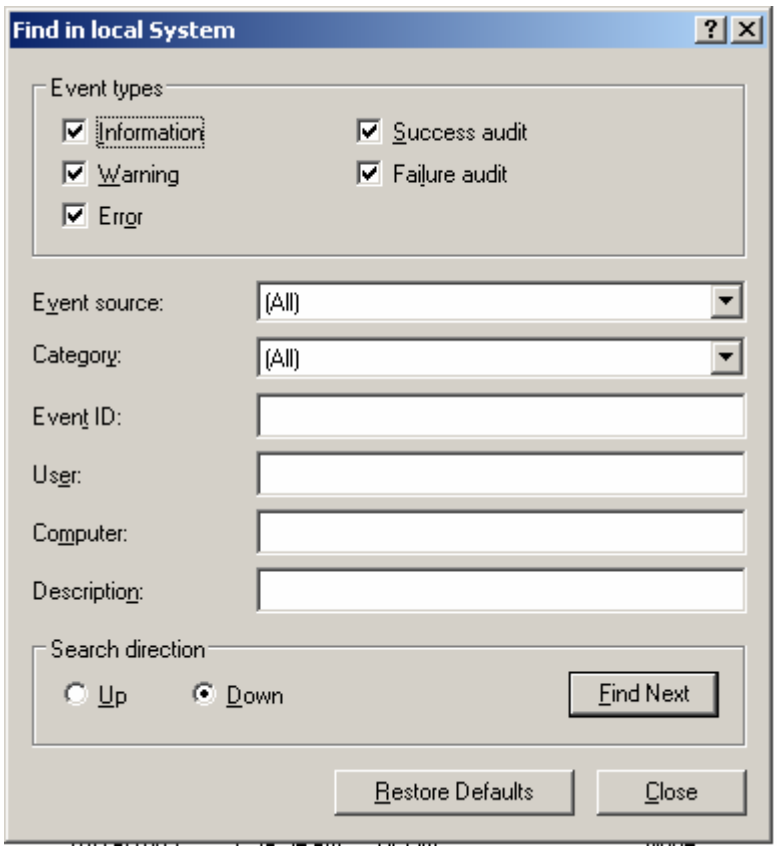
Để triển khai một Bộ lọc trên một nhật ký trong ***Event Viewer***, từ thực đơn ***View***, lựa chọn ***Filter*** để hiển thị thẻ ***Filter*** trong hộp thoại ***Properties*** của nhật ký sự kiện, như thể hiện trong Hình 3-4. Trong hộp thoại này, bạn có thể chỉ định kiểu sự kiện nào bạn muốn hiển thị và lựa chọn các sự kiện tiêu biểu để giảm bớt danh sách sự kiện về kích thước có thể quản lý được.



Hình 3-4: Thẻ *Filter* trong hộp thoại *Properties* của nhật ký sự kiện

Để kiểm tra các mục đặc biệt trong danh sách các sự kiện, bạn có thể lựa chọn lệnh ***Find*** từ thực đơn ***View*** để hiển thị hộp thoại ***Find*** (Thể hiện trong Hình 3-5)

Cả hai hộp thoại trong Thẻ ***Filter*** và ***Find*** đều cho phép bạn lựa chọn từ các danh sách sự kiện tiêu biểu trong "Các kiểu sự kiện Windows 2000" đã nói đến trong chương trước, để định vị các mục đặc biệt.



Hình 3-5: Hộp thoại *Find* trong *Event Viewer*

Truy cập nhật ký sự kiện từ xa

Như rất nhiều snap-in MMC khác, bạn có thể sử dụng ***Event Viewer*** để xem các nhật ký trên các máy tính Window khác như là xem trên máy tính bạn đang làm việc. Để thực hiện điều này, trong khung Phạm vi, lựa chọn đối tượng ***Event Viewer (Local)*** và lựa chọn "***Connect To Another Computer***" (*Kết nối tới máy tính khác*) từ thực đơn ***Action.*** Trong hộp thoại ***Select Computer***, chỉ ra tên của máy tính mà bạn muốn xem các nhật ký sự kiện trên máy đó.

Lưu giữ các Nhật ký sự kiện

Snap-in ***Event Viewer*** có thể lưu các nhật ký thành file trong một số định dạng, bao gồm dạng văn bản (***.txt***), dạng bảng (***.csv***) và một định dạng nhật ký sự kiện có phần mở rộng là ***.evt***, định dạng này có thể mở bằng snap-in. Khi bạn lưu các nhật ký này vào một file, bạn đã có một bản ghi lâu dài của

các mục vào và khi đó bạn có thể xóa các nhật ký này. Lưu nhật ký thường xuyên đều đặn để đảm bảo rằng các file nhật ký không tăng trưởng quá lớn và gây ra mất mát dữ liệu.

SỬ DỤNG TASK MANAGER

Task Manager (*Trình Quản lý Tác vụ*) là một ứng dụng quan trọng của Windows mà bạn có thể sử dụng để hiển thị thông tin về các mức hiệu năng hiện tại của máy tính cũng như quản lý các chương trình hoặc các tiến trình đang chạy trong hệ thống. Bạn có thể mở ***Task Manager*** bằng cách nhấn phải chuột vào vùng trống của thanh tác vụ và lựa chọn ***Task Manager*** từ thực đơn ngữ cảnh, hoặc có thể nhấn đồng thời ***Ctrl+Alt+Del*** và chọn vào phím ***Task Manager***. Hộp thoại ***Windows Task Manager*** theo mặc định sẽ chứa 5 thẻ:

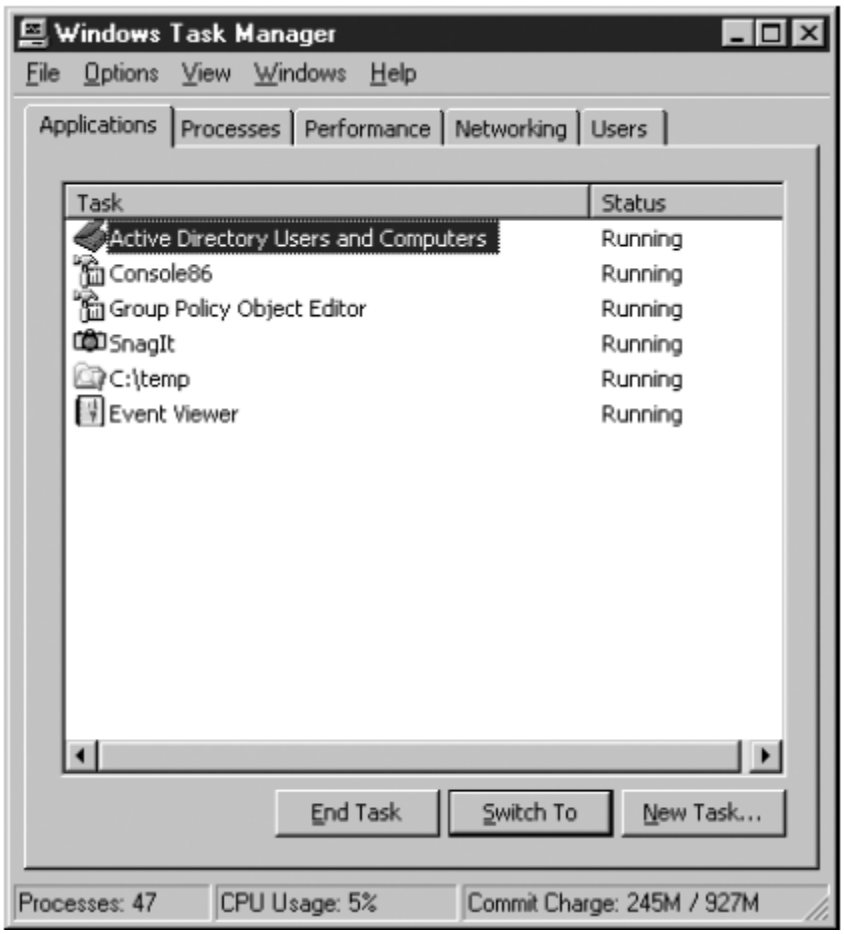
- ***Applications*** (Ứng dụng)
- ***Processes*** (Tiến trình)
- ***Performance*** (Hiệu năng)
- ***Networking*** (Mạng)
- ***Users*** (người dùng)

Chức năng của mỗi thẻ được mô tả trong các phần sau đây của chương.

> ***LƯU Ý: Mục đích của khóa học****. Mục đích của khóa học 70-290 là học viên có khả năng "giám sát file và máy chủ in ấn". Các công cụ có thể sử dụng bao gồm Task Manager, Event Viewer và System Monitor*

Làm việc với các ứng dụng

Thẻ ***Applications*** (Thể hiện trong Hình 3-6) chỉ ra trạng thái của các chương trình mức người dùng đang chạy trong hệ thống. Các dịch vụ và ứng dụng hệ thống chạy trong các ngữ cảnh khác với người dùng đang đăng nhập sẽ không hiển thị. Đối với các ứng dụng liệt kê ở đây, cột ***Status*** (*Trạng thái*) sẽ chỉ ra liệu ứng dụng đang chạy (***running***) hay là không phản ứng (***not responding***).



Hình 3-6: Thẻ *Applications* trong *Task Manager*

Bằng cách lựa chọn một ứng dụng từ trong danh sách đó và nhấn vào ***Switch To***, bạn có thể chuyển sang màn hình hoạt động của ứng dụng này và vẫn để Task Manager mở như là ứng dụng nền. Bạn còn có thể lựa chọn một mục trong danh sách và nhấn ***End Task*** để đóng ứng dụng đó lại.

> ***LƯU Ý: Đóng các tác vụ.*** *Đóng một ứng dụng bằng cách sử dụng Task Manager không phải là cách được khuyến khích trừ khi ứng dụng đó có trạng thái* ***Not Responding*** *và không thể đóng được bằng các cách khác. Khi bạn kết thúc một tác vụ bằng cách này, bạn thường mất các dữ liệu mà bạn chưa kịp lưu vào trong đĩa cứng.*

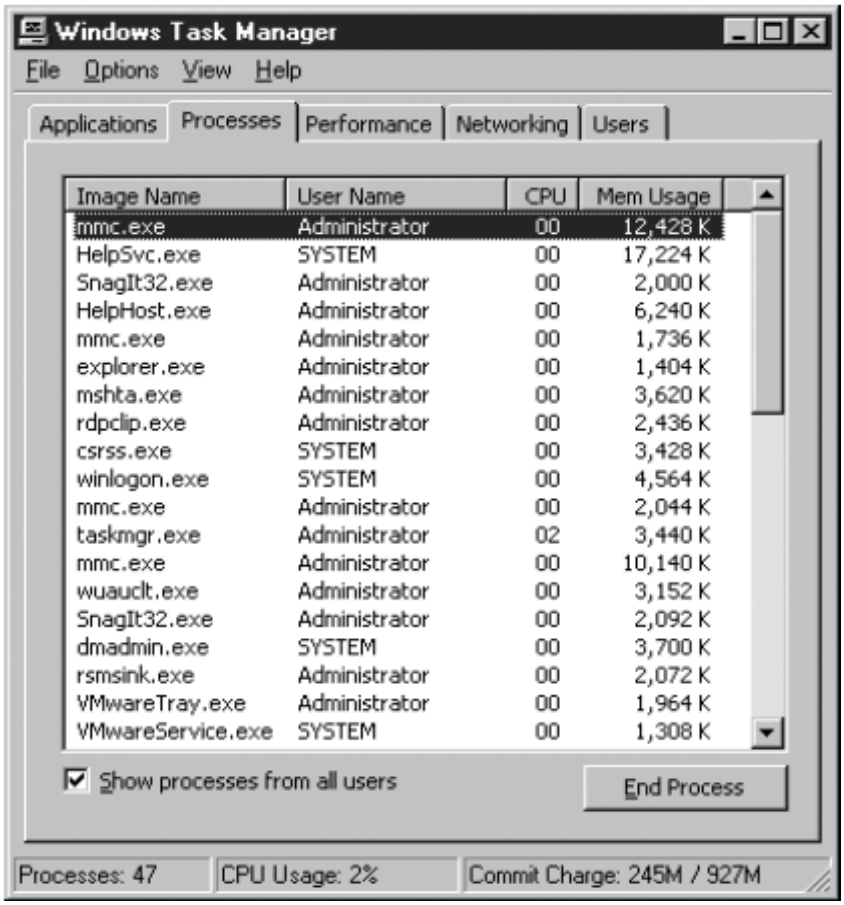
Khi bạn nhấn phải chuột vào một ứng dụng trong danh sách và lựa chọn ***Go To Process*** từ thực đơn ngữ cảnh, hộp thoại chuyển sang thẻ ***Processes*** và trỏ vào tiến trình liên quan đến ứng dụng đó. Đây là một tính năng hữu ích khi bạn đang muốn tìm xem tiến trình của một ứng dụng đặc biệt nào đó khi tên của tiến trình khó có thể đoán bằng trực giác.

Khi bạn nhấn vào phím ***New Task***, một hộp thoại ***Create New Task*** (tạo tác vụ mới) xuất hiện, trong đó bạn có thể nhập vào hoặc duyệt đến tên của bất kì một file chạy hoặc lệnh chuẩn nào đó. Hộp thoại này có chức năng tương tự như hộp thoại ***Run*** mà có thể truy cập từ thực đơn ***Start***.

Giám sát các tiến trình

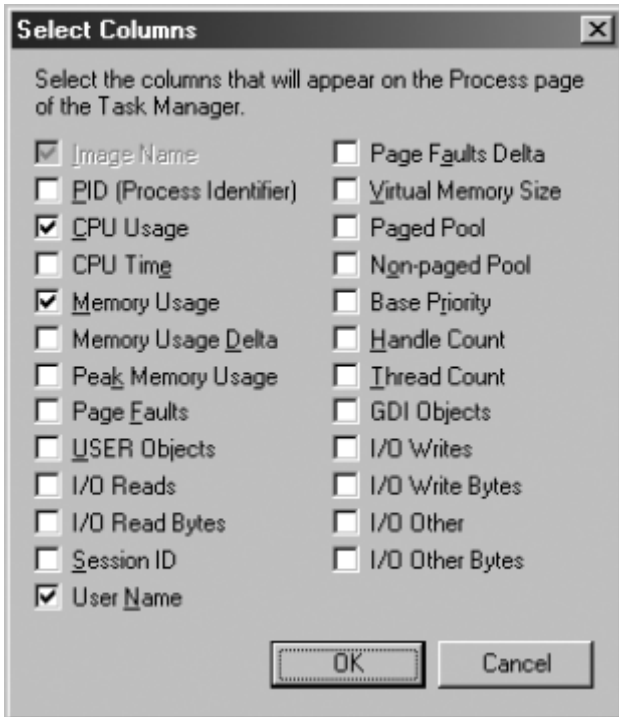
Thẻ ***Processes*** (Thể hiện trong Hình 3-7) liệt kê tất cả các tiến trình của các người dùng hiện tại đang chạy trên máy tính. Khi bạn lựa chọn "***Show Processes From All Users***" (Hiển thị các tiến trình từ tất cả người dùng), bên cạnh các ứng dụng mức người dùng, danh sách này còn hiển thị cả các dịch vụ và các tiến trình hệ thống. Theo mặc định, danh sách này bao gồm các thông tin sau đây về mỗi tiến trình:

- ***Image Name***: Tên của file chạy tiến trình này.
- ***User Name***: Tên tài khoản người dùng là chủ nhân của tiến trình này
- ***CPU***: Phần trăm của bộ vi xử lý do tiến trình này sử dụng
- ***Mem Usage***: Dung lượng bộ nhớ tiến trình này sử dụng



Hình 3-7: Thẻ *Processes* trong *Task Manager*

Bằng cách chọn ***Select Columns*** từ thực đơn ***View***, bạn mở hộp thoại ***Select Columns*** (Thể hiện trên Hình 3-8), trong đó bạn có thể thêm hoặc bớt các cột dữ liệu trong khung hiển thị. ***Task Manager*** cung cấp một bộ sưu tập các ***counters*** (biến đếm), cho phép bạn có thể hiển thị các thông tin chi tiết về bộ vi xử lý, bộ nhớ và khả năng sử dụng I/O của mỗi tiến trình trong danh sách. Bạn có thể sắp xếp danh sách hiển thị theo bất kì ***biến đếm*** nào bằng cách nhấn vào tiêu đề của cột đó.



Hình 3-8: Hộp thoại *Select Columns*

Để giám sát thông tin dễ dàng về các tiến trình hệ thống, bạn có thể thao tác chúng bằng ***Task Manager***. Bằng cách nhấn phải chuột vào bất kì tiến trình nào trong danh sách, bạn có thể thực hiện các tác vụ sau:

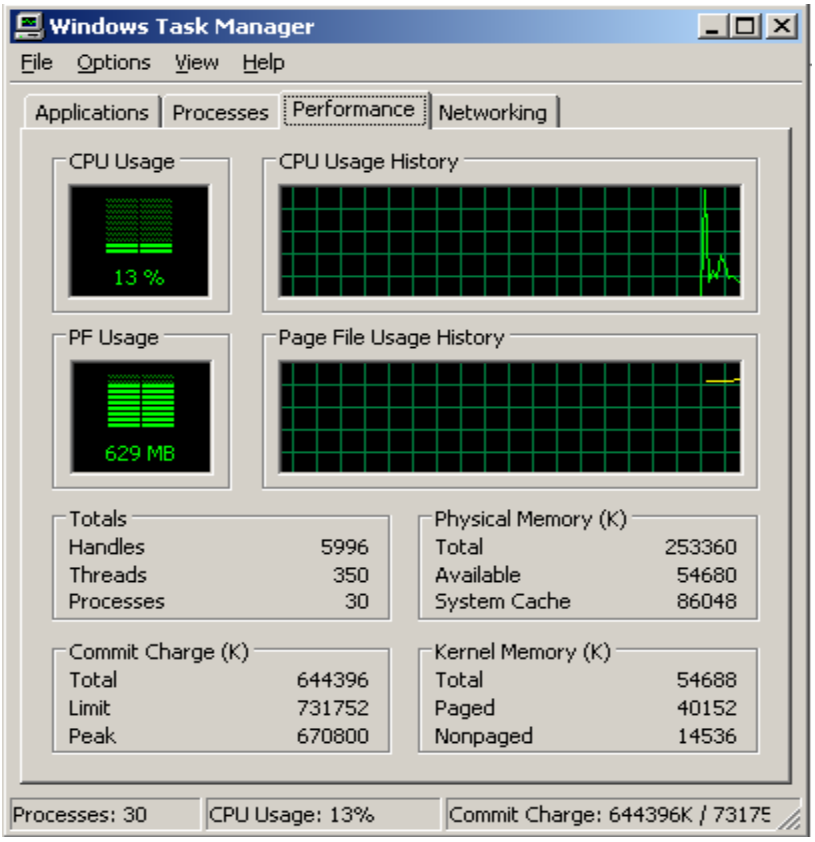
- ***Set Priority (****Thiết lập mức ưu tiên***)**: Chỉnh sửa thời gian bộ vi xử lý sử dụng cho tiến trình đó trong mối tương quan với các tiến trình khác trong hệ thống
- ***Set Proccessor Afinity (****Thiết lập mối quan hệ vi xử lý***)**: Chỉ định bạn muốn chạy tiến trình bằng bộ vi xử lý nào trên một hệ thống máy tính có nhiều bộ vi xử lý.
- ***End Proccess* (*Kết thúc tiến trình*)**: Dừng tiến trình ngay lập tức. Mọi tài nguyên chưa lưu sẽ bị mất

- ***End Proccess Tree (****Kết thúc cây tiến trình*)**: Dừng mọi tiến trình và các tiến trình con hoặc tiến trình liên quan ngay lập tức. Mọi dữ liệu chưa lưu sẽ bị mất.
- ***Debug (****Gỡ lỗi*)**:** Tạo ra một trường hợp ngoại lệ để ngắt tiến trình và gắn nó với một trình gỡ lỗi được cài đặt trong hệ thống.

  CẢNH BÁO: Thao tác với các tiến trình. *Thay đổi các thiết lập của một tiến trình ví dụ như mức ưu tiên hay mối liên hệ với bộ vi xử lý có thể gây ra những tác động có hại đến hiệu năng của các ứng dụng khác trong hệ thống. Kết thúc một tiến trình và đặc biệt là một cây tiến trình chỉ nên làm khi các thao tác thông thường để kết thúc tiến trình đó là không thực hiện được. Windows Server 2003 có cơ chế bảo vệ các tiến trình của hệ điều hành không bị ngắt bởi* ***Task Manager****, tuy nhiên chúng vẫn có thể dễ bị ảnh hưởng bởi sự thiếu tài nguyên hệ thống do việc điều chỉnh mức ưu tiên của các tiến trình khác gây ra.*

Giám sát mức hiệu năng

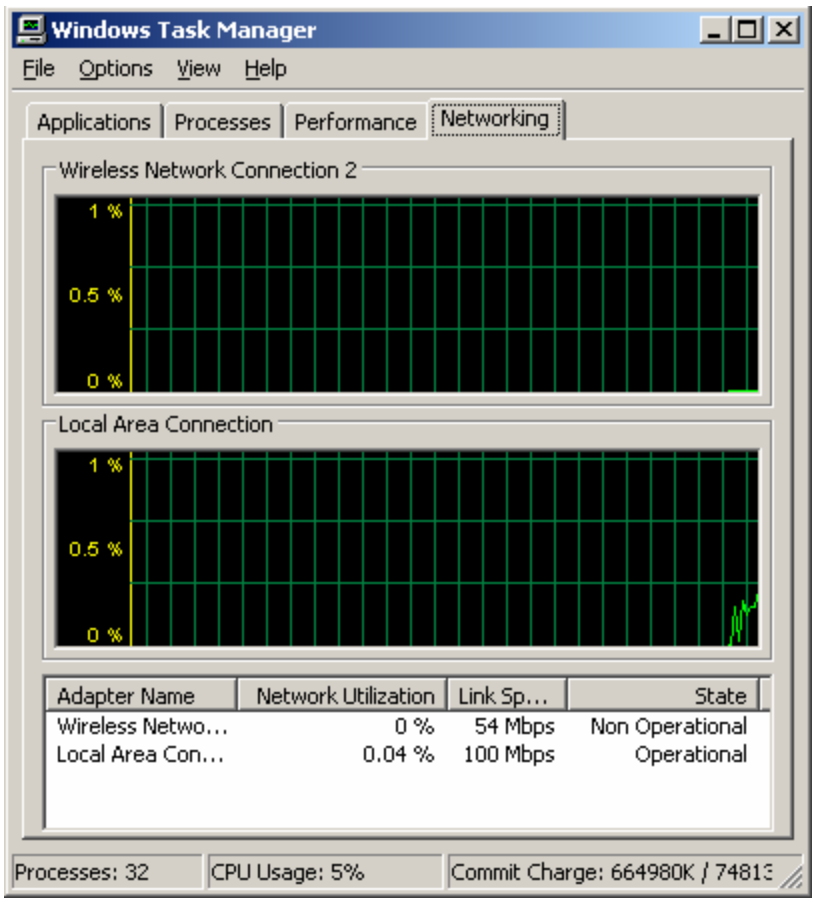
Thẻ ***Performance*** (Thể hiện trong Hình 3-9) hiển thị cách nhìn trong thời gian thực về hiệu suất sử dụng bộ vi xử lý và bộ nhớ. Mức sử dụng của mỗi bộ vi xử lý và mức sử dụng của page file (file phân trang bộ nhớ) được hiển thị bằng đồ thị cùng với các giá trị thống kê từ trước của các thông số này. Nhấn đúp chuột vào một trong các đồ thị sẽ mở rộng nó theo chiều dọc (trục tung) để hiển thị các giá trị một cách rõ ràng hơn. Các hiển thị số bên dưới sẽ cho biết mức độ sử dụng bộ nhớ vật lý (***Physical***), bộ nhớ lõi (***Kernel***) và bộ nhớ cam kết (***Commit***), đồng thời cả số lượng các ***Handle*** (*Liên kết giữa các tiến trình*), ***Thread*** (*Luồng*), và các tiến trình đang hoạt động



Hình 3-9: Thẻ *Performance* trong *Task Manager*

Giám sát các hoạt động của mạng

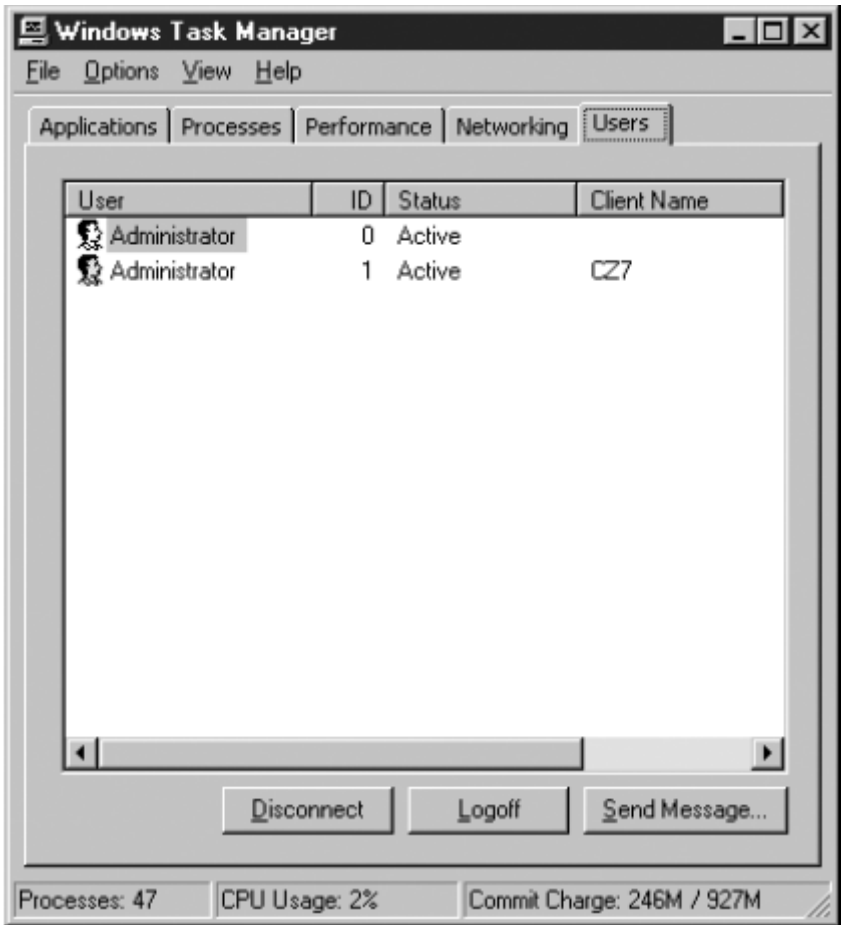
Thẻ ***Networking*** (Thể hiện trong Hình 3-10) cho thấy các kết nối mạng đang hoạt động theo tên, cùng với tốc độ kết nối, phần trăm băng thông sử dụng và trạng thái hoạt động của nó. Đồng thời có một đồ thị hiển thị băng thông sử dụng trong kết nối mạng đang chọn hiện tại. Cũng giống như trên, việc nhấn đúp vào trong đồ thị này sẽ hiển thị đồ thị một cách rõ ràng hơn bằng cách mở rộng trục tung y của nó.



Hình 3-10: Thẻ *Networking* trong *Task Manager*

Giám sát người dùng

Thẻ ***Users*** (Thể hiện trong Hình 3-11) sẽ liệt kê tất cả các người dùng đang đăng nhập vào máy tính. Các người dùng đăng nhập có thể là người dùng làm việc trực tiếp tại màn hình điều khiển hoặc người dùng đăng nhập qua kết nối từ xa trên mạng. Sử dụng các điều khiển trong thẻ này, bạn có thể đăng xuất người dùng đó, ngắt kết nối của họ đến máy tính hoặc gửi thông báo cho họ.



Hình 3-11: Thẻ *Users* trong *Task Manager*

SỬ DỤNG PERFORMANCE CONSOLE (BẢNG ĐIỀU KHIỂN HIỆU NĂNG)

Performance console (Bảng điều khiển hiệu năng) là một trong những công cụ giám sát mạnh nhất trong Windows Server 2003. Bảng điều khiển này chứa hai snap-in sau đây:

- ***System Monitor*** **(***Giám sát Hệ thống***)**: Hiển thị các dữ liệu hiệu năng thời gian thực thu thập được từ các phần tử cấu hình gọi là các ***performance counters*** (Biến đếm hiệu năng)
- ***Performance Logs and Alerts*** **(***Nhật ký và Cảnh báo Hiệu năng***)**: Ghi dữ liệu từ các ***Biến đếm Hiệu năng*** theo một chu kỳ thời gian nhất định và thực thi các hành động xác định khi các ***biến đếm*** này đạt đến một giá trị nào đó.

Performance là một bảng điều khiển MMC có thể truy cập từ một ***shortcut*** trong nhóm chương trình ***Administrative Tools***. Bạn cũng có thể thêm các

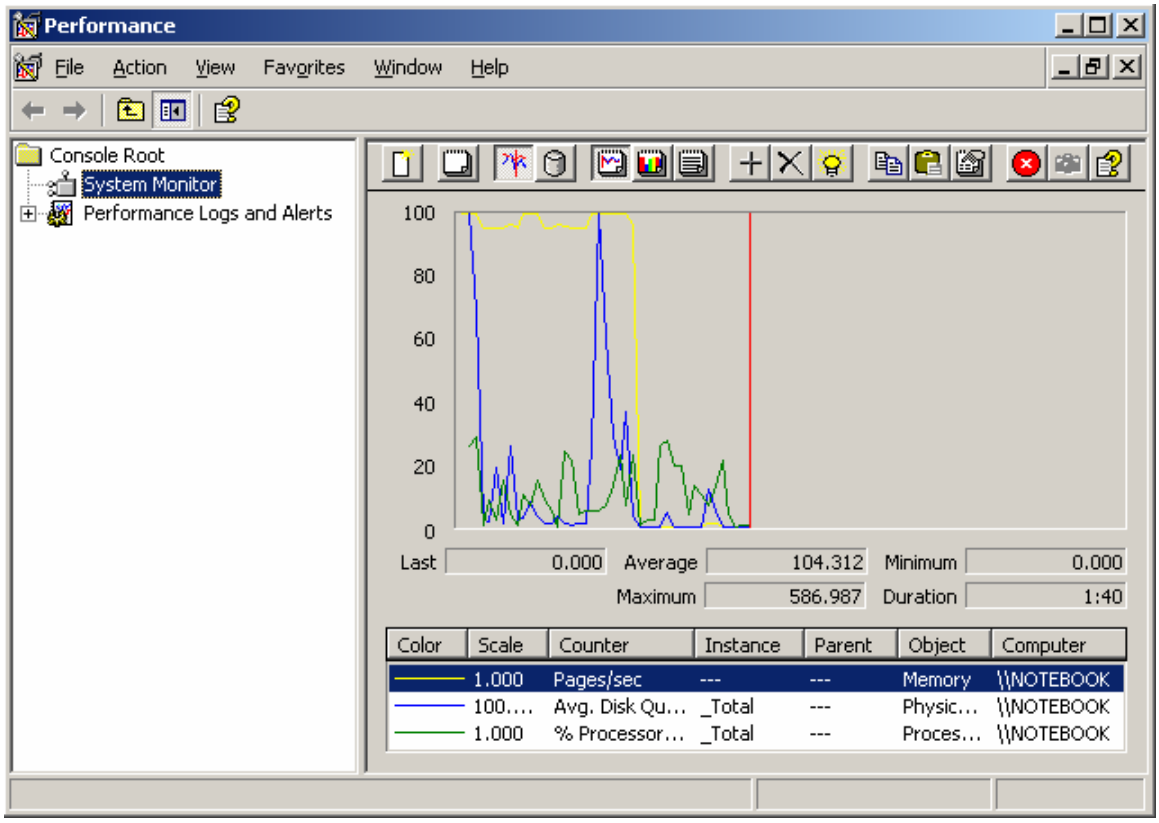
snap-in khác vào trong bảng điều khiển tùy chọn. Theo mặc định, Bảng điều khiển ***Performance*** sẽ giám sát máy tính hiện tại, tuy nhiên bạn có thể cấu hình snap-in này để giám sát hiệu năng của bất kỳ máy tính nào trong mạng nếu như bạn có các quyền thích hợp.

> ***THÔNG TIN THÊM. Sử dụng các Snap-in trong MMC***. *Để có thêm thông tin về việc tạo ra các bảng điều khiển MMC, xem Chương 2 trong cuốn sách này.*
>
> ***LƯU Ý. Mục đích của kỳ thi***. *Mục đích của kỳ thi 70-290 là học viên phải có khả năng "giám sát hiệu năng hệ thống"*

Sử dụng System Monitor (Giám sát Hệ thống)

Khi bạn mở Bảng điều khiển ***Performance***, theo mặc định thì snap-in ***System Monitor*** (*Giám sát hệ thống*) xuất hiện, thể hiện trong Hình 3-12. Khung Chi tiết của snap-in có một đồ thị dạng đường, được cập nhật theo thời gian thực, cho ta thấy các mức hiện tại của ba ***Biến đếm Hiệu năng*** sau đây:

- **Memory: Pages/Second (Bộ nhớ:Trang/giây)**: Tỉ lệ các trang bộ nhớ được đọc từ hay ghi vào đĩa để giải quyết các lỗi ***hard page*** (lỗi ***Hard page*** xẩy ra khi các tiến trình gọi đến các đoạn mã hay dữ liệu cần thiết nhưng hiện không sẵn sàng trong các tập làm việc (***worrking set***) hay trong bộ nhớ RAM, và chúng buộc phải tái tạo các thông tin trên từ đĩa cứng). Biến đếm này là thông số chính cho biết các kiểu/dạng lỗi gây ra độ trễ trong hệ thống.
- **PhysicalDisk(_Total): Average Disk Queue Length (Đĩa cứng: Độ dài Hàng đợi Đĩa Trung bình)**. Biến đếm đo độ dài có giá trị là trung bình số lượng của các yêu cầu đọc và ghi trong hàng đợi truy cập đĩa cứng được lấy mẫu theo một khoảng thời gian xác định.

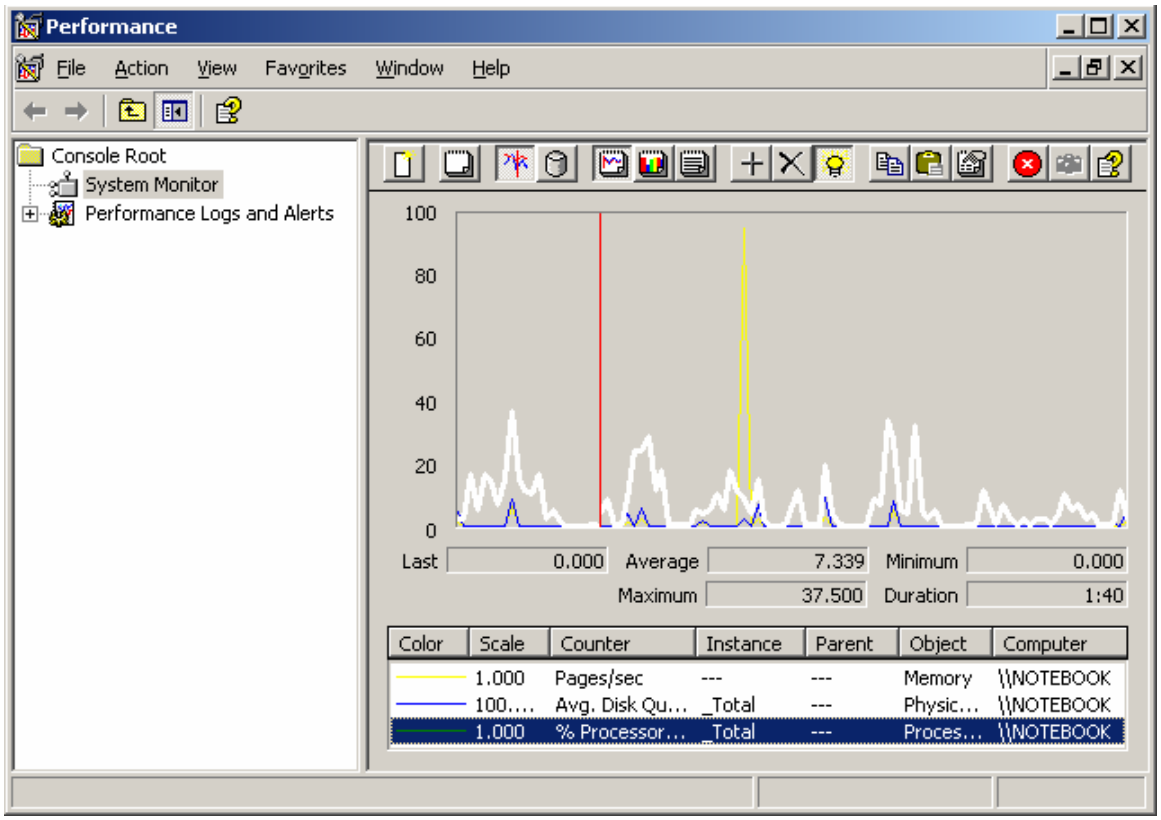


Hình 3-12: Màn hình hiển thị *System Monitor* theo mặc định

- **Processor(_Total): % Processor Time (Bộ vi xử lý: % Thời gian của Bộ vi xử lý)**. Phần trăm của thời gian trôi qua mà bộ vi xử lý tiêu tốn để thực hiện một chuỗi lệnh liên tục (***non-idle thread***). Biến đếm này là thông số chủ yếu thể hiện hoạt động của bộ vi xử lý và hiển thị trung bình phần trăm thời gian bận ghi được trong một khoảng thời gian lấy mẫu nhất định.

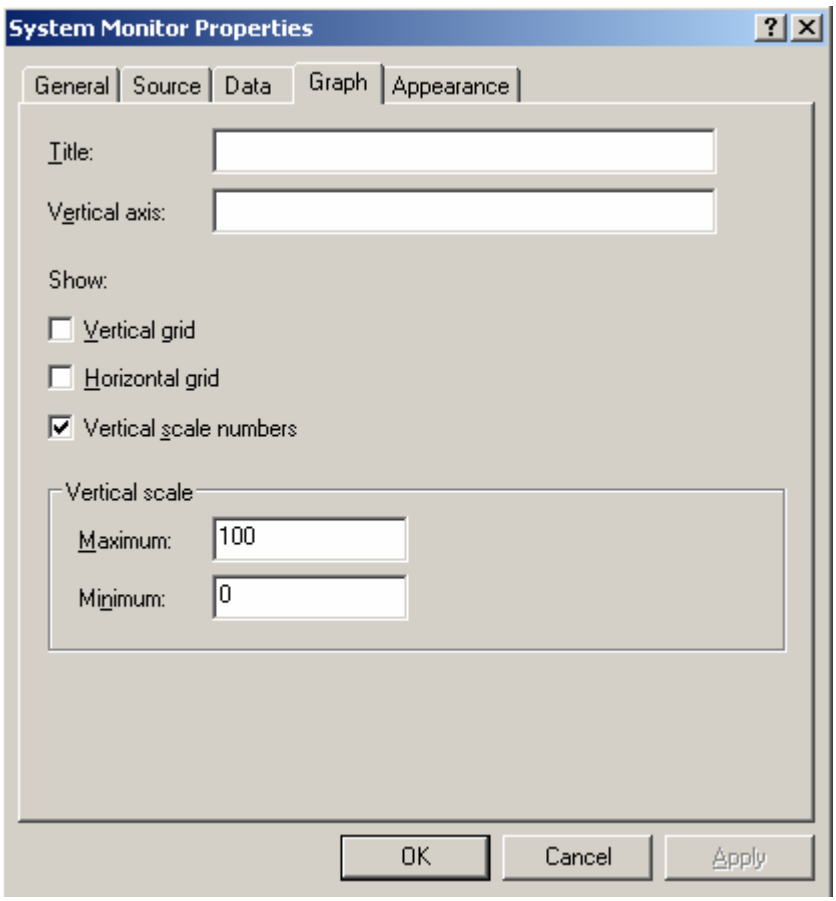
Thay đổi cách Quan sát Đồ thị

Mẫu định dạng được trình bầy bên dưới của đồ thị thể hiện màu dòng kẻ của mỗi ***biến đếm*** trong ba biến đếm trên, giá trị tương ứng của mỗi ***biến đếm*** và các thông số nhận dạng khác về các ***biến đếm*** này. Khi bạn lựa chọn một ***biến đếm*** trong số đó, giá trị hiện tại sẽ hiển thị dưới dạng số ở dưới đáy của đồ thị. Nhấn vào phím ***Highlight*** trong thanh công cụ (hoặc nhấn ***Ctrl+H***) để thay đổi đồ thị của ***biến đếm*** đã chọn thành một dòng kẻ rộng màu trắng giúp ta dễ dàng phân biệt được chúng trên đồ thị (Thể hiện trong Hình 3-13)



Hình 3-13: Một đồ thị *System Monitor* với biến đếm (*counter)* được tô sáng

Nếu máy tính của bạn đang trong trạng thái nghỉ, bạn có thể lưu ý rằng các đường kẻ trong đồ thị mặc định sẽ nằm lơ lửng gần đáy của thang chia độ và sẽ khó khăn để nhìn thấy được các giá trị của chúng. Bạn có thể giải quyết vấn đề này bằng cách chỉnh sửa thang chia độ trong trục y (trục tung). Nhấn vào phím ***Properties*** trên thanh công cụ (hoặc nhấn ***Ctrl+Q***) để hiển thị hộp thoại ***System Monitor Properties***, sau đó lựa chọn thẻ ***Graph*** (Thể hiện trong Hình 3-14). Trong hộp ***Vertical Scale***, bạn có thể giảm giá trị tối đa của trục y, đều này sẽ dẫn đến việc ta sẽ có một đồ thị rộng hơn để hiển thị các dữ liệu của biến đếm



Hình 3-14: Thẻ *Graph* của hộp thoại *System Monitor Properties*

Trong thẻ ***General*** của hộp thoại ***System Monitor Properties***, bạn còn có thể chỉnh sửa tần suất lấy mẫu của đồ thị. Theo mặc định, đồ thị cập nhật các giá trị của biến đếm sau mỗi 1 giây, tuy nhiên bạn có thể tăng giá trị này để hiển thị dữ liệu trong khoảng thời gian lâu hơn trên một trang của đồ thị. Điều này cho phép ta có thể dễ dàng phát hiện các xu hướng có tính chất lâu dài trong các giá trị của ***biến đếm***.

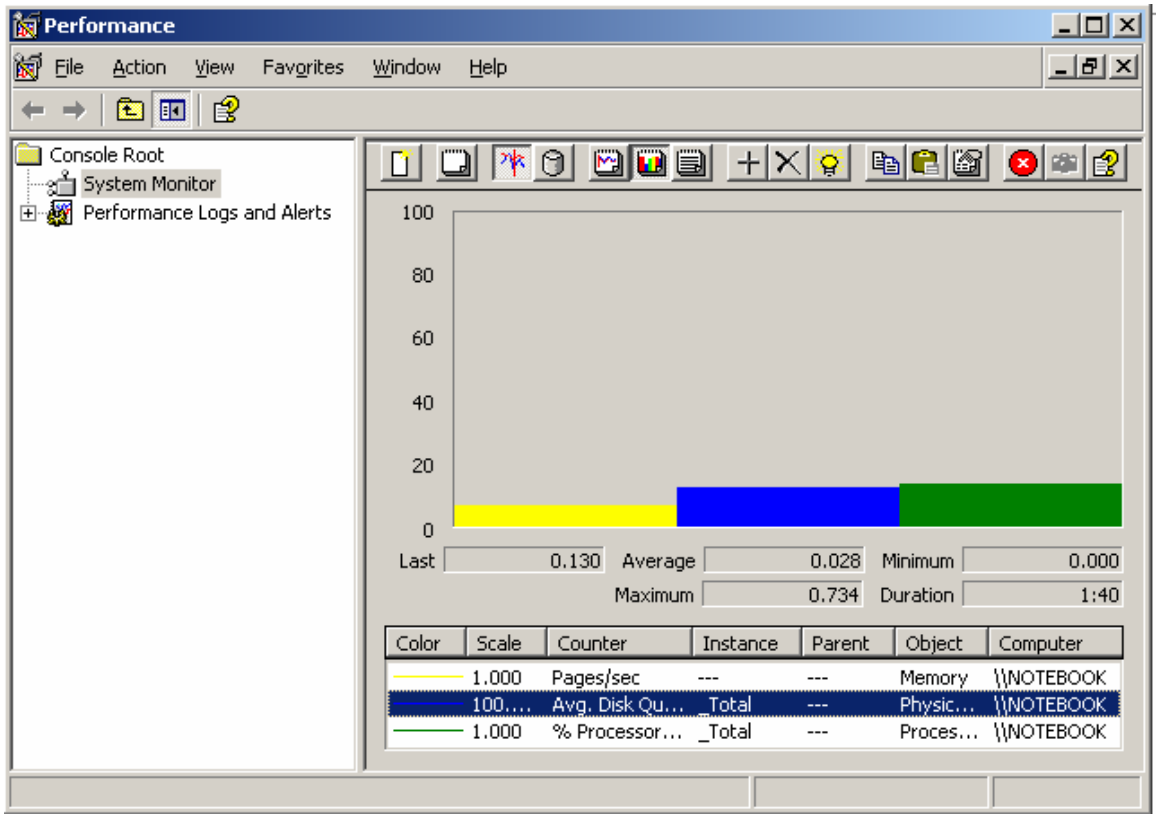
> ***LƯU Ý. Chỉnh sửa thuộc tính của đồ thị****. Hộp thoại* ***System Monitor Properties*** *chứa một lượng lớn các điều khiển khác mà bạn có thể sử dụng để chỉnh sửa cách hiển thị bề ngoài của đồ thị. Ví dụ, trong thẻ* ***Graph****, bạn có thể thêm vào Tiêu đề của trục và các đường kẻ lưới đồng thời trong thẻ* ***Appearance****, bạn có thể thay đổi màu nền của đồ thị và lựa chọn các kiểu (font) chữ khác.*

Sử dụng các cách Quan sát khác.

Bên cạnh đồ thị dạng đường, ***System Monitor*** còn hai cách thức xem khác để bạn có thể quan sát cùng một dữ liệu: Cách xem Biểu đồ và cách xem Báo cáo. Bạn có thể thay đổi cách hiển thị sang các cách trên bằng cách

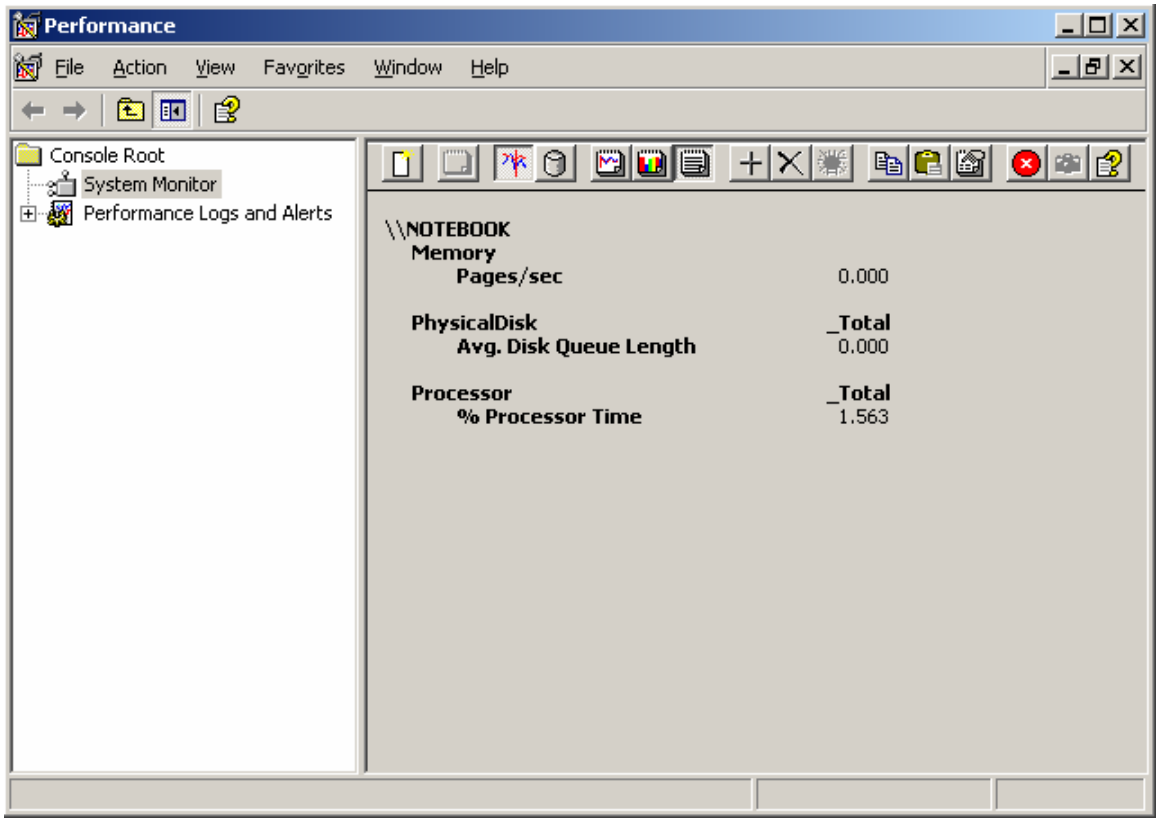
nhấn vào các phím ***View Histogram*** hoặc ***View Report*** trên thanh công cụ, hoặc bằng cách nhấn ***Ctrl+B*** hay ***Ctrl+R***. Để trở về cách xem đồ thị cũ, bạn nhấn vào phím ***View Graph*** hoặc nhấn ***Ctrl+G***.

Cách xem bằng Biểu đồ là một đồ thị bao gồm các thanh thẳng đứng cho mỗi ***biến đếm***, thể hiện trong Hình 3-15. Trong cách xem này, dễ dàng giám sát một lượng lớn các ***biến đếm*** bởi vì các dòng kẻ không trùng đè lên nhau.



Hình 3-15: Cách xem bằng biểu đồ trong *System Monitor*

Cách xem bằng Báo cáo (Thể hiện trong Hình 3-26) hiển thị các giá trị số cho mỗi ***performance counters*** (Biến đếm hiệu năng)

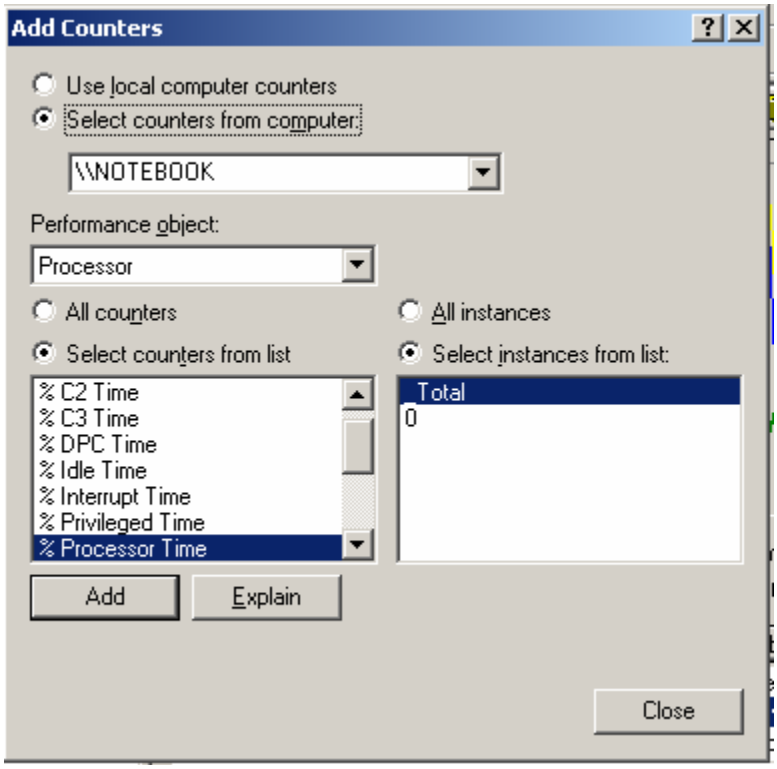


Hình 3-16: Cách xem bằng Báo cáo trong *System Monitor*

Cũng như cách dùng đồ thị, cách xem bằng Biểu đồ và Báo cáo đều cập nhật các giá trị của ***biến đếm*** sau khoảng thời gian cố định được thiết lập trong thẻ ***General*** của hộp thoại ***System Properties***. Nhược điểm chính của hai cách xem này là chúng không hiển thị giá trị trước của các ***biến đếm***, chỉ hiển thị giá trị hiện tại. Mỗi lần lấy mẫu mới sẽ ghi đè giá trị trước trên màn hình hiển thị, không giống như kiểu Đồ thị dạng đường hiển thị cả các giá trị trước đó.

Thêm các biến đếm (counter).

Ba ***Biến đếm Hiệu năng*** xuất hiện trong ***System Monitor*** theo mặc định là các thước đo rất hữu ích cho hiệu năng máy tính, tuy nhiên các snap-in còn bao gồm hàng tá các ***biến đếm*** khác mà bạn có thể thêm vào khung hiển thị. Để thêm các ***biến đếm*** vào trong khung Chi tiết của ***System Monitor***, nhấn vào phím ***Add*** trên thanh công cụ hoặc nhấn ***Ctrl+I*** để hiển thị hộp thoại ***Add Counters*** (Thể hiện trên Hình 3-17)



Hình 3-17: Hộp thoại *Add counter*

> ***LƯU Ý. Truy cập các chức năng của System Monitor***. *Không giống như các snap-in MMC khác,* ***System Monitor*** *không thêm các chức năng thường xuyên sử dụng của nó vào trong thực đơn* ***Action*** *của bảng điều khiển. Cách duy nhất để truy cập vào các chức năng của* ***System Monitor*** *là sử dụng thanh công cụ, kết hợp với các phím tắt và thực đơn ngữ cảnh xuất hiện khi bạn nhấn phải chuột vào khung hiển thị.*

Trong hộp thoại này, bạn phải chỉ rõ bốn mục thông tin sau đây để thêm một biến đếm vào khung hiển thị.

- **Computer (Máy tính)**. Tên của máy tính bạn muốn giám sát ***biến đếm*** đã chọn. Không giống như các snap-in MMC khác, bạn không thể chuyển hướng toàn bộ việc theo dõi của ***System Monitor*** vào một máy tính khác trên mạng cùng lúc. Thay vào đó, bạn phải chỉ rõ tên máy tính cho mỗi ***biến đếm*** mà bạn thêm vào khung hiển thị. Điều này cho phép bạn tạo ra một khung hiển thị thể hiện các ***biến đếm*** cho các máy tính khác nhau trong mạng, ví dụ một đồ thị đơn hiển thị các hoạt động của bộ vi xử lý của tất cả các máy tính trên mạng.
- **Performance object (Đối tượng cần đo hiệu năng).** Là việc phân loại đối tượng thể hiện các thành phần phần cứng và phần mềm riêng

biệt trong máy tính. Mỗi đối tượng cần đo hiệu năng này chứa một số các ***Biến đếm Hiệu năng*** liên quan đến các thành phần đó

- **Performance counters (Biến đếm hiệu năng).** Một biến số thể hiện một khía cạnh đặc biệt nào đó trong các hoạt động của các ***Performance object***.
- **Instance (Trường hợp riêng):** Một phần tử thể hiện một trường hợp riêng nhất định của ***Biến đếm Hiệu năng*** đã chọn. Ví dụ, trên một máy tính có hai giao tiếp mạng, mỗi ***biến đếm*** trong đối tượng cần đo hiệu năng Giao tiếp Mạng sẽ có hai ***instance***, mỗi ***instance*** cho một Giao tiếp, cho phép bạn theo dõi hiệu năng của mỗi cạc mạng riêng biệt. Một số ***biến đếm*** cũng có một số ***instance*** như Tổng số hoặc Trung bình, cho phép bạn theo dõi hiệu năng của tất cả mọi ***instance*** kết hợp lại hoặc giá trị trung bình của các ***instance***.

Khi bạn đã xác định tên một máy tính, một đối tượng cần đo hiệu năng, một biến đếm hiệu năng và ***instance*** của đối tượng đó, nhấn vào ***Add*** để thêm biến đếm này vào khung hiển thị. Hộp thoại vẫn còn mở để cho bạn có thể thêm vào nhiều biến đếm khác nữa. Nhấn ***Close*** khi bạn đã hoàn thành công việc thêm biến đếm hiệu năng.

> ***LƯU Ý: Hiểu các biến đếm***. *Nhấn vào phím* ***Explain*** *sẽ mở ra một hộp thông báo* ***Explain Text*** *chứa mô tả chi tiết về Biến đếm Hiệu năng mà bạn lựa chọn.*

Các ***Perfomance Object, Perfomance counter***, và các ***instance*** xuất hiện trong hộp thoại ***Add Counter*** tùy thuộc vào cấu hình phần cứng của máy tính, phần mềm trên máy tính đó và vai trò của máy tính đó trong mạng. Ví dụ, việc cài đặt dịch vụ DNS Server trên máy tính sẽ thêm vào Đối tượng cần đo Hiệu năng DNS, đối tượng này chứa một loạt các biến đếm để bạn theo dõi các hoạt động của máy chủ DNS.

Tạo cách hiển thị hiệu quả nhất.

Trong hầu hết các trường hợp, khi người dùng lần đầu tiên khám phá snap-in ***System Monitor***, họ sẽ lúng túng khi nhìn thấy hàng trăm ***biến đếm hiệu năng*** sẵn sàng để sử dụng và họ có thể tạo ra một đồ thị chứa hàng tá các ***biến đếm*** khác nhau. Số lượng của các ***biến đếm*** bạn có thể hiển thị một cách hiệu quả phụ thuộc vào kích thước của màn hình và độ phân giải của cạc màn hình.

Bạn nên quan tâm đến các lời khuyên sau đây khi lựa chọn các ***biến đếm***:

- **Giới hạn số lượng của các biến đếm**. Quá nhiều ***biến đếm*** sẽ dẫn tới khung đồ họa trở nên khó hiểu đồng thời làm giảm đáng kể hiệu năng của hệ thống. Để hiển thị một lượng lớn các thông số thống kê, bạn có thể hiển thị nhiều màn hình cửa sổ trong bảng điều khiển và lựa chọn các ***biến đếm*** khác nhau trong mỗi cửa sổ, hoặc sử dụng cách xem Biểu đồ hoặc Báo cáo để hiển thị một số lượng lớn các ***biến đếm*** trong một định dạng hiệu quả hơn (đồng nghĩa với việc bạn sẽ phải hài lòng khi không xem được các giá trị trước đó như cách xem trong đồ thị)
- **Chỉnh sửa thuộc tính hiển thị của biến đếm.** Tùy thuộc vào kích thước và khả năng của màn hình của bạn, màu mặc định và độ rộng của các đường sử dụng trong đồ thị của ***System Monitor*** có thể gây khó khăn khi phân biệt các ***biến đếm***. Trong thẻ ***Data*** của hộp thoại ***System Monitor Properties*** của mỗi ***biến đếm***, bạn có thể chỉnh sửa màu sắc, kiểu và độ rộng của đường thể hiện ***biến đếm*** đó trong đồ thị để dễ dàng phân biệt với các ***biến đếm*** khác.
- **Lựa chọn biến đếm với các giá trị có thể so sánh được.** ***System Monitor*** chấp nhận không giới hạn sự kết hợp của của các ***biến đếm*** bạn lựa chọn trong một đồ thị đơn, tuy nhiên một số thông số thống kê sẽ không thể hiển thị cùng với nhau bởi vì các giá trị của chúng khác hẳn nhau. Khi một đồ thị chứa một ***biến đếm*** có giá trị điển hình là dưới 20 và một biến đếm khác có giá trị điển hình là hàng trăm, rất khó có thể sắp xếp hiển thị các giá trị này để ta có thể đọc được cả hai ***biến đếm*** cùng lúc. Lựa chọn các ***biến đếm*** có giá trị khác nhau không đáng kể để bạn có thể hiển thị các giá trị đó cho dễ đọc. Hơn nữa, nếu bạn muốn hiển thị các ***biến đếm*** với các khoảng giá trị khác nhau, bạn có thể sử dụng cách xem bằng Báo cáo thay cho cách xem bằng Đồ thị.

Lưu Bảng điều khiển System Monitor

Khi bạn hài lòng với cách hiển thị mà bạn đã tạo ra, bạn có thể lưu nó lại như một file bằng cách chọn ***Save as*** từ thực đơn ***File*** và chỉ ra tên của file với phần mở rộng .msc. Nạp bảng điều khiển từ file này sẽ mở ***Performance console*** và hiển thị snap-in ***System Monitor***, với tất cả các biến đếm và các thuộc tính hiển thị mà bạn đã cấu hình trước khi lưu nó lại.

Giám sát hiệu năng của máy chủ.

Khi bạn đã hiểu cách sử dụng ***System Monitor***, bước tiếp theo là quyết định ***biến đếm*** nào trong hàng trăm ***biến đếm hiệu năng*** mà bạn sử dụng để giám sát hiệu năng máy tính hiệu quả nhất. Hiển nhiên là không thể có một câu trả lời đơn giản cho vấn đề trên trong mọi trường hợp. Có thể, bạn sẽ muốn tạo ra vài bảng điều khiển để giám sát các khía cạnh khác nhau của hiệu năng máy chủ hoặc cùng một khía cạnh nhưng trên nhiều máy chủ khác nhau.

Phương pháp thực hành tốt nhất là tạo ra một chiến lược giám sát máy chủ ngay sau khi máy chủ này được cài đặt và cấu hình đầy đủ. Theo cách này, bạn có thể thiết lập một đường cơ sở hiệu năng (baseline) cho máy chủ trong các trạng thái hiệu năng lúc sử dụng thông thường, lúc nghỉ và lúc làm việc tại mức đỉnh. Khi có sự cố xảy ra trong các lần giám sát sau đó, việc đo lại lần nữa giá trị đường cơ sở này có thể giúp bạn tìm ra giải pháp cho việc giải quyết sự cố.

> ***LƯU Ý: Tăng mức tải khi giám sát****. Cần nhớ rằng trong một số trường hợp, mức hiệu năng đo được bởi* ***System Monitor*** *bao gồm cả tài nguyên sử dụng bởi chính tiến trình đo này. Ví dụ, snap-in* ***System Monitor*** *sử dụng một số tài nguyên của bộ nhớ và thời gian của CPU giống như bất kỳ chương trình nào khác, và nếu bạn đang giám sát các* ***biến đếm*** *trên máy tính khác, tiến trình này có thể gây ra một số tải lưu thông mạng nhất định. Cần phải tính đến các yếu tố thêm vào này khi bạn phân tích kết quả của System Monitor*

Lý do chính của việc giám sát hiệu năng máy chủ sử dụng ***System Monitor*** là để đảm bảo các ứng dụng chạy trên máy chủ hoạt động tốt và để phát hiện ra hiện tượng nghẽn cổ chai ảnh hưởng đến hiệu suất hoạt động của máy tính. Việc các quản trị hệ thống phải đối mặt với các vấn đề sự cố hiệu năng máy tính là rất bình thường và không thể ngay lập tức qui cho một nguyên nhân cụ thể nào ví dụ như việc trục trặc của một dịch vụ nào đó. Người dùng có thể phàn nàn về việc máy chủ chậm trong khoảng thời gian nào đó trong ngày hoặc hiệu năng giảm dần sau một khoảng thời gian tính bằng tuần hoặc tháng. Khi điều này xảy ra, một trong những nguyên nhân là hiện tượng nghẽn cổ chai tại đâu đó trong đường truyền mạng giữa máy khách và dữ liệu trên máy chủ mà người dùng cần sử dụng.

Hiện tượng nghẽn cổ chai (***Bottleneck***) xẩy ra khi một thành phần nào đó không cung cấp một mức hiệu năng chấp nhận được so với hiệu năng của các thành phần khác trong hệ thống. Ví dụ người dùng có thể phàn nàn rằng hiệu năng máy chủ file của họ rất chậm và bạn có thể mất nhiều thời gian và

tiền bạc để nâng cấp mạng LAN của bạn từ 10Base-T thành 100Base-TX, hy vọng có thể cải thiện được tình hình. Tuy nhiên nếu máy chủ của bạn là một máy chủ cũ sử dụng các bộ vi xử lý Pentium thời đầu, sự cải thiện là không đáng kể bởi vì rất có thể là do bộ vi xử lý máy chủ, chứ không phải công nghệ mạng LAN, là nguyên nhân của hiện tượng nghẽn cổ chai. Mọi thành phần khác có thể chạy tốt nhưng bộ vi xử lý không thể xử lý kịp với luồng dữ liệu do hệ thống mạng mới và nhanh cung cấp được.

> ***LƯU Ý: Mục đích của kỳ thi.*** *Mục đích của kỳ thi 70-290 là học viên phải có khả năng "giám sát hiện tượng nghẽn cổ chai ở phần cứng máy chủ" và "giám sát và tối ưu môi trường máy chủ cho hiệu năng của ứng dụng" bằng cách giám sát các Đối tượng cần đo Hiệu năng như bộ nhớ, mạng, bộ vi xử lý và đĩa cứng.*

Hiện tượng nghẽn cổ chai có thể xuất hiện do rất nhiều nguyên nhân như sau:

- **Tăng mức tải trên máy chủ**. Một máy chủ có thể hoạt động tốt trong một vai trò cụ thể nào đó lúc đầu, tuy nhiên sau khi bạn tăng mức tải của máy chủ bằng cách thêm vào nhiều người dùng và nhiều tác vụ, có thể nhận thấy các phần tử trong máy chủ không hoạt động tốt như trước nữa. Ví dụ một máy chủ Web có thể là đủ dùng cho Web site của công ty trong giai đoạn đầu, tuy nhiên sau khi công ty giới thiệu thêm nhiều sản phẩm và lưu lượng dữ liệu đến site tăng lên gấp 3 lần. Đột nhiên bạn nhận thấy hiệu năng của đĩa trên máy chủ Web là không đủ để đáp ứng các lưu lượng dữ liệu tăng này.
- **Lỗi Phần cứng.** Lỗi Phần cứng không phải lúc nào cũng gây ra việc ngừng hoạt động nghiêm trọng của hệ thống. Một phần tử nào đó có thể hoạt động không đúng chức năng một cách không liên tục trong một khoảng thời gian dài, gây nên việc giảm hiệu năng của máy chủ một cách khó chịu. Ví dụ lỗi cáp mạng kết nối máy chủ đến thiết bị switch/hub có thể gây nên việc lưu thông mạng thỉng thoảng bị ngắt và làm giảm hiệu năng của máy chủ.
- **Thay đổi vai trò của máy chủ.** Các ứng dụng khác nhau yêu cầu các tài nguyên khác nhau. Bạn có một máy tính thực hiện chức năng của một máy chủ Web, tuy nhiên khi bạn thay đổi vai trò của máy chủ này thành máy chủ CSDL, bạn có thể thấy bộ vi xử lý hoạt động không đủ nhanh để chịu mức tải của ứng dụng mới trên nó.

Việc xác ddinhj vị trí nghẽn cổ chai gây ra việc giảm hiệu năng hệ thống là một nhiệm vụ rất phức tạp, nhưng giám sát các Biến đếm Hiệu năng một

cách hợp lý trong ***System Monitor*** là một cách tốt để bắt đầu nhiệm vụ này. Trong rất nhiều trường hợp, nguyên nhân của hiện tượng này có thể thu hẹp về bốn phân hệ chính liệt kê ở phần đầu của chương (Bộ vi xử lý, bộ nhớ, đĩa cứng và mạng)

Khi bạn giám sát các mức hiệu năng máy chủ, tốt nhất là nên bắt đầu từ trên xuống dưới-có nghĩa là bạn bắt đầu với việc giám sát bao quát toàn bộ cấu hình của mỗi phân hệ để xác định một phân hệ nào có khả năng gây ra sự cố nhất. Khi bạn đã xác định được vùng gây sự cố tổng quát, bạn có thể nhìn sâu hơn vào từng dịch vụ và ứng dụng sử dụng phân hệ đó nhiều nhất và thậm chí xem cả mức giao thức và luồng nếu cần. Thông thường, sự cố gây ra bởi một ứng dụng hoặc thiết bị, hoặc thiếu tài nguyên trong hệ thống. Một thiết bị đơn có thể được cấu hình lại hoặc thay thế và các tài nguyên chung có thể được tăng cường (ví dụ bằng cách thêm nhiều bộ nhớ RAM hoặc thêm bộ vi xử lý) một cách thích hợp.

Các mục sau đây sẽ thảo luận về các vấn đề cần tìm hiểu và các Biến đếm Hiệu năng được sử dụng để giám sát mỗi phân hệ trong bốn phân hệ trên.

Giám sát hiệu năng của bộ vi xử lý

Một mảng các bộ vi xử lý bị trục trặc hoặc hoạt động không đủ công suất có thể dẫn đến việc máy chủ sẽ đưa các yêu cầu của máy khách vào hàng đợi, ngăn cản việc máy chủ đáp ứng các yêu cầu của người dùng một cách nhanh chóng. Để giám sát tổng quan phân hệ vi xử lý, sử dụng các Biến đếm Hiệu năng sau đây:

> ***LƯU Ý. Xác định các biến đếm.*** *Các biến đếm hiệu năng trong phần này và phần sau được viết theo định dạng sau: Đối tượng cần đo Hiệu năng:biến đếm hiệu năng*

- **Processor: % Processor time (Vi xử lý:% Thời gian xử lý).** Cho biết phần trăm thời gian mà bộ vi xử lý bận. Giá trị này càng thấp càng tốt và dưới 85% thì coi là chấp nhận được. Nếu giá trị này luôn giữ ở mức cao, bạn phải xác định tiến trình nào chiếm quá nhiều thời gian xử lý, nâng cấp bộ vi xử lý hoặc thêm một bộ vi xử lý khác nếu có thể
- **System: Processor Queue Length (Hệ thống:Độ dài hàng đợi vi xử lý).** Chỉ ra số lượng các luồng chương trình đang đợi để được xử lý bởi bộ vi xử lý. Giá trị này càng thấp càng tốt, thông thường dưới 10 là có thể chấp nhận được. Nếu giá trị này luôn giữ ở mức cao, nâng cấp bộ vi xử lý hoặc thêm một bộ vi xử lý khác.

- **Server Work Queues: Queue Length (Hàng đợi công việc của máy chủ**:**Độ dài hàng đợi).** Chỉ ra số lượng yêu cầu đang nằm đợi để sử dụng một bộ vi xử lý nào đó. Giá trị này càng thấp càng tốt và thông thường dưới 4 là chấp nhận được. Nếu giá trị này luôn giữ ở mức cao, nâng cấp bộ vi xử lý hoặc thêm một bộ vi xử lý khác.
- **Processor: Interrupts/sec (Bộ vi xử lý:Ngắt/giây).** Chỉ ra số lượng các ngắt phần cứng mà vi xử lý phục vụ tính theo giây. Giá trị này có thể biến đối rất lớn và có ý nghĩa chỉ trong mối tương quan với mức đường cơ sở được thiết lập trước đó. Một thiết bị phần cứng sinh ra nhiều ngắt có thể độc quyền chiếm bộ vi xử lý, ngăn cản bộ vi xử lý phục vụ các tác vụ khác. Nếu giá trị này tăng một cách nhanh chóng, kiểm tra các thành phần phần cứng khác nhau trong hệ thống để xác định thành phần nào sinh ra quá nhiều ngắt.

Giám sát hiệu năng bộ nhớ

Một bộ nhớ không đủ trong máy chủ có thể không cho máy tính lưu đệm thường xuyên các dữ liệu cần thiết, gây ra việc các tiến trình phải dựa vào việc đọc đĩa hơn là đọc bộ nhớ và do đó làm giảm tốc độ của toàn hệ thống. Bộ nhớ là một phân hệ đơn quan trọng nhất cần phải giám sát bởi vì các sự cố trong bộ nhớ có thể ảnh hưởng đến tất cả các phân hệ khác. Ví dụ, khi tình trạng của bộ nhớ gây ra quá nhiều thao tác phân trang đến đĩa, hệ thống trông có vẻ như có trục trặc trong phân hệ lưu trữ trong khi thực tế bộ nhớ là thủ phạm

Một trong các nguyên nhân thông thường có thể gây ra các trục trặc liên quan đến bộ nhớ là rò rỉ bộ nhớ (***Memory leak***). Việc rò rỉ bộ nhớ là kết quả của việc một chương trình chiếm dụng quá nhiều bộ nhớ mà không giải phóng sau khi không sử dụng nữa. Theo thời gian, các bộ nhớ trống trong máy tính có thể bị chiếm dụng hoàn toàn, làm giảm hiệu năng hệ thống và cuối cùng làm dừng hệ thống. Việc rò rỉ bộ nhớ có thể rất nhanh, gây ra sự suy giảm ngay lập tức đối với hiệu năng hệ thống, tuy nhiên ta cũng có thể mất nhiều thời gian và rất khó khăn để phát hiện ra chúng, khi mà việc giảm hiệu năng hệ thống này diễn ra từ từ theo hàng ngày hoặc hàng tuần. Trong hầu hết các trường hợp, sự rò rỉ bộ nhớ có thể gây ra bởi các ứng dụng của các hãng thứ ba mà hệ điều hành chưa từng biết đến.

Để giám sát hiệu năng cơ bản của bộ nhớ, sử dụng các ***biến đếm*** sau đây:

- **Memory: Page Faults/Sec (Bộ nhớ:Lỗi trang/giây).** Chỉ ra số lần trên giây mà đoạn mã hoặc dữ liệu cần để xử lý không tìm thấy trong bộ nhớ. Giá trị này càng thấp càng tốt, thông thường dưới 5 là chấp

nhận được. ***Biến đếm*** này bao gồm cả lỗi nhẹ (trong đó trang yêu cầu có thể tìm thấy đâu đó trong bộ nhớ) và lỗi nặng (trong đó trang yêu cầu buộc phải truy cập từ đĩa cứng). Các lỗi nhẹ sinh ra không phải là một vấn đề lớn, tuy nhiên các lỗi nặng có thể gây ra trễ đáng kể vì truy cập đĩa cứng chậm hơn rất nhiều so với truy cập bộ nhớ. Nếu giá trị này quá lớn, bạn nên kiểm tra xem hệ thống có đang phải chịu quá nhiều lỗi nặng bằng cách sử dụng Biến đếm ***Memory: Pages/Sec***. Nếu số lượng lỗi nặng là quá nhiều, bạn nên xem xét tiến trình nào gây nên việc phân trang quá nhiều hoặc cài đặt thêm bộ nhớ RAM cho hệ thống.

- **Memory: Pages/Sec (Bộ nhớ:Trang /giây).** Chỉ ra số lượng trang dữ liệu trên giây không nằm trong RAM và phải truy cập từ đĩa hoặc phải ghi lên đĩa để tạo không gian trống cho RAM. Giá trị này càng thấp càng tốt và thông thường dưới 20 là có thể chấp nhận được. Nếu giá trị này quá cao, bạn nên xem xét tiến trình nào gây nên sự phân trang quá nhiều hoặc cài đặt thêm RAM cho hệ thống.
- **Memory: Available Bytes (Bộ nhớ:Các byte trống).** Chỉ ra dung lượng bộ nhớ vật lý còn trống tính theo Byte. (Còn có các biến đếm khác hiển thị cùng loại giá trị này nhưng được tính theo kilobyte hoặc megabyte). Giá trị này càng cao càng tốt và không nên dưới 5% của tổng số bộ nhớ RAM trong hệ thống, việc bộ nhớ còn trống còn quá ít có thể là biểu hiện của bộ nhớ đang bị rò rỉ. Nếu giá trị này quá thấp, xem xét việc thêm RAM cho hệ thống.
- **Memory: Committed Bytes (Bộ nhớ: Các Byte đã cam kết).** Cho biết dung lượng bộ nhớ ảo có khoảng không gian được dự trữ trên tệp phân trang. Giá trị này nên càng thấp càng tốt và nên luôn giữ thấp hơn dung lượng RAM vật lý có trong hệ thống. Giá trị này quá lớn cho thấy có thể có sự rò rỉ bộ nhớ và bạn nên xem xét việc thêm RAM cho hệ thống
- **Memory: Pool Non-Paged Bytes (Bộ nhớ: các byte của vùng không phân trang).** Cho biết kích thước của vùng trong bộ nhớ được sử dụng bởi hệ điều hành cho các đối tượng mà không thể ghi vào trong đĩa. Giá trị này nên là một số ổn định và không tăng trưởng khi không có thêm các hoạt động của máy chủ. Nếu giá trị này tăng theo thời gian, điều đó thể hiện có thể hệ thống đang bị rò rỉ bộ nhớ.

Giám sát hiệu năng đĩa cứng.

Phân hệ đĩa cứng bị quá tải khi đọc và ghi lệnh có thể làm giảm tỷ lệ máy chủ xử lý các yêu cầu của máy khách. Các đĩa cứng trong máy chủ chứa một lượng lớn các dữ liệu vật lý hơn bất kì một phân hệ nào do phải đáp ứng các yêu cầu I/O của rất nhiều máy khách, đầu đọc đĩa cứng phải di chuyển liên tục tới các vị trí khác nhau trên vùng đĩa phẳng. Kĩ thuật mà đầu đọc di chuyển là rất nhanh, tuy nhiên một khi đĩa đạt đến tốc độ đọc/ghi tối đa, các yêu cầu thêm nữa có thể bắt đầu gây ra sự chèn ép trong hàng đợi xử lý. Đối với lý do này, phân hệ lưu trữ là một phần tử cần quan tâm hàng đầu khi có nghẽn cổ chai.

- **PhysicalDisk: Disk Bytes/sec (Đĩa vật lý:Byte/giây).** Cho biết số byte trung bình được chuyển đến hoặc ra khỏi đĩa trong mỗi giây. Giá trị này nên tương ứng với mức thiết lập trong đường cơ sở ban đầu hoặc cao hơn. Việc giá trị này giảm đi cho thấy trục trặc trong đĩa cứng thậm chí có thể là hỏng. Nếu trường hợp này xảy ra, xem xét việc nâng cấp phân hệ đĩa lưu trữ.
- **PhysicalDisk: Avg. Disk Bytes/Transfer (Đĩa vật lý: byte trung bình /Giao dịch).** Cho biết số byte trung bình được chuyển vận trong quá trình vận hành đọc và ghi. Giá trị này nên tương ứng với mức thiết lập trong đường cơ sở ban đầu hoặc cao hơn. Việc giá trị này giảm đi cho thấy trục trặc trong đĩa cứng thậm chí có thể là hỏng. Nếu trường hợp này xảy ra, xem xét việc nâng cấp phân hệ đĩa lưu trữ.
- **PhysicalDisk: Current Disk Queue Length (Độ dài hàng đợi đĩa hiện tại).** Cho biết số lượng yêu cầu đọc hoặc ghi đĩa đang tồn đọng. Giá trị này nên càng thấp càng tốt, với mức thông thường thấp hơn 2 là có thể chấp nhận được trên 1 trục quay đĩa. Giá trị biến đếm này mà lớn có thể cho thấy đĩa cứng đang trục trặc hoặc nó không có khả năng đáp ứng các yêu cầu đối với nó. Trong trường hợp này, bạn nên xem xét việc nâng cấp phân hệ đĩa lưu trữ
- **PhysicalDisk: % Disk Time (Đĩa cứng:Phần trăm thời gian đĩa).** Cho biết phần trăm thời gian mà đĩa cứng bận. Giá trị này càng thấp càng tốt và thông thường dưới 80% là chấp nhận được. Giá trị của biến đếm này cao chứng tỏ rằng hoạt động của đĩa đang trục trặc, hoặc nó không có khả năng theo kịp các yêu cầu đối với nó, hoặc trục trặc trong bộ nhớ gây nên việc phân trang đĩa quá nhiều. Kiểm tra việc bộ nhớ rò rỉ hoặc các vấn đề liên quan và nếu không có lỗi nào tìm thấy, bạn nên xem xét việc nâng cấp phân hệ đĩa lưu trữ.
- **LogicalDisk: % Free Space (Đĩa logic:%Đĩa trống).** Cho biết phần trăm đĩa trống trên đĩa cứng. Giá trị này càng lớn càng tốt, thông

thường lớn hơn 20% là chấp nhận được. Nếu giá trị này quá thấp, bạn nên thêm đĩa cứng.

Hầu hết các sự cố trong phân hệ đĩa cứng, khi không phải do phần cứng trục trặc gây ra, đều dẫn đến kết quả là phải nâng cấp hệ thống lưu trữ. Việc nâng cấp này có thể bao gồm các phương pháp sau đây:

- Cài đặt các đĩa cứng mới nhanh hơn
- Cài đặt thêm đĩa cứng và phân chia dữ liệu trên các đĩa đó, giảm truy cập I/O trên mỗi đĩa
- Thay thế các đĩa đơn bằng các dãy đĩa RAID (***Redundant Array of Independent Disks*** – Dãy các đĩa độc lập dư thừa)
- Thêm nhiều đĩa vào trong dãy đĩa RAID sẵn có

Giám sát hiệu năng mạng.

Giám sát hiệu năng mạng là nhiệm vụ phức tạp hơn rất nhiều việc giám sát các phân hệ khác bởi vì rất nhiều yếu tố bên ngoài máy tính có thể ảnh hưởng đến hiệu năng mạng. Bạn có thể sử dụng các ***biến đếm*** sau đây để thử xác định nếu như một sự cố mạng xảy ra, nhưng nếu bạn nghi ngờ một sự cố nào đó, bạn nên bắt đầu tìm kiếm nguyên nhân từ ngoài máy tính của bạn trước

- **Network Interface: Bytes Total/sec (Giao tiếp mạng:Tổng số Byte/giây).** Cho biết số lượng byte gửi và nhận trên giây trên một giao tiếp mạng. Giá trị này nên tương ứng với mức thiếp lập tại đường cơ sở dự kiến ban đầu hoặc cao hơn. Giá trị này giảm chứng tỏ có trục trặc trong thiết bị mạng hoặc sự cố khác trong mạng.
- **Network Interface: Output Queue Length (Giao tiếp mạng:Độ dài hàng đợi ra).** Cho biết số lượng gói tin đợi để truyền đi qua giao tiếp mạng. Giá trị này càng thấp càng tốt và có thể là zero mặc dù giá trị là 2 hoặc thấp hơn là có thể chấp nhận được. Nếu giá trị này là quá cao, giao tiếp mạng có thể bị trục trặc hoặc có thể tồn tại sự cố mạng khác.
- **Server: Bytes Total/Sec (Máy chủ: Tổng số byte/giây).** Cho biết tổng số byte gửi và nhận bởi máy chủ trên tất cả các giao tiếp mạng của nó. Giá trị này nên không quá 50% của tổng băng thông của giao tiếp mạng trong máy chủ. Nếu giá trị này quá cao, xem xét việc chuyển một số ứng dụng sang máy chủ khác hoặc nâng cấp sang một mạng nhanh hơn.

Băng thông của các kết nối mạng giới hạn lưu lượng đến máy chủ thông qua các giao tiếp mạng. Nếu giá trị của các biến đếm này cho biết rằng mạng đang bị nghẽn, có hai cách để nâng cấp mạng và không có cách nào là đơn giản cả:

- **Tăng tốc độ của mạng**. Điều này có nghĩa là thay thế tất cả các giao tiếp mạng trong mọi máy tính, hub, router và các thiết bị khác trên mạng và có thể thay thế cả cáp mạng.
- **Cài đặt thêm thiết bị giao tiếp mạng trong máy chủ và tái phân bố lại mạng**. Nếu lưu lượng dữ liệu thường xuyên làm ngập tràn giao tiếp mạng trên máy chủ, chỉ có một cách để tăng cường băng thông mạng mà không cần tăng tốc độ mạng là cài đặt thêm các giao tiếp mạng. Tuy nhiên, việc kết nối thêm các giao tiếp trong cùng một mạng sẽ không cho phép tải được nhiều lưu lượng mạng hơn đến máy chủ. Thay vào đó, bạn phải tạo thêm các subnet (mạng con) trên mạng và tái phân bố các máy tính vào trong mạng con đó, do đó sẽ có ít lưu lượng mạng hơn trong mỗi subnet.

Giám sát các vai trò máy chủ

Khi bạn giám sát hiệu năng máy chủ và tìm kiếm các nghẽn cổ chai, điều quan trọng là bạn phải hiểu sự liên quan của các vai trò mà máy chủ đó thực thi. Các ứng dụng và dịch vụ có các yêu cầu khác nhau đến tài nguyên hệ thống và chính sách giám sát của bạn cho mỗi máy chủ nên tập trung vào các Đối tượng cần đo Hiệu năng và các Biến đếm Hiệu năng của các tài nguyên ảnh hưởng lớn nhất đến máy chủ đó. Bảng 3-3 liệt kê một số vai trò máy chủ thông dụng, tài nguyên quan trọng đối với mỗi vai trò và các Đối tượng cần đo Hiệu năng mà bạn nên giám sát.

Bảng 3-3: Vai trò máy chủ và các đối tượng cần giám sát

Vai trò máy chủ	Tài nguyên sử dụng	Các Performance Object cần giám sát
Máy chủ ứng dụng	Bộ nhớ, mạng và bộ vi xử lý	Bộ nhớ, Bộ vi xử lý, Giao tiếp mạng và Hệ thống
Máy chủ sao lưu	Bộ vi xử lý và mạng	Hệ thống, Máy chủ, Bộ vi xử lý và Giao tiếp mạng
Máy chủ CSDL	Lưu trữ, mạng và bộ vi xử lý	Đĩa vật lý, Đĩa logic, Bộ vi xử lý, Giao tiếp mạng và Hệ thống

Máy chủ quản trị miền	Bộ nhớ, bộ vi xử lý, mạng và đĩa	Bộ nhớ, Bộ vi xử lý, Hệ thống, Giao tiếp mạng, các đối tượng giao thức (phụ thuộc vào mạng nhưng có thể bao gồm TCPv4, UDPv4, ICMP, IPv4, Kết nối NBT, NWLink IPX, NWLink IPX, NWLink NetBIOS, và NWLink SPX), Đĩa vật lý và Đĩa logic
Máy chủ file và in ấn	Bộ nhớ, đĩa và các phần tử mạng	Bộ nhớ, Giao tiếp mạng, Đĩa vật lý, Đĩa logic và Hàng đợi máy in
Máy chủ Mail/Truyền tin	bộ vi xử lý, đĩa, mạng và bộ nhớ	Bộ nhớ, Cache, Bộ vi xử lý, Hệ thống, Đĩa vật lý, Giao tiếp mạng và Đĩa logic
Máy chủ Web	Cache trên đĩa và các phần tử mạng	Cache, Giao tiếp mạng, Đĩa vật lý và Đĩa logic

Sử dụng Performance Logs and Alerts

Mặc dù snap-in ***System Monitor*** là rất hữu ích tuy nhiên rất ít quản trị mạng có thời gian hay sở thích ngồi xem các đồ thị dạng đường trên màn hình đồ họa để tìm các dấu hiệu sự cố trên máy chủ của họ. ***Performance Logs and Alerts*** (*Nhật ký và Cảnh báo Hiệu năng*) làm giảm thiểu được nhu cầu làm việc đó. ***Performance Logs and Alerts*** là một snap-in trong MMC cung cấp khả năng giám sát bằng nhật ký sử dụng các Đối tượng cần đo Hiệu năng và Biến đếm Hiệu năng giống như ***System Monitor*** sử dụng. Với snap-in này, bạn có thể thu thập các dữ liệu hiệu năng tự động từ các máy tính nội bộ và ở xa, lưu nó trong các định dạng khác nhau và tạo ra các cảnh báo khi một ***biến đếm*** cá biệt nào đó đạt đến mức ngưỡng xác định.

Khi bạn lựa chọn snap-in ***Performance Logs And Alerts*** trong bảng điều khiển Hiệu năng (***Performance console***), bạn có thể thấy ba tiêu đề phụ như sau:

- **Counter Logs (Nhật ký các biến đếm).** Cho phép ***Performance console*** chụp các thông số thống kê cho các ***biến đếm*** nhất định vào một file nhật ký tại các thời điểm xác định và đều đặn sau một khoảng thời gian cố định
- **Trace Logs (Nhật ký theo dõi).** Cho phép ***Performance console*** ghi lại các thông tin về các ứng dụng hệ thống khi một sự kiện nào đó xảy ra, ví dụ như lỗi hoạt động I/O của đĩa hoặc lỗi phân trang bộ nhớ.
- **Alerts (Cảnh báo).** Cho phép ***Performance console*** giám sát giá trị của một ***biến đếm*** nhất định nào đó theo các khoảng thời gian lặp và

thực hiện một hành động xác định khi ***biến đếm*** đó đạt đến giá trị giới hạn nào đó.

Một trong những lợi ích chính của ***Performance Logs and Alerts*** là cho phép bạn chụp các thông tin về hiệu năng của các ***biến đếm*** để nghiên cứu về sau. Snap-in này hỗ trợ rất nhiều định dạng file cho phép bạn lưu các thông tin chụp được vào các chương trình bảng và CSDL. Bạn có thể sử dụng nhật ký các ***biến đếm*** để thiết lập một đường cơ sở cho hiệu năng hệ thống và sau đó đều đặn kiểm tra các nhật ký này để xem sai lệch so với đường cơ sở chuẩn là bao nhiêu. Bạn còn có thể tạo ra các cảnh báo để báo động cho bạn biết khi tình trạng mạng sai lệch quá nhiều so với trạng thái thông thường.

> ***LƯU Ý: Ghi nhật ký tự động***. ***Performance Logs and Alerts*** *chạy như một dịch vụ, điều này có nghĩa là bạn có thể cấu hình snap-in này để giám sát các* ***biến đếm hiệu năng*** *nhất định. Dịch vụ này sẽ được nạp trong quá trình hệ thống khởi động và tiếp tục hoạt động thậm chí cả khi không có người dùng nào đăng nhập vào hệ thống.*

Tạo ra các counter log (Nhật ký biến đếm):

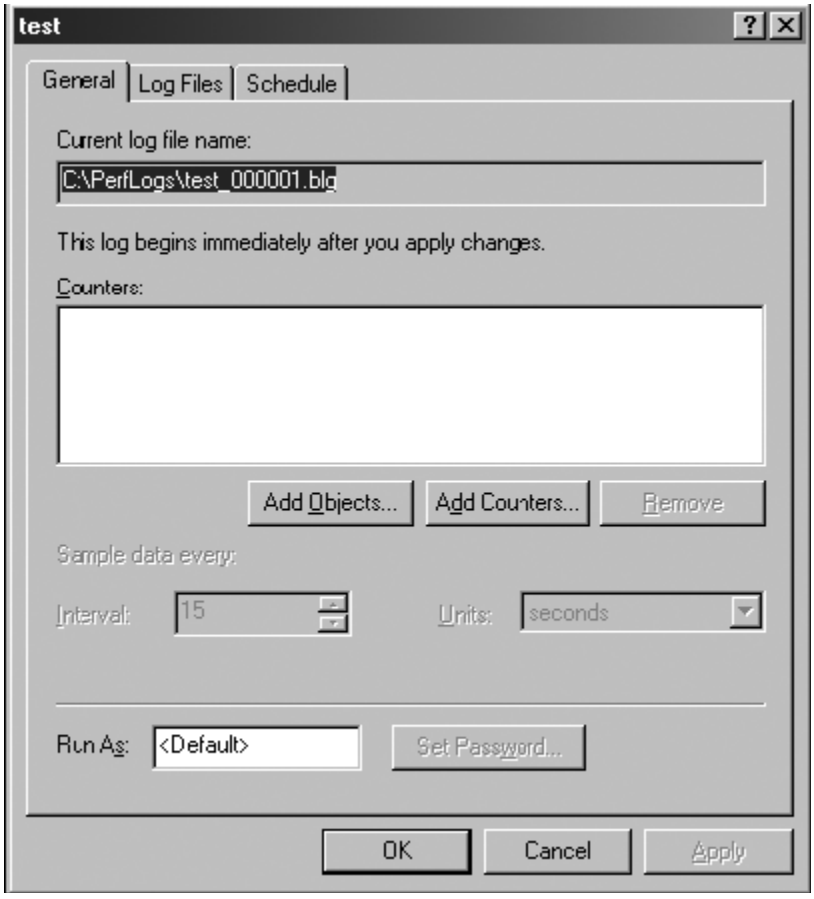
Để tạo ra các ***nhật ký biến đếm*** trong snap-in ***Performance Logs and Alerts***, bạn có thể lựa chọn đối tượng ***Counter Logs*** trong khung Phạm vi và lựa chọn ***New Log Settings*** từ thực đơn ***Action***. Sau khi bạn nhập vào tên của nhật ký mới, bạn sẽ thấy một hộp thoại (Thể hiện trong Hình 3-18) trong đó bạn nhập vào các thông tin sau đây:

- **Các Performance objects và Performance counters**. Bạn sẽ chọn các ***Performance objects*** và ***Performance counters*** và cả giao diện giống như khi bạn sử dụng ***System Monitor***.
- ***Sample Interval (*****Thời gian lặp lấy mẫu)**. Thời gian lặp mà tại đó snap-in này sẽ ghi vào nhật ký giá trị của biến đếm bạn đã lựa chọn. Lưu ý rằng thời gian lặp lấy mẫu mà ngắn sẽ cho ra file nhật ký lớn và đồng thời hệ thống sẽ phải làm việc nhiều hơn. Giá trị chọn nên tùy thuộc vào thời gian bạn mà dự định ghi nhật ký cho ***biến đếm*** là bao lâu.
- ***Run as credentials*** **(Các thông số đăng nhập Run as)**. Tên người dùng và mật khẩu mà dịch vụ ***Performance Logs and Alerts*** sử dụng để đăng nhập vào hệ thống trước khi chụp các thông tin vào trong ***nhật ký biến đếm***.

- ***Log file type (*Kiểu file nhật ký)**. Định dạng file nhật ký mà bạn muốn sử dụng cho ***nhật ký biến đếm*** và thư mục mà bạn muốn lưu. Bạn có thể lưu nhật ký này như một file văn bản có phân cách các trường dữ liệu bằng dấu phẩy hoặc dấu cách (tab), một file nhị phân dạng thông thường hoặc dạng lặp vòng (có thể xem trong ***System Monitor***), hoặc một file CSDL trong SQL. Bạn còn có thể chỉ ra kích thước tối đa của file nhật ký và cách tạo tên của file tự động.

  ***LƯU Ý: Sử dụng file lặp vòng**. Môt file lặp vòng nhị phân là file trong đó snap-in liên lục ghi các thông tin vào cùng một file và ghi đè các dữ liệu cũ nhất mà nó đã từng ghi trước đó.*

- ***Scheduling information (*Các thông tin lập lịch).** Bạn có thể cấu hình ***nhật ký biến đếm*** khởi động và dừng tại các thời điểm ngày và giờ xác định hoặc bạn có thể lựa chọn khởi động hoặc dừng quá trình ghi nhật ký một cách thủ công từ snap-in.
- ***Close Command* (Lệnh khi đóng).** Cho phép bạn chỉ định lệnh mà snap-in phải chạy khi file nhật ký được đóng lại.

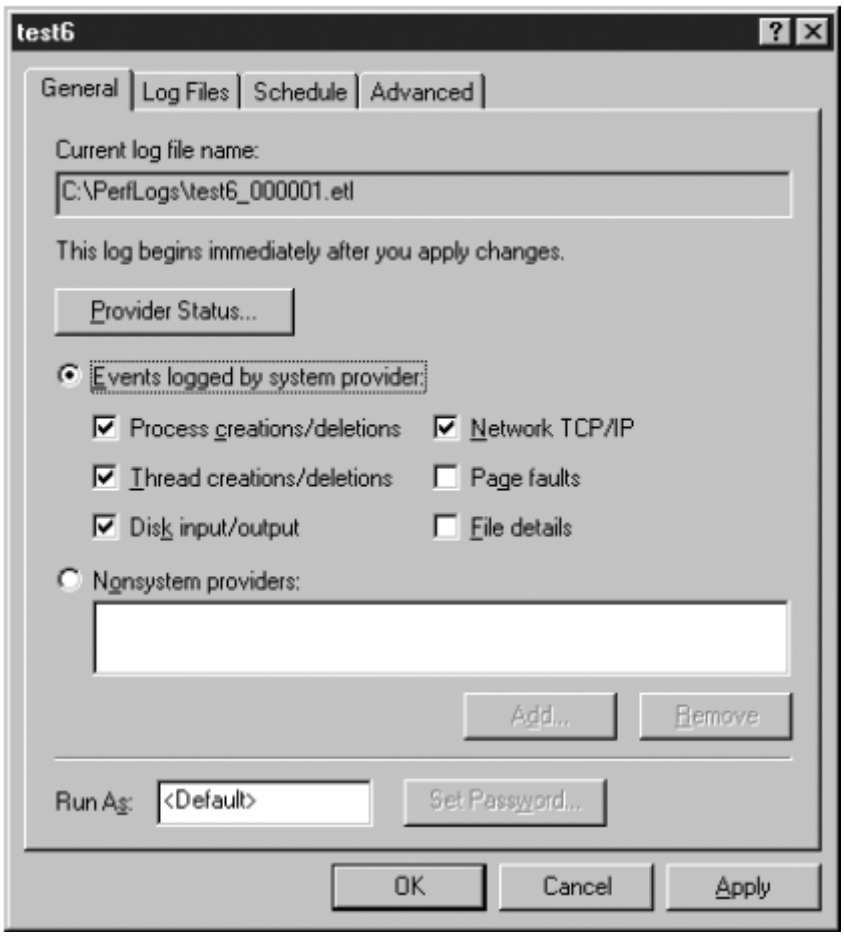


Hình 3-18: Hộp thoại cấu hình *nhật ký biến đếm (Counter Log)*

Khi bạn cấu hình ***nhật ký biến đếm***, nó xuất hiện trong khung Phạm vi của snap-in với một biểu tượng, màu của biểu tượng thể hiện trạng thái hiện tại của nhật ký. Một biểu tượng màu đỏ có nghĩa là đang dừng và màu xanh có nghĩa là đang chạy.

Tạo ra một Trace log.

Quá trình tạo ra một ***trace log*** (*Nhật ký Theo dõi*) tương tự như quá trình tạo ra một ***nhật ký biến đếm***, ngoài trừ việc thay vì lựa chọn ***performance counters***, bạn lại lựa chọn các sự kiện hệ thống (***System events***) mà bạn muốn giám sát, sử dụng giao diện trong Hình 3-19.

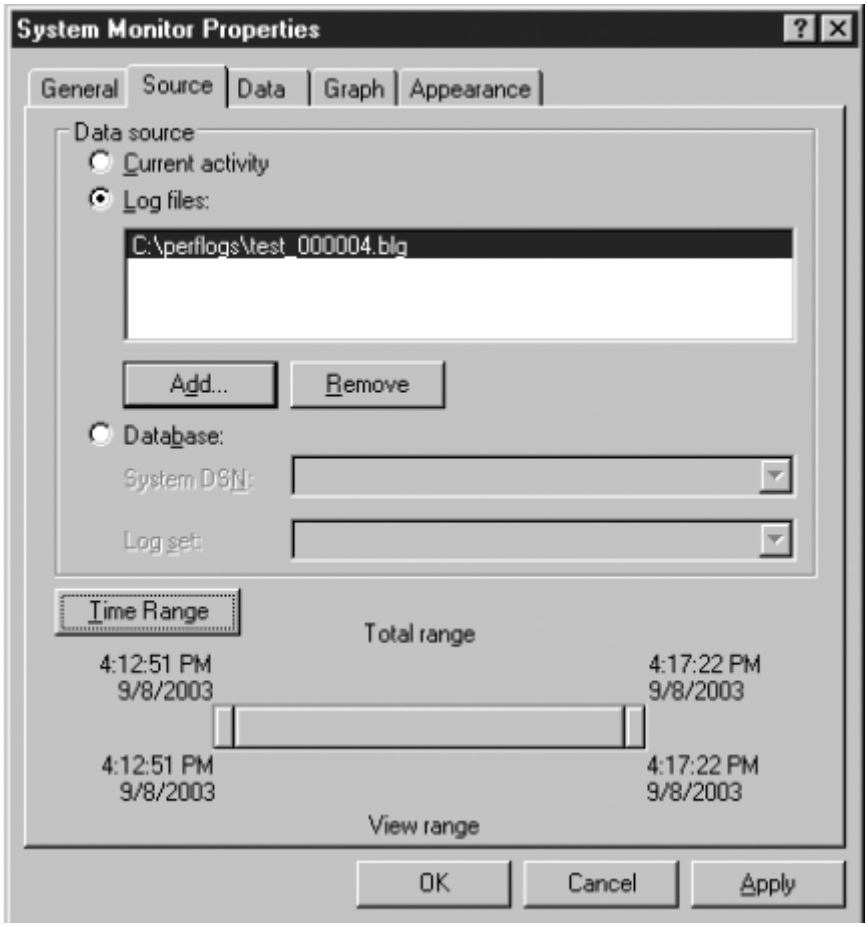


Hình 3-19: Hộp thoại cấu hình *trace log*

Xem nhật ký biến đếm (counter log).

Khi bạn lựa chọn lưu một ***nhật ký biến đếm*** thành một file nhị phân, nó sẽ xuất hiện trong thư mục đích như một file có phần mở rộng ***.blg***. Để mở một trong các file này và xem nội dung của nó, bạn vào snap-in ***System Monitor*** và nhấn vào thanh công cụ ***View Log Data*** hoặc nhấn ***Ctrl+L***. Trong hộp thoại ***System Monitor Properties*** (Thể hiện trong Hình 3-20), bạn phải cấu hình các thành phần sau đây:

- **Nguồn dữ liệu**. Trong Thẻ ***Source***, nhấn vào tùy chọn ***Log Files*** và lựa chọn file nhật ký mà bạn muốn hiển thị.
- **Khoảng thời gian**. Trong thẻ ***Source***, nhấn vào phím ***Time Range*** để hiển thị một thanh trượt chứa khoảng thời gian mà dữ liệu được chụp vào trong nhật ký. Bạn có thể sử dụng thanh trượt này để lựa chọn tất cả hoặc một phần của nhật ký để hiển thị.
- **Biến đếm**. Trong thẻ ***Data***, nhấn vào ***Add*** và lựa chọn các ***biến đếm*** mà bạn muốn hiển thị. Trong trường hợp này, hộp thoại ***Add Counter*** chỉ chứa các Đối tượng cần đo Hiệu năng và Biến đếm Hiệu năng mà bạn đã từng chọn ghi lại trong nhật ký.



Hình 3-20: Hộp thoại *System Monitor Properties* được cấu hình để hiển thị một file nhật ký

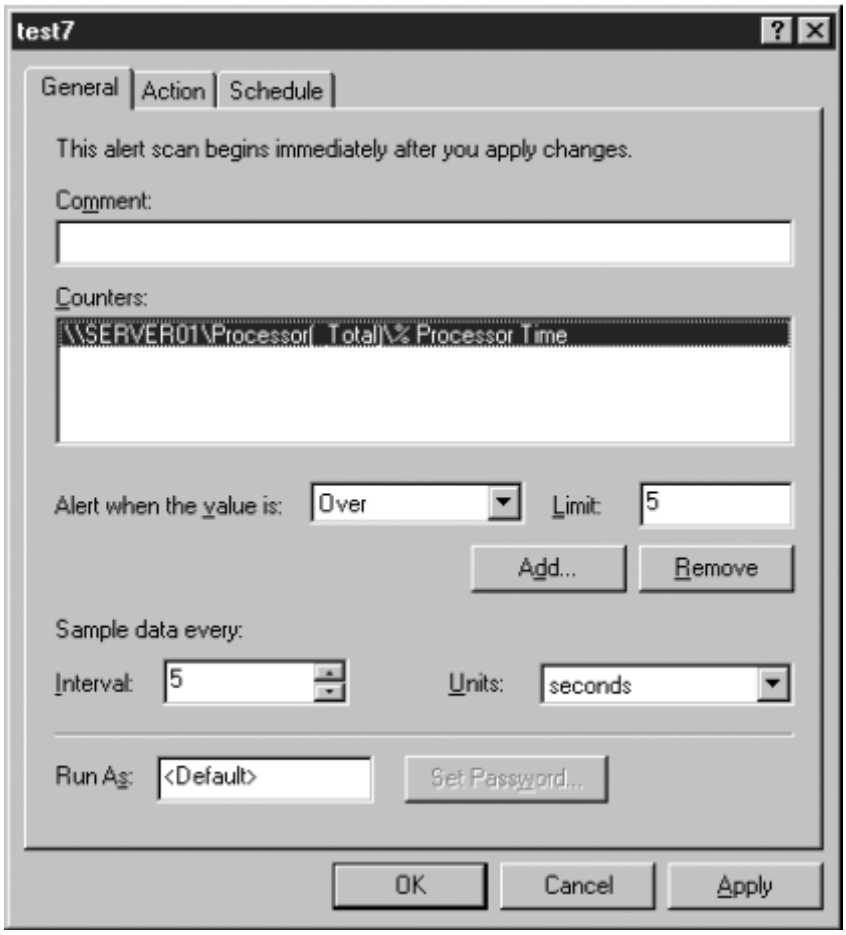
Khi bạn nhấn vào ***OK*** để đóng hộp thoại này lại, đồ thị dạng đường trong ***System Monitor*** hiển thị các dữ liệu đã được ghi trong nhật ký. Bạn có thể thực hiện thao tác cấu hình cách hiển thị trong đồ thị cũng giống như cách mà bạn làm khi màn hình hiển thị các hoạt động hiện tại trong hệ thống.

Tạo các Alerts (Cảnh báo)

Chức năng cảnh báo cho phép máy tính chạy Windows Server 2003 thông báo cho bạn khi mức hiệu năng hệ thống đạt đến giá trị ngưỡng xác định. Để tạo các cảnh báo, bạn lựa chọn đối tượng ***Alerts*** trong khung Phạm vi của snap-in ***Performance Logs and Alerts*** và lựa chọn ***New Alert Setting*** từ thực đơn ***Action*** để hiển thị hộp thoại (Thể hiện trong Hình 3-21) trong đó bạn sẽ nhập vào các thông tin sau đây:

- **Counters (biến đếm).** Các ***performance object*** và các ***performance counter*** mà bạn có thể lựa chọn để cảnh báo, và giao diện mà bạn sử dụng để lựa chọn chúng giống như trong ***System Monitor***
- **Giá trị giới hạn của biến đếm**. Đối với mỗi ***biến đếm*** bạn lựa chọn, bạn phải chỉ ra một giá trị giới hạn và liệu bạn muốn cảnh báo này sẽ được kích hoạt khi giá trị của ***biến đếm*** này thấp hơn hay cao hơn giới hạn.
- **Quãng ngắt lấy mẫu.** Thời gian lặp mà theo đó snap-in sẽ thu thập giá trị của ***biến đếm*** mà bạn lựa chọn
- **Các thông số đăng nhập Run as**. Tên người dùng và mật khẩu mà dịch vụ ***Performance Logs and Alerts*** sử dụng để đăng nhập vào hệ thống trước khi giám sát các biến đếm được lựa chọn.
- **Hành động (*Action*)**. Hành động mà bạn muốn snap-in thực hiện khi một trong các biến đếm lựa chọn của bạn đạt đến giá trị giới hạn. Snap-in có thể tạo ra một mục trong nhật ký sự kiện, gửi một thông báo qua mạng đến người dùng xác định nào đó, bắt đầu ghi các dữ liệu hiệu năng của ***biến đếm*** đó vào nhật ký hoặc chạy một chương trình hoặc dòng lệnh nào đó.

- **Các thông tin lập lịch**. Bạn có thể cấu hình snap-in khởi động và dừng khi giám sát các ***biến đếm*** đã lựa chọn tại các thời điểm ngày giờ cụ thể hoặc bạn có thể lựa chọn khởi động hoặc dừng tiến trình giám sát thủ công từ snap-in.



Hình 3-21: Hộp thoại cấu hình cảnh báo

TỔNG KẾT

- ***Event Viewer*** là một snap-in MMC hiển thị các nhật ký đượoc máy tính duy trì. Mọi máy tính Windows Server 2003 đều có các nhật ký Ứng dụng, Bảo mật và Hệ thống; máy chủ quản trị miền còn có thêm hai nhật ký cho Dịch vụ Thư mục và Dịch vụ đồng bộ File và máy chủ DNS còn có thêm nhật ký cho dịch vụ DNS Server.
- Mỗi mục vào của nhật ký sự kiện có thể chứa các thông tin, cảnh báo, thông báo lỗi hoặc kết quả kiểm định.
- **Task Manager** hiển thị các dữ liệu về hiệu năng theo thời gian thực của bộ vi xử lý, bộ nhớ máy tính, liệt kê các ứng dụng và tiến trình chạy trong máy tính, các thông tin về mạng và người dùng. Bạn có thể đồng thời sử dụng ***Task Manager*** để dừng một ứng dụng và tiến trình, thiết lập mức ưu tiên hoặc ngắt người dùng khỏi kết nối tới máy tính đang theo dõi.
- **Performance console** chứa hai snap-in: ***System Monitor*** và ***Performance Logs and Alerts***
- **System Monitor** hiển thị các dữ liệu về hiệu năng theo thời gian thực của các thành phần phần cứng và phần mềm trong hệ thống, sử dụng các cách xem kiểu Đồ thị, Biểu đồ và Báo cáo
- Để giám sát thông tin thống kê về một hệ thống nào đó bằng ***System Monitor***, bạn lựa chọn một ***performance object*** thể hiện một phần tử xác định, mỗi ***performance counter*** thể hiện một khía cạnh xác định của đối tượng đã lựa chọn, hoặc trong một số trường hợp là của một trường hợp riêng (***instance***) của đối tượng đã lựa chọn.
- **Performance Logs and Alerts** ghi các thông tin về hiệu năng của các ***biến đếm*** vào nhật ký và các sự kiện của hệ điều hành để theo dõi các nhật ký này theo các chu kỳ thời gian được lập lịch trước, cho phép bạn chụp được một số lớn các mẫu dữ liệu để kiểm tra sau này.
- **Performance Logs and Alerts** còn có thể giám sát các biến đếm xác định và thực hiện một hành động nào đó khi giá trị của các biến đếm này đạt đến một mức ngưỡng xác định.

BÀI TẬP THỰC HÀNH

Bài tập thực hành 3-1: Sử dụng Event Viewer

Trong bài tập thực hành này, bạn sử dụng bảng điều khiển ***Event Viewer*** để kiểm tra nhật ký Hệ thống của máy tính.

1. Đăng nhập vào máy tính với tài khoản ***Administrator***.
2. Nhấn ***Start***, trỏ vào ***Administrative Tools*** và nhấn vào ***Event Viewer***. Bảng điều khiển ***Event Viewer*** xuất hiện
3. Trong khung Phạm vi của bảng điều khiển, nhấn vào đối tượng ***System***. Một danh sách các mục nhật ký hệ thống hiện lên trong khung Chi tiết
4. Nhấn đúp vào một trong những mục trong khung Chi tiết để hiển thị hộp thoại ***Event Properties***

Bài tập thực hành 3-2: Sử dụng Task Manager

Trong bài tập thực hành này, bạn sử dụng ***Task Manager*** để khởi động một ứng dụng và nhận biết các tiến trình

1. Đăng nhập vào máy tính với tài khoản ***Administrator***
2. Nhấn phải chuột vào vùng trống trong thanh tác vụ và lựa chọn ***Task Manager*** từ thực đơn ngữ cảnh. Cửa sổ ***Windows Task Manager*** xuất hiện.
3. Trong thẻ ***Applications***, nhấn vào ***New task***. Nhập vào "***notepad***" và nhấn ***OK***. Một cửa sổ soạn thảo văn bản ***Untitled-Notepad*** hiện ra và một mục ***Untitled-Notepad*** xuất hiện trong thẻ ***Applications*** của ***Task Manager***
4. Trong thẻ ***Applications*** của ***Task Manager***, nhấn phải chuột vào mục ***Untitled-Notepad*** và lựa chọn ***Go to Process*** từ thực đơn ngữ cảnh. ***Task Manager*** chuyển sang thẻ ***Process*** với tiến trình ***Notepad*** được tô sáng.

Bài tập thực hành 3-3: Tạo một Bảng điều khiển System Monitor

Trong bài tập thực hành này, bạn sẽ tạo một bảng điều khiển ***System Monitor*** mới

1. Đăng nhập vào máy tính với tài khoản ***Administrator***

2. Nhấn ***Start***, trỏ vào ***Administrative Tools*** và nhấn vào ***Performance***. Bảng điều khiển ***Performance*** xuất hiện
3. Trong khung khung Chi tiết, nhấn vào phím ***Add*** trong thanh công cụ. Hộp thoại ***Add*** xuất hiện
4. Để đối tượng ***Processor*** được lựa chọn như mặc định, nhấn vào ***biến đếm % Idle Time*** và sau đó nhấn ***Add***. Sau đó thêm vào các ***biến đếm % Interrupt Time*** và ***Interrupts/Sec*** theo cách trên và nhấn ***Close***.
5. Từ thực đơn ***File***, lựa chọn ***Save as***. Hộp thoại ***Save as*** xuất hiện
6. Lưu bảng điều khiển lại với tên là ***procmon.msc***.

CÁC CÂU HỎI ÔN TẬP

1. Bạn không muốn dữ liệu trong nhật ký Bảo mật bị ghi đè, tuy nhiên bạn cũng không muốn máy tính của bạn ngừng giao tiếp với mạng bất kỳ lúc nào. Thiết lập nào mà bạn nên cấu hình trong máy chủ ?
2. Mục đích của bạn là giám sát tất cả các máy chủ của mình để chúng có thể được chống phân mảnh đều đặn theo lịch sắp xếp sao cho hiệu quả nhất. Chương trình chống phân mảnh đĩa mà bạn muốn sử dụng yêu cầu tối thiểu 20% dung lượng đĩa cứng trong mỗi đĩa để thực hiện tốt nhiệm vụ. Bạn nên làm gì ?
3. Máy tính mà bạn sử dụng để giám sát các hệ thống khác trong mạng đang quá tải với nhiệm vụ này, do đó bạn muốn giảm nhẹ mức tải cho nó. Bạn nên làm gì để giảm nhẹ mức tải của nhiệm vụ giám sát trong khi duy trì các dữ liệu giám sát ở mức tối đa có thể ?
4. Bạn đang chạy một ứng dụng CSDL trên máy tính với hai bộ vi xử lý. Bạn muốn ứng dụng CSDL này chạy trên bộ vi xử lý thứ hai. Làm thế nào để bạn có thể sử dụng ***Task Manager*** để thực hiện việc này?
5. Mệnh đề nào sau đây là đúng nếu ***System Monitor*** hiển thị giá trị của biến đếm ***PhysicalDisk:Current Disk Queue Length*** lớn hơn 2 trong một hệ thống đĩa không phải là RAID ?
    a. Bạn cần nhiều không gian đĩa cứng hơn
    b. Bạn cần đĩa cứng nhanh hơn
    c. Bạn cần thông tin thêm để xác định liệu đĩa có vấn đề gì không?
    d. Bạn gặp trục trặc với bộ nhớ, không phải với đĩa cứng .

6. Các nhật ký nào sau đây có thể sử dụng ***Event Viewer*** để xem trên một máy chủ thành viên có chức năng máy chủ ứng dụng (Chọn tất cả các câu trả lời đúng) ?
    a. Ứng dụng
    b. Dịch vụ thư mục
    c. Hệ thống
    d. Bảo mật
    e. Dịch vụ đồng bộ file
7. Tại sao một số các Biến đếm Hiệu năng trong ***System Monitor*** lại có nhiều trường hợp riêng (***instance***) khác nhau ?
8. Hai cách để chữa phân hệ đĩa lưu trữ bị nghẽn cổ chai trong phần hiệu năng máy chủ?

CÁC KỊCH BẢN TÌNH HUỐNG

Kịch bản 3-1: Phát hiện trường hợp nghẽn cổ chai

Bạn là quản trị mạng cho công ty công nghệ cao Fabrikam, Inc., công ty gần đây ký kết được một hợp đồng lợi nhuận cao với chính phủ. Kết quả của hợp đồng này là công ty sẽ phải trải qua quá trình mở rộng diễn ra trong 12 tháng tới. Số lượng người dùng truy cập vào CSDL máy khách của công ty dự kiến là gấp đôi và Giám đốc IT đã chỉ thị cho bạn xác định liệu máy chủ CSDL của công ty, với cấu hình hiện tại của nó, có thể đáp ứng được nhu cầu tăng mức tải theo dự tính không, và nếu không thì sẽ phải nâng cấp cái gì. Để hoàn thành nhiệm vụ này, hành động đầu tiên của bạn là triển khai một kế hoạch giám sát máy chủ để xem có nghẽn cổ chai hay không. Bước đầu tiên của kế hoạch này, bạn thiết lập một đường cơ sở bằng cách sử dụng snap-in ***Performance Logs and Alerts*** để tạo ra một ***nhật ký biến đếm*** theo dõi giá trị của các ***biến đếm*** quan trọng của các Đối tượng cần đo Hiệu năng như bộ vi xử lý, bộ nhớ, đĩa vật lý và giao tiếp mạng. Sau khi thiết lập các giá trị cho các ***biến đếm*** này trong quá trạng thái hoạt động thông thường, bạn phải làm gì tiếp theo để cấu hình ***Performance console*** để phát hiện ra sự nghẽn cổ chai ?

a. Để các ***nhật ký hiệu năng*** này chạy toàn thời gian và kiểm tra giá trị của các ***biến đếm*** này theo các khoảng thời gian lặp đều đặn.

b. Sử dụng ***System Monitor***, tạo ra đồ thị của cùng các ***biến đếm*** trên và cấu hình snap-in để tạo ra một cảnh báo bằng âm thanh khi bất kì giá trị của một ***biến đếm*** nào vượt quá mức ngưỡng tối đa.

c. Trong snap-in ***Performance Logs And Alerts***, tạo ra một loạt các cảnh báo gửi thông báo đến máy trạm của bạn khi bất kì giá trị của ***biến đếm*** nào vượt quá một mức xác định.

d. Trong snap-in ***Performance Logs And Alerts***, tạo ra một ***trace log*** sử dụng cùng các ***biến đếm*** như khi xác định đường cơ sở.

Kịch bản 3-2: Loại bỏ nghẽn cổ chai

Bạn là quản trị mạng dược giao nhiệm vụ xác định tại sao máy chủ file và in ấn chạy Windows Server 2003 trong một mạng LAN lại hoạt động kém. Bạn cũng đồng thời phải triển khai cách để giải quyết trường hợp này. Sau khi giám sát các Biến đếm Hiệu năng trong máy chủ bằng cách sử dụng ***Performance console***, bạn đã xác định được rằng hệ thống mạng gây nghẽn làm giảm hiệu suất hoạt động của máy chủ. Giải pháp nào sau đây sẽ cho phép bạn đạt được mục tiêu tăng cường mức hiệu năng của máy chủ file và in ấn này?

a) Cài đặt thêm một thiết bị giao tiếp mạng trong máy chủ này và kết nối nó với cùng mạng của giao tiếp còn lại.

b) Tăng tốc độ của mạng bằng cách thay thế các giao tiếp mạng 10Base-T trong các máy tính trên mạng và thiết bị hub mà các máy tính kết nối đến bằng các thiết bị có tốc độ 100Base-TX

c) Phân chia mạng thành 2 mạng LAN riêng biệt với số lượng máy tính ngang nhau trong mỗi mạng. Sau đó cài đặt một thiết bị giao tiếp mạng thứ hai trong máy chủ file và in ấn và kết nối máy chủ đến cả hai mạng LAN này

d) Thay thể các thiết bị giao tiếp mạng trong máy chủ file và in ấn này bằng một thiết bị có bộ nhớ đệm lớn hơn.

CHƯƠNG 4: SAO LƯU VÀ PHỤC HỒI DỮ LIỆU

Sự so sánh tương đồng thông dụng nhất được sử dụng để mô tả mối liên hệ giữa một đĩa trong ổ đĩa cứng (nơi lưu trữ dữ liệu) và đầu đọc của nó (để đọc và ghi dữ liệu lên đĩa) là hình ảnh một chiếc máy bay dân dụng 747 loại lớn bay với tốc độ 600 dặm một giờ trên độ cao 5 feet so với mặt đất. Khi bạn quan tâm đến điều này, bạn sẽ thật sự kinh ngạc khi đĩa cứng có khả năng làm việc tốt và lâu được như thế. Một ngày nào đó, bạn rất có thể bị mất một đĩa cứng chứa các dữ liệu rất quan trọng. Điều này có thể chưa xảy ra ngay ngày hôm này hoặc ngày mai, tuy nhiên cũng có thể nó sẽ đến vào một ngày nào đó. Các đĩa cứng này có thể bị lấy trộm cùng với máy tính, bị phá hủy bởi cháy nhà hoặc các thảm họa khác, hoặc đơn giản là nó bị hỏng. Và cho dù tại bất kì nguyên nhân gì, dữ liệu của bạn cũng sẽ bị mất và việc có lấy lại được dữ liệu hay không là tùy thuộc vào bạn. Ngày xảy ra chuyện đó là ngày bạn sẽ phải cảm ơn chính mình vì tất cả những nỗ lực của bạn khi thiết lập chiến lược sao lưu cho hệ thống. Nếu bạn không có một chiến lược sao lưu đúng đắn, rất có thể một ngày nào đó bạn phải bắt đầu công việc bằng cách viết sơ yếu lí lịch xin việc.

Thực hiện việc sao lưu đều đặn là một trong những chức năng cơ bản nhất của quản trị mạng và quản trị hệ thống. Không giống như hầu hết các thành phần khác trong máy tính, đĩa cứng có một bộ phận chuyển động với tốc độ cao, làm việc với một dung sai rất nhỏ. Và kết quả đĩa cứng hỏng là một điều khá thông thường, và bạn phải chuẩn bị cho điều đó bằng cách đều đặn sao lưu dữ liệu của mình trên các phương tiện lưu trữ khác.

Sau khi hoàn thành chương này, bạn có thể:

- Mô tả các kiểu phần cứng khác nhau sử dụng để sao lưu.
- Hiểu biết về khả năng của các phần mềm sao lưu mạng.
- Hiểu biết sự khác nhau giữa các tác vụ sao lưu ***full*** (Toàn bộ), sao lưu ***incremental*** (Tăng lên) và sao lưu ***differential*** (Sai khác).
- Liệt kê các khả năng của chương trình ***Microsoft Windows Server 2003 Backup***
- Sao lưu và khôi phục CSDL của ***Active Directory***
- Sử dụng ***volume shadow copies*** (Các bản sao của đĩa)

HIỂU BIẾT VỀ SAO LƯU

Nhiệm vụ sao lưu đơn giản là sao chép dữ liệu của bạn một cách đều đặn để nếu như thiết bị lưu trữ của bạn bị hư hỏng hoặc phá hủy và dữ liệu trên đó bị mất, bạn có thể khôi phục lại các dữ liệu này một cách kịp thời. Sao lưu là một tiêu chuẩn đánh giá khả năng chống lỗi cơ bản. Thậm chí nếu như bạn có các công nghệ lưu trữ khác cung cấp khả năng chống lỗi, ví dụ như hệ thống đĩa RAID hoặc cụm máy chủ cluster, bạn vẫn cần phải có một giải pháp sao lưu cho mình.

Hệ thống mạng làm cho tác vụ sao lưu đều đặn trở nên vừa phức tạp vừa đơn giản. Một chiến lược sao lưu cho một máy tính đơn bao gồm việc cài đặt một thiết bị sao lưu trong hệ thống. Quá trình sao lưu mạng sẽ phức tạp hơn bởi vì bạn có dữ liệu lưu trên nhiều máy tính cần bảo vệ và việc cài đặt một thiết bị sao lưu trên mỗi máy là không thực tế. Tuy vậy, quá trình sao lưu mạng lại đơn giản bởi thực tế bạn có thể sử dụng mạng để truy cập đến các máy chủ cần sao lưu, điều này cho phép bạn sử dụng một thiết bị sao lưu để bảo vệ rất nhiều máy tính.

Một chiến lược sao lưu sẽ phải chỉ ra dữ liệu nào cần sao lưu, sao lưu theo tần suất như thế nào và phương tiện lưu trữ nào mà bạn sử dụng để lưu các dữ liệu sao lưu. Quyết định của bạn tùy thuộc vào phần cứng và phần mềm sao lưu đồng thời các chính sách quản trị mà bạn sử dụng, tùy thuộc vào dung lượng dữ liệu mà bạn phải sao lưu, thời gian bạn sao lưu và mức bảo vệ mà bạn muốn áp dụng.

Một giải pháp sao lưu mạng bao gồm hai thành phần sau đây:

- Một hoặc nhiều thiết bị sao lưu
- Sản phẩm phần mềm sao lưu

Một kế hoạch sao lưu hiệu quả phải chỉ ra cách tận dụng các khả năng của hai thành phần trên để cung cấp mức độ bảo vệ mà doanh nghiệp cần. Tiêu chuẩn mà bạn nên sử dụng khi đánh giá các sản phẩm phần cứng và phần mềm sao lưu sẽ được bàn luận trong các phần sau.

> ***LƯU Ý. Mục đích của kỳ thi***. *Mục đích của kỳ thi 70-290 là học viên phải có khả năng "quản lý các tác vụ sao lưu"*

Phần cứng sao lưu

Bạn có thể sao lưu bằng bất kỳ loại thiết bị lưu trữ nào, mặc dù thông thường người ta hay dùng các thiết bị sử dụng các phương tiện lưu trữ có

khả năng tháo rời. Ba tiêu chí quan trọng nhất để đánh giá các thiết bị phần cứng sao lưu là:

- **Dung lượng**. Một trong những mục đích chính của việc phát triển một chiến lược sao lưu hiệu quả là để tự động hóa quá trình sao lưu càng nhiều càng tốt. Mặc dù bạn có thể sao lưu hàng gigabyte dữ liệu trên các đĩa mềm 1.44MB, tuy nhiên chắc bạn không muốn phải ngồi liên tục để nhét 712 chiếc đĩa mềm vào ổ đĩa. Do đó, bạn nên lựa chọn một thiết bị có khả năng lưu trữ dữ liệu nhiều nhất có thể mà không cần phải thay thế các phương tiện lưu trữ. Trường hợp lý tưởng nhất là một phương tiện lưu trữ và khi đó toàn bộ tác vụ sao lưu có thể lưu vừa đủ trong một cuộn băng từ đơn hoặc các phương tiện lưu trữ khác. Điều này cho phép bạn có thể lập lịch sao lưu và chạy hoàn toàn tự động mà không cần can thiệp. Tuy nhiên điều này không có nghĩa là bạn phải mua một thiết bị lưu trữ có thể chứa toàn bộ dữ liệu của tất cả các máy tính trong mạng của bạn. Bạn có thể lựa chọn cẩn thận dữ liệu nào mà bạn muốn sao lưu. Vì vậy cho nên việc xác định dung lượng dữ liệu cần bảo vệ và tần suất bao lâu là điều rất quan trọng trước khi bạn quyết định dung lượng của thiết bị lưu trữ.
- **Tốc độ**. Một trong những tiêu chí quan trọng khác khi bạn lựa chọn một thiết bị sao lưu là tốc độ mà thiết bị này có thể ghi dữ liệu lên các phương tiện lưu trữ. Các thiết bị lưu trữ có thể hoạt động với rất nhiều tốc độ khác nhau và thật không ngạc nhiên khi thiết bị nhanh nhất thông thường cũng sẽ đắt nhất. Một tác vụ sao lưu điển hình sẽ chạy khi hệ thống mạng đang không sử dụng, điều này để đảm bảo mọi dữ liệu trên mạng sẵn sàng cho nhiệm vụ sao lưu. Khoảng thời gian mà bạn sử dụng để sao lưu đôi khi được gọi là ***backup window*** (cửa sổ sao lưu). Thiết bị sao lưu mà bạn sử dụng nên phụ thuộc một phần vào dung lượng dữ liệu bạn muốn bảo vệ và khoảng thời gian mà bạn muốn sử dụng để sao lưu. Ví dụ nếu bạn có 10GB dữ liệu cần sao lưu và công ty của bạn sẽ đóng cửa từ 5 giờ chiều đến 9 giờ sáng hôm sau, như vậy bạn có một khoảng thời gian sao lưu (***backup window***) là 16 giờ - rất nhiều thời gian để sao chép dữ liệu sử dụng các thiết bị lưu trữ tốc độ trung bình. Tuy nhiên, nếu như công ty bạn hoạt động trong ba ca và cho bạn chỉ 1 giờ, từ 7 giờ đến 8 giờ, để sao lưu 100 GB dữ liệu, bạn phải sử dụng một thiết bị sao lưu nhanh hơn nhiều hoặc trong trường hợp này có thể là vài thiết bị.
- **Chi phí.** Chi phí luôn luôn là một nhân tố trong việc lựa chọn một sản phẩm phần cứng. Bạn có thể mua một thiết bị sao lưu loại thường với

giá khoảng 100$ đến 200$, thiết bị này phù hợp để sao lưu một máy tính gia đình vì tốc độ và dung lượng không phải là các nhân tố chính. Tuy nhiên, khi bạn chuyển sang các thiết bị có tốc độ và dung lượng phù hợp với nhiệm vụ sao lưu mạng, giá cả của chúng sẽ tăng đột ngột. Các thiết bị sao lưu cao cấp có thể có mức giá gồm 5 con số. Khi bạn định giá một thiết bị lưu trữ, bạn phải quan tâm đến các chi phí thêm vào của thiết bị. Các thiết bị sao lưu sử dụng các phương tiện lưu trữ có thể tháo dời, ví dụ như băng từ hoặc đầu quay đĩa. Các phương tiện lưu trữ này cho phép bạn có thể lưu các bản sao dữ liệu của bạn tại nơi khác (***offsite***), ví dụ như trong hầm an toàn có két sắt của một ngân hàng nào đó. Nếu tòa nhà mà hệ thống mạng của bạn đặt tại đó bị phá hủy bởi lửa hoặc thảm họa nào đó, bạn vẫn còn dữ liệu và bạn có thể khởi động lại hoạt động của hệ thống tại một nơi nào đó. Do đó, ngoài việc mua một thiết bị lưu trữ, bạn cũng phải mua thêm các phương tiện lưu trữ. Một số sản phẩm lúc đầu có vẻ là kinh tế bởi vì thiết bị là không đắt, tuy nhiên sau một thời gian dài chạy thì nó không còn như thế nữa bởi các phương tiện lưu trữ là quá đắt. Một trong những phương pháp thông thường để định giá các thiết bị sao lưu là xác định chi phí trên một MB (hoặc GB) trong khả năng lưu trữ của nó. Chia giá của các phương tiện lưu trữ cho số lượng MB (hoặc GB) nó có thể lưu trữ và sử dụng con số này để so sánh với chi phí của các thiết bị khác tương ứng. Đương nhiên, trong một số trường hợp, bạn có thể cần thiết phải hy sinh tính kinh tế để có được khả năng tốc độ hoặc dung lượng.

Một số thiết bị lưu trữ có khả năng tháo rời có thể sử dụng như là thiết bị sao lưu sẽ được xem xét trong các phần sau đây:

Các thiết bị CD-ROM và DVD-ROM.

Sự phổ biến của các thiết bị CD-ROM có khả năng ghi, ví dụ như các đĩa ***compact disc-recordable (CD-R)*** và ***compact disc-rewritable (CD-RW)***, đã tăng cường khả năng sử dụng chúng như các thiết bị lưu trữ. Mặc dù dung lượng của một đĩa CD bị giới hạn xấp xỉ khoảng 650MB nhưng với chi phí thấp của các đĩa lưu trữ, ta có thể xem việc sử dụng đĩa CD như là một giải pháp có tính kinh tế, thậm chí cả khi các đĩa này chỉ được sử dụng một lần như trong trường hợp các đĩa CD-R. Hiện tại giá cả của các đĩa DVD-ROM đã giảm, sử dụng DVD-ROM thích hợp hơn CD-ROM bởi vì khả năng lưu trữ của nó lớn hơn rất nhiều (trên 4GB). Yếu tố lớn nhất trong việc sử dụng rộng rãi CD-ROM hay DVD-ROM để sao lưu là rất nhiều máy tính đều đã

được trang bị các thiết bị ổ CD, DVD cho các mục đích khác, do đó giảm đi sự cần thiết phải mua thêm các thiết bị sao lưu chuyên dụng khác.

Đối với việc sao lưu mạng, CD-ROM không được sử dụng thường xuyên bởi hầu hết các hệ thống mạng đều có hàng gigabyte dữ liệu giá trị để sao lưu, khi đó sẽ yêu cầu rất nhiều việc thay đĩa. DVD-ROM giảm số lượng đĩa phải thay và có thể phù hợp với các hệ thống mạng nhỏ, tuy nhiên chúng vẫn không đủ dung lượng để sao lưu một cách hiệu quả trong các mạng của doanh nghiệp lớn. Hơn nữa, CD-ROM và DVD-ROM cũng thường không được các sản phẩm phần mềm sao lưu mạng hỗ trợ. Mặc dù các thiết bị này thường có gắn kèm các phần mềm có khả năng sao lưu hạn chế (thường áp dụng cho các nhiệm vụ sao lưu hệ thống đơn, qui mô nhỏ), các phần mềm này thường xuyên không cung cấp đủ các tính năng cần thiết để sao lưu một hệ thống mạng một cách hiệu quả.

Các ổ đĩa Cartrigde

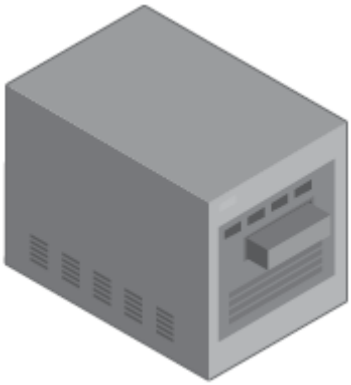
Một trong những thiết bị lưu trữ thông dụng khác có thể sử dụng dễ dàng cho việc sao lưu là các ổ đĩa Cartrigde (*ổ đĩa có bọc*) có khả năng tháo dời. Các sản phẩm như ***Iomega ZIP*** hay ***JAZ*** có thể được dùng như các đĩa cứng, tuy nhiên chúng lại sử dụng các Cartrigde có khả năng tháo dời. Các thiết bị này được gắn vào trong hệ thống file của máy tính và bạn có thể làm việc như với các đĩa cứng.

Các ***Cartrigde ZIP*** chứa không nhiều hơn 750MB, do đó chúng có ý nghĩa thực tế hơn không đáng kể so với CD. Tuy nhiên, các ổ ***JAZ*** có các phiên bản 1GB và 2GB, đủ cho nhiệm vụ sao lưu, thậm chí cho một hệ thống mạng nhỏ. Nhược điểm của việc sử dụng thiết bị này để sao lưu là chi phí cao của các phương tiện lưu trữ. Một ***Cartrigde*** 2GB cho ổ ***JAZ*** có thể có giá khoảng 125$ - như vậy là 6 cent trên một MB – đắt hơn rất nhiều so với hầu hết các thiết bị lưu trữ khác.

Các ổ đĩa băng từ

Thiết bị phần cứng được sử dụng thông dụng nhất cho nhiệm vụ sao lưu dữ liệu là các băng từ, trông giống như thiết bị trong hình 4-1. Không giống như ổ đĩa cứng, ổ đĩa mềm và ổ đĩa CD-ROM, băng từ không phải là thiết bị truy cập ngẫu nhiên. Điều này có nghĩa là thiết bị không thể di chuyển đầu đọc của nó để đọc bất kì file cá biệt nào đó trên băng từ mà không phải cuộn qua tất cả các file nằm trước nó. Cũng giống như các loại thiết bị băng từ khác, ví dụ như audio và video, thiết bị này tháo băng từ ra khỏi ống trục và kéo nó qua đầu đọc đến khi tìm được điểm trên băng từ chứa dữ liệu mà nó cần. Kết quả là bạn không thể gắn một ổ băng từ vào hệ thống file của một máy

tính, cấp cho nó một kí tự ổ đĩa và sao chép file vào đó như bạn làm với các đĩa cứng được. Một chương trình phần mềm được yêu cầu để đánh địa chỉ cho ổ băng này, gửi dữ liệu bạn lựa chọn đến nó để lưu trữ và khôi phục dữ liệu sau này. Điều này có nghĩa là các ổ băng từ rất ít sử dụng cho các nhiệm vụ khác ngoài sao lưu, trong khi các loại thiết bị lưu trữ có thể tháo dời khác, ví dụ như đĩa CD-ROM, có thể sử dụng cho các chức năng khác.



Hình 4-1: Một ổ băng từ lưu trữ ngoài

Các ổ đĩa băng từ là rất phù hợp cho nhiệm vụ sao lưu. Chúng khá nhanh, có thể chứa một lượng lớn dữ liệu, có thể lưu trữ lâu dài không giới hạn thời gian, và các phương tiện lưu trữ của nó có giá trên một MB là thấp – thông thường thấp hơn 1,5 cent trên một MB. Có rất nhiều dạng thiết bị băng từ, chúng khác nhau về tốc độ, dung lượng và giá cả. Nguyên tắc chung cho các thiết bị băng từ là bạn trả chi phí khá lớn khi cần nhiều tốc độ và dung lượng. Các sản phẩm loại cấp thấp như các ổ băng từ ¼ inch (QIC), giá của chúng vào khoảng 200$. Có rất nhiều định dạng QIC khác nhau, với dung lượng của một cuộn băng từ QIC trong khoảng từ 150MB đến 20GB. Các sản phẩm cao cấp trên thị trường là các thiết bị băng từ số tuyến tính (***digital linear tape*** - DLT) và băng từ tuyến tính chuẩn mở (***linear tape-open*** - LTO) với giá trị có thể lên đến vài ngàn USD và có thể chứa hàng trăm GB trên một băng từ đơn. Các công nghệ băng từ thông thường được sử dụng để sao lưu được liệt kê trong Bảng 4-1.

Bảng 4-1. Các kiểu thiết bị băng từ

Type	Tape Width	Cartridge Size	Capacity (uncompressed)	Speed
QIC, Travan	.25 inch	4 × 6 × 0.625 inches (data cartridge); 3.25 × 2.5 × 0.6 inches (minicartridge)	50 GB	600 MB/min
DAT	4 mm	2.875 × 2.0625 × 0.375 inches	20 GB	360 MB/min
8 mm	8 mm	3.7 × 2.44 × 0.59 inches	100 GB	1400 MB/min
DLT, Super DLT	.50 inch	4.16 × 4.15 × 1 inches	160 GB	960 MB/min
LTO, Ultrium	.50 inch	4.0 × 4.16 × 0.87 inches	200 GB	Up to 3600 MB/min

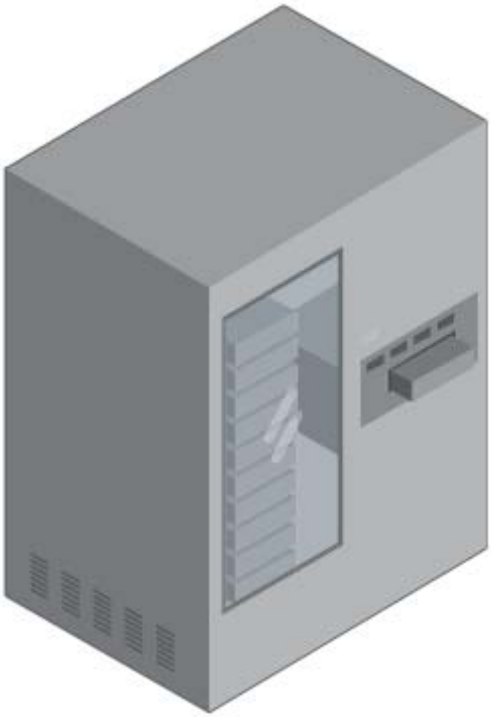
***LƯU Ý: Nén băng từ**. Dung lượng của các thiết bị băng từ thông thường được phân chia thành 2 loại, ví dụ như 40GB và 80GB. Các con số này thể hiện dung lượng của một băng từ chưa nén và đã nén. Hầu hết các thiết bị băng từ đều có khả năng nén dữ liệu bằng phần cứng được trang bị sẵn, nhưng dung lượng trống mà bạn có thể có thêm khi nén thì dựa vào kiểu của dữ liệu được lưu trữ. Dung lượng thông thường mà nhà sản xuất thiết bị sử dụng được giả định dựa trên tỷ lệ nén 2:1, đây là tỉ lệ nén điển hình áp dụng với các kiểu file chạy và các dạng file ứng dụng khác. Một số loại file khác, ví dụ như file hình ảnh mà sử dụng các định dạng chưa nén như BMP hay TIF, có thể được nén với tỷ lệ cao hơn như 8:1. tuy nhiên các file hình ảnh đã được nén như file GIF hay JPG sẽ không thể nén thêm được nữa và được lưu trữ với tỷ lệ nén là 1:1.*

Các Autochanger

Trong một số trường hợp, thậm chí các thiết bị băng từ có dung lượng cao nhất cũng không đủ để sao lưu một hệ thống mạng với các dữ liệu liên tục thay đổi. Một hệ thống mạng có thể phải làm việc với một lượng dữ liệu rất lớn để sao lưu hoặc thời gian sao lưu (***backup window***) rất nhỏ. Để tạo ra một giải pháp sao lưu tự động với dung lượng lớn hơn khả năng cung cấp của một băng từ đơn, bạn có thể mua một thiết bị được gọi là ***autochanger*** (*Thiết bị có khả năng nạp tự động*).

Một ***autochanger*** (Thể hiện trong Hình 4-2) là một thiết bị phần cứng có chứa một hoặc nhiều ổ đĩa (thông thường là các ổ băng từ, tuy nhiên cũng có các thiết bị ***autochanger*** sử dụng đĩa quang và CD-ROM), một dãy các đĩa

lưu trữ và một kết cấu robot máy có thể tráo đổi các đĩa lưu trữ vào và ra khỏi ổ đĩa. Đôi khi các thiết bị này còn được gọi là ***jukeboxe*** hoặc ***tape library***. Khi các tác vụ sao lưu ghi đầy dữ liệu vào một băng từ (hoặc các phương tiện lưu trữ khác), kết cấu robot này sẽ rút đĩa từ này ra khỏi ổ và nhét một đĩa khác vào, sau đó tác vụ sao lưu sẽ tiếp tục. Thiết bị ***autochanger*** này đồng thời duy trì một bộ nhớ ghi lại đĩa nào còn chưa sử dụng, thông thường được gọi là một danh mục, và do đó nó có thể tự động nạp các băng từ tương ứng cần để tiếp tục nhiệm vụ.



Hình 4-2. Một thiết bị *autochanger* sử dụng băng từ

Một số ***autochanger*** là các thiết bị nhỏ với một ổ ghi đơn và một dãy bốn hoặc năm băng từ, trong khi đó rất nhiều thiết bị có bốn hoặc năm ổ ghi và một dãy gồm một trăm băng từ hoặc nhiều hơn. Nếu bạn mua một ***autochanger*** đủ lớn, bạn có thể tạo ra một chiến lược sao lưu lâu dài, cho phép nhiệm vụ sao lưu của bạn luôn hoạt động một cách tự động hoàn toàn vào một thời gian nhất định hàng tuần. Tuy nhiên, trước khi bạn có thể xem xét và củng cố kế hoạch của mình một lần nữa để quyết định mua một thiết bị ***autochanger*** có kích thước như cái tủ lạnh để không bao giờ phải nạp một băng từ bằng tay, bạn hãy nên biết rằng chi phí để mua các thiết bị này là rất lớn, lớn một cách đáng kinh ngạc và trong một số trường hợp có thể đạt đến một con số có sáu chữ số.

Lựa chọn giao tiếp cho thiết bị

Các thiết bị sao lưu có thể sử dụng bất kì một giao tiếp máy tính chuẩn nào, ví dụ như Thiết bị Điện tử Tích hợp (***Integrated Device Electronics*** - IDE), Đường Nối tiếp Đa năng (***Uuniversal Serial Bus*** - USB), và Giao tiếp Hệ thống Máy tính Nhỏ (***Small Computer System Interface*** - SCSI), cộng với giao tiếp mới nhất theo xu thế chủ yếu hiện nay, IEEE 1394 (***FireWire***). Một số thiết bị sao lưu thậm chí còn có thể kết nối đến máy tính thông qua cổng song song mặc dù đây chỉ là một dạng của giao tiếp SCSI sử dụng các cổng khác. Giao tiếp thông dụng nhất được sử dụng hiện nay trong các giải pháp sao lưu mạng cao cấp là SCSI.

Các thiết bị SCSI hoạt động độc lập hơn các thiết bị sử dụng IDE, điều này có nghĩa là các chu trình sao lưu, thường phải đọc từ một thiết bị và ghi vào một thiết bị khác trên cùng một giao diện, sẽ hoạt động hiệu quả hơn. Khi hai thiết bị IDE chia sẻ một kênh thì chỉ một thiết bị có thể hoạt động. Mỗi thiết bị phải nhận, thực thi, và hoàn thành một lệnh trước khi thiết bị kia có thể nhận lệnh tiếp theo. Mặt khác, các thiết bị SCSI có thể duy trì một hàng đợi các lệnh mà chúng nhận được từ các thiết bị giao tiếp máy tính và thực thi chúng một cách tuần tự và độc lập.

Các ổ băng từ thông thường yêu cầu một dòng dữ liệu liên tục để ghi vào các băng từ với hiệu suất cao nhất. Nếu có sự ngắt quãng liên tiếp trong dòng dữ liệu này, điều hay xảy ra với các giao tiếp IDE, thiết bị băng từ phải lặp đi lặp lại việc khởi động và dừng ổ băng từ (còn gọi là ***shoeshining***), điều này làm giảm tốc độ và khả năng lưu trữ tổng thể của nó. Một thiết bị SCSI có thể thường xuyên hoạt động liên tục mà không cần phải tạm dừng để đợi các thiết bị khác trên kênh truyền.

Một thiết bị sao lưu SCSI thông thường đắt hơn khi so sánh với các thiết bị IDE tương ứng bởi vì các ổ đĩa yêu cầu nhiều linh kiện điện tử hơn và cũng bởi vì bạn phải có một bộ giao tiếp SCSI được cài đặt trong máy tính. Hầu hết các thiết bị SCSI đều có các sản phẩm loại cắm trong hoặc nằm ngoài máy tính. Thiết bị nằm ngoài có các bộ cấp nguồn riêng của nó và chi tiết này sẽ tốn thêm chi phí. Tuy nhiên, các chi phí thêm cho các thiết bị SCSI sẽ đáng giá cho các giải pháp sao lưu mạng nhanh và đáng tin cậy.

Phần mềm sao lưu

Bên cạnh phần cứng, một thành phần chính trong một giải pháp sao lưu mạng là phần mềm mà bạn sử dụng để thực hiện nhiệm vụ sao lưu. Các thiết bị lưu trữ được thiết kế cho các giải pháp sao lưu chuyên dụng sẽ không giống như các phân hệ lưu trữ khác trong máy tính; một sản phẩm phần

mềm đặc biệt được yêu cầu để lấy dữ liệu mà bạn cần sao lưu và gửi chúng đến ổ đĩa. Windows Server 2003 có kèm theo một chương trình phần mềm sao lưu cung cấp chức năng cơ bản cho các nhiệm vụ sao lưu hệ thống đơn, nhưng cũng giống như hầu hết các chương trình sao lưu đi kèm hệ điều hành, phần mềm này thiếu các tính năng tiên tiến cần thiết để sao lưu hiệu quả trong một môi trường mạng phức tạp.

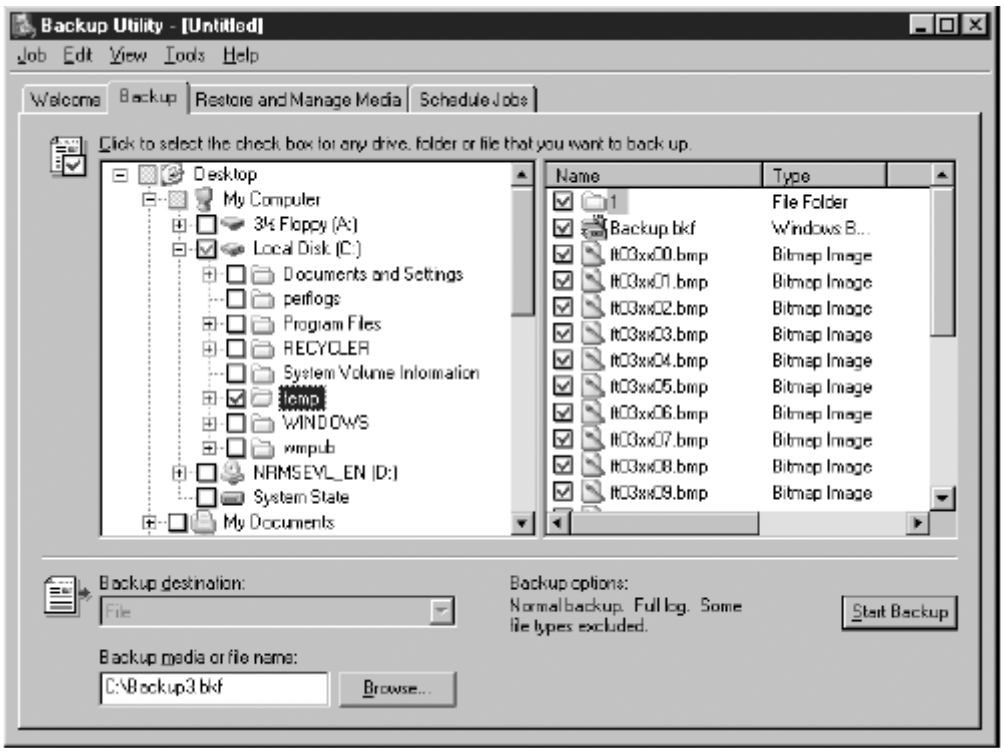
Chức năng chính của một phần mềm sao lưu tốt sẽ được xem xét trong các phần sau đây.

Khả năng lựa chọn mục tiêu.

Chức năng cơ bản nhất của một chương trình phần mềm sao lưu là cho phép bạn lựa chọn cái gì bạn muốn sao lưu, đôi khi còn được gọi là mục tiêu (***Target***). Một chương trình sao lưu tốt cho phép bạn làm việc này theo rất nhiều cách. Trong hầu hết các trường hợp, bạn có thể lựa chọn

- Toàn bộ máy tính
- Các đĩa cứng xác định trong một máy tính
- Các thư mục xác định trong một đĩa cứng
- Các file xác định trong một thư mục

Sử dụng lựa chọn trong cây. Hầu hết các chương trình sao lưu đều cung cấp một cách hiển thị hình cây mà bạn có thể sử dụng để lựa chọn mục tiêu cho tác vụ sao lưu. Hình 4-3 thể hiện giao diện mà chương trình ***Backup*** của Windows Server 2003 sử dụng để lựa chọn mục tiêu sao lưu.



Hình 4-3. Thẻ *Backup* trong chương trình *Windows Server 2003 Backup*

Trong hầu hết các trường hợp, bạn không cần thiết phải sao lưu mọi dữ liệu trong các ổ đĩa của máy tính. Nếu một đĩa cứng bị xóa hoặc phá hủy hoàn toàn, bạn có thể phải cài đặt lại hệ điều hành trước khi bạn khôi phục các file từ một băng từ sao lưu và do đó việc sao lưu mọi file của hệ điều hành mỗi khi bạn chạy một tác vụ sao lưu là không có giá trị nhiều. Tương tự đối với các ứng dụng, bạn có thể cài đặt lại một ứng dụng từ bộ cài gốc, do đó bạn có thể chỉ cần sao lưu các file dữ liệu và các thiết lập cấu hình của ứng dụng đó. Hơn nữa, hầu hết các hệ điều hành hiện nay đều tạo ra các file tạm khi chạy, những file này bạn cũng không cần thiết phải sao lưu. Ví dụ Windows tạo ra file phân trang bộ nhớ có thể có kích cỡ hàng trăm hoặc hàng ngàn MB. Bởi vì các file này được tạo ra tự động, bạn có thể tiết kiệm dung lượng trong các băng từ sao lưu của bạn bằng cách bỏ qua file này và các file tương tự trong các tác vụ sao lưu. Sự lựa chọn đúng đắn các mục tiêu để sao lưu có ý nghĩa trong trường hợp hoặc bạn có thể lưu vừa đủ toàn bộ dữ liệu cần sao lưu vào trong một băng từ hoặc có thể bạn phải ở lại muộn sau giờ làm việc để nhét băng từ thứ hai vào trong ổ đĩa.

Sử dụng các Filter (Bộ lọc). Việc lựa chọn các file, thư mục và ổ cứng riêng rẽ mà bạn muốn sao lưu có thể khá nhàm chán trong một mạng lớn, do đó rất nhiều các chương trình sao lưu cung cấp một cách khác để lựa chọn mục tiêu. Một trong những phương pháp thông dụng là sử dụng bộ lọc, cho phép

phần mềm đánh giá từng file và thư mục trên một đĩa cứng và sau đó quyết định liệu có sao lưu không. Các chương trình phần mềm sao lưu điển hình có hỗ trợ bộ lọc thường cho phép bạn sử dụng các bộ lọc bao hàm và bộ lọc loại trừ; có nghĩa là một bộ lọc có thể nhận biết các file bạn muốn sao lưu hoặc các file bạn muốn loại bỏ ra khỏi quá trình sao lưu.

Một chương trình sao lưu tốt cung cấp rất nhiều bộ lọc cho phép bạn lựa chon mục tiêu dựa trên các thông số sau đây:

Tên file và thư mục. Việc chọn từng file và thư mục bằng bộ lọc là không dễ hơn cách hiển thị bằng cây thư mục, tuy nhiên khả năng sử dụng các kí tự đại diện trong tên file và thư mục là một tính năng rất mạnh. Bạn có thể sử dụng các dấu hỏi (?) để đại diện cho các kí tự đơn hoặc dấu hoa thị (*) để đại diện cho nhiều ký tự. Ví dụ tạo ra một bộ lọc loại trừ sử dụng đại diện file *.tmp sẽ loại bỏ các file có phần mở rộng là .tmp (thông thường được sử dụng cho các file tạm) trong tác vụ sao lưu.

Kích thước file. Bộ lọc dựa trên kích thước file cho phép bạn loại trừ các file có độ lớn zero ra khỏi tác vụ sao lưu hoặc loại trừ các file rất lớn, ví dụ như file phân trang bộ nhớ ***Pagefile.sys***

Ngày giờ của file. Một hệ thống file sẽ duy trì tối thiểu một thông số ngày và giờ cho mỗi file lưu trữ, điển hình là các thông tin khi file đó được chỉnh sửa gần đây nhất. Một số hệ thống file, ví dụ như hệ thống file Windows NTFS, bao gồm rất nhiều thông tin ngày giờ cho mỗi file, ví dụ như thời điểm file được tạo ra, thời điểm file được truy cập lần cuối cùng, và thời điểm file được chỉnh sửa lần cuối. Bộ lọc dựa trên các thông số thời gian này cho phép bạn sao lưu chỉ các file đã thay đổi từ một thời điểm nhất định hoặc chỉ các file cũ hơn một ngày xác định nào đó.

Thuộc tính của file. Thuộc tính là các cờ giá trị 1-bit được gắn kèm theo các file cho biết các đặc tính của chúng. Hầu hết các hệ thống file hỗ trợ bốn thuộc tính DOS chuẩn, đó là H – Thuộc tính ẩn, R - thuộc tính Chỉ đọc, S - thuộc tính Hệ thống và A – thuộc tính Lưu trữ, tuy nhiên một số hệ thống file còn có các thuộc tính khác nữa. Phần lớn các chương trình sao lưu đều dựa chủ yếu vào các bộ lọc thuộc tính để làm nhiệm vụ sao lưu, điều này cho phép chúng sao lưu chỉ các file thay đổi từ lần sao lưu gần nhất trước đó. Kiểu bộ lọc này là kiểu cơ bản sử dụng cho các tác vụ sao lưu ***incremental*** (*Tăng lên*) và ***differential*** (*vi sai*).

> ***LƯU Ý: Bộ lọc trong Windows Server 2003 Backup***. *Chương trình sao lưu Windows Server 2003 Backup cho phép bạn tạo ra các bộ lọc tùy chọn theo tên file và thư mục để loại bỏ các file cá biệt ra khỏi tác vụ sao lưu. Tuy nhiên, chương trình này không hỗ trợ các*

bộ lọc bao hàm hoặc các bộ lọc kích thước, ngày/giờ và thuộc tính ngoài các bộ lọc sẵn có trong các tác vụ sao lưu chuẩn.

Hiểu biết về các kiểu tác vụ sao lưu. Hầu hết, tuy nhiên không phải là tất cả, các phần mềm sao lưu đều bao gồm một loạt các kiểu tác vụ sao lưu chuẩn mà thực chất là việc kết hợp các bộ lọc cấu hình trước. Ví dụ chương trình Windows Server 2003 Backup cho phép bạn lựa chọn từ năm kiểu tác vụ sau (Thể hiện trong Hình 4-4):

- **Normal** (Thông thường). Sao lưu tất cả các file vào phương tiện lưu trữ và đặt lại bit lưu trữ trong mỗi file để chỉ định rằng các file này đã được sao lưu.
- **Copy** (Sao chép). Sao lưu tất cả các file vào phương tiện lưu trữ và không đặt lại bit lưu trữ của các file này.
- **Differential** (Vi sai). Chỉ sao lưu các file đã thay đổi từ lần sao lưu ***Normal*** gần đây nhất và không đặt lại bit lưu trữ của chúng.
- **Incremental** (tăng lên). Chi sao lưu các file đã thay đổi từ các lần sao luu ***Normal*** hoặc ***Incremental*** gần đây nhất và đặt lại bit lưu trữ của các file
- **Daily** (Hàng ngày). Chỉ sao lưu các file mà được tạo ra hoặc chỉnh sửa ngày hôm nay và không đặt lại bit lưu trữ trong các file đó.

Hình 4-4: Thẻ *Backup Type* trong hộp thoại *Option* của chương trình *Windows Server 2003 Backup*

Kiểu cơ bản nhất của tác vụ sao lưu là sao lưu đầy đủ toàn bộ (còn gọi là sao lưu ***normal*** trong ***Windows Server 2003 Backup***), kiểu này sẽ sao chép toàn bộ các mục tiêu lựa chọn vào băng từ hay các phương tiện sao lưu khác. Bạn có thể thực hiện việc sao lưu đầy đủ hàng ngày, nếu bạn muốn, hoặc chỉ làm thế mỗi khi bạn tiến hành sao lưu một máy tính cụ thể nào đó. Tuy nhiên, việc làm như thế có thể không thực tế do các lý do sau:

- **Có quá nhiều dữ liệu để sao lưu.** Các đĩa cứng điển hình trong các máy tính ngày nay chứa nhiều dữ liệu hơn bao giờ hết và trong một mạng lớn, tổng dung lượng lưu trữ có thể dễ dàng đạt tới hàng ngàn GB. Trừ khi bạn muốn tiêu rất nhiều tiền vào các băng từ lưu trữ và phần cứng ***autochanger***, còn lại nếu bạn sao lưu toàn bộ dữ liệu trong mỗi máy tính hàng ngày là không khả thi chút nào.
- **Không có đủ thời gian để tiến hành sao lưu**. Hầu hết các quản trị mạng đều lập lịch sao lưu mạng để việc này được tiến hành vào buổi đêm hoặc khi hết giờ làm việc. Sao lưu trong thời gian không làm việc sẽ cho phép chương trình sao lưu không phải bỏ qua các file đang

trong trạng thái mở và nó cũng tối thiểu hóa các tác động đến lưu lượng mạng gây ra bởi các quá trình sao lưu từ xa. Đối với một số doanh nghiệp, thời gian để tiến hành sao lưu là không đủ để sao lưu toàn bộ hệ thống mạng trừ khi sử dụng rất nhiều thiết bị sao lưu tốc độ cao.

- **Có quá nhiều dữ liệu dư thừa.** Hầu hết các dữ liệu lưu trong một ổ cứng của máy tính điển hình là dữ liệu tĩnh; nó không thay đổi hàng ngày. Các file ứng dụng và file hệ điều hành không bao giờ thay đổi, và một số file tài liệu văn bản có thể tồn tại lâu dài mà không có người dùng nào thay đổi nó cả. Sao lưu các file như vậy hàng ngày có nghĩa là lưu các dữ liệu giống nhau vào băng từ mãi mãi và mãi mãi, rất tốn thời gian và phương tiện lưu trữ.

  LỜI KHUYÊN. Lưu trữ trên máy chủ. *Mức độ dễ dàng của sao lưu là một trong những lý do mà nhiều quản trị mạng yêu cầu người dùng lưu các file dữ liệu của họ trên máy chủ hơn là trên các đĩa cứng của máy trạm nội bộ. Bằng cách cấp cho mỗi người dùng một* ***home directory*** *(thư mục gốc riêng) trên một máy chủ, ta có khả năng sao lưu các file dữ liệu của người dùng bằng việc sao lưu một máy chủ đơn thay cho việc phải cấu hình phần mềm sao lưu kết nối đến mỗi máy trạm hàng ngày.*

Để lưu băng từ và làm ngắn thời gian sao lưu, rất nhiều quản trị hệ thống tiến hành sao lưu đầy đủ một lần trong một tuần hoặc thậm chí ít hơn. Giữa các lần sao lưu đầy đủ đó, họ tiến hành các kiểu sao lưu đặc biệt khác mà chỉ sao lưu các file được chỉnh sửa gần đây. Kiểu tác vụ sao lưu này được gọi là ***incremental backup*** và ***differential backup*** (*Sao lưu phần thay đổi và sao lưu vi sai*). ***Incremental backup*** là tác vụ sao lưu mà chỉ sao lưu các file đã thay đổi từ bất kì lần sao lưu nào trước đó. ***Differential backup*** là tác vụ sao lưu mà chỉ sao lưu các file đã thay đổi từ lần sao lưu đầy đủ trước đó. Phần mềm sao lưu sẽ lọc các file cho các tác vụ này bằng cách sử dụng thuộc tính Lưu trữ, còn được gọi là ***archive bit*** (*bit lưu trữ*), mà mỗi file trong máy tính đều có.

Thực tế bit lưu trữ không chỉnh sửa các chức năng của file giống như các thuộc tính Chỉ đọc và Ẩn, nó chỉ đơn giản là một bit đánh dấu để phần mềm sao lưu sử dụng để xác định liệu có sao lưu file này không. Trạng thái của các bit lưu này trong các tác vụ sao lưu điển hình như sau:

1. Khi một file được ghi vào trong đĩa cứng máy tính lần đầu tiên, bit lưu của nó được kích hoạt, giá trị của nó được thiết lập là 1.

2. Trong lần sao lưu đầy đủ đầu tiên bạn tiến hành trên máy tính, phần mềm sao lưu sẽ sao lưu toàn bộ nội dung của đĩa cứng và đồng thời đặt lại (nghĩa là đưa giá trị này về 0) bit lưu trữ của tất cả các file. Tại thời điểm này, bạn có một bản sao lưu đầy đủ của đĩa cứng trên băng từ và không một file nào trên đĩa cứng có bit lưu trữ được kích hoạt.
3. Khi bất kì một file trên đĩa cứng được chỉnh sửa bởi bất kì ứng dụng hoặc tiến trình nào, hệ thống file sẽ tái kích hoạt bit lưu trữ của file đó
4. Trong lần sao lưu tiếp theo, bạn tiến hành một tác vụ sao lưu kiểu ***incremental*** hoặc ***differential.*** Phần mềm sao lưu sẽ quét tất cả các bit lưu trữ của các file trên đĩa cứng và chỉ sao lưu các file có bit lưu trữ đang được kích hoạt. Tại thời điểm này, bạn có một bản sao lưu đầy đủ của toàn bộ đĩa cứng và một bản sao lưu của tất cả các file đã thay đổi từ lần sao lưu đầy đủ trước. Nếu sự cố hoặc thảm họa xảy ra dẫn đến toàn bộ nội dung của đĩa cứng bị mất, bạn có thể khôi phục về trạng thái hiện tại bằng cách tiến hành khôi phục từ băng từ sao lưu đầy đủ trước, sau đó khôi phục từ băng từ incremental hay differential, cho phép phiên bản đã thay đổi của các file ghi đè lên phiên bản gốc.

Bởi vì các các bản sao lưu ***incremental*** hay ***differential*** chỉ chứa một phần của nội dung đĩa nên chúng sẽ chạy nhanh hơn và tốn ít băng từ hơn là sao lưu đầy đủ. Một chiến lược sao lưu mạng điển hình bao gồm một lần sao lưu đầy đủ vào một ngày trong tuần và các tác vụ sao lưu ***incremental*** hoặc ***differential*** trong các ngày còn lại. Với cách bố trí này, bạn luôn luôn có thể khôi phục được đĩa cứng về trạng thái gốc mà không mất quá 24 giờ.

Khác nhau giữa một tác vụ sao lưu ***incremental*** và ***differential*** nằm ở cách xử lý của phần mềm sao lưu khi nó đặt lại hoặc không đặt lại bit lưu trữ của các file mà nó sao chép vào băng từ. Tác vụ sao lưu ***incremental*** sẽ đặt lại bit lưu trữ còn ***differential*** thì không. Việc chạy các tác vụ sao lưu ***incremental*** hay ***differential*** thường xuyên cho phép tự động hóa chế độ sao lưu của bạn mà không tốn nhiều phần cứng. Ví dụ bản sao lưu đầy đủ của bạn tổng số là 50GB, bạn có thể mua một thiết bị ổ đĩa 20GB. Bạn sẽ phải tự tay nhét hai băng từ thêm vào trong quá trình sao lưu đầy đủ, một tuần một lần, tuy nhiên bạn có thể chạy các tác vụ sao lưu ***incremental*** hay ***differential*** trong các ngày còn lại trong tuần sử dụng chỉ một tape cho mỗi lần, điều này có nghĩa là tác vụ này có thể chạy tự động mà không cần phải giám sát.

Sử dụng sao lưu Incremental. Điều này có nghĩa là khi bạn chạy một tác vụ sao lưu Incremental, bạn chỉ sao lưu các file đã thay đổi từ lần sao lưu

trước gần nhất, lần đó có thể là sao lưu đầy đủ hoặc sao lưu ***incremental***. Thực hiện sao lưu ***Incremental*** giữa các lần sao lưu đầy đủ sẽ sử dụng ít băng từ nhất, tuy nhiên điều này cũng kéo dài thời gian khôi phục. Nếu bạn phải khôi phục lại toàn bộ máy tính, đầu tiên bạn phải khôi phục từ băng từ sao lưu đầy đủ trước, sau đó bạn phải tiếp tục khôi phục theo thứ tự các lần sao lưu ***Incremental*** sau lần khôi phục đầy đủ.

Ví dụ, bạn có thể xem xét lịch sao lưu thể hiện trong Bảng 4-2:

Bảng 4-2: Lịch sao lưu mẫu theo kiểu Incremental

Day	Job Type	Files Included in Job
Sunday	Full	Data1.txt, Data2.txt, Data3.txt
Monday	Incremental	Data1.txt
Tuesday	Incremental	Data1.txt, Data3.txt
Wednesday	Incremental	Data1.txt, Data2.txt
Thursday	Incremental	Data1.txt, Data3.txt
Friday	Incremental	Data1.txt
Saturday	Incremental	Data1.txt

Bản sao lưu ngày Chủ nhật là bản sao đầy đủ duy nhất của đĩa cứng máy tính và mỗi bản sao lưu ***Incremental*** chứa các file đã thay đổi trong 24 giờ trước. Bởi vì Data1.txt thay đổi hàng ngày, nó xuất hiện trong mọi bản sao lưu incremental. Bit lưu của file này được kích hoạt mỗi lần nó thay đổi và mỗi lần sao lưu ***incremental*** sẽ đặt lại bit này lần nữa. Data2.txt thay đổi chỉ một lần vào thứ Tư nên nó chỉ xuất hiện trong bản sao lưu đầy đủ và bản sao lưu ***incremental*** của ngày thứ Tư. Data3.txt thay đổi hai lần vào ngày thứ Ba và thứ Năm, do đó nó xuất hiện trong bản sao lưu đầy đủ và bản sao lưu ***incremental*** của ngày thứ ba và thứ năm.

Nếu các đĩa cứng trong máy tính bị trục trặc trong ngày thứ Sáu, hậu quả là mọi dữ liệu đều bị mất hết, bạn có thể bắt đầu quá trình khôi phục bằng cách khôi phục bản sao lưu đầy đủ của ngày Chủ nhật gần nhất, sau đó bạn sẽ phải khôi phục các bản sao lưu ***incremental*** của ngày thứ Hai, thứ Ba, thứ Tư và thứ Năm theo đúng thứ tự sau bản sao lưu đầy đủ đó. Kết quả của quá trình khôi phục là ba file dữ liệu sẽ như sau:

- **Data1.txt**. Bản sao chép gốc từ lần sao lưu đầy đủ sẽ bị ghi đè bởi bản sao chép mới hơn trong các lần khôi phục ***incremental,*** để lại phiên bản mới nhất (của thứ Năm) trên đĩa cứng sau khi quá trình khôi phục chấm dứt.
- **Data2.txt**. Bản sao chép gốc từ lần sao lưu đầy đủ ngày Chủ nhật sẽ được duy trì trên đĩa cứng đến khi khôi phục bản sao lưu ***incremental***

của ngày thứ Tư, đến lúc đó phiên bản mới nhất (ngày thứ Tư) sẽ ghi đè phiên bản của ngày Chủ nhật. Phiên bản của ngày thứ Tư sẽ còn lại trên đĩa cứng sau khi quá trình khôi phục chấm dứt.

- **Data3.txt**. Bản sao chép gốc từ lần sao lưu đầy đủ ngày Chủ nhật sẽ bị ghi đè hai lần, lần đầu bởi phiên bản của lần sao lưu ***incremental*** ngày thứ Ba và sau đó là bởi phiên bản của lần sao lưu incremental ngày thứ Năm, để lại phiên bản mới nhất (của thứ Năm) trên đĩa cứng sau khi quá trình khôi phục chấm dứt.

  LƯU Ý: Khôi phục Incremental*. Khi bạn khôi phục từ các bản sao lưu* ***Incremental****, thư tự của các băng từ bạn khôi phục là rất quan trọng. Bạn phải khôi phục các phiên bản* ***Incremental*** *theo thứ tự đúng nhu khi nó được ghi vào, nếu không bạn có thể kết thúc với phiên bản cũ của file ghi đè lên phiên bản mới nhất.*

Sử dụng sao lưu Differential. Nếu bạn tiến hành các bước sao lưu giống như trên nhưng thay các tác vụ ***incremental*** bằng ***differential***, kết quả sẽ được như trong Bảng 4-3.

Bảng 4-3. Lịch sao lưu mẫu theo kiểu Differential

Day	Job Type	Files Included in Job
Sunday	Full	Data1.txt, Data2.txt, Data3.txt
Monday	Differential	Data1.txt
Tuesday	Differential	Data1.txt, Data3.txt
Wednesday	Differential	Data1.txt, Data2.txt, Data3.txt
Thursday	Differential	Data1.txt, Data2.txt, Data3.txt
Friday	Differential	Data1.txt, Data2.txt, Data3.txt
Saturday	Differential	Data1.txt, Data2.txt, Data3.txt

Bởi vì các file Data1.txt thay đổi hàng ngày, nó sẽ xuất hiện trong tất cả bản sao lưu ***differential***, cũng như khi nó xuất hiện trong các lần ***incremental***. Tuy nhiên, bởi vì các tác vụ ***differential*** không đặt lại bit lưu trữ trong các file nó sao lưu, nên khi một file đã xuất hiện trong một lần ***differential***, nó sẽ xuất hiện trong mọi lần tiếp theo cho đến lần sao lưu đầy đủ kế tiếp. Do đó, file Data2.txt lần đầu tiên xuất hiện trong bản ***incremental*** ngày thứ Tư sẽ đồng thời được sao lưu trong các ngày thứ Năm, thứ Sáu và thứ Bảy bởi vì bit lưu trữ của nó vẫn còn được kích hoạt. Cũng giống như thế, file Data3.txt mà xuất hiện lần đầu tiên trong bản ***differential*** ngày thứ Ba cũng sẽ xuất hiện trong tất cả các bản sao lưu ***differential*** tiếp theo trừ bản ***Differential*** vào ngày thứ Năm, đây là phiên bản mới hơn bản đã được sao lưu hàng đêm

trước đó. Các bit lưu trữ của ba file này không được đặt lại cho đến lần sao lưu đầy đủ tiếp theo, diễn ra vào ngày Chủ nhật kế tiếp.

Khi bạn sử dụng các sao lưu ***differential***, tác vụ này diễn ra lâu hơn và sử dụng nhiều băng từ hơn một chút bởi vì trong một số trường hợp, bạn phải sao lưu các file giống nhau trong vài ngày liên tiếp. Tuy nhiên, khôi phục từ các lần sao lưu ***differential*** sẽ đơn giản hơn và nhanh hơn bởi vì bởi vì bạn chỉ phải khôi phục bản sao lưu đầy đủ và bản sao lưu ***differential*** gần nhất. Nếu ổ đĩa trong ví dụ này bị sự cố trong ngày thứ Bảy, bạn chỉ phải khôi phục bản sao lưu đầy đủ của ngày Chủ nhật trước và bản sao lưu ***differential*** của ngày hôm trước (Thứ Sáu). Băng từ của ngày thứ Sáu sẽ chứa các file Data1.txt, Data2.txt và Data3.txt trong nó. Phiên bản của Data1.txt sẽ là của ngày thứ Sáu, Data2.txt sẽ là phiên bản của ngày thứ Tư và Data3.txt sẽ là phiên bản của ngày thứ Năm.

Sử dụng các tác vụ Copy và Daily. Các chương trình phần mềm sao lưu cho phép bạn tiến hành các kiểu sao lưu Norman, ***incremental*** và ***differential***, tuy nhiên ứng dụng Windows Server 2003 Backup còn bao gồm thêm hai tính năng mà không nhất thiết sẽ có trên các sản phẩm phần mềm khác. Một tác vụ sao lưu Daily (Hàng ngày) sử dụng một bộ lọc dựa trên ngày thay cho dựa trên các bit lưu để chỉ sao lưu các file được tạo ra hoặc thay đổi trong ngày mà tác vụ sao lưu này chạy. Một tác vụ sao lưu kiểu ***Copy*** (Sao chép) giống như một tác vụ sao lưu đầy đủ ngoại trừ việc phần mềm sao lưu này không chỉnh sửa giá trị của bit lưu trữ trong các file mà nó sao chép ra băng từ. Bạn có thể sử dụng kiểu sao lưu ***Copy*** để tiến hành các bản sao lưu đầy đủ vào bất kì thời điểm nào, ví dụ như cho các thiết bị lưu trữ ngoài hệ thống, mà không ảnh hưởng đến trình tự đều đặn thường xuyên của các tác vụ sao lưu đầy đủ và ***incremental*** hoặc ***differential***.

> ***LƯU Ý. Các tên của tác vụ sao lưu.*** *Chỉ có chương trình Windows Server 2003 Backup sử dụng tên của tác vụ sao lưu đầy đủ là* ***Normal*** *và không có gì lạ nếu các chương trình phần mềm sao lưu khác sử dụng các tên khác nhau khi đề cập đến các kiểu sao lưu cơ bản.*

Lập lịch cho các tác vụ

Mọi sản phẩm sao lưu đều cho phép bạn tạo ra các tác vụ sao lưu và thực hiện chúng ngay lập tức, nhưng chìa khóa cho việc tự động hóa các chu trình sao lưu là khả năng lập lịch các tác vụ sao lưu để thực hiện mà không cần giám sát. Không phải tất cả các chương trình sao lưu trang bị cùng hệ điều hành hoặc thiết kế cho các máy tính đơn đều hỗ trợ khả năng lập lịch, nhưng mọi sản phẩm phần mềm sao lưu mạng đều có.

> ***LƯU Ý. Mục đích của kỳ thi***. *Mục đích của kỳ thi 70-290 là học viên có khả năng "lập lịch cho các tác vụ sao lưu"*

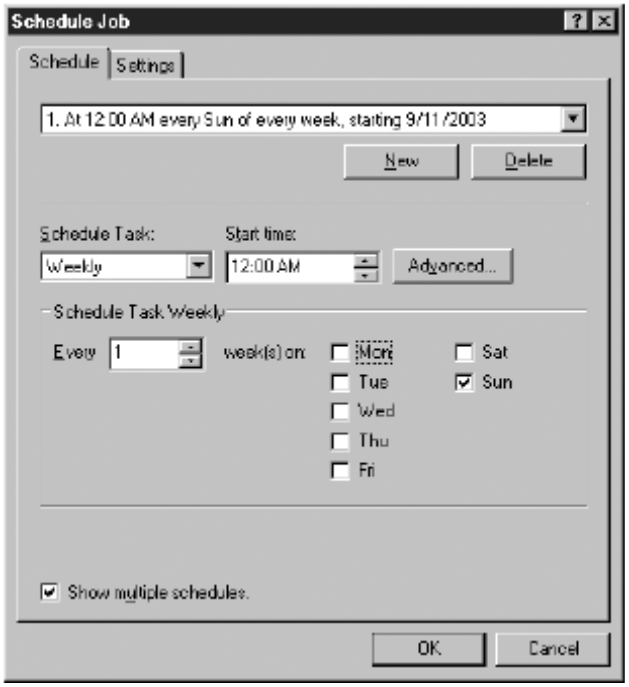
Hầu hết các doanh nghiệp đều tiến hành các tác vụ sao lưu ***incremental*** hoặc ***differential*** hàng ngày và một lần sao lưu đầy đủ một lần trong tuần. Cách bố trí này cung cấp một sự cân bằng tốt giữa khả năng bảo vệ với thời gian và phương tiện lưu trữ dành cho nhiệm vụ sao lưu là rất hợp lý. Trường hợp lý tưởng cho một quản trị mạng là dữ liệu của mỗi lần sao lưu ***incremental*** hay ***differential*** hàng ngày sẽ chứa vừa đủ trong một băng từ đơn. Điều này cho phép người quản trị có thể lập lịch cho các tác vụ này để có thể chạy không cần giám sát khi văn phòng đã đóng cửa và hệ thống mạng đang rỗi rãi. Kết quả là mọi tài nguyên đều sẵn sàng cho nhiệm vụ sao lưu và hiệu suất làm việc của người dùng không bị giảm bởi sự nghẽn mạng do các lưu lượng dữ liệu trong quá trình sao lưu, đồng thời không cần phải có người thay thế các phương tiện lưu trữ. Khi bạn đã có một lịch sao lưu, bạn chỉ cần đơn giản nhét đúng các băng từ vào các ổ đĩa mỗi ngày. Các lần sao lưu đầy đủ có thể yêu cầu nhiều hơn một băng từ và do vậy ai đó phải có mặt để thay thế các phương tiện lưu trữ.

> ***LỜI KHUYÊN. Lựa chọn phần cứng sao lưu***. *Khả năng tạo ra các lịch sao lưu tự động không cần giám sát là nhân tố quan trọng nhất để xem xét khi bạn đánh giá các sản phẩm phần cứng sao lưu. Trước khi lựa chọn một ổ đĩa, bạn nên ước lượng dung lượng dữ liệu mà bạn sẽ phải sao lưu mỗi ngày (có tính đến cả phần dữ liệu tăng trưởng) và xem xét các ổ đĩa có thể lưu trữ tối thiểu là lượng dữ liệu trên trong một băng từ đơn.*

Các chương trình sao lưu sử dụng rất nhiều phương pháp để thi hành các tác vụ tự động. Chương trình ***Windows Server 2003 Backup*** thêm các tác vụ này vào trong danh sách ***Scheduled Tasks*** của hệ điều hành; các chương trình khác thường cung cấp chương trình hoặc dịch vụ riêng của chúng mà liên tục chạy và kích hoạt các tác vụ tại các thời điểm tương ứng. Một số sản phẩm sao lưu mạng cao cấp có thể sử dụng dịch vụ thư mục ví dụ như ***Microsoft's Active Directory*** hay ***Novell's eDirectory*** để lập lịch. Các chương trình này chỉnh sửa ***schema*** (lược đồ) của thư mục (mã cho biết kiểu đối tượng nào có thể tồn tại trong thư mục) để tạo ra các đối tượng thể hiện hàng đợi của tác vụ chờ để được xử lý.

,Chu trình lập lịch của các phần mềm sao lưu là giống nhau, không phụ thuộc vào kĩ thuật nào mà chúng sử dụng để nạp các tác vụ. Bạn có thể chỉ ra liệu bạn có muốn thực hiện tác vụ một lần hay lặp lại tại các thời điểm xác định mỗi ngày, tuần hoặc tháng, sử dụng một giao diện giống như chương

trình ***Windows Server 2003 Backup*** (Thể hiện trong Hình 4-5). Một ý tưởng của tính năng lập lịch là để cho người quản trị mạng tạo ra sự tuần tự logic của các tác vụ sao lưu mà tự thực hiện bởi chính chúng sau các khoảng thời gian lặp đều đặn. Sau khi người quản trị mạng làm điều đó, hành động duy nhất yêu cầu là thay đổi các băng từ mỗi ngày. Nếu bạn có một thiết bị ***autochanger***, bạn thậm chí còn có thể loại bỏ thao tác này và tạo ra một tác vụ sao lưu tuần tự chạy hàng tuần hoặc hàng tháng mà không cần phải giám sát một chút nào.



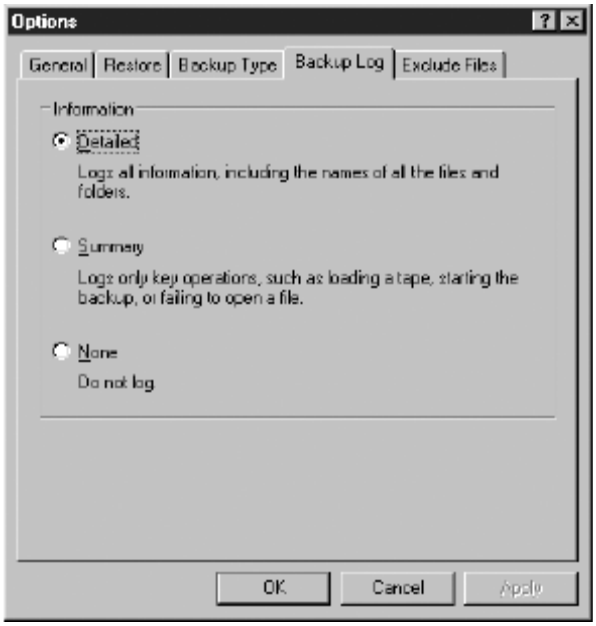
Hình 4-5. Hộp thoại *Schedule Job* của chương trình *Windows Server 2003 Backup*

Duy trì các nhật ký sao lưu (Backup Logs).

Khi một tác vụ sao lưu chạy, phần mềm truy cập vào mục tiêu xác định và lưu dữ liệu vào trong ổ đĩa sao lưu theo các cách thích hợp. Do chức năng vốn có của các phương tiện lưu trữ thường được sử dụng cho sao lưu, nên việc dữ liệu đi đến thiết bị lưu trữ một cách ổn định và với một tốc độ thích hợp là điều rất quan trọng. Phần mềm, vì vậy, phải được thiết kế để xác định các ổ đĩa theo các phương thức thích hợp đối với các thiết bị này.

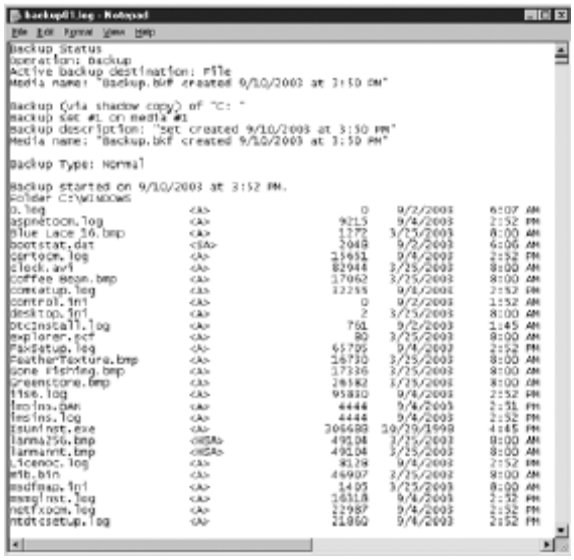
Khi phần mềm đưa dữ liệu vào trong ổ băng, nó cũng đồng thời theo dõi các hoạt động của phần mềm. Hầu hết các sản phẩm phần mềm có thể duy trì một nhật ký các chu trình sao lưu khi nó diễn ra. Bạn có thể thường xuyên chỉ định mức độ chi tiết của nhật ký, ví dụ như liệu nó có chứa một danh sách hoàn chỉnh của mọi file được sao lưu hay chỉ ghi lại các sự kiện chính

diễn ra trong quá trình sao lưu. Chương trình ***Backup*** trong Windows Server 2003 sử dụng một giao diện như trong Hình 4-6 để xác định liệu chương trình sẽ giữ một nhật ký ***Detail*** (Chi tiết), một bản ***Summary*** (Tổng kết) hay ***None*** (Không lưu nhật ký nào cả).



Hình 4-6. Thẻ Backup Log trong hộp thoại *Options* của chương trình *Windows Server 2003 Backup*.

Trong hầu hết các trường hợp, một nhật ký chi tiết của tác vụ sao lưu là không cần thiết. Kiểu nhật ký này thường chứa một danh sách các file mà chương trình thực hiện sao lưu (Thể hiện trong Hình 4-7) và do tác vụ sao lưu thường chứa hàng ngàn file nên một nhật ký chi tiết có thể rất dài và các mục cần chú ý (ví dụ như lỗi) lại rất khó để tìm kiếm. Việc xem kích thước của các file nhật ký cũng là rất quan trọng, nhất là khi bạn cấu hình để duy trì mức độ rất chi tiết. Các file này có thể tăng dung lượng rất nhanh và có thể sử dụng hết dung lượng trống trên đĩa cứng nơi chúng được lưu trữ.



Hình 4-7. Một bản nhật ký sao lưu của chương trình *Windows Server 2003 Backup*

Việc kiểm tra định kỳ các nhật ký là một phần thiết yếu của việc quản trị chương trình sao lưu mạng. Các nhật ký cho bạn biết khi nào các file cụ thể nào bị bỏ qua do lý do bất kì nào đó, ví dụ như khi file đó đang được mở bởi ứng dụng hoặc không thể tìm thấy máy tính mà chúng được lưu trên đó. Nhật ký cũng cho bạn biết khi nào lỗi xảy ra trên các đĩa sao lưu hoặc trên một trong các máy tính nằm trong chu trình sao lưu. Một số sản phẩm phần mềm sao lưu còn có thể tạo ra các cảnh báo khi lỗi xảy ra, thông báo cho bạn bằng cách gửi đi các thông điệp trạng thái tới một bảng điều khiển quản trị mạng, bằng cách gửi cho bạn một thông điệp email hoặc bằng các phương pháp khác.

> ***LƯU Ý. Mục đích của kỳ thi**. Mục đích của kỳ thi là học viên phải có khả năng "xác nhận sự hoàn thành của các tác vụ sao lưu"*

Cataloging (Lập mục lục)

Bên cạnh nhiệm vụ ghi nhật ký các hoạt động của mình, các chương trình phần mềm sao lưu còn lập mục lục cho các file chúng sao lưu để làm cho quá trình khôi phục sau này được dễ dàng hơn. Một mục lục bản chất là một danh sách các file mà phần mềm sao lưu lại trong các tác vụ sao lưu. Để khôi phục các file từ các phương tiện sao lưu, bạn duyệt qua mục lục và lựa chọn các file, thư mục hay ổ đĩa mà bạn muốn khôi phục. Các sản phẩm phần mềm sao lưu khác nhau sẽ lưu thư mục theo các cách khác nhau. Các chương trình cấp thấp, ví dụ như các phần mềm sao lưu cho các máy tính đơn, thường lưu mục lục cho mỗi băng từ trong chính các băng từ này. Vấn

đề với phương pháp này là bạn phải đưa một băng từ vào trong ổ băng thì mới đọc được mục lục và duyệt các file trên băng từ đó.

Các chương trình sao lưu mạng công phu hơn có các phương thức tiếp cận khác nhau bằng các duy trì một CSDL của các mục lục cho mọi băng từ sao lưu trong máy tính, nơi mà phần mềm sao lưu này được cài đặt. CSDL này cho phép bạn duyệt qua các mục lục của tất cả các băng từ và bạn có thể lựa chọn khôi phục bất kỳ phiên bản nào của file hoặc thư mục. Trong một số trường hợp, bạn có thể xem nội dung của các CSDL này theo các cách khác nhau, ví dụ như theo máy tính, ổ đĩa hay thư mục nơi lưu trữ gốc của các file này, theo các tác vụ sao lưu hoặc theo các băng từ hay các tên khác của phương tiện lưu trữ. Sau khi bạn lựa chọn, chương trình sẽ định vị băng từ nào chứa các file hay thư mục bạn cần; bạn đưa nó vào trong ổ băng và quá trình khôi phục sẽ được tiến hành.

Các tính năng của CSDL có thể sử dụng rất nhiều không gian đĩa trên máy tính và nhịp xử lý của bộ vi xử lý, tuy nhiên chúng lại tăng cường rất nhiều khả năng cho phần mềm, đặc biệt là trong môi trường mạng.

> ***LƯU Ý. CSDL sao lưu***. *Các sản phẩm phần mềm sao lưu dựa trên CSDL thường lưu một bản sao của CSDL trên các băng từ đồng thời trên các đĩa cứng máy tính. Với tính năng này, nếu máy tính dùng chạy các tác vụ sao lưu của bạn bị hỏng ổ đĩa cứng thì bạn vẫn có thể khôi phục các được CSDL này. Rất nhiều sản phẩm đồng thời cho phép bạn xây dựng lại CSDL trên máy tính bằng cách đọc nội dung của băng từ và chuyển các chỉ mục của nó sang một file CSDL mới.*

Quay vòng sử dụng các phương tiện sao lưu.

Một số quản trị mạng khó tính sử dụng các băng từ mới cho các tác vụ sao lưu và lưu chúng lâu dài. Tuy nhiên, cách làm này khá tốn kém. Việc sử dụng lại các băng từ sao lưu là thông dụng hơn. Để làm tốt điều này, bạn phải định ra chính sách quay vòng các phương tiện sao lưu một cách cẩn thận để không vô tình ghi đè một băng từ nào đó sau này. Bạn có thể tự tạo chính sách riêng của mình, tuy nhiên một số phần mềm sao lưu sẽ làm việc này cho bạn.

> ***LƯU Ý. Mục đích của kỳ thi.*** *Mục đích của kỳ thi 70-290 chỉ ra rằng học viên phải có khả năng "quản lý các phương tiện sao lưu"*

Một trong những chính sách quay vòng phương tiện sao lưu thông dụng nhất được gọi là phương pháp ***Grandfather-Father-Son*** (Ông-Bố-Con). Trong phương pháp này, các khái niệm Ông, Bố và Con tham chiếu tướng ứng đến

các băng từ hàng tháng, hàng tuần và hàng ngày. Với các tác vụ sao lưu hàng ngày, bạn có một tập các băng từ mức "con" được sử dụng lại hàng tuần. Đối với các tác vụ sao lưu hàng tuần, bạn có các băng từ mức "cha" được sử dụng lại hàng tháng. Sau đó, vào mỗi tháng, bạn tiến hành thêm một lần sao lưu đầy đủ vào tập các băng từ mức "Ông", các băng từ này được sử dụng lại hàng năm. Phương thức này cho phép bạn tiến hành khôi phục một cách hoàn chỉnh tại bất kỳ thời điểm nào và duy trì danh mục các file trong một năm của bạn. Ngoài ra còn có các chính sách sao lưu khác có thể thay đổi mức độ phức tạp và sự tiện dụng, tùy vào sản phẩm phần mềm sao lưu.

Khi chương trình phần mềm thực thi chính sách quay vòng, nó cung cấp một lịch trình cho các tác vụ (mà bạn có thể chỉnh sửa để các tác vụ đó được thực hiện tại các thời gian xác định trong ngày), cho bạn biết tên cần ghi trên mỗi băng từ để sử dụng nó và khi bạn bắt đầu sử dụng lại các băng từ này, nó sẽ cho bạn biết băng từ nào cần cho vào ổ băng cho mỗi tác vụ. Kết quả cuối cùng là bạn duy trì một bản ghi lâu dài các dữ liệu của bạn trong khi lại sử dụng tối thiểu số lượng băng từ mà không sợ ghi đè lên bất cứ một băng từ nào bạn cần.

Cấu hình thiết bị

Bởi vì các ổ sao lưu chuyên dụng chỉ có thể truy cập được thông qua việc sử dụng các chương trình đặc biệt nên hầu hết các chương trình sao lưu đều có các giao diện cho phép bạn tương tác trực tiếp với các ổ băng để thực hiện các tác vụ sau:

- **Định dạng băng từ**. Mọi băng từ đều phải được định dạng trước khi phần mềm sao lưu có thể ghi dữ liệu vào. Phần lớn các phần mềm sao lưu đều tự động định dạng băng từ mới khi bắt đầu tác vụ sao lưu, tuy nhiên chúng ta vẫn có thể định dạng một cách thủ công. Các dạng khác nhau của các cuộn băng từ yêu cầu các kiểu định dạng khác nhau. Một số định dạng còn yêu cầu toàn bộ băng từ phải được ghi đè lại trong khi một số loại chỉ yêu cầu ghi một ***header*** (đề mục) mới tại phần đầu của băng từ. Việc định dạng sẽ ghi đè tất cả các dữ liệu hiện đang có trên băng từ.
- **Xóa băng từ**. Xóa một băng từ thỉnh thoảng chỉ đơn giản là tái định dạng lại bởi vì quá trình tái định dạng sẽ ghi đè lại toàn bộ chiều dài của cuộn băng. Đối với một số loại băng từ khác, tái định dạng chỉ là thay thế ***header*** và phần còn lại của băng từ là không thay đổi. Phần lớn các sản phẩm phần mềm sao lưu mạng đều cho phép bạn xóa dữ liệu từ bất kỳ băng từ nào bằng cách ghi đè lên toàn bộ chiều dài của cuộn băng do mục đích bảo mật. Điều này không có nghĩa là toàn bộ

dữ liệu không thể tái tạo lại bằng các phương pháp khác, trừ bản thân phần mềm sao lưu không thể đọc được các dữ liệu đã bị xóa khỏi băng từ.

- **Duy trì băng từ**. Một số dạng băng từ có thể cait thiện được tình trạng của nó nhờ việc Duy trì Băng từ,, trong đó ổ băng sẽ quay băng từ từ đầu đến cuối cuộn băng và lại quay ngược trở lại để đảm bảo rằng toàn bộ chiều dài của băng từ được quấn vào trong ống cuộn với độ căng đều đặn. Sản phẩm phần mềm có khả năng này thường chỉ làm như trên đối với một số loại băng từ cần thiết thực hiện động tác này.
- **Ổ đĩa nén**. Hầu hết các nhà sản xuất ổ băng từ hiện nay đều tích hợp khả năng nén dữ liệu vào trong sản phẩm phần cứng của mình và các chương trình phần mềm sao lưu cũng thường cung cấp khả năng lựa chọn tắt hoặc bật chức năng nén của phần cứng ổ đĩa. Một số chương trình còn cung cấp khả năng tự nén dựa vào phần mềm để sử dụng với các thiết bị không có khả năng nén bằng phần cứng. Tuy nhiên, khả năng sử dụng của nén bằng phần cứng luôn được ưa thích hơn nén bằng phần mềm bởi vì việc nén bằng phần mềm sẽ tiêu tốn một lượng tài nguyên của bộ vi xử lý máy tính.

Thực hiện phục hồi.

Khôi phục dữ liệu từ các bản sao lưu, tất nhiên, là lý do duy nhất để tạo nên các bản sao lưu như trong phần trước. Cảm giác thanh thản của bạn khi xem và duyệt các file để khôi phục là một trong những tính năng quan trọng của bất kì phần mềm sao lưu nào. Điều cốt yếu là bạn nên tiến hành thử nghiệm một cách định kỳ khả năng khôi phục dữ liệu từ các băng từ đã sao lưu hoặc các phương tiện lưu trữ khác để đảm bảo bạn có khả năng lấy lại mọi dữ liệu bị mất. Thậm chí khi các tác vụ sao lưu của bạn dường như thành công hoàn toàn và các file nhật ký chỉ ra rằng mọi dữ liệu đều đã được sao lưu, không có bài kiểm tra khả năng của các tác vụ sao lưu nào tin cậy bằng việc khôi phục thực tế từ chính các bản sao lưu đó. Có rất nhiều câu chuyện ly kỳ về những người quản trị mạng, thực hiện sao lưu hàng ngày, nhưng chỉ đến khi có một sự cố xảy ra mới biết được rằng các băng từ dán nhãn cẩn thận kia đều trống rỗng do một ổ đĩa hoạt động không được tốt.

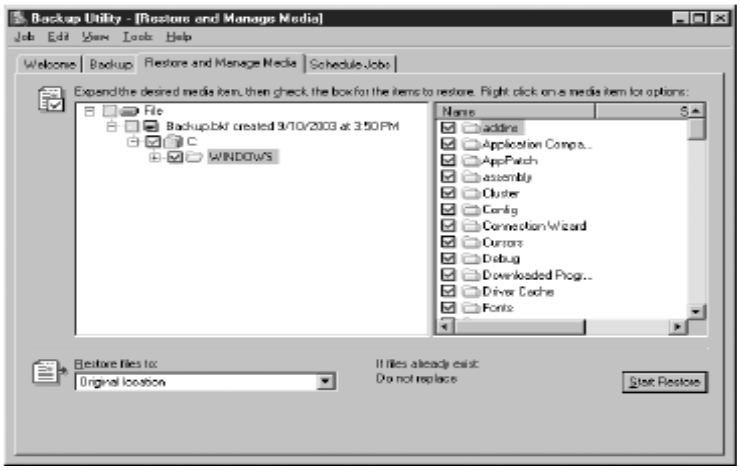
> ***LƯU Ý. Mục đích của kỳ thi****. Mục đích của kỳ thi chỉ ra rằng học viên phải có khả năng "khôi phục các dữ liệu đã sao lưu".*

Mặc dù tiến hành sao lưu đều đặn là một biện pháp dự phòng bảo vệ dữ liệu khỏi thảm cảnh mất toàn bộ ổ cứng nhưng phần lớn các tác vụ khôi phục

tiến hành trong môi trường mạng lại thường chỉ vì một số file mà người dùng đã vô tính xóa đi mất. Như đã đề cập ở trên, khả năng tạo mục lục của các phần mềm sao lưu là một phần quan trọng của quá trình khôi phục. Nếu người dùng cần khôi phục một số file và bạn phải nhét hết băng từ đến băng từ kia vào trong ổ đĩa để định vị ra các file đó thì thời gian của mọi người đang bị lãng phí. Một chương trình sao lưu với một CSDL sẽ cho phép bạn tìm kiếm các file đặc biệt đó, làm cho nhiệm vụ của bạn dễ dàng hơn đồng thời cho phép bạn có thể khôi phục bất kỳ file nào trong vài phút.

Nhiệm vụ khôi phục cũng tương tự như nhiệm vụ sao lưu trong đó bạn lựa chọn file hoặc thư mục nào mà bạn muốn khôi phục, sử dụng một giao diện trông giống như trong Hình 4-8. Khi bạn tạo ra một bản sao lưu, một phần mềm sao lưu thông thường sẽ cho phép bạn cấu hình các tham số sau đây:

- **Lựa chọn file.** Bạn sẽ có thể lựa chọn bất kỳ sự kết hợp nào của các file, thư mục hay ổ đĩa trên bất kỳ băng từ nào. Một số phần mềm sao lưu cho phép bạn chuyển qua giữa cách nhìn phương tiện lưu trữ, trong đó hiển thị nội dung của từng băng từ trong tủ đĩa, và cách nhìn đĩa, trong đó hiển thị các mục tiêu sao lưu và một danh sách các phiên bản khác nhau của từng file có trong rất nhiều các băng từ.
- **Vị trí khôi phục.** Bạn sẽ có khả năng lựa chọn khôi phục các file bạn chọn vào vị trí gốc của nó một cách tự động hoặc chỉ ra địa điểm thay thế; bạn sẽ có khả nằng tái tạo lại cây thư mục gốc hoặc chuyển tất cả các file vào trong một thư mục đơn.
- **Lựa chọn ghi đè.** Khi khôi phục các file vào vị trí gốc của nó, bạn sẽ phải chỉ ra các luật cho phép ghi đè các file đã có với cùng tên dựa trên ngày của chúng hoặc các thông số khác.



Hình 4-8. Thẻ *Restore And Manage Media* trong chương trình Windows Server 2003 Backup

Các tính năng lựa chọn thêm của sao lưu mạng

Khi bạn đang phát triển một giải pháp sao lưu cho một hệ thống mạng, một điều rất quan trọng là bạn lựa chọn sản phẩm phần mềm sao lưu được thiết kế cho mục đích sao lưu mạng. Sự khác nhau chính giữa phần mềm sao lưu mạng và một ứng dụng thiết kế cho các hệ thống đơn là nó có khả năng sao lưu các máy tính khác trong mạng. Điều này có nghĩa là bạn có thể mua một ổ đĩa sao lưu và sử dụng nó để bảo vệ toàn mạng. Rất nhiều sản phẩm sao lưu đơn có thể truy cập các đĩa cứng trên các máy tính mạng, tuy nhiên một sản phẩm sao lưu mạng hoàn chỉnh còn có khả năng sao lưu các tính năng quan trọng của hệ điều hành trên các máy tính khác, ví dụ như ***Windows registry*** và CSDL của dịch vụ thư mục. Kiểu sao lưu từ xa này có thể yêu cầu bạn cài đặt thêm các thành phần phần mềm trên máy tính đích.

Trong rất nhiều trường hợp, sản phẩm sao lưu mạng đều có thêm các thành phần cho phép bạn thực hiện các tác vụ sao lưu đặc biệt, ví dụ như sao lưu các CSDL đang chạy hoặc các máy tính chạy các hệ điều hành khác. Một số các thành phần này được mô tả trong phần sau đây.

> ***LƯU Ý. Các thành phần bổ sung****. Trong rất nhiều trường hợp, các gói phần mềm sao lưu mạng chỉ bao gồm các thành phần cơ bản mô tả trong các chương trước. Để thêm vào các tính năng tốt hơn mô tả trong phần sau, bạn phải mua các thành phần khác như là các modul bổ sung riêng rẽ mà có thể cùng làm việc với phần mềm sao lưu chính.*

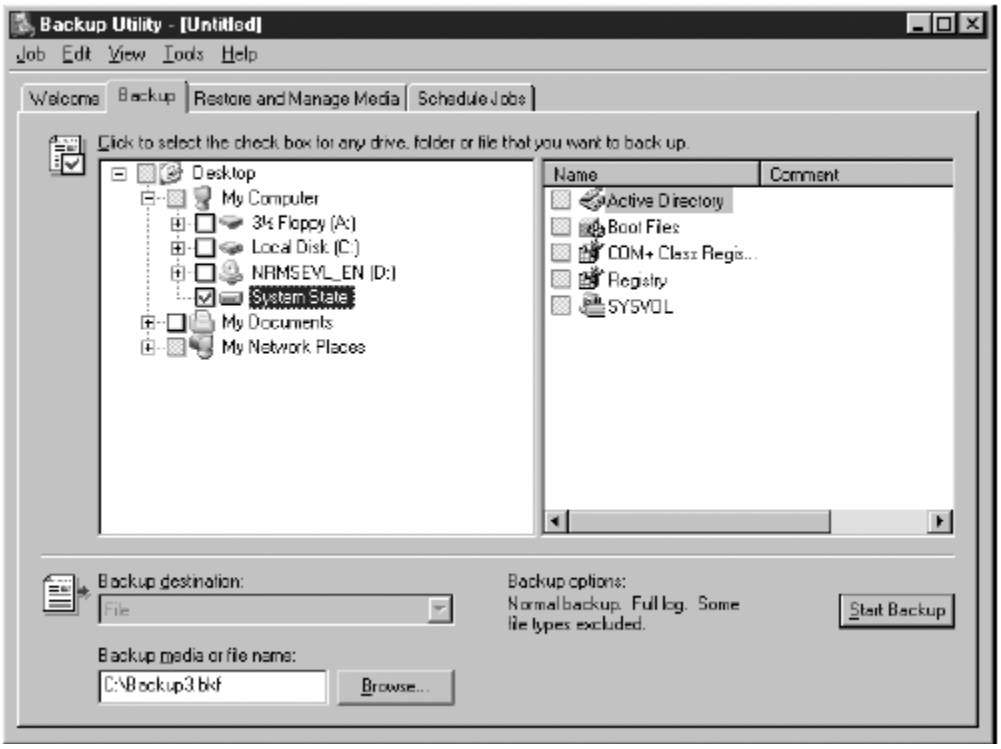
Các Agent để sao lưu từ xa.

Hầu như tất cả mọi phần mềm sao lưu đều có thể sao lưu các ổ đĩa đã được chia sẻ trên các máy tính mạng bên cạnh khả năng sao lưu trên chính máy cài đặt phần mềm đó, tuy nhiên điều này không có nghĩa là chúng được coi là các phần mềm sao lưu mạng. Một bản sao lưu đúng nghĩa là một bản có thể sử dụng để khôi phục lại một đĩa cứng đã bị xóa hoàn toàn trở về trạng thái tốt trước đó. Việc truy cập một máy tính Windows từ xa thông qua một đĩa cứng hay thư mục chia sẻ, về lý thuyết sẽ cho phép bạn sao lưu mọi thứ xuất hiện trong hệ thống file nhưng bạn không thể truy cập đến các phần tử ví dụ như ***Windows registry*** hoặc một CSDL ***Active Directory*** theo cách này. Do đó, một bản sao lưu của một thư mục hoặc ổ đĩa chia sẻ sẽ không hoàn chỉnh và không thể sử dụng để khôi phục một máy tính ở xa về trạng thái nguyên gốc của nó.

Trong chương trình ***Windows Server 2003 Backup***, bạn lựa chọn một đối tượng tên là ***System State*** (Trạng thái Hệ thống - Thể hiện trong Hình 4-9) để sao lưu các phần tử sau trong máy tính nội bộ.

- Các file khởi động hệ thống
- Các file hệ thống nằm trong ***Windows File Protection***
- ***Windows registry***
- CSDL đăng ký ***COM+ Class***
- Dịch vụ thư mục ***Active Directory*** (chỉ trong máy chủ quản trị miền)
- Thư mục ***Sysvol*** (chỉ trong máy chủ quản trị miền)
- Các thông tin về dịch vụ ***Cluster*** (chỉ đối với các nút trong cluster)
- Siêu thư mục ***Internet Information Services*** (IIS) (chỉ trong máy chủ IIS)
- CSDL dịch vụ ***Certificate*** (Chỉ với ***certification authority*** - Ủy quyền chứng nhận)

  LƯU Ý. Sao lưu và khôi phục System State*. Bạn có thể sao lưu và khôi phục* ***System State*** *như là một đối tượng đơn. Ví dụ bạn không thể chỉ khôi phục CSDL* ***Windows registry*** *từ một bản sao lưu* ***System State*** *và cũng không thể đối với các phần tử khác trong đối tượng này, ví dụ như các file khởi động hệ thống.*



Hình 4-9. Sao lưu đối tượng *System State*

Tuy vậy, trong Windows Server 2003, bạn không thể sao lưu đối tượng ***System State*** trên một máy tính khác ngoài máy tính mà bạn đang chạy chương trình ***Backup*** này.

Sử dụng các sản phẩm phần mềm sao lưu mạng, bạn có thể sao lưu các phần tử hệ thống này trên một máy tính ở xa, tuy nhiên trong phần lớn các trường hợp, bạn phải cài đặt một thành phần phần mềm – thông thường được gọi là ***agent*** – trên các máy tính ở xa này trước. ***Agent*** này cho phép máy chủ sao lưu thiết lập mỗi liên lạc với máy tính ở xa và tải về các thành phần hệ điều hành cần thiết để thực hiện việc sao lưu hoàn chỉnh của các ổ đĩa máy tính.

> ***LƯU Ý. Mua các agent****. Các sản phẩm sao lưu có thể bao gồm các* ***agent*** *sao lưu từ xa khác nhau kèm theo thành phần cơ bản. Ví dụ, khi bạn mua một sản phẩm mà chạy phần sao lưu chính trên một máy tính Windows Server 2003, sản phẩm này có thể bao gồm các* ***agent*** *cần thiết để sao lưu các máy tính Windows khác trong mạng. Tuy nhiên, nếu bạn có các máy tính chạy các hệ điều hành khác, bạn có thể phải mua thêm các* ***agent*** *riêng cho các hệ điều hành này.*

Sao lưu các file đang mở.

Trong rất nhiều trường hợp, khi một ứng dụng mở một file văn bản, file này bị khóa ở trạng thái mở và do đó không có ứng dụng hoặc tiến trình nào

khác có thể truy cập nó. Điều này để bảo vệ không cho các chương trình khác thay đổi bản sao trên đĩa của một file đang nằm trong bộ nhớ. Một trong những lý do chính tại sao các quản trị mạng lại tiến hành sao lưu sau giờ làm việc là để ngăn cản tình trạng bỏ qua các file vì chúng đang được mở bởi người dùng. Do vậy, nếu người dùng để ứng dụng chạy với một file đang mở, tác vụ sao lưu vẫn có thể không bảo vệ được file này. Để giải quyết vấn đề này, một số phần mềm sao lưu có khả năng sao lưu các file đang mở cho phép khả năng sao lưu các kiểu file này thậm chí ngay cả khi các ứng dụng khác đang mở chúng.

Sao lưu CSDL

Các CSDL hay có vấn đề khi sao lưu, bởi vì chúng thường chứa các dữ liệu quan trọng sống còn cần bảo vệ và cũng bởi chúng thường xuyên ở trạng thái chạy liên tục không nghỉ. Các CSDL đang chạy thường khóa các file dữ liệu của chúng ở trạng thái mở giống như các ứng dụng khác, cho phép các tác vụ sao lưu bảo vệ các file chương trình CSDL (mà rất dễ dàng thay thế) tuy nhiên lại bỏ qua chính bản thân các CSDL này.

Để sao lưu CSDL, bạn phải tắt chúng đi trước để mở khóa trạng thái của các file dữ liệu. Trong trường hợp việc tắt các ứng dụng là không thể được bởi vì các CSDL này luôn phải sẵn sàng đối với người dùng, rất nhiều phần mềm sao lưu có một ***agent*** đặc biệt cho CSDL cho phép dễ dàng sao lưu các CSDL này bằng cách sử dụng các thủ tục như sau:

1. ***Agent*** tạo ra một bản sao tạm thời của các file CSDL được gọi là ***delta file***
2. ***Agent*** này hướng các yêu cầu của người dùng đối với các thông tin CSDL vào ***delta file***
3. ***Agent*** đóng file CSDL nguyên gốc lại
4. ***Agent*** giao tiếp với máy chủ sao lưu và chuyển phát nội dung của các file CSDL này để sao lưu sang băng từ.
5. Sau khi quá trình sao lưu hoàn thành, ***agent*** sao chép tất cả các thay đổi bởi người dùng đối với ***delta file*** sang file CSDL nguyên gốc
6. ***Agent*** lại mở lại file CSDL
7. ***Agent*** hướng các yêu cầu người dùng trở lại vào file CSDL nguyên gốc
8. ***Agent*** xóa ***delta file***.

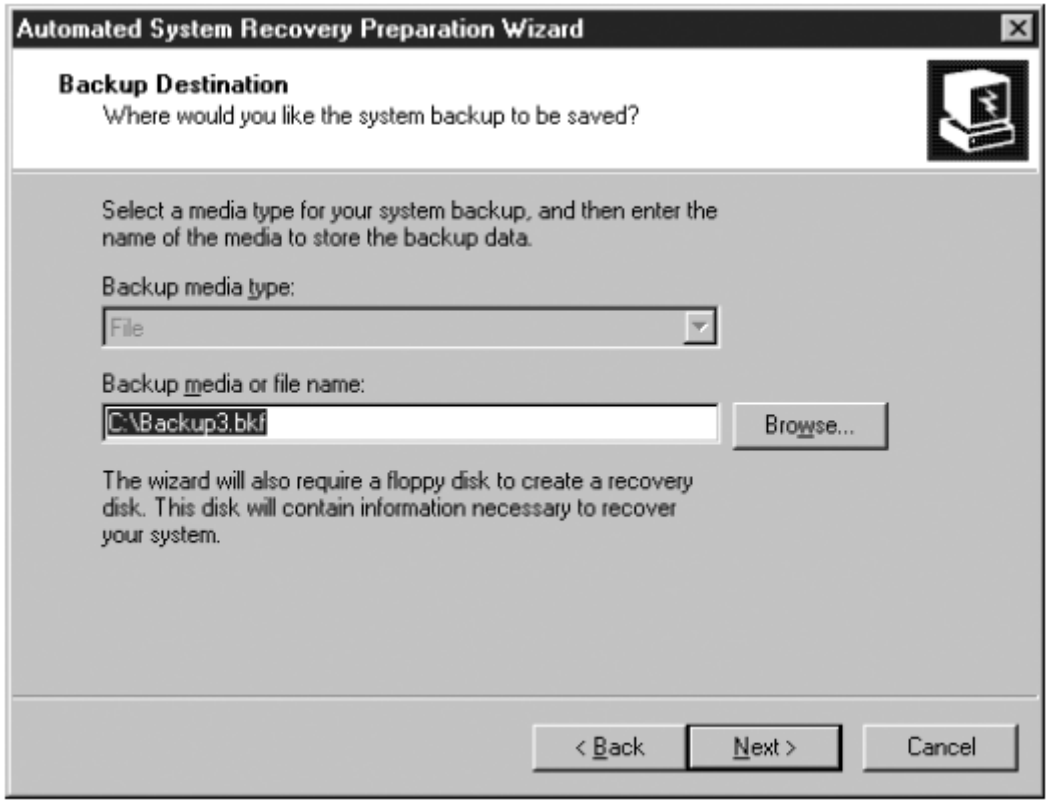
Khôi phục sau thảm họa

Cũng giống như bất kỳ ứng dụng nào, phần mềm sao lưu yêu cầu một hệ điều hành để chạy. Nếu như các đĩa hệ thống hoặc máy chủ sao lưu của bạn có sự cố, bạn có một bản sao lưu đầy đủ của đĩa cứng thì bạn phải làm thế nào để khôi phục lại nó. Trong điều kiện bình thường, bạn phải cài đặt lại hệ điều hành và sau đó cài đặt lại phần mềm sao lưu trước khi bạn có thể khôi phục lại đĩa cứng trở về trạng thái nguyên gốc. Đối với một doanh nghiệp mà thời gian chết có nghĩa là tổn thất về doanh thu, thì sự chậm trễ này có thể không thể chấp nhận được

> ***LƯU Ý. Mục đích của kỳ thi.*** *Mục đích của kỳ thi 70-290 chỉ ra rằng học viên phải có khả năng "thực hiện khôi phục hệ thống cho một máy chủ" và "tái tạo lại hệ thống sau khi phần cứng máy chủ có sự cố"*

Một số phần mềm sao lưu có thể giải quyết vấn đề này bằng cách cung cấp tính năng khôi phục thảm họa. Phần mềm có tính năng này được thiết kế cho phép người quản trị tiến hành khôi phục lại hoàn toàn các đĩa hệ thống trên máy tính trong thời gian ngắn nhất. Phần mềm này tạo ra một bản sao lưu đầy đủ kết hợp với một đĩa khởi động chỉ chứa các file hệ điều hành cần thiết để chạy chương trình sao lưu và thực hiện việc khôi phục. Sau khi khởi động từ đĩa khởi động này, bạn có thể tiến hành việc khôi phục và máy tính sẽ trở lại trạng thái nguyên gốc, nhanh hơn rất nhiều so với việc bạn phải cài lại hệ điều hành một cách thủ công.

Chương trình ***Windows Server 2003 Backup*** có tính năng khôi phục sau thảm họa được gọi là ***Automated System Recovery*** (Khôi phục hệ thống tự động-ASR). Khi bạn chạy ***Automated System Recovery Preparation Wizard*** (Trình chuẩn bị khôi phục hệ thống tự động) (thể hiện trong Hình 4-10), phần mềm sẽ hướng dẫn bạn qua các quá trình tạo ra bản sao lưu đầy đủ của máy chủ và sau đó nhắc bạn đưa đĩa mềm vào, trình này sẽ sử dụng đĩa mềm đó để tạo ra đĩa khởi động cho hệ thống. Trong trường hợp thảm họa mà toàn bộ nội dung của đĩa hệ thống bị mất, bạn chỉ cần đơn giản là đưa băng từ sao lưu vào trong ổ băng từ và khởi động từ đĩa mềm nói trên để hoàn tất việc khôi phục hệ điều hành.



Hình 4-10. Trình *Automated System Recovery Preparation Wizard*

> ***LƯU Ý. Mục đích của kỳ thi***. *Mục đích của kỳ thi 70-290 chỉ ra rằng học viên phải có khả năng "sử dụng **Automated System Recovery** (ASR)"*

Bảo mật sao lưu

Các bản sao lưu chứa các bản sao của cùng dữ liệu bạn lưu trên các đĩa cứng, do đó bạn sẽ phải mất công sức để bảo mật các bản sao lưu này như khi bạn bảo mật các dữ liệu gốc. Các chương trình sao lưu mang cho phép bạn chỉ định tên tài khoản và mật khẩu mà phần mềm này sử dụng để truy cập các mục tiêu sao lưu. Phương pháp thực hành tốt nhất là tạo ra một tài khoản đặc biệt cho mục đích này mà chỉ có đủ quyền cần thiết để thực hiện sao lưu hơn là sử dụng tài khoản Administrator hoặc các tài khoản khác có nhiều tính năng. Bạn có thể dễ dàng cung cấp một tài khoản người dùng với các quyền này bằng cách thêm nó vào trong nhóm ***Backup Operators*** tạo sẵn trong ***Active Directory***. Cách này sẽ ngăn cản các người dùng chưa xác thực không thể gây hại cho tính bảo mật của mạng bằng cách sử dụng các phần mềm sao lưu.

> ***LƯU Ý. Mục đích của kỳ thi***. *Mục đích của kỳ thi 70-290 chỉ ra rằng học viên phải có khả năng "cấu hình bảo mật cho các nhiệm vụ sao lưu"*

Để giữ cho dữ liệu của bạn được bảo mật, bạn phải bảo vệ các file trong các băng từ sao lưu. Các phần mềm sao lưu mạng thông thường cho phép bạn sử dụng mật khẩu để bảo vệ các băng từ sao lưu này. Bạn có thể chỉ định mật khẩu trong quá trình tạo ra các tác vụ sao lưu và bạn phải cung cấp mật khẩu giống thế để khôi phục dữ liệu từ các bản sao lưu đó. Khi sử dụng mật khẩu để bảo vệ băng từ của bạn, bạn nên sử dụng cùng yêu cầu cho mật khẩu mà bạn dùng cho hệ thống mạng, ví dụ như độ dài và tính phức hợp của mật khẩu.

Bạn cũng phải bảo mật mức vật lý các băng từ, không chỉ bảo mật dữ liệu mà còn phải đảm bảo tính an toàn của nơi cất giữ. Bảo vệ bằng mật khẩu có thể ngăn ngừa những kẻ xâm phạm vô tình không khôi phục dữ liệu của bản bằng phần mềm sao lưu nhưng thực tế dữ liệu vẫn trong băng từ với một định dạng không được bảo vệ và một ai đó có đủ kĩ năng và thiết bị có thể vẫn truy cập được các file này. Do đó, bạn nên luôn giữ bản sao lưu của mình được khóa chặt chẽ, tốt nhất là trong các tủ chống cháy hoặc các khu vực lưu trữ bảo mật nào đó. Bạn cũng nên lưu các bản sao lưu này ở xa khu vực làm việc để nếu có trộm hoặc thảm họa cũng không làm cho các bản sao lưu này mất đi cùng với máy tính của bạn.

SỬ DỤNG WINDOWS SERVER 2003 BACKUP

Chương trình Backup trang bị trong Windows Server 2003 không phải là một gói phần mềm sao lưu đầy đủ tính năng như mô tả ở phần trước, tuy nhiên nó cũng đủ để sao lưu một máy chủ. Với chương trình ***Backup***, bạn có thể thực hiện các tác vụ sau đây:

- Sao lưu các ổ cứng tại chỗ, các ổ chia sẻ trên mạng và đối tượng ***System State*** nội bộ
- Lựa chọn mục tiêu sao lưu bằng cách sử dụng cách hiển thị hình cây
- Thực hiện các tác vụ sao lưu ***normal, incremental, differential, copy*** hoặc ***daily.***
- Loại bỏ các file đặc biệt được đánh dấu khỏi tác vụ sao lưu
- Sao lưu các file sang một ổ băng từ hoặc sang file trên các đĩa nội bộ khác, sau đó bạn có thể chuyển sang một đĩa CD-ROM, DVD-ROM hoặc các phương tiện lưu trữ khác.

- Lập lịch sao lưu để diễn ra tại các thời gian xác định hoặc lặp lại sau các khoảng thời gian xác định.
- Xác nhận các bản sao lưu bằng cách so sánh dữ liệu ảnh trên các phương tiện sao lưu với bản nguyên gốc của nó.
- Khôi phục các file đã sao lưu vào vị trí nguyên gốc của nó hoặc đến một vị trí thay thế khác
- Chỉ định khi nào và liệu các file khôi phục có ghi đè các file đã tồn tại.

Một số các tính năng liên quan đến sao lưu mà Windows Server 2003 cung cấp được đề cập trong các phần sau đây.

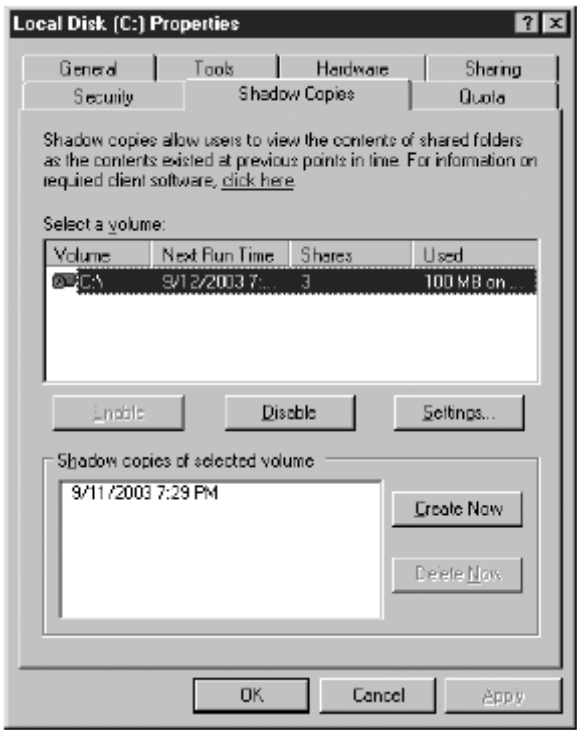
Sử dụng Volume Shadow Copy

Volume Shadow Copy (Bản sao hình bóng của đĩa) là một tính năng của Windows Server 2003 cho phép duy trì một thư viện chứa các phiên bản khác nhau của các file đã lựa chọn. Mặc dù không thể thay thế cho việc sao lưu hệ thống, ***Volume Shadow Copy*** cho phép người dùng truy cập các phiên bản lưu trước đó của file mà họ vô tình xóa hoặc phá hủy. Tính năng này giảm bớt cho người quản trị một trong các công việc lặt vặt phiền hà nhất: khôi phục file đơn lẻ cho người dùng khi họ lỡ xóa file đó.

> ***LƯU Ý. Mục đích của kỳ thi***. *Mục đích của kỳ thi 70-290 chỉ ra rằng học viên phải có khả năng "khôi phục dữ liệu từ **shadow copy volume**"*

Để kích hoạt ***volume shadow copy*** cho một đĩa trên máy tính của bạn, bạn cho hiển thị hộp thoại ***Local Disk Properties*** của đĩa logic đó và lựa chọn thẻ ***Shadow Copies*** (thể hiện trong Hình 4-11). Khi bạn lựa chọn một đĩa logic trong danh sách và nhấn vào ***Enable***, Windows Server 2003 tạo ra một bản sao chép của tất cả các fie trong thư mục chia sẻ trên đĩa logic đó và dán nhãn lên bản sao chép đó thông tin ngày giờ hiện tại. Sau khi kích hoạt tính năng này cho đĩa, Windows Server 2003 tiếp tục tạo ra hai bản sao của các file này mỗi ngày trong tuần và lưu chúng cho đến khi dung lượng đĩa chỉ định dành cho chức năng này đầy. Bạn có thể chỉnh sửa cả tần suất mà hệ điều hành Windows tạo ra các bản sao và kích thước của không gian đĩa sử dụng để lưu các bản sao này.

> **QUAN TRỌNG**. ***Giới hạn của Volume Shadow Copy***. *Volume Shadow Copy chỉ bảo vệ các file trên đĩa logic mà lưu trong các thư mục chia sẻ, và đĩa này phải sử dụng định dạng hệ thống file NTFS.*



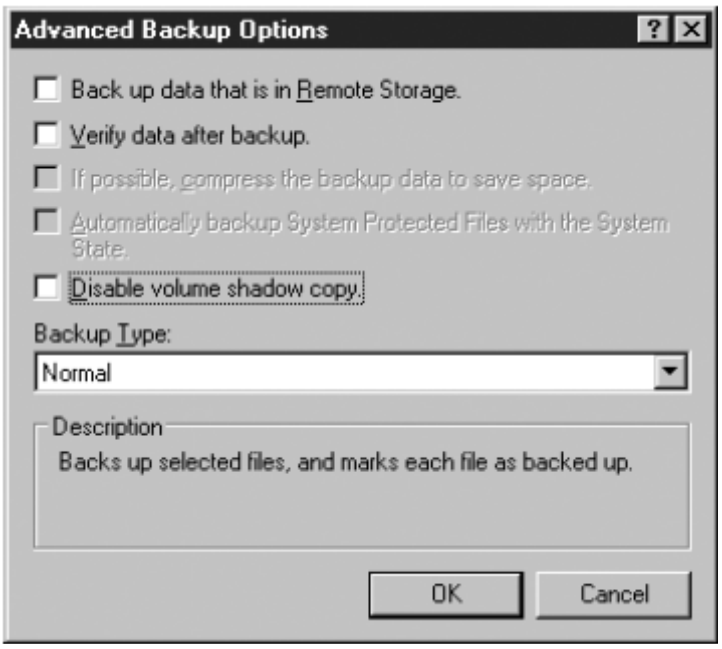
Hình 4-11. Thẻ *Shadow Copy* của hộp thoại *Local Disk Properties* của một đĩa logic

Chỉ những máy tính chạy Windows Server 2003 và Windows XP mới có thể truy cập các file ***shadow copy*** trên các ổ đĩa. Trên các máy trạm Windows XP, đầu tiên bạn phải cài đặt phần mềm máy khách để có thể sử dụng chức năng này. Sau đó người dùng có thể truy cập ***shadow copy*** bằng cách hiển thị hộp thoại ***Properties*** của file trong ***shadow volume*** và lựa chọn thẻ ***Previous Versions*** (thể hiện trong hình 4-12)

Hình 4-12. Thẻ *Previous Versions* trong hộp thoại *Properties* của file.

> ***LƯU Ý. Volume Shadow Copy Clients****. Windows Server 2003 bao gồm phần mềm máy khách của* ***volume shadow copy*** *trong thư mục* ***Systemroot\System32\Clients\Twclient.*** *Bạn có thể cài đặt phần mềm này một cách thủ công trên các máy trạm Windows XP hoặc bằng cách cài đặt tự động, ví dụ như sử dụng chính sách nhóm*

Bên cạnh việc cung cấp cho người dùng khả năng truy cập vào các phiên bản khác nhau của các file, ***volume shadow copy*** còn cung cấp kĩ thuật sao lưu các file mở cho trương trình ***Windows Server 2003 backup***. Theo mặc định, ***Backup*** sử dụng các bản sao ***volume shadow*** của các file mà đang khóa ở trạng thái mở khi thực hiện sao lưu. Điều này cho phép chương trình Backup sao lưu các file mà đang sử dụng bởi các ứng dụng trong thời điểm tiến hành sao lưu. Bạn có thể không cho ***Backup*** sử dụng các bản sao ***volume shadow*** trong các tác vụ sao lưu đặc biệt nào đó bằng cách lựa chọn ***Disable Volume Shadow Copy*** trong hộp thoại ***Advanced Backup Options*** (thể hiện trong hình 4-13)



Hình 4-13. Hộp thoại *Advanced Backup Options*

Sao lưu và khôi phục Active Directory.

Như đề cập trong phần trước của chương, bạn có thể sao lưu CSDL A***ctive Directory*** trên máy chủ quản trị miền Windows Server 2003 bằng cách sử dụng chương trình Backup và lựa chọn đối tượng ***System State*** như là mục tiêu sao lưu. Tuy nhiên việc khôi phục máy chủ quản trị miền ***Active Directory*** là không đơn giản. Trước khi bạn có thể khôi phục CSDL ***Active Directory*** từ bản sao lưu ***System State***, bạn phải khởi động máy tính trong chế độ ***Directory Services Restore Mode***. Bạn làm điều này bằng cách nhấn F8 khi máy tính đang khởi động và lựa chọn ***Directory Services Restore Mode*** từ thực đơn ***Windows Advanced Options***. Theo cách này máy tính sẽ khởi động với CSDL ***Active Directory*** được đóng và do đó bạn có thể truy cập chương trình ***Backup*** và khôi phục lại CSDL này từ băng từ.

> ***LƯU Ý. Đăng nhập****. Khi bạn khởi động máy tính trong chế độ* ***Directory Services Restore Mode*** *bạn phải đăng nhập với tài khoản* ***Administrator*** *sử dụng tên tài khoản và mật khẩu* ***Security Accounts Manager*** *(SAM) chứ không phải tên tài khoản và mật khẩu trong* ***Active Directory****. Đó là bởi vì* ***Active Directory*** *đang* ***offline*** *(ở trạng thái đóng, không kích hoạt) nên việc xác nhận tài khoản không thể thực hiện được. CSDL tài khoản SAM được sử dụng để điều khiển truy cập vào* ***Active Directory*** *trong khi* ***Active Directory*** *đang* ***offline****. Bạn phải nhập mật khẩu này khi bạn cài đặt* ***Active Directory***

Khi máy tính khởi động trong chế độ ***Directory Services Restore Mode***, bạn có thể chạy chương trình ***Backup*** và khôi phục lại đối tượng ***System State*** từ băng từ hoặc các phương tiện sao lưu khác. Chương trình ***Windows Server 2003 Backup*** hỗ trợ 2 kiểu khôi phục ***Active Directory***:

Khôi phục non-authoritative (không có thẩm quyền). Các đối tượng trong CSDL ***Active Directory*** được khôi phục chính xác như nó xuất hiện trong ***System State*** với các số thứ tự cập nhật gốc được giữ nguyên. Bởi vì các số thứ tự này có giá trị bằng với giá trị mà các đối tượng có được khi tác vụ sao lưu được tiến hành, chúng đã quá hạn và quá trình đồng bộ ***Active Directory*** sẽ ghi đè các đối tượng này bằng các phiên bản mới hơn trong các máy chủ quản trị miền khác. Bạn có thể sử dụng phương pháp khôi phục ***non-authoritative*** này khi bạn muốn xây dựng lại một máy chủ quản trị miền mà đã bị hỏng với các thông tin ***Active Directory*** mới nhất được cập nhật từ các máy chủ quản trị miền khác. Chương trình ***Windows Server 2003 Backup*** theo mặc định sẽ thực hiện tác vụ khôi phục theo kiểu ***non-authoritative***.

Khôi phục Authoritative (có thẩm quyền). Các đối tượng trong CSDL ***Active Directory*** sẽ được khôi phục mà các số thứ tự cập nhật sẽ không bị ghi đè trong các quá trình đồng bộ ***Active Directory*** sau đó. Bạn sử dụng khôi phục kiểu ***Authoritative*** khi bạn muốn dùng bản sao lưu ***System Stat***e để phục hồi lại các đối tượng ***Active Directory*** mà bạn đã vô tình xóa đi.

Để thực hiện việc khôi phục ***Authoritative***, ban đầu bạn phải thực hiện khôi phục kiểu ***non-authoritative*** trước, sau đó trước khi khởi động lại máy tính, bạn sử dụng một tiện ích dòng lệnh được gọi là ***Ndsutil.exe*** để đánh dấu các đối tượng trong ***Active Directory*** hiện tại như là ***authoritative***. Tiện ích ***Ndsutil.exe*** có thể tìm thấy trong thư mục ***Systemroot\System32***. Việc đánh dấu các đối tượng là ***authoritative*** sẽ thay đổi số thứ tự cập nhật của đối tượng đó cao hơn bất kì số thứ tự cập nhật nào khác trong khi đồng bộ hệ thống ***Active Director***y. Điều này đảm bảo rằng mọi dữ liệu mà bạn khôi phục sẽ được đồng bộ trong toàn hệ thống.

Khi máy chủ quản trị miền được khôi phục về trạng thái trực tuyến và kết nối vào hệ thống mạng, các tác vụ đồng bộ thông thường sẽ đưa các dữ liệu trong máy chủ quản trị miền này cập nhật với các thay đổi trong các máy chủ quản trị miền khác mà không bị ghi đè bởi nó đã được khôi phục kiểu authoritative. Việc đồng bộ đồng thời cũng phân tán các đối tượng đã được khôi phục sang các máy chủ quản trị miền khác trong forest. Các đối tượng đã từng bị xóa được đánh dấu là ***authoritative*** sẽ được đồng bộ từ máy chủ quản trị miền được khôi phục tới các máy chủ quản trị miền khác. Bởi vì các

đối tượng được khôi phục có cùng thuộc tính đối tượng nên khả năng bảo mật được giữ nguyên và sự phụ thuộc của các đối tượng sẽ được duy trì.

Ví dụ, giả sử bạn sao lưu hệ thống vào này thứ Hai và sau đó tạo một người dùng mới tên là Jeff Smith vào thứ Ba, thông tin này sẽ dược đồng bộ với các máy chủ quản trị miền khác trong miền. Sau đó, vào ngày thứ Tư, bạn vô tình xóa đối tượng người dùng Nancy Anderson. Để khôi phục người dùng Nancy Anderson mà không phải tạo lại các thông tin và không mất tài khoản của Jeff Smith, bạn tiến hành khôi phục ***nonauthoritative*** máy chủ quản trị miền với bản sao lưu ***System State*** được tạo trong ngày thứ Hai. Sau đó, sử dụng ***Ntdsutil.exe*** bạn sẽ đánh dấu đối tượng người dùng Nancy Anderson là ***authoritative*** và khởi động lại máy chủ quản trị miền này. Kết quả là đối tượng Nancy Anderson được khôi phục mà không tác động gì đến tài khoản Jeff Smith.

> ***LƯU Ý.Mục đích của kỳ thi***. *Mục đích của kỳ thi 70-290 chỉ ra rằng học viên phải có khả năng "sao lưu các file và dữ liệu* ***System State*** *sang các phương tiện lưu trữ"*

TỔNG KẾT

- Một giải pháp sao lưu mạng bao gồm phần cứng sao lưu, phần mềm sao lưu và kế hoạch sử dụng chúng.
- Khi bạn đánh giá một phần cứng sao lưu, tốc độ cao hơn và dung lượng lớn hơn gần như có nghĩa là giá sẽ đắt hơn.
- Băng từ là phương tiện sao lưu thông dụng nhất để sao lưu bởi băng từ có tốc độ sao lưu nhanh, không đắt và chứa được rất nhiều dữ liệu. Các ổ băng từ có rất nhiều loại khác nhau về tốc độ, dung lượng và khoảng giá cả để phù hợp với các nhu cầu cài đặt khác nhau.
- Chức năng chính của phần mềm sao lưu là cho phép người quản trị mạng có thể lựa chọn các mục tiêu để sao lưu và sau đó chuyển dữ liệu này đến các băng từ hoặc các thiết bị khác.
- Các tác vụ sao lưu ***Incremental*** và ***differential*** sẽ tiết kiệm băng từ bằng cách chỉ sao lưu các file mà thay đổi từ lần sao lưu cuối cùng, dựa trên tình trạng của bit lưu trong mỗi file.
- Một phần mềm sao lưu tốt cho phép bạn lập lịch sao lưu để chạy vào bất kỳ thời điểm nào và nó duy trì phiên bản mục lục của tất cả các file sao lưu trên cả băng từ và trên đĩa cứng
- Phần mềm sao lưu mạng cho phép bạn sao lưu mọi dữ liệu trong các máy tính trong mạng của bạn và cũng cung cấp các tính năng tiên tiến ví dụ như sao lưu các CSDL trực tuyến.
- Để sao lưu ***Windows registry***, CSDL ***Active Directory*** và các tài nguyên hệ thống khác, bạn phải sao lưu đối tượng ***System State***.
- ***Volume shadow copy*** là một tính năng của Windows Server 2003 cho phép nười dùng có thể truy cập các bản sao khác nhau của các file mà họ đã vô tình xóa mất hoặc bị hỏng
- Khi bạn khôi phục dữ liệu ***System State*** trong chế độ ***nonauthoritative***, mọi thành phần trong dữ liệu ***System State*** mà được đồng bộ với các máy chủ quản trị miền khác, ví dụ như CSDL ***Active Directory***, sẽ được cập nhật bởi quá trình đồng bộ sau khi bạn khôi phục.
- Khi bạn khôi phục dữ liệu ***System State*** trong chế độ ***Authoritative***, các thay đổi sau khi sao lưu lần cuối cùng sẽ không được khôi phục, các đối tượng bị xóa sẽ được phục hồi và đồng bộ. Để thực hiện khôi phục ***authoritative***, bạn sử dụng tiện ích dòng lệnh ***Ntdsutil.exe***.

BÀI TẬP THỰC HÀNH

Bài tập thực hành 4-1: Lựa chọn mục tiêu sao lưu

Trong bài tập thực hành này, bạn thực hành sử dụng cách hiển thị cây thư mục trong chương trình Backup để lựa chọn các mục tiêu để sao lưu.

1. Đăng nhập vào máy tính Windows Server 2003 bằng tài khoản ***Administrator***
2. Nhấn ***Start,*** trỏ vào ***All Programs***, chọn ***Accessories,*** chọn ***System Tools*** và sau đó chọn ***Backup***. Trang ***Welcome To The Backup Or Restore Wizard*** xuất hiện.
3. Nhấn vào liên kết ***Advanced Mode***. Cửa sổ ***Backup Utility*** xuất hiện
4. Lựa chọn thẻ ***Backup***
5. Mở rộng đĩa ***Local disk (C)*** và lựa chọn thư mục ***Windows***
6. Lựa chọn hộp chọn ***System State***
7. Từ thực đơn ***Job***, lựa chọn ***Exit***

Bài tập thực hành 4-2: Sao lưu Incremental và Differential

1. Nếu bạn sao lưu hệ thống mạng của bạn bằng cách thực hiện sao lưu đầy đủ vào các ngày thứ Tư lúc 6h P.M và sao lưu ***differential*** trong các buổi chiều sáu ngày còn lại trong tuần, bao nhiêu tác vụ mà bạn cần thiết phải thực hiện để khôi phục lại máy tính khi một đĩa cứng bị hỏng vào trưa ngày thứ Ba ?
2. Nếu bạn sao lưu hệ thống mạng của bạn bằng cách sao lưu đầy đủ vào 6h P.M ngày thứ Tư, bao nhiêu tác vụ cần thiết nếu bạn đã tiến hành các tác vụ sao lưu ***incremental*** trong các buổi chiều sáu ngày còn lại trong tuần và một đĩa cứng bị hỏng vào trưa ngày thứ Ba ?
3. Để khôi phục lại hoàn toàn một máy tính bị hỏng vào trưa ngày thứ Ba, bao nhiêu tác vụ cần thiết nếu bạn tiến hành sao lưu đầy đủ vào 6h A.M các ngày tư Tư và thứ Bảy hàng tuần và sao lưu ***incremental*** vào 6h P.M các ngày còn lại?

Bài tập thực hành 4-3. Kích hoạt Volume Shadow Copy

1. Trong bài tập thực hành này, bạn kích hoạt tính năng ***volume shadow copy*** trong ổ đĩa C: của máy tính.

2. Đăng nhập vào máy tính Windows Server 2003 bằng tài khoản ***Administrator***
3. Nhấn ***Start***, trỏ vào ***All Programs,*** chọn ***Accessories***, và chọn ***Windows Explorer***. Cửa sổ ***Windows Explorer*** xuất hiện
4. Mở rộng đối tượng ***My Compute***r trong khung phạm vi, lựa chọn ***Local Disk (C:)***, và từ thực đơn ***File***, lựa chọn ***Properties.*** Hộp thoại ***Local Disk (C:) Properties*** xuất hiện
5. Lựa chọn thẻ ***Shadow Copy*** và nhấn ***Enable***. Hộp thông báo ***Enable Shadow Copy*** xuất hiện
6. Đọc cảnh báo và nhấn ***Yes***. Sau một khoảng thời gian trễ, ngày và giờ xuất hiện trong danh sách ***Shadow Copies Of Selected Volume,*** chỉ định rằng hệ thống đã tạo ra bản ***shadow copy*** đầu tiên

CÁC CÂU HỎI ÔN TẬP

1. Tại sao tiến hành sao lưu lại tốt nhất sau khi hết giờ làm việc?
2. Các kiểu tác vụ sao lưu nào sau đây không đặt lại bit lưu trữ trong các file mà nó sao chép sang các phương tiện lưu trữ ? (Lựa chọn tất cả các câu trả lời đúng)
    a. ***Full***
    b. ***Incremental***
    c. ***Differential***
    d. ***Copy***
3. Các thiết bị ổ băng từ nào sau đây có dung lượng lớn nhất ?
    a. ***LTO***
    b. ***QIC***
    c. ***DAT***
    d. ***DLT***
4. Các tiêu chuẩn nào dưới đây được sử dụng nhiều nhất để lọc các file trong các tác vụ sao lưu?
    a. ***Tên file***
    b. ***Phần mở rộng của file***
    c. ***Các thuộc tính của file***

   d. Kích thước của file

5. Làm thế nào mà một ***autochanger*** tăng dung lượng lưu trữ tổng của một giải pháp sao lưu?
6. Ba thành phần của hệ thống quay vòng sử dụng phương tiện sao lưu ***Grandfather-Father-Son*** là gì ?

   a. Các ổ đĩa cứng, ổ CD-ROM và các ổ băng từ

   b. Các tác vụ sao lưu Incremental, differential và full

   c. Các tác vụ sao lưu hàng tháng, hàng tuần và hàng ngày?

   d. ***Các ổ băng từ QIC, DAT và DLT***
7. Các thiết bị sao lưu mạng sử dụng thường xuyên nhất giao tiếp thiết bị nào?

   a. IDE

   b. SCSI

   c. USB

   d. ***Parallel port***
8. Làm thế nào ***Windows Backup*** xác nhận các dữ liệu ghi vào phương tiện sao lưu ?
9. Khi bạn khởi động máy tính trong chế độ ***Directory Services Restore Mode***, bạn sử dụng đăng nhập như thế nào? Tại sao ?

KỊCH BẢN TÌNH HUỐNG

Bạn đang thiết kế một giải pháp sao lưu cho hệ thống mạng của công ty. Để dễ dàng sao lưu các dữ liệu quan trọng của công ty, bạn cấp cho 125 người dùng mạng mỗi người một thư mục gốc trên một ổ đĩa chia sẻ trên máy chủ và hướng dẫn người dùng lưu các file dữ liệu của họ trên các thư mục đó. Bạn cũng đồng thời tạo ra một hạn ngạch đĩa cho phép mỗi người dùng được sử dụng tối đa 1GB dung lượng đĩa.

Bởi thiết kế như trên, bạn sẽ phải sao lưu chỉ máy chủ mà không phải là các máy trạm người dùng. Bên cạnh máy chủ file chứa các thư mục gốc của mỗi người dùng, trong mạng còn có 6 máy chủ Web, mỗi máy chủ có một ổ cứng 40 GB chứa các file trang chủ, một máy chủ CSDL với ổ cứng 80GB chứa xấp xỉ 10GB file dữ liệu và một máy chủ Email với 25GB dữ liệu thư.

Dựa trên các thông tin như trên, bạn hãy trả lời các câu hỏi sau:

1. Tổng dung lượng xấp xỉ của dữ liệu thay đổi thường xuyên mà bạn phải sao lưu mỗi ngày là bao nhiêu ?
    a. 60 GB
    b. 160 GB
    c. 360 GB
    d. 480 GB
2. Giả định rằng bạn quyết định thực hiện sao lưu đầy đủ hàng tuần và sao lưu incremental hàng ngày, dung lượng dữ liệu xấp xỉ từ 6 máy chủ Web mà bạn mong đợi tìm thấy trong mỗi băng từ sao lưu Incremental là bao nhiêu? Giải thích câu trả lời của bạn.
3. Dựa trên các thông tin ở trên trong Bảng 4-1, kiểu băng từ nào phù hợp nhất cho hệ thống mạng này, giả định rằng bạn muốn sử dụng chỉ một băng từ đơn cho các tác vụ sao lưu Incremental hàng ngày ?
    a. DLT
    b. 8 mm
    c. QIC
    d. DAT

CHƯƠNG 5: DUY TRÌ HỆ ĐIỀU HÀNH

Các sản phẩm phần mềm hiện nay đang trong giai đoạn phát triển liên tục và các nhà sản xuất luôn đều đặn đưa ra các bản cập nhật và nâng cấp . Hệ điều hành cũng không phải là một ngoại lệ và một điều rất quan trọng là giữ cho hệ điều hành Windows Server 2003 của bạn luôn được cập nhật. Việc cập nhật các máy tính đơn lẻ là một việc đơn giản, tuy nhiên cập nhật một hệ thống mạng lớn một cách đúng lúc và hiệu quả thì phức tạp hơn rất nhiều. Trong chương này bạn sẽ học về các kiểu cập nhật hệ điều hành mà Microsoft đưa ra và một số phương pháp bạn có thể sử dụng để triển khai các bản cập nhật này

Sau khi hoàn thành chương này, bạn có thể:

- **Hiểu sự khác nhau giữa các *service pack* (Các gói dịch vụ) và *hotfix* (Bản sửa lỗi nóng)**
- **Triển khai service pack bằng các ứng dụng *Windows Update* (Cập nhật Windows), *Automatic Update* (Tự động cập nhật) và các chính sách nhóm**
- **Tích hợp các bản *service pack* and *hotfix* vào trong các bộ cài đặt của hệ điều hành Windows Server 2003**
- **Sử dụng phần mềm *Microsoft Baseline Security Analyzer* (Trình phân tích ranh giới bảo mật)**
- **Cài đặt và cấu hình một máy chủ *Microsoft Software Update Services* (Dịch vụ cập nhật phần mềm của Microsoft)**
- **Hiểu các chế độ giấy phép bản quyền *Per Server* và *Per Device* hoặc *Per User* (Tính theo máy chủ, thiết bị hoặc theo người dùng)**
- **Cấu hình các giấy phép bản quyền sử dụng công cụ *Choose Licensing Mode* (Lựa chọn Chế độ Giấy phép) trong *Control Panel* và công cụ *Licensing Administrative* (Quản trị Giấy phép)**
- **Tạo các nhóm giấy phép bản quyền**

CÁC BẢN CẬP NHẬT CỦA HỆ ĐIỀU HÀNH WINDOWS

Đã có thời kỳ, việc cập nhật phần mềm là một vấn đề rất nhỏ. Nếu có một sự cố nào trong một ứng dụng hay hệ điều hành, nhà sản xuất sẽ phát hành một bản cập nhật dưới dạng một bản vá lỗi mà người dùng có thể áp dụng cho các máy tính của mình. Một bản cập nhật (Update) là một phần phụ của bản cài đặt phần mềm đã được sửa lại và thường có xu hướng giải quyết một vấn đề cá biệt nào đó hơn là thêm vào các tính năng mới cho phần mềm đó. Khi nhà sản xuất đưa ra phiên bản tiếp theo của phần mềm, họ sẽ tích hợp các bản vá đó vào trong phiên bản nâng cấp (Upgrade). Một phiên bản nâng cấp là một bản cài đặt phần mềm chính và có thể chứa các tính năng mới cũng như chứa cả các bản vá của phiên bản trước của sản phẩm này.

> ***LƯU Ý. Mục đích của kỳ thi****. Mục đích của kỳ thi 70-290 yêu cầu học viên có khả năng "quản trị một cơ sở hạ tầng cập nhật phần mềm "*

Khi sản phẩm phần mềm phát triển ngày càng phức tạp, số lượng của các sự cố trong chương trình cũng có xu hướng tăng theo và tương ứng là số lượng các bản vá lỗi. Một số sản phẩm, thông thường là các hệ điều hành, có thể có hàng tá các bản vá lỗi được phát hành giữa các lần nâng cấp. Việc cập nhật các chương trình và các hệ điều hành do đó thường làm tăng thêm các vấn đề khó giải quyết bởi một số lý do sau:

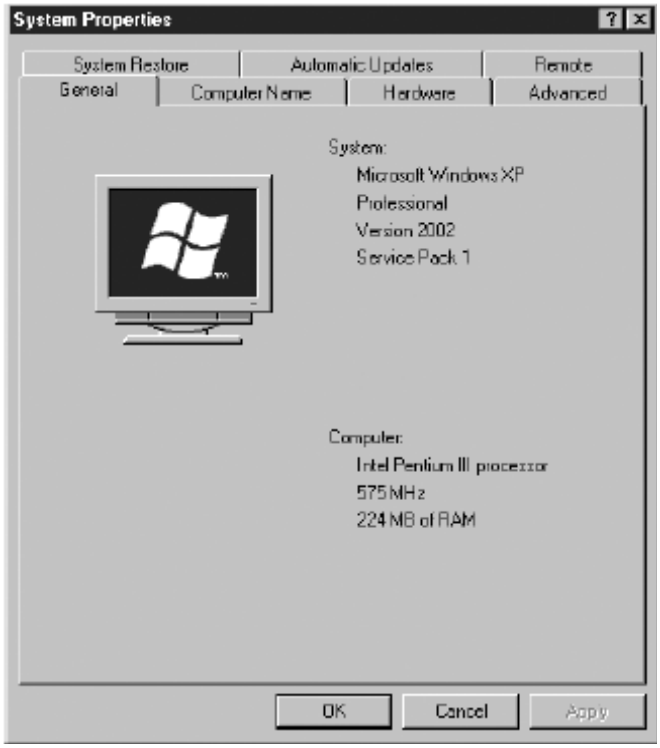
- **Số lượng các bản vá lỗi**. Khi một sản phẩm phần mềm có số lượng lớn các bản vá lỗi, nó sẽ trở nên khó khăn trong việc theo dõi xem các bản vá nào đã được áp dụng và phiên bản nào của file sản phẩm đang được sử dụng trong lần cài đặt nào.
- **Thứ tự của các bản vá**. Khi các bản vá được áp dụng theo các thứ tự khác nhau, kết quả là cấu hình phần mềm có thể thay đổi, điển hình là việc một sản phẩm có nhiều bản vá sẽ chứa các phiên bản khác nhau của cùng một file.

Các bản Service Pack

Khi đối mặt với hàng trăm các bản vá cho hệ điều hành hiện đại ngày nay, Microsoft quyết định lựa chọn sử dụng một phương pháp khác để phát hành các bản cập nhật này. Thay vì rất nhiều bản vá nhỏ, Microsoft tạo ra một bản cập nhật tạm thời lớn hơn dược gọi là ***service pack***. Một bản ***service pack*** là một tập hợp của các bản vá và các bản cập nhật khác đã từng được kiểm tra

và đóng gói lại thành một khối đơn lẻ. Một chương trình cài đặt đơn sẽ áp dụng tất cả các bản cập nhật cùng một lúc, thống nhất một cấu hình phần mềm cho mọi máy tính mà trên đó bản ***service pack*** được áp dụng.

Các bản ***service pack*** đơn giản quá trình cập nhật cho tất cả mọi người tham gia. Đối với Microsoft, phát hành các bản cập nhật trong một bản ***service pack*** có nghĩa là có thể kiểm tra toàn bộ gói phần mềm này thay cho việc phải kết hợp việc kiểm tra rất nhiều các bản vá khác nhau lại. Đối với người quản trị hệ thống và người dùng cuối, quá trình cài đặt sẽ được giảm bớt và chỉ cần chạy một chương trình đơn thay cho tiến hành cài đặt rất nhiều lần các bản vá riêng biệt. Đối với các nhân viên hỗ trợ kĩ thuật, quá trình giải quyết sự cố cũng đơn giản hơn bởi vì họ không gặp phải tình trạng một số lượng lớn các bản vá đã được cài đặt theo bất kỳ thứ tự nào. Dễ dàng xác định được bản ***service pack*** nào đã được cài đặt trên một máy tính Windows Server 2000, Windows XP hay Windows Server 2003 bằng cách nhìn vào thẻ ***General*** trong hộp thoại ***System Properties*** (Thể hiện trong Hình 5-1)



Hình 5-1. Hộp thoại *System Properties*

Các bản ***service pack*** của Microsoft được phát hành theo kiểu tích lũy dần, nghĩa là mọi bản ***service pack*** cho một sản phẩm nào đó đều chứa các bản cập nhật từ khi bản cài đặt chính gần nhất của sản phẩm đó được phát hành, bao gồm cả các bản ***service pack*** trước đó. Do đó, khi bạn tiến hành cài đặt

một hệ điều hành Windows hoặc một sản phẩm nào đó của Microsoft, bạn chỉ phải áp dụng bản ***service pack*** gần đây nhất.

Phát hành các bản service pack

Microsoft phát hành các bản ***service pack*** của hệ điều hành theo ba dạng:

- **CD-ROM**. Chúng ta có thể nhận được các bản ***service pack*** chứa trong CD-ROM trực tiếp từ Microsoft chỉ với chi phí danh nghĩa không đáng kể. Đĩa CD này có chứa các file cài đặt ***service pack*** và một chương trình cài đặt tên là ***Update.exe***. Đĩa này còn chứa các tài liệu của bản ***service pack***, các công cụ triển khai và các công cụ hỗ trợ cập nhật mà thông thường không có trong các bản cài đặt được tải về từ Internet.
- **Express Download (Bản rút gọn)**. Bản rút gọn chỉ chứa một số file cần thiết để bắt đầu quá trình tải bản ***service pack*** về. Khi bạn chạy chương trình cài đặt, phần mềm sẽ kiểm tra hệ thống, truy cập trang Web của Microsoft và tải các file cần thiết về để hoàn thành quá trình cập nhật. Bởi vì chương trình cài đặt kiểm tra xem bản ***service pack*** nào đã được cài đặt trong máy tính, nó có thể chỉ tải các file nó cần, điều này có thể làm giảm đáng kể kích thước tổng của các file cần tải về. Để chạy quá trình cài đặt rút gọn, máy tính phải có khả năng truy cập Internet.
- **Network Download (tải về từ mạng)**. Việc tải về từ mạng sẽ bao gồm toàn bộ bản ***service pack*** dưới dạng một file chạy đơn. Cách thức này sử dụng cho các quản trị mạng khi triển khai ***service pack*** trên một số lượng lớn máy tính. Khi bạn đã tiến hành tải xong, bạn có thể nạp file chạy và cài đặt ***service pack*** trên bất kỳ máy tính nào đang chạy hệ điều hành mà không cần thiết phải có khả năng truy cập Internet. Tuy nhiên bởi vì phiên bản này chứa tất cả các file ***service pack*** nên bản này có thể rất lớn, thông thường là 100MB hoặc hơn.

Cài đặt một lần.

Khi bạn cài đặt bản ***service pack*** trên máy tính chạy một trong các hệ điều hành Windows, chương trình cài đặt sẽ áp dụng chỉ các cập nhật cho các thành phần có trong hệ thống. Ví dụ, nếu bạn đã cài đặt ***Microsoft Internet Information Services*** (IIS) và ***Certificates Services*** trên máy tính chạy Windows Server 2003, việc cài đặt ***service pack*** sẽ chỉ áp dụng các bản cập nhật cho hai thành phần này mà không cập nhật cho các thành phần khác mà không được cài đặt trong hệ thống.

Một lúc nào đó, nếu bạn chỉnh sửa cấu hình phần cứng hoặc phần mềm trong một máy tính chạy Windows NT, bạn sẽ phải cài đặt lại bản ***service pack*** mới nhất để áp dụng phần mềm cập nhật cho các thành phần đã được cài đặt. Tuy nhiên, bắt đầu từ Windows Server 2000, điều này không còn cần thiết nữa. Chương trình cài đặt ***service pack*** ngày nay lưu vị trí của các file ***cabinet*** (.cab) chứa tất cả các trình điều khiển đã được cập nhật cho máy tính cũng như các file thông tin được gọi là ***Layout.inf***. Điều này để đảm bảo bất cứ khi nào bạn cài đặt lại các thành phần hệ điều hành mới, kể cả là các trình điều khiển thiết bị, một ứng dụng hay một dịch vụ, hệ thống sẽ sử dụng các phiên bản mới nhất của các file từ các bản ***service pack*** đã phát hành.

Các bản sửa lỗi nóng (Hotfix).

Mặc dù lịch trình của việc phát hành các bản ***service pack*** là dễ thay đổi, các bản cập nhật xuất hiện ngày càng ít đi, thường là không hơn một lần trong một năm. Mặc dù vậy, một điều cũng rất bình thường khi một hệ điều hành nẩy sinh ra các vấn đề mà yêu cầu cần phải chú ý ngay lập tức và không thể đợi đến khi phát hành bản ***service pack*** tiếp theo được. Đối với các trường hợp này, Microsoft phát hành các bản vá lỗi riêng rẽ, được gọi là hotfix (bản sửa lỗi nóng). Một **hotfix** là một phần mềm cập nhật mà giải quyết một lỗi đặc biệt nào đó. Giống như các bản ***service pack***, ***hotfix*** được phát hành như là một file chạy đơn và sẽ cài đặt bản vá lỗi trên máy tính mà nó chạy. Microsoft thường phát hành các bản ***hotfix*** kết hợp với một bài ***Knowledge Base*** (Kiến thức Cơ bản) giải thích cho sự cố này và các trường hợp mà người dùng hoặc quản trị mạng nên áp dụng bản cập nhật này.

> ***THÔNG TIN THÊM. Microsoft Knowledge Base. Microsoft Knowledge Base*** *là một thư viện của các bài viết cung cấp các thông tin hỗ trợ cho mọi sản phẩm Microsoft. Bạn có thể truy cập* ***Knowledge Base*** *tại địa chỉ http://support.microsoft.com.*

Không giống như các bản ***service pack***, mà Microsoft yêu cầu cài đặt trên mọi máy tính, các bản ***hotfix*** thường được áp dụng cho các máy tính bị một sự cố đặc biệt nào đó hoặc chạy một cấu hình phần cứng hoặc phần mềm đặc biệt. Bạn phải luôn luôn làm quen với chức năng của các bản ***hotfix*** và điều kiện để sử dụng trước khi cài đặt nó vào các máy tính.

Khi nào phải cập nhật

Câu hỏi khi nào phải áp dụng các bản ***service pack*** và ***hotfix*** là một vấn đề được tranh cãi nóng hổi giữa các quản trị mạng trong nhiều năm. Không phải tất cả các bản cập nhật phát hành đều có thể tin cậy được và một số

quản trị mạng rất khó tính trong việc áp dụng các bản ***service pack*** cho tới khi họ thấy được sự ổn định mà chúng mang lại. Trong thực tế, một số người dùng thích đợi đến bản ***service pack 3*** được phát hành trước khi họ cài đặt bản ***service pack 2***.

Sự cẩn trọng này đã từng được coi là thích hợp với thời gian trước, tuy nhiên bây giờ thì hoàn toàn không phải như vậy. Các bản ***service pack*** và ***hotfix*** được phát hành thường xuyên để giải quyết các vấn đề về bảo mật ví dụ các virus mới hoặc sâu máy tính khác, và việc triển khai các bản cập nhật này đúng lúc là điều rất quan trọng. Tuy nhiên, nói như thế không có nghĩa là nhất thiết mọi người dùng đều phải áp dụng tất cả các bản cập nhật này ngay lập tức sau khi nó được phát hành.

Đối với các máy tính đơn, trang Web ***Windows Update*** sẽ làm cho quá trình tải và áp dụng các bản cập nhật trở nên dễ dàng hơn và trong hầu hết các trường hợp, bạn có thể gỡ cài đặt các bản cập nhật của Microsoft khi cần. Do đó, hầu hết người dùng đều có thể áp dụng các bản cập nhật một cách an toàn ngay sau khi chúng được phát hành. Tuy nhiên trong một môi trường mạng lớn, quyết định bản cập nhật nào cần được cài đặt và khi nào phải cài đặt sẽ không thể tùy thuộc vào người dùng. Người quản trị mạng phải chịu trách nhiệm lấy các bản cập nhật về sau khi chúng được phát hành và triển khai chúng trong mạng của mình đúng lúc. Tuy nhiên người quản trị mạng không cần thiết phải cài đặt mọi bản cập nhật ngay lập tức sau khi nó được phát hành. Điều rất quan trọng là bạn phải kiểm tra các bản cập nhật này trước và đó là lý do tại sao một doanh nghiệp phải có các chính sách cập nhật được thiết lập trước trong hệ thống của mình.

Chính sách cập nhật phần mềm được thiết kế để hỗ trợ quản trị mạng trong việc tiến hành các tác vụ sau:

- **Duy trì khả năng nhận biết các bản cập nhật mới dược phát hành**. Microsoft thường xuyên phát hành các bản cập nhật mà có thể cần thiết áp dụng hoặc không trong hệ thống mạng của bạn. Quản trị mạng phải biết được các bản cập nhật mới khi chúng được phát hành và phải hiểu mỗi bản cập nhật đề cập và giải quyết những vấn đề gì.
- **Xác định máy tính nào cần phải cập nhật**. Trong một số trường hợp, một bản cập nhật có thể chỉ áp dụng cho các máy tính thực hiện một chức năng nhất định, sử dụng một ứng dụng hoặc tính năng đặc biệt nào đó, hoặc có một thành phần phần cứng đặc biệt. Các quản trị mạng phải hiểu được chức năng cụ thể của mỗi lần phát hành và xác định được máy tính nào cần bản cập nhật đó.

- **Kiểm tra các bản cập nhật phát hành trên các cấu hình máy tính khác nhau**. Một bản cập nhật phần mềm có thể gây ra sự trục trặc trong hoạt động của một máy tính đơn. Điều này có thể chỉ gây ra phiền phức cho chính máy tính này, tuy nhiên trong một hệ thống mạng lớn, nó có thể gây ra một thảm họa. Quản trị mạng phải tiến hành các biện pháp kiểm tra của riêng mình đối với các bản cập nhật trước khi triển khai chúng cho toàn hệ thống mạng.
- **Triển khai các bản cập nhật trên một mạng có qui mô lớn**. Việc cài đặt các bản cập nhật một cách thủ công trên hàng trăm máy tính yêu cầu rất nhiều thời gian, công sức và chi phí. Để triển khai các bản cập nhật trên một mạng lớn một cách hiệu quả, quá trình này phải được tự động hóa.

Microsoft cung cấp các công cụ hỗ trợ quản trị mạng hoàn thành các tác vụ này, ví dụ như các công cụ được trình bày trong các phần sau đây của chương trình.

Thử nghiệm các bản cập nhật bảo mật.

Trước khi bạn có thể cập nhật các bản cập nhật phần mềm trong mạng, bạn phải thử nghiệm chúng để đảm bảo chúng tương thích với các tất cả các cấu hình hệ thống của bạn. Số lượng và cách thức kiểm tra phụ thuộc vào nguồn gốc của các bản cập nhật và sự phức tạp của hệ thống mạng của bạn.

Đối với một bản cập nhật như một bản ***service pack***, việc thử nghiệm nên dược thực hiện rộng rãi. Bạn có thể nên tiến hành thử nghiệm bản phát hành này trong một mạng thí nghiệm độc lập với mạng đang vận hành trước, sau đó thực hiện triển khai thí điểm trong một phần của hệ thống mạng trước khi tiến hành việc triển khai đại trà. Đối với các bản cập nhật phụ và nhỏ, việc triển khai thí điểm có thể coi như là đã hoàn thành việc thử nghiệm và sau đó có thể triển khai đại trà luôn nếu như không có sự cố nào xảy ra.

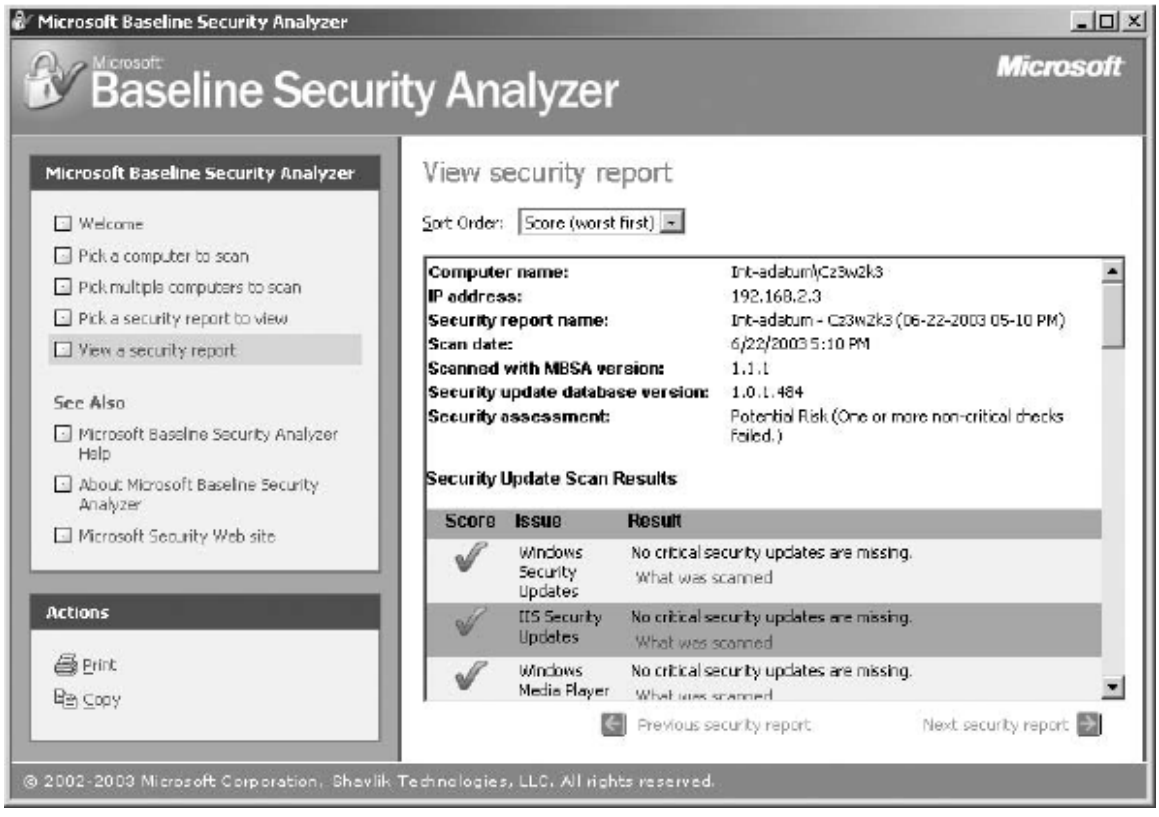
Gỡ cài đặt các bản Service pack

Khi bạn cài đặt một bản ***service pack***, chương trình cài đặt luôn cho phép bạn cơ hội để lưu các bản sao lưu dự phòng của các file hệ điều hành mà bản ***service pack*** này thay thế. Điều này cho phép bạn gỡ cài đặt bản ***service pack*** sau đó và khôi phục lại cấu hình nguyên gốc của hệ thống nếu cần thiết.

SỬ DỤNG MICROSOFT BASELINE SECURITY ANALYZER

Microsoft Baseline Security Analyzer (Trình phân tích ranh giới bảo mật của Microsoft - MBSA) là một công cụ đồ họa (Thể hiện trong Hình 5-2) có thể kiểm tra các lỗ hổng bảo mật thông thường trong một máy tính đơn hoặc nhiều máy tính chạy các phiên bản hệ điều hành Windows khác nhau. Các lỗ hổng thông thường là do việc cấu hình các tính năng bảo mật không chuẩn hoặc chưa hoàn chỉnh và việc cài đặt các bản cập nhật bảo mật là không được thực hiện hoàn hảo. Các lỗi bảo mật mà MBSA có thể phát hiện tra như sau:

- **Thiếu các bản cập nhật bảo mật**. Sử dụng một bản liệt kê các bản cập nhật đã phát hành từ máy chủ của Microsoft trên Internet hoặc từ một máy chủ ***Microsoft Software Update Services*** (SUS) nội bộ, MBSA xác định liệu các bản ***service pack*** và các bản cập nhật mà nó yêu cầu đã được cài đặt trong máy tính hay chưa và nếu chưa, nó sẽ soạn ra một danh sách các bản cập nhật cần thiết phải cài đặt.



Hình 5-2. Giao diện *Microsoft Baseline Security Analyzer*

> ***LƯU Ý. Hfnetchk.exe****. MBSA là chương trình thay thế tiện ích kiểm tra cập nhật trước kia của Microsoft có tên* ***Hfnetchk.exe****, tiện ích này thực hiện từ giao diện dòng lệnh và chỉ kiểm tra các bản cập nhật còn thiếu trong máy tính. MBSA bao gồm tất cả các tính năng của* ***Hfnetchk.exe****, bao gồm cả giao diện dòng lệnh, trong đó bạn có thể kích hoạt bằng cách chạy file chạy* ***Mbsacli.exe*** *với tham số* ***/hf****. Điều này cho phép người quản trị tiếp tục sử dụng các file bó (batch) và các kịch bản (script), kết hợp với dòng lệnh* ***Htnetchk.exe*** *với rất ít chỉnh sửa.*

- **Các điểm yếu của Tài khoản**. MBSA kiểm tra xem liệu tài khoản ***Guest*** có được kích hoạt trong máy tính hay không, liệu có nhiều hơn hai tài khoản có quyền ***Administrator***, liệu các người dùng ẩn danh (***anonymous***) có quá nhiều quyền truy cập đến các thông tin hệ thống hay không và liệu máy tính có sử dụng tính năng ***Autologon***.
- **Mật khẩu không hoàn chỉnh**. MBSA kiểm tra mật khẩu của các tài khoản máy tính để xem liệu chúng có cấu hình giới hạn thời gian hiệu lực của mật khẩu không, có là mật khẩu trống hoặc quá đơn giản không. Việc kiểm tra này không được thực hiện trên các máy chủ quản trị miền.
- **Các điểm yếu của hệ thống file**. MBSA kiểm tra xem liệu các ổ đĩa trên máy tính có sử dụng hệ thống file NTFS hay không.
- **Các điểm yếu của các ứng dụng IIS và SQL.** Nếu máy tính chạy dịch vụ IIS hay SQL, MBSA kiểm tra các ứng dụng này để xem có các điểm yếu bảo mật không.

Bên cạnh đó, MBSA còn hiển thị các thông tin khác về các vấn đề bảo mật trên máy tính, ví dụ như danh sách các chia sẻ trên mạng, số phiên bản của hệ điều hành Windows và liệu việc kiểm định (audit) có được kích hoạt hay không.

> ***LƯU Ý. Tải MBSA****. MBSA không đi kèm trong hệ điều hành Windows Server 2003, tuy nhiên nó lại có thể tải về miễn phí từ trang Web của Microsoft.*

MBSA là một công cụ thông tin mà có thể hiển thị các thông tin bảo mật của máy tính, tuy nhiên nó không thể thực hiện bất kể một hành động nào để giải quyết các điểm yếu dễ bị tấn công mà nó tìm thấy. Bạn có thể sử dụng MBSA để xác định xem bản cập nhật bảo mật nào cần thiết để cài đặt trên các máy tính nhất định, tuy nhiên để xây dựng một chính sách cập nhật hiệu

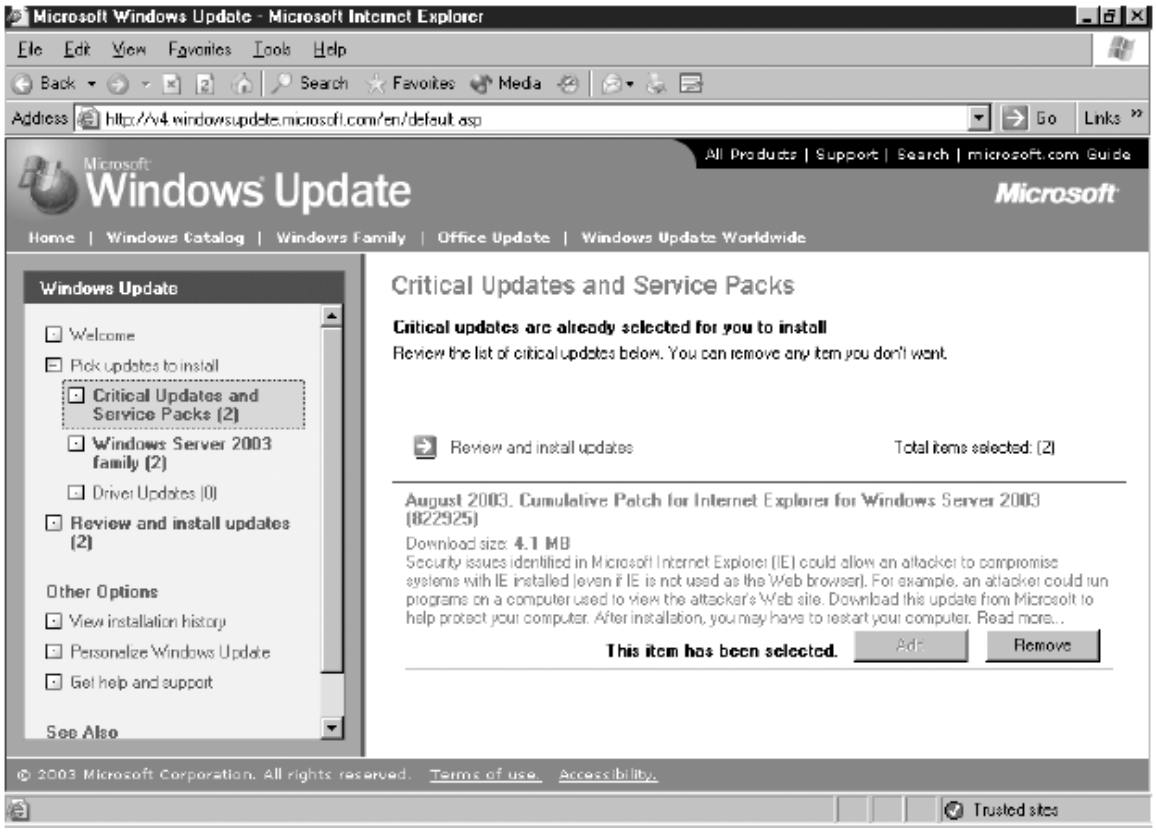
quả, bạn phải triển khai hệ thống theo dõi xem các bản cập nhật nào đã được cài đặt trên các máy tính trong doanh nghiệp.

SỬ DỤNG WINDOWS UPDATE

Windows Update là một ***Web site***, do Microsoft duy trì, cho phép các máy tính chạy Windows Server 2003 và hầu hết các phiên bản khác của Microsoft Windows có thể định vị và tải các bản cập nhật và bản vá lỗi mới nhất của hệ điều hành và các trình điều khiển. Khi bạn truy cập ***site Windows Update*** bằng cách nhấn vào ***Start***, trỏ vào ***All Program*** và lựa chọn ***Windows Update***, hoặc bằng cách sử dụng địa chỉ URL ***http://windowsupdate.microsoft.com***, máy tính sẽ tải một ứng dụng kiểm tra cấu hình hiện tại của máy tính của bạn và liệt kê ra một danh sách các bản cập nhật và bản vá lỗi mà hệ thống có thể cần (Thể hiện trong Hình 5-3), trong các mục sau đây:

- Các bản cập nhật và ***service pack*** mang tính quan trọng mấu chốt
- Các bản cập nhật cho các phiên bản nhất định của Windows
- Các bản cập nhật trình điều khiển

Người dùng có thể lựa chọn từ một danh sách các cập nhật, tải chúng và cài đặt tất cả cùng lúc, do đó sẽ đơn giản hóa quá trình bảo dưỡng.



Hình 5-3. Giao diện Web của *Windows Update*

Đối với người dùng đơn lẻ sử dụng máy tính gia đình, ***Website Windows Update*** là phương thức hữu hiệu nhất để giữ cho máy tính của bạn được cập nhật, tuy nhiên sẽ là không phù hợp khi sử dụng trong hệ thống mạng, do các lý do sau:

- **Băng thông**. Mỗi khi một máy tính nhận một bản cập nhật phát hành bằng ***Windows Update***, nó tải phần mềm từ máy chủ Microsoft trên Internet. Trong một hệ thống mạng lớn, điều này có nghĩa hàng trăm máy tính sẽ cùng tải các file giống nhau. Đối với các bản cập nhật nhỏ, điều này có thể không có vấn đề gì, tuy nhiên các bản ***service pack*** của Windows thường lớn hơn 100MB và việc tải các file giống nhau cho mỗi máy tính sẽ gây ra sự chiếm dụng một lượng lớn băng thông kết nối Internet của mạng.
- **Kiểm thử**. Mặc dù Microsoft đã thử nghiệm các bản cập nhật cẩn thận trước khi phát hành chúng nhưng họ không thể kiểm tra kết hợp tất cả các kiểu thiết lập cấu hình và các sản phẩm phần mềm được. Do đó, một bản cập nhật cá biệt nào đó có thể gây ra sự cố cho một số máy tính trong hệ thống mạng của bạn. Hơn nữa, đối với một máy tính đơn, đều này có thể không phải là vấn đề lớn, tuy nhiên nếu bản

cập nhật này gây ra sự cố trên tất cả các máy tính trong mạng, thiệt hại về năng suất và gánh nặng cho các nhân viên hỗ trợ kĩ thuật có thể là rất lớn.

> ***LƯU Ý. Windows Update và Software Update Service****. Hạn chế liệt kê ở đây khi sử dụng* ***Windows Update*** *giả định rằng máy tính được cấu hình để truy cập* ***Web site Windows Update*** *trên Internet. Tuy nhiên, cũng có thể cấu hình* ***Windows Update*** *để truy cập đến các bản cập nhật phần mềm này từ một máy chủ SUS trong mạng nội bộ. Việc làm này sẽ giảm thiểu các vấn đề về sử dụng băng thông và vấn đề thử nghiệm. Bạn có thể học thêm về SUS trong phần sau của chương này.*

Sử dụng Automatic Update.

Mặc dù bạn luôn luôn có thể truy cập ***Web site*** một cách thủ công bằng cách sử dụng ***Internet Explorer***, bạn còn có thể cấu hình Windows Server 2003 để tải tự động và cài đặt các bản cập nhật phần mềm ngay sau khi chúng được phát hành. Tính năng này được gọi là ***Automatic Updates*** (Tự động cập nhật) và nó có sẵn trong Windows Server 2003, Windows XP đã cài đặt ***service pack 1*** và trong Windows Server 2000 đã cài đặt ***service pack 3***.

> ***LƯU Ý. Cập nhật bằng Automatic Update****. Đối với các máy trạm chạy các hệ điều hành trước đây nhưng có hỗ trợ khả năng cập nhật, bạn có thể tải* ***Automatic Update*** *như là một phần mềm cho máy trạm từ trang Web* ***Microsoft SUS*** *tại địa chỉ* ***http://go.microsoft.com/fwlink/?LinkID=6930.***

Theo mặc định, ứng dụng ***Automatic Update*** trong Windows Server 2003 được cấu hình để kết nối tự động đến một máy chủ ***Windows Update***, tải các bản cập nhật và sau đó nhắc người dùng cài đặt chúng. Bạn có thể chỉnh sửa cách hoạt động mặc định này bằng cách mở hộp thoại ***System Properties*** từ ***Control Panel*** và lựa chọn thẻ ***Automatic Update*** (thể hiện trong Hình 5-4), hoặc bằng cách chạy trình hướng dẫn cài đặt ***Automatic Updates Setup Wizard*** (Trình Hướng dẫn Cài đặt Cập nhật Tự động) bằng cách nhấn vào biểu tượng ***Stay Current With Automatic Updates*** trên khay tác vụ. Bạn còn có thể cấu hình ***Automatic Update*** bằng cách sử dụng đối tượng chính sách nhóm GPO, như mô tả trong mục "***Configuring Automatic Updates***" ở phần sau của chương này.

Hình 5-4: Thẻ *Automatic Updates* trong hộp thoại *System Properties*

Khi bạn cấu hình ***Automatic Update***, bạn có thể lựa chọn một trong ba lựa chọn sau đây:

- **Notify Me Before Downloading Any Updates And Notify Me Again Before Installing Them On My Computer (Thông báo cho tôi trước khi tải bất kỳ bản cập nhật nào và thông báo cho tôi lần nữa trước khi cài đặt chúng trên máy tính)**. Khi các bản cập nhật đã sẵn sàng, máy tính sẽ tạo ra một mục trong nhật ký Hệ thống (mà bạn có thể truy cập bằng Event Viewer) và thông báo cho quản trị hệ thống bằng một hình quả bóng bay trong khay tác vụ
- **Download The Updates Automatically And Notify Me When They Are Ready To Be Installed (Tải các bản cập nhật tự động và thông báo cho tôi khi chúng đã sẵn sàng để cài đặt)**. Máy tính sẽ tải tự động các bản cập nhật từ Web site ***Windows Update*** ngay khi chúng được phát hành, sử dụng dịch vụ ***Background Intelligent Transfer Service*** (BITS – *Dịch vụ Vận chuyển Thông minh Dưới nền*) để tiến hành việc truyền file khi băng thông mạng rỗi rãi. BITS đảm bảo rằng hiệu năng hệ thống không bị ảnh hưởng bởi việc truyền file. Phần mềm máy khách ***Automatic Update*** sẽ xác nhận chữ ký số của Microsoft trên các file được tải, Thực hiện việc xác nhận CRC (Cyclical Redundancy Check – *một bit đặc biệt trong mỗi gói tin được*

gửi, đảm bảo cho gói tin là nguyên vẹn trong suốt quá trình vận chuyển) trên mỗi gói cài đặt và thông báo quản trị mạng về sự hiện diện của chúng bằng cách ghi một mục vào nhật ký Hệ thống và hiển thị một hình quả bóng trên khay tác vụ. Người quản trị sau đó sẽ lựa chọn các bản cập nhật để cài đặt từ danh sách các bản đã tải về được.

- **Automatically Download The Updates, And Install Them On The Schedule That I Specify (Tải tự động các bản cập nhật và cài đặt chúng theo lịch mà tôi đã chỉ định).** Máy tính sẽ tải các bản cập nhật từ ***site Windows Update*** ngay khi chúng được phát hành, sử dụng BITS, và cài đặt chúng theo thời gian xác định hàng ngày hoặc hàng tuần. Nếu người quản trị mạng đăng nhập vào máy tính tại thời điểm trong lịch, một thông báo hiển thị số đếm ngược hiện ra trước khi cài đặt và người quản trị mạng có thể lựa chọn lùi việc cài đặt đến thời điểm tiếp theo trong lịch. Nếu một người dùng không phải là quản trị mạng đăng nhập vào, một hộp thoại cảnh báo xuất hiện nhưng người dùng không thể lùi việc cài đặt. Nếu không có người dùng nào đăng nhập vào, việc cài đặt sẽ được thực hiện tự động. Nếu các bản cài đặt cập nhật yêu cầu hệ thống khởi động, một thông báo với bộ đếm lùi năm phút xuất hiện, thông báo người dùng về việc khởi động sắp xảy ra. Chỉ có người quản trị mạng mới có thể hủy bỏ việc khởi động này.

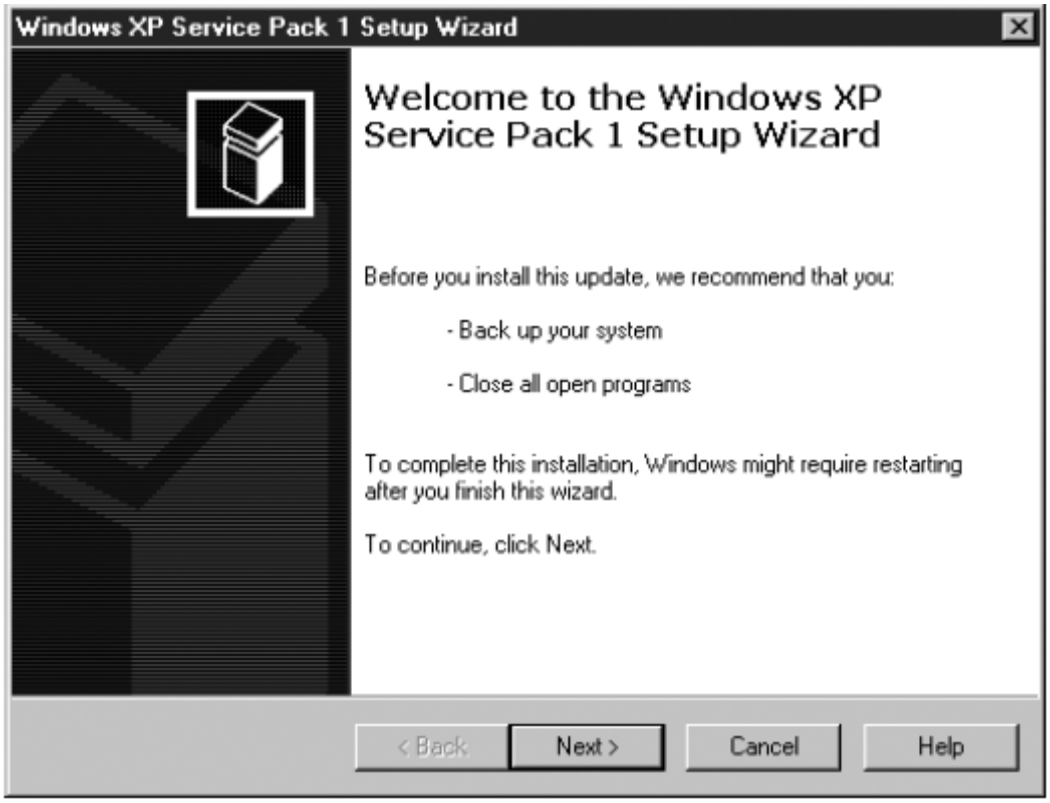
TRIỂN KHAI CÁC BẢN CẬP NHẬT TRONG HỆ THỐNG MẠNG

Một người quản trị mạng khi quyết định rằng người dùng không phải tải các bản cập nhật hệ điều hành từ Internet có thể sử dụng rất nhiều phương pháp khác nhau để chuyển các bản cập nhật này đến từng máy tính trong mạng, như mô tả trong các phần sau:

Cài đặt các bản service pack thủ công.

Khi bạn mua một đĩa CD chứa các bản service pack, bạn sẽ nhận được một đĩa có tất cả các file của bản service pack trong một định dạng mở rộng. Để cài đặt bản service pack này, bạn chạy chương trình Update.exe trong folder Update. Việc này sẽ nạp trình cài đặt Service Pack Setup Wizard (Thể hiện trong Hình 5-5), trình này sẽ hướng dẫn bạn qua các bước để cài đặt bản service pack. Sau khi bạn đồng ý thỏa thuận giấy phép cho người dùng cuối bổ sung, trình cài đặt này sẽ nhắc bạn để bạn chỉ định rằng liệu bạn có muốn tạo ra các bản sao lâu dài của các file mà service pack thay thế để bạn có thể

gỡ cài đặt bản service pack này sau đó nếu cần. Sau khi quá trình cài đặt hoàn thành, bạn sẽ được nhắc nhở để khởi động máy tính.



Hình 5-5: ***Windows XP Service Pack 1 Setup Wizard***

Khi bạn tải về phiên bản trên mạng (***Network version***) của một bản ***service pack***, bạn sẽ nhận được một file chạy nén đơn (*File chạy có thể tự giải nén*) với tên file cho biết hệ điều hành mà bản cập nhật này áp dụng và số phát hành của bản ***service pack*** này. Ví dụ, file chạy của ***Windows XP service pack 1*** là ***Xpsp1.exe***. Khi bạn chạy file này, máy tính sẽ bung tất cả các file trong file nén này, ghi chúng vào folder tạm trong ổ đĩa hệ thống, sau đó chạy file ***Update.exe*** và quá trình cài đặt sẽ giống như là cài đặt từ phiên bản trên CD. Bạn có thể đặt file này lên một folder chia sẻ trên mạng và có thể chạy file đó từ bất kỳ máy tính nào trong mạng. Chương trình chạy này luôn sao chép các file cài đặt vào ổ cứng cục bộ và chạy chương trình cài đặt từ folder đó. File ***Update.exe*** trong bản ***service pack*** và file chạy tải từ mạng cũng hỗ trợ khả năng sử dụng các khóa chuyển dòng lệnh mà bạn có thể sử dụng để tác động đến quá trình cài đặt. Bạn có thể chạy file chạy này với các khóa chuyển sau đây từ một dấu nhắc dòng lệnh hoặc từ hộp thoại ***Run***. Các khóa chuyển, giống nhau đối với cả file ***Update.exe*** và file chạy nén đơn, có các tham số như sau:

- **/D:Tên folder**. Theo mặc định, chương trình cài đặt sẽ tạo ra các bản sao lưu của tất cả các file mà nó bị ghi đè trong folder gọi là ***$ntservicepackuninstall$***. Khóa chuyển này cho phép bạn chỉ định một tên folder khác để chứa các file sao lưu.
- **/F**. Chương trình cài đặt sẽ đóng tất cả các chương trình đang mở mà không lưu các dữ liệu khi nó khởi động máy tính sau khi quá trình cài đặt hoàn thành.
- **/L**.hiển thị một danh sách các ***hotfix*** đã được cài đặt trong máy tính
- **/N** Không cho chương trình cài đặt tạo ra các bản sao lưu của các file bị ghi đè trong quá trình cài đặt
- **/O** Chương trình cài đặt sẽ ghi đè các file thông tin về nhà sản xuất thiết bị gốc (OEM) trong quá trình cài đặt mà không thông báo với người dùng.
- **/Q**. Chạy chương trình cài đặt trong chế độ không hiển thị. Trong chế độ này, chương trình cài đặt sử dung các giá trị mặc định cho các lựa chọn, tuy nhiên không hiển thị thanh tiến trình hoặc bất kỳ thông báo lỗi nào.
- **/S:Tên folder**. Kết hợp các file ***service pack*** với các file cài đặt của hệ điều hành để tạo ra một bộ cài đặt tích hợp. Quá trình này còn được gọi là ***slipstreaming***. Tên folder là folder mà bạn chỉ định là đường dẫn đến folder chứa các file cài đặt của hệ điều hành.
- **/U**. Quá trình cài đặt sẽ được thực hiện trong chế độ không cần giám sát. Trong chế độ này, chương trình cài đặt sử dụng các giá trị mặc định cho mọi lựa chọn và hiển thị thanh tiến trình, tuy nhiên chỉ các thông báo lỗi nghiêm trọng mới làm dừng quá trình cài đặt này được.
- **/X** Việc nạp file chạy của ***service pack*** sẽ bung các file trong nó và lưu chúng trong một cấu trúc thư mục ***i386*** trên đĩa cứng mà không chạy file ***Update.exe***.
- **/X:Tên folder.** Việc nạp file chạy của service pack sẽ bung các file trong nó và lưu chúng trong folder mà bạn chỉ định trên đĩa cứng mà không chạy file Update.exe.
- **/Z.** Không cho quá trình cài đặt khởi động lại máy tính sau khi việc cài đặt hoàn thành. Lựa chọn này được sử dụng thường xuyên khi bạn có kế hoạch cài đặt các ***hotfix*** ngay sau khi cài ***service pack*** và muốn hoãn việc khởi động lại cho tới khi hoàn thành việc cài đặt ***hotfix***.

Cài đặt thủ công các hotfix

Cũng giống như các bản ***service pack***, người dùng có thể tải và cài đặt các bản ***hotfix*** thông qua trang Web ***Windows Update***, tuy nhiên ta cũng có thể tải chúng như các file chạy riêng rẽ. Điều này cho phép các quản trị mạng triển khai các bản ***hotfix*** cho một lượng lớn các máy tính mà không cần phải tiến hành tải nhiều lần từ Internet. Một file ***hotfix*** là một file chạy nén, giống như file tải trên mạng của ***service pack***, nhưng có dung lượng nhỏ hơn. Tên của file này sử dụng định dạng sau đây:

OperatingSystem-KBKnowledgeBase#-Platform-Language.exe (*Hệ điều hành-KB+"số hiệu bài viết về vấn đề bản hotfix sẽ chỉnh sửa"-"loại CPU"-"ngôn ngữ"*)

Ví dụ, một bản cập nhật bảo mật điển hình cho Windows Server 2003 tên là ***WindowsServer2003-KB823980-x86-ENU.exe***. Số 823980 là số của bài viết trong ***Knowledge Base*** mô tả vấn đề mà bản ***hotfix*** này giải quyết được, ***x86*** là nền tảng bộ vi xử lý mà bản ***hotfix*** này áp dụng và ***ENU*** cho biết bản ***hotfix*** này cho phiên bản U.S English của Windows Server 2003.

> ***LƯU Ý. Thay thế các file của hotfix****. Không giống như* ***service pack****, các* ***hotfix*** *chỉ cập nhật phần mềm mà thực tế đã cài đặt trong máy tính khi bạn chạy chương trình cài đặt này. Nếu bạn hủy bỏ một thành phần hệ điều hành và sau đó cài đặt lại thành phần đó, bạn phải đồng thời cài đặt lại các bản* ***hotfix*** *mà áp dụng cho thành phần này.*

Việc nạp file chạy của ***hotfix*** sẽ bung các file trong nó ra một folder tạm trên hệ thống nội bộ và chạy file chương trình ***Update.exe***, cũng giống như trong ***service pack***. Các ***hotfix*** theo mặc định luôn luôn tạo ra các bản sao chép để sao lưu của các file bị ghi đè để bạn có thể gỡ bỏ cài đặt. Lưu chúng trong một folder ẩn trong folder gốc hệ thống và có tên ***$NtUninstallKB######$***, trong đó ###### là số của bài viết trong ***Knowledge Base*** của bản ***hotfix*** đó.

Để thay đổi các hành xử mặc định của chương trình cài đặt của ***hotfix***, bạn có thể chạy file này với bất kỳ trong các khóa chuyển sau đây:

- **/F.** Chương trình cài đặt sẽ đóng tất cả các ứng dụng đang mở mà không lưu dữ liệu khi nó khởi động máy tính sau khi quá trình cài đặt hoàn thành.
- **/L** Hiển thị danh sách các bản ***hotfix*** cài đặt trong máy tính
- **/N** Không cho phép quá trình cài đặt tạo các bản sao chép để sao lưu các file bị ghi đè trong quá trình cài đặt.

- **/Q**. Chạy chương trình cài đặt trong chế độ không hiển thị. trong chế độ này, chương trình cài đặt sử dung các giá trị mặc định cho các lựa chọn, tuy nhiên không hiển thị thanh tiến trình hoặc bất kỳ thông báo lỗi nào.
- **/U.** Quá trình cài đặt sẽ được thực hiện trong chế độ không cần giám sát. Trong chế độ này, chương trình cài đặt sử dụng các giá trị mặc định cho mọi lựa chọn và hiển thị thanh tiến trình, tuy nhiên chỉ các thông báo lỗi nghiêm trọng mới làm dừng quá trình cài đặt này được.
- **/X** Việc nạp file chạy của ***service pack*** sẽ bung các file trong nó và lưu chúng trong một cấu trúc thư mục trên đĩa cứng mà không chạy file ***Update.exe.***
- **/Z.** Không cho phép quá trình cài đặt khởi động máy tính sau khi việc cài đặt hoàn thành.

  LƯU Ý. Kiểm tra các hotfix*. Khi bạn cài đặt các bản* ***hotfix****, chương trình cài đặt luôn luôn kiểm tra xem bản* ***service pack*** *nào đã từng được cài đặt trong máy tính. Nếu bản* ***hotfix*** *bạn đang cài đặt là cũ hơn bản* ***service pack*** *hiện tại đang có trong máy tính, quá trình cài đặt sẽ bị dừng bởi vì bản* ***hotfix*** *luôn được áp dụng như là một phần của bản* ***service pack****. Nếu bản hotfix là mới hơn bản* ***service pack*** *hiện tại trong máy tính, quá trình cài đặt sẽ được thực hiện.*

Xâu chuỗi các hotfix.

Bắt đầu từ bản ***Windows Server 2000 service pack 3***, mọi ***hotfix*** đều có một chương trình gọi là ***Qchain.exe*** cho phép cài đặt rất nhiều ***hotfix***, bản này ngay sau bản kia mà không cần phải khởi động lại máy tính sau mỗi lần cài đặt. Nếu bạn cài đặt nhiều ***hotfix*** mà bao gồm các phiên bản khác nhau của cùng một file, ***Qchain.exe*** đảm bảo rằng hệ thống sẽ sử dụng đúng phiên bản chuẩn nhất của các file sau khi quá trình cài đặt hoàn thành.

Để xâu chuỗi các quá trình cài đặt các bản ***hotfix***, bạn có thể chạy các chương trình cài đặt ***hotfix*** với khóa chuyển dòng lệnh ***/Z***, điều này sẽ ngăn cản các chương trình này khởi động máy tính. Tuy nhiên, bạn phải nhớ khởi động máy tính sau khi bản ***hotfix*** cuối cùng được cài đặt để các bản ***hotfix*** này có tác dụng. Để tự động quá trình cài đặt các bản ***hotfix*** này, bạn có thể tạo ra một file bó (***batch***) giống như sau đây:

WindowsServer2003-KB8239809-x86-ENU.exe /Z /U

WindowsServer2003-KB8239810-x86-ENU.exe /Z /U

WindowsServer2003-KB8239811-x86-ENU.exe /U

Lưu ý rằng lệnh cài đặt 2 ***hotfix*** đầu tiên trong file bó nói trên bao gồm khóa chuyển ***/Z***, ngăn không cho khởi động hệ thống trong khi dòng lệnh cuối lại không có khóa chuyển này để máy tính có thể khởi động lại sau khi tất cả các ***hotfix*** đã được cài đặt xong. Cả ba dòng lệnh này đều có khóa chuyển /U, khóa này không cho phép chương trình tạm dừng để nhận thông tin nhập vào của người dùng.

Bạn có thể tích hợp một quá trình cài đặt ***service pack*** trong một file bó, điều này sẽ cho phép tự động hóa toàn bộ quá trình cập nhật như sau:

Update.exe /Z /U

WindowsServer2003-KB8239809-x86-ENU.exe /Z /U

WindowsServer2003-KB8239810-x86-ENU.exe /Z /U

WindowsServer2003-KB8239811-x86-ENU.exe /U

Thực hiện Slip streaming

Khi bạn cài đặt một máy tính mới trong mạng, việc cài đặt hệ điều hành không hẳn đã là quá trình cuối cùng. Bạn còn có thể phải cài đặt thêm các bản ***service pack*** và rất nhiều ***hotfix***. Ngay cả khi có thể cài đặt các thành phần này một cách riêng rẽ, người ta thường chọn một phương pháp hiệu quả hơn là phương pháp tích hợp các bản ***service pack*** và ***hotfix*** này trong quá trình cài đặt hệ điều hành. Quá trình này được gọi là ***Slipstreaming*** (*Kết hợp liền mạch các quá trình*)

Slipstreaming một bản service pack

Để ***Slipstreaming*** một bản ***service pack*** trong quá trình cài đặt hệ điều hành Windows Server 2003, đầu tiên bạn phải tạo ra một folder phân phối trên một folder chia sẻ trên mạng và sao chép folder I386 trong đĩa CD cài đặt Windows Server 2003 vào folder này. Sau đó, từ folder chứa file chương trình cài đặt ***service pack***, bạn nạp file ***Update.exe*** hoặc file chạy cài đặt với khóa chuyển ***/S***, chỉ định vị trí của folder phân phối mà bạn đã tạo ra như trong ví dụ sau đây:

Update.exe /s:distfolder

W2k3sp1.exe /s:distfolder

Chương trình cài đặt sẽ bung các file của ***service pack*** từ file chạy sang một folder tạm (nếu cần) và sau đó sao chép các file đó vào vị trí tương ứng trong folder phân phối. Sau đó bạn có thể bắt đầu quá trình cài đặt hệ điều

hành từ folder phân phối này và các file ***service pack*** sẽ được cài đặt đồng thời trong cùng thời điểm này.

Sử dụng các chính sách nhóm

Phương pháp khác để tự động hóa quá trình cài đặt ***service pack*** là sử dụng kết hợp ***Windows Installer*** (Trình cài đặt Windows) và chính sách ***Software Installation*** (Cài đặt phần mềm) trong một GPO. ***Windows Installer*** là một chương trình cài đặt phần mềm mà được lưu như là một file ***Windows Installer Packet*** (Gói phần mềm cài đặt Windows) với phần mở rộng ***.msi***. Các bản ***service pack*** được phát hành đều bao gồm một phiên bản ***Windows Installer Packet*** của chương trình cài đặt gọi là ***Update.msi***. ***Update.msi*** nằm trong folder ***Update*** trên đĩa CD ***service pack***. Nếu bạn đã tải phiên bản trên mạng của ***service pack***, bạn phải bung các file trong nó ra bằng cách chạy file này với khóa chuyển ***/X*** trước khi bạn có thể sử dụng ***Update.msi***.

Để triển khai một bản ***service pack*** bằng cách sử dụng file ***Update.msi*** và chính sách nhóm, bạn phải lựa chọn một đối tượng trong ***Active Directory*** có chứa các máy tính mà bạn muốn cập nhật. Nếu tất cả máy tính trong hệ thống mạng của bạn đều chạy cùng một phiên bản Windows, bạn có thể cấu hình chính sách ***Software Installation*** trong ***GPO*** mặc định của miền và gắn với các đối tượng trong miền sử dụng ***Active Directory*** của bạn. Nếu bạn có các máy tính chạy nhiều phiên bản hệ điều hành khác nhau, bạn có thể tạo ra các đối tượng OU cho mỗi phiên bản và sau đó tạo ra một ***GPO*** chứa các bản ***Windows Installer Package*** tương ứng vào trong mỗi ***OU*** này, hoặc bạn có thể tạo ra nhiều ***Windows Installer Package*** trong ***GPO*** miền mặc định và sử dụng việc gán các Cấp phép để chỉ định máy tính nào sẽ nhận được các gói phần mềm này.

> ***THÔNG TIN THÊM. Sử dụng chính sách nhóm GPO***. *Để có thêm thông tin về việc sử dụng đối tượng chính sách nhóm, xem khóa học cho kỳ thi 70-294 "Lập kế hoạch, triển khai và duy trì một cơ sở hạ tầng dựa trên **Windows Server 2003 Active Directory**"*

Thêm Windows Installer Package

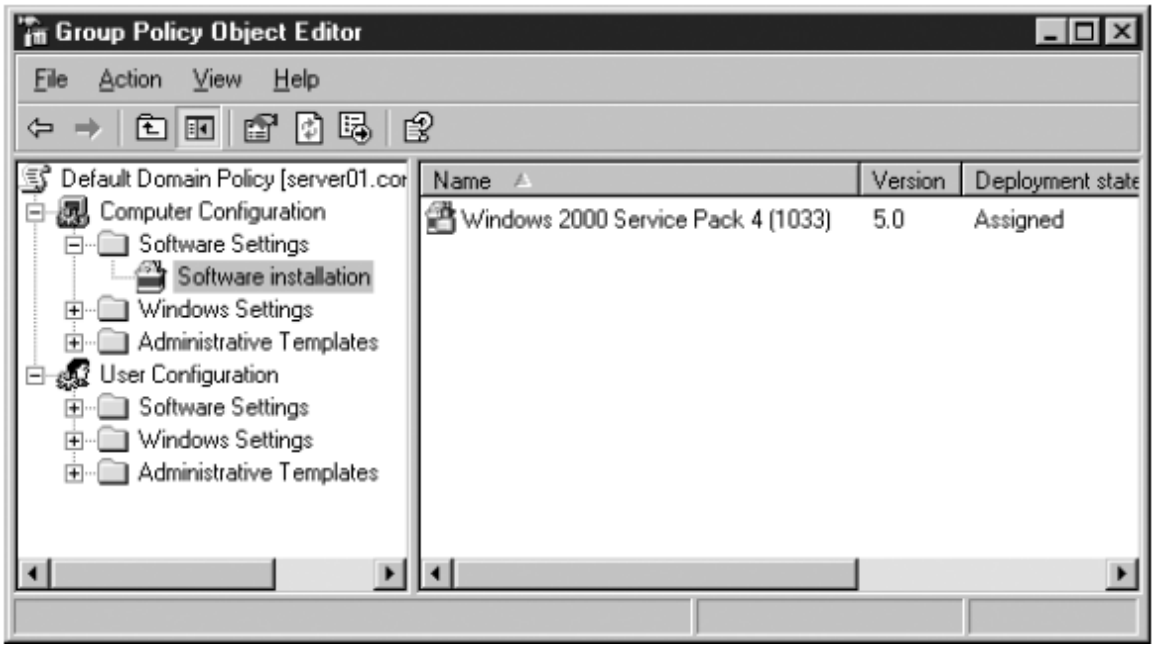
Để thêm một ***Windows Installer Package*** (Gói phần mềm cài đặt Windows) vào trong chính sách nhóm ***GPO*** mặc định của miền, sử dụng các thao tác sau đây:

1. Đăng nhập vào máy tính Windows Server 2003 bằng tài khoản ***Administrator***

2. Bung các file trong file nén ***service pack*** vào một folder trong một chia sẻ trên mạng
3. Nhấn ***Start***, trỏ vào ***administrative Tools*** và nhấn vào ***Active Directory Users And Computers***. Bảng điều khiển ***Active Directory Users And Computers*** xuất hiện
4. Lựa chọn biểu tượng miền trong khung Phạm vi và từ thực đơn ***Action***, lựa chọn ***Properties***. Hộp thoại ***Properties*** của đối tượng miền của bạn xuất hiện
5. Lựa chọn thẻ ***Group Policy*** và sau đó nhấn ***Edit***. Bảng điều khiển ***Group Policy Object Editor*** xuất hiện
6. Trong khung Phạm vi, mở rộng folder ***Computer Configuration/Software Settings*** và lựa chọn biểu tượng ***Software Installation***

   Mục ***User Configuration*** cũng có một folder ***Software Settings*** và một biểu tượng ***Software Installation***, tuy nhiên bạn không thể sử dụng chúng để cài đặt một ***service pack***. Bạn phải sử dụng mục ***Computer Configuration***
7. Trong thực đơn ***Action***, trỏ vào ***New*** và lựa chọn ***Package***. Một hộp thoại ***Open*** xuất hiện
8. Nhập vào đường dẫn đầy đủ của file ***Windows Installation Package Update.msi*** trong folder con ***Update*** của folder chia sẻ của bạn. Một hộp thoại ***Deploy Software*** xuất hiện.

   Hãy chắc chắn rằng đang bạn sử dụng tên ***Universal Naming Convention (UNC)*** của đường dẫn đến file đóng gói, chứ không phải bằng các ký tự ổ đĩa. Ví dụ, bạn có thể sử dụng \\Server01\d$\sp1\i386\update\update.msi nhưng không thể là ***D:\sp1\i386 \update\update.msi.***
9. Nhấn vào ***OK*** để chấp nhận lựa chọn mặc định ***Assigned***. Gói phần mềm cài đặt của bản ***service pack*** xuất hiện trong khung Chi tiết (Thể hiện trong hình 5-6).



Hình 5-6. Bảng điều khiển *Group Policy Object Editor* với một gói cài đặt *service pack*

Lần khởi động sau của các máy tính trong miền, hệ thống sẽ tải file cài đặt ***service pack*** từ folder chia sẻ nói trên để cài đặt chúng.

SỬ DỤNG MICROSOFT SOFTWARE UPDATE SERVICES - SUS (DỊCH VỤ CẬP NHẬT PHẦN MỀM CỦA MICROSOFT)

Việc triển khai bất kỳ phần mềm nào trong một hệ thống mạng lớn là một nhiệm vụ phức tạp, và các bản cập nhật hệ điều hành cũng không là một ngoại lệ. Những tác vụ được coi là đơn giản trong một máy tính đơn sẽ là vấn đề lớn khi bạn có hàng trăm hoặc hàng ngàn máy tính. **SUS** là một sản phẩm miễn phí, nó thông báo cho người quản trị mạng khi một bản cập nhật bảo mật mới xuất hiện, tải bản cập nhật đó và triển khai chúng đến các máy tính trên mạng (thể hiện trên hình 5-7)

Hình 5-7. Giao diện quản trị SUS

> ***THÔNG TIN THÊM. Sử dụng SUS***. ***SUS*** *có* ***service pack 1*** *không có sẵn trong Windows Server 2003 hoặc bất kì hệ điều hành Windows nào nhưng nó có thể được tải miễn phí từ trang Web của Microsoft tại địa chỉ: http:// www.microsoft.com/windowsserversystems/SUS/default.mspx.*

Như đã đề cập ở phần trên của chương, việc người dùng tự tải và cài đặt các bản cập nhật hệ điều hành bằng cách sử dụng Web Site ***Windows Update*** là lãng phí thời gian và băng thông. SUS về bản chất là một phiên bản ***intranet*** của Web Site ***Windows Update***, cho phép giảm thiểu nhu cầu tải bản cập nhật cho phần mềm cho mỗi máy tính từ Internet và giúp người quản trị không phải triển khai các bản cập nhật một cách thủ công trên các máy tính. Người quản trị có thể điều khiển bản cập nhật nào áp dụng vào các máy tính trên mạng và khi nào thì quá trình này xảy ra, cho phép tự động hóa quá trình này do đó việc cập nhật có thể hoàn thành mà người dùng không hề hay biết

SUS bao gồm các thành phần sau đây:

- **Máy chủ đồng bộ**. Một máy tính chạy SUS, đóng vai trò như một máy chủ đồng bộ, sẽ tải các bản cập nhật phần mềm từ Web Site ***Windows Update*** ngay sau khi chúng được phát hành. Người quản trị có thể cho phép việc tải này diễn ra nếu cần, lập lịch cho chúng diễn ra tại các thời điểm xác định (ví dụ như thời điểm hết giờ làm việc) hoặc có thể kích hoạt việc này một cách thủ công. Khi mà máy chủ

SUS tải các bản cập nhật, nó lưu chúng trên máy chủ. Điều này giảm thiểu việc quản trị mạng liên tục kiểm tra Web Site ***Windows Update*** để tìm kiếm các bản mới phát hành.

- **Máy chủ Intranet Windows Update.** Khi máy chủ SUS đã tải các bản cập nhật, người quản trị phải quyết định liệu máy chủ có triển khai chúng trên mạng ngay lập tức hoặc lưu chúng lại để thử nghiệm và triển khai sau. Khi các bản cập nhật đã sẵn sàng để triển khai, chức năng của SUS như là máy chủ ***Windows Update*** cho các máy tính trên mạng ngoại trừ việc nó là máy chủ trong mạng intranet và không yêu cầu người dùng kết nối ra Internet.
- **Automatic Update.** Automatic Update là một tính năng của hệ điều hành Windows cho phép máy tính tải và cài đặt các bản cập nhật phần mềm mà không cần người dùng tác động. Bạn có thể cấu hình tính năng này trên máy trạm để các máy này có thể nhận các bản cập nhật từ một máy chủ SUS trong mạng nội bộ hơn là từ ***Web site Windows Update***, do đó hạn chế việc cập nhật sử dụng chỉ các bản cập nhật mà người quản trị mạng cho phép.

  LẬP KẾ HOẠCH. Các yêu cầu hệ điều hành của SUS. *SUS chỉ chạy trên các hệ điều hành Windows Server 2003 và Windows Server 2000 với* ***service pack 2*** *hoặc hơn. Các máy khách sử dụng SUS phải chạy trên nền hệ điều hành Windows Server 2003, Windows 2000 hoặc Windows XP*

Triển khai SUS

Quá trình triển khai SUS bao gồm các bước cơ bản sau đây:

1. **Cài đặt máy chủ SUS**. SUS là một loạt các trang Web và ứng dụng intranet, cung cấp cho máy khách và người quản trị khả năng truy cập đến dịch vụ này, Bạn phải cài đặt IIS trên máy chủ trước khi bạn cài đặt SUS
2. **Đồng bộ hóa máy chủ**. Đồng bộ hóa là một quá trình trong đó máy chủ SUS tải các bản cập nhật từ Web site ***Windows Update*** trên Internet và lưu chúng trên đĩa cứng nội bộ
3. **Phê chuẩn các bản cập nhật**. Trước khi các máy khách có thể truy cập các bản cập nhật lưu trong máy chủ SUS, chúng phải được phê chuẩn (***Approve***), hoặc thủ công bởi người quản trị mạng hoặc tự động. Người quản trị có thể lựa chọn đặt các bản cập nhật mới trên

trong một chế độ thử nghiệm trước khi phê chuẩn chúng cho các máy khách truy cập.

4. **Cấu hình Automatic Updates trên các máy khách**. Sử dụng các chính sách nhóm, bạn có thể cấu hình tính năng ***Automatic Update*** trên các máy khách để lấy các bản cập nhật về từ máy chủ SUS chứ không phải từ Web site ***Windows Update***

Cài đặt SUS

Do SUS sử dụng Web site cho cả máy khách và các tác vụ quản trị truy cập, bạn phải cài đặt IIS trên máy chủ này trước khi bạn cài đặt SUS. Windows Server 2003 chứa IIS trong bộ cài đặt nhưng không cài đặt nó theo mặc định. Để cài đặt IIS, mở ***Add Or Remove Programs*** trong ***Control Panel***, nhấn vào ***Add/Remove Windows Components*** và lựa chọn ***Internet Information Services (IIS)*** từ trong danh sách các thành phần của ***Application Server***

Khi bạn đã cài đặt IIS, bạn có thể chạy chương trình cài đặt SUS mà bạn tải về từ Web Site của Microsoft và ***Microsoft Software Update Services Setup Wizard*** (*Trình Hướng dẫn Cài đặt Dịch vụ Cập nhật*) sẽ được nạp. Sau khi bạn đồng ý với các điều khoản thoả thuận về giấy phép của người dùng phần mềm, trình hướng dẫn cài đặt này sẽ hướng dẫn bạn qua các bước cấu hình các tham số như sau:

- **Vị trí của file**. Mỗi bản vá ***Windows Update*** bao gồm hai thành phần: Bản thân file vá lỗi và ***metadata*** (Siêu dữ liệu) trong đó chỉ định nền tảng hệ thống và ngôn ngữ mà bản vá này sẽ áp dụng. SUS luôn luôn tải ***metadata***, đây là dữ liệu mà bạn sử dụng để phê chuẩn các bản cập nhật và các máy khách trong mạng intranet có thể tái tạo được các dữ liệu này từ máy chủ SUS. Bạn có thể lựa chọn liệu có tải các file hay không và nếu có thì lưu các file này ở đâu. Nếu bạn lựa chọn duy trì các file cập nhật trên máy chủ ***Microsoft Windows Update***, các máy khách sẽ kết nối đến máy chủ SUS để lấy danh sách các bản cập nhật đã được phê chuẩn nhưng lại kết nối đến ***Web site Windows Update*** để tải các file. Nếu bạn lựa chọn lưu các file cập nhật ở máy nội bộ, bạn sẽ phải sử dụng một folder trên đĩa cứng có định dạng NTFS. Đề xuất một dung lượng tối thiểu khoảng 6GB cho việc lưu trữ này.
- **Các thiết lập về ngôn ngữ**. Chỉ định ngôn ngữ nào mà bạn muốn lưu các bản cập nhật trên máy chủ. Nếu tất cả các máy khách của bạn sử dụng phiên bản ngôn ngữ tiếng Anh của Windows, bạn có thể sử dụng lựa chọn ***English Only***. Nếu các máy khách của bạn sử dụng các ngôn ngữ khác ngoài tiếng Anh, bạn có thể tải các bản cập nhật cho tất cả

các ngôn ngữ có sẵn hoặc lựa chọn một số ngôn ngữ cụ thể. Tham số này được cấu hình chỉ khi bạn lựa chọn lưu các bản cập nhật nội bộ.

- **Các thiết lập phê chuẩn bản cập nhật**. Khi SUS tải phiên bản mới của một bản cập nhật mà đã được phê chuẩn, thiết lập này chỉ định liệu phiên bản mới này có được phê chuẩn một cách tự động hay đợi đến khi được phê chuẩn một cách thủ công.

  ***LƯU Ý. Các địa chỉ URL của SUS**. Khi trình cài đặt kết thúc, nó hiển thị một URL cho giao diện quản trị của máy chủ SUS và URL mà máy khách phải sử dụng để nhận được các bản cập nhật từ máy chủ. Hãy lưu ý đến các URL này bởi vì bạn sẽ cần chúng để quản trị máy chủ và cấu hình các máy khách.*

Trình ***Microsoft Software Update Services Setup Wizard*** cài đặt ba thành phần sau đây vào máy chủ:

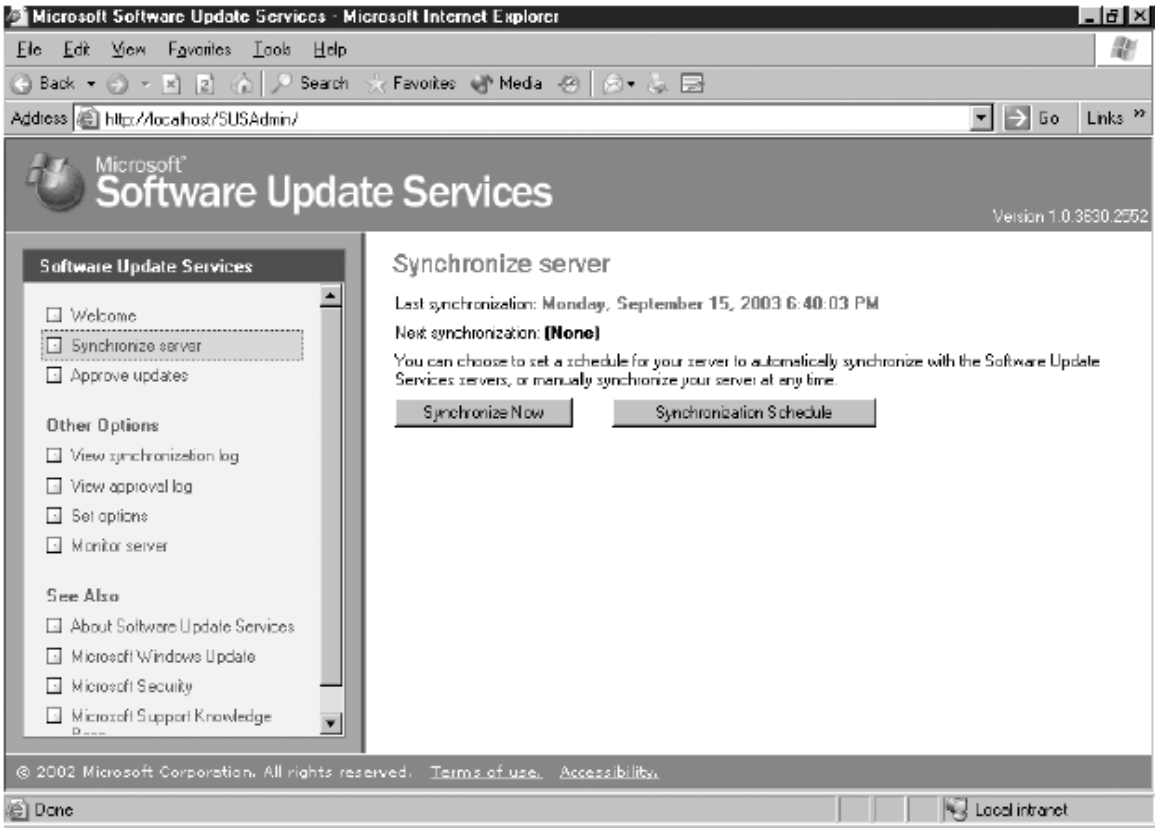
- Dịch vụ Software Update Synchronization Service, dịch vụ này tải nội dung bản cập nhật về máy chủ SUS
- Một Web site sử dụng IIS phục vụ cho các yêu cầu cập nhật của các máy khách có đặt chế độ ***Automatic Update***
- Một trang Web quản trị SUS, từ đó bạn có thể tiến hành đồng bộ máy chủ SUS và phê chuẩn các bản cập nhật.

Khi quá trình cài đặt kết thúc, Internet Explorer hiển thị giao diện quản trị Web của SUS

***LƯU Ý. Cấu hình các tính năng bảo mật tiên tiến của Internet Explorer.** Bạn có thể cần phải thêm máy chủ của bạn vào trong danh sách các site nội bộ mạng intranet được tin cậy để truy cập site này. Mở **Internet Explorer** và lựa chọn **Internet Option** từ thực đơn **Tool**. Lựa chọn thẻ **Security**, lựa chọn **Trusted Site** và nhấn vào **Sites**. Thêm tên máy chủ của bạn vào danh sách các site tin cậy.*

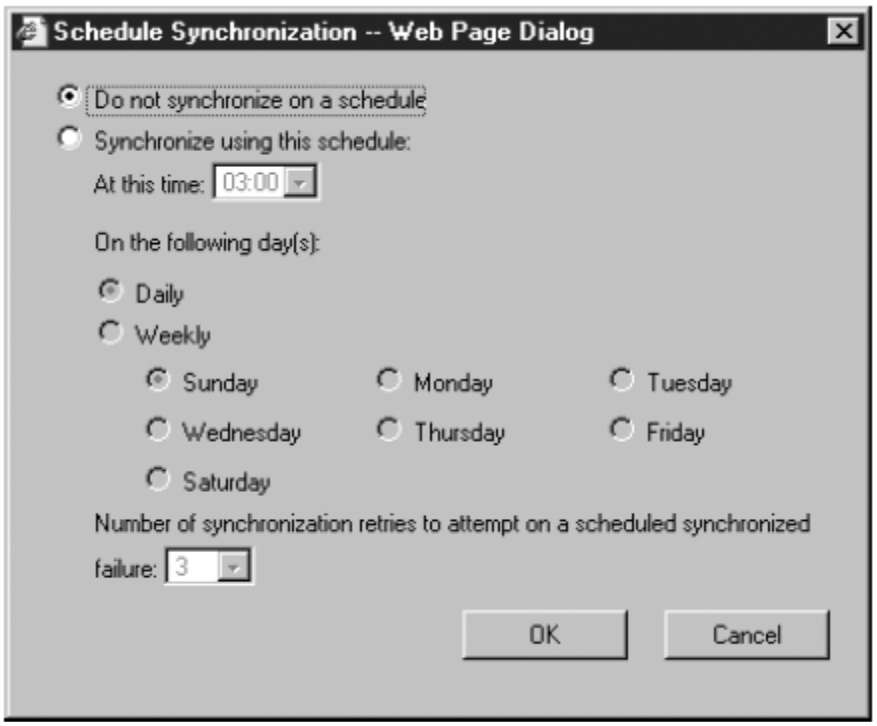
Đồng bộ SUS

Hai tác vụ quản trị chính cho máy chủ SUS là đồng bộ máy chủ và phê chuẩn các bản cập nhật. Khi bạn nhấn vào siêu liên kết ***Synchronize Server*** trong trang quản trị chính, bạn sẽ thấy một giao diện như Hình 5-8. trong trang này, bạn có thể lập lịch đồng bộ để việc này diễn ra theo một lịch đều đặn hoặc kích hoạt chúng một cách thủ công.



Hình 5-8. Trang *SUS Synchronize Server*

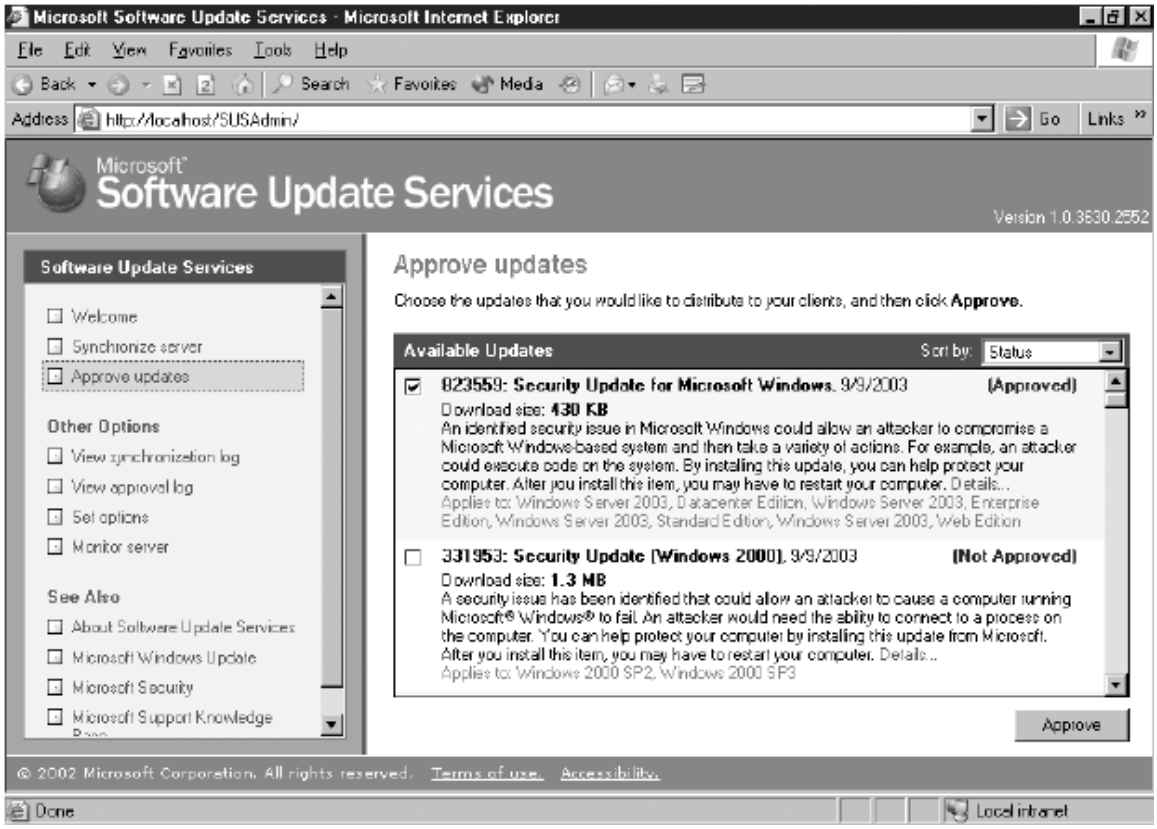
Để lập lịch đồng bộ, bạn nhấn vào phím ***Synchronization Schedule*** (Lịch đồng bộ) để hiển thị hộp thoại ***Schedule Synchronization*** (Thể hiện trong hình 5-9). Trong quá trình đồng bộ, máy chủ kết nối đến Web site ***Windows Update*** và tải danh mục của các bản cập nhật có sẵn. Sau đó, tùy vào các thiết lập mà bạn đã chỉ định trong quá trình cài đặt, SUS hoặc tải tất cả các bản cập nhật hoặc tích hợp metadata vào trong danh mục cập nhật riêng của nó.



Hình 5-10. Hộp thoại *Schedule Synchronization*

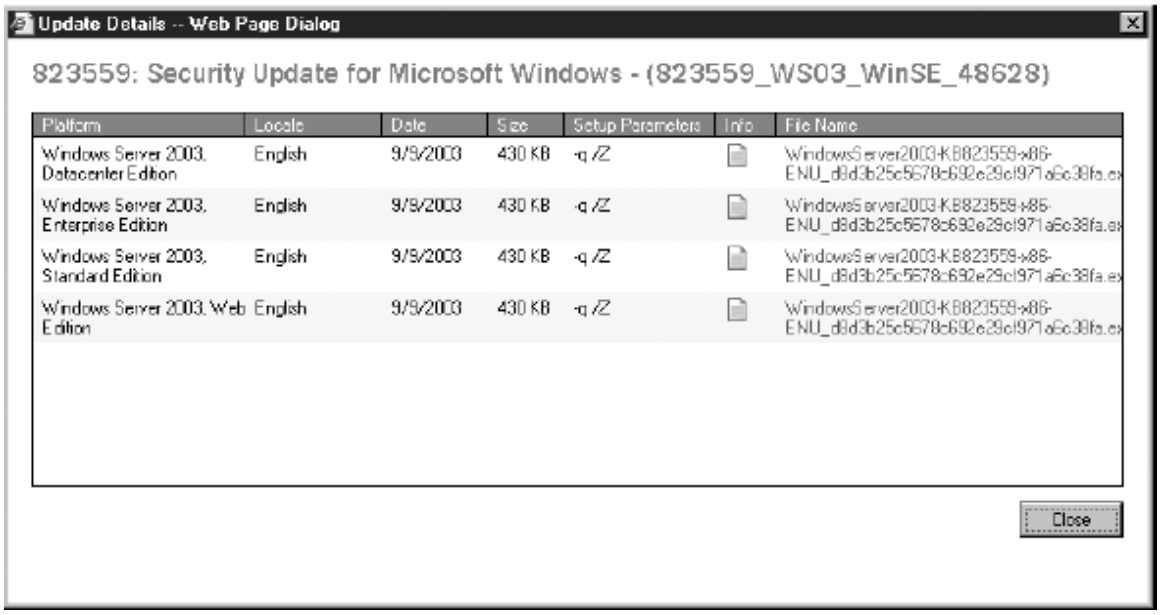
Phê chuẩn các bản cập nhật

Khi quá trình cập nhật hoàn thành, bạn được đưa tới trang ***Approve Update***, thể hiện trên Hình 5-10. tại đây, người quản trị có thể xem một danh sách các bản cập nhật đã được đồng bộ và lựa chọn bản nào có thể cung cấp cho các máy khách.



Hình 5-10. Trang *SUS Approve Updates*

Mỗi mục trong danh sách các bản cập nhật này có một siêu liên kết ***Details*** (Chi tiết) hiển thị một trang ***Update Details*** (Chi tiết Cập nhạt) giống như thể hiện trong Hình 5-11. Trang này cung cấp các thông tin về bản cập nhật được lựa chọn, kích thước và ngày của bản đó, đồng thời các tham số cài đặt mà bản cập nhật này sẽ sử dụng khi nó được cài đặt trong các máy khách. Trang ***Update Details*** cũng chứa một liên kết đến các bài viết ***Knowledge Base*** (trên Web site hỗ trợ của Microsoft) tương ứng với bản cập nhật này và một liên kết đến chính file chạy của bản cập nhật này để người quản trị có thể truy cập bản cập nhật cho mục đích thử nghiệm.

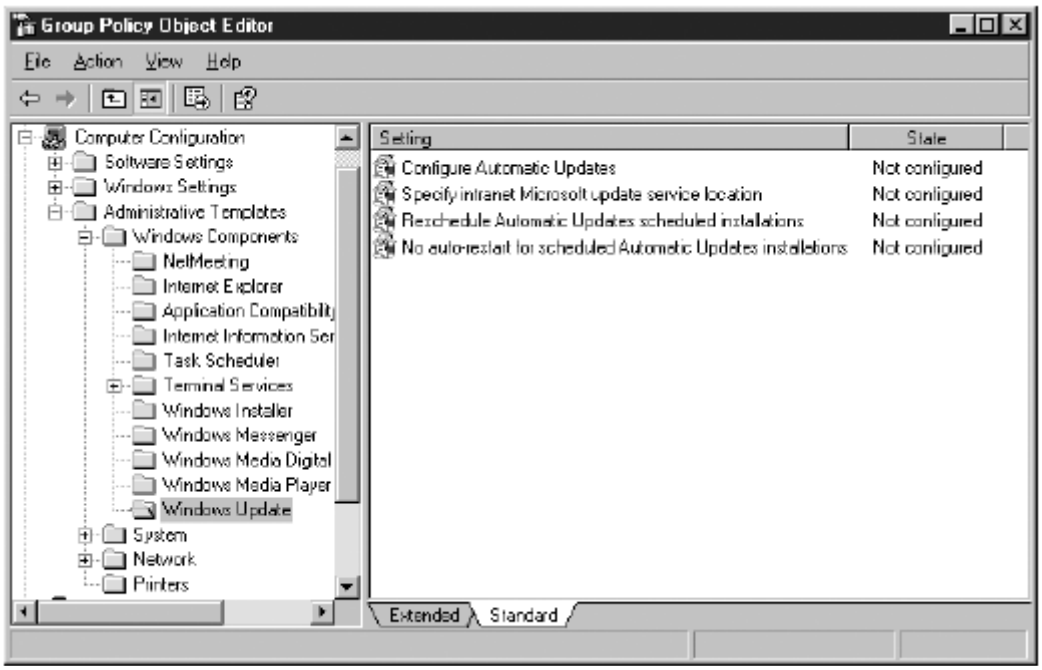


Hình 5-11. Trang *SUS Update Details*

Cấu hình Automatic Update

Khi các máy chủ SUS đã được cài đặt và hoạt động, bước tiếp theo là cấu hình các máy khách để sử dụng nó. Như đã đề cập trong phần trước của chương, bạn đã học về các tính năng sẵn có của ***Automatic Update*** trong Windows Server 2003, Windows XP và Windows 2000. Theo mặc định, ***Automatic Update*** sẽ tải các file cập nhật từ Web site ***Windows Update***, tuy nhiên bạn có thể cấu hình máy khách này lấy các bản cập nhật từ một máy chủ SUS. Để làm điều này, bạn phải cấu hình phần mềm máy khách ***Automatic Update*** bằng các chính sách nhóm.

Để triển khai các tính năng này hoặc bất kỳ chính sách nhóm nào, bạn phải lựa chọn một miền sử dụng ***Active Directory***, ***site*** hoặc đối tượng ***OU***, mở hộp thoại ***Properties*** của nó, lựa chọn thẻ ***Group Policy*** và nạp bảng điều khiển ***Group Policy Object Editor*** bằng cách chọn ***Group Policy*** thích hợp và nhấn ***Edit***, Trong bảng điều khiển này, bạn mở rộng các folder ***Computer Configuration, Administrative Templates*** và ***Windows Components***, sau đó lựa chọn ***Windows Update*** để hiển thị bốn chính sách như trong Hình 5-12



Hình 5-12. Các chính sách *Windows Update* trong bảng điều khiển *Group Policy Object Editor*

Các chính sách như sau:

- **Cấu hình Automatic Update**. Chỉ định hoạt động mặc định của phần mềm máy khách ***Automatic Update*** sử dụng một trong ba lựa chọn sau: ***Notify For Download And Notify For Install, Auto Download And Notify For Install,*** và ***Auto Download And Schedule The Install*** (Thông báo để tải và thông báo để cài đặt, Tự động tải và thông báo để cài đặt và Tự động tải và lập lịch cài đặt). Các lựa chọn này bạn cũng có thể cấu hình trong thẻ ***Automatic Update*** của hộp thoại ***System Properties*** trên máy khách.
- **Chỉ định máy chủ Intranet Microsoft Update Service.** Chỉ định máy chủ mà từ đó các máy khách truy cập các bản cập nhật của Windows. Đây là chính sách cho phép bạn hướng các phần mềm máy khách ***Automatic Update*** vào một máy chủ SUS thay cho việc sử dụng Web site ***Windows Update***. Trong hộp thoại ***Set The Intranet Update Service For Detecting Updates*** (Thiết lập máy chủ dịch vụ cập nhật Intranet để phát hiện các bản cập nhật), bạn nhập vào URL của máy chủ SUS mà trình cài đặt ***Microsoft Software Update Server Setup Wizard*** đã cung cấp cho bạn trong quá trình cài đặt. Theo mặc định, máy trạm ghi nhật ký lại các tương tác giữa nó và máy chủ SUS, nơi mà nó lấy các bản cập nhật về. Tuy nhiên chính sách này cũng đồng thời cho phép bạn trỏ máy trạm vào một máy chủ IIS khác để

ghi nhật ký thống kê. Điều này sẽ cho phép máy khách lấy các bản cập nhật từ một máy chủ SUS nội bộ trong khi lại ghi nhật ký các hoạt động của nó vào một máy chủ trung tâm đơn nào đó để dễ dàng thu hồi và phân tích các dữ liệu nhật ký. Nhật ký IIS được đặt trong folder ***systemroot\System32\Logfiles\W3svc1***

- **Reschedule Automatic Updates Scheduled Installations (Tái lập lại lịch cài đặt Automatic Update trước đó)**. Nếu việc cài đặt được lập lịch nhưng các máy tính khách lại tắt tại thời điểm đặt lịch, cách thức hoạt động mặc định là đợi đến thời điểm tiếp theo trong lịch. Trong chính sách này, nếu thiết lập giá trị là giữa 1 và 60, sẽ làm cho ***Automatic Update*** tái sắp xếp lại lịch để việc cài đặt diễn ra sau một số phút sau khi hệ thống khởi động lần tiếp theo.
- **No Auto-Restart For Scheduled Automatic Updates Installations (Không tự động khởi động lại khi cài đặt các bản cập nhật theo lịch).** Khi người dùng đăng nhập vào hệ thống, ***Automatic Update*** sẽ yêu cầu khởi động lại hệ thống khi bản cập nhật được cài đặt. Thay vào việc hệ thống tự khởi động, người dùng nhận được thông báo rằng hệ thống cần khởi động để việc cài đặt được hoàn tất.

Khi bạn cấu hình ***GPO*** và các chính sách nhóm được áp dụng, phần mềm máy khách ***Automatic Update*** sẽ truy vấn máy chủ SUS với khoảng thời gian lặp 22 giờ, cộng với một khoảng dịch chuyển ngẫu nhiên (Để tránh sự tăng cao đột ngột trong lưu lượng mạng). Sau khi máy khách tải các bản cập nhật được phê chuẩn từ máy chủ SUS, chúng sẽ được cài đặt và cấu hình – thủ công hoặc tự động – tại thời điểm được lập lịch trước. Nếu một bản cập nhật đã được phê chuẩn mà sau đó lại không được phê chuẩn bởi quản trị mạng, bản cập nhật đó sẽ không bị gỡ cài đặt nhưng nó không thể được cài thêm nữa bởi bất kỳ máy khách nào khác. Các bản cập nhật được cài đặt thông qua SUS có thể được gỡ cài đặt một cách thủ công, tuy nhiên phải sử dụng ***Add Or Remove Programs*** trong ***Control Panel***.

> ***LƯU Ý. Các bản cập nhật quan trọng then chốt****. Trong một số trường hợp, một bản cập nhật sẽ giải quyết một vấn đề bảo mật then chốt nào đó và quan trọng đến mức bạn không cần phải đợi đến khi các máy khách truy vấn, tải và cài đặt. Trong trường hợp này, bạn vẫn có thể tự cài đặt một cách thủ công.*

Xây dựng kiến trúc SUS

Một máy chủ SUS đơn có thể là đủ cho một doanh nghiệp nhỏ, tuy nhiên đối với các doanh nghiệp lớn, bạn có thể muốn có nhiều hơn một máy chủ này.

Khi bạn cài đặt nhiều máy chủ SUS trong hệ thống mạng, bạn có thể cấu hình chúng tương tác với nhau theo một trong bất kỳ các kiến trúc sau đây:

- **Kiến trúc đa máy chủ**. Mỗi máy chủ SUS sẽ đồng bộ nội dung của nó từ trang ***Windows Update*** và quản trị danh sách các bản cập nhật riêng của nó. Kiến trúc này cho phép người quản trị mỗi máy chủ có thể điều khiển được bản danh sách cập nhật trong máy chủ đó và cũng cho phép một doanh nghiệp có thể duy trì rất nhiều các bản vá và các cấu hình cập nhật.
- **Kiến trúc cha/con chặt chẽ**. Một máy chủ SUS mức cha sẽ đồng bộ nội dung của nó từ Web Site ***Windows Update*** và lưu các bản cập nhật trong folder nội bộ. Người quản trị SUS sau đó sẽ phê chuẩn các bản cập nhật này để áp dụng cho các máy khách. Các máy chủ SUS khác trong doanh nghiệp sẽ đồng bộ từ máy chủ mức cha và được cấu hình để đồng bộ cả các file cập nhật và bản danh sách các bản cập nhật được phê chuẩn. Các máy khách có thể lấy các bản cập nhật từ máy chủ SUS gần nhất. Trong kiến trúc này, người quản trị của máy chủ SUS mức con không thể phê chuẩn hoặc không phê chuẩn các bản cập nhật, tác vụ này chỉ được thực hiện trên máy chủ SUS mức cha.
- **Kiến trúc cha/con lỏng lẻo**. Máy chủ SUS mức cha đồng bộ nội dung của nó từ ***Windows Update*** và lưu các bản cập nhật này trên folder nội bộ. Các máy chủ SUS khác trong doanh nghiệp đồng bộ từ máy chủ mức cha này. Không giống như trong cấu hình chặt chẽ, các máy chủ SUS thêm vào này không đồng bộ danh sách các bản cập nhật được phê chuẩn, do đó người quản trị mạng của mỗi máy chủ có thể phê chuẩn hoặc không đối với các bản cập nhật này một cách độc lập. Mặc dù kiến trúc này tăng công việc quản trị nhưng nó rất hữu ích khi một doanh nghiệp muốn tối ưu hóa việc sử dụng Internet và yêu cầu phân phối quyền phê chuẩn các bản cập nhật, các bản vá lỗi và các cấu hình cập nhật.

SUS sử dụng kiến trúc đa máy chủ theo mặc định. Để triển khai một kiến trúc cha/con, bạn truy cập trang ***Set Option*** (Thiết lập lựa chọn) trong trang quản trị máy chủ SUS và cấu hình lựa chọn ***Select Which Server To Synchronize Content From*** (Lựa chọn máy chủ nào để đồng bộ nội dung). Đối với kiến trúc cha/con, bạn có thể giữ nguyên các thiết lập mặc định trên máy chủ SUS mức cha và cấu hình máy chủ mức con với lựa chọn ***Synchronize From A Local Software Update Services Server*** (Đồng bộ từ máy chủ dịch vụ cập nhật phần mềm nội bộ) là tên của máy chủ SUS mức cha. Đối với kiến trúc cha/con chặt chẽ, bạn cũng lựa chọn ***Synchronize List***

Of Approved Items Updated From This Location (Đồng bộ danh sách các bản cập nhật được phê chuẩn từ nơi đây); đối với kiến trúc cha/con lỏng lẻo, bạn có thể xóa bỏ lựa chọn này.

Giám sát SUS

Trang ***Monitor Server*** (Giám sát máy chủ) của Web site quản trị SUS hiển thị các thông số thống kê thể hiện số lượng của các bản cập nhật khả thi đối với từng nền tảng máy chủ và các thông số thời gian, ngày giờ của các bản cập nhật mới nhất. Thông tin này được tổng kết từ các dữ liệu ***metadata*** của ***Windows Update*** mà đã được tải trong mỗi quá trình đồng bộ. Thông tin ***metadata*** dược ghi vào đĩa cứng và lưu trong bộ nhớ để cải thiện hiệu năng khi hệ thống yêu cầu các bản cập nhật tương ứng của các nền tảng máy chủ

Bạn có thể giám sát ***SUS*** và ***Automatic Update*** bằng các nhật ký sau:

- **Nhật ký đồng bộ**. Bạn có thể lấy các thông tin về các quá trình đồng bộ trong quá khứ hoặc hiện tại và các gói phần mềm xác định đã được tải bằng cách nhấn vào ***View Synchronization Log*** trong thanh duyệt bên trái.
- **Nhật ký phê chuẩn**. Để có thông tin về các gói phần mềm đã được phê chuẩn, nhấn vào phím ***View Approval Log*** (Xem nhật ký phê chuẩn) trong thanh duyệt bên trái
- **Nhật ký Windows Update**. Các máy khách ***Automatic Update*** sẽ ghi nhật ký về các hoạt động trong file ***systemroot\Windows Update.log*** trên đĩa cứng nội bộ của máy khách.
- **Wutrack.bin**. Các tương tác giữa máy khách với máy chủ SUS sẽ được ghi lại vào trong nhật ký thông kê đặc biệt của máy chủ IIS, thông thường được lưu trong folder ***systemroot \System32\Logfiles\W3svc1***

Các sự kiện hệ thống SUS

Dịch vụ đồng bộ sẽ tạo ra các thông báo nhật ký sự kiện cho mỗi khi việc đồng bộ được thực hiện bởi máy chủ và khi bản cập nhật được phê chuẩn. Các thông báo này có thể xem được trong Nhật ký Hệ thống bằng cách sử dụng ***Event Viewer***. Các sự kiện liên quan đến tình huống này:

- **Không thể kết nối**. ***Automatic Update*** không thể kết nối đến dịch vụ cập nhật (***Windows Update*** hoặc máy tính được chỉ định làm máy chủ SUS)

- **Sẵn sàng cài đặt – lịch không định kỳ**. Các bản cập nhật liệt kê trong sự kiện này được tải và chờ cài đặt. Quản trị mạng phải nhấn vào biểu tượng thông báo và nhấn ***Install***
- **Sẵn sàng cài đặt – lịch định kỳ**. Các bản cập nhật liệt kê trong sự kiện này đươc tải và sẽ được cài đặt vào ngày và giờ xác định ghi trong sự kiện.
- **Cài đặt thành cônng** – Các bản cập nhật được liệt kê trong sự kiện này đã được cài đặt thành công.
- **Cài đặt thất bại**. Các bản cập nhật liệt kê trong sự kiện này bị trục trặc và không được cài đặt
- **Yêu cầu khởi động lại – lịch không định kỳ.** Một bản cài đặt yêu cầu khởi động lại hệ thống. Nếu việc cài đặt được thiết lập là phải thông báo thì quá trình khởi động lại phải được thực hiện thủ công. Windows không thể tìm kiếm các bản cập nhật khác trước khi việc khởi động lại được thực hiện.
- **Yêu cầu khởi động lại – Lịch định kỳ.** Khi ***Automatic Update*** được cấu hình để tự động cài đặt các bản cập nhật, một sự kiện sẽ được ghi lại nếu một bản cập nhật nào đó yêu cầu khởi động. Hệ thống sẽ khởi động trong vòng 5 phút. Windows không thể tìm kiếm các bản cập nhật mới cho đến khi khởi động xong

Giải quyết sự cố SUS

SUS trong một máy tính Windows Server 2003 có thể yêu cầu các bước khắc phục sự cố như sau:

- **Nạp lại bộ nhớ đệm cache**. Nếu không có bản cập nhật mới nào xuất hiện từ lần cuối cùng bạn đồng bộ máy chủ, có khả năng là không có bản cập nhật nào. Tuy nhiên cũng có thể là do bộ nhớ đệm (***cache)*** không nạp các bản cập nhật mới một cách tốt đẹp. Từ site quản trị SUS, nhấn vào ***Monitor Server*** và nhấn ***Refresh***
- **Khởi động lại dịch vụ đồng bộ**. Nếu bạn nhận được thông báo rằng dịch vụ đồng bộ không chạy tốt hoặc bạn không thể chỉnh sửa các thiết lập trong trang ***Set Option*** của Web Site quản trị SUS, mở bảng điều khiển ***Service*** từ nhóm chương trình ***Administrative Tools***, nhấn phải chuột vào ***Software Update Services Synchronization Service*** (Dịch vụ đồng bộ SUS) và lựa chọn ***Restart***.

- **Khởi động lại IIS**. Nếu bạn không thể kết nối đến site quản trị hoặc nếu máy khách không thể kết nối đến máy chủ SUS, khởi động lại ***World Wide Web Publishing Service*** bằng cách sử dụng bảng điều khiển ***Service***.

QUẢN LÝ CÁC BẢN QUYỀN PHẦN MỀM

End-User License Agreement (Thỏa thuận Giấy phép cho Người dùng Cuối - EULA) khá là phiền toái khi các bạn phải đọc và nhấn vào để bắt đầu cài đặt hệ điều hành, các bản cập nhật hoặc các ứng dụng mới. EULA là một hợp đồng kết hợp cho bạn quyền hợp pháp để sử dụng phần mềm. Trong một môi trường doanh nghiệp lớn, quản lý các giấy phép sử dụng phần mềm là điều quan trọng then chốt và Windows Server 2003 bao gồm nhiều công cụ giấy phép mà bạn có thể sử dụng để đăng ký và giám sát các giấy phép và mức độ tuân thủ của người dùng trong doanh nghiệp..

> ***LƯU Ý. Các phiên bản thử nghiệm****. Phiên bản thử nghiệm để đánh giá của Windows Server 2003 là không hỗ trợ chế đọ quản trị giấy phép. Bạn không thể theo hết các ví dụ trong bài học này khi không có một phiên bản thương mại đầy đủ của sản phẩm này.*

Nhận Giấy phép Truy cập Máy khách (Client Access License – CAL)

Giấy phép cho máy chủ Windows Server 2003 cho phép bạn cài đặt hệ điều hành lên máy tính, tuy nhiên bạn còn cần **Client Access License (Giấy phép truy cập cho máy khách - CAL)** trước khi người dùng hoặc thiết bị có thể được xác thực một cách hợp pháp để kết nối đến máy chủ. CAL thường được mua dưới dạng gói và có thể bao gồm trong bản mua hệ điều hành. Ví dụ bạn thường thấy một bản Windows Server 2003 bán ra với một gói giấy phép 5 hoặc 10 người dùng. Tuy nhiên, nếu hệ điều hành không bao gồm bất kỳ một CAL nào, bạn phải mua chúng riêng biệt. Giữ lại các chứng nhận CAL và EULA của bạn trong một kẹp tài liệu để đề phòng trường hợp doanh nghiệp của bạn bị kiểm định xem có tuân thủ theo giấy phép hay không.

> ***LƯU Ý. Các giấy phép nâng cấp****. Khi bạn nâng cấp một máy chủ từ Windows NT hoặc Windows 2000 sang Windows Server 2003, bạn phải mua CAL nâng cấp tương ứng.*

Bạn phải mua CAL cho bất kỳ kết nối nào tới máy tính Windows Server 2003 mà sử dụng các thành phần của máy tính, bao gồm dịch vụ file và in ấn

hay xác thực. Rất ít ứng dụng máy chủ chạy độc lập mà kết nối máy chủ/máy khách không yêu cầu CAL. Trường hợp ngoại lệ có ý nghĩa nhất mà không yêu cầu CAL là các kết nối không xác thực được kiểm soát thông qua Internet. Khi không có sự trao đổi thông tin xác thực trong quá trình truy cập Internet, ví dụ như người dùng Internet duyệt các Web site một cách vô danh, thì CAL là không cần thiết. Do đó cũng không yêu cầu CAL cho phiên bản Web của Windows Server 2003.

Có hai loại CAL: ***Windows Device CAL(****Giấy phép Truy cập theo Thiết bị****)***, loại này cho phép một thiết bị kết nối đến một máy chủ mà không quan tâm đến số lượng người dùng có thể sử dụng thiết bị đó, và ***Windows User CAL(****Giấy phép Truy cập theo Người dùng****)***, loại này cho phép một người dùng kết nối đến một máy chủ từ rất nhiều thiết bị. ***Windows Device CA***L có lợi cho một doanh nghiệp mà có nhiều người dùng trên một thiết bị, ví dụ như công nhân làm ca. ***Windows User CAL*** sử dụng cho hầu hết các doanh nghiệp có nhân viên truy cập mạng từ rất nhiều thiết bị, kể cả các thiết bị chưa từng được biết đến.

> ***LƯU Ý. User CAL và Device CAL****. Các công cụ giấy phép và giao diện người dùng sẽ không phân biệt giữa* ***Windows User*** *và* ***Windows Device CAL****. Một* ***Device CAL*** *được đăng ký gián tiếp, sử dụng nhóm giấy phép*

Số lượng các giấy phép CAL bạn yêu cầu và làm thế nào để có thể theo dõi các giấy phép đó phụ thuộc vào chế độ giấy phép cho máy khách mà bạn có. Có hai chế độ giấy phép: Giấy phép ***Per Server*** và giấy phép ***Per Device*** hay ***Per User***

Giấy phép Per Server

Giấy phép Per Server yêu cầu một ***Windows User*** hoặc ***Windows Device CAL*** cho mỗi kết nối đồng thời. Nếu một máy chủ được cấu hình với 1000 CAL, kết nối đồng thời thứ 1001 sẽ bị từ chối truy cập. CAL được thiết kế để sử dụng trên một máy chủ cụ thể, do đó nếu 1000 người dùng đó yêu cầu kết nối đồng thời đến một máy chủ thứ hai, bạn phải mua thêm 1000 CAL nữa.

Giấy phép ***Per Server*** có lợi điểm chỉ trong các trường hợp giới hạn truy cập, ví dụ như một mạng nhỏ người dùng truy cập vào rất ít máy chủ. Giấy phép ***Per Server*** là không hiệu quả trong trường hợp nhiều người dùng truy cập vào nhiều tài nguyên trong nhiều máy chủ. Nếu bạn không chắc chắn về các chế độ giấy phép tương ứng, hãy chọn ***Per Server***. Thỏa thuận giấy phép cho phép chuyển đổi không mất chi phí, một lần, một chiều từ ***Per Server***

sang chế độ giấy phép ***Per Device*** hay ***Per User*** khi bạn có thể thực hiện điều này một cách thích hợp.

Giấy phép Per Device hay Per User.

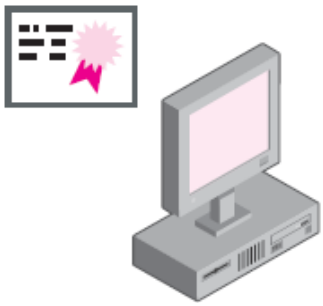
Chế độ giấy phép **Per Device** hay **Per User** chuyển đổi từ mô hình Per Seat trong các phiên bản trước đó của Windows. Trong chế độ mới này, mỗi thiết bị hoặc người dùng có thể kết nối đến một số máy chủ trong doanh nghiệp. Chế độ ***Per Device*** hay ***Per User*** thường là chế độ lựa chọn cho các môi trường máy tính phân tán trong đó nhiều người dùng truy cập nhiều máy chủ.

Ví dụ, một ***developer*** (Nhân viêc phát triển phần mềm) sử dụng một máy xách tay và hai máy để bàn sẽ yêu cầu chỉ một ***Windows User CAL***. Một mạng ngang hàng gồm 10 máy PC để bàn mà sử dụng bởi 30 công nhân làm ca sẽ yêu cầu chỉ 10 ***Windows Device CAL***.

Tổng số CAL bằng với số lượng người dùng hoặc thiết bị, hoặc sự pha trộn của các đối tượng trên mà truy cập đến các máy chủ. CAL có thể được cấp lại trong các điều kiện đặc biệt. Ví dụ, một giấy phép ***Windows User CAL*** có thể được cấp lại từ một người dùng lâu dài sang một người dùng tạm thời trong khi người dùng lâu dài đó đã rời công ty. Một ***Windows Device CAL*** có thể được cấp lại cho một thiết bị mượn trong khi thiết bị gốc đang được sửa chữa.

Các chế độ giấy phép ***Per Server*** và ***Per Device*** hay ***Per User*** được minh họa trong Bảng 5-1

Bảng 5-1. Các chế độ giấy phép CAL



Cấp giấy phép kiểu truyền thống trong chế độ ***Per Server*** khi có ít máy chủ và chúng yêu cầu truy cập giới hạn	Cấp giấy phép kiểu truyền thống trong chế độ ***Per User*** hay ***Per Device*** khi có nhiều máy chủ và chúng yêu cầu các truy cập trường

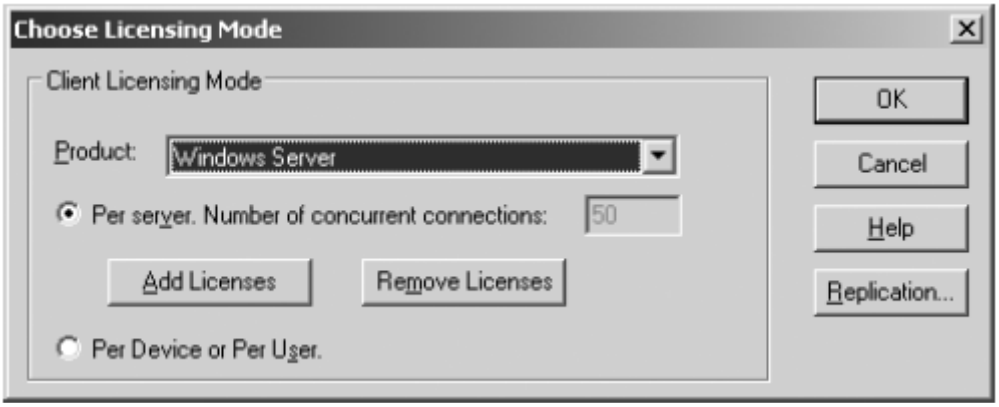
	xuyên trên diện rộng
Số lượng cần thiết của CAL được xác định bởi số kết nối đồng thời yêu cầu	Thường kinh kế hơn khi số lượng các CAL cần thiết được xác định bởi số lượng người dùng hoặc thiết bị, hoặc cả hai, có yêu cầu truy cập đến máy chủ

LƯU Ý. Các giấy phép cho Terminal Services*. Windows Server 2003 bao gồm* ***Terminal Services****, dịch vụ này có sẵn giấy phép cho 2 kết nối đồng thời cho phép quản trị mạng có thể kết nối đến một máy chủ từ xa. Khi* ***Terminal Services*** *thực hiện chức năng của một máy chủ ứng dụng, để cho phép một người dùng không có quyền quản trị kết nối đến và chạy ứng dụng thì bạn phải có các* ***Terminal Services CAL****, các CAL này có kèm theo trong Windows XP Professional*

Các công cụ cho giấy phép

Có hai tiện ích mà bạn có thể sử dụng để theo dõi và quản lý giấy phép sử dụng phần mềm:

- **Licensing trong Control Panel**. Công cụ ***Choose Licensing Mode*** trong ***Control Panel***, thể hiện trong hình 5-13, quản lý các giấy phép yêu cầu cho một máy tính đơn chạy Windows Server 2003. Bạn có thể sử dụng ***Licensing*** để thêm hoặc bớt các CAL cho máy chủ chạy trong chế độ ***Per Server***, thay đổi chế độ giấy phép từ ***Per Server*** sang ***Per Device*** hoặc ***Per User***, hoặc cấu hình việc đồng bộ giấy phép.



Hình 5-13. Công cụ *Choose Licensing Mode* trong *Control Panel*

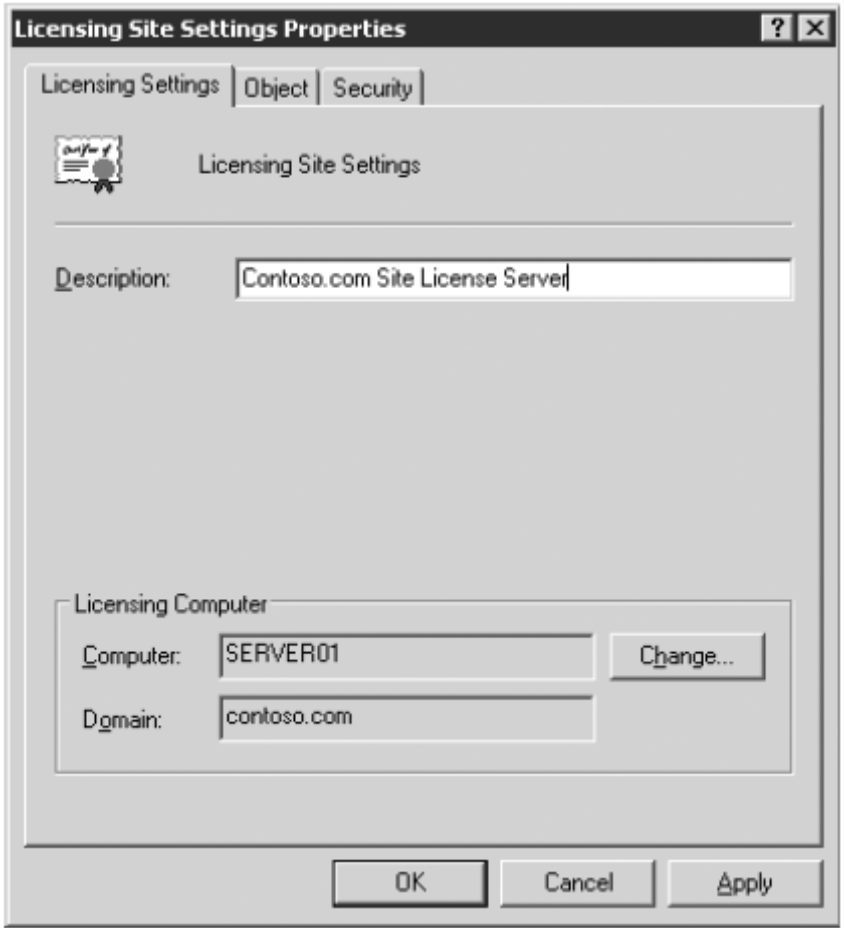
- **Licensing trong Administrative Tools**. Công cụ quản trị ***Licensing***, thảo luận trong phần tới đây, cho phép bạn quản lý các giấy phép cho một doanh nghiệp bằng cách tập trung việc điều khiển các giấy phép và đồng bộ giấy phép trong mô hình dựa trên các site.

Quản lý giấy phép cho các site.

Dịch vụ ***License Logging*** (Ghi nhật ký giấy phép), chạy trong mỗi máy tính Windows Server 2003, thực hiện việc cấp phép và theo dõi các giấy phép khi máy khách truy cập tài nguyên máy chủ. Để đảm bảo việc tuân thủ giấy phép, thông tin về các giấy phép sẽ được đồng bộ với một CSDL giấy phép tập trung trên một máy chủ trong site. Máy chủ này được gọi là máy chủ giấy phép của site. Người quản trị site, hoặc người quản trị máy chủ giấy phép của site có thể sử dụng công cụ ***Licensing*** trong nhóm chương trình ***Administrative Tools*** để xem và quản lý các giấy phép cho toàn site. Tính năng quản lý và theo dõi giấy phép mới này tích hợp các giấy phép không chỉ cho các dịch vụ file và in ấn, mà còn cho IIS, ***Terminal Services*** và các sản phẩm khác của Microsoft (ví dụ như máy chủ Exchange và SQL)

Máy chủ giấy phép của site

Một máy chủ giấy phép của site thông thường là một máy chủ quản trị miền được tạo ra trong một site. Để tìm kiếm máy chủ nào là máy chủ giấy phép cho một site, mở ***Active Directory Sites And Services***, mở rộng để lựa chọn nút ***Site*** và sau đó nhấn phải chuột vào ***Licensing Site Settings*** (Các thiết lập giấy phép của site) và lựa chọn ***Properties***. Máy chủ giấy phép hiện tại của site hiển thị, như trong Hình 5-14.



Hình 5-14. Nhận biết và thay đổi máy chủ giấy phép của site bằng *Active Directory Sites and Services*

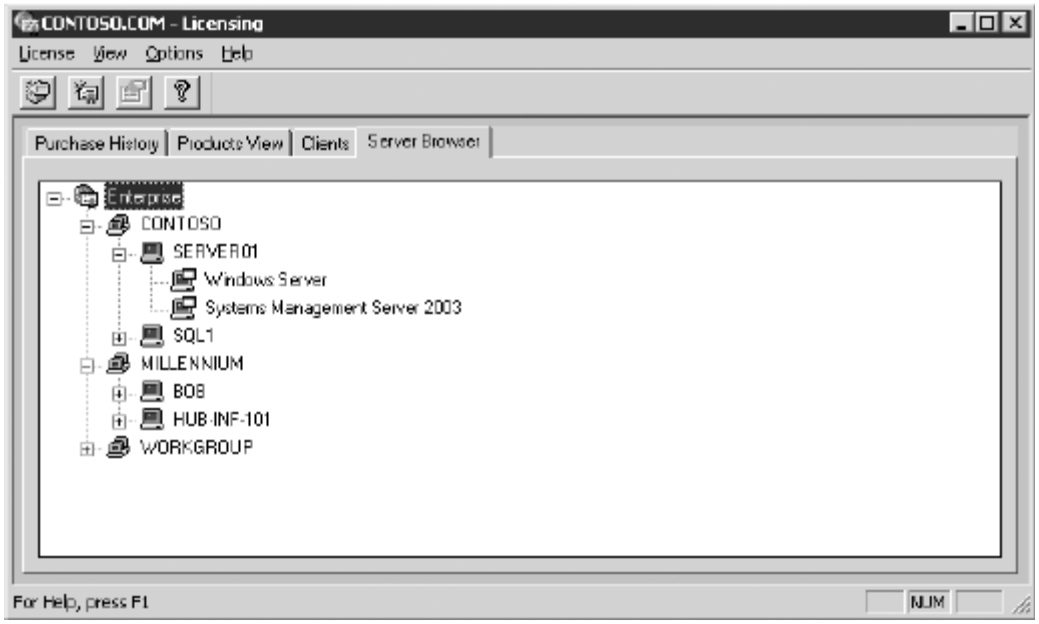
Để gán vai trò máy chủ giấy phép của site cho một máy chủ khác hoặc máy chủ quản trị miền, nhấn vào ***Change*** và lựa chọn máy tính muốn gán. Để duy trì lịch sử của các giấy phép trong doanh nghiệp của bạn, bạn phải dừng dịch vụ ***License Logging*** trên máy chủ giấy phép mới ngay lập tức sau khi chuyển giao vai trò và sau đó sao chép các file sau đây từ máy chủ cũ sang máy chủ giấy phép mới:

- ***Systemroot**System32**Cpl.cfg***, trong đó chứa lịch sử việc mua bán của doanh nghiệp
- ***Systemroot*\Lls\Llsuser.lls**, trong đó chứa thông tin người dùng về số lượng kết nối
- ***Systemroot*\Lls\Llsmap.lls**, trong đó chứa các thông tin nhóm giấy phép

Sau khi tất cả các file được sao chép, khởi động dịch vụ ***License Logging***

Quản trị các giấy phép của site.

Khi bạn đã xác định máy chủ quản lý giấy phép của site, bạn có thể xem các thông tin về giấy phép trên máy chủ đó bằng cách mở ***Licensing*** từ nhóm chương trình ***Administrative Tools***. Thẻ ***Server Browser*** trong ***Licensing*** (Thể hiện trong Hình 5-15) cho phép bạn quản lý các giấy phép cho một site hoặc doanh nghiệp.



Hình 5-15. Thẻ *Server Browser* trong công cụ quản trị *Microsoft Licensing*

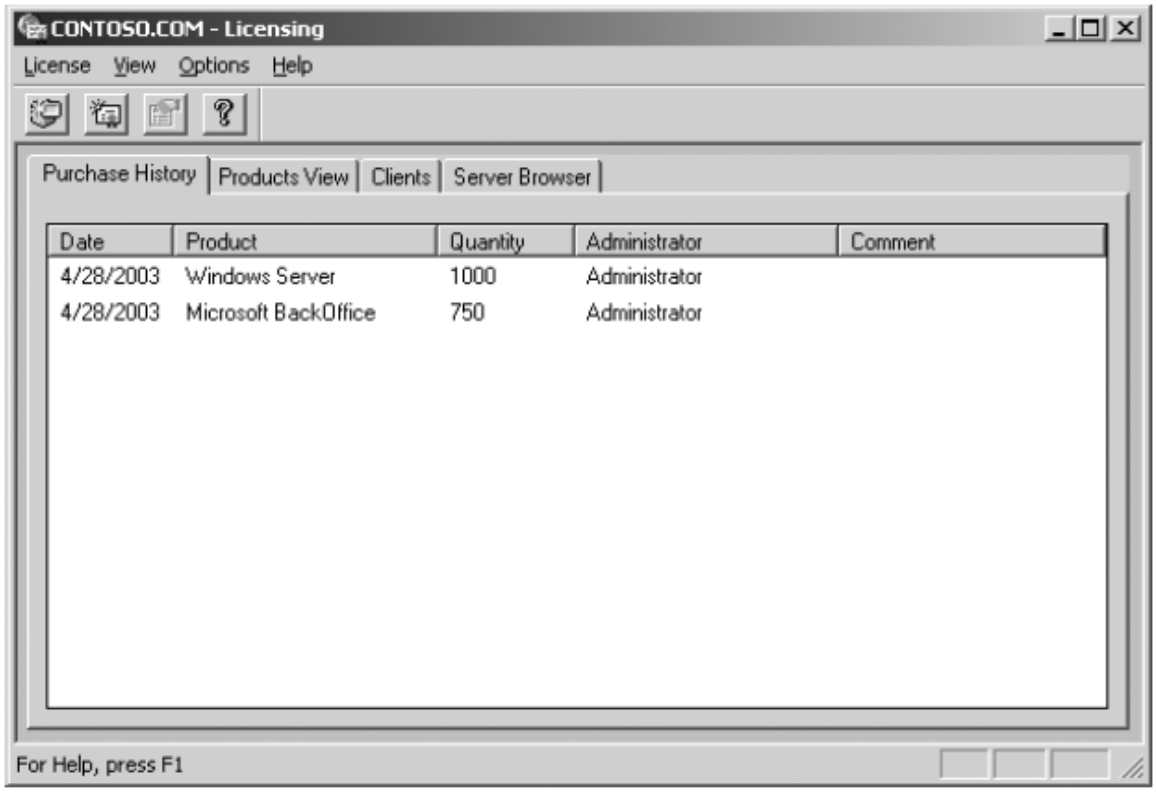
Thể ***Server Browser*** trong ***Licensing*** cho phép bạn quản lý bất kỳ máy chủ nào trong bất kỳ site hoặc miền nào mà bạn có quyền quản trị. Bạn có thể định vị máy chủ và quản lý các giấy phép của máy chủ đó bằng cách nhấn phải chuột vào nó và lựa chọn ***Properties***. Đối với các sản phẩm máy chủ được cài đặt trong máy chủ đó, bạn có thể thêm hoặc bớt các giấy phép ở chế độ ***Per Server***. Bạn còn có thể chuyển đổi các chế độ giấy phép tại nơi nào thích hợp. Hãy nhớ rằng chế độ giấy phép ***Per Server*** sẽ xuất ra một giấy phép khi một người dùng nào đó kết nối đến sản phẩm máy chủ. Khi một người dùng ngắt kết nối từ một sản phẩm máy chủ, dịch vụ ***License Logging*** sẽ để cho giấy phép này sẵn sàng với người dùng khác.

Các thuộc tính của máy chủ còn cho phép bạn cấu hình việc đồng bộ các giấy phép, trong đó bạn có thể cấu hình một máy chủ bằng cách sử dụng các thuộc tính ***Licensing*** của nó trong ***Control Panel***. Theo mặc định, các thông tin về giấy phép được đồng bộ từ một máy chủ dịch vụ ***License Logging*** đến máy chủ giấy phép của site cứ sau 24 giờ và hệ thống sẽ tự động bố trí việc đồng bộ xen kẽ để tránh việc quá tải cho máy chủ giấy phép của site. Nếu

bạn muốn điều khiển lịch đồng bộ hoặc tần suất xảy ra, bạn phải thay đổi thời gian ***Start At*** và tần suất ***Start Every*** của mỗi máy chủ để đồng bộ với máy chủ giấy phép của site cụ thể nào đó

Để quản lý các giấy phép ***Per Device*** hay ***Per User***, nhấn vào ***Licensing*** trong nhóm chương trình ***Administrative Tools*** và sau đó lựa chọn lệnh ***New License*** từ thực đơn ***License***. Trong hộp thoại ***New Client Access License*** (Giấy phép truy cập cho máy trạm mới), lựa chọn sản phẩm máy chủ và số giấy phép đã mua. Các giấy phép sẽ được thêm vào trong quĩ của các giấy phép. Khi một thiết bị hoặc một người dùng kết nối đến bất cứ sản phẩm nào trong site, chúng sẽ được phân chia một giấy phép từ quĩ này và mỗi giấy phép là cho một thiết bị hoặc người dùng. Khi quĩ các giấy phép này được phát hết, sự vi phạm giấy phép xảy ra khi bất kỳ một thiết bị hay người dùng thêm vào nào truy cập đến sản phẩm.

Thẻ ***Purchase History*** (Lịch sử mua) trong ***Licensing*** (Thể hiện trong hình 5-16) cung cấp một cách nhìn tổng quát các giấy phép mua cho một site, cũng như số lượng, ngày và các vấn đề quản trị liên quan đến việc thêm hay bớt các giấy phép này.



Hình 5-16. Thẻ *Purchase History* trong công cụ quản trị *Microsoft Licensing*

Để xem các thông tin tích lũy về các giấy phép và sự tuân thủ theo đúng giấy phép hay không, lựa chọn thẻ ***Products View***. thẻ này cho biết bao nhiêu giấy phép đã được mua và phân chia cho người dùng hoặc thiết bị (trong chế độ ***Per Device*** hay ***Per User***) hoặc số lượng các giấy phép mua được cho các máy chủ trong site và số lượng kết nối nhiều nhất trong ngày (trong chế độ ***Per Server***). Bạn cũng có thể xác định xem hoạt động có đúng như giấy phép đã mua hay không bằng cách sử dụng các biểu tượng trạng thái giấy phép thể hiện trong Bảng 5-2.

Bảng 5-2. Các ký tự trạng thái của giấy phép

	Sản phẩm này đang tuân thủ đúng với yêu cầu giấy phép hợp pháp. Số lượng kết nối ít hơn số lượng giấy phép đã mua
	Sản phẩm này không tuân thủ đúng với yêu cầu giấy phép hợp pháp. Số lượng kết nối vượt quá số lượng giấy phép đã mua
	Sản phẩm này đã đạt đến mức ngưỡng hợp pháp. Số lượng các kết nối bằng với số lượng giấy phép đã mua. Nếu một thiết bị hoặc người dùng khác kết nối đến sản phẩm máy chủ, bạn phải mua thêm và ghi nhật ký lại các giấy phép mới

Các nhóm giấy phép.

Các giấy phép ***Per Device*** hoặc *Per User* yêu cầu một CAL cho mỗi thiết bị. tuy nhiên, dịch vụ ***License Logging*** cung cấp và theo dõi các giấy phép này theo tên người dùng. Khi nhiều người dùng chia sẻ một hoặc nhiều thiết bị, bạn phải tạo ra các nhóm giấy phép, hoặc nếu không các giấy phép sẽ được dùng đến hết rất nhanh. **Một nhóm giấy phép** là một tập hợp các người dùng cùng chung một hoặc nhiều CAL. Khi một người dùng kết nối đến một sản phẩm máy chủ, dịch vụ ***License Logging*** theo dõi người dùng đó bằng tên nhưng lại cấp một CAL từ các CAL đã cấp cho nhóm giấy phép. Khái niệm dễ hiểu nhất có thể hiểu qua ví dụ như sau:

- **10 người dùng chia sẻ một thiết bị cầm tay để thực hiện việc kiểm kê**. Bạn tạo ra một nhóm giấy phép với thành viên là 10 người dùng này, Nhóm giấy phép này được cấp 1 CAL, thể hiện như một thiết bị đơn mà họ chia sẻ.
- **100 sinh viên ít khi sử dụng một phòng lab máy tính với 10 máy tính**. Bạn tạo ra một nhóm giấy phép với thành viên là 100 người dùng và cấp cho nhóm đó 10 CAL.

Để tạo ra nhóm giấy phép, nhấn vào thực đơn ***Options*** và từ thực đơn ***Advanced***, lựa chọn ***New License Group***. Nhập vào tên nhóm và cấp một giấy phép cho mỗi thiết bị mà bạn sử dụng để kết nối đến máy chủ. Số lượng của các giấy phép phân chia cho một nhóm sẽ tương ứng với số lượng thiết bị sử dụng bởi thành viên của nhóm.

> ***LƯU Ý. Mục đích của kỳ thi***. *Mục đích của kỳ thi 70-290 yêu cầu sinh viên có khả năng "quản lý giấy phép phần mềm của site"*

TỔNG KẾT

- Microsoft phát hành các bản cập nhật cho hệ điều hành dưới dạng các bản ***service pack*** và ***hotfix***
- Một bản ***service pack*** là một tập hợp của các bản cập nhật mà đã được kiểm thử cùng nhau và được phê chuẩn để cài đặt trong tất cả các máy tính
- Một ***hotfix*** là một bản vá lỗi giải quyết một vấn đề đơn lẻ nào đó và được giải thích trong một bài viết đi kèm của ***Microsoft Knowledge Base***. Các ***hotfix*** không cần thiết phải cài đặt trên tất cả các máy tính, một số chỉ dành cho các máy tính thực hiện các tác vụ đặc biệt hoặc gặp phải sự cố cụ thể nào đó.
- Các bản ***service pack*** có thể được lấy về từ Microsoft trên một đĩa CD chỉ với một ít lệ phí hoặc có thể tải miễn phí trên Internet. Nếu các bản ***service pack*** này là một file đơn, nó có thể được giải nén bằng cách thực hiện file đó với khóa chuyển /X
- Các bản ***service pack*** có thể được triển khai một cách thủ công trên mỗi máy tính, tích hợp trong bản cài đặt gốc của hệ điều hành (***slipstreamed***) và có thể tự động cài đặt thông qua các chính sách nhóm.
- ***Microsoft Software Update Services*** cho phép bạn tập trung và quản lý các phê chuẩn và phân phối của các bản cập nhật then chốt trong Windows cũng như các bản vá bảo mật của Windows. Một hay nhiều máy chủ SUS chứa danh sách các bản cập nhật được phê chuẩn và bản thân các file cập nhật, việc chứa các file cập nhật này là một tùy chọn nhưng khá thông dụng, Phần mềm máy khách ***Automatic Update*** được cấu hình, thông thường thông qua các GPO, để lấy các bản cập nhật từ các máy chủ SUS trong intranet thay cho lấy trực tiếp từ ***Microsoft Windows Update***
- Theo dõi và quản lý các giấy phép và sự tuân thủ của người dùng là một phần quan trọng của nhiệm vụ quản trị. Windows Server 2003 cho phép bạn cấp các giấy phép cho các kết nối đồng thời cho một máy chủ cụ thể hoặc duy trì giấy phép cho mỗi thiết bị hoặc người dùng mà kết nối đến bất kỳ máy chủ nào trong doanh nghiệp của bạn.
- Các giấy phép được đồng bộ giữa máy chủ dịch vụ ***License Logging*** và máy chủ giấy phép của site. Máy chủ giấy phép của site có thể được nhận biết thông qua ***Active Directory Sites And Services***, tuy

nhiên giấy phép cho site được quản trị bằng công cụ ***Licensing*** trong nhóm chương trình ***Administrative Tools***

- Một nhóm giấy phép cho phép người dùng chia sẻ một hoặc nhiều thiết bị. Một số lượng nhất định các ***Windows Device CAL*** được cấp cho nhóm giấy phép này.

BÀI TẬP THỰC HÀNH

Bài tập thực hành 5-1: Sử dụng Windows Update

Trong bài tập thực hành này, bạn sử dụng ***Windows Update*** để tải các bản ***hotfix*** mới nhất cho Windows Server 2003

1. Đăng nhập vào máy tính Windows Server 2003 mà có khả năng truy cập Internet bằng tài khoản ***Administrator***
2. Kết nối vào Internet (nếu cần)
3. Nhấn ***Start***, trỏ vào ***All Program*** và lựa chọn ***Windows Update***. ***Site Windows Update*** xuất hiện, sau đó hộp thoại ***Security Warning*** xuất hiện, hỏi bạn có muốn tải và cài đặt ứng dụng ***Windows Update*** hay không.
4. Xem các cảnh báo bảo mật để đảm bảo rằng nội dung đã được ký bởi Microsoft và nhấn ***Yes*** để tiếp tục
5. Nhấn vào liên kết ***Scan For Updates*** (Quét các bản cập nhật)
6. Nhấn vào liên kết ***Review And Install Updates*** (Xem qua và cài đặt các bản cập nhật)
7. Xem lại các bản cập nhật được liệt kê và nhấn vào ***Install Now***. Một hộp thoại ***Microsoft Windows Update*** xuất hiện, chứa thỏa thuận giấy phép cho các bản cập nhật này.
8. Nhấn ***Accept*** để đồng ý với các điều khoản trong thỏa thuận giấy phép. Một hộp thoại ***Windows Update*** xuất hiện, chứa một thanh chỉ thị tiến trình
9. Khi việc cài đặt hoàn thành, nếu các bản cập nhật cài đặt yêu cầu khởi động lại, một thông báo ***Microsoft Internet Explorer*** xuất hiện, nhắc nhở bạn khởi động lại hệ thống. Nhấn ***OK*** để khởi động lại hệ thống.

Bài tập thực hành 5-2: Cấu hình Automatic Updates

Trong bài tập thực hành này, bạn cấu hình ***Automatic Update*** để tải các bản cập nhật theo một thời gian lập lịch có trước.

1. Đăng nhập vào Windows Server 2003 bằng tài khoản ***Administrator***
2. Nhấn ***Start***, trỏ vào ***Control Panel*** và sau đó nhấn ***System***. Hộp thoại ***System Properties*** xuất hiện.
3. Lựa chọn thẻ ***Automatic Updates***
4. Trong hộp ***Settings***, lựa chọn ***Automatically Download The Updates***, ***And Install Them On The Schedule That I Specify***
5. Trong danh sách lập lịch xổ xuống, lựa chọn ***Every Sunday*** và ***6:00 A.M***, sau đó nhấn ***OK***.

Bài tập thực hành 5-3: Giải nén một bản Service Pack

Trong bài tập thực hành này, bạn sẽ giải nén phiên bản mạng của một bản ***service pack*** vào trong một cấu trúc folder.

1. Đăng nhập vào máy tính bằng tài khoản ***Administrator***
2. Mở ***Windows Explorer*** và tạo ra một folder trên ổ C: có tên là ***temp***
3. Lấy bản ***service pack*** cho Windows Server 2003 hoặc Windows XP từ trang Web của Microsoft hoặc từ giảng viên của bạn và sao chép nó vào trong folder ***temp*** mà bạn vừa tạo ra.
4. Nhấn vào ***Start***, trỏ vào ***All program***, trỏ vào ***Accessories*** và lựa chọn ***Command Prompt***. Một cửa sổ dấu nhắc dòng lệnh xuất hiện
5. Trong cửa sổ dòng lệnh, nhập vào ***cd \temp***. Một dấu nhắc ***C:\temp>*** xuất hiện. Tại dấu nhắc, nhập vào tên đầy đủ của file ***service pack*** đã tải về, theo sau là dấu cách và khóa chuyển ***/X***, giống như trong ví dụ sau: **xpsp1.exe /X**
6. Sau đó nhấn ***Enter***. Một hộp thoại ***Directory For Extracted Files*** xuất hiện
7. Nhấn ***OK*** để chấp nhận folder mặc định ***C:\temp***. Chương trình cài đặt sẽ tạo ra một folder mức cha ***i386*** trong folder ***tem***p chứa các file cài đặt ***service pack*** đã giải nén.
8. Đóng cửa sổ ***Command Prompt***

CÁC CÂU HỎI ÔN TẬP

1. Bạn đang cấu hình một cơ sở hạ tầng ***Software Update Services*** sử dụng kiến trúc cha/con lỏng lẻo. Một máy chủ được đồng bộ các dữ liệu ***metadata*** và nội dung từ ***Windows Update***. Các máy chủ khác (một máy trong một site) được đồng bộ nội dung từ máy chủ SUS mức cha. Các bước nào sau đây được yêu cầu để hoàn thành cơ sở hạ tầng SUS? (Lựa chọn tất cả các câu trả lời đúng)
    a. Cấu hình máy khách ***Automatic Update*** sử dụng ***Control Panel*** trong mỗi máy.
    b. Cấu hình ***GPO*** để hướng các máy khách vào máy chủ ***SUS*** trong site của chúng.
    c. Cấu hình một điểm phân phối nội dung một cách thủ công
    d. Phê chuẩn các bản cập nhật bằng cách sử dụng trang quản trị SUS trên các máy chủ mức con
2. Bạn đang cấu hình SUS cho một nhóm các máy chủ Web. Bạn muốn các máy chủ Web này tự cập nhật hàng đêm dựa trên một danh sách các bản cập nhật được phê chuẩn trên máy chủ SUS. Tuy nhiên, khi một người quản trị đăng nhập vào, thực hiện việc bảo trì vào lúc đêm muộn trên máy chủ Web và bạn không muốn cài đặt các bản cập nhật vì có thể yêu cầu khởi động lại làm ảnh hưởng đến các tác vụ này. Chính sách cấu hình ***Windows Update*** nào mà bạn sử dụng trong kịch bản này?
    a. Notify For Download And Notify For Install
    b. Auto Download And Notify For Install
    c. Auto Download And Schedule The Install
    d. ***Auto Download And Install Immediately***
3. Bạn muốn tất cả máy khách trên mạng tải và cài đặt các bản cập nhật một cách tự động vào giờ đêm và bạn đã cấu hình lập lịch cách cài đặt cho ***Automatic Update***. Tuy nhiên, bạn phát hiện ra rằng một số người dùng tắt máy tính của họ vào buổi đêm và các bản cập nhật không được áp dụng. Chính sách nhóm nào cho phép bạn xử lý tình huống này mà không phải thay đổi lịch cài đặt?
    a. Chỉ định một ***Intranet Microsoft Update Service Location***

   b. No Auto-Restart For Scheduled Automatic Updates Installations

   c. ***Reschedule Automatic Updates Scheduled Installations***

   d. Cấu hình ***Automatic Updates***

4. Lệnh nào bạn muốn sử dụng để giải nén file đơn bạn tải của một bản ***service pack***?

   a. Setup.exe -u

   b. Update.exe -x

   c. ***Update.msi***

   d. Servicepackname.exe –x

5. Chế độ giấy phép hợp lý trong Windows Server 2003 (Lựa chọn tất cả các câu trả lời đúng)

   a. ***Per User***

   b. ***Per Server***

   c. ***Per Seat***

   d. ***Per Device hay Per User***

6. Bạn đang thuê một đội ngũ để giải quyết một dự án phát triển phần mềm. Sẽ có ba ca cho sáu lập trình viên. Mỗi lập trình viên sử dụng bốn máy tính để lập trình và kiểm thử phần mềm, phần mềm này xác thực qua một máy tính Windows Server 2003. Số CAL tối thiểu mà bạn yêu cầu nếu máy chủ này đang ở trong chế độ giấy phép ***Per Device*** hay ***Per User***?

   a. 6

   b. 4

   c. 18

   d. 24

7. Công cụ nào cho phép bạn nhận biết máy chủ giấy phép của site trong site của bạn ?

   a. ***Active Directory Domains And Trusts***

   b. Công cụ ***Licensing trong Control Panel***

   c. ***Active Directory Sites And Services***

   d. ***DNS***

8. Bạn quản trị một mạng cho một đội ngũ gồm 500 nhân viên kinh doanh điện thoại. Bạn có 550 giấy phép cấu hình trong chế độ giấy phép ***Per Device*** hay ***Per User***. Một chiến dịch mới được khởi động và bạn sẽ phải thuê thêm một ca làm việc nữa cho 500 nhân viên này. Bạn cần làm gì để quản lý hiệu quả nhất việc theo dõi và kiểm tra việc thực hiện có đúng theo các giấy phép này không ?
    a. Yêu cầu lại các giấy phép từ các máy khách đã có sẵn
    b. Xóa các giấy phép cũ và mua thêm 500 giấy phép mới
    c. Tạo ra các nhóm giấy phép
    d. Chuyển đổi chế độ giấy phép ***Per Server***

CÁC KỊCH BẢN TÌNH HUỐNG

Kịch bản 5-1. Triển khai Microsoft SUS

Bạn là người quản trị mạng cho một doanh nghiệp cỡ vừa và đang quan tâm xem xét việc triển khai SUS một cách rộng rãi trên các máy trạm Windows XP Professional và các máy Windows Server 2003. Trước khi triển khai đại trà việc này, một chương trình triển khai thí điểm được sẽ được thực hiện. Bạn được giao cho một phòng Lab với 10 máy tính Windows XP Professional, một máy chủ thành viên chạy Windows Server 2003, một máy chủ quản trị miền chạy Windows Server 2003 và một máy chủ đơn chạy Windows Server 2003. bạn muốn cấu hình tất cả các máy tính ngoại trừ máy chủ SUS để thực hiện việc tự động kết nối đến máy chủ SUS mỗi buổi sáng vào lúc 7.A.M để tải và cài đặt các bản cập nhật mới. Bạn phải thực hiện các bước nào sau đây để hoàn thành nhiệm vụ trên ? (Lựa chọn tất cả các câu trả lời đúng)

Sử dụng thẻ ***Automatic Update*** trong hộp thoại ***System Properties*** trong tất cả các máy trạm Windows XP để thiết lập máy chủ cập nhật là địa chỉ của máy chủ SUS. Thiết lập tất cả các máy trạm Windows XP tự động tải và cài đặt các bản cập nhật vào lúc 7 A.M mỗi ngày.

a) Sử dụng thẻ ***Automatic Update*** trong hộp thoại ***System Properties*** trong tất cả các máy tính Windows Server 2003 ngoại trừ máy chủ SUS để thiết lập máy chủ cập nhật là địa chỉ của máy chủ SUS. Thiết lập tất cả các máy tính Windows Server 2003 tự động tải và cài đặt các bản cập nhật vào lúc 7 A.M mỗi ngày.

b) Đặt các máy trạm Windows XP và máy chủ quản trị miền Windows Server 2003 trong một OU riêng biệt có tên ***SUStest***. Cấu hình thuộc

tính ***Windows Update*** của GPO sẽ áp dụng cho ***OU SUStest***, chỉ ra địa chỉ của máy chủ cập nhật là máy chủ SUS trong phần chính sách ***Specify Intranet Microsoft Update Service Location***. Thiết lập ***Configure Automatic Updates Policy to Automatic Download And Schedule The Install*** và thiết lập lịch cài đặt là hàng ngày và thời gian là 7 A.M. Áp dụng ***GPO*** này vào ***OU SUStest***

c) Trên máy tính Windows Server 2003 đơn, cấu hình thuộc tính ***Windows Update*** trong ***GPO*** nội bộ của máy, chỉ định địa chỉ của máy chủ cập nhật là máy chủ SUS trong phần chính sách ***Specify Intranet Microsoft Update Service Location***. Thiết lập ***Configure Automatic Updates Policy to Automatic Download And Schedule The Install*** và thiết lập lịch cài đặt là hàng ngày và thời gian là 7 A.M. Áp dụng ***GPO*** này vào ***OU SUStest***

d) Trên máy chủ SUS, cấu hình thuộc tính ***Windows Update*** trong GPO nội bộ của máy, chỉ định địa chỉ của máy chủ cập nhật là máy chủ SUS trong phần chính sách ***Specify Intranet Microsoft Update Service Location***. Thiết lập ***Configure Automatic Updates Policy to Automatic Download And Schedule The Install*** và thiết lập lịch cài đặt là hàng ngày và thời gian là 7 A.M. Áp dụng ***GPO*** này vào ***OU SUStest***

Kịch bản 5-2: Triển khai một bản service pack

Fred là người quản trị hệ thống cho một văn phòng học viện tại một trường đại học. Văn phòng có 40 máy trạm Windows XP và 2 máy chủ Windows Server 2003. Một trong hai máy chủ này được cấu hình thành một máy chủ quản trị miền, còn lại là máy chủ dịch vụ file và in ấn. Các máy tính trong văn phòng là thành viên của một miền Windows Server 2003 đơn. Microsoft gần đây có phát hành một bản ***service pack*** cho Windows XP và, sau khi kiểm thử nó, Fred cảm thấy đủ tự tin để triển khai bản ***service pack*** trên cho các máy trạm Windows XP trong văn phòng. Anh ta giải nén file ***service pack*** vào một folder trên máy chủ file là ***\\Fileshare\newsrvpk***. phương pháp nào sau đây có thể sử dụng được để cài đặt bản ***service pack*** trên tất cả các máy trạm Windows XP? (Lựa chọn tất cả các câu trả lời đúng)

a) Anh ta có thể vào từng máy Windows XP và cài đặt bản ***service pack*** một cách thủ công từ file chia sẻ này

b) Anh ta có thể tạo ra một nhóm có tên là ***Xpwkstn*** và đặt tất cả các máy trạm Windows XP vào trong nhóm đó. Sau đó anh ta có thể tạo ra một GPO trong đó cấu hình gói phần mềm mới trong mục ***Computer***

Configuration\Software Settings, sử dụng địa chỉ của file ***.msi*** của bản ***service pack*** trên folder chia sẻ ***\\Fileshare\newsrvpk***. Trong hộp thoại ***Deploy Software***, anh ta lựa chọn ***Assign*** và sau đó áp dụng ***GPO*** này vào nhóm ***Xpwkstn***

c) Anh ta có thể tạo ra một nhóm có tên là ***Xpusrs*** và đặt tất cả các người dùng sử dụng máy trạm Windows XP vào trong nhóm đó. Sau đó anh ta có thể tạo ra một ***GPO*** trong đó cấu hình gói phần mềm mới trong mục ***Computer Configuration\Software Settings***, sử dụng địa chỉ của file ***.msi*** của bản ***service pack*** trên folder chia sẻ ***\\Fileshare\newsrvpk.*** Trong hộp thoại ***Deploy Software***, anh ta lựa chọn ***Assign*** và sau đó áp dụng ***GPO*** này vào nhóm ***Xpusrs***

d) Anh ta có thể tạo ra một ***OU*** có tên là ***Xpwkstn*** và đặt tất cả các máy trạm Windows XP vào trong OU đó. Sau đó anh ta có thể tạo ra một ***GPO*** trong đó cấu hình gói phần mềm mới trong mục ***Computer Configuration\Software Settings***, sử dụng địa chỉ của file ***.msi*** của bản ***service pack*** trên folder chia sẻ ***\\Fileshare\newsrvpk***. Trong hộp thoại ***Deploy Software***, anh ta lựa chọn ***Assign*** và sau đó áp dụng ***GPO*** này vào ***OU Xpwkstn***

PHẦN 2
QUẢN LÝ VÀ DUY TRÌ HỆ ĐIỀU HÀNH

CHƯƠNG 6: LÀM VIỆC VỚI TÀI KHOẢN NGƯỜI DÙNG

Trước khi bất cứ người dùng nào có thể truy nhập vào máy tính chạy Microsoft Windows 2003 từ bất cứ bảng điều khiển nào hoặc qua mạng thì học đều phải được xác thực. Xác thực là một quá trình nhận dạng và xác nhận các điều kiện của người dùng. Trong hầu hết các trường hợp, quá trình xác thực yêu cầu người dùng cung cấp tên tài khoản và mật khẩu để máy chủ kiểm tra bản ghi đó trước khi truy nhập. Quản lý tài khoản người dùng và mật khẩu là một trong các tác vụ thông thường của người quản trị. Trong chương này, các bạn sẽ học cách tạo, quản lý và xử lý các tình huống xảy ra đối với tài khoản người dùng.

Sau khi hoàn thành chương này, bạn có khả năng:

- **Hiểu được sự khác nhau giữa tài khoản người dùng cục bộ, tài khoản người dùng miền.**
- **Lập kế hoạch tạo tài khoản người dùng.**
- **Tạo và quản lý tài khoản người dùng.**
- **Tạo và quản lý tài khoản người dùng bằng mẫu (*template*), nhập vào từ nguồn có sẵn và các công cụ dạng dòng lệnh.**
- **Quản lý khái lược người dùng (*User Profile*)**
- **Hiểu được sự khác nhau giữa các khái lược cục bộ (*Local*), di trú (*Roaming*) và bắt buộc (*Mandatory*).**
- **Xử lý các tình huống đối với việc xác thực người dùng.**

TÌM HIỂU TÀI KHOẢN NGƯỜI DÙNG (USER ACCOUNT)

Mạng Microsoft Windows dựa trên hai mô hình tổ chức thường được biết đến là nhóm (***Group***) và miền (***Domain***). Cả hai mô hình này đều yêu cầu NSD có Tài khoản Người dùng để xác thực. Nhưng về mặt bản chất các tài khoản người dùng và các công cụ dùng để tạo và quản lý chúng đối với hai mô hình này có khác nhau đôi chút. Các điểm khác nhau giữa tài khoản người dùng cục bộ sử dụng cho nhóm và tài khoản người dùng miền được tổng kết trong bảng 6-1.

Bảng 6-1 Các đặc điểm của *Local User Name* và *Domain User Name*.

	Local User Names	**Domain User Names**
Công cụ quản lý	Local Users And Groups	Active Directory Users And Computers
Nơi chứa tài khoản người dùng.	Trình Quản lý các Tài khoản Bảo mật (SAM-Security Accounts Manager) trên mỗi máy tính cục bộ.	CSDL Active Directory
Nơi đăng nhập	Máy tính cục bộ	Miền Active Directory
Truy nhập tới	Tài nguyên trên máy tính cục bộ	Tài nguyên trên miền và trên mạng.

NHÓM LÀM VIỆC (*Workgroup*)

Nhóm làm việc (***Workgroup***) là tập hợp các máy tính mà trong đó chúng tương tác một cách không chính thức với quyền không tập trung. Mỗi máy tính trong nhóm có một tập các tài khoản người dùng cục bộ riêng để lưu tại cơ sở dữ liệu của máy tính này, được gọi là Trình Quản lý các Tài khoản Bảo mật (SAM - ***Sercurity Accounts Manager***). Các máy tính sử dụng các tài khoản này để xác thực và cho phép người dùng truy nhập vào tài nguyên chỉ trên riêng máy tính này. Nếu muốn truy nhập vào tài nguyên trên máy tính khác trong nhóm thì người dùng phải có các tài khoản khác trên chính các máy tính đó và được nó xác thực bởi tách biệt riêng trước khi được phép truy nhập vào.

Mặc dù mỗi máy tính trong nhóm thực hiện việc xác thực riêng của mình nhưng không nhất thiết người dùng phải cung cấp tên tài khoản và mật khẩu kết nối tới từng máy tính. Nếu mỗi máy tính đều có tài khoản cho người

dùng có cùng tên tài khoản và cùng mật khẩu thì tất cả các lần xác thực sau lần đầu tiên sẽ thực hiện ngầm và tự động.

Để tạo tài khoản người dùng cục bộ, bạn sử dụng MMC snap-in gọi tới ***Local User and Group***. Muốn đăng nhập bằng tài khoản người dùng cục bộ, tại hộp thoại ***Log On To Windows*** bạn cung cấp tên tài khoản, mật khẩu và chọn ***This Computer*** tại danh sách ***Log On To***.

Quá trình tạo tài khoản người dùng cục bộ khá đơn giản, nhưng hạn chế của mô hình nhóm làm việc là buộc người quản trị duy trì các tài khoản cho cùng một người dùng trên đồng thời nhiều máy tính khác nhau. Ví dụ, nếu người dùng có tài khoản trên 10 máy tính khác nhau thì bạn phải thay đổi mật khẩu từng tài khoản riêng rẽ trên 10 máy tính. Vì vậy, mô hình nhóm làm việc là không thực tế, trừ khi đó là mạng nhỏ.

MIỀN (Domain)

Mô hình miền do Microsoft Windows 2003, Microsoft Windows XP và Microsoft Windows 2000 sử dụng dựa trên nền tảng dịch vụ ***Microsoft Active Directory.***

Trong chương 1, bạn đã hiểu về kiến trúc và chức năng của ***Active Directory.*** Các Tài khoản Người dùng ***Active Directory*** nằm dưới dạng của các Đối tượng Người dùng, và chúng được lưu, cũng giống như tất cả các thông tin của Active Directory, trên máy tính điều khiển miền, nơi mà chúng có thể được truy nhập tới từ mọi nơi trong miền. Khi đăng nhập bằng tài khoản người dùng miền người dùng sẽ được xác thực bởi máy chủ điều khiển miền, chứ không phải bởi máy tính mà người dùng đang làm việc hoặc truy nhập vào.

Tài khoản người dùng miền gồm có tên đăng nhập và mật khẩu, tên này là duy nhất và được gọi là mã nhận dạng bảo mật (***SID - Security Identifier***). Trong khi đăng nhập, ***Active Directory*** xác thực tên người dùng và mật khẩu đưa vào. Tiếp theo, hệ thống bảo mật sẽ tạo thẻ truy nhập tương ứng với người dùng này. Thẻ truy nhập chứa mã nhận dạng bảo mật của tài khoản người dùng và mã nhận dạng bảo mật các nhóm của người dùng này. Thẻ này sau đó có thể được sử dụng để kiểm tra lại quyền đã gán cho người dùng, bao gồm cả quyền đăng nhập cục bộ và quyền được phép truy nhập vào tài nguyên được bảo mật bởi danh sách điều khiển truy nhập(ACLs-Access Control Lists).

Trong mô hình miền, mỗi người dùng chỉ có một tài khoản miền, nhờ vậy sẽ giảm nhẹ công việc của người quản trị mạng. Chỉ một tài khoản này có thể được người dùng sử dụng để truy nhập vào mọi tài nguyên trên mạng. CSDL ***Active Directory*** thường xuyên được đồng bộ giữa các máy tính điều khiển

miền, nên các tài khoản người dùng gần như luôn sẵn sàng xác thực cho người dùng truy nhập tới tài nguyên mới.

Người Quản trị sử dụng snap-in ***Active Directory User and Computer*** để tạo đối tượng người dùng miền . Để đăng nhập bằng tài khoản người dùng miền bạn phải cung cấp tên tài khoản, mật khẩu và tại ***Log On To*** lựa chọn miền muốn đăng nhập, chỉ ra trong hình 6-1.

Hình 6-1: Hộp thoại đăng nhập vào Windows

> ***LƯU Ý: Đăng nhập vào máy tính điều khiển miền.*** *Khi máy tính Microsoft Windows 2003 đóng vai trò là máy tính điều khiển miền thì không có sự lựa chọn nào khác nngoại trừ việc đăng nhập vào miền. Tài khoản người dùng cục bộ và snap-in* ***Local User And Group*** *cũng không được sử dụng.*

LẬP KẾ HOẠCH TÀI KHOẢN NGƯỜI DÙNG

Khi bạn thực sự bắt tay vào việc tạo tài khoản người dùng cục bộ hoặc tài khoản người dùng miền, bạn nên cân nhắc giữa các kế hoạch được vạch ra, nhất là khi bạn làm việc với một mạng lớn và phức tạp. Mặc dù việc tạo tài khoản người dùng ban đầu dường như là đơn giản, thu thập các tên và lựa chọn tài khoản, mật khẩu cho phép và cấu trúc của phân cấp ***Active Directory*** sẽ giúp bạn giải quyết các vấn đề sau này.

ĐẶT TÊN CHO TÀI KHOẢN

Khi bạn tạo tài khoản người dùng, cả dạng cục bộ và miền, bạn phải xác định ***Firt Name*** (Tên gọi) và ***Last Name*** (Họ) của người dùng, nhưng thực sự được dùng khi đăng nhập và xác thực là **tên tài khoản**. Tên của tài khoản người dùng cục bộ và tài khoản người dùng miền có độ dài tối đa cho phép là 20 ký tự, nhưng để thuận lợi cho người dùng nên đặt ngắn hơn. Các tên không phân biệt chữ hoa chữ thường (mặc dù Microsoft Windows 2003 giữ nguyên kiểu chữ bạn nhập vào) và không được chứa các ký tự sau:

“ / \ [ ] : ; | = , + * ? < > @

> ***LƯU Ý: tên tài khoản và địa chỉ thư điện tử.*** *Khi tạo tên tài khoản mà đồng thời muốn sử dụng chúngcho địa chỉ E-mail, phải đảm bảo chắc chắn nó chỉ gòm các ký tự cho phép của phần mềm E-Mail, một số hệ thống E-mail không cho phép sử dụng tên có dấu cách hoặc dấu ngoặc đơn, cho dù nó vẫn được Microsoft Windows 2003 chấp nhận..*

Dạng của tên tài khoản, tại nhiều tổ chức sử dụng một số kiểu kết hợp của ***Firt Name*** hoặc ***Last Name*** và một hoặc thêm các chữ cái đầu. Ví dụ , tên người dùng là Mark Lee có thể có tên tài khoản là “mlee” hoặc “markl”, Mặc dù vậy, đối với các tổ chức có qui mô lớn, sử dụng ***First Name*** là không thực tế vì rất dễ có hai người cùng tên là Mark, thậm chí rất có thể cả hai Mark đều có ***Last Name*** bắt đầu bằng chữ “L".

Cho dù bạn sử dụng bất cứ dạng nào cho Tên Tài khoản của bạn, Điều quan trọng nhất là bạn phải tạo được một tập các luật để tạo ra chúng và trung thành với chúng. Việc gán các tên tài khoản một cách không thống nhất, sử dụng các biệt hiệu (***Nickname***) tối nghĩa hay theo sở thích của người sử dụng sẽ dẫn đến việc nhầm lẫn của các quản trị khác khi xác định tên tài khoản cho một người sử dụng cụ thể nào đó. Luật của bạn nên chỉ ra một sự kết hợp chuẩn giữa ***First Name*** và ***Last Name*** hay các chữ viết tắt, cũng như các phương pháp được chuẩn hóa để tạo ra các tên tài khoản duy nhất. và khi bạn nghe tên tài khoản bạn có thể dễ dàng suy ra được tên người dùng .

LỰA CHỌN MẬT KHẨU

Ngày nay, bảo mật ảnh hưởng mạnh mẽ đến nhiệm vụ của quản trị trên toàn mạng và việc tạo tài khoản người dùng cũng không thuộc ngoại lệ. Khi tạo tài khoản người dùng mới bạn phải xác định mật khẩu và áp dụng chính sách với mật khẩu tuỳ theo mức độ bảo mật mà tổ chức của bạn muốn.

Mặc định, khi tạo tài khoản người dùng miền trong Microsoft Windows 2003, bạn phải đặt mật khẩu dạng phức tạp, có độ dài tối thiểu 7 ký tự. Những ràng buộc này bược ấn định tại chính sách nhóm, được cấu hình mặc định tại ***Default Domain Policy Group Object*** - GPO. Tài khoản người dùng cục bộ sẽ không bị các ràng buộc này. Bạn có thể điều chỉnh lại các ràng buộc và các quy tắc gán mật khẩu mặc định bằng cách sử dụng bảng điều khiển ***Group Policy Object Editor*** để sửa lại các thiết lập chính sách mật khẩu.

- **Enforce Password History**: Xác định số lượng mật khẩu khác nhau trước khi người dùng được phép sử dụng lại mật khẩu cũ, giá trị mặc định là 24.

- **Maximun Password Age (*Tuổi dài nhất của mật khẩu)***: Xác thời gian bao lâu một mật khẩu có thể được dùng trước khi hệ điều hành buộc người dùng đổi lại, giá trị mặc định là 42 ngày.
- **Minimun Password Age (*Tuổi ngắn nhất của mật khẩu*):** Xác thời gian bao lâu một mật khẩu phải sử dụng trước khi hệ điều hành cho phép người dùng đổi lại, giá trị mặc định là 1 ngày.
- **Minimum Password Length (*Độ dài mật khẩu tối thiểu*)**: Độ dài tối thiểu của mật khẩu mà hệ điều hành cho phép, giá trị mặc định là 7.
- **Password Must Meet Complexity Requirements *(Mật khẩu phải thỏa mãn điều kiện phức tạp)***: Xác định điều kiện đối với mật khẩu như độ dài ít nhất là 6 ký tự, không trùng với toàn bộ tên hoặc một phần của tên tài khoản, bao gồm ít nhất 3 trong số 4 kiểu kí tự: Chữ hoa, chữ thường, số và ký tự đặc biệt. Mặc định, hệ điều hành ***enable*** (*cho phép*) chính sách này.

Các thiết lập mặc định cho người dùng mới là thiết lập ***User Must Change Password At Next Logon*** (*Người dùng bắt buộc phải đổi mật khẩu tại lần đăng nhập sau*). Thiết lập này giả sử là các người dùng sẽ có trách nhiệm cung cấp mật khẩu của họ và thay đổi chúng định kỳ. Người quản trị tạo tài khoản chỉ là cấp mật khẩu tạm thời cho lần đăng nhập đầu tiên của người dùng.

Việc bạn muốn người dùng cung cấp mật khẩu của họ là một quyết định về bảo mật mà bạn phải thực hiện trước khi bạn bắt tay vào tạo tài khoản. Nói chung, việc người dùng tự cấp mật khẩu là thông dụng hơn vì hai lý do, một là sẽ dễ dàng hơn cho người dùngđể nhớ được mật khẩu và hai là việc phải thay đổi mật khẩu định kỳ 42 ngày một lần sẽ là gánh nặng lớn đối với quản trị mạng. Chính sách mật khẩu mặc định bắt người dùng thay đổi định kỳ thay đổi lại mật khẩu đồng thời cũng ngăn cản việc họ sử dụng lại cùng một mật khẩu thường xuyên.

Tùy thuộc vào yêu cầu bảo mật mạng, bạn có thể muốn thiết lập các chính sách mật khẩu khác cho người dùng mà không thể thực hiện bằng phần mềm được, như:

- Không tiết lộ mật khẩu cho đồng nghiệp hoặc với bất kỳ ai trong hoặc ngoài tổ chức
- Không ghi mật khẩu và để ở nơ có thể dễ dàng được tìm thấy
- Không tạo mật khẩu sử dụng thông tin như ngày sinh, tên, con hoặc vật nuôi.
- Nói mật khẩu qua điện thoại hoặc gửi bằng thư điện tử.

THIẾT KẾ MÔ HÌNH PHÂN CẤP ACTIVE DIRECTORY

Do các tài khoản người dùng cục bộ không được dự định dùng trong các mạng lớn, chúng được lưu tại cơ sở dữ liệu dạng CSDL không phân cấp. SAM thực sự nhỏ hơn một danh sách người dùng và nhóm với một vài thuộc tính chính cơ bản cho mỗi tài khoản. Do vậy không cần có một thiết kế cho loại tài khoản này. Ngược lại, Tài khoản người dùng miền là một phần của kiến trúc ***Active Directory***, và việc thiết kế kiến trúc này là một phần rất quan trọng của kế hoạch cơ sở hạ tầng mạng.

Như bạn đã tìm hiểu tại chương 1, cấu trúc cơ bản của miền ***Active Directory*** là theo kiểu hình cây, tương tự như cấu trúc thư mục của hệ thống file. Trong đó, đối tượng miền là ngọn của cây (đôi khi cũng được gọi là gốc) và với một hoặc một số phân cấp dưới nó là OU - ***Organization Unit***(*đơn vị tổ chức*). Tốt nhất là chúng ta nên giành các tác vụ thực sự của việc thiết kế kiến trúc này cho các nhà thiết kế mạng, nhưng người quản trị có trách nhiệm tạo các tài khoản người dùng cần biết rõ các kiến trức này và các mô hình cơ sở đã tạo nên chúng.Để tạo người dùng miền, đầu tiên là bạn phải quyết định đặt họ vào OU nào. Quyết định này dựa vào chức năng của OU đã tạo. Cây Active Directory thiết kế có thể dựa vào chính sách phân chia của tổ chức như theo phòng ban, theo nhóm hoặc vị trí địa lý như toàn nhà, tầng, văn phònghoặc hết hợp của các yếu tố trên và nhiều các yếu tố khác nữa. Mục đích của phân cấp giúp đơn giản hoá việc định vị cácc đối tượng trong cây và thực hiện việc gán các thuộc tính cho một số lượng lớn các đối tượng bằng cách gán chúng cho các OU và các thuộc tính này, lập tức sẽ được các dối tượng con thừa hưởng theo kiến trúc hình cây.

Đặt các đối tượng người dùng vào đúng vị trí trong kiến trúc sẽ giúp chúng sẽ nhận được các thiết lập cấu hình cần thiết mà không phải thực hiện cấu hình đơn lẻ và tránh cho bạn không phải di chuyển các người dùng sau này.

LÀM VIỆC VỚI TÀI KHOẢN NGƯỜI DÙNG CỤC BỘ

Tài khoản cục bộ được phép truy nhập vào tài nguyên trên máy tính mà bạn đã tạo tài khoản đó từ bảng điều khiển hoặc qua mạng. Mặc định, Microsoft Windows 2003 sẽ tạo 3 tài khoản người dùng cục bộ sau:

Administrator (*Quản trị*): Tài khoản này yêu cầu cho lần đăng nhập hệ thống đầu tiên, sử dụng mật khẩu được cấp trong quá trình cài đặt hệ thống. Người dùng ***Administrator*** là thành viên nhóm ***Administrators***, có toàn quyền truy nhập đến mọi nơi trong hệ thống. Bao gồm cả việc có thể khởi

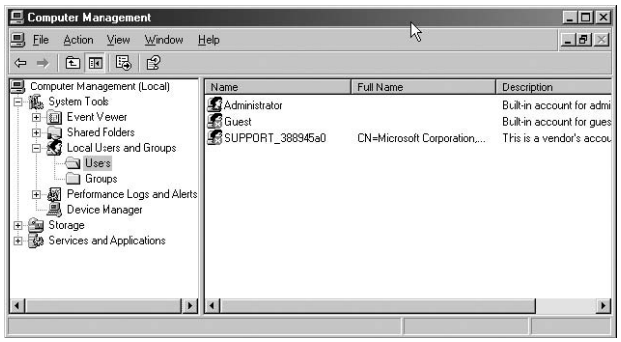
tạo tài khoản người dùng cục bộ, phân quyền cho các tài khoản người dùng cục bộ, cài đặt phần cứng và phần mềm.

Tài khoản ***Administrator*** cục bộ luôn được cần đến, thậm chí trên mạng ***Active Directory,*** do có các công việc đòi hỏi ***Administrator*** cục bộ truy nhập tới chính máy tính này.

Guest (*Khách*): Tài khoản sử dụng cho người dùng tạm thời và bị giới hạn truy nhập vào hệ thống. Tài khoản này sẽ được tạo tự động trong quá trình cài đặt hệ thống, mặc định sẽ được để ở trạng thái vô hiệu hoá và không có mật khẩu. Bạn cần phải kích hoạt (***Enable***) tài khoản này trước khi có bất ký một ai đó sử dụng nó để đăng nhập. Tài khoản ***Guest*** là thành viên của nhóm ***Guests*** và bị giới hạn quyền truy nhập vào hệ thống. Trong hầu hết các trường hợp, bạn nên vô hiệu hoá nó và tạo các tài khoản mới, riêng cho các người dùng cụ thể thay cho việc cho họ đăng nhập vào tất cả đều sử dụng tài khoản ***Guest***.

SUPPORT_number Tài khoản này tạo cho Nhân viên Hỗ trợ Kỹ thuật của Microsoft khi họ kết nối vào hệ thống sử dụng tính năng ***Remote Assistance***. Mặc định tài khoản này ở trạng thái vô hiệu hoá và phải được kích hoạt trước khi ký thuật viên của Microsoft có thể truy nhập vào máy tính.

Nếu máy tính được kết nối vào miền không cần thiết tạo thêm tài khoản người dùng cục bộ bởi vì người dùng sẽ đăng nhập sử dụng tài khoản người dùng miền và từ đó có thể truy nhập vào tài nguyên hệ thống. Nhưng nếu máy tính cấu hình tham gia vào nhóm làm việc thì bạn có thể tạo tài khoản người dùng cục bộ mới bằng cách sử dụng snap-in ***Local Users And Groups***. Tại máy không phải là máy chủ điều khiển miền, snap-in này được tích hợp với bảng điều khiển ***Computer Managerment*** chạy từ nhóm chương trình ***Administrator Tools*** tại thực đơn ***Start***Thực đơn

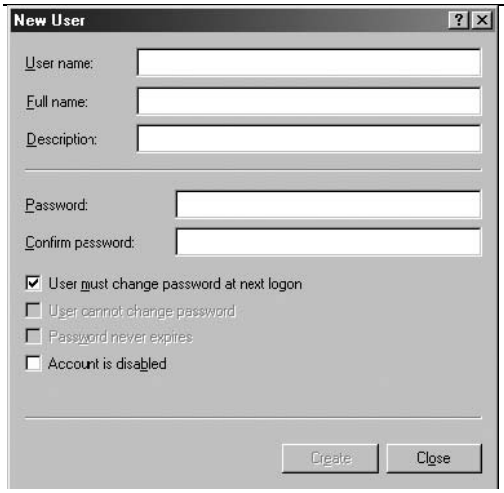


Hình 6-2: Snap-in *Local Users and Groups*

TÀI KHOẢN NGƯỜI DÙNG CỤC BỘ

Để tạo tài khoản người dùng cục bộ bạn chọn Folder ***User*** từ thực đơn ***Action***, sẽ xuất hiện hộp thoại (hình 6-3), bạn đưa vào các thông tin sau:

- **User Name:** Tên tài khoản để đăng nhập vào máy tính (bắt buộc).
- **Full Name:** Tên đầy đủ của người dùng (tuỳ chọn).
- **Description:** Diễn giải về người dùng hoặc chức năng của người dùng (tuỳ chọn).
- **Password**: mật khẩu để xác thực người dùng, có độ dài tối đa là 127 ký tự (tuỳ chọn).
- **Confirm Password**: Vào lại mật khẩu thêm một lần nữa để chắc chắn bạn đã gõ vào đúng. Nếu hai lần không trùng khớp nhau thì sẽ yêu cầu bạn vào lại thêm một lần nữa.
- **User Must Change Password At Next Logon**: Chọn lựa chọn này nếu bạn muốn người dùng thay đổi lại mật khẩu khi đăng nhập vào hệ thống lần đầu. Bạn sẽ không thể chọn lựa chọn này nếu bạn đã chọn ***Password Nerver Expires (****Mật khẩu không gới hạn thời gian)***. Lựa chọn này cũng sẽ tự động xoá bỏ lựa chọn ***User Cannot Change Password (****Người dùng không thay đổi được mật khẩu)*
- **User Cannot Change Password**: Chọn lựa chọn này, người dùng sẽ không thay đổi lại được mật khẩu, thường thì bạn sẽ dùng lựa chọn này khi có đồng thời từ hai người trở lên dùng chung một tài khoản người dùng miền hoặc bạn muốn quản lý dịch vụ mật khẩu người dùng. Bạn không thể chọn lựa chọn này nếu đã chọn ***User Must Change Password At Next Logon***.
- **Password Nerver Expires:** Bạn chọn lựa chọn này nếu muốn mật khẩu không bao giờ bị hết hạn. Bạn sẽ không chọn được lựa chọn này nếu bạn đã chọn ***User Must Change Password At Next Logon***. Thường bạn sẽ chọn lựa chọn này để quản lý dịch vụ mật khẩu tài khoản.
- **Account Is Disable:** Chọn lựa chọn này để vô hiệu hoá tài khoản, ví như là cho nhân viên mới, nhưng người này lại chưa cần truy nhập vào mạng.

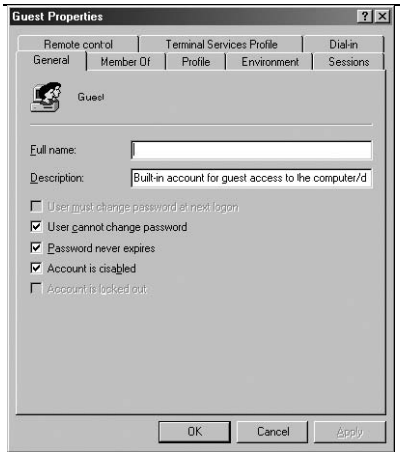


Hình 6-3: Hộp thoại *New User*

QUẢN LÝ TÀI KHOẢN NGƯỜI DÙNG CỤC BỘ

Tài khoản người dùng cục bộ có tương đối ít các thuộc tính. Bạn chọn ***Account*** tại Folder ***Users*** từ snap-in ***Local User And Group*** và chọn ***Properties từ*** Thực đơn ***Action.*** Hộp thoại ***Properties*** sẽ xuất hiện (chỉ ra tại hình 6-4). Hộp thoại này cho phép bạn sửa lại các thuộc tính trong khi tạo tài khoản người dùng, ngoại trừ tên người dùng và mật khẩu. Để đổi lại tên bạn chọn lệnh ***Rename*** và đổi lại mật mật khẩu chọn ***Set Password*** từ Thực đơn ***Action***. Hộp thoại này cung cấp các thông số của tài khoản tại các thẻ sau:

- **General**
- **Member Of**
- **Profile**
- **Environment**
- **Sessions**
- **Remote Control**
- **Terminal Services Profile**
- **Dial-in**



Hình 6-4: Hộp thoại *Properties* của người dùng cục bộ

Thiết lập tại các thẻ giống như tại hộp thoại ***Properties*** của hộp thoại người dùng miền. Xem thêm "Quản lý tài khoản người dùng miền" tại chương sau.

LÀM VIỆC VỚI TÀI KHOẢN NGƯỜI DÙNG MIỀN

Làm việc với tài khoản người dùng miền tương tự như là với tài khoản người dùng cục bộ nhưng tài khoản người dùng miền có nhiều thông tin hơn. Khi bạn tạo miền ***Active Directory*** bằng cách thăng cấp máy tính điều khiển miền đầu tiên, Microsoft Windows 2003 mặc định sẽ tạo các người dùng sau:

- **Administrator:** Tài khoản miền ***Administrator*** là thành viên của nhóm ***Administrators*** của miền và thực hiện cùng chức năng chính như tài khoản người dùng cục bộ. Đó là tài khoản đầu tiên đăng nhập vào miền và có toàn quyền truy nhập tới tất cả các chức năng và tính năng của miền. Điều quan trọng là bạn phải phân biệt tài khoản miền ***Administrator*** và tài khoản cục bộ ***Administrator*** là hai tài khoản tách biệt nhau. Hai tài khoản này có mật khẩu khác nhau, các Cấp phép khác nhau và các khả năng khác nhau. Với máy tính chạy Microsoft Windows 2003 thì máy chủ thành viên của miền (nhưng không phải là máy chủ điều khiển miền) có thể đăng nhập sử dụng cả hai tài khoản này tuỳ theo thiết lập tại lựa chọn ***Log On To*** tại hộp thoại ***Log On To Windows***.
- **Guest:** Tương tự như tài khoản cục bộ ***Guest***, tài khoản miền ***Guest*** để ở trạng thái vô hiệu hoá và dành cho người dùng tạm thời truy nhập vào miền.

  LƯU Ý: Mục đích của bài thi*. Mục đích của bài thi 70-290 xác định bạn có thể tạo và quản lý tài khoản người dùng.*

Microsoft Windows 2003 cũng tạo các tài khoản dựng sẵn mặc định khác khi bạn cài đặt các dịch vụ trên máy tính này. Ví dụ, khi thăng cấp một máy chủ thành máy chủ điều khiển miền sẽ tạo các đối tượng người dùng ẩn gọi là ***krbtgt*** có chức năng như là Đối tượng bảo mật của dịch vụ Trung tâm Phân phối Khoá (***Key Distribution Center - KDC***). Khi bạn cài ***Microsoft Internet Information Services*** (IIS) có hai người dùng được tạo là ***IUSR_computerName*** là người dùng vô danh để kết nối tới máy chủ Web và ***IWAM_computername*** mà IIS sử dụng để khởi chạy các ứng dụng độc lập (***out-of-process***)

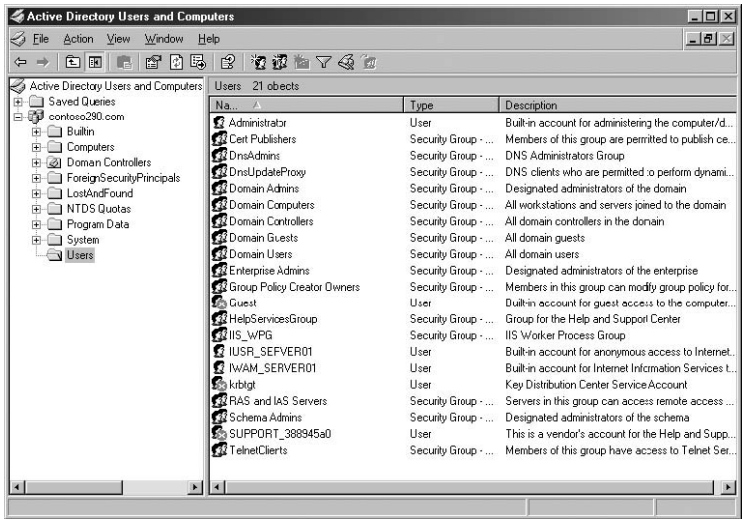
Các đối tượng người dùng dựng sẵn trong miền được đặt tại đối tượng chứa (***Container***) tên là ***Users***. Thậm chí, bạn có thể tạo đối tượng người dùng mới tại đây hoặc tại đối tượng chứa khác, thậm trí trực tiếp tại chính miền. Tốt nhất là bạn nên tạo tại OU để tiện cho việc sử dụng chính sách nhóm sau này. Bạn chỉ có thể liên kết một đối tượng chính sách nhóm (***Group Policies Objects***- GPO) với một miền, Site hoặc OU nhưng không thể liên kết với đôi tượng chứa ***Users***. Do đó, Bạn nên tạo các OU phù hợp với thiết kế ***Active Directory*** của cơ quan bạn, trước khi bạn bắt đầu tay vào tạo người dùng.

> ***LƯU Ý***: ***Các đối tượng chứa***. *Các đối tượng* ***Users, Builtin, Computers****, và* ***ForeignSecurity- Principals*** *thuộc về các lớp đối tượng đặc biệt được gọi là đối tượng chứa (****Container****). Trong Dịch vụ Thư mục (****Directory Service****) thuật ngữ* ***Container*** *được sử dụng một cách khái quát để chỉ đến một đối tượng nào đó có chứa các đối tượng con khác. Do đó, trong trường hợp bốn đối tượng đã liệt kê ở trên, theo đúng định nghĩa, đều được gọi là* ***Container****. Bạn không thể áp dụng GPOs cho bốn đối tượng chứa này, hoặc xoá nó đi hay tạo các đối tượng mới cùng kiểu. Tuy vậy, bạn có thể chuyển các đối tượng từ các* ***Container*** *này tới các đối tượng OU mà bạn tạo ra để tiện cho việc quản lý hơn.*

Trong máy chủ điều khiển miền, chạy Microsoft Windows 2003 bạn tạo đối tượng người dùng miền bằng cách sử dụng snap-in ***Active Directory Users And Computer***s (hình 6-5),. chọn từ nhóm chương trình ***Administrative Tools*** trong Thực đơn ***Start*** . Để tạo đối tượng người dùng, bạn phải là thành viên của nhóm ***Enterprise Admins, Domain Admins*** hoặc ***Account Operators*** hoặc bạn phải được uỷ quyền quản trị cần thiết để tạo đối tượng người dùng.

> ***LƯU Ý: Cài đặt bảng điều khiển.*** *Mặc dù, Bảng điều khiển* ***Active Directory Management*** *trong nhóm chương trình* ***Administrative Tools*** *chỉ có tại máy máy điều khiển miền, nhưng bạn cũng có thể*

chạy chúng từ Microsoft Windows 2003 Server, Windows XP workstations. Để cài gói ***Administrative Tools*** *bạn chạy* ***Adminpak.msi*** *từ Folder* ***I386*** *trên đĩa CD cài đặt Microsoft Windows 2003.*



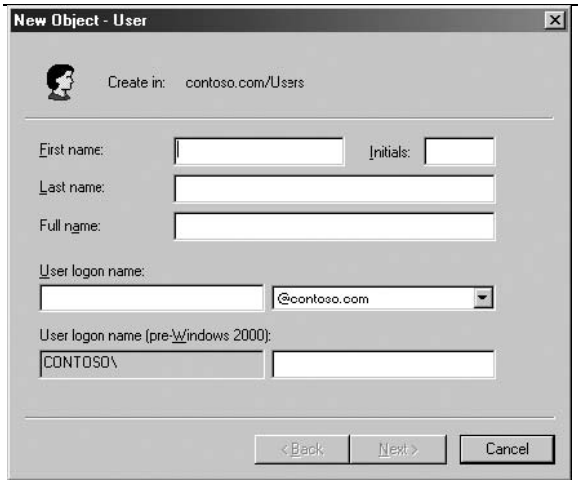
Hình 6-5: Bảng điều khiển *Active Directory Users And Computers*

TẠO TÀI KHOẢN NGƯỜI DÙNG MIỀN

Để tạo đối tượng người dùng từ thực đơn ***Action*** chọn ***New*** chọn tiếp ***User*** khi đó sẽ xuất hiện ***New Object – User wizard***. Không như hộp thoại ***New User*** để tạo đối tượng người dùng cục bộ, trình hướng dẫn ***New Object – User*** xuất hiện như sau:

Tại trang đầu của trình hướng dẫn (chỉ ra tại hình 6-6) gồm các tham số sau:

- **First Name:** Tên gọi của người dùng (tuỳ chọn).
- **Initials:** Chữ cái đầu tên đệm của người dùng (tuỳ chọn).
- **Last Name:** Tên họ của người dùng (tuỳ chọn).



Hình 6-6: Trang đầu của trình hướng dẫn *New Object – User*

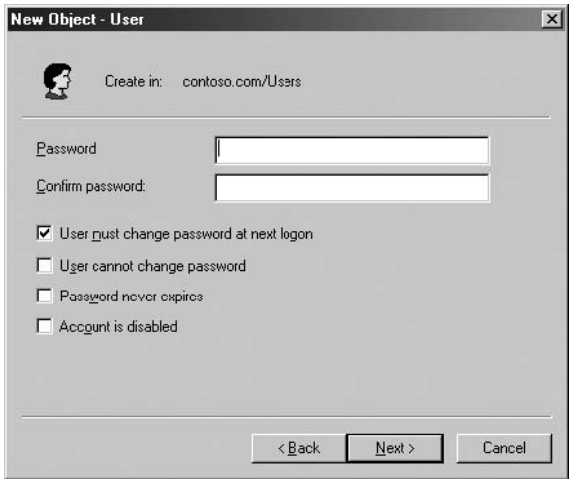
- **Full Name:** Tên đầy đủ của người dùng (bắt buộc). Khi bạn gõ vào ***First Name*** hoặc ***Last Name*** thì giá trị ***Full Name*** được tự động đưa vào và sau đó bạn có thể sửa lại được. Giá trị đưa vào này sẽ sinh ra một số các thuộc tính của đối tượng người dùng: ***common Name*** (CN – *tên phổ biến*), ***distinguished Name*** (DN – *tên phân biệt*), ***Name*** (*tên*) và ***DisplayName*** (*tên hiển thị*) . Do thuộc tính CN buộc phải là duy nhất trong một ***Container***. nên, tên đầy đủ bạn nhập vào đây phải là duy nhất một cách tương đối so với các đối tượng khác trong OU nơi mà đối tượng người dùng được tạo ra(hoặc với các ***Container*** khác) .

- **User Logon Name (*Tên đăng nhập*):** Tên của tài khoản sử dụng để đăng nhập (bắt buộc). Tên này sẽ được dùng trong ***User principal Name*** (UPN – *tên chính của người dùng*), bao gồm tên đăng nhập và đuôi UPN, mặc định là tên hệ thống tên miền (***Domain Name System*** - DNS) của miền. toàn bộ tên UPN có định dạng *Tên-đăng-nhập@ đuôi-UPN (**logon-Name@UPN-suffix**)* và phải là duy nhất trong rừng ***Active Directory***. Ví dụ UPN là ***someone@ACNA.com***. UNP sử dụng để đăng nhập vào mọi máy tính chạy Microsoft Windows 2003, Windows XP hoặc Windows 2000.

- **User Logon Name (Pre–Windows 2000):** tên tài khoản sử dụng để đăng nhập vào các máy khách trước Windows 2000 (bắt buộc), có thể là Windows 95, Windows 98, Windows Millennium Edition (Windows Me) hoặc Windows NT. Giá trị này sẽ được đưa vào tự động theo tên người dùng đăng nhập và có độ dài tới 20 ký tự. Giá trị này cũng phải là duy nhất trong một miền.

Sau khi vào các giá trị cho trang đầu bạn chọn ***Next***, sẽ xuất hiện trang thứ 2 bao gồm các tham số sau:

- **Password**: Mật khẩu để xác thực người dùng, có độ dài tối đa là 127 ký tự (tuỳ chọn).
- **Confirm Password**: Vào lại mật khẩu thêm một lần nữa để chắc chắn bạn đã gõ vào đúng. Nếu hai lần không trùng khớp nhau hệ thống sẽ yêu cầu bạn vào lại thêm một lần nữa.
- **User Must Change Password At Next Logon**: Chọn lựa chọn này nếu bạn muốn người dùng thay đổi lại mật khẩu khi đăng nhập vào hệ thống lần đầu. Bạn sẽ không thể chọn lựa chọn này nếu bạn đã chọn ***Password Nerver Expires***. Lựa chọn này cũng sẽ tự động xoá bỏ lựa chọn ***User Cannot Change Password***



Hình 6-7: Trang thứ hai của trình hướng dẫn *New Object-User*

- **User Cannot Change Password**: Chọn lựa chọn này, người dùng sẽ không thay đổi lại được mật khẩu, thường thì bạn sẽ dùng lựa chọn này khi có đồng thời từ hai người trở lên dùng chung một tài khoản người dùng miền hoặc bạn muốn quản lý dịch vụ mật khẩu người dùng. Bạn không thể chọn lựa chọn này nếu đã chọn ***User Must Change Password At Next Logon.***
- **Password Nerver Expires:** Bạn chọn lựa chọn này nếu muốn mật khẩu không bao giờ bị hết hạn. Bạn sẽ không chọn được lựa chọn này nếu bạn đã chọn ***User Must Change Password At Next Logon***. Thường bạn sẽ chọn lựa chọn này để quản lý cácmật khẩu của tài khoản dịch vụ
- **Account Is Disable:** Chọn lựa chọn này để vô hiệu hoá tài khoản, ví như là cho người mới đến, nhưng người này lại chưa cần truy nhập vào mạng.

Một số tuỳ chọn của tài khoản có thể mâu thuẫn với chính sách nhóm đã thiết lập mà nó được kế thừa từ miền hoặc đối tượng chứa. Ví dụ, chính sách

nhóm của miền mặc định là mật khẩu phải đổi theo chu kỳ là 42 ngày. Trong khi đó bạn lại chọn ***Password Never Expires*** thì nó sẽ ghi đè lên chính sách nhóm và người dùng sẽ không nhận được nhắc nhở phải đổi lại mật khẩu nữa.

Sau khi bạn vào các giá trị tại trang thứ 2 này chọn ***Next,*** khi đó sẽ xuất hiện tramh ***summary***. Chọn ***Finish*** để hoàn thành việc khởi tạo đối tượng người dùng mới tại đối tượng chứa đã chọn.

QUẢN LÝ TÀI KHOẢN NGƯỜI DÙNG MIỀN

Sau khi bạn tạo đối tượng người dùng, bạn sử dụng bảng điều khiển ***Active Directory Users And Computers*** để quản lý các thuộc tính của nó. Bằng cách chọn đối tượng người dùng, sau đó chọn thực đơn ***Action***, bạn có thể thực thi các công việc sau:

- **Add To A Group**: Đưa đối tượng người dùng vào thành thành viên của nhóm đã có
- **Disable Account:** Vô hiệu hoá tài khoản, không cho phép đăng nhập với tài khoản này. Nếu muốn dùng lại bạn chỉ cần xoá dấu chọn tại hộp kiểm tra ***Account Is Disable*** trong danh sách ***Account Option*** trên thẻ ***Account*** của hộp thoại ***Properties*** của đối tượng người dùng này.
- **Reset Password**: Cho phép quản trị đặt lại mật khẩu tài khoản mà không cần biết mật khẩu cũ.
- **Open Home Page:** Mở Microsoft Internet Explorer và kết nối tới địa chỉ trang web (***Uniform Resource Locator*** - URL) được xác định tại hộp ***Web Page*** trong thẻ ***General*** tại hộp thoại ***Properties*** của đối tượng người dùng
- **Send Mail :** Dùng ứng dụng Thư điện tử mặc định, tạo thư mới với địa chỉ tại hộp ***Email*** trong thẻ General tại hộp thoại ***Properties*** của đối tượng người dùng.
- **Delete :** Xoá đối tượng người dùng khỏi CSDL ***Active Directory***.
- **Rename:** Sủa đổi lại trường ***Full Name*** của đối tượng người dùng và mở hộp thoại ***Rename User*** để bạn có thể sửa đổi lại ***First Name***, ***Last Name, Display Name, User Logon Name*** và ***User Logon Name (Pre–Windows 2000)***.

Lưu ý: ***Mục đích của bài thi.*** *Mục đích của bài thi 70-290 xác định bạn có thể tạo mới và sửa đổi lại tài khoản bằng cách sử dụng snap-in* ***Active Directory Users And Computers***..

Khi bạn tạo tài khoản người dùng mới, bạn chỉ cần đưa vào các thuộc tính cơ bản nhất. Sau đó, bạn có thể sử dụng một công cụ quản trị mạnh dành cho đối tượng người dùng là hộp thoại ***Properties*** của chính đối tượng này. Bạn mở hộp ***Properties*** bằng cách chọn đối tượng người dùng sau đó tại thực đơn ***Action*** chọn tiếp ***Properties*** để sửa lại. Mặc định hộp thoại này có 13 thẻ, với rất nhiều các thuộc tính mà bạn có thể thiết lập cho User. Các thẻ này được phân loại như theo bảng 6-2 đưới đây

> ***LƯU Ý: Active Directory Schema and Object Properties.*** *Trong một số trường hợp hộp thoại* ***Properties*** *có nhiều hơn 13 thẻ hay có thể có thêm các trường khác trên một vài thẻ mặc định.Điều này xẩy ra do lược đồ (schema)* ***Active Directory,*** *nơi xác định số các thuộc tính cho mỗi kiểu đối tượng, là có thể mở rộng được. . Người quản trị có thể mở rộng thêm lược đò một cách thủ công bằng cách thêm các thuộc tính cho kiểu đối tượng (Microsoft khuyến cáo là không nên làm như vậy) hoặc lược đồ cũng có thể tự động được mở rộng khi cài đặt các sản phẩm phần mềm như cài đặt Microsoft Exchange thì sẽ tạo thêm các thẻ* ***Exchange General****,* ***Exchange Features****, and* ***E-mail Addresses*** *tại hộp thoại* ***Properties*** *của đối tượng người dùng.*

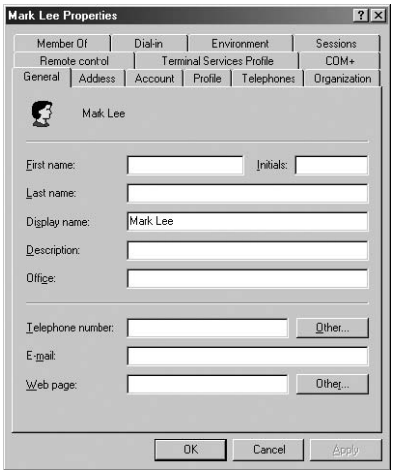
Bảng 6-2: Phân loại các thuộc tính người dùng trong các thẻ của hộp thoại *User Properties*

Phân loại	Thẻ
Thông tin cá nhân (***Personal information***)	**General**
	Address
	Telephones
	Organization
Thuộc tính Tài khoản (***Account properties***)	**Account**
Quản lý cấu hình người dùng (***User configuration management)***	**Profile**
Quan hệ thành viên nhóm (***Group membership***)	**Member Of**

Dịch vụ Đầu cuối (***Terminal Services***)	**Terminal Services Profile**
	Environment
	Remote Control
	Sessions
Truy cập từ xa (***Remote Access***)	**Dial-in**
Ứng dụng (***Applications***)	**COM+**

Thiết lập tại từng thẻ sẽ được nêu rõ trong các phần sau:

Thẻ General

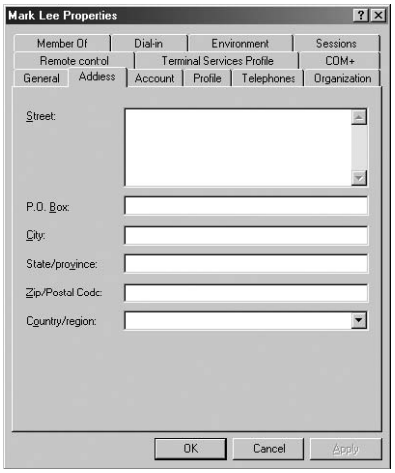


Thẻ ***General*** gồm các thông tin cơ bản của người dùng như ***First Name*** và ***Last Names*** mà bạn nhập vào khi tạo đối tượng người dùng. Bạn cũng có thể đưa vào các trường khác như ***Display Name***, ***Office Location*** (vị trí cơ quan) và ***Description***, thêm vào đó là ***Telephone Numbers*** (số điện thoại), ***Web page addresses*** (địa chỉ trang WEB) và ***E-mail address*** (địa chỉ Thư điện tử) của người dùng.

Rất nhiều trường trong các Thẻ ***General***, ***Address, Telephones*** và ***Organization*** là các thông tin cá nhân và các trường này là tuỳ chọn và các giá trị của nó không có mối liên quan trực tiếp tới các hoạt động của đối tượng người dùng hay của dịch vụ ***Active Directory***, nó đơn giản chỉ cung cấp các thông tin về người dùng.. Việc cung cấp các thông tin này giúp cho người quản trị dễ dàng tìm kiếm tài khoản người dùng miền bằng cách sử dụng công cụ tìm kiếm (***Search)*** với bất kể thông tin nào họ có về người

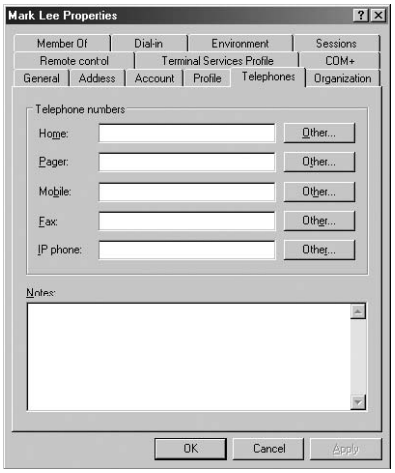
dùng . các người dùng trên mạng cũng có thể tìm kiếm một người dùng cụ thể nào đó để tìm ra các thông tin liên hệ hoặc dữ liệu khác.

Thẻ Address



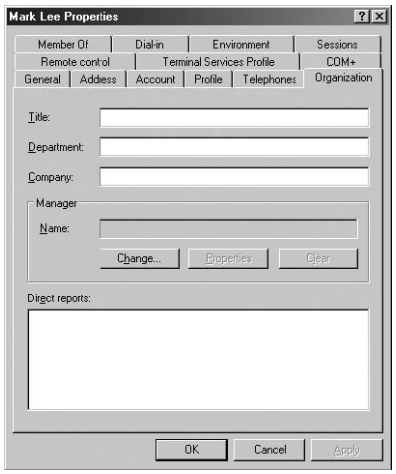
Thẻ ***Address*** gồm các trường thông tin cho phép quản trị nhập các thông tin địa chỉ người dùng vào ***Active Directory***.

Thẻ Telephones



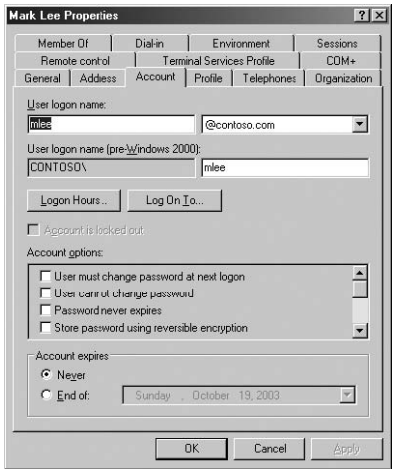
Thẻ ***Telephones*** gồm các trường cho phép quản trị lưu các số điện thoại của người dùng. Mặc dù các trường như vậy chỉ đơn thuần là thông tin trong cấu hình mặc định của ***Active Directory***, nhưng cũng không thể nói là nó chẳng để làm gì cả. Có rất nhiều thông tin có ích, ví dụ như có thể tạo ứng dụng quay số điện thoại cho phép bạn tìm kiếm tài khoản người dùng khác trong Active Directory và tự động quay số vào số điện thoại đặt trong thẻ này.

Thẻ Organization



Thẻ ***Organization*** bao gồm các trường mà ở đó người quản trị có thể xác định thông tin về ví trí của người dùng trong tổ chức, có cả trường mà ở đó bạn có thể chọn tài khoản người quản lý của người dùng này trogn CSDL ***Active Directory*** .

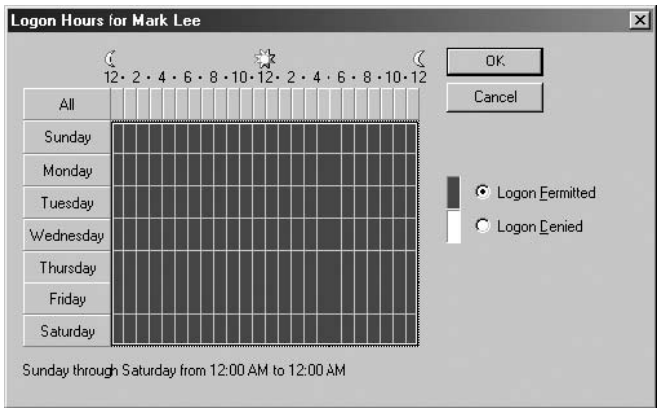
Thẻ Account



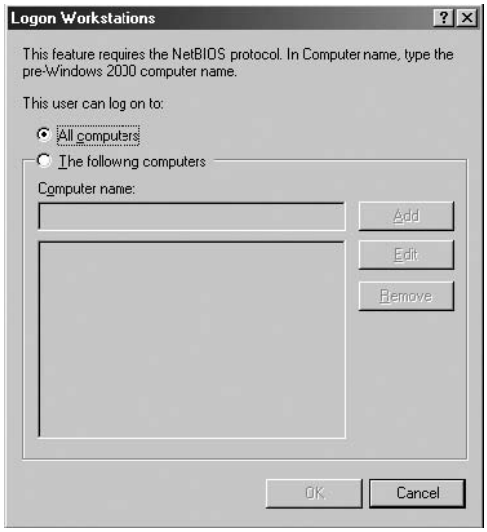
Thẻ Account chứa các trường ***User Logon Name***, ***UPN Suffix***, and ***User Logon Name (Pre–Windows 2000)*** có các giá trị bạn đưa vào khi tạo người dùng, tuỳ theo bốn lựa chọn từ ttrình hướng dẫn ***Create Object – User***. Thẻ này cũng sẽ bao gồm một số các tuỳ chọn khác như sau.

- **Logon Hours (Giờ đang nhập):** Hiện hộp thoại ***Logon Hours***, tại đó quản trị có thể đặt thời gian hàng ngày hoặc theo ngày xác định trong tuần mà người dùng sẽ được phép đăng nhập vào miền. Mặc định, tính năng này chỉ cấm người dùng đăng nhập vào. Nếu người dùng đã đăng nhập và hết thời gian cho phép thì sẽ không bị ngắt. Nhưng nếu trong ***Network Security*** tại đối tượng chính sách nhóm (GPO) chọn

Network Security là ***Force Logoff When Logon Hours Expire***, thì quản trị sẽ ngắt kết nối của người dùng một cách tự động. Hạn chế của ***Logon Hours*** là chỉ áp dụng cho đăng nhập miền chứ không áp dụng cho đăng nhập cục bộ.



- **Log On To (Đăng nhập vào):** Hiện hộp thoại ***Logon Workstations***, tại đó quản trị có thể xác định tên của các máy tính trên mạng mà người dùng này có thể đăng nhập vào. Tính năng này còn được gọi là ***Computer Restrictions***. Bạn phải chọn ***Enable NetBIOS over TCP/IP*** trên mạng để sử dụng tính năng này do nó hạn chế việc đăng nhập vào máy tính dựa trên tên NetBIOS của máy.



- **Account Is Locked Out (Tài khoản đã bị khóa):** Mặc định để ở chế độ vô hiệu hoá, nó chỉ được kích hoạt và chọn khi tài khoản người dùng bị khoá do nhiều lần cố tình đăng nhập không thành. Bạn có thể đặt khóa các tài khoản tuỳ theo các giá trị ***Account Lockout Duration*** (*Thời gian khóa tài khoản*), ***Account Lockout Threshold*** (*ngưỡng khóa tài khoản*), và ***Reset Account Lockout Counter After*** (*Đặt lại biến đếm khóa tài khoản sau*) của chính sách nhóm (GPO). Ví dụ, ***Account Lockout Threshold*** đặt là 3 thì tài khoản sẽ bị khoá sau 3

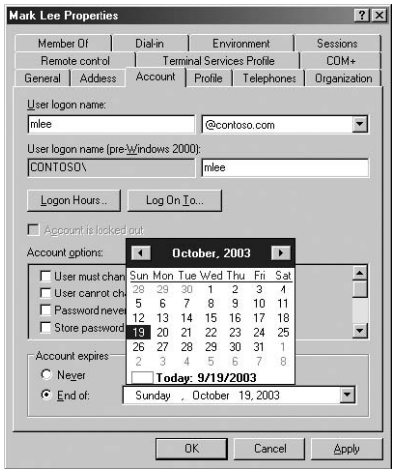
lần đăng nhập không thành công. Khi tài khoản bị khoá thì quản trị có thể mở lại bằng cách xoá lựa chọn này.

- **Store Password Using Reversible Encryption (Lưu mật khẩu sử dụng mã hóa đảo):** Buộc ***Active Directory*** lưu mật khẩu của đối tượng với thuật toán mã hoá đảo, thay cho việc sử dụng các thuật toán mã hóa thuận chiều, mạnh hơn và hiện đang được sử dụng phổ biến trong việc mã hóa mật khẩu. Lựa chọn này được thiết kế để cho các ứng dụng yêu cầu đảo mật khẩu , như phiên bản đầu tiên của ***Challenge Handshake Authentication Protocol*** (CHAP). Trong tất cả các trương hợp khác, lựa chọn này nên để ở dạng vô hiệu hoá. Bạn cũng có thể thiết lập là kích hoạt hoặc vô hiệu hoá lựa chọn này bằng cách sử dụng ***Group Policies***. Khi lựa chọn này được chọn thì nó sẽ đè lên giá trị cùng loại trên các ***Group Policy*** khác nếu có xung đột.
- **Account Is Disabled (Tài khoản bị vô hiệu hóa):** Cho phép quản trị vô hiệu hoá hoặc kích hoạt tài khoản người dùng
- **Smart Card Is Required For Interactive Logon (Yêu cầu có Smart Card khi đăng nhập):** người dùng được yêu cầu ***smart card*** khi đăng nhập. ***Smart card*** là thiết bị thẻ chứa thông tin định danh của người dùng, thường là dưới dạng chứng chỉ số và khoá mã riêng. Để người dùng đăng nhập bằng ***smart card*** thì máy tính phải có thiết bị đầu đọc và phần mềm tương ứng và người dùng phải có chính xác số PIN (***personal identification number***) của Card. Lựa chọn này dành cho các tài khoản yêu cầu tăng cường tính năng bảo mật. Bởi vì việc dùng ***smart card*** không cần tới mật khẩu , lựa chọn này thay đổi mật khẩu tài khoản thành giá trị phức tạp và ngẫu nhiên và kích hoạt lựa chọn ***Password Never Expires.***
- **Account Is Trusted For Delegation (*Tài khoản được tin cậy cho ủy quyền*):** Lựa chọn này cho phép dịch vụ chạy dưới tên tài khoản người dùng (gọi là ***service account*** – *tài khoản dịch vụ*) nhằm đóng vai trò là một người dùng truy nhập vào tài nguyên máy tính thay mặt cho tài khoản người dùng khác trên mạng.

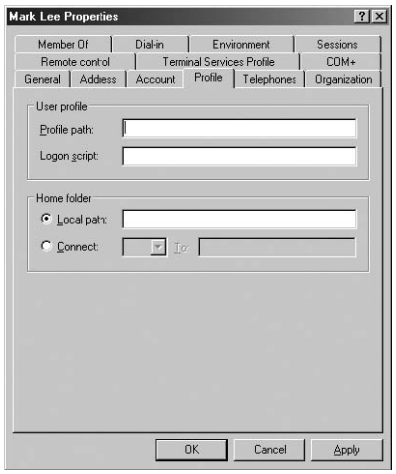
Trên mạng, lựa chọn này hiếm khi được chọn, nếu có, trong đối tượng người dùng để thay mặt cho người dùng thực sự.

- **Account Is Sensitive And Cannot Be Delegated (*Tài khoản là nhạy cảm và không được ủy quyền*):** Uỷ quyền cho phép quản trị trao quyền kiểm soát cho một tài khoản cụ thể, thường là dùng tạm thời, ví dụ như là tài khoản Guest. Lựa chọn này ngăn cấm tài khoản được uỷ quyền bởi các tài khoản khác,

- **Use DES Encryption Types For This Account (*Sử dụng kiểy mã hóa DES cho tài khoản này*): *Active Directory*** sẽ sử dụng thuật toán mã hoá DES (***Data Encryption Standard***) cho các đối tượng người dùng này.
- **Do Not Require Kerberos Preauthentication (*không yêu cầu quá trình tiền xác thực Kerberos)*: *Active Directory*** bỏ qua thủ tục tiền xác thực ***Kerberos (****quá trình tiền xác thực kerberos là quá trình so sánh thời gian trên máy khách đã được mã hoa bằng mật khẩu của người dùng, nếu thành công mới thực hiện tiếp quá trình xác thực****)*** khi thực hiện việc xác thực người dùng này. Lựa chọn này là dành cho các tài khoản sử dụng các thực thi xác thực khác của giao thức xác thực kerberos, mà không hỗ trợ việc xác thực trước. Bỏ qua việc thực thi tiền xác thực giao thức ***Kerberos***, sẽ gây giảm tính năng an toàn được cung cấp bởi giao thức này, do vậy, không nên kích hoạt lựa chọn này trừ khi có lý do đặc biệt.
- **Account Expires:** Cho phép quản trị xác định ngày tài khoản tự động bị vô hiệu hoá, sử dụng giao diện sau:



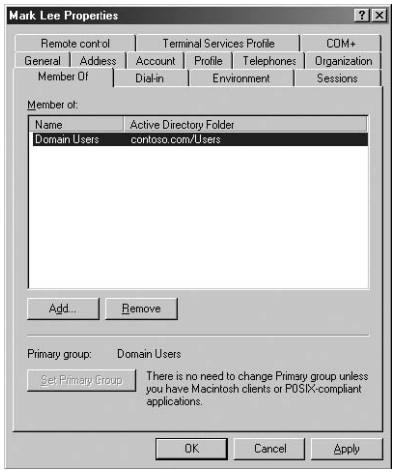
Thẻ Profile



Thẻ Profile gồm các trường bạn có thể chỉ định vị trí đặt ***User profile (****Khái lược Người dùng****)***, ***Home Folder (****Thư mục chủ****)*** và ***Logon Script (****Kịch bản đăng nhập****)*** sẽ thực thi khi người dùng đăng nhập.

> ***THÔNG TIN THÊM****: Để biết thêm thông tin về* ***User Profiles*** *xem phần "Quản lý* ***User Profiles****" tại chương sau.*

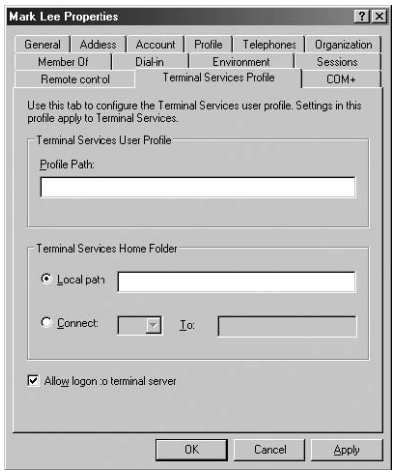
Thẻ Member Of



Thẻ ***Member Of*** liệt kê các nhóm mà người dùng là thành viên và cho phép quản trị sửa đổi lại các quan hệ thành viên nhóm của người dùng. Mặc định, người dùng mới tạo là thành viên của nhóm ***Domain Users***.

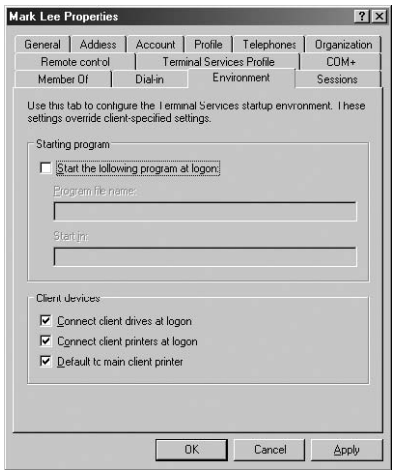
> ***LƯU Ý:*** *Để biết thêm thông tin về nhóm* ***Active Directory*** *xem chương 7 "Làm việc với Nhóm"*

Thẻ Terminal Services Profile



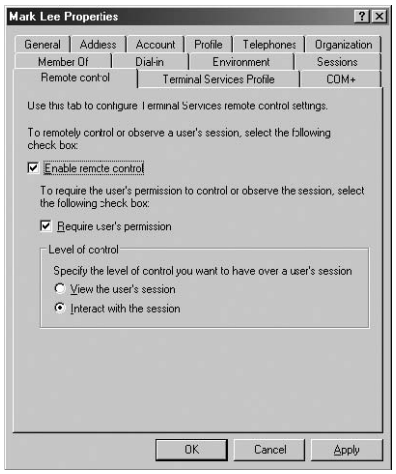
Cho phép quản trị cho phép người dùng kết nối vào ***Terminal Servers*** (*Máy chủ Dịch vụ Đầu cuối*) và chỉ định vị trí của ***User Profile*** và ***Home Folder*** sẽ được áp dụng khi người dùng kết nối vào ***Terminal Server***.

Thẻ Environment



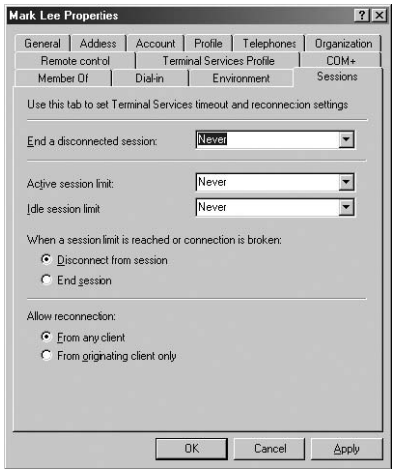
Thẻ ***Environment*** (*Môi trường*) cho phép quản trị chỉ định ứng dụng sẽ chạy ngay khi người dùng kết nối vào Máy chủ Dịch vụ Đầu cuối. Tại đây còn có các lựa chọn có cho phép hay không kết nối tới các ổ đĩa đã được gắn kết (***Map***) và các máy in trên máy trạm ngay sau khi đăng nhập. Và chỉ định liệu có in vào máy in mặc đinh tại mmáy trạm hay không.

Thẻ Remote Control



Thẻ ***Remote Control*** cho phép bạn cấu hình các thiết lập điều khiển từ xa Dịch vụ Đàu cuối (***Terminal Services***) cho đối tượng người dùng. Các lựa chọn này chỉ định liệu các phiên làm việc của người dùng có thể được truy nhập bằng cách sử dụng tính năng kiểm soát từ xa của Dịch vụ Đầu cuối hay không, liệu các Cấp phép cho người dùng có cần thiết hay không khi thực hiện truy cập nói trên, và liệu người kiểm định (***Auditor***) chỉ đơn thuần quan sát các phiên làm việc của người dùng hay thực sụ tham gia vào các phiên làm việc này. Các lựa chọn này cũng còn có thể được cấu hình thông qua bảng điều khiển ***Terminal Services Configuration*** hoặc Chính sách Nhóm (***Group Policies-GP)***, Trong trường hợp nếu các thiết lập cho các lựa chọn này sử dụng các công cụ khác nhau nói trên có xung đột thì các thiết lập trong Chính sách Nhóm sẽ được ưu tiên.

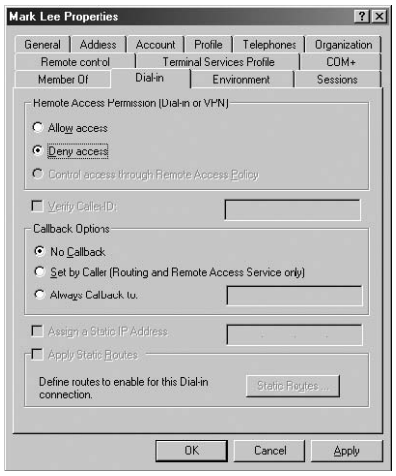
Thẻ Sessions



Thẻ ***Sessions*** (*Phiên*) cho phép quản trị có thể cấu hình hành vi khi ngắt kết nối phiên làm việc Dịch vụ Đầu cuối của người dùng, sử dụng các điều khiển sau:

- **End A Disconnected Session (***Kết thúc phiên làm việc đã được ngắt***):** Đặt thời gian cho phiên làm việc (***secsion***) của người dùng sử dụng Terminal Services tiếp tục duy trì trên máy chủ sau khi người dùng đã ngắt kết nối.
- **Active Session Limit (***Giới hạn của Phiên làm việc đang hoạt động***):** Đặt khoảng thời gian tối đa cho phiên làm việc của người dùng sử dụng Dịch vụ Đầu cuối, Phiên làm việc sẽ bị ngắt khi đạt tới giới hạn đã đặt.
- **Idle Session Limit (***Giới hạn của phiên làm việc đang dừng* **):** Đặt khoảng thời gian nghỉ tối đa cho phép của phiên làm việc trước khi máy chủ ngắt kết nối.
- **When A Session Limit Is Reached Or Connection Is Broken (***Khi đạt tới giớihạn của phiên làm việc háy kết nối bị đứt***):** Thiết lập Máy chủ Dịch vụ Đầu cuối ngắt hay hủy bỏ phiên làm việc khi phiên đạt đến giới hạn, người dùng có thể lập lại phiên đã bị ngắt nhưng không thể kết nối lại đến phiên đã bị máy chủ hủy bỏ.
- **Allow Reconnection (***Cho phép kết nối lại***):** Chỉ định liệu người dùng có hay không được phép kết nối lại tới Máy chủ Dịch vụ Đầu cuối từ một máy trạm bất kỳ hoặc từ máy trạm đã khởi tạo phiên.

Thẻ Dial-in



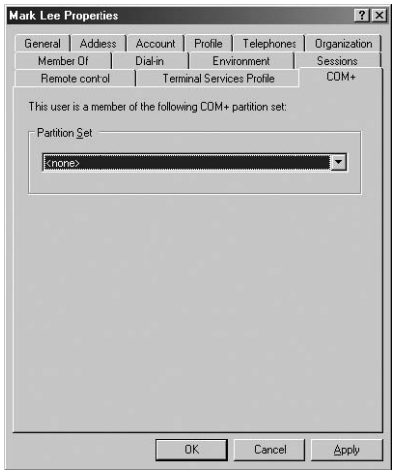
thẻ ***Dial-in*** (*quay số vào*) bao gồm các điều khiển cho phép quản trị thiết lập các khả năng truy nhập từ xa của người dùng, bao gồm:

- **Remote Access Permission (Dial-In Or VPN)** *(Cấp phép Truy nhập Từ xa – Quay số hay VPN)***:** Bạn có thể chọn các lựa chọn cho phép truy nhập, từ chối truy nhập hoặc điều khiển truy nhập thông qua các thiết lập trong Chính sách Truy nhập Từ xa (***Remote Access Policy***).

Nếu bạn lựa chọn "***Allow Access***" (*cho phép truy nhập*), các dự định két nối của người dùng tới máy chủ thậm chí vẫn bị từ chối do các thiết lập đã đặt trong Chính sách Truy nhập Từ xa, các thuộc tính của Tài khoản Người dùng hay tại các thuộc tính của Khái lược (***Profile***) Dịch vụ Đầu cuối .

- **Verify Caller ID (***Kiểm tra Định danh Người gọi***):** Máy chủ kết nối từ xa kiểm tra lại số Định danh Người gọi mà người dùng sử dụng để kết nối bằng cách so sánh nó với Định danh Người gọi (***Caller ID***) đã được nhập trong thẻ này. Nếu số Định danh Người goi của người dùng không được xác nhận hoặc không đúng số điện thoại đã định trước thì kết nối này sẽ bị từ chối.
- **Callback Options (***các tùy chọn gọi lại***):** Cho phép người quản trị cho phép người dùng sử dụng tính năng gọi lại khi kết nối tới máy chủ từ xa hay không. Nếu có, sau khi người dùng kết nối tới máy chủ thì nó sẽ ngắt kết nối đồng thời sau đó thiết lập kết nối quay lại tới người dùng theo số điện thoại đã được người dùng chỉ định hay theo số mà quản trị đã đặt trước ngay trong thẻ này. Tính năng gọi lại sẽ tiết kiện cho người dùng, các hóa đơn sẽ được tính cho số điện thoại tại máy chủ, và đảm bảo tính an toàn, do chỉ những người gọi tại một trong các số điện thoại nhất định đã được cho phép mới có thể truy nhập từ xa vào máy chủ.
- **Assign A Static IP Address (***Gán IP tĩnh***):** Cho phép quản trị đặt địa chỉ IP tĩnh mà máy chủ từ xa sẽ luôn gán cho người dùng này.
- **Apply Static Routes:** Cho phép quản trị chỉ định các bản ghi định tuyến tĩnh sẽ được thêm vào bảng định tuyến của máy trạm khi kết nối ***Demand-Dial*** (*Quay theo yêu cầu*) được thiết lập.

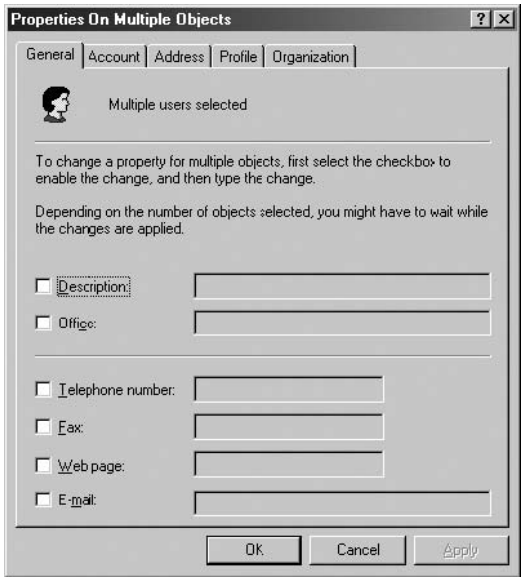
Thẻ COM+



Thẻ COM+ cho phép quản trị gán một tập ***partition COM+*** xác định cho người dùng. *Tập **Partition COM+** là tập hợp của các các **partition COM+** mà ở đó các ứng dụng **COM+** được lưu*. Chọn một tập ***partition COM+*** nào đó sẽ cho phép người dùng truy nhập đến các ứng dụng khác nhau có trong tập này.

QUẢN LÝ ĐỒNG THỜI NHIỀU NGƯỜI DÙNG

Khi quản lý các tài khoản người dùng miền, khi bạn phải làm các công việc sửa đổi giống nhau cho nhiều tài khoản người dùng và bạn thực hiện chúng một cách riêng lẻ thì sẽ thực sự là một công việc mất thời gian và nhàm chán. Trong những trường hợp như vậy, bạn hoàn toàn có thể cùng lúc thay đổi các thuộc tính của nhiều tài khoản người dùng bằng cách sử dụng bảng điều khiển ***Active Directory Users And Computers***. Đơn giản là bạn chọn đồng thời các đối tượng người dùng bằng cách giữ phím ***CTRL*** trong khi bám chọn từng người dùng trong khung chi tiết, sau đó chọn ***Properties*** từ thực đơn ***Action***. Hộp thoại ***Properties On Multiple Objects*** xuất hiện như hình 6-8.



Hình 6-8: Hộp thoại *Properties On Multiple Objects*

> ***LƯU Ý: Chỉnh sửa các lớp đối tượng (Object Classes).*** *Khi bạn chọn đồng thời các đối tượng để thay đổi, bạn sẽ nhận được các kết quả tốt nhất khi tất cả các đối tượng đó là cùng một lớp. Ví dụ, nếu bạn chọn đồng thời các đối tượng là người dùng thì sẽ sửa được rất nhiều các thuộc tính, nhưng nếu bạn chọn đối tượng người dùng và đối tượng máy tính thì chỉ có một thuộc tính chung của chúng có thể sửa được là **Description**.*

Hộp thoại ***Properties On Multiple Objects*** khác một chút so với hộp thoại ***Properties*** chuẩn của đối tượng người dùng. Nó chỉ có một số giới hạn các thuộc tính, là các thuộc tính được áp dụng \cho đồng thời nhiều đối tượng. Các thuộc tính của hộp thoại này được tổng kết trong bảng 6-3

Bảng 6-3: Các thuộc tính có thể được hiện cho việc chỉnh sửa khi chọn đồng thời các đối tượng người dùng

Thẻ	Thuộc tính
General	Description Office Telephone Number Fax Web Page E-mail
Account	UPN Suffix Logon Hours Computer Restrictions Account Options Account Expires
Address	Street P.O. Box City State/Province Zip/Postal Code Country/Region
Profile	Profile Path Logon Script Home Folder
Organization	Title Department Company Manager

DI CHUYỂN CÁC ĐỐI TƯỢNG NGƯỜI DÙNG

Mặc dù việc có trong tay bản thiết kế về cấu trúc ***Active Directory*** cho tổ chức của bạn khi bạn tạo các đối tượng người dùng thật sự là một điều lý tưởng do bạn có thể tạo chúng trong đúng các đối tượng chứa cụ thể, nhưng việc phải di chuyển các đối tượng này sau đó vẫn hoàn toàn có thể xẩy ra.

Khả năng này cũng còn cho phép bạn điều chỉnh lại cho phù hợp với việc thuyên chuyển nhân sự hoặc tái cơ cấu lại công việc.

Để di chuyển đối tượng người dùng (hay bất cứ một đối tượng nào khác) bạn chọn đối tượng này và sau đó từ thực đơn ***Action*** bạn chọn ***Move***, khi đó sẽ xuất hiện hộp thoại ***Move*** (chỉ ra trong hình 6-9). Sau đó chọn đối tượng chứa bạn muốn chuyển nó đến và nhấn ***OK***. Bạn cũng nó thể di chuyển đối tượng bằng cách kéo và thả.

Hình 6-9: Hộp thoại *Move*

> ***LƯU Ý: Xoá các đối tượng*** *Khi bạn chuyển các đối tượng trong cấu trúc* ***Active Directory****, bạn phải cẩn thận để không tình cờ xoá chúng.* ***SID*** *tương ứng với đối tượng người dùng là một giá trị duy nhất được gán cho đối tượng khi nó được khởi tạo. Khi bạn xoá và tạo lại với cùng tên và các thuộc tính thì* ***SID*** *vẫn là khác nhau. Đây không phải là vấn đề lớn khi tạo mới đối tượng, nhưng nếu bạn xoá đối tượng thì bạn phải cấu hình lại mọi Cấp phép của người dùng vì chúng được cấp cho người dùng theo* ***SID*** *của họ.*

KHỞI TẠO ĐỒNG THỜI NHIỀU NGƯỜI DÙNG

Đôi khi, quản trị mạng được yêu cầu phải tạo nhiều đối tượng người dùng một cách nhanh chóng, để đáp ứng cho một đợt tuyển dụng mới hoặc một lớp sinh viên mới nhập học. Khi đó, bạn sẽ có các phương pháp mà bạn có thể sử dụng để làm đơn giản hóa hay tự động hóa quá trình tạo đối tượng người dùng thay cho việc phải tạo riêng lẻ từng tài khoản. Bảng điều khiển ***Active Directory Users And Computers*** là một công cụ thiết kế chủ yếu dành cho việc tạo và quản lý các đối tượng một cách đơn lẻ. Tuy nhiên, Windows Server 2003 có cả các công cụ khác dùng cho việc tạo các đối tượng sử dụng các kỹ thuật như **nhập** (***import***) và các kịch bản dạng dòng lệnh (***command-line scripting)***.

Sử dụng các mẫu (*Template*) đối tượng

Thông thường thì các đối tượng của Active Directory ở trong cùng một lớp (***class***) sẽ chia sẻ các thuộc tính tương tự nhau. Ví dụ, tất cả các thành viên cùng một phòng ban sẽ ở cùng các nhóm giống nhau, được phép đăng nhập vào mạng cùng giờ và có các ***Home Folders*** (*Thư mục chủ*) và ***Roaming Profiles (****Khái lược di trú)* đặt trên cùng một máy chủ. Trong trường hợp này sẽ rất thuận tiện khi bạn bắt đầu việc tạo tài khoản cho các người dùng mới bằng cách tạo một đối tượng có các thuộc tính chung, đối tượng người dùng chung, hay còn gọi là **T*emplate* (*Mẫu*)** và sau đó sử dụng việc sao chép đối tượng này để tạo các đối tượng người dùng mới.

Để tạo đối tượng người dùng mẫu, ta tạo đối tượng người dùng mới, gán tên cho nó ví dụ là ***UserTemplate*** và đặt cấu hình các thuộc tính của nó là các thuộc tính chung của tất cả mọi người dùng mới mả bạn muốn tạo, cách làm như là bạn cấu hình cho từng người dùng vậy. Các thuộc tính sẽ được sao chép tới đối tượng mới được tổng kết trong bảng 6-4. Sau khi cấu hình các thuộc tính cho đối tượng mẫu này, bạn phải vô hiệu hoá (***Disable***) chúng để không ai có thể sử dụng đối tượng này này để truy nhập vào mạng.

Bảng 6-4: Các Propertie sao chép tới đối tượng người dùng mới.

Thẻ	**Các thuộc tính (Properties) sẽ được chép**
General	Không
Address	Tất cả, ngoại trừ ***Street Address***
Telephones	Không
Organization	Tất cả, ngoại trừ ***Title***
Account	Tất cả, ngoại trừ ***User Logon Name và User Logon Name (Pre-Windows 2000)***, sẽ được xác định trong quá trình thực hiện sao chép.
Profile	Tất cả, gồm ***Profile Path*** và ***Local Path***, sẽ được chỉnh sửa tương ứng ***logon Name*** của người dùng mới
Member Of	Tất cả
Terminal Services Profile	Không

Environment	Không
Remote Control	Không
Sessions	Không
Dial-in	Không
COM+	Không

> ***LƯU Ý: Tạo đồng thời nhiều Templates.*** *Tuỳ theo quy mô của tổ chức và mức độ phức tạp cấu hình đối tượng người dùng, bạn phải tạo đồng thời một số các đối tượng mẫu tại các vị trí khác nhau trong cây* ***Active Directory****. Ví dụ, tạo riêng rẽ các đối tượng mẫu của người dùng tại mỗi OU sẽ cho phép bạn cấu hình các giá trị thuộc tính theo từng OU đó.*

Một khi đối tượng mẫu đã được tạo ra, bạn có thể sử dụng nó để tạo tài khoản người dùng mới bằng cách chọn đối tượng mẫu thích hợp, sau đó chọn thực đơn ***Action,*** chọn ***Copy***, khi đó sẽ xuất hiện trình Hướng dẫn Chép Đối tượng Người dùng (***Copy Object-User***) gần giống như trình Hướng dẫn Tạo Đối tượng Người dùng Mới (***New Object-User***) bạn đã sử dụng trong phần trước của chương này. Trình hướng dẫn sẽ dẫn bạn qua các bước của quá trình cấu hình các thuộc tính của đối tượng bắt buộc phải có các giá trị duy nhất, như ***First Name, Last Name, Initials, Logon Name***, ***Password*** và các tuỳ chọn của tài khoản. Khi trình Hướng dẫn kết thúc, đối tượng người dùng mới sẽ được tạo với các giá trị thuộc tính giống như của đối tượng mẫu đối với các thuộc tính đã được liệt kê trong bảng trên.

> ***LƯU Ý: Việc sao chép đối tượng và các Cấp phép.*** *Một người dùng được tạo bằng cách sao chépđối tượng mẫu có cùng quan hệ nhóm giống như đối tượng mẫu,do vậy các Cấp phép và Quyền gán cho nhóm này cũng sẽ được áp dụng cho người dùng mới. Tuy nhiên, các Cấp phép và các Quyền được gán trực tiếp cho đối tượng mẫu sẽ không được sao chép tới đối tượng người dùng, do vậy, đối tượng người dùng mới cũng không có được các Cấp phép và Quyền này..*

NHẬP ĐỐI TƯỢNG NGƯỜI DÙNG SỬ DỤNG CSV DIRECTORY EXCHANGE

CSV Directory Exchange (Csvde.exe) là tiện ích dạng dòng lệnh cho phép nhập vào hoặc kết xuất ra các đối tượng từ ***Active Directory***, sử dụng file văn bản có các trường được phân cách bằng dấu phẩy (“**,**”), Các file này,

còn được gọi là file CSV (***Comma-Separated Value***), là dạng liệt kê dạng văn bản tường minh (***Plain-text***) của các thông tin CSDL với mỗi bản ghi là một dòng, và các trường được phân cách bởi dấu phẩy (“**,**”).

> ***LƯU Ý**: **Mục đích kỳ thi**. Mục đích bài thi 70-290 xác định bạn thấy có thể “**import User Accounts” (**nhập các tài khoản người dùng).*

Tạo CSV file

Phần khó nhất của việc sử dụng ***CSV Directory Exchange*** để tạo đối tượng người dùng nằm ở chính bản thân định dạng của file CSV. Dòng đầu của file CSV được gọi là tiêu đề, bắt buộc phải bao gồm danh sách các thuộc tính có trong tất cả các hàng tiếp theo. Bạn liệt kê các thuộc tính sử dụng tên gán cho chúng trong ***Lightweight Directory Access Protocol*** (LDAP), là giao thức giao tiếp ***Active Directory*** tiêu chuẩn. Dòng CSV tiêu đề có dạng tiêu biểu như sau:

DN,ObjectClass,sAMAccountName,sn,givenName,UserPrincipalName

Trong dòng này, tên trường đại diện cho các thuộc tính như sau:

- ***DN: Distinguished Name*** (DN), nó xác định không chỉ riêng tên của đối tượng mà cả vị trí của nó trong cây phân cấp AD. DN gồm có tên thông dụng (***Common Name*** - CN) của người dùng và tiếp theo sau là tên của tất cả các đối tượng chứa bên trên của nó, toàn bộ đường đi tới gốc (Root, Top) của cây.
- ***ObjectClass:*** Xác định kiểu của đối tượng.
- ***sAMAccountName:*** Xác định ***pre–Windows 2000 logon Name*** của đối tượng
- ***sn:*** Xác định tên họ ***(Surname***) của người dùng
- ***givenName:*** Xác định tên gọi (***first Name***) của người dùng
- ***UserPrincipalName:*** Xác định UPN đầy đủ, bao gồm cả tên, của người dùng miền (***UserName@DomainName.com***).

Các dòng tiếp theo sau tiêu đề (***header)*** phải xác định giá trị cho từng thuộc tính đã liệt kê trên tiêu đề. Ví dụ các bản ghi trong file CSV như sau:

"CN=Scott Bishop,OU=Employees,DC=ACNA,DC=com",

User,sbishop,Bishop,Scott,scott.bishop@ACNA.com

File này, khi được nhập vào, sẽ tạo đối tượng người dùng trong OU ***Employees*** có tên là ***Scott Bishop***. ***Logon Name, First Name*** và ***Last Name*** cũng được cấu hình bằng file CSV này. Đây chỉ là một ví dụ đơn giản của

file CSV với chỉ một vài thuộc tính. Dòng tiêu đề có thể dài hơn nhiều và có thể bao gồm bất kỳ một thuộc tính nào bạn có thể tìm thấy ở đối tượng.

> ***LƯU Ý: Tạo các thuộc tính trống.*** *Khi tạo các dòng trong file CSV, bạn có thể để giá trị của của một vài thuộc tính nhất định là trống, nhưng bạn vẫn phải tính đến nó khi trình bầy.. Ví dụ, nếu bạn bỏ trống* ***First Name*** *trong ví dụ trên thì file CSVsẽ có dạng sau:*
>
> ***"CN=Scott Bishop,OU=Employees,DC=ACNA,DC=com", user,sbishop,Bishop,,scott.bishop@ACNA.com***
>
> *Số lượng các dấu phẩy(**","**) vẫn hoàn toàn giống nhau giữa hai ví dụ, do đó trường* ***Givenname*** *(tên gọi) vẫn được tính đến, nhưng không có giá trị.*

Cách tốt nhất để tạo file CSV là sử dụng một file có sẵn như là một ví dụ. Bạn có thể sử dụng ***CSV Directory Exchange*** để kết xuất ra toàn bộ CDSL ***Active Directory*** thành tệp CSV, bằng cách gõ lệnh sau tại của sổ dòng lệnh:

csvde –f *outputFileName*

Trong đó: ***outputFileName*** là file được kết xuất ra

Bạn có thể mở file này bằng bất cứ hệ soạn thảo văn bản nào, như ***Notepad*** chẳng hạn và sử dụng nó để xác định các tên LDAP cho các thuộc tính bạn muốn sử dụng và để lấy định dạng chuẩn của mối bản ghi.

Nhập vào tệp CSV

Sau khi bạn đã tạo tạo được file CSV đã được định dạng chuẩn, có chứa các thông tin của rất nhiều các đối tượng ***Active Directory***, bạn có thể nhập chúng vào CSDL thư mục của bạn tất cả cùng lúc bằng cách chạy chương trình ***Csvde.exe*** từ cửa sổ dòng lệnh của Windows cùng với tên của file CSV, theo cú pháp sau:

csvde –i –f *FileName* –k

Chức năng của các tham số như sau:

- **-i :** Chuyển sang chế độ nhập. Nếu không có tham số này thì ngầm định là chế độ kết xuất ra.
- **-f *fileName:*** Xác định tên của file CSV sẽ được nhập vào
- **–k:** Buộc chương trình bỏ qua các lỗi, ví dụ như ***"Object already exists"(****Đối tượng đã tồn tại****) , "constraint violation"(****vi phạm các ràng buộc****) "attribute or value already exists" (****thuộc tính hay giá trị*

đã tồn tại), trong khi việc nhập vào đang thực hiện và tiến trinh vẫn được thực hiện tiếp.

TẠO ĐỐI TƯỢNG NGƯỜI DÙNG BẰNG DSADD.EXE

Dsadd.exe là chương trình của Windows Server 2003 cho phép bạn tạo mới các đối tượng ***Active Directory***, với đầy đủ các thuộc tính,từ của sổ dòng lệnh. Khi bạn có một số lượng lớn các đối tượng người dùng để tạo, sự ưu việt của việc sử dụng ***Dsadd.exe*** là bạn có thể tạo file bó (***batch***) gồm nhiều dòng lệnh nhằm tạo đồng thời nhiều đối tượng cùng lúc với số lượng lớn bao nhiêu tùy thích.

> ***LƯU Ý: Mục đích của kỳ thi***. *Mục đích bài thi 70-290 yêu cầu các thí sinh có khả năng "Tạo và sửa các tài khoản người dùng một cách tự động".*

Cú pháp chính tạo đối tượng người dùng bằng ***Dsadd.exe*** như sau:

dsadd User ***UserDN [parameters]***

> ***LƯU Ý: Tạo các kiểu đối tượng khác.*** *Bạn có thể sử dụng* ***Dsadd.exe*** *để tạo bất kỳ một kiểu đối tượng* ***Active Directory*** *nào bằng cách thay các tham số người dùng bằng tên của bất kỳ một lớp đối tượng nào mà dịch vụ thư mục hỗ trợ và cung cấp các tham số tương ứng với lớp đối tượng đó.*

Tham số ***UserDN*** là một hoặc nhiều hơn các tên phân biệt (***Distinguished Names***) cho một (hoặc nhiều) đối tượng người dùng mới. DN sử dụng cùng một định dạng giống như định dạng của nó trong tệp CSV, như đã nêu ở phần trên. Trong trường hợp DN có dấu cách, thì bạn phải đặt nó trong dấu ngoặc kép (***""***). Khi bạn sử dụng ***Dsadd.exe*** một cách tương tác từ dấu nhắc dòng lệnh, bạn có thể cung cấp tham số ***UserDN*** theo một trong các cách sau:

- Nhập từng tên DN một, phân cách nhau bởi dấu cách, trong vị trí của nó tại dòng lệnh.
- Lấy danh sách các DN từ câu lệnh khác, ví dụ như từ ***Dsquery.exe***
- Bỏ trống tham số DN, Bạn sẽ nhập DN tại dấu nhắc đưa ra từ chương trình. Bạn ấn ***Enter*** sau mỗi DN và nhấn ***CTRL+Z*** và ***Enter*** sau DN cuối cùng.

Ngoài tham số ***UserDN,*** bạn có thể thêm bất cứ một trong các tham số sau trong câu lệnh ***Dsadd.exe***, nhằm chỉ định các giá trị cho các thuộc tính của đối tượng:

- **-samid *SAMName*** *(tên truy nhập với các hệ điều hành trước Windows 2000)*
- **-upn UPN** *(tên chính của người dùng)*
- **-fn *FirstName*** *(Tên gọi)*
- **-mi *Initial*** *(Chữ cái đầu của tên đệm)*
- **-ln *LastName*** *(Tên họ)*
- **-display *DisplayName*** *(Tên hiển thị)*
- **-empid *EmployeeID*** *(Mã định danh nhân viên)*
- **-pwd {*Password* | *}**, *(mật khẩu),* nếu bạn đặt dấu "*" trong câu lệnh, màn hình sẽ hiện dấu nhắc cho bạn gõ mật khẩu.
- **-desc *Description***(mô tả)
- **-Memberof *GroupDN*** *(Tên đầy đủ của nhóm)*
- **-office *Office*** *(tên văn phòng)*

-tel *PhoneNumber* (*số điện thoại***)**

- **-email *Email***
- **-hometel *HomePhoneNumber*** *(điện thoại nhà riêng)*
- **-pager *PagerNumber*** *(Số máy nhắn tin)*
- **-mobile *CellPhoneNumber*** *(số di động)*
- **-fax *FaxNumber***
- **-iptel *IPPhoneNumber***
- **-webpg *WebPage***
- **-title *Title***
- **-dept *Department***
- **-company *Company***
- **-mgr *ManagerDN***
- **-hmdir *HomeDirectory*** *(thư mục chủ)*
- **-hmdrv *DriveLetter*** *(Ký tự ổ đĩa)*
- **-profile *ProfilePath*** *(đường dẫn đên khái lược người dùng)*

- **-loscr *ScriptPath*** (*đường dẫn đến kịch bản đăng nhập*)
- **-mustchpwd {yes | no}**
- **-canchpwd {yes | no}**
- **-reversiblepwd {yes | no}**
- **-pwdneverexpires {yes | no}**
- **-acctexpires *Số ngày sẽ hết hạn***
- **-Disabled {yes | no}**

Bạn cũng có thể thêm các tham số ***–s, -u*** và ***– p*** chỉ định máy điều khiển miền sẽ thực thi ***Dsadd.exe*** và tên người dùng, mật khẩu cũng sẽ được dùng để chạy lệnh này.

- **{-s *Server* | -d *Domain*}**
- **-u *UserName***
- **-p {*Password* | *}**

Một biến đặc biệt, ***$UserName$*** (không phân biệt chữ hoa hay chữ thường), có thể sử dụng để cung cấp tên tài khoản SAM của người dùng trong giá trị của các tham số ***-email***, ***-hmdir***, ***-profile*** và ***-webpg***. Ví vụ, nếu tên SAM của tài khoản là "***Denise***" tham số ***-hmdir*** sẽ được ghi là một trong các dạng sau:

-hmdir\Users\Denise\home

-hmdir\Users\$UserName$\home

Để tạo đối tượng cho người dùng Scott Bishop tại ví dụ trước đây, bạn có thể sử dụng dòng lệnh ***Dsass.exe*** như sau:

dsadd User "CN=Scott Bishop, OU=Employees, DC=ACNA, DC=com" –samid sbishop –ln Bishop –fn Scott –upn scott.bishop@ACNA.com

Sửa đối tượng người dùng bằng Dsmod.exe

Dsmod.exe là một lệnh khác của Windows Server 2003 bạn có thể dùng để chỉnh sửa các đối tượng ***Active Directory***. Cú pháp và dòng lệnh sửa đối tượng người dùng hoàn toàn giống như với ***Dsadd.exe***.

dsmod User *UserDN [parameters]*

Ngoại trừ, bạn không thể dử dụng tham số ***–samid*** để sửa thuộc tính ***User Logon Name***, bạn cũng không thể dùng tham số ***–Memberof*** để thay đổi nhóm chứa nó. Mặc dù vậy, ban vẫn có thể sửa quan hệ nhóm bằng lệnh ***Dsmod Group***.

QUẢN LÝ KHÁI LƯỢC NGƯỜI DÙNG

Khái lược người dùng (***User Profile***) là tập hợp của các Folder và dữ liệu mà trong đó lưu trữ các môi trường nền, các thiết lập ứng dụng và các dữ liệu cá nhân hiện thời của người dùng. Khái lược người dùng gồm tất cả các khoản mục của thực đơn ***Start*** của người dùng và các ổ đĩa ánh xạ tới máy chủ. Khái lược người dùng duy trì cho người dùng có cùng môi trường nền mà chúng có từ lần đăng nhập cuối vào máy tính.

> ***LƯU Ý: Mục đích của kỳ thi.*** *Mục đích của kỳ thi 70-290 nhằm xác định sinh viên có khả năng "Quản lý khái lược người dùng cục bộ, di trú và bắt buộc."*

Trên máy tính chạy Windows Server 2003, khái lược người dùng sẽ tự động được tạo và duy trì thiết lập nền cho từng người dùng tại chính máy này. Hệ thống tạo khái lược người dùng mới cho mỗi người dùng khi họ đăng nhập vào máy lần đầu.

Khái lược người dùng cung cấp một vài tính năng ưu việt cho người dùng như sau:

- Nhiều người dùng có thể làm việc trên cùng một máy, và mỗi người trong số họ đều có thể duy trì các thiết lập nền riêng của mình mỗi khi đăng nhập vào máy tính.
- Khi người dùng vào máy trạm của mình, họ sẽ nhận được các thiết lập nền giống như lần thoát ra trước đó.
- Việc chỉnh sửa môi trường nền của một người dùng nào đó sẽ không làm ảnh hưởng tới các thiết lập của bất kỳ người nào khác.
- Khái lược người dùng có thể để trên máy chủ, bởi vậy với cùng một người dùng trên các máy khác nhau thì vẫn dùng chung được một khái lược người dùng. Khi đó, nó được gọi là khái lược người dùng di trú **(*Roaming User Profiles*).**
- Những ứng dụng mà được xác nhận là tương thích với Windows 2000 và các hệ điều hành sau đó sẽ lưu các thiết lập của chúng tại Khái lược Người dùng.
- Giống như một công cụ quản trị, Khái lược Người dùng cung cấp các lựa chọn sau:
    - Bạn có thể tạo khái lược người dùng mặc định thích hợp với các tác vụ của người dùng.

- Bạn có thể thiết lập Khái lược Người dùng Bắt buộc (***Mandatory User Profile***), là loại Khái lược mà người dùng không thể thay đổi được, áp đặt một cấu hình hệ thống nhất định cho mọi người dùng.
- Bạn có thể chỉ định các thiết lập mặc định cho người dùng, sẽ được đưa vào Khái lược Người dùng của tất cả các người dùng riêng lẻ.

NỘI DUNG KHÁI LƯỢC NGƯỜI DÙNG

Khái lược người dùng bao gồm cấu hình các sở thích các tùy chọn cho một người dùng cụ thể. Bảng 6-5 sẽ liệt kê các thiết lập có trong Khái lược Người dùng.

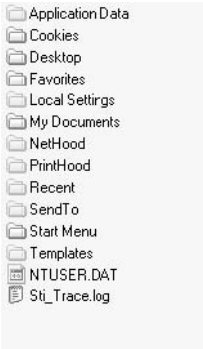
Bảng 6-5: Các thiết lập tại khái lược người dùng

Các thông số được lưu	**Nguồn**
Tất cả các thiết lập cho Windows Explorer người dùng có thể xác định	Windows Explorer
Các văn bản lưu trữ của người dùng	My Documents
Các file ảnh lưu trữ của người dùng	My Pictures
các ***Shortcut*** và ***cookie*** cho các web site ưa thích trên Internet	Favorites/Cookies
Các ổ mạng được ánh xạ mà người dùng tạo ra	Mapped network drive
Liên kết tới các máy tính khác trên mạng	My Network Places
Biểu tượng đặt trên màn hình nền, thanh tác vụ và các yếu tố ***shortcut***.	Desktop contents
Màu màn hình và các thiết lập hiện thị chữ	Screen colors and fonts
Dũ liệu ứng dụng và các thiết lập cấu hình do người dùng xác định	Application data and registry
Các kết nối tới máy in mạng	Printer settings

Tất cả các thiết lập người dùng có thể xác định trong ***Control Panel***	Control Panel
Các thiết lập chương trình hướng người dùng (***Per-User***) cho các ứng dụng được thiết kế để theo dõi các thiết lập chương trình.	Programs certified for use with Windows 2000 and later operating systems
Chứng chỉ	Certificate store

Cấu trúc Thư mục Khái lược Người dùng

Khái lược người dùng cục bộ đặt tại ổ đĩa hệ thống của máy tính tại Folder ***Documents And Settings***. Khi bạn đăng nhập vào lần đầu, Windows Server 2003 tạo Folder con trong ***Documents And Settings***, với tên là tên đăng nhập. Hình 6-10 chỉ ra cấu trúc thư mục của khái lược người dùng.



Hình 6-10: Cấu trúc của thư mục Khái lược Người dùng

Chức năng của các Folder trong khái lược người dùng như sau:

- **Application Data:** Folder ẩn chứa dữ liệu xác định trong chương trình, như từ điển tùy chỉnh. Nhà phát triển ứng dụng sẽ quyết định dữ liệu nào sẽ được lưu trong Folder này.
- **Cookies:** Chứa các thông tin người sử dụng trang WEB và các sở thích của người dùng được Internet Explorer lưu.
- **Desktop:** Chứa các biểu tượng trên màn hình nền, bao gồm ***shortcut*** đến các file và Folder.
- **Favorites:** Chứa ***shortcut*** tới các trang được ưa thích trên Internet.
- **Local Settings:** Là Folder ẩn,chứa Folder ***Application Data*** và Folder ***History***, cũng như các Folder phụ thêm khác dành cho việc chứa các file tạm thời .

- **My Documents:** Chứa các tài liệu được lưu trữ bởi người dùng.
- **My Recent Documents:** Là Folder ẩn, chứa ***shortcuts*** của các tài liệu mới vừa được sử dụng hoặc các Folder mới được truy nhập tới.
- **NetHood:** Là Folder ẩn**,** chứa các ***shortcut*** tới các mục trong ***My Network Places***.
- **PrintHood:** Là Folder ẩn, chứa các ***shortcut*** tới các mục của Folder ***printer***.
- **SendTo:** Là Folder ẩn, chứa các ***shortcut*** tới các tiện ích quản lý văn bản (***document-handling***).
- Thực đơn **Start :** Chứa các ***shortcut*** đến các file chạy và các file khác tạo thành thực đơn Start .
- **Templates:** Chứa các mục mẫu của người dùng.

Thêm vào đó, khái lược người dùng còn chứa một bản của file ***NtUser.dat***, Đây là file đăng ký của Windows Server 2003 chứa các thiết lập của người dùng. Ngoài ra, các thiết lập này còn gồm rất nhiều các tùy chọn mà bạn có thể cấu hình tại ***Control Panel***.

Sử dụng Khái lược Người dùng Cục bộ

Việc sử dụng Khái lược Người dùng Cục bộ trên máy tính sử dụng Windows Server 2003 là hoàn toàn ẩn đối với các người dùng thông thường. Hệ điều hành khởi tạo Khái lược Người dùng một các tự động cho mỗi người dùng khi đăng nhập lần đầu. Các lần đăng nhập tiếp theo, Windows Server 2003 sẽ tải cấu hình từ đúng Khái lược Người dùng của họ trước đó.

Thậm chí người dùng không biết được rằng chính họ đã các thay đổi Khái lược Người dùng Cục bộ của mình, đơn giản như là thay đổi thiết lập màn hình nền, lưu các địa chỉ ưa thích mới hoặc đổi lại màu màn hình. Khi người dùng thay đổi môi trường màn hình nền, Windows Server 2003 sẽ kết hợp các thay đổi đó vào khái lược người dùng lưu trên máy tính và sử dụng cho lần đăng nhập tiếp theo. Như vậy, người dùng đăng nhập vào máy tính chạy Windows Server 2003 sẽ luôn nhận được thiết lập màn hình nền như phiên kết nối cuối trước đó. Khi nhiều người dùng chung một máy tính thì môi người dùng duy trì và nhận được Khái lược Người dùng riêng.

Sử dụng Khái lược Người dùng Di trú (*Roaming Profiles*)

Để hỗ trợ người dùng làm việc trên nhiều máy tính, quản trị mạng có thể thiết lập các Khái lược Người dùng Di trú cho người dùng. Khái lược Người dùng Di trú đơn giản là bản sao chép của Khái lược Người dùng Cục bộ và

được lưu trữ chia sẽ trên mạng (tại nơi người dùng có các Cấp phép phù hợp), do đó người dùng có thể truy nhập tới từ bất cứ máy tính nào trên mạng. Cho dù người dùng đăng nhập từ bất ký máy tính nào, họ cũng sẽ luôn nhận được cùng một thiết lập màn hình nền và và kết nối từ Khái lược Người dùng được để trên máy chủ, hoàn toàn ngược lại với Khái lược Người dùng Cục bộ, chỉ nằm tại một máy trạm.

Để người dùng truy nhập vào Khái lược Người dùng Di trú thay cho Khái lược Người dùng Cục bộ, bạn phải mở hộp thoại ***Properties*** của người dùng và chỉ định vị trí của Khái lược Người dùng Di trú tạo hộp Profile Path trong Profile thẻ. Lần tiếp theo người dùng đăng nhập, Windows Server 2003 truy nhập vào Khái lược Người dùng Di trú theo cách sau:

1. Khi người dùng đăng nhập lần đầu tiên, máy tính sao chép toàn bộ nội dung của Khái lược Người dùng Di trú vào Folder con và file tương ứng trong Folder ***Documents And Settings*** trên đĩa cục bộ của máy tính này.

1. Nội dung Khái lược Người dùng Di trú của người dùng chứa trên đĩa cho phép người dùng đăng nhập và truy nhập tới Khái lược Người dùng ngay cả khi máy chủ chứa Khái lược Người dùng Di trú không hoạt động.

2. Máy tính áp dụng các thiết lập có trong Khái lược Người dùng Di trú dành cho nó.

3. Khi người dùng làm việc mà có bất kỳ thay đổi nào ảnh hưởng tới Khái lược Người dùng, chúng sẽ được lưu vào bản sao trên đĩa cục bộ.

4. Khi người dùng thoát khỏi Windows (*log off*), máy tính sẽ đồng bộ các thay đổi từ bản sao cục bộ lên Khái lược Người dùng Di trú trên máy chủ.

5. Lần đăng nhập tiếp theo trên cùng máy tính này, hệ thống sẽ so sánh nội dung của Khái lược Người dùng đuợc để tại máy cục bộ với Khái lược Người dùng Di trú để trên máy chủ

6. Máy tính chỉ sao chép những thành phần của Khái lược Người dùng Di trú bị thay đổi vào bản sao cục bộ, việc này làm tiến trình đăng nhập vào nhanh và hiệu quả hơn.

Bạn nên tạo Khái lược Người dùng Di trú trên Máy chủ Quản lý File (***File Sever***) nào bạn thường xuyên thực hiện việc sao lưu (***Backup***), nhờ đó bạn sẽ có được các bản sao của các Khái lược Người dùng mới nhất cho các người dùng của bạn. Để tăng tốc độ đăng nhập trên các mạng co nhiều lưu thông, hãy đặt Khái lược Người dùng Di trú trên máy chủ thành viên thay

cho máy chủ điều khiển miền. Việc sao chép Khái lược Người dùng Di trú giữa máy chủ và các máy trạm có thể tốn nhiều tài nguyên hệ thống như băng thông mạng và các chu kỳ xử lý. Nếu để Khái lược Người dùng trên máy chủ điều khiển miền, tiến trình xác thực của các người dùng miền sẽ bị chậm.

> ***LƯU Ý: Lý do chia sẻ profile.*** *Khi bạn tạo một Khái lược Người dùng Di trú cho nhiều máy trạm, cần đảm bảo là bạn đã cân nhắc đến việc phân chia các chủng loại cấu hình phần cứng khác nhau trên các hệ thống sẽ dùng chung một if. Ví dụ như nếu các* ***Shortcut*** *trên màn hình nền được cấu hình cho độ phân giải màn hình là 1024×768 và bạn đang nhập vào hệ thống có cạc màn hình chỉ đáp ứng độ phân giải 800×600 thì một số* ***shortcut*** *có thể không nhìn thấy được. Các Khái lược Người dùng cũng không hoàn toàn là có thể dùng cho tất cả các hệ điều hành.. Khái lược Người dùng thiết kế cho Windows 98 không có đầy đủ các chức năng như trên Windows Server 2003. Thậm chí, bạn sẽ gặp phải các sự không đồng nhất khi thực hiện di trú giữa các hệ thống chạy Windows Server 2003 và chạy Windows XP hoặc Windows 2000.*

SỬ DỤNG KHÁI LƯỢC NGƯỜI DÙNG BẮT BUỘC

Khái lược Người dùng Bắt buộc chính là Khái lược Người dùng Di chủ dạng chỉ đọc. Người dùng cũng nhận được các thiếp lập màn hình nền như khi họ làm việc với Khái lược Người dùng Di trú và họ có thể cấu hình màn hình nền sau khi đã đăng nhập nhưng không một thay đổi nào được ghi lại khi họ thoát ra khỏi Windows. Lần đăng nhập tiếp theo, Khái lược Người dùng lại giống như lần đăng nhập trước. Windows Server 2003 tải Khái lược Người dùng Bắt buộc vào máy tính cục bộ mỗi lần người dùng đăng nhập. Bạn có thể gán một Khái lược Người dùng Bắt buộc cho nhiều người dùng có chung một yêu cầu đối với các thiết lập màn hình nền, ví dụ như một nhóm người dùng có cùng một công việc. Do Khái lược Người dùng không bao giờ bị thay đổi, nên bạn không cần lo lắng là ai đó làm thay đổi gây ảnh hưởng tới những người dùng khác. Ngoài ra, Khái lược Người dùng Bắt buộc còn giúp bạn có thể thay đổi môi trường màn hình nền cho nhiều người dùng bằng cách chỉ thay đổi duy nhất một Khái lược Người dùng mà thôi.

Để tạo Khái lược Người dùng Bắt buộc bạn chỉ cần đổi lại tên file ***NtUser.dat*** trong Folder chứa Khái lược Người dùng Di trú thành ***NtUser.man***, ***NtUser.dat*** là file ẩn chứa các thiết lập đăng ký của Windows Server 2003 áp dụng cho cho từng tài khoản người dùng đơn lẻ và chứa các

thiết lập môi trường của người dùng như hiển thị nền. Đổi tên file này với phần mở rộng là ***.man*** làm nó thành chỉ đọc, ngăn không cho các máy tính người dùng lưu các thay đổi vào Khái lược Người dùng khi người dùng thoát ra khỏi Windows.

GIÁM SÁT VÀ KHẮC PHỤC SỰ CỐ VIỆC XÁC THỰC NGƯỜI DÙNG

Khi bạn đã cấu hình đối tượng người dùng và và các người dùng sẽ được xác thực thông qua các tài khoản như vậy, bạn sẽ gặp phải hai thách thức đó là các *điểm yếu bảo mật*, trong trường hợp nếu không được xác định rõ sẽ làm ảnh hưởng.đến tính toàn vẹn của mạng, và các thách thức về *kỹ năng xã hội*, khi bạn làm cho quá trình xác thực trở nên thân thiện và đáng tin cậy đối với người dùng. Không may là hai điểm này lại bất đồng với nhau, nếu tính bảo mật càng cao bao nhiêu thì tính thân thiện với người dùng càng kém bấy nhiêu.

Việc thực thi các tính năng bảo mật cho qúa trình xác thực người dùng của Windows Server 2003 sẽ thường xuyên gay ra các rắc rối khi người dùng đang nhập. và một phần công việc của người quản trị mạng là giải quyết các rắc rối khi chúng xảy ra. Trong phần tiếp theo, chũng ta sẽ khảo sát một số các nguyên nhân phổ biến gây ra các rắc rối khi xác thực người dùng và các công cụ mà bạn có thể dùng để phát hiện và khu trú chúng.

Sử dụng các Chính sách Mật khẩu

Trong phần trước của chương này, tại phần "*Lựa chọn Mật khẩu"*, bạn đã tìm hiểu về Chính sách Mật khẩu mà Windows Server 2003 cung cấp, cho phép bạn xác định chiều dài, độ phức tạp và thời hạn của mật khẩu được người dùng cấp cho tài khoản của họ. Mục đích chính của các chính sách này là buộc người dùng đặt mật khẩu một cách hiệu quả và họ phải định kỳ thay đổi mật khẩu.

Thật là dễ dàng khi sử dụng Chính sách Mật khẩu để buộc người dùng phải sử dụng các mật khẩu có độ an toàn rất cao, nhưng việc yêu cầu người dùng mật khẩu phức tạp có 15 ký tự và thay đổi lại hàng tuần dường như làm nảy sinh thêm các vấn đề rắc rối nhiều hơn là các lợi ích mà nó mang lại. Nhân viên hỗ trợ mạng có lẽ sẽ nhận được các cuộc goi "quên mật khẩu" thường xuyên của người dùng, và thậm chí còn tệ hơn, người dùng sẽ ghi mật khẩu lại và để ở những nơi không đảm bảo an toàn.

Bạn phải thiết kế Chính sách Mật khẩu sao cho nó làm nản chí một cách có hiệu quả các kẻ xâm nhập trong khi vẫn đảm bảo được tính thân thiện tốt cho người dùng, để họ không bị quên mật khẩu hay phải viết chúng ra.

> ***LƯU Ý: Xác định độ dài mật khẩu.*** *Khi bạn triển khai chính sách mật khẩu cần nhớ rằng Windows Server 2003, Windows XP Professional và Windows 2000 hỗ trợ các mật khẩu dài tới 127 ký tự, nhưng Windows 95, Windows 98 và Windows Me chỉ hỗ trợ các mật khẩu có độ dài tối đa tới 14 ký tự.*

Có năm chính sách mật khẩu được đưa ra ở phần trên của chương này có thể áp dụng với các đối tượng Chính sách Nhóm ***Active Directory***. Mà bạn có thể cấu hình bằng cách sử dụng bảng điều khiển ***Group Policy Object Editor***, trong đó bạn duyệt đên ***Computer Configuration\Windows Settings \Security Settings\Account Policies\Password Policy***. Tuy nhiên, bạn cũng có thể xác định cũng các chính sách như vậy cho các Tài khoản Người dùng Cục bộ bằng cách sử dụng bảng điều khiển ***Local Security Policy,*** có trong nhóm chương trình ***Administrative Tools*** trên bất cứ một máy chủ thành viên chạy Windows Server 2003 nào

> ***LƯU Ý: Thay đổi Chính sách Mật khẩu.*** *Cấu hình độ dài mật khẩu và các yêu cầu về độ phức tạp không gây ảnh hưởng tới các mật khẩu đã đặt từ trước. Những thay đổi này chỉ ảnh hưởng với các tài khoản mới và mật khẩu sẽ thay đổi sau khi đã áp dụng chính sách mật khẩu mới.*

SỬ DỤNG CHÍNH SÁCH KHOÁ TÀI KHOẢN

Việc khoá tài khoản xảy ra sau một số lần cố tình đăng nhập không thành công của người dùng, hệ thống giả thiết là có tấn công có hại tới tài khoản bằng cách dò tìm mật khẩu, bởi vậy sẽ khoá tài khoản để không được đăng nhập tiếp nữa. Chính sách khoá tài khoản miền xác định số lần đăng nhập không hợp lệ được phép thực hiện trong một khoảng thời gian đã định trước trước thì tài khoản bị khoá. Các chính sách này thậm chí còn được xác định có phải liên hệ với quản trị để bỏ khoá tài khoản này hay không hay chỉ đơn giản là bỏ khóa sau khi hết một thời hạn xác định.

> ***LƯU Ý: Mục đích của kỳ thi.*** *Mục đích của kỳ thi 70-290 xác định thí sinh có khả năng "chẩn đoán và giải quyết các tài khoản bị khoá."*

Bạn sử dụng chính sách nhóm để kiểm soát khoá tài khoản như sau:

- **Account Lockout Threshold:** Xác định số lần cố tình đăng nhập không thành công gây ra việc khoá tài khoản, giá trị này trong khoảng từ 0 tới 999. Giá trị quá thấp (ví dụ là 3) có thể gây nên khoá đối với lỗi người dùng thông thường trong khi đăng nhập. Giá trị là 0 ngăn không cho tài khoản người dùng bị khoá.

- **Account Lockout Duration:** Xác định thời hạn mà tài khoản người dùng sau khi bị khoá sẽ được ***Active Directory*** tự động mở lại. Chính sách này không đực thiết lập mặc định do nó chỉ có tác dụng khi sử dụng kết hợp với chính sách ***Account Lockout Threshold***. Giá trị này trong khoảng từ 0 tới 99.000 phút (khoảng 10 tuần). Việc đặt giá tri này thấp (5 tới 15 phút) là đủ để giảm đáng kể các cuộc tấn công mà không làm ảnh hưởng các người dùng hợp lệ bị khóa do lỗi. Giá trị 0 yêu cầu người dùng liên hệ với người quản trị để mở khóa tài khoản này.
- **Reset Account Lockout Counter After:** Xác định thời hạn sau lần cố tình đăng nhập không thành trước khi biến đếm khóa (***Lockout counter***) được đặt lại về giá trị 0. Giá trị trong khoảng từ 1 tới 99.999 phút và phải nhỏ hơn hay bằng giá trị của ***Account Lockout Duration***.

Cũng giống như đối với Chính sách Mật khẩu, bạn có thể cấu hình chính sách tài khoản tại bảng điều khiển ***Group Policy Object Editor***, chọn ***Computer Configuration\Windows Settings\Security Settings\Account Policies\Account Lockout Policy***. Chính sách khoá tài khoản cũng có thể có tại bảng điều khiển ***Local Security Policy***.

Khi bạn triển khai chính sách khoá tài khoản trên mạng, bạn chắc chắn là sẽ nhận được một số cuộc gọi hỗ trợ nhất định từ người dùng mà họ không biết là đã tự khoá chính mình. Các cuộc gọi như vậy đôi khi lại được báo cáo là họ gặp một số trục trặc khác, như mât mật khẩu hay các chức năng khác hoạt động không đúng. Khi dó các nhân viên hỗ trợ kỹ thuật hiểu biết cần phải biết rõ về chính sách khoá tài khoản trên mạng và thủ tục để mở tài khoản bị khoá để có thể xác định được chính xác về trục trặc thực tế xẩy ra dựa trên báo cáo dường như không mấy chính xác của người dùng.

> ***LƯU Ý: Mục đích của kỳ thi.*** *Mục đích của kỳ thi 70-290 xác định thí sinh có khả năng "khắc phục sự cố của tài khoản người dùng"và "Khắc phục các sự cố liên quan đến việc xác thực người dùng."*

DỊCH VỤ ACTIVE DIRECTORY MÁY KHÁCH

Khi bạn làm việc trên một mạng hỗn hợp, bạn cần nhớ là không phải mọi hệ điều hành thâm chí không phải tất cả các hệ điều hành Windows đều hỗ trợ ***Active Directory***. ***Active Directory*** được giới thiệu đầu tiên tại Windows 2000 và chỉ trên các hệ điều hành Windows 2000, Windows XP và Windows Server 2003 mới có các tính năng của dịch vụ ***Active Directory*** máy khách.

Các máy tính chạy Windows 95, Windows 98, Windows Me, and Windows NT 4 có thể có chức năng của dịch vụ Active Directory máy khách, nhưng trước hết bạn phải tải phần mềm ***Active Directory Client*** từ trang Web của Microsoft và cài đặt nó. Các máy khách có thể thực hiện rất nhiều tính năng của ***Active Directory*** trên hệ thống Windows Server 2003, Windows XP và Windows 2000, gồm có:

- **Site-awareness:** Máy tính chạy dịch vụ ***Active Directory*** máy khách sẽ đăng nhập vào máy điều khiển miền gần nhất trên mạng thay cho vào máy chủ điều khiển miền chính (PDC - *Primary Domain Controller*).
- **Active Directory Service Interfaces (ADSI):** kích hoạt khả năng sử dụng các kịch bản (***script***) để quản lý ***Active Directory***.
- **Distributed File System (Dfs):** Cho phép máy khách truy nhập vào tài nguyên chia sẻ của hệ thống file phân phối (***Dfs***) trên máy chủ chạy Windows Server 2003 và Windows 2000.
- **NT LAN Manager (NTLM) version 2 authentication:** Máy khách sử dụng tính năng xác thực cải tiến trong ***NTLM version 2***.
- **Active Directory search capability:** máy khách có thể tìm kiếm các đối tượng ***Active Directory*** bằng cách sử dụng các tính năng tìm kiếm (***Find*** hoặc ***Search***). Người dùng có các Cấp phép thích hợp còn có thể sử dụng các trang thuộc tính của ***Windows Address Book*** (WAB) để cấu hình các thuộc tính của các đối tượng.

Các tính năng sau đầy hỗ trợ trong Windows 2000 Professional and Windows XP Professional nhưng không dành cho dịch vụ ***Active Directory*** máy khách trên Windows 95, Windows 98, and Windows NT 4:

- Xác thực Kerberos V5
- Hỗ trợ ***Group Policy*** hoặc ***Change And Configuration Management***
- ***Service Principal Name*** (SPN) hoặc xác thực lẫn nhau
- Hỗ trợ ***Internet Protocol Security*** (IPSec) hoặc ***Layer 2 Tunneling Protocol*** (L2TP).

Thêm vào đó, bạn nên ý thức được các vấn đề sau trong môi trường hỗn hợp:

- Không có dịch vụ ***Active Directory*** máy khách, người dùng trong hệ thống chạy các phiên bản trước Windows 2000 chỉ có thể thay đổi mật khẩu nếu hệ thống truy nhập được tới máy điều khiển miền có chức năng như là ***Primary Domain Controller Emulator***. Để xác định

PDC-Emulator trong miền, mở ***Active Directory Users And Computers***, chọn miền, chọn lệnh ***Operations Masters*** từ thực đơn ***Action*** , sau đó chọn thẻ PDC. ***Nếu PDC Emulator*** không làm việc (hoặc khôgn ở trên mạng (***offline***) hoặc ở đang nằm trên phía bên kia của kết nối mạng bị đứt) thì người dùng không thể thay đổi được mật khẩu của họ.

- Như bạn đã bạn tìm hiểu trong phần trước của chương này, đối tượng người dùng duy trì hai thuộc tính tên người dùng đăng nhập. Tên đăng nhập ***Pre–Windows 2000***, hay tên SAM là tương ứng với tên người dùng trong Windows 95, Windows 98 hoặc Windows NT 4. Khi người dùng đăng nhập, họ nhập tên người dùng và chọn miền từ danh sách chọn ***Log On To***. Cách khác nữa là tên người dùng có thể được vào theo dạng ***DomainName\UserLogonName***. Người dùng đăng nhập vào máy chạy Windows 2000 hoặc các phiên bản sau đó của hệ điều hành Windows có thế đăng nhập theo cùng cách như vậy, hoặc họ có thể sử dụng tên UPN theo dạng ***UserLogonName@UPN Suffix***, trong đó ***UPN suffix*** mặc định là tên DNS miền của đối tượng người dùng. Khi đó bạn không cần phải chọn miền từ ***Log On To***. Trên thực tế hộp chọn này sẽ bị vô hiệu hoá ngay sau khi bạn gõ ký hiệu ***@***.

KIỂM ĐỊNH XÁC THỰC

Nếu bạn lo lắng rằng có thể có các cuộc tấn công dò tìm mật khẩu hoặc bạn muốn biết thêm thông tin về khắc phục các vấn đề sự cố xác thực, bạn có thể cấu hình ***Chính sách Kiểm định*** để ghi các sự kiện lại vào nhtj ký bảo mật (***Security log***) giúp bạn thấy rõ quá trình xác thực đã diễn ra như thế nào..

Các chính sách kiểm định sau được đặt tại ***Computer Configuration \Windows Settings\Security Settings\Local Policies\Audit Policy*** ở cả hai bảng điều khiển ***Group Policy Object Editor*** và ***Local Security Policy***. Bạn có thể cấu hình để ghi lại các sự kiện thành công hoặc bị lỗi.

- **Audit Account Logon Events:** Ghi lại từng sự kiện đăng nhập thành công hoặc lỗi. Đối với Máy chủ Điều khiển Miền, chính sách này được xác định trong Chính sách Máy chủ Điều khiển Miền Mặc định (***Default Domain Controllers Policy*** GPO). Việc kích hoạt chính sách trên sẽ khởi tạo một mục vào của nhật ký bảo mật trên Máy chủ Điều khiển Miền mỗi lần người dùng đăng nhập trực tiếp hoặc qua mạng sử dụng tài khoản miền. Để đánh giá đầy đủ kết quả của việc kiểm định bạn phải kiểm tra nhật ký bảo mật trên tất cả các Máy chủ Điều khiển

Miền do người dùng được xác thực phân tán trên tất các các Máy chủ Điều khiển Miền trong site hoặc miền

- **Audit Account Management:** Cấu hình kiểm định trong tác vụ quản trị bao gồm tạo, xoá hoặc sửa tài khoản người dùng, nhóm, máy, máy tính, cũng như việc đặt lại mật khẩu
- **Audit Logon Events:** Sự kiện đăng nhập gồm đăng nhập và thoát ra khởi Windows, trực tiếp hoặc qua mạng. Nếu bạn kích hoạt chính sách kiểm định sự kiện tài khoản đăng nhập cho những lần thành công trên máy điều khiển miền, việc đăng nhập máy trạm sẽ không tạo ra các mục vào kiểm định khi đăng nhập. Chỉ đăng nhập trực tiếp và qua mạng vào Máy chủ Điều khiển Miền mới tạo ra các sự kiện đăng nhập. Các sự kiện đăng nhập của tài khoản được tạo trên máy cục bộ cho tài khoản cục bộ và trên Máy chủ Điều khiển Miền cho các tài khoản mạng. Các sự kiện đăng nhập được sinh ra bất cứ lúc nào khi việc đăng nhập xảy ra.

LƯU Ý: Mục đích kỳ thi. *Mục đích của kỳ thi 70-290 xác định thí sinh có khả năng "Phán đoán và giải quyết các vấn đề liên quan tới các thuộc tính tài khoản người dùng".*

Một khi bạn đã cấu hình chính sách kiểm định, nhật ký bảo mật sẽ bắt đầu điền các thông điệp sự kiện. Bạn có thể xem các thông điệp này bằng cách sử dụng bảng điều khiển ***Event Viewer*** .

THÔNG TIN THÊM: Để *biết thêm thông tin về việc sử dụng bảng điều khiển* ***Event Viewer****, xem chương 3 "Giám sát Microsoft Windows Server 2003."*

TỔNG KẾT

- Các máy tính chạy Windows Server 2003 có thể có tài khoản người dùng cục bộ và miền. Tài khoản người dùng cục bộ được lưu tại hệ thống cục bộ và có thể cho người dùng truy nhập vào chỉ các tài nguyên cục bộ mà thôi. Tài khoản người dùng miền để tại CSDL ***Active Directory*** của Máy chủ Điều khiển Miền và cho người dùng truy nhập vào toàn bộ tài nguyên trên mạng.
- Để tạo tài khoản người dùng miền, bạn phải là thành viên của nhóm ***Enterprise Admins, Domain Admins*** hoặc ***Account Operators***. Hoặc bạn phải được uỷ quyền tạo đối tượng người dùng.
- Đối tượng người dùng gồm các thuộc tính chính tương ứng với "tài khoản" người dùng, bao gồm tên đăng nhập, mật khẩu và mã nhận dạng bảo mật (SID) của người dùng. Chúng còn bao gồm một số các thuộc tính liên quan đến cá nhân người dùng mà nó đại diện như thông tin cá nhân, quaqn hệ nhóm và các thiết lập quản trị. Windows Server 2003 cho phép bạn có thể thay đổi một số các thuộc tính này cho nhiều đối tượng người dùng một cách đồng thời.
- Đối tượng người dùng mẫu (***Template***) là các đối tượng được sao chép trong quá trình tạo các người dùng mới. Nếu mẫu không là người dùng "thật", nó nên để là vô hiệu hoá. Chỉ một số các thuộc tính của người dùng là được chép từ mẫu.
- ***CSV Directory Exchange*** cho phép bạn có thể nhập các đối tượng từ tệp văn bản có phân cách các trường bởi dấu phẩy ("**,**").
- Windows Server 2003 gồm các công cụ dạng dòng lệnh mà bạn có thể sử dụng để tạo và quản lý các đối tượng ***Active Directory*** bao gồm cả ***Dsadd.exe*** và ***Dsmod.exe***
- Khái lược người dùng là các tập các Folder của các Folder và file tạo thành môi trường cho người dùng xác định. Khái lược người dùng gồm các tài liệu cá nhân, biểu tượng trên màn hình nền, các thực đơn ***Start shortcut*** và các thiết lập ***Control Panel*** như màu màn hình, …
- Windows Server 2003 tạo khái lược người dùng riêng cho từng cá nhân đăng nhập vào hệ thống. Khái lược Người dùng được đặt mặc định cục bộ tại ***Systemdrive\Documents and Settings\UserName***.
- Khái lược người dùng cục bộ được để tại đĩa cục bộ, còn khái lược người dùng di trú để trên máy chủ. Khái lược Người dùng Di trú cung cấp cho người dùng có cùng khái lược người dùng từ bất kỳ máy tính nào trên mạng.

- Khái lược Người dùng Bắt buộc không bao giờ bị thay đổi, cung cấp cùng một cấu hình nền thống nhất tại mỗi lần người dùng đăng nhập.
- Kiểm định xác thực tạo ra các sự kiện cho nhật ký bảo mật của Máy chủ Điều khiển Miền.

BÀI TẬP THỰC HÀNH

Bài tập thực hành 6-1: Thay đổi các Thiết lập Chính sách Mật khẩu

Trong Bài tập thực hành này, bạn sửa lại các thiết lập chính sách mật khẩu mặc định trên máy tính của bạn.

1. Đăng nhập vào Windows Sever 2003 domain như ***Administrator***.
2. Bấm chọn ***Strat***, chỉ đến ***Administrative Tools*** và chọn ***Active Directory Users And Computer***, khi đó sẽ xuất hiện bảng điều khiển ***Active Directory Users And Compute***.
3. Chọn đối tượng miền, chọn thực đơn ***Action,*** chọn ***Properties***, xuất hiện hộp thoại ***Properties*** .
4. Tại thẻ ***Group Policy***, chọn ***Default Domain Policy*** và chọn ***Edit***, xuất hiện bảng điều khiển ***Group Policy Object Editor***.
5. Dưới ***Computer Configuration***, mở ***Windows Settings***, ***Security Settings*** và ***Account Policies***, sau đó chọn ***Password Policy***.
6. Kích đúp ***Minimum Password Length policy***, xuất hiện hộp thoại ***Minimum Password Length Properties***.
7. Thay đổi ***Minimum Password Length*** thành 8 ký tự và sau đó chọn ***OK***.
8. Kích đúp ***Maximum Password Age***, xuất hiện hộp thoại ***Maximum Password Age Properties.***
9. Thay đổi thiết lập ***maximum password age*** thành 7 ngày, sau đó chọn ***OK***.
10. Đóng bảng điều khiển ***Group Policy Object Editor***.
11. Bấm ***OK*** và đóng hộp thoại ***Properties*** của miền**.**
12. Đóng the bảng điều khiển ***Active Directory Users And Computers***.

Bài tập thực hành 6-2: Tạo đối tượng người dùng miền

Trong Bài tập thực hành này, bạn sẽ tạo đối tượng mới trong đối tượng chứa ***Active Directory***.

1. Đăng nhập vào Windows Server 2003 Máy chủ Điều khiển Miền như ***Administrator***.

2. Bấm ***Start***, chỉ đến ***Administrative Tools*** và bấm ***Active Directory Users And Computers***. Xuất hiện bảng điều khiển ***Active Directory Users And Computers***.
3. Mở đối tượng miền và chọn the đối tượng chứa ***Users***. Trong thực đơn ***Action*** trỏ tới ***New*** và bấm ***User***. Xuất hiện trình hướng dẫn ***New Object – User***.
4. Tại ***Full Name***, gõ vào **Mark Lee**.
5. Tại ***User Logon Name***, gõ **mlee**, và bấm ***Next***.
6. Tại ***Password*** và ***Confirm Password***, type **rabbit!runs4all**, và chọn ***Next***.
7. Bấm ***Finish*** để tạo đối tượng mới.
8. Đóng bảng điều khiển ***Active Directory Users And Computers***.

Bài tập thực hành 6-3

Trong Bài tập thực hành này, bạn sẽ di chuyển một đối tượng người dùng đến một đối tượng chứa khác.

1. Đăng nhập vào Windows Server 2003 máy điều khiển miền như ***Administrator***.
2. Bấm ***Start***, trỏ tới ***Administrative Tool***s và bấm ***Active Directory Users And Computers***. Xuất hiện bảng điều khiển ***Active Directory Users And Computers***.
3. Mở đói tượng miền và chọn đối tượng chứa ***Users***. Chọn tiếp ***Guest***.Trên thực đơn ***Action*** , chọn ***Move***. Xuất hiện hộp thoại ***Move***.
4. Chọn đối tượng chứa ***Computers***, bấm ***OK***. Người dùng ***Guest*** đã được chuyển tới đối tượng chứa ***Computers***.
5. Chọn đối tượng chứa ***Computers***.
6. Chọn đối tượng người dùng ***Guest*** và kéo nó vào đối tượng vhứa ***Users***. Đối tượng ***Guest*** đã được chuyển lại vào đối tượng chứa ***Users***.

CÁC CÂU HỎI ÔN TẬP

1. Bạn sử dụng bảng điều khiển ***Active Directory Users And Computers*** để cấu hình đối tượng người dùng trong miền, và bạn có thể thay đổi thuộc tính ***address*** và ***telephone number*** của đối tượng người dùng. Tuy nhiên, Lệnh ***New User*** không chọn được. Hãy giải thích?
2. Các thuộc tính nào sau đây có thể cấu hình đồng thời trên hơn một đối tượng người dùng.
   a. Password Never Expires
   b. ***Direct Reports***
   c. ***User Must Change Password At Next Logon***
   d. ***Last Name***
   e. ***Logon Hour***s
   f. ***Computer Restrictions (Logon Workstation***s)
   g. User Logon Name
   h. Title
3. Trong ba phương pháp tạo đồng thời nhiều đối tượng người dùng đã thảo luận trong chương này, phương pháp nào là hiệu quả nhất để sinh ra 100 đối tượng người dùng mới, với tất cả các thuộc tính đã xác định của ***Profile Path, Home Folder***, ***Title, Web Page, Company, Department*** và ***Manager***
4. Biến nào có thể được sử dụng trong với lệnh chương trình ***Dsadd.exe*** và ***Dsmod.exe*** để tạo ***folder chủ*** và ***folders Profile*** cho người dùng xác định.
   a. ***%Username%***
   b. ***$Username$***
   c. ***CN=Username***
   d. ***<Username>***
5. Bạn làm thế nào để tạo một khái lược người dùng di trú bắt buộc?
   a. Cấu hình Cấp phép trong thuộc tính ***Security*** của folder với quyền ***write*** là ***Deny***.
   b. Cấu hình Cấp phép trong thuộc tính ***Sharing*** của folder với chỉ có quyền ***read only*** là ***allow***.

c. Cấu hình thuộc tính của folder ***profile*** là ***Read Only***

d. Đổi tên file ***Ntuser.dat*** thành ***Ntuser.man***.

6. Phân biệt sự khác nhau giữa khái lược người dùng cục bộ và khái lược người dùng di trú?
7. Làm thế nào bạn có thể chắc chắn là một người dùng trên máy tính chạy Windows Server 2003 có Khái lược Người dùng Bắt buộc?
8. Bạn có thể kích hoạt yêu cầu ***Password Must Meet Complexity Requirements*** trong miền của bạn. Hãy diễn tả các yêu cầu cho mật khẩu và khi nào thì các yêu cầu này sẽ thực hiện

CÁC KỊCH BẢN TÌNH HUỐNG

Kịch bản 6-1: Cấu hình đối tượng người dùng Properties

Bạn sẽ tạo một số các đối tượng người dùng cho một nhóm công nhân thời vụ của tổ chức của bạn. Họ sẽ làm việc hàng ngày từ 9 A.M. đến 5 P.M., theo hợp đồng thời gian kết thúc trong khoảng từ một đến hai tháng và họ sẽ không làm việc ngoài giờ. Thuộc tính nào sau đây bạn sẽ cấu hình để đảm bảo bảo mật tối đa cho các đối tượng này?

1. Password
2. Logon Hours
3. Account Expires
4. Store Password Using Reversible Encryption
5. Account Is Trusted For Delegation
6. User Must Change Password At Next Logon
7. Account Is Disabled
8. Password Never Expires

Kịch bản 6-2: Quản lý khoá tài khoản

Người dùng bị quên mật khẩu nhưng lại cố tình đăng nhập vài lần với mật khẩu sai. Rốt cục là người dùng nhận được thông báo đăng nhập chỉ ra tài khoản này đã bị vô hiệu hoá hoặc bị khoá, thông báo đề nghị liên hệ với quản trị mạng. Khi đó quản trị sẽ phải làm gì?

1. Xoá đối tượng người dùng và tạo lại.
2. Đổi tên đối tượng người dùng.
3. Kích hoạt đối tượng người dùng.

4. Mở khóa đối tượng người dùng.
5. Đặt lại mật khẩu của đối tượng người dùng.

CHƯƠNG 7: LÀM VIỆC VỚI NHÓM

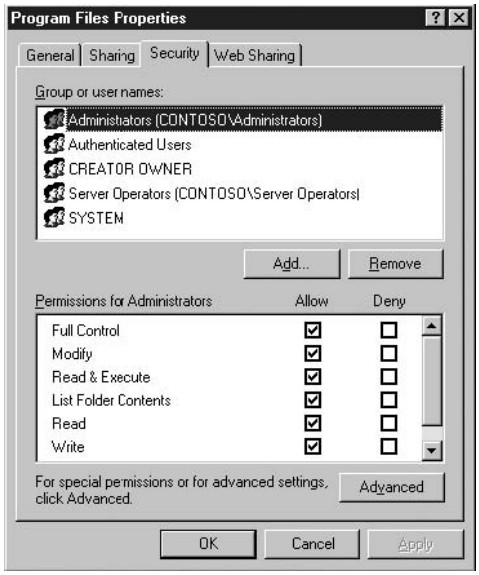
Trong chương 6, bạn đã biết các Đối tượng người dùng cung cấp sự truy cập đến các tài nguyên trong mạng sử dụng Active Directory cho các người sử dụng mạng như thế nào. Một công cụ quản trị quan trọng khác là Đối tượng Nhóm (***Group Object***). Sử dụng Nhóm, các quản trị viên có thể đơn giản hóa quá trình cấp phép truy cập cho người dùng. Trong chương này bạn sẽ được học về các loại nhóm mà Active Directory hỗ trợ, tạo chúng như thế nào, và làm thế nào để có thể sử dụng chúng một cách hiệu quả.

Kết thúc chương này, bạn có thể

- **Hiểu được các chức năng của Nhóm và cách sử dụng chúng như thế nào.**
- **Hiểu được sự khác nhau giữa Nhóm Cục bộ (Local Group) và Nhóm Miền (Domain Group).**
- **Nhận biết hai Kiểu Nhóm (Group type) và ba loại Phạm vi Nhóm (Group Scope) và làm thế nào để sử dụng chúng có hiệu quả.**
- **Liệt kê các Nhóm Dựng sẵn (Build-in) và các Nhóm Xác định Trước (Predefined) trong Microsoft Windows Server 2003.**
- **Hiểu được sự khác nhau giữa các Nhóm và các nhóm Đồng nhất Đặc biệt (Special Identities)**

HIỂU VỀ NHÓM

Để người dùng có khả năng truy cập các tài nguyên trên mạng ***Active Directory***, họ nhất thiết phải có các cấp phép thích hợp. Các thư mục, ổ đĩa, máy in được chia sẻ, và nói rộng hơn là tất cả các loại tài nguyên khác trên mạng đều có một Danh sách Kiểm soát Truy cập (***Access Control List*** - ACL). ACL chính là danh sách của các đối tượng được cho phép truy cấp đến tài nguyên, theo các mức độ truy cập khác nhau mà mỗi đối tượng được cấp. Trong ***Microsoft Windows Server 2003***, ACL được hiển thị tại thẻ ***Sercurity*** (Bảo mật) của phần lớn trong bất cứ hộp thoại ***Properties*** nào, như được thể hiện trong hình 7-1. Các đối tượng trong ACL được gọi là ***Sercurity Principals*** (Đối tượng bảo mật). Bạn có thể sử dụng Dối tượng người dùng như là các Đối tượng Bảo mật để trao cho người dùng quyền truy cập đến các tài nguyên họ cần, do Đối lượng người dùng xác định tính duy nhất của người dùng thông qua quá trình xác thực



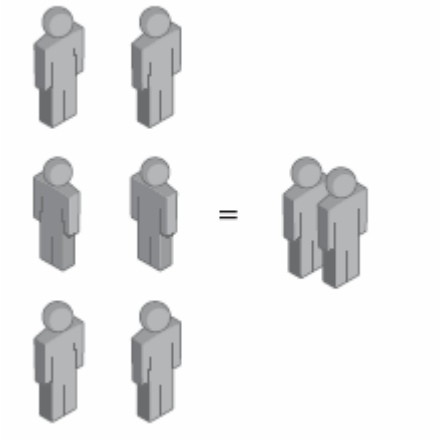
Hình 7-1: Thẻ Security trong hộp thoại Properties của thư mục

Về mặt lý thuyết, Quản trị viên có thể tạo toàn bộ các cấp phép cho mọi người dùng bằng cách thêm các Đối tượng người dùng vào ACL, và việc thực hiện điều này với toàn bộ các mạng máy tính (trừ trường hợp đối với các mạng rất nhỏ) là điều không thể do việc tiêu tốn một cách lãng phí thời gian và lao động. Hãy tưởng tượng bạn đang tuyển thêm 250 nhân viên mới và, sau khi đã tạo các Đối tượng người dùng cho họ, phải cấp phép cho họ truy cập khoảng một tá hoặc hơn các nguồn tài nguyên trải dài trên toàn bộ mạng. Thậm chí với trường hợp xấu nhất, giả sử máy chủ bị hỏng và bạn cần

cài đặt nhanh một máy chủ thay thế và sau đó tiến hành cấp phép cho 250 người để họ có thể truy cập đến máy chủ mới.

Để tránh những công việc kinh hoàng như đã nêu trên, Quản trị mạng sử dụng Nhóm. Nhóm sẽ làm đơn giản hóa danh sách của các người dùng có chức năng như các Đối tượng Bảo mật. Trong Active Directory Đối tượng Nhóm có thể bao gồm các Đối tượng người dùng, Máy tính, Mối liên hệ (***Contact***), và trong những điều kiện nhất định, thậm chí bao gồm cae Nhóm. Khi bạn sử dụng Đối tượng Nhóm như là Đối tượng Bảo mật bằng cách thêm chúng vào trong danh sách ACL, tất cả các thành viên trong nhóm đều nhận các cấp phép mà bạn đã gán cho nhóm (như đã chỉ ra trong hình 7-2). Nếu bạn thêm thành viên mới vào nhóm tại các thời điểm sau này, họ cũng sẽ nhận được các cấp phép giống như vậy. Nếu bạn loại bỏ thành viên nào đó, các cấp phép cho họ cũng bị loại bỏ theo.

Trong ví dụ đã nêu ở trên, bạn có thể tạo ra một Đối tượng Nhóm và gán cho nó các cấp phép mà những người mới được nhận vào làm việc cần có. Khi các nhân viên mới đến làm việc, toàn bộ các công việc bạn phải làm chỉ là tạo ra các Đối tượng người dùng cho họ và thêm họ vào Nhóm. Để đơn giản hóa việc tổ chức một máy chủ thay thế, bạn cần tạo ra một nhóm chứa toàn bộ các người dùng của máy chủ ban đầu. Nếu máy chủ hỏng và bạn cần chuyển sang sử dụng máy chủ thay thế, tất cả các công việc bạn cần làm là gán các cấp phép truy cập đến máy chủ mới cho Đối tượng Nhóm đã tạo, và tất cả các người dùng sẽ được chuyển qua sử dụng máy chủ mới một cách êm thấm. Trên các mạng có hệ thống các nhóm được thiết kế tốt, Quản trị mạng rất hiếm khi, nếu có, phải gán các cấp phép cho các người dùng riêng lẻ.



Hình 7-2: Là Đối tượng Bảo mất, một Nhóm tương đương với nhiều người dùng

Nhóm cũng có thể giúp chúng ta gán Quyền của người dùng cho nhiều người dùng cùng lúc. Trong ***Microsoft Windows Server 2003***, khái niệm Quyền (***Right***) hoàn toàn khác với khái niệm Cấp phép (***Permission***). Quyền của người dùng (***User right***) trao cho người dùng hay nhóm khả năng thực hiện một tác vụ nhất định, như truy cập đến một máy tính nào đó thông qua mạng, thay đổi thời gian hệ thống, hoặc giành quyền sở hữu (***Take ownership***) đối với file hay các đối tượng khác. Thêm vào đó, bạn cũng có thể sử dụng Nhóm để tạo ra các danh sách phân phối thư điện tử.

Sử dụng Nhóm (Group) và các Chính sách Nhóm (Group Policies - GP).

Trong chương 6, bạn đã biết rằng cấu trúc của cây ***Active Directory*** là một phần rất quan trọng của quá trình tạo Tài khoản người dùng trong Miền do các Quyền và Cấp phép ta đã gán cho các Đối tượng chứa sẽ được các Đối tượng con của nó thừa hưởng, bao gồm cả các Đối tượng người dùng. Việc thừa kế giữa các nhóm cũng làm việc giống như thế, với các thành viên sẽ nhận được các thiết lạp đã gán cho nhóm. Sự kác biết chủ yếu giữa đối tượng nhóm và Đối tượng Chứa là Đối tượng Nhóm không bị chi phối bởi cấu trúc hình cây của Active Directory. Bạn có thể tạo ra nhóm với các thành viên ở bất cứ đâu trong miền, thậm trí tại các miền khác, và trao cho chúng các đặc quyền chỉ với một thao tác đơn giản.

Chính sách Nhóm, mặc dù với tên như vậy, được kết hợp chặt chẽ với các Đối tượng Chứa nhiều hơn là với các Đối tượng Nhóm. Đối tượng Chính sách Nhóm (***Group Policy Object*** - GPO) chỉ có thể gán với các Đối tượng Miền, Vị trí (Site), OU có sử dụng ***Active Directory***, và các thiết lập của chúng sẽ được truyền xuống theo cây ***Active Directory***. Bạn không thể gán GPO cho nhóm, mặc dù trong nhiều trường hợp, bạn có thể cấu hình các thiết lập Chính sách Nhóm để cấu hình một vài tính năng của hệ điều hành trên tất cả các thành viên của Nhóm.

Ví dụ, bạn có thể tạo đối tượng OU trong cây ***Active Directory*** bao gồm tất cả các đối tượng máy trạm trong miền của bạn và gán GPO cho OU này. Tất cả các máy tính trong OU sẽ được thừa hưởng các thiết lập chính sách nhóm từ GPO này, và một trong các thiết lập này có thể kích hoạt Quyền Quản lý Kiểm định và Nhật ký Bảo mật (***Manage Auditing And Security Log***), gán quyền này cho đối tượng nhóm có các Nhân viên Hỗ trợ Kỹ thuật Tin học. Trong trường hợp náy, các máy tính trong OU nhận được các thiết lập chính sách nhóm từ GPO, và các chính sách như vậy sẽ trao quyền cho các đối tượng nhóm nhất định.

Tìm hiểu về các Cấp Chức năng của Miền

Một trong số các hiểu lầm phổ biến nhất đối với khái niệm ***Active Directory*** chính là Cấp Chức năng. Các Quản trị mạng đôi khi cũng nản lòng trước viễn cảnh của việc thay đổi Cấp Chức năng của Miền hay Rừng do nó là một trong vài quyết định mà bạn sẽ không thể thu hồi được trong ***Microsoft Windows Server 2003***. Khi bạn đã thay đổi cấp chức năng, bạn sẽ không có cơ hội để đổi ngược nó lại.

Nói nột cách đơn giản, các phiên bản khác nhau của Windows có một chút khác nhau trong việc thực thi các chức năng của ***Active Directory***. Mỗi phiên bản thành công sẽ có một vài tính năng mới không được sử dụng tới khi một vài Máy chủ Quản trị Miền (DC) hiện đang chạy các phiên bản cũ của Windows. Việc thay đổi Cấp Chức năng của Miền sẽ thông báo cho hệ điều hành biết rằng tất cả các Máy chủ Quản trị Miền đều tương thích và là an toàn để kích hoạt các tính năng chỉ có trong phiên bản mới.

Trong ***Microsoft Windows Server 2003***, bốn Cấp Chức năng có thể có của chúgn bao gồm: ***Windows 2000 mixed*** (Pha trộn), ***Windows 2000 Native*** (Tự nhiên), ***Windows 2003 Interim*** (Chuyển tiếp), và ***Windows Server 2003***. Các cấp chức năng nói trên hỗ trợ các Máy chu Quản trị Miền chạy trong môi trường kết hợp rất nhiều các hệ điều hành, và chúng sẽ cung cấp rất nhiều các tính năng phụ thêm, và một vài tính năng này sẽ được áp dụng cho chức năng của Đối tượng Nhóm trong Miền. Các đặc tính của Cấp Chức năng cho Miền được liệt kê sau đây:

> ***LƯU Ý: Cấp Chức năng cho Miền và các Máy chủ Thành viên:*** *Nâng cấp Chức năng cho Miền không hạn chế các máy tính chạy các phiên bản cũ của Windows gia nhập vào miền. Cấp chức năng chỉ đề cập đến các Máy chủ Quản trị Miền. Các miền đang chạy ở cấp chức năng Windows Server 2003 vẫn có thể hỗ trợ các máy chủ thành viên và máy trạm chạy các hệ điều hành Windows 2000, Windows NT, Windows XP, Windows Me, Windows 98 và Windows 95 một khi chúng được cài đặt đúng các phần mềm Active Directory máy khách.*

- **Windows 2000 Mixed:** là Cấp chức năng mặc định của Máy chủ Quản tri Miền Windows Server 2003.
    - Hỗ trợ các Máy chủ Quản tri Miền chạy Windows Server 2003, Windows Server 2000, và Windows NT 4.
    - Hỗ trợ Nhóm Phân phối Tổng hợp (Universal Distribution Group), nhưng không hỗ trợ Nhóm Bảo mật Tổng hợp (Universal Security Group).

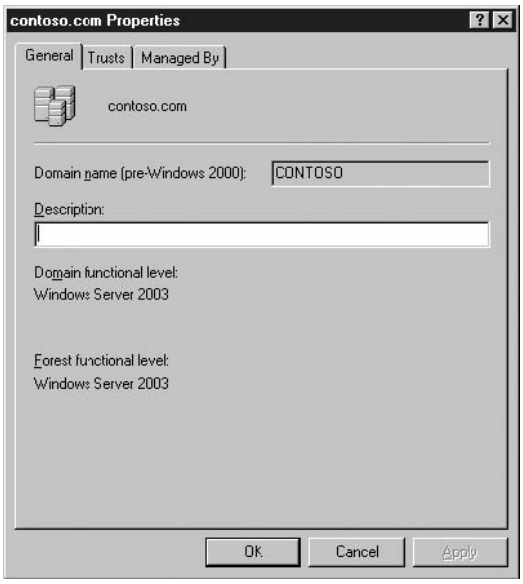
  - Nhóm Toàn cục (Global Group) không thể chứa các nhóm khác (nhóm trong nhóm).
  - Việc chuyển đổi các nhóm là không được phép.

- **Windows 2000 Native:** Hỗ trợ các Máy chủ Quản tri Miền chạy Windows Server 2003 và Windows Server 2000.
  - Hỗ trợ các Nhóm Phân phối và Bảo mật Tổng hợp.
  - Cho phép một hay nhiều nhóm là thành viên của nhóm khác.
  - Cho phép chuyển đổi qua lại giữa các Nhóm Bảo mật và Nhóm Phân phối.
  - Cho phép di chuyển các Đối tượng Bảo mất (Security Principal) từ Miền này qua Miền khác (Lịch sử SID).
- **Windows Server 2003 Interrim:** Hỗ trợ các Máy chủ Quản tri Miền chạy Windows Server 2003 và Windows NT 4. Cấp chức năng này chỉ được sử dụng khi bạn có ý định nâng cấp các Máy chủ Quản tri Miền đang chạy Windows NT 4 lên Máy chủ Quản tri Miền chạy Windows Server 2003.
  - Không cung cấp các tính năng mới.
- **Windows Server 2003:** Chỉ hỗ trợ các Máy chủ Quản tri Miền chạy Windows Server 2003.
  - Hỗ trợ các Nhóm Phân phối và Bảo mật Tổng hợp.
  - Cho phép một hay nhiều nhóm là thành viên của nhóm khác (nhóm trong nhóm).
  - Cho phép chuyển đổi qua lại giữa các Nhóm Bảo mật và Nhóm Phân phối.
  - Cho phép di chuyển các Đối tượng Bảo mất (Security Principal) từ Miền này qua Miền khác (Lịch sử SID).

LƯU Ý: Các tính năng của Cấp chức năng trong Miền*: các chức năng đã liệt kê trên chỉ bao gồm các tính năng của Active Directory đối với các Cấp chức năng mà gắn liền với Đối tượng nhóm và các hoạt động của nó. Tăng cấp chức năng cho miền đồng thời cũng kích hoạt nhiều tính năng khác, như khả năng đổi tên miền, . Một vài tính năng phụ thêm của Active Directory cũng sẽ được kích hoạt trong trường hợp bạn tăng cấp chức năng cho rừng trên mạng của bạn, khi tất cả các Máy chủ Quản tri Miền trong toàn bộ rừng đều*

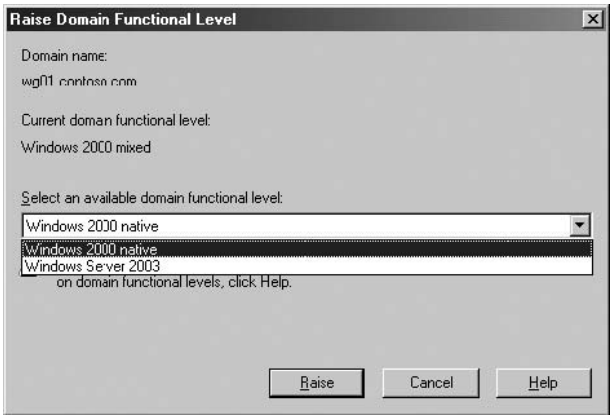
chạy Windows Server 2003. Và mặc dù vậy, các chức năng này không hề ảnh hưởng đến việc sử dụng các Đối tượng Nhóm.

*Để quản trị Cấp chức năng trong Windows Server 2003, ta sử dụng bảng điều khiển **Active Directory Domain And Trusts** nằm trong nhóm chương trình "**Administrative Tools**". Để xem được Cấp chức năng hiện tại của Miền và Rừng, Chọn đối tượng Miền trong ô Phạm vi và nhấn **Properties** trong thực đơn **Action**. Hộp thoại **Properties** của miền sẽ hiển thị Cấp chức năng hiện tại trên thẻ **General**, như được chỉ ra trên hình 7-3.*



Hình 7-3: Hộp thoại Properties của miền.

Để thay đổi Cấp chức năng, chọn đối tượng miền và từ thực đơn Action, nhấn "***Raise Domain Functional Level***" (*Tăng cấp chức năng cho miền*) để hiển thị hộp thoại như hình 7-4. Trong danh sách xổ "***Select An Available Doamain Functional Level***" (*Lựa chọn cấp chức năng cho miền*), chọn cấp chức năng bạn muốn sử dụng và nhấn ***Raise*** (*Nâng cấp*). Như đã nói ở trên, bạn không thể hạ cấp chức năng sau khi đã nâng cấp chúng, ngoại trừ trường hợp bạn cài đặt lại Active Directory trên toàn bộ các Máy chủ Quản tri Miền trong mạng của bạn, do vậy chương trình sẽ cảnh báo bạn cần chắc chắn về các quyết định của chính mình. Một khi cấp chức năng đã được nâng cấp tại một Máy chủ Quản tri Miền, thay đổi sẽ được nhân bản đến toàn bộ các Máy chủ Quản tri Miền khác trong miền.



Hình 7-4: Hộp thoại "Raise Domain Functional Level"

> ***LƯU Ý Nâng cấp chức năng cho Rừng:*** *Để nâng cấp chức năng cho rừng, bạn chọn đối tượng "**Active Directory Domains And Trusts**" trong ô Phạm vi và từ thực đơn Action, nhấn "**Raise Forest Function Level**".*

SỬ DỤNG NHÓM CỤC BỘ

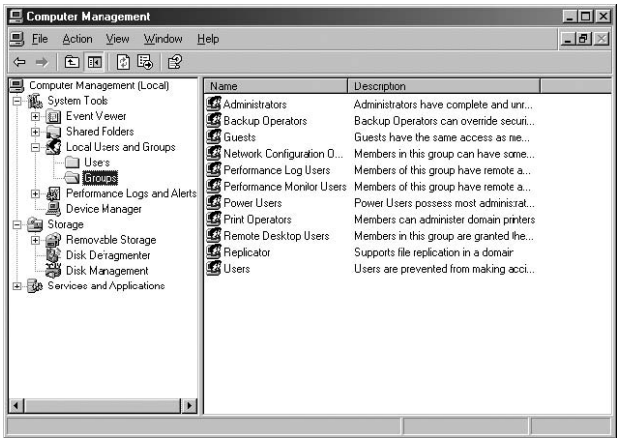
Trong chương 6, bạn đã biết Windows Server 2003 hỗ trợ cả hai loại tài khoản: Tài khoản người dùng Cục bộ, và Tài khoản người dùng trong Miền. Mọi việc cũng đúng như vậy với Nhóm. Windows Server 2003 hỗ trợ các Nhóm Cục bộ (***Local Group***) và Nhóm trên Miền (***Domain Group***).

Một nhóm Cục bộ là một tập hợp của các Tài khoản người dùng Cục bộ trên một máy tính nhất định. Nhóm cục bộ thực hiện cùng các chức năng cơ bản của Nhóm: nó cho phép bạn có thể gán các Cấp phép cho nhiều người dùng trong cùng một bước thực hiện. Bạn tạo Nhóm cục bộ bằng Snap-in "***Local Users And Groups***" đã được tích hợp trong bảng điều khiển "***Computer Management***" (có thể truy cập từ nhóm chương trình "***Administrative Tools***"), như đã chỉ ra trong hình 7-5. Khi bạn tạo ta Nhóm Cục bộ, hệ thống sẽ lưu chúng tại CSDL của Trình Quản lý Tài khoản bảo mật (***Security Accounts Manager*** - SAM)

Các nhóm Cục bộ cũng có những hạn chế giống như đối với các người dùng cục bộ. Các hạn chế của nhóm cục bộ được liệt kê sau:

- Bạn chỉ có thể sử dụng Nhóm Cục bộ chỉ trên máy tính nơi bạn tạo ra nó.
- Chỉ có các người dùng cục bộ trên cùng máy tính có thể là thành viên của Nhóm cục bộ.

- Khi máy tính là thành viên của một miền, thành viên của nhóm cục bộ có thể bao gồm các người dùng và các nhóm toàn cục của miền này hay bất cứ miền nào khác được tin cậy.
- Nhóm cục bộ không thể có các thành viên là các nhóm cục bộ khác.
- Việc cấp phép cho nhóm cục bộ chỉ cung cấp việc truy cập đến các nguồn tài nguyên trên chính máy tính mà bạn tạo ra nhóm.
- Bạn không thể tạo ra nhóm cục bộ trên máy tính chạy Windows Server 2003 đóng vai trò như là Máy chủ Quản tri Miền



Hình 7-5: Snap-in "Local Users And Groups"

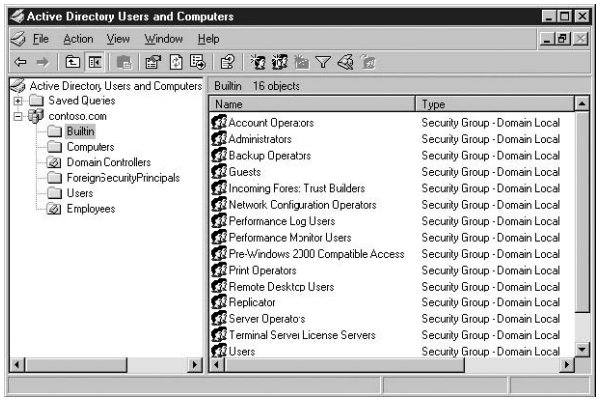
SỬ DỤNG NHÓM ACTIVE DIRECTORY

Các nhóm Active Directory được phân biệt bởi Kiểu (***Type***) và Phạm vi (***Scope***) của chúng. Nhóm Active Directory có hai kiểu, mà mỗi kiểu đều có ba Phạm vị khác nhau. Việc xây dựng các nhóm này đúng phạm vi của nó sẽ giúp chúng ta sử dụng tốt nhất nguồn lực quản trị khi tạo, gán, và quản lý việc truy cập đến các nguồn tài nguyên. Khả năng của việc xây dựng các nhóm cũng phụ thuộc vào Cấp chức năng của miền mà tại đó các nhóm được tạo ra. Windows Server 2003 có hàng loạt các nhóm được tạo sẵn, và bạn cũng có thể tạo ra thêm bao nhiêu nhóm là tùy vào yêu cầu của bạn.

Nhóm Active Directory, không phụ thuộc vào kiểu hay phạm vi của nó, là các đối tượng trong CSDL Active Directory, cũng giống như Tài khoản người dùng và đối tượng Chứa là các đối tượng. So sánh với đối tượng người dùng, đối tượng nhóm là hoàn toàn tương tự. Thay vào hàng tá các thuộc tính (***attribute***) của đối tượng người dùng, đối tượng nhóm chỉ có một vài thuộc tính, mà quan trọng nhất trong số đó là danh sách các thành viên. Như tên của nó đã chỉ ra, Danh sách Thành viên đơn giản chỉ là một danh sách các đối tượng, như người dùng, các nhóm khác, máy tính, và Liên lạc

(***Contact***), đó là các thành viên của nhóm. Tất cả các Cấp phép và Quyền được gán cho nhóm sẽ được mọi đối tượng có tên trong danh sách thành viên của nhóm thừa kế.

Trong Windows Server 2003, bạn có thể tạo và quản trị tất cả các nhóm Active Directory bằng cách sử dụng bảng điều khiển "A***ctive Directory Users And Computers***", mà ta có thể truy cập từ nhóm chương trình "***Adminitrative Tools***". Như chỉ ra trên hình 7-6. Giống như đối với bất cứ một đối tượng Active Directory nào, để có thể tạo và quản trị được nhóm bạn cần có các cấp phép thích hợp tại đối tượng chứa, nơi nhóm được bố trí.



Hình 7-6: Bảng điều khiển "Active Directory Users And Computers"

Kiểu của Nhóm Active Directory

Nhóm Active Directory có hai kiểu: nhóm Bảo mật (***Security***) và nhóm Phân phối (***Distribution***).

Nhóm Bảo mật

Nhóm bảo mật là nhóm bạn dùng để gán các cấp phép để nó có thể truy cập tới các tài nguyên mạng. Khi một người nào đó nói tới nhóm liên quan tới Windows Server 2003 hay Active Directory, thông thường là họ đề cập đến nhóm Bảo mật. Các chương trình được thiết kế để làm việc với Active Directory cũng có thể sử dụng các nhóm Bảo mật cho các mục đích không liên quan tới việc bảo mật, ví dụ như gọi các thông tin người dùng để sử dụng trong các ứng dụng Web.

> ***LƯU Ý Windows Server 2003 chỉ sử dụng nhóm Bảo mật:*** *Nhóm Bảo mật có thể sử dụng như các nhóm Phân phối, ngược lại, nhóm Phân phối không thể sử dụng như nhóm Bảo mật. Bản thân Windows Server 2003 chỉ có thể sử dụng nhóm Bảo mật nhưng do nhóm Bảo mật có đầy đủ các tính năng của nhóm Phân phối nên đây không phải là một thiếu sót của hệ điều hành.*

Nhóm Phân phối

Nhóm Phân phối được sử dụng cho các chương trình có các chức năng không liên quan tới bảo mật. Bạn sử dụng nhóm Phân phối chỉ khi chức năng của nhóm không liên quan đến việc bảo mật, như gửi E-mail đến một nhóm các người dùng trong cùng thời điểm. Bạn không thể sử dụng nhóm Phân phối để gán Quyền hay Cấp phép. Chỉ các chương trình được thiết kế làm việc với Active Directory là co sthể sử dụng nhóm Phân phối. Thí dụ như Microsoft Exchange sử dụng nhóm Phân phối như là danh sách gửi thư để gửi E-mail

Phạm vi của nhóm Active Directory.

Phạm vi của nhóm xác định việc các Cấp phép được gán cho các thành viên của nhóm như thế nào. Tất cả các nhóm ***Active Directory***, cả nhóm Phân phối và nhóm Bảo mật, đều có thể xếp vào một trong ba Phạm vi: ***Domain Local*** (*cục bộ Miền*), ***Global*** (*Toàn thể*), và ***Universal*** (*Tổng hợp*).

Nhóm *Domain Local* (*cục bộ miền)*

Nhóm cục bộ miền thường được sử dụng để gán các Cấp phép truy cập đến các tài nguyên, hoặc trực tiếp hoặc bằng cách thêm nhóm ***Global*** vào nhóm ***Doain Local***. Nhóm ***Doain Local*** có các đặc tính sau:

- Nhóm ***Doain Local*** tồn tại trong tất cả các cấp chức năng: ***Windows 2000 Mixed, Windows 2000 native, Windowws Server 2003 interim***, và ***Windows Server 2003***.
- Bạn chỉ thể sử dụng nhóm cục bộ miền để trao các Cấp phép truy cập chỉ đến các tài nguyên trên cùng miền bạn tạo ra nhóm.
- Khi bạn sử dụng Cấp Chức năng ***Windows 2000 mixed*** hay ***Windows 2003 interim***, thành viên của nhóm cục bộ miền có thể bao gồm các Tài khoản người dùng, Tài khoản Máy tính và các nhóm ***Global*** từ bất cứ miền nào trong rừng. Ngoài ra, không tồn tại bất cứ một kiểu nhóm trong nhóm nào khác.
- Khi bạn sử dụng Cấp chức năng Windows 2000 native hay Windows Server 2003, nhóm cục bộ miền có thể bao gồm các Tài khoản người dùng, Máy tính, các nhóm ***Global*** và ***Universal*** từ bất cứ miền nào trong rừng, và các nhóm cục bộ miền khác trong cùng miền. Nhóm cục bộ miền có thể được chuyển thành nhóm ***Universal*** khi nó không có thành viên nào là nhóm cục bộ miền.

LƯU Ý Nhóm cục bộ (Local) và nhóm cục bộ trên miền (Domain Local) : *do các nhóm* ***Active Directory*** *có phạm vi* ***Domain Local*** *đôi khi được đề cập đến như là nhóm* ***local****, cần có sự phân biệt chính xác giữa các nhóm* ***local*** *trên một máy tính nào đó (đôi khi được gọi là nhóm* ***local*** *trên máy tính) và nhóm* ***Active Directory*** *có Phạm vi* ***Domain Local****.*

Nhóm cục bộ miền được sử dụng thông thường nhất để kiểm soát sự truy cập tới các tài nguyên chỉ trong một miền đơn. Ví dụ như bạn có thể tạo một nhóm cục bộ miền để trao cấp phép cho các thành viên của nó được truy cập đến một máy in nhất định. Sau đó bạn có thể thêm trực tiếp các người dùng trong miền vào nhóm cục bộ miền đã tạo, hoặc bạn có thể tạo ra các nhóm ***Global*** gồm các người dùng cần truy cập đến máy in và đặt nhóm ***Global*** này là thành viên của nhóm cục bộ miền đã tạo.

Nhóm *Global*

Nhóm Global được sử dụng để cung cấp các thành viên đã được phân loại trong nhóm cục bộ miền cho các đối tượng Bảo mật hay cho việc gán các Cấp phép một cách trực tiếp (riêng cho trường hợp mạng sử dụng Cấp chức năng ***Windows 2000 mixed***, hay ***Windows Server 2003 interim***). Thông thường, nhóm ***Global*** được sử dụng để gom các người dùng và Máy tính trong cùng một miền mà có cùng công việc, vai trò, hay chức năng hoặc họ có cùng các nhu cầu tương tự trong việc truy cập mạng. Nhóm ***Global*** có các đặc tính sau:

- Nhóm ***Global*** có mặt tại tất cả các Cấp Chức năng: ***Windows 2000 Mixed, Windows 2000 native, Windowws Server 2003 interim***, và ***Windows Server 2003***.
- Nhóm ***Global*** chỉ bao gồm các thành viên từ cùng một miền.
- Khi bạn sử dụng Cấp chức năng ***Windows 2000 native*** hay ***Windows Server 2003***, thành viên của nhóm ***Global*** có thể bao gồm các Tài khoản người dùng, Máy tính cũng như các các nhóm ***Global*** khác trong cùng miền.
- Nhóm ***Global*** có thể chuyển đổi thành nhóm ***Universal*** một khi nó không phải là thành viên của bất cứ một nhóm ***Global*** nào khác.
- Khi bạn sử dụng Cấp Chức năng ***Windows 2000 Mixed***, nhóm ***Global*** chi bao gồm các thành viên là Tài khoản người dùng, Máy tính trong cùng miền mà thôi.

- Nhóm ***Global*** có thể là thành viên của nhóm ***Machine Local*** (Máy tính Cục bộ) hay nhóm ***Domain Local*** (*cục bộ miền*)**.**
- Nhóm ***Global*** có thể được trao các Cấp phép truy cập đến các tài nguyên trên bất cứ miền nào trong rừng và trên các miền được tin cậy nằm trên rừng khác.

Nhóm ***Global*** được sử dụng thông dụng nhất trong việc quản lý các Cấp phép cho các đối tượng Thư mục, như Tài khoản người dùng và Máy tính, thường yêu cầu việc bảo trì trường xuyên. Trên một mạng bao gồm nhiều miền, lợi ích chính của việc sử dụng nhóm ***global*** thay cho nhóm ***Universal*** trong việc quản lý các Cấp phép là ở chỗ nhóm ***global*** không bị nhân bản ngoài phạm vi của miền. Điều này làm giảm các lưu thông mạng được dùng cho việc nhân bản đến ***Global Catalog,*** là thư mục của toàn bộ các tài nguyên trong rừng. Sử dụng nhóm ***Global*** để gán các Cấp phép cho các đối tượng cần nhân bản đến ***Global Catalog*** sẽ là thích hợp hơn so với việc sử dụng nhóm ***Domain Local*** cho mục đích này.

Nhóm *Universal*

Nhóm ***Universal*** được sử dung chủ yếu để trao các Cấp phép truy cập đến các tài nguyên trên nhiều miền. Nhóm ***Universal*** có các đặc tính sau:

- Nhóm Universal chỉ xuất hiện trong các Cấp chức năng ***Windows 2000 native*** và ***Windows Server 2003***.
- Thành viên của nhóm ***Universal*** có thể bao gồm các Tài khoản người dùng, Máy tính, các nhóm ***Global***, và các nhóm ***Universal*** khác trong bất cứ miền nào trong rừng. Nhóm ***Universal*** có thể chuyển đổi thành nhóm ***Domain Local***, nhóm ***Global*** khi chúng không có các nhóm ***Universal*** khác là thành viên.
- Khi bạn sử dụng Cấp Chức năng Windows 2000 mixed, bạn không thể tạo ra nhóm ***Universal***.
- Nhóm ***Universal*** có thể được trao các Cấp phép để truy cập đến các tài nguyên trong bất kể miền nào trong rừngvà trong các miền nằm trong các rừng đã được tin cậy.

Chức năng chính của nhóm ***Universal*** là tập hợp các nhóm mở rộng qua nhiều miền. Nói chung, nhóm ***Universal*** là không cần thiết trên mạng chỉ bao gồm một miền đơn. Để sử dụng nhóm ***Universal*** một cách hiệu quả, tốt nhất là chúng ta tạo nhóm ***Global*** trên mỗi miền, trong đó có chứa các Tài khoản người dùng và Máy tính, sau đó thêm các nhóm ***Global*** này vào danh sách thành viên của nhóm ***Universal***. Việc này cho phép bạn có thể tạo ra

một nhóm ***Universal*** đơn mà có thể sử dụng trên toàn bộ doanh nghiệp, với mối quan hệ thành viên không bị xáo trộn một cách thường xuyên.

Phương pháp trên thường được lựa chọn hơn so với việc thêm trực tiếp người dùng và Máy tính vào nhóm ***Universal*** một cách trực tiếp do mối thay đổi về thành viên tại nhóm ***Universal*** sẽ dẫn tới việc toàn bộ các mối quan hệ thành viên đều phải được nhân bản đến ***Global Catalog***. Quản lý các người dùng và Máy tính trong nhóm ***Global*** sẽ không ảnh hưởng đến quan hệ thành viên của nhóm ***Universal*** và do đó không sinh ra các lưu thông phụ thêm cho việc nhân bản.

Nhóm ***Universal*** cũng là hữu dụng khi chúng ta muốn trao Cấp phép cho người dùng được truy cập đến các tài nguyên nằm trên nhiều hơn một miền. Không giống nhóm cục bộ miền, ban có thể gán các Cấp phép cho nhóm ***Universal*** được truy cập đến các nguồn tài nguyên được bố trí tại bất cứ miền nào trên mạng của bạn. Ví dụ, nếu ban lãnh đạo cần truy cập đến các máy in trên toàn bộ mạng của ban, bạn có thể tạo nhóm ***Universal*** cho mục đích này và gán Cấp phép cho nó, như vậy toàn bộ các thành viên của nhóm này có thể sử dụng tất cả các máy in hiện có trên tất cả các miền trong mạng.

Nhóm trong nhóm (*Group nesting*).

Như đã biết trong phần trước, khả năng đưa một nhóm là thành viên của nhóm khác là một trong các tính năng hữu dụng của việc thực thi đối tượng nhóm Active Directory. Kỹ thuật này được gọi là "Nhóm trong nhóm: -(*Group nesting*). Thực thi nhóm trong nhóm tạo cho bạn có khả năng quản lý việc cấp phép truy cập tài nguyên một cách hiệu quả hơn trong doanh nghiệp của bạn mà không gây ra các lưu thông phụ thêm bất thường cho việc nhân bản. Như đã nhắc tới ở trên, miền của bạn bắt buộc phải sử dụng Cấp chức năng Windows 2000 native hay Windows Server 2003 để nhận được đầy đủ các tính năng ưu việt của khả năng nhóm trong nhóm của Active Directory, và thậm chí như vậy, vẫn còn các hạn chế trong việc thực thi kỹ thuật nhóm trong nhóm của các loại Phạm vi nhóm khác nhau. Các hạn chế này, cũng với toàn bộ các hạn chế về thành viên trong ba phạm vi nhóm, được tổng kết trong bảng 7-1

Bảng 7-1: Các qui tắc thành viên của Phạm vi nhóm

Phạm vi nhóm cục bộ miền	Thành viên đối với cấp chức năng Windows 2000 Mixed hay Windows Server 2003 Interim: Tài khoản người dùng, Máy tính và nhóm global từ bất cứ miền nào	Thành viên đối với cấp chức năng Windows 2000 Native hay Windows Server 2003: Tài khoản người dùng, Máy tính, nhóm universal, and nhóm global từ bất cứ miền nào; nhóm cục bộ miền trong cùng miền
Global	Tài khoản người dùng, Máy tính trong cùng miền	Tài khoản người dùng, Máy tính, nhóm global khác trong cùng miền
Universal	Không áp dụng	Tài khoản người dùng, Máy tính, nhóm universal, và nhóm global từ bất cứ miền nào trong rừng

Các qui tắc thành viên trong bảng trên là yếu tố đầu tiên của việc quản trị nhóm một cách hiệu quả. Nếu bạn rơi vào trường hợp bạn không thể thêm thành viên nhất định nào đó vào một nhóm hay không thể sử dụng nhóm để cung cấp việc truy cập đến một nguồn tài nguyên nào đó, quá trình xử lí sự cố nên bắt đầu bằng việc thử lại Phạm vị nhóm và Cấp chức năng, để xác định bạn có được hỗ trợ trong việc thực hiện các tác vụ nói trên không.

Mặc dù kỹ thật *nhóm trong nhóm* là một công cụ đáng giá, Quản trị mạng nên thận trọng với các tính năng của nó. Khi bạn bố trí nhóm theo nhiều lớp sâu, có thể làm cho việc theo dõi các quan hệ thành viên và các cấp phép được thừa kế thế nào trên toàn mạng trở nên khó khăn hơn. Một qui luật chung, bố trí *nhóm trong nhóm* một cấp là hữu hiệu trong phần lớn các môi trường mạng và là dễ duy trì hơn.

Chuyển đổi nhóm

Khi bạn tạo nhóm, bạn phải xác định kiểu và phạm vi của nó. Mặc dù vậy, trong miền sử dụng cấp chức năng Windớ 2000 Native hay Windows Server 2003, bạn có thể chuyển đổi các nhóm đã tạo sang phạm vi khác bất cứ lúc nào, có lưu ý đến mọt số hạn chế trong quan hệ thành viên. Bảng 7-2 tổng kết các chuyển đổi Phạm vi nhóm được phép và các điều kiện cần thiết để chuyển đổi.

Bảng 7-2: Các hạn chế chuyển đổi Phạm vi nhóm Active Directory

	Đến Domain Local	Đến Global	Đến Universal
Từ Domain Local	Không áp dụng	Không được phép	Cho phép chỉ trong trường hợp không có thành viên là nhóm cục bộ miền
Từ Global	Không được phép	Không áp dụng	Cho phép nếu không là thành viên của nhóm Global khác
Từ Universal	Không hạn chế	Cho phép nếu không có nhóm Universal khác là thành viên	Không áp dụng

Xây dựng Nhóm Global và Domain Local

Sẽ là một ý tưởng tốt nếu bạn có một chiến lược nhóm sẵn sàng trước khi tạo ra các nhóm Active Directory. Tạo ra các nhóm với Kiểu và Phạm vi sai sẽ dẫn đến việc gặp các lỗi khi thực thi các tác vụ đã định. Đối với phần lớn việc cài đặt mạng, phương pháp thường thấy nhất là phát triển các nhóm sủ dụng Phạm vi ***Global*** và ***Domain Local*** theo các tiêu chí sau:

- **Tạo nhóm cục bộ miền cho các tài nguyên được chia sẻ:** Xác định các tài nguyên, như thư mục hay máy in mà người dùng cần truy cập, và tạo một hay hai nhóm cho các tài nguyên này. Ví dụ: nếu bạn có một số các máy in mầu trong công ty, tạo nhóm cục bộ miền có tên "***Color Printer***".
- **Gán các Cấp phép truy cập tài nguyên cho nhóm cục bộ miền :** gán các Cấp phép cần thiết để truy cập tài nguyên cho nhóm cục bộ miền tương ứng. Ví dụ: bạn cần gán các Cấp phép cần thiết để có thể sử dụng các máy in mầu cho nhóm "***Color Printer***".
- **Tạo các nhóm Global cho các người dùng có cùng các yêu cầu công việc:** Xác định các người dùng có cùng các yêu cầu công việc và thêm đối tượng người dùng của họ vào nhóm ***Global***. Ví dụ: trong phòng Kế toán, thêm Đối tượng người dùng của tất cả các kế toán viên vào nhóm "***Accounting***".
- **Thêm nhóm Global cần truy cập tài nguyên vào nhóm cục bộ miền tương ứng:** Xác định tất cả các nhóm ***Global*** có yêu cầu truy

cập đến một nguồn tài nguyên nhất định, và đưa các nhóm ***Global*** đó là thành viên của nhóm ***domain local*** tương ứng. Ví du: để các kế toán viên có thể truy cập đến các máy in mầu, thêm nhóm ***Global "Accounting"*** vào nhóm ***domain local*** "***Color Printer***". Các người dùng trong nhóm "***Accounting***" sẽ nhận được các Cấp phép đã trao cho nhóm "***Color Printer***".

Khi bạn đã tạo ra các nhóm theo các tiêu chí trên, bạn sẽ điều chỉnh các Cấp phép cho nhóm cục bộ miền khi nguồn tài nguyên cần thay đổi và sẽ điều chỉnh thành viên của nhóm ***Global*** khi nhân sự cần thay đổi.

Có thể bạn sẽ nghĩ rằng việc sử dụng cả hai loại Phạm vi nhóm: ***Domain Local*** và ***Global*** là không cần thiết. Sau hết, bạn vẫn có thể chỉ tạo một nhóm đơn, hoặc ***Domain Local*** hoặc ***Global***, trao cho nó các cấp phép cần thiết để truy cập tài nguyên, và thêm các đối tượng người dùng của các nhân viên cần truy cập tài nguyên đó vào là thành viên của nhóm. Mặc dù vậy, sẽ có các hạn chế rõ rệt trong chiến lược này, bất kể bạn đang sử dụng nhóm ***domain local*** hay nhóm ***Global***.

- **Đặt Đối tượng người dùng vào nhóm cục bộ miền và trao cấp phép cho nhóm cục bộ miền:** Chiến lược này không cho phép bạn gán các Cấp phép cho các tài nguyên ngoài miền, nó làm giảm mức độ linh hoạt của chiến lược nhóm khi mạng của bạn phát triển.
- **Đặt Tài khoản người dùng vào nhóm Global và trao Cấp phép cho nhóm Global:** Chiến lược này làm phức tạp hơn công việc quản trị khi bạn sử dụng mô hình nhiều miền. Nếu các nhóm ***Global*** trong các miền khác nhau yêu cầu cùng một tập các cấp phép, bạn phải gán các cấp phép này cho mỗi nhóm ***Global*** riêng rẽ.

CÁC NHÓM MẶC ĐỊNH CỦA WINDOWS SERVER 2003

Windows Server 2003 sẽ tự động tạo ra một số lớn các nhóm trong đó chứa các Tài khoản người dùng dựng sẵn. Bạn có thể sử dụng các nhóm này, thay đổi chúng nếu cần (trong một vài trường hợp), hay tạo ra các nhóm mới của riêng bạn. Có bốn loại nhóm mặc định trong Windows Server 2003: Nhóm Cục bộ dựng sẵn, chỉ tồn tại trong trường hợp máy tính không phải là Máy chủ Quản tri Miền, và ba loại nhóm mặc định trong Active Directory - nhóm xác định trước (***Predefined Group***), nhóm dựng sẵn (***Built-in Group***), và nhóm đồng nhất đặc biệt (***Special Identities Group***). Ta sẽ thảo luận về các nhóm mặc định này trong phần tiếp theo.

Nhóm Cục bộ Dựng sẵn (Built-in Local Group)

Máy chủ độc lập chay Máy chủ thành viên chạy Windows Server 2003 tất cả đều có các nhóm cục bộ dựng sẵn. Máy chủ Quản tri Miền không có các nhóm cục bộ (hay người dùng cục bộ) do SAM của nó đã được chuyển đổi sang sử dụng Active Directory. Các nhóm cục bộ dựng sẵn trao cho người dùng quyền để thực thi các tác vụ hệ thống trên một máy tính đơn lẻ, như là việc sao lưu và phục hồi file, thay đổi thời gian hệ thống, và quản trị các nguồn tài nguyên hệ thống. Các nhóm cục bộ dựng sẵn nằm trong thư mục ***Group*** của Snap-in "***Local Users And Groups***".

Các nhóm cục bộ dựng sẵn trong Windows Server 2003 và các khả năng của nó được chỉ ra dưới đây. Ngoại trừ tại những chỗ sẽ được chỉ ra cụ thể, không một nhóm nào khác có sẵn các thành viên.

- **Administrators (Nhóm Quản trị):** Thành viên của nhóm này có các quyền đầy đủ và không hạn chế khi truy cập đến máy tính và miền, giúp họ có thể thưch thi tất cả các tác vụ quản trị. Mặc đinh, người dùng cục bộ dựng sẵn "***Administrator***" là thành viên của nhóm này. Khi máy tính gia nhập vào miền, Windows Server 2003 thêm nhóm xác định trước "***Domain Admins***" vào nhóm này.
- **Backup Operators (nhóm Sao lưu):** Các thành viên của nhóm này có Quyền ***(User Rights***) cho phép họ có thể bỏ qua các hạn chế về bảo mật để có thể thực hiện các tác vụ Sao lưu và Phục hồi file.
- **Guests (Nhóm Khách):** Thành viên của nhóm này chỉ có thẻ thực hiện các tác vụ mà bạn trao quyền cho họ, và chỉ có thể truy cập đến các tài nguyên mà bạn đã cập phép cho họ truy cập. Họ cũng không thể tạo ra các thay đổi thường trực trên môi trường màn hình của họ. Mặc định, Tài khoản người dùng cục bộ dựng sẵn của máy tính "***Guest***" là thành viên của nhóm này. Khi máy tính gia nhập miền, Windows Server 2003 thêm nhóm toàn cục xác định trước "***Domain Guest***" vào nhóm này.
- **Network Configuration Operators** (**Nhóm cấu hình mạng**): Thành viên của nhóm này có một số quyền quản trị giới hạn, giúp họ có thể thực hiện các thay đổi thiết lập của TCP/IP, và làm mới hay giải phóng địa chỉ IP.
- **Performance Log Users (Nhóm ghi chép hiệu năng):** Thành viên của nhóm này được trao các quyền giúp họ có thể quản lý

được các biến đếm hiệu năng (***Performance Counter***), nhật ký (***Logs***), và Cảnh báo (***Alerts***) trên máy tính, cả tại chỗ lẫn từ xa.

- **Performance Monitor Users (Nhóm Theo dõi Hiệu năng):** Thành viên của nhóm này được trao các quyền giúp họ có thể theo dõi các biến đếm hiệu năng trên máy tính, cả tại chỗ lẫn từ xa.
- **Power Users (Nhóm Quyền lực):** Thành viên của nhóm này có thể tạo ra các Tài khoản Nhóm hay hay người dùng cục bộ trên máy tính và thay đổi các người dùng hay nhóm họ đã tạo ra đó. Họ cũng có thể thêm hay loại bỏ người dùng trong các nhóm cục bộ ***Power Users, Users*** và ***Guest***, tạo các nguồn tài nguyên chia sẻ, quản trị các nguồn tài nguyên chia sẻ họ đã tạo ra. ***Power Users*** không thể chiếm quyền sở hữu (***Take Ownership***) file, Sao lưu và Phục hồi thư mục, tải và dỡ bỏ các trình điều khiển thiết bị, hay quản trị các Bản ghi Bảo mật (***Security Log***).
- **Print Operators (Nhóm Vận hành Máy in):** Thành viên của nhóm này có thể quản trị các máy in và hàng đợi in trên máy tính.
- **Remote Desktop Users (Nhóm Truy cập Màn hình Từ xa):** Thành viên của nhóm này có thể sử dụng dịch vụ đầu cuối (***Terminal Service***) để truy cập từ xa vào máy tính.
- **Replicator (Nhóm Nhân bản):** Nhóm này được tạo để hỗ trợ chức năng nhân bản thư mục. Thành viên duy nhất của nó, thường là Tài khoản người dùng trong miền, là tài khoản thường xuyên đăng nhập vào dịch vụ nhân bản (***Replicator***) của Máy chủ Quản tri Miền. Không thêm các tài khoản của người dùng thực sự vào nhóm này.
- **Users (Nhóm Người dùng):** Thành viên của nhóm này có thể thực thi các tác vụ như chạy các ứng dụng, sử dụng các máy tính cục bộ hay trên mạng, và khóa máy chủ. Thành viên của nhóm này không thể chia sẻ thư mục hay cài đặt các máy in cục bộ. Tất cả các tài khoản người dùng cục bộ dược tạo ra trên máy tính sẽ được tự động thêm vào nhóm này. Khi máy tính gia nhập miền, Windows Server 2003 thêm các nhóm "***Domain Users***", "***Authenticate Users***", và "***Interactive***" vào nhóm cục bộ ***Users***. Và do đó, toàn bộ các tài khoản người dùng trên miền trở thành thành viên của nhóm cục bộ ***Users*** này.

Trong phần lớn các trường hợp, các đặc quyền mà các nhóm cục bộ này có được là do việc gán các quyền người dùng cho các nhóm này. Bảng 7-3 liệt kê danh sách các Quyền người dùng được gán cho các nhóm cục bộ dững sẵn (Các nhóm không liệt kê không có các quyền mặc định gán cho chúng)

Bảng 7-3 Các Quyền người dùng mặc định được gán cho nhóm cục bộ dựng sẵn.

Local Group	Default User Rights
Administrators	■ **Access This Computer From The Network (***Truy cập máy tính từ mạng***)** ■ **Adjust Memory Quotas For A Process (***Điều chỉnh hạn ngạch bộ nhớ dành cho các tiến trình* **)** ■ **Allow Log On Locally (***Cho phép đăng nhập cục bộ***)** ■ **Allow Log On Through Terminal Services** *(Cho phép đăng nhập qua dịch vụ đầu cuối)* ■ **Back Up Files And Directories** *(Sao lưu file và thư mục)* ■ **Bypass Traverse Checking** *(Không kiểm tra Cấp phép khi người dùng duyệt thư mục)* ■ **Change The System Time** *(thay đổi thời gian hệ thống)* ■ **Create A Pagefile** *(tạo bộ nhớ ảo)* ■ **Debug Programs** *(gỡ rối chương trình)* ■ **Force Shutdown From A Remote System** *(Tắt Windows từ xa)* ■ **Increase Scheduling Priority** *(tăng cấp ưu tiên của chương trình đã lập lịch)* ■ **Load And Unload Device Drivers** *(cài đặt và dỡ bỏ Trình điều khiển thiết bị)* ■ **Manage Auditing And Security Log** *(Quản lý việc kiểm định và nhật ký bảo mật)* ■ **Modify Firmware Environment Variables** *(thay đổi các biến môi trường phần sụn)* ■ **Perform Volume Maintenance Tasks** *(thực thi việc bảo trì ổ cứng)* ■ **Profile Single Process** *(lập hồ sơ các tiến trình đơn)* ■ **Profile System Performance** *(lập hồ sơ hiệu năng của hệ thống)*

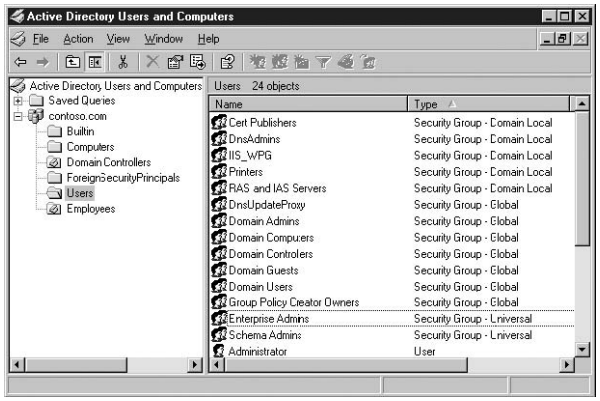
	■ **Remove Computer From Docking Station** *(dỡ bỏ máy tính khỏi trạm nối)* ■ **Restore Files And Directories** *(Phục hồi file và thư mục)* ■ **Shut Down The System** *(Tắt windows)* ■ **Take Ownership Of Files Or Other Objects** *(Chiếm quyền sở hữu của file hay các đối tượng khác)*
Backup Operators	■ **Access This Computer From The Network** ■ **Allow Log On Locally** ■ **Back Up Files And Directories** ■ **Bypass Traverse Checking** ■ **Restore Files And Directories** ■ **Shut Down The System**
Power Users	■ **Access This Computer From The Network** ■ **Allow Log On Locally** ■ **Bypass Traverse Checking** ■ **Change The System Time** ■ **Profile Single Process** ■ **Remove Computer From Docking Station** ■ **Shut Down The System**
Remote Desktop Users	■ **Allow Log On Through Terminal Services**
Users	■ **Access This Computer From The Network** ■ **Allow Log On Locally Bypass Traverse Checking** ■ **Bypass Traverse Checking**

Nhóm Xác định trước Active Directory

Tất cả các miền Active Directory đều có một tập các nhóm xác định trước (***Predefined Group***). Đây là nhóm Bảo mật, phần lớn thuộc Phạm vi ***Global***, với mục đích là nhóm các loại tài khoản người dùng miền thông dụng lại với nhau. Mặc định, Windows Server 2003 sẽ tự động thêm các thành viên vào một vài nhóm xác định trước. Bạn cũng có thể thêm các đối tượng người dùng vào các nhóm xác định trước này để họ được thừa hưởng các Quyền và Cấp phép đã được trao cho các nhóm này.

Khi bạn tạo miền Active Directory, Windows Server 2003 tạo ra các nhóm toàn cục xác định trước trong đối tượng chứa ***Users***, như trên hình 7-7. Mặc định, các nhóm xác định trước này không được thừa hưởng bất cứ một

Quyền hay Cấp phép nào. Bạn có thể gán Quyền và Cấp phép cho chúng bằng cách thêm các nhóm toàn cục xác định trước này vào nhóm miền cục bộ hay bằng cách gán trực tiếp các Quyền hay Cấp phép cho các nhóm toàn cục xác định trước này.



Hình 7-7: Thư mục Users của miền Active Directory chứa các nhóm toàn cục xác định trước.

Các nhóm toàn cục xác định trước do Windows 2000 tạo ra và các thành viên của nó bao gồm:

- **CertPublishers (Xuất bản Giấy Chứng nhận)** Thành viên của nhóm này được trao các Cấp phép để có thể tạo và trao các ***Certificate*** (*Giấy chứng nhận*) cho người dùng và Máy tính. Không giống phần lớn các nhóm xác định trước khác, nhóm này là nhóm cục bộ miền.
- **Domain Admins (Quản trị Miền)** Thành viên của nhóm này có toàn quyền quản trị trên miền. Mặc đinh, người dùng của miền "***Administrator***" là thành viên của nhóm này. Khi máy tính gia nhập miền hay nó được nâng cấp thành Máy chủ Quản tri Miền, nhóm "***Domain Admins***" sẽ trở thành thành viên của nhóm cục bộ "***Administrators***" của máy tính. Điều này cho phép các quản trị miền có toàn quyền truy cập đến tất cả các máy tính trong miền.
- **Domain Computers (Các Máy tính trong Miền)** nhóm này chứa toàn bộ các máy tính trong miền (trừ các Máy chủ Quản tri Miền). Mặc định, tất cả các đối tượng máy tính mới được tạo ra trong miền (trừ các Máy chủ Quản tri Miền mới tạo) sẽ trở thành thành viên của nhóm này.
- **Domain Controlers (Máy chủ Quản tri Miền)** nhóm này có các thành viên là các đối tượng máy tính của toàn bộ các Máy chủ Quản tri Miền ở trong miền. Mặc định, các đối tượng nói trên khi được thêm vào miền sẽ trở thành thành viên của nhóm này.

- **Domain Guests (Khách của miền)** Mặc định, đối tượng ***Domain Guest*** là thành viên của nhóm này, và Windows Server 2003 sẽ tự động thêm nhóm toàn cục "***Domain Guests***" vào nhóm cục bộ miền dựng sẵn "***Guests***".
- **Domain Users (người dùng của miền)** Nhóm này được tạo ra để đại diện cho tất cả các người dùng của miền. Windows Server 2003 tự động thêm tất cả các đối tượng người dùng của miền vào nhóm này và đồng thời cũng thêm nhóm toàn cục "***Domain Users***" vào nhóm cục bộ miền dựng sẵn "***Users***".
- **Enterprise Admins (Quản trị Doanh nghiệp)** Nhóm "***Enterprise Admins***" chỉ xuất hiện ở miền gốc của rừng (miền đầu tiên trong rừng), các thành viên của nó, có toàn quyền quản trị trên tất cả các miền trong rừng. Mặc định, nhóm "***Enterprise Admins***" là thành viên của nhóm cực bộ trên miền "***Administrators***" và đối tượng người dùng miền "***Administrator***" là thành viên của nhóm "***Enterprise Admins***".
- **Group Policy Creator Owners (nhóm Tạo ra Chính sách Nhóm)** Thành viên của nhóm này được phép thay đổi các thiết lập chĩnh sách trong miền. Mặc định, tài khoản miền "***Administrator***" là thành viên của nhóm này.
- **RAS and IAS Servers (nhóm Máy chủ RAS và IAS)** Các máy chủ là thành viên của nhóm này được phép truy cập các thuộc tính truy cập từ xa của người dùng.
- **Schema Admins (nhóm Quản trị Lược đồ)** Nhóm này chỉ xuất hiện tại miên gốc của rừng, và các thành viên của nó được phép thay đổi Lược đồ Active Directory. Mặc định, tài khoản miền "***Administrator***" là thành viên của nhóm này.

  LƯU Ý Enterprise Admins và Schema Admins *Phạm vi của các nhóm xác định trước này phụ thuộc vào Cấp chức năng của miền. với miền chạy tại Cấp chức năng Windows 2000 Mixed hay Windows Server 2003 Interim, nó là* ***Global****, với miền chạy tại Cấp chức năng Windows 2000 Native hay Windows Server 2003, nó là* ***Universal****.*

Ngoài những nhóm xác định trước đã liệt kê trên, một vài nhóm khác sẽ được tạo ra khi bạn cài đặt các cấu thành phần mềm nhất định của Windows

Server 2003, như nhóm ***DnsAdmins*** và ***DnsUpdateProxy*** (Khi bạn cài dịch vụ DNS Server), nhóm IIS_WPG (khi bạn cài IIS).

Cũng giống như đối với các nhóm dựng sẵn cục bộ, một vài nhóm xác định trước Active Directory cũng có các đặc quyền thông qua việc gán các Quyền người dùng. Trong trường hợp này, mặc dù vậy, chỉ đúng với các nhóm "***Domain Admins***" và "***Enterprise Admins***". Các Quyền người dùng được gán cho các nhóm này một cách mặc định được liệt kê trong bảng 7-4.

Bảng 7-4: Các Quyền người dùng mặc định được gán cho các nhóm xác định trước

Local Group	Default User Rights
Domain Admins and Enterprise Admins	■ Access This Computer From The Network ■ Adjust Memory Quotas For A Process ■ Back Up Files And Directories ■ Bypass Traverse Checking ■ Change The System Time ■ Create A Pagefile ■ Debug Programs ■ Enable Computer And User Accounts To Be Trusted For Delegation ■ Force Shutdown From A Remote System ■ Increase Scheduling Priority ■ Load And Unload Device Drivers ■ Allow Log On Locally ■ Manage Auditing And Security Log ■ Modify Firmware Environment Values ■ Profile Single Process ■ Profile System Performance ■ Remove Computer From Docking Station ■ Restore Files And Directories

	■ Shut Down The System ■ Take Ownership Of Files Or Other Objects

Các nhóm Active Directory dựng sẵn

Mọi miền Active Directory đều có các đối tượng chứa, trong đó hệ thống sẽ tạo ra hàng loạt các nhóm Bảo mật, mà tất cả chúng đều là các nhóm có phạm vi ***Domain Local***. Các nhóm này cung cấp cho người dùng có các Quyền người dùng và Cấp phép khả năng thực hiện các tác vụ trên Máy chủ Quản tri Miền và trong cây Active Directory. Các nhóm cục bộ miền dựng sẵn cung cấp các Quyền và Cấp phép xác định trước cho các tài khoản người dùng khi bạn thêm các đối tượng người dùng hay nhóm ***Global*** vào là thành viên của nhóm cục bộ miền dựng sẵn này.

Nhóm cục bộ miền dựng sẵn và các khả năng được gán cho các thành viên của nó như sau:

- **Accounts Operators (Nhóm Vận hành Tài khoản)** Thành viên của nhóm có thể tạo, xóa và thay đổi các đối tượng người dùng, Máy tính và Nhóm trong đối tượng chứa "***Users and Computers***" và trong toàn bộ các OU ngoại trừ đối tượng chứa "***Domain Controlers***". Họ không được cấp phép để thay đổi nhóm "***Administrators***" và nhóm "***Domain Admins***", cũng như không được thay đổi các tài khoản là thành viên của các nhóm này. Thành viên của nhóm này có thể đang nhập cục bộ vào Máy chủ Quản tri Miền và tắt Windows của chúng.
- **Administrators (Quản trị)** Thành viên của nhóm có toàn quyền truy cập đến stất cả các Máy chủ Quản tri Miền và tới toàn bộ miền. Mặc định, nhóm "***Domain Admins***", nhóm "***Enterprise Admins***" và tài khoản "***Administrator***" là thành viên của nhóm này.
- **Backup Operators (Vận hành Sao lưu)** Thành viên của nhóm có các Quyền người dùng cho phép họ tiến hành Sao lưu và phục hồi file trên toàn bộ các Máy chủ Quản tri Miền trong miền, thậm chí khi họ không có các Cấp phép nhất định đối với file. Thành viên của nhóm này cũng có thể đăng nhập cục bộ vào Máy chủ Quản tri Miền và tắt windows của chúng.
- **Guests (Khách)** Thành viên của nhóm không có các Quyền mặc định. Một cách mặc định, nhóm Global "***Domain Guest***" và đối tượng người dùng trong miền "***Guest***" là thành viên của nhóm này.

- **Incoming Forest Trust Builders (Người Xây dựng mối Quan hệ Tin cậy Trong rừng)** Thành viên của nhóm có thể tạo các mối quan hệ tin cậy một chiều trong rừng đến miền gốc của rừng.
- **Network Configuration Operators (Vận hành Cấu hình Mạng)** Thành viên có thể thay đổi các thiết lập TCP/IP, làm mới hay dỡ bỏ các địa chỉ TCP/IP trên các Máy chủ Quản tri Miền trong miền.
- **Perfomance Log Users (Người quản lý nhật ký hiệu năng)** Thành viên của nhóm được trao các đặc quyền đẻ họ có khả năng quản lý các biến đếm hiệu năng, các nhật ký, và các cảnh báo trên Máy chủ Quản tri Miền trong miền, cả ngay trên máy cục bộ hay từ xa.
- **Perfomance Monitor Users (Người Giám sát hiệu năng)** Thành viên của nhóm được tra các đặc quyền để có thể theo dõi các bộ đếm hiệu năng trên Máy chủ Quản tri Miền, ngay trên máy cục bộ hay từ xa.
- **Pre-Windows 2000 Compatible Access (Truy cập tương thích các phiên bản trước Windows 2000)** Thành viên của nhóm có thể truy cập để "đọc" các đối tượng nhóm và người dùng trong miền. nhóm này được xây dựng nhằm thỏa mãn sự tương thích ngược đối với các máy tính chạy các phiên bản Windows NT 4 hay các phiên bản trước đõ. Khi bạn chọn tùy chọn "***Permissions Compatible With Pre-Windows 2000 Server Operating Systems***" (*các Cấp phép tương thích với các hệ điều hành trước Windows 2000 Server*) trong Trình hướng dẫn cài đặt Active Directory, nhóm Đồng nhất Đặc biệt "***Everyone***" sẽ trở thành thành viên của nhóm này.
- **Print Operators (Vận hành in ấn)** Thành viên của nhóm này có thể quản lý, tạo, chia sẻ và xóa các máy in được nối tới Máy chủ Quản tri Miền trong miền và họ cũng có thể quản lý các đối tượng máy in trong Active Directory. Các thành viên này cũng có thể đăng nhập cục bộ vào Máy chủ Quản tri Miền và tắt Windows của chúng.
- **Remote Desktop Users (người dùng Màn hình Từ xa)** Thành viên của nhóm có thẻ đăng nhập vào Máy chủ Quản tri Miền trong miền thông qua Dịch vụ Đầu cuối.
- **Replicators (nhóm Nhân bản)** Nhóm này được dùng để hỗ trợ các chức năng nhân bản thư mục. Thành viên duy nhất của nó, thường là Tài khoản người dùng trong miền, là tài khoản thường xuyên đăng nhập vào dịch vụ nhân bản (Replicator) của Máy chủ Quản tri Miền. Không thêm các tài khoản của người dùng thực sự vào nhóm này.

- **Server Operators (nhóm Vận hành Máy chủ)** Trên Máy chủ Quản tri Miền, thành viên của nhóm này có thể đăng nhập, tạo và xóa các nguồn tài nguyên chia sẻ, khởi động hay dừng một vài dịch vụ, Sao lưu và phục hồi file, định dạng ổ cứng và tắt Windows của máy.
- **Terminal Server Licence Servers (nhóm các máy chủ quản lý giấy phép của máy chủ chạy dịch vụ đầu cuối)** Thành viên của nhóm này có thể truy cấp các máy chủ quản lý giấy phép của máy chủ chạy dịch vụ đầu cuối, được sử dụng để cung cấp các giấy phép (***License***) cho các máy khách chạy Dịch vụ Đầu cuối trên mạng.
- **Users (nhóm người dùng)** Thành viên của nhóm này có thể thực thi các tác vụ thông thường nhất như chạy các ứng dụng, sử dụng các máy tính cục bộ hay trên mạng, và khóa máy chủ. Mặc định, nhóm "***Domain User***s", và các nhóm Đồng nhất Đặc biệt "***Authenticated Users***" (*người dùng được xác thực*), "***Interactive***" là thành viên của nhóm này. Do vậy, bất cứ tài khoản người dùng nào được tạo ra trong miền đều là thành viên của nhóm này.
- **Windows Authorization Access Group (Nhóm Truy cập Xác thực của Windows)** Thành viên của nhóm này được phép truy cập đến thuộc tính ***TokenGroupsGlobalAndUniverrsal*** của các đối tượng người dùng miền.

  LƯU Ý Nhóm cực bộ dựng sẵn và nhóm cục bộ dựng sẵn trong miền Một vài nhóm cục bộ dựng sẵn trong miền, như nhóm "BackUp Operators", "Network Configuration Operators" và mhóm "Remote Access Users" là do nhân bản (duplicate) từ các nhóm cục bộ dựng sẵn có cùng tên trên các máy chủ độc lập và máy chủ thành viên chạy Windows Server 2003. Các nhóm này được sử dụng để thực hiện cũng các chức năng như với các nhóm cục bộ dựng sẵn nhưng trên Máy chủ Quản tri Miền không tồn tại các nhóm cục bộ dựng sẵn của chính nó.

Các Quyền người dùng mặc định được trao cho các nhóm cục bộ miền dựng sẵn được liệt kê trong bảng 7-5.

Bảng 7-5: Quyền người dùng Mặc định được gán cho các nhóm dựng sẵn Active Directory .

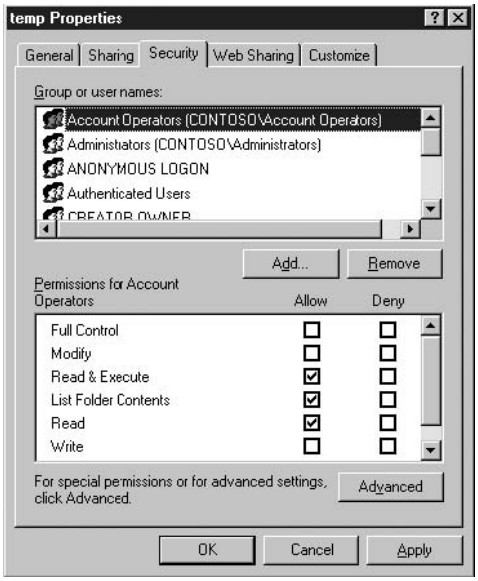
Local Group	Default User Rights

Account Operators	■ Allow Log On Locally ■ Shut Down The System
Administrators, domain local	■ Access This Computer From The Network ■ Adjust Memory Quotas For A Process ■ Back Up Files And Directories ■ Bypass Traverse Checking ■ Change The System Time ■ Create A Pagefile ■ Debug Programs ■ Enable Computer And User Accounts To Be Trusted For Delegation ■ Force Shutdown From A Remote System ■ Increase Scheduling Priority ■ Load And Unload Device Drivers ■ Allow Log On Locally ■ Manage Auditing And Security Log ■ Modify Firmware Environment Values ■ Profile Single Process ■ Profile System Performance ■ Remove Computer From Docking Station ■ Restore Files And Directories ■ Shut Down The System ■ Take Ownership Of Files Or Other Objects
Backup Operators, domain local	■ Back Up Files And Directories ■ Allow Log On Locally ■ Restore Files And Directories ■ Shut Down The System

Pre–Windows 2000 Compatible Access Local Group	■ Access This Computer From The Network ■ Bypass Traverse Checking Default User Rights
Print Operators	■ Allow Log On Locally ■ Shut Down The System
Server Operators	■ Back Up Files And Directories ■ Change The System Time ■ Force Shutdown From A Remote System ■ Allow Log On Locally ■ Restore Files And Directories ■ Shut Down The System

Các nhóm Đồng nhất Đặc biêt (Special Identities)

Các nhóm đồng nhất đặc biệt tồn tại trên tất cả các máy tính chạy ***Windows Server 2003.*** Đó không phải là các nhóm thực sự do bạn không thể tạo ra, xóa hay trực tiếp thay đổi các thành viên của nó. Các nhóm Đồng nhất Đặc biệt không xuất hiện trong Snap-in "***Local Users And Groups***" hay trong bảng điều khiển "***Active Directory Users And Groups***". Nhưng bạn có thể sử dụng chúng giống như nhóm, bằng cách thêm chúng vào ACL của hệ thống và các tài nguyên mạng, như hình 7-8 đưới đây:



Hình 7-8: Nhóm Đồng nhất Đặc biệt trong ACL

Các nhóm Đồng nhất Đặc biệt ban đầu chỉ là các khoảng trống dành cho một hay nhiều người dùng. Khi bạn thêm nhóm đồng nhất Đặc biệt vào ACL, hệ thống sẽ thêm các người dùng thỏa mãn các đặc điểm nhận dạng của nhóm tại thời điểm ACL xử lý. Các nhóm Đồng nhất Đặc biệt đại diện cho các người dùng khác nhau tại các thời điểm khác nhau, phụ thuộc vào cách thức người dùng truy cập vào máy tính hay các nguồn tài nguyên như thế nào. Ví dụ, nhóm Đồng nhất Đặc biệt "***Authenticated Users***" sẽ bao gồm toàn bộ các người dùng hiện tại đang đăng nhập, đã được Máy tính hay Máy chủ Quản tri Miền xác thực thành công. Tại bất cứ thời điểm nào được chỉ ra, danh sách người dùng xuất hiện trong nhóm Đồng nhất Đặc biệt "***Authenticated Users***" có thể thay đổi, do người dùng có thể đăng nhập hay thoát khỏi Windows.

Danh sách chính xác của các người dùng nằm trong nhóm Đồng nhất Đặc biệt "***Authenticate Users***" được xác định tại thời điểm tài nguyên được truy cập và ACL của nó được xử lý, chứ không phải tại thời điểm mà nhóm Đồng nhất Đặc biệt này được thêm vào ACL.

Các nhóm Đồng nhất Đặc biệt hiện có trong Windows Server 2003 được liệt kê sau đây:

- **Anonymous Logon (Đăng nhập khuyết danh)** Bao gồm tất cả các người dùng kết nối tới máy tính nhưng không tiến hành xác thực.
- **Authenticated Users (người dùng đã xác thực)** bao gồm tất cả các người dùng có các tài khoản cục bộ hay trên miền hợp lệ, và các yếu tố nhận dạng của họ đã được xác thực. Nhóm này không bao gồm người dùng "***Guest***" ngay cả trong trường hợp tài khoản này có mật khẩu.
- **Batch (Bó)** Gồm tất cả các người dùng hiện tại đang đăng nhập thông qua các tiện nghi dạng bó, ví dụ các tác vụ được dặt lịch (***Task Scheduler Job***).
- **Creator Owner (người sở hữu)** Gồm nhóm người dùng chính đã tạo ra hay đã chiếm quyền sở hữu (***Take Ownership***) tài nguyên.
- **DialUp (Quay số)** Gồm tất cả các người dùng hiện đang đăng nhập thông qua đường điện thoại.
- **Everyone (Mọi người)** Trên các máy tính chạy Windows Server 2003, nhóm Đồng nhất Đặc biệt ***Everyone*** bao gồm tất cả nhóm "***Authenticated Users***" cộng với tài khoản người dùng "***Guest***". Trên các máy tính chạy các phiên bản trước của Windows, ***Everyone*** bao

gồm "***Authenticated Users***", tài khoản "***Guest***" và nhóm "***Anonymous***".

- **Interactive (Tương tác)** bao gồm tất cả các người dùng hiện đang đăng nhập qua mạng.
- **Service (Dịch vụ)** Gồm tất cả các đối tượng Bảo mật hiện đang đăng nhập như là một dịch vụ.
- **Terminal Service Users (người dùng Dịch vụ Đầu cuối)** Gồm tất cả các người dùng hiện đang đăng nhập vào Máy chủ Dịch vụ Đầu cuối (***Terminal Service Server***) đang chạy Dịch vụ Đầu cuối phiên bản 4, ở chế độ ứng dụng.

TẠO VÀ QUẢN LÝ CÁC ĐỐI TƯỢNG NHÓM

Một khi bạn đã xác định bạn định sử dụng nhóm như thế nào trên mạng của bạn và đã nghiên cứu các hướng dẫn cũng như các hạn chế của rất nhiều kiểu và phạm vi nhóm khác nhau, bạn đã sẵn sàng để bắt tay thực sự vào việc tạo ra các nhóm mình cần. Rất may mắn là việc tạo ra nhóm là dễ ràng hơn nhiều so với việc bạn hiểu về chúng và các khả năng của chúng. Phần sau đây mô tả về một vài trong các tác vụ thông thường nhất của việc quản trị nhóm mà các nhà quản trị mạng và hệ thống cần thực hiện một cách thường xuyên.

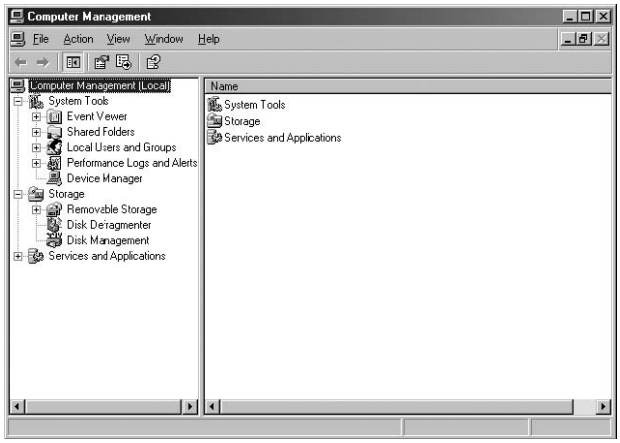
> *LƯU Ý* ***Mục đích của kỳ thi*** *Mục đích của kỳ thi 70-290 yêu cầu sinh viên có khả năng "Tạo và Quản lý nhóm"*

Tạo nhóm cục bộ

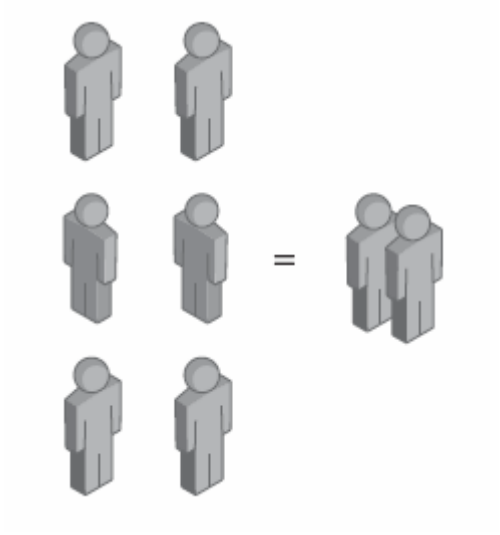
Để tạo nhóm cục bộ trong Windows Server 2003, bạn bắt buộc phải làm việc trên máy chủ độc lập hay máy chủ thành viên do Máy chủ Quản tri Miền không có nhóm cục bộ. bạn cũng nhất thiết phải đăng nhập với một tài khoản người dùng là thành viên của nhóm cục bộ "***Administrators***" hay nhóm cục bộ "***Power Users***" (hoặc nhóm "***Domain Admins***" trong miền, mà bản thân nó là thành viên của nhóm cục bộ "***Administrators***").

Để tạo ra nhóm cục bộ, bạn theo các bước sau:

1. Đăng nhập vào máy tính với tài khoản "***Administrator***" (hoặc có thể sử dụng các tài khoản khác có các đặc quyền thích hợp).
2. Nhấn chuột vào ***Start,*** trỏ đến "***Administrative Tools***" và chọn ***"Computer Management".*** Bảng điều khiển "***Computer Management***" xuất hiện.



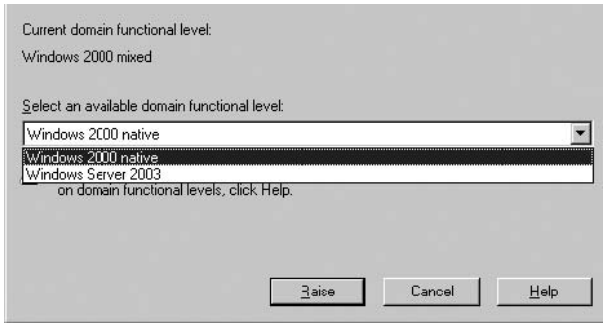
3. Mở rộng điểm "***Local Users And Groups***" trong ô phạm vi, sau đó chọn thư mục "***Groups***".



Trong Snap-in "***Local Users And Group***", người dùng và nhóm được đặt trong các thư mục riêng rẽ, không được đặt lẫn nhau trong các đối tượng chứa như trong Active Directory.

4. Từ thực đơn "***Action***" chọn "***New Group***" (*nhóm mới*). Hộp thoại "***New Group***" xuất hiện.

5. Trong hộp văn bản "***Group Name***" (*tên nhóm*), gõ tên của nhóm bạn cần tạo.
6. Nhấn "***Add***" (*thêm*). Hộp thoại "***Select Users***" (*chọn người dùng*) xuất hiện.



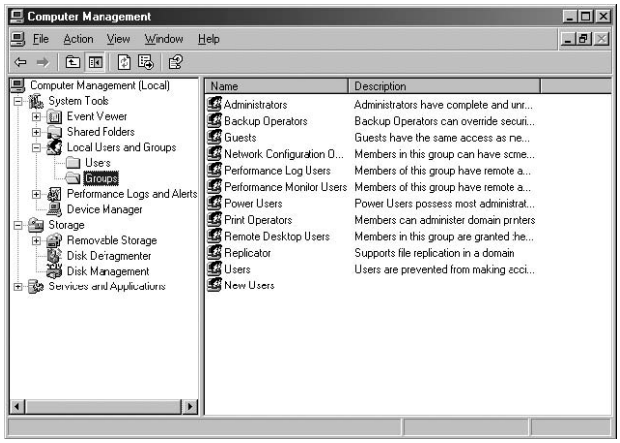
7. Gõ tên của người dùng cục bộ hay của nhóm Đồng nhất Đặc biệt trong hộp văn bản "***Enter The Object Name To Select***" (*Nhập tên của đối tượng để lựa chọn*). Sau đó nhấn ***OK***. người dùng hay nhóm Đồng nhất Đặc biệt đã được thêm vào danh sách thành viên.

   Bạn cũng có thể nhấn vào "***Advanced***" (*nâng cao*) để tìm kiếm người dùng cục bộ hay các nhóm Đồng nhất Đặc biệt.

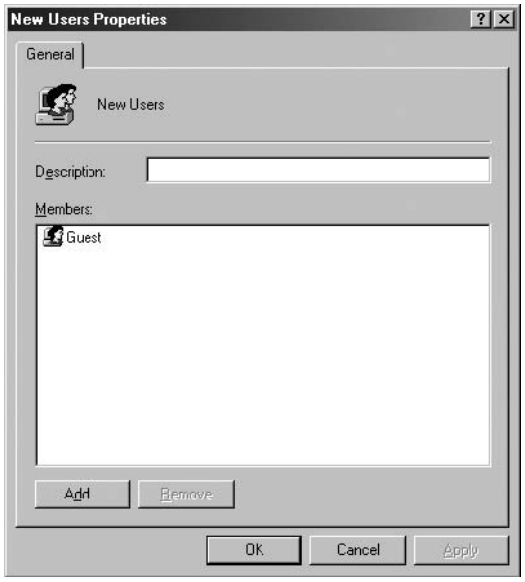
8. Nhấn "***Create***" (*tạo*).

   Snap-in sẽ tạo ra nhóm mới trong thư mục Groups, và nó làm trống hộp thoại "***New Group***" để bạn có thể tiếp tục tạo nhóm khác.

9. Nhấn "***Close***" (*đóng*).



Sau khi tạo nhóm cục bộ, bạn có thể chọn nó và từ thực đơn "***Action***", chọn "***Properties***" (*thuộc tính*) để mở hộp thoại ***Properties*** của nhóm, như chỉ ra trên hình 7-9. Tại đây, bạn có thể thêm thành viên hay loại bỏ chúng khỏi nhóm vào bất cứ lúc nào.



Hình 7-8: Hộp thoại Properties của nhóm cục bộ.

Bạn cũng có thể quản lý thành viên của nhóm cục bộ từ hộp thoại ***Properties*** của tài khoản người dùng, như chỉ ra trong hình 7-10. mỗi hộp thoại ***Properties*** của người dùng cục bộ đều chứa thẻ "***Member Of***" (*Thành viên của*) mà bạn có thể dùng để thêm các nhóm cục bộ bạn muốn người dùng đó trở thành thành viên.

Hình 7-10: Thẻ "member Of" trong hộp thoại Properties của người dùng cục bộ

Làm việc với nhóm Active Directory

Mặc dù nhóm Active Directory phức tạp hơn nhóm cục bộ rất nhiều, do có rất nhiều loại Kiểu và Phạm vi khác nhau, nhưng quá trình tạo và quản lý chúng cũng khá là đơn giản. Trong phần sau, bạn sẽ học cách tạo, quản lý các thành viên của nó và thay đổi các thuộc tính (Properties) của chúng như thế nào bbằng cách sử dụng bảng điều khiển "Active Directory Users And Computers".

> ***LƯU Ý*** ***Mục đích kỳ thi*** *Mục đích của kỳ thi 70-290 yêu cầu sinh viên có khả năng "Sử dụng bảng điều khiển '**Active Directory Users Anh Computers**' để tạo và thay đổi nhóm".*

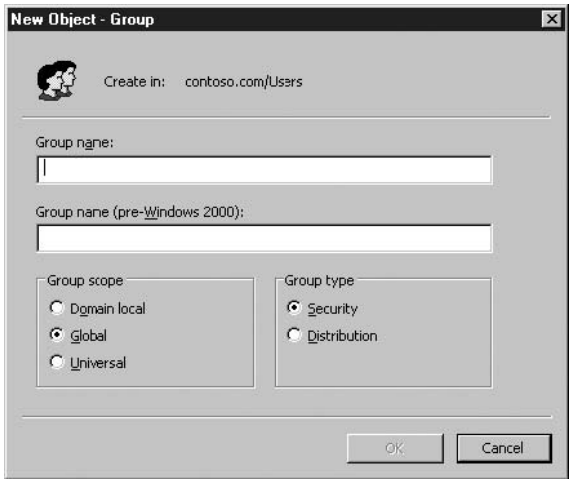
Tạo nhóm Bảo mật

Không giống như trong "***Local Users Anh Computers***", bắt buộc bạn phải tạo nhóm trong một thư mục riêng, Bảng điều khiển "***Active Directory Users And Computers***" cho phép bạn tạo các đối tượng nhóm tại bất cứ đâu bạn muốn. Bạn có thể tạo nhóm của mình tại đối tượng chứa "***Users***" với các nhóm toàn cục xác định trước, hay tạo trong đối tượng chứa "***Built-in***" với nhóm cục bộ miền dựng sẵn, trong bất cứ đối tượng OU nào do bạn tạo ra, và thậm chí trực tiếp ngay dưới đối tượng miền. Cũng như đối với việc tạo ra bất cứ đối tượng Active Directory nào, vị trí bạn chọn cho đối tượng cần dựa trên thiết kế cây thư mục của bạn.

Nếu bạn có kế hoạch sử dụng nhóm để gán Quyền người dùng cho các người dùng của bạn, bạn cần tạo các đối tượng OU thích hợp, trong đó bạn sẽ đặt các nhóm. Như các bạn đã biết trong chương 6, các đối tượng chứa "***Users***" và "***Built-in***" không phải là các OU và bạn không thể gán các Chính

sách Nhóm cho chúng. Để gán các Quyền người dùng cho nhóm trong các đối tượng chứa này, bạn phải sử dụng GPO áp dụng cho Miền (***Domain***) hay Vị trí (***Site***), và các Chính sách như vậy sẽ được tất cả các đối tượng trong Miền hay trong Vị trí (***Site***) thừa kế.

Để tạo đối tượng nhóm, bạn chọn đối tượng chứa trong ô Phạm vi của bảng điều khiển "***Active Directory Users And Computers***" và từ thực đơn "***Action***", trỏ đến "***New***" và chọn "***Group***". Hộp thoại "***New Object - Group***" sẽ xuất hiện như trong hình 7-11.



Hình 7-11: Hộp thoại "New Object - Group"

Trong hộp thoại này, bạn cần xác định các thông tin sau:

- **Group Name (tên nhóm):** Tên bạn muốn đặt cho đối tượng nhóm. Tên này có thể dài tới 64 kí tự và nhất thiết phải là duy nhất trong miền.
- **Group Name (Pre-Windows 2000) (tên tương thích với các phiên bản trước Windows 2000):** ngay khi bạn nhập tên nhóm, tên tương thích với các phiên bản trước Windows 2000 sẽ xuất hiện trong ô này.
- **Group Scope (Phạm vi nhóm):** Chọn tùy chọn nào đáp ứng được mong muốn của bạn khi chọn Phạm vi nhóm: ***Domain Local***, ***Global*** hay ***Universal***. Các Phạm vi bạn có thể chọn lựa phụ thuộc vào Cấp chức năng của miền bạn đang làm việc, như đã mô tả tại phần trên của chương này. Bảng điều khiển "***Active Directory Users Anh Computers***" không cho phép bạn chọn các loại Phạm vi không được phép trong Cấp chức năng hiện tại đang dùng.

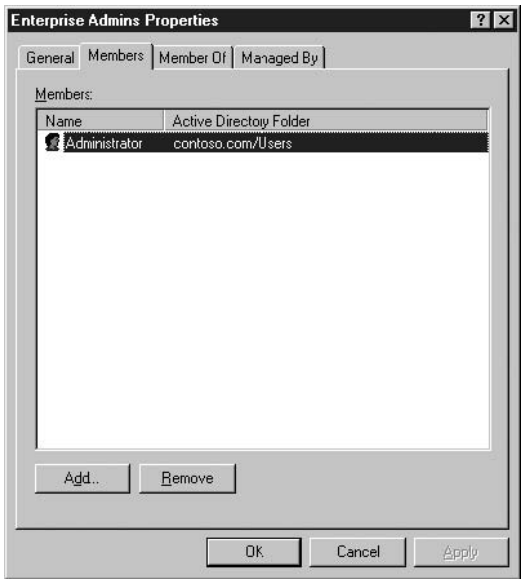
- **Group Type (Kiểu nhóm):** chọn tùy chọn nào đáp ứng được mong muốn của bạn: ***Security*** (*Bảo mật*), hay ***Distribution*** (*Phân phối*). Trong phần lớn các trường hợp, bạn sẽ tạo các nhóm Bảo mật.

Khi bạn nhấn "***OK***", bảng điều khiển sẽ tạo ra đối tượng nhóm mới trong đối tượng chứa bạn đã chọn.

Quản lý thành viên nhóm

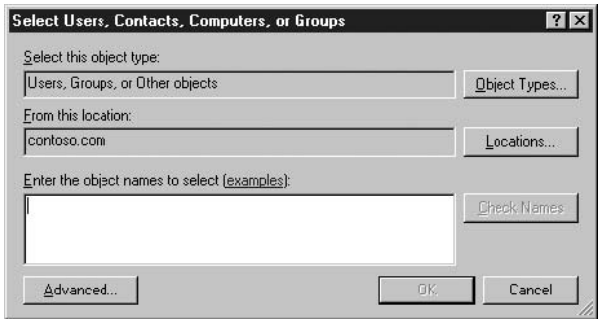
Không giống như Snap-in "***Local Users And Groups***", ở đó bạn có thể xác định các thành viên của nhóm ngay khi tao ra nhóm, trong "***Active Directory Users And Computers***", bạn phải tạo đối tượng nhóm trước, sau đó thêm các thành viên vào. Để thêm thành viên vào nhóm, bạn chọn nó trong bảng điều khiển và từ thực đơn "***Action***", chọn "***Properties***" để mở hộp thoại ***Properties*** của nhóm, như chỉ ra trong hình 7-12.

> ***LƯU Ý*** ***Mục đích của kỳ thi*** *Mục đích của kỳ thi 70-290 yêu cầu sinh viên có khả năng "Quản lý thành viên nhóm"*



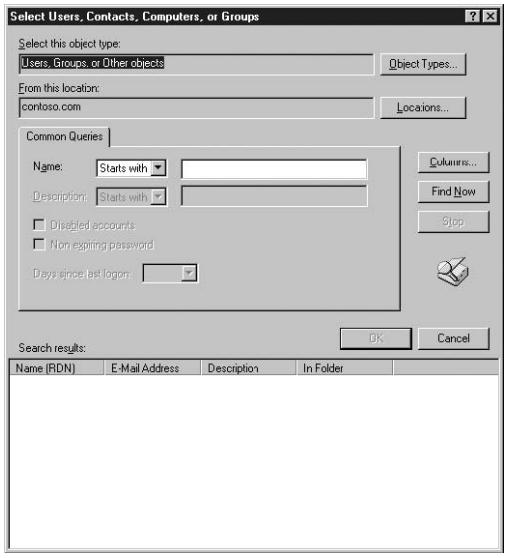
Hình 7-12: Hộp thoại Properties của đối tượng nhóm.

Hộp thoại ***Properties*** của mọi đối tượng nhóm đều có thẻ "***Member***" (*thành viên*) và thẻ "***Member Of***" (*thành viên của*), cho phép bạn thêm thành viên vào nhóm và đưa nhóm trở thành thành viên của một nhóm khác. Để thêm thành viên vào nhóm, chọn thẻ "***Member***" sau đó nhấn "***Add***", hộp thoại tiêu chuẩn "***Select Users, Contacts, Computers, Or Groups***" (*chọn người dùng, Liên lạc, Máy tính hay Nhóm*) xuất hiện, như chỉ ra trong hình 7-13.



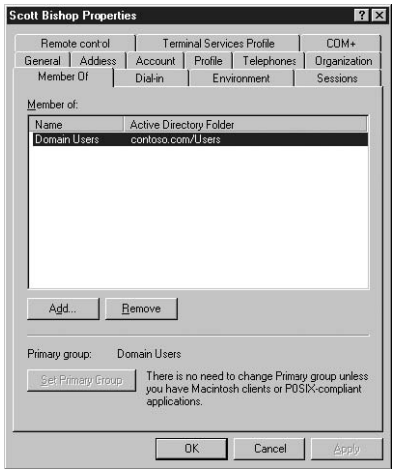
Hình 7-13: Hộp thoại "Select Users, Contacts, Computers, Or Groups"

Trong hộp thoại này, bạn có thể gõ tên của đối tượng bạn muốn thêm vào danh sách thành viên của nhóm, hoặc bạn có thể nhấn "***Advanced***" để xuất hiện hộp thoại như hình 7-14, trong đó bạn có thể tìm các đối tượng bạn muốn thêm.



Hình 7-14: Hộp thoại Advanced của "Select Users, Contacts, Computers, Or Groups"

Một khi bạn nhập hay tìm các đối tượng bạn muốn thêm, nhấn "***OK***" trong hộp thoại "***Select Users, Contacts, Computers, Or Groups***" sẽ thêm các đối tượng này vào danh sách thành viên của nó. Khi bạn đã thêm tát cả các thành viên cần thiết vào nhóm, nhấn "***OK***" để đóng hộp thoại ***Properties***. Lúc này, bạn nên mở hộp thoại ***Properties*** của đối tượng bạn vừa thêm vào nhóm và xem đối tượng nhóm trong thẻ "***Member Of***", như hình 7-15 đưới đây.



Hình 7-15: Thẻ "Member Of" của hộp thoại đối tượng người dùng.

Lập Nhóm trong nhóm

Như bạn dã biết trong phần trước của chương này, khả năng lập nhóm trong nhóm của các đối tượng nhóm phụ thuộc vào Cấp chức năng của miền bạn đang dùng và vào Kiểu và Phạm vi của nhóm bạn đang sử dụng. Xem lại bảng 7-1 nếu bạn không chắc chắn liệu Cấp chức năng của miền bạn đang dùng có hỗ trợ kiểu nhóm trong nhóm mà bạn định tạo hay không.

Bạn không thể đặt nhóm trong nhóm trong bảng điều khiển "***Active Directory Users And Computers***" bằng cách tạo nhóm mới trong một nhóm dã tồn tại. Thay vào đó, bạn phải tạo hai nhóm riêng biệt, sau đó thêm nhóm này vào là thành viên của nhóm kia. "***Active Directory Users And Computers***" sẽ không cho phép bạn thực hiện nhóm trong nhóm nếu miền của bạn không hỗ trợ việc này.

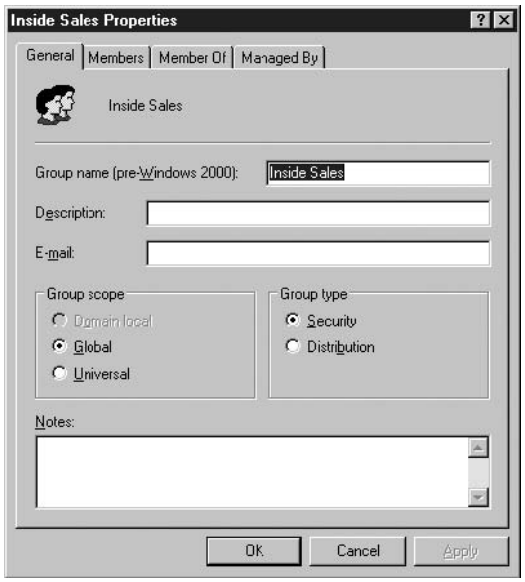
Thay đổi Kiểu và Phạm vi của nhóm.

Khi các chức năng của nhóm thay đổi, bạn có thể cần thiết phải đổi đối tượng nhóm từ Kiểu này sang Kiểu khác. Ví dụ, bạn có thể đã tạo ra nhóm Phân phối gồm 100 thành viên ở trong nhiều phòng ban khác nhau cùng làm việc với một dự án với mục đích dùng để gửi E-mail. Trong quá trình tiến triển của dự án, các thành viên có thể cần truy cấp đến CSDL chung. Bằng việc chuyển nhóm từ Phân phối sang Bảo mật và gán các Cấp phép cho nhóm, bạn có thể cung cấp khả năng truy cập CSDL chung mà không cần tạo ra nhóm mới và thêm 100 thành viên vào nhóm lại một lần nữa. Bạn chỉ có thể chuyển đổi Kiểu nhóm khi miền của bạn đang sử dụng Cấp chức năng ***Windows 2000 Native*** hay ***Windows Server 2003***.

LƯU Ý ***Mục đích kỳ thi*** *mục đích của kỳ thi 70-290 yêu cầu sinh viên có khả năng "Nhận dạng và thay đổi Phạm vi của nhóm".*

Để thay đổi Kiểu nhóm, mở hộp thoại ***Properties*** của nhóm trong bảng điều khiển "***Active Directory Users And Computers***", như hình 7-16. Trên thẻ "***General***" bạn có thể nhìn thấy "***Group Type option***" (*các lựa chọn Kiểu nhóm*), nhấn chuột vào lựa chọn chưa được chọn và nhấn "***OK***".

Quá trình thay đổi Phạm vi nhóm cũng giống hệt như vậy, ngoại trừ việc bạn chọn một trong các "***Group Scope Option***" trong thẻ "***General***". Bảng điều khiển chỉ cho phép bạn chọn các phạm vi có thể. Trong hình đưới đay, vi dụ, bạn có thể thấy lựa chọn "***Domain Local***" không có hiệu lực do bạn không thể chuyển đổi nhóm ***Global*** thành nhóm ***domain local***. Xem bảng 7-2 để biết thêm các thông tin về các phạm vi bạn được phép chuyển đổi.



Hình 7-16: Thẻ "General" trong hộp thoại Properties của đối tượng nhóm.

Xóa nhóm

Cũng như đối với đối tượng người dùng, mỗi đối tượng nhóm bạn tạo ra trong ***Active Directory*** là có một Định danh Bảo mật (***Security Identifier*** - SID) duy nhất và không sử dụng lại được. ***Windows Server 2003*** sử dụng SID để nhận dạng nhóm và các Cấp phép được gán cho nó. Khi bạn xóa nhóm, ***Windows Server 2003*** không sử dụng cùng SID lại cho nhóm đó một lần nữa, thậm chí nếu bạn tạo nhóm mới cùng tên với nhóm đã xóa. Do vậy, bạn không thể phục hồi các Cấp phép truy cập bạn đã gán cho tài nguyên

bằng cách tạo lại nhóm đã xóa. Bạn bắt buộc phải tạo lại tất cả từ đầu một nhóm mới như là một Đối tượng Bảo mật trong ACL của tài nguyên.

Khi bạn xóa nhóm, bạn chỉ xóa đối tượng nhóm và các Cấp phép cùng các Quyền chỉ ra rằng nhóm là một đối tượng bảo mật. Việc xóa nhóm sẽ không xóa các đối tượng là thành viên của chúng.

> *LƯU Ý* ***Lỗi xóa nhóm*** *Bạn không thể xóa nhóm nếu một trong các thành viên của nó có thiết lập nhóm đặt nhóm định xóa là nhóm chính (**Primary Group**). Thoát khỏi sự hạn chế của việc xóa nhóm này, nhóm chính chỉ liên quan đến các máy khách Macintosh và trong các ứng dụng POSIX. Để thay đổi nhóm chính của người dùng, mở hộp thoại Properties của đối tượng người dùng, và trong thẻ "**Member Of**", chọn một nhóm khác và nhấn "**Set Primary Group**".*

Để xóa nhóm, bạn cần chọn chúng trong bảng điều khiển "***Active Directory Users And Computers***" và từ thực đơn "***Action***", chọn "***Delete***". Một hộp thông báo ***Active Directory*** xuất hiện, nhắc bạn xác nhận lại quyết định của mình. Nhấn "***Yes***", nhóm sẽ bị xóa.

QUẢN LÝ NHÓM TỰ ĐỘNG

Mặc dù bảng điều khiển "Active Directory Users And Computers" là một công cụ thuận tiện trong việc tạo và quản lý nhóm, nó vẫn không phải là phương pháp hiệu quả nhất trong việc tạo một số lượng lớn các đối tượng bảo mật. Các công cụ dòng lệnh ***Active Directory*** do ***Windows Server 2003*** cung cấp giúp bạn có khả năng tạo và quản lý các nhóm với số lượng lớn bằng cách sử dụng các file bó hoặc các kịch bản (***script***), tương tự như diều các bạn đã làm trong chương 6 đối với người dùng. Chúng ta sẽ thảo luận về một vài công cụ như vậy trong phần dưới đây.

> *LƯU Ý* ***Mục đích của kỳ thi*** *Mục đích của kỳ thi 70-290 yêu cầu các sinh viên có khả năng "Tạo và quản lý nhóm bằng cách sử dụng các công cụ tự động".*

Tạo Đối tượng Nhóm bằng Dsadd.exe

Bạn đã sử dụng công cụ Dsadd.exe trong chương 6 để tạo người dùng mới, bạn cũng hoàn toàn có thể dùng cùng công cụ này để tạo các đối tượng nhóm.

Cú pháp cơ bản trong việc sử dụng Dsadd.exe để tạo nhóm như sau:

Dsadd GroupDN [parameters]

Trong đó, ***GroupDN*** là tên phân biệt (*Distinguished Name - DN*) của đối tượng nhóm bạn muốn tạo. Tên DN sử dụng cùng định dạng của nó trong file CSV, như chúng ta đã thảo luận trong "***Importing User Objects Using CSV Directory Exchange***" (*Nhập đối tượng người dùng sử dụng Exchange Directory CSV*) trong chương 6. Nếu tên DN có khoảng trống, bạn phải đặt chúng trong dấu ngoặc. Khi bạn sử dụng ***Dsadd.exe*** một cách tương tác từ dấu nhắc lệnh, bạn có thể cung cấp tham số ***GroupDN*** băng một trong các cách sau:

- Bằng cách gõ tên DN của các nhóm ngay trong dòng lệnh, giữa các tên DN cách nhau bằng khoảng trống.
- Bằng cách dẫn ra danh sách của DN từ một lệnh khác, như ***Dsquery.exe***
- Bằng cách để trống tham số tên DN, và bạn có thể gõ từng tên một sau dấu nhắc của chương trình, nhấn "***Enter***" sau mỗi tên DN, nhấn "***Ctrl + Z***" và "***Enter***" sau tên DN cuối cùng.

Mặc định, ***Dsadd.exe*** tạo ra nhóm bảo mật ***Global***, nhưng bạn vẫn có thể sử dụng các tham số dạng dòng lênh để tạo các nhóm với Kiểu và Phạm vi khác, chỉ định các thành viên của nó hay các nhóm chứa nó, cũng như các thuộc tính khác của nhóm. Các tham số (***parameters***) dòng lệnh thông thường nhất được trình bầy dưới đây:

- ***-secgrp [yes|no]*** Chỉ định chương trình hoặc tạo ra nhóm Bảo mật (***yes***) hay nhóm Phân phối (***no***). Giá trị mặc định là "***yes***".
- ***-scope [l|g|u]*** Chỉ định chương trình sẽ tạo ra nhóm có phạm vi ***Domain Local*** (l), ***Global*** (g), hay ***Universal*** (u). Giá trị mặc định là "g".
- ***-samid SAMname*** Chỉ định tên của SAM (***Security Accounts Manager*** – Trình Quản lý các Tài khoản Bảo mật) cho đối tượng nhóm, được sử dụng đối với các hệ thống chạy các phiên bản trước Windows 2000.
- ***-desc description*** Chỉ định các "mô tả" cho đối tượng nhóm.
- ***-memberof GroupDN*** chỉ định tên DN của một hay nhiều nhóm mà nhóm mới tạo ra sẽ là thành viên của chúng.
- ***-member GroupDN*** Chỉ định tên DN của một hay nhiều nhóm sẽ trở thành thành viên của nhóm mới tạo.

Bạn cũng có thể thêm các tham số ***-s, -u, -p*** để chỉ định Máy chủ Quản tri Miền mà lệnh ***Dsadd.exe*** sẽ chạy, và tên người dùng và mật khẩu được sử dụng để chạy lệnh.

- **{-s *Server* | -d *Domain*}**
- **-u *UserName***
- **-p {*Password* | *}**

  LƯU Ý ***Chỉ định mật khẩu khi sử dụng Dsadd.exe*** *sử dụng ký tự thay thế "*" cùng với khóa* ***–p*** *thay cho việc nhập mật khẩu sẽ làm cho chương trình nhắc bạn nhập mật khẩu trước khi thực hiện lệnh.*

Ví dụ, để tạo ra nhóm có tên "***Sales***" trong đối tượng chứa "***Users***" và đưa người dùng "***Administrator***" là thành viên của nhóm này, bạn sẽ sử dụng câu lệnh sau:

Dsadd group "CN=Sales, CN=Users, DC=ACNA, DC=com" –member "CN=Administrator, CN=Users, DC=ACNA, DC=com"

Quản lý đối tượng nhóm bằng Dsmod.exe

Dsmod.exe cho phép bạn có thể thay đổi các thuộc tính của các đối tượng nhóm đang tồn tại từ dấu nhắc lệnh của ***Windows Server 2003***. Sử dụng lệnh này, bạn có thể thực hiện các tác vụ như thêm thành viên cho nhóm, loại bỏ chúng ra khỏi nhóm, và thay đổi Kiểu và Phạm vi của nhóm. Cú pháp cơ bản của lệnh ***Dsmod.exe*** như sau:

dsmod group GroupDN [parameters]

Các tham số (***parrameters***) thông dụng nhất của lệnh này như sau:

- **-secgrp {*yes*|*no*}** đặt kiểu nhóm là Bảo mật (***yes***) hay Phân phối (***no***).
- **-scope {*l*|*g*|*u*}** Đặt phạm vi nhóm là ***Domain Local*** (*l*), ***global*** (*g*), hay ***Universal*** (*u*).
- **-addmbr *members*** Thêm thành viên vào nhóm. Thay tham số phụ ***members*** bằng tên DN của một hay nhiều đối tượng.
- **-rmmbr *members*** Loại bỏ các thành viên ra khỏi nhóm. Thay tham số phụ ***members*** bằng tên DN của một hay nhiều đối tượng.

- **-chmbr *members*** Thay toàn bộ danh sách của các thành viên nhóm. Thay tham số phụ ***members*** bằng tên DN của một hay nhiều đối tượng.

Ví dụ, để thêm người dùng "***Administrator***" vào nhóm "***Guests***", bạn sẽ dừng lệnh sau:

dsmod group "CN=Guests,CN=Builtin,DC=ACNA,DC=com" –addmbr "CN=Administrator,CN=Users,DC=ACNA,DC=com"

Tìm kiếm Đối tượng sử dụng Dsget.exe

Một khi CSDL ***Active Directory*** bắt đầu phát triển, nó có thể rất nhanh đạt tới qui mô mà khi đó, ta khó có thể dùng các bảng điều khiển, ví dụ như "***Active Directory Users And Computers***", khi cần làm việc với một đối tượng cụ thể nào đó, do vấn đề thời gian và sự phức tạp. Khi chuyện đó xẩy ra, rất nhiều quản trị mạng sẽ quay sang sử dụng các công cụ dạng dòng lệnh. Một trong các công cụ như vậy, là chương trình ***Dsget.exe,*** cho phép bạn có thể định vị và hiển thị các thông tin về bất kể một đối tượng nào trong CSDL ***Active Directory***.

Dsget.exe sử dụng cú pháp tương tự như các cú pháp đã sử dụng trong ***Dsadd.exe, Dsmod.exe***. trong đó bạn sẽ chỉ định lớp đối tượng (*Object class*), tên DN của một hay nhiều đối tượng, và các tham số chỉ ra các thông tin bạn cần hiển thị, thí dụ:

dsget objectclass ObjectDN [parameters]

Giá trị của biến ***ObjectClass*** có thể là

- ***Computer***
- ***Contact***
- ***Subnet***
- ***Group***
- ***OU***
- ***Server***
- ***User***
- ***Quote***
- ***Partition***

Mỗi lớp đối tượng trên lại có một tập hợp các tham số liên quan dến lớp đó, cho phép bạn có thể hiển thị giá trị của các thuộc tính của kiểu đối tượng đó. Với lệnh ***Dsget user,*** vài trong các tham số của nó là:

- ***–dn*** hiển thị tên DN của người dùng.
- ***–samid*** Hiển thị tên SAM của tài khoản người dùng
- ***–sid*** Hiển thị Mã số Nhận dạng Bảo mật (SID) của người dùng
- ***–upn*** Hiển thị tên chính (principal) của người dùng.
- ***–fn*** Hiển thị tên gọi (first name) của người dùng
- ***–ln*** Hiển thị tên gia đình (last name) của người dùng
- ***–display*** Hiển thị tên hiển thị (display name) của người dùng
- ***–tel*** Hiển thị số diện thoại của người dùng
- ***–email*** Hiển thị địa chỉ E-mail của người dùng
- ***–memberof*** Hiển thị các nhóm mà người dùng là thành viên trực tiếp
- ***–expand*** Hiển thị danh sách các nhóm đề qui mà người dùng là thành viên

Ví dụ, để hiển thị danh sách các nhóm mà người dùng là thành viên, ta sử dụng câu lệnh sau:

dsget user "CN=Administrator,CN=Users,DC=ACNA,DC=com" -Memberof

> ***LƯU Ý*** ***Mục đích của kỳ thi*** *Mục đích của kỳ thi 70-290 yêu cầu các sinh viên có khả năng "Tìm các nhóm trên miền mà một người dùng cụ thể nào đó là thành viên".*

TỔNG KẾT

- Nhóm là một đối tượng gồm có một danh sách các người dùng. Bạn có thể Cấp phép bảo mật cho nhóm bằng cách thêm nó vào trong danh sách ACL, giống như bất cứ một đối tượng bảo mật nào khác, ví dụ người dùng hay Máy tính. Tất cả các Cấp phép bạn gán cho nhóm sẽ được các thành viên trong nhóm thừa kế.
- Windows Server 2003 hỗ trợ các nhóm cục bộ và các nhóm ***Active Directory*** trên miền theo cùng phương thức mà nó đã hỗ trợ cho người dùng cục bộ và người dùng trên miền.
- Cấp chức năng ***Active Directory*** của miền xác định các Kiểu và Phạm vi của nhóm bạn có thể sử dụng, loại nhóm nào bạn có thể đặt trong các nhóm khác, và loại nhóm nào bạn có thể chuyển đổi.
- Trong ***Active Directory***, có hai Kiểu nhóm: Bảo mật (***Securitiy***) và Phân phối (***Distribution***), và có ba loại Phạm vi: ***Domain Local, Global, Universal.***
- Nhóm Bảo mật có thể được gán các Cấp phép, trong khi nhóm Phân phối được sử dụng để truy vấn các đối tượng chứa, như các nhóm Phân phối E-mail, và không thể Cấp phép truy cập tài nguyên cho nó.
- Nhóm cục bộ miền được sử dụng để gán các Cấp phép truy cập các tài nguyên. Nhóm ***Global*** nhằm tập hợp các người dùng có cùng một nhu cầu đối với tài nguyên. Nhóm ***Universal*** được sử dụng chính cho việc truy cập đến các tài nguyên nằm trên nhiều miền.
- Để tạo và quản lý nhóm cục bộ, bạn sử dụng Snap-in "***Local Ussers And Groups***". Để tạo và quản lý nhóm Active Directory, bạn sử dụng bảng điều khiển "***Active Directory Users And Computers***".
- Bạn có thể tạo các nhóm trên miền tại bất kể đối tượng chứa nào hay tại OU trong cây ***Active Directory***.
- Kỹ thuật "*Nhóm trong nhóm*" (***Nesting***) là bạn làm cho một nhóm này trở thành thành viên của nhóm kia.
- Bạn có thể tạo ra hay chỉnh sửa nhóm bằng các công cụ dạng dòng lệnh, ví dụ như: ***Dsadd.exe, Dsmod.exe, Dsget.exe.***

BÀI TẬP THỰC HÀNH

Bài tập thực hành 7-1: Tạo nhóm Bảo mật

Trong bài tập thực hành này, bạn sẽ tạo nhóm ***Active Directory*** trên miền của bạn.

1. Đăng nhập vào Máy chủ Quản tri Miền Windows Server 2003 với tài khoản của ***Administrator***.
2. Nhấn ***Start***, trỏ đến ***Administrative Tools***, và nhấn ***Active Directory Users And Computers***. Bảng điều khiển ***Active Directory Users And Computers*** xuất hiện.
3. Chọn đối tượng chứa ***Users*** trong ô Phạm vi (scope pane), và trên thực đơn ***Action,*** trỏ đến ***New*** và nhấn ***Group***. Hộp thoại ***New Object – Group*** xuất hiện.
4. Trong hộp văn bản ***Group Name***, gõ "***Accountants"***.
5. Trong hộp ***Group Scope***, chọn tùy chọn ***Global***, và nhấn ***OK***.
6. Thực hiện các bước tương tự như trên để tạo nhóm bảo mật có Phạm vi ***Global*** thứ hai có tên "***Development"***.

Bài tập thực hành 7-2: Thêm thành viên vào nhóm

Trong bài tập thực hành này, ta thêm các đối tượng người dùng vào làm thành viên của nhóm.

1. Đăng nhập vào Máy chủ Quản tri Miền Windows Server 2003 với tài khoản của ***Administrator***.

2. Nhấn ***Start***, trỏ đến ***Administrative Tools***, và nhấn ***Active Directory Users And Computers***. Bảng điều khiển ***Active Directory Users And Computers*** xuất hiện.

3. Chọn đối tượng chứa ***Users*** trong ô Phạm vi.

4. Trong ô Chi tiết, chọn nhóm trên miền ***Users*** và từ thực đơn ***Action***, chọn ***Properties***. Hộp thoại ***Domain Users Properties*** xuất hiện.

5. Chọn thẻ ***Members*** và nhấn ***Add***. Hộp thoại ***Select Users, Computers, Contacts, Or Groups*** xuất hiện.

6. Trong hộp ***Enter The Object Names To Select***, gõ "***Guest"***, và nhấn ***OK***. Đối tượng người dùng ***Guest*** được thêm vào danh sách thành viên của nhóm.

7. Nhấn ***OK*** để đóng hộp thoại ***Domain Users Properties***.

Bài tập thực hành 7-3: Đưa nhóm vào trong nhóm

Trong bài tập thực hành này, bạn sẽ tạo các nhóm chứa nhau bằng cách thêm một nhóm vào làm thành viên của một nhóm khác.

1. Đăng nhập vào Máy chủ Quản tri Miền Windows Server 2003 với tài khoản của ***Administrator***.
2. Nhấn ***Start***, trỏ đến ***Administrative Tools***, và nhấn ***Active Directory Users And Computers***. Bảng điều khiển ***Active Directory Users And Computers*** xuất hiện.
3. Chọn đối tuượng chứa ***Users*** trong ô Phạm vi, và trên thực đơn ***Action*** menu, trỏ đến ***New*** và nhấn ***Group***. Hộp thoại ***New Object – Group*** xuất hiện.
4. Trong hộp văn bản ***Group Name*** , gõ "***Printers"***.
5. Trong hộp ***Group Scope***, chọn tùy chọn ***Domain Local***, và nhấn ***OK***.

   Lúc này, bạn nên gán cho nhóm ***Printers*** các Cấp phép cần thiết để có thể truy cập các máy in trên mạng.
6. Tạo đối tượng nhóm bảo mật thứ hai sử dụng phạm vi Global có tên "***Sales"***.
7. Chọn đối tượng nhóm ***Printers*** bạn vừa tạo, và từ thực đơn ***Action***, chọn ***Properties***. Hộp thoại ***Printers Properties*** xuất hiện.
8. Chọn thẻ ***Members***, và nhấn ***Add***. Hộp thoại ***Select Users, Computers, Contacts, Or Groups***.
9. Trong hộp ***Enter The Object Names To Select***, gõ ***Sales***, và nhấn ***OK***. Đối tượng nhóm ***Sales*** đã được thêm vào danh sách thành viên của nhóm ***Printers***.
10. Nhấn ***OK*** để đóng hộp thoại ***Domain Users Properties***.

    Lúc này, nhóm ***Sales*** sẽ thừa hưởng toàn bộ các Cấp phép bạn đã trao cho nhóm ***Printers*** và truyền nó cho các thành viên của mình.

CÁC CÂU HỎI ÔN TẬP.

1. Loại nhóm nào trong miền là giống nhất so với nhóm cục bộ (Local Group) trên các máy chủ thành viên? Chúng giống nhau như tế nào?
2. Trong miền chạy Cấp chức năng ***Windows Server 2003***, các đối tượng bảo mật nào có thể là thành viên của nhóm ***Global***? (chọn tất cả các câu trả lời đúng).
   a. ***Users***
   b. ***Computers***
   c. ***Universal groups***
   d. ***Global groups***
3. Trong hộp thoại ***Properties*** bạn truy cập vào thẻ nào để thêm người dùng vào nhóm?
4. Bạn cần đưa nhóm ***IT Administrators*** vào trong nhóm ***Sales*** để các thành viên của nó có thể truy cập đến cùng các tài nguyên (đã được đặt các Cấp phép trong ACL) như là các thành viên của nhóm ***Sales***. Từ trang ***Properties*** của nhóm ***IT Administrator,*** bạn cần truy cập thẻ nào để thực hiện việc này?
5. Nếu môi trường của bạn có hai miền, một chạy Windows Server 2003, một chạy Windows NT 4, các phạm vi nhóm nào bạn có thể sử dụng để gán các Cấp phép đối với bất kỳ tài nguyên nào nằm trên một Máy chủ Quản tri Miền bất kỳ?
6. Các sự thay đổi phạm vi nhóm nào sau đây là được phép? (Chọn tất cả các câu trả lời đúng.)
   a. ***Global*** thành ***universal***
   b. ***Domain local*** thành ***universal***
   c. ***Universal*** thành ***global***
   d. ***Domain local*** thành ***local***
   e. ***Global*** thành ***domain local***
7. Bạn sẽ sử dụng công cụ nào để tạo nhóm cục bộ trên máy tính chạy Windows 2000 không phải là Máy chủ Quản tri Miền?
8. Bạn dự định xóa nhóm Bảo mật Global bằng bảng điều khiển ***Active Directory Users And Computers***, và bảng điều khiển không cho phép

bạn thực hiện tác vụ này. Các nguyên nhân nào sau đây đã gây nên lỗi trên? (Chọn tất cả các câu trả lời đúng.)

a. Vẫn còn thành viên trong nhóm.

b. Một trong các thành viên của nhóm có thiết lập nhóm đặt nó là nhóm chính (Primary Group.)

c. Bạn không có đầy đủ các Cấp phép cần thiết đối với đối tượng chứa mà nhóm này đang được định vị trong nó.

d. Bạn không thể xóa nhóm Global bằng cách sử dụng bảng điều khiển ***Active Directory Users And Computers***.

9. Tại sao bạn không nên sử dụng các nhóm cục bộ trên máy tính sau khi nó trở thành thành viên của miền.

CÁC KỊCH BẢN TÌNH HUỐNG

Kịch bản 7-1: Sử dụng Phạm vi nhóm

Bạn là Quản trị của miền Windows Server 2003 đang hoạt động tại Cấp chức năng Windows 2000 Mixed. Miền Windows 2003 của bạn, ***Consoto.com,*** đã được thiết lập quan hệ tin cậy với miền Windows NT 4, ***ACNA_north***, trong đó ***ACNA_north*** là miền được tin cậy. Bạn đang lập kế hoạch để sử dụng các nhóm trong miền của bạn và cần phải xác định loại phạm vi nhóm nào có thể sử dụng trên bất cứ miền nào trong rừng của bạn. Loại Phạm vi nhóm nào bạn có thể sử dụng như là các đối tượng bảo mật thỏa mãn các điều kiện trên?

a. ***Domain local***
b. ***Global***
c. ***Universal***
d. ***Domain local with a nested global group***

Kịch bản 7-2: Tạo nhóm sử dụng Dsadd.exe

Bạn là Quản trị mạng đang xây dựng ***Active Directory*** trên một mạng mới có tên ***Fabrikam, Inc.***, và bạn cần tạo đối tượng người dùng cho 75 nhân viên của phòng ***Inside Sales***. Bạn đã tạo miền ***Fabrikam.com*** và một OU có tên ***Inside Sales*** cho mục đích này. Phòng nhân sự cấp cho bạn một bản danh sách các nhân viên và yêu cầu bạn tạo tên tài khoản với chữ cái đầu của tên gọi và tên họ. Mối người dùng nhất thiết phải có giá trị ***Inside Sales*** trong thuộc tính ***Department*** và giá trị ***Fabrikam, Inc.*** trong thuộc tính ***Company***. Sử dụng tên đầu tiên trong danh sách, ***Mark Lee,*** làm ví dụ, các định dạng câu lệnh nào sau đây giúp bạn có thể tạo được 75 đối tượng người dùng có các giá trị thuộc tính đúng theo yêu cầu?

a. ***dsadd "Mark Lee" –company "Fabrikam, Inc." –dept "Inside Sales"***
b. ***dsadd user CN=Mark Lee,CN=Inside Sales,DC=fabrikam,DC=com –company Fabrikam, Inc. –dept Inside Sales***
c. ***dsadd –company "Fabrikam, Inc." –dept "Inside Sales""CN=Mark Lee,CN=Inside Sales,DC=fabrikam,DC=com"***
e. ***dsadd user "CN=Mark Lee, CN=Inside Sales, DC=fabrikam, DC=com" –company "Fabrikam, Inc." –dept "Inside Sales"***

CHƯƠNG 8: LÀM VIỆC VỚI TÀI KHOẢN MÁY TÍNH

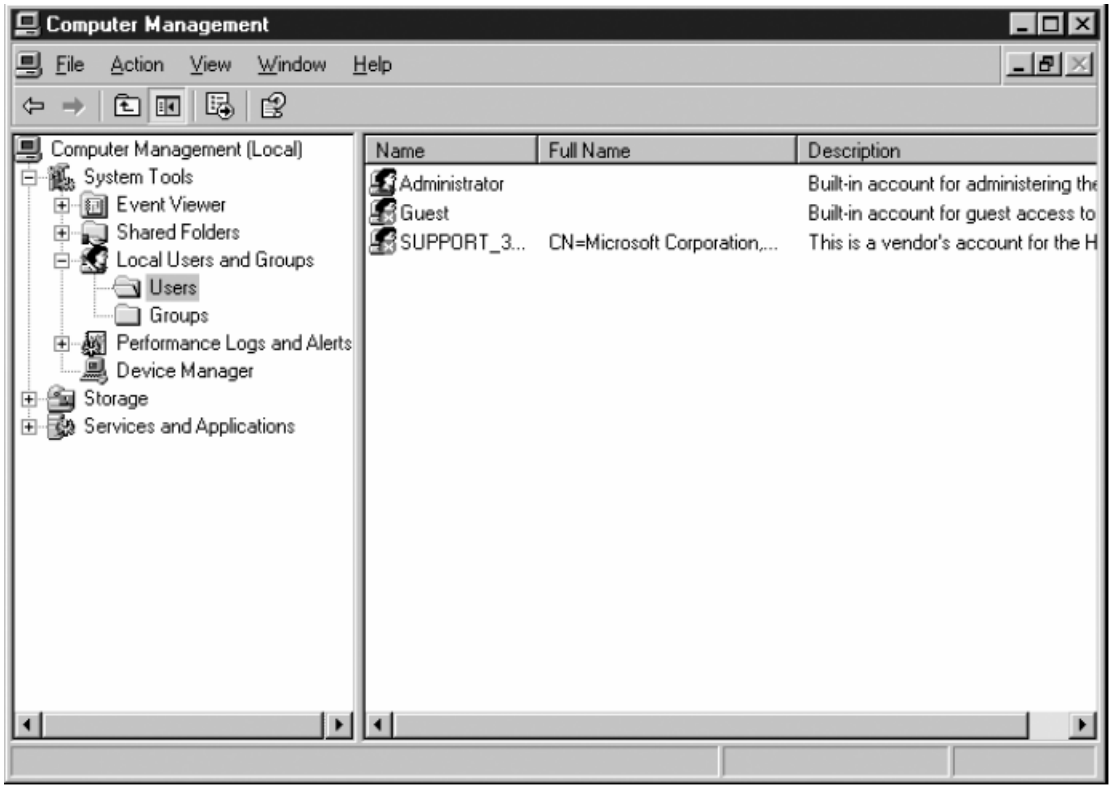
Trong hai chương trước, bạn đã tìm hiểu kỹ về các đối tượng của ***Active Directory*** như người dùng, nhóm và OU, đó là cấu trúc logic cho phép người dùng truy nhập vào các tài nguyên trên mạng. Tuy nhiên, còn có các đối tượng của ***Active Directory*** đại diện cho những tài nguyên cụ thể, vật lý và một trong những đối tượng quan trọng nhất này là **Computer Object** (*đối tượng máy tính*). Không có đối tượng máy tính người dùng vẫn có thể có các Cấp phép để truy nhập vào các tài nguyên nhưng họ lại không có cơ chế vật lý cung cấp truy nhập đó. Trong chương này bạn sẽ tìm hiểu làm thế nào để tạo và quản lý các đối tượng máy tính trên mạng ***Active Directory***.

Sau khi hoàn thành chương này, bạn có khả năng:

- **Mô tả quá trình đưa thêm máy tính vào miền *Active Directory***
- **Tạo và quản lý Đối tượng Máy tính**
- **Giải quyết sự cố của Tài khoản Máy tính**

TÌM HIỂU ĐỐI TƯỢNG MÁY TÍNH (*COMPUTER OBJECT*)

Trong cấu hình mặc định của Windows Server 2003 và tất cả các hệ điều hành khác của Windows, một máy tính thuộc về một nhóm làm việc (Workgroup). Như bạn đã tìm hiểu trong chương 6, các máy tính thuộc Nhóm làm việc xác thực người dùng bằng tài khoản được lưu trữ tại hệ thống cục bộ. Nếu người dùng muốn truy nhập vào một tài nguyên trên một máy tính thuộcNhóm làm việc thì người đó phải có một tài khoản người dùng trên máy tính đó, như đã chỉ ra trong hình 8-1. Thậm chí, bạn vẫn có thể kết nối tới máy tính thuộc Nhóm làm việc thông qua mạng, nhưng mỗi hệ thống chịu trách nhiệm bảo mật và kiểm soát truy nhập riêng của mình. Do đó, ở trên Nhóm làm việc không có bất cứ câu hỏi nào về máy tính nào mà bạn đang sử dụng bởi vì bạn phải được xác thực sử dụng tài khoản trên chính máy tính này.



Hình 8-1 Lưu trữ tài khoản người dùng trongNhóm làm việc

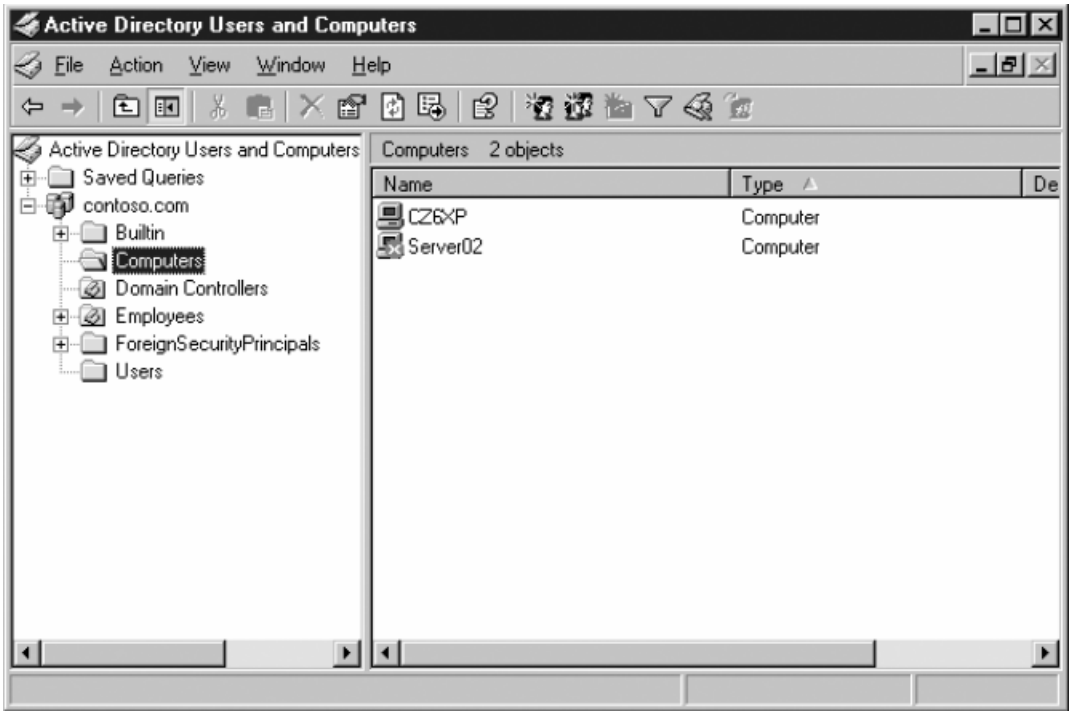
Hầu hết ở các mạng chạy Windows có nhiều hơn một vài máy tính người ta không sử dụng mô hình Nhóm làm việc (*Workgroup*) mà họ sử dụng mô hình Miền (*Domain*), được thực thi trong Windows Server 2003 nhờ Dịch

vụ Thư mục ***Active Directory***.Trong Dịch vụ ***Active Directory***, người dùng có tài khoản trong một Miền thay cho tài khoản trên những máy tính riêng rẽ. Người quản trị có thể sử dụng tài khoản miền để gán người dùng truy nhập vào tài nguyên trên các máy tính trên toàn mạng. Tài khoản người dùng miền được lưu trữ tại thư mục tập trung trên máy chủ được gọi là Máy chủ Điều khiển Miền, người dùng có thể đăng nhập vào Miền từ máy tính bất kỳ trên mạng và được xác thực bởi Máy chủ Điều khiển Miền.

Do mạng Miền Windows sử dụng thư mục tập trung, việc theo dõi các máy tính thực sự, là một phần của Miền, sẽ có một số ý nghĩa nhất định. Để làm được việc này, Active Directory sử dụng Tài khoản Máy tính, trong định dạng của Đối tượng Máy tính trong cây Active Directory (chỉ ra như trong hình 8-2). Bạn có thể có một tài khoản người dùng Active Directory và mật khẩu hợp lệ, nhưng nếu máy tính của bạn không được biểu diễn bằng một Đối tượng Máy tính thì bạn sẽ không thể đăng nhập vào Miền.

Các Đối tượng Máy tính được lưu trữ tại phân cấp Active Directory giống như việc lưu các Đối tượng Người dùng hay Đối tượng Nhóm, chúng có cùng các khả năng như sau:

- Chúng chứa các thuộc tính xác định tên của máy tính, nơi mà nó định vị và ai là người được phép quản lý nó.
- Chúng kế thừa các thiết lập Chính sách Nhóm từ các Đối tượng Chứa như là Miền, Site và OU.
- Chúng có thể là thành viên của các nhóm Bảo mật (***Security Group***) và nhóm Phân Phối (***Distribution Groups***) và kế thừa các Cấp phép của các Đối tượng Nhóm.



Hình 8-2 Lưu trữ tài khoản máy tính Miền Active Directory.

Khi một người dùng thực hiện đăng nhập vào Miền Active Directory, máy trạm thiết lập một kết nối tới một Máy chủ Điều khiển Miền để xác thực định danh của người dùng. Nhưng trước khi xảy ra việc xác thực người dùng, hai máy tính thực hiện chuẩn bị xác thực sử dụng các Đối tượng Máy tính tương ứng để đảm bảo là cả hai hệ thống đều là các phần của Miền này. Dịch vụ Truy nhập Mạng (***NetLogon service***) đang chạy trên máy trạm kết nối tới cùng dịch vụ này trên Máy chủ Điều khiển Miền và sau đó từng máy kiểm tra lại hệ thống kia đã có tài khoản máy tính hợp lệ chưa. Khi sự kiểm tra được hoàn tất, hai hệ thống thiết lập một kênh kết nối bảo mật mà sau đó chúng có thể sử dụng để bắt đầu quá trình xác thực người dùng.

Sự kiểm tra Tài khoản Máy tính giữa máy trạm và Máy chủ Điều khiển Miền là quá trình xác thực thực sự dùng tên tài khoản và mật khẩu đúng như khi xác thực người dùng Miền. Sự khác nhau là ở chỗ mật khẩu được sử dụng bởi tài khoản máy tính được sinh ra một cách tự động và được giữ dưới dạng ẩn. Người quản trị có thể khởi tạo lại (*Reset*) Tài khoản Máy tính nhưng họ không phải cung cấp mật khẩu cho chúng.

> ***LƯU Ý**: **Hệ điều hành Windows và các Đối tượng Máy tính:** Các máy tính chạy trên nền tảng hệ điều hành Windows NT như Windows Server 2003, Windows XP, Windows 2000 và Windows NT hỗ trợ Miền một cách tự nhiên và luôn được đại diện bởi các Đối tượng Máy tính trong Active Directory . Các hệ điều hành Window*

trên nền tảng MS-DOS gồm có Windows Millennium Edition (Me), Windows 98 và Windows 95 có thể tham gia vào Miền thông qua việc cài đặt Active Directory máy khách nhưng chúng sử dụng tên Miền được chỉ ra trong khi cài đặt Active Directory trên máy trạm và không có Đối tượng Máy tính cho các máy trạm nói trên trong Miền này.

BỔ SUNG THÊM MÁY TÍNH VÀO MIỀN

Người quản trị, ngoài việc tạo tài khoản người dùng và tài khoản nhóm trong Miền, cũng phải chắc chắn rằng các máy tính mạng là một phần của Miền. Việc bổ sung thêm máy tính vào Miền ***Active Directory*** bao gồm hai bước sau:

- **Tạo tài khoản máy tính** Bạn tạo tài khoản máy tính bằng cách tạo một Đối tượng Máy tính mới trong ***Active Directory*** và gán tên của nó cho một máy tính thực sự trên mạng.

Kết nối máy tính vào Miền Khi bạn kết nối máy tính vào Miền, hệ thống liên lạc với Máy chủ Điều khiển Miền, thiết lập một quan hệ tin cậy với Miền, định vị (hoặc tạo) Đối tượng Máy tính tương ứng với tên của máy tính, sửa nhận dạng bảo mật SID của nó phù hợp với Đối tượng Máy tính và chỉnh sửa quan hệ thành viên nhóm của nó.

Thực hiện các bước này như thế nào và ai thực hiện chúng, phụ thuộc vào việc các máy tính được triển khai trên mạng như thế nào. Có nhiều cách để tạo Đối tượng Máy tính mới và làm thế nào để người quản trị lựa chọn làm việc này phụ thuộc vào một số các yếu tố, gồm số lượng các đối tượng họ cần tạo, vị trí của các đối tượng này khi tạo và công cụ gì họ thích dùng.

Nói chung, bạn sẽ tạo các Đối tượng Máy tính khi bạn triển khai các máy tính mới trong Miền. Khi đó một máy tính được đại diện bởi một Đối tượng Máy tính và kết nối vào Miền, bất cứ người dùng nào trong Miền có thể đăng nhập vào từ máy tính đó. Ví dụ, bạn không phải tạo Đối tượng Máy tính mới hoặc kết nối lại các máy tính vào Miền khi có nhân viên rời khỏi công ty và nhân viên mới sử dụng các máy tính của họ. Tuy nhiên, nếu bạn cài lại hệ điều hành trên máy tính thì bạn phải tạo Đối tượng Máy tính mới cho nó (hoặc khởi tạo lại (*Reset*) Tài khoản Máy tính đã có) bởi vì máy tính này sẽ có mã nhận dạng bảo mật (SID) khác sau khi cài đặt lại.

Việc kết nối một máy tính mới vào Miền luôn được thực thi tại chính máy tính đó bởi người quản trị hoặc bởi người dùng. Tuy nhiên, việc tạo Đối tượng Máy tính có thể xảy ra trước hoặc trong khi xảy ra quá trình kết nối.

Người quản trị thường chịu trách nhiệm tạo Đối tượng Máy tính nhưng người dùng cuối cũng có thể tự tạo các đối tượng của họ với những điều kiện nhất định.

> ***LƯU Ý:*** ***Mục đích kỳ thi*** *Mục đích của kỳ thi 70-290 yêu cầu các thí sinh có khả năng "Tạo và quản lý tài khoản máy tính trong môi trường* ***Active Directory****."*

TẠO ĐỐI TƯỢNG MÁY TÍNH

Việc tạo Đối tượng Máy tính luôn luôn phải xảy ra trước khi máy tính tương ứng thực sự có thể kết nối vào Miền, mặc dù nó đôi khi không xuất hiện theo cách đó. Có hai chiến lược cơ bản cho việc tạo Đối tượng Máy tính trong ***Active Directory***:

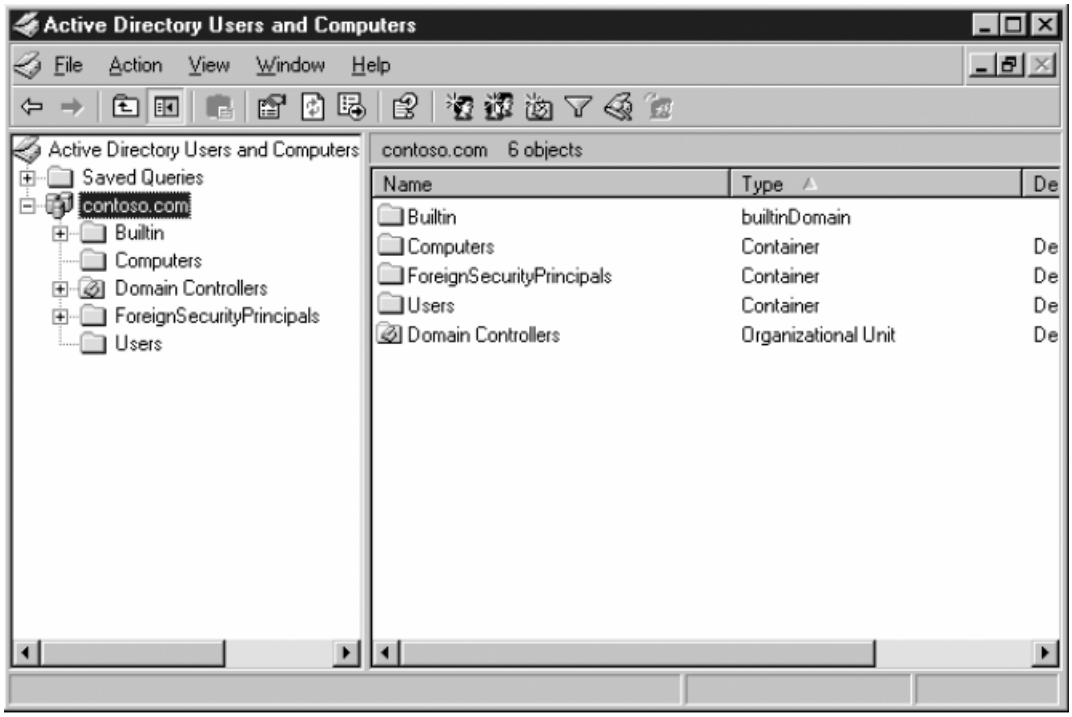
- Tạo các Đối tượng Máy tính trước sử dụng công cụ ***Active Directory***, sao cho các máy tính có thể định vị các đối tượng sẵn có khi chúng gia nhập Miền.
- Bắt đầu quá trình gia nhập Miền trước và cho phép máy tính này tự tạo các Đối tượng Máy tính của mình.

Trong mỗi trường hợp, Đối tượng Máy tính luôn xuất hiện trước khi sự kiện máy tính gia nhập miền xẩy ra. Tại chiến lược thứ hai, quá trình gia nhập xuất hiện trước nhưng máy tính sẽ tạo ra Đối tượng Máy tính trước khi thực sự bắt đầu quá trình gia nhập Miền.

Khi bạn có một số các máy tính cần triển khai, đặc biệt là ở nhiều vị trí khác nhau, hầu hết các quản trị thích tạo các Đối tượng Máy tính trước hơn. Đối với số lượng máy tính lớn thậm chí có thể thực hiện quá trình tạo các Đối tượng Máy tính tự động bằng cách sử dụng các công cụ dạng dòng lệnh và các file bó (*.BAT). Trong các phần tiếp theo ta sẽ nghiên cứu các công cụ bạn có thể sử dụng để tạo các Đối tượng Máy tính.

Tạo các Đối tượng Máy tính sử dụng Active Directory And Computers

Cũng như đối với các Đối tượng Người dùng và Đối tượng Nhóm bạn đã nghiên cứu tại các chương trước, tiện ích chính của Windows Server 2003 để tạo các Đối tượng Máy tính là bảng điều khiển ***Active Directory Users And Computers***, như được chỉ ra trong hình 8-3.



Hình 8-3 Bảng điều khiển Active Directory Users And Computers

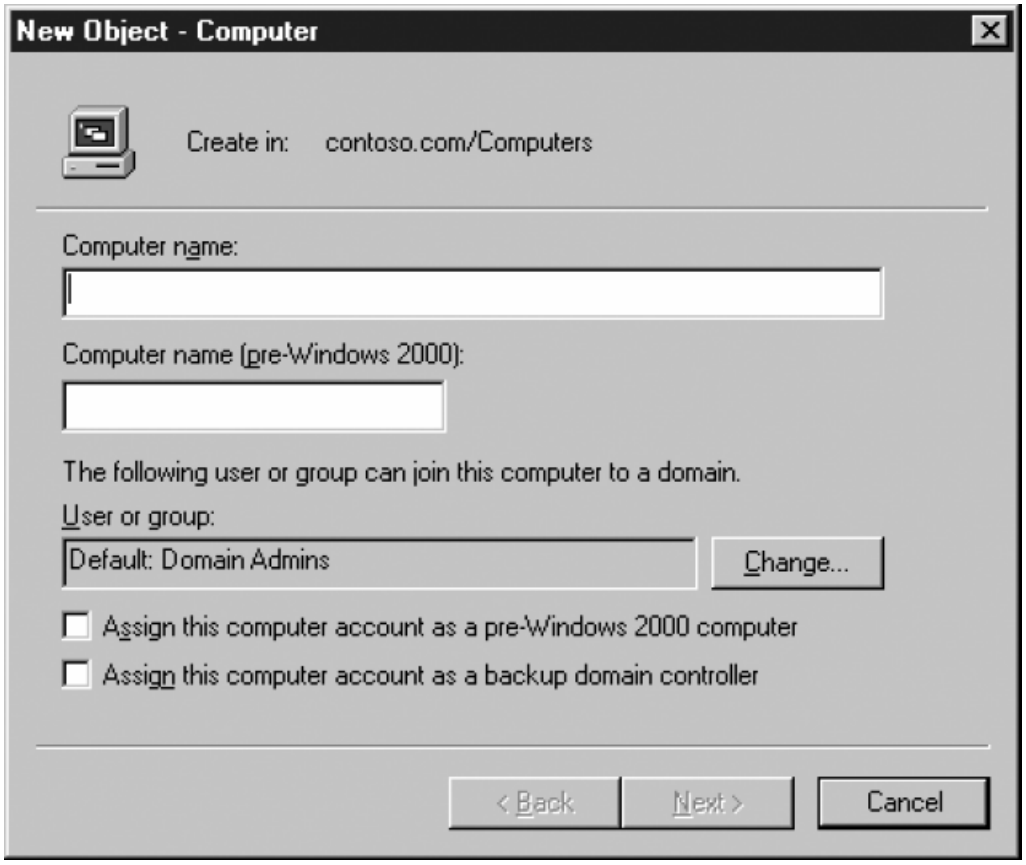
Để tạo các Đối tượng Máy tính tại Miền ***Active Directory*** bằng cách sử dụng bảng điều khiển ***Active Directory Users And Computers*** hay bất cứ tiện ích nào khác bạn phải có các Cấp phép thích hợp cho Đối tượng Chứa sẽ bố trí các đối tượng này. Mặc định, nhóm ***Administrators*** có Cấp phép tạo các đối tượng tại bất kỳ nơi nào trên Miền và nhóm ***Account Operators*** có Cấp phép đặc biệt ***Create Computer Objects*** và ***Delete Computer Objects*** để tạo và xoá Đối tượng Máy tính ra khỏi Đối tượng Chứa ***Computers***, cũng như là ra khỏi bất kỳ OU mới nào mà bạn tạo. Nhóm ***Domain Admins*** và ***Enterprise Admins*** là thành viên của nhóm ***Administrators***, bởi vậy thành viên của các nhóm này cũng có thể tạo các Đối tượng Máy tính tại bất cứ nơi nào. Người quản trị cũng có thể uỷ quyền điều khiển Đối tượng Chứa cho các người dùng hay các nhóm nhất định cho phép họ tạo các Đối tượng Máy tính tại các Đối tượng Chứa này.

> ***THÔNG TIN THÊM****: Người dùng bình thường cũng được phép tạo một số lượng giới hạn các Đối tượng Máy tính. Để biết chi tiết hơn, xem "Nhập Máy tính vào Miền" tại phần sau của chương này.*

Quá trình tạo một Đối tượng Máy tính tại ***Active Directory Users And Computers*** tương tự như quá trình tạo người dùng hoặc nhóm. Bạn chọn Đối tượng Chứa mà bạn muốn đặt đối tượng và chọn thực đơn ***Action***, trỏ tới ***New*** và chọn ***Computer***. Xuất hiện trình hướng dẫn ***New Object – Computer***, như trong hình 8-4.

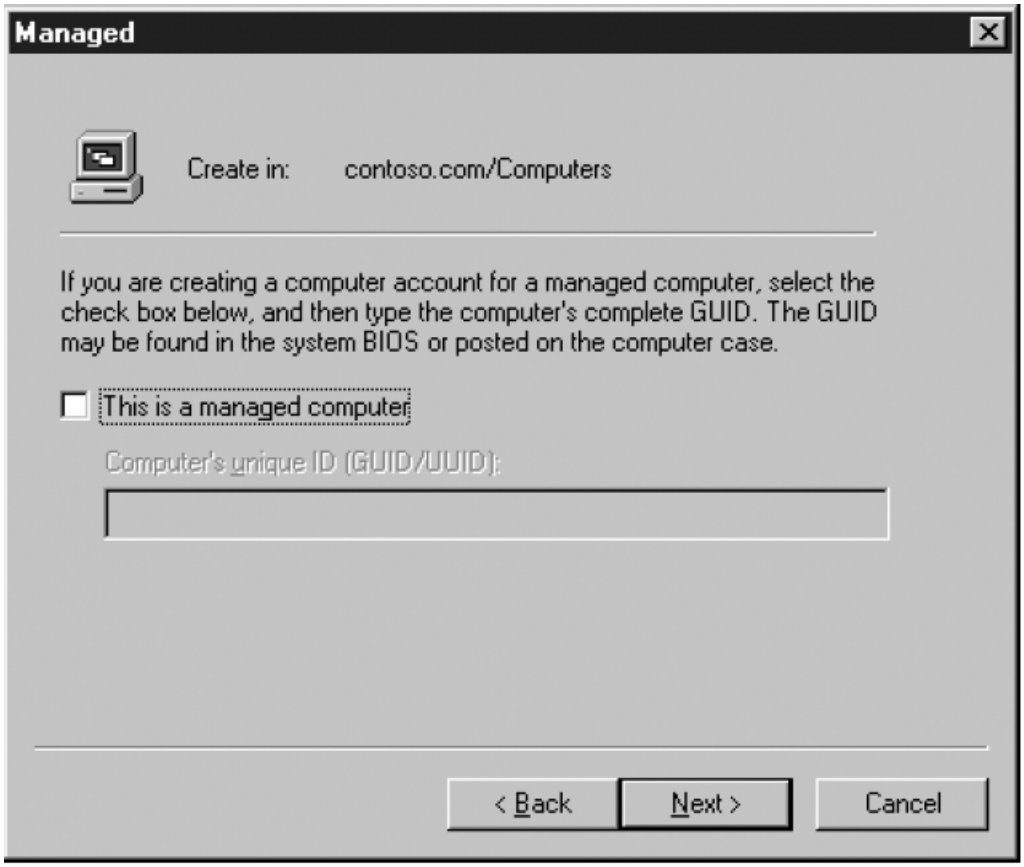
Tại trang đầu của trình hướng dẫn, bạn có thể cấu hình các thuộc tính sau của Đối tượng Máy tính :

- **Computer Name** Chỉ ra tên của máy tính có độ dài tới 63 ký tự, được gán cho Đối tượng Máy tính. Tên này phải đúng với tên của máy tính được kết nối với đối tượng này.
- **Computer Name (Pre–Windows 2000)** Khi bạn nhập vào tên máy tính, 15 ký tự đầu xuất hiện trong trường này. Đây là tên của máy tính mà các máy tính trước Windows 2000 trên mạng sẽ dùng.
- **User Or Group** Chỉ ra người dùng và nhóm được phép nhập máy tính vào Miền. Giá trị mặc định là nhóm ***Domain Admins***. Để thay đổi bấm ***Change*** để mở hộp thoại chuẩn ***Select User or Group***.
- **Assign This Computer Account As A Pre–Windows 2000 Computer** Chọn hộp chọn này nếu máy tính gia nhập vào Miền sử dụng đối tượng này chạy Windows NT 4.0.
- **Assign This Computer Account As A Backup Domain Controller** Chọn hộp chọn này nếu máy tính gia nhập vào Miền sử dụng đối tượng này có chức năng như Máy chủ Điiều khiển Miền Dự phòng chạy Windows NT 4.0 (***Backup Domain Controller - BDC***).



Hình 8-4 Trình hướng dẫn New Object – Computer

Sau khi hoàn thành trang này, bấm ***Next*** để hiện thị trang ***Managed***, chỉ ra tại hình 8-5. Trên trang này, bạn có thể chỉ ra liệu máy tính được ánh xạ tới Đối tượng Máy tính trên miền là có thể quản lý được mà bạn sẽ cài đặt sử dụng Dịch vụ Cài đặt Từ xa (***Remote Installation Services*** - RIS) hay không. Nếu bạn chọn hộp chọn này, bạn phải cung cấp Mã nhận dạng Duy nhất Toàn cục (***Globally Unique Identifier*** - GUID) hoặc Mã nhận dạng Duy nhất Tổng hợp (***Universally Unique Identifier*** - UUID) cho máy tính này.



Hình 8-5 Trang *Managed* của trình hướng dẫn *New Object – Computer*

Bấm ***Next*** hiển thị trang ***Summary*** và bấm ***Finish***, trình hướng dẫn sẽ tạo Đối tượng Máy tính trong Đối tượng Chứa đã chọn.

Tạo Đối tượng Máy tính sử dụng Dsadd.exe

Cũng như đối với người dùng và nhóm, bảng điều khiển ***Active Directory Users And Computers*** rất tiện lợi cho việc tạo và quản lý các đối tượng đơn lẻ, nhưng rất nhiều người quản trị dùng các công cụ dạng dòng lệnh của ***Active Directory*** trong Windows Server 2003 khi họ phải tạo đồng thời nhiều đối tượng. Tiện ích ***Dsadd.exe*** cho phép bạn tạo các Đối tượng Máy tính từ dòng lệnh tương tự như việc tạo Đối tượng Người dùng và Đối tượng Nhóm trong các chương trước. Bạn có thể tạo file bó (*.BAT) của lệnh ***Dsadd.exe*** để sinh ra đồng thời các đối tượng. Cú pháp cơ bản để tạo một Đối tượng Máy tính bằng ***Dsadd.exe*** như sau:

dsadd computer *ComputerDN [parameters]*

Tham số ***ComputerDN*** là Tên Phân biệt (***Distinguished Name***) của Đối tượng Máy tính mới bạn muốn tạo. DN sử dụng cùng định dạng như tại file CSV (***Comma-Separated Value***), như chúng ta đã thảo luận trong chương 6.

Nếu DN chứa dấu cách thì bạn phải để trong dấu ngoặc kép (***""***). Khi sử dụng ***Dsadd.exe*** một cách tương tác từ dấu nhắc lệnh bạn sẽ cung cấp tham số ***ComputerDN*** theo một trong các cách sau:

- Bằng cách gõ DN ngay trên dòng lệnh, phân tách nhau bởi dấu cách.
- Bằng cách dẫn nhập danh sách DN từ dòng lệnh khác, như ***Dsquery.exe***.
- Bằng cách bỏ trống tham số DN, tại dấu nhắc của chương trình bạn có thể gõ DN vào. Ấn phím ***Enter*** sau mỗi DN , ấn ***Ctrl+Z*** và ***Enter*** sau DN cuối cùng.

Bạn cũng có thể bổ sung thêm bất kỳ một tham số nào sau đây vào dòng lệnh ***Dsadd.exe***, để xác định các giá trị cho các thuộc tính của Đối tượng Máy tính:

- **-samid** ***SAMName*** Chỉ ra tên SAM (***Security Accounts Manager***) cho Đối tượng Máy tính, được các hệ thống trước Windows 2000 sử dụng.
- **-desc** ***description*** Chỉ ra diễn giải cho Đối tượng Máy tính
- **-loc** ***location*** Chỉ ra vị trí của máy tính tương ứng với Đối tượng Máy tính
- **-memberof** ***GroupDN*** Chỉ ra DN của một hoặc nhiều nhóm mà máy tính mới sẽ trở thành thành viên.

Bạn cũng có thể bổ sung thêm các tham số ***-s***, ***-u*** và ***-p*** để chỉ ra Máy chủ Điều khiển Miền mà lênh ***Dsadd.exe*** sẽ chạy trên đó, tên người dùng và mật khẩu sẽ được dùng để thực thi lệnh này, như chỉ ra dưới đây:

- **{-s** ***Server*** **| -d** ***Domain*****}**
- **-u** ***UserName***
- **-p {*****Password*** **| *}** , Khi có dấu "*****", bạn sẽ được nhắc nhập mật khẩu tại dấu nhắc lệnh.

Ví dụ, để tạo một Đối tượng Máy tính có tên là ***webserver1*** trong Đối tượng Chứa ***Computers***, bạn sẽ sử dụng lệnh sau:

dsadd computer "CN=webserver1, CN=Computers, DC=ACNA, DC=com"

Tạo Đối tượng Máy tính sử dụng Netdom.exe

Netdom.exe là công cụ dòng lệnh khác nữa mà bạn có thể dùng để tạo Đối tượng Máy tính cũng như thực hiện nhiều các công việc về tài khoản Miền

và các tác vụ bảo mật khác. Lợi ích của việc sử dụng ***Netdom.exe*** thay cho ***Dsadd.exe*** là bạn không phải chỉ ra tên của Đối tượng Máy tính bạn muốn tạo như là DN. Lệnh đơn giản sau tạo ra một Đối tượng Máy tính trong Đối tượng Chứa ***Computers*** :

netdom add webserver1

> ***LƯU Ý*** ***Netdom.exe*** *Netdom.exe đã có sẵn trong Windows Server 2000, nhưng nó không được cài cùng với hệ điều hành. Bạn có thể cài* ***Netdom.exe*** *từ* ***Windows Support Tools*** *bằng cách chạy* ***Suptools.msi*** *từ folder* ***Support\Tools*** *trong đĩa CD cài đặt Windows Server 2003.*

Cú pháp đầy đủ của ***Netdom.exe***, khi bạn sử dụng câu lệnh phụ ***add*** như sau:

netdom add ***computername*** **[/Domain:*DomainName*]**
/UserD:*User*/PasswordD:*UserPassword*] [*/OU:OUDN*]

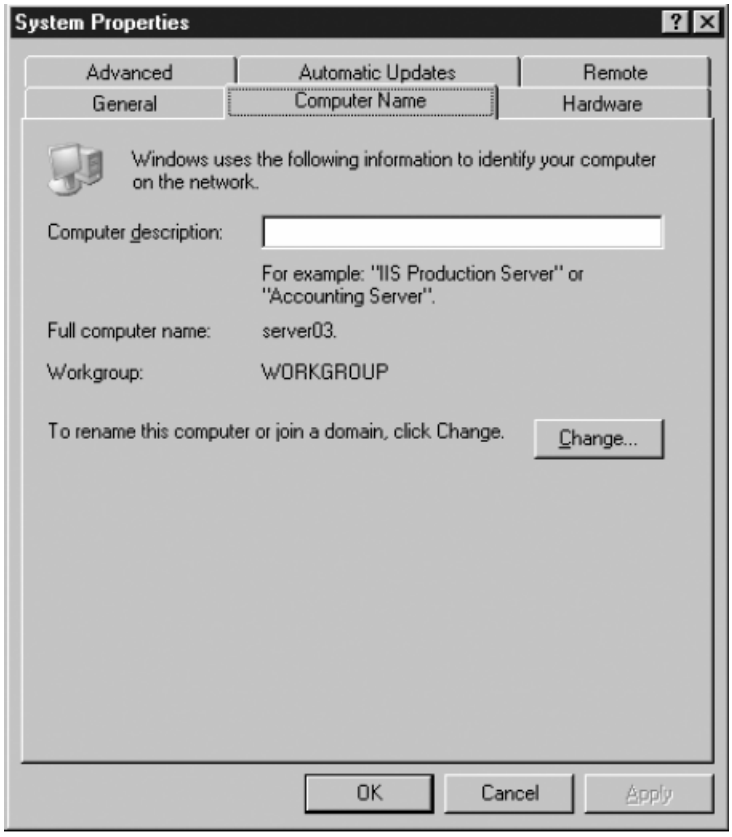
Chức năng của tham số của dòng lệng như sau:

- ***computername*** Chỉ ra Tên Phổ biến (***Common Name***) của Đối tượng Máy tính được tạo.
- **/Domain:*DomainName*** Chỉ ra tên Miền mà tại đó bạn tạo Đối tượng Máy tính. Khi bỏ qua, chương trình tạo đối tượng này trong Miền mà người dùng hiện thời đang đăng nhập.
- **/UserD:*User*** Chỉ ra tên của tài khoản người dùng mà chương trình sẽ sử dụng để tạo Đối tượng Máy tính. Khi bỏ trống, chương trình sử dụng tài khoản của người dùng hiện đang đăng nhập.
- **/PasswordD:*UserPassword*** Chỉ ra mật khẩu tương ứng với tài khoản người dùng chỉ ta bởi tham số ***/UserD***. Tham số này phải có khi dòng lệnh chứa tham số ***/UserD***. Ký tự đại diện (*) có thể được sử dụng để nhắc bạn nhập mật khẩu.
- **/OU:*OUDN*** Chỉ ra DN của OU tại nơi mà Đối tượng Máy tính sẽ được tạo. Khi bỏ trống, chương trình tạo đối tượng trong Đối tượng Chứa ***Computers***.

Nhập máy tính vào Miền

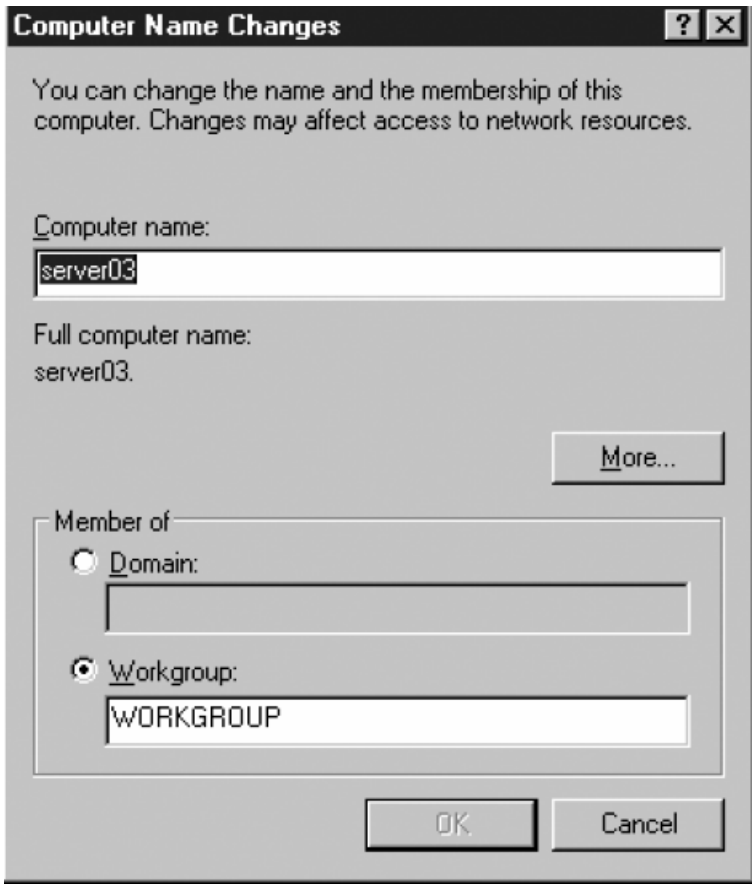
Quá trình nhập một máy tính vào Miền phải thực sự xảy ra tại chính máy tính này và được thực thi bởi thành viên của nhóm Administrators của máy tính cục bộ. Sau khi đăng nhập, bạn nhập máy tính chạy Windows Server

2003 vào Miền từ thẻ ***Computer Name*** tại hộp thoại ***System Properties*** (chạy từ biểu tượng ***System*** tại ***Control Panel***), như trong hình 8-6.



Hình 8-6 Thẻ *Computer Name* trong hộp thoại *System Properties*

Trên máy tính không gia nhập vào Miền, Thẻ ***Computer Name*** hiển thị tên gán cho máy tính trong khi cài đặt hệ điều hành và tên của Nhóm làm việc mà hệ thống hiện đang thuộc về (đó là ***WORKGROUP*** theo mặc định). Để nhập máy tính vào Miền bấm ***Change*** để hiển thị hộp thoại ***Computer Name Changes*** (chỉ ra trong hình 8-7).

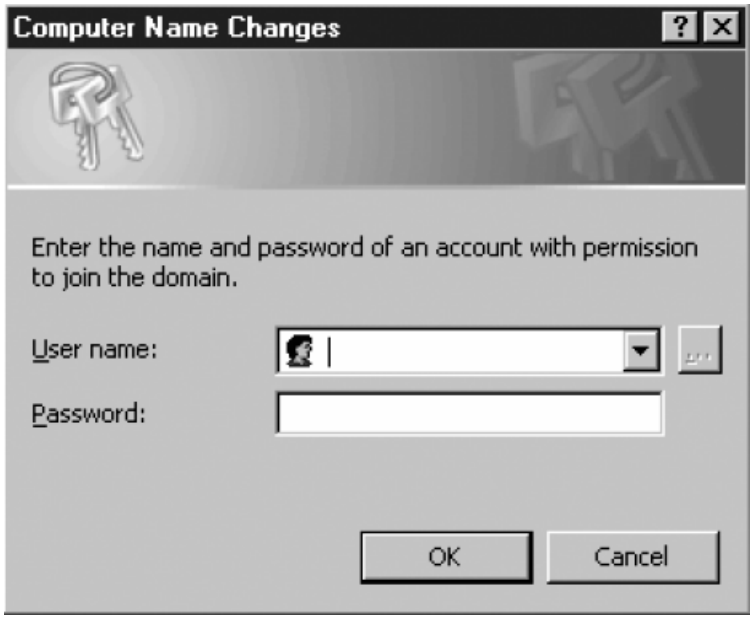


Hình 8-7 Hộp thoại *Computer Name Changes*

Tại hộp thoại này, hộp ***Computer Name*** cho phép bạn thay đổi tên đã gán cho máy tính trong khi cài đặt. Phụ thuộc vào việc bạn đã tạo Đối tượng Máy tính hay chưa, cân nhắc kỹ các khả năng đề phòng sau:

- Nếu bạn muốn nhập máy tính vào Miền đã có Đối tượng Máy tính trong ***Active Directory***, tên nhập vào tại hộp này phải phù hợp chính xác với tên của đối tượng đã tồn tại.
- Nếu bạn dự định tạo Đối tượng Máy tính trong khi thực hiện tiến trình nhập máy tính vào Miền, tên tại hộp này phải chưa tồn tại trong Miền.

Tiếp theo, chọn tuỳ chọn ***Domain*** và gõ tên của Miền mà máy tính sẽ kết nối tới và bấm ***OK***. Khi máy tính thiết lập liên hệ với Máy chủ Điều khiển Miền của Miền này, xuất hiện hộp thoại ***Computer Name Changes*** thứ hai, như chỉ ra trong hình 8-8, nhắc bạn cho vào tên tài khoản và mật khẩu của tài khoản người dùng miền có Cấp phép nhập máy tính vào Miền.



Hình 8-8 Hộp thoại xác thực *Computer Name Changes*

> ***LƯU Ý*: *Giao tiếp với Máy chủ Điều khiển Miền*** *Nếu bạn nhìn thấy thông báo cho bạn biết là máy tính không thể tìm thấy máy chủ điều khiển miền mà bạn đã chỉ ra, đây thường là lỗi cấu hình mạng. Thông thường, là địa chỉ máy chủ DNS tại cấu hình TCP/IP không đúng. Windows Server 2003 dựa vào Hệ thống Tên Miền (**Domain Name System - DNS**) để tìm máy chủ điều khiển miền và nếu máy tính không có kết nối tới máy chủ DNS giữ tên miền thì giao tiếp với máy chủ điều khiển miền không thể thực hiện được.*

Khi bạn đã được xác thực với Máy chủ Điều khiển Miền, có một thông báo với nội dung chào đón máy tính đã gia nhập vào Miền và bạn được chỉ dẫn để khởi động lại máy tính.

Nhập máy tính vào Miền sử dụng Netdom.exe

Bạn cũng có thể sử dụng tiện ích dòng lệnh ***Netdom.exe*** để kết nối máy tính tới Miền. Cú pháp của dòng lệnh như sau:

netdom join *computername* /Domain:*DomainName* [/UserD:*User* /PasswordD:*UserPassword*] [/UserO:*User* /PasswordO:*UserPassword*] [/OU:*OUDN*] [REBoot:seconds]

Chức năng của các tham số dòng lệnh như sau:

- ***computername*** Chỉ ra tên máy tính được kết nối.
- **/Domain:*DomainName*** Chỉ ra tên Miền máy tính sẽ kết nối tới.

■ **/UserD:*User*** Chỉ ra tên tài khoản người dùng miền mà chương trình sẽ sử dụng để nhập máy tính vào Miền.

■ **/PasswordD:*UserPassword*** Chỉ ra mật khẩu tương ứng với tài khoản người dùng miền chỉ ra bởi tham ***/UserD***.

■ **/UserO:*User*** Chỉ ra tên của tài khoản người dùng cục bộ mà chương trình sẽ sử dụng để truy nhập tới máy tính này.

■ **/PasswordO:*UserPassword*** Chỉ ra mật khẩu tương ứng với tài khoản người dùng cục bộ chỉ ra bởi tham số ***/UserO***.

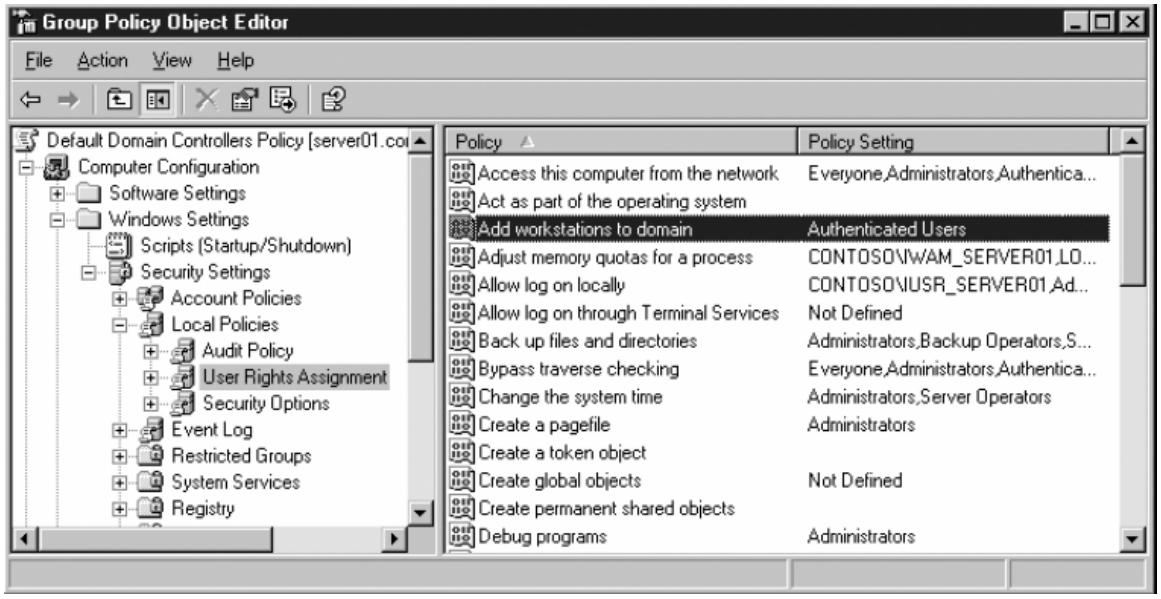
■ **/OU:*OUDN*** Chỉ ra DN của OU mà tại đó Đối tượng Máy tính sẽ được tạo ra. Nếu để trống, chương trình tạo đối tượng tại Đối tượng Chứa ***Computers***.

■ **/REBoot:*seconds*** Chỉ ra máy tính sẽ tự động tắt và khởi động lại sau khi gia nhập Miền. Bạn cũng có thể chỉ thời gian tính theo giây trước khi máy tính khởi động lại. Giá trị mặc định là 20 giây.

Tạo Đối tượng Máy tính trong khi nhập máy tính vào Miền

Bạn có thể nhập máy tính vào Miền cho dù bạn đã tạo Đối tượng Máy tính cho nó hay chưa. Khi máy tính xác thực với Máy chủ Điều khiển Miền, Máy chủ Điều khiển Miền sẽ quét CSDL ***Active Directory*** để tìm Đối tượng Máy tính cùng tên với máy tính này. Nếu không tìm thấy Đối tượng phù hợp Máy chủ Điều khiển Miền sẽ tạo Đối tượng Máy tính tại Đối tượng Chứa ***Computers*** dùng tên do máy dự định gia nhập Miền cung cấp.

Đối với Đối tượng Máy tính được tạo tự động theo cách này, nó sẽ đòi hỏi tài khoản người dùng mà bạn chỉ ra khi kết nối tới Máy chủ Điều khiển Miền phải có quyền Khởi tạo Đối tượng (***Create Object***) tại Đối tượng Chứa ***Computers***,ví dụ như là thành viên của nhóm ***Administrators***. Tuy nhiên, không phải lúc nào cũng đúng như vậy. Người dùng miền cũng có thể tự tạo Đối tượng Máy tính của họ một cách gián tiếp. Chính sách Nhóm của Máy chủ Điều khiển Miền Mặc định (***Default Domain Controllers Policy***) gán Quyền Người dùng ***Add Workstations To Domain*** cho nhóm đồng nhất đặc biệt ***Authenticated Users***, như trong hình 8-9. Điều này có nghĩa là bất cứ người dùng nào đã xác thực thành công với ***Active Directory*** sẽ được quyền nhập tới 10 máy trạm vào Miền và tạo 10 Đối tượng Máy tính tương ứng, thậm chí cả khi họ không có quyền ***Create Object***.

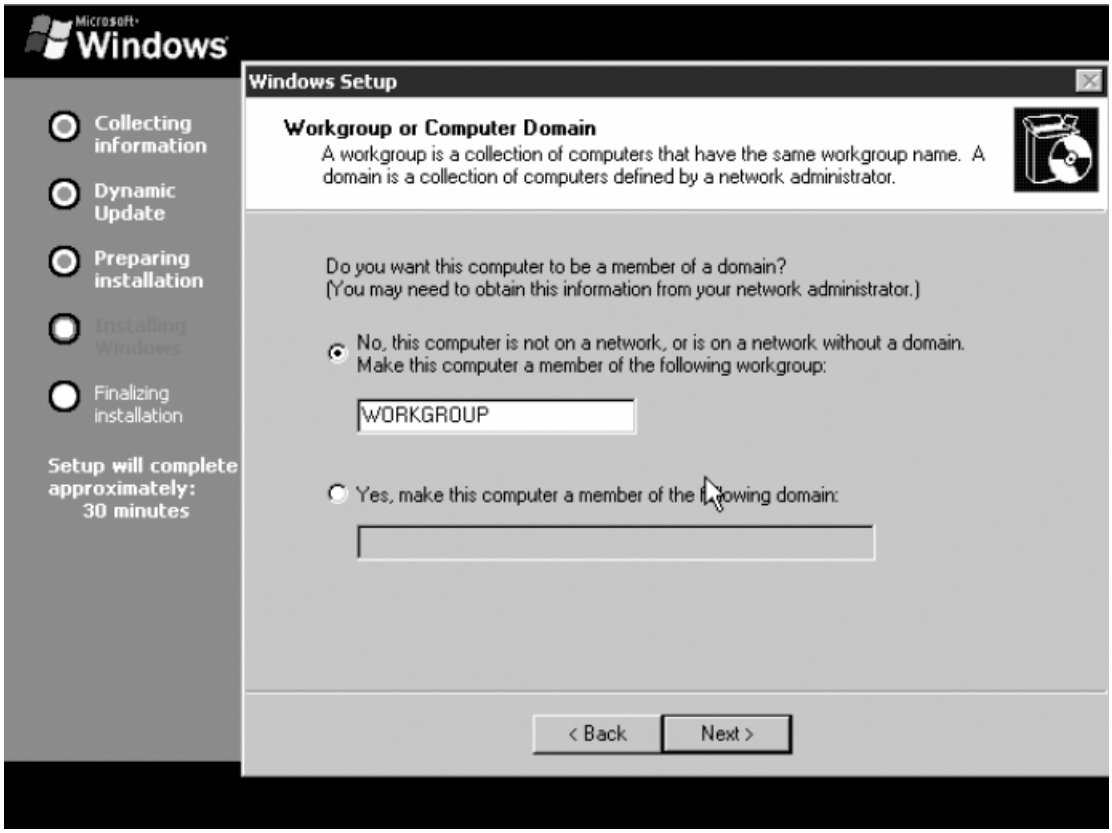


Hình 8-9 Phân quyền người dùng *Default Domain Controllers Policy*

Điều quan trong cần phải lưu ý về Quyền Người dùng ***Add Workstations To Domain***, mặc dù vậy, là ***Workstations*** là từ có ý nghĩa nhất. Người dùng đã xác thực có thể thêm tới 10 máy trạm vào Miền còn máy chủ thì không. Điều này có nghĩa máy tính phải chạy Windows XP Professional, Windows 2000 Professional hoặc một trong những bản ***Active Directory*** máy khách thấp hơn. Người dùng đã xác thực không thể nhập máy tính chạy Windows Server 2003 hoặc Windows 2000 Server vào Miền.

Nhập vào Miền trong khi cài đặt hệ điều hành

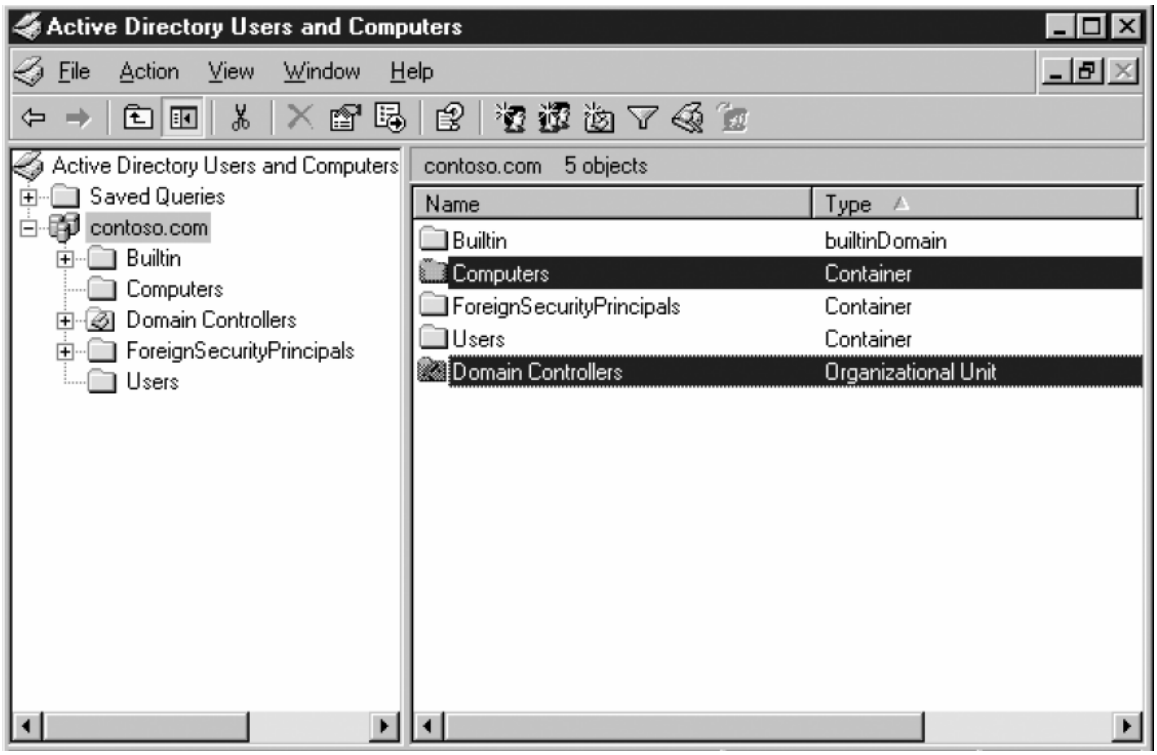
Mặc dù bạn có thể nhập một máy tính Windows Server 2003 đã tồn tại vào Miền bất kỳ lúc nào, bạn cũng có thể thực hiện nhập chúng trong khi cài đặt hệ điều hành. Khi trình hướng dẫn cài đặt Windows hiện trang ***Workgroup Or Computer Domain***, như trong hình 8-10, bạn có thể chỉ ra tên của Miền mà máy tính sẽ gia nhập. Bạn được nhắc vào tài khoản người dùng miền và mật khẩu để xác thực với Máy chủ Điều khiển Miền và quá trình gia nhập đã được diễn tả ở trên.



Hình 8-10 Trang The Workgroup Or Computer Domain của trình Hướng dẫn Cài đặt Windows

Định vị Đối tượng Máy tính

Mặc định, mỗi Miền ***Active Directory*** mới có hai Đối tượng Chứa là ***Computers*** và ***Domain Controllers***, như chỉ ra trong hình 8-11. Khi bạn tạo Miền bằng cách thăng cấp Máy chủ Điều khiển Miền đầu tiên, Trình hướng dẫn cài đặt ***Active Directory*** tạo ra hai Đối tượng Chứa này và tiếp đó là tạo Đối tượng Máy tính cho Máy chủ Điều khiển Miền mới tại Đối tượng Chứa ***Domain Controllers***.



Hình 8-11 Đối tượng Chứa *Computers* và *Domain Controllers* trong Miền Active Directory

Định vị Đối tượng Máy tính của Máy chủ Điều khiển Miền

Đối tượng Chứa ***Domain Controllers*** là một Đối tượng OU. Bạn không bao giờ phải tạo Đối tượng Máy tính cho Máy chủ Điều khiển Miền bởi vì Trình hướng dẫn cài đặt ***Active Directory*** đã tạo và đặt chúng vào OU ***Domain Controllers***. Đối tượng Chứa này phải là một OU bởi vì có GPO áp dụng cho nó được gọi là ***Default Domain Controllers Policy GPO***. GPO này chứa các thiết lập của chính sách chủ yếu cho việc bảo mật của Máy chủ Điều khiển Miền. Trong hầu hết các bản cài đặt ***Active Directory*** thì Đối tượng Máy tính của Máy chủ Điều khiển Miền vẫn ở đúng chỗ cũ của nó. Nếu bạn muốn di chuyển chúng, bạn phải đảm bảo áp dụng chính sách ***Default Domain Controllers Policy GPO*** cho OU mới có chứa Máy chủ Điều khiển Miền hoặc tạo một GPO tương đương có chứa các thiết lập dành riêng cho vai trò Máy chủ Điều khiển Miền.

Định vị các Đối tượng Máy tính khác

Đối tượng Chứa ***Computers*** là vị trí mặc định cho tất cả các Đối tượng Máy tính khác mà đã được tạo bằng phương pháp tự động, như là khi một máy tính gia nhập Miền và chưa tồn tại Đối tượng Máy tính tương ứng với nó. Sử dụng bảng điều khiển ***Active Directory Users And Computers***, bạn có thể

tạo Đối tượng Máy tính tại một Đối tượng Chứa bất kỳ, quản lý và di chuyển chúng.

Có thể, bạn sẽ thấy rất lạ, là Đối tượng Chứa ***Computers*** không phải là một OU, nó là một trong các đối tượng đặc biệt, là loại Đối tượng mà lớp đối tượng này theo nghĩa đen thì đúng là một Đối tượng Chứa, cũng như các Đối tượng Chứa ***Users***, ***Builtin*** và ***Foreign- SecurityPrincipals***. Như bạn đã tìm hiểu tại chương 6, bạn không thể tạo hoặc xoá những Đối tượng Chứa này và bạn không thể áp dụng GPO cho chúng. Do vậy bạn không thể triển khai các thiết lập chính sách nhóm cho các Đối tượng Máy tính cất giữ ở đó một cách đơn giản. Vì lý do này, nên tạo ít nhất một OU và di chuyển các Đối tượng Máy tính từ Đối tượng Chứa ***Computers*** tới đó.

Nhiều mạng ***Active Directory*** tạo đồng thời các OU cho các Đối tượng Máy tính theo tổ chức hoặc theo phân cấp địa lý trong cây ***Active Directory*** hoặc tạo các Đối tượng Chứa riêng rẽ theo các vai trò khác nhau mà các máy tính thực hiện. Ví dụ, bạn nên tạo một OU cho máy trạm của bạn và một loạt các OU cho các Máy chủ Thành viên (***Member Server***). Điều này cho phép bạn triển khai một GPO chứa các thiết lập chính sách cho từng OU, từ đó tạo một cấu hình hệ thống khác theo mỗi vai trò của từng máy tính.

Chuyển hướng Đối tượng Máy tính

Mặc dù bạn có thể tạo các Đối tượng Máy tính trong Đối tượng Chứa ***Computers*** và di chuyển chúng tới bất kỳ vị trí nào mà bạn muốn và bạn cũng có thể cấu hình Windows Server 2003 tự động đặt các Đối tượng Máy tính nó tạo ra vào một Đối tượng Chứa khác. Cách này thường được sử dụng hơn vì nó cho phép bạn đặt Đối tượng Máy tính mới vào OU thích hợp trước khi máy tính thực sự gia nhập Miền. Việc này đảm bảo là máy tính được kiểm soát bởi các chính sách áp dụng cho OU ngay sau khi máy tính gia nhập Miền.

Để chuyển hướng Đối tượng Máy tính mới, Miền của bạn phải sử dụng ***Domain functional level*** (Cấp chức năng Miền) Windows Server 2003 . Mở cửa sổ dấu nhắc lệnh và từ dòng lệnh chạy tiện ích ***Redircmp.exe***, được cung cấp cùng với Windows Server 2003, chỉ ra DN của OU hoặc Đối tượng Chứa khác bạn muốn đặt đối tượng mới vào, như ví dụ sau:

redircmp ou=workstations,DC=ACNA,dc=com

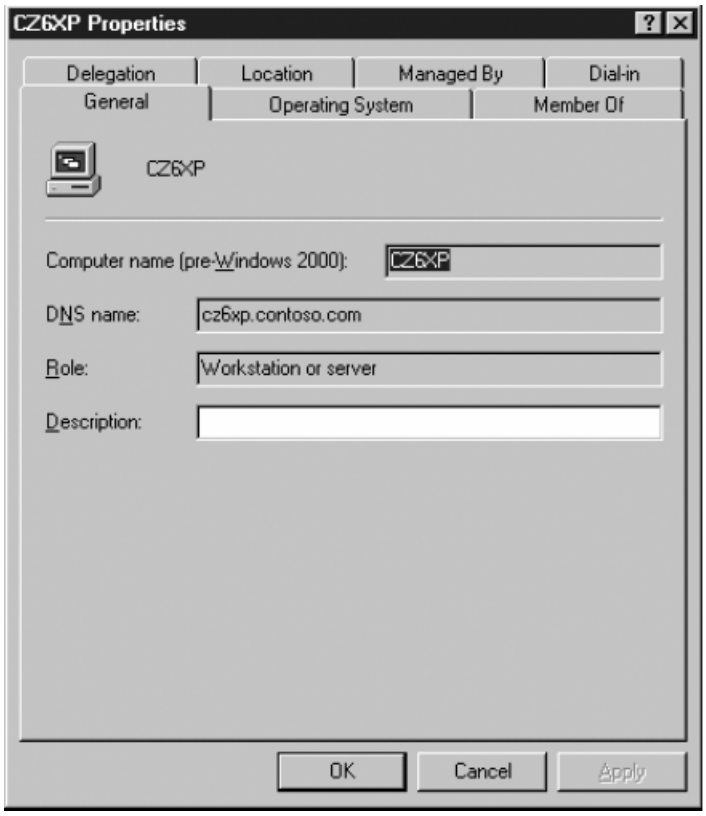
> ***THÔNG TIN THÊM****: Để biết chi tiết hơn về Cấp chức năng Miền (domain functional level) và làm thế nào chúng ảnh hưởng đến việc tạo và quản lý các Đối tượng của Active Directory, xem "Tìm hiểu về các Cấp Chức năng Miền" tại chương 7.*

QUẢN LÝ CÁC ĐỐI TƯỢNG MÁY TÍNH

Khi bạn tạo các Đối tượng Máy tính và nhập chúng vào Miền, bạn có thể quản lý các đối tượng và các máy tính từ bảng điều khiển ***Active Directory Users and Computers***. Một số các chức năng quản lý bạn có thể thực thi được mô tả ở phần sau.

CHỈNH SỬA CÁC THUỘC TÍNH CỦA ĐỐI TƯỢNG MÁY TÍNH

Giống như là tất cả các đối tượng trong ***Active Directory***, Đối tượng Máy tính cũng bao gồm các thuộc tính chứa rất nhiều các thông tin về hệ thống mà đối tượng đại diện cho nó. Để chỉnh sửa các thuộc tính của Đối tượng Máy tính, bạn chọn nó tại bảng điều khiển ***Active Directory Users and Computers*** và từ thực đơn ***Action,*** chọn ***Properties*** để hiển thị hộp thoại ***Properties*** của đối tượng, như chỉ ra trong hình 8-12.



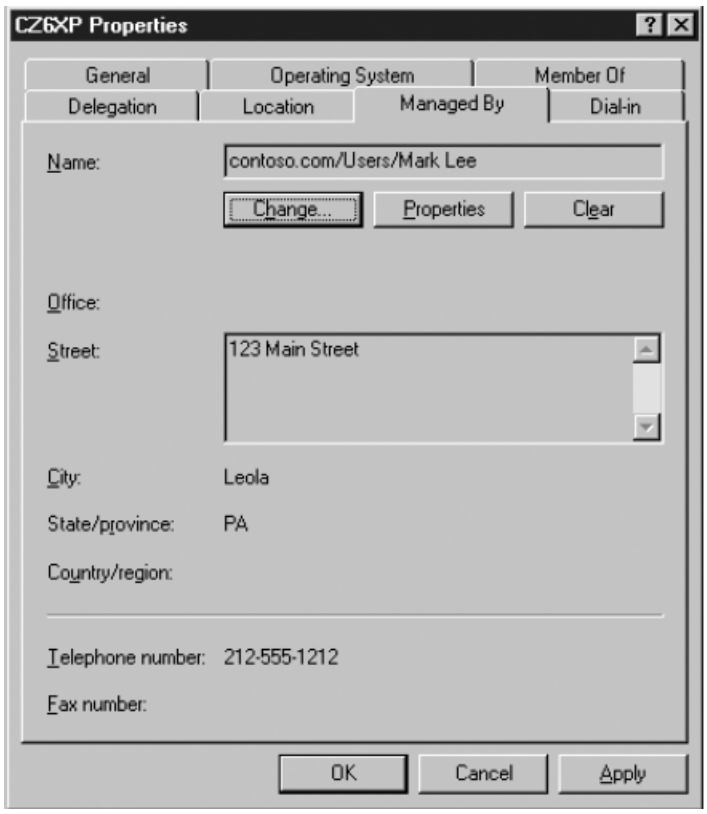
Hình 8-12 A Hộp thoại *Properties* của Đối tượng Máy tính

Hộp thoại có 7 thẻ:

- **General** Tại đây, bạn có thể gõ vào diễn giải cho máy tính đại diện bởi đối tượng này. Các hộp khác (***Computer Name [Pre–Windows***

2000], DNS Name, và ***Role***) chứa các thông tin có thể được cung cấp tự động khi máy tính gia nhập Miền.

- **Operating System** Gồm có tên, phiên bản và mức của gói dịch vụ (***service pack level***) của hệ điều hành chạy đang chạy trên máy tính được đại diện bởi đối tượng này. Thông tin này được cấp tự động khi máy tính nhập vào Miền. Không có thược tính nào do người dùng định nghĩa tại thẻ này.
- **Member Of** Cho phép bạn chỉ ra nhóm mà Đối tượng Máy tính này là thành viên. Mặc định, tất cả các Đối tượng Máy tính mới không phải là Máy chủ Điều khiển Miền được đưa vào nhóm toàn cục ***Domain Computers***.
- **Delegation** Cho phép bạn gán các dịch vụ chạy dưới Cấp phép của tài khoản máy tính để gửi các yêu cầu dịch vụ tới máy tính khác trên mạng với tư cách một người dùng. Bạn có thể cho phép đối tượng này yêu cầu dịch vụ bất kỳ hoặc tạo danh sách các dịch vụ đặc biệt nó có thể yêu cầu, sử dụng tài khoản uỷ quyền khác.
- **Location** Có chứa hộp mà bạn có thể sử dụng để xác định ví trí của máy tính tương ứng với đối tượng này.
- **Managed By** Cho phép bạn chỉ ra đối tượng người dùng chịu trách nhiệm quản lý của máy tính đại diện bởi đối tượng này. Khi bạn làm như vậy, các thuộc tính thích hợp từ của đối tượng người dùng đã chọn sẽ hiển thị trong thẻ này, như trong hình 8-13. Các thông tin này được lấy một cách động từ đối tượng người dùng; chỉ có tên của người dùng là được lưu trữ như là một phần của Đối tượng Máy tính.
- **Dial-In** Cho phép bạn chỉ ra giá trị cho các thuộc tính kiểm soát truy nhập quay số từ xa tới máy tính đại diện bởi Đối tượng này, như là sẽ được phép truy nhập hay bị từ chối và sẽ sử dụng hay không các tính năng như là định danh người gọi (***caller ID***) và gọi lại (***callback***).



Hình 8-13 Thẻ *Managed By* trong hộp thoại *Properties* của Đối tượng Máy tính

XOÁ , VÔ HIỆU HOÁ VÀ KHỞI TẠO LẠI ĐỐI TƯỢNG MÁY TÍNH

Dưới các điều kiện bình thường, các Đối tượng Máy tính không đòi hỏi người quản trị bảo trì và chăm sóc. Tuy nhiên, trong một số hoàn cảnh người quản trị nên thao tác với các Đối tượng Máy tính, như là tránh cho chúng bị sử dụng sai hoặc tiến hành các thay đổi cho phù hợp với máy tính vật lý.

Xóa Đối tượng Máy tính

Xoá một Đối tượng Máy tính trong bảng điều khiển ***Active Directory Users and Computers*** rất đơn giản, bạn chọn đối tượng này và từ thực đơn ***Action*** chọn ***Delete***. Sau khi bạn xác nhận lại thao tác này thì đối tượng bị xoá vĩnh viễn. Tuy nhiên, trước khi bạn bắt đầu xoá Đối tượng Máy tính cần bảo đảm là bạn đã hiểu rất rõ hành động này của bạn.

Cũng như với các Đối tượng Người dùng và Nhóm, SID của Đối tượng Máy tính mà có giá trị duy nhất cũng bị mất khi đối tượng bị xoá.Việc tạo một đối tượng mới có cùng tên và cùng giá trị thuộc tính sẽ không tạo lại cùng SID như cũ và bất cứ quyền và nhóm nào gán cho nó ban đầu khi đối tượng bị

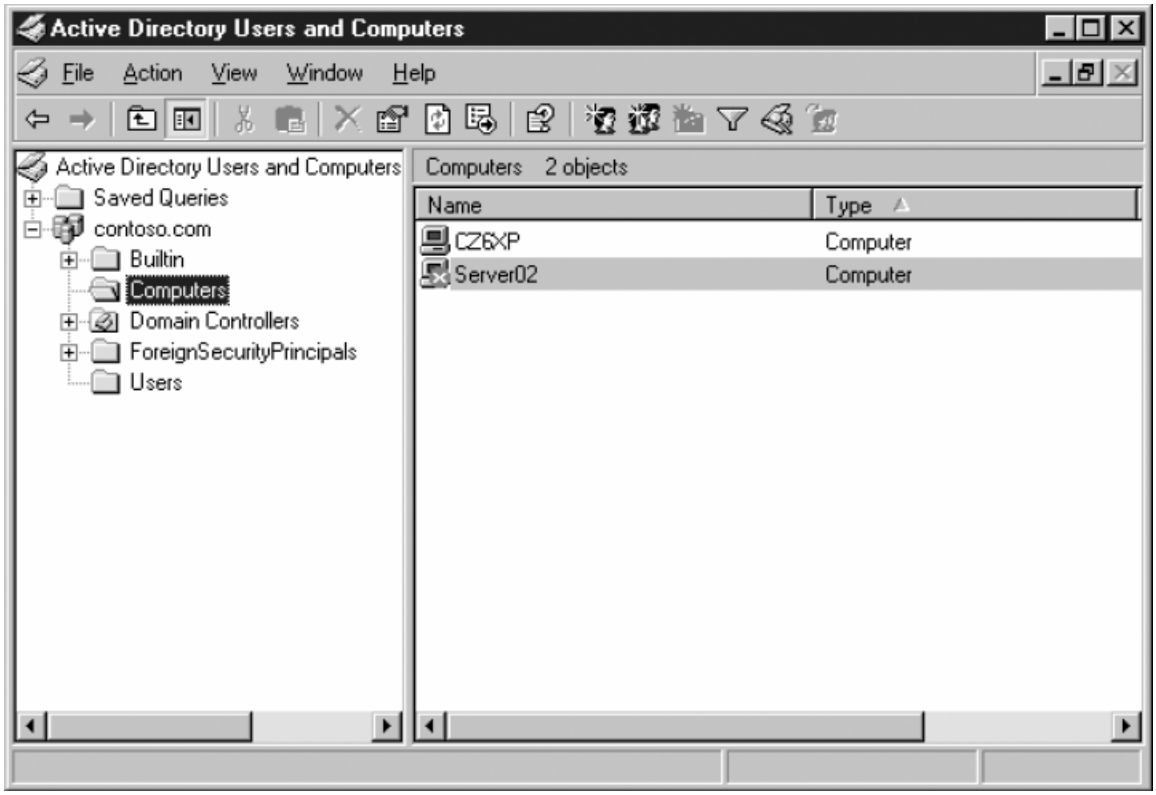
xoá cũng đều bị mất không thể cứu lại được. Bởi thế bạn không nên xoá các Đối tượng Máy tính (hoặc bất kỳ đối tượng nào, chính vì lý do này) trừ khi bạn hoàn toàn chắc chắn là bạn kkông cần lại đến chúng. Bạn có thể tránh cho đối tượng bị sử dụng thay bằng cách khác là vô hiệu hoá nó.

> ***LỜI KHUYÊN Tách rời máy tính ra khỏi Miền*** *Khi một máy tính bị di chuyển ra khỏi Miền bằng cách nhập nó tới một nhóm hoặc một Miền khác, nó sẽ cố gắng xoá Đối tượng Máy tính của mình. Nếu máy tính không thể xoá được đối tượng do vấn đề trục trắc về mạng, do không đủ quyền hoặc bất kể lý do nào khác, tài khoản này vẫn còn trên* ***Active Directory****. Nó có thể xuất hiện, ngay lập tức hoặc từ từ, như là bị vô hiệu hoá. Nếu đối tượng này là không cần thiết tại Miền đó thì nó phải được xoá thủ công.*

Vô hiệu hoá Đối tượng Máy tính

Nếu bạn dự kiến sẽ đặt máy tính rời khỏi mạng (***offline***) trong một thời gian dài, cách tốt nhất là đừng xoá nó, hãy vô hiệu hóa (***Disable***) nó. Một những nguyên tắc cơ bản nhất của bảo mật là lưu giữ các định danh nhận dạng càng ít càng tốt, cho phép việc xác thực xẩy ra chỉ với một số lượng tối thiểu các tài khoản cần thiết để phục vụ cho cơ quan của bạn. Khi bạn vô hiệu hoá một Đối tượng Máy tính, SID và tất tất cả các giá trị thuộc tính của nó vẫn còn nguyên vẹn, bởi vậy khi bạn kích hoạt lại đối tượng này có thể dùng ngay mà không cần chỉnh sửa.

Để vô hiệu hoá một Đối tượng Máy tính, tại bảng điều khiển ***Active Directory Users And Computers***, chọn đối tượng này và từ thực đơn ***Action*** chọn ***Disable Account***. Xuất hiện dấu X màu đỏ tại biểu tượng của đối tượng báo là nó đã bị vô hiệu hoá, như trong hình 8-14. Khi Đối tượng bị vô hiệu hoá, máy tính này không thể thiết lập kênh bảo mật tới Miền. Người dùng trước đó chưa từng đăng nhập vào máy tính, do đó sẽ không có các thông tin đăng nhập được lưu tạm trên máy tính sẽ không thể đăng nhập được cho tới khi bạn thiết lập lại kênh thông tin bảo mật bằng cách kích hoạt lại tài khoản này.



Hình 8-14 Vô hiệu hoá tài khoản máy tính

Để kích hoạt lại đối tượng, sử dụng cùng qui trình như trên và chọn ***Enable Account*** từ thực đơn ***Action***.

Reset (khởi tạo lại) Đối tượng Máy tính

Đôi khi người quản trị muốn thay thế một máy tính trên mạng để nâng cấp phần cứng hoặc vì các lý do khác, nhưng vẫn muốn sử dụng Đối tượng Máy tính ban đầu cùng với nhóm và các quyền được gán của nó. Khi một máy tính gia nhập vào một Miền và tương ứng với một Đối tượng Máy tính cụ thể, bạn không thể nhập một máy tính khác vào cùng Đối tượng đó và bạn cũng không thể tách rời máy tính ra khỏi Miền và nhập lại một máy tính khác có cùng tên mà không cần tạo lại Đối tượng này và không bị mất SID cũng như nhóm và các quyền tương ứng.

Mặc dù vậy, bạn vẫn có thể sử dụng lại cùng Đối tượng Máy tính cho hai máy tính khác nhau bằng cách khởi tạo lại (***Reset***) Đối tượng này. Việc khởi tạo lại một Đối tượng Máy tính phải đặt lại mật khẩu của nó nhưng vẫn duy trì được tất cả các thuộc tính của nó. Bằng cách đặt lại mật khẩu, đối tượng này được phép dùng lại. Bất cứ một máy tính nào được đặt tên thích hợp là có thể gia nhập vào Miền và sử dụng lại được Đối tượng đó. Để khởi tạo lại một Đối tượng Máy tính ta sử dụng bảng điều khiển ***Active Directory Users***

And Computers, chọn đối tượng và từ thực đơn ***Action*** chọn tiếp ***Reset Account***. Sau khi xác nhận lại sẽ xuất hiện hộp thông báo tình trạng tài khoản đã được khởi tạo lại thành công. Bạn cũng có thể khởi tạo lại tài khoản máy tính bằng cách sử dụng tiện ích dòng lệnh ***Netdom.exe***.

> ***LƯU Ý Mục đích kỳ thi*** *Mục đích kỳ thi 70-290 đòi hỏi thí sinh có khả năng "Khởi tạo lại tài khoản máy tính".*

Quản lý máy tính từ xa

Ngoài các thao tác với các Đối tượng Máy tính, bảng điều khiển ***Active Directory Users And Computers*** cũng cho phép bạn truy nhập vào máy tính của chính nó. Khi bạn chọn Đối tượng Máy tính và từ thực đơn ***Action*** chọn ***Manage*** sẽ mở ra bảng điều khiển ***Computer Management*** mới, trỏ tới máy tính được chọn. Tiếp theo bạn có thể thực hiện bất cứ chức năng chuẩn nào từ bảng điều khiển này với máy tính đã chọn (với các Cấp phép thích hợp).

Quản lý các Đối tượng Máy tính bằng dòng lệnh

Tất cả các công việc quản lý Đối tượng Máy tính mà bạn đã tìm hiểu trong các phần trước cũng có thể sử dụng các công cụ dòng lệnh có trong Windows Server 2003. Phần trình bày sau đây sẽ khảo sát việc sử dụng các công cụ này.

Quản lý thuộc tính của Đối tượng Máy tính bằng Dsmod.exe

Công cụ ***Dsmod.exe*** có thể chỉnh sửa các thuộc tính của Đối tượng Máy tính, cũng giống như đối với đối tượng người dùng và đối tượng nhóm. Ngoài ra, bạn có thể sử dụng ***Dsmod.exe*** để vô hiệu hoá, kích hoạt và khởi tạo lại Đối tượng Máy tính (nhưng không xóa được chúng). Cú pháp để chỉnh sửa lại Đối tượng Máy tính của công cụ này như sau:

dsmod computer *ComputerDN [parameters]*

Chức năng của các tham số dòng lệnh như sau:

■ ***ComputerDN*** Chỉ ra DN của Đối tượng Máy tính cần chỉnh sửa.

■ **-desc *Description*** Chỉ ra giá trị thuộc tính ***Description*** của Đối tượng Máy tính.

■ **-loc *Location*** Chỉ ra giá trị thuộc tính ***Location*** của Đối tượng Máy tính.

■ **-disabled [yes|no]** Vô hiệu hoá hoặc kích hoạt Đối tượng Máy tính đã định.

■ **-Reset** Đặt lại mật khẩu của Đối tượng Máy tính đã định.

■ **-s *Server*** Chỉ ra tên của Máy chủ Điều khiển Miền mà chương trình dùng để truy nhập tới Đối tượng Máy tính này. Khi bỏ trống thì chương trình mặc định trỏ tới Máy chủ Điều khiển Miền mà người dùng đang đăng nhập.

■ **-d *Domain*** Chỉ ra tên của Miền mà Đối tượng Máy tính đang định vị trong đó. Khi bỏ trống chương trình sẽ mặc định lấy Miền mà người dùng đang đăng nhập.

■ **-u *UserName*** Chỉ ra tên của tài khoản người dùng chương trình sẽ sử dụng truy nhập vào Miền. Khi bỏ trống, chương trình sẽ mặc định tài khoản người dùng mà hệ thống đang đăng nhập.

■ **-p [*Password* | *]** Chỉ ra mật khẩu ứng với tài khoản người dùng đã chỉ ra tại tham số **-u** . Nếu có dấu hoa thị (*), chương trình dừng lại và nhắc người dùng nhập mật khẩu.

Để vô hiệu hoá tài khoản máy tính, sử dụng dòng lệnh sau:

dsmod computer CN=webserver1, CN=Computers, DC=ACNA, DC=com – disabled yes

Để khởi tạo lại tài khoản máy tính, sử dụng dòng lệnh sau

dsmod computer CN=webserver1, CN=Computers, DC=ACNA, DC=com – Reset

Xóa Đối tượng Máy tính bằng Dsrm.exe

Dsmod.exe có thể chỉnh sửa Đối tượng Máy tính nhưng không xoá chúng được. Để xoá Đối tượng Máy tính bạn phải sử dụng tiện ích ***Dsrm.exe***. Bạn cần chỉ ra DN cuả đối tượng mà bạn muốn xoá tại dòng lệnh ***Dsrm.exe***, sử dụng cú pháp sau:

Dsrm *ObjectDN*

Khi bạn xác nhận yêu cầu xoá, chương trình sẽ xoá đối tượng này. Một ví dụ của chương trình ***Dsrm.exe*** như sau:

dsrm CN=webserver1,CN=Computers,DC=ACNA,DC=com

KHẮC PHỤC SỰ CỐ TÀI KHOẢN MÁY TÍNH

Active Directory xem Đối tượng Máy tính như là Chủ thể Bảo mật (***Sercurity Principal***). Điều này có nghĩa là máy tính cũng giống người dùng là có các thuộc tính như tên, mật khẩu và SID, cho phép nó được đưa vào Danh sách Kiểm soát Truy nhập (ACLs) của các đối tượng khác. Các tài khoản máy tính và quan hệ bảo mật giữa các máy tính và Miền thường rất

mạnh. Tuy nhiên, giống như các tài khoản người dùng, các tài khoản máy tính đôi khi yêu cầu được bảo trì và khắc phục sự cố. Hiếm khi gặp tình huống là một tài khoản hoặc kênh bảo mật bị bẻ gẫy, các dấu hiệu của lỗi thường rất rõ ràng.

Các dấu hiệu phổ biến của sự cố tài khoản máy tính như sau:

- Thông báo lúc đăng nhập chỉ ra là không thể liên hệ được với Máy chủ Điều khiển Miền, tài khoản máy tính đó có thể bị mất hoặc quan hệ tin cậy (cách khác chỉ tới kênh bảo mật) giữa máy tính này và Miền bị mất. Một ví dụ thông báo lỗi từ máy trạm Windows XP, như hình 8-15.
- Thông báo lỗi hoặc ghi lại các sự kiện chỉ ra các vấn đề tương tự hoặc gợi ý là mật khẩu, sự tin cậy, kênh bảo mật, hoặc quan hệ với Miền hoặc Máy chủ Điều khiển Miền bị lỗi.
- Tài khoản máy tính trong ***Active Directory*** bị mất.

Hình 8-15 Thông báo đăng nhập Windows XP chỉ ra có thể tài khoản máy tính gặp sự cố

> ***LƯU Ý Mục đích kỳ thi*** *Mục đích của kỳ thi 70-290 yêu cầu thí sinh có khả năng "khắc phục sự cố tài khoản máy tính" và "dự đoán và giải quyết các vấn đề liên quan đến các tài khoản máy tính bằng cách sử dụng bảng điều khiển* ***Active Directory Users and Computers****."*

Nếu một trong các tình huống này xảy ra thì bạn phải khắc phục sự cố Tài khoản Máy tính. Bạn đã được học ở phần trên là làm thế nào để xóa, vô hiệu hóa, và khởi tạo lại tài khoản máy tính và làm thể nào để nhập được máy tính vào Miền. Các quy tắc khắc phục sự cố tài khoản máy tính khi một trong các sự kiện xảy ra như sau:

1. Nếu tài khoản máy tính đã có trong ***Active Directory*** thì bạn phải khởi tạo lại nó.

2. Nếu tài khoản máy tính bị mất trong Active Directory thì bạn phải tạo lại tài khoản máy tính.
3. Nếu máy tính vẫn thuộc Miền thì bạn phải di chuyển nó ra khỏi miền bằng cách thay đổi quan hệ thành viên của nó sang Nhóm làm việc (*Worrkgroup*). Tên của Nhóm làm việc là không quan trọng.
4. Nhập lại máy tính vào Miền. Cách khác là nhập một máy tính khác vào Miền này, nhưng máy tính mới phải có cùng tên như tài khoản máy tính.

Để khắc phục bất kỳ sự cố nào của tài khoản máy tính bạn áp dụng tất cả các quy tắc này. Chúng có thể được tiến hành theo một thứ tự bất kỳ, trừ quy tắc 4, nhập lại máy tính vào Miền phải luôn là bước cuối cùng. Hai tình huống dưới đây minh hoạ việc sử dụng các quy tắc này:

- Người dùng phàn nàn là khi cô ấy đăng nhập, hệ thống xuất hiện thông báo lỗi thống báo tài khoản máy tính có thể bị mất. Áp dụng quy tắc 1, bạn mở ***Active Directory Users And Computers*** và tìm thấy tài khoản máy tính trong Miền. Bạn khởi tạo lại đối tượng này. Không áp dụng quy tắc 2 - đối tượng đã tồn tại. Sau đó, sử dụng quy tắc 3, bạn tách rời hệ thống này ra khỏi Miền và theo quy tắc 4, kết nối lại nó vào Miền này.
- Tài khoản máy tính bị khởi tạo lại do rủi ro, vì thế quy tắc 1 là đã được áp dụng. Dù cho việc khởi tạo lại là ngẫu nhiên, bạn vẫn phải tiếp tục cứu lại bằng cách áp dụng ba quy tắc còn lại. Quy tắc 2 không áp dụng do Đối tượng Máy tính đã tồn tại trong Miền. Theo quy tắc 3 và 4, tách máy tính ra khỏi Miền và sau đó nhập lại.

TỔNG KẾT

- Để người dùng đăng nhập vào Miền ***Active Directory***, họ không chỉ cần có Đối tượng Người dùng, mà còn phải có cả đối tượng đại diện cho máy tính của họ. Đối tượng Máy tính đại diện cho một hệ thống cụ thể trên mạng và chứa các thông tin thuộc tính về hệ thống.
- Các Đối tượng Máy tính có chức năng như là Chủ thể Bảo mật . Bạn có thể đưa chúng vào các nhóm và gán cho chúng các Cấp phép.
- Để thêm máy tính vào Miền, bạn phải tạo Đối tượng Máy tính cho nó trong Active Directory và sau đó kết nối máy vật lý với Miền. Đối tượng Máy tính có thể được tạo trước hoặc trong tiến trình kết nối.
- Bạn phải đăng nhập với tư cách như là thành viên của nhóm ***Administrators*** cục bộ để thay đổi quan hệ thành viên Miền của máy tính.
- Để tạo Đối tượng Máy tính bạn có thể sử dụng bảng điều khiển ***Active Directory Users And Computers***, tiện ích ***Dsadd.exe*** hoặc ***Netdom.exe***. Nhóm ***Administrators*** và ***Account Operators*** có đủ quyền tạo Đối tượng Máy tính mới và bạn cũng có thể uỷ quyền thích hợp tới người dùng và nhóm khác.
- Đối tượng Máy tính mà không đóng vai trò là Máy chủ Điều khiển Miền mặc định được đặt tại Đối tượng Chứa ***Computers*** . Bạn không thể áp dụng chính sách nhóm cho Đối tượng Chứa này, bởi vậy các Đối tượng Máy tính thường được đặt tại OU thay cho việc đặt tại vị trí mặc định này.
- Để nhập một máy tính vào Miền, bạn sử dụng thẻ ***Computer Name*** tại hộp thoại ***System Properties*** hoặc dùng tiện ích ***Netdom.exe***. Nếu Đối tượng Máy tính của máy tính chưa tồn tại thì khi bạn tiến hành nhập nó vào Miền thì hệ thống sẽ tạo ra đối tượng này (giả thiết là bạn có đủ các Cấp phép cần thiết để tạo nó.)
- Sử dụng bảng điều khiển ***Active Directory Users and Computers***, tiện ích ***Dsmod.exe*** và ***Dsrm.exe***, bạn có thể quản lý các thuộc tính của Đối tượng Máy tính cũng như xoá, vô hiệu hoá và khởi tạo lại chúng.
- Đối tượng Máy tính có Mã Định danh Bảo mật - SID mà ***Active Directory*** sử dụng để chỉ dẫn đến các quan hệ thành viên nhóm của nó và các Cấp phép khác. Việc bị xoá ngẫu nhiên là nguyên nhân làm cho SID của nó bị mất không cứu lại được, bắt buộc bạn phải tạo lại

các Cấp phép. Phải cẩn thận khi xoá Đối tượng Máy tính, thay vào đó hãy vô hiệu hóa chúng và ta có thể kích hoạt lại chúng mà không mất thông tin.

- Các bước chính để giải quyết sự cố của Đối tượng Máy tính bao gồm việc tạo hoặc khởi tạo lại đối tượng, loại bỏ máy tính khỏi Miền và nhập lại nó vào Miền.

BÀI TẬP THỰC HÀNH

Bài tập thực hành 8-1: Tạo Đối tượng Máy tính sử dụng *Active Directory Users And Computers*

Trong bài tập thực hành thực hành này, bạn tạo Đối tượng Máy tính mới sử dụng bảng điều khiển ***Active Directory Users and Computers***.

1. Đăng nhập vào Máy chủ Điều khiển Miền Windows Server 2003 với tư cách là ***Administrator***.
2. Bấm ***Start***, trỏ tới ***Administrative tools*** và chọn ***Active Directory Users And Computers***. Xuất hiện ***Bảng điều khiển Active Directory Users And Computers***.
3. Chọn ***Computers*** Đối tượng Chứa và thực đơn ***Action*** trỏ tới ***New*** và chọn ***Computer***. Xuất hiện ***New Object – Computer*** trình hướng dẫn.
4. Tại hộp ***Computer Name*** , gõ ***Computer1*** và tiếp theo chọn ***Next***.
5. Bấm ***Next*** và sau đó bấm ***Finish***. Đối tượng Máy tính của ***Computer1*** xuất hiện trong ***Computers*** Đối tượng Chứa.

Bài tập thực hành 8-2: Tạo Đối tượng Máy tính sử dụng Dsadd.exe

Trong bài tập thực hành này, bạn tạo Đối tượng Máy tính mới sử dụng tiện ích ***Dsadd.exe***.

1. Đăng nhập vào Máy chủ Điều khiển Miền Windows Server 2003 với tư cách là ***Administrator***.
2. Bấm ***Start*** chạy ***Command Prompt***. Xuất hiện dấu nhắc lệnh.
3. Tại dấu nhắc, gõ lệnh sau (với *xx* là số hiệu của bạn) và nhấn ***Enter***:

   dsadd computer "CN=Computer2, CN=Computers, DC=ACNA*xx*, DC=com" –desc "Mark Lee's Workstation"

4. Bấm ***Start***, trỏ tới ***Administrative tools*** và chọn ***Active Directory Users And Computers***. Xuất hiện bảng điều khiển ***Active Directory Users And Computers***.
5. Chọn Đối tượng Chứa ***Computers*** . Xác nhận là Đối tượng Máy tính của máy tính ***Computer2*** xuất hiện trong Đối tượng Chứa và có diễn giải ***Description*** là "***Mark Lee's Workstation***" trong thẻ ***General*** của hộp thoại ***Properties*** của Đối tượng.

Bài tập thực hành 8-3: Vô hiệu hoá và kích hoạt Đối tượng Máy tính

Trong bài tập thực hành này, bạn sẽ vô hiệu hoá và kích hoạt lại Đối tượng Máy tính sử dụng *Bảng điều khiển* ***Active Directory Users And Computers***.

1. Đăng nhập vào Máy chủ Điều khiển Miền Windows Server với tư cách là ***Administrator***.
2. Bấm ***Start***, trỏ tới ***Administrative tools*** và chọn ***Active Directory Users And Computers***. Xuất hiện *Bảng điều khiển* ***Active Directory Users And Computers***.
3. Chọn Đối tượng Chứa ***Computers*** . Sau đó chọn Đối tượng Máy tính ***Computer1*** bạn đã tạo ở bài tập thực hành 8-1 và tại thực đơn ***Action*** chọn ***Disable Account***. Xuất hiện thông báo của ***Active Directory*** nhắc bạn xác nhận lại lệnh.
4. Bấm ***Yes***. Xuất hiện thông báo khác xác nhận là Đối tượng ***Computer1*** đã bị vô hiệu hoá.
5. Bấm ***Yes***. Biểu tượng ***Computer1*** xuất hiện cùng với dấu ***X*** màu đỏ.
6. Chọn lại Đối tượng Máy tính của máy tính ***Computer1*** và tại thực đơn ***Action*** chọn ***Enable Account***. Xuất hiện thông báo của ***Active Directory*** cho bạn biết là Đối tượng đã được kích hoạt.
7. Bấm ***Yes***. Biểu tượng ***Computer1*** xuất hiện không có dấu ***X*** màu đỏ nữa.

CÁC CÂU HỎI ÔN TẬP

1. Tối thiểu cần phải là thành viên của nhóm nào để có thể tạo được tài khoản máy tính Windows Server 2003 trong một OU của Miền? Cân nhắc tất cả các bước xử lý và giả thiết là Đối tượng Máy tính của hệ thống này chưa từng tồn tại trong ***Active Directory***. (Chọn tất cả các câu trả lời đúng.)
    a. ***Domain Admins***
    b. ***Enterprise Admins***
    c. ***Administrators*** trên Máy chủ Điều khiển Miền
    d. ***Account Operators*** trên Máy chủ Điều khiển Miền
    e. ***Server Operators*** trên Máy chủ Điều khiển Miền
    f. ***Account Operators*** trên máy tính này

g. ***Server Operators*** trên máy tính này

h. ***Administrators*** trên máy tính này

2. Các công cụ dòng lệnh nào sau đây có thể tạo được Đối tượng Máy tính trong ***Active Directory***?

   a. ***Dsmod.exe***

   b. ***Dsrm.exe***

   c. ***Netdom.exe***

   d. ***Dsadd.exe***

   e. ***Net.exe***

3. Trên nền Windows nào sau đây có khả năng nhập một Đối tượng Máy tính vào Miền ***Active Directory***?

   a. Windows 95

   b. Windows NT 4

   c. Windows 98

   d. Windows 2000

   e. Windows Me

   f. Windows XP

   g. Windows Server 2003

4. Khi bạn mở hộp thoại ***Properties*** của Đối tượng Máy tính trong *Bảng điều khiển* ***Active Directory Users And Computers***, bạn phát hiện ra rằng không có thuộc tính nào được hiển thị trong thẻ ***Operating System***. Các nguyên nhân nào làm cho các thuộc tính này bị vắng mặt?

5. Sau một thời kỳ dài, công ty của bạn tạo Miền thứ hai. Tuần cuối cùng, một số các máy tính mà đã từng trong Miền của bạn được chuyển tới Miền mới. Khi bạn mở ***Active Directory Users And Computers*** thì Đối tượng của máy tính này vẫn ở Miền của bạn và xuất hiện biểu tượng X mà đỏ. Việc thích hợp tiếp theo là gì?

   a. Kích hoạt Đối tượng này

   b. Vô hiệu hoá Đối tượng này

   c. Khởi tạo lại Đối tượng này

   d. Xoá Đối tượng này

6. Người dùng thông báo là khi tiến hành đăng nhập, anh ấy nhận được thông báo tình trạng máy tính không thể liên hệ được với Miền vì Máy chủ Điều khiển Miền bị tắt hoặc tài khoản máy tính có thể bị mất. Bạn mở ***Active Directory Users And Computers*** và phát hiện ra là tài khoản của máy tính bị mất. Các bước bạn nên làm là gì?
7. Một người dùng thông báo là khi tiến hành đăng nhập, anh ấy nhận được thông báo tình trạng máy tính không thể liên hệ được với Miền vì Máy chủ Điều khiển Miền bị tắt hoặc tài khoản máy tính có thể bị mất. Bạn mở ***Active Directory Users And Computers*** và nhìn thấy tài khoản xuất hiện bình thường. Các bước bạn nên làm là gì?

CÁC KỊCH BẢN TÌNH HUỐNG

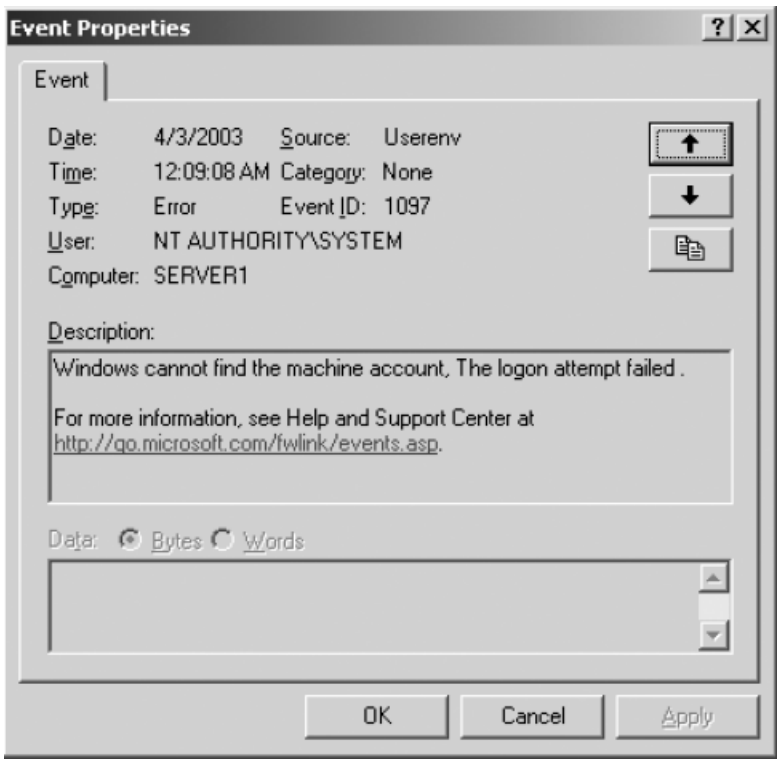
Kịch bản 8-1: Khởi tạo lại Đối tượng Máy tính

Tại Windows Server 2003 Miền ***ACNA.com***, bạn có Đối tượng Máy tính của một Máy chủ Thành viên (***Member Server)*** có tên là ***Pserver01*** trong OU có tên là ***Pservers***. Đối tượng này đại diện cho máy chủ ***Print server*** bị rớt mạng trong thời gian dài và không liên hệ được với máy tính khác trong Miền để chấp nhận lệnh in. Bạn xác định là mật khẩu của tài khoản máy tính trong Miền cần phải được khởi tạo lại. Lệnh nào bạn có thể sử dụng để khởi tạo lại chính xác tài khoản máy tính này?

a. ***dsmod CN=pserver01, CN=PSERVERS, DC=ACNA, DC=com –Reset***
b. ***dsmod computer pserver01.ACNA.com –Reset***
c. ***dsmod ACNA\pserver01 –Reset***
d. ***dsmod computer CN=pserver01, CN=PSERVERS, DC=ACNA, DC=com –Reset***

Kịch bản 8-2: Khắc phục sự cố Đối tượng Máy tính

Sau khi thực hiện bảo trì các máy tính ở văn phòng chi nhánh tại phía Đông vào cuối tuần, người dùng phàn nàn gặp trục trặc đăng nhập. Bạn kiểm tra các nhật ký sự kiện của máy tính tại chi nhánh này, thấy ghi lại như sau:



Dường như có vấn đề với tài khoản máy tính. Chỉ ra tại các bước nào sau đây bạn nên thực hiện để giải quyết vấn đề này, theo đúng trật tự.

a. Xoá tài khoản máy tính.

b. Khởi tạo lại tài khoản người dùng.

c. Nhập máy tính vào Nhóm làm việc.

d. Vô hiệu hoá tài khoản máy tính.

e. Khởi tạo lại tài khoản máy tính.

f. Kích hoạt tài khoản máy tính.

g. Tạo tài khoản máy tính mới.

h. Nhập máy tính vào Miền.

PHẦN 3
QUẢN LÝ VÀ DUY TRÌ CÁC NGUỒN TÀI NGUYÊN CHIA SẺ

CHƯƠNG 9: CHIA SẺ CÁC TÀI NGUYÊN HỆ THỐNG FILE

Một trong những lý do chính của sự tồn tại các mạng dữ liệu đó là khả năng chia sẻ các file cho nhiều người sử dụng trên các máy tính khác nhau. Trên một mạng nhỏ, chia sẻ file thường là một tiến trình thông thường được thực hiện bởi người sử dụng đầu cuối, ở đó tính chất bảo mật ít được chú ý tới. Tuy nhiên, trên một mạng lớn, mà đặc biệt là trong các tổ chức thường xuyên vận hành với các dữ liệu nhạy cảm. Người quản trị mạng cần đảm bảo rằng các file cần thiết đã được chia sẻ, đảm bảo chúng phải được bảo vệ để tránh những phá hủy do yếu tố khách quan hoặc chủ quan và chỉ những người nào được xác thực mới có thể làm việc với chúng.Trong chương này, chúng ta sẽ điểm lại các nội dung và các yêu cầu để chia sẻ file cho những người sử dụng mạng một cách hiệu quả và an toàn.

Hoàn thành chương này bạn có khả năng:

- Tạo/quản lý các thư mục chia sẻ và làm việc với các Cấp phép chia sẻ
- Sử dụng các Cấp phép truy cập NTFS để kiểm soát quá trình truy cập đến các file
- Quản lý việc chia sẻ file bằng Microsoft Internet Information Services

TÌM HIỂU VỀ CÁC CẤP PHÉP

Cấp phép là một trong những khái niệm cơ bản trong quá trình quản trị hệ thống trên hệ điều hành Windows Server 2003. Nói cách khác, Cấp phép là một đặc ân được gán cho một thực thể xác định như một người sử dụng, nhóm hoặc máy tính chẳng hạn nhằm cho phép thực thể này hình thành một hành động xác định hoặc truy cập tới một tài nguyên cụ thể. Windows Server 2003 và tất cả các hệ điều hành Windows khác sử dụng các Cấp phép theo một loạt các phương pháp khác nhau để kiểm soát truy cập tới các thành phần khác nhau trên hệ điều hành.

Windows Server 2003 có nhiều loại Cấp phép, trong đó nổi bật là các Cấp phép được liệt kê ở dưới đây. Mỗi loại Cấp phép này được phân biệt hoàn toàn với nhau mặc dù chúng có thể được cấp cho cùng các thành phần hệ thống.

- **Các Cấp phép trên file**: được sử dụng để kiểm soát việc truy cập tới các file và thư mục trên các ổ đĩa NTFS. Tất cả các người dùng đều sử dụng các Cấp phép này để truy cập tới các file và thư mục NTFS, bất kể họ đang làm việc trên mạng hoặc trên máy tính chứa dữ liệu.
- **Các Cấp phép chia sẻ**: được sử dụng để kiểm soát việc truy cập tới các file/folder/máy in được chia sẻ. Để có thể truy cập đến các tài nguyên chia sẻ này, các người dùng phải có các Cấp phép nhất định.
- **Các Cấp phép *Active Directory***: được sử dụng để kiểm soát việc truy cập tới các đối tượng của dịch vụ ***Active Directory***. Người dùng phải có một số Cấp phép nhất định để có thể đăng nhập vào Miền và truy cập tới các tài nguyên trên mạng. Người quản trị cần có các Cấp phép cao hơn nhằm duy trì các đặc tính của các đối tượng và cấu trúc cây ***Active Directory***.
- **Các Cấp phép registry**: được sử dụng để kiểm soát việc truy cập tới các khóa của ***registry***. Để có thể thay đổi các khóa này, người quản trị cần có các Cấp phép tương ứng.

Trong số các Cấp phép nói trên, một số cần có sự duy trì nhiều hơn so với những cái còn lại. Một người quản trị mạng thông thường có thể làm việc với các Cấp phép trên file mỗi ngày nhưng sẽ không bao giờ thay đổi bằng tay các Cấp phép ***registry***. Trong các chương 6,7 và 8 bạn đã được học về các Cấp phép ***Active Directory*** nhằm cho phép người quản trị

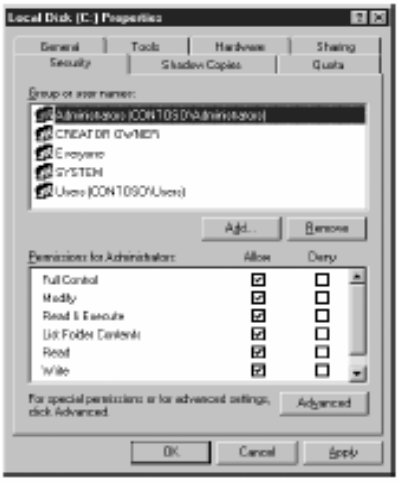
(***Administrator***) tạo và quản trị các đối tượng như: người dùng, nhóm và máy tính chẳng hạn. Trong nhiều trường hợp, các Cấp phép ***Active Directory*** được chuyển giao một lần cho các nhóm quản trị cụ thể và không cần phải điều chỉnh lại trừ phi có sự tái cơ cấu lại cấu trúc tổ chức doanh nghiệp của bạn.

Danh sách Kiểm soát Truy cập (ACL)

Chức năng của các Cấp phép nói trên dựa trên khái niệm Danh sách Điều khiển Truy cập (***Access Control List -*** ACL). Hầu hết các thành phần của Windows bao gồm các file, các tài nguyên chia sẻ, các đối tượng của ***Active Directory*** và các khóa của ***registry*** đều có một ACL. ACL thực chất là một danh sách các Cấp phép nhằm xác định xem ai có Cấp phép truy cập và truy cập đến mức độ nào. ACL của một thành phần xác định bao gồm các Mục vào Kiểm soát Truy cập (***Access Control Entry -*** ACE). Một ACE xác định tên của Chủ thể Bảo mật (đó có thể là người dùng, nhóm hoặc máy tính được gán Cấp phép) và các Cấp phép xác định được gán cho chủ thể đó.

> ***CHÚ Ý: Vậy các ACL được đặt ở đâu?*** *Người quản trị hệ thống cần phải hiểu rằng ACL luôn luôn được đi kèm với các thành phần được kiểm soát chứ không phải đi kèm với các Chủ thể Bảo mật. Ví dụ, một thư mục trên ổ đĩa NTFS có một ACL chứa danh sách các người dùng hay nhóm có Cấp phép truy cập tới thư mục đó. Nếu bạn xem đặc tính của một đối tượng cụ thể, bạn sẽ không thể tìm thấy danh sách các thư mục mà đối tượng đó được phép truy cập. Đây chính là một điểm quan trọng khi bạn khi bạn di chuyển các thành phần giữa các vị trí khác nhau hoặc sao lưu chúng ra một thiết bị lưu trữ khác. Di chuyển các file từ một ổ đĩa NTFS tới một ổ đĩa FAT, sẽ làm cho các Cấp phép bị mất đi do hệ thống file FAT không chứa các ACL.*

Làm việc trên các ACL là khá đơn giản do tất cả các Cấp phép trên hệ điều hành Windows Server 2003 đều sử dụng một giao diện giống nhau. Tất cả các thành phần hệ thống được bảo vệ bằng các Cấp phép đều có hộp thoại ***Properties*** chứa thẻ ***Security***, như được chỉ ra trong hình vẽ 9-1. Trong hộp thoại này, phần trên hiển thị danh sách các ACE (đó chính là các chủ thể bảo mật) còn phần dưới xác định các Cấp phép tương ứng được cấp cho các ACE phía trên. Bạn có thể thêm và xóa các ACE khi cần và xác định các Cấp phép được cho phép hoặc cấm cho từng ACE.



Hình 9-1: Thẻ Security trong hộp thoại Properties

Các Cấp phép

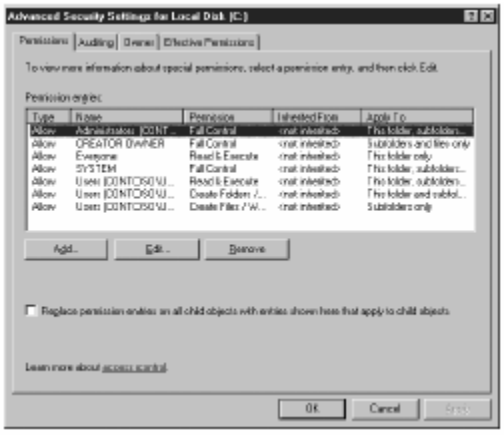
Các Cấp phép trong các ACE được thiết kế nhằm cung cấp cho việc kiểm soát truy cập một cách tập trung cho các thành phần mà chúng cung cấp. Khi bạn gán Cấp phép truy cập đến một thư mục cho một người dùng, việc truy cập không chỉ đơn thuần là ***Có*** hay ***Không***. Bạn có nhiều lựa chọn cho phép xác định mức độ truy cập mà người dùng nhận được. Mỗi Cấp phép của hệ thống Cấp phép được liệt kê ở trên đều có một danh sách các Cấp phép riêng rẽ nhằm xác định các loại tài nguyên mà chúng kiểm soát. Khi tạo một ACE, bạn lựa chọn một chủ thể bảo mật sau đó lựa chọn các Cấp phép riêng lẻ mà bạn định gán cho đối tượng đó.

Ví dụ, các Cấp phép NTFS cho phép bạn xác định một người dùng có khả năng đọc các file trong một thư mục nhưng không được phép thay đổi chúng hoặc bạn cũng có thể cấp nhiều Cấp phép hơn so với nhu cầu của anh ta. Tùy thuộc vào tài nguyên bạn đang làm việc, bạn có thể có hàng tá các Cấp phép khác nhau, ở đó bạn có thể kết hợp chúng theo bất kỳ cách nào mà bạn thích.

Trong một số trường hợp, số lượng các Cấp phép chính xác có thể làm cho người quản trị ACL cảm thấy phức tạp. Để đơn giản hóa vấn đề này, Windows Server 2003 sử dụng 02 mức Cấp phép: các Cấp phép Chuẩn và Cấp phép Đặc biệt. Các Cấp phép Chuẩn là các Cấp phép mà bạn nhìn thấy trong thẻ ***Security*** trong hộp thoại ***Properties***. Đây là các Cấp phép mà bạn có thể làm việc hàng ngày do chúng cung cấp điều khiển cơ bản tới thành phần được bảo vệ.

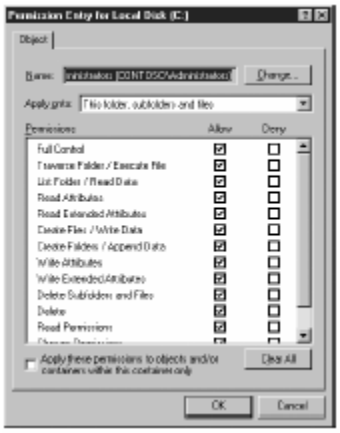
Tuy nhiên, các Cấp phép Chuẩn là sự kết hợp của hai hay nhiều Cấp phép Đặc biệt (bạn có thể đọc thêm về việc sử dụng các Cấp phép Đặc biệt này

như thế nào trong chương này). Để truy cập đến các Cấp phép Đặc biệt, bạn kích chuột vào nút ***Advanced*** trong Thẻ ***Security***, để hiển thị hộp thoại ***Advanced Security Settings*** như trong hình vẽ 9.2.



Hình 9-2: Hộp thoại Advanced Security Settings

Trong hộp thoại này, bạn có thể kiểm soát quá trình truy cập tới một tài nguyên với mức độ tập trung cao hơn bằng cách lựa chọn từ một danh sách đầy đủ các Cấp phép đặc biệt trong hộp thoại ***Permission Entry*** (xem hình 9-3 để biết thêm chi tiết). Điều này thường không cần thiết trên một mạng thông dụng, nhưng một số các thiết lập về Cấp phép mặc định được Windows Server 2003 tạo ra trong suốt tiến trình cài đặt hệ điều hành lại dựa trên các Cấp phép Đặc biệt này.



Hình 9-3: Hộp thoại Permission Entry

> ***CHÚ Ý****: Bạn làm việc với tất cả các hệ thống Cấp phép trên Windows Server 2003 theo cùng một phương pháp, ngoại trừ các Cấp phép Chuẩn và Đặc biệt có thể khác nhau tùy thuộc vào tài nguyên mà bạn cần bảo vệ.*

Tính kế thừa

Một trong những đặc tính quan trọng của các hệ thống Cấp phép trên Windows Server 2003 đó là các đối tượng con sẽ thừa hưởng các Cấp phép từ đối tượng cha. Các Cấp phép luôn luôn đi theo một "dòng chảy" dựa trên tính chất phân cấp của hệ thống file, kiến trúc phân cấp của dịch vụ ***Active Directory*** hay cấu trúc của ***registry***. Khi bạn gán Cấp phép truy cập đến một thư mục NTFS hoặc chia sẻ, một đối tượng ***Active Directory*** hoặc khóa ***registry*** cho một đối tượng bảo mật nào đó, đối tượng này cũng sẽ nhận được các Cấp phép giống hệt khi truy cập đến các thư mục con bên trong thư mục NTFS hoặc chia sẻ, các đối tượng con bên trong đối tượng ***Active Directory*** hoặc các khóa con bên trong một khóa xác định.

Ví dụ, bạn gán Cấp phép cho một người dùng tại thư mục gốc của ổ đĩa NTFS điều đó có nghĩa rằng người dùng sẽ nhận được các Cấp phép giống hệt trên tất cả các file và thư mục con nằm trên ổ đĩa đó. Trong hầu hết các trường hợp, sự kế thừa Cấp phép có ưu điểm to lớn là tránh cho người quản trị phải cung cấp các Cấp phép riêng biệt cho từng thư mục con, từng đối tượng trên dịch vụ ***Active Directory*** hoặc các khóa. Trong thực tế, đối với hầu hết các nhà quản trị mạng, ưu điểm tiếp theo được tính đến của tính kế thừa là ứng dụng chúng khi thiết kế cấu trúc dịch vụ thư mục, chia sẻ trạng thái và các cây ***Active Directory***.

Tuy nhiên, trong một số trường hợp sự kế thừa này là không cần thiết và để loại bỏ tính chất mặc định này chúng ta có hai phương pháp:

- **Tắt tính năng kế thừa**: khi bạn làm việc trên các Cấp phép đặc biệt, bạn có thể điều khiển các Cấp phép mà bạn gán cho một thành phần xác định có được cho một số hoặc tất cả các thành phần con bên trong kế thừa hay không.
- **Cấm các Cấp phép**: tất cả các hệ thống Cấp phép đều cho phép bạn ngăn cấm một Cấp phép cụ thể đối với một đối tượng xác định. Điều này sẽ ngăn cản Cấp phép kế thừa mà đối tượng nhận được từ các đối tượng cha.

Các Cấp phép Hiệu dụng

Các đối tượng được gán Cấp phép thường là các người dùng, nhóm hoặc máy tính, vì vậy rất dễ xảy ra trường hợp một đối tượng sẽ nhận được các Cấp phép khác nhau từ các nguồn khác nhau và trong một số trường hợp các Cấp phép này là xung đột với nhau. Vì lý do này mà có một số chính sách cho phép xác định xem các Cấp phép mà đối tượng nhận được từ các nguồn

khác nhau tương tác với nhau như thế nào. Tất cả các Cấp phép mà một đối tượng nhận được một cách riêng rẽ thông qua tính kế thừa và thành viên nhóm đều là các thông số đầu vào cho các luật này. Chúng có nhiệm vụ kết hợp các Cấp phép này lại và tạo nên các Cấp phép Hiệu dụng của người dùng.

Các luật tạo nên các Cấp phép Hiệu dụng của các đối tượng bao gồm:

- **Các Cấp phép cho phép (*Allow*) là tích lũy**: tất cả các Cấp phép cho phép được gán cho một đối tượng được kết hợp để tạo nên các Cấp phép ảnh hưởng của đối tượng đó. Ví dụ, một người dùng nào đó được gán Cấp phép truy cập toàn quyền (***Full Control***) đến một thư mục trên ổ đĩa NTFS. Tuy nhiên lúc này người dùng cũng đang là thành viên của một nhóm có Cấp phép truy cập chỉ đọc (***read-only***) trên thư mục này. Ngoài ra, người dùng còn thừa hưởng Cấp phép ***read*** và ***write*** từ thư mục cha của thư mục nói trên. Trong trường hợp này tất cả các Cấp phép của người dùng bất kể là được gán hay thừa hưởng từ bất kỳ nguồn nào cũng sẽ được kết hợp lại.
- **Các Cấp phép ngăn cấm (*Deny*) loại bỏ các Cấp phép cho phép (Allow)**: các Cấp phép ***deny*** mà một đối tượng nhận được sẽ loại bỏ tất cả các Cấp phép ***allow*** bất kể từ nguồn nào. Ví dụ, nếu một người dùng nhận được Cấp phép truy cập toàn quyền tới một thư mục thông qua tính kế thừa và đồng thời cũng nhận được Cấp phép truy cập toàn quyền thông qua cơ chế thành viên nhóm. Tuy nhiên Cấp phép mà bạn tạo ra nhằm ngăn chặn người dùng này truy cập tới thư mục nói trên sẽ ghi đè tất các Cấp phép thừa hưởng từ thư mục cha và nhóm. Vì vậy trong trường hợp này, Cấp phép Hiệu dụng của người dùng là không được phép (***Deny***) truy cập tới thư mục này.
- **Các Cấp phép gán riêng rẽ có mức độ ưu tiên cao hơn các Cấp phép kế thừa**: khi một đối tượng bảo mật kế thừa các Cấp phép từ đối tượng cha hoặc thông qua nhóm, bạn có thể loại bỏ các Cấp phép này bằng cách gán trực tiếp các Cấp phép khác nhau cho chính đối tượng đó. Các Cấp phép kế thừa tuân theo luật còn các Cấp phép gán riêng rẽ nằm ngoài luật đó. Vì vậy, các Cấp phép ***cho phép*** gán riêng rẽ sẽ loại bỏ các Cấp phép kế thừa ***ngăn cấm***.

CÁC THƯ MỤC CHIA SẺ

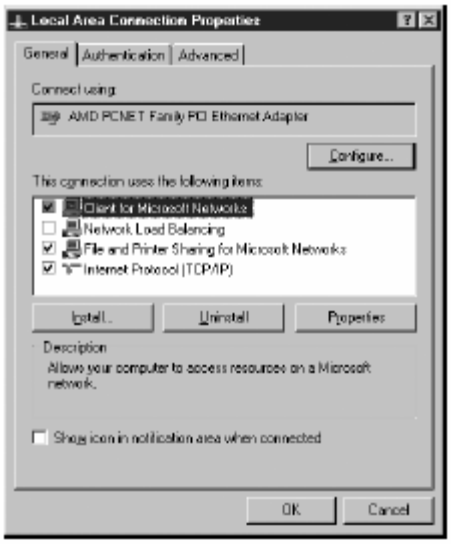
Khi bạn đang ngồi vào một máy tính sử dụng hệ điều hành Windows Server 2003, bạn có thể truy cập đến các file và thư mục trên các ổ đĩa của nó từ

màn hình giao diện (*hay còn gọi là bảng điều khiển hệ thống – System Console*) với giả thiết bạn có các Cấp phép thích hợp. Bạn cũng có thể cho phép các người dùng trên mạng truy cập tới các file và thư mục trên máy tính của bạn, nhưng để làm được điều đó trước hết bạn phải tạo một chia sẻ nhằm xác định những gì mà họ có thể truy cập.

> ***THÔNG TIN THÊM*** *Bạn có thể tạo ra hai loại chia sẻ trên các máy tính sử dụng hệ điều hành Windows: các chia sẻ trên hệ thống file và các chia sẻ máy in. Trong chương này bạn sẽ được làm quen với các chia sẻ trên hệ thống file. Việc tạo các chia sẻ máy in sẽ được đề cập trong chương 10.*

Tính năng để tạo ra các chia sẻ trên Windows Server 2003 được dựa trên hai dịch vụ được chạy trên mỗi máy tính Windows: dịch vụ ***Workstation*** (dịch vụ máy trạm) và dịch vụ ***Server*** (dịch vụ máy chủ). Hai dịch vụ này được thực hiện bởi hai module: ***Client For Microsoft Networks*** và ***File And Printer Sharing For Microsoft Networks***. Cả hai module nói trên đều xuất hiện trong hộp thoại ***Local Area Connection Properties*** của tất cả các giao diện mạng được cài đặt trên máy tính (xem hình vẽ 9-4). Dịch vụ ***Server*** chịu trách nhiệm tạo ra các tài nguyên chia sẻ sẵn sàng trên mạng còn dịch vụ ***Workstation*** cho phép các máy tính khác truy cập tới những tài nguyên này.

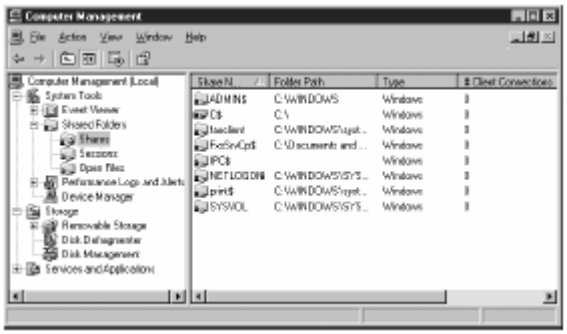
> ***CHÚ Ý*** ***Workstations và Servers*** *Mặc dù các tên này có nhiều phiên bản khác nhau nhưng Windows là một hệ điều hành ngang hàng (**peer-to-peer**) có nghĩa là mỗi máy tính đều có khả năng hoạt động được cả ở chế độ máy trạm lẫn máy chủ. Thậm chí các máy tính không sử dụng hệ điều hành có tên **Server** trên đó vẫn có thể chạy dịch vụ **Server**.*



Hình 9-4: Hộp thoại Local Area Connection Properties

Các chia sẻ dùng để quản trị

Trước khi bạn tạo ra các chia sẻ trên hệ điều hành Windows Server 2003, đã có một số chia sẻ mặc định. Mặc định, tiến trình cài đặt Windows Server 2003 tạo ra các chia sẻ sau nhằm mục đích quản trị (xem hình 9-5):



Hình 9-5: Các chia sẻ quản trị trong snap-in *Shared Folders*

- **Các chia sẻ ổ đĩa** Mỗi ổ đĩa trên máy tính đều có một chia sẻ quản trị mặc định tại mức gốc. Chia sẻ này sẽ được đặt tên dựa theo ký tự ổ đĩa viết hoa và ký tự $ (ví dụ C$). Ký tự này làm cho chia sẻ không được hiển thị trong ***My Network Places*** mặc dù vẫn có thể truy cập chúng trực tiếp bằng cách sử dụng snap-in ***Shared Folders*** trong MMC bằng việc tạo một shortcut hoặc sử dụng Windows Explorer. Mặc định nhóm ***Administrators*** (*nhóm quản trị*) được gán Cấp phép ***Full Control*** cho các chia sẻ này. Các Cấp phép này là không thể thay đổi hay xóa được.

- **Admin$** Thư mục gốc hệ thống (mặc định nó có đường dẫn là ***C:\Windows***) tự động được chia sẻ với tên ***Admin$***. Đây cũng là một chia sẻ ẩn, nó cho phép các thành viên của nhóm ***Administrators*** truy cập đầy đủ tới thư mục gốc hệ thống mà không cần biết chính xác vị trí của chúng.
- **IPC$** Một chia sẻ được tạo ra nhằm cung cấp quá trình truy cập từ xa tới các ***Named Pipe*** trên máy tính. Đây là một phần của bộ nhớ được sử dụng để chuyển thông tin từ một tiến trình này sang một tiến trình khác. Chia sẻ này là cần thiết để thực hiện các công việc quản trị máy tính từ xa qua mạng.

Ngoài ra, Windows Server 2003 còn tạo ra các chia sẻ quản trị khác khi bạn cài đặt các thành phần xác định:

- **Print$** Khi bạn cài đặt một máy in được chia sẻ đầu tiên trên máy tính, Windows Server 2003 tạo ra một chia sẻ ẩn tại thư mục ***<Systemroot>\System32\Spool\Drivers*** với tên là ***Print$***. Chia sẻ này cho phép các hệ thống khác trên mạng truy cập tới các trình điều khiển máy in được cài đặt tên máy tính. Các nhóm ***Administrators***, ***Print Operators***, ***Server Operators*** có Cấp phép ***Full Control*** đối với chia sẻ này. Nhóm đồng nhất đặc biệt ***Everyone*** chỉ có Cấp phép ***Read***.
- **Faxclient** Khi bạn cài đặt dịch vụ Fax trên máy tính, Windows Server 2003 tự động tạo ra một chia sẻ tại thư mục ***C:\WINDOWS\system32\clients\faxclient*** có tên là ***faxclient***. Chia sẻ này cho phép các người dùng trên mạng truy cập đến phần mềm fax dành cho máy trạm. Nhóm đồng nhất đặc biệt ***Everyone*** có Cấp phép ***Read*** trên chia sẻ này.
- **FxsSrvCp$** Khi bạn cài đặt dịch vụ Fax trên máy tính, Windows tự động tạo ra một chia sẻ ẩn tại thư mục ***C:\Document and Settings\All Users\Application Data\Microsoft\Windows NT\MSFax\Common Coverpage*** với tên chia sẻ là ***FxsSrvCp$***. Chia sẻ này cho phép các máy khách fax truy cập tới các trang được lưu trên máy chủ. Nhóm ***Administrators*** có Cấp phép ***Full Control*** (*toàn quyền*) trên chia sẻ này trong khi nhóm đồng nhất đặc biệt ***Everyone*** chỉ có Cấp phép ***Read***.
- **SYSVOL** Khi bạn nâng cấp một máy tính Windows Server 2003 thành một DC (Máy chủ Điều khiển Miền), hệ thống sẽ chia sẻ thư mục ***<Systemroot>\SYSVOL\sysvol*** và đặt tên nó là ***SYSVOL***. Máy chủ Điều khiển Miền sử dụng chia sẻ này để lưu trữ các GPO

(***Group Policy Object*** *– chính sách nhóm*) và các ***script*** (*kịch bản*), chúng sẽ được nhân bản đến các máy tính khác thuộc Miền. Các nhóm ***Administrators*** và ***Authenticated Users*** (*nhóm những người sử dụng được xác thực*) có Cấp phép ***Full Control*** trên chia sẻ này trong khi nhóm đặc biệt ***Everyone*** chỉ có Cấp phép ***Read***.

- **NETLOGON** Khi bạn nâng cấp một máy tính Windows Server 2003 thành một Máy chủ Điều khiển Miền, hệ thống sẽ chia sẻ thư mục ***Systemroot\SYSVOL\sysvol\<tên Miền>\SCRIPTS*** và đặt tên nó là ***NETLOGON***. Đây là một chia sẻ được tạo ra nhằm tạo tính tương thích ngược cho các hệ điều hành mạng trước đây. Máy chủ Điều khiển Miền sử dụng chia sẻ này nhằm cung cấp chức năng cơ bản giống như ***SYSVOL*** cho các Máy chủ Điều khiển Miền Windows NT4. Nhóm ***Administrators*** có Cấp phép ***Full Control (***toàn quyền) trên chia sẻ này trong khi nhóm đặc biệt ***Everyone*** chỉ có Cấp phép ***Read***.

  CHÚ Ý Các chia sẻ ẩn *Bản chất ẩn của các chia sẻ quản trị không giới hạn các chia sẻ xác định khác. Bạn có thể ẩn bất kỳ chia sẻ nào bằng cách sử dụng ký tự $ tại cuối của tên chia sẻ. Nó không ngăn ngừa người sử dụng truy cập tới các chia sẻ, nó chỉ ngăn không cho chúng hiển thị trong Windows Explorer.*

Chuẩn bị cho quá trình tạo các thư mục chia sẻ

Để tạo một hệ thống file chia sẻ, bạn phải có các quyền sau:

- **Trên Máy chủ Điều khiển Miền**: trên máy chủ Điều khiển Miền, để tạo các thư mục chia sẻ, bạn phải là thành viên của nhóm ***Administrators*** hoặc ***Server Operators***. Do các nhóm ***Enterprise Admins*** và ***Domain Admin***s là thành viên của nhóm ***Administrators*** nên các nhóm này cũng có thể tạo các thư mục chia sẻ.
- **Trên Máy chủ thành viên hoặc máy trạm đã gia nhập miền**: Để tạo các thư mục chia sẻ trên máy chủ thành viên hoặc máy trạm thuộc Miền, bạn phải là thành viên của nhóm ***Administrators***, ***Server Operators*** hoặc ***Power Users***.
- **Trên nhóm làm việc hay máy độc lập**: Để tạo các thư mục chia sẻ trên một máy tính không phải là thành viên của một Miền, bạn phải là thành viên của nhóm ***Administrators*** hoặc ***Power Users***.

- **Trên ổ đĩa NTFS**: Nếu thư mục mà bạn định chia sẻ trên ổ đĩa NTFS, bạn phải đăng nhập vào máy tính với tài khoản có ít nhất Cấp phép ***Read*** rrên thư mục đó.

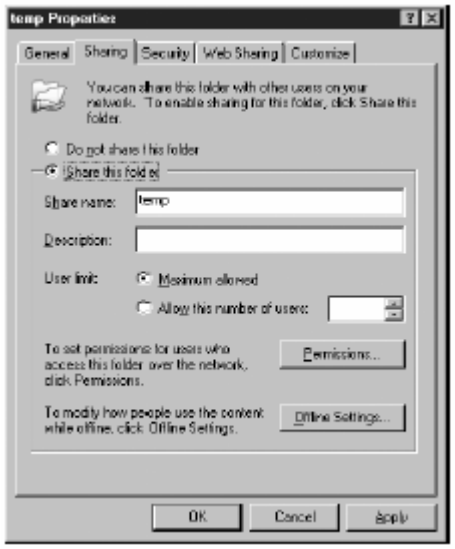
Cũng như nhiều các công việc khác trên Windows Server 2003, bạn có thể tạo các thư mục chia sẻ theo nhiều cách. Trong phần sau sẽ cung cấp một số các công cụ giúp bạn tạo và quản trị các thư mục chia sẻ.

> ***CHÚ Ý Mục đích của kỳ thi*** *Mục đích của kỳ thi 70-290 yêu cầu học viên có thể "cấu hình truy cập tới các thư mục chia sẻ"*

Tạo thư mục chia sẻ bằng Windows Explorer

Phương pháp thông dụng nhất đó là sử dụng Windows Explorer để lựa chọn thư mục cần chia sẻ sau đó thực hiện chia sẻ chúng. Bạn có thể chia sẻ bất kỳ thư mục nào trên bất kỳ ổ đĩa nào của máy tính. Khi người sử dụng trên mạng duyệt các thư mục chia sẻ, chúng sẽ xuất hiện như các thư mục riêng biệt nhưng không có lời chú thích. Trừ phi bạn nói với người sử dụng, còn họ không thể biết được các thư mục chia sẻ nằm trên ổ đĩa nào hoặc vị trí của chúng.

Để chia sẻ thư mục trong Windows Explorer, nhấp chuột phải vào nó và lựa chọn ***Sharing And Security*** để hiển thị hộp thoại như trên hình vẽ 9-6. bạn cũng có thể truy cập tới hộp thoại này bằng cách lựa chọn một thư mục rồi chọn theo đường dẫn ***File -> Properties -> Sharing***.



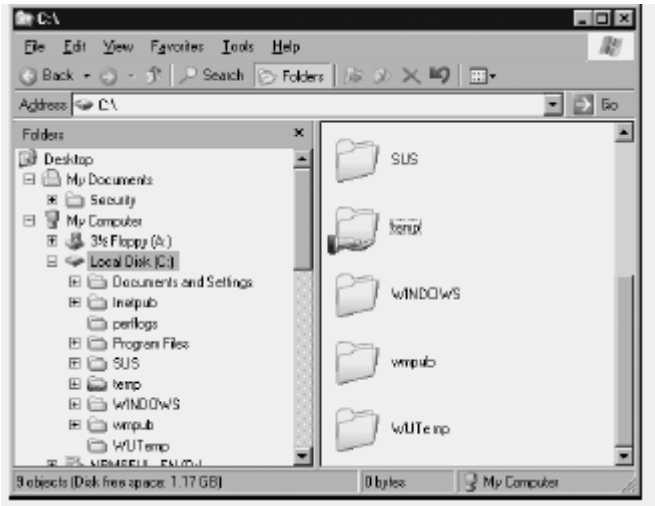
Hình 9-6: Thẻ Sharing trên hộp thoại Properties của folder

Khi bạn lựa chọn ***Share This Folder***, bạn sẽ thực hiện công việc kích hoạt các điều khiển khác trong thẻ ***Sharing*** cho phép cấu hình các tham số sau:

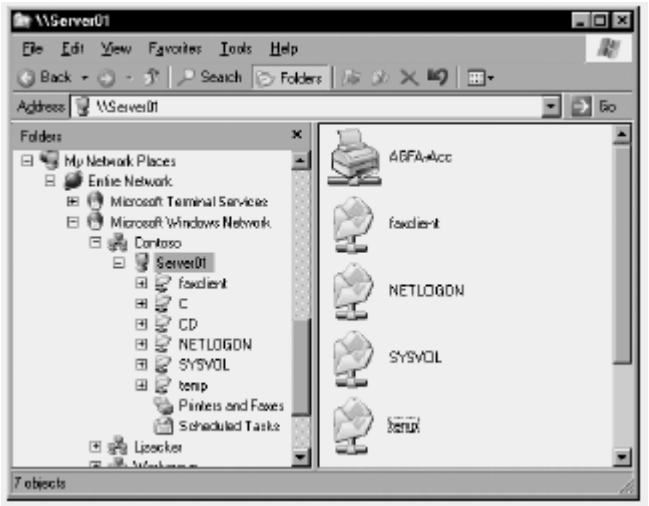
- **Share Name** (*tên chia sẻ*): Xác định tên hiển thị trên mạng của thư mục chia sẻ. Mặc định, tên của thư mục xuất hiện trong hộp văn bản nhưng bạn có thể đặt bất cứ tên nào với chiều dài cho phép lên tới 80 ký tự. Trường này là bắt buộc.
- **Description** (*mô tả*): cho phép bạn cung cấp các thông tin thêm về thư mục chia sẻ như: mục đích của thư mục chia sẻ, nội dung của nó hoặc bất kỳ thông tin khác. Trường này là không bắt buộc.
- **User limit** (*giới hạn người sử dụng*): cho phép bạn xác định có bao nhiêu người có khả năng kết nối tới thư mục chia sẻ tại cùng một thời điểm. Đặc tính này giúp bạn ngăn ngừa tình trạng các tài nguyên hệ thống bị qúa tải do có quá nhiều người sử dụng truy cập đồng thời.
- **Permissions** (*Cấp phép truy cập*): cho phép bạn xác định ai có Cấp phép truy cập đến thư mục chia sẻ và mức độ truy cập. Để biết thêm chi tiết về vấn đề này xem phần "quản lý các Cấp phép chia sẻ" trong chương này.
- **Offline Settings** (*các thiết lập về cơ chế làm việc không kết nối*): có cho phép người sử dụng mạng lưu trữ tạm thời nội dung thư mục chia sẻ trên máy tính của họ hay không. Để biết thêm chi tiết về vấn đề này, xin xem phần "điều khiển lưu trữ không kết nối" trong chương này.

Một khi bạn đã hoàn tất việc cấu hình các tham số trong thẻ ***Sharing***, nhấp ***OK*** để tạo thư mục chia sẻ. Để xác nhận thư mục đã được chia sẻ, bạn có một vài phương pháp bao gồm:

- Trong Windows Explorer, phần ***My Computer*** thư mục được chia sẻ sẽ có biểu tượng hình bàn tay mở ra.



■ Trong Windows Explorer, phần ***My Network Places***, một biểu tượng thư mục chia sẻ sẽ xuất hiện trên máy tính mà bạn đã tạo nó.



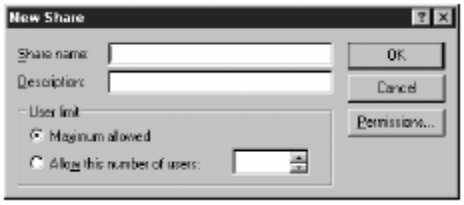
Lúc này, các người dùng trên mạng có thể truy cập đến thư mục chia sẻ và các file/thư mục bên trong nó nếu họ có Cấp phép truy cập thích hợp.

Chia sẻ ổ đĩa bằng cách sử dụng Windows Explorer

Bạn có thể tạo ra một chia sẻ cho ổ đĩa cụ thể bằng cách sử dụng Windows Explorer nhưng tiến trình thực hiện có khác đôi chút so với thông thường do sự tồn tại của chia sẻ quản trị trên mỗi ổ đĩa. Khi bạn lựa chọn ổ đĩa trong Windows Explorer và nhấp vào thẻ ***Sharing***, bạn sẽ thấy một giao diện như hình vẽ 9-7.

Hình 9-7: Một ổ đĩa chia sẻ

Ở đây, bạn có thể thấy lựa chọn ***Share This Folder*** đã được lựa chọn và tên của chia sẻ quản trị xuất hiện trong hộp văn bản ***Share Name***. Nếu bạn muốn gán Cấp phép truy cập cho người sử dụng nhưng không muốn xung đột với tính bảo mật của chia sẻ quản trị, bạn phải tạo ra một chia sẻ thứ hai tại mức gốc của ổ đĩa. Để thực hiện công việc này, bạn nhấp ***New Share*** để hiển thị hộp thoại ***New Share*** như hình vẽ 9-8.



Hình 9-8: Hộp thoại New Share

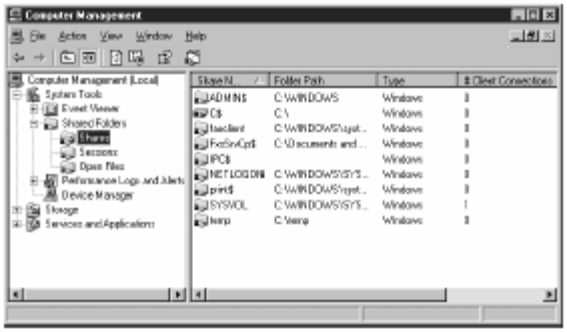
Trong hộp thoại này, bạn xác định một tên mới chia sẻ, mô tả về nó, giới hạn số lượng người sử dụng, các Cấp phép chia sẻ giống như bạn tạo một thư mục chia sẻ lúc trước. Khi bạn nhấp vào ***OK***, chia sẻ mới được tạo ra và được đưa vào hộp danh sách số ***Share Name*** trong thẻ ***Sharing***. Bây giờ bạn có thể lựa chọn bất kỳ chia sẻ mức gốc nào từ hộp liệt kê thả để phục vụ cho công tác quản trị. Bất kể bạn lựa chọn chia sẻ nào thì nó cũng được kiểm soát bởi các thông số: giới hạn về người sử dụng, Cấp phép và các thiết lập về cơ chế không kết nối.

Tạo thư mục chia sẻ bằng cách sử dụng snap-in Shared Folders

Sử dụng Windows Explorer là một phương pháp thuận tiện để tạo các thư mục chia sẻ nhưng nó cũng có một nhược điểm: bạn chỉ có thể tạo ra các chia sẻ khi bạn đang làm việc trên chính máy tính đó. Bạn không thể lựa

chọn các thư mục trên các máy tính khác và chia sẻ nó. Tuy nhiên, Windows Server 2003 cho phép bạn thực hiện điều đó nhờ công cụ ***Shared Folders,*** một dang snap-in MMC.

Snap-in ***Shared Folders*** được tích hợp vào trong màn hình quản trị Windows Server 2003 như trên hình vẽ 9-9. Bạn cũng có thể tạo một màn hình quản trị MMC tùy biến chứa ***Shared Folders*** và bất kỳ snap-in nào mà bạn muốn. Nhấp vào thư mục con ***Shares*** của snap-in sẽ hiển thị một danh sách các chia sẻ hiện tại trên máy tính kể cả những chia sẻ ẩn không hiển thị trong Windows Explorer.

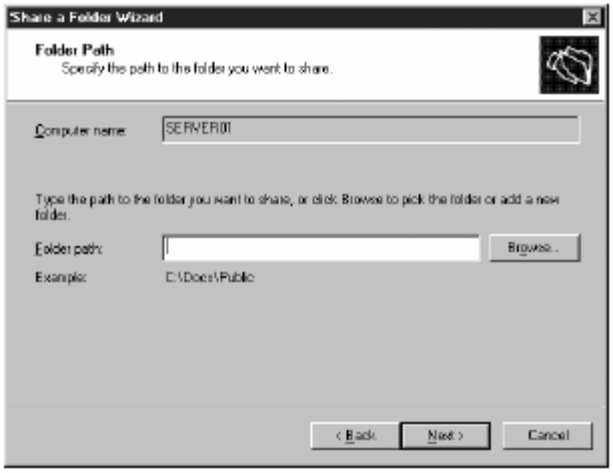


Hình 9-9: Snap-in Shared Folders

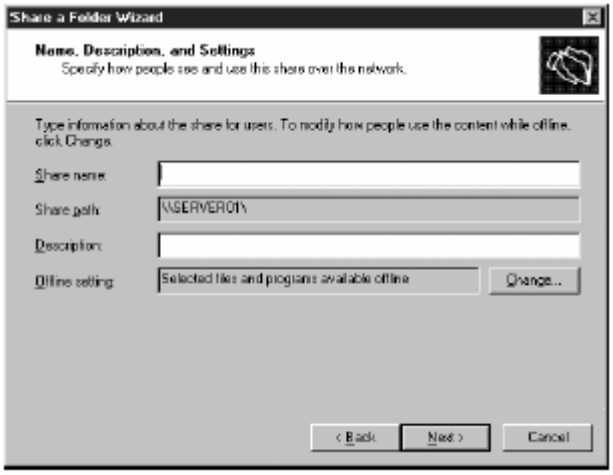
> ***CHÚ Ý Quản lý các chia sẻ từ xa*** *Để quản trị một máy tính khác trên mạng, lựa chọn biểu tượng* ***Computer Management (Local)****, tiếp theo trên thực đơn* ***Action*** *lựa chọn* ***Connect To Another Computer****. Nhập tên máy tính mà bạn muốn quản trị và nhấp OK. Sau đó, bạn có thể tạo và quản trị các chia sẻ trên máy tính khác như thể bạn đang làm việc trên máy tính đó.*

Để tạo một chia sẻ mới lựa chọn thư mục con ***Shares*** và trên thực đơn ***Action*** lựa chọn ***New Share*** để khởi tạo Trình hướng dẫn ***Share A Folder***. Trình hướng dẫn này bao gồm 03 trang:

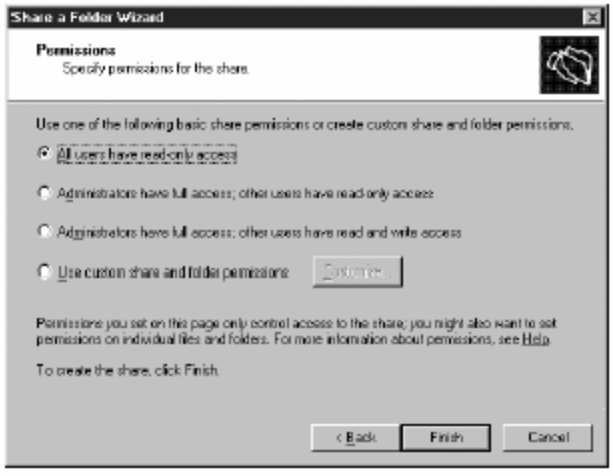
- **Folder Path** (*đường dẫn thư mục*) xác định đường dẫn tới thư mục mà bạn muốn chia sẻ



- **Name, Description, And Settings** (*tên, mô tả và các thiết lập*) xác định tên và mô tả dành cho chia sẻ. Bạn cũng có thể nhấp ***Change*** để cấu hình các thiết lập không kết nối cho chia sẻ.



- **Permissions** (*các Cấp phép*) lựa chọn Cấp phép mà bạn muốn gán cho thư mục chia sẻ.



Kết thúc Trình hướng dẫn, hệ thống sẽ đưa chia sẻ mới vào danh sách.

Tạo một hệ thống file chia sẻ bằng cách sử dụng Net.exe

Windows Server 2003 cho phép bạn tạo chia sẻ từ chế độ dòng lệnh bằng cách sử dụng chương trình ***net.exe*** với câu lệnh con ***share***. Cú pháp câu lệnh như sau:

net share <tên chia sẻ>=<ổ đĩa>:\<đường dẫn> [<các tham số>]

Các tham số mà bạn có thể đưa vào trong câu lệnh bao gồm:

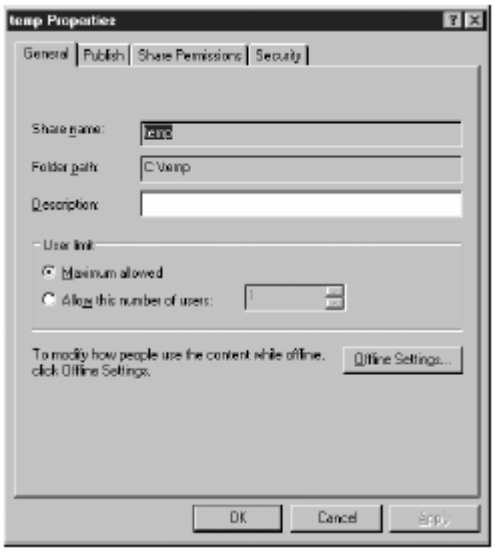
- **/grant:<đối tượng bảo mật>, [read|change|full]** gán cho một đối tượng bảo mật Cấp phép ***Read*** (*đọc*), ***Change*** (*thay đổi*) hoặc ***Full Control*** (toàn quyền điều khiển) đối với thư mục chia sẻ.
- **/users:<số lượng>** xác định số lượng lớn nhất người sử dụng có thể truy cập đồng thời đến thư mục chia sẻ.
- **/unlimited** không hạn chế số lượng người sử dụng truy cập đến thư mục chia sẻ.
- **/cache:[manual|documents|programs|none]** cấu hình các thiết lập không kết nối dành cho thư mục chia sẻ.

Ví dụ dưới đây minh họa việc tạo một thư mục chia sẻ ***Documents*** nằm trong thư mục ***C:\Docs*** và gán cho nhóm ***Users*** Cấp phép ***Read***:

net share documents=c:\docs /grant:users. read

QUẢN LÝ CÁC THƯ MỤC CHIA SẺ

Khi bạn đã tạo các hệ thống file chia sẻ, bạn có thể quản lý chúng bất cứ lúc nào với Windows Explorer, bằng cách sử dụng thẻ ***Sharing*** của hộp thoại ***Properties*** mà bạn đã sử dụng để chia sẻ. Bạn cũng có thể lựa chọn chia sẻ trong snap-in ***Shared Folders*** khi đó trong thực đơn ***Action,*** lựa chọn ***Properties*** để hiển thị hộp thoại trên hình 9-10.



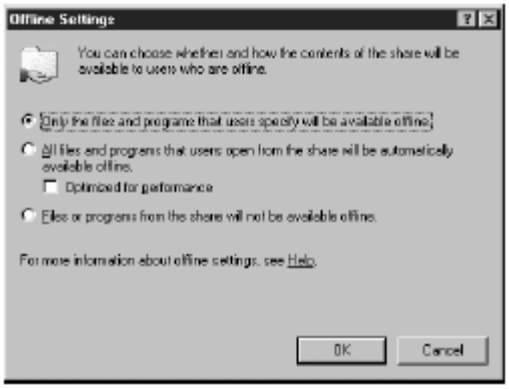
Hình 9-10: Hộp thoại Properties của thư mục chia sẻ

Hơn nữa, để có thể thay đổi các đặc tính chia sẻ đã được thiết lập trong quá trình tạo chia sẻ chẳng hạn như giới hạn người dùng hoặc miêu tả, bạn cũng có thể cấu hình các tính năng được mô tả trong các phần dưới đây.

Kiểm soát **lưu trữ không kết nối (*offline*)**

Bảo mật thường là một vấn đề quan trọng đối với hệ thống chia sẻ dữ liệu. Bạn muốn các file lưu trên thư mục chia sẻ luôn luôn sẵn sàng đối với những người sử dụng thích hợp và chỉ những người dùng đó mà thôi. Người quản trị có thể dùng các Cấp phép để kiểm soát ai sẽ là người có thể truy cập đến các thư mục chia sẻ nhưng anh ta không thể làm như vậy đối với các file đang được sử dụng. Một phương án cho phép khắc phục tình trạng này đó là giới hạn tính năng ***Offline Files*** (*các file ở chế độ không kết nối*) của người dùng truy cập tới các chia sẻ.

Khi bạn nhấn vào lựa chọn ***Offline Settting*** trong hộp thoại ***Properties*** của chia sẻ, bạn sẽ thấy hộp thoại như trên hình vẽ 9-11. Ở đây bạn có thể lựa chọn các máy tính trạm khi truy cập vào chia sẻ có được phép lưu thông tin vào bộ nhớ đệm thông qua tính năng ***Windows Offline Files*** hay không.



Hình 9-11: Hộp thoại Offline Settings

Trên Windows Server 2003, Microsoft Windows XP, và Microsoft Windows XP, ***Offline Files*** là cơ chế nhằm duy trì một phiên bản của các file nằm trên máy tính của người sử dụng khi họ truy cập trên mạng. Nếu liên kết mạng của các máy trạm tới máy chủ bị mất hay đứt, người dùng vẫn có thể tiếp tục làm việc với các phiên bản này của các file. Khi kết nối được thiết lập lại, máy trạm sẽ cập nhật những thay đổi trên phiên bản ***offline*** lên phiên bản gốc của các file nằm trên thư mục chia sẻ.

Vấn đề phát sinh với các file ***offline*** đó là các phiên bản nằm trên máy tính cục bộ không có Cấp phép bảo vệ như các file gốc nằm trên thư mục chia sẻ. Các file nhạy cảm mặc dù được bảo vệ cẩn mật trên thư mục chia sẻ nhưng khi được lưu trữ tại các máy trạm lại không được bảo vệ tí nào. Lựa chọn trong hộp thoại ***Offline Settings*** sẽ cho phép người quản trị quyết định có cho phép các máy trạm lưu các phiên bản ***offline*** của các file hay không với tính năng ***Offline Files***. Lựa chọn này được miêu tả như sau:

> ***CHÚ Ý***: ***Sử dụng Net.exe*** *Bạn cũng có thể cấu hình các thiết lập* ***offline*** *từ dòng lệnh, bằng cách sử dụng chương trình* ***Net.exe*** *với câu lệnh con* ***share****. Các thông số dòng lệnh tương ứng với các lựa chọn trong hộp thoại* ***Offline Settings*** *được liệt kê dưới đây.*

- **Only The Files And Programs That Users Specify Will Be Available Offline** (*Chỉ các file và chương trình mà người sử dụng xác định mới có thể dùng* ***offline***): cho phép người dùng lựa chọn tài liệu và các chương trình được lưu trữ ***offline*** trên các máy trạm của người sử dụng. Các tham số dòng lệnh cho ***Net.exe*** là ***/cache:manual***
- **All Files And Programs That Users Open From The Share Will Be Automatically Available Offline** (*Tất cả các file và chương trình mà người sử dụng mở từ thư mục chia sẻ sẽ tự động* ***offline***)

Tự động lưu tất cả tài liệu chia sẻ ***offline*** trên các máy trạm của người sử dụng. Đánh dấu chọn tại hộp kiểm tra ***Optimized For Performance*** sẽ tự động ghi vào bộ nhớ đệm tất cả các chương trình dùng để thực thi nội bộ trên máy trạm. Các tham số dòng lệnh cho ***Net.exe*** là ***/cache:documents*** *và* ***/cache:programs***.

- **Files And Programs From The Share Will Not Be Available Offline** (*Các file và chương trình trên thư mục chia sẻ sẽ không được dùng ở cơ chế* ***offline***) Ngăn không cho tất cả các tài liệu và các file thực thi được lưu trữ ***offline*** trên máy trạm. Các thông số dòng lệnh tương ứng cho ***Net.exe*** là ***/cache:none***.

Công bố các thư mục chia sẻ trong Active Directory

Khi bạn nhấn thẻ ***Publish*** trên hộp thoại ***Properties*** của thư mục chia sẻ trong snap-in ***Shared Folders*** (xem hình 9-12), thẻ này sẽ cho phép bạn công bố các thư mục chia sẻ trên ***Active Directory***. Công bố các thư mục chia sẻ trên ***Active Directory*** không có nghĩa là lưu chúng trong cơ sở dữ liệu của ***Active Directory*** mà nó sẽ tạo ra một đối tượng thư mục chia sẻ trỏ đến vị trí thực sự của thư mục này ở trên mạng. Khi thư mục chia sẻ được công bố, người dùng có thể tìm kiếm nó trên ***Active Directory*** bằng cách sử dụng ngay công cụ ***Active Directory Users and Computers***.

Hình 9-12: Thẻ Publish trong hộp thoại Properties của thư mục chia sẻ

Để công bố một thư mục chia sẻ trên ***Active Directory***, bạn cần lựa chọn hộp kiểm tra ***Publish This Share In Active Directory*** và cung cấp tên của người sở hữu thư mục chia sẻ đó. Bạn cũng có thể cung cấp các từ khóa miêu tả

nội dung đối tượng chia sẻ nhằm tăng tính hiệu quả của quá trình tìm kiếm thông tin.

Quản lý các Cấp phép chia sẻ

Như đã đề cập ở trong chương trước, các đối tượng chia sẻ đều có các hệ thống Cấp phép riêng cho phép ai được phép truy cập chúng. Để xác định Cấp phép cho các thư mục chia sẻ, bạn có thể dùng một trong các giao diện sau:

- Trong Windows Explorer, mở hộp thoại ***Properties*** của thư mục và nhấn ***Permissions*** trong phần thẻ ***Sharing***.
- Trong snap-in ***Shared Folders***, mở hộp thoại ***Properties*** của thư mục chia sẻ và chọn thẻ ***Share Permissions***.

CHÚ Ý: Mục tiêu của kỳ thi *Môn thi 70-290 yêu cầu học viên có thể "quản lý các Cấp phép chia sẻ thư mục"*

Bất kể bạn dùng phương pháp nào, bạn đều thấy giao diện như trên hình 9-13.

Hình 9-13: Thẻ Share Permissions trong hộp thoại Properties của thư mục chia sẻ

Hệ thống phân Cấp phép cho các chia sẻ là một trong những hệ thống đơn giản nhất trong Windows Server 2003. Trong trường hợp này, không có sự phân biệt giữa các Cấp phép Chuẩn và Cấp phép Đặc biệt mà chỉ có 3 Cấp phép đơn giản như sau:

- **Read** (*Đọc*): Người dùng có thể hiển thị tên thư mục, tên file, nội dung file và các thuộc tính. Người dùng cũng có thể thực thi các file chương trình (ví dụ các file .exe, .com,….) và truy cập tới các thư mục khác trong thư mục chia sẻ.
- **Change** (*Thay đổi*): Người dùng có thể tạo các thư mục, thêm file vào thư mục, thay đổi nội dung của file, thêm dữ liệu vào file, thay đổi thuộc tính file, xóa thư mục và file cũng như thực hiện các hoạt động cho phép trên Cấp phép ***Read***.
- **Full Control** (*Toàn quyền điều khiển*): người dùng có thể thay đổi các Cấp phép truy cập file, chiếm Cấp phép sở hữu file và thực hiện mọi công việc cho phép trên Cấp phép ***Change***.

Để thiết lập các Cấp phép truy cập, nhấp vào ***Add***, lựa chọn đối tượng bảo mật (như người dùng, nhóm hoặc máy tính) rồi xác định các Cấp phép mà bạn cho phép hay ngăn cấm đối với các đối tượng đó. Bạn có thể chọn các đối tượng đã có sẵn trong danh sách ***Group Or User Names*** để thay đổi các Cấp phép theo ý muốn.

Sử dụng các Cấp phép chia sẻ

Các Cấp phép chia sẻ là một dạng của điều khiển truy cập nhưng chỉ cung cấp một cách hạn chế khả năng bảo vệ cho các file chia sẻ. Một vài hạn chế của các Cấp phép chia sẻ bao gồm:

- **Phạm vi bị giới hạn**: các Cấp phép chia sẻ chỉ áp dụng cho các truy cập tới file và folder qua mạng. Các Cấp phép chia sẻ này không ngăn chặn được khả năng truy cập của người sử dụng khi họ làm việc ngay trên máy tính chứa thư mục này hoặc truy cập đến máy tính bằng các công cụ khác như: ***Web, FTP, Telnet*** và các ứng dụng ***Terminal Server***.
- **Thiếu tính mềm dẻo**: Các Cấp phép truy chia sẻ không có tính mềm dẻo. Chúng chỉ cung cấp một phương tiện chia sẻ đơn giản với ba lựa chọn, được ứng dụng cho mọi file và thư mục bên dưới thư mục chia sẻ. Bạn không thể thay đổi Cấp phép chia sẻ cho các thư mục hoặc file cụ thể bên trong thư mục chia sẻ.
- **Không thể sao chép**: các Cấp phép chia sẻ không thể sao chép bằng dịch vụ sao chép file (FRS - ***File Replication Service***)
- **Không có tính phục hồi**: Các Cấp phép chia sẻ không thể sao lưu được hoặc phục hồi khi xảy ra mất mát dữ liệu.

- **Dễ mất**: Các Cấp phép chia sẻ sẽ bị mất khi bạn di chuyển hay đổi tên thư mục đang chia sẻ.
- **Không kiểm soát (*Audit*)**: Bạn không thể cấu hình sự kiểm soát dựa trên các Cấp phép chia sẻ.

Ưu điểm duy nhất của các Cấp phép chia sẻ là đơn giản hóa hệ thống và chúng luôn sẵn sàng đối với mọi hệ thống file được Windows Server 2003 hỗ trợ. Trong ổ đĩa dùng hệ thống file FAT, các Cấp phép chia sẻ là cách duy nhất để quản lý sự truy cập vào đĩa.

Trong các mạng nhỏ với ít các yêu cầu bảo mật, Cấp phép chia sẻ có thể là một giải pháp chấp nhận được. Tuy nhiên trong hầu hết các trường hợp, người quản trị mạng sẽ lựa chọn các Cấp phép linh hoạt và mạnh mẽ hơn được cung cấp bởi hệ thống file NTFS. Nếu bạn lựa chọn giải pháp này, cần chú ý đến các điểm sau:

- Hệ thống Cấp phép chia sẻ sẽ vẫn có bất kể bạn có dùng NTFS hay không
- Hệ thống Cấp phép chia sẻ là hoàn toàn độc lập đối với hệ thống Cấp phép NTFS
- Cả hai hệ thống Cấp phép này đều có thể áp dụng trên cùng một đối tượng.

Do đó, cách tốt nhất để sử dụng Cấp phép NTFS để quản lý truy cập là cho tất cả người sử dụng (được biết đến thông qua nhóm ***Everyone***) Cấp phép ***Full Control*** trên tất cả các thư mục chia sẻ. Điều này sẽ tránh mọi xung đột giữa hai hệ thống Cấp phép. Nghĩa là bạn nên sử dụng một trong hai Cấp phép nói trên để quản lý file nhưng không nên dùng đồng thời cả hai.

Nếu không dùng cách này, Cấp phép Hiệu dụng người dùng nhận được là sự kết hợp Cấp phép của cả hai hệ thống. Ví dụ nếu bạn gán Cấp phép chia sẻ Đọc (***Read***) và Cấp phép NTFS là toàn quyền điều khiển (***Full Control***) cho nhóm ***Users*** thì tổng hợp lại người sử dụng sẽ chỉ nhận được các giới hạn do Cấp phép chia sẻ cung cấp. Điều này, cùng với sự phức tạp khi thừa kế, thành viên nhóm, các Cấp phép bị từ chối có thể sẽ gây nên một cơn ác mộng.

Một trong những nguyên nhân thông thường nhất đối với việc truy cập hệ thống file chia sẻ là xung đột giữa Cấp phép chia sẻ và Cấp phép NTFS. Khi giải quyết các vấn đề như thế này, cần kiểm tra cả hai loại Cấp phép để chắc chắn người dùng nhận được Cấp phép truy cập tới file họ cần.

> ***THÔNG TIN THÊM:*** *Lợi ích và khả năng của hệ thống Cấp phép NTFS sẽ được miêu tả chi tiết ở phần sau của chương này.*

Cấp phép chia sẻ mặc định

Tất cả các hệ điều hành windows trước đây cho đến Windows 2000, khi tạo ra một thư mục chia sẻ mới mặc định Cấp phép ***Full Control*** sẽ được gán cho tất cả người dùng (***Everyone***). Điều này khiến các chia sẻ được là mở toang theo quan điểm bảo mật, dễ dàng hơn cho người quản trị khi lên kế hoạch các Cấp phép NTFS, nhưng gây khó khăn cho những người muốn dùng các Cấp phép chia sẻ. Kể từ Windows XP trở đi , các Cấp phép mặc định cho các file chia sẻ đã được thay đổi. Windows XP và Windows 2003 Server gán Cấp phép ***Read*** cho nhóm đồng nhất đặc biệt ***Everyone*** và trao Cấp phép ***Full Control*** cho nhóm quản trị ***Administrators*** . Điều này có nghĩa nếu muốn dùng các Cấp phép NTFS để kiểm soát truy cập, bạn phải nhớ thay đổi bằng cách gán Cấp phép ***Full Control*** cho nhóm ***Everyone***.

Tạo chiến lược cho hệ thống file chia sẻ

Chiến lược đơn giản nhất cho hệ thống file chia sẻ là chia sẻ thư mục gốc của các ổ đĩa (***volume***) trên mọi máy tính trên mạng. Tuy nhiên có hai lý do khiến đây là một phương pháp tồi:

- **Gây nhầm lẫn**: Khi người dùng gặp các chia sẻ khác nhau thể hiện cho các ổ đĩa trên các máy tính khác nhau, sẽ rất khó khăn cho họ để tìm ra đâu là file mà họ muốn tìm. Người dùng có thể phải tìm kiếm qua một vài hệ thống khác nhau trước khi họ có thể xác định đúng vị trí file cần tìm. Thậm chí với một ổ đĩa lớn duy nhất, chia sẻ từ thư mục gốc có thể dẫn tới cấu trúc thư mục lớn và phức tạp.
- **Bảo mật**: chia sẻ toàn bổ ổ đĩa, đặc biệt là các ổ đĩa hệ thống sẽ cho phép người dùng có Cấp phép truy cập tới rất nhiều file và thư mục mà họ không nên nhìn thấy. Người dùng thông thường không cần truy cập tới các file hệ thống và ứng dụng trên các máy tính khác, họ có thể gây hư hỏng nếu vô tình xóa mất một file hay thư mục cần thiết.

Giải pháp cho vấn đề này là tạo chia sẻ đối với thư mục xác định chứ không phải trên cả ổ đĩa. Trên thực tế, snap-in ***Shared Folders*** sẽ hiển thị một hộp thoại cảnh báo khi bạn cố gắng chia sẻ một ổ đĩa nào đó vì lý do bảo mật. Các file thường được truy cập qua mạng là các file tài liệu và dữ liệu. Do đó, bạn nên tổ chức các cấu trúc thư mục trên hệ thống sao cho các tài liệu và

các file chia sẻ được lưu trên thư mục có tên riêng và tạo các Cấp phép chia sẻ trên các thư mục này.

Chia sẻ các ổ đĩa di động

Một ngoại lệ đối với chiến lược trên là khi bạn chia sẻ file trên các ổ đĩa di động như: CD-ROM, DVD-ROM hay các ổ băng. Không có gì ngăn cản bạn thực hiện công việc chia sẻ một thư mục trên các ổ đĩa này nhưng cần nhớ rằng chia sẻ sẽ chỉ có hiệu lực khi đĩa hoặc băng lưu thư mục nằm trong ổ. Chia sẻ gốc của các ổ này cho phép bạn hoán đổi các phương tiện theo ý muốn mà vẫn đảm bảo tính sẵn sàng của thư mục chia sẻ.

Lồng các chia sẻ

Như đã được đề cập ở trên, bạn có thể chia sẻ bất kỳ thư mục nào trên ổ đĩa, thậm chí cả các thư mục nằm trong các thư mục đã được chia sẻ. Ví dụ: bạn có thể chia sẻ ổ đĩa D với tên chia sẻ ***D***, sau đó tạo ra một thư mục chia sẻ khác ***D:\docs*** với tên chia sẻ ***Docs***. Hai đối tượng này có thể có các Cấp phép truy cập khác nhau. Tuy nhiên bạn cần nhớ rằng mặc dù các thư mục chia sẻ lồng vào nhau trên Windows Explorer nhưng đối với người dùng trên mạng thì chúng vẫn là hai đối tượng chia sẻ riêng biệt và hoàn toàn độc lập. Hơn nữa, các Cấp phép cho hai đối tượng cũng riêng biệt. Ví dụ như nếu bạn gán cho người dùng Cấp phép ***Full Control*** trên D và chỉ cho Cấp phép ***Read*** trên ***Docs***, sự giới hạn Cấp phép truy cập trên thư mục ***D:\docs*** qua đối tượng ***Docs*** không ảnh hưởng tới Cấp phép điều khiển toàn bộ của họ khi truy cập tới thư mục đó dùng đối tượng ***D.***

SỬ DỤNG CÁC CẤP PHÉP NTFS

Windows 2003 Server hỗ trợ hai hệ thống file chính: FAT và NTFS. Hệ thống file FAT được phát triển từ hệ điều hành MS-DOS cung cấp các chức năng cơ bản nhưng có rất ít các tính năng dành cho lưu trữ trên mạng. Thuận lợi duy nhất khi sử dụng các ổ đĩa FAT đó là bạn có thể khởi động máy tính bằng đĩa khởi động MS-DOS và vẫn có thể truy cập được tới chúng. Hệ thống file NTFS được giới thiệu đầu tiên trên Microsoft Windows NT 3.1 bao gồm một số các tính năng thuận tiện cho người quản trị mạng. Tính năng quan trọng nhất mà NTFS mang lại đó là cho phép bạn cung cấp các Cấp phép một cách chi tiết đến tất cả các file và thư mục trên ổ đĩa.

> ***CHÚ Ý: Mục đích của kỳ thi:*** *Mục đích của môn thi 70-290 yêu cầu học viên có thể "cấu hình Hệ thống cấp phép file"*

Mọi file và thư mục trên ổ đĩa NTFS có một ACL chứa các ACE, liệt kê các đối tượng bảo mật được gán Cấp phép trên các file/thư mục đó. Khi người dùng truy cập tới một file hoặc thư mục, hệ thống sẽ so sánh thẻ truy cập bí mật của người sử dụng (chứa các nhận dạng bảo mật (SIDs) của tài khoản người dùng) với các SID trong các ACE của ACL (các SID này là của các nhóm mà người dùng là thành viên). Một khi người sử dụng đã được xác thực, Cấp phép truy cập tới file/folder sẽ được cấp.

So với Cấp phép chia sẻ được đề cập trong chương trước, Cấp phép NTFS có rất nhiều ưu điểm bao gồm:

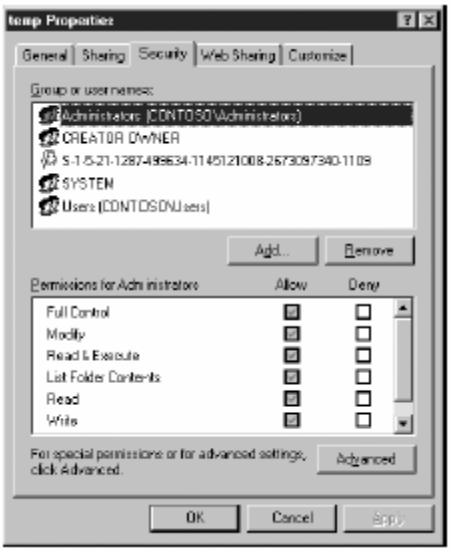
- **Phạm vi (scope)**: các Cấp phép NTFS áp dụng trên file và thư mục bất kể phương pháp mà nó được truy cập. Người dùng truy cập cục bộ hay kết nối qua mạng bằng bất cứ phương tiện nào đều bị quản lý bởi các Cấp phép giống nhau.
- **Tính linh hoạt (Flexibility)**: NTFS cung cấp một danh sách dài các Cấp phép đặc biệt, chúng có thể kết hợp lại với nhau để tạo nên các Cấp phép chuẩn, đều có thể áp dung cho bất cứ file/folder nào trên ổ đĩa. Đồng thời NTFS cho phép điều khiển toàn bộ thông qua tính kế thừa Cấp phép.
- **Tính sao chép (replication)**: Cấp phép NTFS được sao chép bởi FRS.
- **Tính giữ nguyên trạng thái (resilience)**: khi sao lưu hay khôi phục dữ liệu trên một ổ đĩa, các Cấp phép NTFS cũng được đính kèm. Vì vậy bạn không phải lo lắng về việc sửa chữa lại các Cấp phép NTFS khi có sự cố xảy ra.
- **Không thay đổi (Less fragile)**: Cấp phép NTFS sẽ không bị mất nếu bạn di chuyển hay đổi tên file/folder có các Cấp phép đang áp dụng (miễn là file hay thư mục vẫn nằm trên cùng ổ NTFS)
- **Khả năng kiểm định (*Audit*)**: bạn có thể giám sát và ghi lại quá trình truy cập tới các file/folder NTFS của các đối tượng bảo mật.

Làm việc với các Cấp phép NTFS phức tạp hơn nhiều so với Cấp phép chia sẻ, nhưng với các tính năng bảo vệ mà nó đem lại thì NTFS thực sự là một công cụ tuyệt vời cho người quản trị mạng.

Quản trị các Cấp phép NTFS chuẩn

Hầu như người quản trị mạng đều làm việc với các Cấp phép NTFS chuẩn vì nó cung cấp đủ tính linh hoạt để kiểm soát truy cập tới các file/folder chia sẻ. Trong Windows Explorer, mọi file và thư mục trên ổ đĩa NTFS đều có

hộp thoại ***Properties*** với thẻ ***Security*** như trên hình 9-14, bạn có thể dùng để thiết lập các Cấp phép NTFS chuẩn cho file/folder đó cũng như truy cập tới các Cấp phép điều khiển phức tạp hơn được thảo luận ở phần dưới của chương này.



Hình 9-14: Thẻ Security của một thư mục NTFS.

> ***CHÚ Ý**: **Quản trị NTFS từ xa** Windows Explorer có khả năng cấu hình các Cấp phép NTFS cho bất cứ file hay thư mục nào trên mạng miễn là người sử dụng có các đặc quyền phù hợp. Điều này trái ngược với Cấp phép chia sẻ của Windows Explorer, chỉ dùng được trong các hệ thống file cục bộ.*

Quá trình gán các Cấp phép NTFS chuẩn cho file/folder tương tự như việc gán các Cấp phép chia sẻ. Bạn phải chọn đối tượng chia sẻ trong danh sách "***Group Or User Names***" hay nhấp "***Add***" để thêm đối tượng bảo mật mới. Tiếp theo bạn phải lựa chọn các hộp kiểm tra ***Allow*** (*cho phép*) hay ***Deny*** (*cấm*) trên các Cấp phép mà bạn muốn cung cấp cho đối tượng trong hộp ***Permissions***. Các Cấp phép NTFS chuẩn và các công việc mà bạn có thể thực hiện được với các Cấp phép đó được liệt kê trên bảng 9-1.

> ***CHÚ Ý: Các Cấp phép trên file/folder** Có một sự khác biệt nhỏ giữa Cấp phép được gán một file và thư mục. Cấp phép **List Folder Contents** (liệt kê nội dung thư mục) không áp dụng cho file.*

Bảng 9-1: Các Cấp phép NTFS chuẩn

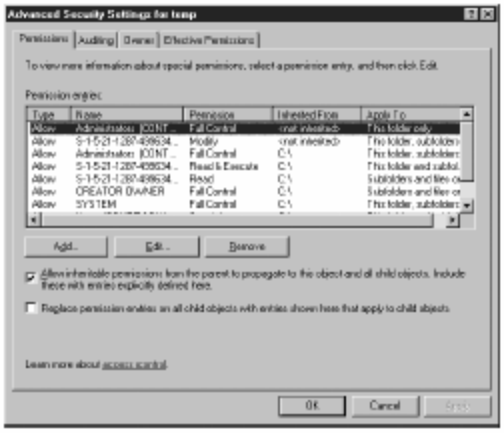
Cấp phép NTFS chuẩn	Khi gán cho một thư mục, cho phép chủ thể bảo mật:	Khi gán cho một file, cho phép chủ thể bảo mật:
Read	■ Xem các file và các thư mục con trong thư mục đó. ■ Xem chủ sở hữu, các Cấp phép và các đặc tính của thư mục.	■ Đọc nội dung file ■ Xem chủ sở hữu, các Cấp phép và các đặc tính của file.
Read and Excute	■ Cho phép đi qua các thư mục bị ngăn cản để tới các file và thư mục khác. ■ Cho phép thực hiện tất cả các chức năng do Cấp phép ***Read*** và ***List Folder Contents*** cung cấp.	■ Cho phép thực hiện tất cả các chức năng do Cấp phép ***Read*** cung cấp. ■ Chạy các ứng dụng
Write	■ Tạo các file và các thư mục con mới bên trong một thư mục. ■ Thay đổi các đặc tính thư mục. ■ Xem chủ sở hữu và các Cấp phép trên thư mục	■ Cho phép ghi đè lên file ■ Thay đổi các đặc tính của file ■ Xem chủ sở hữu và các Cấp phép trên file
Modify	■ Xóa thư mục ■ Cho phép thực hiện tất cả các chức năng do Cấp phép ***Write*** và Cấp phép ***Read***	■ Thay đổi file ■ Xóa file ■ Cho phép thực hiện tất cả các chức năng do Cấp phép ***Write*** và

	and Excute cung cấp.	Cấp phép ***Read and Excute*** cung cấp.
List Folder Contents	■ Xem các tên của các file và các thư mục con chứa trong thư mục cha.	■ Không áp dụng
Full Control	■ Thay đổi các Cấp phép trên thư mục ■ Chiếm Cấp phép sở hữu thư mục ■ Xóa các thư mục con và các file nằm trong thư mục cha ■ Cho phép thực hiện tất cả các chức năng do tất cả các Cấp phép NTFS khác cung cấp.	■ Thay đổi các Cấp phép trên file ■ Chiếm Cấp phép sở hữu file ■ Cho phép thực hiện tất cả các chức năng do tất cả các cấp phép NTFS khác cung cấp.

CHÚ Ý: Các Cấp phép thừa kế *Khi hộp kiểm tra trong thẻ* ***Security*** *được chọn và có màu xám, có nghĩa là Cấp phép này được kế thừa từ thư mục cha.*

Sử dụng các thiết lập bảo mật nâng cao

Giao diện cơ bản trong thẻ ***Security*** cho phép người quản trị thiết lập các Cấp phép thông thường nhanh chóng và dễ dàng nhưng nó không cung cấp nhiều thông tin hay cung cấp đủ công cụ để sử dụng hết các tính năng của hệ thống file NTFS. Nhấn vào nút ***Advanced*** trong hộp thoại ***Advanced Security Settings*** (hình vẽ 9-15) bạn sẽ thu được giao diện tương tự như bạn xem ACL thực sự của file hay thư mục trong giao diện đồ họa của Windows.



Hình vẽ 9-15: Hộp thoại Advanced Security Settings

Thẻ ***Permissions*** mặc định của hộp thoại ***Advanced Security Settings*** chứa một danh sách các mục vào Cấp phép, về cơ bản đây là một danh sách của các ACE riêng lẻ trong ACL của file/folder. Mỗi mục vào chứa các thông tin sau:

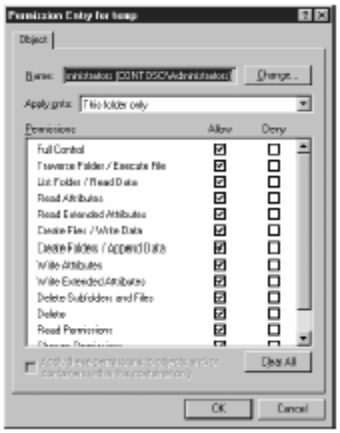
- **Type** (*loại*) Cho biết mục vào cho phép hay từ chối Cấp phép
- **Name** (*tên*) Cho biết tên của đối tượng bảo mật nhận các Cấp phép đó.
- **Permission** (*Cấp phép*): cho biết các Cấp phép NTFS chuẩn được gán cho đối tượng bảo mật. Nếu ACE được dùng để gán các Cấp phép đặc biệt, từ "***Special***" sẽ xuất hiện trong trường này.
- **Inherited From** (*kế thừa từ*) Cho biết Cấp phép có được kế thừa không và nếu có thì kế thừa từ đâu.
- **Apply to** (*áp dụng cho*) Cho biết Cấp phép này có được áp dụng cho các thư mục con hay các file bên trong nó hay không. Nếu có thì đó là những thư mục con hoặc file nào.

Danh sách các mục vào Cấp phép có thể chứa nhiều mục vào cho cùng một đối tượng. Điều đó có nghĩa rằng đối tượng nhận được nhiều Cấp phép từ các nguồn khác nhau ví dụ như có Cấp phép được gán trực tiếp cho đối tượng, có Cấp phép được kế thừa hoặc có thể có các đối tượng được thiết lập cả hai Cấp phép ***Allow*** và ***Deny***. Trong trường hợp này, mỗi mục vào trong danh sách được quản lý riêng biệt. Để làm việc với mỗi mục vào trong danh sách, bạn lựa chọn và nhấn ***Edit*** để mở hộp thoại ***Permission Entry***. Ngoài ra, chỉ có hai điều khiển được kích hoạt trong hộp thoại ***Advanced Security Settings*** cung cấp thêm hai lựa chọn:

- **Allow Inheritable Permissions From The Parent To Propagate To This Object And All Child Objects** (*cho phép các Cấp phép kế thừa từ đối tượng cha được truyền đến đối tượng này và tất cả các đối tượng con*): Xác định xem các file/folder có kế thừa Cấp phép từ đối tượng cha hay không. Mặc định hộp kiểm tra này được lựa chọn. Khi bạn loại bỏ lựa chọn này một thông báo sẽ xuất hiện cho phép hoặc xóa bỏ hoặc giữ lại các Cấp phép kế thừa từ thư mục cha xuống. Nếu bạn lựa chọn giữ lại, các Cấp phép ảnh hưởng vẫn được giữ nguyên nhưng file/folder không còn kế thừa Cấp phép từ thư mục cha nữa. Nếu bạn thay đổi các Cấp phép trên thư mục cha, file và các thư mục con sẽ không bị ảnh hưởng gì.
- **Replace Permission Entries On All Child Objects With Entries Shown Here That Apply To Child Objects** (*Thay thế* Mục vào Cấp phép *ở đây cho các đối tượng con*) Lựa chọn này làm cho các đối tượng con được thừa hưởng các Cấp phép từ thư mục này trừ các Cấp phép được gán riêng chúng. Hộp kiểm tra này chỉ áp dụng cho các thư mục.

Quản lý các Cấp phép đặc biệt

Khi bạn thay đổi một trong các Mục vào Cấp phép trong hộp thoại ***Advanced Security Settings*** hay thêm một Mục vào mới vào hộp thoại đó bạn đều nhận được hộp thoại ***Permission Entry*** được mô tả trong hình 9-16. Lần đầu tiên, bạn truy cập trực tiếp đến các Cấp phép đặc biệt tạo nên xương sống của hệ thống Cấp phép NTFS.



Hình 9-16: Hộp thoại Permission Entry

NTFS có 14 Cấp phép đặc biệt, chức năng của chúng được mô tả chi tiết ở dưới. Trong trường hợp các Cấp phép đặc biệt xuất hiện theo cặp và được

ngăn cách bởi một dấu chéo có nghĩa là Cấp phép đầu tiên sẽ được áp dụng cho thư mục và Cấp phép tiếp theo sẽ áp dụng cho file.

- **Traverse Folder/Execute File** (*duyệt thư mục/thực thi các file*) Cấp phép ***Traverse Folder*** cho phép hay ngăn cấm các đối tượng bảo mật khả năng di chuyển qua các thư mục mà họ không có Cấp phép truy cập, vì vậy họ có thể tới được file hay thư mục mà họ có Cấp phép. Cấp phép này chỉ áp dụng cho các thư mục. Cấp phép ***Execute File*** cho phép hay ngăn cấm các đối tượng chạy chương trình. Cấp phép này chỉ áp dụng cho file.
- **List Folder/Read Data** (*Liệt kê thư mục/Đọc dữ liệu*) Cấp phép ***List Folder*** cho phép hay ngăn cấm các đối tượng bảo mật khả năng hiển thị file và tên các thư mục con. Cấp phép này chỉ áp dụng vào các thư mục. Cấp phép ***Read Data*** cho phép hay ngăn cấm các đối tượng xem nội dung file. Cấp phép này chỉ áp dụng cho các file.
- **Read Attributes** (*Đọc thuộc tính*) Cho phép hay ngăn cấm các đối tượng bảo mật khả năng xem các thuộc tính NTFS của file hay thư mục.
- **Read Extended Attributes** (*Đọc thuộc tính mở rộng*) Cho phép hay ngăn cản các đối tượng bảo mật khả năng xem các thuộc tính mở rộng của file hay thư mục.
- **Create Files/Write Data** (*tạo các file/thay đổi nội dung*) Cấp phép ***Create Files*** cho phép hay ngăn cản đối tượng bảo mật khả năng tạo file trong thư mục. Cấp phép này chỉ áp dụng cho các thư mục. Cấp phép ***Write Data*** cho phép hay ngăn cấm đối tượng khả năng thay đổi nội dung file sẵn có. Cấp phép này chỉ áp dụng cho các file.
- **Create Folders/Append Data** (*Tạo thư mục/Chèn dữ liệu*) Cấp phép ***Create Folders*** cho phép hay ngăn cản đối tượng bảo mật khả năng tạo thư mục con trong một thư mục. Cấp phép này chỉ áp dụng cho các thư mục. Cấp phép ***Append Data*** cho phép hay ngăn cấm đối tượng khả năng thêm dữ liệu vào cuối file nhưng không được thay đổi nội dung sẵn có trong file. Cấp phép này chỉ áp dụng cho file.
- **Write Attributes (***thay đổi thuộc tính***)** Cho phép hay ngăn cấm đối tượng bảo mật khả năng thay đổi các thuộc tính NTFS của một file hay thư mục sẵn có.

- **Write Extended Attributes** (*thay đổi thuộc tính mở rộng*) Cho phép hay ngăn cấm đối tượng bảo mật khả năng thay đổi các thuộc tính mở rộng của một file hay thư mục sẵn có.
- **Delete Subfolders and Files** (*Xóa các thư mục con và file*) Cho phép hay ngăn cấm đối tượng bảo mật khả năng xóa các thư mục con và file thậm chí Cấp phép ***Delete*** không được gán các thư mục con hay file.
- **Delete** (*xóa*) Cho phép hay ngăn cấm đối tượng bảo mật khả năng xóa file hay thư mục.
- **Read Permissions** (*cho phép hiển thị các Cấp phép*) Cho phép hay ngăn cấm đối tượng bảo mật khả năng đọc các Cấp phép trên file hay thư mục.
- **Change Permissions** (*Thay đổi Cấp phép*) Cho phép hay ngăn cấm đối tượng bảo mật khả năng thay đổi các Cấp phép của file hay thư mục.
- **Take Ownership** (*Chiếm quyền sở hữu*) Cho phép hay ngăn cấm đối tượng bảo mật khả năng chiếm quyền sở hữu của file hay thư mục.
- **Synchronize** (*Đồng bộ*) Cho phép hay ngăn cấm các ***thread*** (*chuỗi*) khác nhau của một ***multithread*** (đa chuỗi), các chương trình đa xử lý có khả năng "chờ đợi" việc điều khiển file hay thư mục và đồng bộ nó với các ***thread*** khác thông báo cho nó.

Hộp thoại ***Permission Entries*** cho một ACE hiển thị các Cấp phép đặc biệt riêng rẽ mà về chức năng nó tương đương với các Cấp phép NTFS chuẩn được xác định trong hộp thoại ***Advanced Security Settings***. Các Cấp phép đặc biệt tạo nên sáu Cấp phép NTFS chuẩn được liệt kê trong bảng 9-2.

Bảng 9-2: Các Cấp phép NTFS chuẩn và các Cấp phép đặc biệt tương ứng

Cấp phép NTFS chuẩn	Các Cấp phép đặc biệt
Read	■ List Folder/Read Data (liệt kê thư mục/đọc dữ liệu) ■ Read Attributes (*đọc các đặc tính*) ■ Read Extended Attributes (*đọc các đặc*

	tính mở rộng) ■ Read Permissions (đọc các Cấp phép) ■ Synchronize (*đồng bộ*)
Read and Excute	■ List Folder/Read Data (liệt kê thư mục/đọc dữ liệu) ■ Read Attributes (*đọc các đặc tính*) ■ Read Extended Attributes (*đọc các đặc tính mở rộng*) ■ Read Permissions (đọc các Cấp phép) ■ Synchronize (*đồng bộ*) ■ Traverse Folder/Execute File (cho phép duyệt thư mục/thực thi file)
Modify	■ Create Files/Write Data (tạo các file/có khả năng ghi dữ liệu) ■ Create Folders/Append Data (tạo thư mục/thêm dữ liệu) ■ Delete (*xóa*) ■ List Folder/Read Data (liệt kê thư mục/đọc dữ liệu) ■ Read Attributes (*đọc các đặc tính*) ■ Read Extended Attributes (*đọc các đặc tính mở rộng*) ■ Read Permissions (đọc các Cấp phép) ■ Synchronize (*đồng bộ*) ■ Traverse Folder/Execute File (cho phép duyệt thư mục/thực thi file) ■ Write Attributes (thay đổi các đặc tính) ■ Write Extended Attributes (thay đổi các đặc tính mở rộng)
Write	■ Create Files/Write Data (tạo các file/có khả năng ghi dữ liệu)

	■ Create Folders/Append Data (tạo thư mục/có khả năng thêm dữ liệu) ■ Read Permissions (đọc các Cấp phép) ■ Synchronize (đồng bộ) ■ Write Attributes (thay đổi các đặc tính) ■ Write Extended Attributes (thay đổi các đặc tính mở rộng)
List Folder Contents	■ List Folder/Read Data (liệt kê thư mục/đọc dữ liệu) ■ Read Attributes (*đọc các đặc tính*) ■ Read Extended Attributes (*đọc các đặc tính mở rộng*) ■ Read Permissions (đọc các Cấp phép) ■ Synchronize (*đồng bộ*) ■ Traverse Folder/Execute File (cho phép duyệt thư mục/thực thi file)
Full Control	■ Change Permissions (thay đổi các Cấp phép) ■ Create Files/Write Data (tạo các file/có khả năng ghi dữ liệu) ■ Create Folders/Append Data (tạo thư mục/có khả năng thêm dữ liệu) ■ Delete (*xóa*) ■ Delete Subfolders and Files (xóa các thư mục con và các file) ■ List Folder/Read Data (liệt kê thư mục/đọc dữ liệu) ■ Read Attributes (*đọc các đặc tính*) ■ Read Extended Attributes (*đọc các đặc tính mở rộng*) ■ Read Permissions (đọc các Cấp phép)

- Synchronize (*đồng bộ*)
- Take Ownership (đoạt Quyền sở hữu)
- Traverse Folder/Execute File (cho phép duyệt thư mục/thực thi file)
- Write Attributes (thay đổi các đặc tính)
- Write Extended Attributes (thay đổi các đặc tính mở rộng)

Khi thay đổi một Mục vào Cấp phép, bạn có thể thay đổi bất kỳ thông số nào dưới đây:

- **Name** (*Tên*) Xác định tên của đối tượng bảo mật được gán Cấp phép. Khi bạn muốn thay đổi Cấp phép từ một đối tượng này sang một đối tượng khác, thay vì tạo ra một ACE mới, bạn có thể dùng giao diện này để thay đổi tên đối tượng được gán
- **Apply Onto** (*Gán cho*) Xác định đối tượng nào được gán Cấp phép bằng cách sử dụng các lựa chọn trên hình 9-17. Giao diện này cho phép bạn điều khiển hoàn toàn tính kế thừa các Cấp phép được gán cho một thư mục cha: cho các file, các thư mục, các thư mục con và các file sâu hơn nữa.

Hình 9-17: Các lựa chọn Apply Onto

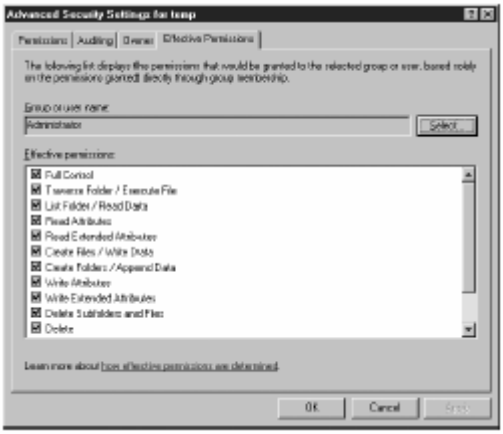
- **Permissions** (*Cấp phép*) Xác định các Cấp phép đặc biệt được gán cho các đối tượng bảo mật. Hộp danh sách ***Permissions*** bao gồm tất cả các Cấp phép đặc biệt có thể dùng được liệt kê ở trên cộng thêm Cấp phép NTFS chuẩn ***Full Control***.

CHÚ Ý: Sử dụng lựa chọn Apply Onto *Khi bạn sử dụng lựa chọn* ***Apply Onto*** *để giới hạn các đối tượng nhận Cấp phép kế thừa, tất cả*

*các thư mục con và file vẫn nhận được ACE từ thư mục cha. Để ngăn không cho các đối tượng con kế thừa chỉ cần ngăn không cho chúng nhận các Cấp phép trong ACE. Trường hợp ACE được kế thừa bởi một số lượng lớn các đối tượng con điều này sẽ ảnh hưởng tới hoạt động của mạng, khi đó sử dụng lựa chọn **Apply Onto** sẽ không phải là một giải pháp tốt để giới hạn kế thừa Cấp phép.*

Hiển thị các Cấp phép Hiệu dụng

Mặc dù hệ thống Cấp phép NTFS phức tạp nhưng rất may mắn là Windows Server 2003 chứa một cơ chế cho phép hiển thị Cấp phép Hiệu dụng của một đối tượng bảo mật trên một file hoặc thư mục xác định. Để xem các Cấp phép Hiệu dụng, hãy mở hộp thoại ***Advance Security Settings*** của file hoặc thư mục và chọn thẻ ***Effective Permissions*** như trên hình 9-18. Khi bạn nhấn ***Select*** và xác định tên của đối tượng bảo mật trong hộp thoại "***Select User, Computer, Or Group***" hộp kiểm tra trong danh sách ***Effective Permission*** sẽ thay đổi để hiển thị Cấp phép tổng hợp đối tượng đó nhận được.



Hình 9-18: Thẻ Effective Permissions của hộp thoại Advanced Security Settings

CHÚ Ý Mục tiêu của kỳ thi *Mục tiêu cho môn thi 70-290 yêu cầu học viên có thể "xác định Cấp phép Hiệu dụng khi gán Cấp phép"*

Mặc dù thẻ ***Effective Permissions*** rất thuận tiện để sửa các lỗi liên quan tới việc truy cập các file chia sẻ tuy nhiên nó cũng không được thật sự hoàn hảo. Cấp phép Hiệu dụng hiển thị trên giao diện này được xác định nhờ tổng hợp các vấn đề sau:

- Các Cấp phép được gán riêng rẽ cho đối tượng
- Cấp phép kế thừa từ đối tượng cha

- Cấp phép kế thừa từ nhóm cục bộ hay Miền

Tuy nhiên danh sách Cấp phép Hiệu dụng không tính đến các Cấp phép chia sẻ hay Cấp phép được kế thừa từ các nhóm đồng nhất đặc biệt do chúng phụ thuộc vào trạng thái truy cập của đối tượng bảo mật.

Ví dụ, thẻ ***Effective Permissions*** có thể chỉ ra rằng một nhóm cụ thể có Cấp phép ***Full Control*** trên một thư mục của ổ đĩa chia sẻ. Tuy nhiên nếu bạn vẫn sử dụng Cấp phép chia sẻ mặc định điều đó có nghĩa là nhóm đồng nhất đặc biệt ***everyone*** chỉ có Cấp phép ***Read*** (*đọc*) tức là nhóm này chỉ có Cấp phép đọc bất kể ***Effective Permissions*** hiển thị như thế nào.

Cũng theo cách như vậy, Cấp phép Hiệu dụng không thể tính đến trạng thái truy cập của đối tượng bảo mật tại một thời điểm bất kỳ. Windows Server 2003 cho phép gán Cấp phép dựa trên các nhóm Đồng nhất Đặc biệt như: Truy cập nặc danh (***Anonymous Logon***), quay số qua đường thoại (***Dialup***) và tương tác (***Interactive***). Như đã học ở chương 7, những Đồng nhất Đặc biệt này được xác định dựa trên cách mà người dùng truy nhập vào hệ thống hay mạng. Ví dụ một người sử dụng truy cập vào mạng bằng cách sử dụng ***dialup*** là một phần của nhóm Đồng nhất Đặc biệt ***Dialup*** trong suốt quá trình kết nối đó. Vì đối tượng bảo mật không cần truy nhập khi bạn xem Cấp phép Hiệu dụng của họ vì vậy không có cách nào để hệ thống có thể biết được Đồng nhất Đặc biệt nào sẽ có ảnh hưởng tới các đối tượng khi họ truy nhập.

> ***CHÚ Ý: Liên quan đến Cấp phép Hiệu dụng*** *Để xem xét các Cấp phép được cấp cho các nhóm Đồng nhất Đặc biệt có thể có ảnh hưởng thế nào tới người sử dụng của bạn, bạn có thể dùng thẻ* ***Effective Permissions*** *để hiển thị Cấp phép Hiệu dụng của một nhóm Đồng nhất Đặc biệt nào đó, sau đó bạn có thể chuyển những kết quả đó vào Cấp phép Hiệu dụng của người sử dụng.*

Sở hữu tài nguyên (Resource Ownership)

Mọi file và thư mục trên hệ thống file NTFS (cũng như mọi đối tượng trên ***Active Directory***) đều có một chủ sở hữu. Mặc định, chủ sở hữu là người đã tạo ra file hay thư mục đó. Trong trường hợp file hay thư mục được tạo bởi hệ điều hành thì nhóm ***Administrators*** sẽ là chủ sở hữu. Tuy nhiên các thành viên của nhóm ***Administrators*** hoặc những người sử dụng được cấp Cấp phép đặc biệt ***Take Ownership*** (*chiếm quyền sở hữu*) đối với file hay thư mục đều có khả năng chiếm đoạt quyền sở hữu của file hay thư mục tại bất kỳ thời điểm nào.

CHÚ Ý Mục tiêucủa kỳ thi *Mục tiêu của môn thi 70-290 yêu cầu học viên có khả năng "thay đổi quyền sở hữu của file hay thư mục"*

Quyền sở hữu file hay thư mục có hai mục tiêu chính sau

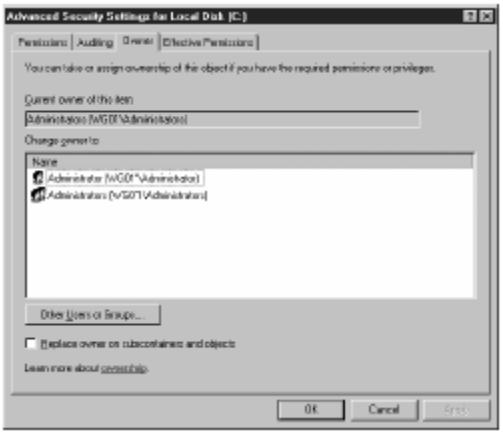
- **Các chủ sở hữu có thể thay đổi các ACL** Bất kể chủ sở hữu của một file hay thư mục có Cấp phép gì anh ta vẫn có thể thay đổi được ACL của file hay thư mục. Vì vậy có thể coi sự sở hữu như một cơ chế dự phòng khi có một ai đó khóa file hay thư mục đối với tất cả mọi người. Ví dụ nếu bạn tạo một file mới và ngẫu nhiên bỏ hết mọi Cấp phép của bạn đối với file đó, quyền sở hữu file cho phép bạn có thể thay đổi ACL và khôi phục lại các Cấp phép.
- **Hạn ngạch đĩa được xác định theo chủ sở hữu** Hạn ngạch đĩa cho phép người quản trị theo dõi và kiểm soát mỗi người sử dụng có thể sử dụng bao nhiêu không gian đĩa cứng trên máy chủ. Bạn sẽ được học vấn đề này trong chương 12.

Ngoài Cấp phép ***Take Ownership*** (*chiếm quyền sở hữu*) cũng có hai Cấp phép nhằm cung cấp khả năng quản lý chủ sở hữu của file hoặc thư mục NTFS:

- **Take Ownership Of Files Or Other Objects** (c*hiếm quyền sở hữu của các file và các đối tượng khác*) Người dùng hay nhóm sở hữu Quyền này có thể chiếm quyền của bất kỳ file hay thư mục NTFS. Mặc định, nhóm ***Administrators*** nhận được quyền này từ chính sách nhóm ***Default Domain Controller Policy*** (*chính sách nhóm mặc định dùng cho các máy chủ điều khiển vùng*).
- **Restore Files And Directories** (*phục hồi các file và thư mục*) Người dùng hay nhóm sở hữu Quyền này có thể chiếm quyền sở hữu của bất kỳ file hoặc thư mục NTFS nào hay gán quyền sở hữu cho người dùng hay nhóm khác. Mặc định, chính sách nhóm ***Default Domain Controller Policy*** sẽ gán Quyền này cho các nhóm ***Administartors*** *(nhóm quản trị*), nhóm ***Backup Operator*** (*thực hiện các công việc sao lưu*) và nhóm ***Server Operators*** (*nhóm quản trị các hoạt động trên máy chủ*).

Để xem hay chiếm quyền sở hữu của file hay thư mục, mở hộp thoại ***Advanced Security Settings*** và chọn thẻ ***Owner*** như trên hình 9-19. Thẻ này liệt kê chủ sở hữu hiện thời của file hay thư mục. Nếu bạn có Cấp phép đặc biệt ***Take Ownership*** đối với file hay thư mục hoặc có quyền ***Take Ownership Of Files Or Other Objects***, bạn có thể lựa chọn tài khoản của bạn trong hộp ***Change Owner To*** rồi nhấn ***Apply*** hay ***OK*** để chiếm quyền sở

hữu đối tượng đó. Nếu bạn có quyền ***Restore Files And Directories***, bạn cũng có thể nhấn vào ***Other Users Or Groups*** để lựa chọn đối tượng bảo mật khác rồi cấp quyền sở hữu đối tượng đó cho nó.



Hình 9-19: Thẻ Owner của hộp thoại Advanced Security Settings

Nếu bạn là người chủ sở hữu hiện tại cuả file hay thư mục và bạn muốn chuyển quyền sở hữu cho người khác nhưng bạn lại không có quyền ***Restore Files And Directories***, bạn vẫn có thể thay đổi ACL và cấp cho người sử dụng đó Cấp phép ***Take Ownership***. Sau đó người sử dụng kia sẽ dùng các tiến trình như trên để chiếm quyền sử dụng của file hay thư mục.

QUẢN TRỊ IIS

Cho tới chương này, chúng ta đã học cách cung cấp cho người dùng mạng khả năng truy cập tới các file trên một máy tính chạy Windows Server 2003 thông qua việc công bố các điểm chia sẻ bằng dịch vụ ***Server***. Dịch vụ này cho phép các máy trạm sử dụng dịch vụ ***Worksbantion*** có thể truy nhập được. Tuy nhiên trên Windows Server 2003, đây không phải là cách duy nhất để chia sẻ các file. Thay vào đó bạn cũng có thể sử dụng các dịch vụ ***Internet*** được cung cấp bởi ***Microsoft IIS*** kể cả khi máy trạm của bạn nằm trong mạng LAN.

> ***CHÚ Ý Mục tiêu của kỳ thi*** *Các mục tiêu cho môn thi 70-290 yêu cầu các học viên có khả năng "quản trị dịch vụ IIS"*

IIS là một ứng dụng của Windows Server 2003 có khả năng công bố các file và các ứng dụng bằng việc sử dụng các giao thức chuẩn Internet như ***HTTP*** (*là một giao thức chuẩn cho truyền thông Web*) và ***FTP*** . So sánh với việc chia sẻ file thông thường, việc chia sẻ file trong IIS, với cấu hình mặc định của IIS, là một phương pháp hạn chế trong việc công bố các file . Vì các lý do an ninh , IIS được cài đặt trong chế độ khóa và bảo mật cho phép máy

chủ chỉ cung cấp nội dung tĩnh cho các máy trạm. Người dùng có thể lấy các file từ một máy chủ IIS về ổ đĩa nội bộ của mình và làm việc với chúng trên máy cá nhân nhưng họ không thể mở file trực tiếp từ máy chủ cũng như lưu các phiên bản được sửa đổi so với trạng thái ban đầu của file như họ vẫn làm trên hệ thống file chia sẻ thông thường. Tuy nhiên , kể cả khi ở trong trạng thái khóa, IIS vẫn cung cấp những phương tiện để phổ biến các file một cách dễ dàng và bảo mật. Trong các phần sau đây, chúng bạn sẽ học cách cài đặt và cấu hình IIS trên một máy tính chạy Windows Server 2003 và quản lý vấn đề bảo mật của một máy chủ IIS .

Cài đặt IIS

Không giống như Windows 2000, mặc định Windows Server 2003 không cài đặt IIS. Việc làm này nhằm phòng ngừa lỗ hổng an ninh tiềm ẩn trong hệ điều hành. Mặc định, các phiên bản trước đó của Windows cài đặt dịch vụ IIS, kích hoạt dịch vụ ***World Wide Web Publishing*** và tạo một trang Web mặc định . Trong các trường hợp mà người quản trị không dùng tới và quên tắt dịch vụ, nó sẽ trở thành một lối vào tiềm ẩn cho những người dùng trái phép . Trong Windows Server 2003 , bạn phải cài đặt IIS một cách thủ công sau khi đã hoàn tất việc cài đặt hệ điều hành. Để cài đặt IIS, mở ***Add Or Remove Programs*** trong ***Control Panel*** rồi chọn ***Add/Remove Windows Components*** để khởi động Trình hướng dẫn ***Windows Components*** . Trong Trình hướng dẫn này , chọn ***Application Server*** , nhấn ***Details*** , rồi chọn ***Internet Information Services (IIS)*** . Bạn có thể nhấn ***Details*** một lần nữa để chỉ rõ các thành phần IIS nào mà bạn muốn cài đặt . Mặc định, Trình hướng dẫn sẽ cài đặt các thành phần sau :

- **Common Files**: Cài đặt các file chương trình cần thiết dành cho IIS .
- **Internet Information Services Manager**: cài đặt snap-in ***IIS Manager***. Bạn sử dụng snap-in này để quản lý các dịch vụ IIS và cấu hình an ninh site .
- **World Wide Web Service**: Cài đặt dịch vụ cung cấp kết nối HTTP với các máy trạm TCP/IP trên mạng .

CHÚ Ý Cài đặt các thành phần bổ sung *Mặc dù chúng không cần thiết cho các chức năng sẽ được mô tả trong chương này, bạn vẫn có thể chọn các thành phần IIS bổ sung để cung cấp tính năng cao hơn cho máy chủ, nhưng không được bỏ bất cứ thành phần mặc định nào liệt kê ở đây .*

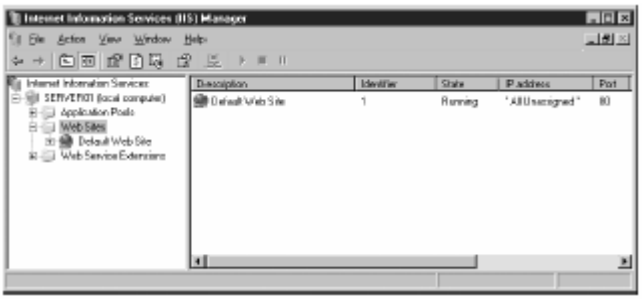
Sau khi bạn hoàn tất Trình hướng dẫn , Windows Server 2003 sẽ cài đặt các thành phần mà bạn đã lựa chọn và kích hoạt dịch vụ ***World Wide Web Publishing***.

Quản trị một Web Site IIS

Khi IIS đã được cài đặt, một trang Web mặc định được tạo ra, cho phép bạn thực thi một môi trường Web nhanh chóng và dễ dàng. Ban đầu, site mặc định chưa có nội dung gì (ngoại trừ một bản tin ***Under Construction***) . Bằng cách bổ sung các file của bạn vào thư mục gốc của site mặc định , bạn có thể tạo ra một trang chủ nhằm cung cấp cho các máy trạm khả năng truy cập tới bất kỳ file, thư mục và thông tin nào mà bạn muốn công bố.

> ***CHÚ Ý Mục tiêu của kỳ thi*** *Các mục tiêu cho môn thi 70-290 yêu cầu các học viên có khả năng "quản trị một máy chủ Web"*

Để quản trị các Web site trên một Máy chủ IIS, bạn sử dụng snap-in ***IIS Manager*** (như trong hình 9-20) , bằng cách truy nhập ***Administrative Tools*** trên thực đơn ***Start*** . Snap-in này cho phép bạn tạo và quản lý một số lượng Web site riêng biệt nhiều tới mức mà phần cứng của máy chủ có thể chạy được.



Hình 9-20: Snap-in quản trị dịch vụ IIS

Ban đầu chỉ có một Web site duy nhấy trên máy chủ, gọi là ***Default Web Site***. Để xem các site trên máy chủ, mở rộng nút của máy chủ trong khung Phạm vi rồi mở rộng thư mục ***Web Sites***. Bằng cách chọn một trong các web site được liệt kê rồi chọn ***Properties*** từ thực đơn ***Action***, bạn có thể mở hộp thoại ***Properties*** của site đó . Hộp thoại này chứa một lượng lớn các chức năng điều khiển cho phép bạn cấu hình các thông số cho Web site này . Các phần sau đây xem xét một vài chức năng điều khiển quan trọng của hộp thoại này .

Sử dụng thẻ ***Web Site***

Thẻ ***Web Site*** của hộp thoại ***Properties*** (hình vẽ 9-21), chứa các thiết lập xác định cách thức các máy trạm có thể truy nhập tới Web Site. IIS có thể duy trì (***Host***) một số lượng không giới hạn các Web site ảo trên một máy tính, nhưng để cho các máy trạm có thể truy nhập được tới chúng, phải có một cách thức để phân biệt giữa site này với các site khác.

Hình 9-21: Thẻ Web Site trong hộp thoại Properties của một Web site

Các máy chủ Web thông thường sử dụng các kỹ thuật sau đây để duy trì nhiều site cùng lúc :

- **Các địa chỉ IP khác nhau**: Bằng cách cấu hình máy tính với nhiều địa chỉ IP khác nhau và gán mỗi địa chỉ IP khác nhau cho một Web site, máy chủ Web có thể hướng các yêu cầu tới site thích hợp, dựa trên địa chỉ IP được xác định trong yêu cầu.
- **Các cổng khác nhau**: Mặc định, giao thức HTTP sử dụng cổng thông dụng là 80 cho thông tin TCP/IP của nó. Khi kết nối vào một Web site, trình duyệt sẽ mặc định sử dụng cổng 80 trừ phi bạn chỉ định khác đi, bằng cách sử dụng một địa chỉ URL như ***http://www.ACNA.com:81***. Bằng cách gán các cổng khác nhau cho các Web site, một máy chủ có thể hướng các yêu cầu tới site thích hợp dựa trên số cổng được chỉ rõ trong yêu cầu.
- **Host headers**: Mặc dù các máy trạm thông thường sử dụng tên để truy nhập vào các Web site nhưng quá trình truyền thông TCP/IP vẫn dựa trên các địa chỉ IP. Các máy chủ DNS chịu trách nhiệm chuyển đổi các tên này sang các địa chỉ IP. **Host Header** là một trường tùy chọn trong bản tin yêu cầu HTTP bao hàm tên URL của máy chủ Web. Các yêu cầu với các giá trị ***host header*** khác nhau có thể được hướng tới một máy chủ Web đơn với một địa chỉ IP và một cổng duy nhất. Sau đó, máy chủ có thể hướng các yêu cầu tới site thích hợp dựa vào giá trị ***host header***. Ví dụ, một công ty có thể

duy trì (***host***) hai Web site ***www.adatum.com*** và ***www.ACNA.com*** trên một máy chủ Web. Máy chủ DNS của công ty sẽ chuyển đổi cả hai tên gọi sang cùng một địa chỉ IP vì vậy các bản tin yêu cầu gửi đến mỗi site đều tới cùng một máy chủ. Máy chủ Web sau đó sẽ phân biệt hai đích bằng cách xem xét các trường ***host header***.

Với các chức năng điều khiển trong thẻ ***Web Site***, bạn có thể sử dụng bất cứ phương pháp nào trong 3 phương pháp nêu trên để phân biệt các Web site với nhau. Web site mặc định được cấu hình sử dụng cổng 80 và tất cả các địa chỉ IP của máy tính sẽ không được gán cho các Web site khác. Nếu bạn muốn tạo thêm các Web site khác trên máy chủ, bạn có thể thay đổi các giá trị này bằng cách chọn một giá trị địa chỉ IP xác định, thay đổi giá trị cổng TCP hoặc nhấp vào nút ***Advanced*** để xác định tên ***host header*** cho site .

Thẻ này còn cho phép bạn định ra một giới hạn thời gian trước khi những người dùng ở trạng thái ***inactive*** (không hoạt động mặc dù vẫn đang kết nối) bị ngắt kết nối ra khỏi máy chủ, cũng như kiểm soát cách thức đăng nhập của máy chủ đối với site này bằng cách chọn một định dạng file nhật ký, xác định thông tin nào được ghi vào nhật ký và cấu hình thời gian biểu để ghi nhật ký.

Sử dụng thẻ Home Directory

Thư mục gốc của một web site là vị trí mặc định chứa các file nội dung của một web site. Khi bạn xác định một URL trong trình duyệt Web với tên site nào đó (như ***www.ACNA.com*** chẳng hạn), máy chủ sẽ tự động cung cấp cho bạn các file nội dung trong thư mục gốc của site đó. Trong thẻ ***Home Directory*** (hình vẽ 9-22) bạn có thể xác định vị trí của thư mục gốc cho một Web site nhất định. Bằng cách tạo ra các thư mục gốc khác nhau cho các site khác nhau chạy trên một máy chủ duy nhất, bạn có thể duy trì nội dung riêng biệt cho mỗi site.

Hình 9-22: Thẻ Home Directory trong hộp thoại Properties của một Web site

IIS cho phép bạn xác định một thư mục gốc bằng cách chọn một trong ba tùy chọn sau :

- **A Directory Located On This Computer** (*thư mục trên máy tính này*) sử dụng ký hiệu chữ cái ổ đĩa chuẩn để xác định thư mục gốc trên một trong các ổ đĩa logic của máy tính.
- **A Share Located On Another Computer** (*thư mục chia sẻ trên máy tính khác*) sử dụng đường dẫn **Universal Naming Convention** (**UNC**) để xác định thư mục gốc nằm trên một vùng chia sẻ ở đâu đó trên mạng.
- **A Redirection To A URL (***chuyển hướng tới URL***)** sử dụng đường dẫn URL để xác định thư mục gốc trên một máy chủ Web khác.

Web site mặc định sử dụng một thư mục gốc cục bộ được tạo ra mặc định trong quá trình cài đặt IIS đặt tại thư mục ***C:\Inetpub\wwwoot***. Ban đầu thư mục này không chứa một nội dung thực sự nào ngoại trừ các file để thể hiện trang ***Under Construction*** nhưng bằng việc đưa các file nội dung vào thư mục này, bạn có thể biến chúng sử dụng được ngay lập tức đối với các máy trạm.

Ngoài việc cho phép bạn xác định vị trí thực sự của thư mục gốc, thẻ này còn cho phép bạn cấu hình các kiểu truy nhập mà máy trạm có thể sử dụng để truy nhập tới thư mục này. Bạn có thể chọn các tùy chọn dưới đây sau khi xác định thư mục gốc trên ổ đĩa cục bộ hay trên điểm chia sẻ trên mạng:

- **Script Source Access**: cho phép các máy trạm có thể truy nhập các file kịch bản (***script***) trong thư mục với giả thiết rằng các Cấp phép ***Read*** hay ***Write*** đã được thiết lập.
- **Read**: cho phép các máy trạm có thể đọc và tải về các file trong thư mục .
- **Write**: cho phép các máy trạm tải lên thư mục các file hoặc thay đổi nội dung của các file cho phép ghi.
- **Directory Browsing**: giả thiết rằng không có tài liệu mặc định (***Default Documents***), cho phép người dùng xem một danh sách các liên kết siêu văn bản liệt kê các file và các folder có trong thư mục .

- **Log Visits**: giả thiết rằng tính năng ghi nhật ký đã được kích hoạt cho site này, cho phép ghi lại các cuộc truy nhập vào thư mục vào nhật ký
- **Index This Resource**: tạo một chỉ mục của các nội dung văn bản (***full-text index)*** của thư mục trong dịch vụ ***Microsoft Indexing*** (*bạn phải cài đặt dịch vụ* ***Indexing*** *bằng cách nhấn* ***Add/Remove Windows Components*** *trong công cụ* ***Add or Remove Programs***).
- **Application Settings**: cho phép bạn xác định các kiểu ứng dụng Web mà máy trạm được phép chạy.

Sử dụng thẻ ***Documents***

Trong thẻ ***Documents*** (hình vẽ 9-23) bạn có thể xác định tên của file nội dung mà IIS phân phối tới các máy trạm một cách mặc định. Khi một máy trạm đưa một URL không chứa bất cứ một tên tệp nào trong trình duyệt, máy chủ Web phân phối file với tên mặc định được chỉ rõ trong hộp ***Enable Default Content Page***. Nếu tên tệp đầu tiên được liệt kê không tồn tại trong thư mục, máy chủ sẽ kiểm tra lần lượt các file được liệt kê trong hộp nói trên theo thứ tự từ trên xuống. Nếu không có tệp nào trong danh sách tồn tại, máy chủ hoặc hiển thị một siêu văn bản liệt kê nội dung của thư mục (nếu tùy chọn ***Directory Browsing*** được kích hoạt trong thẻ ***Home Directory***) hoặc một bản thông báo lỗi (nếu ***Direcoty Browsing*** bị vô hiệu).

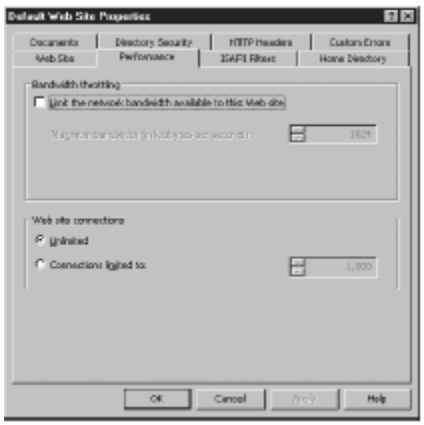
Hình 9-23: Thẻ Documents trong hộp thoại Properties của một Web site

Hộp ***Enable Document Footer*** cho phép bạn cung cấp tên của file ***footer*** được gắn vào tất cả các tài liệu được Website xuất bản.

Sử dụng thẻ Performance

Trong thẻ ***Performance*** (hình vẽ 9-24) bạn có thể giới hạn băng thông sử dụng cho site này cũng như số lượng người dùng có thể kết nối đồng thời.

Nó cho phép bạn ngăn chặn tình trạng một Web site độc chiếm toàn bộ băng thông hệ thống.



Hình 9-24: Thẻ Perfomance trong hộp thoại Properties của Web site

Tạo các thư mục ảo

Khi bạn xác định một thư mục gốc cho một Website IIS, tất cả các file trong thư mục và các thư mục con của nó đều được máy chủ công bố và sẵn sàng phục vụ cho các máy trạm. Tuy nhiên, nếu bạn muốn công bố các file và thư mục sẵn có thì bạn cũng không cần phải di chuyển chúng đến cấu trúc thư mục gốc. Thay vào đó bạn có thể tạo ra một thư mục ảo. Một thư mục ảo là một con trỏ đến một thư mục nằm tại một vị trí khác và đối với các máy trạm chúng là một phần trong cấu trúc thư mục của Web site.

Để tạo ra một thư mục ảo trên một IIS Web site, bạn lựa chọn ***site*** trên màn hình quản trị ***IIS Manager***, sau đó trên thực đơn ***Action*** trỏ tới ***New*** rồi lựa chọn ***Virtual Directory***. Hoạt động này kích hoạt Trình hướng dẫn ***Virtual Directory Creation***, ở đó bạn phải cung cấp những thông tin sau:

- **Virtual Directory Alias** (*các bí danh cho thư mục ảo*): cung cấp tên của thư mục ảo cho các máy trạm. Bí danh mà bạn nhập sẽ xuất hiện như một thư mục con của Web site trong các URL của máy trạm. Bí danh mà bạn chọn không cần thiết phải là tên thật của thư mục mà bạn muốn công bố.
- **Web Site Content Directory** (*thư mục chứa nội dung của Web site*): xác định đường dẫn tới thư mục mà bạn định chia sẻ cho thư mục ảo. Đường dẫn mà bạn đưa vào có thể sử dụng một ký tự ổ đĩa hoặc đường dẫn UNC và có thể được đặt trên một ổ đĩa cục bộ hoặc một thư mục chia sẻ trên mạng.

- **Virtual Directory Access Permissions** (c*ác Cấp phép truy cập đến thư mục ảo*): xác định Cấp phép cấp cho các máy trạm khi truy cập đến thư mục ảo (như ***Read*** (*đọc*), ***Run Scripts*** (*chạy các kịch bản*), ***Excute*** (*thực thi*), ***Write*** (*ghi*) và ***Browse*** (*duyệt trang Web*)).

Một khi bạn đã tạo thư mục ảo, các file trong thư mục nội dung mà bạn muốn công bố trên Web site sẽ nằm trong một thư mục con được xác định theo bí danh bạn cung cấp ở trên.

Cấu hình bảo mật IIS

Hầu hết các Web site trên Internet đều cung cấp cho các máy trạm Cấp phép truy cập nặc danh (***anonymous***). Khi bạn cấu hình một IIS Web site cho việc truy cập nặc danh, tất cả các máy trạm kết nối tới máy chủ đều sử dụng một tài khoản đặc biệt được thiết kế cho mục đích này. Tên tài khoản mặc định trong Windows Server 2003 là **IUSR_*servername*** trong đó ***servername*** là tên của máy tính. Về mặt kỹ thuật, các máy khách vẫn được xác thực nhưng không có sự trao đổi các thông tin bí mật và chúng không bị hạn chế trong quá trình truy cập tới Web site.

> ***CHÚ Ý Mục tiêu của kỳ thi*** *Các mục tiêu cho kỳ thi 70-290 yêu cầu các học viên có khả năng "quản trị tính bảo mật của IIS"*

Tuy nhiên, nếu bạn muốn hạn chế việc truy cập tới một Web site, bạn có thể gia tăng mức bảo mật theo một vài phương pháp sau đây:

- **Authentication and Access Control** (*kiểm soát truy cập và xác thực*): yêu cầu các máy trạm cung cấp tên truy cập và mật khẩu khi truy cập Web site. IIS cung cấp một số loại mã hóa với mức độ bảo mật khác nhau.
- **IP Address and Domain Name Restrictions** (*các hạn chế về tên miền và địa chỉ IP*): bạn có thể cho phép hoặc ngăn cấm các máy khách nhất định truy cập tới site dựa trên địa chỉ IP và tên miền của chúng.
- **Secure Communications** (*các kênh truyền thông bảo mật*): yêu cầu các máy trạm sử dụng một giao thức truyền thông bảo mật hoặc một chứng chỉ số khi truy cập tới Web site.

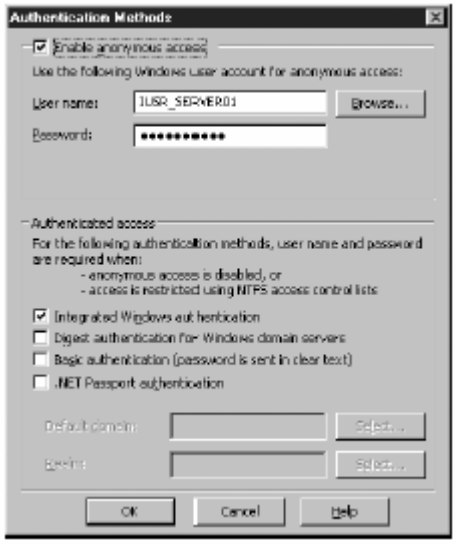
Bạn có thể cấu hình tất cả các cơ chế bảo mật nói trên trong thẻ ***Directory Security*** trong hộp thoại ***Properties*** của Web site như hình vẽ 9-25.

Hình 9-25: Thẻ Directory Security trong hộp thoại Properties của Web site

> ***CHÚ Ý IIS và các Cấp phép NTFS*** *Ngoài các cơ chế bảo mật ở trên bạn cũng có thể sử dụng các Cấp phép NTFS để bảo vệ các Web site. Như đã đề cập trong chương trước, các Cấp phép NTFS cung cấp cho các người dùng bất kể họ truy cập bằng phương pháp nào. Điều đó có nghĩa rằng một người dùng truy cập tới một Web site với nội dung được lưu trên ổ đĩa NTFS phải có các Cấp phép tương ứng để truy cập các file nội dung. Xem phần "Sử dụng các Cấp phép NTFS" trong chương trước để biết thêm thông tin.*

Cấu hình xác thực IIS

Để cấu hình một IIS Web site sử dụng một mô hình nhận thực khác với truy cập nặc danh mặc định, bạn nhấp vào nút ***Edit*** trong hộp ***Authentication And Access Control*** trên thẻ ***Directory Security*** để hiển thị hộp thoại ***Authentication Methods*** (xem hình vẽ 9-26).



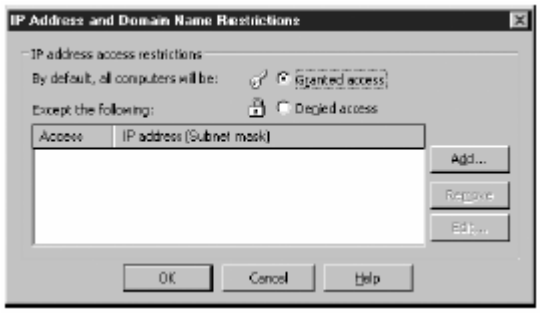
Hình 9-26: Hộp thoại Authentication Methods

Để ngăn chặn hình thức truy cập không xác thực tới Web site, bạn phải bỏ dấu chọn tại hộp kiểm tra ***Enable Anonymous Access***. Bạn cũng phải cấp các Cấp phép NTFS cho các file và thư mục mà bạn muốn bảo vệ. Kế đó bạn phải lựa chọn một hình thức xác thực thay thế từ các lựa chọn sau:

- **Integrated Windows Authentication** (*xác thực tích hợp với Windows*): máy chủ thực hiện trao đổi mật mã với máy trạm vì vậy tên truy cập và mật khẩu được truyền đi trong dạng các mớ rối (***Hash***) nhằm ngăn chặn những người nghe trộm có thể đọc được nội dung về tài khoản của người sử dụng. Hình thức xác thực này không phù hợp với việc truy cập qua máy chủ ***proxy*** hoặc các tường lửa.
- **Digest Authentication For Windows Domain Servers** (*xác thực dạng phân loại cho các máy chủ Miền*): chỉ dành cho các máy trạm có các tài khoản ***Active Directory***, Máy chủ sẽ thu thập các chứng thực người sử dụng và lưu chúng trên Máy chủ Điều khiển dưới dạng ***MD5 (Message Digest 5) Hash*** (*mớ rối MD5*).
- **Basic Authentication** (*xác thực cơ bản*): máy trạm truyền tên truy cập và mật khẩu theo dạng văn bản tường minh, vì vậy sẽ tạo nên một nguy cơ tiềm ẩn về bảo mật. Bạn chỉ sử dụng lựa chọn này khi không có khả năng chọn các lựa chọn khác mang tính bảo mật hơn.
- **.NET Passport Authentication** (*xác thực dựa trên .NET Passport*): các máy trạm kết nối tới máy chủ bằng cách sử dụng các tài khoản ***.NET Passport*** sẵn có của chúng. Chúng được xác thực bởi một máy chủ ***.NET Passport*** trung tâm trên Internet.

Cấu hình các hạn chế về địa chỉ IP và tên miền

Khi bạn nhấp vào nút ***Edit*** trong hộp ***IP Address And Domain Name Restrictions***, bạn sẽ nhìn thấy hộp thoại ***IP Address And Domain Name Restrictions*** như hình vẽ 9-27. Ở đây bạn có thể xác định các địa chỉ IP riêng rẽ, các địa chỉ mạng và các tên miền sau đó bạn sẽ cho phép hoặc cấm chúng truy cập tới Web site.



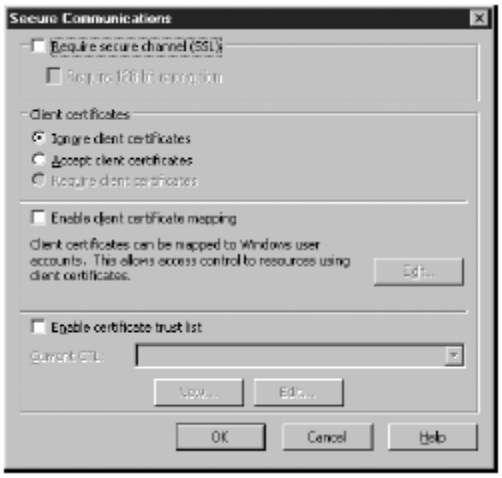
Hình 9-27: Hộp thoại IP Address And Domain Restrictions

Trong hộp thoại ***IP Address And Domain Name Restrictions***, trước hết bạn phải xác định xem bạn muốn các địa chỉ và các tên mà bạn lựa chọn sẽ được phép hay ngăn cấm truy cập đến Web site. Tiếp theo bạn nhấp vào ***Add*** để mở hộp thoại ***Granted Access or Denied Access***, ở đó bạn sẽ nhập địa chỉ IP của máy tính nào đó, địa chỉ mạng và mặt nạ mạng con hoặc tên miền.

Loại hạn chế này được dựa trên máy tính chứ không phải dựa trên người sử dụng. Khi bạn gán Cấp phép truy cập đến Web site cho một địa chỉ IP nào đó thì bất kỳ người sử dụng nào làm việc trên máy tính đó cũng có thể truy cập đến Web site đó ngoại trừ có các cơ chế bảo mật khác được thực thi. Do những hạn chế này là độc lập với cơ chế xác thực của Web site nên bạn có thể sử dụng nó để thay thế hoặc kết hợp với cơ chế xác thực. Ví dụ, bạn có thể gán Cấp phép truy cập đến Web site cho một người dùng xác định nhưng với một điều kiện là người dùng đó phải truy cập từ một máy tính cụ thể. Bằng cách cho phép xác thực và thực hiện hạn chế theo địa chỉ IP, bạn có thể sử dụng đồng thời cả hai.

Cấu hình bảo mật truyền thông

Khi bạn nhấp vào nút ***Edit*** trong hộp ***Secure Communications***, hộp thoại ***Secure Communications*** sẽ xuất hiện (hình vẽ 9-28), ở đó bạn có thể cấu hình các lựa chọn sau:



Hình 9-28: Hộp thoại Secure Communications

- **Require Secure Channel (SSL)** (*yêu cầu kênh bảo mật*): yêu cầu các máy tính sử dụng một giao thức truyền thông mã hóa khi kết nối tới Web server như giao thức SSL chẳng hạn. Bạn cũng có thể yêu cầu các máy trạm sử dụng mã hóa 128-bit để tăng tính bảo mật.
- **Client Certificates** (*các chứng thực máy trạm*): xác định xem các máy trạm có thể, không thể hoặc phải sử dụng các chứng thực số khi truy cập tới Web site. Để yêu cầu các chứng thực, bạn phải chọn lựa chọn ***Secure Socket Layer (SSL)***.
- **Enable Client Certificate Mapping** (*cho phép ánh xạ chứng thực máy trạm*): cấu hình máy chủ xác thực các máy trạm truy nhập với các chứng thực hợp lệ. Nhấp ***Edit*** để ánh xạ các chứng thực với các tài khoản người sử dụng.
- **Enable Certificate Trust List** (*kích hoạt danh sách chứng thực tin cậy*): cấu hình máy chủ sử dụng một danh sách các trung tâm ủy quyền chứng thực tin cậy để xác minh tính hợp lệ các chứng thực của người sử dụng. Các người dùng không nhận một chứng thực từ một trong các trung tâm ủy quyền được liệt kê ở trên bị cấm truy cập.

TỔNG KẾT

- Windows Server 2003 chứa một số các hệ thống Cấp phép độc lập bao gồm: các Cấp phép chia sẻ, các Cấp phép NTFS, các Cấp phép ***Active Directory*** và các Cấp phép trên ***registry***. Mỗi một hệ thống Cấp phép cho phép bạn kiểm soát việc truy cập tới một loại tài nguyên hệ thống xác định.
- Mỗi đối tượng được bảo vệ thông qua các Cấp phép đều có một ACL (Danh sách Kiểm soát Truy cập). Mỗi ACL là một danh sách các ACE (Mục vào Kiểm soát Truy cập) chứa một đối tượng bảo mật (như người dùng, nhóm hoặc máy tính chẳng hạn) và các Cấp phép được gán cho đối tượng đó.
- Hệ thống file chia sẻ cho phép các người dùng trên mạng truy cập tới các file và các thư mục nằm trên các máy tính khác. Để tạo ra các chia sẻ, bạn có thể sử dụng Windows Explorer hoặc snap-in ***Shared Folders*** hoặc công cụ ***Net.exe*** ở chế độ dòng lệnh.
- Các Cấp phép chia sẻ cung cấp mức bảo vệ cơ bản cho các thư mục chia sẻ, nhưng chúng không có tính đa dạng và mềm dẻo như các Cấp phép NTFS. Các Cấp phép chia sẻ chỉ áp dụng cho các truy cập mạng thông qua dịch vụ ***Server***. Các file được bảo vệ bằng các Cấp phép chia sẻ vẫn có thể truy cập được từ máy tính cục bộ hoặc thông qua các dịch vụ mạng khác như IIS hay ***dịch vụ đầu cuối (Terminal)*** chẳng hạn.
- Các Cấp phép NTFS có thể cho phép hoặc ngăn cấm, gán Cấp phép một cách riêng rẽ hoặc được kế thừa từ trên. Cấp phép ngăn cấm sẽ loại bỏ tất cả các Cấp phép cho phép khác và các Cấp phép gán riêng rẽ sẽ có mức ưu tiên cao hơn so với các Cấp phép kế thừa. Kết quả là một Cấp phép cho phép gán riêng rẽ sẽ loại bỏ Cấp phép ngăn cấm kế thừa. Các Cấp phép Hiệu dụng trên một file hoặc thư mục là sự tổng hợp của tất cả các Cấp phép gán cho đối tượng xác định bao gồm cả Cấp phép gán trực tiếp hoặc thông qua cơ chế kế thừa.
- Các Cấp phép truy cập NTFS có thể bị hạn chế hơn nữa nhờ các Cấp phép khác và các nhân tố khác như các Cấp phép IIS trên một Web site. Bất kể hai kiểu Cấp phép nào được gán cho một tài nguyên, như các Cấp phép chia sẻ và Cấp phép NTFS chẳng hạn, mỗi kiểu cung cấp một tập hợp các Cấp phép khác nhau và bạn phải tính toán xem kiểu nào hạn chế hơn.

- Tính kế thừa cho phép người quản trị điều khiển việc truy cập các file và thư mục bằng cách cấp Cấp phép cho một thư mục cha và cho phép các Cấp phép này được đưa xuống tất cả các thư mục con và các file nằm bên trong nó.
- Mỗi file và thư mục NTFS đều có một chủ sở hữu. Chủ sở hữu luôn luôn được phép thay đổi các ACL (Danh sách Kiểm soát Truy cập) trên một file hoặc thư mục thậm chí đối tượng này không có Cấp phép.
- Bất kỳ người sử dụng có Cấp phép ***Take Ownership*** (chiếm đoạt quyền sở hữu) hoặc quyền hạn người sử dụng ***Take Ownership Of Files Or Other Objects*** (*quyền hạn chiếm đoạt quyền sở hữu các file hoặc các đối tượng khác*) đều có thể đoạt lại quyền sở hữu một đối tượng. Một người sử dụng với quyền hạn người sử dụng ***Restore Files And Directories*** đều có thể gán quyền sở hữu của bất kỳ đối tượng nào cho bất kỳ người sử dụng nào.
- IIS là một dịch vụ trên hệ điều hành Windows Server 2003 cho phép chia sẻ các file và thư mục bằng cách sử dụng dịch vụ máy chủ Web và FTP. Bạn có thể bảo mật các IIS site bằng cách gán các Cấp phép NTFS và yêu cầu xác thực người sử dụng thông qua việc hạn chế truy cập đối với các địa chỉ và tên Miền xác định hoặc bằng cách sử dụng các giao thức truyền thông mã hóa và các chứng chỉ số.

BÀI TẬP THỰC HÀNH

==========

Bài tập thực hành thực hành 9-1: Tạo một chia sẻ bằng cách sử dụng Windows Explorer

Trong bài thực hành này, bạn sẽ thực hiện việc chia sẻ một thư mục bằng cách sử dụng Windows Explorer

- Truy cập vào hệ điều hành Windows Server 2003 bằng tài khoản ***Administrator***.
- Nhấp ***Start*** và chọn ***Windows Explorer***. Màn hình ***Windows Explorer*** xuất hiện.
- Mở rộng biểu tượng ***My Computer*** và ổ đĩa ***C:***
- Kích chuột phải vào thư mục ***Documents And Settings***, từ thực đơn ngữ cảnh chọn ***Sharing And Security***. Hộp thoại ***Documents And Settings Properties*** xuất hiện với thẻ ***Sharing*** được kích hoạt.
- Nhấp vào ***Share This Folder***. Trong hộp văn bản ***Share Name*** gõ **Test Share**. Nhấp ***OK***. Biểu tượng của thư mục ***Documents And Settings*** bị thay đổi và xác nhận rằng nó đã được chia sẻ.

==========

Bài tập thực hành thực hành 9-2: Sử dụng snap-in Shared Folders

Trong bài thực hành này, bạn sẽ sử dụng snap-in ***Shared Folders*** để tạo một chia sẻ mới và cấu hình các Cấp phép cho nó.

1. Truy cập vào hệ điều hành Windows Server 2003 bằng tài khoản ***Administrator.***

- Nhấp ***Start -> Administrative Tools -> Computer Management***. Màn hình quản trị ***Computer Management*** xuất hiện.
- Mở rộng biểu tượng ***Shared Folders*** và lựa chọn thư mục con ***Shares***.

- Trên thực đơn ***Action*** lựa chọn ***New Share***. Trình hướng dẫn ***Share A Folder*** xuất hiện.
- Nhấp ***Next*** để bỏ qua trong giới thiệu. Trang ***Folder Path*** xuất hiện.
- Trong hộp văn bản ***Folder Path***, gõ **C:\Windows** và nhấp ***Next.*** Trang ***Name, Description, And Setttings*** xuất hiện.
- Trong hộp văn bản ***Share Name***, gõ **Test Share 2** và nhấp ***Next***. Trang ***Permissions*** xuất hiện.
- Lựa chọn ***Administrators Have Full Access; Other Users Have Read-Only Access*** (các thành viên nhóm quản trị có toàn quyền còn các người dùng khác chỉ có Cấp phép đọc mà thôi) rồi nhấp ***Finish***. Trang ***Sharing Was Successful*** xuất hiện.
- Nhấp ***Close.***

==========

Bài tập thực hành thực hành 9-3: Cấu hình các Cấp phép NTFS

Trong bài thực hành này, bạn sẽ cấu hình các Cấp phép NTFS cho một thư mục trên máy tính của bạn bằng Windows Explorer.

2. Truy cập vào hệ điều hành Windows Server 2003 bằng tài khoản ***Administrator***.

- Nhấp ***Start*** và chọn ***Windows Explorer***. Màn hình Windows Explorer xuất hiện.
- Mở rộng biểu tượng ***My Computer*** và ổ đĩa ***C:***
- Kích chuột phải vào thư mục ***Documents And Settings***, từ thực đơn ngữ cảnh chọn ***Sharing And Security.*** Hộp thoại ***Documents And Settings Properties*** xuất hiện với thẻ ***Sharing*** được kích hoạt.
- Lựa chọn thẻ ***Security*** và nhấp ***Add***. Hộp thoại ***Select Users, Computers, Or Groups*** xuất hiện.

- Trong hộp văn bản ***Enter The Object Names To Select,*** gõ **Guests** rồi nhấp ***OK***. Nhóm này sẽ được thêm vào hộp danh sách ***Group Or User Name*** trong thẻ ***Security***.
- Lựa chọn đối tượng ***Guests*** và trong hộp danh sách ***Permissions For Guests*** lựa chọn các hộp kiểm tra ***Modify*** và ***Write*** trong cột *Allow*.
- Nhấp ***OK*** để gán các Cấp phép và đóng hộp thoại ***Documents And Settings Properties*** lại.

CÁC CÂU HỎI ÔN TẬP

1. Trong các công cụ dưới đây, công cụ nào cho phép bạn tạo một chia sẻ trên một máy chủ ở xa? (Lựa chọn tất cả các câu trả lời đúng)
    a. Một màn hình quản trị MMC tùy biến chứa snap-in ***Shared Foldes.***
    b. ***Windows Explorer*** chạy trên máy tính cục bộ và kết nối tới chia sẻ ***ADMIN$*** của máy tính ở xa
    c. ***Net.exe***
    d. Màn hình quản trị ***Computer Management***
2. Một thư mục được chia sẻ nằm trên ổ đĩa FAT. Nhóm ***Project Managers*** được gán toàn quyền (***Full Control***) trên thư mục này. Nhóm ***Project Engineers*** được gán Cấp phép đọc trên đó. Lúc đầu, ***Julie*** là thành viên của nhóm ***Project Engineers***. Sau đó cô ta được đưa vào nhóm ***Project Manager***s. Các Cấp phép Hiệu dụng của cô ta trên thư mục này là gì?
3. Một thư mục được chia sẻ nằm trên ổ đĩa NTFS với các Cấp phép chia sẻ mặc định. Nhóm ***Project Managers*** được gán toàn Cấp phép NTFS. ***Julie*** là một thành viên của nhóm ***Project Managers***, thông báo với bạn rằng cô ta không thể tạo các file trong thư mục nói trên. Tại sao?

4. Các Cấp phép NTFS yêu cầu tối thiểu để cho phép người sử dụng mở các tài liệu và chạy các chương trình trên một thư mục chia sẻ là gì?

    e. Full Control

    f. Modify

    g. Write

    h. Read & Excute

    i. List Folder Contents

5. ***Bill*** phàn nàn rằng anh ta không thể truy cập tới tài liệu có chứa thông về thông tin tài chính của phòng. Bạn mở thẻ ***Security*** của tài liệu đó và thấy rằng tất cả các Cấp phép trên đó đều được thừa hưởng từ thư mục cha. Cấp phép ngăn cấm ***Read*** được gán cho nhóm ***Acctg3*** mà Bill là thành viên. Trong các phương pháp dưới đây, cái nào cho phép Bill truy cập tới tài liệu này? (lựa chọn tất cả các câu trả lời đúng)

    a. Thay đổi các Cấp phép trên thư mục cha bằng cách thêm Cấp phép cho phép ***Full Control*** cho Bill

    b. Thay đổi các Cấp phép trên thư mục cha bằng cách thêm Cấp phép cho phép ***Read*** cho Bill.

    c. Thay đổi các Cấp phép trên tài liệu bằng cách gán thêm Cấp phép cho phép ***Read*** cho Bill.

    d. Thay đổi các Cấp phép trên tài liệu bằng cách loại bỏ ***Allow Inheritable Permissions***, lựa chọn ***Copy*** và loại bỏ Cấp phép ngăn cấm.

    e. Thay đổi các Cấp phép trên tài liệu bằng cách loại bỏ ***Allow Inheritable Permissions***, lựa chọn ***Copy*** và thêm Cấp phép cho phép ***Full Control*** cho Bill.

    f. Loại bỏ Bill ra khỏi nhóm được gán Cấp phép ngăn cấm.

6. Bạn muốn đảm bảo mức độ bảo mật cao nhất cho máy chủ IIS trong tổ chức của bạn mà không phải thêm bất kỳ dịch vụ chứng chỉ nào. Mục tiêu là cung cấp quá trình xác thực trong suốt đối với người sử dụng và cho phép bạn bảo mật các tài nguyên Intranet với các tài khoản nhóm hiện có trên ***Active Directory***. Tất cả người sử dụng đều được bảo vệ bởi tường lửa của tổ chức. Các phương pháp xác thực nào dưới đây chop phép thực hiện mục tiêu trên?

    a. Truy cập nặc danh

    b. Xác thực cơ bản

    c. Xác thực dựa trên ***.NET Passport***

    d. Xác thực tích hợp với Windows

7. Bạn đang cấu hình các Cấp phép chia sẻ cho một thư mục chia sẻ trên một máy chủ file. Bạn muốn tất cả người sử dụng đã được xác thực đều có Cấp phép lưu các file lên thư mục, đọc tất cả các file trong đó và thay đổi hoặc xóa các file do họ làm chủ. Các Cấp phép tối thiểu bạn cần đặt trên thư mục chia sẻ để đạt được mục tiêu trên là gì? (lựa chọn tất cả các câu trả lời đúng)

    a. ***Authenticated Users*** (nhóm người dùng được xác thực): ***Full Control*** (toàn quyền)

    b. ***Authenticated Users: Read*** (đọc)

    c. ***Creator Owner*** (chủ sở hữu tạo file): ***Change***

    d. Creator Owner: Read

CÁC KỊCH BẢN TÌNH HUỐNG

==========

Kịch bản 9-1: công bố Web server

Các file nội dung máy chủ Web của công ty bạn hiện đang được đặt trên ổ đĩa ***D*** của một máy tính Windows Server 2003 đã cài đặt IIS. Tên của máy

chủ là ***Web1*** và URL của nó là ***http://intranet.ACNA.com.*** Bạn được yêu cầu tạo ra một giải pháp IIS cho phép phòng nhân sự có thể công bố các tài liệu về lợi ích và chính sách của công ty từ máy chủ của họ. URL cho phép truy cập tới các thông tin nói trên sẽ là ***http://intranet.ACNA.com/hr.*** Bạn phải làm gì?

a. Cài đặt IIS trên máy chủ của phòng nhân sự.

b. Tạo một Web site mới trên ***Web1*** và đặt tên là ***hr***.

c. Cài đặt dịch vụ FTP trên ***Web1***.

d. Tạo một thư mục ảo trên ***Web1*** với bí danh là ***hr.***

==========

Kịch bản 9-2: Cấu hình các Cấp phép chia sẻ

Phòng kế toán có một file server ***acctg01*** cài đặt hệ điều hành Windows Server 2003 nhằm cung cấp bảng thời gian và các mẫu thông báo công tác phí cho các nhân viên. Bạn là quản trị mạng chịu trách nhiệm cấu hình các Cấp phép chia sẻ trên các thư mục chia sẻ, các Cấp phép phải đáp ứng các yêu cầu sau:

- Các mẫu dùng cho nhân viên được lưu trữ trên thư mục ***Forms*** và được chia sẻ với tên chia sẻ là ***Forms***. Tất cả các nhân viên đều có thể truy cập đến các mẫu này.
- Chỉ có những người sử dụng đã được xác thực mới có thể truy cập đến các mẫu nói trên.
- Các nhân viên có thể tải lên các mẫu đã được điền đầy đủ lên thư mục có tên là ***Forms\Reports\username*** và có tên chia sẻ là ***username***.
- Người sử dụng phải đọc được các mẫu của chính họ nhưng không thể đọc được các mẫu của người sử dụng khác.
- Các mẫu dành cho các giám sát viên được lưu trên thư mục ***Forms\Supervisors*** và có tên chia sẻ là ***Supervisors.*** Chỉ có các thành viên của nhóm toàn cục ***Supervisors*** mới có khả năng truy cập đến thư mục này.

Nhằm đáp ứng những yêu cầu nói trên, bạn gán các Cấp phép chia sẻ như bảng dưới đây:

Thư mục chia sẻ	Các Cấp phép chia sẻ
Forms	***Everyone***: ***Allow read*** (*cho phép đọc*)
Supervisors	***Supervisors***: ***Allow read*** (*cho phép đọc*)
Username	***Username***: ***Allow change (****cho phép thay đổi****)***

Giả thiết rằng các Cấp phép NTFS cho tất cả các thư mục đều gán Cấp phép ***Modify*** (*thay đổi*) cho nhóm ***Authenticated Users***. Với Cấp phép chia sẻ được gán như trên, những yêu cầu nào dưới đây được đáp ứng? (lựa chọn tất cả các câu trả lời đúng)

a. Tất cả các nhân viên đều có thể tải xuống các mẫu của họ.

b. Tất cả các nhân viên đều có thể tải lên các mẫu đã được điền đầy đủ lên các thư mục của họ.

c. Các nhân viên chỉ đọc được các mẫu của chính họ.

d. Chỉ có các thành viên nhóm ***Authenticated Users*** mới có thể tải xuống các mẫu.

e. Chỉ có các thành viên nhóm ***Supervisors*** mới có thể tải xuống các mẫu dành cho họ.

CHƯƠNG 10: LÀM VIỆC VỚI MÁY IN

Ngoài chia sẻ file, một động lực thúc đẩy khác cho sự phát triển của các mạng LAN đó là khả năng chia sẻ các máy in. Các máy in thường đem đến những phiền toái cho quản trị mạng do chúng không chỉ đơn thuần liên quan đến các thành phần điện tử mà còn liên quan đến các công việc không được sạch sẽ cho lắm như mực in và các tiến trình liên quan đến máy móc như cho giấy vào khay chẳng hạn. Microsoft Windows Server 2003 cung cấp một tập hợp các đặc tính mạnh mẽ nhằm hỗ trợ cho các dịch vụ in ấn trong một tổ chức lớn. Đồng thời các tính năng này cũng giúp bạn tìm hiểu cách thức sử dụng nhằm tối thiểu hóa những rắc rối bạn gặp phải khi có trục trặc xảy ra. Trong chương này, bạn sẽ được học phương pháp cài đặt, quản trị và xử lý sự cố các máy in cục bộ, máy in mạng và máy in Internet.

Hoàn thành chương này bạn có khả năng:

- **Hiểu 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**

TÌM HIỂU VỀ MÔ HÌNH IN ẤN TRONG WINDOWS SERVER 2003

Windows Server 2003 cung cấp các công cụ mạnh mẽ, bảo mật và mềm dẻo cho các dịch vụ in ấn. Bằng cách sử dụng một máy tính cài đặt Windows Server 2003 để quản lý các máy in, các nhà quản trị mạng có thể tạo nên khả năng sẵn sàng đối với các ứng dụng chạy cục bộ trên máy tính đó hoặc các người dùng trên bất kỳ mô hình nào bao gồm các phiên bản trước của Windows cũng như hệ điều hành Novell Netware, UNIX và Macintosh.

Windows Server 2003 và các phiên bản trước của Windows hỗ trợ hai loại máy in:

- **Các máy in được gắn trực tiếp**: là các máy in được kết nối tới một cổng vật lý trên máy chủ in ấn thông thường là cổng USB hoặc cổng song song LPT.
- **Các máy in được gắn vào mạng**: là các máy in được kết nối trực tiếp đến mạng thay vì kết nối tới một cổng vật lý trên một máy tính. Một máy in mạng chứa (hoặc được kết nối tới) một card mạng và hoạt động như một nút trên mạng. Các máy tính liên lạc với máy in bằng cách sử dụng giao thức mạng chuẩn như TCP/IP hoặc DLC chẳng hạn.

Khi bạn cài đặt một máy in trên một máy tính sử dụng Microsoft Windows, hệ điều hành tạo ra một máy in logic mô tả cho thiết bị in ấn vật lý. Máy in logic định nghĩa các đặc tính và cách thức điều khiển của máy in. Nó chứa trình điều khiển máy in, các thiết lập về máy in, các thiết lập in ấn mặc định và các đặc tính khác nhằm điều khiển cách thức một tác vụ in ấn được xử lý ra sao và được gửi tới máy in vật lý như thế nào. Việc ảo hóa máy in thông qua khái niệm máy in logic cho phép các nhà quản trị mềm dẻo và linh hoạt trong việc cấu hình các dịch vụ in ấn.

Sử dụng các máy in gắn trực tiếp

Khi bạn cài đặt một máy in gắn trực tiếp trên máy tính cài đặt Windows Server 2003 (hoặc bất kỳ phiên bản nào của Windows), máy tính đó sẽ sử dụng nó để xử lý các tác vụin ấn. Vì vậy bạn có thể chia sẻ máy in này cho các máy tính khác trên mạng. Khi bạn chia sẻ máy in, máy tính kết nối trực tiếp với máy in sẽ trở thành một ***print server*** (*máy chủ in ấn*). Một máy chủ in ấn là một máy tính (hoặc một thiết bị độc lập) nhận các tác vụtừ các máy trạm

trên mạng, lưu các tác vụ này trong một hàng đợi và gửi từng cái một đến máy in vật lý.

> ***CHÚ Ý: Thuật ngữ in ấn*** *Trong tài liệu trên các phiên bản trước của Windows, máy in vật lý được xem như một thiết bị in ấn và máy in logic được xem như một máy in. Nhằm tránh những sự hiểu lầm về thuật ngữ này, Microsoft đã có những sự thay đổi trong Windows Server 2003. Bây giờ chúng ta sử dụng thuật ngữ máy in* ***(printer)*** *và máy in logic* ***(logical printer)****.*

Sử dụng các máy in gắn vào mạng

Khi bạn đang sử dụng một máy in được gắn vào mạng, bạn có thể sử dụng hai mô hình in ấn trên mạng. Chúng được mô tả trong các phần dưới đây.

Tạo một máy in logic trên tất cả các máy trạm

Trong mô hình này, bạn sẽ cài đặt một máy in logic trên mỗi máy trạm và kết nối trực tiếp chúng tới máy in mạng. Trong trường hợp này không có máy chủ in ấn. Mỗi máy trạm sẽ duy trì các thiết lập in của riêng chúng, xử lý các tác vụ in ấn của chúng và lưu các tác vụ in ấn lên hàng đợi riêng. Trong môi trường mạng, mô hình này có những nhược điểm sau:

- Khi người sử dụng kiểm tra nội dung của hàng đợi, họ chỉ thấy các tác vụ in ấn của chính họ.
- Người sử dụng không thể biết được có những tác vụ nào do những người sử dụng khác được gửi tới máy in.
- Các nhân viên quản trị mạng không thể quản lý tập trung hàng đợi in ấn.
- Các nhân viên quản trị không thể thực hiện các tính năng in ấn tiên tiến như khả năng in trên nhiều máy in khác nhau.
- Các thông báo lỗi chỉ xuất hiện trên các máy tính đang thực hiện tác vụ in ấn.
- Tất cả các tiến trình xử lý tác vụ in ấn đều được hình thành trên máy trạm do đó chúng không thể biết được tình trạng quá tải trên máy chủ in ấn.

Mô hình này có thể phù hợp với mô hình mạng nhóm làm việc (***workgroup***) nhỏ nhưng trong môi trường mạng lớn thì nó không thể cung cấp khả năng quản trị tập trung. Ưu điểm duy nhất của mô hình này đó là dễ dàng cài đặt kể cả đối với người sử dụng đầu cuối. Mỗi máy trạm cài đặt máy in theo phương

pháp thông thường và không cần quan tâm đến các máy trạm khác (ngoại trừ khi đợi các tác vụ in ấn của chúng hoàn thành).

Tạo một máy chủ in ấn

Do những nhược điểm của mô hình nói trên nên cấu trúc in ấn thông dụng nhất dành cho các tổ chức lớn đó là mô hình gồm ba phần. Mô hình này gồm có các thành phần sau:

- Máy in vật lý
- Máy chủ in ấn bao gồm một máy in logic được kết nối tới máy in vật lý.
- Máy khách in ấn được kết nối tới máy in logic của máy chủ.

In ấn thông qua một máy chủ in ấn mang lại những ưu điểm sau:

- Máy in trên máy chủ in ấn định nghĩa các thiết lập in ấn và quản trị các trình điều khiển.
- Máy in logic sử dụng một hàng đợi in duy nhất và các máy trạm đều có thể nhìn được hàng đợi này. Do đó các nhân viên quản trị mạng và người sử dụng đều có thể thấy được danh sách đầy đủ các tác vụ in ấn đang chờ đợi.
- Các bản thông báo như hết giấy hoặc kẹt giấy được gửi tới tất cả các máy trạm do đó người sử dụng và các nhân viên quản trị có thể thực hiện xử lý sự cố.
- Hầu hết các ứng dụng và các trình điều khiển máy in đều có thể phân nhỏ tiến trình in ấn trước khi gửi tới máy chủ in ấn. Điều này gia tăng sự phản hồi của máy trạm. Tức là, khi một máy trạm thực hiện in một tài liệu, tác vụ in sẽ được gửi ngay lập tức đến máy chủ in và kiểm soát các phản hồi của máy tính tới người sử dụng trong khi máy chủ in đảm nhận tác vụ xử lý công việc in ấn.
- Các chức năng bảo mật, kiểm định và kiểm tra, giám sát và ghi nhật ký được quản trị tập trung.

TRIỂN KHAI MÁY IN CHIA SẺ

Tiến trình triển khai một máy in chia sẻ sử dụng mô hình máy chủ in bao gồm các bước sau:

- Cài đặt máy in trên máy chủ in ấn
- Tạo một chia sẻ máy in trên máy chủ in ấn

- Kết nối các máy trạm với máy chủ in ấn

Các bước nói trên được mô tả chi tiết trong các phần sau.

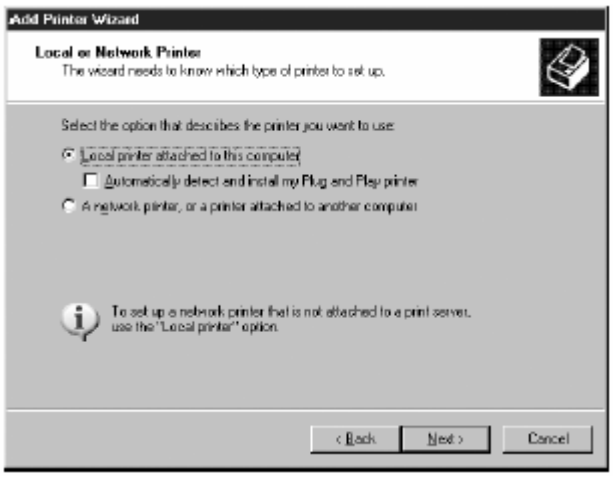
Cài đặt một máy chủ in ấn Windows Server 2003

Bước đầu tiên trong việc triển khai một máy chủ in ấn trên mạng là cài đặt máy in trên máy tính đóng vai trò như một máy chủ in ấn. Quá trình này không khác với việc cài đặt một máy in trên máy tính thông thường. Thực hiện công tác chia sẻ máy in sẽ cho phép Windows Server 2003 hoạt động như một máy chủ in ấn.

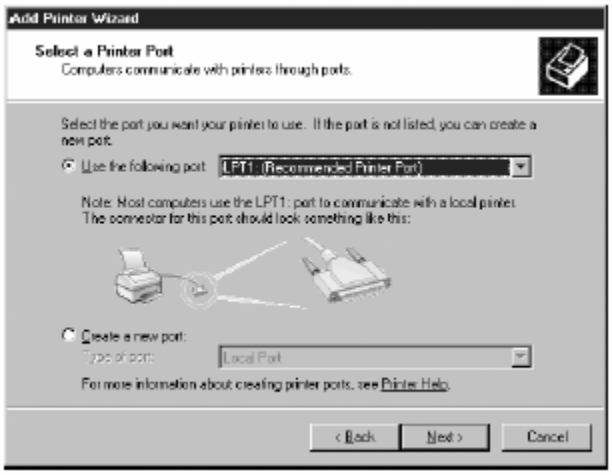
Trong Windows Server 2003, bạn quản trị các máy in bằng cách sử dụng màn hình ***Printers And Faxes*** từ ***Control Panel*** hoặc từ thực đơn ***Start***. Kích đúp vào biểu tượng ***Add Printer***, trình hướng dẫn ***Add Printer*** xuất hiện. Sau khi nhấp ***Next*** để bỏ qua trang ***Welcome***, bạn sẽ hoàn thành các trang còn lại trong trình hướng dẫn được mô tả danh sách dưới đây.

> ***CHÚ Ý Sử dụng các máy in USB*** *Các máy in kết nối tới máy tính thông qua cổng USB không yêu cầu bạn khởi tạo trình hướng dãn* ***Add Printer*** *bằng tay. Do các thiết bị USB là* ***plug and play*** *nên máy tính sẽ tự động phát hiện và cài đặt chúng. Tuy nhiên, bạn có thể cung cấp các trình điều khiển không được Microsoft hỗ trợ cho các máy in.*

- **Local Or Network Printer** (*máy in mạng hay cục bộ*) Trong trang này, bạn cần xác định bạn đang cài đặt một máy in cục bộ hay một máy in mạng. Trong ngữ cảnh của trình hướng dẫn này, máy in cục bộ được xem như một máy in vật lý được gắn trực tiếp vào một máy tính hoặc được gắn vào mạng nhưng hiện nay chưa được chia sẻ bởi máy chủ in ấn khác. Máy in mạng được xem như một máy in chia sẻ bởi máy tính khác trên mạng. Vì vậy để cài đặt một máy chủ in ấn, bạn luôn luôn lựa chọn ***Local Printer Attached To This Computer*** (*máy in cục bộ được gắn với máy tính này*). Nếu máy in này hiện đã được kết nối và sẵn sàng, bạn có thể lựa chọn hộp kiểm tra ***Automatically Detect And Install My Plug And Play Printer*** (*tự động phát hiện và cài đặt máy in plug and play*) để cài đặt máy in tự động. Tuy nhiên, bạn cũng có thể cài đặt máy in logic mà không cần có sự hiện diện của một máy in vật lý.



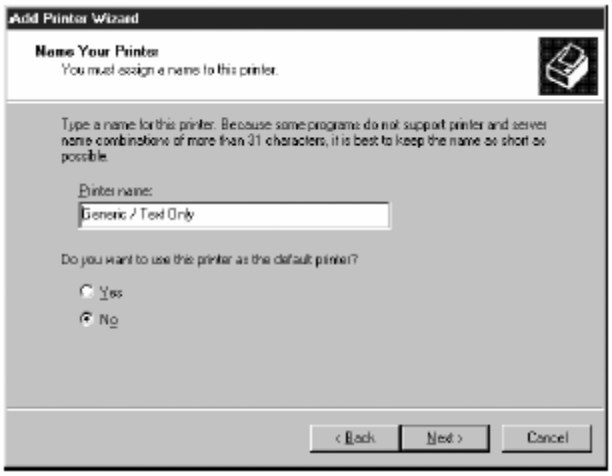
- **Select A Printer Port** (*lựa chọn cổng máy in*) Trong trang này, bạn sẽ xác định máy tính liên kết với máy in như thế nào. Nếu máy in được kết nối tới cổng LPT (cổng song song) hoặc cổng COM (cổng nối tiếp), bạn sẽ lựa chọn ***Use The Following Port*** (*sử dụng cổng dưới đây*) từ danh sách thả xuống. Nếu máy in được kết nối bằng một số phương tiện khác, bạn lựa chọn ***Create A New Port*** (*tạo một cổng mới*) và lựa chọn một trong các kiểu cổng từ danh sách thả xuống. Ví dụ, các máy in được gắn vào mạng thông thường yêu cầu một cổng TCP/IP. Khi bạn lựa chọn ***Standard TCP/IP Port*** (*cổng TCP/IP chuẩn*), trình hướng dẫn ***Add Standard TCP/IP Printer Port*** (*thêm cổng máy in TCP/IP chuẩn*) xuất hiện. Ở đó bạn sẽ xác định địa chỉ IP mà bạn gán cho máy in và nếu cần thiết bạn có thể gán loại giao diện mạng dùng để kết nối máy in tới mạng.



- **Install Printer Software** (*cài đặt phần mềm máy in*) Nếu tính năng plug and play không phát hiện và cài đặt chính xác trình điều khiển cho máy in, bạn có thể lựa chọn máy in của bạn từ một danh sách các trình

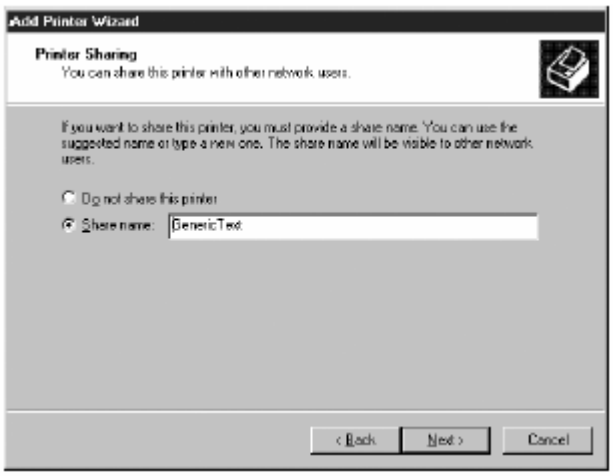
điều khiển máy in được phân loại theo nhà sản xuất và các model sẵn có trên Windows Server 2003. Nếu máy in không xuất hiện trong danh sách nói trên, bạn có thể nhấp *Have Disk* để cài đặt các trình điều khiển máy in do nhà sản xuất thiết bị cung cấp.

- **Name Your Printer** (*tên máy in của bạn*) Trong trang này, bạn cần xác định tên cho máy in nhằm cung cấp cho các ứng dụng chạy trên máy tính. Mặc định, trình hướng dẫn sẽ gán một tên dựa trên tên nhà sản xuất và chủng loại kết hợp với trình điều khiển máy in được cài đặt nhưng bạn có thể thay đổi tên này. Nhằm tương thích đầy đủ với các ứng dụng, bạn nên hạn chế chiều dài tên máy in (tối đa 31 ký tự). Khi các máy in khác được cài đặt, trang này còn cho phép bạn xác định máy in nào là máy in mặc định trên máy tính này có nghĩa là các ứng dụng sẽ tự động in trên máy in đó trừ phi bạn lựa chọn cái khác. Thiết lập này chỉ áp dụng cho các ứng dụng chạy trên máy tính cục bộ mà thôi chứ không áp dụng cho các máy trạm trên mạng.

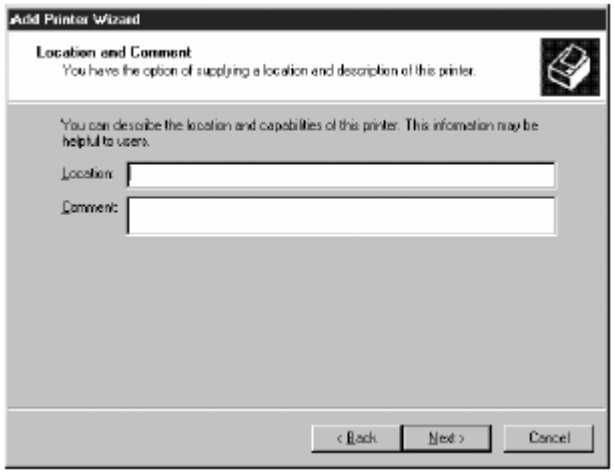


- **Printer Sharing** (*chia sẻ máy in*) Trong trang này, bạn cần xác định bạn có muốn chia sẻ máy in này không để làm cho nó hoạt động như một máy chủ in ấn. Để tạo một máy in chia sẻ, bạn lựa chọn ***Share Name*** và xác định tên dùng để công bố trên mạng. Mặc định, trình hướng dẫn sẽ gán một tên bao gồm 8 ký tự đầu tiên của tên bạn cung cấp ở trang trước tuy nhiên bạn có thể sử dụng bất kỳ tên nào mà bạn muốn. Nhằm mục đích tương thích, tốt nhất tên máy in không chứa các ký tự trống.

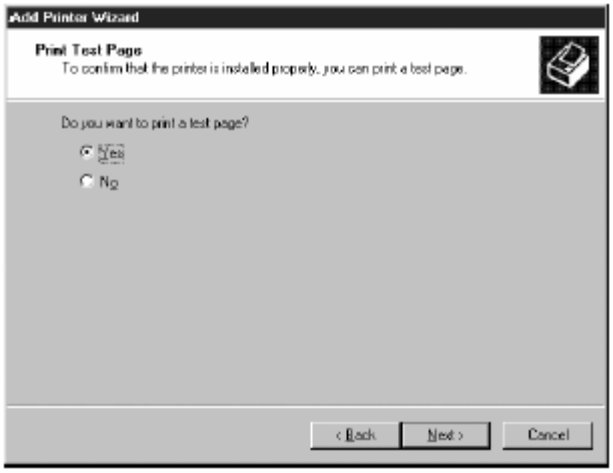
  CHÚ Ý ***Các máy in chia sẻ*** *Trang* ***Printer Sharing*** *trong trình hướng dẫn* ***Add Printer*** *chỉ cung cấp các chức năng chia sẻ máy in cơ bản nhất. Để cấu hình các lựa chọn chia sẻ khác, bạn phải sử dụng hộp thoại* ***Properties*** *của máy in được mô tả trong phần kế tiếp.*



- **Location And Comment** (*vị trí và chú thích*) Trang này chứa các trường mà bạn có thể cung cấp thông tin về vị trí hay khả năng của máy in. Thông tin này sẽ hiển thị khi người sử dụng duyệt mạng và giúp cho họ xác định máy in chính xác.



- **Print Test Page** (*in trang kiểm tra*) Trang này cho phép bạn thực hiện một tác vụ in kiểm tra nhằm xác định xem máy tính kết nối với máy in như thế nào.



Khi bạn hoàn thành trình hướng dẫn ***Add Printer***, hệ thống sẽ cài đặt trình điều khiển máy in tương ứng và tạo một biểu tượng máy in logic cho máy in này trong cửa sổ ***Printers And Faxes***. Bạn sẽ sử dụng biểu tượng này để truy cập đến tất cả các công cụ cấu hình và duy trì máy in. Từ thời điểm này, các ứng dụng trên máy tính cục bộ có thể sử dụng máy in và nếu bạn chia sẻ nó thì các máy trạm trên mạng cũng có thể sử dụng nó.

Chia sẻ máy in

Bạn có thể chia sẻ một máy in bằng cách sử dụng trình hướng dẫn ***Add Printer*** nhưng bạn có thể điều khiển chia sẻ này nhiều hơn nữa bằng cách sử dụng thẻ ***Sharing*** trong hộp thoại ***Properties*** của máy in (xem hình vẽ 10-1). Để truy cập tới thẻ này, lựa chọn một biểu tượng máy in trong cửa sổ ***Printers And Faxes*** và chọn ***Sharing*** từ thực đơn ***File***.

Hình 10-1: Thẻ Sharing trong hộp thoại Properties của một máy in

Để chia sẻ máy in (nếu nó chưa được chia sẻ) lựa chọn ***Share This Printer*** (*chia sẻ máy in này*) và xác định tên chia sẻ trong hộp văn bản ***Share Name***.

Bạn cũng có thể lựa chọn hộp kiểm tra ***List In The Directory*** (*liệt kê trong dịch vụ thư mục Active Directory*) để tạo một đối tượng máy in trong Active Directory. Kết quả là một đối tượng máy in được tạo ra như một con trỏ cho phép người sử dụng xác định một máy in bằng cách tìm kiếm trên dịch vụ dựa theo tên hoặc các tính năng của nó. Một trong những ích lợi của các tham số trong trường ***Location*** và các đặc tính tương tự đó là tăng cường khả năng tìm kiếm một máy in dựa trên các đặc tính này.

Nhấp vào ***Additional Drivers*** để mở hộp thoại ***Additional Drivers,*** như hình vẽ 10-2. Khi một máy trạm trên mạng truy cập đến một máy in chia sẻ, nó có thể tự động tải về trình điều khiển máy in từ thư mục chia sẻ ***Print$*** trên máy chủ. Đây là tính năng mà Windows gọi là ***Point and Print*** (trỏ tới và in). Hộp thoại này cho phép bạn cài đặt các trình điều khiển máy in cho các hệ điều hành khác nhau mà máy trạm của bạn có thể sử dụng. Đây là ưu điểm nếu máy in sử dụng các trình điều khiển không có trong Windows Server 2003. Khi bạn lựa chọn các hệ điều hành khác trong hộp thoại này và nhấp OK, hệ thống sẽ cài đặt các trình điều khiển yêu cầu và thông báo cho bạn đưa đĩa chứa trình điều khiển của nhà sản xuất nếu cần thiết.

Hình 10-2: Hộp thoại Additional Drivers

> ***CHÚ Ý Cập nhật các trình điều khiển*** *Các máy trạm cài đặt hệ điều hành Windows NT, Windows 2000, Windows XP và Windows Server 2003 sẽ tải trình điều khiển máy in từ máy chủ in ấn về khi kết nối tới máy in chia sẻ lần đầu tiên. Mỗi lần in, chúng xác nhận rằng đã có trình điều khiển máy in và nếu không có chúng sẽ tải một trình điều khiển cập nhật từ máy chủ. Với các máy trạm này, bạn chỉ cần giữ các cập nhật của trình điều khiển máy in trên máy chủ in ấn. Các máy trạm cài đặt Windows 95, Windows 98 và Windows Me có thể tự động tải về và cài đặt các trình điều khiển khi chúng kết nối tới máy in chia sẻ lần đầu tiên nhưng sau đó chúng sẽ không kiểm tra các cập*

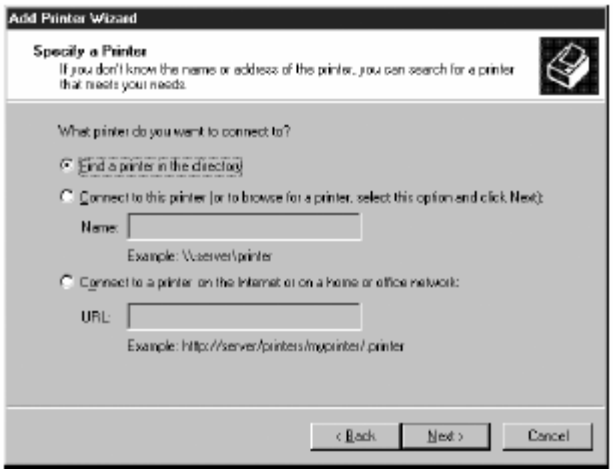
nhật. Nếu bạn nhận được một cập nhật của trình điều khiển, bạn phải cài đặt nó bằng tay trên các máy trạm này cũng như trên máy chủ.

Kết nối các máy trạm đến một máy chủ in ấn

Khi bạn đã cài đặt một máy in và chia sẻ nó thì các máy trạm có thể truy cập tới máy in này thông qua mạng. Chúng có thể truy cập đến máy in theo vài cách khác nhau được mô tả trong phần dưới đây.

Sử dụng trình hướng dẫn Add Printer

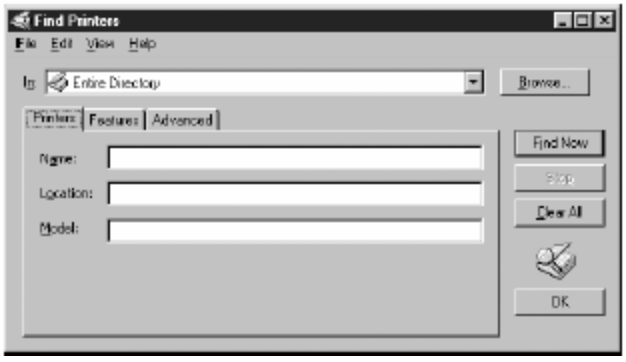
Tiến trình cài đặt một máy in trên máy trạm bằng cách sử dụng trình hướng dẫn ***Add Printer*** cũng tương tự như bạn cài đặt trên một máy chủ in ấn. Chỉ khác một chút đó là khi cài đặt trên máy chủ trong trang ***Local Or Network Printer***, bạn lựa chọn ***A Network Printer*** hoặc ***A Printer Attached To Another Computer*** thì bây giờ trên máy trạm bạn phải xác định máy in muốn sử dụng trong trang ***Specify A Printer*** (hình vẽ 10-3).



Hình vẽ 10-3: Trang Specify A Printer của trình hướng dẫn Add Printer

Các phương pháp được liệt kê ở dưới đây sẽ giúp bạn xác định một máy in:

- **Find A Printer In The Directory** (*tìm kiếm một máy in trong dịch vụ thư mục*) Nếu máy trạm gia nhập vào ***Miền*** Active Directory, trang này sẽ hiển thị lựa chọn này. Với lựa chọn này, trình hướng dẫn sẽ hiển thị hộp thoại ***Find Printers*** giúp bạn tìm kiếm các máy in theo tên, vị trí hoặc các đặc tính khác mà bạn xác định khi tạo các đối tượng máy in.



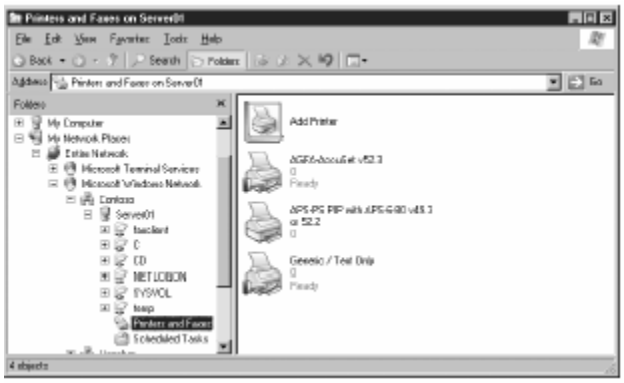
- **Browse For A Printer** (*duyệt máy in*) Nếu máy trạm là thành viên của một nhóm làm việc (***workgroup***), trang ***Printer*** sẽ hiển thị lựa chọn này đầu tiên. Với lựa chọn này, trình hướng dẫn sẽ hiển thị trang ***Browse For Printer*** cho phép bạn duyệt các máy tính xác định trong các ***Miền*** hoặc các nhóm làm việc và lựa chọn các máy in chia sẻ được cài đặt trên mỗi máy tính.
- **Connect To This Printer** (*kết nối tới máy in này*) Chọn lựa chọn này cho phép bạn xác định tên của một máy in chia sẻ trên mạng bằng cách sử dụng đường dẫn UNC (***Universal Naming Connvention*** – *quy ước đặt tên tổng hợp*) như ***\\tênmáychủ\tênmáyinchiasẻ.*** Nhấp ***Next*** mà không cần xác định tên tương tự như lựa chọn ***Browse For A Printer*** thực hiện trong trang ***Browse For Printer***.
- **Connnect To A Printer On The Internet Or On A Home Or Office Network** (*Kết nối tới một máy in trên Internet hay mạng ở nhà hoặc mạng văn phòng*) Lựa chọn này cho phép bạn xác định tên của một máy in ở trên mạng hoặc trên Internet bằng cách sử dụng một URL (***Uniform Resouce Locator*** – *quy ước đặt tên chuẩn hướng tới một trạm Internet hoặc mạng nội bộ*) như ***http://www.adatum.com/printers/printername.***

Một khi bạn đã xác định chính xác máy in cần cài đặt, trình hướng dẫn sẽ cài đặt trình điều khiển tương ứng (giả thiết rằng trình điều khiển này đã sẵn có trên máy chủ hoặc máy trạm) và tạo ra một máy in logic trong cửa sổ ***Printers And Faxes***.

Duyệt trong Windows Explorer

Bạn có thể cài đặt đơn giản một máy in chia sẻ trên một máy trạm bằng cách duyệt trong ***My Network Places*** thông qua ***Windows Explorer***. Khi bạn mở rộng một biểu tượng máy tính trong ***My Network Places***, Windows Server 2003 sẽ hiển thị một danh sách các chia sẻ trên máy tính đó. Các máy in chia

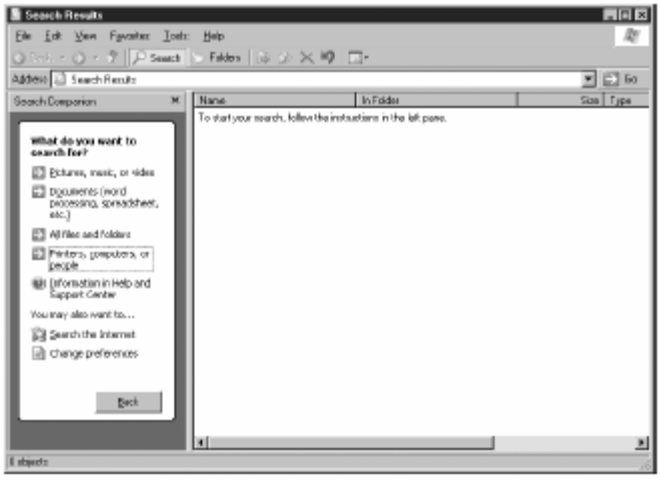
sẻ được hiển thị trong một khoang chứa có tên là ***Printers And Faxes*** (xem hình vẽ 10-4). Lựa chọn một máy in chia sẻ, từ thực đơn ***File*** chọn ***Connect*** để bắt đầu tiến trình cài đặt trình điều khiển máy in logic.



Hình 10-4: Duyệt các máy in trong Windows Explorer

Tìm kiếm trong Active Directory

Đối với các máy trạm trong các Miền Active Directory , trình hướng dẫn ***Add Printer*** sẽ cung cấp khả năntg tìm kiếm các đối tượng máy in trong dịch vụ thư mục. Bạn có thể tìm kiếm chúng theo nhiều cách khác nhau trong Active Directory như thực đơn ***Start*** trong trang ***Search*** chính. Khi bạn lựa chọn ***Other Search Options***, trang này cho phép bạn xác định các cách tìm kiếm khác nhau bao gồm một lựa chọn ***Printers, Computers, Or People*** như hình vẽ 10-5. Lựa chọn để tìm kiếm một máy in trên mạng sẽ hiển thị hộp thoại ***Find Printers*** giống như trình hướng dẫn ***Add Printer*** hiển thị. Bạn có thể truy cập đến hộp thoại này theo nhiều cách khác nhau thông qua giao diện Windows Server 2003.



Hình 10-5: Tìm kiếm các máy in trong Active Directory

CẤU HÌNH CÁC ĐẶC TÍNH MÁY IN

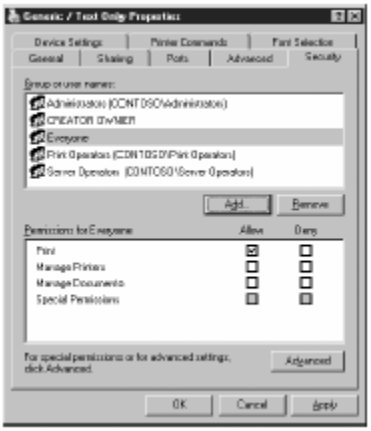
Sau khi cài đặt máy in logic trên máy chủ in ấn, bạn có thể cấu hình một loạt các đặc tính bằng cách mở hộp thoại ***Properties*** của máy in (xem hình vẽ 10-6). Một số điều khiển trong hộp thoại này là giống hệt nhau đối với tất cả các máy in nhưng một số cái được trình điều khiển máy in cung cấp được đặc trưng theo từng chủng loại sản phẩm. Ví dụ, một máy in màu có thể có các điều khiển quản lý màu trong khi đó các máy in đen trắng lại không cần.

Hình 10-6: Thẻ General trong hộp thoại Properties của máy in

Thẻ ***General*** cho phép bạn cấu hình tên máy in, vị trí và các lời chú thích. Tất cả các thông số này đều được cấu hình dựa trên các giá trị bạn đưa vào trong trình hướng dẫn ***Add Printer***. Như đã đề cập ở trên, thẻ ***Sharing*** cho phép bạn xác định máy in logic đã được chia sẻ chưa và cho phép các máy trạm trên mạng truy cập chưa. Một số chức năng khác, bạn có thể điều khiển trong hộp thoại ***Properties***, sẽ được đề cập trong các phần dưới đây.

Kiểm soát bảo mật máy in

Với các hệ thống file chia sẻ, bạn có thể sử dụng các Cấp phép để gán truy cập nhất định đến chúng. Với các máy in chia sẻ bạn cũng thực hiện tương tự thông qua thẻ ***Security*** trên hộp thoại ***Properties*** của máy in như hình vẽ 10-7.



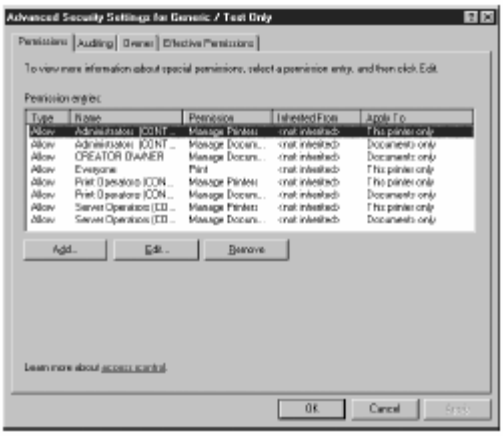
Hình 10-7: Thẻ Security trên hộp thoại Properties của một máy in

Các Cấp phép chuẩn mà bạn có thể gán cho một máy in gồm có:

- **Print** (*in ấn*) cho phép các đối tượng bảo mật kết nối tới máy in và thực hiện các tác vụ in ấn trên đó. Mặc định nhóm ***Everyone*** được gán Cấp phép này. Để hạn chế việc truy cập tới máy in bạn có thể loại bỏ Cấp phép này khỏi nhóm ***Everyone*** và gán nó cho các đối tượng bảo mật khác hoặc bạn có thể ngăn cấm đối với các đối tượng cụ thể.
- **Manage Printers** (*quản trị máy in*) cho phép các đối tượng bảo mật thực hiện tất cả các công việc mà Cấp phép ***Print*** cung cấp đối tượng bảo mật đồng thời cung cấp Cấp phép điều khiển quản trị máy in. Đối tượng nhận Cấp phép này có thể thay đổi các đặc tính máy in, dừng và khởi động lại máy in, điều khiển trạng thái chia sẻ máy in, điều chỉnh các thiết lập bộ đệm (một chương trình tiện ích của hệ điều hành cho phép lưu trữ tạm thời các lệnh in vào một file trên đĩa hoặc RAM khi máy đang bận sau đó sẽ gửi tới máy in khi CPU rảnh) và thay đổi các Cấp phép máy in. Mặc định trên một máy tính không phải là Máy chủ Điều khiển Miền nhóm ***Administrators*** và ***Power Users*** được gán Cấp phép này còn trên máy Máy chủ Điều khiển Miền các nhóm ***Server Operators*** và ***Print Operators*** sẽ có Cấp phép này.
- **Manage Documents** (*quản trị tài liệu*) cho phép các đối tượng bảo mật điều khiển các tài liệu trong hàng đợi như: dừng, phục hồi, khởi tạo lại, loại bỏ hoặc sắp xếp lại thứ tự. Tuy nhiên Cấp phép này không cung cấp khả năng gửi tài liệu tới máy in hoặc điều khiển trạng thái máy in. Mặc định, nhóm ***Creater Owner*** được gán Cấp phép này. Cấp phép gán cho nhóm ***Creator Owner*** được kế thừa từ

người tạo ra đối tượng đó nên Cấp phép này cho phép người sử dụng quản lý các tác vụ in ấn mà họ tạo ra. Cấp phép này cũng được gán cho các nhóm ***Administartors, Print Operators*** và ***Server Operators*** nên thành viên của các nhóm này có thể điều khiển bất cứ tài liệu nào trên hàng đợi. Trên các máy không phải Máy chủ Điều khiển Miền, nhóm ***Power Users*** được gán Cấp phép này.

Ngoài việc cung cấp các Cấp phép chuẩn, thẻ ***Security*** còn cho phép truy cập đến hộp thoại ***Advanced Security Settings*** (xem hình vẽ 10-8). Ở đó bạn có thể sử dụng để quản trị các chỉ mục ACL riêng lẻ và làm việc trên các Cấp phép đặc biệt giống như bạn đang làm việc với các Cấp phép NTFS. Tuy nhiên không giống như NTFS các Cấp phép đặc biệt cho máy in chỉ có thêm ba tính năng cho phép các đối tượng bảo mật đọc các Cấp phép, thay đổi các Cấp phép và đoạt quyền sở hữu một máy in.



Hình 10-8: Hộp thoại Advanced Security Settings

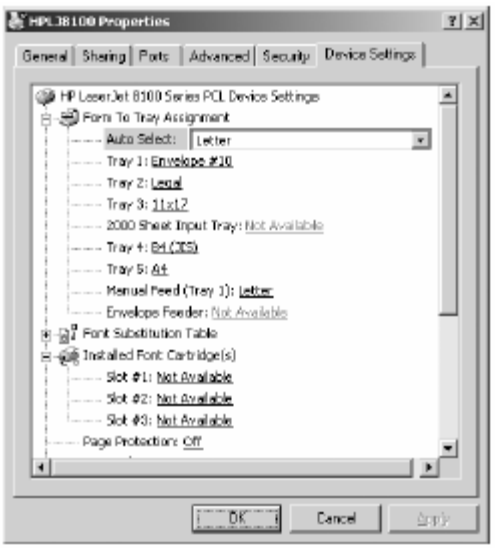
CHÚ Ý Thông tin thêm *Xem chương 9 để biết rõ hơn về việc sử dụng các Cấp phép chuẩ và đặc biệt để điều khiển truy cập tới các tài nguyên hệ thống.*

Thiết lập các định dạng cho khay giấy

Nếu một máy in có nhiều khay cho phép bạn sử dụng các kích thước giấy khác nhau, bạn có thể thiết lập một định dạng cho một khay xác định. Định dạng dùng để định nghĩa kích thước giấy in. Khi người sử dụng in một tài liệu với định dạng trang in xác định, Windows Server 2003 sẽ định tuyến tác vụ in ấn đó đến khay tương ứng với kích thước đó. Ví dụ về các định dạng gồm có: ***Legal, Letter, A4, Envelope*** và ***Executive***.

Để gán một định dạng cho một khay, lựa chọn thẻ ***Device Settings*** trên hộp thoại ***Properties*** của máy in (hình vẽ 10-9). Số lượng các khay hiển thị trong

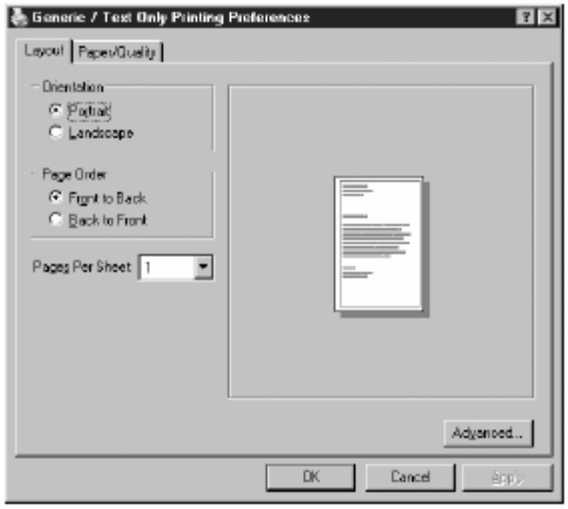
phần ***Form To Tray Assignment*** phụ thuộc vào loại máy in mà bạn cài đặt và số lượng khay nó hỗ trợ. Với mỗi khay liệt kê, bạn có thể lựa chọn một định dạng khác nhau. Ngoài ra, khi mở rộng cây ***Device Settings*** bạn sẽ thấy các thiết lập cho phép xác định trạng thái cài đặt của các lựa chọn máy in như các khay giấy thêm vào, các thành phần điều khiển giấy in, phông chữ và bộ nhớ máy in. Tất cả các thiết lập này đều được dành cho máy in và phụ thuộc vào khả năng của nó cũng như trình điều khiển.



Hình 10-9: Thẻ Device Settings trên hộp thoại Properties của máy in

Thiết lập các tác vụ in ấn mặc định

Thẻ ***General*** trên hộp thoại ***Properties*** của máy in có lựa chọn ***Printing Preferences*** và thẻ ***Advanced*** có lựa chọn ***Printing Defaults***. Cả hai lựa chọn này đều hiển thị hộp thoại cho phép bạn điều khiển cách thức thực hiện các tác vụ in ấn trên máy in logic bao gồm định dạng kiểu in (in theo khuôn dạng nằm ngang hay nằm dọc), in hai mặt (nếu máy in hỗ trợ tính năng này), độ phân giải và các thiết lập tài liệu in ấn khác như hình vẽ 10-10. Các hộp thoại này giống nhau và cũng giống hộp thoại hiển thị khi bạn nhấp ***Properties*** hoặc ***Preferences*** trên hộp thoại ***Print*** của ứng dụng.



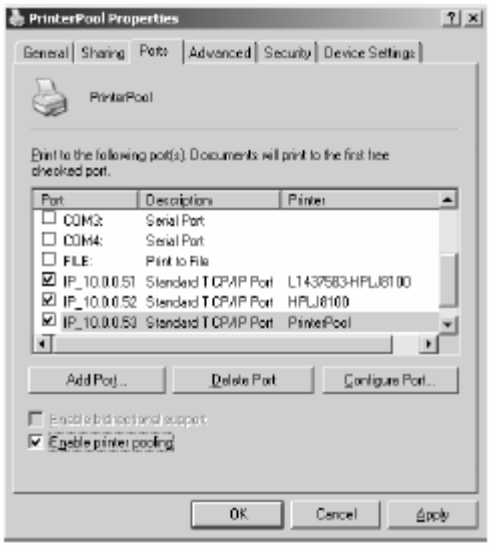
Hình 10-10: Hộp thoại Printing Preferences

Sự tồn tại của ba hộp thoại riêng biệt với các điều khiển giống nhau không phải là sự nhầm lẫn hay dự phòng. Hộp thoại ***Printing Defaults*** cấu hình các thiết lập mặc định cho tất cả người sử dụng của máy in logic. Nếu máy in được chia sẻ, các thiết lập in ấn mặc định này sẽ trở thành các đặc tính mặc định cho tất cả các máy in trên máy trạm. Hộp thoại ***Printing Preferences*** dùng để cấu hình cho một đối tượng cụ thể. Nếu có xung đột xảy ra thì với quyền ưu tiên cao hơn các thiết lập trong ***Printing Preferences*** sẽ được cấp cho người sử dụng. Hộp thoại ***Properties*** hoặc ***Preferences*** trên các ứng dụng dùng để cấu hình các đặc tính dành cho tác vụ in ấn mà ứng dụng đó xử lý. Các đặc tính trong các hộp thoại này sẽ quyền ưu tiên cao hơn hai hộp thoại nêu ở trên (***Printing Defaults*** và ***Printing Preferences***).

Tạo một tổ hợp máy in (*Printer Pool*)

Tổ hợp máy in là một máy in logic hỗ trợ nhiều máy in vật lý. Các máy in vật lý có thể được gắn vào máy chủ hay vào mạng hoặc cả hai. Khi bạn tạo một tổ hợp máy in, máy chủ in ấn sẽ gửi các tác vụ in ấn được xác nhận phía máy trạm tới máy in sẵn sàng đầu tiên. Máy in logic đại diện cho tổ hợp máy in sẽ kiểm tra cổng nào đang sẵn sàng và hướng tác vụ in đến cổng đó.

Bạn cấu hình tổ hợp máy in trong thẻ ***Ports*** trên hộp thoại ***Properties*** của máy in. Nếu bạn lựa chọn hộp kiểm tra ***Enable Printer Pooling***, bạn có thể xác định nhiều cổng chứa các thiết bị in ấn thuộc một tổ hợp. Hình vẽ 10-11 biểu diễn một tổ hợp máy in được kết nối tới ba máy in gắn vào mạng.



Hình 10-11: Thẻ Ports trên hộp thoại Properties của máy in biểu diễn một tổ hợp với ba máy in vật lý

> ***CHÚ Ý Những yêu cầu về phần cứng*** *Do một tổ hợp máy in gồm có nhiều máy in vật lý được điều khiển bởi một máy in logic duy nhất nên chỉ có một trình điều khiển được cài đặt. Trong khi đó các máy in vật lý không giống nhau hoàn toàn và chúng phải tương thích với trình điều khiển được cài đặt trên máy in logic.*

Cấu hình nhiều máy in logic trên một máy in vật lý

Trong khi một tổ hợp máy in là một máy in logic duy nhất được kết nối tới nhiều máy in vật lý thì ngược lại cấu trúc nhiều máy in logic kết nối tới một máy in vật lý duy nhất thông dụng hơn và mạnh hơn. Bằng cách tạo ra nhiều máy in logic hướng trực tiếp các tác vụ in ấn tới cùng một máy in vật lý, bạn có thể cấu hình các đặc tính khác nhau, các thiết lập in mặc định, các thiết lập mặc định, cơ chế kiểm soát và ghi lại, giám sát với mỗi máy in logic.

Ví dụ, bạn muốn các cán bộ điều hành trong công ty có thể thực hiện các tác vụ in ngay lập tức bất kể các tác vụ khác đang được thực thi bởi người sử dụng khác. Để làm được điều này, bạn có thể tạo ra một máy in logic thứ hai trỏ tới cùng một máy in vật lý nhưng với mức độ ưu tiên cao hơn.

Để thực hiện điều này, bạn chỉ cần sử dụng trình hướng dẫn ***Add Printer*** để tạo thêm các máy in logic sử dụng cùng một cổng với máy in logic đầu tiên. Mỗi máy in logic phải có một tên và tên chia sẻ duy nhất. Tiếp theo bạn cấu hình riêng rẽ các máy in logic với các thiết lập phù hợp với các máy trạm sẽ sử dụng máy in logic đó.

Để cấu hình các đặc tính khác nhau cho các máy in logic, bạn lựa chọn thẻ ***Advanced*** trên hộp thoại ***Properties*** (hình vẽ 10-12) và xác định một giá trị trong trường ***Priority*** (*độ ưu tiên*) nằm trong dải từ 1 (độ ưu tiên thấp nhất) đến 99 (độ ưu tiên cao nhất). Nếu bạn gán giá trị 99 cho máy in logic của các cán bộ điều hành và 1 cho máy in logic của những người sử dụng khác, thì các tài liệu gửi tới máy in logic với độ ưu tiên 99 sẽ được thực hiện trước các tài liệu khác trong hàng đợi. Tuy nhiên như thế không có nghĩa là tài liệu của cán bộ điều hành sẽ loại bỏ tác vụ in ấn của người sử dụng khác mà ở đây muốn đề cập khi máy in rỗi, nó sẽ chấp nhận các tác vụ từ máy in logic có độ ưu tiên cao hơn trước khi chấp nhận các tác vụ từ máy in logic có độ ưu tiên thấp hơn. Để ngăn không cho người sử dụng thực hiện in ấn trên máy in logic của cán bộ điều hành, bạn có thể cấu hình ACL của nó và loại bỏ Cấp phép in được gán cho nhóm ***Everyone***, thay vào đó chỉ cấp cho các cán bộ điều hành Cấp phép in.

Hình 10-12: Thẻ Advanced trên hộp thoại Properties của máy in

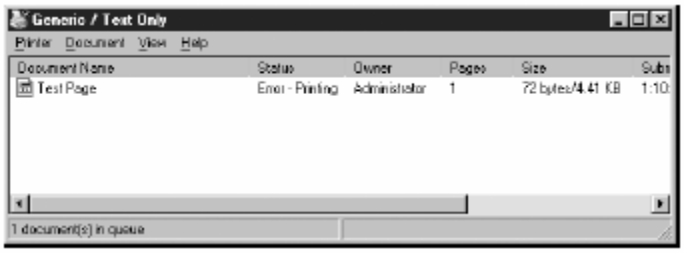
GIÁM SÁT CÁC MÁY IN

Một khi bạn đã tạo, cấu hình và chia sẻ máy in cục bộ trên máy chủ in ấn cũng như các máy trạm trên mạng đã kết nối tới máy các máy in này thì bạn phải bắt đầu xem xét các công việc quản trị chúng trong suốt quá trình in ấn. Các phần dưới đây mô tả các công cụ khác nhau được Windows Server 2003 cung cấp giúp bạn giám sát tiến trình in ấn trên mạng khi cần thiết.

> ***CHÚ Ý: Mục tiêu của kỳ thi*** *Các mục tiêu cho kỳ thi 70-290 yêu cầu các học viên có khả năng "giám sát các máy chủ file và in ấn. Các công cụ gồm có* ***Task Manager, Event Viewer*** *và* ***System Monitor****".*

Giám sát các hàng đợi in

Kích đúp vào một biểu tượng máy in trong màn hình ***Printers And Faxes*** sẽ mở ra một cửa sổ khác có tiêu đề là tên của máy in (xem hình vẽ 10-13). Đây là cửa sổ hàng đợi in, nó liệt kê tất cả các tác vụ hiện nay đang đợi để gửi tới máy in vật lý. Tùy thuộc vào Cấp phép của mình trên máy in, người sử dụng có thể can thiệp vào hàng đợi máy in và các tác vụ in ấn theo nhiều cách khác nhau và các mức khác nhau bằng cách sử dụng các thực đơn trên cửa sổ. Các công việc chung mà người sử dụng và người quản trị thực hiện bao gồm: dừng, khôi phục, loại bỏ các tác vụ cụ thể trong hàng đợi, sắp xếp lại thứ tự các tác vụ, dừng và khôi phục hàng đợi xác định.



Hình 10-13: Cửa sổ hàng đợi in

> ***CHÚ Ý Mục tiêu của kỳ thi*** *Các mục tiêu cho kỳ thi 70-290 yêu cầu các học viên có khả năng "quản lý các hàng đợi in"*

Định hướng lại các tác vụ in ấn

Nếu một máy in gặp trục trặc, bạn có thể gửi tài liệu trong hàng đợi trên máy in đó tới một máy in khác được kết nối tới một cổng cục bộ trên máy tính hoặc được gắn vào mạng. Động tác này gọi là định hướng lại tác vụ in ấn. Định hướng lại cho phép người sử dụng tiếp tục gửi các tác vụ tới một máy in logic cùng loại và tránh cho người sử dụng phải thực hiện lại tác vụ in.

Để định hướng lại một máy in, đơn giản bạn có thể thay đổi cổng mà ở đó máy in logic đang gửi tác vụ tới. Bạn thực hiện điều này bằng cách mở hộp thoại ***Properties*** của máy in, lựa chọn thẻ ***Ports*** và chọn một cổng khác hoặc thêm một cổng mới. Hộp kiểm tra chứa cổng kết nối tới máy in bị lỗi ngay lập tức bị xóa đi trừ phi tổ hợp máy in được lựa chọn. Trong trường hợp này, bạn phải xóa bằng tay hộp kiểm tra này. Do các tác vụ trong hàng đợi đã được máy in logic sẵn sàng cho việc in ấn nên máy in mà bạn muốn định hướng lại phải tương thích với trình điều khiển được máy in logic sử dụng. Tất cả các tác vụ in ấn được định hướng lại tới cổng mới (tuy nhiên bạn không thể định hướng lại các tài liệu riêng rẽ và bất kỳ tài liệu hiện đang in ấn cũng không thể định hướng lại).

Trong hầu hết các trường hợp, việc định hướng lại tác vụ in ấn rất hữu ích khi bạn sử dụng các máy in mạng được truy cập thông qua các cổng TCP/IP. Khi một máy in bị trục trặc, bạn có thể thay đổi cổng trong máy in logic của nó tới địa chỉ IP của máy in vật lý khác trên mạng. Máy in vật lý này phục vụ hai máy in logic cho đến khi bạn xác định được lỗi trên máy in và thay đổi thiết lập cổng trở lại giá trị cũ.

Sử dụng màn hình quản trị hiệu năng (*Performance)*

Bạn có thể truy cập vào màn hình quản trị ***Performance*** từ ***Administrative Tools***. Màn hình này chứa hai snap-in ***System Monitor*** và ***Performance Logs And Alerts*** cho phép bạn giám sát hiệu năng của các máy in theo thời gian thực, sử dụng các file nhật ký cho việc phân tích sau này hoặc thiết lập các mức cảnh báo và các hoạt động.

> ***THÔNG TIN THÊM Để biết thêm thông tin*** *Xem chương 3 để xem lại khả năng và các tiến trình thông qua màn hình quản trị* ***Performance****.*

Để cấu hình ***System Monitor*** hoặc ***Perfomance Logs And Alerts*** nhằm giám sát các hoạt động in ấn trên mạng, thông thường bạn lựa chọn đối tượng đo hiệu năng ***Print Queue*** (*hàng đợi máy in*) trong hộp thoại ***Add Counters*** (*thêm biến đếm*) như hình vẽ 10-14. Đối tượng này cung cấp một hình ảnh hiệu năng về mỗi máy in được cài đặt trên máy tính và một số biến đếm hiệu năng giúp bạn giám sát tiến trình in ấn, bao gồm:

Hình 10-14: Lựa chọn các biến đếm hiệu năng để giám sát các hoạt động trên máy in với màn hình quản trị Performance

- **Bytes Printed/Sec** (*số lượng byte được in trong 1s*) xác định số lượng dữ liệu thô tính theo byte gửi tới máy in trong 1s. Giá trị của

biến đếm này càng thấp đồng nghĩa với việc máy in này hoạt động không đúng mức hoặc do máy in không có tác vụ in, do hàng đợi chưa được tải hoặc do máy chủ quá bận. Giá trị này thay đổi tùy theo chủng loại máy in. Tham khảo tài liệu máy in để biết được giá trị mà máy in có thể chấp nhận được.

- **Job Erros** (*các lỗi tác vụ in*) xác định số lượng các lỗi tác vụ in ấn xảy ra khi bộ đệm khởi tạo lần cuối cùng. Các lỗi tác vụ in thông thường gây ra bởi cấu hình cổng không chính xác; kiểm tra cấu hình cổng về các thiết lập không hợp lệ. Một lỗi tác vụ in sẽ làm tăng giá trị biến đếm này chỉ một lần duy nhất thậm chí lỗi đó có thể xảy ra nhiều lần.
- **Jobs** (*các tác vụ*) xác định số lượng các tác vụ trong hàng đợi. Một giá trị của biến đếm này cao hoặc tăng cố định đồng nghĩa với việc máy in hoạt động không bình thường hoặc các tác vụ không được thực hiện một cách chính xác.
- **Not Ready Errors** (*các lỗi không sẵn sàng*) xác định số lượng các lỗi do máy in không sẵn sàng xảy ra kể từ khi bộ đệm được khởi tạo.
- **Out Of Paper Errors** (*các lỗi về tình trạng hết giấy*) xác định số lượng các lỗi xảy ra do tình trạng hết giấy xảy ra kể từ khi bộ đệm được khởi tạo.
- **Total Jobs Printed** (*tổng số các tác vụ được in*) xác định số lượng các tác vụ được gửi tới máy in kể từ khi bộ đệm được khởi tạo.
- **Total Pages Printed** (*tổng só các trang được in*) xác định số lượng các trang tài liệu được in kể từ khi bộ đệm được khởi tạo. Biến đếm này cung cấp một con số xấp xỉ gần đúng dung lượng của máy in mặc dù nó không phải thật là chính xác do tùy thuộc vào loại tác vụ và các đặc tính tài liệu của các tác vụ đó.

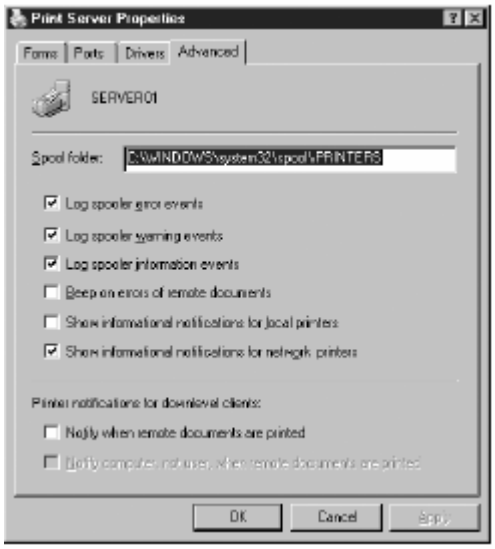
CHÚ Ý ***Sử dụng các biến đếm hiệu năng*** *Một số biến đếm hàng đợi máy in phù hợp với tiến trình ghi lại nhật ký hiệu năng như chúng có thể lưu lại khối lượng hoạt động của máy in chẳng hạn. Nhưng một số cái khác lại phù hợp với các cảnh báo như các biến đếm lỗi chẳng hạn. Sử dụng các cảnh báo, bạn có thể cấu hình cho hệ thống thông báo cho người quản trị mạng khi có lỗi xảy ra.*

Sử dụng Event Viewer

Bạn có thể sử dụng các file nhật ký hệ thống (***System Log***) trong ***Event Viewer*** để kiểm tra hoạt động của máy in và bộ đệm trên máy in. Mặc định,

bộ đệm đăng ký các sự kiện liên quan tới việc tạo, xóa và thay đổi máy in. File nhật ký cũng chứa các sự kiện về lưu lượng máy in, không gian đĩa cứng, các lỗi bộ đệm và các vấn đề bảo dưỡng.

Để điều khiển hoặc thay đổi các sự kiện về bộ đệm được ghi lại, mở thư mục ***Printers And Faxes*** và lựa chọn ***Server Properties*** từ thực đơn ***File***. Lựa chọn thẻ ***Advanced*** để truy cập các đặc tính như hình vẽ 10-15. Trong thẻ này, bạn có thể điều khiển các sự kiện nào được ghi lại và các thông báo tác vụ in ấn. Thẻ này cũng cho phép bạn thực hiện một công việc rất quan trọng đó là di chuyển thư mục bộ đệm khi bạn cấu hình một máy chủ in ấn hoạt động hoặc khi không gian đĩa cứng chứa thư mục bộ đệm trên một máy in sẵn có bị đầy.



Hình 10-15: Thẻ Advanced trên hộp thoại Print Server Properties

Kiểm định truy cập máy in

Bạn có thể kiểm định việc truy cập đến một máy in tương tự như kiểm định trên thư mục và file. Bạn có thể thực hiện kiểm định đối với một nhóm hoặc người sử dụng xác định với một hoạt động cụ thể trên một máy in. Sau khi thiết lập chính sách kiểm định truy cập, bạn có thể xem kết quả trong phần ***Security*** của màn hình quản trị file nhật ký ***Event Viewer***.

Để cấu hình kiểm định cho một máy in, mở hộp thoại ***Properties*** của nó, lựa chọn thẻ ***Security*** rồi nhấp vào ***Advanced***. Trong hộp thoại ***Advanced Security Settings***, lựa chọn thẻ ***Auditing*** và thêm các chỉ mục cho các nhóm và người sử dụng xác định. Với mỗi đối tượng bảo mật mà bạn đưa vào danh sách kiểm định, bạn có thể cấu hình kiểm định các sự kiện thành công hoặc thất bại dựa trên các Cấp phép máy in chuẩn bao gồm ***Print***, ***Manage Documents*** và ***Manage Printers***.

Kế tiếp bạn phải cho phép chính sách ***Audit Object Access*** (*kiểm định việc truy cập đối tượng*) đặt trên màn hình quản trị ***Group Policy Object Editor*** hoặc ***Local Security Policy*** trong ***Computer Configuration\Windows Settings\Security Settings\Local Policies\Audit Policy***. Sau khi chính sách đã có hiệu lực, bạn có thể kiểm tra các file nhật ký trong phần ***Security*** để xem và phân tích các chỉ mục.

> ***LỜI KHUYÊN Khi nào thì thực hiện kiểm định vấn đề in ấn***
> *Kiểm định máy in tạo ra hàng tá các mục vào đối với một tác vụ in, vì vậy nó chỉ phù hợp khi bạn đang xử lý sự cố. Không nên sử dụng cơ chế kiểm định nhằm giám sát mức độ sử dụng hoặc làm hóa đơn tính tiền. Thay vào đó, bạn nên sử dụng các biến đếm như* ***Total Jobs Printed*** *hoặc* ***Total Pages Printed.***

XỬ LÝ SỰ CỐ MÁY IN

Xử lý sự cố là một trong các công việc quan trọng trong quá trình quản trị máy in. Phần này giúp bạn hiểu và xác định các lỗi có thể xảy ra trong quá trình in ấn trên Windows Server 2003.

> ***CHÚ Ý Mục tiêu của kỳ thi*** *Các mục tiêu cho kỳ thi 70-290 yêu cầu các học viên có khả năng "xử lý sự cố hàng đợi"*

Bạn cần lưu ý quá trình xử lý sự cố in ấn gồm nhiều thành phần gồm có:

- Ứng dụng đang thực hiện in ấn
- Máy in logic trên máy tính có ứng dụng đang chạy
- Kết nối mạng giữa máy khách in ấn và máy in logic chia sẻ trên máy chủ.
- Máy in logic trên máy chủ: bộ đệm, các trình điều khiển, các thiết lập bảo mật và các thành phần khác.
- Kết nối giữa máy chủ in ấn và máy in.
- Bản thân máy in vật lý: phần cứng, cấu hình và các trạng thái.

Một phương pháp hiệu quả để giải quyết hầu hết các lỗi trong in ấn là xử lý sự cố theo từng phần riêng biệt một cách logic và có phương pháp.

Xác định phạm vi lỗi

Nếu một người sử dụng không thể thực hiện một tác vụ in ấn từ một ứng dụng trên máy tính của anh ta nhưng vẫn có thể thực hiện được từ các ứng dụng khác cũng trên máy tính đó thì lỗi đó dường như xuất phát từ ứng dụng chứ

không phải từ máy tính, mạng hay máy chủ in ấn hoặc phần cứng máy in. Tuy nhiên, trong một số trường hợp sử dụng một trình điều khiển khác hoặc loại dữ liệu khác có thể giải quyết được các lỗi in ấn của ứng dụng.

Nếu người sử dụng không thể in từ bất kỳ ứng dụng nào, bạn cần xác định xem anh ta có thể in ra các máy in khác trên cùng máy chủ in ấn đó không hay trên máy chủ in ấn khác. Nếu tất cả các khả năng này vẫn không thực hiện được và nếu các người sử dụng khác vẫn có thể in trên các máy in trên mạng thì lỗi dường như xảy ra trên máy tính của họ.

Nếu máy in được kết nối mạng, cố gắng tạo ra một máy in cục bộ trên hệ thống đang có lỗi trỏ trực tiếp tới cổng máy in này. Tức là bỏ qua vai trò quản lý của máy chủ in ấn. Nếu việc in ấn thành công có nghĩa là lỗi ở trên máy chủ hoặc kết nối giữa máy chủ và máy trạm có vấn đề.

Kiểm tra xem máy khách in ấn có thể kết nối tới máy chủ

Bạn có thể kiểm tra lại kết nối giữa máy in khách và máy chủ in ấn bằng cách mở cửa sổ hàng đợi từ thư mục ***Printers And Faxes*** trên máy trạm. Nếu cửa sổ này mở và hiển thị bất kỳ tài liệu nào trên hàng đợi có nghĩa là máy trạm kết nối thành công tới máy chủ. Nếu có lỗi xảy ra có nghĩa rằng mạng có vấn đề hoặc có lỗi về việc xác thực hay Cấp phép. Nếu trường hợp này xảy ra bạn có thể sử dụng công cụ ***Ping*** để kiểm tra kết nối tới địa chỉ IP của máy chủ hoặc nhấp ***Start***, chọn ***Run*** và gõ ***<máy chủ in ấn>***. Nếu ***ping*** thành công hoặc một cửa sổ mở ra hiển thị thư mục ***Printers And Faxes*** và bất kỳ thư mục chia sẻ nào tức là máy trạm đã kết nối tới máy chủ. Trong trường hợp này, bạn nên kiểm tra các Cấp phép bảo mật trên máy in logic.

Xác nhận máy in đang hoạt động

Kiểm tra chính máy in và đảm bảo rằng nó ở trạng thái sẵn sàng. Kiểm tra các vấn đề như mực in bị hết, tắc giấy và các lỗi khác sau đó in một trang kiểm tra từ màn hình quản trị máy in. Kiểm tra cáp kết nối giữa máy in và máy chủ hoặc mạng. Nếu máy in được gắn với mạng, bạn cần chắc chắn rằng đèn trên card giao diện mạng sáng điều đó có nghĩa rằng kết nối mạng tốt.

Xác nhận rằng bạn có thể truy cập tới máy in từ máy chủ

Một số máy in có thể hiển thị địa chỉ IP của chúng trên màn hình quản trị máy in hoặc bạn có thể in ra một trang cấu hình. Xác nhận rằng địa chỉ IP của máy in giống với địa chỉ IP của cổng máy in logic. Địa chỉ IP của cổng có thể kiểm tra trên thẻ ***Port*** trong hộp thoại ***Properties*** của máy in. Đảm bảo rằng bạn có thể kết nối với máy in qua mạng bằng cách ***ping*** địa chỉ IP của máy in.

Xác nhận rằng các dịch vụ trên máy chủ đang hoạt động

Sử dụng Bảng điều khiển ***Services*** để kiểm tra các dịch vụ dưới đây liên quan đến in ấn đang hoạt động tốt:

- **Print Spooler** Quản lý các hàng đợi in ấn cục bộ và trên mạng. Nếu dịch vụ này không hoạt động thì việc in ấn không thể thực hiện được.
- **Remote Procedure Call (RPC)** Một dịch vụ cần thiết cho các kết nối mạng chuẩn tới các máy in chia sẻ.

Bạn cũng có thể kiểm tra dung lượng thư mục mà bộ đệm được lưu trữ trên đó để đảm bảo rằng không gian đĩa cứng còn đủ cho việc lưu đệm. Vị trí của thư mục bộ đệm có thể thay đổi được trong hộp thoại ***Server Properties*** (bạn có thể truy cập vào hộp thoại này từ thực đơn ***File*** của thư mục ***Printers And Faxes***). Mặc định, bộ đệm của các tác vụ in ấn được lưu trữ tại thư mục ***<Systemroot>\system32\spool\Printers***. Với một máy chủ có mật độ in cao, bạn nên cân nhắc di chuyển thư mục này tới một phân vùng khác chứ không nên để trên phân vùng hệ thống hoặc khởi động. Nếu phân vùng chứa thư mục bộ đệm đầy thì quá trình in ấn sẽ ngừng và nghiêm trọng hơn hệ điều hành có thể ảnh hưởng.

Bạn cũng có thể tìm kiếm các file nhật ký trong phần ***System*** để xem bộ đệm có đưa ra bất kỳ thông báo lỗi nào không và trong thư mục ***Printers And Faxes*** đảm bảo rằng máy in của bạn không ở chế độ không kết nối.

Cố gắng thực hiện một tác vụ in ấn từ một ứng dụng trên máy chủ. Nếu bạn có thể in từ máy chủ có nghĩa rằng lỗi không phải do máy in. Nếu bạn không thể thực hiện được điều này, tạo một máy in logic trỏ trực tiếp tới cùng cổng và cố gắng in trên máy in mới này. Nếu thực hiện thành công tức là có vấn đề với cấu hình của máy in logic đầu tiên. Nếu thực hiện không thành công có nghĩa là có vấn đề trong việc kết nối với máy in hoặc chính bản thân phần cứng máy in.

TỔNG KẾT

- Kiến trúc in ấn trong Windows Server 2003 được module hóa bao gồm: máy in vật lý, máy chủ in ấn với máy in logic, chia sẻ kết nối tới máy in vật lý thông qua một cổng cục bộ hoặc mạng và máy in logic trên máy trạm kết nối tới máy in logic, chia sẻ trên máy chủ.
- Máy in logic được tạo ra với mục đích hỗ trợ máy in được gắn trực tiếp với máy tính hoặc mạng. Máy in mạng kết nối tới máy in logic do máy tính khác duy trì, hay còn được gọi là máy chủ in ấn.
- Mặc định, các máy in chia sẻ được công bố trong Active Directory, cho phép người sử dụng dễ dàng tìm kiếm các máy in dựa trên vị trí hoặc các đặc tính khác của máy in.
- Để tạo một máy in logic, bạn sử dụng trình hướng dẫn ***Add Printer*** và xác định trình điều khiển và cổng thích hợp.
- Một máy in logic có thể hướng các tác vụ tới nhiều hơn một cổng bằng cách tạo ra tổ hợp máy in (***Printer pool***).
- Một máy in vật lý có thể phục vụ nhiều máy in logic khác nhau, mỗi máy in có thể cấu hình với các thuộc tính, các trình điều khiển, các thiết lập, các đặc tính theo dõi và các Cấp phép riêng biệt.
- Cửa sổ hàng đợi in ấn, các nhật ký sự kiện và các biến đếm hiệu năng cho phép bạn giám sát các máy in nhằm xử lý sự cố, phát hiện các lỗi tiềm ẩn và mức độ sử dụng máy in.
- Nếu một máy in ở trạng thái không kết nối hoặc bị lỗi, bạn có thể định hướng lại tất cả các tác vụ in ấn chưa thực hiện của nó tới một máy in khác bằng cách thêm hoặc lựa chọn cổng máy in mới trong phần thiết lập đặc tính của máy in logic gốc. Máy in trên cổng thay thế phải tương thích với trình điều khiển mà máy in gốc đang sử dụng.
- Do mô hình in ấn trong Windows Server 2003 được module hóa với chính máy in đó, với máy in logic trên máy chủ và với máy in logic trên máy trạm kết nối tới máy in chia sẻ trên máy chủ nên bạn có thể xử lý sự cố khi máy in có lỗi bằng cách xác định mỗi thành phần có thể gây nên lỗi đó và sự liên quan giữa các thành phần đó với nhau.

BÀI TẬP THỰC HÀNH

==========

Bài tập thực hành thực hành 10-1: Tạo một máy in logic

Trong bài thực hành này, bạn sẽ cài đặt một máy in logic trên máy tính của bạn.

- Truy cập vào hệ điều hành Windows Server 2003 bằng tài khoản ***Administrator***.
- Nhấp ***Start*** và chọn ***Printers And Faxes***. Cửa sổ ***Printers And Faxes*** xuất hiện.
- Kích đúp vào biểu tượng ***Add Printer***. Trình hướng dẫn ***Add Printer*** xuất hiện.
- Nhấp ***Next*** để bỏ qua trang ***Welcome***. Trang ***Local Or Network Printer*** xuất hiện.
- Lựa chọn ***Local Printer Attached To This Computer***. Đảm bảo rằng hộp kiểm tra ***Automatically Detect And Install My Plug And Play Printer*** đã bị xóa rồi nhấp ***Next***. Trang ***Select A Printer Port*** xuất hiện.
- Trong danh sách liệt kê ***Use The Following Port*** lựa chọn cổng máy in LTP3: rồi nhấp ***Next***. Trang ***Install Printer Software*** xuất hiện. Trong trường hợp máy tính của bạn không có cổng LTP3, hãy chọn một cổng mà máy tính của bạn không sử dụng như COM3 và COM4 chẳng hạn.
- Trong cột ***Manufacturer*** lựa chọn ***Generic***. Trong cột ***Printers*** lựa chọn ***Generic/Text Only*** rồi nhấp ***Next***. Trang ***Name Your Printer*** xuất hiện.
- Trong hộp văn bản ***Printer Name***, gõ **Test Printer** rồi nhấp ***Next***. Trang ***Printer Sharing*** xuất hiện.

- Nhấp ***Nex***t để chấp nhận các tham số chia sẻ mặc định. Nhấp ***Next*** một lần nữa để bỏ qua trang ***Location And Comment***. Trang ***Print Test*** xuất hiện.
- Lựa chọn ***No*** rồi nhấp ***Next***. Trang ***Completing The Add Printer*** Trình hướng dẫn xuất hiện.
- Nhấp ***Finish***.

==========

Bài tập thực hành thực hành 10-2: Thiết lập các Cấp phép trên máy in

Trong bài thực hành này, bạn sẽ cấu hình các Cấp phép trên máy in chia sẻ của bạn.

3. Truy cập vào hệ điều hành Windows Server 2003 bằng tài khoản ***Administrator.***
4. Cài đặt một máy in logic như trong bài 10-1.

- Nhấp ***Start*** -> ***Printer And Faxes***. Cửa sổ ***Printer And Faxes*** xuất hiện.
- Lựa chọn biểu tượng ***Test Printer*** trên máy in logic mà bạn vừa tạo và từ thực đơn ***File*** lựa chọn ***Properties***. Hộp thoại ***Properties*** xuất hiện.
- Lựa chọn đối tượng bảo mật ***Everyone*** trên thẻ ***Security*** rồi nhấp ***Remove***.
- Nhấp ***Add***. Hộp thoại ***Select Users, Computers, Or Groups*** xuất hiện.
- Trong hộp văn bản ***Enter The Object Names To Select*** gõ **Users** rồi nhấp ***OK***. Nhóm ***Users*** sẽ xuất hiện trong danh sách các đối tượng bảo mật.
- Lựa chọn hộp kiểm tra ***Allow*** đối với Cấp phép ***Manage Documents*** và nhấp ***OK***.

==========

Bài thực hành 10-3: Loại bỏ một tác vụ in ấn

Trong bài thực hành này, bạn sẽ loại bỏ một tác vụ in chưa hoàn thành trong hàng đợi .

5. Truy cập vào hệ điều hành Windows Server 2003 bằng tài khoản ***Administrator.***

- Cài đặt máy in logic như bài thực hành 10-1.
- Nhấp ***Start*** và lựa chọn ***Printers And Faxes.*** Cửa sổ ***Printers And Faxes*** xuất hiện.
- Trên máy in logic bạn vừa tạo, kích chuột phải vào biểu tượng ***Test Printer*** và lựa chọn ***Properties***. Hộp thoại ***Properties*** của máy in xuất hiện.
- Nhấp ***Print Test Page*** trong thẻ ***General*** để in một trang kiểm tra trên máy in. Hộp thông báo ***Test Printer*** mở ra. Nhấp ***OK*** để đóng hộp thông báo và nhấp ***OK*** để đóng hộp thoại ***Properties*** của máy in.
- Trên máy in logic bạn vừa tạo, nhấp đúp vào biểu tượng ***Test Printer.*** Cửa sổ ***Test Printer*** xuất hiện.
- Lựa chọn tài liệu ***Test Page*** trong danh sách và chú ý trạng thái lỗi của nó do không có một máy in vật lý nào kết nối với cổng bạn đã lựa chọn.
- Trên thực đơn ***Document*** lựa chọn ***Cancel***. Một hộp thông báo ***Printers*** xuất hiện nhắc nhở bạn xác nhận xóa tác vụ in.
- Nhấp ***Yes***. Tác vụ sẽ bị xóa khỏi hàng đợi.

CÁC CÂU HỎI ÔN TẬP

1. Bạn đang cài đặt máy in trên máy trạm. Máy in sẽ được kết nối tới một máy in logic được cài đặt trên một máy chủ in ấn Windows Server 2003. Những kiểu thông tin nào mà bạn phải cung cấp cho tiến trình cài đặt máy in? (Lựa chọn tất cả các câu trả lời đúng)

    a. Một cổng máy in TCP/IP.

b. Nhà sản xuất máy in vật lý và chủng loại của nó.

c. Đường dẫn URL tới máy in trên máy chủ

d. Đường UNC tới máy in chia sẻ

e. Trình điều khiển máy in

2. Một trong những máy in mạng của bạn không làm việc tốt và bạn muốn ngăn không cho người sử dụng gửi các tác vụ tới máy in logic kết nối tới máy in nói trên. Bạn sẽ làm gì?

a. Dừng chia sẻ máy in

b. Loại bỏ máy in ra khỏi dịch vụ thư mục Active Directory

c. Thay đổi cổng máy in

d. Thay đổi tên chia sẻ

3. Bạn đang quản trị một máy tính Windows Server 2003 được cấu hình như một máy chủ in ấn. Bạn muốn thực hiện công tác bảo dưỡng trên máy in vật lý được kết nối với máy chủ. Hiện đang có một số tài liệu trên hàng đợi. Bạn muốn ngăn không cho các tài liệu được in trên máy in này nhưng bạn cũng không muốn người sử dụng phải thực hiện lại tác vụ in ấn. Phương pháp tối ưu nhất của bạn là gì?

a. Mở hộp thoại ***Properties*** của máy in lựa chọn thẻ ***Sharing*** và lựa chọn ***Do Not Share This Printer***.

b. Mở hộp thoại ***Properties*** của máy in và trên thẻ ***Ports*** lựa chọn một cổng chưa được thiết bị in ấn sử dụng.

c. Mở cửa sổ hàng đợi, lựa chọn tài liệu đầu tiên và tiếp theo lựa chọn ***Pause*** từ cửa sổ ***Document***. Lặp lại tiến trình này với mỗi tài liệu.

d. Mở cửa sổ hàng đợi và lựa chọn ***Pause Printing*** từ thực đơn ***Printer***.

4. Bạn đang quản trị một máy tính Windows Server 2003 được cấu hình như một máy chủ in ấn. Người sử dụng trong nhóm Marketing phàn nàn rằng họ không thể in các tài liệu thông qua máy in trên máy chủ. Bạn hiển thị các Cấp phép trên hộp thoại Properties của máy in. Nhóm Marketing có Cấp phép Manage Documents. Tại sao người sử dụng không in được trên máy in này?

    a. Nhóm ***Everyone*** phải được gán Cấp phép ***Manage Documents***.

    b. Nhóm ***Administrators*** phải được gán Cấp phép ***Mange Printers***

    c. Nhóm ***Marketing*** phải được gán Cấp phép ***Print***

    d. Nhóm ***Marketing*** phải được gán Cấp phép ***Manage Printers***

5. Bạn đang cài đặt một tổ hợp máy in trên máy tính Windows Server 2003. Tổ hợp máy in chứa ba thiết bị in ấn và tất cả đều giống nhau. Bạn mở hộp thoại Properties trên máy in này và lựa chọn Enable Printer Pooling trên thẻ Port. Bạn phải làm gì tiếp theo?

    a. Cấu hình cổng LPT1 để hỗ trợ ba máy in

    b. Lựa chọn hoặc tạo các cổng ánh xạ tới ba máy in

    c. Trên thẻ ***Device Settings***, cấu hình các lựa chọn có khả năng cài đặt được nhằm hỗ trợ hai thiết bị in ấn thêm vào

    d. Trên thẻ ***Advanced,*** cấu hình độ ưu tiên cho mỗi thiết bị in ấn nhằm đảm bảo tiến trình in được phấn phối cho ba thiết bị in.

6. Bạn đang quản trị một máy tính Windows Server 2003 được cấu hình như một máy chủ in ấn. Vào ngày giữa tuần làm việc, máy in bị lỗi và cần được thay thế. Người sử dụng đã gửi các tác vụ in đến máy in này và nó có địa chỉ IP là 192.168.1.81.Một máy in tương tự có địa chỉ 192.168.1.217 được máy chủ khác hỗ trợ. Các công việc bạn cần thực hiện sao cho các tác vụ của người sử dụng vẫn được tiếp tục? (Lựa chọn tất cả các câu trả lời đúng)

a. Trên hộp thoại ***Properties*** của máy in lỗi lựa chọn ***Enable Printer Pooling***.

b. Trên hộp thoại ***Properties*** của máy in lỗi nhấp ***Add Port***

c. Trên thư mục ***Printer And Faxes*** kích chuột phải vào máy in lỗi và lựa chọn ***Use Offline***.

d. Trên hộp thoại ***Properties*** của máy in lỗi lựa chọn cổng 192.168.1.217.

7. Trong các mô hình dưới đây, mô hình nào cho bạn bức tranh gần đúng nhất về mức độ sử dụng trên máy in, cho phép bạn hiểu về mức độ tiêu thụ của mực và giấy in?

a. Cấu hình kiểm định máy in logic và kiểm định các sự kiện thành công trong việc sử dụng Cấp phép in của nhóm hệ thống ***Everyone***.

b. Xuất các nhật ký sự kiện hệ thống (***System log***) ra file văn bản phân cách các trường bằng dấu phảy (****.csv***) và sử dụng Excel để phân tích các sự kiện bộ đệm.

c. Cấu hình nhật ký hiệu năng và giám sát biến đếm ***Total Pages Printed*** trên mỗi máy in logic.

d. Cấu hình nhật ký hiệu năng và giám sát biến đếm ***Jobs*** với mỗi biến đếm logic.

CÁC KỊCH BẢN TÌNH HUỐNG

==========

Kịch bản 10-1: Cập nhật các trình điều khiển máy in

Phòng marketing phàn nàn với bạn về chất lượng in trên máy in chia sẻ có tên gọi là ***MarketingPrinter***. Khi người sử dụng in từ máy tính PC Windows XP sử dụng các ứng dụng Microsoft Office, các tài liệu được in tốt. Nhưng khi họ in từ các ứng dụng Adobe, các tài liệu in ra không được như mong muốn. Phòng kinh doanh có một máy in chia sẻ tương tự có tên là ***SalesPrinter*** và sử

dụng hỗn hợp các máy trạm Windows 2000/XP và Office không thông báo bất cứ một lỗi nào. Bạn cân nhắc trường hợp này, nó xảy ra vì một số ứng dụng khác nhau tạo ra các kết quả khác nhau phụ thuộc vào máy in có đang sử dụng PostScript hoặc một trình điều khiển không phải PostScript hay không. Bạn sẽ triển khai trình điều khiển máy in hoạt động tốt ở đâu sao cho các máy tính cần nó được cập nhật?

e. Hộp thoại ***Server Properties*** của máy chủ in ấn

f. Hộp thoại ***Properties*** của máy in ***MarketingPrinter***

g. Hộp thoại ***Properties*** của máy in ***SalesPrinter***

h. Hộp thoại ***Properties*** của các máy in logic được cài đặt trên các máy tính của mỗi người sử dụng phòng marketing.

==========

Kịch bản 10-2: Gia tăng hiệu năng in ấn

Bạn là nhà quản trị mạng cho một công ty luật với một nhóm gồm có 20 nhân viên trợ lý về mặt luật pháp cho các luật sư. Tất cả các nhân viên này đều sử dụng một máy in laser chia sẻ, tốc độ cao được cài đặt trên một hệ thống Windows Server 2003. Theo một lịch trình họ phải in một số lượng lớn tài liệu. Mặc dù máy laser in nhanh nhưng nó cần đảm bảo hoạt động gần như không đổi trong khi in ấn tài liệu. Tại một số thời điểm, các nhân viên trợ lý phải đợi 20 phút hoặc lâu hơn sau khi xác nhận một tác vụ cho các tài liệu của họ cho tới khi lên tới vị trí đầu tiên trong hàng đợi. Không một nhân viên nào muốn tìm kiếm một danh sách các máy in sẵn sàng nhằm kiểm tra xem cái nào có ít tác vụ nhất trước khi thực hiện tác vụ in. Lựa chọn nào dưới đây mà bạn sẽ xem xét nhằm tối thiểu hóa lượng thời gian mà các máy in tiêu tốn để hoàn thành các tài liệu in ấn cho tất cả các nhân viên trợ lý?

a. Cài đặt một máy in máy in laser thứ hai với cùng chủng loại và tạo một tổ hợp máy in.

b. Thiết lập các độ ưu tiên máy in khác nhau cho mỗi nhân viên trợ lý dựa trên danh sách do người đứng đầu nhóm tạo ra. Nhân viên quan trọng nhất sẽ có độ ưu tiên là 1 còn người có vai trò quan trọng thấp nhất sẽ có độ ưu tiên là 99.

c. Thiết lập các độ ưu tiên máy in khác nhau cho mỗi nhân viên trợ lý dựa trên danh sách do người đứng đầu nhóm tạo ra. Nhân viên quan trọng nhất sẽ có độ ưu tiên là 99 còn người có vai trò quan trọng thấp nhất sẽ có độ ưu tiên là 1.

d. Mua thêm các máy in laser tương tự và cài đặt chúng như những máy in chia sẻ riêng rẽ trên máy chủ.

PHẦN 4
QUẢN LÝ VÀ DUY TRÌ PHẦN CỨNG

CHƯƠNG 11: QUẢN LÝ CÁC TRÌNH ĐIỀU KHIỂN THIẾT BỊ

Khi bạn làm việc với một hệ điều hành phức tạp như Microsoft Windows Server 2003 chẳng hạn, nó chứa nhiều mảnh phần mềm phức tạp. Những phần mềm này tuy nhỏ và hầu như bạn không thấy sự hiện diện của nó nhưng lại giúp bạn làm được mọi thứ. Với một hệ điều hành, để có thể sử dụng các phần cứng trên máy tính cần phải có một phần mềm gọi là trình điều khiển thiết bị cho mỗi thiết bị phần cứng. Làm việc với các trình điều khiển thiết bị có thể không phải là công việc hàng ngày nhưng các nhân viên quản trị hệ thống cần phải cẩn trọng với chúng và bạn cần phải biết làm gì khi đến thời điểm để cập nhật hoặc xử lý sự cố.

Hoàn thành chương này bạn có khả năng:

- **Hiểu được mối quan hệ giữa các thiết bị phần cứng và các trình điều khiển.**
- **Cài đặt Trình Điều khiển Thiết bị**
- **Sử dụng Device Manager để hiển thị và quản lý các thiết bị phần cứng và các trình điều khiển thiết bị của chúng.**
- **Xử lý các lỗi về trình điều khiển thiết bị**

TỔNG QUAN VỀ TRÌNH ĐIỀU KHIỂN THIẾT BỊ

Trình điều khiển thiết bị là một tập hợp phần mềm thực hiện các chức năng trên các thiết bị cụ thể cho các hoạt động vào ra (***I/O - Input/Output***). Ví dụ, khi một ứng dụng chạy trên Windows 2003 ghi một file vào đĩa, nó sẽ gọi một hàm hệ điều hành gọi là ***WriteFile***. Hàm này định nghĩa một hoạt động cơ bản như sau: dữ liệu tại vị trí bộ nhớ xác định sẽ được chép tới một thiết bị lưu trữ xác định được cài đặt trên máy tính. Tuy nhiên, hàm ***WriteFile*** không biết gì về thiết bị phần cứng thực sự, nó chỉ làm việc với thiết bị ở khía cạnh thủ tục hoàn toàn độc lập với thiết bị. Để thực hiện các hàm cho một thiết bị cụ thể nhằm hoàn thành các tác vụ, hệ điều hành phải gọi các thủ tục do các trình điều khiển cung cấp cho thiết bị lưu trữ.

Thông thường, ứng dụng sẽ lưu giữ file trên đĩa cứng nhưng nó cũng có thể lưu giữ trên các đĩa mềm hoặc các thiết bị lưu trữ khác. Các trình điều khiển thiết bị khác nhau sẽ cung cấp khả năng truy cập tới các thiết bị lưu trữ mà ứng dụng có thể sử dụng. Các trình điều khiển thiết bị cũng cung cấp khả năng truy cập đến các thủ tục dành cho các thiết bị cụ thể. Đĩa cứng trong máy tính có thể sử dụng giao diện IDE hoặc SCSI. Đĩa cứng có thể được sản xuất bởi hàng chục nhà sản xuất thiết bị. Trình điều khiển thiết bị cung cấp khả năng truy cập đến các thủ tục cho một loại thiết bị xác định, chạy trên một nền hệ điều hành xác định. Nhà sản xuất thiết bị cũng có thể đưa ra các trình điều khiển thiết bị cho các hệ điều hành khác và cho các dòng ổ cứng khác mà họ sản xuất.

Các chức năng của trình điều khiển thiết bị

Các trình điều khiển thiết bị cung cấp hai chức năng cơ bản sau:

- Chúng tạo sự độc lập về thiết bị với hệ điều hành Điều này cho phép các ứng dụng và các thành phần phần mềm khác giao tiếp với với phần cứng đã được cài đặt trên máy tính. Khi một ứng dụng gọi hàm ***WriteFile***, hệ điều hành sẽ gọi trình điều khiển đĩa cứng thực hiện các thủ tục, cho phép đĩa cứng nhận dữ liệu từ hệ thống và ghi nó vào đĩa
- Chúng thao tác với các đặc tính vật lý của thiết bị phần cứng Khi một ứng dụng hay thủ tục trên hệ điều hành gọi một hàm nào đó, trình điều khiển thiết bị có thể thay đổi cấu hình vật lý của thiết bị phần cứng. Ví dụ khi bạn muốn một ứng dụng in tài liệu theo kiểu nằm ngang thay vì kiểu thẳng đứng như mặc định, trình điều khiển

thiết bị sẽ chịu trách nhiệm việc thay đổi cấu hình phần cứng của máy in.

Hai chức năng nói trên thực sự là hai khía cạnh của cùng một tiến trình nhưng trong Windows Server 2003 chúng có thể được thực hiện bởi các trình điều khiển khác nhau. Trong trường hợp này, một trình điều khiển mức thấp chịu trách nhiệm liên kết thực sự với phần cứng còn một trình điều khiển mức cao sẽ tương tác với các ứng dụng và các hàm của hệ điều hành. Bạn không thể nhìn thấy khả năng này trong giao diện Windows tuy nhiên bạn không phải tìm và cài đặt hai trình điều khiển riêng biệt nói trên.

> ***CHÚ Ý Các trình điều khiển và hệ điều hành*** *Thời điểm trước khi hệ điều hành Windows xuất hiện, các trình điều khiển thiết bị được thực thi bởi các ứng dụng đơn lẻ. Khi bạn cài đặt một sản phẩm phần mềm xử lý văn bản, bạn phải lựa chọn một trình điều khiển cho dòng máy in của bạn. Kế đó nếu bạn cài đặt một ứng dụng xử lý bảng tính (như Excel bây giờ chẳng hạn), bạn không thể sử dụng cùng một trình điều khiển đó. Ứng dụng này yêu cầu một trình điều khiển dành riêng cho nó. Windows đã khắc phục được những nhược điểm nói trên bằng cách tích hợp chúng vào hệ điều hành chứ không sử dụng riêng rẽ cho từng ứng dụng. Khi bạn cài đặt một trình điều khiển cho một máy in trên bất kỳ phiên bản nào của Windows, tất cả các ứng dụng chạy trên hệ điều hành đó đều có thể sử dụng các hàm thủ tục của trình điều khiển.*

Các thiết bị và trình điều khiển

Một máy tính bao gồm nhiều thiết bị phần cứng, hoạt động như các thành phần đơn lẻ nhưng hầu hết chúng đều cần một trình điều khiển thiết bị. Tuy nhiên, dựa trên phương thức hoạt động mà một số thiết bị được chuẩn hoá hơn các thiết bị khác. Thiết bị càng được chuẩn hoá thì chúng càng phổ biến và các nhà quản trị hệ thống càng ít quan tâm tới việc cập nhật hay duy trì.

Ví dụ, hầu hết mọi máy tính đều có bàn phím và mọi hệ điều hành đều cần có trình điều khiển thiết bị này. Tuy nhiên chức năng hoạt động của bàn phím cũng như tín hiệu mà nó trao đổi với máy tính đều được chuẩn hóa và ổn định cho nên ít khi hệ điều hành nào cần có trình điều khiển của bàn phím mà vẫn nhận được bàn phím. Trường hợp duy nhất một trình điều khiển thiết bị bàn phím đặc biệt được yêu cầu khi bạn đang sử dụng một phần cứng không bình thường với các khả năng đặc biệt như một thiết bị đầu vào dành cho người khiếm thị.

Cuối cùng là hình ảnh của các thiết bị như card màn hình yêu cầu cần phải có trình điều khiển được thiết kế để làm việc với các thiết bị phần cứng cụ thể. Các thiết bị đặc chủng có thể gây ra các vấn đề cho các quản trị viên hệ thống, bao gồm:

- Chúng ít được hỗ trợ bởi hệ điều hành Hệ điều hành Windows 2003 (cũng giống như tất cả các hệ điều hành Windows) bao gồm một thư viện các trình điều khiển, cung cấp khả năng tương thích với môt danh sách dài các thiết bị phần cứng của mỗi loại. Các thiết bị càng phổ dụng thì càng chắc chắc được hỗ trợ bởi trình điều khiển hệ điều hành. Nhưng đối với các thiết bị các đặc biệt nhất là các thiết bị vừa sản xuất hoặc ngoài luồng thì có thể không có trình điều khiển hỗ trợ trong Windows hoặc không có phiên bản gần nhất của trình điều khiển. Trong những trường hợp này, bạn phải cung cấp cho hệ điều hành trình điều khiển bạn nhận được từ nhà sản xuất thiết bị.

  CHÚ Ý Microsoft và các trình điều khiển thiết bị *Mặc dù Windows Server 2003 và các hệ điều hành Windows khác chứa hàng trăm các trình điều khiển thiết bị cho các sản phẩm phần cứng khác nhau và một số ít trong này thực sự được tạo ra bởi Microsoft. Microsoft nhận trình điều khiển từ nhà sản xuất thiết bị và tích hợp chúng cùng với hệ điều hành Windows. Vì lý do này, khi bạn gặp vấn đề với trình điều khiển, bạn cần sự giúp đỡ từ phía nhà sản xuất hơn là từ phía Microsoft.*

- **Không có trình điều khiển của nhà cung cấp phần cứng** Trong một vài trường hợp thì các nhà sản xuất phần cứng phát triển trình điều khiển cho Windows 2003 cho các thiết bị của họ sau khi họ phát hành phiên bản WindowsXP vì hệ điều hành này chủ yếu dùng cho máy trạm hoặc do họ không xem Windows Server 2003 như là một phần của thị trường sản phẩm.
- **Thiết bị không tương thích** hoặc hoạt động không đúng Nhiều thiết bị thường có hiện tượng hoạt động không đúng, điều này thường xảy ra khi mà chúng được điều khiển để hoạt động ớ chế độ cao hơn. Ví dụ, các trình điều khiển card màn hình có xu hướng bị tình trạng này do các chức năng hoạt động phức tạp của chúng và do nhiều ứng dụng đưa chúng đến trạng thái giới hạn. Các card màn hình gần đây được thiết kế cho chức năng chơi trò chơi điện tử thường gặp trục trặc hơn so với các card màn hình tích hợp trong hệ thống mức thấp. Khi trình điều khiển bị lỗi, người quản trị hệ thống

phải liên lạc trực tiếp với nhà sản xuất thiết bị phần cứng để thay thế chúng.

- **Chúng thường được cập nhật nhiều hơn so với các** trình điều khiển phổ dụng Đây là một kết quả tất yếu của tính chất phức tạp, một số trình điều khiển thường được cập nhật nhiều hơn so với các trình điều khiển khác. Một lần nữa, trình điều khiển card màn hình lại là một ví dụ điển hình. Các trình điều khiển card màn hình gần đây thường xuyên được nhà sản xuất cập nhật. Tùy thuộc vào thời điểm thiết bị phần cứng được phát hành và bạn đang sử dụng phiên bản nào của Windows, trình điều khiển đi kèm với hệ điều hành có thể có một vài phiên bản cũ. Trong hầu hết các trường hợp, trình điều khiển đi kèm cùng với Windows đủ để giúp bạn trong tiến trình cài đặt nhưng bạn có thể phải cài đặt các trình điều khiển cập nhật dành cho thiết bị nhằm đạt được hiệu năng đầy đủ nhất.

Tất cả các thiết bị phần cứng đã được chứng nhận sử dụng cho Windows Server 2003 được liệt kê trong ***Windows Server Catalog***, luôn sẵn sàng tại địa chỉ ***www.microsoft.com/windows/catalog/server***. ***Catalog*** này thay thế cho danh sách liệt kê các thiết bị tương thích (HCL) được sử dụng trong các phiên bản trước của Windows. Khi lựa chọn phần cứng cho các máy tính Windows Server 2003, bạn cần phải đảm bảo rằng các thiết bị bạn lựa chọn được liệt kê trong ***catalog***.

Trình điều khiển thiết bị và các tài nguyên phần cứng

Một máy tính cá nhân bao gồm nhiều thiết bị phần cứng được kết nối (trực tiếp hoặc gián tiếp) tới bo mạch chính. Bộ vi xử lý, các module bộ nhớ, đĩa cứng, màn hình và các thiết bị khác tất cả chúng đều có chức năng duy nhất và hệ thống phải có khả năng liên kết với mỗi thành phần một cách riêng rẽ. Để thực hiện điều này, mỗi thiết bị phải có một số phương tiện để hệ thống có thể xác định tính duy nhất của nó vì vậy khi máy tính tạo ra dữ liệu đầu ra cần hiển thị trên màn hình thì chúng phải được chuyển tới card màn hình chứ không phải bàn phím hay đĩa cứng.

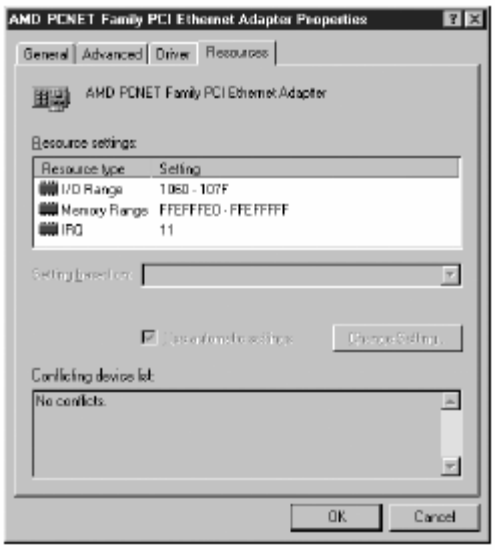
Để cá nhân hoá các thành phần giao tiếp, PC sử dụng các loại tài nguyên phần cứng khác nhau (chúng còn được gọi là các tài nguyên hệ thống). Mỗi trình điều khiển thiết bị được cấu hình để sử dụng các nguồn tài nguyên cho phép nó liên kết với thiết bị phần cứng chính xác và chỉ thiết bị đó mà thôi. Các loại tài nguyên phần cứng mà các thiết bị có thể sử dụng gồm có:

- Interupt Request (IRQ) Line (*chuỗi yêu cầu ngắt*) Một yêu cầu ngắt cũng giống như tên gọi của nó, là một tín hiệu được gửi từ một

thành phần này tới một thành phần khác (thông thường là từ một thiết bị ngoại vi tới bộ vi xử lý) với ngụ ý thông báo cho bên nhận rằng nó nên tạm dừng các hoạt động hiện thời để thực hiện một công việc khác. Ví dụ, mỗi lần bạn ấn một phím trên bàn phím máy tính, bàn phím sẽ gửi một yêu cầu ngắt tới bộ vi xử lý thông báo rằng có dữ liệu đầu vào mới gửi tới bộ vi xử lý. Một PC có 16 chuỗi yêu cầu ngắt được thiết kế cho việc sử dụng các thiết bị phần cứng khác nhau (một số có thể chia sẻ một chuỗi yêu cầu ngắt).

- I/O Address (*địa chỉ vào/ra*) Một địa chỉ vào/ra (còn được gọi là cổng vào/ra) là một vị trí trong bộ nhớ được phân bổ một thiết bị phần cứng xác định cho phép nó trao đổi thông tin với hệ thống. Mỗi thiết bị trong máy tính đều được gán một địa chỉ vào/ra duy nhất, cho phép hệ thống liên kết với các thiết bị đơn lẻ.
- **Direct Memory** Access (DMA) channel (*kênh truy nhập bộ nhớ trực tiếp*) Các kênh DMA là các tuyến đường mà một số thiết bị sử dụng chúng để truyền trực tiếp dữ liệu tới và từ bộ nhớ hệ thống mà không cần liên quan tới bộ vi xử lý. Khi so sánh với các chuỗi yêu cầu ngắt, thì có tương đối ít thiết bị (như các ổ đĩa mềm và các card âm thanh chẳng hạn) sử dụng các kênh DMA do mỗi PC chỉ có 08 kênh DMA.
- **Memory address (***địa chỉ bộ nhớ***)** Một vài thiết bị như card màn hình hay card mạng chẳng hạn cần có không gian trong bộ nhớ cấp trên với mục đích để cài đặt một ***BIOS*** (*hệ thống vào/ra cơ bản*) bổ sung. Một thiết bị thường yêu cầu tài nguyên phần cứng này đó là card giao tiếp SCSI với BIOS của chính thiết bị này cho phép hệ thống khởi động từ một ổ đĩa SCSI.

Màn hình quản trị ***Device Manager*** trong Windows Server 2003 cho phép bạn hiển thị các tài nguyên phần cứng trên máy tính và các thiết bị đang sử dụng chúng như hình vẽ 11-1.



Hình 11-1: Các tài nguyên phần cứng của một thiết bị được hiển thị trong Device Manager

Cấu hình các tài nguyên phần cứng

Để một thiết bị phần cứng có thể liên kết được với máy tính, thiết bị và trình điều khiển của nó cả hai đều được cấu hình để sử dụng các thiết lập tài nguyên phần cứng chính xác. Ví dụ, khi bạn kết nối một máy in tới cổng song song LPT1, bạn cũng phải cấu hình trình điều khiển máy in sử dụng cổng LPT1 để liên kết với máy in. Nếu máy in được kết nối với LPT1 và bạn cấu hình trình điều khiển sử dụng cổng LPT2 thì sự liên kết nói trên sẽ không xảy ra và máy tính sẽ không thể sử dụng được máy in.

Mối quan hệ giữa các thiết lập tài nguyên phần cứng dường như khá đơn giản khi chúng ta đề cập tới vấn đề máy in nhưng khi nói tới các thành phần bên trong của một máy tính thì vấn đề đó lại không hề đơn giản chút nào. Ví dụ, cài đặt một card mạng trên máy tính thường yêu cầu một chuỗi yêu cầu ngắt và một cổng vào/ra. Khi đó, card phần cứng và trình điều khiển card phải được cấu hình sử dụng cùng một chuỗi IRQ và cổng vào/ra. Ngoài ra, không có bất kỳ xung đột nào với thiết bị khác do sử dụng cùng chuỗi IRQ và cổng vào/ra.

Cùng lúc, bạn cần cấu hình cả thiết bị phần cứng và trình điều khiển thiết bị một cách thủ công. Để cấu hình card mạng, bạn có thể thiết lập các cầu nhảy (***jumper***) trên chính card này hoặc chạy một chương trình đặc biệt do nhà sản xuất cung cấp. Tiếp theo bạn cài đặt trình điều khiển và cấu hình nó sử dụng các thiết lập tài nguyên phần cứng giống như bạn cấu hình lúc trước. Với tiến trình này, một số vấn đề không đúng có thể xảy ra gồm có:

- Các thiết lập tài nguyên hạn chế Một số thiết bị chỉ có thể sử dụng được một số tài nguyên phần cứng nhất định. Ví dụ, một số card mạng cũ chỉ có thể sử dụng hai hoặc ba IRQ. Nếu các IRQ này đều đã bị sử dụng thì bạn phải cấu hình lại các thiết bị khác hoặc sử dụng một card khác.
- **Cạn kiệt tài nguyên** Khi vấn đề chia sẻ IRQ không còn phổ biến, các chuỗi IRQ ở các hệ thống được trang bị đầy đủ sẽ bị chiếm dụng hết bởi các thiết bị khác dẫn đến tình trạng ngăn không cho cài đặt các thành phần mới.
- **Xung đột thiết bị** Khi hai thiết bị được cấu hình sử dụng cùng tài nguyên hệ thống, thông thường một trong hai sẽ hoạt động không chính xác. Khi lựa chọn các tài nguyên phần cứng cho một thiết bị mới bạn phải biết được các tài nguyên đã được các thành phần khác trên máy tính sử dụng.

Plug and Play

May mắn, những lỗi này đã được loại trừ bởi sự ra đời của chuẩn ***Plug and Play*** (cắm là chạy) vào năm 1995. **Plug and Play** (PnP) là một chuẩn định nghĩa các đặc tính của các thành phần máy tính nhằm cho phép chúng tự động phát hiện và cấu hình phần cứng trên một máy tính. Với chức năng PnP, tất cả các thành phần dưới đây phải hỗ trợ chuẩn này:

- Phần cứng hệ thống
- Phần cứng thiết bị ngoại vi
- BIOS hệ thống
- Hệ điều hành

Hầu hết các thiết bị phần cứng PC được sản xuất từ năm 1997 và ngày nay tất cả đều hỗ trợ chuẩn PnP. Điều này được áp dụng cho hầu hết các sản phẩm BIOS hệ thống và tất cả các hệ điều hành Microsoft kể từ Windows 95. Điều đó có nghĩa khi bạn cài đặt một thiết bị mới trên một máy tính chạy Windows Server 2003 thì hầu như bạn không phải quan tâm các tài nguyên hệ thống cũng như cấu hình thiết bị. Hệ thống sẽ đảm nhận mọi thứ (với giả thiết trình điều khiển đã có sẵn). Khi bạn cài đặt một thiết bị PnP mới, máy tính sẽ thực hiện như sau:

- Phát hiện phần cứng mới
- Cài đặt trình điều khiển thiết bị tương ứng
- Xác định xem thiết bị yêu cầu tài nguyên hệ thống nào

- Dò quét hệ thống để xác định các tài nguyên phần cứng còn trống
- Lựa chọn các thiết lập tài nguyên tương ứng cho thiết bị
- Cấu hình cả thiết bị lẫn trình điều khiển thiết bị sử dụng các tài nguyên lựa chọn.

Nếu không có thiết lập tài nguyên nào còn trống cho thiết bị mới sử dụng, PnP có khả năng cấu hình lại một cách tự động phần cứng khác trên máy tính để giải phóng các tài nguyên cho thiết bị mới. Nếu Windows Server 2003 không có trình điều khiển, hệ điều hành sẽ nhắc nhở bạn cung cấp đĩa có chứa trình điều khiển hoặc tìm kiếm trình điều khiển tương ứng.

Khi bạn cài đặt một thiết bị phần cứng mới không hỗ trợ chuẩn PnP, Windows Server 2003 có thể hoặc không thể phát hiện ra nó. Tùy thuộc vào loại thiết bị mà có những trường hợp sau xảy ra:

Hệ thống không thể phát hiện ra thiết bị mới Nếu máy tính vẫn duy trì trạng thái không thông báo về thiết bị phần cứng mới, bạn phải chạy *Add Hardware Trình hướng dẫn* từ *Control Panel* và xác định, cài đặt, cấu hình thiết bị và trình điều khiển nó bằng tay.

- Hệ thống phát hiện sự hiện diện của thiết bị mới nhưng không thể xác định nó Đôi khi máy tính phát hiện ra sự hiện diện của thiết bị phần cứng mới nhưng không thể xác định loại thiết bị là gì. Một lần nữa bạn phải lựa chọn bằng tay loại thiết bị, nhà sản xuất và chủng loại thông qua Add Hardware Trình hướng dẫn.
- Hệ thống phát hiện thiết bị mới và xác định nó ở mức cơ bản nhưng không thể xác định được chủng loại cụ thể Máy tính có thể xác định được loại phần cứng cài đặt như card mạng chẳng hạn nhưng không thể xác định nhà sản xuất và chủng loại của nó vì vậy bạn phải lựa chọn chúng bằng tay trong Add Hardware Trình hướng dẫn.
- Hệ thống phát hiện và xác định thiết bị mới, tiếp theo cài đặt và cấu hình trình điều khiển thiết bị nhưng nó không thể cấu hình chính bản thân phần cứng Nếu máy tính xác định thành công phần cứng mới và cài đặt trình điều khiển thích hợp, hệ thống có thể cấu hình trình điều khiển để sử dụng các thiết lập tài nguyên phần cứng hiện tại của thiết bị. Tuy nhiên, nếu các thiết lập mặc định của thiết bị xung đột với các thành phần khác của máy tính thì hệ thống không thể cấu hình lại phần cứng để sử dụng các thiết lập khác. Trong trường hợp này, bạn phải cấu hình bằng tay các thiết lập tài nguyên cho thiết bị phần cứng.

TẠO CHIẾN LƯỢC DUY TRÌ TRÌNH ĐIỀU KHIỂN

Ngoài việc lúc đầu cài đặt các trình điều khiển chính xác, người quản trị hệ thống cũng có trách nhiệm duy trì các trình điều khiển thiết bị và cấu hình của chúng. Việc cập nhật trình điều khiển là công việc thường xuyên do những thay đổi hoạt động trên hệ điều hành và các thiết bị phần cứng sẽ phản ánh những thay đổi một cách tương ứng trong các trình điều khiển. Trong một số trường hợp, những cập nhật này không tương ứng với các phiên bản ***service pack*** định kỳ của hệ điều hành trong khi những cái khác luôn sẵn sàng như các ***hotfix*** (bản vá) từ trang Web ***Windows Update***. Tuy nhiên, trong nhiều trường hợp, phần còn lại thuộc về người quản trị hệ thống nhằm kiểm tra các phiên bản trình điều khiển mới của các nhà sản xuất phần cứng khác nhau và quyết định khi nào và có nên cài đặt chúng cũng như ai là người chịu trách nhiệm cài đặt.

Có cập nhật hay không?

Một trong những câu hỏi đầu tiên mà một người quản trị hệ thống cần phải cân nhắc khi đứng trước một phiên bản cập nhật trình điều khiển mới đó là có nên cài đặt nó hay không. Không may cho bạn, lỗi này không thể giải quyết bằng chính sách "cứng và nhanh" hoặc một chính sách nào đó của công ty. Thông thường các nhà sản xuất phần cứng xuất bản các bản cập nhật trình điều khiển do ba lý do sau:

- Nâng cao hiệu năng các đặc tính của phần cứng hiện tại
- Triển khai các tính năng mới
- Loại trừ các lỗi trong các phiên bản trước

Trong hai trường hợp đầu, việc cài đặt bản cập nhật là một công việc tất nhiên do nó không gây ra các lỗi mới. Trong trường hợp sau, có thể bạn phải xem xét kỹ xem cấu hình hiện tại của bạn có mắc phải những lỗi như những gì mà bản cập nhật đã đưa ra. Nếu không bạn có thể loại bỏ việc cài đặt cập nhật.

Trên tất cả, câu hỏi xem có nên cài đặt các cập nhật trình điều khiển hay không phụ thuộc vào các thiết bị phần cứng, các chính sách và danh tiếng của nhà sản xuất. Một số nhà sản xuất đưa ra các cập nhật cho trình điều khiển một cách thường xuyên và lung tung, thường xuyên gây ra các lỗi mới trong các khi sửa chữa các lỗi cũ. Điều này đúng trong trường hợp một sản phẩm phần cứng là mới trên thị trường với mã trình điều khiển chưa được

kiểm tra một cách cẩn thận. Trong những trường hợp như vậy, trình điều khiển cuối cùng có thể không phải là tốt nhất. Tự động cài đặt tất cả phiên bản trình điều khiển mới có thể dẫn đến những lỗi hiệu năng nghiêm trọng đặc biệt nếu bạn có các thiết bị giống nhau được cài đặt trên hàng trăm máy tính.

Phương pháp tốt nhất dành cho người quản trị hệ thống đó là phân loại các phiên bản cập nhật trình điều khiển, thực hiện việc kiểm tra chúng trên các hệ thống tương tự, cũng giống như khi bạn sử dụng bất kỳ bản cập nhật phần mềm nào, trước khi triển khai chúng trên các máy tính của bạn.

Người sử dụng, nhà quản trị và quá trình cài đặt trình điều khiển thiết bị

Trong hầu hết các môi trường, phương án thích hợp nhất cho người sử dụng đầu cuối là họ không phải cài đặt hoặc cập nhật các trình điều khiển thiết bị. Điều này còn là đặc biệt đúng trong môi trường mạng khi mà các nhà quản trị muốn duy trì một cấu hình hệ thống đồng nhất trên toàn mạng. Nó sẽ làm đơn giản hóa tiến trình duy trì và xử lý sự cố cho các máy tính trên mạng do các nhân viên hỗ trợ kỹ thuật không cần phải kiểm tra mỗi hệ thống để xác định xem các cập nhật đã được cài đặt chưa.

Tuy nhiên, việc cấp nhật các trình điều khiển thiết bị thường là khó khăn hơn khi triển khai trên một lượng lớn máy tính so với việc cập nhật các phần mềm. Đôi khi bạn cần cài đặt trình điều khiển trên mỗi máy tính riêng lẻ và các nhà quản trị không có thời giờ hoặc sự kiên nhẫn để di chuyển tới tất cả các máy tính nhằm cấu hình các thiết bị và trình điều khiển của chúng. Windows Server 2003 bao gồm các tùy chọn trình điều khiển được xác nhận (***driver signing***), khả năng gán các quyền cài đặt trình điều khiển cho các người sử dụng thích hợp, tạo ra một môi trường mềm dẻo trong việc cấu hình thiết bị và cài đặt trình điều khiển.

Kiểm soát truy cập trình điều khiển thiết bị

Đối với hầu hết các công việc cài đặt, các thành viên nhóm ***Administrators*** đều có quyền hạn không hạn chế trong việc cài đặt bất kỳ thiết bị phần cứng nào cũng như các trình điều khiển của chúng. Sở dĩ như vậy là vì nhóm ***Administrators*** nhận được quyền hạn người sử dụng ***Load And Unload Device Drivers*** (*cài đặt và gỡ bỏ các trình điều khiển thiết bị*) thông qua các chính sách cục bộ hoặc thông qua ***GPO Default Domain Controllers***. Tuy nhiên, các thành viên của nhóm ***Users*** và ***Domain Users*** không được gán quyền hạn này nên họ sẽ bị hạn chế quyền thực hiện các công việc trên. Mặc

định, người sử dụng chỉ có thể cài đặt các thiết bị PnP với điều kiện các yêu cầu sau phải được đáp ứng:

- Trình điều khiển phải có một chữ ký số hóa (đây là đặc tính chứng tỏ rằng trình điều khiển này đã được hãng Microsoft tiến hành thử nghiệm và kiểm tra)
- Không có những đòi hỏi yêu cầu Windows hiển thị giao diện cho phép cài đặt thiết bị.
- Trình điều khiển thiết bị đã có sẵn trên máy tính.

Với những yêu cầu này có nghĩa người sử dụng có thể cài đặt các máy in và các thiết bị USB và IEEE 1394 (***FireWire***). Nếu có bất kỳ một điều kiện nào nói trên không đáp ứng, người sử dụng không thể cài đặt thiết bị nếu họ không được gán thêm quyền.

Các lựa chọn trình điều khiển được xác nhận

Tất cả các trình điều khiển thiết bị và các file hệ điều hành trên Windows Server 2003 đều có một chữ ký số hóa của Microsoft. Điều này xác nhận rằng chúng đã được kiểm tra và chưa bị thay đổi kể từ khi nhà sản xuất tạo ra. Đặc tính này được đưa ra nhằm ngăn chặn không cho can thiệp và thay đổi các trình điều khiển thiết bị và các phần mềm khác khi người sử dụng cài đặt các đoạn mã chưa được xác thực như ***virus, Trojan horses*** chẳng hạn. Chúng cũng xác nhận rằng thiết bị này là hoàn toàn tương thích với hệ điều hành. Các trình điều khiển thiết bị do các hãng sản xuất thứ ba cung cấp có thể hoặc không được xác nhận.

Trong Windows Server 2003, bạn có thể điều khiển máy tính sẽ phản ứng ra sao khi bạn cài đặt các file chứa trình điều khiển chưa được xác nhận. Để thực hiện điều này, truy cập vào máy tính bằng tài khoản ***Administrator***, kích đúp vào ***System*** trong ***Control Panel*** sau đó lựa chọn thẻ ***Hardware*** trên hộp thoại ***System Properties***. Nhấp ***Driver Signing*** để hiển thị hộp thoại ***Driver Signing Options*** (như hình vẽ 11-2).

Hình 11-2: Hộp thoại Driver Signing Options

Các lựa chọn trên hộp thoại này gồm có:

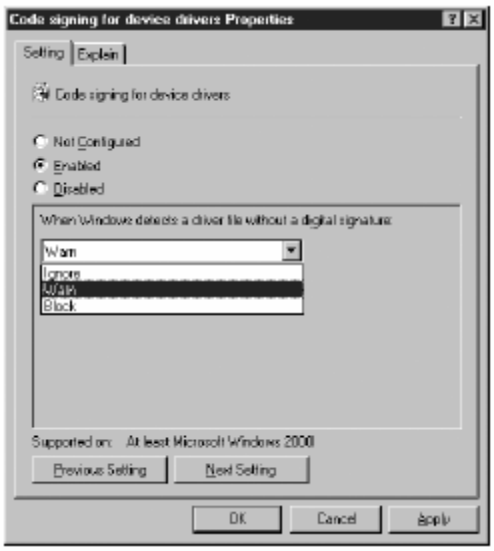
- **Ignore** (*bỏ qua*) Cho phép cài đặt tất cả các trình điều khiển thiết bị lên máy tính bất kế chúng có được xác nhận hay không. Lựa chọn này chỉ cho phép khi bạn truy cập vào hệ điều hành với tài khoản là thành viên của nhóm *Administartors*.
- **Warn** (*cảnh báo*) Hiển thị cảnh báo khi chương trình cài đặt hoặc Windows cài đặt một trình điều khiển thiết bị không có chữ ký số hóa. Tiếp theo người sử dụng có thể lựa chọn hoặc tiếp tục hoặc ngừng cài đặt. Đây là lựa chọn mặc định.
- **Block** (*khóa*) ngăn không cho phép cài đặt các trình điều khiển thiết bị không có chữ ký số hóa.

  CHÚ Ý Mục tiêu của kỳ thi *Các mục tiêu cho kỳ thi 70-290 yêu cầu các học viên có khả năng "cấu hình các lựa chọn về trình điều khiển được xác nhận"*

Khi bạn truy cập hệ điều hành bằng tài khoản là thành viên của nhóm ***Administartors***, thẻ này còn có hộp kiểm tra ***Make This Action The System Default*** (*sử dụng lựa chọn này như thiết lập mặc định của hệ thống*). Khi lựa chọn hộp kiểm tra này có nghĩa là lựa chọn bạn chọn ở trên trở thành thiết lập mặc định cho tất cả người sử dụng truy cập vào hệ thống.

Ngoài ra để cấu hình bằng tay các lựa chọn về trình điều khiển được xác nhận cho các máy tính đơn lẻ, bạn có thể sử dụng các chính sách nhóm để bắt buộc tất cả hoặc một phần các máy tính trên mạng. Trong bảng điều khiển ***Group Policy Object Editor***, trỏ tới thư mục ***User Configuration/Administrative Templates/System***. Ở đây bạn sẽ thấy một chính sách có tên là ***Code Signing For Device Drivers***. Khi bạn mở hộp

thoại ***Code Signing For Device Drivers Properties,*** như hình vẽ 11-3, bạn có thể thấy các lựa chọn giống trong hộp thoại ***Driver Signing Options***.



Hình 11-3: Hộp thoại Code Signing For Device Drivers Properties

SỬ DỤNG TRÌNH HƯỚNG DẪN ADD HARDWARE

Trình hướng dẫn Add Hardware được thiết kế giúp bạn từng bước trong quá trình cài đặt và cấu hình thiết bị phần cứng mới và các trình điều khiển thiết bị. Tuy nhiên trình hướng dẫn (***Wizzard***) bắt đầu như thế nào và việc tương tác được yêu cầu từ phía người sử dụng ra sao lại phụ thuộc vào bản chất của thiết bị phần cứng được cài đặt. Trong hầu hết các trường hợp, trình hướng dẫn được khởi tạo khi hệ thống phát hiện một thiết bị phần cứng mới hoặc thông qua PnP hoặc thông qua tiến trình phát hiện phần cứng mặc định của hệ điều hành.

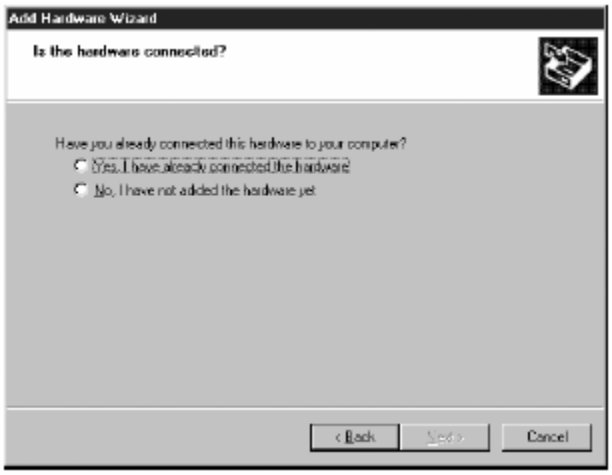
> ***CHÚ Ý Mục tiêu của kỳ thi*** *Các mục tiêu cho kỳ thi 70-290 yêu cầu các học viên có khả năng "cài đặt và cấu hình các thiết bị phần cứng máy chủ"*

Với các thiết bị PnP, trình hướng dẫn thường không tương tác với người sử dụng. Hệ thống sẽ hiển thị một số chỉ thị tiến trình khi nó xác định và nhận diện phần cứng mới. Kế đó nó sẽ cài đặt và cấu hình trình điều khiển thiết bị. Nếu Windows Server 2003 không chứa trình điều khiển thiết bị, trình hướng dẫn sẽ nhắc nhở bạn cung cấp hoặc tìm kiếm nó. Nếu hệ thống không thể xác định thiết bị, trình hướng dẫn sẽ giúp bạn xác định chủng loại thiết bị, nhà sản xuất và kiểu.

Nếu hệ thống không phát hiện sự hiện diện của thiết bị phần cứng mới, bạn có thể khởi tạo trình hướng dẫn bằng tay theo các cách sau:

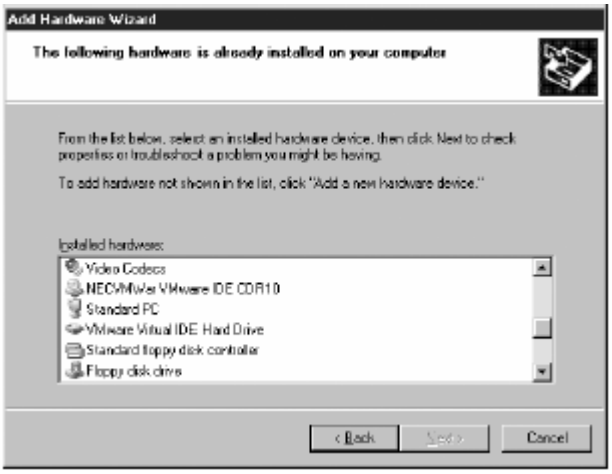
- Lựa chọn Add Hardware trong Control Panel.
- Mở hộp thoại ***System Properties***, lựa chọn thẻ ***Hardware*** và nhấp vào ***Add Hardware Wizard***.

Khi bạn nhấp ***Next*** để bỏ qua trang ***Welcome*** của trình hướng dẫn, hệ thống sẽ thực hiện một tiến trình phát hiện phần cứng PnP. Nếu hệ thống không phát hiện ra có bất kỳ phần cứng mới nào, trang ***Is The Hardware Connected?*** xuất hiện như hình vẽ 11-4 nhắc nhở bạn xác định xem bạn có cài đặt phần cứng mới không. Đây là một câu hỏi thủ thuật: nếu bạn lựa chọn ***No, I Have Not Added The Hardware Yet*** (*không, tôi không thêm phần cứng nào cả*) và nhấp ***Next*** thì trình hướng dẫn sẽ dừng lại, hướng dẫn bạn cài đặt phần cứng và chạy lại trình hướng dẫn. Trong thực tế, bạn có thể cài đặt một số loại phần cứng mà không cần sự hiện diện thực sự của chúng. Ví dụ, bạn có thể cài đặt một máy in cục bộ và trình điều khiển trước khi kết nối máy in vật lý đến máy tính.



Hình 11-4: Trang Is The Hardware Connected? của Add Hardware Wizard

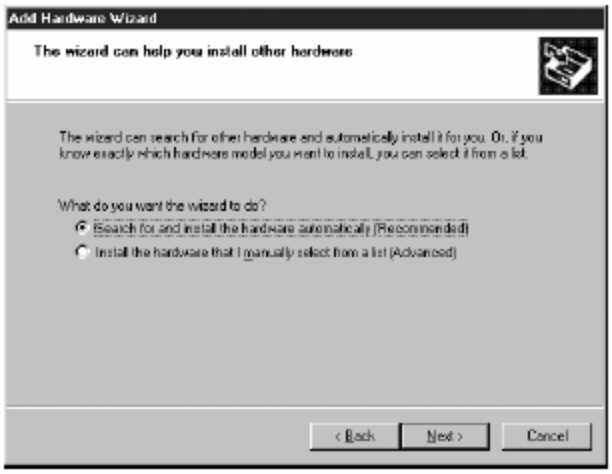
Nếu bạn lựa chọn ***Yes, I Have Already Connected The Hardware*** (*vâng, tôi đã kết nối thiết bị phần cứng vào máy tính*) và nhấp ***Next***, trình hướng dẫn sẽ hiển thị một trang liệt kê tất cả các thiết bị phần cứng được cài đặt trên máy tính như hình vẽ 11-5. Để cài đặt thiết bị mới, di chuyển xuống phía dưới trong danh sách và lựa chọn ***Add A New Hardware Device*** và nhấp ***Next***.



Hình 11-5: Hộp danh sách Installed Hardware trên Add Hardware Wizard

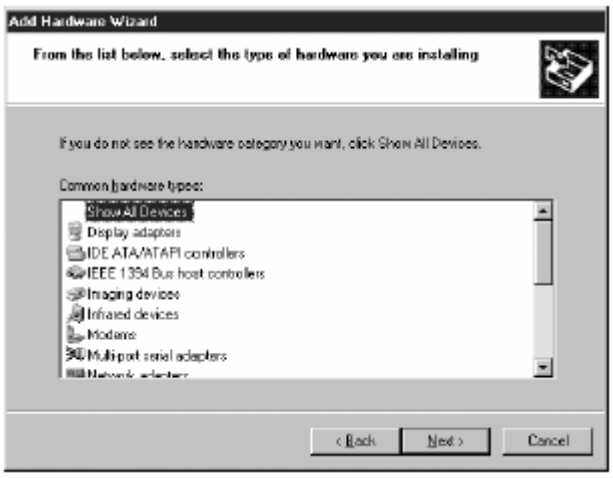
> ***CHÚ Ý Xử lý sự cố thiết bị phần cứng*** *Danh sách các thiết bị được cài đặt cung cấp chức năng cơ bản khác của trình hướng dẫn đó là khả năng xử lý sự cố với các thiết bị phần cứng sẵn có trên hệ thống. Để biết thêm thông tin về quá trình xử lý sự cố trên phần cứng và trình điều khiển thiết bị, xem phần "Xử lý sự cố các thiết bị và trình điều khiển" ở phần sau của chương này.*

Trong trang kế tiếp, xem hình vẽ 11-6, bạn cần xác định xem bạn muốn trình hướng dẫn tìm kiếm phần cứng mới hoặc lựa chọn phần cứng từ một danh sách. Điều này dường như hơi kỳ cục do trình hướng dẫn đã thực sự chạy thông qua một tiến trình phát hiện phần cứng ngay sau khi khởi tạo. Tuy nhiên đó là đối với các thiết bị PnP. Với các thiết bị không phải PnP, bạn cần lựa chọn ***Search For And Install The Hardware Automatically*** để khởi tạo quá trình tìm kiếm.



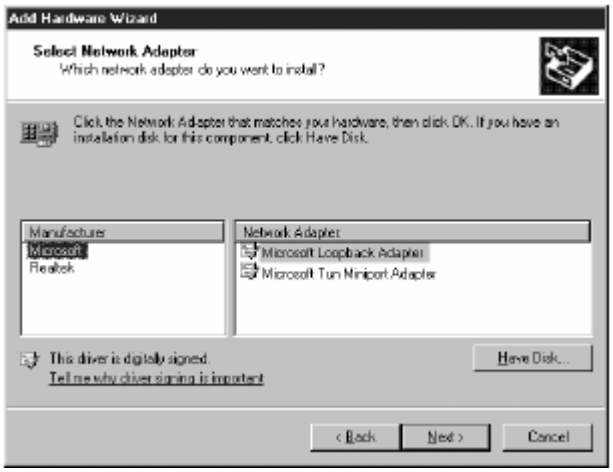
Hình 11-6: Lựa chọn phát hiện phần cứng Add Hardware Wizard

Nếu trình hướng dẫn không thể xác định được phần cứng mới của bạn hoặc nếu bạn lựa chọn ***Install The Hardware That I Manually Select From A List*** và nhấp ***Next***, một trang xuất hiện cho phép bạn lựa chọn chủng loại thiết bị từ danh sách bao gồm các phần cứng thông dụng như hình vẽ 11-7. Lựa chọn loại thiết bị mà bạn muốn cài đặt và nhấp ***Next.***



Hình 11-7: Hộp Common Hardware Types trong Add Hardware Wizard

Tùy thuộc vào loại phần cứng bạn lựa chọn, bạn có thể nhìn thấy thêm một trang phát hiện phần cứng nhưng cuối cùng trình hướng dẫn sẽ hiển thị một trang giống như hình vẽ 11-8. Ở đây bạn có thể lựa chọn nhà sản xuất thiết bị phần cứng và dòng sản phẩm cụ thể. Tất cả các thiết bị phần cứng được liệt kê đều có các trình điều khiển đi kèm với hệ điều hành. Nếu thiết bị phần cứng của bạn không có trong danh sách liệt kê, bạn phải nhấp vào ***Have Disk*** và xác định vị trí các file chứa trình điều khiển thiết bị.



Hình 11-8: Một trong những danh sách lựa chọn phần cứng của Add Hardware Wizard

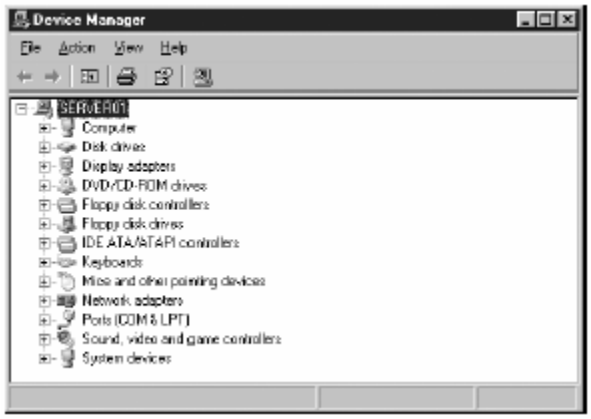
Một khi bạn đã xác định chính xác thiết bị phần cứng cần cài đặt, trình hướng dẫn sẽ hiển thị các điều khiển theo loại thiết bị ở đó bạn sẽ xác định xem hệ thống truy cập tới phần cứng như thế nào. Ví dụ, nếu bạn cài đặt một modem, trình hướng dẫn sẽ nhắc nhở bạn cổng COM mà modem sử dụng. Trong một số trường hợp nếu trình hướng dẫn không thể xác định phần cứng bạn lựa chọn, nó sẽ cài đặt trình điều khiển thiết bị bằng cách sử dụng các thiết lập mặc định. Tiếp theo bạn có thể phải cấu hình lại trình điều khiển bằng tay trước khi hệ thống có thể liên kết với thiết bị.

Khi trình hướng dẫn hoàn thành, thiết bị mới được đưa vào cấu hình phần cứng của máy tính. Bạn có thể truy cập được tới nó hoặc không. Bạn có thể làm việc với bất kỳ thiết bị phần cứng nào đã được cài đặt trên máy tính cũng như trình điều khiển của chúng thông qua màn hình quản trị ***Device Manager*** được mô tả trong phần tiếp theo.

SỬ DỤNG DEVICE MANAGER

Device Manager là một công cụ quản trị phần cứng và trình điều khiển thiết bị chủ yếu trên hệ điều hành Windows Server 2003. Mặc dù nó không xuất hiện trong màn hình mặc định (xem hình vẽ 11-9) nhưng ***Device Manager*** là một MMC snap-in mà bạn có thể truy cập theo các cách khác nhau:

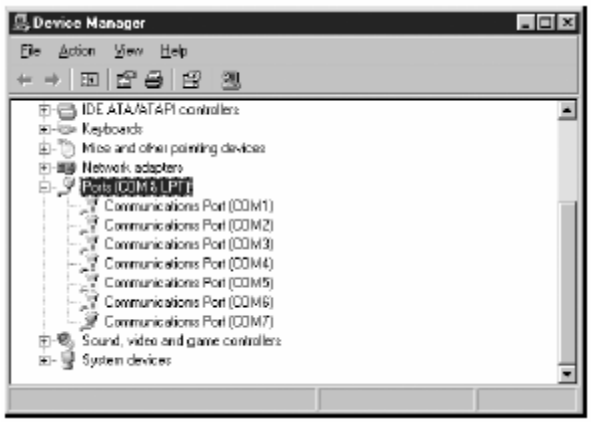
- Nhấp ***Start***, trỏ tới ***Control Panel*** và lựa chọn ***System***. Trong hộp thoại ***System Properties***, lựa chọn thẻ ***Hardware*** và tiếp theo nhấp ***Device Manager***.
- Nhấp ***Start***, trỏ tới ***Administrative Tools*** rồi lựa chọn ***Computer Management***. Trong màn hình quản trị ***Computer Management*** lựa chọn biểu tượng ***Device Manager***.
- Mở hộp thoại ***Run***, gõ mmc trong hộp văn bản ***Open*** và nhấp ***Enter*** để mở một cửa sổ trống MMC. Kế đó từ thực đơn ***File*** chọn ***Add/Remove Snap-in*** và thêm snap-in ***Device Manager*** vào màn hình quản trị.



Hình 11-9: Màn hình quản trị Device Manager

Mặc định, màn hình hiển thị ***Device Manager*** được bố trí theo dạng phân cấp với máy tính ở mức gốc và các loại phần cứng khác nhau bên dưới mức gốc. Mở rộng một trong các thiết bị trong màn hình này bạn sẽ thu được một danh sách tất cả các thành phần được cài đặt trên máy tính. Các thành phần được cấu hình và hoạt động tốt sẽ xuất hiện một biểu tượng biểu diễn chủng loại của thành phần này. Khi có lỗi với một thiết bị, biểu tượng sẽ được thay đổi theo các cách dưới đây (xem hình vẽ 11-10)

- Một dấu cảm thán màu vàng chỉ thị rằng thiết bị chưa được cài đặt, chưa được cấu hình chính xác hoặc chưa cài đặt trình điều khiển.
- Dấu hỏi màu vàng Chỉ thị rằng không thể xác định được thiết bị.
- Dấu X màu đỏ chỉ thị rằng thiết bị bị vô hiệu hóa



Hình 11-10: Các biểu tượng trong Device Manager

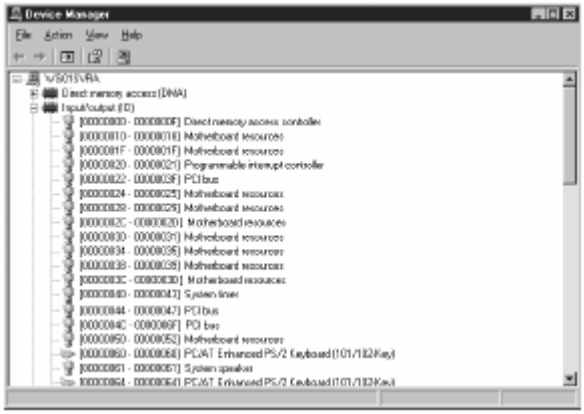
Device Manager có khả năng hiển thị thông tin theo bốn chế độ:

- Sắp xếp các thiết bị theo chủng loại Hiển thị một danh sách các loại thiết bị, cho phép bạn mở rộng để hiển thị một danh sách các thiết

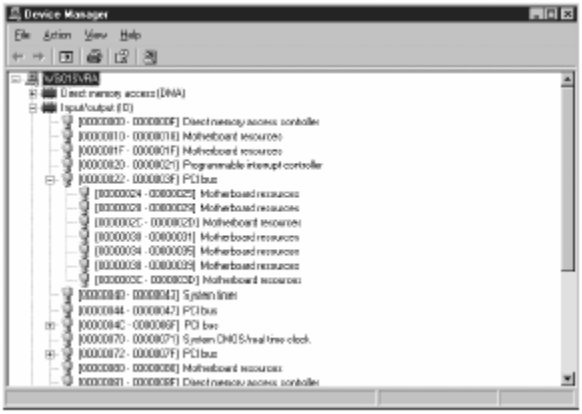
bị theo từng loại. Đây là màn hình hiển thị mặc định của ***Device Manager***.

- Sắp xếp các thiết bị theo kết nối Hiển thị một danh sách các kết nối mà các thiết bị phần cứng sử dụng để liên kết với máy tính. Mở rộng một kết nối sẽ hiển thị một danh sách các thiết bị sử dụng kết nối đó. Ví dụ, kết nối ***PCI Bus*** chứa các biểu tượng cho tất cả các card mở rộng và các thiết bị khác kết nối tới ***PCI Bus*** của hệ thống.

- Sắp xếp các tài nguyên theo chủng loại Hiển thị một danh sách các loại tài nguyên gồm có ***Direct Memory Access*** (*truy cập bộ nhớ trực tiếp*), ***Input/Output*** (*cổng vào/ra*), ***Interrupt Request*** (*yêu cầu ngắt*) và ***Memory*** (*bộ nhớ*). Ở đây bạn có thể mở rộng để hiển thị một danh sách các tài nguyên riêng lẻ của mỗi loại và các thiết bị đang sử dụng chúng.



- Sắp xếp các tài nguyên theo kết nối Hiển thị một danh sách các loại tài nguyên gồm có ***Direct Memory Access*** (*truy cập bộ nhớ trực tiếp*), ***Input/Output*** (*cổng vào/ra*), ***Interrupt Request*** (*yêu cầu ngắt*) và ***Memory*** (*bộ nhớ*). Ở đây bạn có thể mở rộng để hiển thị kết nối được kết hợp với mỗi tài nguyên riêng lẻ và thiết bị sử dụng mỗi kết nối đó.



Bất kể bạn sử dụng chế độ hiển thị nào của ***Device Manager,*** bạn cũng có thể lựa chọn bất kỳ một trong các thiết bị của máy tính và làm việc với phần cứng cũng như trình điều khiển thiết bị của nó như mô tả trong các phần dưới đây.

> ***CHÚ Ý Quản trị thiết bị từ xa*** *Cũng giống như các snap-in MMC khác,* ***Device Manager*** *có thể làm việc với hệ thống cục bộ hoặc với hệ thống khác trên mạng.Tuy nhiên khi* ***Device Maneger*** *được kết nối tới một máy tính khác trên mạng, nó chỉ hoạt động ở chế độ* ***read-only****. Bạn có thể xem thông tin về thiết bị phần cứng trên máy tính ở xa và trình điều khiển của nó nhưng bạn không thể thay đổi chúng. Để có thể thay đổi, bạn phải chạy* ***Device Manager*** *từ màn*

*hình quản trị của máy tính ở xa hoặc sử dụng dịch vụ **Remote Desktop** hoặc **Terminal Services**.*

***CHÚ Ý Mục tiêu của kỳ thi** Các mục tiêu cho kỳ thi 70-290 yêu cầu các học viên phải có khả năng "giám sát phần cứng máy chủ. Các công cụ gồm có **Device Manager**, **Hardware Troubleshooting Wizard** và các mục tương ứng trong **Control Panel** ".*

Cho phép và vô hiệu hóa các thiết bị

Bằng cách lựa chọn một thiết bị trong ***Device Manager*** và chọn ***Disable*** từ thực đơn ***Action*** bạn có thể làm cho thiết bị không hoạt động cho đến khi bạn kích hoạt nó bằng tay. Các thiết bị vô hiệu hóa xuất hiện trong ***Device Manager*** với chữ X màu đỏ trên biểu tượng của chúng.

Vô hiệu hóa một thiết bị không làm ảnh hưởng đến thiết bị đó, chỉ có trình điều khiển bị vô hiệu hóa ngăn không hệ thống truy cập vào nó. Một số thiết bị như bộ vi xử lý chẳng hạn không thể vô hiệu hóa và trong một số trường hợp bạn được hệ thống hướng dẫn khởi động lại máy tính để có thể vô hiệu hóa hoàn toàn thiết bị.

Một khi bạn đã khởi động lại máy tính sau khi đã vô hiệu hóa thiết bị, các tài nguyên hệ thống mà nó đang sử dụng sẽ được giải phóng ra khỏi hệ thống và có thể được gán lại cho các thiết bị khác nếu hệ thống thấy cần thiết. Khi bạn kích hoạt thiết bị trở lại (bằng cách lựa chọn ***Enable*** từ thực đơn ***Action***), nó có thể sử dụng các tài nguyên phần cứng không giống với những tài nguyên mà trước đó nó đã sử dụng.

Gỡ bỏ các trình điều khiển thiết bị

Bằng cách lựa chọn một thiết bị và chọn ***Uninstall*** từ thực đơn ***Action***, bạn có thể gỡ bỏ trình điều khiển thiết bị ra khỏi hệ thống. Ảnh hưởng của việc gỡ bỏ này phụ thuộc vào thiết bị được cài đặt như thế nào trong lần đầu tiên:

- Nếu thiết bị được cài đặt bằng tiến trình PnP Gỡ bỏ thiết bị kiểu này sẽ loại bỏ trình điều khiển thiết bị và xóa hoàn toàn thiết bị phần cứng ra khỏi ***Device Manager***. Tuy nhiên, nếu phần cứng vẫn hiện diện về mặt vật lý trên máy tính thì PnP sẽ cài đặt lại nó tại lần khởi động kế tiếp, hay khi bạn chọn ***Scan For Hardware Changes*** (*quét những thay đổi phần cứng*) từ thực đơn ***Action*** hoặc chạy ***Add Hardware Wizard***.
- Nếu bạn cài đặt thiết bị bằng tay thông qua Add Hardware Wizard Gỡ bỏ thiết bị sẽ loại bỏ trình điều khiển nhưng bản thân thiết bị

vẫn hiện diện trong ***Device Manager.*** Biểu tượng của thiết bị sẽ xuất hiện với dấu cảm thán.

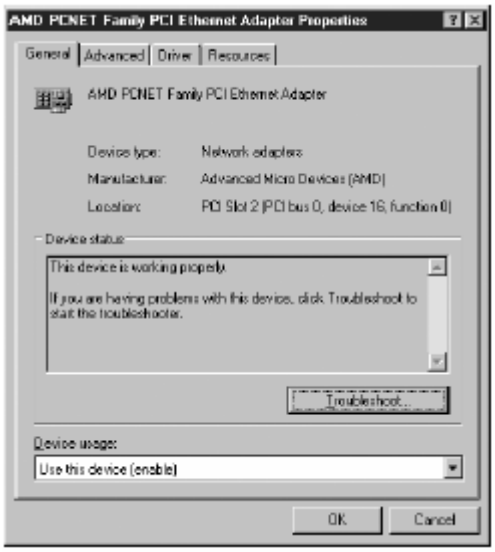
CHÚ Ý Phương pháp khác để gỡ bỏ các trình điều khiển *Bạn cũng có thể gỡ bỏ một trình điều khiển thiết bị bằng cách nhấp* ***Uninstall*** *trên trang* ***Driver*** *hộp thoại* ***Properties*** *của thiết bị.*

Quản lý các đặc tính thiết bị

Khi bạn lựa chọn một thiết bị trong ***Device Manager*** từ thực đơn ***Action*** và lựa chọn ***Properties***, hộp thoại ***Properties*** xuất hiện. Hộp thoại này chứa các thẻ với các nút điều khiển được bố trí cho phép bạn quản lý và cấu hình thiết bị cũng như trình điều khiển của nó. Nội dung của hộp thoại ***Properties*** có thể thay đổi tùy thuộc vào loại thiết bị và trình điều khiển nhưng hầu hết các thiết bị có ít nhất bốn thẻ được mô tả trong danh sách dưới đây.

CHÚ Ý Mục tiêu của kỳ thi *Các mục tiêu cho kỳ thi 70-290 yêu cầu học viên có khả năng "cấu hình các đặc tính và các thiết lập thiết bị"*

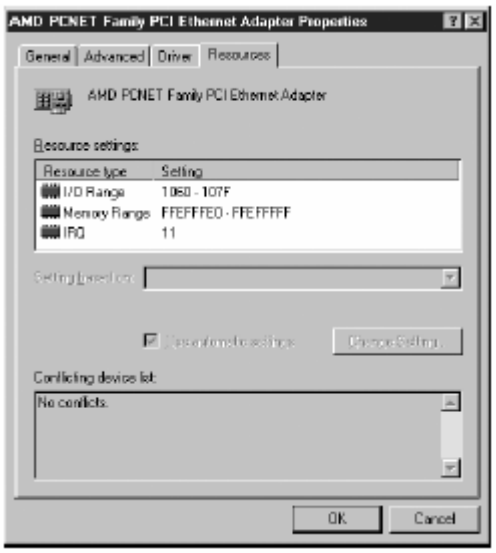
- General (*các đặc tính thông thường*) hiển thị thông tin về thiết bị gồm có chủng loại, hãng sản xuất, vị trí và trạng thái hoạt động hiện tại. Nó cũng bao gồm các điều khiển để cho phép, vô hiệu hóa và xử lý sự cố đối với thiết bị.



- **Advanced** (*nâng cao*) Chứa các điều khiển theo thiết bị do trình điều khiển thực hiện. Không phải lúc này cũng tồn tại thẻ này dó đó đôi khi gọi nó là các thiết lập nâng cao.

- **Driver** (*trình điều khiển*) Hiển thị thông tin về trình điều khiển thiết bị gồm có tên nhà cung cấp, ngày sản xuất, phiên bản, tên file và cũng chứa các điều khiển cho quá trình cập nhật, phục hồi phiên bản trước và gỡ bỏ trình điều khiển.

- **Resources** (*các tài nguyên*) Hiển thị các tài nguyên phần cứng hiện đang được các thiết bị sử dụng và trong các điều kiện cụ thể nó cung cấp các điều khiển để thay đổi cấu hình tài nguyên. Thẻ này không phải lúc nào cũng tồn tại.

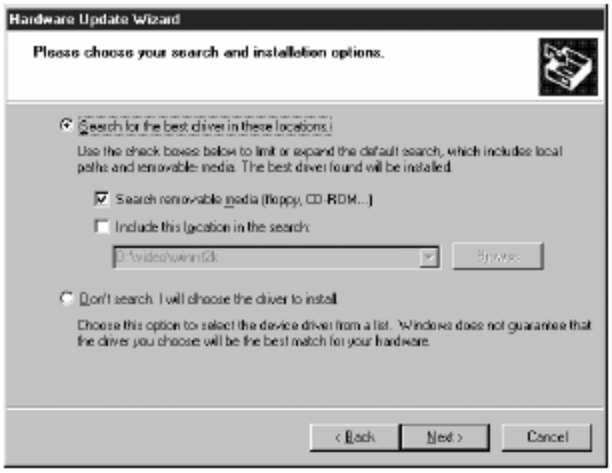


Cập nhật trình điều khiển

Để cập nhật trình điều khiển thiết bị, bạn mở hộp thoại ***Properties*** của thiết bị trong ***Device Manager***, lựa chọn thẻ ***Driver*** và nhấp vào ***Update Driver***. Động tác này sẽ khởi tạo ***Hardware Update Wizard*** cho phép bạn xác định vị trí các trình điều khiển cập nhật mà bạn muốn cài đặt hoặc tìm kiếm nó. Để cập nhật một trình điều khiển thiết bị, bạn phải có quyền giống như khi cài đặt nó lần đầu tiên như thành viên của nhóm ***Administrators*** hoặc có quyền hạn người sử dụng ***Load And Unload Device Drivers*** (*cài đặt và gỡ bỏ các trình điều khiển thiết bị*) chẳng hạn.

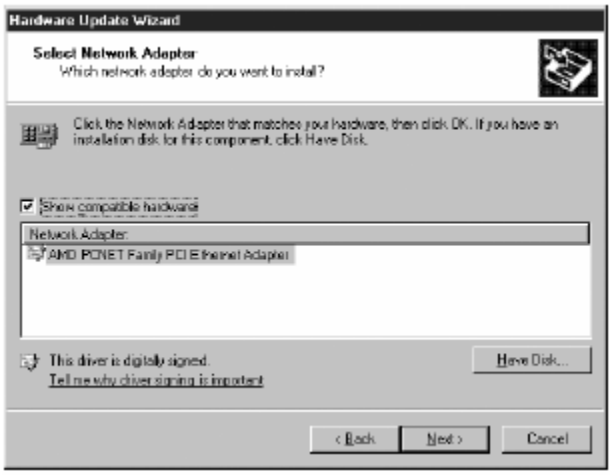
> ***CHÚ Ý Các cập nhật trình điều khiển không cần quyền thích hợp*** *Một trường hợp ngoại lệ đối với những yêu cầu về quyền khi cập nhật các trình điều khiển thiết bị đó là khi bạn nhận chúng qua* ***Windows Update Web site****. Với trường hợp này, bất kỳ người sử dụng nào cũng có thể cài đặt một trình điều khiển thiết bị.*

Khi bạn lựa chọn ***Install From A List Or Specific Location*** (*cài đặt từ một danh sách hoặc một vị trí xác định*) trên trang ***Welcome*** của trình hướng dẫn, nó sẽ cung cấp cho bạn một trang như trong hình vẽ 11-11 ở đó bạn có thể xác định vị trí mà trình hướng dẫn sẽ tìm kiếm các trình điều khiển hoặc cho phép bạn lựa chọn một trình điều khiển từ một danh sách.



Hình 11-11: Các lựa chọn cập nhật trình điều khiển

Thay vì tìm kiếm trình điều khiển, bạn cũng có thể lựa chọn ***Don't Search*** (*không tìm kiếm*) và bạn sẽ nhận được một trang như hình vẽ 11-12. Trang này liệt kê tất cả các trình điều khiển sẵn có trên hệ điều hành và tương thích với phần cứng lựa chọn. Bạn cũng có thể nhấp vào nút ***Have Disk*** để xác định một vị trí khác chứa trình điều khiển.



Hình 11-12: Lựa chọn một trình điều khiển cập nhật

Khi trình hướng dẫn hoàn thành tiến trình cài đặt trình điều khiển cập nhật, bạn có thể nhận được yêu cầu khởi động lại máy tính tùy thuộc vào loại thiết bị liên quan.

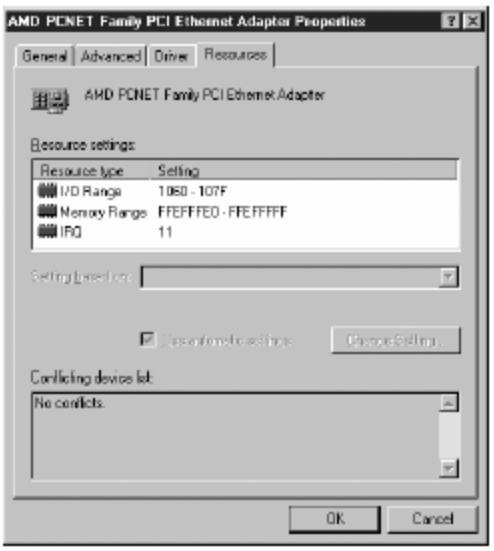
Phục hồi trình điều khiển thiết bị cũ

Trong một số trường hợp, bạn nhận thấy rằng trình điều khiển bạn cập nhật gần đây không hoạt động như mong muốn vì vậy bạn muốn quay trở lại phiên bản mà bạn đã sử dụng trước đây. Rất may mắn, khi bạn sử dụng

Device Manager để cập nhật một trình điều khiển thiết bị, Windows Server 2003 tự động giữ lại một phiên bản của các file được thay thế. Để quay trở lại với phiên bản đã cài đặt trước của trình điều khiển, bạn mở hộp thoại ***Properties*** của thiết bị và trên thẻ ***Driver*** lựa chọn ***Roll Back Driver***.

Quản lý các tài nguyên phần cứng

Mặc dù điều này không xảy ra thường xuyên nhưng bạn có thể cần cấu hình bằng tay các tài nguyên phần cứng mà một thiết bị Windows Server 2003 sử dụng. Điều này chỉ thực sự cần thiết khi bạn buộc phải cài đặt một phần cứng cũ không hỗ trợ chuẩn PnP như card mở rộng ISA chẳng hạn. Để làm việc với các tài nguyên phần cứng trên ***Device Manager***, bạn mở hộp thoại ***Properties*** của một thiết bị và lựa chọn thẻ ***Resources*** như hình vẽ 11-13.



Hình 11-13: Thẻ Resources trên hộp thoại Properties của một thiết bị

> ***CHÚ Ý Mục tiêu của kỳ thi*** *Các mục tiêu cho kỳ thi 70-290 yêu cầu các học viên có khả năng "cấu hình các thiết lập tài nguyên cho thiết bị".*

Trên thẻ này, hộp ***Resource Settings*** xác định các tài nguyên mà thiết bị hiện nay đang sử dụng theo loại và theo thiết lập. Với các thiết bị cài đặt sử dụng PnP, thẻ ***Resources*** chỉ mang tính chất cung cấp thông tin. Bạn không thể thay đổi cấu hình tài nguyên trên đó. Với các thiết bị cấu hình bằng tay, bạn có thể thay đổi các thiết lập tài nguyên mà trình điều khiển sử dụng.

Để thay đổi các thiết lập tài nguyên của một thiết bị, bạn phải xóa hộp kiểm tra ***Use Automatic Settings*** để cho phép các điều khiển khác trên thẻ. Kế đó bạn có thể sử dụng danh sách thả xuống ***Settings Based On*** để lựa chọn một

cấu hình phần cứng được thiết lập trước nếu có bất kỳ cái nào có thể. Bạn cũng có thể thay đổi thiết lập cho bất kỳ tài nguyên nào được liệt kê trong hộp ***Resource Settings*** bằng cách lựa chọn nó, nhấp vào ***Change Settings*** và chọn một giá trị khác.

Nếu bạn xác định một thiết lập tài nguyên trùng với cái mà một thiết bị khác hiện đang sử dụng thì thiết bị đó sẽ xuất hiện trong hộp danh sách ***Conflicting Device***. Bạn phải lựa chọn các tài nguyên chưa được sử dụng nhằm ngăn không cho xảy ra tình trạng các thiết bị xung đột hoạt động không đúng chức năng.

> ***CẢNH BÁO Xác định tài nguyên bằng tay*** *Một khi bạn đã cấu hình thủ công các tài nguyên cho một trình điều khiển thiết bị, các tài nguyên này được cấp phát một cách cố định. PnP không thể sử dụng các thiết lập này khi cấu hình cho các thiết bị khác thậm chí để giải phóng các tài nguyên xác định do các thiết bị khác sử dụng.*

SỬ DỤNG CONTROL PANEL

Device Manager cung cấp một công cụ truy cập toàn diện tới phần cứng cũng như trình điều khiển thiết bị của một máy tính nhưng đó không phải là phương tiện duy nhất. Windows Server 2003 lưu trữ thực sự thông tin về phần cứng và trình điều khiển trong ***Windows Registry*** và các công cụ như ***Device Manager*** chẳng hạn chỉ là giao diện mặt trước cung cấp truy cập đến dữ liệu ***registry***. Một công cụ khác trong Windows Server 2003 cũng cho phép truy cập đến thông tin ***registry*** thân thiện hơn đó là ***Control Panel***.

Một số ứng dụng trong ***Control Panel*** cho phép truy cập đến phần cứng và dữ liệu cấu hình trình điều khiển đối với các thành phần hệ thống khác nhau. Giao diện này không nhất quán và đầy đủ như ***Device Manager*** nhưng người sử dụng có thể truy cập tới một số các trình điều khiển thiết bị quan trọng hơn trên hệ thống theo cách này. Các ứng dụng trong ***Control Panel*** cung cấp khả năng truy cập tới các trình điều khiển thiết bị như sau:

- **Add Hardware** (*thêm thiết bị phần cứng*) Cho phép người sử dụng truy cập tới ***Add Hardware Wizard*** (như mô tả phần trên trong chương này) để cài đặt trình điều khiển thiết bị mới và xử lý sự cố đối với những cái sẵn có.
- **Display** (*hiển thị*) Cho phép người sử dụng truy cập tới các trình điều khiển thiết bị của video card và màn hình của máy tính để thay đổi các đặc tính như độ phân giải màn hình và độ sâu màu sắc.

- **Game Controllers** (*bộ điều khiển trò chơi*) Cho phép truy cập tới các trình điều khiển thiết bị dành cho bất kỳ bộ điều khiển trò chơi nào được cài đặt trên máy tính.
- **Keyboard** (*bàn phím*) Cho phép truy cập tới các trình điều khiển thiết bị dành cho bàn phím được cài đặt trên máy tính.
- **Mouse** (*chuột*) Cho phép truy cập tới các trình điều khiển thiết bị dành cho chuột hoặc thiết bị con trỏ khác được cài đặt trên máy tính.
- **Network Connections** (*các kết nối mạng*) Cho phép truy cập tới các trình điều khiển thiết bị dành cho các card mạng được cài đặt trên máy tính.
- **Phone And Modem Options** (*các lựa chọn về điện thoại và modem*) Cho phép truy cập tới các trình điều khiển thiết bị dành cho bất kỳ modem nào được cài đặt trên máy tính.
- **Printers and Faxes** (*máy in và máy fax*) Cho phép truy cập tới các trình điều khiển thiết bị dành cho các máy in được cài đặt trên máy tính.
- **Scanners and Cameras** (*máy quét và máy ảnh*) Cho phép truy cập tới các trình điều khiển thiết bị dành cho các máy quét và máy ảnh được cài đặt trên máy tính.

- **Soundss and Audio Devices** (*âm thanh và các thiết bị audio*) Cho phép truy cập tới các trình điều khiển thiết bị dành cho các card âm thanh và các thành phần liên quan tới âm thanh khác được cài đặt trên máy tính.

- **System** Cho phép truy cập tới hộp thoại ***Properties*** gồm có ***Device Manager, Add Hardware Wizard*** và các điều khiển về xác nhận trình điều khiển.

Trong hầu hết các trường hợp, ***Control Panel*** cũng như ***Device Manager*** đều cung cấp khả năng truy cập tới cùng hộp thoại ***Properties***. Các điều khiển này cũng bị hạn chế về mặt truy cập như ***Device Manager***.

XỬ LÝ SỰ CỐ CÁC THIẾT BỊ VÀ TRÌNH ĐIỀU KHIỂN

Đôi khi, bạn có thể gặp những rắc rối với các thành phần phần cứng và trình điều khiển thiết bị đặc biệt nếu bạn làm việc với các thiết bị không tuân theo chuẩn PnP. Windows Server 2003 cung cấp cho người sử dụng một số công cụ để bạn có thể xử lý những lỗi này. Một số công cụ nói trên được mô tả trong các phần dưới đây.

Các mã trạng thái của Device Manager

Khi một thiết bị hoặc trình điều khiển của nó hoạt động không đúng, ***Device Manager*** thông thường sẽ phát hiện ra lỗi và thay đổi biểu tượng thiết bị nhằm thông báo với người sử dụng về tình trạng lỗi của thiết bị. Tuy nhiên bạn có thể nhận được nhiều thông tin hơn về tình trạng lỗi của thiết bị nếu bạn mở hộp thoại ***Properties*** của thiết bị. Trên thẻ ***General***, hộp ***Device Status*** thường mô tả về lỗi xảy ra đối với thiết bị và kèm theo có thể là một mã lỗi. Bảng 11-1 sau mô tả các mã lỗi thường xảy ra và phương pháp xử lý sự cố tương ứng.

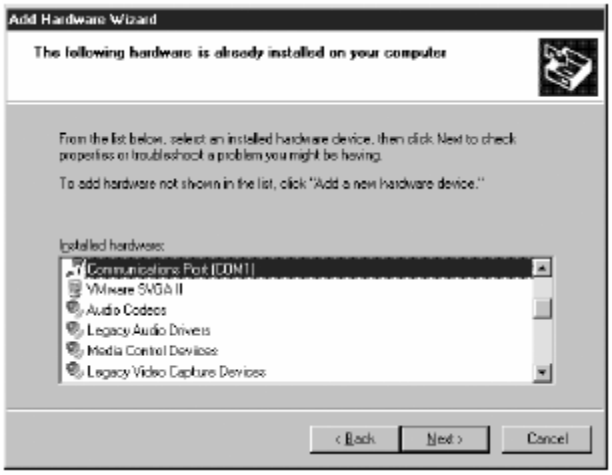
Bảng 11-1: Các mã lỗi trong Device Manager

Mã lỗi	Chú giải	Phương pháp xử lý sự cố
1	Thiết bị này không được cấu hình chính xác	Sử dụng ***Update Driver*** để cập nhật trình điều khiển thiết bị. Nếu không có sẵntrình điều khiển nào cố gắng gỡ bỏ thiết bị ra khỏi ***Device Manager***, sau đó khởi động lại hệ thống và cài đặt lại thiết bị.
3	Trình điều khiển thiết bị này có thể bị hỏng hoặc hệ thống của bạn đang ở trong tình trạng bộ nhớ hoặc các tài nguyên khác thấp	Trình điều khiển có thể bị hỏng. Nếu bạn cố gắng tải một file bị hỏng, hệ thống có thể nghĩ rằng nó cần nhiều bộ nhớ hơn. Sử dụng công cụ ***Task Manager*** để xác nhận rằng hệ thống của bạn không ở trong tình trạng bộ nhớ thấp. Nếu bộ nhớ vẫn đủ, sử dụng ***Update Driver*** để cài đặt một bản sao khác của trình điều

		khiển ấy.
10	Thiết bị không thể khởi động	Kiểm tra để xác nhận rằng phần cứng đã được cài đặt chính xác trên máy tính. Nếu đúng, chạy ***Hardware Update Wizard*** và sử dụng nút ***Update Driver*** nhưng không cho phép Windows Server 2003 tự động phát hiện thiết bị. Thay vào đó lựa chọn ***Install From A List Or Specific Location*** (*cài đặt từ một danh sách hoặc một thư mục xác định*) và trỏ trình hướng dẫn tới trình điều khiển tương ứng.
12	Thiết bị này không thể tìm đủ được tài nguyên trống để sử dụng. Nếu bạn muốn sử dụng thiết bị này, bạn cần vô hiệu một trong các thiết bị khác trên hệ thống này.	Lựa chọn thẻ ***Resources*** trên hộp thoại ***Properties*** chứa các lỗi. Windows Server 2003 sẽ phát hiện được các thành phần đang xung đột với thiết bị. Bạn cần vô hiệu hóa hoặc gỡ bỏ thành phần xung đột này. Sau đó bạn có thể cài đặt lại thiết bị mà bạn vừa gỡ bỏ và xem hệ thống có gán tài nguyên khác cho nó không. Nếu không, bạn phải gán tài nguyên cho nó một cách thủ công.
Các lỗi khác	Tùy thuộc vào từng trường hợp	Hầu hết các lỗi khác đều liên quan tới trình điều khiển không tương thích hoặc cấu hình trình điều khiển không chính xác. Cố gắng sử dụng một trình điều khiển khác hoặc gỡ bỏ thiết bị ra khỏi ***Device Manager*** và cài đặt lại nó.

Sử dụng các công cụ xử lý sự cố phần cứng

Trong các phần trước của chương này, bạn thấy rằng ***Add Hardware Wizard*** cho phép bạn lựa chọn thành phần đã được cài đặt trên máy tính bằng cách sử dụng một giao diện như hình vẽ 11-14. Hộp danh sách ***Installed Hardware*** hiển thị trong trình hướng dẫn luôn luôn bắt đầu với các thiết bị có vấn đề. Vì vậy bạn có thể trình hướng dẫn này để xử lý một thiết bị hoạt động không chính xác. Khi bạn lựa chọn một mục trong hộp danh sách ***Installed Hardware***, trình hướng dẫn sẽ hiển thị trạng thái hiện tại của nó và cho phép bạn bắt đầu tiến trình xử lý. Đôi khi trình hướng dẫn giúp bạn tìm thấy nguyên nhân của lỗi.



Hình 11-14: Danh sách phần cứng cài đặt trong Add Hardware Wizard

Các công cụ xử lý sự cố trên Windows Server 2003 được thực hiện trong ***Help And Support Center*** như hình vẽ 11-15. Màn hình xuất hiện tùy thuộc vào lỗi trên thiết bị và trạng thái hiện tại của phần cứng. Ví dụ, một công cụ xử lý sự cố thông thường sẽ hỏi bạn xác nhận rằng thiết bị có nằm trong HCL (*danh sách phần cứng tương thích*) trên Windows Server 2003 và tiếp theo hỏi bạn gần đây có cài đặt trình điều khiển thiết bị mới không. Tiếp theo công cụ xử lý có thể cung cấp các hướng dẫn giúp bạn xử lý những rắc rối trên thiết bị như sử dụng lại trình điều khiển cũ hoặc cài đặt lại thiết bị chẳng hạn.

Hình 11-15: Màn hình xử lý sự cố phần cứng trên Windows Server 2003

Phục hồi trạng thái từ Device Disaster (*thảm họa thiết bị*)

Đôi khi, việc cài đặt hoặc nâng cấp một trình điều khiển thiết bị có thể gây ra những lỗi nghiêm trọng trên hệ thống của bạn. Tùy thuộc vào sự quan trọng của thiết bị mà ảnh hưởng của nó có thể là từ mức độ không đáng kể đến mức độ cực kỳ nguy hiểm. Điều này đặc biệt đúng đối với các thành phần hệ thống lõi như các trình điều khiển màn hình chẳng hạn bởi vì cấu hình lỗi có thể làm cho máy tính của bạn không thể sử dụng được. Quay trở lại trình điều khiển cũ rất khó khăn do bạn không thể nhìn thấy màn hình.

Windows Server 2003 cung cấp nhiều phương pháp cho phép bạn phục hồi hệ thống do những lỗi liên quan đến trình điều khiển. Các công cụ được thiết kế cho các mục đích khác nhau. Bạn có thể sử dụng các công cụ sau để phục hồi lỗi do quá trình cài đặt trình điều khiển:

- **Driver Rollback** (*sử dụng lại trình điều khiển cũ*) Như đã đề cập ở trên, sử dụng lại phiên bản trình điều khiển cũ là phương pháp dễ dàng để giải quyết lỗi do trình điều khiển sai. Tất nhiên bạn phải có đủ quyền hệ thống để sử dụng ***Device Manager*** và thực hiện chức năng này.
- **Last Known Good Configuration** (*cấu hình tốt nhất mà bạn sử dụng trong lần gần đây nhất*) Được sử dụng khi một thiết bị cập nhật trình điều khiển yêu cầu khởi động lại và máy tính không thể khởi động đến điểm cho phép bạn đăng nhập vào hệ điều hành. Khi bạn thay đổi các trình điều khiển, hệ thống yêu cầu khởi động lại nhưng lỗi nằm trong tiến trình khởi động, bạn có thể nhấn phím F8 khi hệ thống khởi động lại và lựa chọn ***Last Know Good***

Configuration để phục hồi khóa ***registry: HKLM\System\CurrentControlSet*** trở về giá trị bạn đầu chứa thông tin về trình điều khiển cũ. Nếu lỗi trình điều khiển không tự xảy ra cho đến khi bạn đăng nhập thành công vào hệ thống (điều này thường xảy ra đối với những cập nhật trình điều khiển màn hình) thì lựa chọn này ít khi được sử dụng. Bởi vì, một khi bạn đã đăng nhập thành công vào hệ thống thì cấu hình lần cuối cùng tốt sẽ bị ghi đè lên ngay.

- **Safe Mode** (*chế độ an toàn*) Nếu một tiến trình cài đặt trình điều khiển thiết bị làm cho máy tính hoạt động không chính xác, nhấp F8 khi hệ thống khởi động lại và chọn chế độ ***Safe Made***. Chế độ này làm cho Windows Server 2003 khởi động với một cấu hình tối thiểu và chỉ có các trình điều khiển thiết bị cần cho tiến trình khởi động và đăng nhập. Một khi hệ thống đang chạy trong chế độ ***Safe Mode*** bạn có thể sử dụng ***Device Manager*** để vô hiệu hóa thiết bị gây ra lỗi.
- **Recovery Console** (*màn hình phục hồi hệ thống*) Khi cả ***Last Know Good Configuration*** lẫn ***Safe Mode*** đều không thể giúp bạn đăng nhạp vào hệ thống thì ***Recovery Console*** sẽ giúp bạn đăng nhập và truy cập tới một phần hạn chế các file hệ thống từ chế độ dòng lệnh. Từ ***Recovery Console***, bạn có thể vô hiệu hóa lỗi nhưng để làm được điều đó bạn phải biết chính xác tên cuả thiết bị hoặc trình điều khiển (hoặc cả hai).

TỔNG KẾT

- Các trình điều khiển thiết bị là các phần mềm cho phép các ứng dụng và hệ điều hành liên kết với các thiết bị phần cứng xác định. Mỗi thiết bị phần cứng mà bạn cài đặt trên máy tính đều phải có một trình điều khiển tương ứng được thiết kế cho hệ điều hành mà máy tính của bạn đang sử dụng.
- ***Plug and Play*** (PnP) là một chuẩn cho phép các máy tính phát hiện và nhận diện các thiết bị phần cứng và tiếp theo cài đặt, cấu hình trình điều khiển cho chúng. PnP tự động gán các tài nguyên phần cứng cho mỗi thiết bị và bạn có thể cấu hình lại các thiết bị khác để phù hợp với những nhu cầu đặc biệt của mỗi thành phần.
- Windows Server 2003 chứa một thư viện lớn các trình điều khiển dành cho nhiều thiết bị phần cứng khác nhau. Nếu Windows không chứa trình điều khiển cho thiết bị trên máy tính của bạn thì bạn phải lấy chúng từ nhà sản xuất thiết bị đó (thông thường chúng đi kèm theo thiết bị và được chứa trong đĩa CD cài đặt hoặc đĩa mềm)
- Các trình điều khiển sẵn có trên Windows Server 2003 tất cả đều được kiểm chứng và đảm bảo rằng chúng tương thích hoàn toàn với hệ điều hành. Bạn có thể cấu hình cách thức xử lý của hệ điều hành khi bạn thực hiện cài đặt một trình điều khiển chưa qua kiểm chứng bằng cách sử dụng hộp thoại ***Driver Signing Options***.
- Để liên lạc với máy tính, các thiết bị phần cứng sử dụng các tài nguyên phần cứng như các yêu cầu ngắt (**IRQ**), các địa chỉ vào/ra (**I/O**), các kênh **DMA** (*truy cập trực tiếp bộ nhớ*) và các địa chỉ bộ nhớ chẳng hạn.
- ***Device Manager*** là một màn hình quản trị liệt kê tất cả các thiết bị phần cứng trên máy tính của bạn và chỉ rõ những lỗi liên quan đến thiết bị hoặc trình điều khiển.
- Sử dụng ***Device Manager***, bạn có thể cho phép hoặc vô hiệu hóa các thiết bị, cập nhật hoặc sử dụng lại các trình điều khiển, quản lý thiết bị và các đặc tính trình điều khiển của chúng và giải quyết những lỗi xung đột tài nguyên phần cứng.
- Người sử dụng phải có quyền quản trị mới có thể cài đặt và quản lý các thiết bị phần cứng cũng như các trình điều khiển của chúng. Một ngoại lệ đối với trường hợp này đó là người sử dụng không có quyền quản trị vẫn có thể cài đặt các thiết bị PnP khi thiết bị đó

không yêu cầu bạn cấp trình điều khiển hoặc yêu cầu sự can thiệp của người sử dụng.

- Nhiều nhà sản xuất thiết bị phần cứng đưa ra các cập nhật cho trình điều khiển một cách định kỳ. Điều này buộc người quản trị hệ thống phải quyết định có nên cài đặt chúng không và ai là người cài đặt chúng, khi nào thì cài đặt.
- Lựa chọn ***Last Known Good Configuration*** rất hữu dụng cho bạn quay trở lại trình điều khiển đã được sử dụng trước đó nhưng chỉ khi nào bạn chưa đăng nhập thành công vào hệ thống.
- Khởi động máy tính trong chế độ ***Safe Mode*** sẽ chỉ tải một phần tối thiểu các trình điều khiển, cho phép bạn truy cập vào ***Device Manager*** và có thể vô hiệu hóa, gỡ bỏ hoặc quay trở lại trình điều khiển cũ nhằm ngăn không cho hệ thống rơi vào tình trạng hoạt động thiếu ổn định.

BÀI TẬP THỰC HÀNH

==========

Bài tập thực hành thực hành 11-1: Hiển thị các tài nguyên phần cứng

Trong bài thực hành này, bạn sẽ sử dụng ***Device Manager*** để hiển thị các tài nguyên phần cứng trên máy tính của bạn và các thiết bị đang sử dụng chúng.

1. Truy cập vào hệ điều hành Windows Server 2003 bằng tài khoản ***Administrator.***
2. Nhấp ***Start,*** trỏ tới ***Control Panel*** và chọn ***System***. Hộp thoại ***System Properties*** xuất hiện.
3. Lựa chọn thẻ ***Hardware*** và tiếp theo nhấp vào ***Device Manager***. Cửa sổ ***Device Manager*** xuất hiện.
4. Trên thực đơn ***View*** chọn ***Resources By Type***.
5. Mở rộng tiêu đề ***Interrupt Request (IRQ)*** và chú ý các thiết bị sử dụng các chuỗi ***IRQ*** của hệ thống.

==========

Bài tập thực hành thực hành 11-2: Cấu hình các lựa chọn chữ ký trình điều khiển

Trong bài thực hành này, bạn sẽ cấu hình các lựa chọn về trình điều khiển được xác thực trên máy tính.

1. Truy cập vào hệ điều hành Windows Server 2003 bằng tài khoản ***Administrator.***
2. Nhấp ***Start***, trỏ tới ***Control Panel*** và chọn ***System***. Hộp thoại ***System Properties*** xuất hiện.
3. Lựa chọn thẻ ***Hardware*** rồi nhấp vào ***Driver Signing***. Hộp thoại ***Driver Signing Options*** xuất hiện.
4. Lựa chọn ***Block*** và nhấp ***OK.*** Bạn sẽ không được phép cài đặt các trình điều khiển chưa được hãng Microsoft ký xác nhận.

==========

Bài tập thực hành thực hành 11-3: Cài đặt trình điều khiển thiết bị

Trong bài thực hành này, bạn sẽ cài đặt trình điều khiển thiết bị cho một card mạng không có thực trên máy tính của bạn.

1. Truy cập vào hệ điều hành Windows Server 2003 bằng tài khoản ***Administrator***.
2. Nhấp ***Start,*** trỏ tới ***Control Panel*** và chọn ***System***. Hộp thoại ***System Properties*** xuất hiện.
3. Lựa chọn thẻ ***Hardware*** rồi nhấp vào ***Add Hardware Wizard.***
4. Nhấp ***Next*** và đợi trình hướng dẫn quét máy tính của bạn để tìm ra thiết bị mới. Nếu bạn không thêm bất kỳ thiết bị nào, trình hướng dẫn sẽ hỏi bạn xem thiết bị mới đã được kết nối chưa.
5. Lựa chọn ***Yes, I Have Already Connected The Hardware*** và nhấp ***Next.***
6. Cuộn tới phần cuối trong danh sách thiết bị phần cứng cài đặt ***Installed Hardware***, lựa chọn ***Add A New Hardware Device*** và kế đó nhấp ***Next***.
7. Lựa chọn ***Install The Hardware That I Manually Select From A List (Advanced)*** và nhấp ***Next***.
8. Trong danh sách ***Common Hardware Types***, lựa chọn ***Network Adapters*** rồi nhấp ***Next***.
9. Lựa chọn ***Microsoft*** là nhà sản xuất và ***Microsoft Loopback Adapter*** là card mạng rồi nhấp ***Next***.
10. Nhấp ***Next*** để cài đặt card và tiếp theo nhấp ***Finish*** để đóng trình hướng dẫn lại.

11. Windows Server 2003 sẽ tải trình điều khiển và cài đặt thiết bị. Một card mạng mới có tên ***Microsoft Loopback Adapter*** sẽ xuất hiện trong ***Device Manager*** bên dưới nhóm ***Network Adapters***.

CÁC CÂU HỎI ÔN TẬP

1. Một người sử dụng là thành viên của nhóm ***Users*** muốn cài đặt một máy in USB được kết nối tới máy in của bạn. Trình điều khiển máy in có sẵn trong Windows Server 2003. Người sử dụng có thể cài đặt máy in mà không cần tới sự trợ giúp của người quản trị không? Tại sao có và tại sao không?
2. Một người sử dụng là thành viên của nhóm ***Users*** muốn cài đặt một máy in USB được kết nối tới máy in của bạn. Trình điều khiển máy in có sẵn trong Windows Server 2003 nhưng nhà sản xuất cung cấp một trình điều khiển được xác thực trên đĩa CD-ROM. Người sử dụng có thể cài đặt máy in mà không cần tới sự trợ giúp của người quản trị không? Tại sao có và tại sao không?
3. Trong tình huống nào bạn phải thay đổi các thiết lập tài nguyên phần cứng cho một thiết bị?
4. Bạn cần gỡ bỏ tạm thời về mặt logic chứ không phải về mặt lý một thiết bị PnP ra khỏi cấu hình phần cứng của một máy tính. Bạn muốn tối ưu hóa thời gian để khôi phục lại thiết bị sau này. Các lựa chọn dưới đây, đâu là lựa chọn tối ưu nhất để bạn hoàn thành mục tiêu nói trên?
    a. Sử dụng ***Device Manager*** để gỡ bỏ thiết bị
    b. Gỡ bỏ vật lý thiết bị phần cứng ra khỏi máy tính
    c. Sử dụng ***Device Manager*** để vô hiệu hóa thiết bị
    d. Di chuyển file chứa trình điều khiển thiết bị tới một thư mục khác trên ổ đĩa cục bộ.
5. Nhà sản xuất card mạng không dây được cài đặt trên máy tính của bạn vừa đưa ra trình điều khiển mới. Bạn muốn thử trình điều

khiển nhằm kiểm tra quá trình hoạt động của nó. Bạn sẽ sử dụng lựa chọn nào trong Device Manager để thử trình điều khiển mới?

6. Bạn muốn hiển thị danh sách các thiết bị được kết nối tới hệ thống Windows Server 2003 của bạn theo IRQ. Bạn sẽ sử dụng các phương pháp nào dưới đây để thực hiện công việc này? (Lựa chọn tất cả các câu trả lời đúng)

   a. Sử dụng ***Device Manager***, từ thực đơn ***View*** lựa chọn ***Resources By Connection***.

   b. Sử dụng ***Device Manager***, từ thực đơn ***View*** lựa chọn ***Resources By Type.***

   c. Sử dụng ***Device Manager***, từ thực đơn ***View*** lựa chọn ***Device By Connection***.

   d. Sử dụng ***Device Manager***, từ thực đơn ***View*** lựa chọn ***Devices By Type.***

7. Gần đây bạn có cài đặt ba card mạng cũ trên một máy chủ thành viên Windows Server 2003. Hai card làm việc tốt nhưng cái thứ ba bị xung đột với các thiết bị khác trên hệ thống của bạn. Bạn phải làm gì để có thể xác định thiết bị nào trên hệ thống đang xung đột với card mạng thứ ba này?

   a. Sử dụng ***Device Manager*** và tìm kiếm thiết bị khác có ký hiệu màu vàng và dấu cảm thán màu đen bên cạnh nó.

   b. Xem nhật ký sự kiện ứng dụng và tìm kiếm bản ghi mô tả thiết bị đang xung đột với card mạng này.

   c. Sử dụng ***Device Manager*** và tìm kiếm thiết bị khác có ký hiệu màu vàng và dấu cảm thán màu đen bên cạnh nó. Trên thực đơn ***Action***, lựa chọn ***Properties***. Trên thẻ ***Resources,*** một danh sách các thiết bị xung đột sẽ hiển thị các tài nguyên xung đột.

d. Chạy ***Hardware Troubleshooting*** Trình hướng dẫn và lựa chọn ***Resolve All Device Conflicts***.

CÁC KỊCH BẢN TÌNH HUỐNG

==========

Kịch bản 11-1: Xử lý các sự cố liên quan đến trình điều khiển video

Bạn vừa hoàn thành cấu hình một trình điều khiển mới cho card màn hình và nhận được thông báo nhắc nhở bạn khởi động lại máy tính nhằm làm cho những thay đổi có tác dụng. Ngay sau khi bạn khởi động lại máy tính, màn hình xuất hiện một màu đen. Kỹ thuật xử lý sự cố hoặc công cụ nào cho phép bạn phục hồi lỗi về trình điều khiển màn hình này một cách dễ dàng nhất?

a. Last Known Good Configuration

b. Driver Rollback

c. Safe Made

d. Recovery Console

==========

Kịch bản 11-2: Thay đổi các thiết lập tài nguyên phần cứng

Bạn là nhà quản trị hệ thống bán thời gian cho một doanh nghiệp nhỏ. Doanh nghiệp này hiện đang có một máy chủ độc lập chạy Windows Server 2003. Gần đây bạn nhận được một bo mạch fax cũ – đây là một thiết bị cho phép nhận và gửi nhiều bản fax tại cùng một thời điểm. Bạn cài đặt bo mạch này trên máy chủ Windows Server 2003 nhưng nó không làm việc. Bạn mở ***Device Manager*** và thấy rằng biểu tượng của bo mạch fax có một cảnh báo màu vàng với dấu cảm thán màu đen. Bạn phát hiện ra rằng có một sự xung đột về ***IRQ*** với một thiết bị khác trên hệ thống, đó là một bộ điều khiển ***RAID*** cũ. Trong các phương pháp dưới đây, đâu là phương pháp đúng cho phép thay đổi cấu hình bo mạch để không xảy ra xung đột giữa nó với bộ điều khiển ***RAID***?

a. Trên màn hình ***Device Manger,*** lựa chọn bộ điều khiển ***RAID.*** Trên thực đơn ***Action***, lựa chọn ***Properties.*** Lựa chọn thẻ

Resources và kế đó xóa hộp kiểm tra ***Use Automatic Settings.*** Lựa chọn ***IRQ*** và nhấp vào ***Change Settings***. Cuộn màn hình chứa ***IRQ*** cho đến khi bạn nhìn thấy một cái không xung đột với bất kỳ một thiết bị khác. Nhấp ***OK*** và khởi động lại máy chủ.

b. Lựa chọn bản mạch fax trong ***Device Manager***. Trên thực đơn ***Action,*** lựa chọn ***Properties***. Lựa chọn thẻ ***Resources*** và kế đó xóa hộp kiểm tra ***Use Automatic Settings***. Lựa chọn ***IRQ v***à nhấp vào ***Change Settings***. Cuộn màn hình chứa ***IRQ*** cho đến khi bạn nhìn thấy một cái không xung đột với bất kỳ một thiết bị khác. Nhấp ***OK*** và khởi động lại máy chủ.

c. Trên màn hình ***Device Manger***, lựa chọn bộ điều khiển ***RAID***. Trên thực đơn ***Action,*** lựa chọn ***Properties***. Lựa chọn thẻ ***Resources*** và kế đó xóa hộp kiểm tra ***Use Automatic Settings.*** Lựa chọn ***I/O Range*** và nhấp vào ***Change Settings***. Cuộn màn hình ***I/O Range*** cho đến khi bạn nhìn thấy một cái không xung đột với bất kỳ một thiết bị khác. Nhấp ***OK*** và khởi động lại máy chủ.

d. Trên màn hình ***Device Manger***, lựa chọn bộ điều khiển ***RAID.*** Trên thực đơn ***Action,*** lựa chọn ***Properties***. Trong danh sách thả xuống ***Device Usage*** trên thẻ ***General*** lựa chọn ***Do Not Use This Device (Disable).***

CHƯƠNG 12: QUẢN LÝ LƯU TRỮ DỮ LIỆU TRÊN ĐĨA

Nếu có một chân lý về kỹ thuật thông tin thì đó chính là: cho dù ngày hôm nay bạn có bao nhiêu không gian để lưu trữ dữ liệu thì ngày mai không gian đó sẽ trở nên chật hẹp. Chỉ cách đây một thập kỷ, các ổ đĩa cứng hầu hết còn được tính theo đơn vị megabyte. Một ổ đĩa cứng với dung lượng 1GB có kích thước một hộp đựng đôi giày và có giá trị hàng ngàn đôla. Nhiều tổ chức giờ đây đo dung lượng lưu trữ của họ theo đơn vị terabyte và việc quản lý tất cả dữ liệu đó có thể tạo một sức ép khủng khiếp lên hệ thống lưu trữ trên các máy chủ của bạn.

Một số tổ chức lớn đang chuyển hướng sang các mạng lưu trữ (SAN-***Storage Area Network***) với kết nối quang, các dãy đĩa có khả năng chống lỗi nhưng nhìn chung bạn vẫn thấy các máy chủ với lượng lưu trữ lớn và một vấn đề rất quan trọng trong cấu hình khả năng lưu trữ máy chủ đó là cung cấp sự cân bằng tối ưu giữa dung lượng lưu trữ, hiệu năng và khả năng chống lỗi. Microsoft Windows Server 2003 cung cấp các công cụ cho phép bạn mở rộng dung lượng lưu trữ của hệ thống, cung cấp khả năng chống lỗi và nâng cao hiệu năng của hệ thống lưu trữ. Các nhà quản trị hệ thống sẽ cần phải hiểu một cách tường tận về các công cụ này nhằm đảm bảo cho các ổ đĩa cứng hoạt động trơn tru và tránh được tình trạng cạn kiệt không gian lưu trữ.

Hoàn thành chương này bạn có khả năng:

- **Hiểu được các khái niệm và thuật ngữ về lưu trữ trên đĩa.**
- **Phân biệt lưu trữ cơ bản với lưu trữ động.**
- **Xác định các loại volume lưu trữ được Windows Server 2003 hỗ trợ.**
- **Xác định mô hình RAID triển khai nhằm thỏa mãn một yêu cầu lưu trữ cụ thể về mặt mức độ sử dụng, khả năng chống lỗi và hiệu năng.**
- **Thêm không gian lưu trữ cho một máy tính sử dụng Windows Server 2003.**
- **Quản lý các đĩa bằng cách sử dụng Check Disk, Disk Defragmenter và hạn ngạch đĩa.**

TỔNG QUAN VỀ LƯU TRỮ DỮ LIỆU TRÊN ĐĨA TRONG WINDOWS SERVER 2003

Trước khi bạn có thể hiểu một cách đầy đủ về khả năng lưu trữ dữ liệu trên đĩa cứng của hệ điều hành Windows Server 2003, bạn cần nắm được một vài khái niệm cơ bản. Các phần dưới đây sẽ điểm qua một vài phương pháp đặt tên mà Windows Server 2003 sử dụng khi đề cập đến vấn đề lưu trữ dữ liệu trên đĩa và các cấu trúc cơ bản bạn có thể sử dụng để tạo ra một chính sách lưu trữ dữ liệu.

Mặc dù ban đầu sự khác biệt có vẻ như là rõ ràng nhưng khi làm việc với hệ thống lưu trữ trong Windows Server 2003 thì việc duy trì khả năng nhận biết sự khác biệt giữa các thiết bị lưu trữ vật lý với những phân vùng logic mà bạn có thể tạo ra trên chúng (thiết bị vật lý) là một điều hết sức quan trọng. Một ổ đĩa vật lý, đúng như tên gọi của nó là một đơn vị đĩa đơn, độc lập và thường là một ổ đĩa cứng. Về mặt kỹ thuật, khái niệm ***disk*** đề cập tới các đĩa có hình dạng tròn được tráng từ trường bên trong một ổ đĩa. Một ổ đĩa có thể có một đĩa đơn hoặc có thể là một chồng các đĩa, tất cả chúng được xem như đĩa cứng bên trong ổ đĩa.

Để lưu trữ dữ liệu trên một đĩa vật lý, trước hết bạn phải phân vùng cho nó. Cấu hình đơn giản nhất có thể có đó là một đĩa vật lý có một phân vùng đơn được hiển thị trong hệ điều hành bởi một ký tự ổ đĩa. Tuy nhiên bạn cũng có thể tạo được nhiều phân vùng trên một một đĩa vật lý đơn. Một phân vùng là một không gian đĩa có chức năng như một thành phần lưu trữ dữ liệu vật lý riêng biệt. Khi một đĩa vật lý có nhiều hơn một phân vùng, mỗi phân vùng có thể được hiển thị bởi các ký tự ổ đĩa khác nhau trên hệ điều hành.

> ***CHÚ Ý Các ký tự ổ đĩa và các đĩa vật lý*** *Trong thực tế có thể bạn nhìn thấy nhiều ký tự ổ đĩa trên hệ điều hành thì điều đó không có nghĩa là có nhiều ổ đĩa trên máy tính. Một vài ứng dụng khuyến cáo rằng cấu trúc dữ liệu xác định nên lưu trữ trên các đĩa tách rời nhằm mang lại hiệu quả cao nhất cho các hoạt động lưu trữ của ứng dụng. Ví dụ,* ***Active Directory Installation Wizard*** *khuyến cáo rằng cơ sở dữ liệu của Active Directory và các file nhật ký nên được lưu trữ trên các đĩa tách rời. Tuy nhiên việc xác định các ký tự ổ đĩa khác nhau cho các cấu trúc dữ liệu này là không đồng nghĩa với việc chúng được lưu trữ trên các đĩa vật lý khác nhau. Bạn phải nắm rõ về cấu trúc thực tế của đĩa vật lý để biết xem thực tế các ký tự ổ đĩa nào trỏ đến các đĩa vật lý khác nhau.*

Không giống như các đĩa (***Disk***) và các phân vùng (***Partition***), luôn được đặt tại gốc trong cấu hình vật lý của phân hệ thống lưu trữ, ***volume*** (đôi khi còn gọi là một ổ đĩa logic) là một đơn vị lưu trữ logic mà bạn có thể tạo ra và quản lý chúng nhờ các công cụ lưu trữ trong Windows Server 2003. Một ***volume*** có thể chứa tất cả hoặc một phần của một hoặc của nhiều các phân vùng đĩa vật lý. Ở đây một lần nữa, cấu hình đơn giản nhất có thể là một cấu hình mà một ***volume*** đơn chứa toàn bộ một phân vùng, phân vùng này lại bao gồm toàn bộ một đĩa vật lý.

Tuy nhiên, bạn cũng có thể tạo ra nhiều ***volume*** từ một phân vùng đơn hoặc một ***volume*** từ nhiều phân vùng. Có nhiều lý do để sử dụng cả hai phương thức nói trên để quản lý đĩa. Việc tạo ra nhiều ***volume*** từ một phân vùng đơn cho phép bạn tách riêng một cách logic các loại dữ liệu khác nhau. Ví dụ, bạn có thể sử dụng một ***volume*** để cài đặt các ứng dụng và cái khác để lưu trữ các file dữ liệu. Nó làm đơn giản hoá quá trình điều khiển truy cập cho người quản trị và ngăn không cho các loại dữ liệu bị trộn lẫn với nhau. Việc phối hợp các phân vùng từ nhiều đĩa vật lý vào trong một ***volume*** cho phép bạn hợp nhất tất cả các không gian đĩa vào trong một tổ hợp đĩa được hiển thị bởi một ký tự ổ đĩa. Kỹ thuật này cũng cho phép bạn thực hiện các kỹ thuật lưu trữ cao cấp nhằm nâng cao hiệu năng và cung cấp thêm khả năng chống lỗi như ***disk mirroring*** (*ánh xạ đĩa*), ***disk striping (****ghi đĩa theo từng dọc)* và ***redundant array of independent disks*** (RAID_ *dãy các đĩa độc lập có khả năng chống lỗi*) chẳng hạn.

> **CHÚ Ý:** ***Các volume và các ký tự ổ đĩa*** *Trong hầu hết các trường hợp, một* ***volume*** *được hiển thị bởi một ký tự ổ đĩa, thậm chí khi* ***volume*** *bao gồm nhiều phân vùng trên các đĩa vật lý khác nhau. Tuy nhiên, một* ***volume*** *không nhất thiết phải có một ký tự ổ đĩa. Bạn có thể gắn một* ***volume*** *như một thư mục trên một* ***volume*** *khác để kết hợp một cách hiệu quả hai* ***volume*** *vào trong một ký tự ổ đĩa logic.*

Số lượng và tính chất của các phân vùng và các **volume** bạn có thể tạo ra từ không gian trên đĩa vật lý phụ thuộc vào kiểu lưu trữ đang sử dụng trên Windows Server 2003: lưu trữ cơ bản hay lưu trữ động. Các loại hình lưu trữ này sẽ được nêu chi tiết trong các phần dưới đây.

> ***LƯU Ý Sự nhầm lẫn thuật ngữ*** *Nếu bạn có khó khăn trong việc phân biệt giữa các đĩa vật lý, các phân vùng và các* ***volume*** *thì bạn cũng đừng quá lo lắng. Nhiều tài liệu tham khảo và thậm chí là một số tài liệu của Microsoft cũng sử dụng sai các khái niệm này. Tuy nhiên khi bạn tìm hiểu về các khả năng của các hệ thống lưu trữ*

động và cơ bản trên Windows Server 2003 thì sự khác biệt giữa các khái niệm lưu trữ này sẽ trở nên rõ ràng hơn.

Sử dụng cơ chế lưu trữ cơ bản

Lưu trữ cơ bản là chuẩn công nghiệp cho công việc quản lý đĩa cứng và là chế độ lưu trữ mặc định trong Windows Server 2003. Tất cả các phiên bản của Windows cũng như MS-DOS, đều hỗ trợ lưu trữ cơ bản và có thể truy nhập tới các đĩa cơ bản (***Basic Disk***). Trong Windows Server 2003, tất cả các đĩa là đĩa cơ bản cho tới khi bạn chuyển đổi chúng thành đĩa động (***Dynamic Disk***).

Trong chế độ lưu trữ cơ bản, một đĩa vật lý được chia thành các phân vùng và mỗi phân vùng hoạt động như một đơn vị lưu trữ vật lý riêng biệt. Thông tin về vị trí và kích thước của mỗi phân vùng được lưu lại trong bảng phân vùng của ***Master Boot Record*** (MBR) trên đĩa. Để tạo nhiều ***volume*** trên một đĩa vật lý duy nhất, bạn phải tạo ra nhiều phân vùng. Windows Server 2003 hỗ trợ tối đa 4 phân vùng trên một đĩa cơ bản và có hai kiểu phân vùng:

- **Phân vùng chính** (***Primary Partition***) Một đĩa cơ bản có thể có tối đa 04 phân vùng chính với mỗi phân vùng hoạt động như một ***volume*** riêng biệt. Một trong các phân vùng này có thể được chỉ định làm phân vùng khởi động (***Boot Partition***). Máy tính sẽ tìm kiếm trên phân vùng khởi động các file khởi động cần thiết để nạp hệ điều hành. Sau khi tạo ra một phân vùng chính, bạn phải định dạng nó với một kiểu hệ thống tập tin trước khi lưu trữ dữ liệu lên đó.
- **Phân vùng mở rộng** Một đĩa cơ bản có thể có một phân vùng mở rộng sử dụng không gian còn lại sau tiến trình tạo các phân vùng chính. Do một đĩa cơ bản chỉ có tối đa 04 phân vùng nên khi đã có một phân vùng mở rộng thì số phân vùng chính tối đa là 3. Để sử dụng không gian trên một phân vùng mở rộng, bạn phải tạo ra một hoặc nhiều ổ đĩa logic trên phân vùng đó trước, kế đó định dạng chúng một cách riêng rẽ. Bạn có thể tạo ra một số lượng các ổ đĩa logic tùy ý trên không gian phân vùng mở rộng.

  CHÚ Ý Sử dụng các phân vùng mở rộng *Trong các phiên bản trước của hệ điều hành Microsoft gồm có Windows 95, Windows 98 và MS-DOS , một đĩa vật lý chỉ có thể có một phân vùng chính. Nếu bạn muốn tạo nhiều* ***volume*** *trên một đĩa vật lý duy nhất thì bạn phải tạo một phân vùng mở rộng và chia nó thành một hoặc nhiều ổ đĩa*

logic. Bởi vì Windows NT, Windows 2000, Windows XP và Windows Server 2003 đều hỗ trợ việc sử dụng nhiều phân vùng chính nên lý do duy nhất để giải thích việc tạo một phân vùng mở rộng đó là nếu bạn muốn có nhiều hơn 4 volume logic trên một đĩa cơ bản.

CHÚ Ý Các đĩa cơ bản và thiết bị lưu trữ gắn ngoài *Các thiết bị lưu trữ gắn ngoài chỉ có thể chứa các phân vùng chính. Bạn không thể tạo ra các phân vùng mở rộng hoặc các ổ đĩa logic trên chúng. Bạn cũng không thể có một phân vùng được kích hoạt (**Active Partition**) trên đó. Tuy nhiên, cần lưu ý rằng, các ổ cứng gắn ngoài sử dụng kết nối USB2.0 hoặc IEEE 1394 sẽ không được xem như là các đĩa gắn ngoài.*

Sử dụng cơ chế lưu trữ động (*Dynamic Storage*)

Ngoài cơ chế lưu trữ cơ bản, Windows 2000, Windows XP và Windows Server 2003 còn hỗ trợ cơ chế lưu trữ động. Trong lưu trữ động, các phân vùng và ổ đĩa logic được gộp lại thành các volume và chúng được sử dụng một các linh động hơn. Tất cả các đĩa động đều chỉ chứa một phân vùng chứa không gian lưu trữ có thể sử dụng của nó. Các đơn vị lưu trữ riêng trên phân vùng được gọi là các ***volume***.

Với các đĩa cơ bản, phân vùng đơn trên một đĩa động được xác định bởi thông tin lưu trữ trên MBR của đĩa. Tuy nhiên, thông tin về ***volume*** không được lưu trên bảng phân vùng của đĩa mà được lưu trong một cơ sở dữ liệu được điều kiển bởi dịch vụ ***Logical Disk Manager*** (LDM – *Trình Quản lý Đĩa Logic*) của hệ điều hành. Do cơ sở dữ liệu của ***volume*** không bị hạn chế bởi kích thước và cấu trúc MBR của đĩa nên bạn có thể tạo ra một số các ***volume*** không hạn chế trên một đĩa động. Các ***volume*** có khả năng linh hoạt hơn so với các phân vùng. Các đĩa động hỗ trợ các kiểu ***volume*** sau:

- **Simple volume (***Ổ đĩa logic đơn giản***)** Hoạt động như một phân vùng chính trên đĩa cơ bản. **Simple volume** sử dụng không gian trên một đĩa vật lý và tương ứng với một ***volume logic***. Khi một máy tính chỉ có một đĩa động, tất cả các ***volume*** phải là các ***simple volume***. Sau khi tạo ra một ***simple volume*** với kích thước xác định, bạn có thể mở rộng nó bằng việc gắn thêm các không gian chưa sử dùng từ các vùng khác trên cùng một đĩa mà không cần phải xoá nội dung trên ***volume*** này. Do ***simple volume*** chỉ tồn tại trên một đĩa vật lý nên chúng không cung cấp khả năng chống lỗi.
- **Span volume (***Ổ đĩa logic mở rộng***)** Một **span volume** bao gồm các không gian lưu trữ trên nhiều đĩa cứng vật lý. Bạn có thể tạo

một ***span volume*** sử dụng không gian lưu trữ lên tới 32 đĩa vật lý và các kích thước sử dụng trên mỗi đĩa có thể khác nhau. Khi hệ thống thực hiện ghi dữ liệu lên một ***span volume***, nó sẽ bắt đầu bằng cách ghi đầy một đĩa vật lý rồi khi tiếp lên lần lượt các đĩa tiếp theo. Do đó mà ***span volume*** không đem lại khả năng chống lỗi . Bạn có thể mở rộng một ***span volume*** mà không làm mất dữ liệu bằng việc bổ sung không gian từ bất cứ đĩa vật lý nào của hệ thống. Nhược điểm lớn nhất của các ***span volume*** là khả năng mất mát tiềm ẩn của chúng được nhân lên cùng với số các đĩa cứng được sử dụng để cung cấp không gian lưu trữ cho ***volume***. Nếu một đĩa bị hỏng thì cả ***volume*** cũng sẽ mất.

- **Striped Volume (***Ổ đĩa logic ghi theo vạch***)** Một **striped volume** (còn gọi là RAID 0) là sự kết hợp của các vùng không gian trên các đĩa cứng vật lý khác nhau (tối đa 32 đĩa cứng). Tuy nhiên, không giống như ***span volume***, Windows Server 2003 ghi dữ liệu lên tất cả các đĩa vật lý trong ***volume*** (gọi là ***stripe set*** – *Tập các vạch*) với cùng một tốc độ. Hệ thống sẽ thực hiện tiến trình ghi lần lượt các khối (***block***) dữ liệu lên mỗi đĩa vật lý và do có nhiều đầu đọc được sử dụng cùng một lúc nên hiệu suất đọc/ghi tỷ lệ thuận với số lượng đĩa cứng trên ***volume***. Nhưng cũng giống như ***span volume***, nếu một đĩa bị hỏng thì tất cả dữ liệu trên ***volume*** cũng bị mất .

  CHÚ Ý Stripping và hiệu năng *Bạn sẽ không cải thiện được hiệu suất trên một* ***striped volume*** *khi sử dụng các ổ đĩa IDE trừ phi bạn sử dụng các kênh giao tiếp IDE riêng biệt cho mỗi đĩa cứng vật lý. Điều này xảy ra vì hai đĩa sử dụng chung một kênh sẽ không nhận và thực thi các mệnh lệnh một cách đồng thời . Các kênh giao tiếp riêng biệt sẽ cải thiện hiệu suất bằng cách phân phối các yêu cầu I/O giữa các bộ điều khiển cũng như giữa các ổ đĩa. Để đạt hiệu suất cao nhất, bạn nên sử dụng các ổ đĩa SCSI. Các giao tiếp SCSI có thể gửi các câu lệnh tới mọi ổ đĩa trên cùng kênh (****bus****) và các ổ đĩa có thể thực thi chúng một cách đồng thời.*

- **Mirrored volume (***Ổ logic Ánh xạ***)** Một **mirrored volume** (còn gọi là RAID 1) bao gồm hai bản sao y hệt của cùng một ***simple volume*** và mỗi bản sao nằm trên một đĩa vật lý riêng biệt . Tất cả dữ liệu lưu trữ trên ***volume*** được ghi lên cả hai đĩa một cách đồng thời. Các ***mirrored volume*** cung cấp khả năng chống lỗi cho bạn: nếu một đĩa vật lý bị hỏng thì đĩa còn lại vẫn hoạt động như

thường. Nhược điểm của phương pháp này là dung lượng của ***volume*** chỉ bằng một nửa không gian lưu trữ của đĩa vật lý .

- **RAID-5 volume** RAID-5 là kỹ thuật lưu trữ dữ liệu cung cấp khả năng chống lỗi ở đó dữ liệu được ghi lên các đĩa cứng vật lý khác nhau và được xem như một ***volume*** duy nhất. Cũng tương tự như ***striped volume***, trên RAID-5 ***volume*** hệ thống sẽ thực hiện ghi dữ liệu lên tất cả các đĩa cứng vật lý với cùng một tốc độ nhưng kèm theo đó có dữ liệu kiểm tra gọi là chẵn lẻ (***Parity***). Mặc dù dữ liệu chẵn lẻ được phân phối cho tất các đĩa trong dãy đĩa nhưng tổng dung lượng sử dụng cho dữ liệu này không lớn hơn dung lượng của một đĩa. Nếu một đĩa trong ***volume*** bị hỏng, các đĩa còn lại sẽ tái tạo dữ liệu bị mất bằng việc sử dụng dữ liệu chẵn lẻ. Quá trình tính toán sử dụng bit chẵn lẻ trong tiến trình ghi dữ liệu sẽ tạo nên một tải thêm vào lên bộ vi xử lý của hệ thống. Tuy nhiên, RAID-5 lại gia tăng hiệu suất đọc vì dữ liệu được đọc đồng thời từ nhiều đầu đọc .

  CHÚ Ý Các hạn chế của volume hệ thống *Do tính chất quan trọng của* ***volume*** *hệ thống đối với sự hoạt động của hệ thống nên Windows Server 2003 đưa ra những giới hạn đặc biệt đối với* ***volume*** *này. Bạn không thể cài đặt hệ điều hành trên một* ***span, stripe*** *hay* ***RAID-5 volume*** *và cũng không thể mở rộng* ***volume*** *hệ thống sau khi cài đặt. Tuy nhiên bạn vẫn có thể triển khai* ***mirror volume*** *trên* ***volume*** *hệ thống.*

So sánh các đĩa cơ bản với các đĩa động

Câu hỏi đặt ra là bạn nên sử dụng cơ chế lưu trữ cơ bản hay động trên máy tính Windows Server 2003 đòi hỏi sự cân nhắc cẩn thận. Như đã nhắc đến ở trên, mặc định ban đầu tất cả các đĩa Windows Server 2003 đều là đĩa cơ bản cho tới khi bạn cần chuyển đổi chúng thành các đĩa động. Quá trình chuyển đổi giữa đĩa cơ bản và đĩa động rất đơn giản, nhanh chóng và có thể thực hiện được tại bất kỳ thời điểm nào mà không lo sợ mất dữ liệu. Tuy nhiên, việc chuyển đổi một đĩa động thành một đĩa cơ bản lại khó hơn rất nhiều vì tất cả dữ liệu trên đĩa của bạn sẽ bị mất và phải phục hồi chúng từ một bản sao lưu. Do đó bạn cần phải đảm bảo rằng bạn thực sự cần cơ chế lưu trữ động trước khi thực hiện sự chuyển đổi.

Các đĩa động cho phép bạn thực hiện việc chuyển đổi chúng giữa các máy chủ một cách dễ dàng (ngoại trừ các đĩa hệ thống). Tính năng này cho phép bạn di chuyển một đĩa từ máy chủ lỗi sang một máy chủ hoạt động với thời

gian gián đoạn là nhỏ nhất. Mỗi một máy tính Window 20000, Windows XP, Windows Server 2003 có thể hỗ trợ một nhóm đĩa mà bản thân nó có thể bao gồm nhiều đĩa động. Cơ sở dữ liệu LDM được nhân bản giữa các đĩa trong cùng một nhóm làm tăng khả năng phục hồi thông tin cấu hình cho tất cả các đĩa trong nhóm. Tuy nhiên, nếu máy tính của bạn chỉ có một ổ cứng duy nhất thì lưu trữ động sẽ không đem lại bất cứ ưu điểm nào rõ rệt ngoại trừ bạn cần hơn 4 phân vùng trên đĩa cứng đó. Chỉ khi nào bạn có từ 2 ổ đĩa cứng động trở lên thì bạn mới có thể tận dụng những lợi ích của các kiểu ***volume*** như ***span*** hay ***stripe***.

Mặc dù đĩa động với nhiều ưu điểm của nó nhưng bạn vẫn có lý do để sử dụng đĩa cơ bản chẳng hạn như:

- Do cách thức hoạt động của cơ sở dữ liệu LDM nên bạn sẽ rất khó khăn khi chuyển một đĩa động được sử dụng để khởi động hệ điều hành sang một máy tính khác khi hệ thống gốc bị lỗi.
- Đĩa động không hỗ trợ cho các thiết bị ngoại vi và cũng không hỗ trợ trên máy tính xách tay.
- Lưu trữ cơ bản là chuẩn công nghiệp vì vậy các ổ đĩa loại này có thể truy cập được bởi các hệ điều hành khác nhau bao gồm MS-DOS, tất cả các phiên bản Windows và hầu hết các hệ điều hành khác. Do đó bạn sẽ không thể truy nhập được tới các đĩa động nếu bạn khởi động hệ thống từ một hệ điều hành không phải là Windows Server 2003, Windows XP hay Windows 2000.

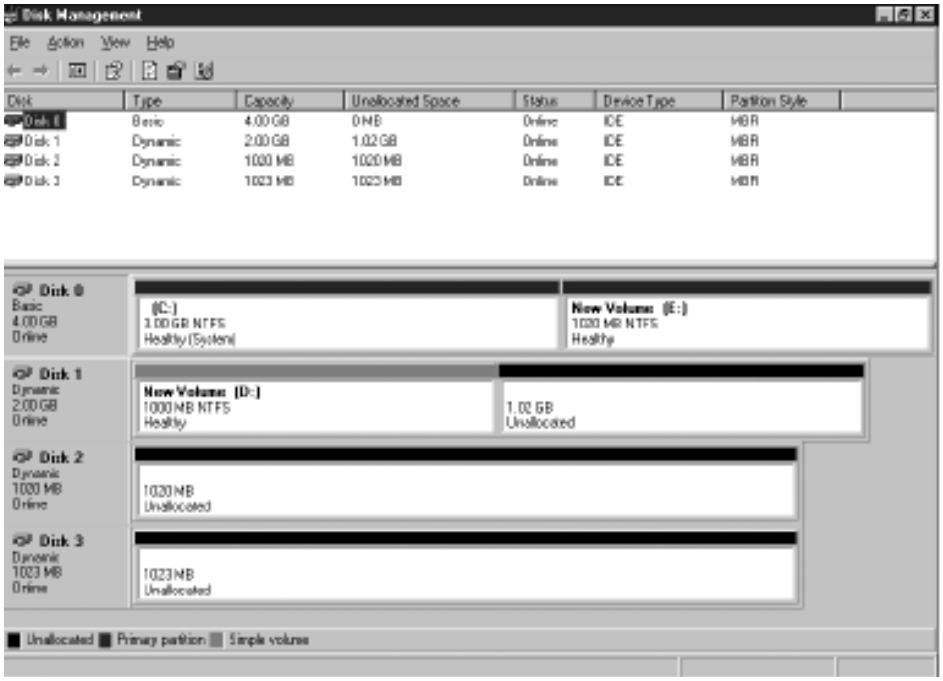
CHÚ Ý Mục tiêu của kỳ thi *Các mục tiêu cho kỳ thi 70-290 yêu cầu các học viên có khả năng "quản trị các đĩa cơ bản và đĩa động".*

SỬ DỤNG CÔNG CỤ QUẢN TRỊ ĐĨA (DISK MANAGEMENT)

Disk Management là công cụ chính trên Windows Server 2003 dùng để tạo, quản trị các đĩa cơ bản và đĩa động. ***Disk Management*** là một phần trong màn hình quản trị ***Computer Management*** – đây là màn hình mà bạn có thể truy cập từ ***Administrative Tools*** trên thanh công cụ ***Start*** hoặc bạn có thể thêm snap-in này từ một màn hình MMC tùy biến.

LỜI KHUYÊN Sử dụng màn hình quản trị Disk Management *Windows Server 2003 cũng cung cấp một màn hình quản trị* ***Disk Management*** *độc lập nhưng không có* ***shortcut*** *cho nó từ thanh công cụ* ***Start.*** *Để mở màn hình quản trị này nhấp* ***Start****, lựa chọn* ***Run*** *và gõ* ***diskmgmt.msc*** *trên hộp thoại* ***Open*** *và nhấp* ***OK****.*

Giao diện ***Disk Management*** khác với hầu hết các MMC snap-in khác. Nó không có một cửa sổ quản trị tập trung, tất cả các điều khiển đều được đặt trong cửa sổ chi tiết. Bản thân cửa sổ chi tiết này được chia thành hai cửa sổ: cửa sổ phía trên và cửa sổ bên dưới như hình vẽ 12-1. Mặc định, cửa sổ phía trên chứa một danh sách các volume hiển thị các volume trên tất cả các đĩa cứng vật lý. Danh sách này chỉ hiển thị các ***volume*** đối với các đĩa động còn với đĩa cơ bản cửa sổ này chứa một danh sách các phân vùng chính và các ổ đĩa logic.



Hình 12-1: Màn hình quản trị Disk Management

Mỗi bản ghi trong danh sách ***volume*** chứa thông tin sau:

- **Volume** Xác định ký tự ổ đĩa và/hoặc tên ***volume***
- **Layout** Xác định kiểu ***volume*** như ***simple, spanned*** hoặc ***striped*** đối với các ***volume*** trên đĩa động hoặc phân vùng đối với các đĩa logic trên đĩa cơ bản.
- **Type** Xác định loại đĩa cứng mà ***volume*** được tạo ra ở trên đó: cơ bản hoặc động.
- **File System** Xác định kiểu hệ thống file mà ***volume*** sử dụng
- **Status** Xác định trạng thái hiện tại của ***volume*** bằng việc sử dụng một trong các giá trị sau:
- **Failed** (*hỏng*)– xác nhận rằng ***volume*** không thể khởi động được

- **Failed Redundancy** (*dư phòng hỏng*)– xác nhận rằng một ***mirrored volume*** hoặc ***RAID-5 volume*** không có khả năng chống lỗi do có một đĩa bị lỗi.
- **Formatting** (*đang đinh dạng*)– xác nhận rằng ***volume*** này đang trong tiến trình định dạng.
- **Healthy (***Khỏe mạnh***)** – xác nhận rằng ***volume*** hoạt động bình thường.
- **Regenerating** (*Tái tạo lại*)– xác nhận rằng một ***RAID-5 volume*** đang ở trong tiến trình tạo lại dữ liệu trên một đĩa phục hồi mới.
- **Resynching** (*Đang đồng bộ lại*)– xác nhận rằng một ***mirrored volume*** đang ở trong tiến trình tạo lại dữ liệu trên một đĩa phục hồi mới.
- **Unknown** (*không biết*)– xác nhận rằng sector khởi động (***Boot sector***) của ***volume*** bị hỏng.
- **Capacity** Xác định dung lượng tổng cộng của ***volume*** theo đơn vị MB hoặc GB.
- **Free Space** Xác định dung lượng của không gian trống trên ***volume*** theo đơn vị MB hoặc GB.
- **%Free** Xác định phần trăm dung lượng của ***volume*** còn trống.
- **Fault Tolerance** Xác định xem kiểu ***volume*** có cung cấp khả năng chống lỗi không.
- **Overhead** Xác định phần trăm dung lượng ***volume*** dành cho việc lưu trữ dữ liệu dự phòng.

Cửa sổ bên dưới của màn hình quản trị ***Disk Management*** chứa một màn hình hiển thị dạng đồ họa các đĩa vật lý trên máy tính. Với mỗi đĩa, màn hình hiển thị xác định thông tin sau:

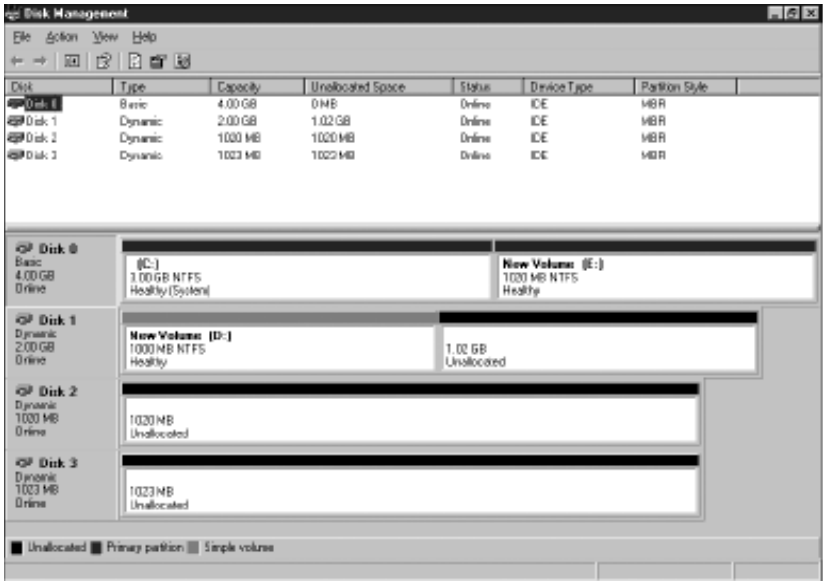
- **Disk Identifier** (*mã nhận diện đĩa*) xác định số hiệu mà hệ thống gán cho đĩa. Mã nhận diện đĩa cứng được bắt đầu với Disk0 và các ổ đĩa CD-ROM với CD-ROM 0.
- **Disk Type** (*chủng loại đĩa*) xác định xem đĩa là một đĩa cơ bản hay đĩa động, là CD-ROM hay DVD-ROM.
- **Disk Size** (*dung lượng đĩa cứng*) xác định dung lượng tổng cộng của đĩa.

- **Disk Status** (*trạng thái của đĩa*) Xác định trạng thái hiện tại của đĩa bằng cách sử dụng một trong các giá trị sau:
- **Audio CD** – xác nhận rằng một ổ đĩa CD-ROM hoặc DVD-ROM có chứa một đĩa audio CD.
- **Foreign** – xác nhận rằng có một đĩa động được di chuyển từ một máy tính khác nhưng chưa được đưa vào cấu hình của hệ thống hiện tại. Chạy lệnh ***Import Foreign Disks*** để truy cập đến đĩa.
- **Initializing** – xác nhận rằng đĩa đang trong tiến trình chuyển đổi từ một đĩa cơ bản thành một đĩa động.
- **Missing** – xác nhận rằng một đĩa động đã bị loại bỏ ra khỏi máy tính hoặc bị đứt kết nối hoặc bị hỏng hóc. Sử dụng câu lệnh ***Reactive Disk*** để truy cập vào đĩa bị ngắt kết nối trước kia.
- **No Media** – xác nhận rằng một ổ đĩa CD-ROM, DVD-ROM hoặc một ổ đĩa di động hiện tại đang trống.
- **Not Initialized** – xác nhận rằng đĩa không có một chữ ký số hợp lệ. Sử dụng ***Initialize Disk*** để kích hoạt đĩa.
- **Online** – xác nhận đĩa có khả năng truy cập và hoạt động bình thường.
- **Online (Errors)** – xác nhận rằng đã phát hiện thấy các lỗi I/O trên khu vực của đĩa động.
- **Offline** – xác nhận rằng không thể truy cập được đến đĩa động.
- **Unreadable** – xác nhận rằng đĩa không thể truy cập, nguyên nhân có thể do lỗi phần cứng, lỗi I/O hoặc cơ sở dữ liệu LDM bị hỏng.

Các thanh (***bar***) được hiển thị theo chiều ngang biểu diễn mỗi đĩa được chia thành các phân đoạn mô tả các ***volume*** hoặc các phân vùng khác nhau trên đĩa cứng đó. Mỗi phân đoạn được đặc trưng bởi các màu khác nhau để bạn có thể dễ dàng xác định chúng là một ***volume*** cơ bản hay là một ***volume*** động hoặc có thể là không gian chưa được sử dụng. Các phân đoạn cũng chứa các thông tin mà bạn nhìn thấy trong danh sách ***volume*** như tên ***volume***, dung lượng, hệ thống file và trạng thái hiện tại.

Disk Management cho phép bạn tùy biến những gì sẽ xuất hiện trong các cửa sổ trên và dưới bằng việc sử dụng các câu lệnh trong thực đơn ***View***. Bạn có thể đảo ngược danh sách ***volume*** và màn hình hiển thị đồ họa hoặc bạn có thể thay thế bằng một danh sách đĩa như hình vẽ 12-2. Danh sách đĩa cũng có các thông tin như trên màn hình đồ họa ngoài ra còn có ***Device Type***

(chủng loại thiết bị) như IDE hay SCSI chẳng hạn và ***Partition Style*** (kiểu phân vùng) như MBR hoặc GPT (***GUID Partition Table*** – đây là một bảng phân vùng có giao diện đồ họa, được sử dụng cho các máy tính chạy trên nền bộ vi xử lý Itanium của hãng Intel).



Hình 12-2: Màn hình Disk Management hiển thị danh sách đĩa

Disk Management cho phép bạn quản lý cục bộ hoặc từ xa khả năng lưu trữ của một hệ thống. Nó không tương tác trực tiếp với cấu hình đĩa mà làm việc với dịch vụ quản trị ***Logical Disk Manager***, một dịch vụ được khởi động trên máy tính bạn quản lý khi khởi tạo màn hình quản trị ***Disk Management***.

Khi bạn lựa chọn một trong các thành phần trên giao diện ***Disk Management***, bạn có thể truy cập đến một loạt các chức năng từ thực đơn ***Action*** và từ thực đơn ngữ cảnh của các thành phần đó. Các chức năng cụ thể giúp bạn xác định xem bạn đang lựa chọn một đĩa hay một phân vùng trên một đĩa cơ bản hay một volume trên một đĩa động. Với mỗi thành phần, bạn cũng có thể mở hộp thoại ***Properties*** để truy cập đến các chức năng ngoại vi. Các chức năng mà bạn có thể thực hiện sẽ được mô tả trong các phần dưới.

> ***CHÚ Ý Sử dụng Diskpart.exe*** *Tất cả các công việc bạn thực hiện trên màn hình quản trị* ***Disk Management*** *đều có thể thực hiện được với công cụ* ***Diskpart.exe*** *ở chế độ dòng lệnh. Đây là một chương trình mà bạn có thể sử dụng trực tiếp hoặc trong các kịch bản nhằm tự động hóa các công việc quản trị đĩa. Để biết thêm thông tin về việc sử dụng công cụ này, bạn có thể tham khảo trong phần* ***help*** *trực tuyến trong Windows Server 2003.*

➢ **Tăng khả năng lưu trữ**

Tiến trình tăng thêm khả năng lưu trữ cho một máy tính Windows Server 2003 bao gồm các bước sau:

- Cài đặt về mặt vật lý các đĩa
- Khởi tạo đĩa
- Trên đĩa cơ bản, tạo các phân vùng và (nếu là một phân vùng mở rộng) các ổ đĩa logic hoặc tạo các ***volume*** trên một đĩa động.
- Định dạng các ***volume.***
- Gán các ký tự ổ đĩa cho các ***volume*** hoặc gắn các ***volume*** đến các thư mục rỗng trên các ***volume*** NTFS sẵn có.

Bạn phải là thành viên nhóm ***Administrators*** hoặc ***Backup Operators*** hoặc bạn được ủy nhiệm quyền quản trị, bạn mới có thể thực hiện hầu hết các nhiệm vụ này. Chỉ duy nhất có các thành viên nhóm ***Administrators*** mới định dạng được một ***volume***.

Các bước này được mô tả chi tiết trong các phần kế tiếp. Hầu hết các bước mà bạn thực hiện trên các volume hoặc đĩa sẵn có cũng như các trên các cấu trúc mới.

Cài đặt đĩa cứng

Để thêm đĩa cứng mới vào máy tính, trước hết bạn phải cài đặt nó. Kế đó, mở màn hình quản trị ***Disk Management*** và nếu hệ thống không tự động phát hiện đĩa cứng, chọn ***Rescan Disks*** từ thực đơn ***Action***. Nếu hệ thống yêu cầu bạn khởi động máy tính để hoàn thành tiến trình cài đặt đĩa mới, bạn hãy thực hiện và mở ***Disk Management*** lại một lần nữa.

Khởi tạo đĩa cứng

Khi bạn thêm đĩa cứng vào máy tính Windows Server 2003, bạn phải khởi tạo đĩa trước khi bắt tay vào việc định vị không gian cho các phân vùng, các ổ đĩa logic và các ***volume***. Khởi tạo đĩa cho phép hệ điều hành ghi chữ ký đĩa, dấu kết thúc sector (còn được gọi là từ ký) và một MBR hoặc GPT lên đĩa cứng đó.

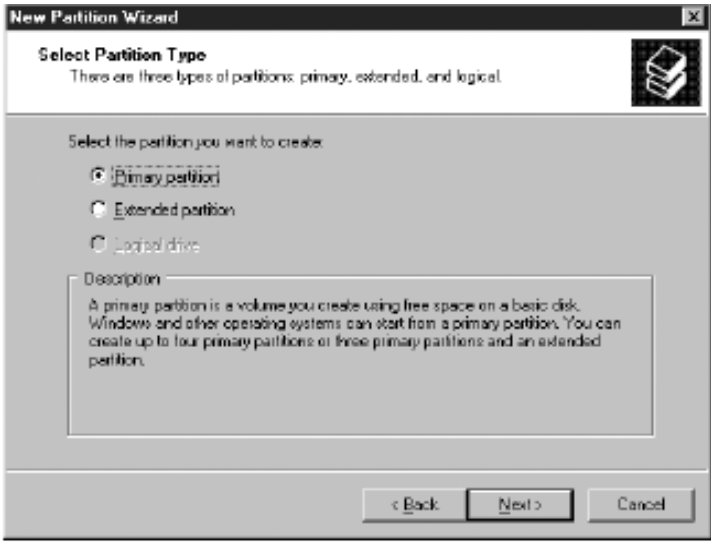
Nếu bạn khởi tạo ***Disk Management*** sau khi cài đặt đĩa mới, Trình hướng dẫn ***Initialize And Convert Disk*** sẽ tự động xuất hiện. Trình hướng dẫn cho

phép bạn tạo chữ ký trên đĩa mới và chuyển đổi đĩa từ cơ chế lưu trữ cơ bản mặc định sang cơ chế lưu trữ động. Để khởi tạo đĩa một cách thủ công từ ***Disk Management***, nhấp chuột phải vào hộp trạng thái của đĩa trên màn hình đồ họa và từ thực đơn ***Action***, trỏ tới ***All Tasks*** rồi lựa chọn ***Initialize Disk***.

> ***CHÚ Ý Chuyển đổi các đĩa cứng mới*** *Mặc định, Trình hướng dẫn* ***Initialize And Convert Disk*** *sẽ không chuyển đổi các đĩa cứng mới, bạn phải thực hiện điều này một cách thủ công.*

Tạo các phân vùng trên đĩa cơ bản

Sau quá trình khởi tạo đĩa cứng mới, giờ đây bạn có thể bắt đầu thực hiện một cấu trúc lưu trữ của các phân vùng, các ổ đĩa logic hoặc các ***volume***. Như đã đề cập ở trên, mặc định các đĩa mới khởi tạo trong Windows Server 2003 đều là đĩa cơ bản. Nếu bạn muốn giữ nguyên cơ chế lưu trữ này, bạn có thể tạo các phân vùng bằng cách lựa chọn không gian chưa được sử dụng trên màn hình đồ họa và trên thực đơn ***Action***, trỏ tới ***All Tasks*** và chọn ***New Partition.*** Trình hướng dẫn ***New Partition*** sẽ xuất hiện, ở đó bạn sẽ xác định xem bạn muốn tạo một phân vùng chính hay phân vùng mở rộng (xem hình vẽ 12-3) và kích thước của nó.



Hình 12-3: Trình hướng dẫn New Partition

Nếu bạn tạo một phân vùng chính, Trình hướng dẫn sẽ hướng dẫn bạn từ việc gán ký tự ổ đĩa cho phân vùng đến định dạng chúng hoặc bạn có thể lựa chọn để thực hiện các công việc này sau. Nếu tạo một phân vùng mở rộng, bạn phải lựa chọn không gian đĩa cứng trống mà bạn vừa tạo và chạy Trình hướng dẫn ***New Partition*** lại một lần nữa, lần này Trình hướng dẫn sẽ cho

phép bạn tạo ổ đĩa logic. Bạn có thể tạo số lượng ổ đĩa logic tùy theo nhu cầu của bạn cho đến khi bạn sử dụng hết không gian đĩa cứng trên phân vùng mở rộng. Và một lần nữa, Trình hướng dẫn d cho phép bạn định dạng các ổ đĩa logic khi bạn tạo chúng hoặc bạn có thể định dạng chúng sau đó.

> ***THÔNG TIN THÊM*** *Để biết thêm thông tin về việc gán các ký tự ổ đĩa cho các phân vùng và định dạng chúng, xem "Gán các ký tự ổ đĩa" và "Định dạng các volume" ở phần sau trong chương này.*

Chuyển đổi một đĩa cơ bản thành một đĩa động

Nếu bạn muốn sử dụng lưu trữ động, bạn phải chuyển đổi đĩa cơ bản thành đĩa động trước khi bạn tạo các ***volume*** mới. Để thực hiện điều này, lựa chọn hộp trạng thái của đĩa trong màn hình đồ họa, trên thực đơn ***Action*** trỏ tới ***All Tasks*** và lựa chọn ***Convert To Dynamic Disk***. Sau khi tiến trình chuyển đổi hoàn thành, hộp trạng thái của đĩa sẽ hiển thị thông báo đĩa hiện là một đĩa động và và bạn có thể tiến trình tạo các volume.

> ***CHÚ Ý Chuyển đổi đĩa hệ thống*** *Trong hầu hết các trường hợp, bạn có thể bắt đầu sử dụng đĩa động ngay lập tức sau khi bạn hoàn thành quá trình chuyển đổi từ đĩa cơ bản. Tuy nhiên, khi bạn chuyển đổi đĩa hệ thống thành đĩa động, bạn phải khởi động lại hệ thống trước khi bạn có thể thực hiện bất kỳ công việc nào trên đĩa.*

Bạn có thể chuyển đổi một đĩa cơ bản thành đĩa động tại bất kỳ thời điểm nào thậm chí khi bạn đã lưu trữ dữ liệu trên đó. Cấu trúc dữ liệu trên đĩa sẽ không bị thay đổi vì vậy dữ liệu sẽ không bị mất mát. Tuy nhiên, phương pháp tốt nhất trước khi thực hiện bất kỳ một sự thay đổi quan trọng nào trên đĩa đó là sao lưu dữ liệu.

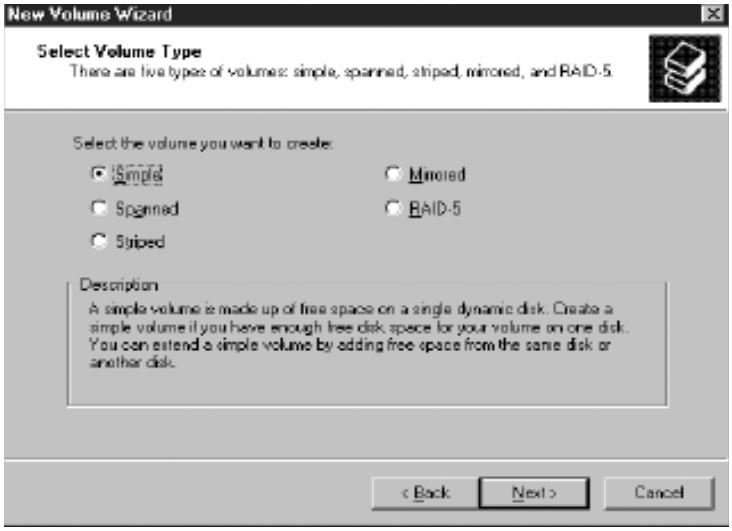
Khi bạn chuyển đổi một đĩa cơ bản đã có các phân vùng và các ổ đĩa logic thành một đĩa động, những thành phần này sẽ được chuyển đổi thành các thành phần tương ứng trên đĩa động. Trong hầu hết các trường hợp, các phân vùng và các ổ đĩa logic trên đĩa cơ bản được chuyển đổi thành các ***simple volume***. Các tập ***volume*** và ***stripe*** trên Windows NT sẽ được chuyển đổi tương ứng thành các ***spanned volume*** và ***striped volume***.

> ***CHÚ Ý Chuyển đổi một đĩa động thành đĩa cơ bản*** *Việc chuyển đổi một đĩa động thành một đĩa cơ bản sẽ làm mất tất cả dữ liệu trên đĩa. Vì vậy, trước tiên bạn phải sao lưu tất cả dữ liệu trên đĩa. Kế đó bạn phải xóa tất cả các* ***volume*** *trên đĩa động. Tiếp theo bạn lựa chọn đĩa và chọn* ***Convert To Basic Disk*** *từ thực đơn* ***Action/All***

***Tasks**. Sau khi tạo các phân vùng cơ bản và các ổ đĩa logic, bạn có thể phục hồi dữ liệu ngược trở lại đĩa.*

Tạo các volume trên đĩa động

Một khi bạn đã chuyển đổi đĩa cứng sang cơ chế lưu trữ động, bạn có thể tiến hành tạo các ***volume*** trên đó. Lựa chọn một vùng không gian chưa sử dụng trên đĩa trong màn hình đồ họa rồi chọn ***New Volume*** từ thực đơn ***Action/All Tasks***. Trình hướng dẫn ***New Volume*** sẽ xuất hiện. Trong Trình hướng dẫn này, bạn phải xác định kiểu ***volume*** bạn muốn tạo trong trang ***Select Volume Type*** như hình vẽ 12-4.



Hình 12-4: Trang Select Volume Type của New Volume Wizard

Các kiểu ***volume*** bạn có thể tạo tùy thuộc vào số lượng đĩa động với không gian chưa sử dụng trên máy tính.

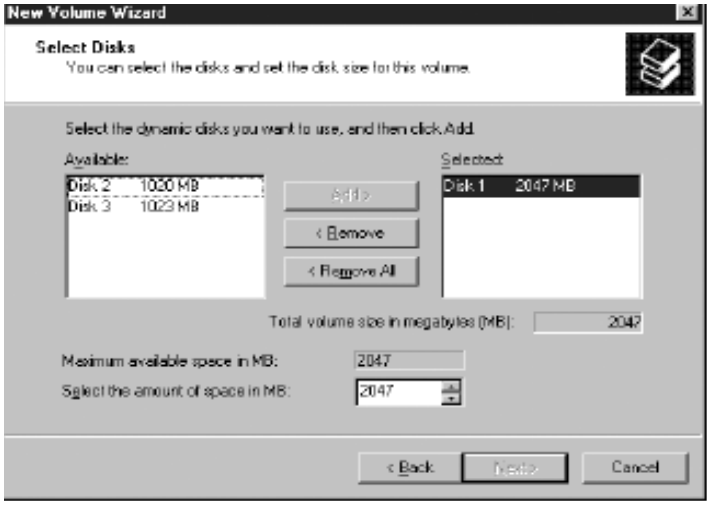
Tạo các simple volume

Nếu bạn chỉ có một đĩa cứng trên máy tính, bạn chỉ có thể tạo được duy nhất các ***simple volume***. Tất cả các công việc bạn cần làm đó là tạo một ***simple volume*** với kích thước xác định. Tiếp theo, Trình hướng dẫn ***New Volume*** sẽ giúp bạn gán ký tự ổ đĩa cho ***volume*** và định dạng nó. Chi tiết quá trình này sẽ được mô tả trong phần sau của chương này.

Tạo các loại volume khác

Để tạo các ***volume spanned, striped*** hoặc ***mirrored***, bạn phải có ít nhất hai đĩa động với các không gian đĩa chưa sử dụng. Để tạo một ***RAID-5 volume*** bạn phải có ít nhất ba đĩa động. Khi bạn lựa chọn bất kỳ loại ***volume*** nào trong số các kiểu trên, Trình hướng dẫn ***New Volume*** sẽ hiển thị trang ***Select***

Disks (xem hình vẽ 12-5), ở đó bạn sẽ lựa chọn các đĩa mà bạn muốn sử dụng để tạo ***volume***.



Hình 12-5: Trang Select Disks của New Volume Wizard

Mặc định, đĩa bạn lựa chọn khi tạo ***volume*** sẽ xuất hiện trong danh sách ***Selected***. Tất cả các đĩa động khác trên máy tính sẽ xuất hiện trong danh sách ***Available***. Để thêm một đĩa vào ***volume***, bạn chọn một đĩa trong danh sách ***Available*** và nhấp ***Add***. Bạn có thể thêm tới 32 đĩa cho các ***spanned***, ***striped*** hoặc ***RAID-5 volume***. Các ***mirrored volume*** chỉ sử dụng duy nhất hai đĩa.

Một khi bạn đã lựa chọn các đĩa để sử dụng cho việc tạo ***volume***, bạn phải xác định kích thước của ***volume***. Tiến trình này cũng thay đổi chút ít tùy thuộc vào kiểu ***volume*** bạn tạo:

- Các ***spanned volume*** có thể sử dụng bất kỳ khoảng không gian nào trên mỗi đĩa cứng. Với mỗi đĩa trong danh sách ***Selected***, bạn xác định dung lượng không gian (tính theo MB) mà bạn muốn đưa vào ***spanned volume***. Trường ***Total Volume Size In Megabytes (MB)*** (*kích thước tổng của volume tính theo đơn vị MB*) sẽ hiển thị không gian kết hợp từ tất cả các đĩa được lựa chọn.
- Các ***stripped, mirrored*** và ***RAID-5 volume*** phải sử dụng cùng một khoảng không gian đĩa trên mỗi đĩa cứng được lựa chọn. Sau khi lựa chọn các đĩa mà bạn muốn sử dụng để tạo ***volume***, hộp kiểm soát ***Select The Amount Of Space in MB*** sẽ xác định dung lượng lớn nhất mà mỗi đĩa có thể đóng góp. Giá trị này được xác định theo khoảng không gian còn trống trên đĩa còn trống ít nhất. Khi bạn thay đổi khoảng không gian trên một đĩa, Trình hướng dẫn cũng thay đổi dung lượng mà các đĩa khác có thể đóng góp.

Kích thước tổng cộng của ***volume*** cũng được tính toán khác nhau tùy thuộc vào kiểu volume khác nhau:

- Với một ***spanned volume***, kích thước tổng của ***volume*** là tổng cộng số MB bạn xác định với mỗi đĩa đã lựa chọn.
- Với một ***stripped volume***, kích thước tổng cộng của volume là số MB bạn xác định nhân với số lượng đĩa bạn lựa chọn.
- Với một ***mirrored volume***, kích thước tổng cộng của ***volume*** là số MB mà bạn xác định. Đó là do mỗi đĩa chứa một phiên bản dữ liệu của đĩa còn lại.
- Với một ***RAID-5 volume***, kích thước tổng cộng của ***volume*** là số MB mà bạn xác định, nhân với số lượng đĩa bạn lựa chọn trừ đi 1. Đó là do ***RAID-5 volume*** sử dụng không gian trên một đĩa để lưu trữ dữ liệu chẵn lẻ.

Sau khi bạn cấu hình các tham số này, Trình hướng dẫn cho phép bạn gán ký tự ổ đĩa cho ***volume*** và định dạng nó. Chi tiết quá trình này sẽ được mô tả trong phần sau của chương này.

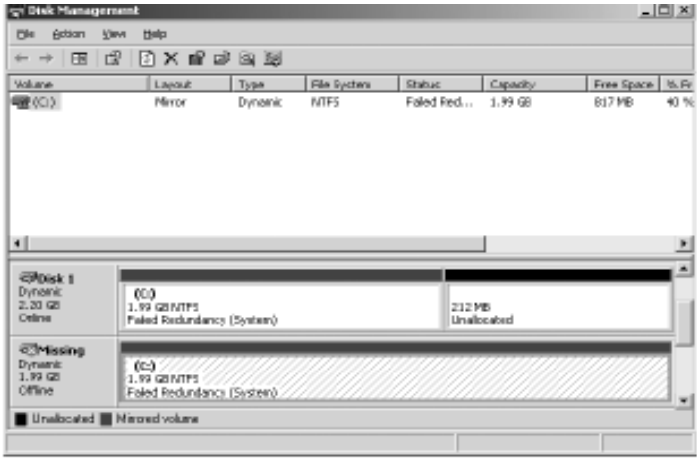
Làm việc với các mirrored volume

Một ***mirrorred volume*** cung cấp hiệu năng cao với khả năng chống lỗi tốt. Hai đĩa tham gia trong một ***mirrorred volume*** và tất cả dữ liệu sẽ được ghi vào cả hai ***volume*** đồng thời. Nhằm đạt được khả năng chống lỗi tốt nhất có thể, bạn sẽ sử dụng các đĩa được kết nối tới các card giao tiếp riêng biệt. Điều này sẽ tạo ra một cấu hình được gọi là **cấu hình kép** nhằm cung cấp hiệu năng tốt hơn và cho phép các ***volume*** vẫn tồn tại trong trường hợp card giao tiếp lỗi cũng như một đĩa lỗi.

Chuyển đổi một simple volume thành một mirrorred volume Ngoài việc tạo một ***mirrorred volume*** mới, bạn cũng có thể chuyển đổi một ***simple volume*** thành một ***mirrorred volume*** bằng cách lựa chọn ***simple volume*** đó, chọn ***Add Mirror*** từ thực đơn ***Action/All Tasks***. Bạn phải có một đĩa động khác trên máy tính với không gian chưa sử dụng đủ để giữ một phiên bản của ***simple volume*** bạn lựa chọn. Một khi bạn đã tạo ***mirrorred volume***, hệ thống bắt đầu chép dữ liệu theo từng cung (***sector***) một tới đĩa mới được thêm vào. Trong suốt thời gian này, trạng thái của ***volume*** sẽ được thông báo là ***Resynching***.

Phục hồi từ đĩa ánh xạ bị lỗi Tiến trình phục hồi một đĩa lỗi trên một ***mirrorred volume*** tùy thuộc vào kiểu lỗi. Nếu một đĩa có lỗi tạm thời về các cổng vào/ra I/O, ***volume*** trên cả hai đĩa sẽ hiển thị trạng thái ***Failed***

Redundancy. Đĩa có lỗi sẽ thông báo trạng thái ***Offline*** hoặc ***Missing*** như hình vẽ 12-6.



Hình 12-6: Một mirrorred volume hiển thị trạng thái Failed Redundancy (*hỏng thông tin dự phòng*)

Sau khi bạn đã sửa lỗi do I/O gây ra – có thể là do cáp kết nối bị hỏng hoặc nguồn điện cung cấp – lựa chọn ***volume*** trên đĩa lỗi và trên thực đơn ***Action*** trỏ tới ***All Tasks*** và lựa chọn ***Reactive Volume***. Hoặc bạn có thể lựa chọn đĩa và lựa chọn ***Reactive Disk***. Tiến trình kích hoạt lại (***reactive***) sẽ làm cho đĩa hoặc ***volume*** quay trở lại trạng thái ***online***. Kế tiếp, hệ thống sẽ tái đồng bộ lại các đĩa.

Nếu bạn muốn dừng ánh xạ, bạn có ba sự lựa chọn tùy thuộc vào bạn muốn kết quả là gì:

- **Xóa volume (Delete the volume)** Nếu bạn xóa ***volume***, ***volume*** và tất cả thông tin chứa trên đó đều bị xóa. Kết quả là một không gian chưa sử dụng sẽ được sử dụng cho các ***volume*** mới.
- **Gỡ bỏ ánh xạ (remove the mirror)** Nếu bạn gỡ bỏ ánh xạ, ***mirrorred volume*** sẽ bị xóa và không gian trên một trong hai đĩa sẽ trở thành chưa được sử dụng. Đĩa còn lại vẫn duy trì một phiên bản dữ liệu nhưng dĩ nhiên dữ liệu này không còn tính năng chống lỗi.
- **Dừng ánh xạ (Break the mirror)** Nếu bạn dừng ánh xạ, ***mirrorred volume*** sẽ bị dừng hoạt động nhưng cả hai đĩa vẫn duy trì hai phiên bản dữ liệu độc lập. Phần ánh xạ mà bạn lựa chọn ***Break Mirror*** sẽ duy trì ký tự ổ đĩa của ***volume*** ánh xạ gốc, các thư mục chia sẻ, file phân trang (***paging***) và các điểm phân tách lại. Đĩa thứ hai sẽ được gán ký tự ổ đĩa kế tiếp còn trống.

Nếu bạn có một ***mirrorred volume*** mà một đĩa vật lý bị lỗi hoàn toàn và cần được thay thế, bạn không thể đơn giản ánh xạ lại ***mirrorred volume*** thậm chí nếu một trong các đĩa trong tập ánh xạ không còn tồn tại nữa. Trước hết, bạn phải gỡ bỏ đĩa lỗi ra khỏi tập ánh xạ để dừng ánh xạ. Lựa chọn ***volume*** và trên thực đơn ***Action*** trỏ tới ***All Tasks*** và lựa chọn ***Remove Mirror***. Trong hộp thoại ***Remove Mirror***, một điều rất quan trọng đó là lựa chọn đĩa bị lỗi. Đĩa bạn lựa chọn sẽ bị xóa khi bạn nhấp vào ***Remove Mirror*** và đĩa còn lại trở thành một ***simple volume***. Một khi tiến trình này hoàn thành, bạn có thể lựa chọn ***simple volume*** và sử dụng câu lệnh ***Add Mirror*** để sử dụng đĩa thay thế nhằm tạo một ***mirror volume*** mới.

> ***LỜI KHUYÊN CHO KÌ THI Khả năng chống lỗi cho các volume hệ thống và volume khởi động*** *Do bạn có thể tạo một* ***mirror volume*** *từ một* ***simple volume*** *sẵn có, nên ánh xạ là kỹ thuật tự nhiên duy nhất trên Windows Server 2003 mà bạn có thể sử dụng nhằm cung cấp khả năng chống lỗi cho các* ***volume*** *hệ thống và khởi động trên máy tính. Bạn không thể sử dụng khả năng* ***RAID-5*** *trên Windows Server 2003 dành cho các* ***volume*** *này bởi vì bạn phải chuyển đổi các đĩa thành lưu trữ động và tạo* ***volume*** *trước khi có bất kỳ dữ liệu nào được ghi lên chúng. Rõ ràng bạn không thể thực hiện điều này khi mà hệ điều hành đã được cài đặt. Tuy nhiên, việc sử dụng RAID cứng cho phép bạn cài đặt hệ điều hành trên một* ***volume RAID-5***.

Làm việc với RAID

Như đã đề cập trong chương trước, RAID là một loạt các kỹ thuật chống lỗi cho phép máy tính hoặc hệ điều hành xử lý các lỗi như một lỗi phần cứng chẳng hạn vì vậy dữ liệu sẽ không bị mất đi và tiến trình hoạt động sẽ không bị ngừng. Bạn có thể thực thi khả năng chống lỗi RAID nhờ giải pháp phần cứng hoặc phần mềm.

Trong giải pháp phần cứng, một card RAID sẽ điều khiển quá trình tạo và phục hồi thông tin dự phòng. Một số nhà sản xuất thực hiện quá trình bảo vệ dữ liệu RAID trực tiếp trên phần cứng bằng card giao tiếp với dãy đĩa. Do các phương pháp này được thực hiện theo nhà sản xuất và bỏ qua khả năng chống lỗi của hệ điều hành, chúng cải thiện hiệu năng so với triển khai RAID mềm.

Cân nhắc các vấn đề sau khi bạn quyết định xem sử dụng RAID cứng hay RAID mềm:

- Triển khai RAID cứng sẽ đắt tiền hơn so với RAID mềm và có thể gặp phải hạn chế trong việc lựa chọn thiết bị chỉ từ một nhà sản xuất.
- Triển khai RAID cứng thông thường cung cấp các tác vụ vào/ra (I/O) trên đĩa nhanh hơn so với RAID mềm.
- Triển khai RAID cứng có thể bao gồm các đặc tính như thay nóng các đĩa cứng, cho phép thay thế một đĩa cứng lỗi mà không cần phải tắt hệ thống và dự phòng nóng cho phép một đĩa bị lỗi được thay thế tự động bởi một đĩa dự phòng thường trực (***online***).

Windows Server 2003 hỗ trợ ba loại RAID dưới đây:

- **RAID-0** Đó là các ***stripped volume*** nhưng không cung cấp tính năng chống lỗi. Chúng được xem xét như một tiến trình thực thi RAID.
- **RAID-1** Các ***mirrorred volume*** là kiểu RAID chống lỗi cơ bản nhất nhưng nó không mang lại hiệu quả lắm. 50% không gian đĩa được dành cho việc lưu trữ các dữ liệu dự phòng.
- **RAID-5** Đó là các ***stripped volume*** với bit chẵn lẻ nhằm cung cấp tính năng chống lỗi với hiệu năng gia tăng và mức độ sử dụng hiệu quả hơn so với RAID-1. Cực đại, chỉ có 33% không gian của dãy đĩa được sử dụng để lưu trữ thông tin chẵn lẻ dự phòng.

Với việc triển khai RAID-1 và RAID-5 trên Windows Server 2003, khả năng chống lỗi chỉ áp dụng cho một đĩa đơn bị lỗi. Nếu một lỗi thứ hai xảy ra trước khi dữ liệu bị mất từ lỗi đầu tiên được tái tạo lại thì dữ liệu sẽ bị mất và chỉ có thể phục hồi chúng từ cơ chế sao lưu.

> ***CHÚ Ý RAID và quá trình sao lưu*** *Kỹ thuật RAID không được thiết kế với mục đích nhằm thay thế các tiến trình sao lưu hệ thống thường nhật. Không cần biết giải pháp lưu trữ của bạn có khả năng chống lỗi ra sao, bạn vẫn phải sao lưu dữ liệu một cách định kỳ.*

Do các ***RAID-5 volume*** được tạo ra như các ***volume*** động thuần chất từ không gian chưa định vị nên bạn không thể chuyển đổi một loại ***volume*** nào khác thành ***RAID-5 volume*** mà không cần sao lưu dữ liệu trên đó và phục hồi chúng trên ***RAID-5 volume*** mới được tạo ra.

Nếu có một đĩa bị lỗi trong ***RAID-5 volume***, các dữ liệu lưu trữ trên đó vẫn có thể truy cập được. Trong suốt tiến trình đọc dữ liệu, bất kỳ dữ liệu nào bị lỗi đều có thể được tái tạo lại nhờ dữ liệu còn lại và dữ liệu chẵn lẻ. Hiệu năng sẽ bị giảm trong suốt thời gian này và nếu một đĩa thứ hai bị lỗi thì dữ

liệu sẽ bị mất hoàn toàn. Một khi đĩa lỗi hoạt động trở lại, bạn cần sử dụng câu lệnh ***Rescan Disks*** trong màn hình quản trị ***Disk Management*** rồi kích hoạt ***volume*** trên đĩa phục hồi mới. Tiếp theo hệ thống sẽ xây dựng lại dữ liệu lỗi từ bit chẵn lẻ, thực hiện phục hồi đĩa và đưa ***volume*** quay trở lại trạng thái ban đầu.

Lựa chọn kỹ thuật RAID

Các ***mirrorred volume (RAID-1)*** và các ***RAID-5 volume*** cung cấp các khả năng chống lỗi và hiệu năng khác nhau. Lựa chọn của bạn sẽ phụ thuộc vào mức độ bảo vệ mà bạn yêu cầu và tài chính dành cho việc mua thiết bị phần cứng của bạn. Sự khác biệt chính giữa các ***mirrorred volume*** và các ***RAID-5 volume*** được tổng kết trong bảng 12-1 dưới đây.

Bảng 12-1 So sánh RAID-1 và RAID-5

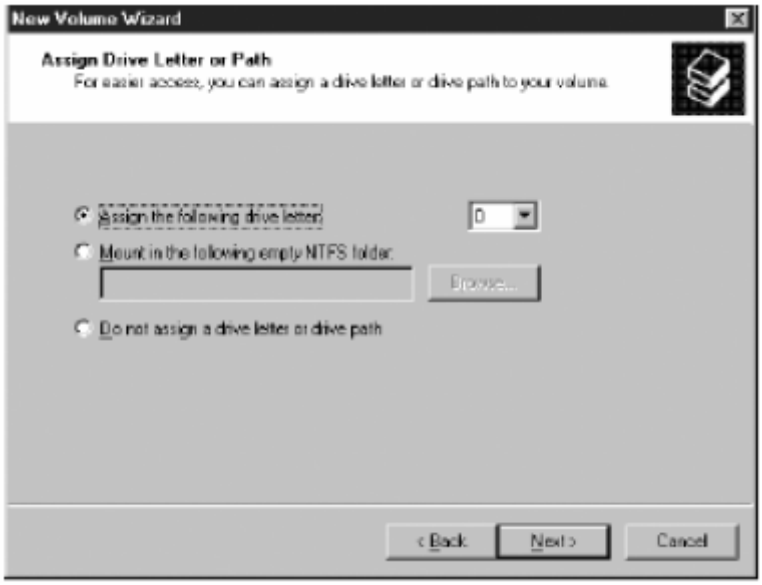
Các Mirrorred Volume (RAID-1)	Các Striped Volume với bit chẵn lẻ (RAID-5)
Có thể bảo vệ phân vùng hệ thống hoặc phân vùng khởi động	Không thể bảo vệ phân vùng hệ thống hoặc phân vùng khởi động
Yêu cầu hai đĩa cứng	Yêu cầu có tối thiểu ba đĩa cứng và cho phép tối đa 32 đĩa cứng
Có một giá trị cao hơn trên mỗi MB	Có một giá trị thấp hơn trên mỗi MB
50% dự phòng	Cực đại 33% dự phòng
Hiệu năng đọc và ghi tốt	Hiệu năng đọc tuyệt vời và hiệu năng ghi vừa phải
Sử dụng ít bộ nhớ hệ thống	Yêu cầu nhiều bộ nhớ hệ thống

> ***CHÚ Ý Mục tiêu của kỳ thi*** *Các mục tiêu cho kỳ thi 70-290 yêu cầu các học viên có khả năng "thực thi giải pháp RAID"*

Gán các ký tự ổ đĩa

Khi bạn tạo một phân vùng trên một đĩa cơ bản hoặc một ***volume*** trên một đĩa động, ***New Partition Wizard*** và ***New Volume Wizard*** sẽ cho phép bạn gán ký tự ổ đĩa cho phân vùng hoặc ***volume*** đó bằng cách sử dụng giao diện

trên trang ***Assign Drive Letter Or Path*** (*gán ký tự ổ đĩa hoặc đường dẫn*) như hình vẽ 12-7. Mặc định, trình hướng dẫn sẽ gán ký tự ổ đĩa kế tiếp còn trống (ngoại trừ A và B) cho phân vùng hoặc ***volume*** mới. Bạn cũng có thể lựa chọn bất kỳ một ký tự ổ đĩa nào còn chưa sử dụng.



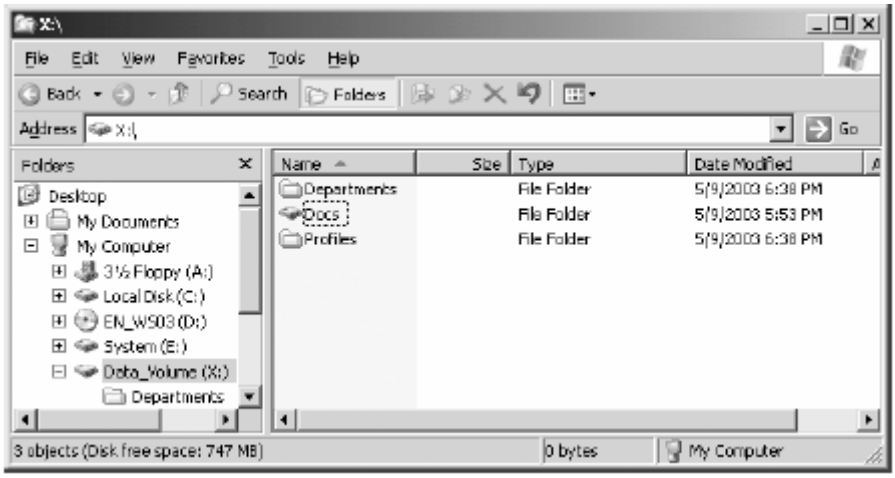
Hình 12-7 Trang Assign Drive Letter Or Path của New Volume Wizard

Thay cho việc gán ký tự ổ đĩa cho một ***volume***, bạn cũng có thể gắn ***volume*** cho một thư mục rỗng trên một ổ đĩa NTFS sẵn có. Bằng cách này, sẽ làm cho nội dung thực sự của ***volume*** sẽ xuất hiện như một thư mục nằm trên ổ đĩa khác. Khả năng cho phép mở rộng một hệ thống con lưu trữ trên Windows Server 2003 do những hạn chế của 24 ký tự ổ đĩa sẵn có và cho phép mở rộng không gian ổ đĩa trên một ***volume*** sẵn có.

Khi bạn lựa chọn ***Mount In The Following Empty NTFS Folder*** (*gắn vào một thư mục NTFS rỗng*) bạn phải trỏ tới thư mục rỗng nằm trên bất kỳ đĩa NTFS còn lại trên hệ thống bằng cách gõ trực tiếp đường dẫn hoặc sử dụng nút ***Browse***. Ổ đĩa NTFS có thể là đĩa cơ bản hoặc đĩa động và không có hạn chế về kiểu ***volume*** mà bạn có thể gắn. Ví dụ, bạn có thể gắn một ***striped volume*** với một thư mục rỗng nằm trên một ***mirrorred volume*** hoặc bạn có thể gắn một phân vùng trên đĩa cơ bản với một thư mục nằm trên ***RAID-5 volume***. Mỗi ***volume*** sẽ duy trì hiệu năng và các tính năng chống lỗi của riêng nó. Cũng không có hạn chế về hệ thống file của ***volume*** bạn gắn. ***Volume*** được gắn có thể sử dụng FAT hoặc NTFS, chỉ có đĩa chứa thư mục rỗng mà bạn gắn volume tới đó thì phải sử dụng hệ thống file NTFS.

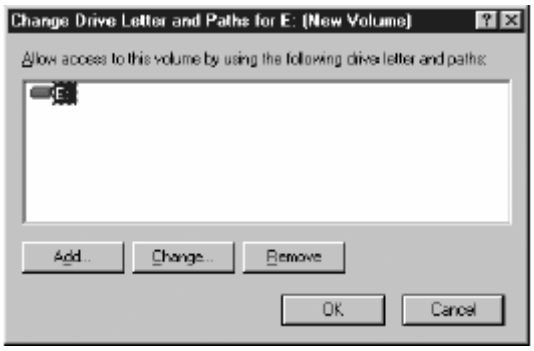
Hình vẽ 12-8 biểu diễn một máy tính có một thư mục trên một đĩa được gắn với một ***volume*** khác. Chú ý rằng thư mục sẽ xuất hiện trong kiến trúc phân

cấp của Explorer một cách chính xác theo đúng vị trí của nó trên ổ đĩa nhưng với một biểu tượng của một ổ đĩa. Khi người sử dụng truy cập đến thư mục, chúng sẽ được định hướng một cách trong suốt đến ***volume*** được gắn.



Hình 12-8 Một volume được gắn với thư mục

Bạn cũng có thể thay đổi ký tự ổ đĩa và các ***volume*** được gắn sau khi đã tạo ra chúng. Để thực hiện điều này, lựa chọn một ổ đĩa trong màn hình quản trị ***Disk Management*** và từ thực đơn ***Action*** trỏ tới ***All Tasks*** và chọn ***Change Drive Letter And Paths***. Hộp thoại ***Change Drive Letter And Paths*** xuất hiện hiển thị ký tự ổ đĩa hiện tại và quá trình gán đường dẫn cho ổ đĩa như hình vẽ 12-9.



Hình 12-9 Hộp thoại Change Drive Letter And Paths

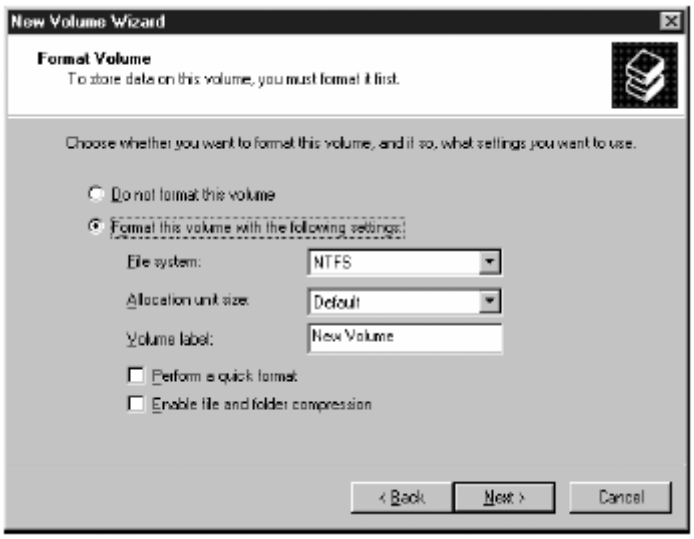
Bằng cách nhấp vào nút ***Change***, bạn có thể thay đổi việc gán ký tự ổ đĩa sẵn có hoặc đường dẫn gắn và bằng cách nhấp ***Add*** bạn có thể tạo ra một cái mới. Thậm chí bạn có thể làm cả hai, gán một ký tự ổ đĩa cho một ***volume*** hoặc phân vùng và gắn nó tới một thư mục NTFS tại cùng thời điểm.

> ***CHÚ Ý Thay đổi các ký tự ổ đĩa*** *Bạn không thể thay đổi ký tự ổ đĩa của* ***volume*** *là một phân vùng hệ thống hoặc phân vùng khởi động.*

*Nếu **volume** mà bạn muốn thay đổi hiện đang sử dụng như một ứng dụng có các file nằm trên **volume** đang mở, hệ thống có thể tạo ra một tiến trình gán ký tự ổ đĩa mới cho **volume** nhưng nó vẫn giữ nguyên ký tự ổ đĩa cũ cho đến khi bạn khởi động lại hệ thống.*

Định dạng các volume

Bước cuối cùng trong ***New Partition Wizard*** và ***New Volume Wizard*** sẽ giúp bạn định dạng phân vùng hoặc ***volume*** mới mà bạn vừa tạo bằng giao diện như hình vẽ 12-10.



Hình 12-10 Trang Format Volume của New Volume Wizard

Các điều khiển trên trang này gồm có:

- **File System (*hệ thống file*)** Windows Server 2003 hỗ trợ ba hệ thống file: FAT, FAT32 và NTFS. FAT và FAT32 sẵn có trên hệ điều hành với mục đích duy nhất là tương thích với các hệ điều hành cũ. FAT nguyên gốc là hệ thống file MS-DOS và FAT32 là một phiên bản nâng cấp của FAT và được giới thiệu lần đầu tiên trên hệ điều hành Windows 95. Cả hai hệ thống file này không đưa ra được những ưu điểm nào khác ngoài việc tương thích với các hệ điều hành cũ. Ví dụ, nếu bạn bắt đầu với một máy tính Windows Server 2003 với một đĩa MS-DOS thì chỉ các ổ đĩa được định dạng theo chuẩn FAT và FAT32 mới có thể truy cập được. Nói cách khác, NTFS bao gồm nhiều tính năn tiên tiến hơn như điều khiển truy cập, nén dữ liệu và hạn ngạch đĩa. Như vậy, có thể thấy rằng trừ phi bạn có một lý do xác đáng cho việc sử dụng FAT hoặc FAT32 bạn nên định dạng các phân vùng và volume của bạn bằng cách sử dụng hệ thống file NTFS.

CHÚ Ý Định dạng các volume trên đĩa động *Khi bạn định dạng một volume trên một đĩa động thì chỉ có duy nhất lựa chọn NTFS sẵn sàng. Vì vậy để định dạng các đĩa động với hệ thống file FAT và FAT32 bạn phải sử dụng công cụ format.exe trong chế độ dòng lệnh.*

- **Allocation Unit Size (***kích thước một đơn vị lưu trữ***)** Xác định kích thước của các liên cung mà hệ thống file sử dụng để xác định không gian đĩa. Kích thước của liên cung càng lớn cho phép đĩa truy cập các file với khả năng đọc và ghi thấp hơn nhưng cũng tốn nhiều không gian đĩa hơn khi mà các khối chỉ làm đầy theo từng phần. Kích thước của liên cung càng nhỏ sẽ tốn không gian đĩa ít hơn nhưng lại gia tăng thời gian đọc/ghi trên đĩa. Trong hầu hết các trường hợp, lựa chọn giá trị mặc định (4KB đối với các đĩa cứng có dung lượng từ 2GB trở lên) là đủ. Nếu bạn có ý định sử dụng ***volume*** chỉ để lưu trữ các file có kích thước lớn, bạn có thể sử dụng một giá trị cao hơn. Còn đối với các file nhỏ, một giá trị nhỏ hơn là phù hợp.
- **Volume Lable (***nhãn của volume***)** xác định tên cho ***volume*** với chiều dài tới 32 ký tự.
- **Perform a Quick Format (***thực hiện định dạng nhanh***)** Lựa chọn này cho phép trình hướng dẫn định dạng ***volume*** mà không cần quét đĩa cứng để dò tìm các cung (***sector***) hỏng. Nếu trước đó đĩa đã được định dạng và bạn chắc chắn rằng nó không có lỗi thì lựa chọn này sẽ làm giảm đáng kể thời gian yêu cầu cho việc định dạng.
- **Enable File and Folder Compression (***cho phép nén file và thư mục***)** Lựa chọn này làm cho tất cả các dữ liệu được lưu trên ***volume*** này đều được nén. Để sử dụng tính năng này, ***volume*** phải được định dạng theo chuẩn NTFS với kích thước đơn vị lưu trữ là 4 KB hoặc nhỏ hơn.

Bạn cũng có thể định dạng một ổ đĩa tại bất kỳ thời điểm nào bằng cách lựa chọn nó, trên thực đơn ***Action*** trỏ tới ***All Tasks*** và lựa chọn ***Format***.

Mở rộng các volume động

Không giống như các phân vùng trên các đĩa cơ bản, chúng bị khóa với kích thước xác định khi bạn tạo chúng, bạn hoàn toàn có thể mở rộng một ***volume*** trên đĩa động với các không gian chưa sử dụng trên đĩa. Điều này cho phép

bạn mở rộng một ***volume*** khi không gian lưu trữ của nó tới ngưỡng mà không cần phải ngắt kết nối ***volume*** cũng như ngắt quãng việc truy cập của người sử dụng.

Bạn có thể mở rộng các ***simple volume*** và ***spanned volume*** trên một đĩa động khi chúng được định dạng theo chuẩn NTFS và không phải là các ***volume*** hệ thống hoặc khởi động. Để mở rộng ***volume***, lựa chọn nó trong ***Disk Management***, trên thực đơn ***Action*** trỏ tới ***All Tasks*** và chọn ***Extend Volume***. ***Extend Volume Wizard*** xuất hiện, ở đó bạn có thể xác định kích thước mới của ***volume*** cũng như thêm không gian từ các đĩa khác để tạo ra một ***spanned volume***.

QUẢN TRỊ LƯU TRỮ DỮ LIỆU TRÊN ĐĨA

Các ***volume*** trên Windows Server 2003 sẽ hiệu quả và ổn định hơn nếu bạn định dạng chúng theo chuẩn NTFS nhưng đôi khi bạn vẫn cần định dạng chúng theo chuẩn FAT và FAT32. Hệ thống file NTFS ghi lại tất cả các phiên làm việc của file, thay thế tự động các liên cung hỏng và lưu trữ các khóa bí mật của tất cả các file trên ***volume*** NTFS. Với cơ chế này, NTFS bảo vệ tính toàn vẹn của cấu trúc ***volume*** và siêu dữ liệu hệ thống (đây là dữ liệu liên quan đến chính bản thân hệ thống file). Tuy nhiên dữ liệu người sử dụng vẫn có thể bị hư hỏng và phân mảnh. Người sử dụng cũng có một thói quen đó là lưu trữ một lượng lớn dữ liệu trên các ***volume*** mà họ truy cập. Các phần dưới đây sẽ giải thích làm sao để duy trì tính toàn vẹn của các ***volume***, tối ưu hóa ***volume*** qua tiến trình chống phân mảnh và đặt các giới hạn lưu trữ bằng cách sử dụng tính năng hạn ngạch đĩa.

> ***CHÚ Ý Mục tiêu của kỳ thi*** *Các mục tiêu cho kỳ thi 70-290 yêu cầu các học viên có khả năng "tối ưu hóa hiệu năng đĩa trên máy chủ"*

Sử dụng Check Disk

Check Disk (hay ***Chkdsk.exe***) là một công cụ trên hệ điều hành Windows Server 2003 cho phép bạn quét một ***volume*** trên đĩa nhằm phát hiện các lỗi trên hệ thống file và bên cạnh đó có thể kiểm tra và phục hồi các cung (***sector***) hỏng trên đĩa cứng.

Có một vài phương pháp để sử dụng công cụ này:

- Mở ***Windows Explorer***, lựa chọn một ổ đĩa cục bộ trong ***My Computer*** và chọn ***Properties*** từ thực đơn ***File***. Trên hộp thoại ***Properties***, lựa chọn thẻ ***Tools*** và nhấp vào ***Check Now***.

- Mở màn hình quản trị ***Disk Management***, lựa chọn một ***volume***, trên thực đơn ***Action*** trỏ tới ***All Tasks*** và chọn ***Properties***. Trên hộp thoại ***Properties*** chọn thẻ ***Tools*** và nhấp vào ***Check Now***.
- Mở cửa sổ màn hình chế độ dòng lệnh, gõ **chkdsk *x*: /f /r** trong đó x: là ký tự ổ đĩa. Kế đó nhấn ***Enter***.
- Khi một phân vùng được gắn trên ổ đĩa khác và không có một ký tự ổ đĩa nào, mở hộp thoại ***Properties*** của điểm gắn kết đó trong ***Windows Explorer***, chọn thẻ ***General*** và nhấp vào ***Properties*** để mở hộp thoại ***Properties*** của phân vùng thực sự. Tiếp theo lựa chọn thẻ ***Tools*** và nhấp vào ***Check Now***.

Khi bạn chạy ***Check Disk*** từ hộp thoại ***Properties*** của ổ đĩa, bạn sẽ thấy hộp thoại ***Check Disk*** như hình vẽ 12-11. Ở đó bạn có thể lựa chọn các công việc mà bạn muốn thực hiện.

Hình 12-11 Hộp thoại Check Disk

Khi bạn lựa chọn ***Automatically Fix File System Errors*** (tự động sửa các lỗi hệ thống file) hoặc thêm lựa chọn ***/f*** trong câu lệnh ***chkdsk.exe***. ***Check Disk*** sẽ cố gắng sửa những phần không tương thích trong danh mục hệ thống file như các file xuất hiện trong danh mục nhưng không xuất hiện trong thư mục trên ***volume***. ***Check Disk*** tạo ra ba bước kiểm tra trên ổ đĩa nhằm kiểm tra siêu dữ liệu – đây là dữ liệu mô tả xem các file được tổ chức như thế nào trên đĩa. Ba bước này cố gắng đảm bảo rằng tất cả các file trên ***volume*** phù hợp với bảng quản lý file MFT, rằng cấu trúc thư mục là chính xác và các mô tả bảo mật là phù hợp.

Nếu bạn lựa chọn ***Scan For And Attempt Recovery Of Bad Sectors*** (*quét và cố gắng phục hồi các sector hỏng*) hoặc thêm lựa chọn ***/r*** vào dòng lệnh ***chkdsk.exe***, ***Check Disk*** sẽ tạo ra bốn bước kiểm tra nhằm kiểm tra xem những cung nào trên ***volume*** được dành cho dữ liệu người sử dụng (nó đối lập với siêu dữ liệu hệ thống, đây là dữ liệu luôn luôn được kiểm tra). Nếu chương trình tìm thấy một cung hỏng, nó sẽ phục hồi dữ liệu và di chuyển nó đến một cung hoạt động tốt nếu ***volume*** có khả năng chống lỗi. Nếu ***volume*** không có tính năng chống lỗi, dữ liệu không thể phục hồi từ ***Check***

Disk mà bạn phải phục hồi từ sao lưu. Kế đó cung hỏng sẽ bị gỡ ra khỏi vùng hoạt động.

Tất cả các file đang mở phải được đóng lại trước khi ***Check Disk*** có thể chạy. Nếu tất cả điều khiển file không được giải phóng (đây là trường hợp bạn chạy ***Check Disk*** trên ***volume*** hệ thống), bạn sẽ được nhắc nhở lập lịch để ***Check Disk*** chạy tại lần kế tiếp khi hệ thống khởi động lại. Khi ***Check Disk*** đang chạy, các tiến trình khác không thể truy cập đến ***volume***. Tùy thuộc vào kích thước của ***volume***, các lựa chọn bạn chọn và các tiến trình khác đang chạy trên máy tính mà ***Check Disk*** mất một khoảng thời gian đáng kể để có thể hoàn thành các tác vụ của nó. Nó cũng đòi hỏi nhiều tài nguyên trên bộ vi xử lý và đĩa trong quá trình hoạt động.

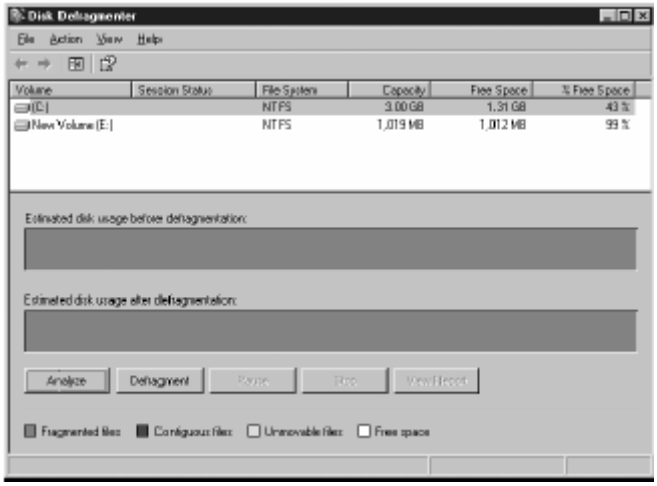
Sử dụng Disk Defragmenter

Các file được lưu trữ trên một ***volume*** theo các đơn vị gọi là các ***cluster*** (*liên cung*). Như đã đề cập ở trên, bạn cần cấu hình kích thước của liên cung khi định dạng một ổ đĩa. Nhiều ***volume*** NTFS sử dụng kích thước liên cung mặc định là 4KB. Mỗi liên cung chỉ có thể chứa một file thậm chí nếu kích thước của file đó nhỏ hơn kích thước của liên cung. Nếu một file có kích thước lớn hơn kích thước liên cung, file sẽ được lưu trên nhiều liên cung khác nhau và mỗi liên cung chứa một con trỏ chỉ đến phân đoạn kế tiếp của file. Khi có một ổ đĩa mới, tất cả các liên cung là trống và khi các file được ghi vào ổ đĩa nó sẽ có xu hướng chiếm dụng các liên cung kế tiếp nhau về mặt vật lý. Nhưng khi các file bị xóa hoặc mở rộng và thu nhỏ lại kích thước, các liên cung trống giờ đây không còn gần nhau về mặt vật lý nữa. Hiện tượng phân mảnh các file sẽ làm giảm hiệu năng đọc và ghi do đầu đọc đĩa cứng phải di chuyển tới nhiều vị trí khác nhau trên đĩa cứng.

Windows Server 2003 cung cấp một công cụ chống phân mảnh ổ đĩa giúp bạn phân tích các ***volume*** và sắp xếp lại các liên cung sao cho các file được đặt trên các không gian liền kề nhau. Công cụ chống phân mảnh đã được cải thiện một cách đáng kể trong phiên bản Windows 2000. Giờ đây nó có thể chống phân mảnh các ***volume*** có kích thước liên cung lớn hơn 4KB và có thể chống phân mảnh bảng điều khiển file MFT (***Master File Table***). Bạn có thể sử dụng công cụ này để chống phân mảnh bất kỳ ***volume*** nào trên đĩa cứng cục bộ.

Để sử dụng công cụ ***Disk Defragmenter*** như hình vẽ 12-12 mở hộp thoại ***Properties*** của một ***volume*** bằng cách sử dụng ***Windows Explorer*** hoặc ***Disk Management***, trong thẻ ***Tools*** nhấp vào ***Defragment Now***. Bạn cũng có thể mở ***Disk Defragmenter*** trong màn hình ***Computer Management*** hoặc trong

một màn hình MMC tùy biến, lựa chọn ***volume*** và nhấp vào ***Analyze***. Công cụ sẽ hiển thị một khuyến nghị dựa trên lượng phân mảnh mà nó phát hiện ra. Công cụ này cũng khuyên bạn chạy ***Check Disk*** trên ***volume*** trước khi thực hiện chống phân mảnh (đây luôn là một ý tưởng tốt).



Hình 12-12 Màn hình Disk Defragmenter

Nếu có khuyến nghị chống phân mảnh nhấp vào ***Defragment***. Bạn có thể chống phân mảnh bất kỳ kiểu ***volume*** nào: FAT32 hoặc NTFS, cơ bản hoặc động. ***Volume*** có thể có các file đang mở trong tiến trình chống phân mảnh nhưng các file mở có thể không được chống phân mảnh một cách hiệu quả và làm chậm cả tiến trình. Vì vậy bạn nên đóng tất cả các file đang mở trước khi thực hiện tiến trình chống phân mảnh. ***Disk Defragmenter*** sẽ di chuyển các file xung quanh ổ đĩa với mục tiêu thu thập tất cả các liên cung của từng file vào một khu vực kề nhau trên không gian đĩa cứng.

Để hoàn thành chống phân mảnh cho một ***volume***, ***volume*** phải có ít nhất 15% không gian trống. Công cụ này sử dụng không gian này để sắp xếp các file trong khi nó chống phân mảnh chúng. Nếu ***volume*** chứa nhiều file lớn cần phân mảnh thì không gian trống này cần phải lớn hơn thì tiến trình chống phân mảnh mới đạt hiệu quả. Nếu ***volume*** có ít hơn 15% không gian trống thì ***volume*** sẽ chỉ có thể chống phân mảnh từng phần.

> ***CHÚ Ý Mục tiêu của kỳ thi*** *Các mục tiêu cho kỳ thi 70-290 yêu cầu các học viên có khả năng "chống phân mảnh các* ***volume*** *và các phân vùng"*

Triển khai các hạn ngạch đĩa

Một trong những thách thức lớn nhất trong quá trình quản trị lưu trữ đó là theo dõi để biết được mỗi người sử dụng chiếm dụng bao nhiêu không gian

đĩa cứng trên máy chủ. Cho đến phiên bản hệ điều hành Windows 2000, có một phương pháp cho phép biết được mức độ sử dụng không gian đĩa đối với từng người sử dụng. Windows 2000 giới thiệu tính năng quản trị hạn ngạch dựa trên NTFS như một đặc tính đính kèm, cho phép các nhà quản trị thiết lập các giới hạn về không gian lưu trữ đối với mỗi người sử dụng và Windows Server 2003 cũng cung cấp chức năng tương tự. Khi tính năng hạn ngạch đĩa được kích hoạt, trình quản lý hạn ngạch sẽ theo dõi các file trên ***volume*** do một người sử dụng cụ thể nào đó làm chủ. Kế đó nó sẽ so sánh mức độ sử dụng đĩa tổng cộng của từng người sử dụng với giới hạn do quản trị viên thiết lập. Khi người sử dụng đạt tới ngưỡng của họ, trình quản lý hạn ngạch sẽ thông báo cho họ hoặc ngăn không cho họ ghi dữ liệu lên đĩa hoặc cả hai.

Trình quản trị hạn ngạch Windows Server 2003 thông báo dung lượng đĩa trống trên một ***volume*** dựa trên hạn ngạch của mỗi người sử dụng. Vì vậy nếu một người sử dụng có hạn ngạch 50MB trên một ***RAID volume*** có dung lượng 500 GB thì lúc đầu người sử dụng sẽ nhìn thấy dung lượng đĩa trống là 50MB. Khi anh ta đạt tới giới hạn ngạch, một thông báo xuất hiện tương tự như những chỉ thị rằng ***volume*** đã đầy; hệ thống cảnh báo không gian đĩa cứng còn ít và đề nghị xóa những file không cần thiết. Mặc dù trong thực tế không gian đĩa vẫn còn trống rất nhiều nhưng người sử dụng không thể biết điều đó.

Tiến trình cấu hình các hạn ngạch bao gồm các bước sau:

1. Kích hoạt tính năng hạn ngạch trên ***volume***
2. Cấu hình các thiết lập hạn ngạch mặc định
3. Tạo các mục vào hạn ngạch cho các người sử dụng cụ thể

Kích hoạt hạn ngạch

Mặc định, trên Windows Server 2003 các hạn ngạch đĩa chưa được kích hoạt. Bạn phải kích hoạt chúng trên từng ***volume*** một. Để cho phép hạn ngạch, mở hộp thoại ***Properties*** của một ***volume*** bằng cách sử dụng ***Windows Explorer*** hoặc ***Disk Management*** và lựa chọn thẻ ***Quota*** như hình vẽ 12-13. Kế đó lựa chọn hộp kiểm tra ***Enable Quota Management***.

> ***LỜI KHUYÊN Mở hộp thoại Properties của một volume*** *Hầu hết các tài liệu đều khuyên mở các đặc tính của* ***volume*** *từ Windows Explorer bằng cách kích chuột phải vào một ổ đĩa và lựa chọn* ***Properties****. Thật không may, tiến trình này hạn chế chỉ cho phép bạn*

*cấu hình các hạn ngạch với các ổ có ký tự ổ đĩa còn Windows Explorer sẽ không hiển thị thẻ **Quota** với **volume** gắn với một thư mục. Vì vậy, bạn nên cấu hình các hạn ngạch bằng cách sử dụng **Disk Management**. Màn hình quản trị này cho phép bạn mở hộp thoại **Properties** của bất kỳ **volume** nào và truy cập thẻ **Quota** của nó.*

Hình 12-13 Thẻ Quota trên hộp thoại Properties của một volume

Nếu bạn lựa chọn hộp kiểm tra ***Deny Disk Space To Users Exceeding Quota Limit*** (*ngăn cấm không cho người sử dụng chiếm dụng không gian đĩa cứng vượt quá ngưỡng hạn ngạch*), người sử dụng nào chạm tới ngưỡng lưu trữ sẽ bị cấm đưa thêm dữ liệu lên ***volume***. Bất kỳ một cố gắng nào nhằm ghi dữ liệu lên ***volume*** đều thất bại. Nếu bạn không lựa chọn hộp kiểm tra này thì người sử dụng chỉ nhận được thông báo khi họ chạm ngưỡng nhưng hệ thống sẽ không ngăn cản việc họ ghi tiếp dữ liệu lên ***volume***.

Cấu hình hạn ngạch mặc định

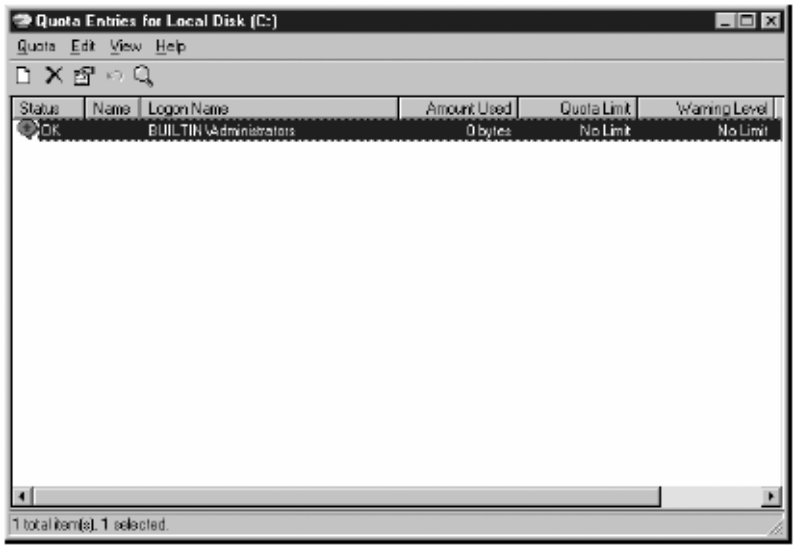
Bạn có thể quản trị hạn ngạch đĩa theo hai cách : đặt một hạn chế lưu trữ mặc định áp dụng cho tất cả mọi người và tạo các mục vào hạn ngạch nhằm định nghĩa các giới hạn cho từng người sử dụng cụ thể. Để cấu hình hạn chế lưu trữ mặc định, bạn lựa chọn ***Limit Disk Space To*** trên thẻ ***Quota*** và xác định dung lượng lưu trữ lớn nhất dành cho mỗi người sử dụng. Bạn cũng có thể xác định xem người sử dụng sẽ nhận được cảnh báo hay không khi họ gần chạm ngưỡng giới hạn.

Cuối cùng, bạn có thể xác định các lựa chọn về file nhật ký cho phép trình quản lý hạn ngạch đăng ký các sự kiện vào nhật ký hệ thống trong trình xem các sự kiện (***Event Viewer***). Các sự kiện sẽ được ghi lại nhằm xác định người sử dụng theo tên và xác định họ đã vượt quá mức cảnh báo hay mức

giới hạn. Các nhà quản trị có thể xem các mục vào này trong màn hình ***Event Viewer***.

Tạo các mục vào hạn ngạch

Về mặt cơ bản, các mục vào hạn ngạch là những ngoại lệ với luật mà bạn đã định nghĩa trong hạn ngạch mặc định. Khi bạn tạo một mục vào hạn ngạch cho một người sử dụng cụ thể, các thiết lập hạn ngạch mặc định sẽ không áp dụng cho người sử dụng đó. Các thiết lập trên các mục vào sẽ được áp dụng thay thế cho phép người sử dụng đó nhận một ngưỡng cao hơn hoặc thấp hơn. Để tạo các mục vào hạn ngạch, nhấp vào nút ***Quota Entries*** để mở cửa sổ ***Quota Entries*** như hình vẽ 12-14.



Hình 12-14 Cửa sổ Quota Entries

> ***CHÚ Ý Mục vào hạn ngạch*** *Mặc định, một mục vào hạn ngạch xuất hiện trong cửa sổ sẽ gán cho nhóm* ***Administrators*** *quyền không hạn chế về mặt lưu trữ trên* ***volume****. Điều này cho phép các nhà quản trị cài đặt hệ điều hành, các dịch vụ, các ứng dụng và dữ liệu mà không cần quan tâm đến việc có vượt quá hạn ngạch hay không. Chú ý rằng đây là nhóm duy nhất được phép gán các mục vào hạn ngạch. Khi tạo các mục vào hạn ngạch riêng, bạn chỉ có thể lựa chọn người sử dụng; bạn có thể tạo các mục vào hạn ngạch mới cho các nhóm.*

Nhấp vào nút ***New Quota Entry*** trên thanh tác vụ hoặc lựa chọn ***New Quota Entry*** từ thực đơn ***Quota*** và bạn có thể lựa chọn một hoặc nhiều người sử dụng để tạo một mục vào hạn ngạch. Một khi bạn đã lựa chọn người sử dụng, hộp thoại ***Add New Quota Entry*** xuất hiện như hình vẽ 12-15 ở đó bạn xác định các ngưỡng lưu trữ và ngưỡng cảnh báo đối với người sử dụng

lựa chọn. Khi bạn tạo một bản ghi cho nhiều người sử dụng, mỗi người sử dụng nhận ngưỡng xác định riêng rẽ.

Hình 12-15 Hộp thoại Add New Quota Entry

Lưu trữ các mục vào hạn ngạch

Nếu bạn muốn áp dụng các mục vào hạn ngạch từ một ***volume NTFS*** này cho một volume NTFS khác, bạn có thể xuất các mục vào đó ra một file nào đó và nhập chúng vào ***volume*** kia. Lựa chọn một hoặc nhiều các mục vào hạn ngạch, trên thực đơn ***Quota*** nhấp ***Export*** và xác định tên file. Trên ***volume*** kia, lựa chọn ***Import*** rồi chọn file có chứa các mục vào mà bạn muốn nhập.

Giám sát các hạn ngạch và khả năng lưu trữ

Hộp thoại ***Quota Entries*** hiển thị mức độ sử dụng dung lượng đĩa với mỗi người sử dụng và xác định xem dung lượng lưu trữ này bằng hoặc trên mức cảnh báo hoặc mức ngưỡng. Không có cơ chế tạo ra các cảnh báo cho người quản trị về việc người sử dụng đạt tới các ngưỡng hạn ngạch của họ. Vì vậy bạn phải giám sát hộp thoại ***Quota Entries*** hoặc các nhật ký nằm trong phần ***System*** của ***Event Viewer***.

> ***CHÚ Ý Mục tiêu của kỳ thi*** *Các mục tiêu cho kỳ thi 70-290 yêu cầu các học viên có khả năng "giám sát các hạn ngạch đĩa"*

TỔNG KẾT

- Windows Server 2003 hỗ trợ hai loại lưu trữ: cơ bản và động cùng với ba hệ thống file: FAT, FAT32 và NTFS. Hầu hết các đặc tính quản trị lưu trữ tiên tiến chỉ sẵn sàng trên các ***volume*** trên đĩa động và được định dạng theo chuẩn NTFS.
- Các đĩa cơ bản và hệ thống file FAT cung cấp tinh tương thích với các hệ điều hành Windows cũ nhưng bị hạn chế bởi dung lượng của chúng. Một đĩa cơ bản có thể cấu hình lên tới bốn phân vùng của cả hai loại: chính và mở rộng. Chỉ có một phân vùng mở rộng duy nhất trên đĩa nhưng bạn có thể tạo nhiều ổ đĩa logic khác nhau tùy theo nhu cầu của bạn.
- Các đĩa động cung cấp các lựa chọn linh hoạt và mạnh mẽ trong các cấu hình với yêu cầu nhiều hơn một đĩa. Một đĩa động chỉ có duy nhất một phân vùng nhưng bạn có thể có tùy thích bao nhiêu ***volume*** trên phân vùng đó.
- Các đĩa cơ bản có thể chuyển đổi thành các đĩa động mà không mất mát dữ liệu nhưng bạn sẽ mất tất cả dữ liệu và các ***volume*** sẽ bị xóa khi thực hiện chuyển đổi một đĩa động thành một đĩa cơ bản.
- Các đĩa động hỗ trợ các loại ***volume*** sau: ***simple, spanned, striped, mirrored*** *và* ***RAID-5*** cung cấp khả năng lưu trữ tùy thuộc vào dung lượng, hiệu năng và khả năng chống lỗi.
- ***Mirrored volume (RAID-1)*** cung cấp khả năng chống lỗi, nó duy trì một phiên bản sao lưu trên cả hai đĩa. Các ***striped volume*** với bit chẵn lẻ (RAID-5) sẽ đưa dữ liệu lên trên nhiều đĩa và sử dụng dữ liệu chẵn lẻ. Các dữ liệu này được duy trì với mục đích tính toán dữ liệu bị lỗi khi có một đĩa bị hư hỏng.
- Các ***simple volume, spanned volume, striped volume (RAID-0)*** và tất cả các ổ đĩa logic trên các đĩa cơ bản đều không có tính năng chống lỗi. Tất cả dữ liệu sẽ bị mất đi nếu có bất kỳ đĩa nào bị lỗi. Các ***volume*** này càng lớn hoặc nhiều đĩa vật lý hỗ trợ cho chúng thì khả năng bị lỗi càng cao.
- Để tạo và quản trị các đĩa cơ bảm và đĩa động, bạn sử dụng ***Disk Management***. Các công việc quản lý đĩa thông dụng gồm có tạo và xóa các phân vùng, các ***volume*** và gán các ký tự ổ đĩa, các điểm gắn kết.

- Các ***volume*** có thể bị hỏng hoặc phân mảnh và thường xuyên bị đầy. Các công cụ như ***Check Disk, Disk Defragmenter*** và ***Quota Manager*** sẽ giúp bạn quản trị các ***volume*** sẵn có.
- Các hạn ngạch đĩa cho phép bạn thiết lập và giám sát các ngưỡng lưu trữ và ngăn cản người sử dụng ghi dữ liệu lên đĩa một khi anh ta vượt quá mức ngưỡng. Các hạn ngạch có thể được cấu hình cho từng người sử dụng, trên từng ***volume***.

BÀI TẬP THỰC HÀNH

==========

Bài tập thực hành 12-1: Sử dụng Check Disk

Trong bài thực hành này, bạn sẽ sử dụng công cụ ***Check Disk*** để kiểm tra điều kiện trên ổ C: máy tính của bạn.

1. Truy cập vào hệ điều hành Windows Server 2003 bằng tài khoản ***Administrator.***
2. Nhấp ***Start***, sau đó nhấp vào ***Windows Explorer.***
3. Lựa chọn ổ đĩa ***C*** trong ***Windows Explorer*** và từ thực đơn ***File*** lựa chọn ***Properties***. Hộp thoại ***Local Disk (C:) Properties*** xuất hiện.
4. Lựa chọn thẻ ***Tools*** và nhấp vào ***Check Now***. Hôp thoại ***Check Disk Local Disk (C:)*** xuất hiện.
5. Lựa chọn các hộp kiểm tra ***Automatically Fix File System Errors*** và ***Scan For And Attempt Recovery Of Bad Sector*** và nhấp ***Start***. Một hộp thông báo ***Checking Disk Local Disk (C:)*** xuất hiện ngụ ý rằng ***Check Disk*** yêu cầu truy cập hoàn toàn đến ổ đĩa.
6. Nhấp ***Yes*** để lập lịch cho tiến trình kiểm tra đĩa tại lần kế tiếp khi bạn khởi động lại máy tính.
7. Khởi động lại máy tính và theo dõi tiến trình kiểm tra đĩa xảy ra.

==========

Bài tập thực hành 12-2: Chống phân mảnh một đĩa cứng

Trong bài thực hành này, bạn sẽ sử dụng công cụ ***Disk Defragmenter*** để chống phân mảnh cho ổ đĩa C máy tính của bạn.

1. Truy cập vào hệ điều hành Windows Server 2003 bằng tài khoản ***Administrator.***
2. Nhấp ***Start*** và nhấp ***Windows Explorer.***
3. Lựa chọn ổ đĩa C trong Windows Explorer và từ thực đơn ***File*** lựa chọn ***Properties.*** Hộp thoại ***Local Disk (C:) Properties*** xuất hiện.
4. Lựa chọn thẻ ***Tools*** và nhấp vào ***Defragment Now.*** Màn hình ***Disk Defragmenter*** xuất hiện.
5. Nhấp ***Analyze***. Sau quá trình phân tích, một hộp thông báo ***Disk Defragmenter*** xuất hiện xác định xem bạn có nên chống phân mảnh ổ đĩa này không.
6. Bất kể những khuyến nghị của chương trình, nhấp ***Defragment*** để bắt đầu tiến trình chống phân mảnh ổ đĩa. Khi tiến trình này kết thúc, một thông báo khác xuất hiện cho phép bạn xem lại báo cáo về quá trình hoạt động của quá trình.

==========

Bài tập thực hành 12-3: Cấu hình các hạn ngạch đĩa mặc định

Trong bài thực hành này, bạn sẽ cấu hình các hạn ngạch đĩa mặc định cho ổ đĩa C máy tính của bạn.

1. Truy cập vào hệ điều hành Windows Server 2003 bằng tài khoản ***Administrator.***
2. Nhấp ***Start*** và nhấp ***Windows Explorer.***
3. Lựa chọn ổ đĩa ***C*** trong ***Windows Explorer*** và từ thực đơn ***File*** lựa chọn ***Properties.*** Hộp thoại ***Local Disk (C:) Properties*** xuất hiện.

4. Lựa chọn thẻ ***Quota*** rồi lựa chọn hộp kiểm tra ***Enable Quota Management***.
5. Lựa chọn ***Limit Disk Space To*** và xác định một dung lượng tối đa là ***5000MB***.
6. Trong điều khiển ***Set Warning Level To*** xác định một mức cảnh báo là ***450MB***.
7. Lựa chọn cả hai hộp kiểm tra về tiến trình ghi lại nhật ký đối với hạn ngạch và nhấp ***OK***. Một hộp thông báo ***Disk Quota*** xuất hiện.
8. Nhấp ***OK*** để đóng hộp thông báo và kích hoạt hệ thống hạn ngạch.

CÂU HỎI ÔN TẬP

1. Những đáp án nào dưới đây cung cấp khả năng phục hồi nếu có lỗi xảy ra đối với một đĩa cứng đơn?

    a. Ổ đĩa logic

    b. Simple volume

    c. Mirrored volume

    d. Striped volume

    e. Phân vùng mở rộng

    f. Spanned volume

    g. ***RAID-5 volume***

    h. Phân vùng chính

2. Bạn có một máy tính có cài đặt hai hệ điều hành trong phòng lab. Máy tính cài đặt Windows NT4 trên phân vùng chính đầu tiên và Windows Server 2003 được cài đặt trên phân vùng thứ hai. Máy tính đang ở trong tình trạng thiếu không gian đĩa cứng vì vậy bạn cần thêm một đĩa cứng mới. Bạn khởi động máy tính với hệ điều hành Windows Server 2003 và cấu hình đĩa này là một đĩa động. Sau đó bạn khởi động với Windows NT4 và bạn không thể nhìn thấy đĩa này. Tại sao?

3. Nhằm cung cấp tính năng chống lỗi, hiệu năng cao nhất và khả năng thay thế nóng một ổ đĩa lỗi bạn mua một RAID cứng với 7 đĩa. Sau khi cài đặt nhóm đĩa này, bạn chỉ nhìn thấy duy nhất một đĩa mới trên Windows Server 2003. Tại sao?

4. Những đáp án nào dưới đây cho phép bạn tạo các ổ đĩa logic?

    a. Các phân vùng chính

    b. Các ***simple volume***

    c. ***Các spanned volume***

d. Các phân vùng mở rộng

e. Không gian đĩa chưa sử dụng

5. Gần đây bạn có thêm một đĩa cứng cho máy tính của bạn. Trước kia đĩa này đã được sử dụng trên một máy tính cài đặt Windows 2000 Server. Đĩa đã xuất hiện trong ***Device Manager*** nhưng lại không hiển thị chính xác trong ***Disk Management***. Mục thực đơn nào bạn phải lựa chọn?

    a. ***Import Foreign Disk*** (*nhập một đĩa bên ngoài*)

    b. ***Format*** (*định dạng*)

    c. ***Rescan Disks*** (*quét lại các đĩa*)

    d. ***Change Drive Letter And Paths*** (*thay đổi ký tự ổ đĩa và đường dẫn*)

    e. ***Convert To Dynamic Disk*** (*chuyển đổi thành đĩa động*)

6. Bạn cố gắng chuyển đổi một đĩa ***FireWire*** ngoại vi từ cơ chế lưu trữ cơ bản thành lưu trữ động nhưng lựa chọn ***Convert*** (*chuyển đổi*) không sẵn sàng. Lý do vì sao?

7. Bạn là nhà quản trị của một máy tính Windows Server 2003. Bạn muốn sửa bất kỳ một lỗi nào xảy ra với hệ thống file và phục hồi các cung hỏng trên đĩa cứng của máy tính. Công cụ nào cho phép bạn thực hiện công việc này?

    a. Check Disk

    b. Disk Defragmenter

    c. Diskpart.exe

    d. Disk quotas

8. Dung lượng không gian đĩa trống yêu cầu trên một ***volume*** để có thể hoàn thành một tiến trình chống phân mảnh là bao nhiêu?

a. 5%

b. 10%

c. 15%

d. 25%

e. 50%

9. Bạn đang triển khai giải pháp RAID mềm trên máy tính Windows Server 2003 của bạn. Bạn muốn cung cấp tính năng chống lỗi cho các phân vùng hệ thống và khởi động. Bạn sẽ sử dụng phiên bản nào của RAID?

   a. RAID-0

   b. RAID-1

   c. RAID-5

   d. Không thể sử dụng RAID mềm để bảo vệ phân vùng khởi động

10. Bạn đang cài đặt một máy tính Windows Server 2003 và bạn muốn bảo vệ dữ liệu trên đĩa cứng. Bạn muốn triển khai một giải pháp nhằm cung cấp đĩa vào/ra nhanh nhất có thể và hỗ trợ thay thế nóng các đĩa cứng. Giải pháp của bạn là gì?

    a. RAID-0

    b. RAID-1

    c. RAID-5

    d. RAID cứng

11. Bạn đang cài đặt RAID-5 trên máy tính Windows Server 2003. Bạn lập kế hoạch sử dụng 5 đĩa cứng mỗi cái có dung lượng 20GB. Phần trăm dung lượng dự phòng bạn có thể dự đoán trong cấu hình?

    a. 20

b. 25

c. 33

d. 50

12. Bạn đang cài đặt RAID mềm trên máy tính Windows Server 2003 nhằm cung cấp tính năng chống lỗi cho dữ liệu lưu trữ trên đó. Máy tính này có vai trò là máy chủ cơ sở dữ liệu trên mạng. Máy chủ này thường thực hiện nhiều chức năng đọc nhưng lại khá ít chức năng ghi. Bạn muốn có một giải pháp chống lỗi nhằm cung cấp hiệu năng cao nhất. Bạn sẽ sử dụng giải pháp RAID nào?

    a. RAID-0

    b. RAID-1

    c. RAID-5

13. Trên một máy tính bạn muốn triển khai RAID-5 có ba đĩa cứng mỗi đĩa có 2GB không gian chưa sử dụng. Sử dụng màn hình ***Disk Management***, bạn khởi tạo ***New Volume Wizard*** bằng cách nhấp vào một trong các vùng không gian đĩa cứng chưa sử dụng. Khi bạn tới màn hình ***Select Volume Type***, lựa chọn ***RAID-5*** không được kích hoạt. Lý do vì sao?

    a. Đã triển khai RAID-5 cứng

    b. Một hoặc hai đĩa cứng được cấu hình ở cơ chế lưu trữ cơ bản

    c. Cả ba đĩa cứng được cấu hình ở cơ chế lưu trữ động

    d. Cả ba đĩa cứng được cấu hình ở cơ chế lưu trữ cơ bản

    e. Đã triển khai RAID-5 mềm

CÁC KỊCH BẢN TÌNH HUỐNG

==========

Kịch bản 12-1: Sử dụng RAID

Minh có hai ổ đĩa cứng 100-GB SCSI trên một máy chủ Windows Server 2003 do anh ta quản trị. Máy chủ này cũng có một bộ điều khiển RAID cứng hỗ trợ RAID-0,1,5. Hiện tại trên đĩa cứng thứ nhất đã sử dụng 70 GB và ổ đĩa thứ hai đang trống. Minh sợ rằng đĩa thứ nhất có thể bị hỏng gây ra mất mát dữ liệu trên đó. Minh đang cân nhắc giải pháp sao lưu định kỳ nhưng không có thiết bị nào cho phép sao lưu dung lượng dữ liệu như vậy. Anh ta muốn triển khai một giải pháp cung cấp tính năng chống lỗi cho đĩa thứ nhất. Trong các giải pháp dưới đây, đâu là giải pháp cho phép anh ta thực hiện với cấu hình hiện tại của máy chủ Windows Server 2003?

1. Cấu hình dịch vụ ***shadow copy*** trên ***volume*** nằm trên đĩa cứng thứ nhất.
2. Cấu hình các đĩa trong cấu hình RAID-5 sử dụng công cụ cấu hình của bộ điều khiển RAID cứng.
3. Cấu hình các đĩa trong cấu hình RAID-0 sử dụng công cụ cấu hình của bộ điều khiển RAID cứng.
4. Cấu hình các đĩa trong cấu hình RAID-1 sử dụng công cụ cấu hình của bộ điều khiển RAID cứng.

==========

Kịch bản 12-2: Tăng khả năng lưu trữ

Minh là nhà quản trị hệ thống của máy chủ file Windows Server 2003. Máy chủ này hiện tại có hai đĩa cứng. Đĩa thứ nhất có dung lượng 30 GB nắm giữ các file của hệ điều hành. Đĩa thứ hai có dung lượng 80 GB nắm giữ dữ liệu người sử dụng trên 05 thư mục chia sẻ riêng biệt. Mỗi thư mục chia sẻ tương ứng với một phòng trong công ty và chúng lại được chia thành 03 thư mục riêng biệt. Thư mục thứ nhất là chứa các tài liệu phòng, thư mục thứ hai chứa các tài liệu làm việc nhóm và thư mục thứ ba chứa dữ liệu của từng cá nhân.

Tất cả người sử dụng đều có quyền ***Read*** đối với thư mục của phòng và có quyền ***Read/Write*** đối với thư mục chứa tài liệu làm việc nhóm. Ngoài ra, mỗi người sử dụng có toàn quyền đối với thư mục dữ liệu cá nhân của mình. Duy nhất chỉ có mình anh ta mới có quyền trên thư mục của mình, những người sử dụng khác không có bất kỳ quyền nào trên đó. Hệ thống 05 thư mục chia sẻ này làm việc tốt và tất cả các nhân viên trong công ty đều hiểu cấu trúc lưu trữ và tìm kiếm tài liệu.

Có một vấn đề trong tiến trình phát triển đó là dữ liệu người sử dụng trên 05 thư mục chia sẻ của các phòng phát triển quá nhanh làm cho đĩa lưu trữ dữ liệu này hầu như đầy. Vấn đề này buộc Minh phải triển khai một giải pháp nhằm giải quyết lỗi này. Mục tiêu chính của anh ta là thêm không gian cho mỗi chia sẻ để đảm bảo rằng đĩa lưu trữ các thư mục chia sẻ này không bị đầy.

Anh ta cũng nhận được yêu cầu từ phía giám đốc, như là một mục tiêu thứ yếu, cần phải đảm bảo các vấn đề sau:

- Chỉ giữ 05 thư mục chia sẻ và đảm bảo thư mục dữ liệu người sử dụng là ngoài mỗi chia sẻ mức phòng.
- Cung cấp tính năng chống lỗi cho các file được chia sẻ
- Giữ nguyên cơ chế bảo mật hiện tại đang sử dụng vì vậy những người sử dụng riêng lẻ có toàn quyền điều khiển với thư mục của họ và những người sử dụng khác không thể truy cập được.

Để đạt được mục tiêu này, Minh tiến hành các công việc sau. Trong quãng thời gian lập lịch sau nửa đêm, khi không có người sử dụng nào kết nối tới máy chủ anh ta tiến hành tắt máy chủ và cài đặt năm đĩa cứng mới có dung lượng 100 GB trên đó. Kế đó anh ta định dạng mỗi đĩa như một ***volume*** với hệ thống file NTFS và tạo ra một thư mục mới có tên ***Temp*** trên mỗi thư mục lưu trữ các chia sẻ của từng phòng. Lần lượt từng cái một, anh ta gắn kết năm đĩa cứng với mỗi thư mục ***Temp*** sao cho mỗi thư mục này trỏ tới một đĩa cứng của riêng chúng. Sau đó anh ta chép dữ liệu của thư mục dữ liệu người sử dụng vào thư mục ***Temp*** trên mỗi chia sẻ và kế đó anh ta xóa thư mục dữ liệu gốc. Cuối cùng, Minh đổi tên thư mục ***Temp*** thành tên của thư mục dữ liệu người sử dụng.

Với giải pháp nói trên, theo bạn Minh có thể đạt được những mục tiêu nào?

a. Anh ta không đạt được bất kỳ mục tiêu chính nào nhưng lại đạt được tất cả các mục tiêu do giám đốc đưa ra.

b. Anh ta đạt được mục tiêu chính và một mục tiêu thứ yếu.

c. Anh ta đạt được mục tiêu chính và hai mục tiêu thứ yếu.

d. Anh ta đạt được tất cả các mục tiêu chính và mục tiêu thứ yếu.

e. Anh ta không đạt được mục tiêu nào cả.

THUẬT NGỮ

access control entry (ACE) ***Mục vào Kiểm soát Truy nhập*****:** một mục vào (*dòng*) trong ***Danh sách Kiểm soát Truy nhập*** (***access control list*** - ACL) xác định các cấp phép được trao cho một Chủ thể Bảo mật cụ thể nào đó..

access control list (ACL) ***Danh sách Kiểm soát Truy nhập*** Một tập hợp các Mục vào Kiểm soát Truy nhập liên quan tới file, folder, đối tượng Active Directory hay các tài nguyên khác xác định các cấp phép mà các Chủ thể Bảo mật (như người dùng, máy tính…) có khi truy nhập các tài nguyên.

ACE *Xem* **access control entry (ACE)**.

ACL *Xem* **access control list (ACL)**.

active partition ***Phân vùng được tích cực*** Phân vùng có chứa các file khởi động của hệ thống.

archive bit ***Bit lưu trữ*** Cờ 1 bit có chứa trong tất cả các file giúp cho các chương trình sao lưu xác định được file nào cần lưu trữ. Các file mới tạo có bit lưu trữ được kích hoạt và việc thực hiện sao lưu toàn phần sẽ xóa bít này. Bit lưu trữ này lại được kích hoạt lại khi ta tiến hành sửa đổi file, giúp cho các chế độ sao lưu tăng lên hay sai khác có thể sao lưu các file đã được sửa đổi..

attribute ***thuộc tính*** Một thành phần nguyên tố của đối tượng Active Directory cung cấp các thông tin về đối tượng, ví dụ đối tượng người dùng có các thuộc tính tên goi, tên họ, địa chỉ E-mail của người dùng.

Autochanger ***Bộ nạp tự động*** Một loại thiết bị phần cứng bao gồm một hay nhiều ổ băng từ, một dẫy các băng từ và cơ cấu tự động đưa các băng tù nhất định vào ổ băng. Bộ nạp tự động giúp các Quản trị hệ thống thực hiện các chiến lược sao lưu tự động.

Baseline ***Đường cơ sở*** Một tập hợp các mức hiệu năng thu được trong điều kiện hoạt động bình thường. Được dùng để so sánh với các mức hiệu năng thu được sau này, khi hệ thống gặp vấn đề khi hoạt động.

Bottleneck ***Nút cổ chai*** Một thành phần nào đó trong hệ thống không cung cấp cùng mức hiệu năng như các thành phần khác, gây nên việc hoạt động chậm chễ của toàn hệ thống.

CAL *Xem* **Client Access License (CAL).**

Client Access License (CAL) ***Giấy phép Truy nhập từ Máy khách*** Một loại giấy phép cho phép người dùng hay thiết bị kết nối tới sản phẩm máy chủ để thực hiện các chức năng sử dụng các thành phần máy chủ, bao gồm các dịch vụ file, in ấn, xác thực. Các truy nhập không xác thực thông qua Internet không yêu cầu có giấy phép này.

commit memory ***Bộ nhớ cam kết*** Lượng bộ nhớ được đặt sẵn cho các chương trình người dùng và hệ thống.

computer object ***Đối tượng Máy tính*** Một kiểu đối tượng Active Directory đại diện cho mọt máy tính cụ thể trong Miền. đối tượng này bao gồm Tài khoản Máy tính, giúp hệ thống có thể thiết lập kênh bảo mật giữa Máy tính và Máy chủ Điều khiển Miền, và các thông tin về máy tính.

container object ***Đối tượng chứa*** Một loại đối tượng Active Directory có thể chứa trong nó các đối tượng khác.

details pane ***Khung chi tiết*** Khung phía bên phải trong Bảng điều khiển Quản trị Microsoft (MMC), hiển thị các thông tin chi tiết về các thành phần được lựa chọn trên khung Phạm vi ở bên trái của sổ MMC.

device driver ***Trình Điều khiển Thiết bị*** Mọt tập các thường trình thực hiện các chức năng chuyên biệt của thiết bị để trợ giúp cho các hoạt động vào/ra của nó.

differential backup ***Sao lưu Sai khác (vi sai)*** Một kiểu sao lưu có sử dụng bộ lọc sao cho chỉ các file đã thay đổi sau lần sao lưu toàn phần gần nhất được sao lưu. Kiểu sao lưu này chỉ sao lưu các file có bit lưu trữ được kích hoạt và không thay đổi giá trị bit sao lưu của file. Sao lưu Sai khác yêu cầu nhiều không gian lưu trữ hơn so với kiểu Sao lưu Tăng lên do các file có thay đổi sẽ được sao lưu trong tất cả các lần thực hiện kiểu sao lưu này cho đến lần thực hiện Sao lưu Toàn phần kế tiếp. Tuy nhiên, kiểu sao lưu này giúp thực hiện việc phục hồi dễ dàng và nhanh chóng hơn do chỉ cần một bản sao lưu toàn phần và một bản sao lưu sai khác gần nhất là đủ.

Xem thêm **incremental backup**.

direct memory access (DMA) channel ***Kênh Truy nhập Bộ nhớ Trực tiếp*** Một kênh dẫn được các thiết bị phần cứng sử dụng để truyền trực tiếp dữ liệu

vào/ra bộ nhớ hệ thống (không thông qua CPU).

directory service *Dịch vụ thư mục* Một cơ sở dữ liệu bao gồm các thông tin về các thực thể và tài nguyên mạng, dược các người dùng sử dụng như là một hướng dẫn truy nhập các tài nguyên mạng và như là một nguồn xác thực. Các hệ điều hành mạng trước đây sử dụng Dịch vụ thư mục dạng các file bảng cơ bản, như Windows NT và Novell NetWare. Ngày nay, các Dịch vụ thư mục, như Active Directory của Microsoft và eDirectory của Novell, được xây dụng có tính cấu trúc trật tự và hỗ trợ cho các mạng doanh nghiệp lớn.

distribution group *Nhóm Phân phối* Một kiểu nhóm Active Directory không thể thực hiện các chức năng như các Chủ thể Bảo mật, dược sử dụng chính để tạo ra các dan sách E-mail.

DMA channel *Kênh DMA* *Xem* **direct memory access (DMA) channel**.

Domain *Miền* Một tập hợp của các người dùng, máy tính, tài nguyên có các thông tin của chúng được lưu trữ trong Dịch vụ Thư mục trên máy chủ (gọi là Máy chủ Quản trị Miền hay DC).

domain controller *Máy chủ Quản trị Miền* Một máy tính chạy hệ điều hành Windows Server 2003, Windows 2000, hay Windows NT được chỉ định để lưu trữ và xử lí các thông tin Dịch vụ Thư mục. Miền Windows NT và dịch vụ Active Directory lưu CSDL dịch vụ thư mục trên máy tính này, đồng thời chúng cũng làm nhiệm vụ xác thực các người dùng muốn truy nhập các tài nguyên mạng..

domain functional level *Cấp Chức năng Miền* Một thiết lập chỉ định các chức năng nào của Active Directory là có thể thực hiện trong Miền. Việc thực thi Active Directory trong các phiên bản khác nhau của Windows có khác nhau đôi chút trong các tính năng của nó và Cấp Chức năng Miền kiểm soát các tổ hợp nhóm hay các sự chuyển đổi nhóm nào là có thể thực hiện được.

domain local group *Nhóm Cục bộ Miền* Một loại phạm vi nhóm Active Directory được sử dụng chính để cung cấp truy nhập tới các nguồn tài nguyên trong một Miền đơn.

Duplexing *Nhân bản* Việc cài đặt theo kiểu ánh xạ đĩa, trong đó mỗi đĩa vật lý sẽ được kết nối tới một kênh/card điều khiển khác nhau. Kỹ thuật này

cho hiệu năng tốt và khả năng chống lỗi cả đối với các hỏng hóc của đĩa cũng như của kênh/card điều khiển.

effective permissions ***Các Cấp phép Hiệu dụng*** là sự kết hợp của các cấp phép Cho phép, Từ chối, Thừa kế, và Trực tiếp đối với Chủ thể Bảo mật. Nó cho phép xem trực tiếp các cấp phép có hiệu lực đối với Chủ thể Bảo mật khi thực hiện chức năng truy cập đến tài nguyên.

Forest ***Rừng*** một nhóm các cây Active Directory sử dụng các khoảng không gian tên khác nhau.

forest functional level ***Cấp Chức năng Rừng*** Một thiết lập xác định các chức năng Active Directory nào là có thể thực hiện trong rừng. nâng cấp chức năng rừng không ảnh hưởng đến các hoạt động của nhóm Active Director.

Fragmentation ***Phân mảnh*** Một trạng thái của đĩa có chứa các file được lưu trữ trên nhiều liên cung cách xa nhau. Do đầu đọc phải di chuyển trên toàn bộ đĩa để đọc các thông tin của một file nên hiệu năng chung sẽ giảm.

global group ***Nhóm Toàn cục*** Một loại phạm vi nhóm Active Directory được sử dụng thông dụng nhất cho việc cấp phép cho các đối tượng thư mục có yêu cầu thường xuyên bảo trì, như tài khoản người dùng, máy tính.

GPO *Xem* **group policy object (GPO).**

group policy object (GPO) ***Đối tượng Chính sách Nhóm*** Một tập hợp của các thiết lập chính sách nhóm áp dụng trên Miền, Site, hay đối tượng OU (*organizational*

unit).

host header ***Tiêu đề Máy chủ*** Một phương pháp dùng để phân biệt các Web Site chạy trên một máy chủ khi nó chỉ sử dụng một địa chỉ IP và một số hiệu cổng. Bằng việc xác định tên của máy chủ Web (Tiêu đề Máy chủ) trong yêu cầu HTTP, máy chủ Web có thể chuyển tiếp mỗi yêu cầu trên tới một Web Ste tương ứng.

hotfix ***Bản sửa lỗi nóng*** Một miếng vá hay bản cập nhật cho các sản phẩm của Microsoft để khắc phục một vấn đề đã nêu trong một bài liên quan tại Microsoft Knowledge Base (*một dạng tập san các kiến thức từ Microsoft*). Bản sửa lỗi nóng được áp dụng cho các máy tính có thực hiện một số tác vụ nhất định hay đã gặp phải các vấn đề tương tự như bài báo đã chỉ ra..

incremental backup *Sao lưu Tăng lên* Một kiểu sao lưu có sử dụng bộ lọc sao cho chỉ thực hiện sao lưu với các file đã bị thay đổi từ lần sao lưu trước. Bộ lọc sẽ đánh giá bít lưu trữ của mỗi file và chỉ sao lưu các file nào có bít lưu trữ được kích hoạt. Sao lưu Tăng lên sẽ sửa lại giá trị bit lưu trữ sau mỗi lần sao lưu (không giống như Sao lưu Sai khác, chúng không sửa bit lưu trữ). Kiểu sao lưu này chũng sử dụng ít băng/đĩa sao lưu hơn do chúng không tiến hnàh sao lưu lại các file đã được sao lưu từ lần sao lưu trước mà không có thay đổi gì. Nhưng việc phục hồi các dữ liệu sao lưu này là khó khăn hơn do phải phục hồi lần lượt theo đúng thứ tự tất cả các bản sao lưu đã có kể từ lần sao lưu toàn phần gần nhất.

interrupt request (IRQ) *Yêu cầu ngắt* một tín hiệu được gửi từ thành phần này đến thành phần khác của hệ thống (thông thường được gửi từ thiết bị ngoại vi đến bộ vi xử lí) báo hiệu rằng thiết bị gửi đòi hỏi sự chú ý của thiết bị nhận.

I/O address *Địa chỉ Vào/Ra* vị trí trong bộ nhớ đành cho một thiết bị phần cứng nào đó sử dụng, dùng để trao đổi thông tin với hệ thống.

IRQ *Xem* **interrupt request (IRQ)**

leaf object *Đối tượng Lá* Một loại đối tượng Active Directory không thể chứa bất cứ một đối tượng khác nào trong nó.

license group *Nhóm Giấy phép* Do Dịch vụ Nhật ký Giấy phép (License Logging Service) phân phối các giấy phép theo tên người dùng chứ không phải tên thiết bị nên các giấy phép truy nhập từ máy trạm cấp cho thiết bị (Device Client Access Licenses) được trao cho Nhóm Giấy phép. Một Nhóm Giấy phép có thể có một hay nhiều người dùng được trao cho một số giấy phép đúng bằng số các thiết bị mà họ dùng để truy nhập các sản phẩm máy chủ.

local group *Nhóm Cục bộ* Là nhóm của các tài khoản trên các máy chủ độc lập hay các máy chủ thành viên chạy Windows Server 2003. Nhóm Cục bộ có thể có các người dùng cục bộ và các nhóm toàn cục miền là thành viên của nó nhưng chỉ cung cấp việc truy nhập đến các tài nguyên có trên hệ thống cục bộ có chứa nhóm này.

locally attached printer *Máy in Kết nối Cục bộ* Một máy in vật lý được kết nối trực tiếp tới máy tính, thông thường sử dụng các cổng song song hay USB.

local user profile ***Khái lược Người dùng Cục bộ*** Là tập hợp của các file và folder xây dựng nên môi trường màn hình nền dành cho một người dùng xác định, được lưu trữ trên ổ đĩa cục bộ.

logical printer ***Máy in Logic*** Là đại diện của máy in vật lý trên máy tính, nó gửi các tác vụ in đến máy in vật lý thông qua cổng xác định. Máy in logic bao gồm hàng đợi in, trình điều khiển máy in, các thiết lập, cấp phép và các thiết lập mặc định in quản lý việc tạo ra các tác vụ in cho máy in vật lý.

mandatory user profile ***Khái lược Người dùng Bắt buộc*** Một loại khái lược người dùng dạng chỉ đọc, nó không duy trì được các thay đổi khái lược giữa các phiên làm việc. Người dùng có thể thay đổi khái lược của họ, nhưng các thay đổi này sẽ không được lưu lại khi họ đăng xuất.

memory leak ***Rò rỉ bộ nhớ*** Là kết quả của việc các chương trình dành bộ nhớ cho mình để hoạt động nhưng sau đó không giải phóng chúng khi không dùng nũa..

mirrored volume ***Đĩa logic ánh xạ*** Hai đĩa cùng duy trì bản sao giống hệt nhau của dữ liệu. Đây là dạng RAID mềm duy nhất có thể áp dụng trên các ổ hệ thống. Nó cung cấp hiệu năng tốt trong việc đọc và ghi, khả năng chống lỗi rất tốt nhưng giá thành cao do phải dành 50% tổng dung lượng đĩa để lưu các thông tin dự phòng.

network-attached printer ***Máy in cắm trực tiếp vào mạng*** Một loai máy in được cắm trực tiếp vào mạng thay cho cắm vào máy tính. Các máy tính thường giao tiếp với máy in này bằng cách sử dụng địa chỉ IP.

network printer ***Máy in mạng*** trong khái niệm của Windows, Máy in logic trên máy trạm là khách của máy in logic nằm trên máy tính khác đã đươc chia sẻ trên mạng. Máy in logic đã được chia sẻ trên mạng này được gọi là Máy in mạng.

object ***Đối tượng*** Một khối cơ bản của dịc vụ thư mục Active Directory. Các đối tượng là các thành phần ddaij diện cho các tài nguyên như người dùng, máy tính Miền hay nhóm. Mỗi đối tượng có mộttập hợp các thuộc tính chứa các thông tin về bản thân đối tượng. Ví dụ, các thuộc tính của đối tượng người dùng bao gồm tên goi, tên họ, và địa chỉ E-mail của người dùng.

organizational unit (OU) ***Đơn vị Tổ chức*** Một loại đối tượng chứa Active Directory được sử dụng trong nội bộ miền. OU là đối tượng chứa logic trong đó ta có thể bố trí người dùng, máy tính và các OU khác. OU chỉ có thể chứa trong nó các đối tượng ở cùng miền. OU là phạm vi nhỏ nhất bạn có thể áp dụng chính sách nhóm hay ủy quyền quản trị.

OU *Xem* **organizational unit (OU).**

Per Device or Per User licensing mode ***Chế độ giấy phép theo người dùng hay theo thiết bị*** Một yêu cầu giấy phép cho phép trao quyền cho một người dùng (có thể sử dụng nhiều thiết bị) hoặc cho một thiết bị (có thể có nhiều người dùng) được truy cập đến bất cứ sản phẩm máy chủ nào.

performance counter ***Biến đếm Hiệu năng*** một loại báo cão dữ liệu liên quan đến đối tượng hiệu năng.

performance instance ***Trường hợp riêng hiệu năng*** Một sự kiện riêng của biến đếm hiệu năng. Nếu máy chủ có bốn bộ vi xử lí, chúng ta sẽ có bốn trường hợp riêng cho mỗi biến đếm hiệu năng của đối tượng bộ vi xử lí, được đánh số từ 0 đến 3.

performance object ***Đối tượng Hiệu năng*** Một tập hợp logic của các mục dữ liệu báo cáo hoặc các biến đếm liên kết với tài nguyên, dịch vụ hay ứng dụng được theo dõi.

Per Server licensing mode ***Chế độ giấy phép theo máy chủ*** Yêu cầu giấy phép sẽ được cấp khi người dùng hay thiết bị kết nối tới máy chủ hay các sản phẩm máy chủ. Khi người dùng ngắt kết nối, giấy phép lại được trả lại vào nhóm giấy phép có thể cấp, sẵn sàng cấp cho các người dùng hay thiết bị khác. Chế độ này yêu cầu một số lượng giấy phép đủ để hỗ trợ cho số lượng người dùng lớn nhất cùng kết nối tới mỗi máy chủ tại một thời điểm..

Plug and Play (PnP) ***Cắm và Chạy*** Một tiêu chuẩn xác định các đặc tính của các thành phần máy tính cho phép việc tự động phát hiện và cấu hình các thành phần phần cứng này.

PnP *Xem* **Plug and Play (PnP).**

print queue ***Hàng đợi in*** Một danh sách các tác vụ in đang đợi để được chuyển sang máy in vật lý.

print server ***Máy chủ in ấn*** Máy tính được cấu hình để chia sẻ máy in với các máy trạm trên mạng. Máy chủ in ấn sắp xếp

các tác vụ in nó nhận được từ máy khách và lần lượt chuyển các tác vụ này tới máy in vật lý.

RAID-5 volume ***Ổ logic RAID-5*** Ổ đĩa logic trên đó dữ liệu được ghi cùng lúc trên nhiều ổ cứng vật lý (từ 3 đến 32 ổ) với cùng tốc độ kèm theo thông tin chẵn lẻ nhằm cung cấp khả năng chóng lỗi khi ổ logic bị hỏng một ổ đơn. Cấu hình ổ nói trên cung cấp hiệu năng đọc tốt và sử dụng tiết kiệm dung lượng ổ đĩa, nhưng tốc độ ghi không tốt và tiêu tốn tài nguyên bộ vi xử lí nhiều hơn do việc phải tính toán thông tin chẵn lẻ trong quá trình ghi.

roaming user profile ***Khái lược Người dùng Di trú*** Một loại khái lược người dùng dựa trên máy chủ, được lưu trên ổ đĩa chia sẻ trên mạng mà người dùng có thể truy nhập từ bất cứ máy tính nào.

scope pane ***Khung phạm vi*** khung bên trái trong của sổ MMC, hiển thị các snap-in đã được cài đặt trong bảng điều khiển.

security group ***Nhóm Bảo mật*** Một kiểu nhóm Active Directory được sử dụng như các chủ thể bảo mật trong các Danh sách Kiểm sóat Truy nhập (ACL).

security identifier (SID) ***mã nhận dạng bảo mật*** Một giá trị duy nhất được gán cho mỗi đối tượng Active Directory khi chúng được tạo ra.

security principal ***Chủ thể Bảo mật*** Người/Đối tượng sở hữu tai khoản được gán mã nhận dạng bảo mật một cách tự động để có thể truy cập đến các tài nguyên. Chủ thể bảo mật có thể là người dùng, nhóm, máy tính hay dịch vụ

service pack ***Gói dịch vụ*** một tập hợp các miếng vá và các bản cập nhật cho một sản phẩm của Microsoft đã được thử nghiệm cùng nhau và được khuyến cáo cài đặt lên tất cả các máy tính chạy sản phẩm nói trên.

SID *Xem* **security identifier (SID)**.

simple volume ***Ổ logic đơn giản*** Tương dương với khái niệm phân vùng trong đĩa cơ bản. ổ này chỉ nàm trên một ổ cứng vật lý do vậy không có khả năng chịu lỗi.

slipstreaming Quá trình tích hợp các service pack và/hoặc các bản sửa lỗi nóng vào bộ cài đặt hệ điều hành Windows.

snap-in Một module ứng dụng có mục dích đặc biệt dùng để chạy trong các MMC. Có hai loại snap-in, độc lập

(*standalone*) – có thể thêm trực tiếp vào MMC và mở rộng (*extension*) – nhất thiết phải gắn với một Snap-in độc lập.

spanned volume *Ổ logic mở rộng* Một ổ đĩa logic bao gồm các khoảng không gian trên nhiều đĩa cứng. do dung lượng lớn cũng như gồm nhiều đĩa cứng nên loại ổ này rất dễ hỏng và là không chịu lỗi.

special permission *Cấp phép Đặc biệt* thành phần cung cấp cho các chủ thể bảo mật các mức độ truy cập chi tiết hơn đến các tài nguyên.

standard permission *Cấp phép tiêu chuẩn* Một tập hợp các cấp phép xác định được sử dụng để cung cấp cho các chủ thể bảo mật với mức độ sử dụng thường xuyên để truy nhập vào tài nguyên.

striped volume *Ổ logic được chia vạch* Một loại ỏ Logic trong đó dữ liệu được ghi trên nhiều ổ vật lý với cùng tốc độ theo từng khối (*vạch*). Nõ cung cấp một hiệu năng dung lượng tốt nhất so với các loại ổ khác nhưng không có khả năng chịu lỗi.

tree *Cây* Một nhóm các miền Active Directory cũng chia sẻ một khoảng không gian tên liên tục. Ví dụ, sales.microsoft.com và developers.microsoft.com là các miền Active Directory trong cùng một cây.

UNC *Xem* **Universal Naming Convention (UNC).**

Uniform Resource Locator (URL) Một kiểu ký hiệu/đường dẫn chuẩn để đinh vị tài nguyên trên Internet, ví dụ ***http://www.adatum.com*.**

universal group *Nhóm tổng hợp* Một loại phạm vi nhóm thường được sử dụng để truy nhập tới các tài nguyên trên nhiều miền.

Universal Naming Convention (UNC) Một kiểu ký hiệu/đường dẫn chuẩn được sử dụng để truy cập các tài nguyên trên mạng, UNC sử dụng định dạng: **\\TênMáyChủ\TênChiaSẻ**.

URL *Xem* **Uniform Resource Locator (URL)**.

virtual directory *Thư mục ảo* một đối tượng IIS cho phép một thư mục bất kỳ trên máy cục bộ hay các ổ đĩa chia sẻ trên máy khác xuất hiện như là một thư mục con trong Web Site.

volume shadow copy *Sao chép bóng của ổ* một tính năng của Windows Server 2003 và Windows XP duy trì một thư viện bao gồm nhiều phiên bản khác nhau của các file được lựa chọn. Người dùng có thể lựa

chọn một phiên bản nhất định để phục hồi khi cần và các chương trình sao lưu sẽ sử dụng các phiên bản này để sao lưu các file đang mở.