

CHƯƠNG 1. KHÁI QUÁT VỀ QUẢN TRỊ MẠNG

Để hiểu, triển khai và quản trị hệ thống mạng một cách đầy đủ và có tính hệ thống, chương này sẽ trình bày một khung nhìn tổng thể về quy trình, mục tiêu, các hoạt động cụ thể cũng như các mô hình, môi trường và công cụ trong quản trị mạng máy tính. Chương này gồm các nội dung cụ thể sau: *Mục 1.1* trình bày về quy trình và các nội dung quản trị trong hệ thống mạng; *Mục 1.2* trình bày về các mô hình mạng, môi trường và các công cụ quản trị mạng; *Mục 1.3* tổng kết các nội dung trong chương.

1.1. MỤC TIÊU, QUY TRÌNH VÀ CÁC HOẠT ĐỘNG QUẢN TRỊ MẠNG

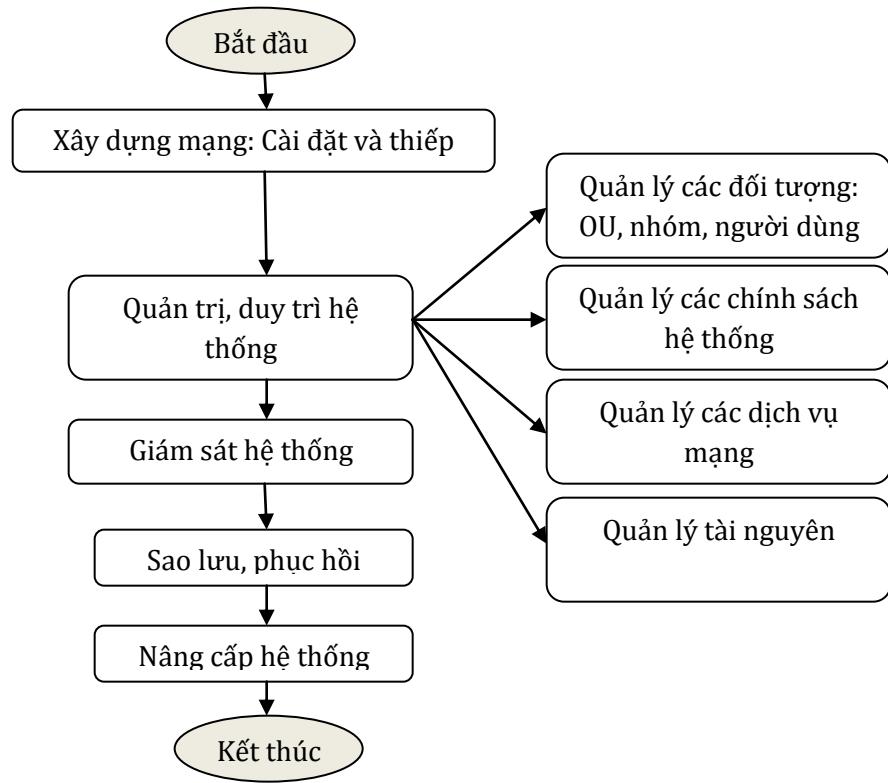
Mục tiêu của việc quản trị mạng là duy trì hoạt động của một hệ thống mạng, đảm bảo hiệu suất làm việc tốt và thuận tiện cho người dùng khi sử dụng. Để đạt được mục tiêu này, người quản trị mạng phải sử dụng kết hợp nhiều kỹ thuật, nhiều sản phẩm phần cứng, nhiều công cụ phần mềm khác nhau để theo dõi sự, quản trị hoạt động của hệ thống mạng tại mọi lúc, trên mọi thiết bị. Các công việc chính của người quản trị mạng bao gồm:

- **Triển khai hệ thống mạng:** Người quản trị phải đặc tả được các yêu cầu của hệ thống mạng mà khách hàng mong muốn và lập kế hoạch triển khai. Sau đó, cần thiết kế hệ thống mạng đáp ứng được các yêu cầu ứng dụng của công ty trong thời điểm hiện tại và trong một tương lai gần. Việc thiết kế hệ thống trước khi triển khai cần một người quản trị có kinh nghiệm từ hạ tầng mạng cho tới các máy chủ phục vụ cho các ứng dụng.
- **Quản trị hay nâng cấp một hệ thống mạng:** Đây là công việc nhiều nhất trong công việc quản trị mạng. Người quản trị phải biết cách nắm bắt toàn bộ hệ

thông một cách chi tiết, có khả năng phán đoán những lỗi xảy ra cho hệ thống. Ngoài ra, việc quản trị cũng cần được ghi chép cẩn thận để làm tài liệu để nghiên cứu, khắc phục nhanh những sự cố đã từng xảy ra. Trên cơ sở đó, người quản trị cần phân tích hệ thống, tổng hợp rồi đưa ra những chính sách quản trị hợp lý.

- **Duy trì hệ thống vận hành ổn định:** Đảm các ứng dụng luôn luôn chạy ổn định là một yêu cầu thiết yếu đối với quản trị mạng. Để khắc phục những sự cố khi xảy ra, người quản trị cần lập những chính sách dự phòng từ nguồn điện, cho tới hệ thống mạng và các ứng dụng cũng như an toàn dữ liệu và phải có chính sách khắc phục và giảm tối thiểu những thiệt hại khi xảy ra sự cố với hệ thống. Một tiêu chí quan trọng trong quản trị mạng là dữ liệu, phải đảm bảo dữ liệu không bị mất mát, không bị truy cập trái phép,v.v.
- **Đảm bảo an toàn và bảo mật trong hệ thống mạng:** Người quản trị cần nắm rõ từng chi tiết của hệ thống, từ đó phân tích từ hạ tầng mạng cho đến lớp ứng dụng, tổng hợp lại hệ thống dựa trên mô hình mạng, mô hình các ứng dụng. Trên cơ sở đó, xây dựng và triển khai những chính sách bảo mật một cách chặt chẽ.

Các công việc xây dựng, triển khai và quản trị mạng nói chung được thực hiện theo quy trình như trong Hình 1.1.



Hình 1.1: Công việc và quy trình quản trị mạng

1.1.1. Các đối tượng quản trị

Đối với một người quản trị thì bước đầu tiên quan trọng nhất trong quy trình quản trị là phải xác định được đối tượng cần quản lý và quyền hạn mà các đối tượng có thể nhận được, nội dung phần này sẽ tóm lược về các đối tượng quản trị như: Người dùng (User), Nhóm (Group), Đơn vị tổ chức (Organization Unit – OU), Máy tính (Computer).

a) Người dùng

Để tham gia vào trong hệ thống người dùng cần phải được hệ thống xác thực. Sau khi xác thực để kiểm tra tính hợp lệ của người dùng, hệ thống sẽ thực hiện thẩm định quyền hạn 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 tài khoản 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. Nội dung phần này chỉ ra cách thức tạo, quản lý và xử lý các tình huống xảy ra đối với tài khoản người dùng. Để tạo và quản trị tốt người dùng trong hệ thống mạng, người quản trị cần:

- 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 thông tin người dùng (User Profile)
- Hiểu được sự khác nhau giữa cục bộ (Local), lan tỏa (Roaming) và mệnh lệnh (Mandatory).
- Xử lý các tình huống đối với việc xác thực người dùng.

b) Nhóm

Một đối tượng quan trọng khác là Nhóm. Sử dụng Nhóm, các quản trị viên có thể đơn giản hóa quá trình cấp phép truy cập cho người dùng. Để có thể quản lý Nhóm tốt, cần nắm rõ các loại nhóm mà Active Directory hỗ trợ, cách thức tạo Nhóm, và các kỹ thuật, kinh nghiệm để sử dụng Nhóm một cách hiệu quả. Cụ thể, người quản trị cần:

- Hiểu được sự khác nhau giữa Nhóm cục bộ (Local Group) và Nhóm miền (Domain Group).
- Nhận biết loại Nhóm (Group type), ba Phạm vi Nhóm (Group Scope) và làm thế nào để sử dụng chúng có hiệu quả.

- Hiểu rõ chức năng của các Nhóm Dựng sẵn (Build-in) và các Nhóm đã định nghĩa (Predefined) trong Microsoft Windows Server.
- Hiểu được các chức năng và cách sử dụng Nhóm.

c) Đơn vị tổ chức

Trong trường hợp miền quá lớn, việc trao quyền điều khiển cho các thành viên gặp khó khăn, rời rạc, cần phân chia và quản lý đồng bộ, bán tự động. cho ai đó. Để giải quyết vấn đề này, Windows Server cung cấp giải pháp phân chia miền thành các đơn vị tổ chức (Organizational Unit – OU). Điều này cho phép tạo ra các biên mới trong miền để dễ quản lý và tăng tính bảo mật.

d) Máy tính

Theo khung nhìn tổng thể, có thể xem hệ thống mạng là một tập hợp các máy tính có kết nối với nhau được sử dụng bởi một tập hợp người dùng – tập người dùng có thể được phân nhóm và quản trị theo OU. Theo đó, cùng với người dùng, Máy tính cũng là một đối tượng quan trọng cần quản lý trong hệ thống. Các máy tính gia nhập mạng nhằm cung cấp môi trường vật lý cho phép người dùng truy cập, khai thác và sử dụng tài nguyên trong hệ thống mạng. Để quản lý toàn bộ các máy tính vật lý kết nối mạng, Active Directory cung cấp các đối tượng Máy tính (Computer). Mỗi đối tượng Máy tính được ánh xạ với một máy tính vật lý. Điều này cho phép người quản trị giám sát, quản trị hoạt động của hệ thống máy tính vật lý thông qua các đối tượng Máy tính. Đối với các đối tượng Máy tính, người quản trị cần:

- Mô tả quá trình đưa thêm máy tính vào miền Active Directory
- Tạo và quản lý đối tượng Máy tính
- Giải quyết sự cố trên đối tượng Máy tính.

1.1.2. Chính sách hệ thống

Người quản trị phải nắm rõ kiến thức về các chính sách hệ thống để giám sát các đối tượng hoạt động trong hệ thống đồng bộ, hiệu quả hơn. Có hai loại chính sách

hệ thống đó là chính sách cục bộ và chính sách nhóm. Các hoạt động quản trị mạng tập trung vào các chính sách nhóm nhiều hơn. Khi làm việc với chính sách nhóm cần chú ý các điểm sau:

- Chính sách nhóm chỉ xuất hiện trên miền Active Directory
- Chính sách nhóm làm được nhiều điều hơn chính sách hệ thống. Chính sách nhóm chứa tất cả các chức năng của chính sách hệ thống và có thể dùng chính sách nhóm để triển khai một phần mềm cho một hoặc nhiều máy tính một cách tự động
- Không giống như các chính sách hệ thống, các chính sách nhóm tự động hủy bỏ tác dụng khi được gỡ bỏ
- Chính sách nhóm được áp dụng thường xuyên hơn chính sách hệ thống. Các chính sách hệ thống chỉ được áp dụng khi máy tính đăng nhập vào mạng. Các chính sách nhóm thì được áp dụng khi máy tính khởi động.
- Có nhiều mức độ để gán chính sách nhóm này cho từng nhóm đối tượng.

1.1.3. Quản lý tài nguyên

Một trong những lý do chính của sự tồn tại mạng máy tính đó là khả năng chia sẻ tài nguyên cho nhiều người sử dụng trên các máy tính khác nhau. Có nhiều loại tài nguyên được quản trị và chia sẻ trong hệ thống mạng như sau: thiết bị chia sẻ như máy in, máy scan, photocopy, v.v.; hệ thống file; hệ thống lưu trữ, sao lưu, phục hồi; phần mềm, dịch vụ, v.v. Trên một mạng nhỏ, chia sẻ tài nguyên thường được thực hiện bởi người sử dụng đầu cuối, tính bảo mật ít được chú ý. Tuy nhiên, trên một hệ thống mạng lớn, mức độ chia sẻ tài nguyên lớn, người quản trị mạng cần đảm bảo tài nguyên chia sẻ phải được bảo vệ theo đúng mức độ sử dụng.

- Tạo/quản lý các tài nguyên chia sẻ
- Phân quyền truy cập NTFS để kiểm soát quá trình truy cập đến tài nguyên

Ngoài ra, người quản trị cũng cần hiểu một cách tường tận về các công cụ hỗ trợ, đảm bảo ổ đĩa cứng hoạt động ổn định và tránh được tình trạng cạn kiệt không gian lưu trữ.

Bên cạnh đó, các ổ đĩa lưu trữ dữ liệu có thể bị hỏng, mất theo các nguyên nhân khác nhau. Để tránh được những rủi ro đó cần phải có một phương thức lưu trữ ,sao lưu dữ liệu phù hợp. Để thực hiện tốt công việc này, người quản trị cần:

- 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
- Sao lưu và khôi phục CSDL của Active Directory
- Sử dụng các bản sao của đĩa.

1.1.4. Giám sát hệ thống

Để đảm bảo hệ thống mạng vận hành tốt, an toàn, bảo mật và tránh được những rủi ro, giám sát hệ thống là hoạt động hết sức quan trọng. Để làm được điều đó người quản trị phải giám sát hiệu năng của máy chủ thường xuyên để có thể kịp thời nhận biết các sự cố có thể ảnh hưởng tới hiệu năng của hệ thống. Giám sát hệ thống gồm các công việc chính sau:

- Sử dụng Event Viewer để giám sát nhật ký hệ thống
- Cấu hình Task Manager để hiển thị các dữ liệu hiệu năng
- Sử dụng Performance Console để giám sát hiệu năng hoạt động của máy tính
- Theo dõi nhật ký các biến đếm và các cảnh báo.

1.2. MÔI TRƯỜNG VÀ CÔNG CỤ QUẢN TRỊ

1.2.1. Các môi trường mạng

Hầu hết các hệ thống mạng của các cơ quan, công ty, doanh nghiệp hiện nay được triển khai theo một trong hai kiểu môi trường là Windows hoặc Unix, Linux:

- Môi trường Unix, Linux với giao diện dòng lệnh (command line), kết hợp giao diện đồ họa
- Môi trường Microsoft Windows với giao diện đồ họa, ngoài ra còn có thể sử dụng các kịch bản có sẵn giống hệ điều hành (HĐH) Linux

Các phiên bản đầu của hệ điều hành Windows được thiết kế cho đơn người dùng trong khi Unix là hệ điều hành đa người dùng. Từ phiên bản Windows 95, hệ điều hành của Microsoft đã hỗ trợ đa người dùng.

Điểm khác biệt của hai họ hệ điều hành này thể hiện ở sự tách biệt giữa giao diện người dùng đồ họa (GUI) và nhân hệ điều hành (kernel). Với HĐH Windows, GUI và kernel không thể tách rời nên tiện dụng cho người dùng. Với HĐH họ Linux, GUI tách biệt hoàn toàn với kernel nên người dùng có thể sử dụng GUI hoặc không, hay sử dụng các GUI khác nhau. Điều này làm cho các HĐH họ Linux có tính tùy biến cao và phù hợp với máy chủ vì không cần GUI nên tiết kiệm bộ nhớ dẫn đến hệ thống ít bị lỗi hơn.

Bên cạnh đó, tất cả những cấu hình của Windows được lưu trong registry, khi người dùng muốn chỉnh sửa thường rất phức tạp hoặc phải sử dụng thêm phần mềm hỗ trợ. Trái lại, cấu hình của Linux thường là các tệp tin văn bản nên người dùng có thể dễ dàng chỉnh sửa hoặc có thể hoàn toàn xóa bỏ khi không cần. Theo đó, đối với HĐH Linux người quản trị không cần một cấu hình chuẩn mà mỗi dịch vụ sẽ được cấu hình riêng, điều này khác biệt hoàn toàn so với Windows.

1.2.2. Các mô hình mạng trong môi trường Microsoft

a) **Mô hình Workgroup**

Workgroup là một mô hình triển khai cụ thể của mô hình mạng peer-to-peer, là mô hình mà trong đó các máy tính có vai trò như nhau được nối kết với nhau. Các dữ liệu và tài nguyên được lưu trữ phân tán tại các máy cục bộ, các máy tự quản lý tài nguyên cục bộ của mình. Trong hệ thống mạng không có máy tính chuyên cung cấp

dịch vụ và quản lý hệ thống mạng. Mô hình này chỉ phù hợp với các mạng nhỏ, với yêu cầu bảo mật không cao.

Trong mô hình mạng này các máy tính sử dụng hệ điều hành đa người dùng; thông tin người dùng được lưu trữ trong một tập tin SAM (Security Accounts Manager) ngay chính trên máy tính cục bộ. Thông tin này bao gồm: tên đăng nhập (username), tên đầy đủ (fullname), mật khẩu (password), v.v. Tất nhiên tập tin SAM này được mã hóa nhằm tránh người dùng khác lấy cắp mật khẩu để tấn công vào máy tính. Do thông tin người dùng được lưu trữ cục bộ trên các máy trạm nên việc xác thực người dùng đăng nhập máy tính cũng do các máy tính này đảm nhận.

b) Mô hình Domain

Khác với mô hình Workgroup, mô hình Domain hoạt động theo cơ chế khách/chủ, trong hệ thống mạng phải có ít nhất một máy tính làm chức năng điều khiển miền (Domain Controller), máy tính này sẽ điều khiển toàn bộ hoạt động của hệ thống mạng. Việc xác thực người dùng và quản lý tài nguyên mạng được tập trung lại tại các máy chủ trong miền.

Trong mô hình Domain, các thông tin người dùng được lưu trữ tập trung trên máy tính điều khiển vùng (domain controller) với tên tập tin là NTDS.DIT do dịch vụ Active Directory quản lý. Tập tin cơ sở dữ liệu này được xây dựng theo công nghệ tương tự như phần mềm Access của Microsoft nên có thể lưu trữ hàng triệu người dùng, cải tiến hơn so với công nghệ cũ chỉ lưu trữ được khoảng 5 nghìn tài khoản người dùng. Do các thông tin người dùng được lưu trữ tập trung nên việc xác thực người dùng đăng nhập vào mạng cũng tập trung và do máy điều khiển vùng xác thực.

1.2.3. Giới thiệu Active Directory

Active Directory được phát triển trên cơ sở cấu trúc miền cũ của NT4 và có bổ sung thêm nhiều điểm cải tiến mới, đây là phần quan trọng nhất và cũng là phần phức tạp nhất của họ HĐH Windows Server, hầu như mọi tính năng của Windows Server

đều đòi hỏi phải có Active Directory. Bởi vậy việc tìm hiểu kỹ về Active Directory phải trải rộng ở hầu hết các tính năng của Windows Server, và phần này chỉ nhằm giới thiệu sơ lược về Active Directory.

a) Vai trò của Active Directory

- **Vấn đề bảo mật**

Bằng cách duy trì một “danh bạ” về các người sử dụng và những đối tượng khác của mạng, Active Directory theo dõi thông tin người dùng truy xuất và sử dụng tài nguyên mạng dựa trên cơ chế xác thực và thẩm định để cấp phép quyền sử dụng tài nguyên cho người sử dụng.

- **Vấn đề tìm kiếm thông tin trên mạng**

Ngày nay, mô hình Khách - chủ đã trở thành mẫu mực để giải quyết nhu cầu tìm kiếm thông tin. Nhưng cấu trúc này sẽ không có tác dụng nếu không giúp máy khách tìm ra máy chủ. Chức năng tra cứu thông tin của Active Directory giúp các máy khách tìm kiếm nhanh đến tên của một máy chủ mail, máy chủ Web hay một máy chủ File, v.v.

- **Sự phân chia quyền hành trên một miền**

Dưới NT 4, để có sự phân quyền và bảo mật cho các bộ phận khác nhau trên một mạng thì cần phải tổ chức mạng sao cho mỗi một bộ phận thành một miền, mà mỗi miền phải tồn tại ít nhất một máy chủ là máy điều khiển miền chính (Primary Domain Controller - PDC). Sau đó nếu các bộ phận muốn trao đổi thông tin liên lạc với nhau ở mức nào đó, thì phải thiết lập các mối quan hệ ủy quyền (Trust relationship), mà việc thiết lập các quan hệ ủy quyền trong NT 4 có phần phức tạp và không thực sự tin cậy.

Với Active Directory của Windows Server, chỉ cần dùng chung một miền cũng có thể phân quyền và bảo mật cho các bộ phận khác nhau, bằng cách chia miền đó thành các đơn vị tổ chức (Organizational Unit – OU) cho mỗi bộ phận khác nhau. Sau đó có thể uỷ quyền kiểm soát các OU đó cho một nhóm điều hành nào đó.

b) Cấu trúc của Active Directory

Khi thiết kế cấu trúc của mạng NT4, chỉ có một vài công cụ như: các miền (domain), tài khoản máy (machine account), nhóm (group) mối quan hệ uỷ quyền (trust relationship). Còn khi thiết kế mạng Windows Server, ngoài tất cả các công cụ trên, còn có các công cụ khác nữa là: đơn vị tổ chức (unit organization), cây (tree), rừng (forest), và địa bàn (site).

- **Miền (Domain)**

Miền là một tập hợp các máy tính trong mạng cho phép quản trị cũng như bảo mật một cách tập trung. Một miền có chứa máy chủ và các máy trạm làm việc của miền. Các máy chủ của miền được chia thành hai loại như sau:

Máy điều khiển miền (DC - Domain Controller)

Mỗi một miền phải có ít nhất một máy chủ điều khiển miền gọi là DC (Domain Controller - DC), để duy trì cơ sở dữ liệu (CSDL) khoán mục của miền (trong đó có những khoán mục chính là: tài khoản người sử dụng, tài khoản nhóm và tài khoản máy). Bất kỳ máy chủ khác nào có lưu giữ một bản sao CSDL khoán mục của miền cũng đều được gọi là DC, những máy chủ này có nhiệm vụ phân tải sự truy nhập vào CSDL khoán mục của miền.

Máy chủ (Server)

Là những máy chủ khác của miền, dùng để cung cấp các dịch vụ như: dịch vụ tệp, dịch vụ in, v.v. Các máy chủ này không được cập nhật thông tin về CSDL khoán

mục của miền, do vậy không thể cân bằng tải và điều khiển miền trong trường hợp xảy ra sự cố.

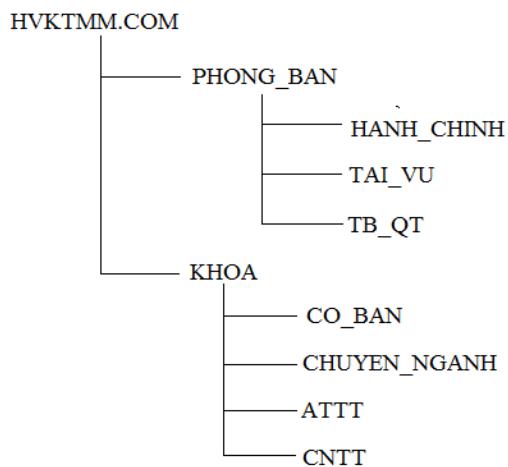
- **Đơn vị tổ chức (OU)**

Mỗi OU thường chứa các tài khoản người dùng, tài khoản nhóm, hoặc tài khoản máy của miền, các tài khoản này là duy nhất trên mạng và chỉ được xuất hiện nhiều nhất là trong một OU.

Công dụng chính của OU là để tập hợp các tài khoản người dùng và tài khoản máy vào một nơi (trong một OU), sau đó có thể trao quyền kiểm soát OU này cho một người hoặc một tập hợp người quản trị. Điều này cho phép quy định một nhóm điều hành viên có khả năng, chẳng hạn như, định lại mật khẩu của một bộ phận nào đó, mà không cần biến họ thành những quản trị viên có những quyền lực lớn hơn mức mong muốn. Nhờ vậy mà xác định được rõ hơn về sơ đồ tổ chức, và thiết lập các biện pháp an toàn trong miền.

Trong một OU lại có thể tạo ra các OU con của nó.

Ví dụ: Hình 1.2 dưới đây minh họa các OU được tạo ra trong miền HVKTMM.COM:



Hình 1.2: **Cấu trúc các OU trong miền HVKTMM.COM**

- **Địa bàn (Site)**

Với Active Directory, ngoài việc nắm những thông tin về máy và người dùng trong một mạng, nó còn theo dõi cả khía cạnh địa lý của mạng.

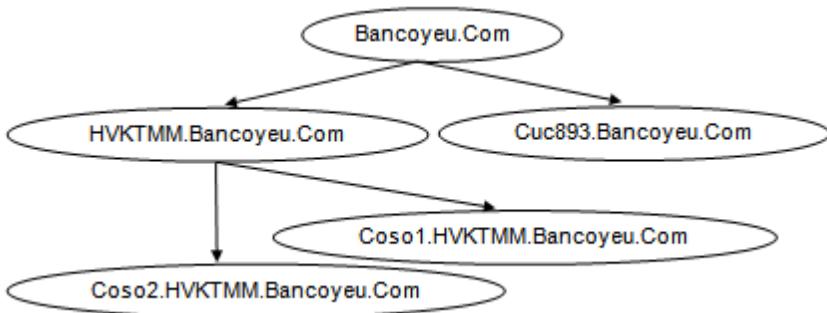
Mỗi khu vực mà được nối kết bằng một mạng LAN thì được gọi là một Site. Windows Server dùng những thông tin chi tiết về cách bố trí vật lý của mạng mà ta cung cấp cho để tính ra nơi nào có những đường liên kết WAN chậm và chi phí cao. Sau đó nó làm hai việc rất có ích sau: Thứ nhất, nó nén những dữ liệu cần sao chép trước khi gửi đi, và thứ hai, nó dùng những thông tin chi phí định tuyến (route costing information) để xác định cách gửi chuyển tiếp tốt nhất những dữ liệu cần sao chép đó với chi phí thấp nhất.

Mỗi một Site thông thường cần một máy DC để thuận tiện cho các cuộc đăng nhập tại địa bàn đó. Một miền cũng có thể có nhiều Site và một Site lại có thể chứa nhiều miền.

- **Cây của các miền (Tree of domains)**

Các doanh nghiệp có mạng đa miền đều mong muốn xây dựng hệ thống cấp bậc theo cấu trúc cây cho các miền. Microsoft đã thiết kế Windows Server sao cho nó dùng DNS làm hệ thống giải đáp tên, và DNS được thiết kế đã có bản chất cấu trúc cây, cho nên Windows Server khai thác sự trùng hợp này và khuyến khích thành lập các mạng đa miền dưới dạng có cấp bậc.

Ví dụ: Một mạng gồm năm miền có cấu trúc như minh họa trong Hình 1.3 sau:



Hình 1.3: Cấu trúc cây của các miền

Miền đầu tiên được tạo ra trong một mạng đa miền được gọi là gốc (root) của cây. Trong ví dụ trên, gốc của cây là *Bancoyeu.Com*. Ở đây cũng có tên gọi cha, con như cấu trúc phân cấp cây thư mục của DOS. Các miền ở mức trên được gọi là miền cha của các miền ở mức ngay dưới nó, Các miền ở mức ngay dưới được gọi là miền con của miền ngay bên trên nó.

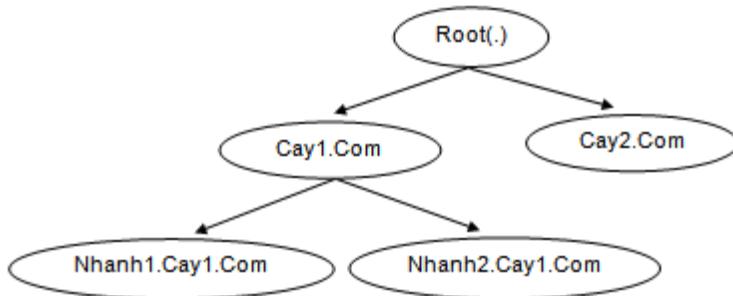
Khi các miền được tổ chức theo cấu trúc cây, Windows Server sẽ tự động tạo ra các quan hệ uỷ quyền giữa miền cha và các miền con. Ví dụ, khi tạo ra miền con *HVKTMM.Bancoyeu.Com*, thì tự động sẽ có một mối quan hệ uỷ quyền hai chiều giữa *Bancoyeu.Com* và *HVKTMM.Bancoyeu.Com*. Mỗi quan hệ uỷ quyền hai chiều này có nghĩa là: các quản trị viên của miền *Bancoyeu.Com* có thể quyết định mở rộng những quyền truy cập tập tin và máy in trong miền của họ cho những người dùng của miền *HVKTMM.Bancoyeu.Com* và ngược lại.

Ngoài ra, với Windows Server, các mối quan hệ uỷ quyền còn có tính bắc cầu. Điều đó dẫn tới tất cả các miền trong một cây đều có quan hệ uỷ quyền hai chiều với nhau.

Như vậy, cây của các miền đem lại lợi điểm là tự động tạo ra các quan hệ uỷ quyền. Nhưng tất cả các tên miền phải được đặt theo hệ thống cấp bậc chính xác tương tự như ví dụ trên thì mới hình thành được một cây của Windows Server.

- **Rừng của các miền (Forest of domains)**

Rừng là tập hợp của hai hay nhiều cây. Các cây thường được nối qua tuyến truyền thông. Hình 1.4 là một ví dụ về một rừng có hai cây.



Hình 1.4: Rừng của các cây

Windows Server đòi hỏi phải có một miền làm gốc của rừng, và miền đầu tiên được tạo ra sẽ là miền gốc của rừng.

Các quan hệ uỷ quyền giữa các miền thuộc hai cây khác nhau trong một rừng không được tự động tạo ra, mà phải xác lập bằng tay.

Chú ý: Với Windows Server, ta không thể nối hai miền có sẵn vào trong một cây, và cũng không thể ghép một cây có sẵn vào trong một rừng, mà cách duy nhất để đưa thêm một miền vào trong một cây, hoặc một cây vào trong một rừng, là xây dựng nó từ đầu trên một cây hoặc rừng có sẵn.

1.2.4. Các công cụ quản trị

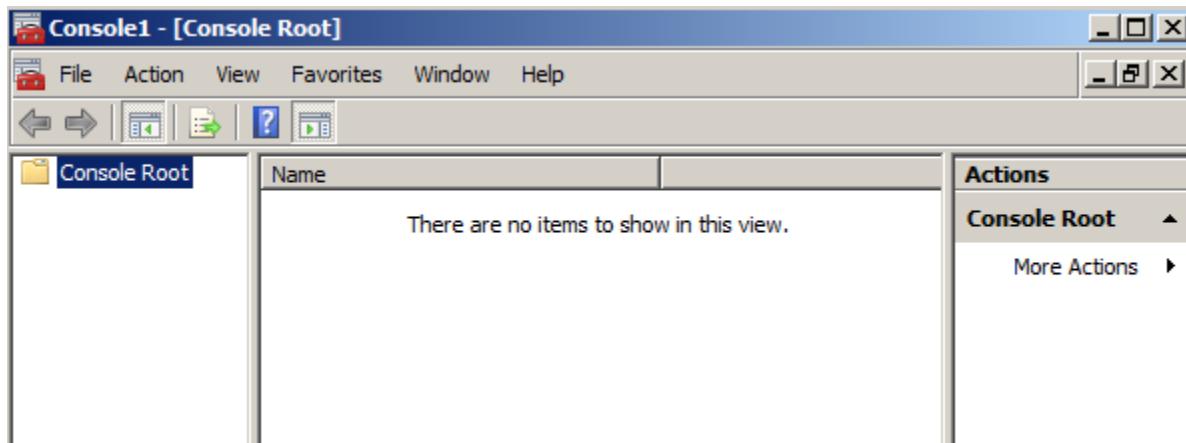
a) **Bảng quản trị Microsoft (MMC - Microsoft Management Console)**

MMC là một bộ khung dành cho các công cụ quản trị mạng Windows Server, bộ khung này đưa ra một giao diện thống nhất cho các công cụ của Microsoft và các hãng khác. MMC không thay thế các ứng dụng quản trị; nó chỉ tích hợp chúng vào trong một giao diện duy nhất mà thôi. Không có một chức năng có sẵn nào trong MMC, mà chỉ sử dụng các công cụ thành phần sẵn có gọi là **Snap-in** (công cụ ghép thêm) để

thực hiện tất cả mọi việc. MMC chỉ cung cấp một giao diện người dùng, nó không thay đổi gì đối với cách làm việc của các **Snap-in**.

- **Xây dựng một MMC đơn giản**

Trước hết mở một MMC trống trong chế độ Author mode, bằng cách thực hiện chương trình MMC.EXE từ hộp thoại Run (chọn Start/Run) để hiện ra cửa sổ như Hình 1.5.



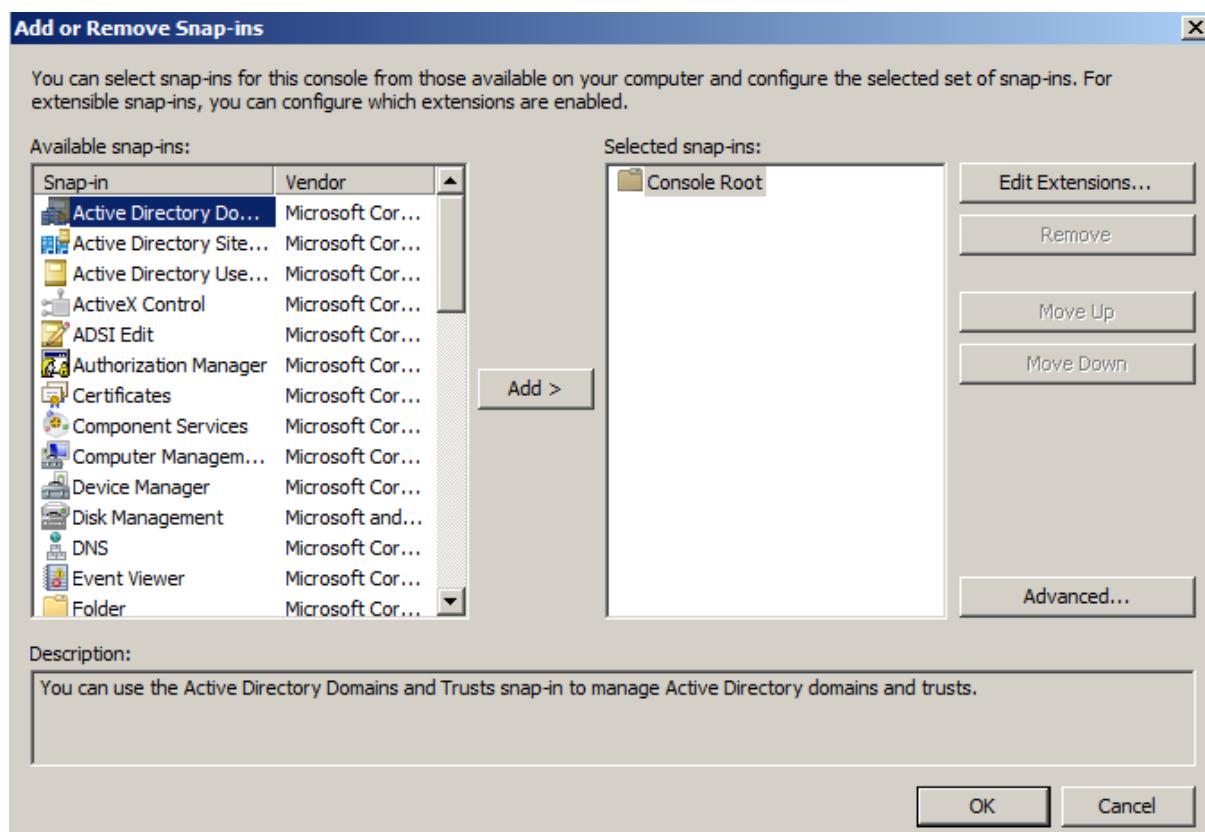
Hình 1.5: Cửa sổ MMC trống

Từ đây ta có mở các file .MSC có sẵn (cũng giống như cách mở các file .DOC của Word) để thêm vào các Snap-in, bằng cách chọn Console/Open từ cửa sổ MMC chính.

Giả sử ta cần có một công cụ để quản lý và giải quyết những trực trắc về phần cứng. Để tạo nó ta thực hiện các bước sau:

1. Đổi tên Console Root thành Hardware Tools, như cách đổi tên một thư mục.
2. Bây giờ ta có thể đưa vào các Snap-in ngay bên dưới Hardware Tools, nhưng nếu muốn gom các Snap-in vào thành từng nhóm để dễ tìm kiếm và thao tác, ta tạo thêm hai thư mục bên dưới Hardware Tools là: Disk Tools và Other Tools bằng cách sau:

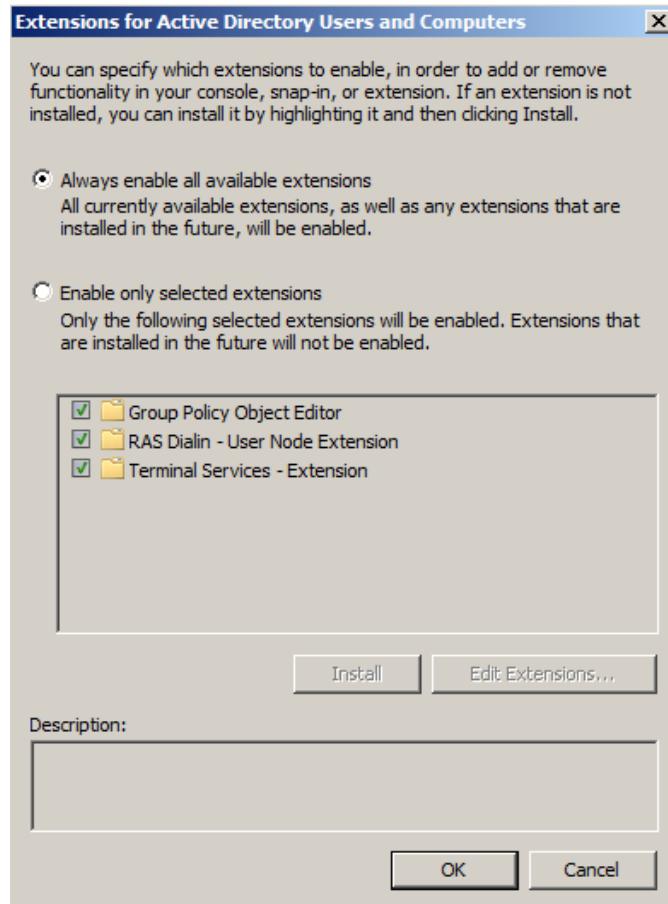
- Chọn **Console/Add/Remove Snap-in** từ cửa sổ MMC chính để hiện ra cửa sổ như Hình 1.6.



Hình 1.6:Cửa sổ thêm/loại bỏ các Snap-in hoặc thư mục

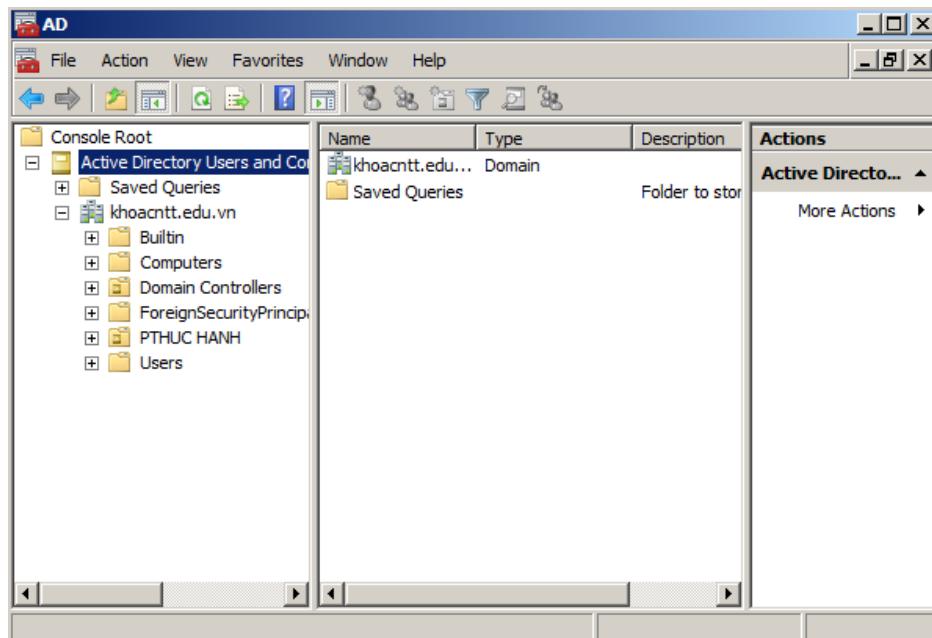
Trong đó ý nghĩa của các mục như sau:

- + **Available Snap-ins:** để chọn nơi đưa Snap-ins hoặc các thư mục con vào.
- + **Add:** để chọn Snap-ins hoặc thư mục mới cần đưa vào
- + **Remove:** để loại bỏ Snap-ins hoặc thư mục đã được đưa vào
- + **Edit Extensions:** để xem/chọn/bỏ chọn các extension (phần mở rộng) vào Snap-in. chọn lựa Always enable all available extensions cho phép chọn tất cả các extension của snap-in được chọn. Nếu chỉ muốn chọn một số extension cho snap-in thì ta chọn enable only selected extensions và tích vào những Snap-ins cần chọn như minh họa trong Hình 1.7.



Hình 1.7: **Lựa chọn chỉnh sửa phần mở rộng**

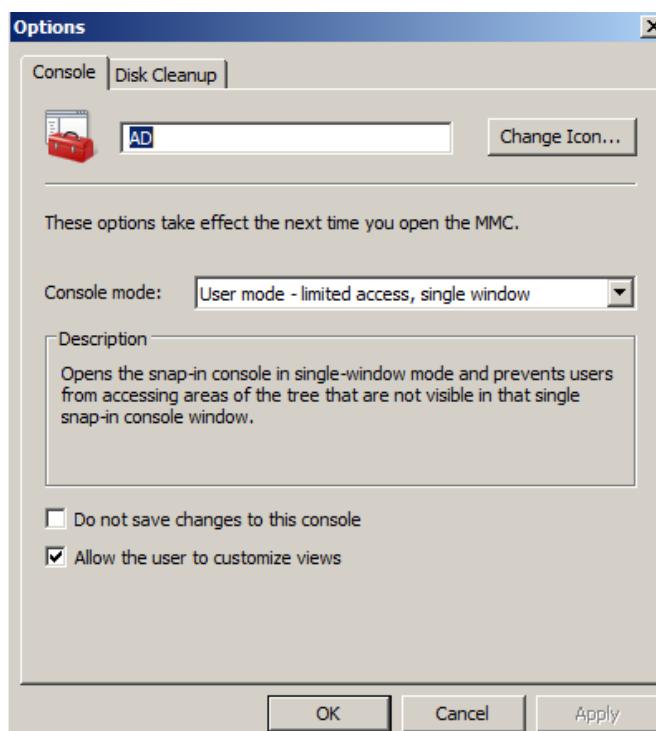
Kết quả cuối cùng của console này được thể hiện trên Hình 1.8



Hình 1.8: Cửa sổ console sau khi hoàn tất

- **Hoàn chỉnh MMC**

Từ cửa sổ Hình 1.8, chọn Console/Options để hiện ra cửa sổ như Hình 1.9.



Hình 1.9: Cửa sổ console Hardware sau khi hoàn tất

Tại đây ta có thể đổi tên MMC từ *Console1* thành *AD* (đây không phải là tên file). Nếu muốn đổi biểu tượng khác thì nhấn chuột tại nút Change icon. Tên và biểu tượng này sẽ được hiện trên thanh tiêu đề.

Mục *Console mode* dùng để chọn chế độ cho Console là *Author mode* hoặc *User mode*, ở đây ta chọn *User mode*.

Chú ý: Một console đang ở chế độ Console mode có thể mở ở chế độ Author mode để chỉnh sửa lại bằng cách thêm tùy chọn /a vào cuối tên file console khi được gọi thực hiện từ hộp thoại Run, ví dụ: quan_tri.msc /a, hoặc mở nó từ cửa sổ MMC chính, bằng cách chọn Console/Open.

b) Sử dụng Remote Desktop Connection (RDC)

Đây là công cụ cho phép kết nối với máy tính khác trong hoặc ngoài mạng dựa trên địa chỉ IP. Để khởi tạo công cụ trên ta vào **Start/Run** gõ **mstsc** và kết nối như minh họa trong Hình 1.10.



Hình 1.10: Kết nối quản trị từ xa

1.3. TỔNG KẾT CHƯƠNG

Hệ thống mạng đóng vai trò quan trọng trong việc điều hành, tác nghiệp góp phần nâng cao hiệu quả trong quản lý cũng như giảm bớt chi phí, và chuyên

nghiệp hóa môi trường làm việc trong mỗi cơ quan, tổ chức. Quy trình xây dựng và quản trị hệ thống mạng gồm nhiều giai đoạn như: khảo sát, phân tích, thiết kế, cài đặt triển khai, quản trị, nâng cấp hệ thống. Để xây dựng và vận hành một hệ thống mạng tốt, người quản trị cần nắm vững mục tiêu, quy trình và các hoạt động trong quản trị hệ thống mạng.

Mục tiêu của quản trị mạng nhằm duy trì hệ thống mạng hoạt động ổn định, an toàn, đạt hiệu suất tốt và tiện dụng cho người sử dụng. Để đạt được mục tiêu này, các nhóm chức năng chính mà người quản trị phải nắm được bao gồm: quản lý hiệu năng, quản lý cấu hình, quản lý lỗi, quản lý kiểm toán, quản lý vấn đề an toàn và bảo mật. Các nhóm chức năng này được tập trung trong các hoạt động chính là: triển khai hệ thống mạng, quản trị và nâng cấp hệ thống, vận hành hệ thống ổn định và đảm bảo an toàn.

Các hoạt động quản trị mạng được triển khai trên các đối tượng quản trị bao gồm: Người dùng, nhóm, đơn vị tổ chức và đối tượng máy tính. Để triển khai các hoạt động quản trị mạng hiệu quả, cần phân chia miền thành các đơn vị tổ chức, xây dựng các chính sách và áp dụng các chính sách phù hợp và đồng bộ. Các chính sách hệ thống được chia thành hai loại chính là chính sách cục bộ và chính sách nhóm. Các chính sách nhóm được sử dụng phổ biến và ưu việt hơn khi áp dụng trên toàn miền hoặc trên các OU cụ thể.

Quản lý tài nguyên cũng là một hoạt động quan trọng trong quản trị mạng. Vấn đề chia sẻ tài nguyên là một trong những khởi nguồn dẫn đến sự ra đời của hệ thống mạng. Các tài nguyên được khai thác và chia sẻ trong hệ thống mạng được phân nhóm theo các thiết bị chia sẻ, hệ thống phần mềm và dịch vụ, hệ thống tệp tin mạng, thiết bị lưu trữ chia sẻ, v.v.

Giám sát hệ thống là hoạt động không thể thiếu trong quản trị mạng, phục vụ cho nhiều chức năng như: đảm bảo hiệu năng, đảm bảo an toàn và bảo mật dữ liệu, an ninh mạng, theo vết và giám sát hoạt động người dùng, v.v.

Các môi trường triển khai hệ thống mạng được phân thành hai nhóm chính là môi trường Windows và môi trường Unix/ Linux tùy theo hệ điều hành được cài đặt trên máy điều khiển miền.

Các mô hình mạng triển khai thực tế trong môi trường Windows Server cũng được phân thành hai loại chính. Mô hình Workgroup là một mô hình thực tế của mạng ngang hành (Peer to Peer); mỗi máy trong mạng vừa đóng vai trò máy khách vừa đóng vai trò máy chủ; dữ liệu được lưu trữ phân tán tại mỗi máy; khả năng bảo mật kém; được dùng cho các mạng nhỏ. Mô hình Domain (miền) là mô hình khách – chủ; thông tin về hệ thống mạng cũng như thông tin tài khoản người dùng, nhóm, OU, v.v. được lưu trữ tập trung trong máy chủ điều khiển miền trong cơ sở dữ liệu Active Directory; tính năng bảo mật tốt hơn mô hình Workgroup; được dùng cho các mạng lớn.

Các công cụ quản trị mạng thường được sử dụng là MMC và công cụ truy xuất, quản trị từ xa (RDC). MMC hoạt động như một bảng điều khiển được gắn các công cụ quản trị mạng để quản lý tập trung và tiện dụng. RDC cho phép kết nối và quản trị dựa trên địa chỉ IP.

CHƯƠNG 2. CÀI ĐẶT VÀ THIẾT LẬP MẠNG WINDOWS

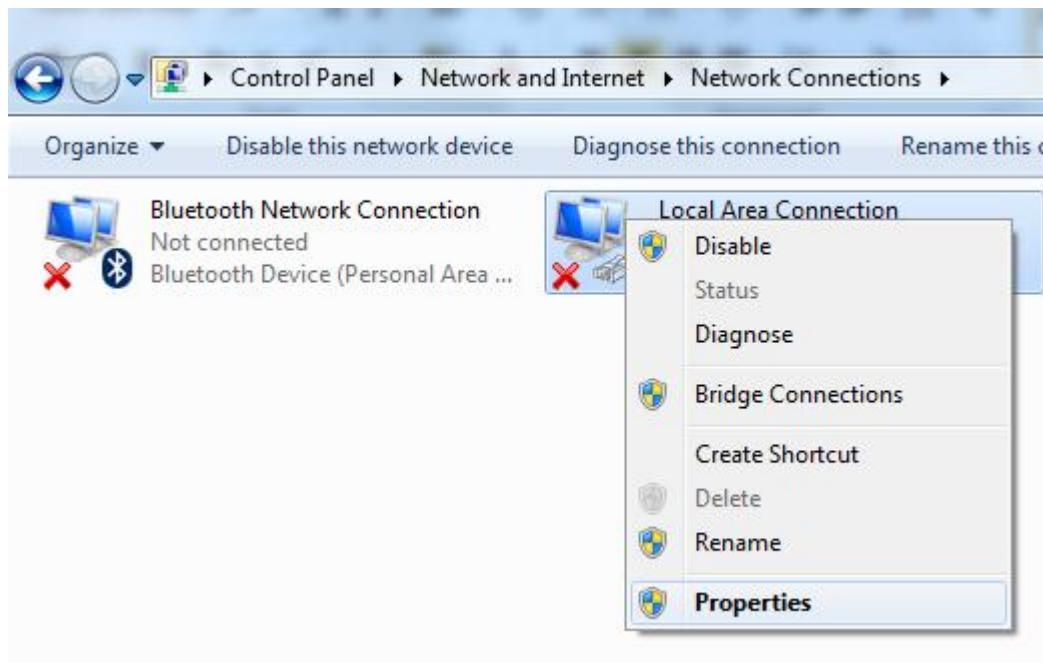
Trước khi tiến hành các hoạt động giám sát, quản trị, cần phải xây dựng hệ thống mạng máy tính. Chương này nhằm cung cấp cho độc giả kiến thức lý thuyết và thực hành để triển khai hệ thống mạng Windows trên cả máy trạm và máy chủ cho cả mô hình mạng ngang hàng và mạng khách/chủ. Nội dung chương được bố cục như sau: *Mục 2.1* trình bày vấn đề cài đặt và thiết lập mạng ngang hàng; *Mục 2.2* trình bày vấn đề xây dựng mạng khách/ chủ; *Mục 2.3* tổng kết các nội dung của chương.

2.1. THIẾT LẬP MẠNG NGANG HÀNG

2.1.1. Thiết lập cấu hình TCP/IP

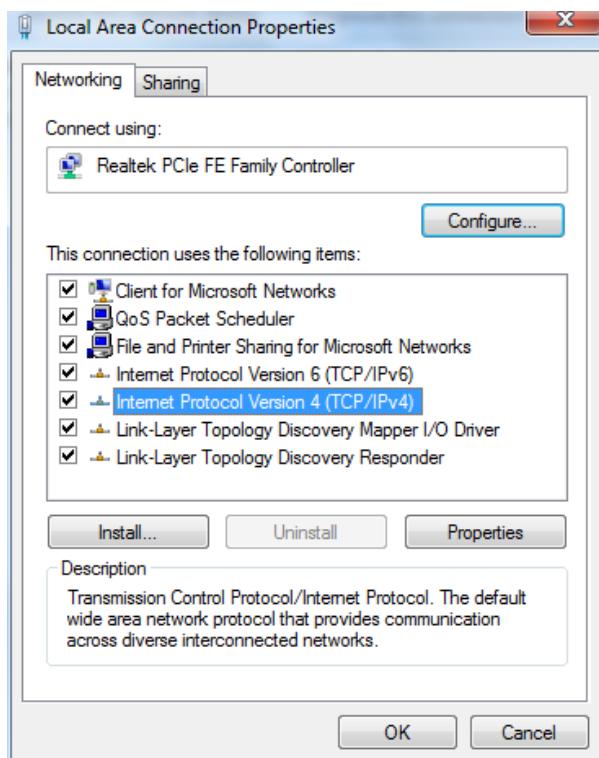
Bước 1. Nhấn chuột phải lên **My Network Places** và chọn **Properties**.

Bước 2. Trên NIC thường có nhãn là **Local Area Connection** - nhấn chuột phải lên đó và chọn **Properties** như trong Hình 2.1.



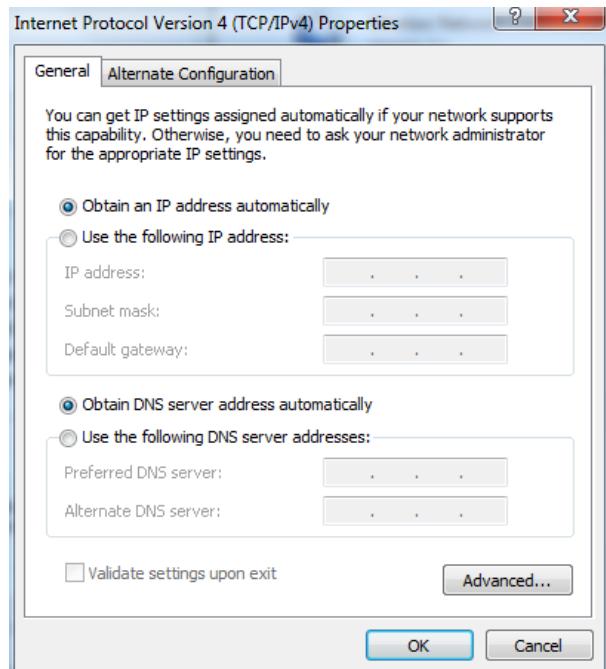
Hình 2.1: **Lựa chọn kết nối mạng để cấu hình**

Bước 3. Chọn **TCP/IP** (Hãy chắc chắn rằng không bỏ dấu chọn ở đây) và nhấn nút **Properties** như Hình 2.2.



Hình 2.2: Lựa chọn giao thức TCP/IP

Bước 4. Chọn **Obtain an IP address automatically** nếu muốn để IP động. Chọn **Use the following IP address** nếu muốn sử dụng IP tĩnh (Hình 2.3)



Hình 2.3: Cấu hình địa chỉ IP

Kiểm tra cấu hình TCP/IP

Kiểm tra thiết đặt của mình bằng cách chạy lệnh: ipconfig/all tại cửa sổ cmd (Hình 2.4):

```

Select Command Prompt
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\Administrator>ipconfig /all

Windows IP Configuration

Host Name . . . . . : xppro1
Primary Dns Suffix . . . . . :
Node Type . . . . . : Unknown
IP Routing Enabled. . . . . : No
WINS Proxy Enabled. . . . . : No

Ethernet adapter Local Area Connection:

        Connection-specific DNS Suffix . . . . . : dptri.net
        Description . . . . . : Intel 21140-Based PCI Fast Ethernet
Adapter (Generic)
        Physical Address. . . . . . . . . . . : 00-03-FF-21-BA-5C
        Dhcp Enabled. . . . . : Yes
        Autoconfiguration Enabled . . . . . : Yes
        IP Address. . . . . . . . . . . . . . . . . : 192.168.0.120
        Subnet Mask . . . . . . . . . . . . . . . . . : 255.255.255.0
        Default Gateway . . . . . . . . . . . . . . . . . : 192.168.0.1
        DHCP Server . . . . . . . . . . . . . . . . . : 192.168.0.200
        DNS Servers . . . . . . . . . . . . . . . . . : 192.168.0.200
        Lease Obtained. . . . . . . . . . . . . . . . . : Friday, January 23, 2004 11:31:26 AM
        Lease Expires . . . . . . . . . . . . . . . . . : Saturday, January 31, 2004 11:31:26
AM

```

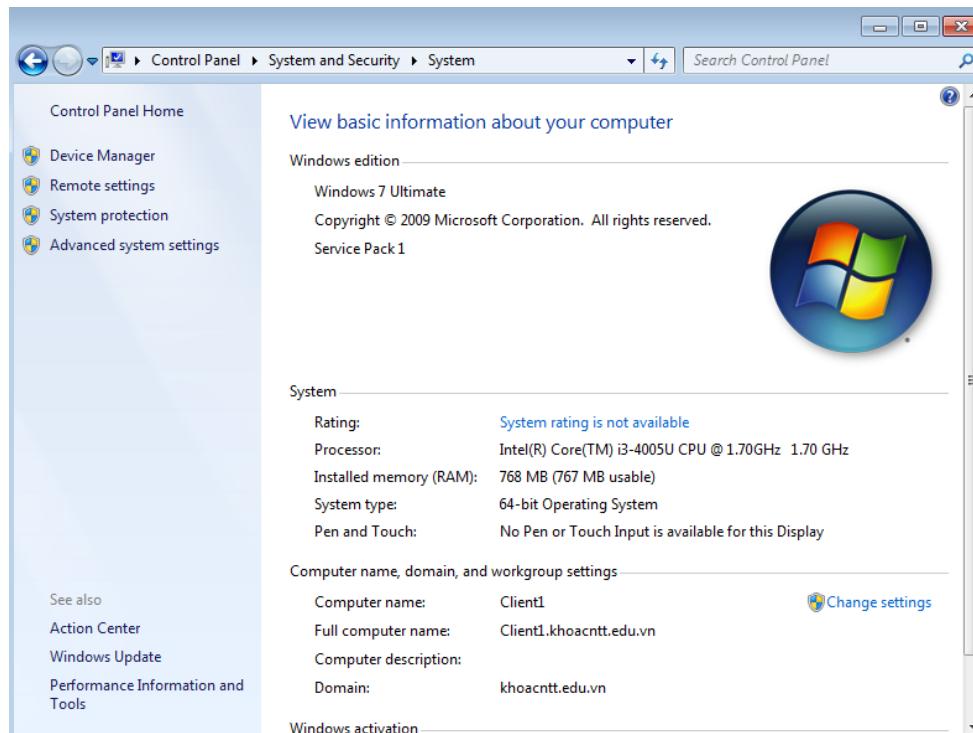
Hình 2.4: Kiểm tra cấu hình IP

2.1.2. Xây dựng Workgroup

Nhóm làm việc(Workgroup) được sử dụng cho các mạng nhỏ, trong đó mỗi máy tính được thiết lập riêng với các quy tắc riêng của mình. Nhóm được sử dụng chủ yếu cho mạng trong một gia đình hoặc mạng doanh nghiệp nhỏ. Để truy cập vào một máy tính từ các nhóm làm việc, cần phải có một tài khoản người dùng được xác định trên máy tính đó. Trong trường hợp này, người dùng có tài khoản trong miền cũng không thể sử dụng được trên tất cả các máy tính trong mạng.

Truy cập Workgroup trong Windows 7

Để xem tên nhóm làm việc trên cả máy tính chạy Windows 7 truy cập vào **Control Panel\System and Security\System**(Hình 2.5).



Hình 2.5: Xem thông tin Workgroup

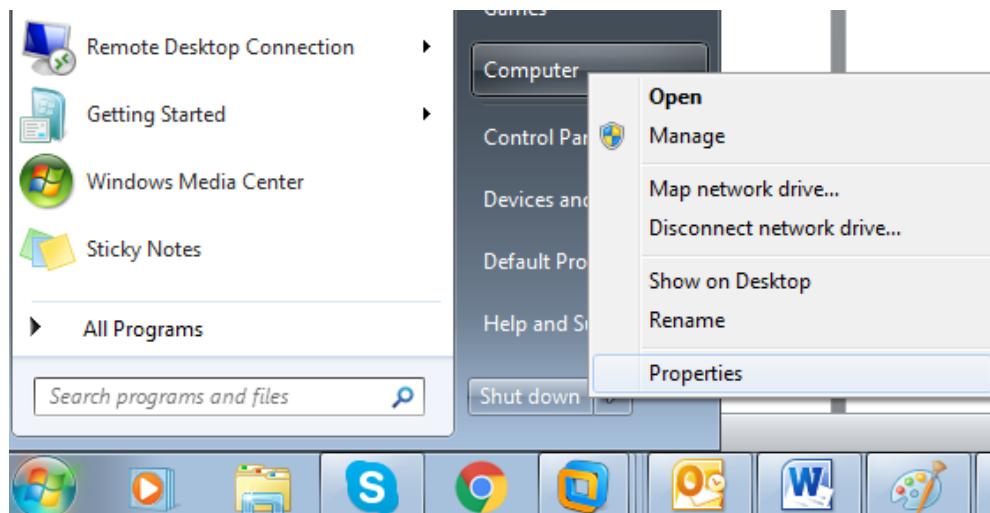
Ngoài ra, có thể sử dụng công cụ tìm kiếm. Trên màn hình Start của Windows 7, nhập từ khoá workgroup vào khung Search, rồi chọn chức năng mong muốn trong mục **Settings**. Minh họa trong Hình 2.6.

Control Panel (17)

-  Change workgroup name
-  Show which workgroup this computer is on
-  Change how your keyboard works
-  Change how your mouse works

Hình 2.6: Tìm kiếm thiết lập workgroup trên Windows 8

Hoặc trong Windows 7, truy cập vào **Start Menu** sau đó kích chuột phải vào Computer chọn Prooerties (Hình 2.7)..



Hình 2.7: Tìm kiếm thiết lập workgroup trên Windows 7

Thay đổi Workgroup trong Windows 7

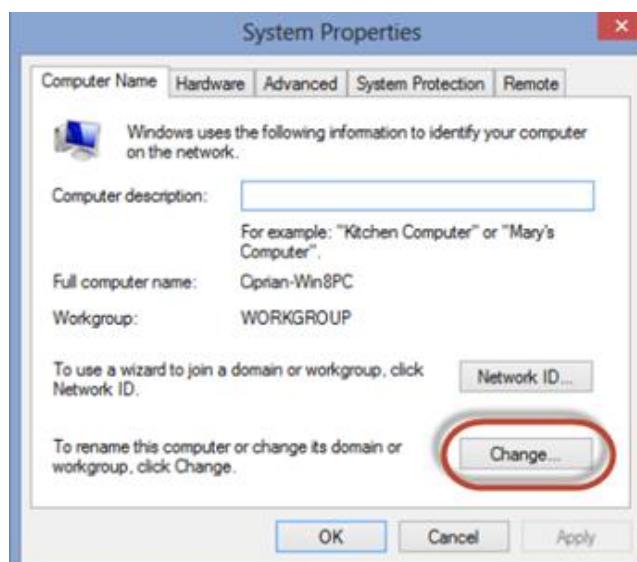
Để thay đổi nhóm làm việc hiện tại. Trong cửa sổ System, chọn **Change settings** bên phải mục **Computer name**(Hình 2.8).

Computer name, domain, and workgroup settings

Computer name:	Ciprian-Win8PC	 Change settings
Full computer name:	Ciprian-Win8PC	
Computer description:		
Workgroup:	WORKGROUP	

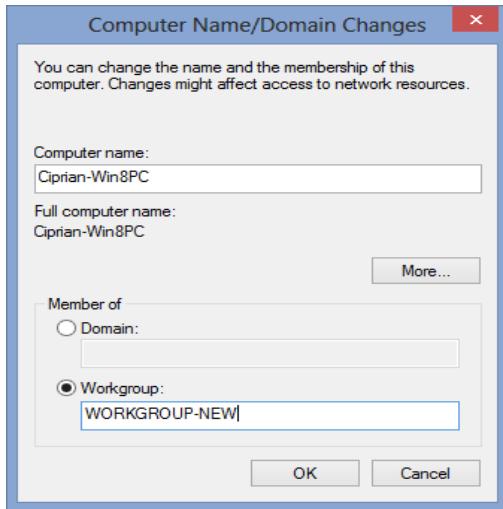
Hình 2.8: Lựa chọn thay đổi các thiết lập cho workgroup

Trong cửa sổ **System Properties** mở ra, chọn thẻ **Computer Name** sau đó chọn **Change** như trong Hình 2.9.



Hình 2.9: Thay đổi Workgroup

Cửa sổ **Computer Name/Domain Changes** hiển thị, tại mục **Workgroup** nhập tên của nhóm muốn tham gia và chọn **OK** như trong Hình 2.10. Sau đó, một hộp thoại thông báo về thay đổi nhóm đã thực hiện, chọn **OK**.



Hình 2.10: Thiết lập Workgroup mới

Sau khi máy tính được khởi động lại, máy tính sẽ được tham gia vào nhóm làm việc vừa đổi tên, từ đó có thể tương tác với các máy tính khác trong mạng và trở thành một phần của nhóm để có thể làm việc cùng.

2.2. CÀI ĐẶT VÀ THIẾT LẬP MẠNG KHÁCH/CHỦ

2.2.1. Cài đặt máy chủ

Để triển khai hệ thống mạng trong môi trường Windows cần cài đặt Windows Server trên máy chủ. Phần này trình bày về cài đặt Windows Server. Các nội dung cài đặt được trình bày chi tiết trong **Phụ lục B**. Tuy nhiên, trước khi cài đặt, người quản trị cần nắm được các yêu cầu phần cứng khi cài đặt cũng như các tính năng của từng phiên bản Windows Server để có lựa chọn hợp lý. Hình 2.11 chỉ ra yêu cầu phần cứng và Hình 2.12 mô tả các tính năng tương ứng với mỗi phiên bản.

Thành phần	Yêu cầu
Bộ xử lý	Tối thiểu: 1 GHz (bộ xử lý x86) hoặc 1.4 GHz (bộ xử lý x64) Khuyên nghị: Tốc độ xử lý 2 GHz hoặc nhanh hơn Chú ý: Cân bộ xử lý Intel Itanium 2 cho Windows Server đối với các Hệ thống dựa trên kiến trúc Itanium.
Bộ nhớ	Tối thiểu: RAM 512 MB Khuyên nghị: RAM 2 GB hoặc lớn hơn Tối ưu: RAM 2 GB (Cài đặt toàn bộ) or RAM 1 GB (Cài Server Core) hoặc hơn Tối đa (hệ thống 32 bit): 4 GB (Bản Standard) hoặc 64 GB (Bản Enterprise và Datacenter) Tối đa (các hệ thống 64 bit): 32 GB (Bản Standard) hoặc 2 TB (Bản Enterprise, Datacenter, và Các hệ thống dựa trên kiến trúc Itanium)
Không gian ổ đĩa còn trống	Tối thiểu: 10 GB Khuyên nghị : 40 GB hoặc lớn hơn Chú ý: Các máy tính có RAM lớn hơn 16 GB sẽ cần nhiều không gian ổ đĩa trống hơn dành cho paging, hibernation, and dump files
Ổ đĩa	Ổ DVD-ROM
Màn hình	Super VGA (800×600) hoặc màn hình có độ phân giải cao hơn
Thành phần khác	Bàn phím, Chuột của Microsoft hoặc thiết bị trò tương thích

Hình 2.11: Các yêu cầu phần cứng cho Windows Server 2008

Feature	Enterprise	Datacenter	Standard	Web	Itanium
ADFS Web Agent	Yes	Yes	Yes	No	No
Directory uIDM	Yes	Yes	Yes	No	No
Desktop Experience	Yes	Yes	Yes	Yes	No
Windows Clustering	Yes	Yes	No	No	Yes
Windows Server Backup	Yes	Yes	Yes	Yes	Yes
Windows Network Load Balancing (WNLB)	Yes	Yes	Yes	Yes	Yes
Simple TCP/IP Services	Yes	Yes	Yes	No	Yes
SMTP	Yes	Yes	Yes	Yes	No
Subsystem for Unix-Based Applications (SUA)	Yes	Yes	Yes	No	Yes
Telnet Client	Yes	Yes	Yes	Yes	Yes
Telnet Server	Yes	Yes	Yes	Yes	Yes

Hình 2.12: Các tính năng chính theo các phiên bản của Windows Server 2008

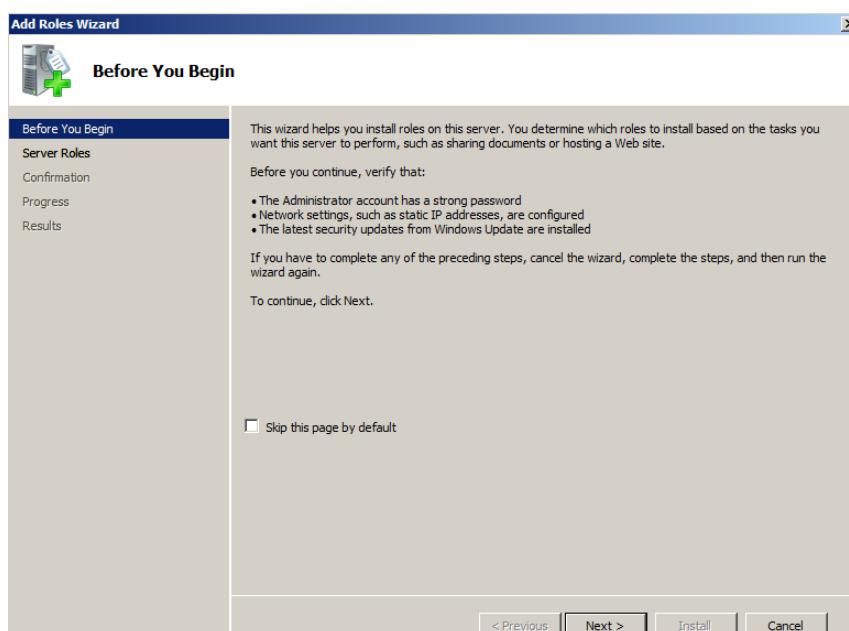
2.2.2. Xây dựng cấu trúc Active Directory

Giống như Windows Server 2003, để xây dựng cấu trúc Active Directory trong Windows Server 2008 cần chạy **dcpromo** từ nhǎc lệnh **Run**, tuy nhiên cần phải cài đặt **Active Directory Domain Controller** role. Đầu tiên cần cài đặt **role**, sau đó chạy **dcpromo**. Vào **Server Manager** → **Roles** → **Add Roles** như trong Hình 2.13.



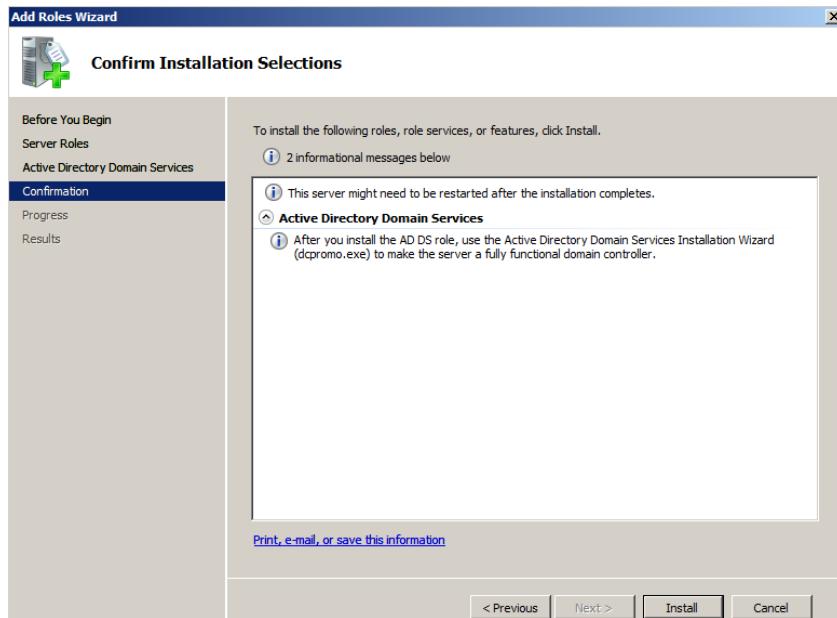
Hình 2.13: Giao diện quản lý role

Xuất hiện trang **Before You Begin** (Hình 2.14), nhấn **Next** để tiếp tục.



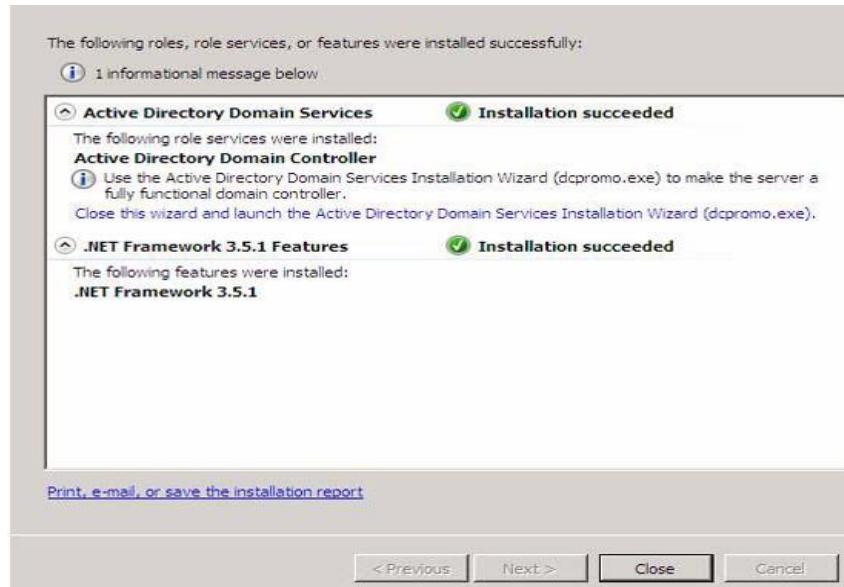
Hình 2.14: Thông báo chuẩn bị cài đặt

Chọn **Active Directory Domain Services** → **Add Required Features** để cài đặt thêm các tính năng này với Active Directory Server Role. Sau khi chọn Active Directory DC Server Role, các thông tin về Server Role sẽ xuất hiện (Hình 2.15). Chọn **Install** để cài đặt các file yêu cầu nhằm chạy **dcpromo**.



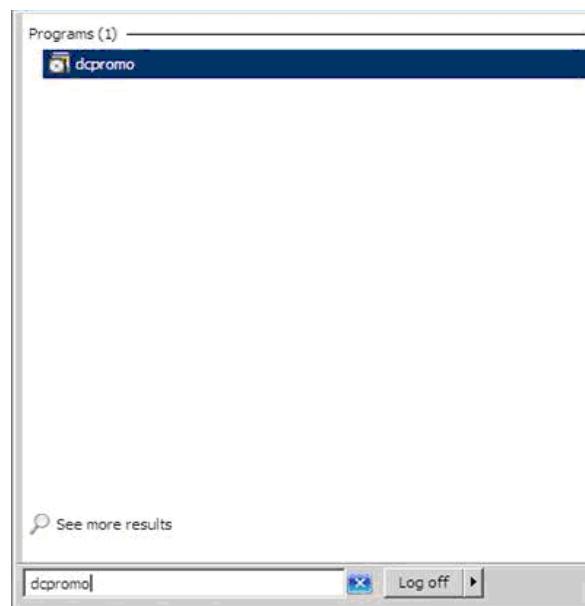
Hình 2.15: Các thư viện yêu cầu để chạy dcpromo

Sau khi cài đặt được thực hiện thành công như trong Hình 2.16, chọn **Close**.



Hình 2.16: Giao diện cài đặt thành công

Tiếp theo, vào menu **Start**, đánh **dcpromo** vào hộp tìm kiếm. Chọn **dcpromo** (Hình 2.17) để cài đặt.



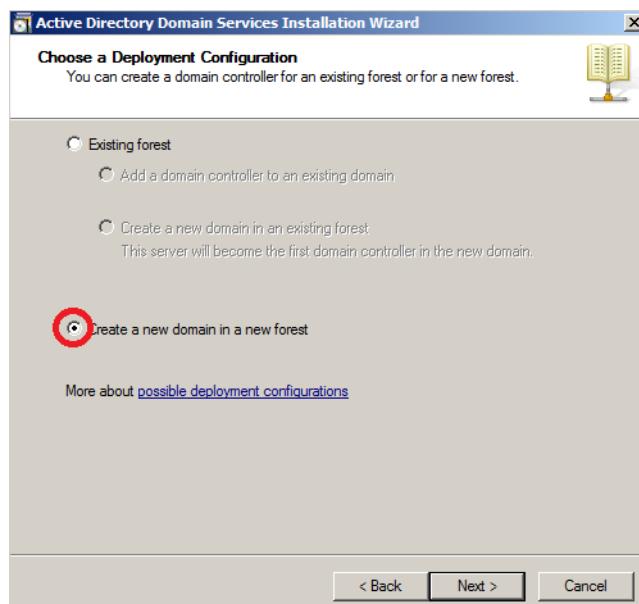
Hình 2.17: Lựa chọn cài đặt dcpromo

Thao tác này sẽ khởi chạy **Welcome to the Active Directory Domain Service Installation Wizard**. Chọn **Next**(Hình 2.18).



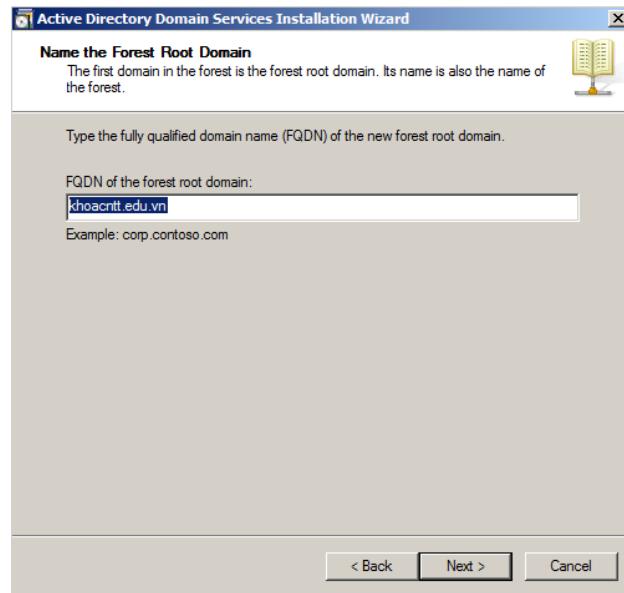
Hình 2.18: **Bắt đầu cài đặt dcromo**

Sau đó, tiếp tục nhấn **Next**. Trong trang **Choose a Deployment Configuration** → **Create a new domain in a new forest** (Hình 2.19).



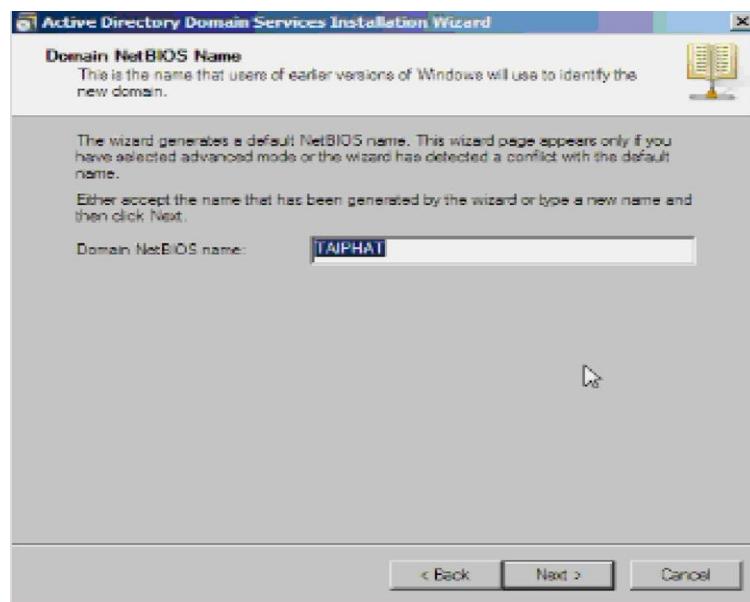
Hình 2.19: **Lựa chọn để tạo một rừng mới**

Trong trang **Name the Forest Root Domain**, nhập vào tên của miền trong hộp nhập liệu **FQDN of the forest root domain**(Hình 2.20). Nhấn **Next** để tiếp tục.



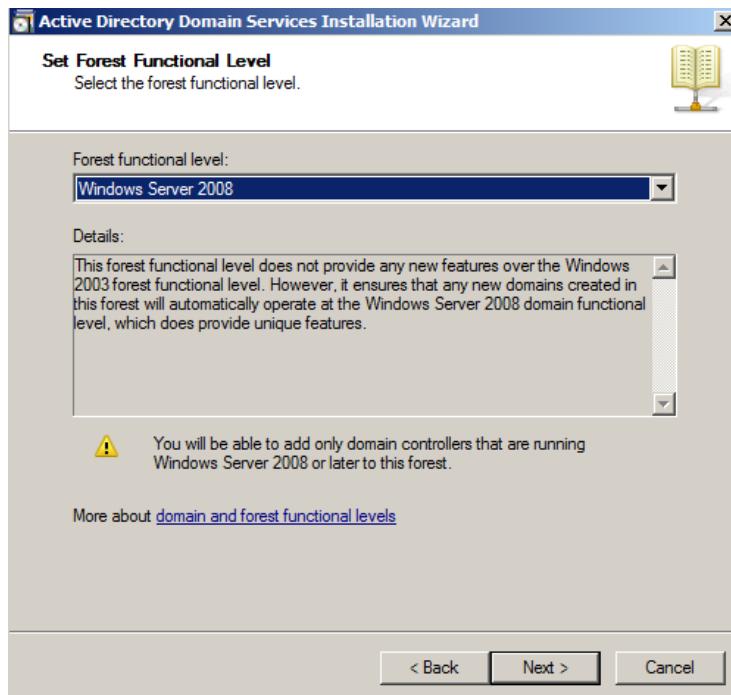
Hình 2.20: Nhập tên miền

Nhấn **Next** để tiếp tục (Hình 2.21).



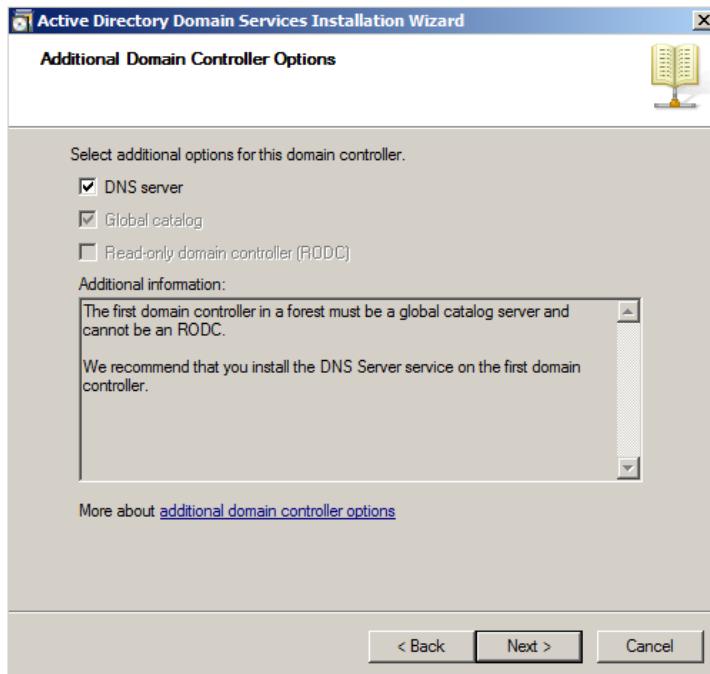
Hình 2.21: Lựa chọn tên miền tương thích với NetBIOS

Trong trang **Set Forest Functional Level**, chọn Windows Server 2008. Nhấn **Next** để tiếp tục (Hình 2.22).



Hình 2.22: Thiết lập chức năng mức rừng

Trong trang **Additional Domain Controller Options**, Chọn **DNS server** và kích **Next**(Hình 2.23).



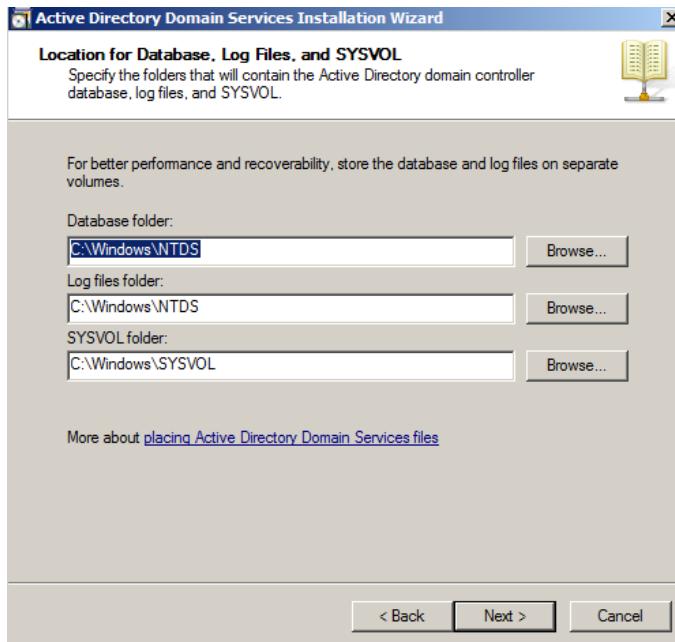
Hình 2.23: Giao diện lựa chọn máy chủ DNS

Một hộp thoại sẽ xuất hiện thông báo không thể tạo được đại diện cho máy chủ DNS này vì không thể tìm thấy vùng xác thực hoặc không chạy dịch vụ Windows DNS server (Hình 2.24). Cảnh báo này xuất hiện vì đây là DC đầu tiên trên mạng. Nhấn **Next** để tiếp tục.



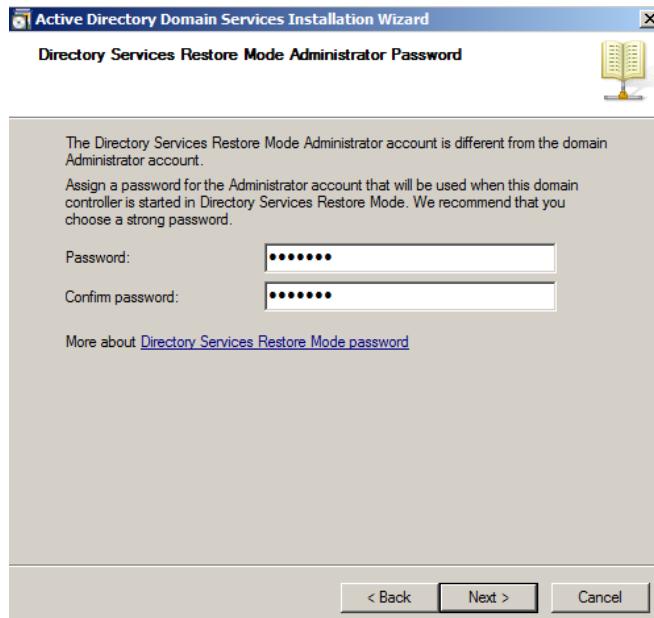
Hình 2.24: Cảnh báo khi tạo máy chủ DNS đầu tiên

Định vị thư mục Database, Log Files và SYSVOL, kích **Next** (Hình 2.25).



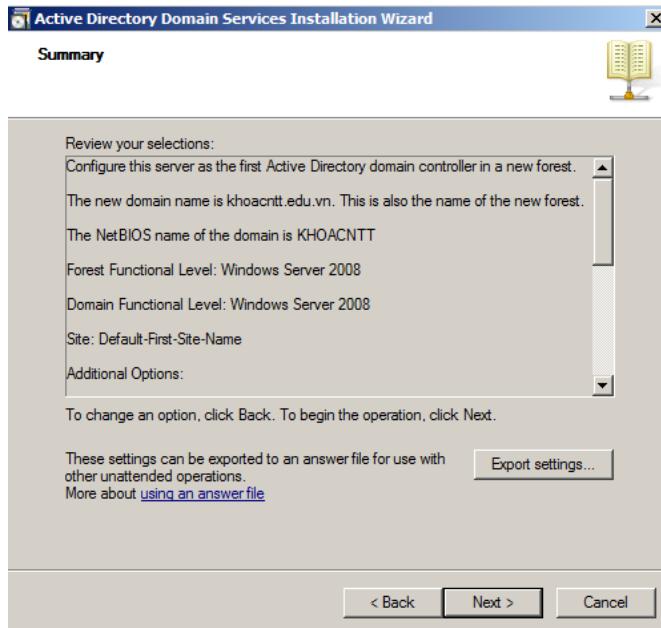
Hình 2.25: Định vị các thư mục cho DNS

Trong **Directory Service Restore Mode Administrator Password**, nhập một mật khẩu mạnh vào các hộp nhập liệu **Password** và **Confirm password** (Hình 2.26).



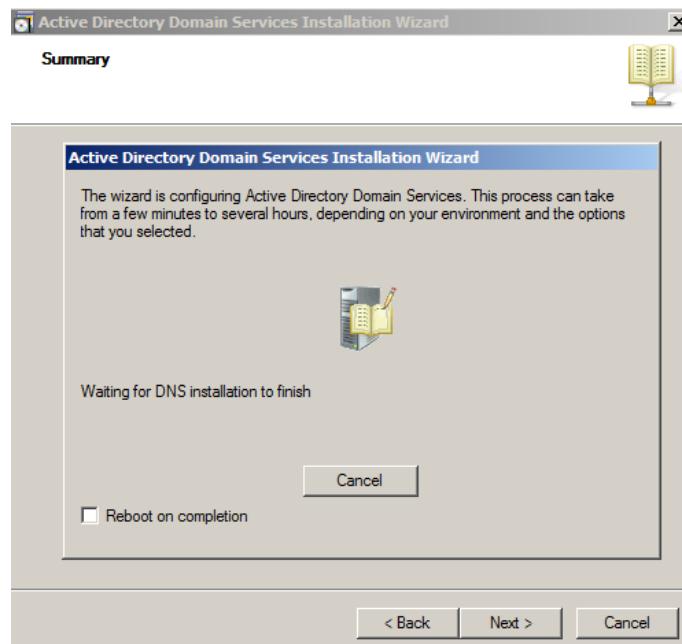
Hình 2.26: Mật khẩu và xác nhận mật khẩu

Xác nhận các thông tin trên trang **Summary** và kích **Next**(Hình 2.27).



Hình 2.27: Xác nhận thông tin về DNS

Tiếp theo, Active Directory sẽ được cài đặt. Đặt một dấu kiểm vào hộp **Reboot on completion** để máy tính sẽ tự động khởi động lại khi cài đặt DC được hoàn tất (Hình 2.28). Cuối cùng, cài đặt sẽ hoàn tất khi đăng nhập.

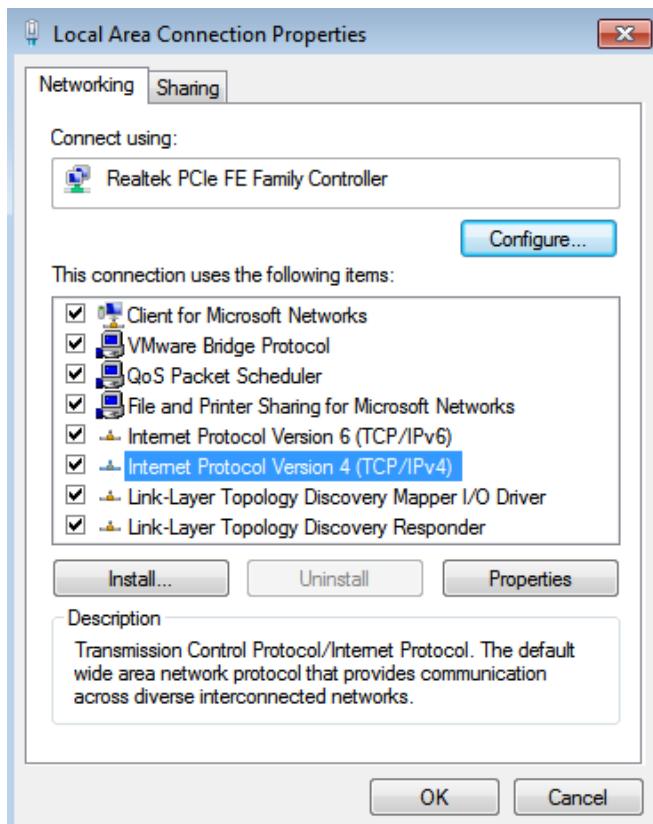


Hình 2.28: Lựa chọn khởi động lại khi cài đặt thành công

2.2.3. Gia nhập miền cho máy tính trạm

Thiết lập địa chỉ IP máy trạm:

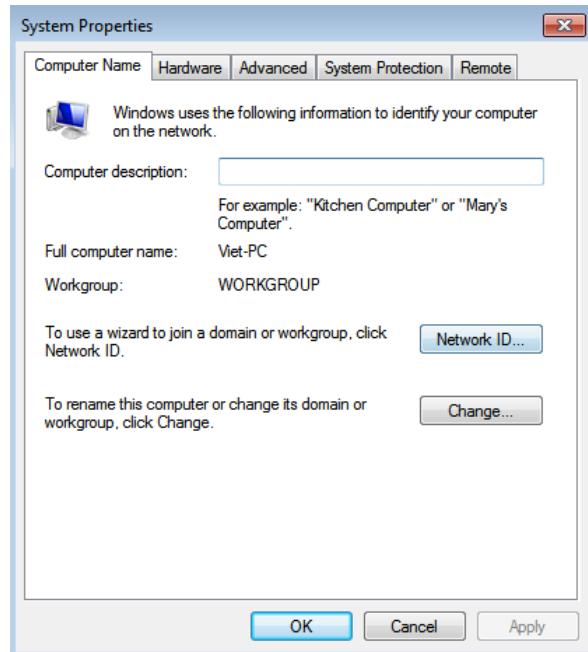
Địa chỉ IP của máy phải nằm trong mạng. Để thiết lập địa chỉ IP, click phải vào **My Network places** → **Properties**. Chọn **Manager network connections** → Click phải vào biểu tượng card mạng chọn **Properties**. Chọn **Internet Protocol Version 4 (TCP/IPv4)** → **Properties** (Hình 2.29).



Hình 2.29: Lựa chọn thiết lập địa chỉ IP

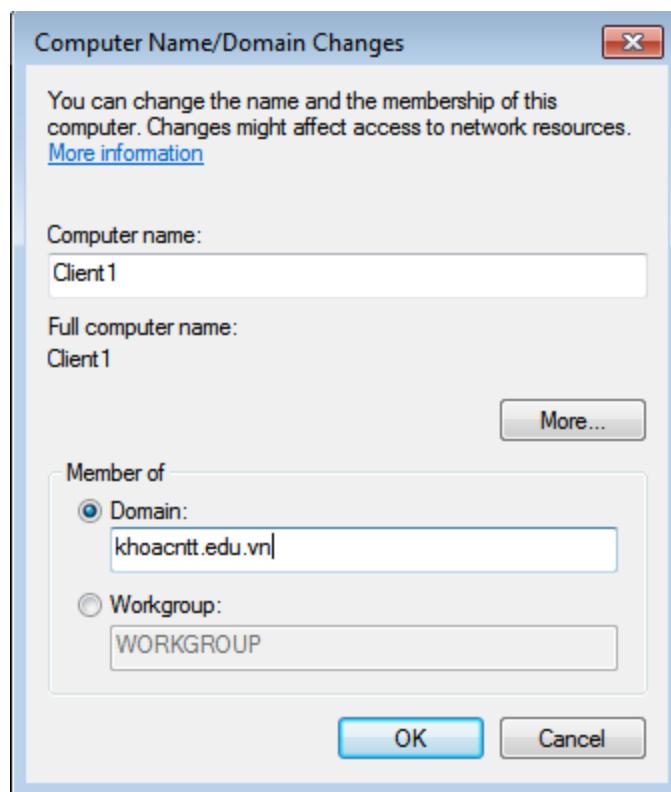
Gia nhập miền cho máy trạm:

Click phải **My Computer** → **Properties** → **Change Settings** rồi chọn nút **Change** (Hình 2.30).



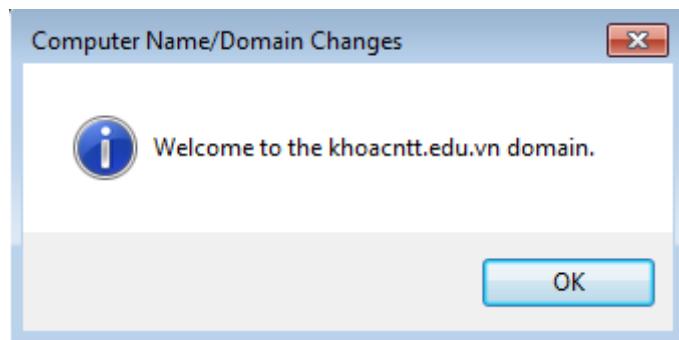
Hình 2.30: Lựa chọn Change để gia nhập miền

Tiếp theo, chọn **Domain** → Nhập tên domain (Hình 2.31).

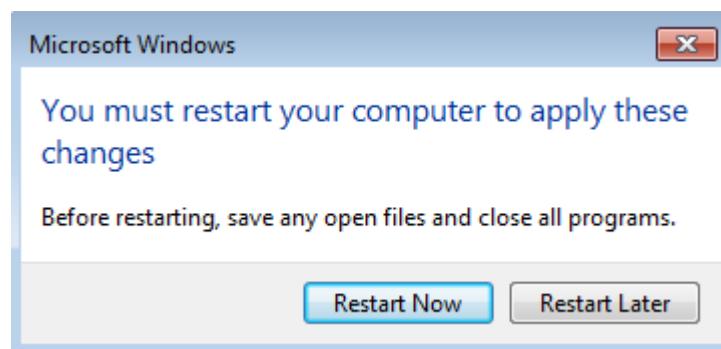


Hình 2.31: Lựa chọn tên miền muôn gia nhập

Công việc thành công.Nhấn **OK** để chấp nhận khởi động lại máy (Hình 2.32). Chọn **Restart Now** (Hình 2.33).



Hình 2.32: Lựa chọn khởi động lại máy sau khi gia nhập miền



Hình 2.33: Khởi động lại

Sau khi khởi động lại, đăng nhập vào domain Administrator → máy tính đã trở thành 1 máy trạm của miền **khoacntt.edu.vn**.

2.2. TỔNG KẾT CHƯƠNG

Giai đoạn đầu trong nghiệp vụ quản trị mạng là xây dựng và cấu hình mạng. Nội dung chương này đã trình bày các kỹ năng cần thiết để triển khai một hệ thống mạng Windows theo cả hai mô hình mạng ngang hàng và khách/chủ.

Triển khai mạng ngang hàng (Workgroup) được thực hiện đơn giản trong các máy tính cài đặt hệ điều hành họ Windows. Mỗi máy tính cài đặt hệ điều hành họ Windows luôn có một Workgroup mặc định. Do đó, chỉ cần hai máy cài đặt hệ

điều hành họ Windows có cùng địa chỉ mạng là có thể kết nối và có thể làm việc trong Workgroup. Theo đó, để thiết lập mạng ngang hàng trong các máy tính Windows, vấn đề cốt yếu là các máy có cùng địa chỉ mạng khi cấu hình địa chỉ IP. Ngoài ra, cũng có thể xây dựng một Workgroup mới thông qua các thiết lập đơn giản.

Mạng khách/chủ được triển khai trong môi trường Windows theo mô hình miền, và việc cài đặt, cấu hình phức tạp hơn. Để triển khai mô hình miền, trước hết cần cài đặt hệ điều hành Windows Server trên máy điều khiển miền. Sau đó, tiến hành cài đặt cấu trúc Active Directory, xây dựng và cấu hình miền. Cuối cùng cần tiến hành gia nhập miền cho các máy trạm.

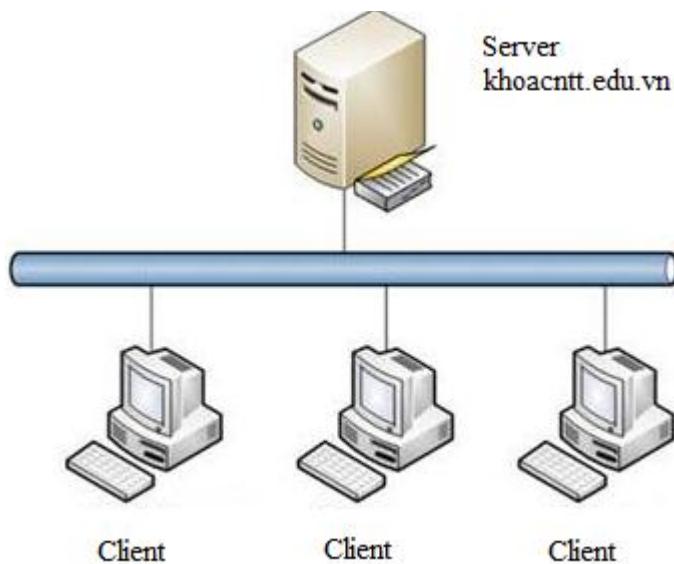
CÂU HỎI VÀ BÀI TẬP THỰC HÀNH

Câu 1. Có mấy loại mô hình mạng máy tính? Sự khác nhau giữa các loại mô hình mạng máy tính này.

Câu 2. Trình bày cấu trúc của AD?

Câu 3. Trình bày vai trò của AD?

Bài thực hành 1. Sử dụng máy ảo xây dựng hệ thống mạng sau:



Nâng cấp máy chủ windows server 2008 lên thành máy chủ quản trị miền Khoacntt.edu.vn

Tiến hành đưa các máy client vào làm thành viên của miền.

CHƯƠNG 3. QUẢN LÝ ĐỐI TƯỢNG

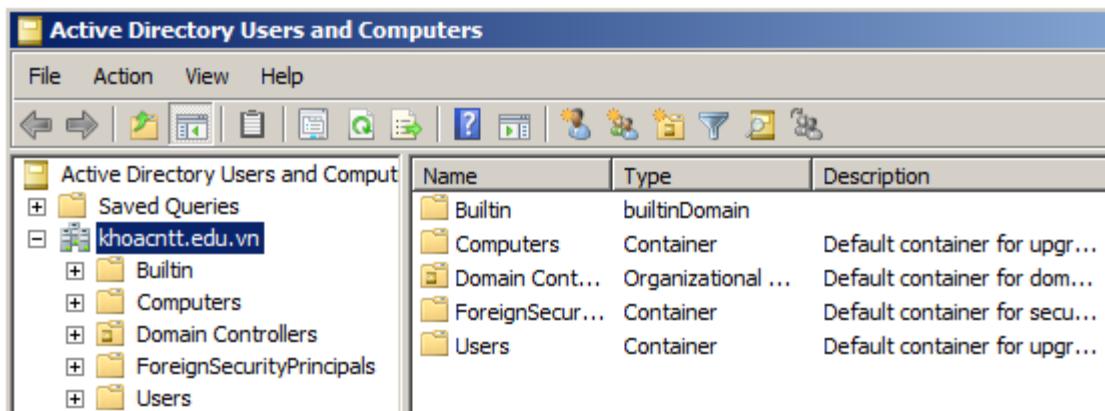
Để chi tiết hóa quy trình và các hoạt động trong bài toán quản trị mạng tổng thể, chương này sẽ trình bày vấn đề quản lý các đối tượng trong hệ thống mạng máy tính. Các đối tượng quản lý bao gồm tài khoản người dùng, tài khoản nhóm và các OU. Nội dung chương này được bô cục như sau: *Mục 3.1* trình bày vấn đề quản lý các OU; *Mục 3.2* trình bày vấn đề quản lý các tài khoản người dùng; *Mục 3.3* trình bày vấn đề quản lý tài khoản nhóm; *Mục 3.4* trình bày vấn đề quyền hạn người dùng; *Mục 3.5* thảo luận về vấn đề ủy thác quyền quản lý OU; *Mục 3.6* tổng hợp và hệ thống lại kiến thức của chương.

3.1. QUẢN LÝ CÁC OU

3.1.1. Tạo các OU

Để tạo các OU, ta sử dụng công cụ **Active Directory Users and Computers** bằng cách chọn lần lượt các mục sau:

Start/Administrator Tools/Active Directory Users and Computers. Khi đó sẽ hiện ra cửa sổ sau:



Hình 3.1: Cửa sổ Active Directory Users and Computers

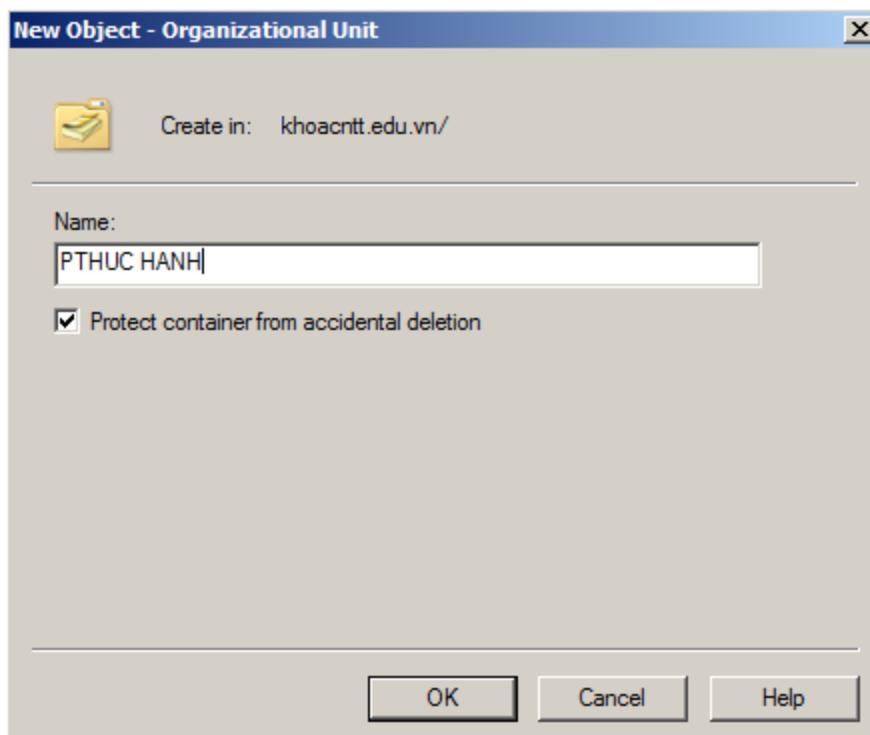
Phần bên trái của cửa sổ trên chính là cấu trúc cây của một Active Directory đơn miền. Do đó tên miền `khoaCNTT.edu.vn` cũng chính là gốc của cây và cũng là

gốc của rừng. Bên phải là phần chi tiết để hiện nội dung của một mục được chọn ở phần bên trái.

Các mục ngay bên dưới miền khoacntt.edu.vn được coi như những *khoang chứa* (container), tương tự như khái niệm Folder của Windows. Các mục này được tự động tạo ra trong quá trình cài đặt, dùng để chứa các tài khoản người dùng, tài khoản nhóm, tài khoản máy, v.v. Tuy có sự phân chia thành các mục như vậy nhưng ta có thể tạo ra hoặc di chuyển các tài khoản vào bất kỳ mục nào, kể cả ở mức miền khoacntt.edu.vn, vì nó cũng được coi như một container.

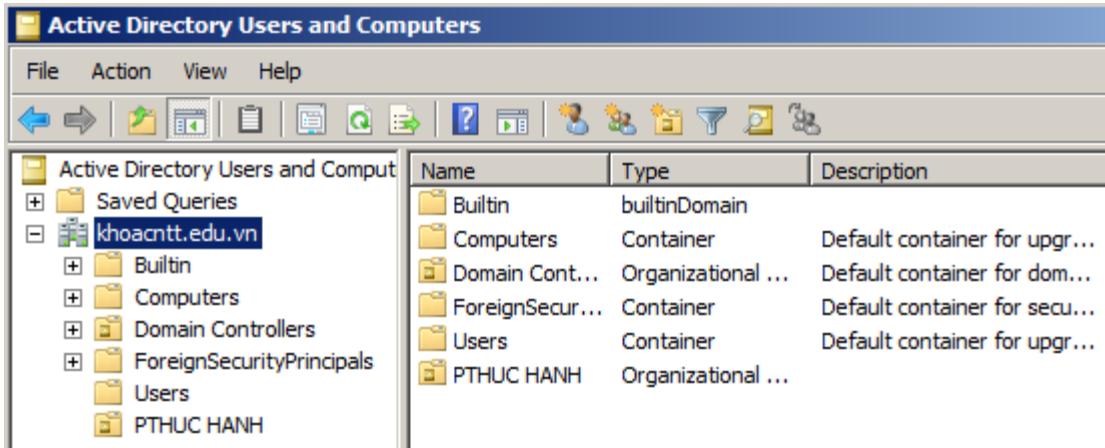
Các OU sẽ có biểu tượng quyền sách mở ở giữa để phân biệt, hay có thể phân biệt qua cột **Type** ở phần chi tiết bên phải. Như trong Hình 3.1 ở trên thì có một OU là **Domain Controllers**, cộng thêm bản thân miền khoacntt.edu.vn cũng được coi như một OU.

Để tạo một OU mới, ta chọn một OU sẽ chứa OU sắp tạo, sau đó mở menu **Action**, rồi lần lượt chọn **New/Organizational Unit**. Khi đó sẽ hiện ra cửa sổ:



Hình 3.2: Cửa sổ khai báo OU mới

Trong cửa sổ trên, giả sử ta muốn tạo một OU có tên là PTHUC HANH nằm ngay dưới miền khoacntt.edu.vn để chứa tất cả các học viên tham gia thực hành tại phòng máy của khoa CNTT. Khi kết thúc tạo ta nhấn **OK**. Hình ảnh của Active Directory khi đó sẽ như sau:

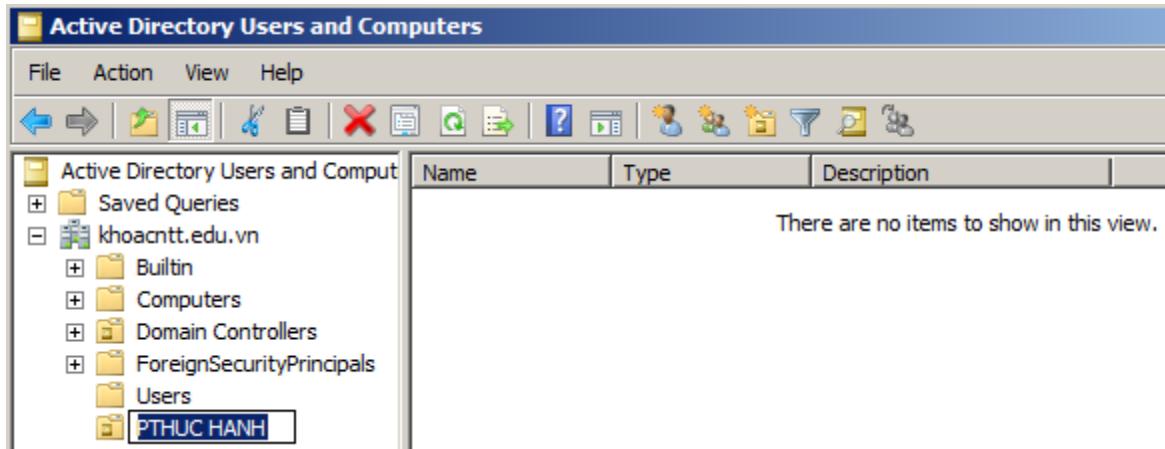


Hình 3.3: Cửa sổ Active Directory Users and Computers sau khi tạo thêm OU PTHUCHANH

Chú ý: Tên của các OU có thể đặt dài tới 64 ký tự và có thể chứa các ký tự bất kỳ. Ở cùng một mức thì tên của các OU phải khác nhau, nhưng ở các mức khác nhau thì chúng có thể có tên giống nhau.

3.1.2. Đổi tên OU

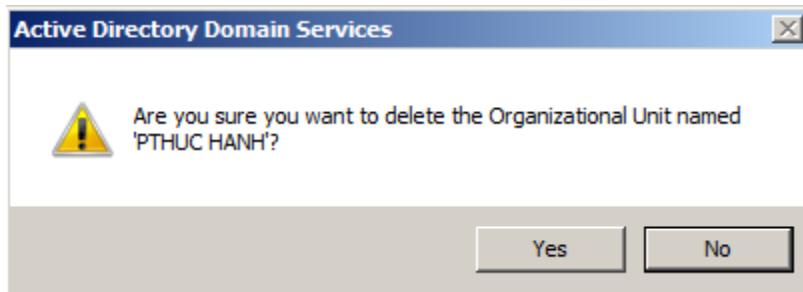
Chọn OU cần đổi tên, chọn **ReName** từ menu **Action**, rồi tiến hành đổi tên mới.



Hình 3.4: Đổi tên OU

3.1.3. Xoá OU

Chọn OU cần xoá, chọn **Delete** từ menu **Action** hoặc bấm phím **Delete**, sau đó chọn: Yes - để xoá, No – không xoá.



Hình 3.5: Xóa OU

Chú ý: Khi xoá một OU thì tất cả các tài khoản nằm trong nó kể cả các OU con của nó cũng đều bị xoá khỏi cấu trúc của Active Directory.

3.2. QUẢN LÝ TÀI KHOẢN NGƯỜI DÙNG

3.2.1. Quản lý tài khoản người dùng của máy

Trong mạng Windows server, tất cả những máy trạm cài đặt Windows 7 và những máy chủ không phải là máy điều khiển vùng (DC), đều có một CSDL khoán mục riêng để quản lý các tài khoản người dùng và tài khoản nhóm của riêng nó. Những tài khoản này được gọi là tài khoản tại chỗ, trong đó cũng có tài khoản người quản trị Administrator.

Đối với những máy không phải là DC. Khi khởi động máy, ta có thể chọn hai mức đăng nhập là: đăng nhập vào mạng hoặc đăng nhập vào chính máy này.

Nếu muốn đăng nhập vào mạng thì tại mục **Log on to**, ta chọn tên miền cần đăng nhập. Khi đó tài khoản người sử dụng phải là tài khoản của miền. Nếu đăng nhập thành công, thì ta có thể khai thác và sử dụng những tài nguyên cá nhân trên mạng và trên máy tính này, tùy theo quyền truy cập được trao.

Nếu muốn đăng nhập vào máy thì tại mục **Log on to**, ta chọn tên máy có kèm theo dòng chữ (this computer) ở cuối. Khi đó tài khoản người sử dụng phải là tài khoản của máy. Nếu tài khoản đó là Administrator thì sẽ có toàn quyền sử dụng máy, còn với những tài khoản người dùng khác thì chỉ có một số quyền hạn nhất định.

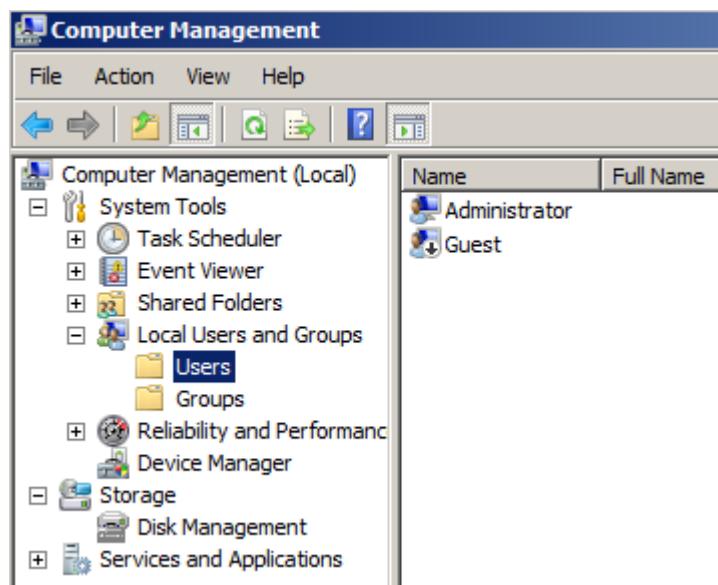
định do người quản trị trao cho. Nhưng trong cả hai trường hợp này ta đều không thể khai thác và sử dụng được các tài nguyên trên mạng.

Chú ý: Khi làm việc với các đối tượng, chức năng nào liên quan đến đối tượng mà được chọn từ một menu nào đó trên màn hình thì chức năng đó cũng có thể được chọn từ menu ngữ cảnh (là menu được hiện ra khi ta nhấn nút phải chuột tại đối tượng được chọn).

3.2.1.1. Tạo tài khoản người dùng của máy

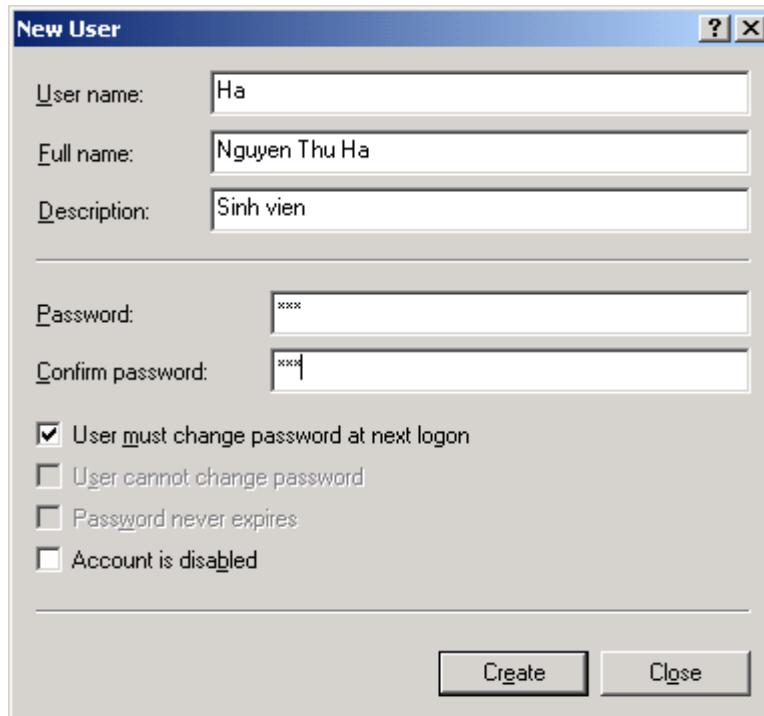
Để tạo ra tài khoản người dùng tại chỗ của máy, ta sử dụng công cụ **Computer Management** bằng cách chọn lần lượt các mục sau:

Start/Administrator Tools/Computer Management, hoặc nhấn chuột phả tại biểu tượng My Computer, rồi chọn mục Manage. Khi đó sẽ hiện ra cửa sổ như Hình 3.6:



Hình 3.6: Cửa sổ Computer Management

Trong cửa sổ trên, ta chọn **Local Users and Groups/Users**, rồi chọn **New User** từ menu **Action**, để hiện ra cửa sổ khai báo như Hình 3.7.



Hình 3.7: Cửa sổ tạo tài khoản người dùng của máy

Trong cửa sổ khai báo trên:

- Mục **User name** bắt buộc phải nhập vào, đây chính là tên để người sử dụng đăng nhập vào máy. Các mục còn lại có thể nhập vào hoặc không.
- Mục **User must change password at next logon**, nếu được chọn thì người sử dụng này phải thay đổi lại mật khẩu tại lần đăng nhập kế tiếp, sau đó ô chọn này sẽ được tự bỏ.
- Mục **Account is disabled**, nếu được chọn thì tài khoản người dùng này tạm thời không có hiệu lực đăng nhập vào máy.
- Sau khi vào xong các thông tin cần thiết, ta nhấn nút **Create** để tạo. Khi đó các mục trong cửa sổ trên sẽ tự xoá để chuẩn bị tạo người sử dụng mới. Để kết thúc quá trình tạo người sử dụng, ta nhấn nút **Close**.

3.2.1.2. Đổi tên tài khoản người dùng của máy

Chọn người sử dụng cần đổi tên tại phần bên phải của cửa sổ **Computer Management**, rồi chọn **Rename** từ menu **Action**. Sau đó gõ vào tên mới.

3.2.1.3. Xoá tài khoản người dùng của máy

Chọn người sử dụng cần xoá tại phần bên phải của cửa sổ **Computer Management**, rồi chọn **Delete** từ menu **Action**, hoặc bấm phím **Delete**. Sau đó nhấn: Yes – để xoá, No – không xoá.

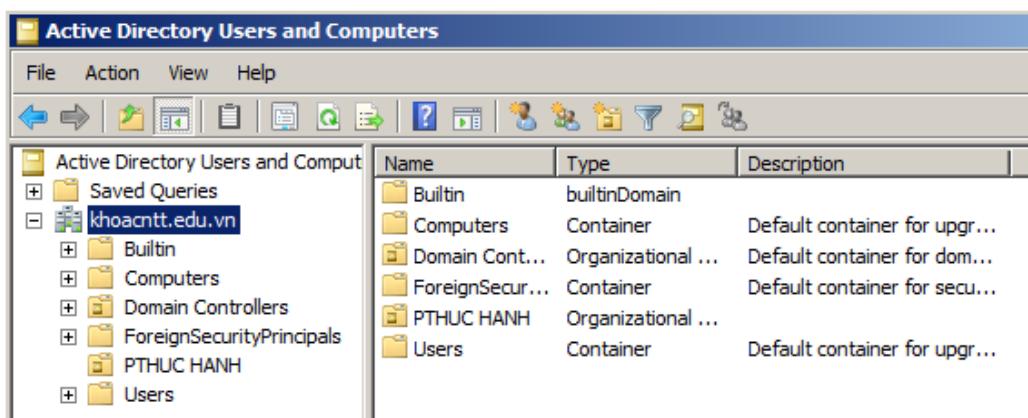
Chú ý: Nếu máy là một DC, thì không thể tạo được tài khoản người sử dụng tại chỗ của máy đó, nên khi đó mục **Local Users and Groups** sẽ bị vô hiệu hoá trong cửa sổ **Computer Management**. Đối với những máy chủ này ta chỉ có thể tạo được các người sử dụng của miền bằng cách dùng công cụ Active Directory Users and Computers.

3.2.2. Quản lý tài khoản người dùng của miền

Trong Windows server, Active Directory Users and Computers là công cụ chính để quản lý các tài khoản người dùng, các nhóm bảo mật, các đơn vị tổ chức (OU), và các chính sách trong mạng đơn miền hoặc đa miền. Công cụ này có thể được chạy trên bất kỳ máy tính chạy hệ điều hành nào, mặc dù nó chỉ được cài đặt và xuất hiện mặc định trong menu Programs trên các máy DC. Để chạy công cụ này trên một máy không phải DC, ta phải quảng bá (publish) hoặc phân bổ (assign) công cụ đó bằng Active Directory. Sau đó nó có thể được cài đặt trên các máy Windows server (không phải DC) hoặc Window 7,... bằng cách dùng công cụ **Add/Remove Programs**

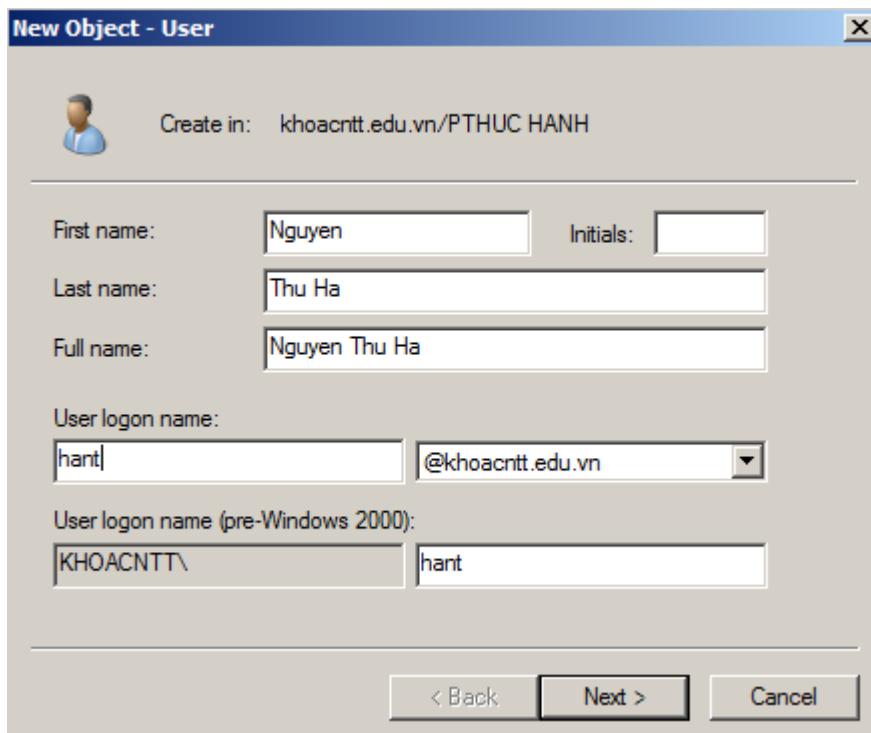
3.2.2.1. Tạo tài khoản người dùng của miền

Để tạo ra tài khoản người dùng của miền, ta mở cửa sổ Active Directory Users and Computers. Cửa sổ này khi được mở có dạng sau:



Hình 3.8: Cửa sổ Active Directory Users and Computers

Tiếp theo ta chọn nơi muốn đặt tài khoản mới vào đó, rồi chọn **New/User** từ menu **Action**, để hiện ra cửa sổ khai báo sau:



Hình 3.9: Cửa sổ tạo tài khoản người dùng của miền

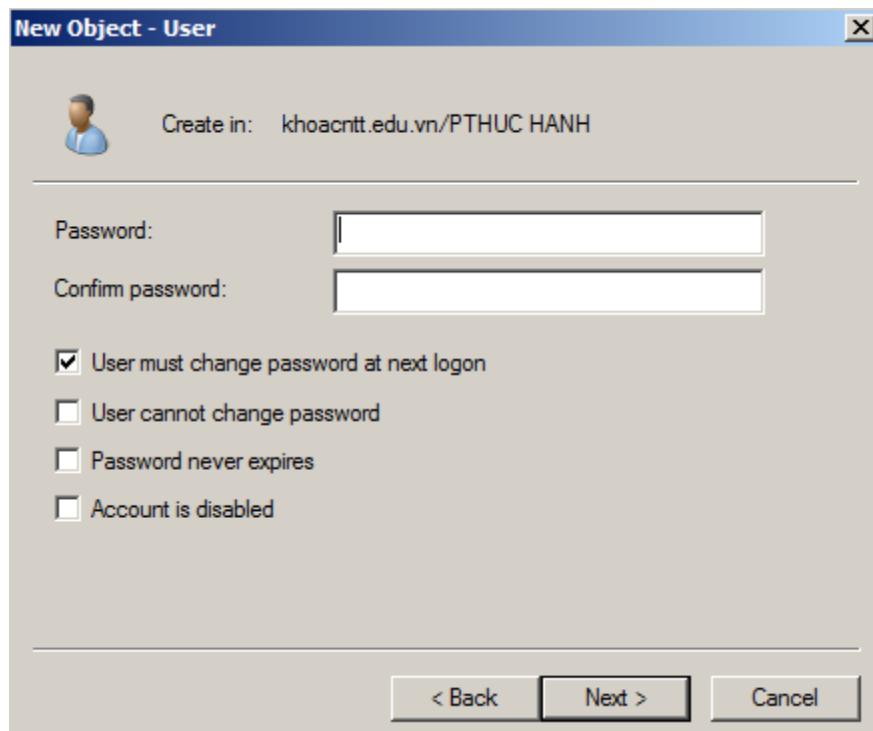
Trong cửa sổ khai báo trên ta điền vào các mục: tên (**First name**), họ (**Last name**), các ký tự viết tắt của tên (**Initials**), và tên đầy đủ (**Full name**). Hai mục **Last name** và **Initials** là tùy chọn, nên có thể điền vào hoặc không.

Mục **User logon name** dùng để gõ vào tên đăng nhập (chính là **User name** khi đăng nhập vào mạng), kế đó ta thấy dòng chữ @khoacntt.edu.vn, đây được gọi là hậu tố *tên chính của người sử dụng* (UPN - User Principal Name), sẽ được tự động gắn vào đuôi của User name lúc đăng nhập để tạo thành tên UPN dạng hant@khoacntt.edu.vn. Những cái tên UPN này bắt chước theo kiểu tên địa chỉ E-mail, cho nên có ký hiệu @. Hậu tố UPN thông thường là tên của miền chứa User được tạo, nhưng cũng có thể đặt một tên gợi nhớ khác (tên này được coi như bí danh của tên miền thật). Về bản chất hậu tố UPN là một con trỏ, chỉ đến miền có chứa tài khoản người dùng đang xét, cho nên rất thuận tiện khi người dùng đăng nhập vào một môi trường mạng đa miền, vì không cần quan tâm đến tên miền thật của miền.

Mục User logon name (pre-Windows 2000) dùng để vào một tên đăng nhập theo kiểu cũ dạng DOMAINNAME\Username tồn tại từ các phiên bản NT trước đây, tên này có thể khác với tên trong **User logon name**. Mục đích của tên này là để tạo sự tương thích trong một mạng đa miền, mà trong đó có cài đặt cả Windows 2000 và NT.

Chú ý: Các tên trong hai mục **First name** và **User logon name** có thể là các ký tự tuỳ ý (trong **First name** dài nhất là 28 ký tự, còn trong **User logon name** nói chung là không hạn chế), nhưng phải là duy nhất đối với các tài khoản khác trên miền (kể cả tài khoản người sử dụng và tài khoản nhóm). Tuy nhiên, tên của một tài khoản người dùng trên miền có thể giống với tên của một tài khoản tại chỗ trên một máy nào đó không phải là DC.

Sau khi điền vào xong những thông tin trên ta chọn **Next** để mở tiếp cửa sổ sau:



Hình 3.10: Cửa sổ ấn định các tuỳ chọn về mật khẩu và tài khoản

Trong cửa sổ trên ta ấn định một mật khẩu cho tài khoản người dùng tại mục **Password** rồi xác nhận nó tại mục **Confirm password**.

Chú ý: Các chữ cái trong mật khẩu có phân biệt chữ hoa và chữ thường (kể cả mật khẩu tài khoản người dùng của miền và của máy).

Các tuỳ chọn bên dưới có thể chọn hoặc không, nếu chọn thì chúng có ý nghĩa như sau:

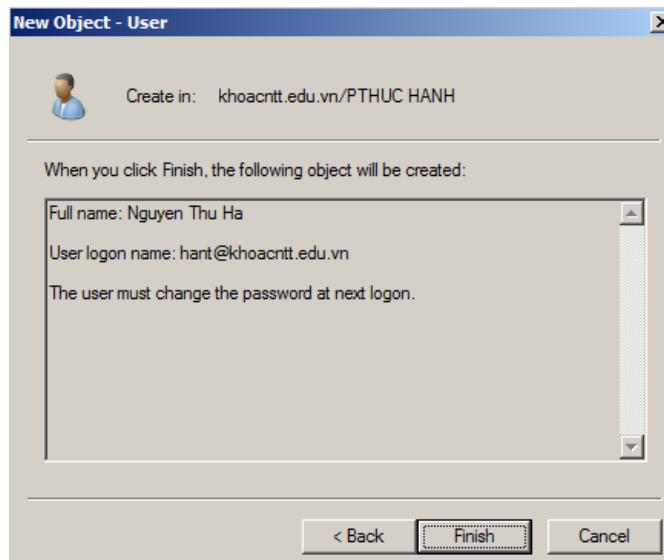
User must change password at next logon: Buộc người dùng này phải đổi mật khẩu vào lần đăng nhập kế tiếp, sau đó ô chọn này sẽ được tự bỏ.

User cannot change password: Ngăn không cho người dùng thay đổi mật khẩu của tài khoản này. Tuỳ chọn này hữu ích đối với các tài khoản dùng chung.

Password never expires: Tài khoản người dùng này sẽ lờ đi chính sách hết hạn mật khẩu, do đó mật khẩu dành cho tài khoản này sẽ không bao giờ hết hạn. Tuỳ chọn này hữu ích đối với các tài khoản dùng chung để chạy các dịch vụ.

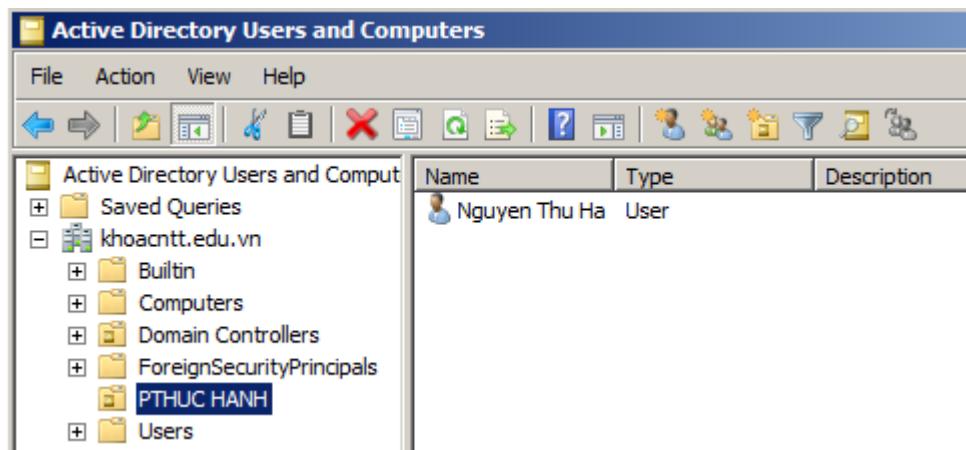
Account is disabled: Tài khoản này tuy vẫn nằm trong cơ sở dữ liệu khoán mục của vùng, nhưng tạm thời bị vô hiệu hoá, và chừng nào chưa bỏ tuỳ chọn này thì không thể dùng nó để đăng nhập vào mạng được.

Tiếp theo chọn **Next** để hiện ra cửa sổ cuối cùng của quá trình tạo, như Hình 3.11 Cửa sổ này hiện ra một số thông tin chính mà ta đã nhập vào cho tài khoản người dùng. Nếu chọn **Finish** thì tài khoản đó sẽ được tạo ngay, còn nếu muốn quay lại sửa một số thông tin ở các cửa sổ trước đó thì ta chọn **Back**.



Hình 3.11: Cửa sổ xác nhận thông tin của tài khoản người dùng trước khi tạo

Sau khi chọn Finish, ở phần chi tiết (bên phải) của cửa sổ Active Directory Users and Computers sẽ hiện ra tài khoản người dùng mới tạo như Hình 3.12.

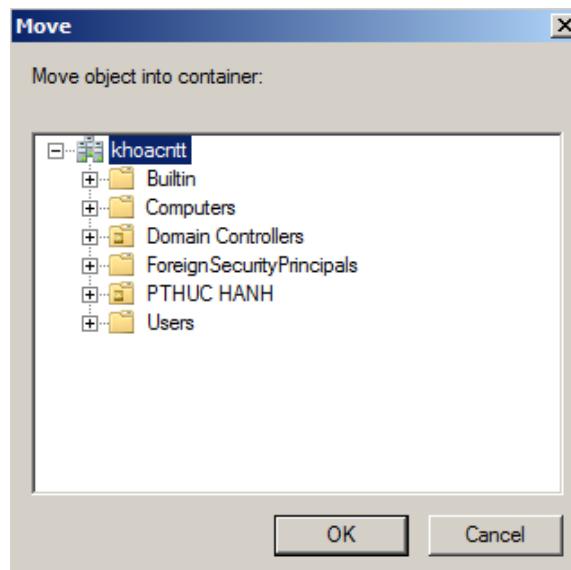


Hình 3.12: Cửa sổ Active Directory Users and Computers sau khi tạo thêm tài khoản người dùng mới Nguyen Thu Ha

Trong cửa sổ trên ta thấy chỉ hiện tên đầy đủ của tài khoản người dùng, mà không hiện tên đăng nhập (hant).

3.2.2.2. Di chuyển tài khoản người dùng đến nơi chứa mới

Chọn người sử dụng cần di chuyển, chọn **Move** từ menu **Action**, để hiện ra cửa sổ như Hình 3.13 Tại cửa sổ này ta chọn nơi chứa mới rồi nhấn **OK**.



Hình 3.13: Cửa sổ chọn nơi chứa mới của tài khoản người dùng

3.2.2.3. Đổi tên đầy đủ của tài khoản người dùng

Chọn người sử dụng cần đổi tên, chọn **Rename** từ menu **Action**, rồi gõ vào tên mới.

3.2.2.4. Đổi lại mật khẩu người dùng

Chọn người sử dụng cần đổi mật khẩu, chọn **Reset Password** từ menu **Action**, để hiện ra cửa sổ như Hình 3.14 Sau đó tiến hành vào mật khẩu mới.



Hình 3.14: Cửa sổ đổi mật khẩu mới của tài khoản người dùng

3.2.2.5. Xoá tài khoản người dùng

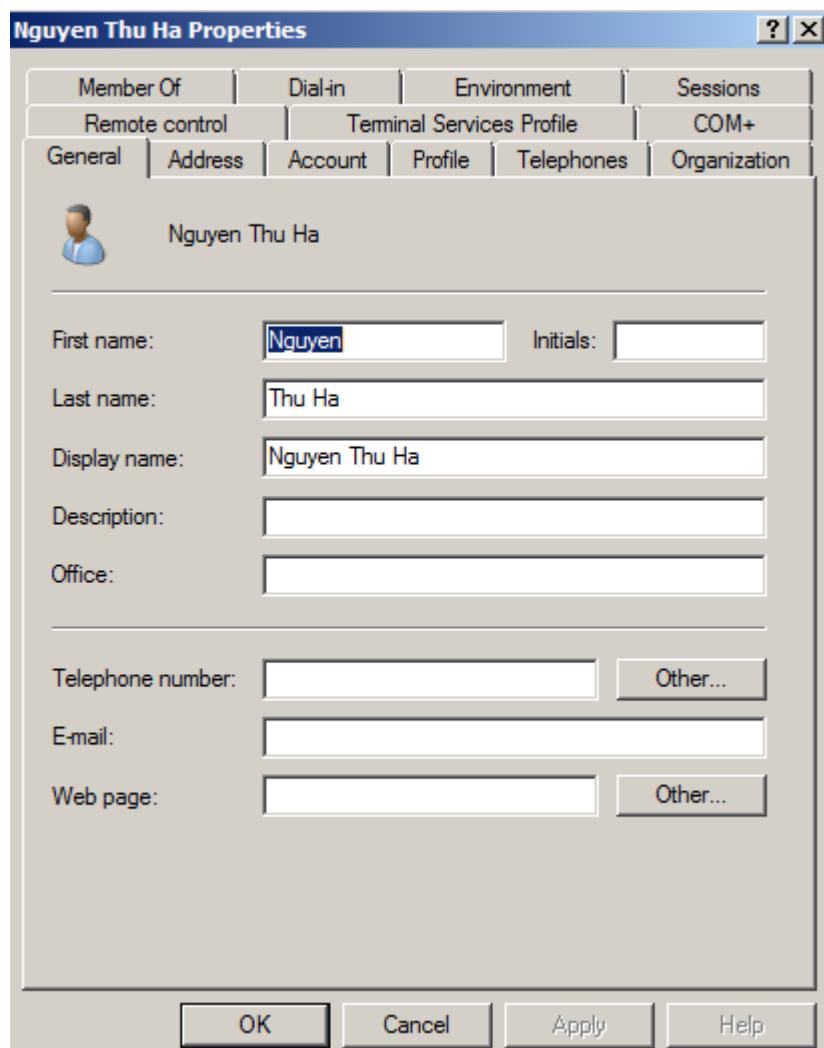
Chọn người sử dụng cần xoá, chọn **Delete** từ menu **Action** hoặc bấm phím **Delete**. Sau đó nhấn: **Yes** – để xoá, **No** – không xoá.

3.2.3. Thay đổi các thiết định về tài khoản người dùng

Các thiết định cho tài khoản người dùng của miền bao gồm rất nhiều thiết định, ở đây chỉ quan tâm tới một số thiết định chính như: giờ đăng nhập vào mạng, máy được đăng nhập vào, ngày hết hạn của tài khoản. Các thiết định về ẩn định mật khẩu và chính sách khoá chặt tài khoản được thực hiện thông qua chính sách nhóm.

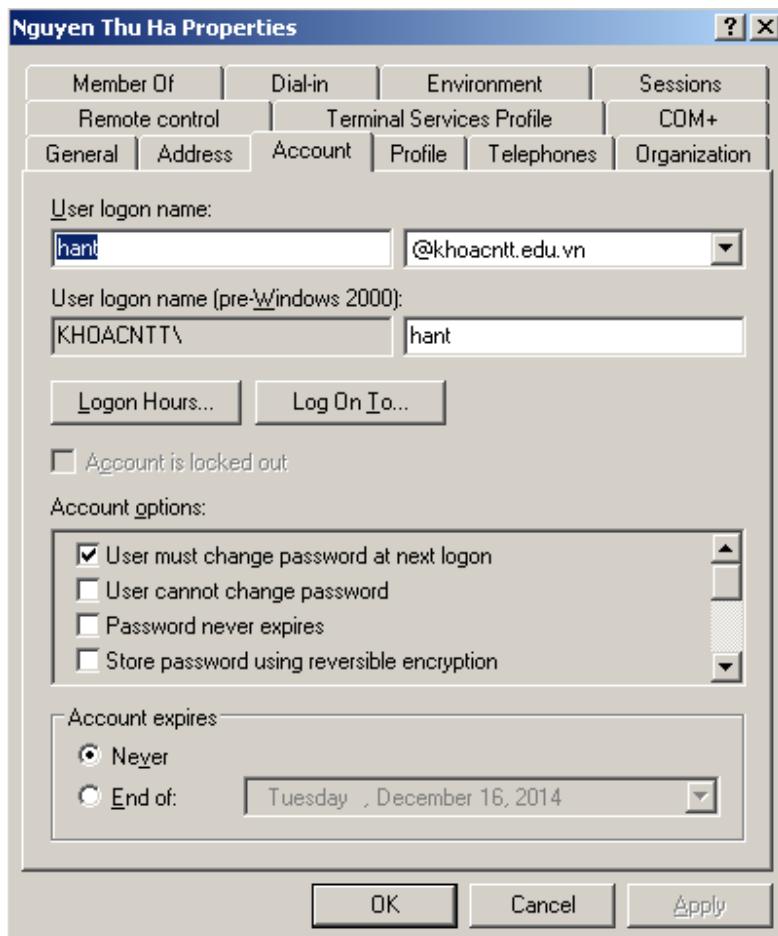
Để thay đổi các thiết định về tài khoản người dùng của miền, ta chọn khoản người dùng cần thay đổi (ví dụ Nguyen Thu Ha), chọn **Properties** để hiện ra cửa sổ đặc tính của người dùng này như Hình 3.15, với trang được chọn hiện đầu tiên là **General**. Tại trang này ta thấy hiện lên một số thông tin đã nhập trong quá

trình tạo tài khoản, và ta vẫn có thể sửa lại ở đây nếu muốn. Ngoài ra ta có thể bổ sung cho người dùng này một lời mô tả (Description), tên văn phòng làm việc (Office), các số điện thoại (Telephone number), địa chỉ E-mail, địa chỉ các trang Web (Web page).



Hình 3.15: Cửa sổ đặc tính của tài khoản người dùng

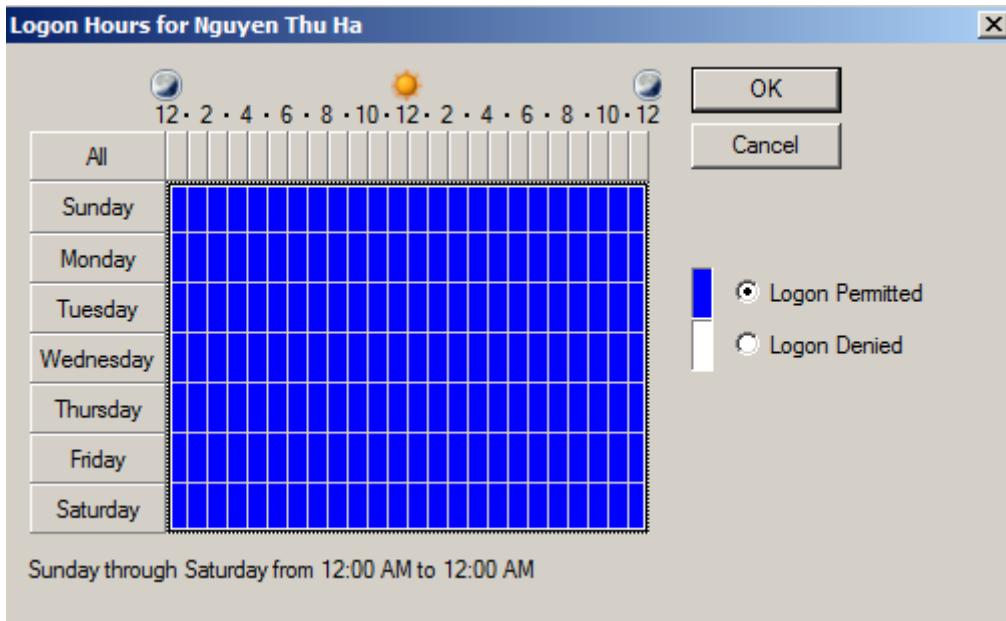
Tiếp theo ta chọn trang **Account** để hiện ra nội dung như Hình 3.16.



Hình 3.16: Trang Account của cửa sổ đặc tính

Tại đây ta có thể đổi lại tên đăng nhập vào mạng tại mục **User logon name**, thay đổi lại các tuỳ chọn về mật khẩu tại mục **Account options**. Tại mục **Account Expires**, nếu chọn **Never** thì tài khoản của người dùng này sẽ không bao giờ hết hạn, còn nếu chọn **End of** và vào một ngày nào đó thì đến ngày đó, tài khoản người dùng này sẽ không thể đăng nhập vào mạng.

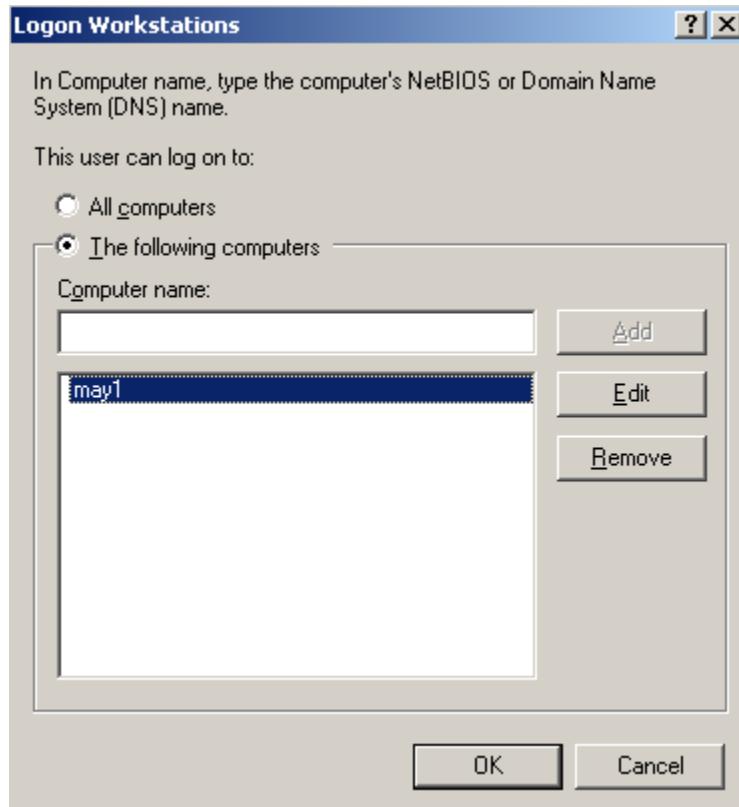
Theo mặc định, mọi người dùng đều được phép đăng nhập vào mọi ngày trong tuần và vào bất kỳ giờ nào trong ngày (tức là 24/7), nhưng ta vẫn có thể ấn định những ngày giờ cụ thể nào đó mà mỗi người được phép đăng nhập bằng cách chọn mục **Logon Hours** để hiện ra cửa sổ như Hình 3.17.



Hình 3.17: Cửa sổ **Ấn định ngày, giờ đăng nhập vào mạng**

Trong cửa sổ trên, các hàng biểu thị các ngày từ chủ nhật (Sunday) đến thứ bảy (Saturday), các cột biểu thị các giờ trong ngày (từ 1 giờ sáng đến 12 giờ đêm). Các ô có tô màu biểu thị giờ đó được phép đăng nhập. Nếu muốn cấm người sử dụng đăng nhập vào một khoảng thời gian nào đó, thì ta đánh dấu vùng ô tương ứng bằng cách nhấn chuột tại ô đầu, giữ và kéo chuột tới ô cuối, sau đó chọn **Logon Denied**. Nếu muốn cho người sử dụng đăng nhập vào những giờ đã cấm, ta cũng chọn vùng giờ đó, sau đó chọn **Logon Permitted**. Cuối cùng nhấn **OK**.

Cũng theo mặc định, mọi người sử dụng có thể đăng nhập vào mạng từ mọi máy, nếu muốn hạn chế người sử dụng chỉ được phép đăng nhập vào một số máy nào đó, thì ta chọn mục **Log On To** từ cửa sổ trong Hình 3.16 để hiện ra cửa sổ như Hình 3.18.



Hình 3.18: Cửa sổ ấn định người dùng được phép đăng nhập từ máy nào

Trong cửa sổ trên, nếu chọn mục **All computers** thì người sử dụng có thể đăng nhập từ mọi máy trên mạng. Còn nếu chọn **The following computers** thì người sử dụng chỉ có thể đăng nhập vào mạng từ những tên máy ta gõ vào tại đây. Nếu muốn gõ vào tên máy nào, ta nhập tên máy đó tại mục **Computer name**, rồi nhấn **Add** để chuyển tên đó xuống ô bên dưới (như cửa sổ trên ta đã làm với May1).

Nếu muốn sửa lại tên máy đã ấn định, ta chọn tên máy đó, chọn **Edit**, rồi sửa.

Nếu muốn bỏ tên máy đã ấn định, ta chọn nó, rồi nhấn **Remove**.

Cuối cùng nhấn **OK** để kết thúc.

3.3. QUẢN LÝ CÁC TÀI KHOẢN NHÓM

3.3.1. Khái niệm nhóm

Nhóm là một khoản mục có thể chứa những khoản mục người sử dụng hoặc nhóm khác như là các thành viên.

Nhóm dùng để cho phép đồng thời nhiều người sử dụng truy cập vào các tài nguyên như tệp, thư mục, máy in hay thực hiện các công việc hệ thống như lưu trữ và phục hồi các tệp, thay đổi thời gian hệ thống ...

Theo mặc định khi khoản mục người sử dụng mới tạo ra, họ không có một chút quyền gì đáng kể trên mạng. Gán người dùng vào các nhóm sẽ khiến việc trao cho họ những quyền hạn thực hiện tác vụ (**rights**) cùng với quyền truy cập các tài nguyên mạng (**Permissions**) trở nên dễ dàng hơn. Bởi vì chỉ cần trao quyền cho nhóm, sau đó mọi thành viên trong nhóm đều sẽ được thừa hưởng quyền của nhóm. Điều này cho phép người quản trị xử lý một số lượng lớn người sử dụng thông qua chỉ một khoản mục nhóm.

Khi tạo ra các tài khoản nhóm của miền trong Windows server, ta được lựa chọn là xếp nhóm đó vào loại nhóm bảo mật (security group) hay nhóm phân phối thư tín (distribution group). Các nhóm bảo mật thực ra không có gì mới mẻ, chúng cũng tương tự như các nhóm người dùng trong tất cả các phiên bản NT trước đây. Nay gọi chúng là nhóm bảo mật chỉ để phân biệt với các nhóm phân phối thư tín (không bảo mật), chỉ mới có trong Windows server 2000, 2003 và 2008...

Mỗi tài khoản nhóm bảo mật và mỗi tài khoản người dùng khi mới được tạo ra, đều được tự động cấp một mã nhận diện bảo mật SID (Security Identifier). Mỗi SID là một mã độc nhất để phân biệt một tài khoản, tức là mỗi tài khoản có một SID khác nhau. Hơn nữa các SID không bao giờ được tái sử dụng. Khi một tài khoản bị xoá đi, thì SID của nó cũng bị xoá theo. Do vậy nếu ta đã tạo ra một tài khoản người sử dụng hoặc tài khoản nhóm bảo mật với một tên nào đó, rồi xoá đi, sau đó tạo lại với đúng tên cũ, thì về thực chất Windows server vẫn coi là khác với tài khoản đã xoá trước đó, nên không thể thừa hưởng những quyền hạn và quyền truy cập được gán trước khi xoá.

Các nhóm thư tín không phải để phục vụ mục đích bảo mật, nên không có mã nhận diện bảo mật SID, và không xuất hiện trên các danh sách kiểm soát truy cập ACL (Access Control List – danh sách này được hiện khi cần chọn các đối tượng là người sử dụng hoặc nhóm bảo mật). Các nhóm này được dùng làm địa chỉ để nhận thư tín hay thông điệp.

Mỗi máy tính trong mạng, đều có một tài khoản máy, đó chính là tên của máy được khai báo khi cài đặt. Tài khoản này cũng được lưu trữ trong cấu trúc của Active Directory (thường là trong mục Computers). Với NT 4, ta không được phép đặt các tài khoản này vào trong một nhóm, và đó là điều không hay, bởi vì thường thì rất tiện lợi nếu tạo ra các nhóm máy để áp dụng chung các chính sách hệ thống lên đó. Windows server 2000, 2003, 2008... đã sửa chữa thiếu sót này, nên giờ đây ta có thể có các nhóm mà thành viên của nó có thể là tài khoản người dùng, hoặc tài khoản máy, hoặc cả hai loại đó.

Trong NT 4, các nhóm chỉ có thể được lồng vào nhau nhiều nhất là một cấp. Còn trong Windows server 2000, 2003, 2008..., các nhóm có thể được lồng vào nhau sâu hơn một cấp.

3.3.2. Các loại nhóm bảo mật

Có ba kiểu nhóm bảo mật là: nhóm cục bộ (local group), nhóm toàn miền (global group) và nhóm toàn rùng (universal group).

3.3.2.1. Nhóm cục bộ (Local group)

Nhóm cục bộ là nhóm được gắn với từng máy tính, được dùng để cấp phát các quyền hạn tại chỗ và quyền truy cập vào các tài nguyên tại chỗ.

Đối với các máy trong mạng không phải là DC, thì các tài khoản nhóm cục bộ được lưu trữ trong CSDL khoán mục của máy. Còn với các máy DC, thì chúng được lưu trữ trên CSDL khoán mục của vùng, tức là lưu trữ trong Active Directory.

Thành viên của nhóm cục bộ có thể là:

- Các tài khoản người sử dụng của miền chứa nhóm cục bộ hoặc từ một miền khác được uỷ quyền.
- Nếu là nhóm cục bộ trên máy không phải DC thì có thể tiếp nhận cả các tài khoản người dùng của chính máy này làm thành viên.
- Các nhóm toàn rùng, nhóm toàn miền, trên cùng miền chứa nó.
- Các nhóm toàn rùng, nhóm toàn miền, từ một miền khác được uỷ quyền.

Windows server cung cấp nhiều nhóm cục bộ tạo sẵn để quản lý các công việc hệ thống.

Người quản trị có thể tạo thêm các nhóm cục bộ mới để quản lý việc truy cập tài nguyên.

3.3.2.2. Nhóm toàn miền (Global group)

Nhóm toàn miền được dùng để tập hợp những người dùng và các nhóm toàn miền khác, vốn cần có những quyền hạn và quyền truy cập tài nguyên giống nhau.

Nhóm toàn miền không được uỷ quyền thực hiện các chức năng mạng như nhóm cục bộ. Để có thể làm việc này nó phải là thành viên của nhóm cục bộ có các quyền trên.

Nhóm toàn miền được lưu trong CSDL khoản mục của vùng.

Thành viên của nhóm toàn miền chỉ có thể là:

- Các tài khoản người sử dụng trên cùng một miền.
- Các nhóm toàn miền khác trên cùng một miền.

2.3.2.3. Nhóm toàn rùng (universal group)

Trong hai loại nhóm đã xét ở trên ta thấy có sự khác biệt cơ bản là:

- Nhóm cục bộ ngoài việc tiếp nhận các người sử dụng, còn có thể tiếp nhận các nhóm loại khác là thành viên, nhưng không là thành viên của các nhóm loại khác.
- Còn nhóm toàn miền, thì không được phép tiếp nhận các nhóm loại khác làm thành viên, mà thành viên của nó chỉ có thể là các người sử dụng và các nhóm toàn miền.

Nhóm toàn rùng là loại nhóm mới chỉ có trong họ HĐH Windows server nhằm dung hoà giữa hai nhóm trên: nó vừa có thể tiếp nhận nhóm loại khác làm thành viên, vừa có thể là thành viên của nhóm loại khác. Nhóm toàn rùng cũng giống nhóm toàn miền ở chỗ: không được uỷ quyền thực hiện các chức năng mạng như nhóm cục bộ.

Nhóm toàn rùng cũng được lưu trong CSDL khoản mục của vùng.

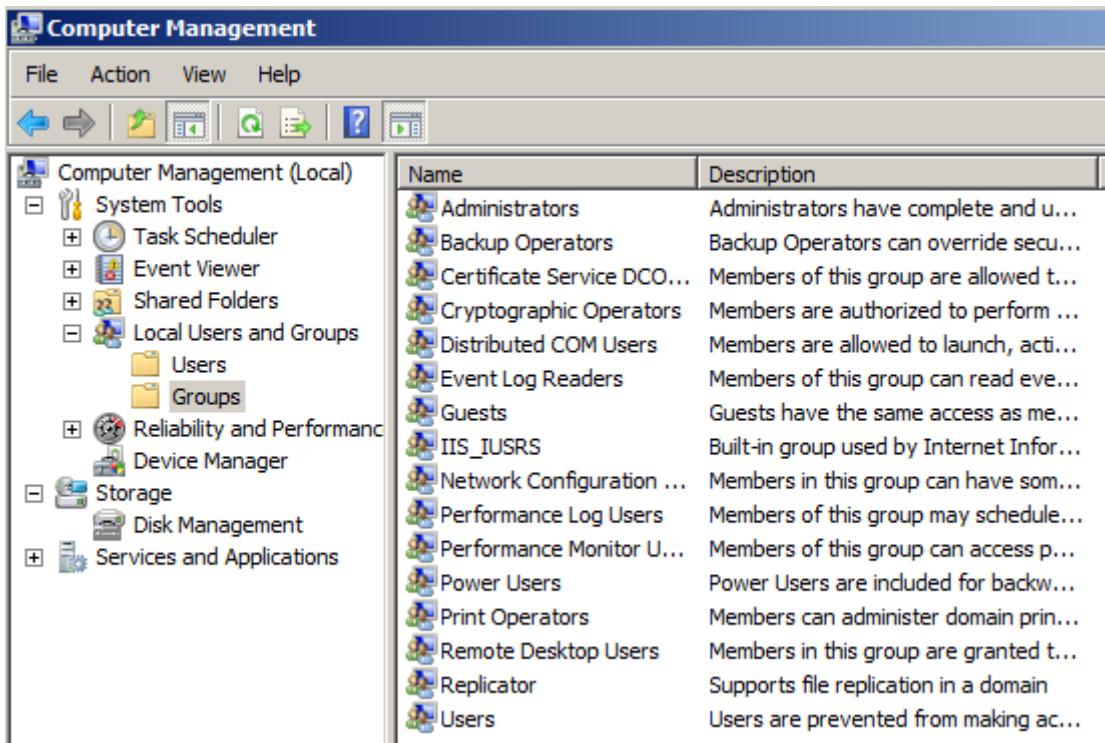
Thành viên của nhóm toàn rùng có thể là:

- Các tài khoản người sử dụng của miền từ một miền bất kỳ trong rùng.

- Các nhóm toàn miền từ một miền bất kỳ trong rừng.
- Các nhóm toàn rừng khác.

3.3.3. Các nhóm cục bộ được tạo sẵn

Các nhóm cục bộ được tạo sẵn của máy được đặt trong mục **Groups** như Hình 3.19



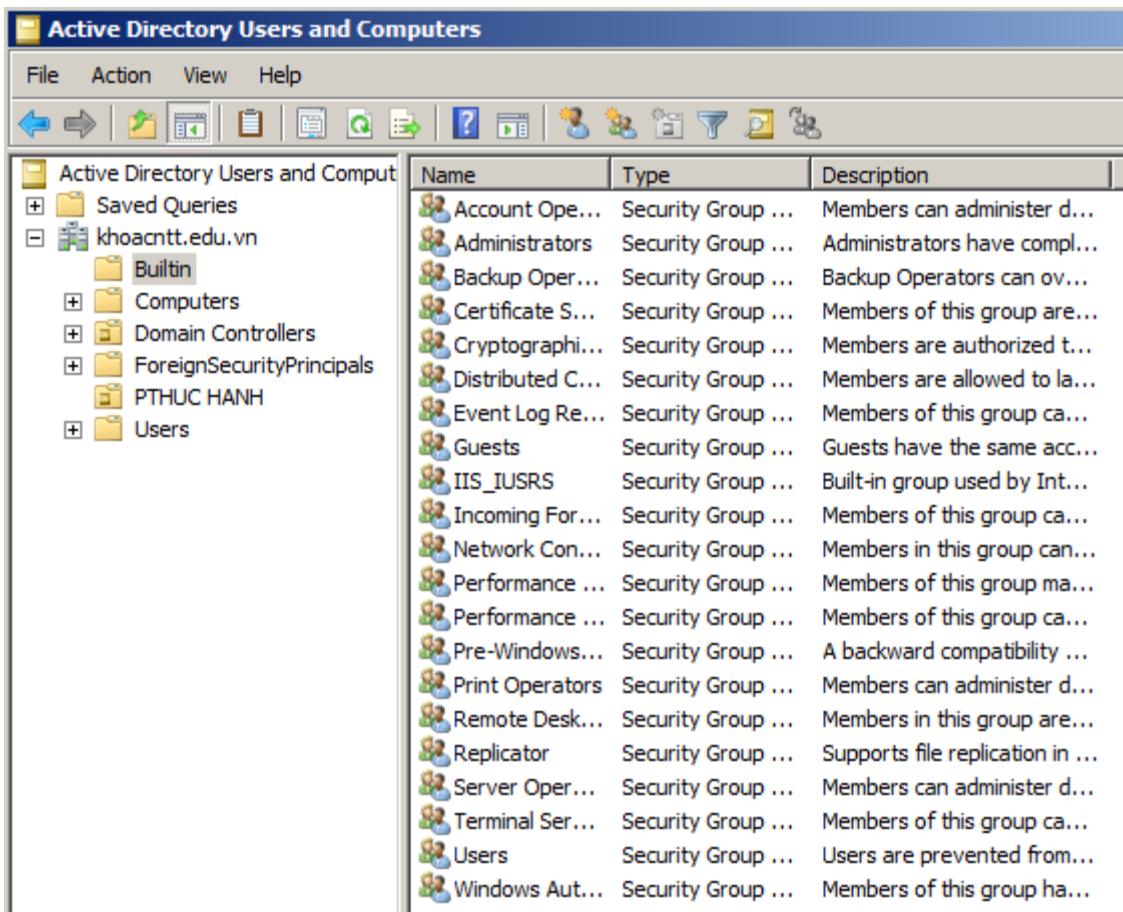
Hình 3.19: Các nhóm cục bộ được tạo sẵn của máy

Bảng 3.1. Các nhóm cục bộ tạo sẵn của máy cùng với quyền hạn và khả năng của chúng

Quyền hạn của nhóm	Khả năng của nhóm
<u>Administrators</u> Chiếm quyền sở hữu các tập tin Quản lý bản ghi chép kiểm toán và bảo mật Thay đổi giờ của máy Lưu dự phòng các tập tin và thư mục Khôi phục lại các tập tin và thư mục	Tạo ra và quản lý các tài khoản người dùng, tài khoản nhóm Trao quyền hạn cho người dùng Quản lý chính sách kiểm toán và bảo mật Định dạng đĩa cứng của máy Chia sẻ và chấm dứt chia sẻ các thư

Thêm và bớt các trình điều khiển thiết bị	mục Chia sẻ và chấm dứt chia sẻ các máy in
Power Users Thay đổi giờ của máy	Tạo ra và quản lý các tài khoản người dùng, tài khoản nhóm Chia sẻ và chấm dứt chia sẻ các thư mục Chia sẻ và chấm dứt chia sẻ các máy in
Backup Operators Lưu dự phòng các tập tin và thư mục Khôi phục lại các tập tin và thư mục	
Replicator Quản lý sự nhân bản các tập tin và thư mục	
Users (Không có quyền gì)	
Guests (Không có quyền gì)	

Các nhóm cục bộ được tạo sẵn của miền được đặt trong mục **Builtin** như
Hình 3.20



Hình 3.20: Các nhóm cục bộ được tạo sẵn của miền

Bảng 3.2. Các nhóm cục bộ tạo sẵn cùng với quyền hạn và khả năng của chúng

Quyền hạn của nhóm	Khả năng của nhóm
<p><u>Administrators</u></p> <p>Đăng nhập tại chỗ</p> <p>Truy cập máy này từ mạng</p> <p>Chiếm quyền sở hữu các tập tin</p> <p>Quản lý bản ghi chép kiểm toán và bảo mật</p> <p>Thay đổi giờ của máy</p> <p>Tắt máy</p> <p>Buộc tắt máy này từ một máy ở xa</p> <p>Lưu dự phòng các tập tin và thư mục</p> <p>Khôi phục lại các tập tin và thư mục</p>	<p>Tạo ra và quản lý các tài khoản người dùng, tài khoản nhóm: cục bộ, toàn miền, toàn rừng</p> <p>Trao quyền hạn cho người dùng</p> <p>Quản lý chính sách kiểm toán và bảo mật</p> <p>Khoá chặt Server console</p> <p>Mở khoá Server console</p> <p>Định dạng đĩa cứng của Server</p> <p>Tạo ra các nhóm chương trình chung</p> <p>Chia sẻ và chấm dứt chia sẻ các thư mục</p>

Thêm và bớt các trình điều khiển thiết bị Tăng độ ưu tiên của một quá trình xử lý	Chia sẻ và chấm dứt chia sẻ các máy in
<u>Server Operators</u> Đăng nhập tại chỗ Thay đổi giờ của máy Server này Tắt máy Server này Buộc tắt máy Server này từ một máy ở xa Lưu dự phòng các tập tin và thư mục Khôi phục lại các tập tin và thư mục	Khoá chặt Server Phủ quyết khoá của Server Định dạng đĩa cứng của Server Tạo ra các nhóm chương trình chung Chia sẻ và chấm dứt chia sẻ các thư mục Chia sẻ và chấm dứt chia sẻ các máy in
<u>Account Operators</u> Đăng nhập tại chỗ Tắt máy Server này	Tạo ra và quản lý các tài khoản người dùng, tài khoản nhóm: cục bộ, toàn miền, toàn rừng ¹
<u>Print Operators</u> Đăng nhập tại chỗ Tắt máy	Chia sẻ và chấm dứt chia sẻ các máy in
<u>Backup Operators</u> Đăng nhập tại chỗ Tắt máy Lưu dự phòng các tập tin và thư mục Khôi phục lại các tập tin và thư mục	
<u>Everyone</u> Truy cập máy này từ mạng	Khoá chặt Server ²
<u>Users</u> (Không có quyền gì)	Tạo vào quản lý các nhóm cục bộ ³
<u>Guest</u> (Không có quyền gì)	
<u>Replicator</u> Quản lý sự nhân bản các tập tin và thư mục	

1. Tuy nhiên, không thể sửa đổi các tài khoản sau: người quản trị Administrator; nhóm toàn bộ Domain Admins; các nhóm cục bộ Administrators, Server Operators, Account Operators, Print Operators và Backup Operators.

2. Để thực hiện được điều này, thành viên của nhóm phải có quyền đăng nhập tại chỗ trên Server này.

3. Để thực hiện được điều này, thành viên của nhóm hoặc phải có quyền đăng nhập tại chỗ trên Server này, hoặc phải có quyền truy cập vào công cụ Active Directory Users and Computers.

3.3.4. Các nhóm toàn miền và nhóm toàn rừng được tạo sẵn

Các nhóm toàn miền và nhóm toàn rừng được tạo sẵn được đặt trong mục Users như Hình 3.21

Active Directory Users and Computers			
File Action View Help			
Name	Type	Description	
Administrator	User	Built-in account for admini...	
Allowed ROD...	Security Group ...	Members in this group can...	
Cert Publishers	Security Group ...	Members of this group are...	
Denied ROD...	Security Group ...	Members in this group can...	
DnsAdmins	Security Group ...	DNS Administrators Group	
DnsUpdatePr...	Security Group ...	DNS clients who are permis...	
Domain Admins	Security Group ...	Designated administrators...	
Domain Com...	Security Group ...	All workstations and serve...	
Domain Cont...	Security Group ...	All domain controllers in th...	
Domain Guests	Security Group ...	All domain guests	
Domain Users	Security Group ...	All domain users	
Enterprise A...	Security Group ...	Designated administrators...	
Enterprise R...	Security Group ...	Members of this group are...	
Group Policy ...	Security Group ...	Members in this group can...	
Guest	User	Built-in account for guest ...	
RAS and IAS ...	Security Group ...	Servers in this group can ...	
Read-only D...	Security Group ...	Members of this group are...	
Schema Admins	Security Group ...	Designated administrators...	

Hình 3.21: Các nhóm toàn miền và nhóm toàn rừng được tạo sẵn

Bảng 3.3. Các nhóm toàn miền và nhóm toàn rùng được tạo sẵn

Nhóm	Công dụng của nó
Domain Admins (nhóm toàn miền)	<p>Theo mặc định nhóm này là thành viên của nhóm cục bộ Administrators của miền và của những máy không phải DC trong cùng miền chứa nó. Do vậy các thành viên của nhóm này có thể quản trị miền nhà, cùng với các máy trong miền. Ngoài ra còn quản trị được miền uỷ quyền nếu đã lồng nhóm này vào nhóm cục bộ Administrators của miền uỷ quyền.</p> <p>Thành viên mặc định ban đầu của nhóm này là người quản trị Administrator của miền.</p>
Domain Users (nhóm toàn miền)	Nhóm này chứa mọi tài khoản người dùng của miền, và theo mặc định là thành viên của mọi nhóm local group Users trên mọi máy trạm của miền. Bởi vậy các thành viên của nhóm này có quyền truy cập và quyền hành của người dùng bình thường đối với cả miền chứa nhóm ấy, cùng với các máy trong miền ấy.
Domain Guests (nhóm toàn miền)	Nhóm này dùng để chứa những tài khoản người dùng tạm thời (với tư cách là khách) của miền, quyền hạn truy cập và sử dụng mạng của nhóm này do quản trị viên quy định và thường là rất hạn chế, chỉ có ý nghĩa thăm quan vào mạng. Tài khoản người dùng đầu tiên của nhóm này là Guest (khách), người dùng này được tạo mặc định trong quá trình cài đặt.
Enterprise Admins (nhóm toàn rùng)	<p>Theo mặc định nhóm này là thành viên của nhóm cục bộ Administrators của mọi máy trong mọi miền của rùng. Do vậy các thành viên của nhóm này được nhìn nhận là một quản trị viên có quyền lực trên toàn rùng.</p> <p>Thành viên mặc định ban đầu của nhóm này là</p>

	người quản trị Administrator trên miền gốc của rừng.
Schema Admins (nhóm toàn rừng)	<p>Theo mặc định nhóm này cũng là thành viên của nhóm cục bộ Administrators của mọi máy trong mọi miền của rừng. Do vậy các thành viên của nhóm này cũng được nhìn nhận là một quản trị viên có quyền lực trên toàn rừng. Ngoài ra các thành viên của nó còn có quyền thay đổi cách sắp xếp tổ chức (schema) của rừng.</p> <p>Thành viên mặc định ban đầu của nhóm này là người quản trị Administrator trên miền gốc của rừng.</p>

3.3.5. Các nhóm đặc biệt

Các nhóm này không được gán thành viên theo nghĩa thông thường, và người quản trị không thể gán thành viên cho các nhóm này. Tuỳ theo cách thức truy nhập của người sử dụng vào các tài nguyên khác nhau trên mạng mà họ sẽ có tư cách khác nhau thông qua các nhóm đặc biệt. Một số nhóm đặc biệt được tạo sẵn gồm:

Interactive: Bất kỳ ai đang dùng máy một cách tại chỗ.

Network: Tất cả những người dùng được nối kết vào một máy trên mạng.

Creator Owner: Người tạo ra và người chủ sở hữu của các thư mục con, các tập tin, và các công việc in (print job).

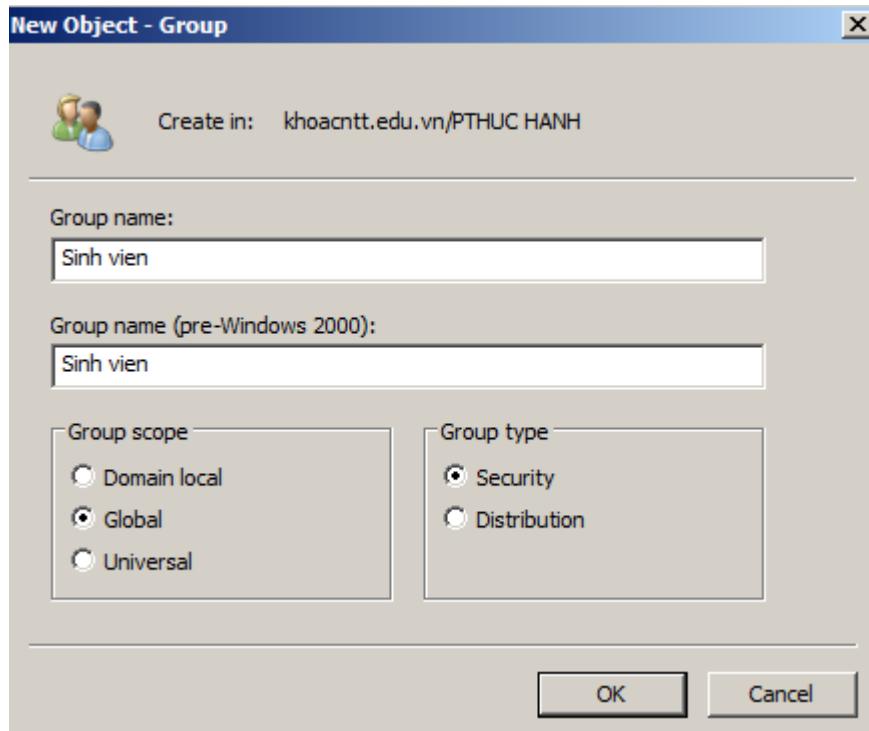
Service: Những tài khoản đăng nhập với tính cách như một dịch vụ.

Dialup: Những người dùng đang truy cập hệ thống thông qua Dial-Up Networking.

3.3.6. Tạo và quản lý tài khoản nhóm của miền

3.3.6.1. Tạo tài khoản nhóm

Để tạo ra các tài khoản nhóm của miền, ta mở cửa sổ Active Directory Users and Computers, chọn nơi chứa nhóm sắp tạo, mở menu Action, chọn New/Group, để hiện ra cửa sổ khai báo như Hình 3.22.



Hình 3.22: Cửa sổ tạo nhóm mới

Trong đó các mục:

Group name: được dùng để vào tên nhóm (tên có thể là các ký tự tùy ý và có thể dài tới 64 ký tự).

Group name (pre-Windows 2000): để vào tên nhóm tương thích dành cho NT 4.

Group scope: dùng để chọn phạm vi (loại) nhóm, có thể là một trong ba loại: cục bộ của miền (Domain local), toàn miền (Global), toàn rừng (Universal).

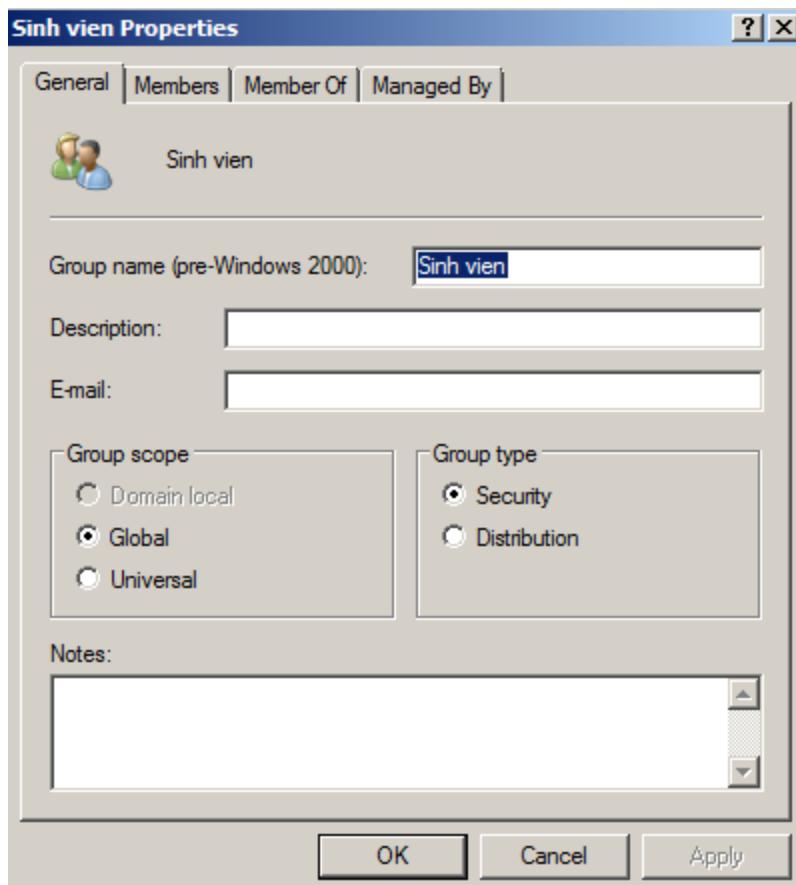
Group type: dùng để chọn kiểu nhóm, là nhóm bảo mật (Security) hay nhóm phân phối thư tín (Distribution).

Kết thúc tạo nhấn OK.

3.3.6.2.Thêm bớt thành viên vào nhóm

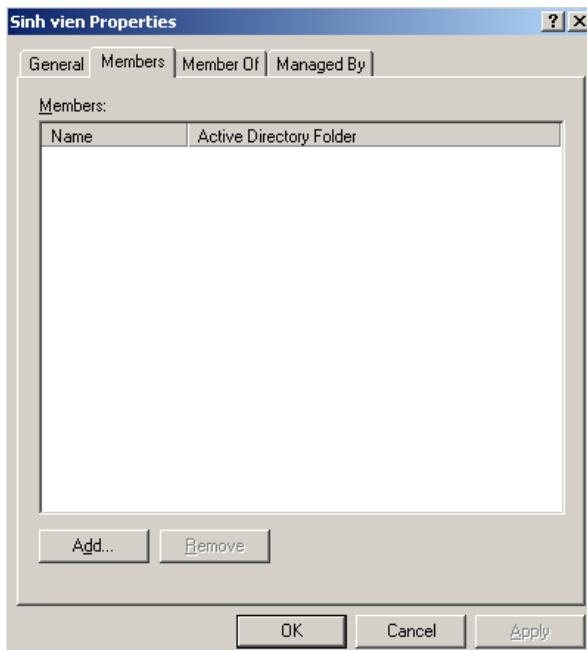
Chọn nhóm cần thêm bớt thành viên, chọn **Properties** từ menu **Action**, để mở cửa sổ Properties của nhóm với trang được chọn đầu tiên là **General** như Hình 3.23. Tại trang này ta có thể thay đổi lại một số thông tin tại các mục như đã

mô tả trong quá trình tạo ở trên. Ngoài ra có vào thêm một số thông tin như: một lời mô tả về nhóm (Description), một địa chỉ E-mail của nhóm.

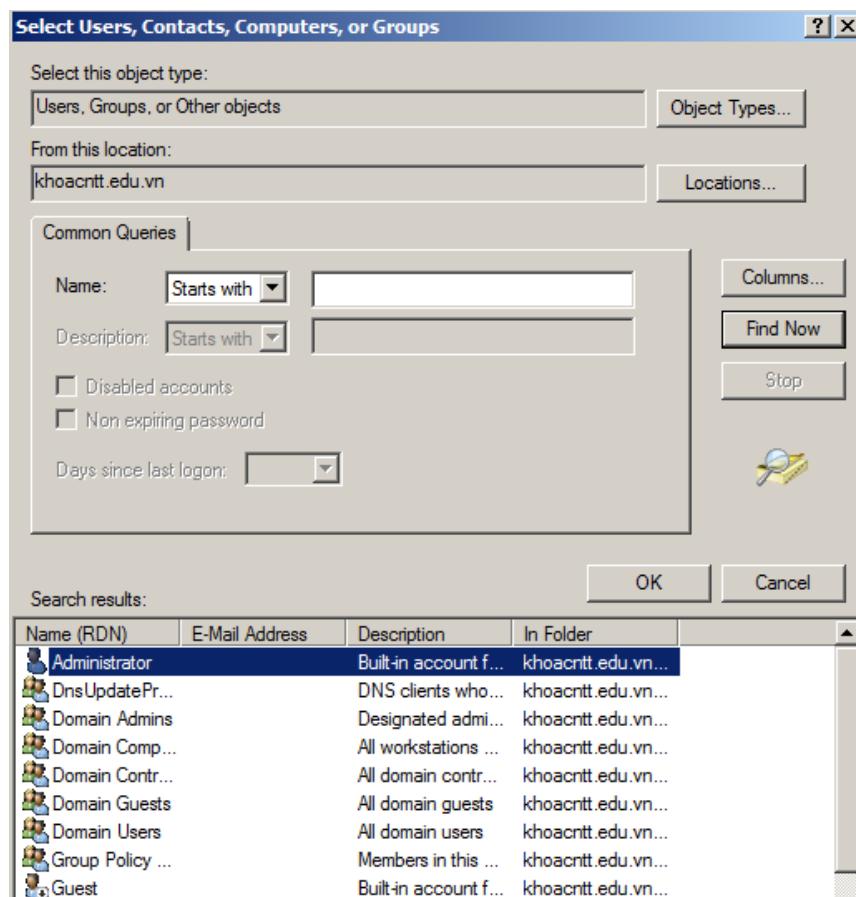


Hình 3.23: Cửa sổ đặc tính của nhóm với trang General

Để thêm bớt các thành viên cho nhóm ta chọn trang **Members** như Hình 3.24. Tiếp theo nhấn nút **Add** để mở cửa sổ chọn thành viên như hình 3.25. Tại cửa sổ này ta chọn các thành viên ở khung **Name**, rồi nhấn **Add** để đưa tạm vào khung bên dưới, cuối cùng nhấn **OK** để đưa các thành viên đã chọn ở đây ra cửa sổ Hình 3.24. Tại cửa sổ Hình 3.24, nếu muốn loại tư cách thành viên của đối tượng nào đó, thì ta chọn đối tượng đó, rồi nhấn **Remove**. Để kết thúc việc thêm bớt thành viên cho nhóm, ta nhấn **OK**.



Hình 3.24: Cửa sổ thêm thành viên mới cho nhóm



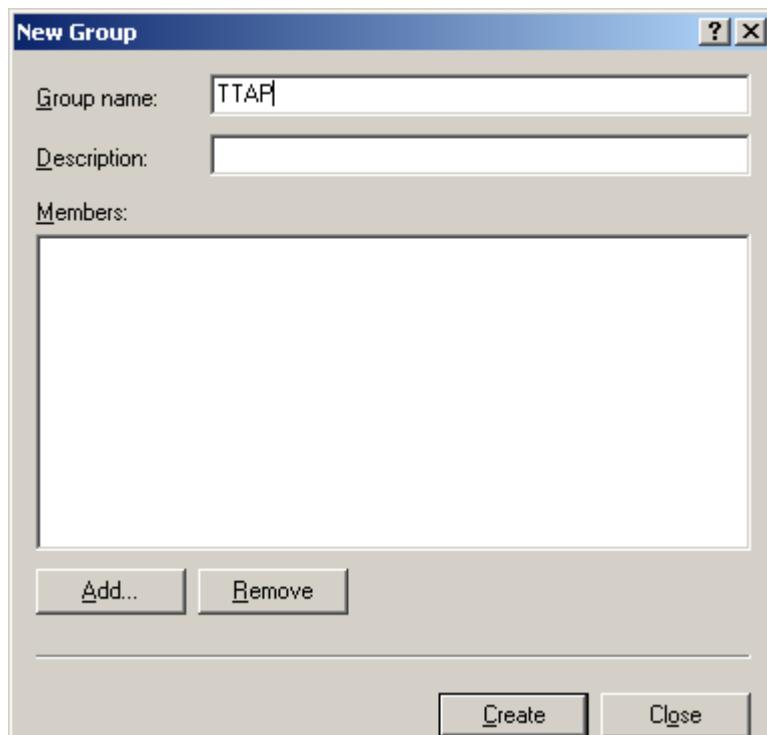
Hình 3.25: Cửa sổ chọn thành viên mới

3.3.6.3. Các thao tác khác với nhóm

Việc thực hiện các thao tác như: di chuyển nhóm tới nơi chứa mới, đổi tên nhóm, xoá nhóm, được thực hiện tương tự như với người sử dụng của miền.

3.3.7. Tạo và quản lý tài khoản nhóm của máy

Để tạo ra các tài khoản nhóm của máy, ta mở cửa sổ Computer Management, chọn **Local Users and Groups/Groups**, mở menu Action, chọn New Group, để hiện ra cửa sổ khai báo như Hình 3.26.



Hình 3.26: Cửa sổ tạo nhóm mới

Trong đó các mục:

Group name: được dùng để vào tên nhóm (tên có thể là các ký tự tuỳ ý và có thể dài tới 64 ký tự).

Description: dùng để vào dòng mô tả tuỳ ý về nhóm

Add: để thêm các thành viên vào nhóm

Remove: để loại bỏ thành viên của nhóm

Các thao tác thêm bớt thành viên của nhóm được thực hiện tương tự như nhóm của miền.

Kết thúc tạo nhấn Create. Ra khỏi cửa sổ tạo nhấn Close

Khi nhóm đã được tạo:

Nếu cần thêm bối thành viên cho nhóm nào thì ta chọn nhóm đó, chọn **Properties** từ menu **Action**, sau đó tiến hành các thao tác thêm bối thành viên như khi đang tạo.

Các thao tác khác như: đổi tên nhóm, xoá nhóm, được thực hiện tương tự như nhóm của miền.

3.4. CÁC QUYỀN HẠN NGƯỜI DÙNG

Quyền sử dụng của người dùng trên mạng Windows server được kiểm soát theo hai cách: bằng cách cấp cho người dùng các quyền hạn (**Rights**), tức là ban cho hoặc bác bỏ khả năng truy cập vào một vài đối tượng hệ thống (ví dụ khả năng đăng nhập vào một server), và bằng cách trao cho các đối tượng những quyền truy cập hay giấy phép truy cập (**Permissions**), tức là chỉ định ai được phép dùng các đối tượng nào và được dùng ở mức nào (ví dụ cấp quyền truy cập **Read** đối với một thư mục cụ thể cho một người dùng cụ thể).

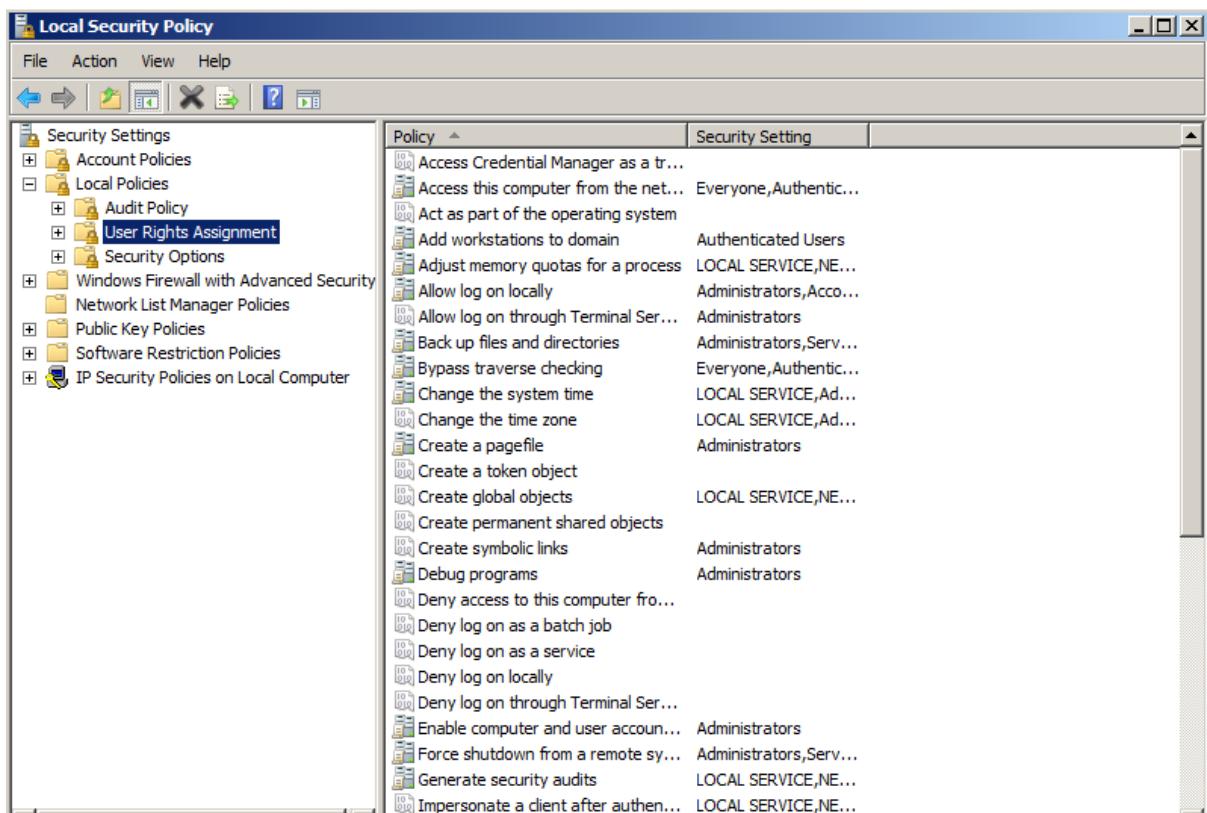
Quyền hạn của một người dùng cho phép họ thực hiện một số tác vụ hệ thống. Trong khi các quyền truy cập lại áp dụng cho các đối tượng cụ thể như các tập tin, thư mục và máy in.

Theo nguyên tắc, các quyền hạn người dùng được ưu tiên hơn các quyền hạn truy cập đối tượng. Ví dụ nếu một người dùng là thành viên của nhóm lưu trữ dự phòng **Backup Operators**, thì khi thực hiện việc lưu dự phòng, họ luôn có quyền đọc (Read) tất cả các thư mục và tập tin trên Server, mặc dù người chủ sở hữu của các thư mục và tập tin có thể bác bỏ quyền truy cập **Read** đối với mọi thành viên thuộc nhóm **Backup Operators**. Tuy nhiên các quyền hạn của nhóm **Backup Operators** chỉ có hiệu lực cùng với một thủ tục lưu dự phòng, nên họ vẫn không thể mở các tập tin trên server và đọc nội dung của nó, nếu không có quyền truy cập tương ứng.

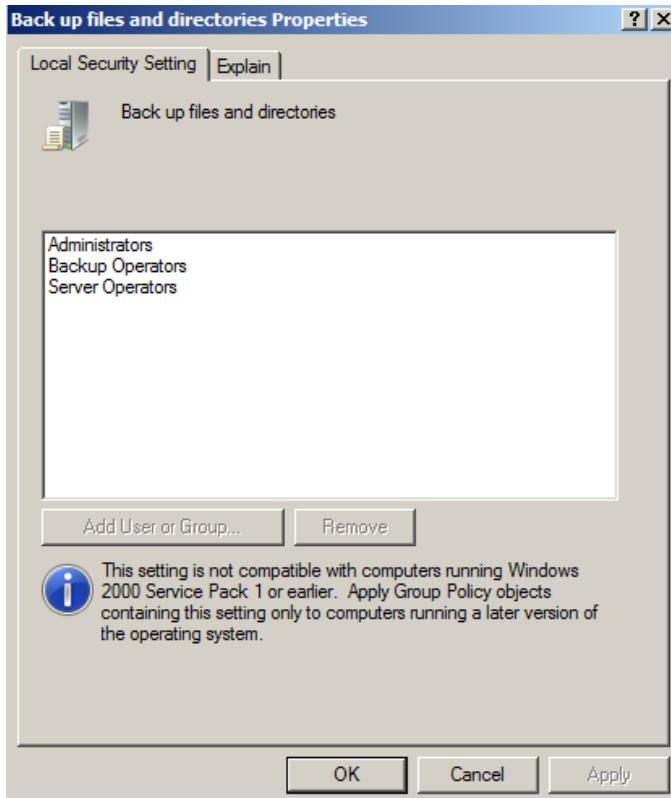
Các nhóm được tạo sẵn của Windows Server có một số quyền hạn đã được cấp sẵn cho chúng, ta cũng có thể tạo ra các nhóm mới rồi cấp một bộ quyền hạn người dùng theo ý riêng cho các nhóm đó. Nhờ đó, việc kiểm soát tính bảo mật sẽ dễ dàng hơn nhiều so với cách cấp các quyền hạn riêng lẻ cho từng người.

Để xem hoặc sửa đổi sự cấp quyền hạn cho một người dùng hoặc nhóm, từ mục **Administrative Tools**, ta mở cụm cụ **Local Security Policy** trên máy. Khi đó một danh sách các quyền hạn sẽ được hiện ra trong mục **User Rights Assignment** như Hình 3.27.

Để thêm hoặc bớt một quyền hạn nào đó cho một người dùng hoặc nhóm, ta chọn quyền hạn đó, chọn **Security** từ menu **Action**. Như trong Hình 3.28 ta thấy một số đối tượng đã được gán quyền **Back up files and directories**.



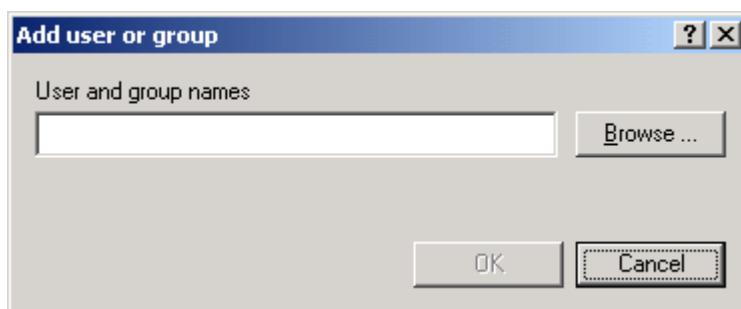
Hình 3.27: Danh sách các quyền hạn người dùng



Hình 3.28: **Thêm bớt đối tượng được cấp quyền hạn người dùng**

Để tước bỏ quyền này đối với một đối tượng nào đó, ta chọn đối tượng đó rồi nhấn nút **Remove**.

Để cấp thêm quyền này cho một nhóm hoặc người dùng, ta nhấn nút **Add**, rồi gõ vào tên người dùng hoặc nhóm cần thêm vào mục **User and group name** trong cửa sổ Hình 3.29, hoặc có thể nhấn nút **Browse** để tìm chọn. Cuối cùng nhấn **OK**. Bảng 3.4 liệt kê các quyền hạn người dùng và giải thích ý nghĩa của chúng.



Hình 3.29: **Cửa sổ chọn đối tượng mới để cấp quyền hạn người dùng**

Bảng 3.4. Các quyền hạn người dùng

Quyền hạn	Ý nghĩa
Access this computer from the network	Nối kết vào máy này ngang qua mạng.
Act as part of the operating system	Đóng vài trò như một phần được uỷ quyền của hệ điều hành. Một số tiểu hệ thống được cấp quyền hạn này.
Add workstations to domain	Thêm các máy trạm vào miền.
Back up files and directories	Lưu dự phòng các tập tin và thư mục. Quyền này phủ quyết các quyền truy cập tập tin và thư mục.
Bypass traverse checking	Duyệt lướt qua một cây thư mục, cho dù người dùng đó không có quyền truy cập nào đối với thư mục đó.
Change the system time	Ánh định giờ đồng hồ trong máy tại chỗ.
Create a pagefile	Tạo một tập tin phân trang (bộ nhớ ảo)
Create a token object	Tạo các thẻ hiệu truy cập (access token). Chỉ bộ phận Local Security Authority mới có quyền này.
Create permanent shared objects	Tạo những đối tượng vĩnh viễn đặc biệt.
Debug programs	Gỡ rối các ứng dụng.
Deny access to this computer from the network	Ngược lại với quyền Access this computer from the network, thu hồi riêng quyền này đối với những người dùng hay nhóm mà bình thường họ vẫn có.
Deny logon as a batch job	Thu hồi quyền Logon as a batch job.

Deny logon as a service	Thu hồi quyền Logon as a service.
Deny logon locally	Thu hồi quyền Logon locally.
Enable computer and user accounts to be trusted for delegation	Chỉ định các tài khoản có thể được ủy quyền.
Force shutdown from a remote system	Buộc máy này phải tắt đi từ một máy ở xa.
Generate security audits	Tạo ra các đề mục ghi chép kiểm toán.
Increase quotas	Tăng các hạn ngạch của đối tượng (mỗi đối tượng có một hạn ngạch được cấp cho nó).
Increase scheduling priority	Tăng cường độ ưu tiên lịch biểu của một quá trình xử lý.
Load and unload device drivers	Thêm/bớt các trình điều khiển thiết bị vào/ra khỏi hệ thống.
Lock pages in memory	Khoá chặt các trang vào trong bộ nhớ để ngăn không cho chúng bị đưa vào trong bộ lưu trữ dự phòng.
Logon as a batch job	Đăng nhập vào hệ thống như một phương tiện hàng đợi theo lô (batch queue facility).
Logon as a service	Thực hiện các dịch vụ bảo mật (ví dụ, người dùng mà thực hiện việc sao chép sẽ đăng nhập với tư cách như một dịch vụ).
Logon locally	Đăng nhập tại chỗ, tại chính máy server này.
Manager auditing and security log	Chỉ rõ những loại sự kiện và kiểu truy cập tài nguyên gì sẽ được kiểm toán. Ngoài ra còn cho phép xem và xoá sạch bản ghi chép bảo mật (security log).

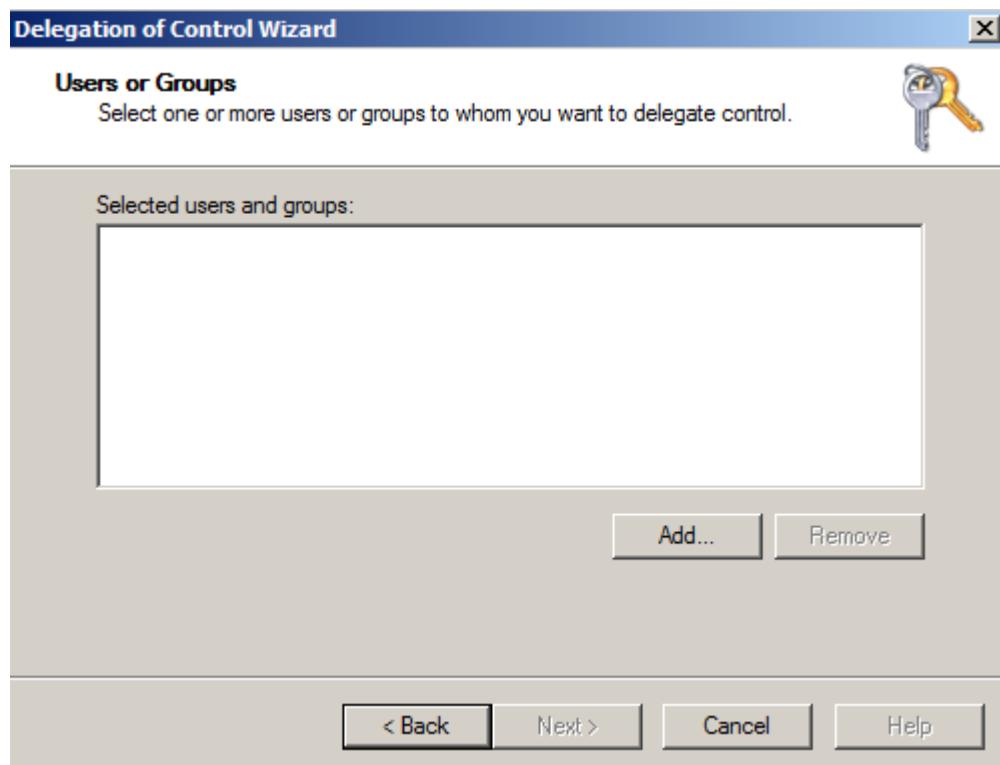
Modify firmware environment values	Sửa đổi các biến môi trường của hệ thống (không phải biến môi trường của người dùng).
Profile single process	Sử dụng những khả năng ghi chép hoạt động (profiling) của Windows 2000 để quan sát, nhận xét hoạt động của một quá trình xử lý.
Profile system performance	Sử dụng các khả năng ghi chép hoạt động của Windows 2000 để quan sát, nhận xét hoạt động của hệ thống.
Remove computer from docking station	Tháo gỡ một máy tính ra khỏi hộp nối ghép vào mạng (docking station) của nó.
Replace a process level token	Sửa đổi thẻ hiệu truy cập của một quá trình.
Restore files and directories	Khôi phục lại các tập tin và thư mục. Quyền này phủ quyết các quyền truy cập tập tin và thư mục.
Shut down the system	Tắt máy Windows 2000.
Synchronize directory service data	Cập nhật thông tin của Active Directory.
Take ownership of files or other objects	Chiếm quyền sở hữu của các tập tin, thư mục, và các đối tượng khác, mà trước đó được những người dùng khác sở hữu.

3.5. ỦY THÁC QUYỀN QUẢN LÝ OU

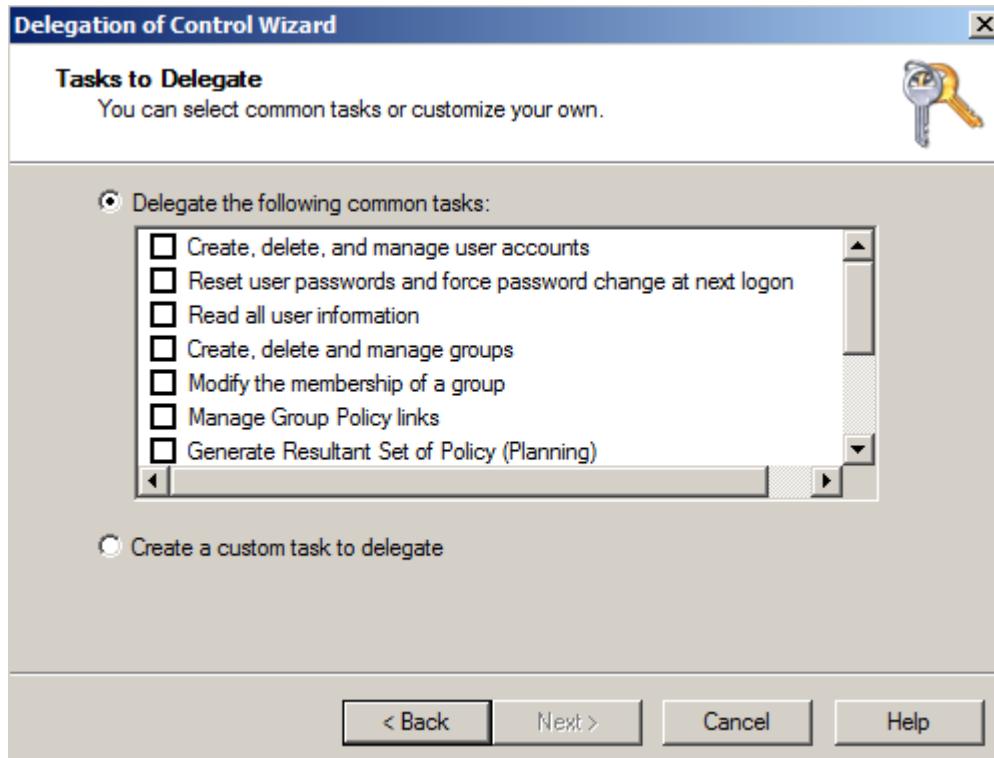
Việc ủy thác quyền quản lý OU là nhằm trao cho các đối tượng nào đó (có thể là User hoặc nhóm) có những quyền hành nào đó đối với các đối tượng nằm trong OU như các quyền: Tạo và quản lý các Users hoặc nhóm trong OU, đặt lại mật khẩu của các người dùng trong OU.

Để ủy thác quyền quản lý OU cho các đối tượng trong menu **Action** chọn **Delegate Control** nhấn **Next** tại cửa sổ ban đầu để chuyển đến cửa sổ (như Hình

3.30) cho phép ta đưa thêm các người dùng và nhóm mà ta muốn ủy thác quyền quản lý OU. Nhấn nút **Add** từ cửa sổ này, rồi chọn đối tượng cần ủy thác, Nhấn **Add, OK** để quay về cửa sổ Hình 3.30. Khi đó đối tượng được ủy thác sẽ xuất hiện trong cửa sổ này, tiếp theo ta chọn đối tượng này và nhấp **Next**, rồi chọn quyền hạn cho đối tượng trong số những công việc thông thường (common tasks) có thể ủy thác (xem Hình 3.31). Cuối cùng nhấn **Next**, rồi nhấn **Finish**.



Hình 3.30: Giao diện ủy thác quản lý OU



Hình 3.31: Các quyền hạn ủy thác

Quyền hạn	Ý nghĩa
Create, delete, and manage user accounts	Có quyền tạo, xóa và quản lý tài khoản người dùng
Reset user passwords and force password change at next logon	Có quyền thiết lập lại mật khẩu người dùng và buộc người dùng phải thay đổi mật khẩu trong lần đăng nhập kế tiếp
Read all user information	Có quyền đọc tất cả thông tin của người dùng
Create, delete, and manage groups	Có quyền tạo, xóa và quản lý tài khoản nhóm
Modify them membership of a group	Có quyền thay đổi thành viên trong nhóm

Bảng 3.5. Các quyền hạn

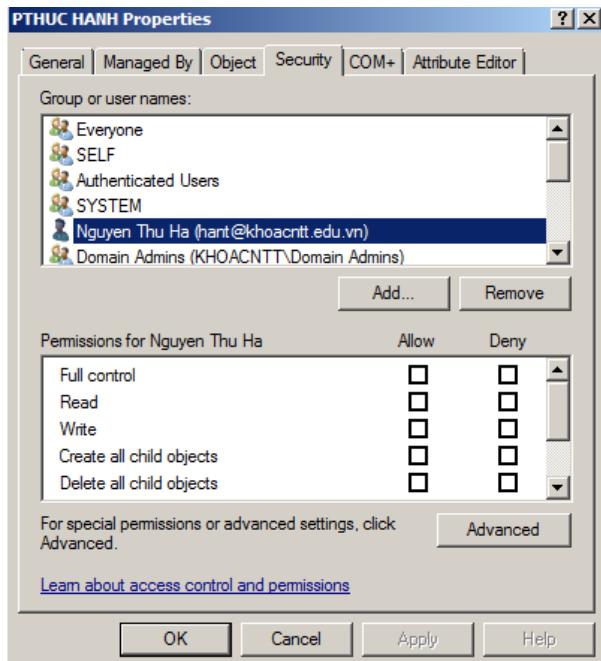
Nếu muốn bỏ quyền quản trị đã ủy thác cho OU, tại cửa sổ Active Directory Users and Computers, ta chọn View/Advanced Features, để hiện ra cửa sổ như Hình 3.32.

The screenshot shows the 'Active Directory Users and Computers' window. On the left, there is a navigation pane with icons for 'Saved Queries', 'khoacntt.edu.vn' (which is expanded to show 'BuiltIn', 'Computers', 'Domain Controllers', 'ForeignSecurityPrincipals', 'LostAndFound', 'Program Data', 'PTHUC HANH', 'System', 'Users', and 'NTDS Quotas'), and 'Infrastructure'. On the right, there is a table titled 'Name' with columns for 'Type' and 'Description'. The table lists several objects:

Name	Type	Description
Builtin	builtinDomain	
Computers	Container	Default container for upgr...
Domain Cont...	Organizational ...	Default container for dom...
ForeignSecur...	Container	Default container for secu...
Infrastructure	infrastructureU...	
LostAndFound	lostAndFound	Default container for orph...
NTDS Quotas	msDS-QuotaCo...	Quota specifications cont...
Program Data	Container	Default location for storag...
PTHUC HANH	Organizational ...	
System	Container	Builtin system settings
Users	Container	Default container for upgr...

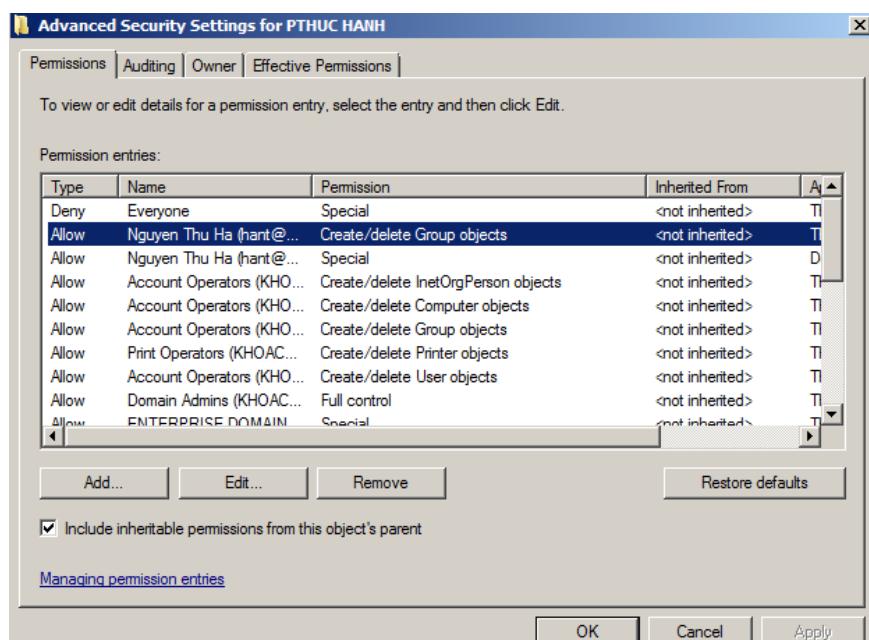
Hình 3.32: Cửa sổ Active Directory Users and Computers ở chế độ xem Advanced Features

Sau đó nhấn phải chuột tại OU cần chọn, chọn Properties để hiện ra cửa sổ đặc tính, tại đây nhấn chuột tại mục Security sẽ thấy cửa sổ như Hình 3.33



Hình 3.33:Trang Security của OU được chọn

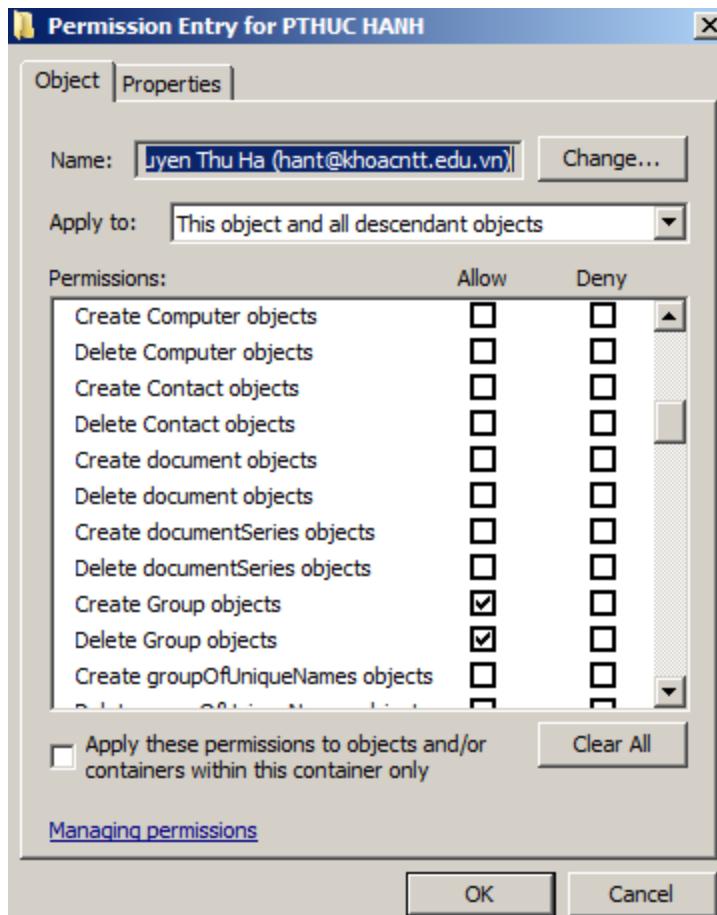
Tiếp theo nhấn nút Advanced để màn hình như Hình 3.34 hiện lên.



Hình 3.34:Những thiết định chi tiết của OU được chọn

Tại cửa sổ này, nếu muốn bỏ những thiết định đã trao cho đối tượng nào thì ta chọn nó rồi nhấn nút Remove. Còn nếu muốn xem/chỉnh sửa lại các quyền

đã trao cho đối tượng nào đó, thì ta chọn nó, rồi nhấn nút **View/Edit** để hiện ra cửa sổ như Hình 3.35



Hình 3.35:Các quyền hạn có thể trao cho đối tượng

Tại đây, nếu muốn trao quyền nào đó thì ta đánh dấu chọn tại cột Allow. Còn nếu không muốn trao thì ta bỏ đánh dấu chọn tại cột này.

3.6. TỔNG KẾT CHƯƠNG

Nội dung chương này đã trình bày chi tiết hoạt động cơ bản nhất trong quản trị hệ thống mạng đó là quản lý các đối tượng bao gồm: OU, tài khoản người dùng, tài khoản nhóm.

Quản lý OU là hoạt động phân chia miền thành các OU để quy hoạch công việc quản trị theo các đơn vị tổ chức cũng như phân quyền quản trị cho các nhóm điều hành khác nhau một cách đồng bộ. Một miền được chia thành các phân vùng

lô-gic nhỏ hơn chính là các OU. Vì thế các đối tượng quản trị như người dùng, nhóm, v.v. phải được định danh duy nhất trên toàn miền. Mỗi OU có thể được chia thành các OU con để phân cấp quản lý và mở rộng không gian tên. Các thông tin về OU được lưu trữ trong cơ sở dữ liệu Active Directory và được quản trị trong mục **Active Directory Users and Computers**. Quản lý OU gồm ba chức năng chính là tạo, sửa và xóa OU.

Quản lý tài khoản người dùng là một trong những hoạt động trung tâm và cốt lõi của quản trị mạng. Có hai loại tài khoản người dùng là tài khoản người dùng của máy và tài khoản người dùng của miền. Tài khoản người dùng của máy được lưu trữ riêng tại các máy trạm, sử dụng để đăng nhập cục bộ. Tất cả các tài khoản người dùng của miền được lưu trữ trong cơ sở dữ liệu Active Directory của máy điều khiển miền và được sử dụng đăng nhập vào mạng. Các hoạt động chính trong quản lý tài khoản người dùng bao gồm: tạo/xóa người dùng, chỉnh sửa thông tin, phân quyền người dùng, phân bổ người dùng vào nhóm, v.v.

Các quyền hạn người dùng cũng được phân thành hai loại đó là quyền cục bộ (Right) và quyền truy cập (Permission).

Quản lý tài khoản nhóm là hoạt động quan trọng hỗ trợ quản lý người dùng, giúp phân nhóm các tài khoản người dùng theo vai trò, chức năng và hoạt động khai thác hệ thống mạng. Khác với OU là một phân vùng lô-gic chứa mọi đối tượng, nhóm là khoản mục chứa người dùng và các nhóm con. Các loại nhóm bao gồm: nhóm bảo mật, nhóm cục bộ, nhóm toàn miền, nhóm toàn rừng và các nhóm đặc biệt. Các hoạt động chính trong quản lý tài khoản nhóm là tạo/ xóa/ cập nhật thông tin nhóm, cấu trúc các nhóm con trong nhóm, phân bổ/ loại bỏ người dùng trong nhóm.

Ủy thác quyền quản lý OU cho phép phân bổ quyền quản lý OU cho người dùng và nhóm. Việc này giúp quản lý tiện dụng và đồng bộ hơn. Có thể ủy thác quyền quản lý OU trực tiếp cho người dùng hoặc cho một nhóm người dùng.

CÂU HỎI VÀ BÀI TẬP THỰC HÀNH

Câu 1. Nêu sự khác nhau giữa tài khoản người dùng của máy và tài khoản người dùng của miền.

Câu 2. Thực hành tạo tài khoản người dùng của máy và tài khoản người dùng của miền, cùng với các thao tác: sửa, xoá, đổi tên, di chuyển và thay đổi các thiết định người dùng.

Câu 3. Nêu khái niệm nhóm, các loại nhóm của Windows Server. Trình bày sự khác nhau giữa nhóm bảo mật và nhóm phân phối thư tín.

Câu 4. Trình bày các loại nhóm bảo mật và sự khác nhau giữa chúng.

Câu 5. Thực hành tạo ra các loại nhóm bảo mật và thêm bớt các thành viên cho nhóm. Sau đó thực hiện các thao tác sửa đổi, xoá và di chuyển nhóm.

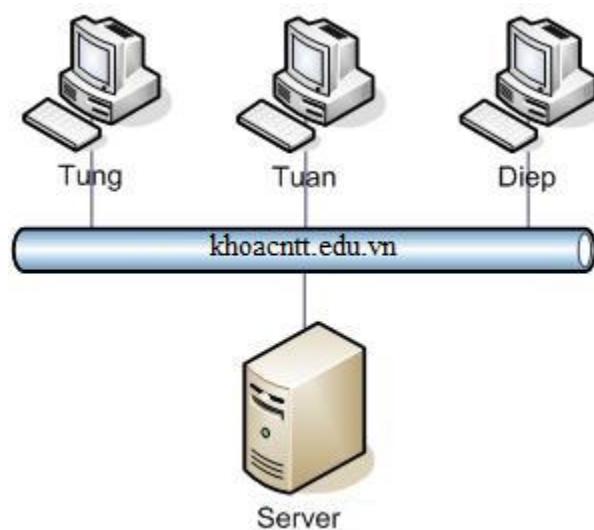
Câu 6. Phân biệt giữa quyền hạn (Rights) và quyền truy cập (Permissions) trên mạng.

Câu 7. Thực hành trao một số quyền hạn cho những đối tượng nào đó, và tước bỏ những quyền hạn đã trao cho các đối tượng.

Câu 8. So sánh giữa OU và nhóm.

Câu 9. Thực hành uỷ thác quyền quản lý OU cho các đối tượng.

Bài thực hành 1. Tạo và quản lý người dùng trên Domain theo yêu cầu
Với hệ thống mạng như trong hình sau:



Anh/Chị hãy tạo tài khoản người dùng và nhóm cho Công ty theo yêu cầu sau:

Nhóm BanGiamDoc gồm: Hung, TrongNhóm NhanVien gồm: Diep, Tuan, Tung. Sau đó, Anh/Chị hãy cấp quyền các tài khoản theo yêu cầu sau:

Tài khoản TUNG chỉ có thể đăng nhập từ máy TUNG, và phải thay đổi mật khẩu ở lần đăng nhập đầu tiên. Tài khoản DIEP chỉ sử dụng đến ngày 30.09.2008 thì sẽ bị khóa. Tài khoản này chỉ có thể đăng nhập trong giờ hành chánh. Tài khoản này không được phép đổi mật khẩu.

Bài thực hành 2. Cấp quyền cho các tài khoản người dùng VỚI hệ thống mạng như trong lab1, Anh/Chị muốn cấp quyền cho người dùng theo yêu cầu sau:

- Tài khoản TUNG có quyền thêm, xóa, sửa tài khoản người dùng.
- Tài khoản DIEP có quyền backup server.
- Tài khoản TUAN có quyền quản lý máy in.

CHƯƠNG 4. CHÍNH SÁCH NHÓM

Chính sách nhóm (Group policy) là một tập các thiết lập cấu hình cho máy tính hoặc người dùng, để áp dụng đồng thời cho nhiều đối tượng trong một OU, một miền hoặc một địa bàn (SDOU – Site, Domain, OU). Chính sách nhóm là một công cụ hữu hiệu giúp cho người quản trị có thể quản lý và điều hành mạng một cách thuận tiện và hiệu quả. Chương này sẽ trình bày các hoạt động quản lý chính sách nhóm để quản trị nhanh chóng, thống nhất, đồng bộ và hiệu quả cho các mạng lớn. Nội dung chương được tổ chức như sau: *Mục 4.1* trình bày về chức năng, phân loại và cách sử dụng chính sách nhóm; *Mục 4.2* trình bày các bước tạo chính sách nhóm; *Mục 4.3* trình bày vấn đề Ủy thác quyền quản trị chính sách nhóm; *Mục 4.4* trình bày vấn đề Quảng bá/ phân bổ gói phần mềm; *Mục 4.5* trình bày việc quản lý các gói phần mềm đã quảng bá/phân bổ; *Mục 4.6* tổng kết các nội dung của chương.

4.1. CHỨC NĂNG, PHÂN LOẠI VÀ SỬ DỤNG CHÍNH SÁCH NHÓM

Chức năng của chính sách nhóm:

Bằng chính sách nhóm ta có thể thực hiện một số công việc sau:

- **Triển khai phần mềm ứng dụng:** Ta có thể thu thập tất cả những tập tin cần thiết để cài đặt một phần mềm nào đó vào trong một gói (package), đặt gói này lên một server ở đâu đó, rồi dùng các chính sách nhóm để hướng các máy trạm của một số người dùng đến gói này, để họ thấy rằng gói phần mềm đó có thể dùng được (những công việc này được thực hiện từ một vị trí trung tâm mà không cần ghé đến từng máy trạm). Ngay lần đầu tiên các người dùng ấy thử khởi động ứng dụng đó, nó sẽ được tự động cài đặt lên máy trạm của họ, mà không cần họ phải can thiệp gì cả.
- **Ấn định quyền hạn của người dùng:** Thông thường việc ấn định các quyền hạn người dùng phải thực hiện trên từng máy. Với chính sách nhóm công việc đó có thể được thực hiện ở một vị trí trung tâm.

- **Giới hạn những ứng dụng mà người dùng được phép sử dụng:** Ta có thể kiểm soát máy trạm của một người dùng nào đó đến mức chỉ cho họ có thể chạy một số ít ứng dụng.
- **Kiểm soát những thiết định trên các hệ thống của Windows server**
- **Thiết lập các kịch bản đăng nhập (logon), đăng xuất (logoff), khởi động (startup), và tắt máy (shutdown):** Windows Server cho phép bắt kỳ một trong bốn sự kiện trên kích hoạt một kịch bản, và các chính sách nhóm dùng để kiểm soát những gì mà các kịch bản đó chạy.
- **Đơn giản hóa và hạn chế các chương trình:** Ta có thể dùng chính sách nhóm để gỡ bỏ nhiều tính năng của các ứng dụng như: Internet Explorer, Windows Explorer và nhiều chương trình khác.
- **Hạn chế tổng quát màn hình desktop:** Bằng chính sách nhóm, ta có thể gỡ bỏ hầu hết hoặc tất cả các đề mục trên menu **Start** của một người dùng, giữ không cho họ cài đặt thêm máy in, không cho phép họ đăng xuất hoặc sửa đổi tí gì trong cấu hình desktop của họ cả. thậm chí có thể khoá chặt máy trạm của một người dùng.

Phân loại chính sách nhóm

Các quản trị viên định cấu hình và triển khai các chính sách nhóm bằng cách xây dựng các *đối tượng chính sách nhóm* (Group Policy Object – GPO). Các GPO là các khoang chứa dành cho tập hợp các thiết định về quản trị và bảo mật, có thể được áp dụng cho các tài khoản người dùng và tài khoản máy trên mạng.

Có hai mục chính trong một GPO là **Computer configuration** và **User configuration**. Các chính sách thuộc Computer configuration dùng để kiểm soát các thiết định đặc trưng cho máy, nên được áp dụng vào lúc khởi động máy và sau những khoảng thời gian định sẵn được làm tươi. Các chính sách thuộc User configuration dùng để kiểm soát các thiết định đặc trưng cho người dùng, nên được áp dụng cho các môi trường làm việc của người dùng vào lúc đăng nhập và cũng sau những khoảng thời gian định sẵn được làm tươi.

Sử dụng chính sách nhóm

Trái ngược với cái tên của chúng, các chính sách nhóm lại không được áp dụng một cách trực tiếp cho các nhóm hoặc người dùng, mà chỉ có thể áp dụng

cho các địa bàn (site), các miền (domain), và các OU (Microsoft viết tắt chúng là SDOU).

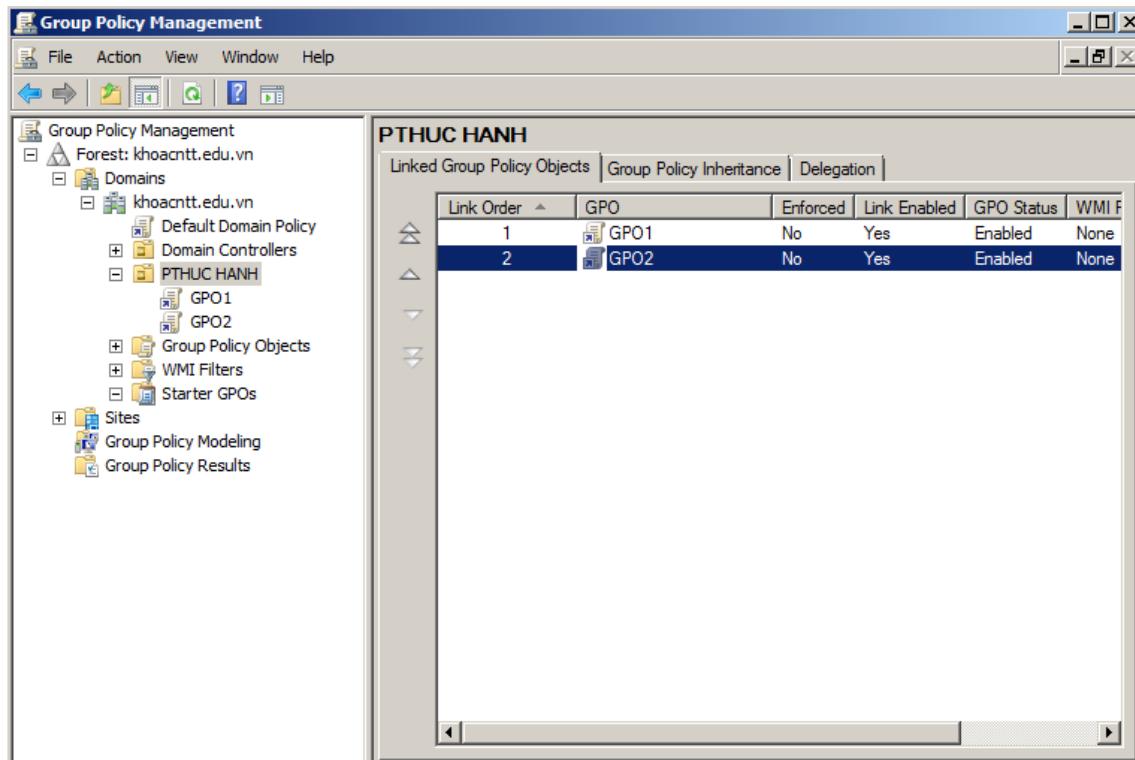
Sự áp dụng một GPO cho một SDOU được gọi là *sự liên kết* (linking). Mỗi quan hệ giữa GPO và SDOU có thể là từ nhiều đến một hoặc là một đến nhiều, tức là có thể nhiều GPO cùng liên kết với một SDOU hoặc một GPO liên kết với nhiều SDOU.

Chỉ những người sử dụng, các nhóm và các tài khoản máy, trong các SDOU liên kết với một GPO, mới có thể áp dụng được GPO này.

- **Các chính sách nhóm được thừa kế và tích luỹ:** Các thiết định của chính sách nhóm áp dụng cho một cấp trong AD được tích luỹ và thừa kế từ các cấp bên trên. Ví dụ, miền **khoaacnnt.edu.vn** có vài GPO khác nhau. Có một GPO ở cấp miền, để ấn định những chính sách về hạn chế về mật khẩu, cách phong toả tài khoản, và các thiết định bảo mật thông thường. Mỗi OU cũng có một GPO, để triển khai và duy trì các ứng dụng máy trạm thông thường, và các hạn chế của máy trạm. Khi đó các người dùng và máy mà vừa ở trong miền vừa ở trong OU sẽ nhận được các thiết định từ cả chính sách cấp miền lẫn chính sách cấp OU. Như vậy một số chính sách có tính bao trùm, có thể được áp dụng cho toàn bộ miền, trong khi các chính sách khác lại được áp dụng riêng cẩn cứ theo OU.
- **Thứ tự áp dụng chính sách nhóm:** Các chính sách được áp dụng theo thứ tự: chính sách địa bàn, chính sách miền, chính sách OU, rồi đến các OU bên trong OU. Như vậy các chính sách ở mức bên trong sẽ được ưu tiên hơn các chính sách ở mức bên ngoài.
- **Các tùy chọn No Override và Block Policy inheritance:** Các tùy chọn này có trong GPO, dùng để lọc chặn các chính sách nhóm. Nếu chọn Block Policy inheritance thì sẽ ngăn không cho các chính sách cấp cao hơn lan truyền xuống. Nhưng nếu GPO ở cấp cao hơn chọn No Override thì các chính sách của nó vẫn được lan truyền xuống các cấp thấp hơn, cho dù các cấp thấp hơn có chọn Block Policy Inheritance.

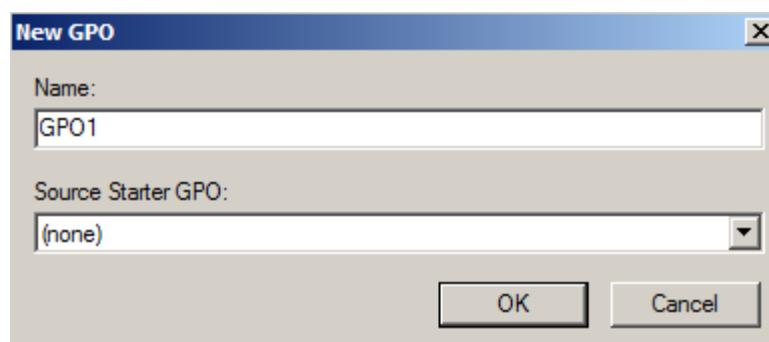
4.2. TẠO CÁC ĐỐI TƯỢNG CHÍNH SÁCH NHÓM

Từ cửa sổ màn hình Start/Administrative Tools/Group Policy management trang **Group Policy** như được minh họa trên Hình 4.1.



Hình 4.1: Giao diện Group Policy Management

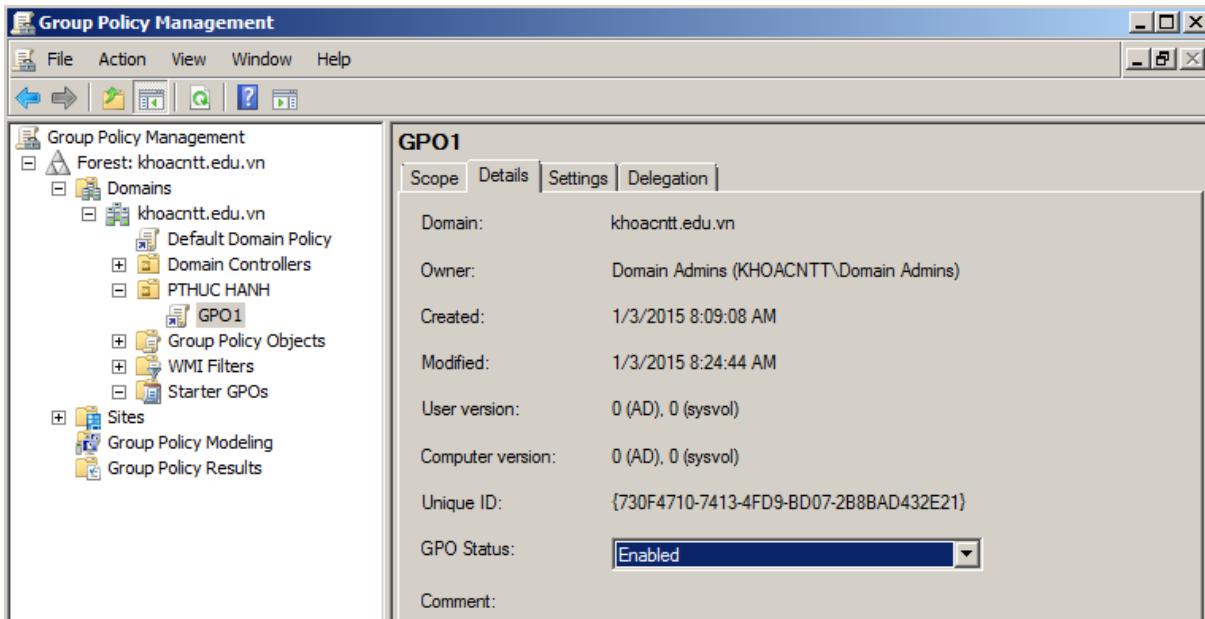
Trong cửa sổ trên ta thấy OU hiện tại là miền **khoaacntt.edu.vn** trong đó đã có 1 chính sách nhóm được liên kết với nó. Để tạo một GPO mới, ta nhấn **Action** chọn **Create a GPO in this domain**, Windows server tự đặt cho tên cho GPO mới là New Group Policy Object, và ta có thể sửa lại tên này. GPO mới tạo sẽ tự động liên kết với OU hiện tại như được minh họa trên Hình 4.2.



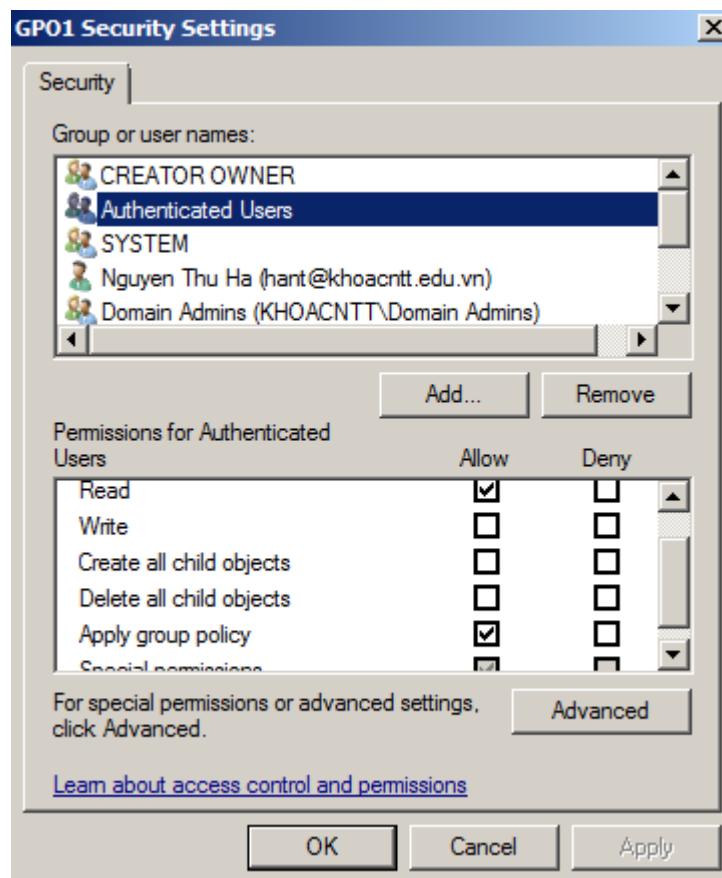
Hình 4.2: Giao diện tạo Group Policy Object

Để đổi tên một GPO, ta nhấp nút phải chuột tại tên cần đổi, chọn **Rename** từ menu ngữ cảnh, rồi gõ vào tên mới.

Cửa sổ trong Hình 4.1 dùng để xem và sửa đổi các đặc tính của GPO được chọn. Khi chọn nút này, trang **Details** trong cửa sổ đặc tính của GPO (xem Hình 4.3) cho thấy những thông tin về ngày tháng tạo lập (creation) và tu chỉnh (Modified), cũng như những tùy chọn cho phép vô hiệu hóa phần cấu hình người dùng hoặc cấu hình máy của GPO đó. Như đã trình bày ở trên, trong một GPO có thể có đồng thời hai loại thiết định là Computer configuration và User configuration. Tuy nhiên, tùy theo cách ta phân chia miền ra thành các OU, mà ta nên chọn tạo ra một số chính sách chỉ gồm các thiết định dành cho máy thôi, và một số chính sách khác chỉ gồm các thiết định dành cho người dùng thôi. Khi đó phần không được dùng đến của GPO nên chọn vô hiệu hoá, để sự áp dụng chính sách và cập nhật nó sẽ nhanh hơn. Trang **Scope** giúp ta tìm kiếm các site, domain, hoặc OU nào áp dụng GPO này, bằng cách tìm kiếm trong **Display links in this location**. Trang **Settings** cho phép cấu hình các chính sách nhóm áp dụng cho OU. Trang **Delegation** xác định các đối tượng được ủy thác sử dụng chính sách nhóm này trong đó **tab Security** trong **Advanced** liệt kê liệt kê danh sách các đối tượng được truy cập (tức ACL) mặc định và quyền truy cập tương ứng của đối tượng đó trên GPO này (xem Hình 4.4). Khi chọn một tên đối tượng nào đó ở bên trên, thì bên dưới sẽ hiện ra các quyền truy cập của đối tượng đó. Muốn thay đổi một chính sách cần có quyền **Read** và **Write**, còn muốn là đối tượng tiếp nhận chính sách, thì phải có quyền **Read** và **Apply Group Policy**.



Hình 4.3: Cửa sổ đặc tính của một GPO

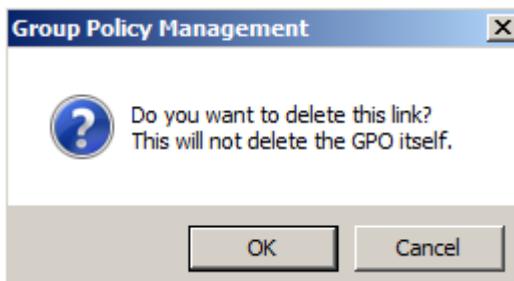


Hình 4.4: Danh sách các đối tượng được phép truy cập một GPO

Nhóm **Authenticated Users** bao gồm mọi người dùng đã đăng nhập vào mạng, mà như Hình 4.4, nhóm này được trao mặc định hai quyền Read và Apply. Điều đó có nghĩa là mọi người dùng trong SDOU đang xét đều có thể áp dụng chính sách này. Để ngăn không cho một đối tượng nào đó nhận được chính sách này, thì ta chọn nó và duyệt vào ô **Deny** của quyền **Apply Group Policy**. Nếu một thành viên thuộc cả hai nhóm A và B, nhóm A có thiết định Deny tại quyền Apply Group Policy, nhóm B không có thiết định này, thì thành viên đó cũng không được áp dụng chính sách này. Do vậy nếu ta đặt thiết định Deny với nhóm Authenticated Users, thì mọi người dùng trên mạng đều không được áp dụng chính sách này. Từ đây ta thấy, nếu muốn áp dụng chính sách này chỉ cho một số người dùng trong một nhóm A nào đó, thì trước ta phải loại nhóm Authenticated Users ra khỏi danh sách truy cập, bằng cách chọn nó rồi nhấn nút **Remove**. Sau đó nhấn nút **Add**, và chọn nhóm A để đưa vào danh sách truy cập, tiếp theo chọn duyệt ô **Allow** tại quyền **Apply Group Policy** cho nhóm này. Công việc này được gọi là **lọc chặn chính sách nhóm**.

Trở lại cửa sổ trong Hình 4.1, ta thấy có thể có nhiều GPO cùng liên kết với một OU. Trong trường hợp đó chúng sẽ được áp dụng từ dưới lên trên. Do đó, các GPO cao hơn trong danh sách sẽ có độ ưu tiên cao hơn. Nếu muốn sắp lại thứ tự của một GPO nào đó, ta chọn nó, rồi nhấn nút **Move Up** để chuyển lên trên một mức, hoặc **Move Down** để chuyển xuống dưới một mức.

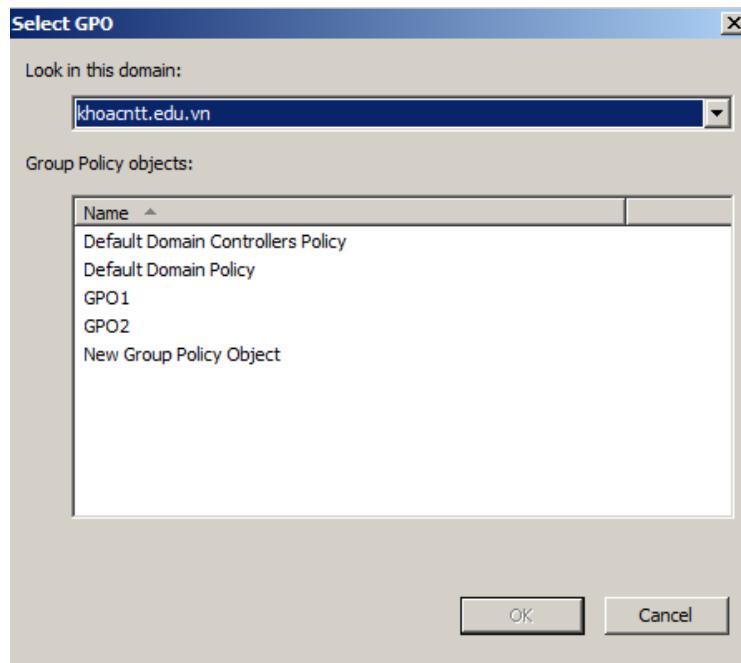
Để xoá bỏ một GPO, hoặc chỉ đơn giản để gỡ nó ra khỏi danh sách, ta chọn nó rồi nhấn Delete. Windows Server khi đó sẽ hiện ra cửa sổ như Hình 4.5



Hình 4.5: Việc tháo gỡ một GPO ra khỏi danh sách các GPO liên kết với OU hiện tại

Nếu muốn OU hiện tại liên kết với một GPO có sẵn, trong **Menu** ta chọn **Link an Existing GPO...** để hiện ra cửa sổ như Hình 4.6. Tại đây ta có thể tìm các kiếm

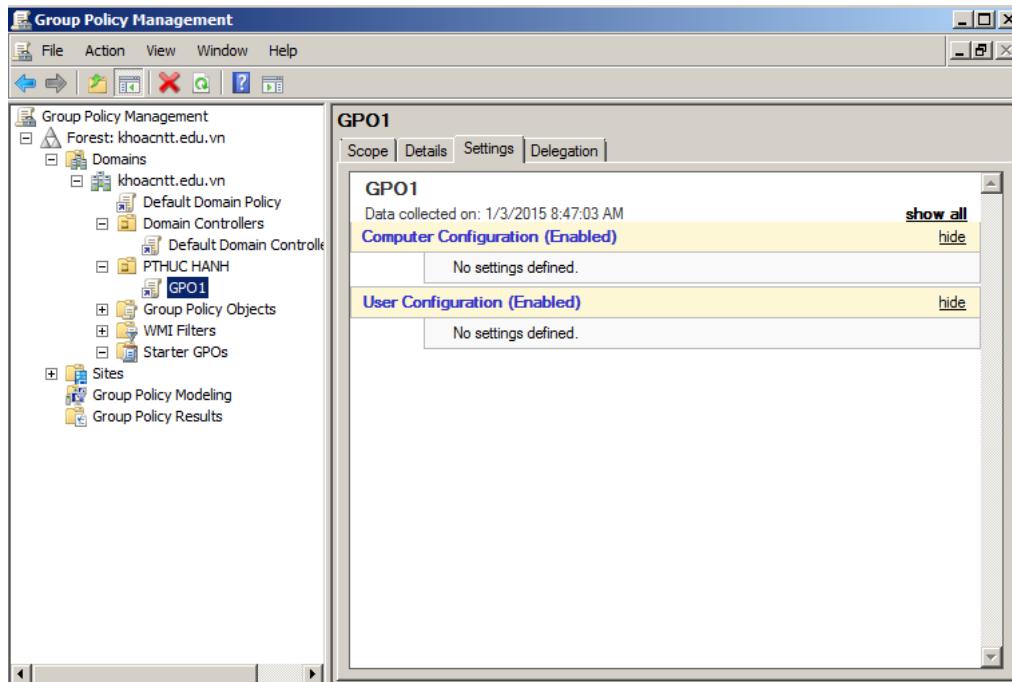
tất cả các GPO đã có. Sau đó chọn GPO cần dùng và nhấn **OK** để đưa nó vào danh sách trong cửa sổ Hình 4.6.



Hình 4.6: Các GPO có sẵn có thể liên kết với OU hiện tại

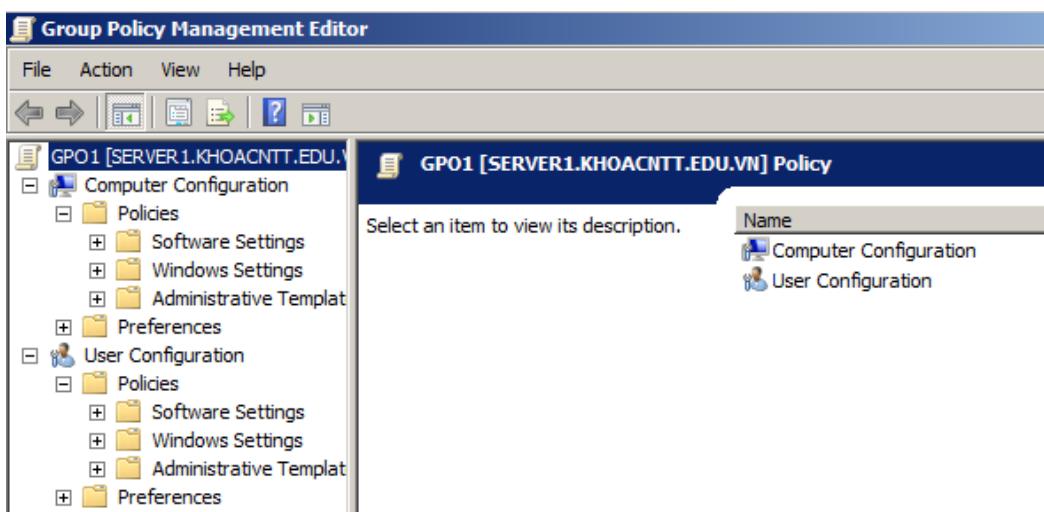
a. Một số thiết định cấu hình người dùng và cấu hình máy trong một GPO

Để xem và sửa đổi các thiết định cho một chính sách nhóm, từ cửa sổ Hình 4.7



Hình 4.7: Giao diện cấu hình GPO

Ta chọn GPO đó, rồi trong Menu của GPO nhấn **Edit** để hiện ra cửa sổ như Hình 4.8.



Hình 4.8: Cửa sổ đặt các thiết định của một chính sách nhóm

Như ta thấy trong hình trên, có hai đốt chính trong cấu trúc phân cấp bậc các thiết định của một chính sách nhóm là **User Configuration** và **Computer Configuration**. Cả hai đốt đó đều có những đốt con là: **Software Settings**, **Windows Settings**, và **Administrative Settings**. Sự khác biệt giữa hai đốt đó là:

các chính sách được ấn định cho User Configuration sẽ áp dụng vào các thiết định của người dùng, trong khi các chính sách được ấn định cho Computer Configuration thì sẽ áp dụng cho cấu hình máy. Đối với cả User Configuration và Computer Configuration, mục Software Installation có thể được dùng để phát hành, phân phối, cập nhật, và thậm chí gỡ bỏ các ứng dụng ra khỏi máy trạm của người dùng nào đó.

b. Các thiết định bảo mật trong một chính sách nhóm

Phần lớn các thiết định bảo mật được tìm thấy trong mục **Computer Configuration\Windows Settings\Security Settings**. Sau đây là phần tóm tắt những nhóm thiết định chính trong **Security Settings**.

Account Policies: Chỉ định những hạn chế đối với mật khẩu, các chính sách khoá chặc tài khoản.

Local Policies: Ấn định chế độ kiểm toán, cấp phát các quyền hạn người dùng và các thiết định bảo mật khác.

Event Log: Tập trung hoá các tuỳ chọn cấu hình dành cho tập tin ghi chép sự cố (event log).

Restricted Groups: Áp đặt và kiểm soát các tư cách thành viên nhóm đối với một số nhóm, như nhóm Administrator.

System Services: Triển khai hàng loạt các cấu hình dịch vụ và phòng ngừa các thay đổi.

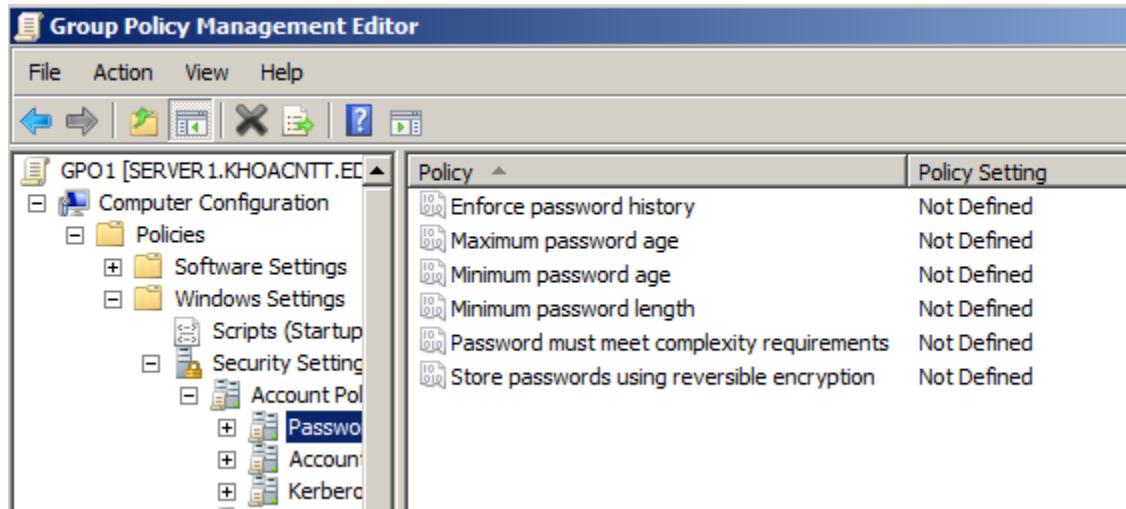
File System: Tạo ra các khuôn mẫu bảo mật đối với các quyền truy cập trên các tập tin và thư mục, nhằm bảo đảm rằng các tập tin và thư mục đó có và giữ các quyền truy cập mà ta cần.

Public Key Policies: Quản lý các thiết định dành cho các công ty hay cơ quan, bằng cách sử dụng một cơ sở hạ tầng khoá công khai.

c. Sử dụng chính sách nhóm để ấn định mật khẩu và chính sách khoá chặc tài khoản

Một chú ý quan trọng đối với các chính sách nhóm về mật khẩu và chính sách khoá chặt tài khoản là: chúng chỉ được áp dụng ở cấp miền. Các máy DC sẽ nhận được các thiết định của chúng từ các chính sách tài khoản cấp miền, và lờ đi những thiết định trong các chính sách được liên kết với các OU.

Các chính sách về ẩn định mật khẩu được tìm thấy trong **Computer Configuration\Windows Settings\Security Settings\ Account Policies\ Password Policy**, như phần bên phải của Hình 4.9.



Hình 4.9. Các thiết định về mật khẩu

Như trên ta thấy các thiết định về mật khẩu ban đầu chưa được đặt (Not defined). Muốn đặt thiết định nào ta nhấn đúp chuột tại thiết định đó. Ý nghĩa của chúng khi được áp dụng sau:

Enforce password history: Ta sẽ phải vào một số nguyên (ví dụ 5). Khi đó, nếu người dùng có đổi mật khẩu mới, thì mật khẩu đó phải khác 5 mật khẩu đã dùng gần đây nhất.

Maximum password age: Ẩn định thời gian tối đa để sử dụng một mật khẩu trước khi hệ thống yêu cầu thay mật khẩu mới.

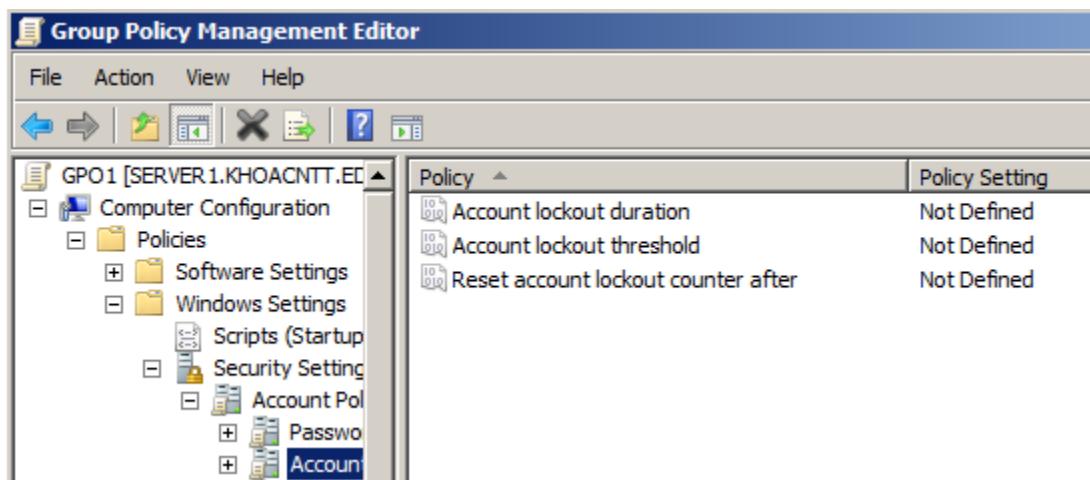
Minimum password age: Ẩn định thời gian tối thiểu mà một mật khẩu phải được dùng trước khi người dùng được phép thay đổi nó.

Minimum password length: Qui định số lượng ký tự tối thiểu mà mật khẩu của người dùng cần chứa.

Passwords must meet the complexity requirements: Mật khẩu có cần phải thoả mãn các yêu cầu đặt ra hay không.

Store passwords using reversible encryption for all users in the domain: Mật khẩu có được mã hoá với một giải thuật mã hoá cấp thấp hay không.

Các thiết định về chính sách khoá chặt tài khoản nằm trong **Computer Configuration\Windows Settings\Security Settings\ Account Policies \Account Lockout Policy**, như phần bên phải của Hình 4.10.



Hình 4.10: Các thiết định về chính sách khoá chặt tài khoản

Các thiết định trên ban đầu cũng chưa được đặt (Not defined). Muốn đặt thiết định nào ta cũng nhấn đúp chuột tại thiết định đó. Ý nghĩa của chúng khi được áp dụng sau:

Account lockout threshold: Ấn định số lần người dùng có thể đăng nhập sai, khi vượt quá số này thì tài khoản sẽ bị khoá chặt.

Reset account lockout counter after: Ta sẽ phải vào một số nguyên để chỉ số phút (ví dụ 10). Khi đó, sau lần đăng nhập sai gần nhất (chẳng hạn đã đăng nhập sai 3 lần), nếu thời gian đã vượt quá 10 phút, thì bộ đếm số lần đăng nhập sai sẽ được khởi động từ đầu (về 0).

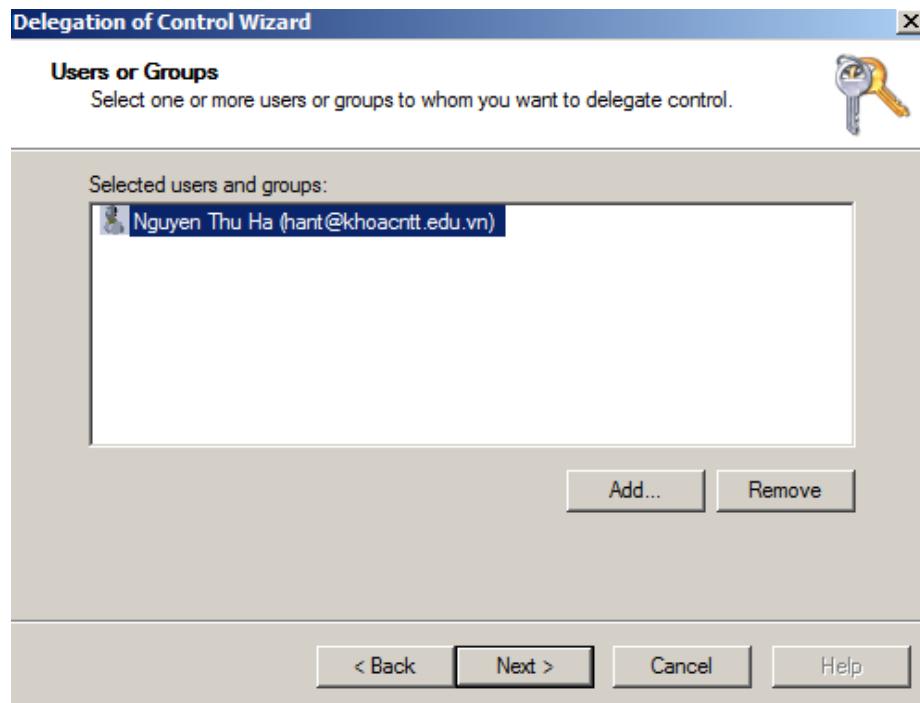
Account lockout duration: Nếu lần đăng nhập sai vượt quá ngưỡng cho phép, tài khoản sẽ bị khoá chặt, nhưng không bị phong tỏa mãi nếu có đặt giá trị này, và nó sẽ quyết định sau bao nhiêu phút thì tài khoản sẽ không bị khoá nữa. Từ đó người dùng lại có thể đăng nhập lại.

4.3. ỦY THÁC QUYỀN QUẢN TRỊ CHÍNH SÁCH NHÓM

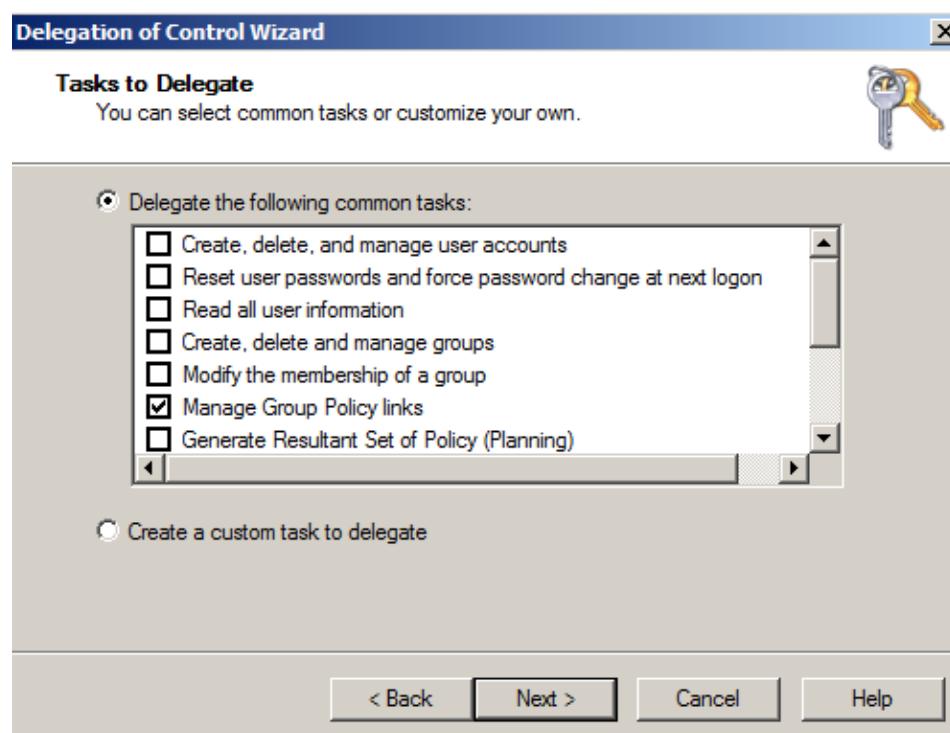
Theo mặc định, các GPO có thể được tạo ra bởi các thành viên của nhóm Administrators của miền, hoặc bởi các thành viên của nhóm toàn miền có tên là Group Policy Creator Owners. Tuy nhiên, trong khi các thành viên của Administrators có đầy đủ quyền hạn đổi với tất cả các GPO, thì các thành viên của Group Policy Creator Owners chỉ có thể sửa đổi những chính sách mà họ đã tạo ra, trừ khi họ đã được trao thêm quyền truy cập sửa đổi một chính sách. Như vậy nếu ta đặt thêm một thành viên nào đó vào nhóm Group Policy Creator Owners, thì thành viên đó có thể tạo ra các GPO mới và sửa đổi chúng.

Đó là về việc tạo ra và sửa đổi GPO. Còn để có thể liên kết các GPO với một SDOU nào đó, thì phải có thêm quyền **Manage Group Policy Links** đối với SDOU này. Các thành viên của Administrators mặc định có quyền hạn này, trong khi nhóm Group Policy Creator Owners thì không có.

Để cho phép các thành viên của nhóm Group Policy Creator Owners tạo ra được các liên kết với một OU cụ thể, ta chọn OU đó từ cửa sổ Active Directory Users or Groups, chọn **Delegate Control** từ menu **Action**, nhấn **Next** tại cửa sổ ban đầu để chuyển đến cửa sổ (như Hình 3.11) cho phép ta đưa thêm các người dùng và nhóm mà ta muốn uỷ thác quyền kiểm soát chính sách nhóm. Nhấn nút **Add** từ cửa sổ này, rồi chọn nhóm Group Policy Creator Owners, Nhấn **Add, OK** để quay về cửa sổ Hình 4.11. Khi đó nhóm Group Policy Creator Owners sẽ xuất hiện trong cửa sổ này, tiếp theo ta chọn nhóm này và nhấp **Next**, rồi chọn Manage Group Policy links trong số những công việc thông thường (common tasks) có thể uỷ thác (xem Hình 4.12). Cuối cùng nhấn **Next**, rồi nhấn **Finish**.

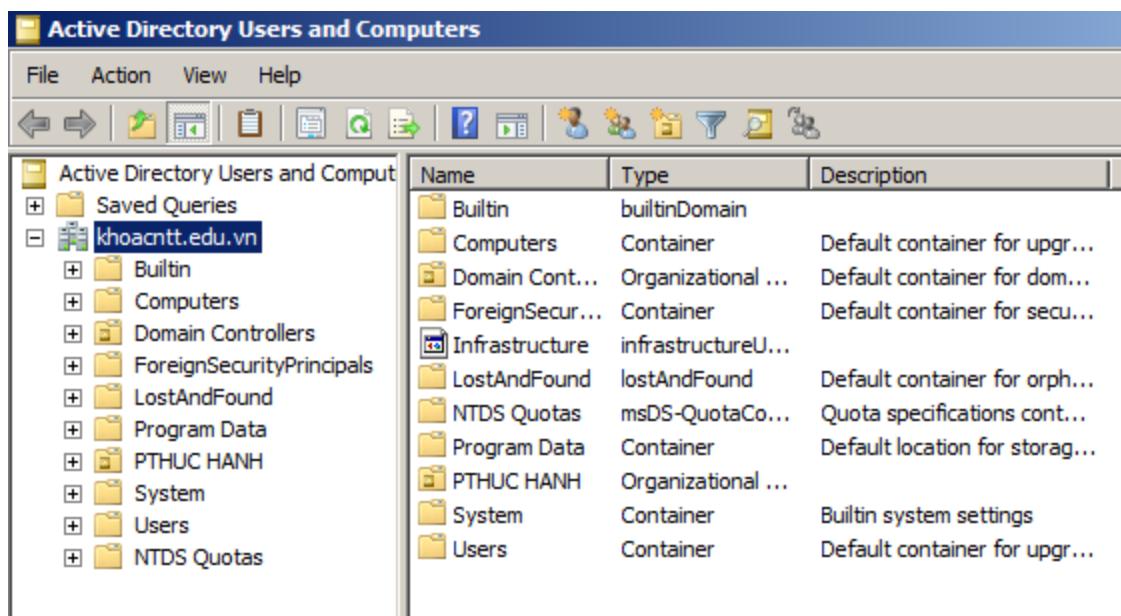


Hình 4.11: Cửa sổ chọn những đối tượng được uỷ quyền kiểm soát chính sách nhóm



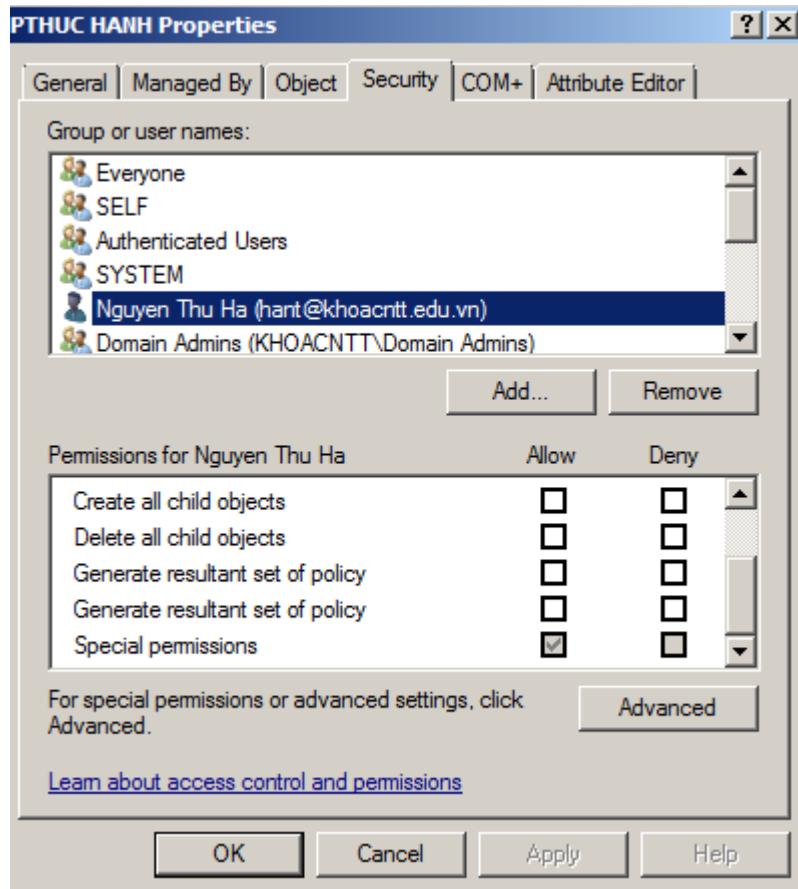
Hình 4.12: Cửa sổ chọn uỷ thác việc liên kết chính sách nhóm

Nếu muốn bỏ quyền quản trị chính sách nhóm đã ủy thác, tại cửa sổ Active Directory Users and Computers, ta chọn View/Advanced Features, để hiện ra cửa sổ như Hình 4.13.



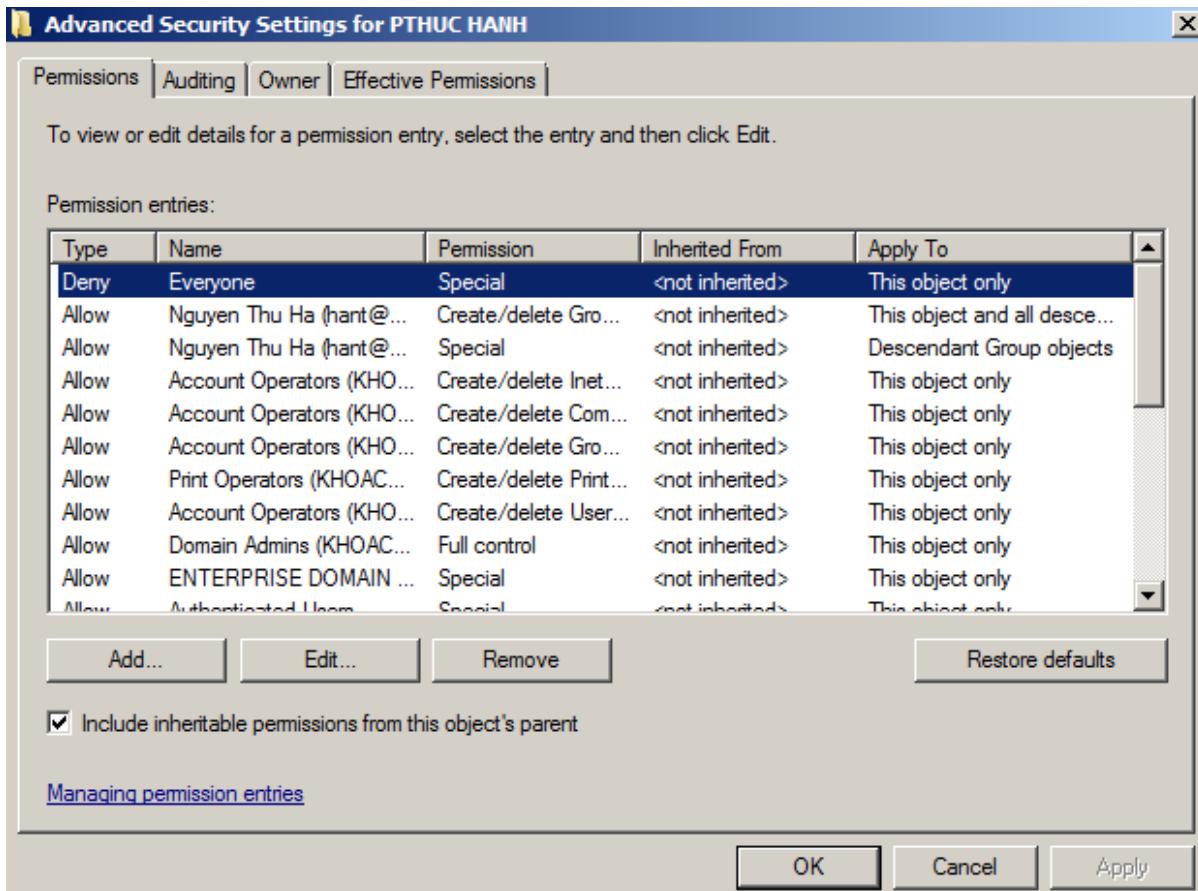
Hình 4.13: Cửa sổ Active Directory Users and Computers ở chế độ xem Advanced Features

Sau đó nhấn phải chuột tại OU cần chọn, chọn Properties để hiện ra cửa sổ đặc tính, tại đây nhấn chuột tại mục Security sẽ thấy cửa sổ như Hình 4.14.



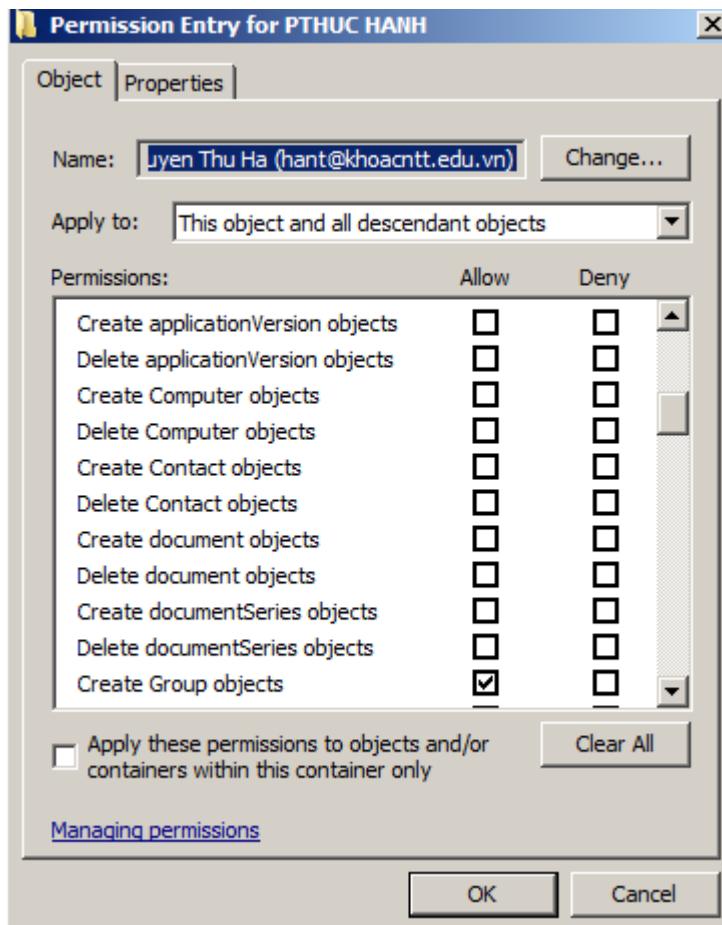
Hình 4.14: Trang Security của OU được chọn

Tiếp theo nhấn nút Advanced để màn hình như Hình 4.15 hiện lên.



Hình 4.15: **Những thiết định chi tiết của OU được chọn**

Tại cửa sổ này, nếu muốn bỏ những thiết định đã trao cho đối tượng nào thì ta chọn nó rồi nhấn nút Remove. Còn nếu muốn xem/chỉnh sửa lại các quyền đã trao cho đối tượng nào đó, thì ta chọn nó, rồi nhấn nút View/Edit để hiện ra cửa sổ như Hình 4.16.



Hình 4.16:Các quyền hạn có thể trao cho đối tượng

Tại đây, nếu muốn trao quyền nào đó thì ta đánh dấu chọn tại cột Allow. Còn nếu không muốn trao thì ta bỏ đánh dấu chọn tại cột này.

4.4. TÍNH NĂNG CÀI ĐẶT GÓI PHẦN MỀM CỦA CHÍNH SÁCH NHÓM

Một trong những công việc thường gặp đối với người quản trị viên là thường xuyên phải cài đặt và phân phối các phần mềm ứng dụng lên các máy trạm. Với một mạng có nhiều máy trạm, mà cứ tiến hành cài đặt thủ công trên từng máy, thì đây quả là một công việc năng nhọc, mất nhiều thời gian. Để khắc phục nhược điểm đó Windows Server đã đưa vào tính năng cài đặt phần mềm (Software Installation - SI). Ở đây đã có sự tích hợp việc cài đặt phần mềm vào trong hệ điều hành, và với sự tích hợp đó, làm cho nó được kiểm soát, phân phối, và quản lý một cách tập trung. Với tính năng mới này, từ một vị trí trung tâm, ta có thể tự động cài đặt một ứng dụng ra toàn mạng, hoặc chỉ cài đặt hạn chế nó cho một

danh sách các phòng ban hoặc một nhóm người dùng nào đó. Sau đó lại có thể gỡ bỏ nó ra khỏi toàn mạng hoặc một bộ phận nào đó chỉ trong một đợt.

Với SI, từ nay ta không phải chạy những chương trình Setup để cài đặt các phần mềm ứng dụng nữa. Thay vì vậy, ta phải cung cấp cho SI một tập tin (có thể gọi là gói phần mềm) có phần mở rộng là .MSI (MicroSoft Installer). Một gói phần mềm MSI không phải là một chương trình mà là một tệp tin tập các lệnh báo cho SI biết cách cài đặt một ứng dụng nằm dưới sự quản lý của Windows Server. Microsoft đang khuyến cáo các nhà chế tạo phần mềm chịu khó đưa ra các phiên bản mới của họ dưới dạng thức MSI (nếu ta thấy trên đĩa CD phân phối của một hãng nào đó có tập tin với phần mở rộng là .MSI, thì có nghĩa là hãng đó đã tạo ra một gói phần mềm sẵn sàng cho Windows). Đồng thời Windows Server cũng đưa ra một giải pháp khá rắc rối và mất nhiều thời gian để chuyển đổi một ứng dụng được cài đặt theo cách thông thường trên Windows thành một gói phần mềm MSI.

SI được dùng bên trong các đối tượng chính sách nhóm (GPO). Việc cài đặt, phân phối, quản lý và gỡ bỏ các gói phần mềm đều được thực hiện thông qua các chính sách nhóm đã được thiết lập.

SI có hai cách để phân phối một gói phần mềm cho các người dùng hoặc các máy là: quảng bá (publish) và phân bổ (assign).

Khi quảng bá một gói phần mềm cho những người dùng là ta đang làm cho nó sẵn dùng (available) đối với những người dùng đã đăng nhập vào mạng (không phân biệt là họ đăng nhập ở máy tính nào), và có cài đặt nó hay không là tùy ý họ. Để cài đặt nó người dùng chỉ cần nhấn chuột vào mục **Add/Remove Programs** trong **Control Panel**. Ta không thể quảng bá một gói phần mềm cho các máy được, vì máy thì không thể nào tự quyết định được là có cài đặt phần mềm đó hay không.

Với cách phân bổ, ta có thể phân bổ một gói phần mềm cho các người dùng hoặc các máy: nếu phân bổ cho người dùng, thì nó sẽ được cài đặt khi người dùng ấy đăng nhập; nếu phân bổ cho máy, thì nó sẽ được cài đặt khi máy được khởi động. Nếu người dùng đã nhận được ứng dụng đó, rồi cố gắng xoá nó đi, thì nó sẽ

tự cài đặt lại (reinstall) hoặc sửa chữa lại (repair) vào lần đăng nhập hoặc khởi động máy kế tiếp.

Điểm đặc biệt trong việc phân bổ một gói phần mềm là, nó chỉ được cài đặt một phần vào lúc đăng nhập hoặc khởi động máy để tạo ra giao diện và những liên kết cần thiết, sao cho người dùng có thể tìm thấy để khởi động. Điều này rất có ích vì trong nhiều trường hợp, có thể người dùng chưa cần ngay đến ứng dụng này, nên không cần phải mất thời gian cài đặt đầy đủ ngay từ đầu, tức là rút ngắn được thời gian đăng nhập hoặc khởi động máy, đồng thời tiết kiệm được không gian đĩa cứng trên máy trạm. Chỉ khi nào người dùng khởi động ứng dụng này, thì nó mới được cài đặt trọn vẹn.

4.4.1. Quảng bá và phân bổ gói phần mềm

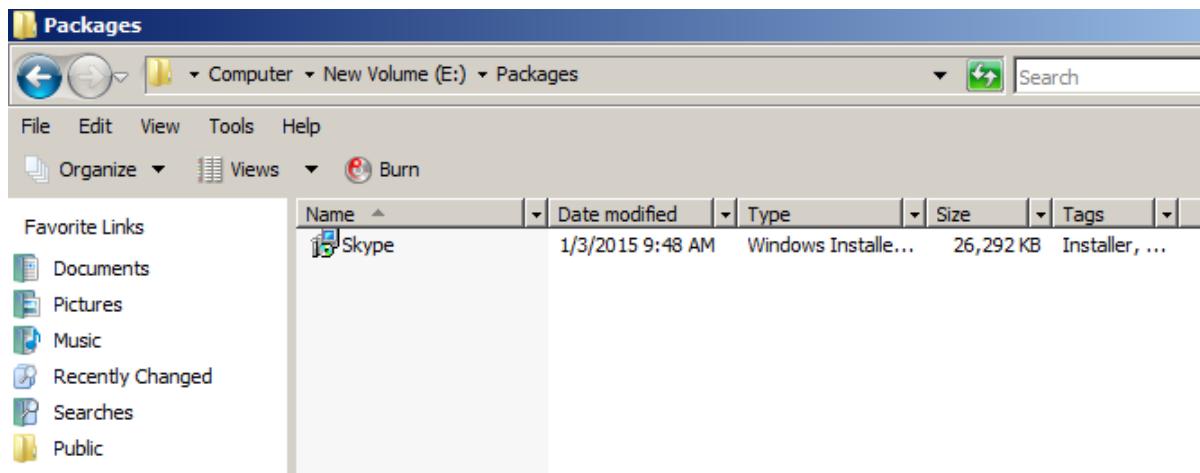
Để quảng bá hoặc phân bổ một gói phần mềm cho các người dùng hoặc máy tính trên mạng, ta thực hiện theo các bước sau:

- 1- Sao chép gói phần mềm vào một thư mục chia sẻ trên mạng
- 2- Tạo ra một GPO để cài đặt phần mềm
- 3- Đưa gói phần mềm vào GPO

Tiếp theo sau đây sẽ minh họa các bước trên bằng cách quảng bá phần mềm cài đặt **Skype** cho những người dùng, để họ có thể cài đặt và sử dụng công cụ này trên các máy trạm bất kỳ.

4.4.1.1. Sao chép gói phần mềm vào một thư mục chia sẻ trên mạng

Để tiện cho việc quản lý các gói phần mềm, ta dùng công cụ Windows Explorer tạo ra thư mục **E:\Packages** để chứa các gói phần mềm được quảng bá hoặc phân bổ. Sau đó chia sẻ thư mục này cũng với tên là Packages. Tiếp theo chép tập tin **Skype.msi** vào thư mục E:\Packages. Hình 4.17 cho thấy kết quả những gì đã làm.

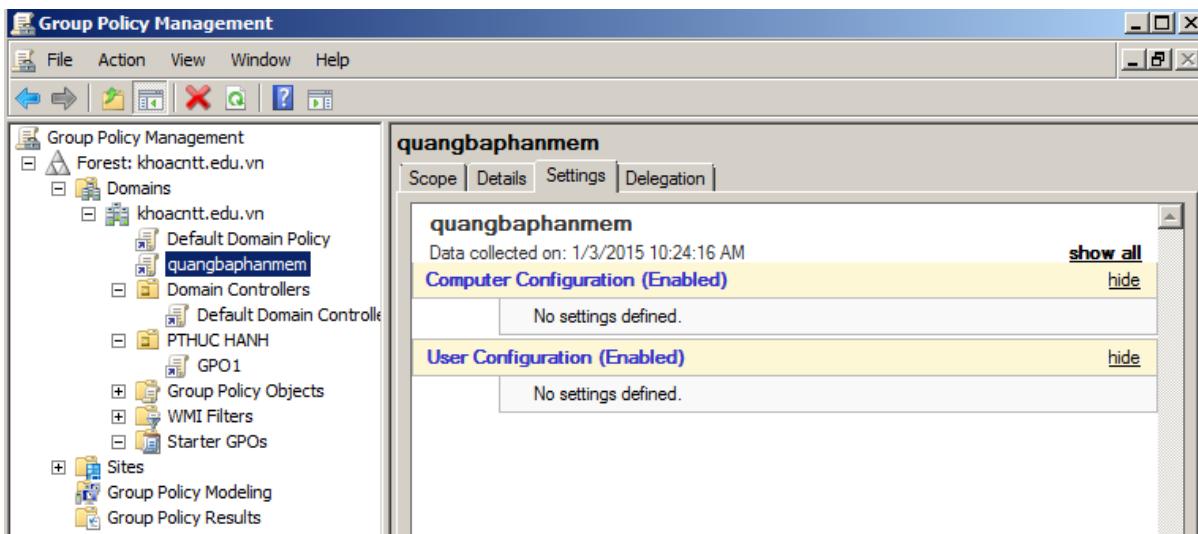


Hình 4.17: Việc sao chép Skype vào một thư mục chia sẻ

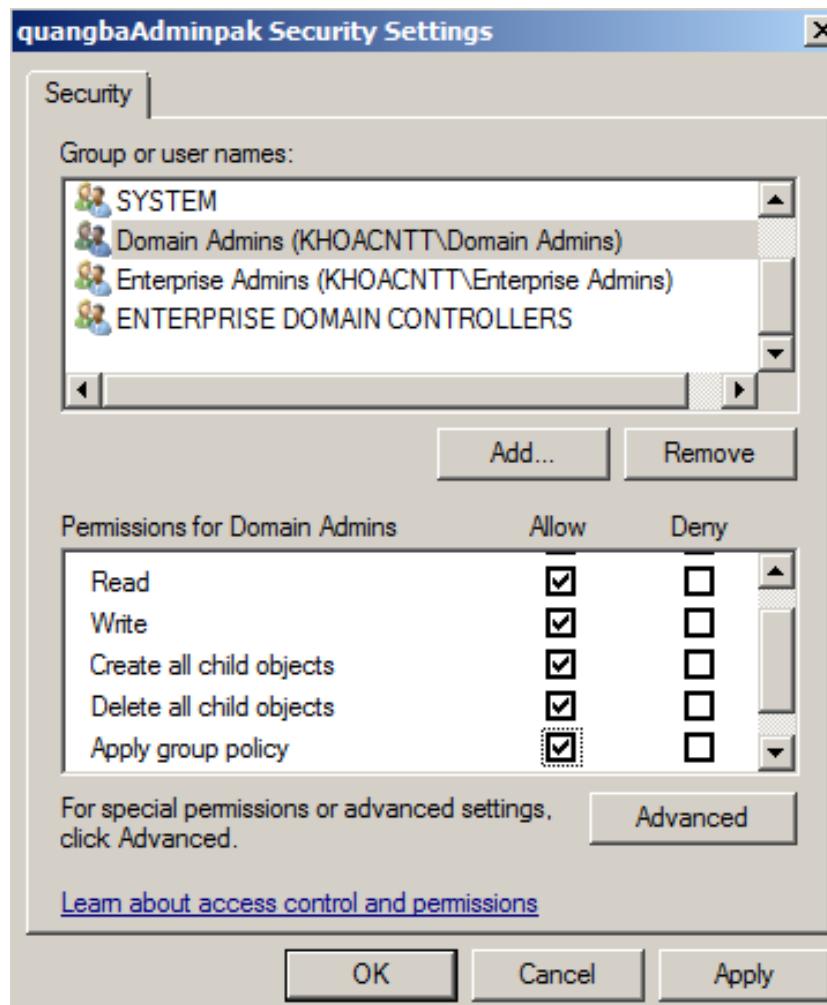
4.4.1.2. Tạo ra một GPO để cài đặt phần mềm

Tạo ra một GPO từ cấp miền có tên là “Quang ba Adminpak”, bằng cách nhấn nút phải chuột tại tên miền, chọn **Properties**, chọn trang **Group Policy**, chọn **New**, rồi gõ vào “Quang ba phan mem”, như Hình 4.18.

Theo mặc định các chính sách nhóm mới tạo sẽ được áp dụng cho mọi người dùng nằm trong SDOU hiện tại (ở đây là miền khoacntt.edu.vn). Để hạn chế việc áp dụng chính sách nhóm này chỉ cho những người quản trị, ta chọn nút **Delegation**, rồi chọn Administrator và kích vào **Advanced...** để hiện lên trang **Security**. Sau đó duyệt quyền **Apply Group Policy** cho hai nhóm Domain Admins và Enterprise Admins. Còn các nhóm khác ta bỏ duyệt quyền này (xem Hình 4.19).



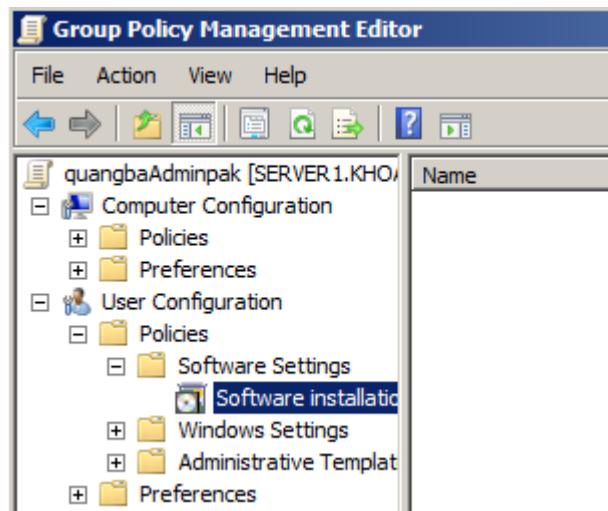
Hình 4.18: Đặt tên cho GPO mới



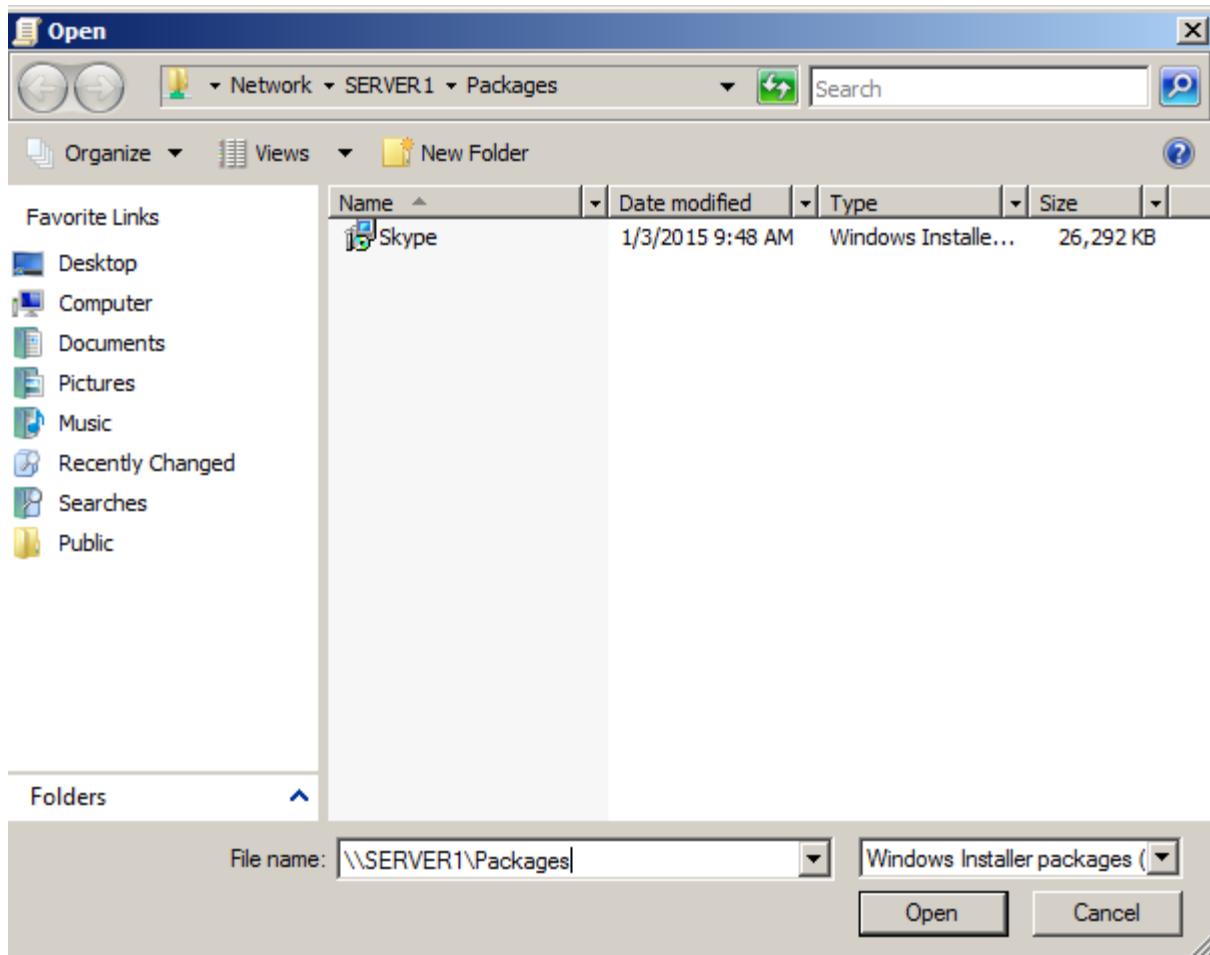
Hình 4.19: Áp dụng GPO này cho hai nhóm Domain Admins và Enterprise Admins

4.4.1.3. Đưa gói phần mềm vào GPO

Tiếp theo vẫn với GPO mới tạo trong Hình 4.18, ta chọn **Edit**. Vì chỉ có thể quảng bá gói phần mềm cho người dùng, nên ta phải đưa gói phần mềm **SKYPE** vào mục User Configuration\Software Settings\Software installation (xem Hình 4.20), bằng cách nhấn nút phải chuột tại mục này, chọn **New/Package**. Sau đó ta chọn gói **SKYPE** và phải gõ đường dẫn mạng đầy đủ đến nó trong mục **File name** như Hình 4.21.



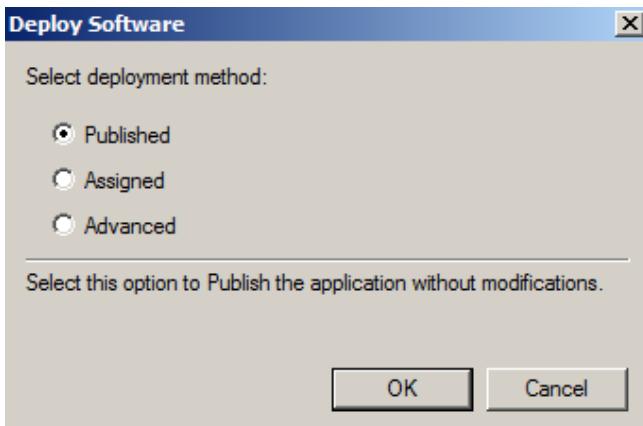
Hình 4.20: **Đưa gói phần mềm vào một GPO**



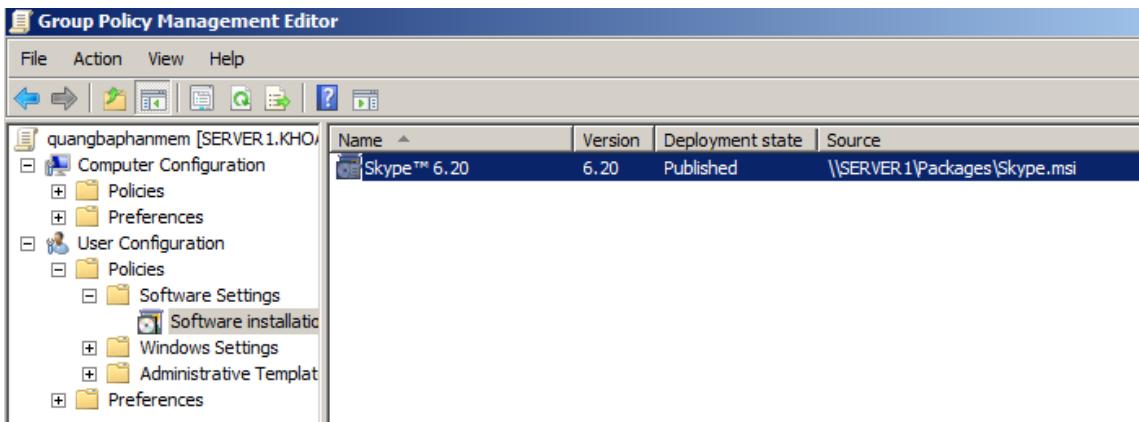
Hình 4.21: Chọn gói phần mềm để đưa vào GPO

Đường dẫn trên mạng dùng để định vị được đúng một tài nguyên trên mạng từ một vị trí bất kỳ. Các máy trạm sẽ dùng đường dẫn này để truy nhập đến gói phần mềm được cài đặt. Đường dẫn mạng được viết theo dạng: \\ tên máy \ tên thư mục chia sẻ \ các thư mục con của thư mục chia sẻ nếu có \ tên tập tin; như trong trường hợp của ví dụ này, đường dẫn mạng đến gói công cụ quản trị SKYPE là: \\ SERVER1\ Packages.

Sau khi vào xong đường dẫn mạng đến gói adminpack, ta nhấn nút **Open**. Đến đây, ta được yêu cầu chọn phương thức triển khai gói phần mềm này là quảng bá (Published), hay phân bổ (Assigned) như được minh họa trong Hình 4.22. Trong trường hợp này ta chọn **Published**, rồi nhấn OK. Khi đó cửa sổ Group Policy sẽ có nội dung như Hình 4.23.



Hình 4.22: Chọn phương thức quảng bá gói phần mềm



Hình 4.23: Gói công cụ quản trị đã được đưa vào GPO với tên gọi Windows Server Administration Tools

4.5. QUẢN LÝ GÓI PHẦN MỀM ĐÃ PHÂN BỐ HOẶC QUẢNG BÁ

4.5.1. Thay đổi một số đặc tính của gói phần mềm

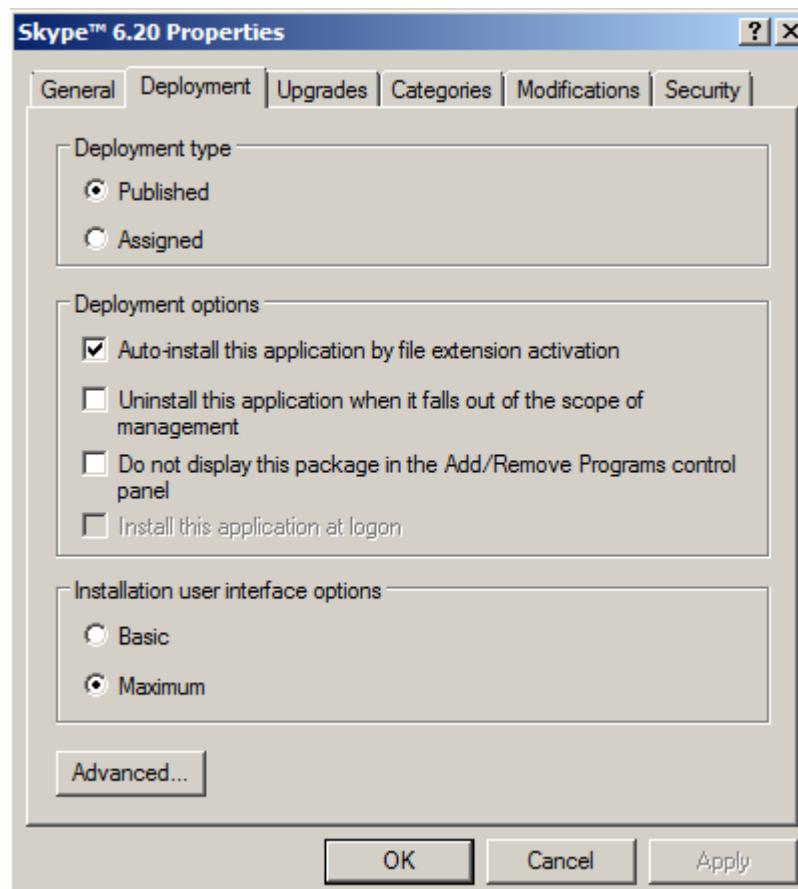
Một số đặc tính của gói phần mềm có thể được thay đổi bằng cách, từ cửa sổ Hình 4.23, ta nhấn đúp chuột tại gói phần mềm cần thay đổi, chọn trang **Deployment**, để hiện ra cửa sổ như Hình 4.24. Tại đây ta vẫn có thể thay đổi lại phương thức triển khai gói phần mềm tại mục **Deployment type**.

Ô duyệt **Uninstall this application when it falls out of the scope of management**, nếu được chọn sẽ tự động gỡ bỏ gói phần mềm đã được cài đặt bởi một người dùng nào đó, khi người dùng này không còn là đối tượng được áp dụng chính sách nhóm cài đặt gói phần mềm. Chẳng hạn người dùng này không

còn là thành viên của một nhóm được áp dụng chính sách nhóm cài đặt gói phần mềm.

Ô duyệt **Do not display this package in the Add/Remove Programs control panel**. Nếu được chọn sẽ không hiển thị gói phần mềm này trong cửa sổ Add/Remove Programs của các máy trạm, nên không thể cài đặt gói phần mềm từ cửa sổ này.

Mục **Installation user interface options** dùng để chọn giao diện khi cài đặt: nếu chọn **Basic** thì sẽ giảm thiểu hết mức những khung hỏi đáp mà người dùng sẽ gặp khi cài đặt gói phần mềm, ngược lại nếu chọn **Maximum** thì sẽ hiện ra tất cả các khung hỏi đáp.



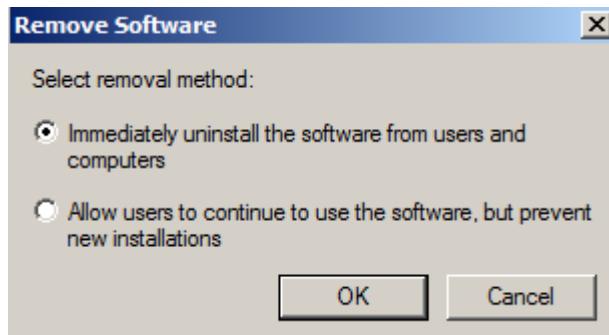
Hình 4.24: Cửa sổ thay đổi một số đặc tính của gói phần mềm

4.5.2. Triển khai lại một gói phần mềm

Trong nhiều trường hợp, khi đã cài đặt xong một ứng dụng, sau một thời gian ta lại có nhu cầu sửa đổi hoặc cài bản nâng cấp của ứng dụng. Khi đó rõ ràng là ta cần phải cài đặt lại phiên bản mới thay cho phiên bản cũ đã được cài đặt ở khắp nơi. Để làm điều đó nhấn nút chuột tại gói phần mềm cần triển khai lại trong cửa sổ Hình 4.23, rồi chọn **All Tasks/Redeploy/Yes**.

4.5.3. Gỡ bỏ một gói phần mềm

Với một gói phần mềm đã được triển khai trên nhiều máy của mạng. Nếu nó không còn cần thiết, hoặc vì một nguyên nhân nào đó, nó không được sử dụng, thì ta không nhất thiết phải đi đến từng máy đã cài đặt để gỡ bỏ, mà chỉ cần nhấn nút chuột tại gói phần mềm cần gỡ bỏ trong cửa sổ Hình 4.23, rồi chọn **All Tasks/Remove**. Khi đó cửa sổ như Hình 4.25 hiện ra để ta chọn một trong hai phương án:



Hình 4.25: Lựa chọn các xử lý các bản đã được cài đặt

+ Nếu chọn **Immediately uninstall software from users and computers**, thì gói phần mềm sẽ được gỡ bỏ ngay lập tức ra khỏi người dùng hoặc máy mà trước kia nó đã phân bổ hay quảng bá. Tuy nhiên ngay lập tức ở đây được hiểu theo nghĩa là: gói phần mềm này sẽ được gỡ bỏ vào lúc những người dùng ấy đăng nhập lần kế (nếu gói phần mềm được quảng bá hoặc phân bổ cho người dùng), hoặc lúc các máy ấy khởi động lần kế (nếu gói phần mềm ấy được phân bổ cho máy).

+ Còn nếu ta chọn mục bên dưới, thì mọi bản đã cài đặt xong của gói phần mềm sẽ được để nguyên ở nơi chúng được cài đặt, và sẽ không có cuộc cài đặt

mới nào được diễn ra nữa. Khi đó những bản cài đặt được giữ nguyên đó sẽ ở ngoài vòng kiểm soát, vì không còn chính sách nhóm nào có thể quản lý được chúng nữa. Điều đó có nghĩa là, nếu sau này ta muốn nâng cấp hoặc gỡ bỏ chúng thì ta phải tiến hành công việc này trên từng máy có cài đặt chúng.

4.6. TỔNG KẾT CHƯƠNG

Như đã trình bày trong các phần trước, chương này nhằm trình bày kỹ thuật hiệu quả hơn trong quản trị mạng dựa trên sử dụng các chính sách nhóm. Chính sách nhóm là một tập các thiết lập cấu hình cho máy tính hoặc người dùng, để áp dụng đồng thời cho nhiều đối tượng trong một OU, một miền hoặc một địa bàn. Sau khi đã phân chia miền thành các phân vùng lô-gic là các OU, cần xây dựng các chính sách nhóm để áp dụng đồng bộ, phù hợp với mỗi OU. Chính sách nhóm cho phép thực hiện đồng bộ các chức năng chính sau: Triển khai phần mềm ứng dụng, ấn định quyền hạn của người dùng, kiểm soát những thiết định trên các hệ thống, thiết lập và tự động hóa các kịch bản truy nhập, đơn giản hóa và hạn chế các chương trình.

Các hoạt động quản lý chính sách nhóm bao gồm: tạo/ sửa/ cập nhật các đối tượng chính sách nhóm (GPO) và ủy thác quyền quản trị chính sách nhóm. Mỗi đối tượng chính sách nhóm có thể được liên kết với một hoặc nhiều OU. Hai hoạt động phổ biến và hiệu quả trong sử dụng chính sách nhóm là quảng bá và phân bổ các gói phần mềm để có thể cài đặt tự động và đồng bộ trên nhiều máy.

Việc quảng bá và phân bổ các gói phần mềm được tiến hành theo ba bước: Đưa gói phần mềm vào một thư mục chia sẻ, tạo một GPO để cài đặt phần mềm, đưa gói phần mềm vào GPO và lựa chọn quảng bá/ phân bổ.

Quản lý các gói phần mềm đã phân bổ gồm các hoạt động như: thay đổi đặc tính của gói phần mềm, triển khai lại một gói phần mềm và gỡ bỏ các gói phần mềm đã quảng bá/ phân bổ. Việc triển khai lại được thực hiện khi cần nâng cấp gói phần mềm lên phiên bản mới. Việc gỡ bỏ các gói phần mềm có hai lựa chọn là gỡ bỏ toàn bộ đối với máy tính/ người dùng đã quảng bá/ phân bổ hoặc cho phép máy tính/ người dùng tiếp tục sử dụng gói phần mềm đã quảng bá/ phân bổ nhưng không cài đặt mới.

CÂU HỎI VÀ BÀI TẬP THỰC HÀNH

Câu 1. Trình bày những đặc điểm chính của tính năng cài đặt phần mềm, phân biệt giữa quảng bá và phân bổ một gói phần mềm.

Câu 2. Trình bày những đặc điểm chính của các bước quảng bá hoặc phân bổ một gói phần mềm.

Câu 3. Thực hành phân bổ gói công cụ **SKYPE** cho một nhóm gồm những máy trạm nào đó. Sau khi phân bổ xong, thử khởi động một máy trạm trong nhóm máy đó và mở công cụ Active Directory Users and Groups trên máy này để tạo một số người sử dụng và nhóm của miền.

Câu 4. Trình bày cách thay đổi một số đặc tính của gói phần mềm, cách triển khai lại, cách gỡ bỏ một gói phần mềm.

Câu 5. Khi chỉnh LocalPolicy ở phần Computer Configuration, policy sẽ có hiệu lực vào thời điểm nào? Khi chỉnh LocalPolicy ở phần User Configuration, policy sẽ có hiệu lực vào thời điểm nào?

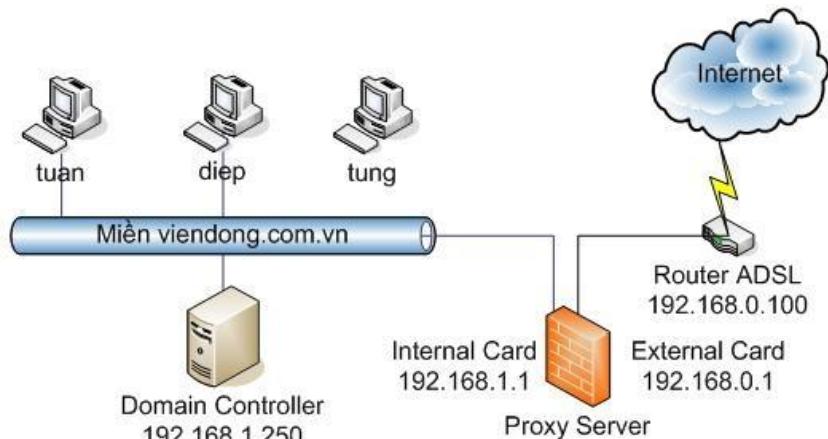
Câu 6. Trình bày ý nghĩa và công dụng của policy: Computerconfiguration>Windows settings >Securitysettings> Securityoptions> Account: Limit local account use of blank password to console logon only

Câu 7. Trình bày ý nghĩa và công dụng của policy: Computerconfiguration>Windows settings> Securitysettings> Securityoptions> Interactivelogon: Do not display last username

Lab1: Thiết lập Group PolicyVới hệ thống mạng theo mô hình bên dưới, Anh/Chị hãy cấu hình hệ thống theo yêu cầu sau:

- Mọi người khi truy cập Internet đều phải thông qua Proxy Server, và không được phép thay đổi địa chỉ Proxy.
- Trên máy làm việc, mọi người khi đăng nhập vào hệ thống thì sẽ tự động ánh xạ thư mục dùng chung và thư mục riêng trong mạng về máy.

Hãy cấu hình hệ thống một cách đơn giản nhất để đáp ứng yêu cầu trên.



Thông tin giả định

Cấu trúc thư mục trên máy Domain Controller như sau:



Mỗi người dùng sẽ sử dụng 2 thư mục trên máy Domain Controller: Thư mục chung là thư mục BaoCao được ánh xạ thành ổ đĩa H:

Thư mục riêng là thư mục có tên trùng với tên tài khoản đó được ánh xạ thành ổ đĩa K:. Ví dụ: thư mục riêng của tài khoản Diep là thư mục Diep.

Bài thực hành 2. Thiết lập mối quan hệ giữa các Group Policy Với hệ thống mạng đang có trong lab1, hãy thiết lập chính sách nhóm cho OU Khachhang theo yêu cầu sau:

OU Khachhang gồm tài khoản Hung và Long

Các tài khoản này chỉ cho chạy chương trình Internet Explorer và Wordpad.

CHƯƠNG 5. QUẢN LÝ TÀI NGUYÊN MẠNG

Chia sẻ tài nguyên, đồng bộ, phối hợp làm việc là một trong những mục tiêu chính của hệ thống mạng máy tính. Các tài nguyên mạng bao gồm: hệ thống file và thư mục, hệ thống ổ đĩa, các máy in mạng, v.v. Chia sẻ, phân quyền và đồng bộ các tài nguyên mạng là nhóm hoạt động quan trọng của công việc quản trị mạng. Chương này tập trung trình bày các nghiệp vụ, kỹ thuật cốt lõi để quản lý tài nguyên mạng. Nội dung chương được bố cục như sau: *Mục 5.1* trình bày vấn đề quản lý file và thư mục; *Mục 5.2* trình bày vấn đề quản lý ổ đĩa; *Mục 5.3* trình bày về dịch vụ in trên mạng; *Mục 5.4* trình bày vấn đề sao lưu và phục hồi; *Mục 5.5* tổng kết và hệ thống các kiến thức của chương.

5.1. QUẢN LÝ FILE VÀ THƯ MỤC

Windows server hỗ trợ 2 hệ thống file là **NTFS** (New Technology File System) và **EFS** (Encrypting File System).

NTFS: Là hệ thống phân hoạch file tiên tiến, Hệ thống phân hoạch này có lợi thế là bảo mật được ở mức file và phân chia làm nhiều mức cho phép truy cập vào thư mục và file.

EFS: Là hệ thống bảo đảm sự bảo mật tối đa cho người sở hữu file bằng cách mã hoá các file.

5.1.1. Chế độ bảo mật của NTFS

5.1.1.1. Một số khái niệm

Quyền truy cập (Permission): Chỉ mức độ người sử dụng có thể truy cập vào một file hoặc một thư mục. Trên hệ thống NTFS có rất nhiều quyền truy cập đáp ứng được như cầu bảo mật dữ liệu đa dạng. Có hai loại quyền truy cập vào tài nguyên file và thư mục là: *quyền truy cập chia sẻ* (share permission) và *quyền truy cập file và thư mục* (file and directory permission). Sau đây để cho ngắn gọn và

dễ phân biệt, ta sẽ gọi *quyền truy cập chia sẻ* là *quyền truy cập từ xa*, gọi *quyền truy cập file* và *thư mục* là *quyền truy cập cục bộ*.

Quyền sở hữu (Ownership): Một người sử dụng có quyền sở hữu đối với một file hoặc thư mục nào đó sẽ có thể cấp cho mình toàn quyền sử dụng file hoặc thư mục này, đồng thời còn có thể cấp quyền truy cập file hoặc thư mục này cho các đối tượng khác. Khi một người sử dụng tạo ra một file hoặc thư mục mới thì quyền sở hữu file hoặc thư mục này sẽ thuộc về họ. Mỗi một file hoặc thư mục chỉ có duy nhất một đối tượng có quyền sở hữu.

5.1.1.2. Quyền truy cập từ xa

Trong hệ thống mạng Windows server, một thư mục (kể cả ổ đĩa) bất kỳ của máy tính nào muốn trở thành tài nguyên chung (cho những người ở máy tính khác cùng sử dụng) đều phải tiến hành thao tác chia sẻ. Khi ta tiến hành chia sẻ một thư mục của một máy tính nào đó, tức là đã đưa thư mục đó ra cho mọi người trên các máy tính khác cùng truy cập. Tuy nhiên mức độ cho người khác truy cập đến đâu là do người chia sẻ quy định thông qua các quyền truy cập từ xa. Như vậy quyền truy cập từ xa cho phép người sử dụng từ những máy tính khác trong mạng, được truy nhập vào hệ thống thư mục của một máy tính có thư mục chia sẻ.

Quyền truy cập từ xa là hàng rào cản đầu tiên (từ xa) mà người sử dụng cần vượt qua khi truy nhập vào hệ thống file và thư mục trên mạng. Có thể ví chúng như cái nút gạt chống ghi trên một đĩa mềm. Cho dù ta có thể xoá, sửa đổi với tất cả các file và thư mục trên đĩa mềm, nhưng chỉ cần cái nút gạt ấy ở đúng vị trí là ta không thể thay đổi được thứ gì.

Windows server chỉ cho phép chia sẻ các thư mục, mà không chia sẻ được các file. Do vậy quyền truy cập từ xa chỉ áp dụng với thư mục. Các quyền truy cập từ xa gồm:

Full Control: Cho phép thực hiện tất cả mọi công việc trên tất cả các file và thư mục con trong thư mục chia sẻ.

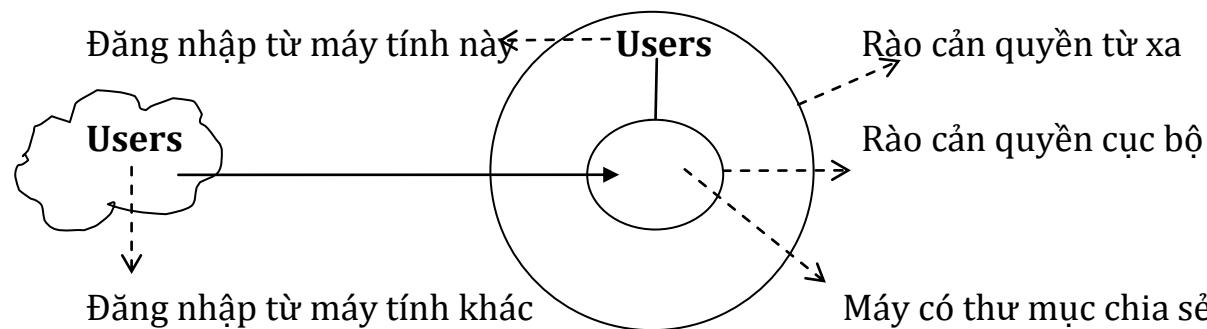
Change: Cho phép đọc và thi hành, cũng như thay đổi và xoá, các file và thư mục trong thư mục chia sẻ.

Read: Cho phép đọc và thi hành các file, xem nội dung thư mục chia sẻ, không có khả năng sửa đổi hoặc xoá bất kỳ thứ gì trong thư mục chia sẻ.

5.1.1.3. Quyền truy cập cục bộ

Như trên ta thấy các quyền truy cập từ xa chỉ được phân thành ba mức và cũng chỉ áp dụng được cho thư mục. Bởi vậy không đáp ứng được nhu cầu bảo mật dữ liệu đa dạng trên mạng, vì có rất nhiều loại đối tượng sử dụng khác nhau trên mạng, đòi hỏi các quyền trên cần được chia nhỏ tiếp và phải được áp dụng chi tiết đến mức file. Sự có mặt của *quyền truy cập cục bộ* chính là nhằm đáp ứng yêu cầu trên.

Quyền truy cập cục bộ được xem như những quyền truy cập trực tiếp (rào cản trực tiếp) mà người dùng phải qua khi truy nhập vào hệ thống file và thư mục trên ổ đĩa cục bộ của máy tính, như hình ảnh minh họa sau:



Chính vì vậy, tại máy tính có thư mục chia sẻ, nếu người dùng truy cập vào thư mục chia sẻ này như một tài nguyên cục bộ của máy, thì quyền truy cập từ xa sẽ không được áp dụng, tức là lúc đó chỉ có các quyền truy cập cục bộ là có hiệu lực.

Đối với các thư mục và file, có hai mức quyền truy cập khác nhau, có thể tạm gọi là *quyền truy cập mức cao* và *quyền truy cập mức thấp*, trong đó quyền truy cập mức cao là tổ hợp của những quyền truy cập mức thấp. Bảng 5.1 trình bày cách kết hợp của các quyền truy cập mức cao từ các quyền truy cập mức thấp.

Bảng 5.1. Các quyền truy cập mức cao và quyền truy cập mức thấp

Mức cao	Write	Read	List Folder	Read & Execute	Modify	Full Control

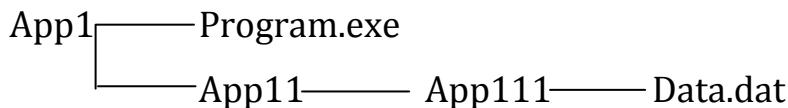
Mức thấp			Contents	e		
Traverse folder/Execute File			×	×	×	×
List Folder/Read Data		×	×	×	×	×
Read Attributes		×	×	×	×	×
Read Extended Attributes		×	×	×	×	×
Create Files/Write Data	×				×	×
Create Folders/Append Data	×				×	×
Write Attributes	×				×	×
Write Extended Attributes	×				×	×
Delete Subfolders and Files						×
Delete					×	×
Read Permissions	×	×	×	×	×	×
Change Permissions						×
Take Ownership						×

Những qui luật hình thành các quyền truy cập mức cao trong bảng trên được áp dụng cho cả file và thư mục, chỉ trừ **List Folder Contents**, vì quyền truy cập này chỉ áp dụng cho thư mục.

Những quyền truy cập mức thấp có dạng chọn một trong hai như: Traverse folder/Execute File, List Filder/Read Data, Create Files/Write Data và Create Folders/Append Data, thì quyền đầu được áp dụng cho thư mục, quyền sau được áp dụng cho file.

Các quyền truy cập ở mức thấp là cơ sở để tạo nên các quyền truy cập ở mức cao thường thấy như: Read, Modify và Full Control. Ý nghĩa của các quyền truy cập mức thấp như sau:

Traverse folder/Execute File: Traverse folder (nghĩa là đi qua thư mục) chỉ áp dụng với các thư mục. Có những lúc ta thực hiện các file chương trình nào đó có gọi đến các file khác trong các thư mục khác. Ví dụ, ta thực hiện một file chương trình Program1.exe, trong thư mục APP1 (như Hình 5.1). Giả sử file chương trình đó lại cố gắng gọi đến một file khác trong một thư mục nằm sâu hơn một cấp bên dưới APP1 (giả sử đó là file Data.dat trong thư mục App111), trong khi ta lại không được phép truy cập các thư mục cấp một bên dưới App1 (là App11). Khi đó ta sẽ nhận được một thông báo lỗi “Access denied” (từ chối truy cập), vì Windows serve không cho phép đi qua một thư mục không được phép truy cập. Nhưng chỉ cần có quyền Traverse folder đối với các thư mục ở mức trên (là App11), thì ta sẽ đi qua được các thư mục trung gian để đến đích (là App111).



Hình 5.1: Minh họa cho quyền truy cập Traverse folder

Còn với Execute File, thì chỉ áp dụng với các file, và nếu file có đuôi là .EXE, .COM, hoặc một kiểu file khả thi khác, thì quyền này cho ta thi hành được file đó.

List Folder/Read Data: List Folder cho phép xem nội dung của thư mục, còn Read Data cho phép xem nội dung của file.

Read Attributes: Cho phép nhìn thấy các thuộc tính cơ bản của file gồm: Read – Only, Hidden, System và Archive.

Read Extended Attributes: Một số chương trình có gộp các thuộc tính khác vào kiểu file của chúng. Ví dụ Microsoft Word có gắn thêm vào file .DOC các thuộc tính như: Author, Subject, Title, ... Các thuộc tính này được gọi là thuộc tính mở rộng (extended attributes), và chúng thay đổi từ chương trình này sang chương trình khác. Quyền truy cập mức thấp này cho phép ta xem được các thuộc tính mở rộng đó.

Create Files/Write Data: Create Files cho phép đặt các file mới vào thư mục đang xét (nghĩa là có thể tạo ra hoặc sao chép, di chuyển từ nơi khác đến). Write Data thì cho phép ghi đè lên (sửa) những dữ liệu hiện có bên trong file, nhưng không cho bổ sung thêm dữ liệu vào file.

Create Folders/Append Data: Create Folders cho phép tạo ra các thư mục con trong thư mục đang xét. còn Append Data cho phép bổ sung thêm dữ liệu vào cuối file đang xét, như không cho sửa những dữ liệu đã có của file đó.

Write Attributes: Cho phép thay đổi các thuộc tính cơ bản của một file.

Write Extended Attributes: Cho phép thay đổi các thuộc tính mở rộng của một file.

Delete Subfolders and Files: Cho phép xoá các thư mục con và các file của thư mục đang xét, nhưng không xoá được chính thư mục này.

Delete: Cho phép xoá một file hoặc thư mục, nếu là thư mục thì chỉ xoá được khi nó đã rỗng.

Read Permissions: Cho phép xem tất cả các quyền truy cập vào file hoặc thư mục đã được trao cho các đối tượng, nhưng không thể thay đổi được các quyền đã trao này.

Change Permissions: Cho phép thay đổi các quyền truy cập vào file hoặc thư mục cho các đối tượng.

Take Ownership: Cho phép chiếm lấy quyền sở hữu file hoặc thư mục.

5.1.2. Chia sẻ và quản lý quyền truy cập từ xa

5.1.2.1. Cách chia sẻ thư mục và trao quyền truy cập từ xa

Muốn tạo ra một thư mục dùng chung (chia sẻ thư mục), thì ta phải có những quyền thích hợp. Điều này đòi hỏi ta phải là một quản trị viên (là thành viên nhóm administrators) hoặc một điều hành viên server (server operators).

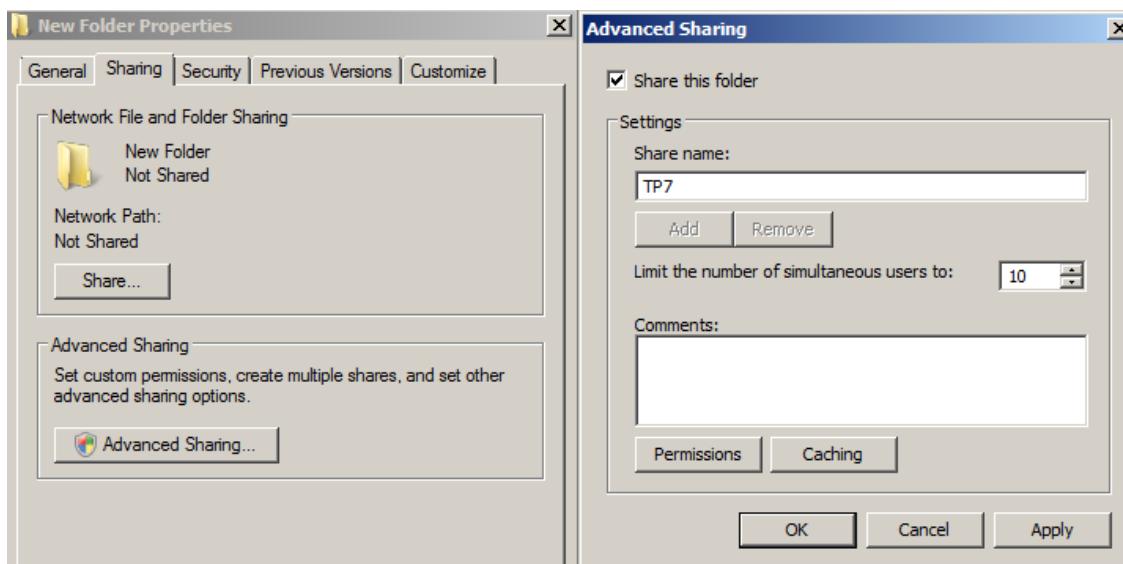
Có nhiều cách để tạo ra các thư mục dùng chung, nhưng nếu ngồi tại máy có thư mục cần tạo, thì giao diện Explorer hoặc My Computer là những phương tiện đơn giản và trực tiếp để tạo ra và quản lý các đặc tính của một thư mục dùng chung.

Từ Explorer hoặc My Computer, ta nhấn phải chuột tại thư mục cần chia sẻ (ví dụ thư mục TP7, chọn **Sharing** từ menu ngữ cảnh, để hiện ra cửa sổ như Hình 5.2. Sau đó để chia sẻ ta chọn **Share this folder**.

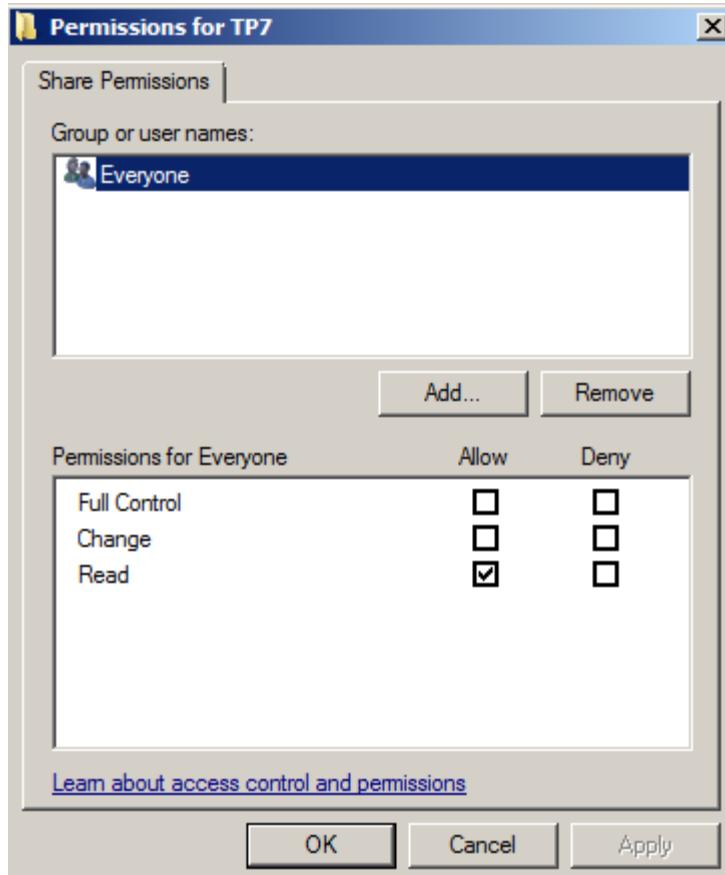
Mục chọn **Share name** để gõ vào tên chia sẻ. Tên chia sẻ giống như một bí danh của thư mục được chia sẻ. Ban đầu tên này được đặt mặc định chính là tên của thư mục được chia sẻ, nhưng ta có thể đổi lại thành một tên bất kỳ. Những người sử dụng trên mạng sẽ dùng tên chia sẻ để tham chiếu đến thư mục dùng chung, mà không cần biết tên thực sự của nó.

Mục **User limit** dùng để giới hạn số người dùng có thể đồng thời truy cập vào thư mục dùng chung này: Nếu chọn **Maximum allowed** thì số người dùng đồng thời là không hạn chế. Còn nếu muốn chỉ một số nhất định người dùng (ví dụ 100 người) được phép đồng thời truy cập, thì ta chọn **Allow** và gõ vào số người tại đó.

Để thiết lập chế độ bảo mật cho thư mục chia sẻ ta chọn nút **Permissions**, cửa sổ như Hình 5.3 sẽ hiện ra cho thấy đã có nhóm Everyone trong khung **Name** được trao mặc định tất cả các quyền truy cập từ xa đối với thư mục này. Nếu muốn trao quyền truy cập từ xa thư mục này cho những người sử dụng hoặc các nhóm khác thì ta nhấn nút **Add**, và tiến hành chọn các đối tượng mong muốn từ danh sách được hiện ra.



Hình 5.2: Cửa sổ thay đổi các đặc tính của thư mục dùng chung



Hình 5.3: Cửa sổ trao quyền truy cập từ xa của thư mục cho các đối tượng

Nếu không muốn trao quyền truy cập từ xa cho một đối tượng (người sử dụng hoặc nhóm) nào thì ta chọn đối tượng đó từ khung **Name** rồi nhấn **Remove**.

Nếu muốn sửa lại quyền truy cập của một đối tượng nào đó, ta chọn đối tượng đó, rồi duyệt / bỏ duyệt vào ô **Allow** tại quyền cần trao / không trao. Nếu muốn cấm tường minh một đối tượng không được nhận quyền nào đó, thì ta duyệt vào ô **Deny** của quyền đó. Để ngăn cấm không tường minh một quyền nào đó, thì ta không duyệt ở cả hai ô Allow và Deny.

Kết thúc mục này nhấn OK để trở về cửa sổ Hình 5.2.

Tại cửa sổ Hình 5.2 ta thấy có một tính năng mới khác với NT4, đó là nút **Caching** (nghĩa là đệm trữ chia sẻ). Nút chọn này sử dụng tính năng **Offline Files** (file ngoại tuyến) làm cho việc truy cập file từ xa được nhanh hơn.

Offline Files hoạt động bằng cách tự động đệm trữ (cache) các file thường được truy cập từ xa, lưu những bản sao đệm trữ (cached copy) đó trong một thư mục (gọi là *cache*) trên một ổ đĩa cứng của mỗi máy trạm có sự truy cập từ xa đến thư mục dùng chung đang xét. Sau đó Offline Files dùng các bản sao đệm trữ đó để tăng tốc độ truy cập, vì việc truy cập đến những file thường được truy cập ấy không phải là từ xa nữa, mà được giải quyết ngay trên bản sao đệm trữ trong cache tại chính máy trạm. Tuy nhiên trước hết Offline Files phải kiểm tra cho chắc chắn rằng file đó đã bị thay đổi tại thư mục dùng chung hay chưa, bằng cách xem xét ngày giờ và kích thước file trên cả thư mục dùng chung và trong cache của máy trạm; nếu thấy giống nhau thì Offline Files sẽ trao cho ta file trong cache; nếu không phải như vậy (hai bản đó có sự khác nhau), thì Offline Files sẽ đọc bản ở mạng (thư mục dùng chung) về, đưa vào cache để máy trạm có được bản cập nhật mới nhất.

Offline Files là một cơ chế đệm trữ *write-through*, nghĩa là khi ta lưu những thay đổi của một file, thì những thay đổi đó luôn luôn được ghi ngay lên mạng (chứ không ghi tạm vào cache rồi một lúc nào đó sau đó mới thực sự ghi lên mạng như loại cache *write-back*), và những thay đổi đó cũng được đệm trữ vào ổ đĩa cứng tại chỗ luôn.

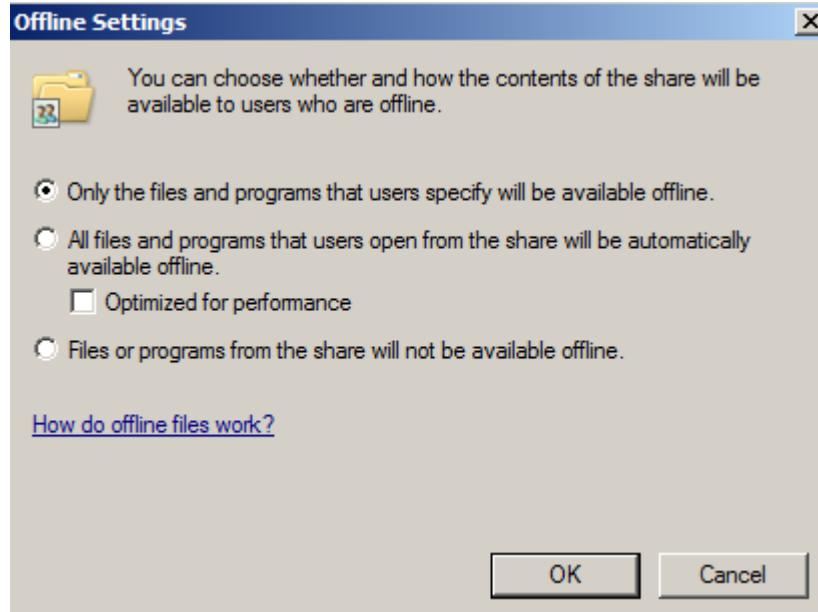
Khi chọn **Caching**, cửa sổ như Hình 5.4 hiện ra.

Chọn lựa mặc định là **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.

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 để thực thi nội bộ trên máy trạm.

Files And Programs From The Share Will Not Be Available Offline (Các file và chương trình trong 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.



Hình 5.4: Cửa sổ đặt thiết định đệm trữ cho thư mục chia sẻ

Kết thúc mục này nhấn OK để trở về cửa sổ Hình 5.2, tại đó nhấn tiếp OK để kết thúc quá trình chia sẻ.

Chú ý: Ta có thể tiến hành chia sẻ nhiều lần một thư mục, mỗi lần với một tên chia sẻ khác nhau. Tại những lần chia sẻ sau, trên cửa sổ Hình 5.2 sẽ có thêm mục **New Share** để chọn tên chia sẻ và những thiết định bảo mật mới.

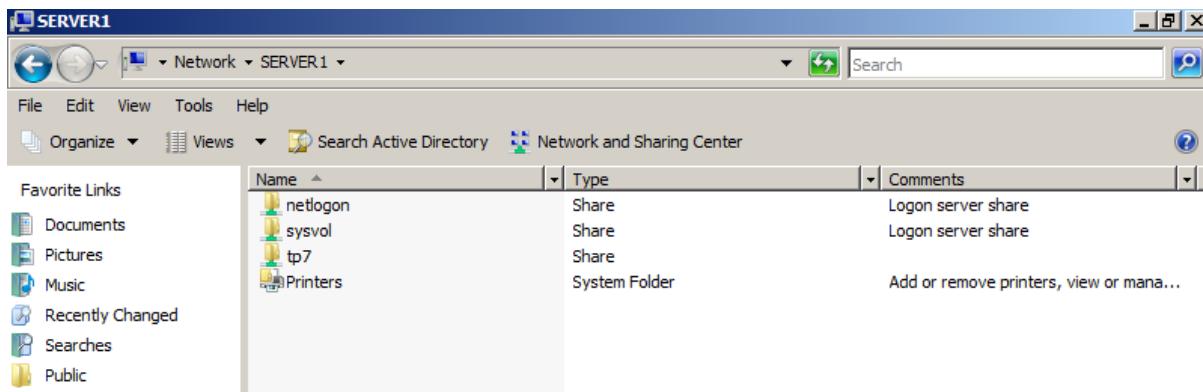
Cửa sổ Hình 5.2 cũng để sửa lại các thiết định bảo mật cho một tên chia sẻ đã tạo, hoặc bỏ một tên chia sẻ đã tạo của một thư mục dùng chung. Khi đó tên chia sẻ được chọn từ mục Share name, các thao tác chỉnh sửa thiết định bảo mật được tiến hành như khi đang chia sẻ, còn nếu muốn bỏ tên chia sẻ đang chọn thì ta chọn mục **Remove Share**. Nếu muốn bỏ tất cả các tên chia sẻ đã có (không chia sẻ nữa) thì chọn mục **Do not share this folder**.

5.1.2.2. Định nghĩa ổ đĩa mạng

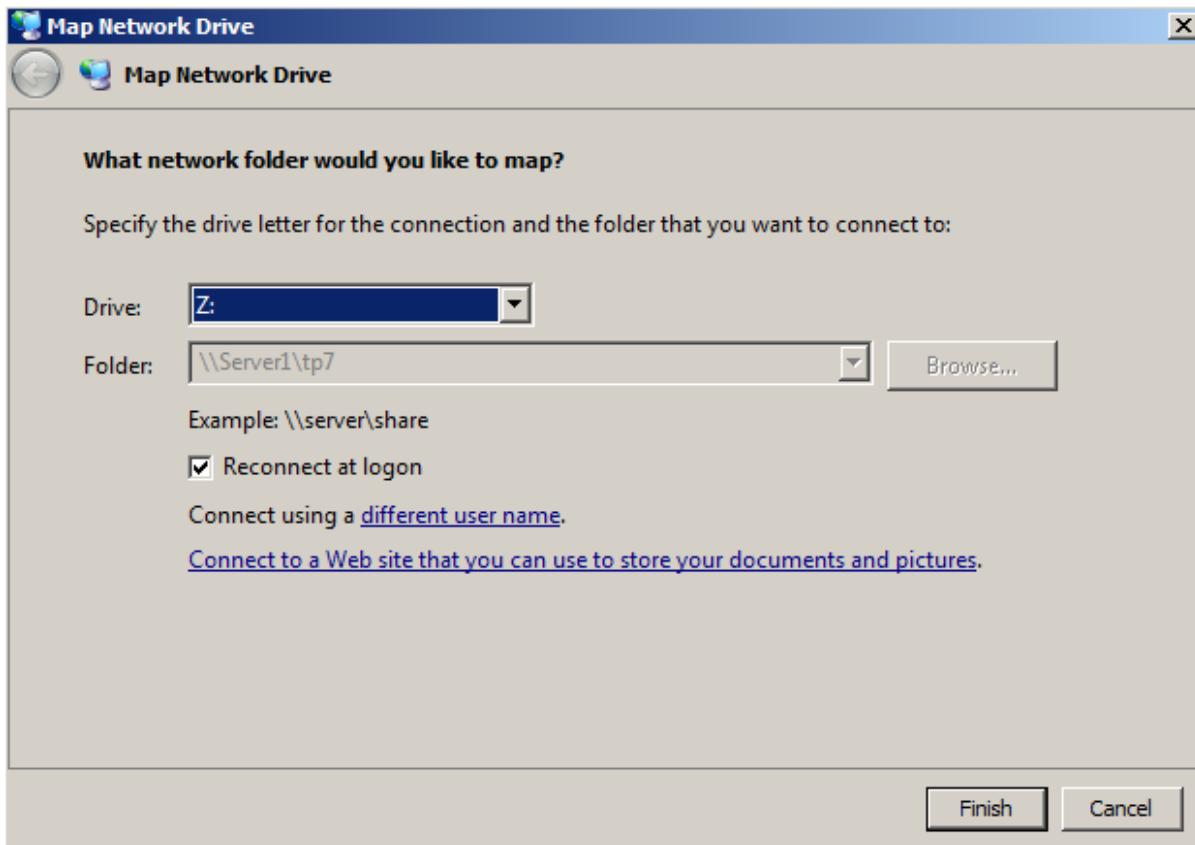
Khi một máy chia sẻ một thư mục, thì các máy khác sẽ nhìn thấy và truy cập qua tên chia sẻ. Tuy nhiên tại các máy khác này ta có thể gắn cho mỗi tên chia sẻ một ký tự ổ đĩa (như là một bí danh của tên chia sẻ), và ổ đĩa này được gọi là ổ đĩa mạng (để phân biệt với ổ đĩa cục bộ được gắn với máy tính). Ổ đĩa mạng sẽ được hiện trong mục My computer.

Tất cả các chữ cái từ A – Z mà chưa dùng đến đều có thể dùng để đặt tên ổ đĩa mạng.

Muốn định nghĩa một ổ đĩa mạng ta phải truy nhập vào tài nguyên mạng để tìm một tên chia sẻ, bằng cách từ giao diện Explorer, lần lượt chọn My Network Places/Entire Network/Microsoft Windows Network/Nhóm máy (ví dụ Khoatin)/Máy cần truy nhập (ví dụ May1). Như Hình 5.5 ta đã truy nhập vào máy tính có tên **May1**, và nhìn thấy các tài nguyên mà máy này đã chia sẻ để dùng chung trên mạng, trong đó có thư mục **Documents**. Nếu muốn gắn một ổ đĩa mạng cho thư mục này, ta nhấn nút chuột phải tại nó, rồi chọn mục **Map Network Drive** từ menu ngữ cảnh để hiện ra cửa sổ như Hình 5.6.



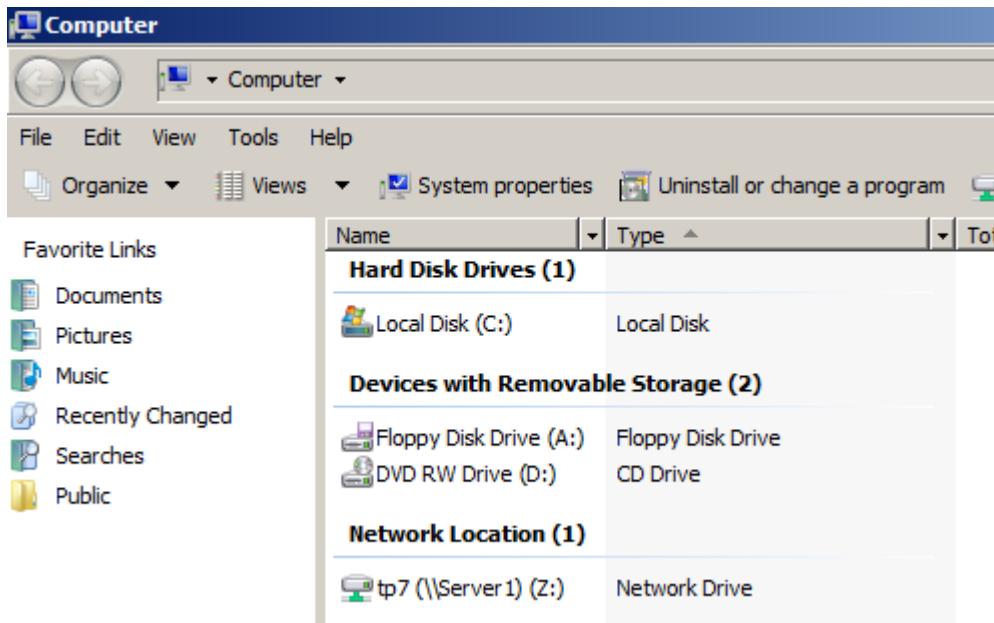
Hình 5.5: Dùng giao diện Explorer để truy nhập tài nguyên mạng



Hình 5.6: Cửa sổ định nghĩa ổ đĩa mạng

Tiếp theo ta chọn ký tự làm ổ đĩa mạng tại mục **Drive**. Ô duyệt **Reconnect at logon** được chọn mặc định có nghĩa là, ổ đĩa mạng này sẽ được dùng lại tại những lần đăng nhập vào mạng sau này. Còn nếu bỏ ô duyệt tại đây, thì ổ đĩa mạng này sẽ không còn hiệu lực tại lần đăng nhập kế tiếp. Kết thúc việc định nghĩa ta nhấn nút **Finish**.

Để xem các ổ đĩa mạng đã định nghĩa, ta vào mục My computer cũng trong giao diện Explorer, trong đó những ổ đĩa mạng sẽ có thêm biểu tượng ở đầu để phân biệt với các ổ đĩa cục bộ, như Hình 5.7 ta thấy có ba ổ đĩa mạng là F, G và M. Tại đây nếu muốn bỏ (không định nghĩa) ổ đĩa mạng nào thì nhấn nút phải chuột tại nó, rồi chọn **Disconnect** từ menu ngữ cảnh.



Hình 5.7: Xem các ổ đĩa mạng

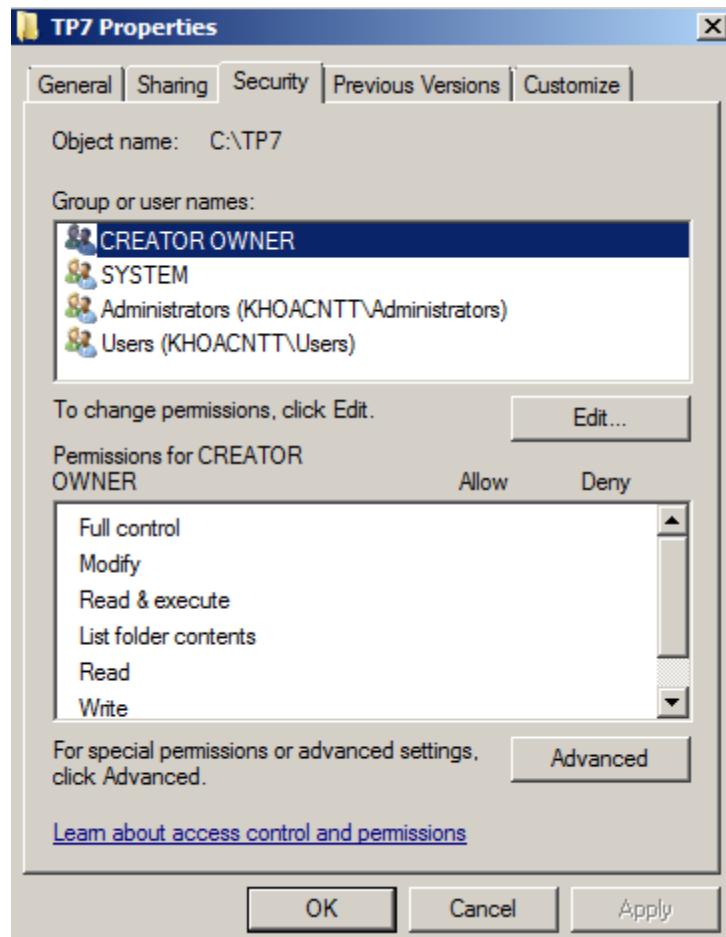
5.1.3. Trao quyền truy cập cục bộ

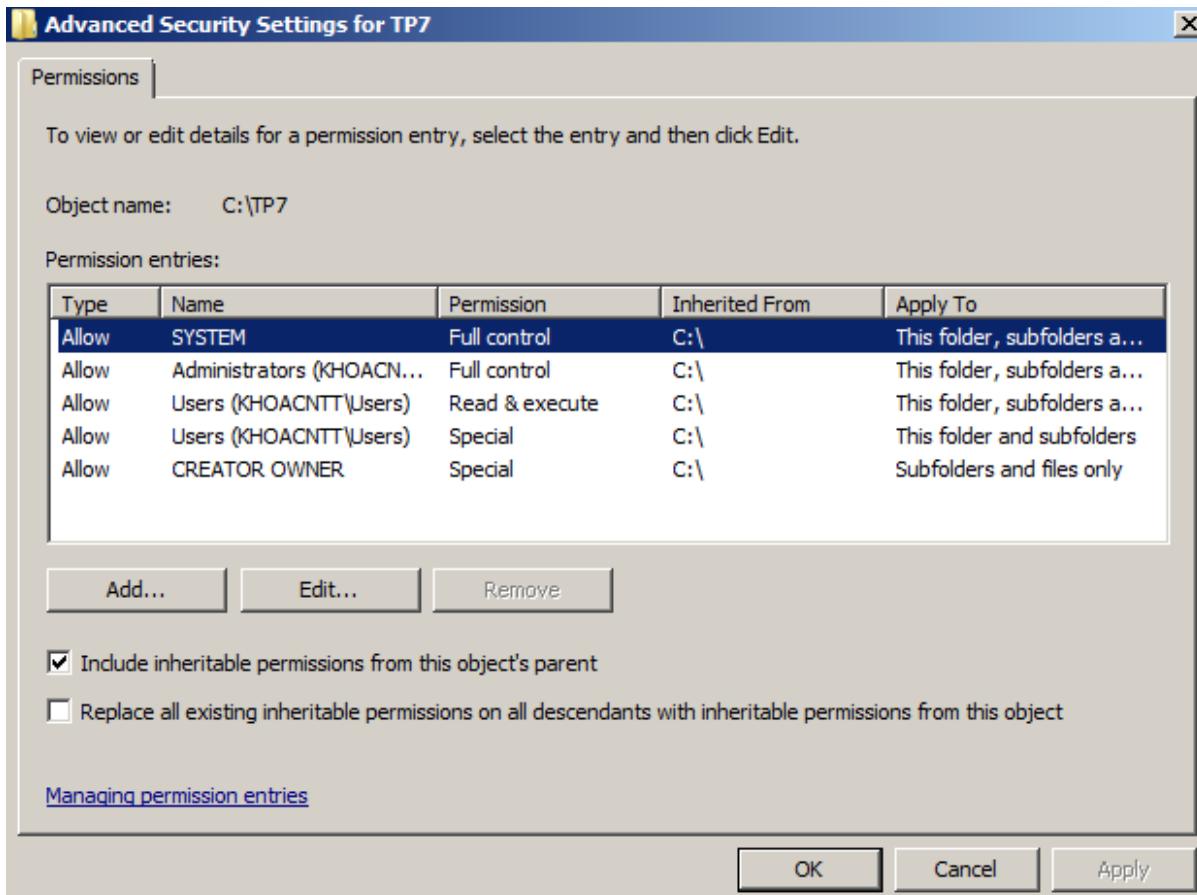
Mỗi file hay thư mục trong hệ thống NTFS đều có một thuộc tính gọi là *Owner*, để chứa chủ nhân hay người sở hữu của nó. Luôn có một chủ nhân nào đó cho mỗi file hay thư mục. Chủ nhân của một file hay thư mục thì có quyền sở hữu (ownership) file hay thư mục đó. Quyền sở hữu hoàn toàn tách biệt với các quyền truy cập, và phải có quyền sở hữu một file hay thư mục thì ta mới có thể trao quyền truy cập file hay thư mục (quyền truy cập cục bộ) cho các nhóm và người sử dụng khác.

Như vậy kể cả người quản trị Administrator, nếu không phải là chủ sở hữu của một file hay thư mục thì cũng không thể trao quyền truy cập cục bộ cho các đối tượng khác. Nhưng người quản trị Administrator và nhóm quản trị Administrators lại có một khả năng đặc biệt là có thể chiếm quyền sở hữu của bất kỳ file hay thư mục nào, cho dù họ không có bất kỳ quyền truy cập nào đối với các file hay thư mục này.

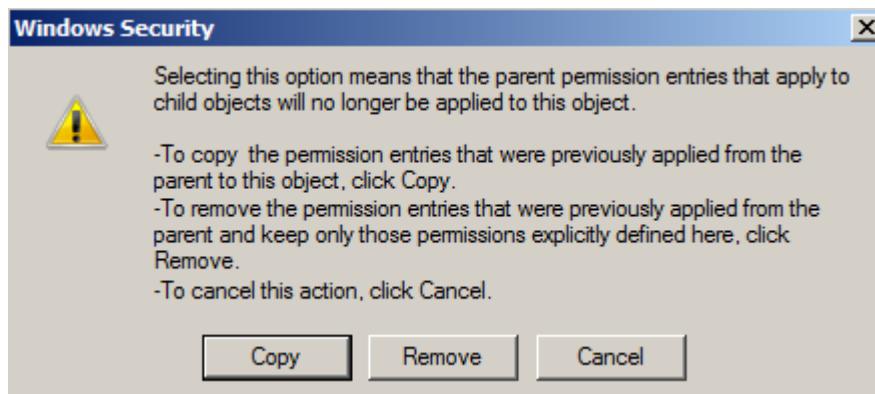
Khi một người sử dụng tạo ra một file hay thư mục, thì họ sẽ mặc định là chủ sở hữu của file hay thư mục này. Với những file hay thư mục mà không có ai là người rõ ràng tạo ra (như các file và các thư mục hệ thống) thì quyền sở hữu của chúng được giao cho nhóm quản trị Administrators.

Khi đã là chủ nhân của một file hay thư mục, nếu muốn thiết định hoặc sửa thiết định chế độ bảo mật cho nó (trao quyền truy cập cục bộ), thì ta nhấn nút phải chuột tại file hay thư mục đó từ giao diện Explorer hoặc My Documents, chọn **Properties** từ menu ngữ cảnh, rồi chọn trang **Security**, để hiện ra cửa sổ như hình 5.8. Trên đó ta thấy có tuỳ chọn **Allow inheritable permissions from parent to propagate to this object** và được chọn duyệt mặc định. Tuỳ chọn này xuất hiện nếu thư mục hoặc file đang xét đang nằm trong thư mục mẹ nào đó ở mức trên. Và ý nghĩa của tuỳ chọn này là thừa hưởng những thiết định bảo mật đã có từ thư mục mẹ. Như trong Hình 5.8, tất cả các quyền truy cập mà nhóm Everyone có được đều là những quyền thừa hưởng từ thư mục mẹ. Nếu không muốn thừa hưởng những thiết định đã có từ thư mục mẹ thì ta bỏ ô duyệt của tuỳ chọn trên. Khi đó sẽ hiện ra cửa sổ như Hình 5.9 để ta chọn một trong những khả năng sau: nếu ta muốn bắt đầu bằng cách lấy các thiết định đã thừa hưởng làm cơ sở thì chọn **Copy**. Khi đó nhóm Everyone vẫn có đầy đủ các quyền như cũ nhưng sẽ được coi là quyền đặt trực tiếp mà không phải là quyền thừa hưởng; nếu muốn bắt đầu từ đầu (bỏ hết các quyền thừa hưởng) thì chọn **Remove**. Khi đó nhóm Everyone sẽ không còn một quyền nào và cũng bị loại luôn ra khỏi khung **Name**; nếu lại muốn thừa hưởng những thiết định đã có thì chọn **Cancel**.





Hình 5.8: Cửa sổ trao quyền truy cập cục bộ cho các đối tượng



Hình 5.9: Những lựa chọn trước khi ngăn không cho thừa hưởng những thiết định đã có

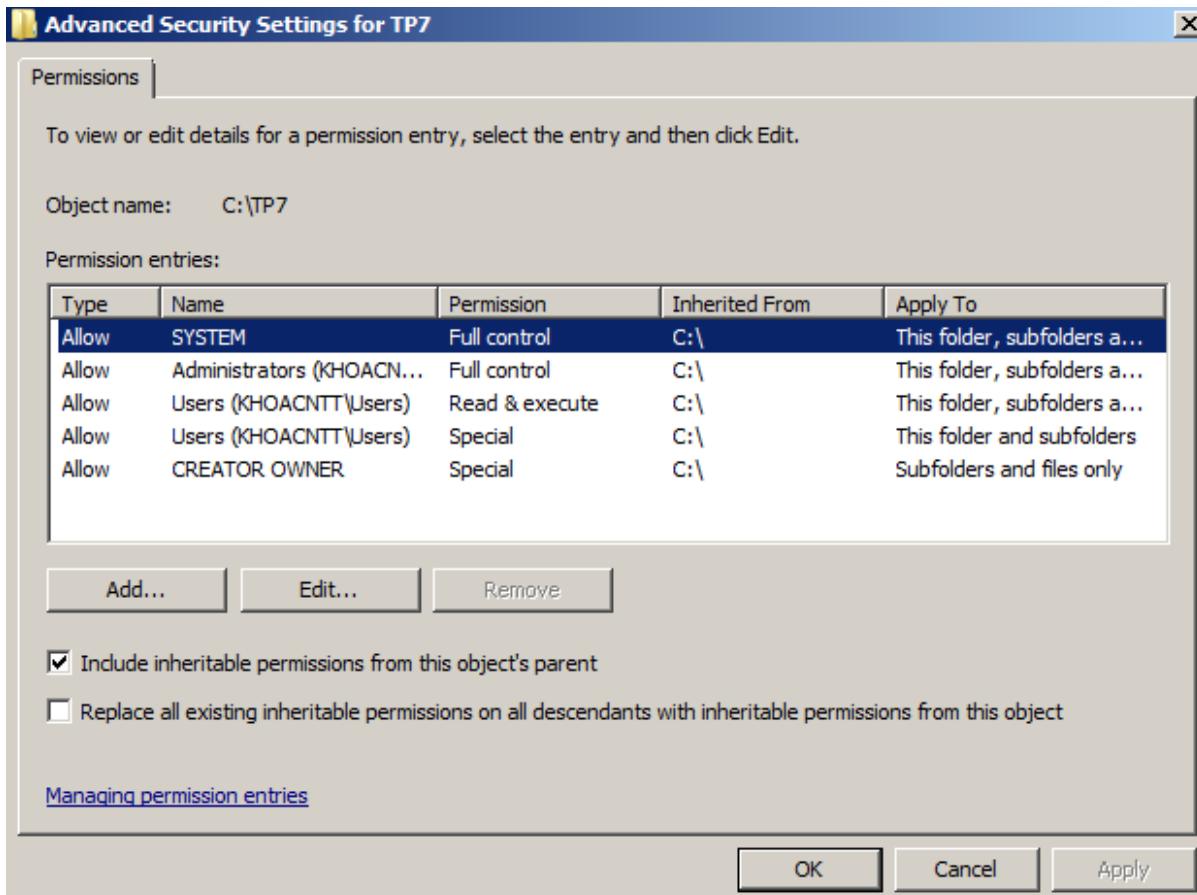
Tại cửa sổ Hình 5.8, nếu muốn trao quyền truy cập cục bộ cho các người sử dụng hoặc nhóm khác thì nhấn nút **Add**, và chọn những đối tượng mong muốn từ danh sách hiện ra.

Nếu không muốn trao quyền truy cập cục bộ cho một đối tượng nào đó thì ta chọn đối tượng đó từ khung **Name** rồi nhấn **Remove**.

Nếu muốn sửa lại quyền truy cập của một đối tượng nào đó, ta chọn đối tượng đó, rồi duyệt / bỏ duyệt vào ô **Allow** tại quyền cần trao / không trao. Nếu muốn ngăn cấm tường minh một đối tượng không được nhận quyền nào đó, thì ta duyệt vào ô **Deny** của quyền đó. Để ngăn cấm không tường minh một quyền nào đó, thì ta không duyệt ở cả hai ô Allow và Deny

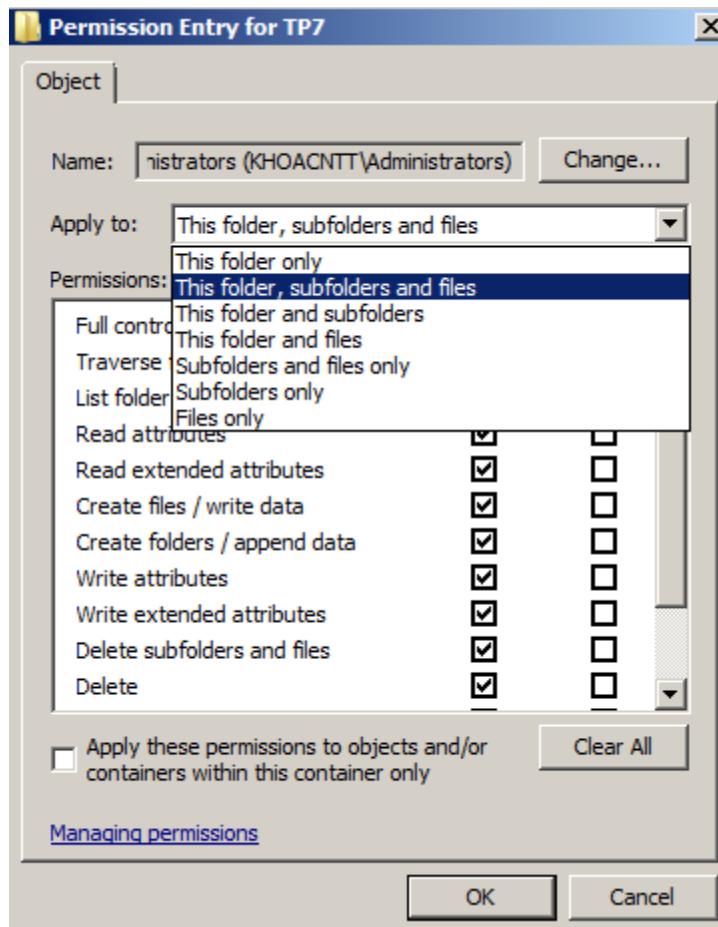
Đến đây ta có thể nhấn nút OK để kết thúc quá trình thiết định chế độ bảo mật cho file hoặc thư mục. Tuy nhiên ta thấy các quyền được đặt ở trên là các quyền truy cập mức cao (luôn là tổ hợp của các quyền truy cập mức thấp). Nếu muốn thiết định tới tận các quyền truy cập mức thấp và cũng để chọn một số thiết định khác, thì ta nhấn nút **Advance** để hiện ra cửa sổ như Hình 5.10. Một số thông tin được trình bày ở cửa sổ này cũng giống và có ý nghĩa như cửa sổ trong Hình 5.8, có chỗ được đổi lại từ ngữ một chút. Chẳng hạn khung **Name** và **Permissions** bây giờ gộp thành **Permission Entries** để cho ta thấy các nhóm và người dùng được chọn, kèm theo những lời mô tả về các quyền truy cập mà họ vừa được cấp.

Ở đây ta thấy có thêm ô duyệt mới là **Reset permissions on all child objects and enable propagation of inheritable permissions**. Ô duyệt này chỉ xuất hiện khi ta tiến hành thiết định chế độ bảo mật cho thư mục, và khi nó được chọn thì có nghĩa là các thiết định bảo mật của thư mục này sẽ được phân bổ cho các file và các thư mục con của nó bằng cách tự chọn ô duyệt **Allow inheritable permissions from parent to propagate to this object** của mỗi file và các thư mục con trong nó.



Hình 5.10: Cửa sổ đặt những thiết định truy cập cao cấp

Nếu muốn trao các quyền truy cập mức thấp cho một đối tượng nào đó, thì ta chọn nó trong khung **Permission Entries**, rồi nhấn nút **View/Edit**. Khi đó ta sẽ có được những chọn lựa như Hình 5.11. Từ đây ta cũng có thêm nhiều cách lựa chọn tổ hợp của các quyền truy cập mức thấp này. Mục **Apply onto** cho phép ta phân bổ các quyền truy cập này cho một sự kết hợp nào đó của: thư mục hiện tại, các thư mục con và các file của thư mục hiện tại. Tuy nhiên nếu muốn phân bổ đến các thư mục con và các file của thư mục hiện tại thì ta phải thêm chọn duyệt ô **Apply these permissions to objects and/or containers within this container only**.



Hình 5.11: Cửa sổ trao quyền truy cập mức thấp

Để kết thúc ta nhấn nút OK tại các cửa sổ.

5.1.4. Lấy quyền sở hữu

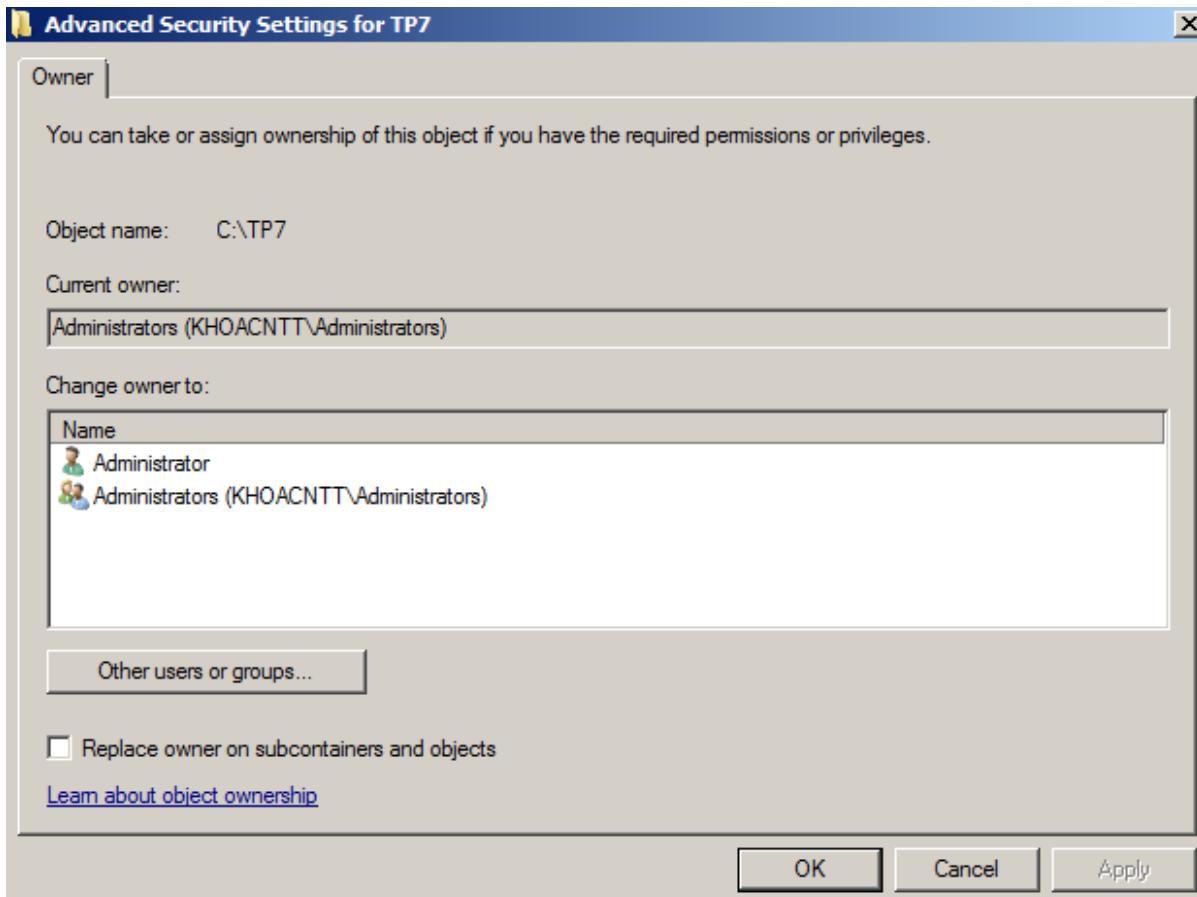
Trong quá trình phân bổ và thu hồi các quyền truy cập, có thể sẽ gặp trường hợp là không một ai, kể cả người quản trị mạng có thể truy cập được vào một file hoặc một thư mục xác định, đồng thời cũng không thể thay đổi được quyền truy cập vào file hoặc thư mục đó. Đó là do người sở hữu file hoặc thư mục đó đã bị xoá. Vậy thì tình huống này sẽ được giải quyết như thế nào?

Trong mục 5.1.2, khi nói về quyền sở hữu ta đã biết là khi một người sử dụng tạo ra một file hoặc thư mục mới thì quyền sở hữu file hoặc thư mục này sẽ thuộc về họ. Và khi một người sử dụng đã có quyền sở hữu đối với một file hoặc thư mục nào đó sẽ có thể cấp cho mình toàn quyền sử dụng file hoặc thư mục này,

đồng thời còn có thể cấp quyền truy cập file hoặc thư mục này cho các đối tượng khác.

Như vậy để giải quyết tình huống này thì trước hết ta phải chiếm lấy quyền sở hữu file hoặc thư mục này. Trong mục 5.1.3 ta thấy nếu đối tượng nào có quyền Take Ownership đối với một file hoặc thư mục thì đều có thể lấy được quyền sở hữu của file hoặc thư mục này. Nhưng hiện tại có thể không có một đối tượng nào có quyền Take Ownership đối với một file hoặc thư mục đó. Rất may là Windows server cho phép người quản trị Administrator và các thành viên của nhóm quản trị Administrators, luôn có thể lấy được quyền sở hữu của bất kỳ file hoặc thư mục nào mặc dù không có quyền Take Ownership đối với một file hoặc thư mục đó.

Để lấy được quyền sở hữu của một file hoặc thư mục, ta phải đăng nhập vào máy với tư cách là người sẽ lấy quyền sở hữu của một file hoặc thư mục đó. Do vậy, trước hết ta đăng nhập vào máy với tư cách là người quản trị Administrator hoặc là thành viên nào của nhóm quản trị Administrators, sau đó thực hiện các thao tác tương tự như khi trao quyền truy cập cục bộ đối với file hoặc thư mục đó, cho đến khi mở tới cửa sổ như Hình 5.10 thì nhấn chuột vào mục Owner để hiện ra cửa sổ như Hình 5.12.



Hình 5.12: Cửa sổ xem/lấy quyền sở hữu

Nhìn vào cửa sổ này ta thấy quyền sở hữu thư mục TP7 đang thuộc về user **Administrator**, Nếu muốn chuyển quyền sở cho đối tượng khác, thì ta nhấn chuột tại đối tượng cần chuyển trong khung Name, rồi nhấn OK.

Khi đã có quyền sở hữu file hoặc thư mục đó, thì ta có thể trao quyền truy cập vào file hoặc thư mục này cho chính mình.

5.1.5. Tổng hợp các quyền truy cập

Khi người sử dụng được trao cả quyền truy cập đối với một thư mục, và cả với một số file hay thư mục con của nó, thì chỉ quyền truy cập đối file hay thư mục con là có hiệu lực. Như vậy nếu một người sử dụng có thể được trao toàn quyền sử dụng một thư mục TP1, nhưng sau đó lại chỉ được trao quyền chỉ đọc đối với file vanban.doc nằm trong TP1, thì người sử dụng đó vẫn không thể sửa được nội dung của file này.

Nhưng cũng có ngoại lệ là nếu người sử dụng có quyền mọi đối tượng trong một thư mục, nhưng lại được trao quyền cấm xoá đối với một file hay thư mục con của nó, thì thực chất người sử dụng vẫn xoá được file hay thư mục con này.

Vì người sử dụng có thể được trao cả quyền truy cập từ xa và quyền truy cập cục bộ đối với một file hoặc thư mục. Đồng thời họ cũng có thể nhận được các quyền này từ các nhóm mà họ là thành viên. Khi đó tổng hợp lại thì họ có những quyền truy cập thực sự nào đối với một file hoặc thư mục? Nguyên tắc của cách tính quyền truy cập tổng hợp như sau:

- Trước hết ta tổng hợp các quyền truy cập mà người sử dụng có được nhờ được trao trực tiếp, và được kế thừa từ các nhóm mà họ là thành viên (khi tổng hợp, ta phân thành hai nhóm là: quyền truy cập từ xa và quyền truy cập cục bộ). Quyền tổng hợp ở đây sẽ là hợp của các quyền mà người sử dụng có được nhờ được trao trực tiếp, và các quyền kế thừa từ các nhóm mà họ là thành viên, trừ ra những quyền bị cấm tường minh.

Ví dụ:

Nếu người sử dụng **A** được trao quyền truy cập từ xa **Change** (bao gồm cả các quyền **Modify, Read, Write**), và quyền truy cập cục bộ **Modify, Write** đối với thư mục **TP7**.

Giả sử **A** là thành viên của nhóm **N1**, nhóm này được trao quyền truy cập từ xa **Read**, và quyền truy cập cục bộ **Read**, trong khi bị cấm tường minh hai quyền truy cập cục bộ **Modify** và **Write** đối với thư mục **TP7**.

Khi đó quyền tổng hợp từ xa mà **A** có được đối với thư mục **TP7** là **Change**, quyền tổng hợp cục bộ là **Read**.

- Sau đó quyền tổng hợp thực sự mà người sử dụng có được sẽ là những quyền hạn chế nhất giữa các quyền tổng hợp từ xa và các quyền tổng hợp cục bộ, tức là sẽ bằng giao của các quyền tổng hợp từ xa và các quyền tổng hợp cục bộ.

Như trong ví dụ trên, thì quyền truy cập thực sự của **A** đối với thư mục **TP7** sẽ bằng giao của **Change** và **Read**, cho kết quả là **Read**.

5.2. QUẢN LÝ Ổ ĐĨA

5.2.1. Cấu hình hệ thống tập tin

Hệ thống tập tin quản lý việc lưu trữ và định vị các tập tin trên đĩa cứng. Windows Server hỗ trợ hệ thống tập tin NTFS.

5.2.2. Cấu hình đĩa lưu trữ

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

5.2.2.1. Basic storage

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

5.2.2.2. Dynamic storage

Đây là một tính năng mới của Windows Server. Đĩa lưu trữ dynamic chia thành các volume dynamic. Volume dynamic không chứa partition hoặc ổ đĩa logic, và chỉ có thể truy cập bằng Windows Server. Windows Server hỗ trợ năm loại volume dynamic: simple, spanned, striped, mirrored và RAID-5.

Ưu điểm của công nghệ Dynamic storage so với công nghệ Basic storage:

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

Năm loại volume dynamic:

- Volume simple : Chứa không gian lấy từ một đĩa dynamic duy nhất. Không gian đĩa này có thể liên tục hoặc không liên tục.
- Volume spanned : Bao gồm một hoặc nhiều đĩa dynamic (tối đa là 32 đĩa). Sử dụng khi muốn tăng kích cỡ của volume. Dữ liệu ghi lên volume theo thứ tự, hết đĩa này đến đĩa khác. Do dữ liệu được ghi tuần tự nên volume loại này không

tăng hiệu năng sử dụng. Nhược điểm chính của volume spanned là nếu một đĩa bị hỏng thì toàn bộ dữ liệu trên volume không thể truy xuất được.

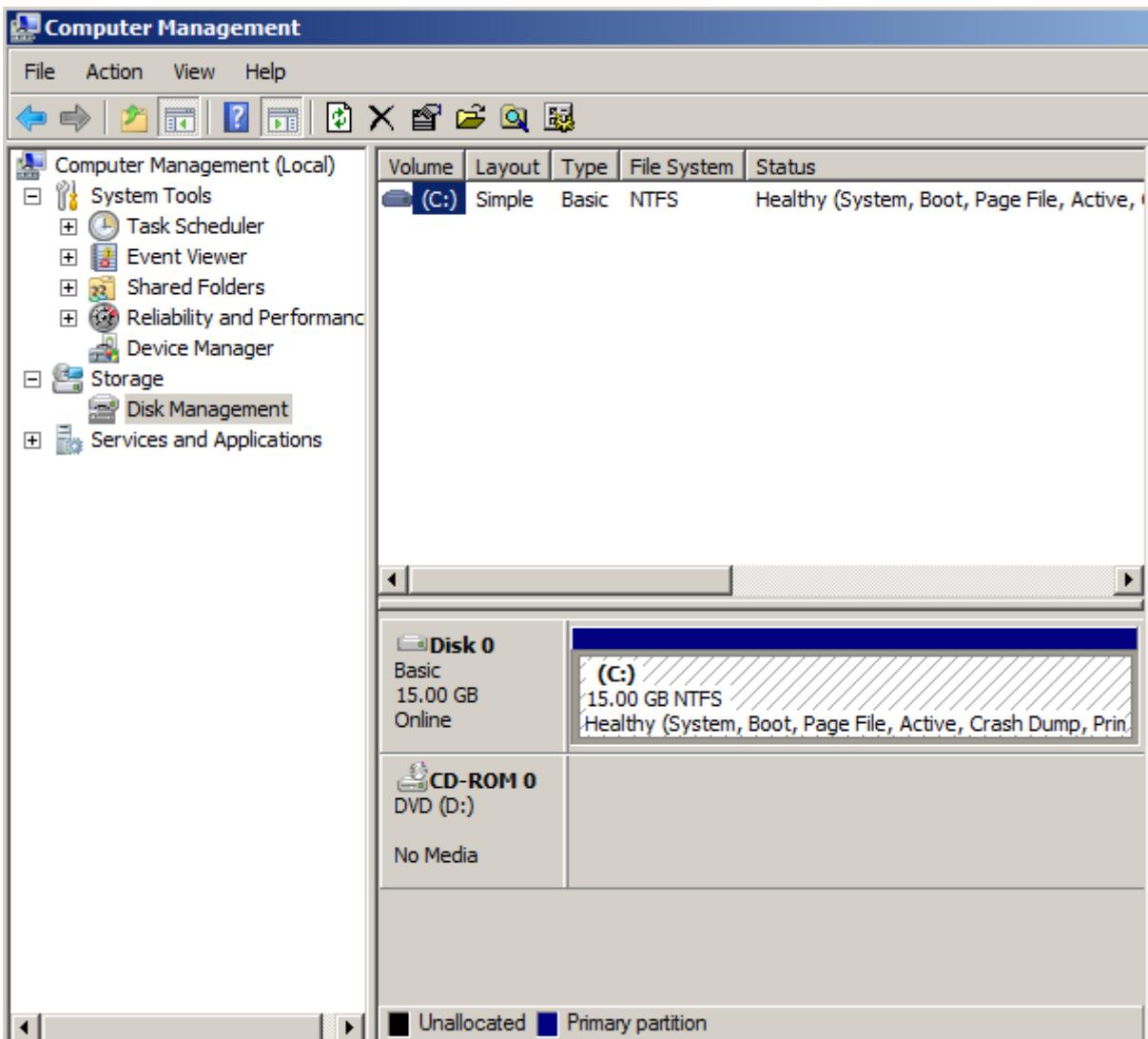
- Volume striped : Lưu trữ dữ liệu lên các dãy (strip) bằng nhau trên một hoặc nhiều đĩa vật lý (tối đa là 32). Do dữ liệu được ghi tuần tự lên từng dãy, nên có thể thi hành nhiều tác vụ I/O đồng thời, làm tăng tốc độ truy xuất dữ liệu. Nhược điểm chính của volume striped là nếu một ổ đĩa bị hỏng thì dữ liệu trên toàn bộ volume mất giá trị.

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

- Volume RAID-5 : Tương tự như volume striped nhưng RAID-5 lại dùng thêm một dãy (strip) ghi thông tin kiểm lỗi parity. Nếu một đĩa của volume bị hỏng thì thông tin parity ghi trên đĩa khác sẽ giúp phục hồi lại dữ liệu trên đĩa hỏng. Volume RAID-5 sử dụng ít nhất ba ổ đĩa (tối đa là 32). Ưu điểm chính của kỹ thuật này là khả năng dung lõi cao và tốc độ truy xuất cao bởi sử dụng nhiều kênh I/O.

5.2.3. Sử dụng chương trình disk Manager

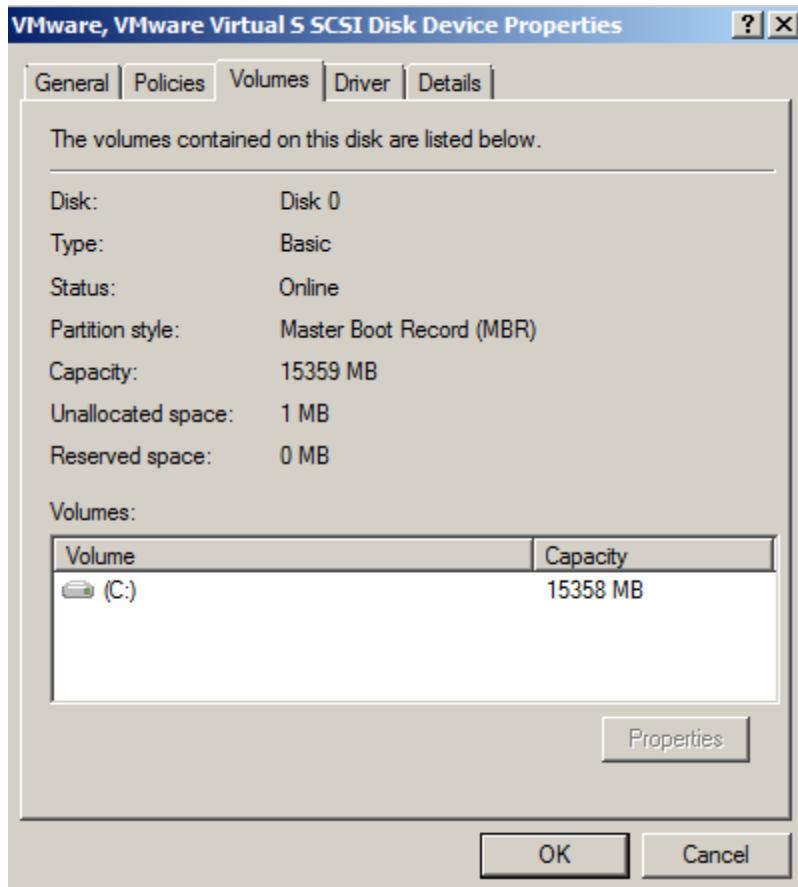
Disk Manager là một tiện ích giao diện đồ họa phục vụ việc quản lý đĩa và volume trên môi trường Windows Server. Để có thể sử dụng được hết các chức năng của chương trình, phải đăng nhập vào máy bằng tài khoản Administrator. Vào menu Start → Programs → Administrative Tools → Computer Management. Sau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



Hình 5.13: Cửa sổ chương trình Disk Management

a. Xem thuộc tính của đĩa

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



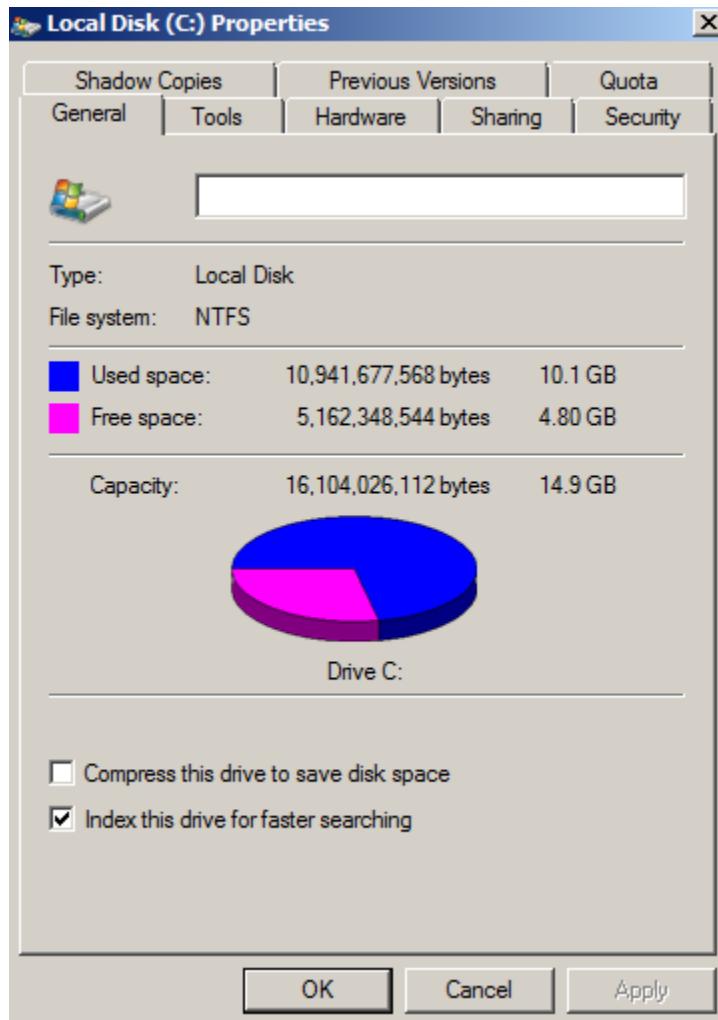
Hình 5.13: Thuộc tính thông tin ổ đĩa

Hộp thoại cung cấp các thông tin:

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

b. Xem thuộc tính của volume hoặc đĩa cục bộ

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



Hình 5.14: Thuộc tính Volume của ổ đĩa

c. Bổ sung thêm một ổ đĩa mới

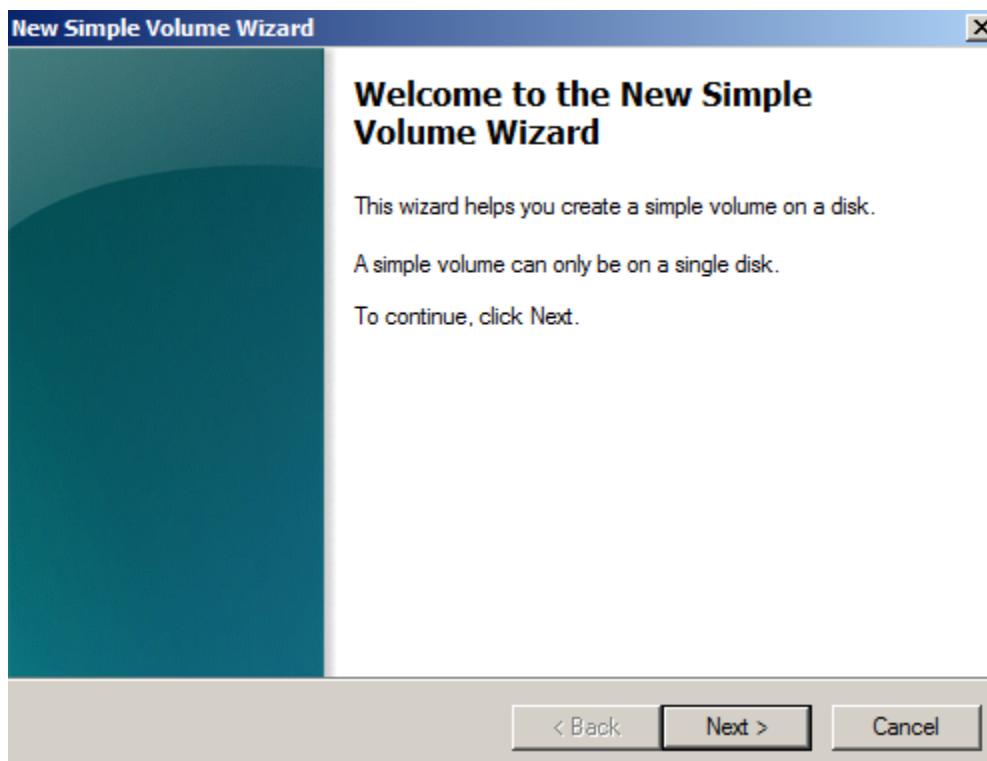
- Máy tính không hỗ trợ tính năng “hot swap”, phải tắt máy tính rồi mới lắp ổ đĩa mới vào. Sau đó khởi động máy tính lại. Chương trình Disk Management sẽ tự động phát hiện và yêu cầu bạn ghi một chữ ký đặc biệt lên ổ đĩa, giúp cho Windows Server nhận diện được ổ đĩa này. Theo mặc định, ổ đĩa mới được cấu hình là một đĩa dynamic.

- Máy tính hỗ trợ “hot swap”, chỉ cần lắp thêm ổ đĩa mới vào theo hướng dẫn của nhà sản xuất mà không cần tắt máy. Rồi sau đó dùng chức năng Action →Rescan Disk của Disk Manager để phát hiện ổ đĩa mới này.

d. Tạo Partition/Volume mới

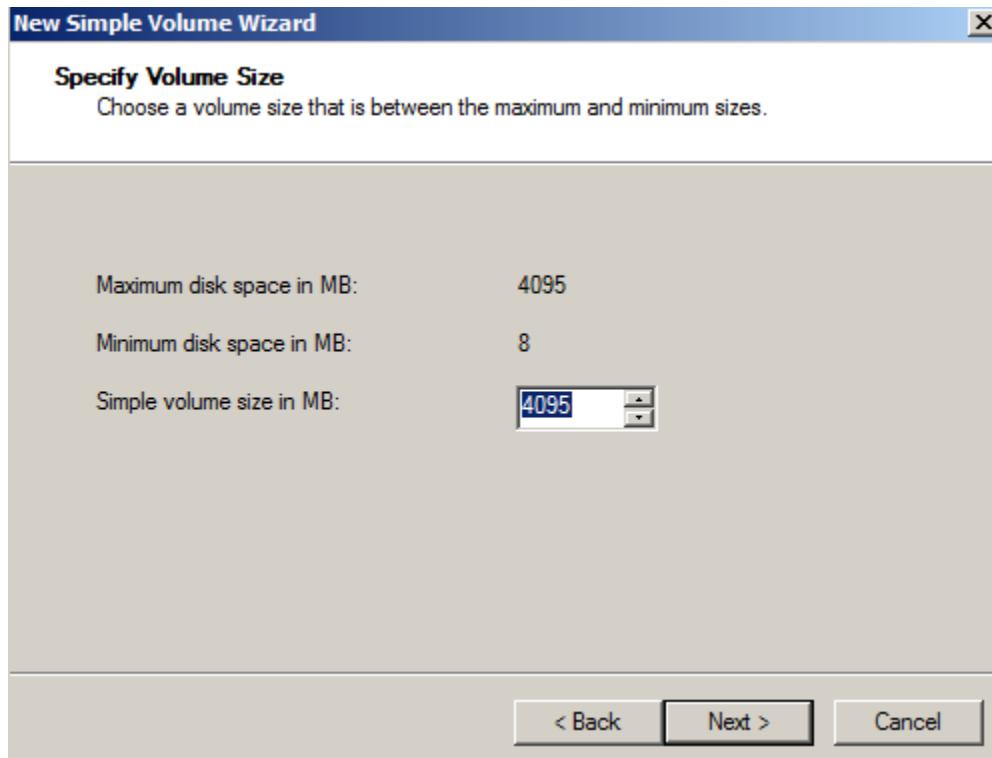
Nếu còn không gian chưa cấp phát trên một đĩa basic thì có thể tạo thêm partition mới, còn trên đĩa dynamic thì có thể tạo thêm volume mới. Sử dụng Create Partition Wizard để tạo một partition mới:

Nhấp phải chuột lên vùng trống chưa cấp phát của đĩa basic và chọn New Simple Volume



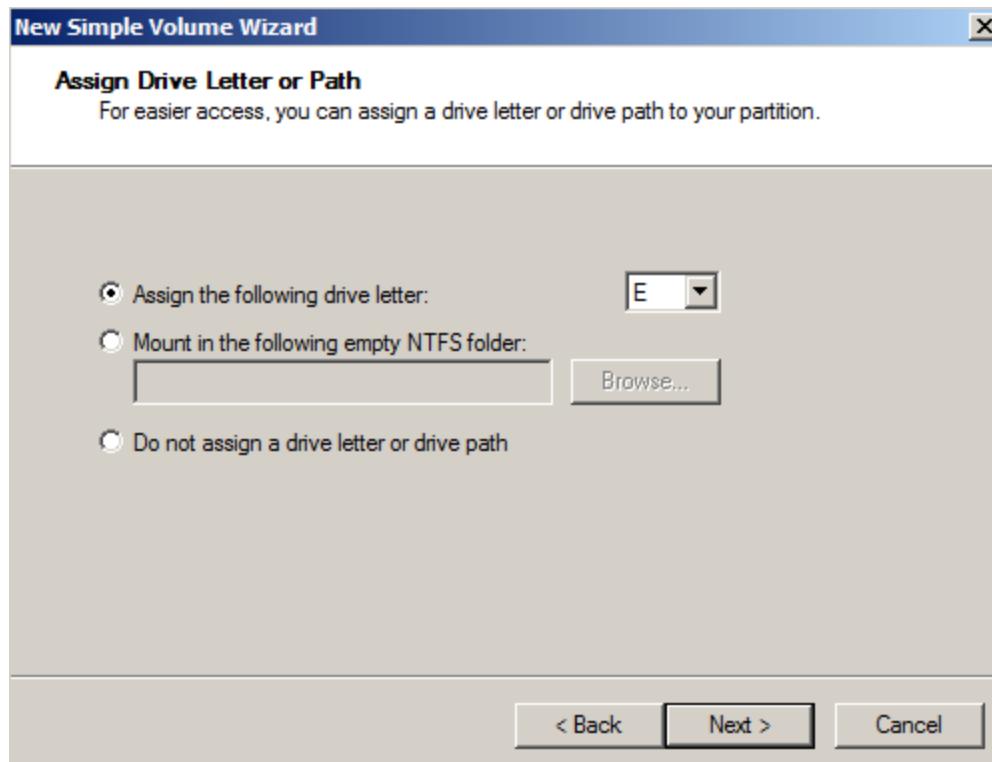
Hình 5.15: Cửa sổ ban đầu tạo Partition

Xuất hiện hộp thoại New Simple Volume. Nhấn nút Next trong hộp thoại này. Tiếp theo, hộp thoại Specify Partition Size yêu cầu cho biết dung lượng định cấp phát. Sau khi chỉ định xong, nhấn Next.



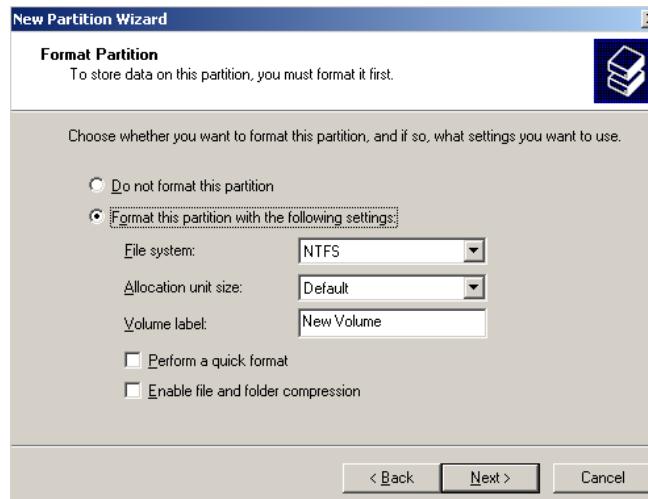
Hình 5.16: Cửa sổ chọn kích thước ổ đĩa

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



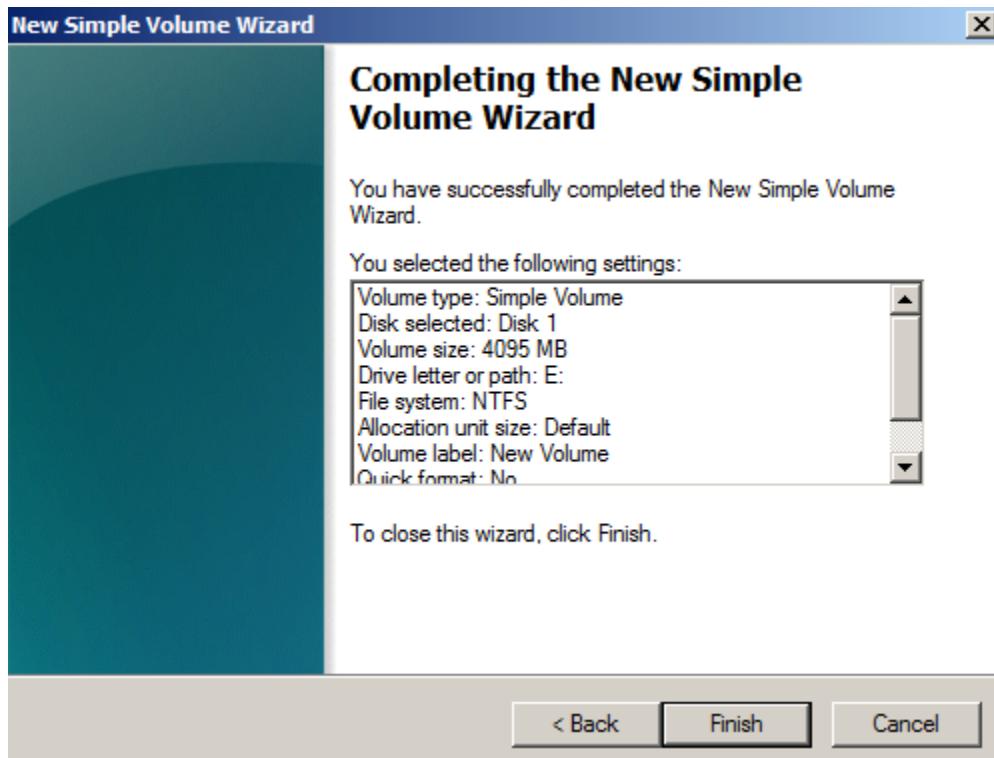
Hình 5.17: Cửa sổ chọn ký tự định danh cho ổ đĩa

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



Hình 5.18: Chọn định dạng ổ đĩa

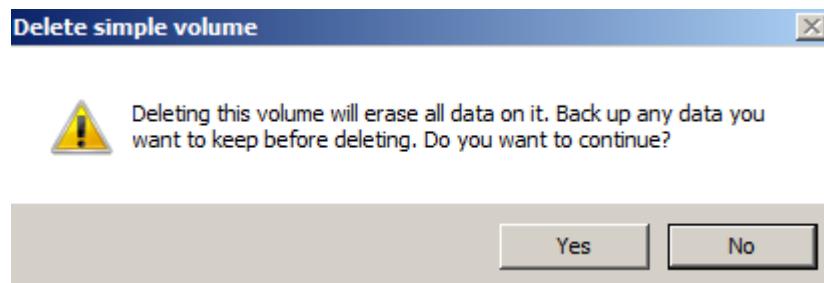
Hộp thoại Completing the Create Partition Wizard tóm tắt lại các thao tác sẽ thực hiện, phải kiểm tra lại xem đã chính xác chưa, sau đó nhấn Finish để bắt đầu thực hiện.



Hình 5.19: Xem lại các thuộc tính đã chọn cho ổ đĩa

e. Xoá Partition/Volume

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

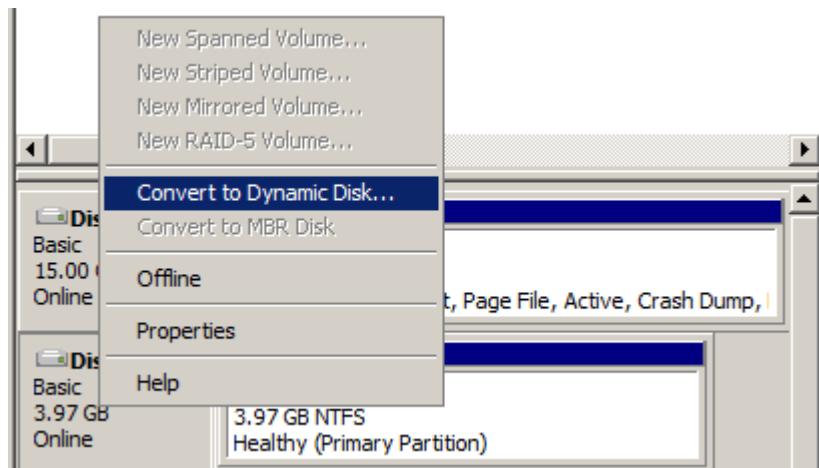


Hình 5.20: Xóa ổ đĩa

f. Cấu hình Dynamic Storage

- Chuyển chế độ lưu trữ.

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



Hình 5.21: Chuyển đổi cơ chế lưu trữ ổ đĩa

5.2.4. Quản lý việc nén dữ liệu

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

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

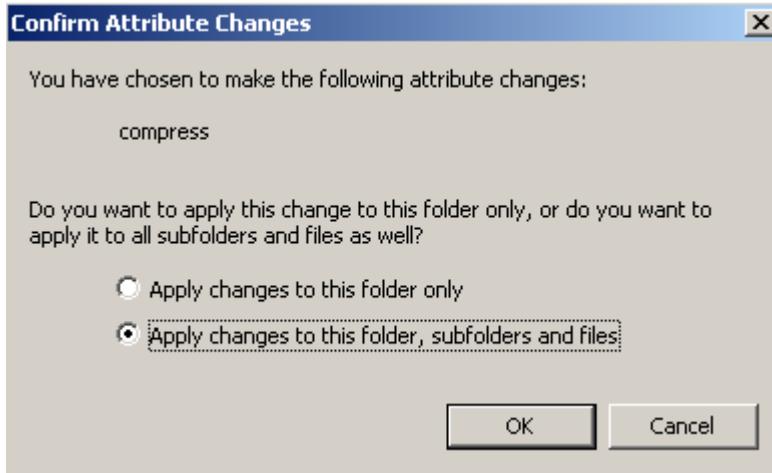
- Trong cửa sổ Windows Explorer, duyệt đến tập tin/thư mục định nén và chọn tập tin/thư mục đó.

- Nhấp phải chuột lên đối tượng đó và chọn Properties.
- Trong hộp thoại Properties, nhấn nút Advanced trong tab General.
- Trong hộp thoại Advanced Properties, chọn mục “Compress contents to save disk space” và nhấn chọn OK.



Hình 5.22: Cửa sổ nén dữ liệu

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



Hình 5.23: **Lựa chọn cách thức nén dữ liệu**

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

5.2.5. Thiết lập hạn ngạch đĩa (Disk Quota)

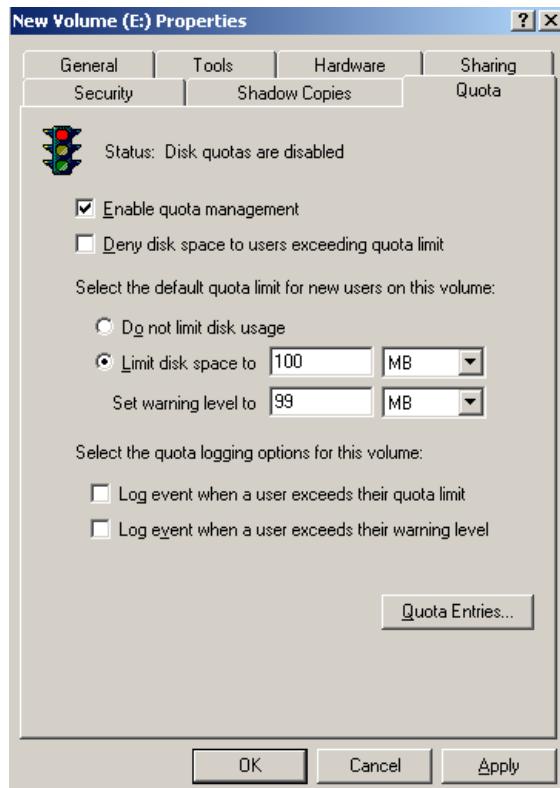
Hạn ngạch đĩa được dùng để chỉ định lượng không gian đĩa tối đa mà một người dùng có thể sử dụng trên một volume NTFS. Có thể áp dụng hạn ngạch đĩa cho tất cả người dùng hoặc chỉ đối với từng người dùng riêng biệt.

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

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

5.2.5.1. Cấu hình hạn ngạch đĩa

Nhấp phải chuột lên ký tự ổ đĩa trong Windows Explorer và chọn Propertise. Trong hộp thoại này nhấp chọn tab Quota. Theo mặc định tính năng hạn ngạch đĩa không được kích hoạt.



Hình 5.24: Thiết lập hạng ngạch đĩa

Các mục trong hộp thoại có ý nghĩa như sau:

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

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

5.2.5.2. Thiết lập hạn ngạch mặc định

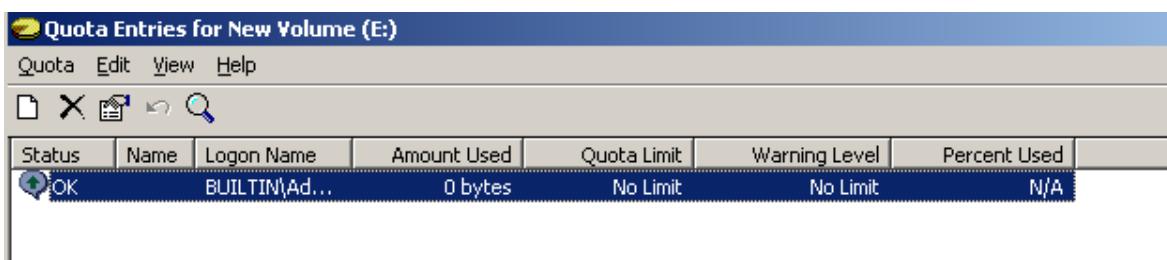
a. Khi thiết lập hạn ngạch mặc định áp dụng cho các người dùng mới trên volume, chỉ những người dùng chưa bao giờ tạo tập tin trên volume đó mới chịu ảnh hưởng. Có nghĩa là những người dùng đã sở hữu các tập tin/thư mục trên volume này đều không bị chính sách hạn ngạch quy định. Như vậy, nếu dự định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

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

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

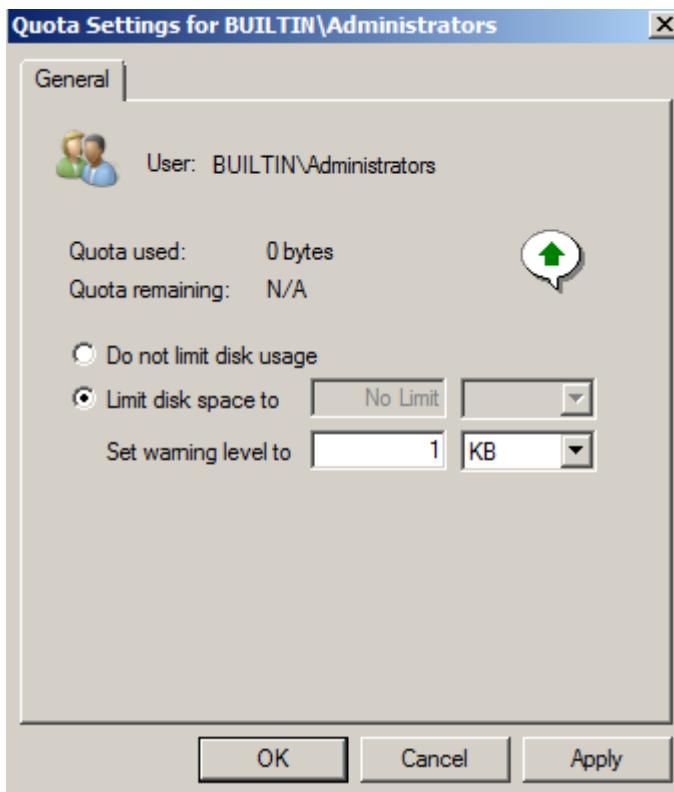
- Người dùng này sẽ giữ nhiệm vụ cài đặt các phần mềm mới, và như vậy họ phải có được lượng không gian đĩa trống lớn.
- Hoặc là người dùng đã tạo nhiều tập tin trên volume trước khi thiết lập hạn ngạch, do vậy họ sẽ không chịu tác dụng. Cần phải tạo riêng một giới hạn mới áp dụng cho người đó.

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



Hình 5.25: Cửa sổ Quota Entries

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



Hình 5.26: Thay đổi giá trị các hạn ngạch

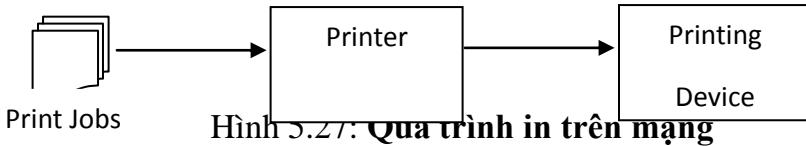
Bổ sung thêm một mục quy định hạn ngạch: trong cửa sổ Quota Entries, vào menu Quota chọn mục New Quota Entry → xuất hiện hộp thoại Select Users, chọn người dùng rồi nhấn OK → xuất hiện hộp thoại Add New Quota Entry, nhập các giá trị hạn ngạch thích hợp và nhấn OK.

5.3. DỊCH VỤ IN TRÊN MẠNG

Trong hệ thống mạng Windows Server, bất kỳ một máy in nào được nối vào một máy tính (máy trạm, hoặc máy chủ) đều có thể được truy cập để in từ các máy tính khác trong mạng. Máy tính có máy in để sẵn sàng phục vụ cho việc in trên mạng thường được gọi là Print server.

5.3.1. Quá trình in trên mạng

Quá trình in trên mạng khá phức tạp, nhưng có thể được hình dung tóm tắt như sau:



Hình 5.27: Quá trình in trên mạng

Trong đó:

- **Print Jobs**: là những *công việc in* được gửi đi khi chọn chức năng in từ các ứng dụng như Word, Excel, ...

- **Printer** (máy in logic): Đây chỉ là một thiết bị có tính cách logic, đóng vai trò trung gian giữa các ứng dụng của người dùng và các thiết bị in, nó thường được gọi ngắn gọn là *máy in*, tên của nó được nhìn thấy trong khi chọn máy in từ các ứng dụng. Tất cả các thiết định về cấu hình in ấn đều áp dụng cho máy in logic, mà không phải là các thiết bị in. Các máy in logic liên lạc, trao đổi thông tin với hệ điều hành thông qua *trình điều khiển in* (printer driver), để gọi các thủ tục in của hệ điều hành. Bởi vậy khi cài đặt một máy in logic, nhất thiết ta phải chọn trình điều khiển cho nó.

- **Printing Device** (thiết bị in): Là *máy in vật lý* cụ thể được gắn với một máy tính để in các công việc in do các máy in logic gửi đến.

Mỗi quan hệ giữa các máy in logic và các máy in vật lý không nhất thiết phải là 1-1, mà có thể nhiều máy in logic ứng với một máy in vật lý (trường hợp này thường dùng khi cần thiết lập nhiều cấu hình in khác nhau cho những nhóm người sử dụng khác nhau, trong khi chỉ có một máy in vật lý), hoặc một máy in logic ứng với nhiều máy in vật lý (trường hợp này được áp dụng khi ta có nhiều máy in vật lý và nhiều người đồng thời cùng in trên một máy in logic. Khi đó máy in logic sẽ tự biết gửi các công việc in đến máy in vật lý còn rỗ).

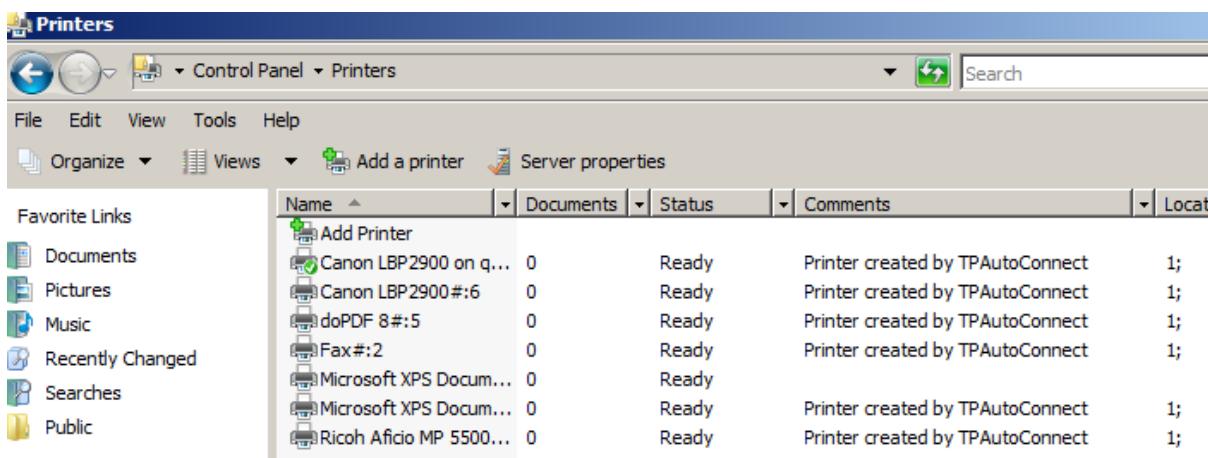
Trên một máy tính có gắn máy in vật lý, để có thể in được, thì trước hết ta phải cài đặt máy in logic cho máy in vật lý. Máy in logic này có thể gọi là *máy in cục bộ*, vì chỉ có thể dùng nó để in ở chính máy tính có cài đặt nó. Muốn các máy tính khác cũng có thể truy nhập đến máy in cục bộ này, thì trước hết ta phải chia sẻ nó. Sau đó trên các máy tính khác ta phải thực hiện việc kết nối với máy in cục bộ đã chia sẻ để tạo ra một máy in logic mới mà ta có thể gọi là *máy in mạng*. Máy in mạng chính là bí danh của máy in cục bộ đã chia sẻ mà nó kết nối vào. Như vậy

quá trình cài đặt để sử dụng được máy in trên mạng phải tuân theo hai bước chính sau:

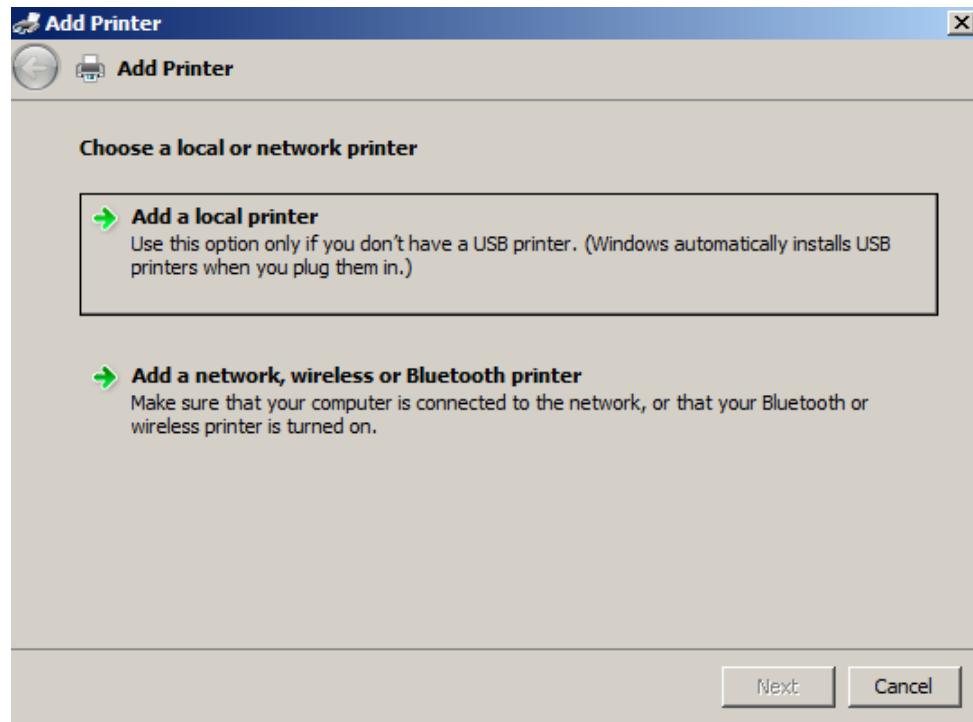
- 1- Cài đặt và chia sẻ máy in cục bộ.
- 2- Kết nối với máy in cục bộ đã chia sẻ.

5.3.2. Cài đặt và chia sẻ máy in cục bộ

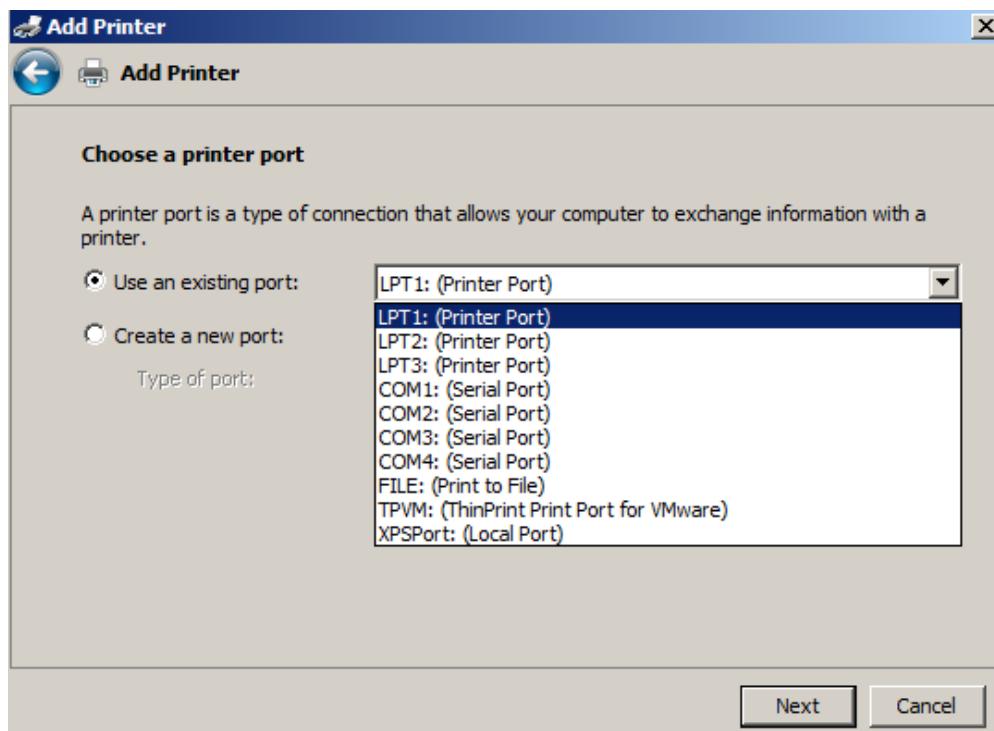
Để cài đặt máy in cục bộ cho một máy in vật lý gắn với một máy tính, ta lần lượt chọn **Start/Settings/Printers** để mở cửa sổ **Printers** như Hình 5.28. Tiếp theo nhấn đúp chuột tại mục **Add Printer**, trong cửa sổ bắt đầu của quá trình cài đặt (Add Printer Wizard), ta nhấn nút **Next** để đến được cửa sổ như Hình 5.29. Tại đây ta chọn **Local printer** vì cần cài máy in cục bộ. Windows server sẽ tự động phát hiện, cài đặt ở các bước tiếp theo, rồi tự chia sẻ máy in logic cục bộ này. Ở đây giả sử ta không chọn ô duyệt trên và chọn **Next** để đến cửa sổ chọn cổng máy in như Hình 5.28.



Hình 5.28: Cửa sổ Printer dùng để quản lý các máy in logic

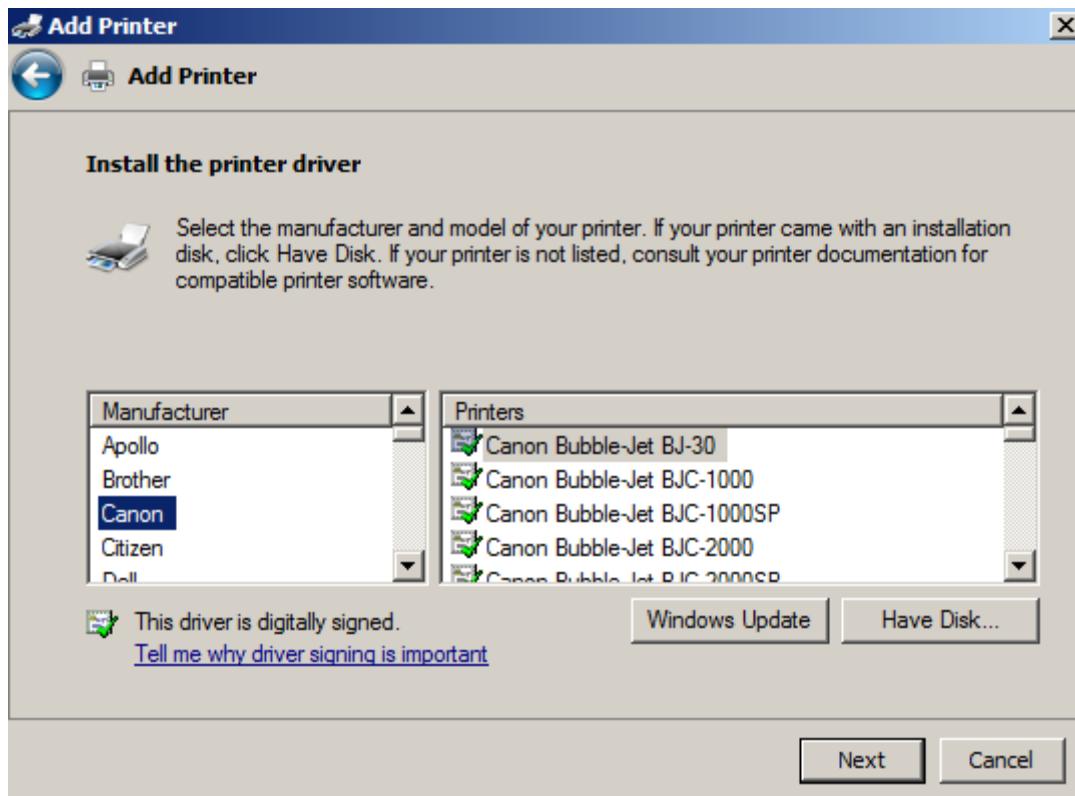


Hình 5.29: Cửa sổ chọn cài đặt máy in cục bộ hay máy in mạng

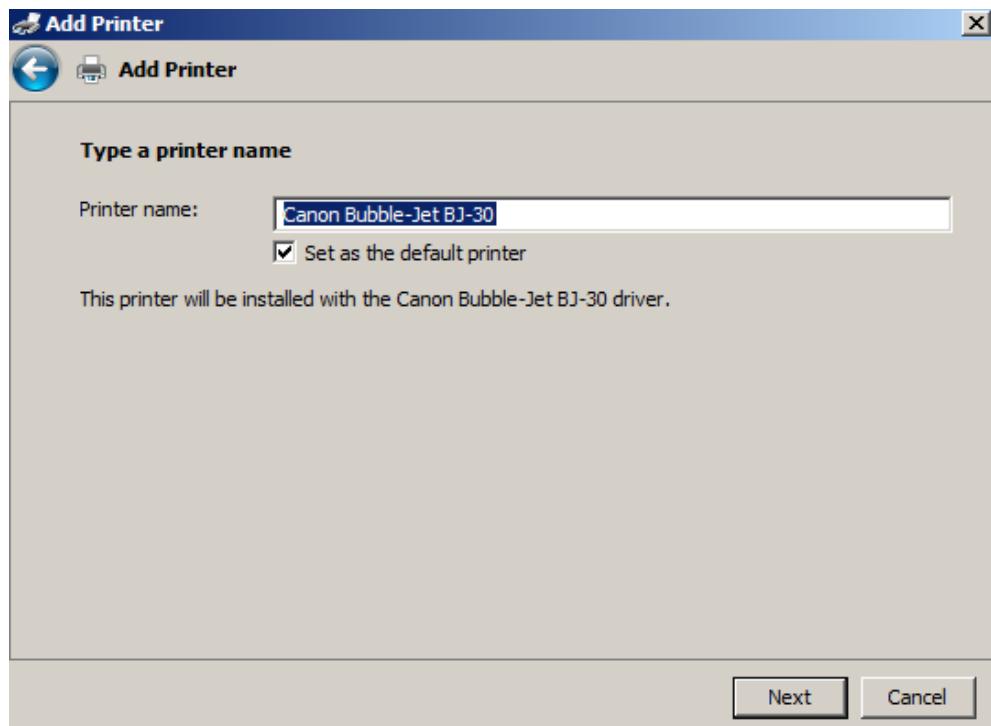


Hình 5.30: Cửa sổ chọn cổng máy in

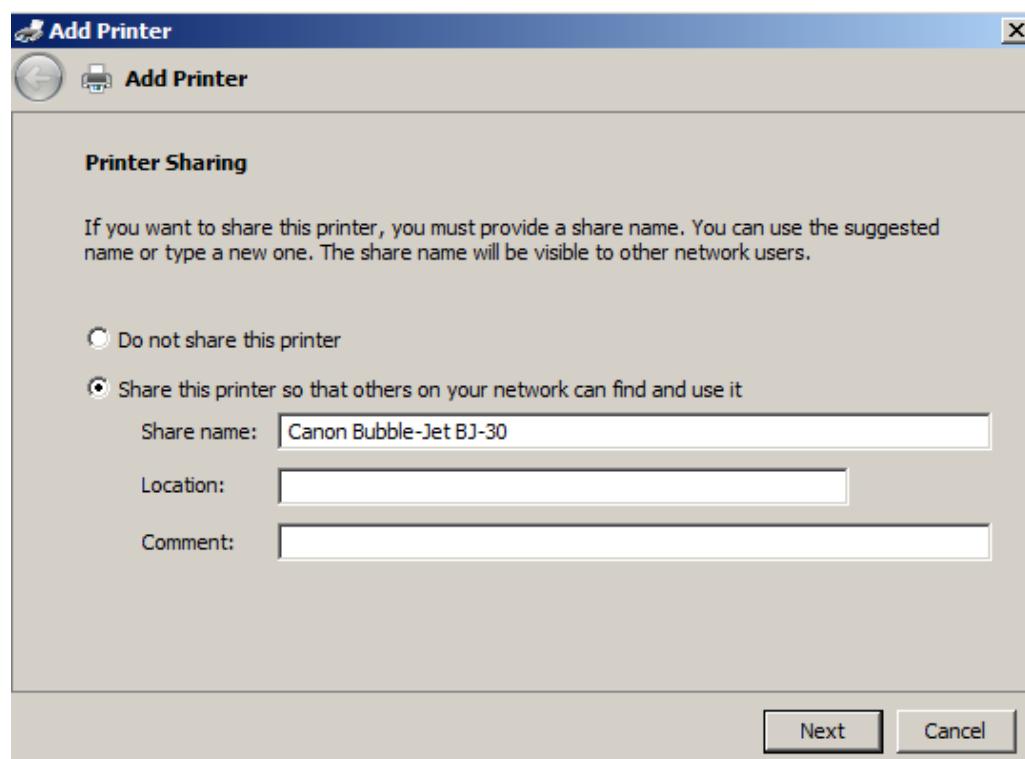
Giả sử máy in vật lý được nối vào cổng song song LPT1, ta chọn cổng đó từ danh sách trên và nhấn nút **Next**. Cửa sổ tiếp theo như Hình 5.31 cho phép ta chọn trình điều khiển in cho máy in. Trong ngăn bên trái (Manufacturers) có hiện các hãng chế tạo, khi chọn hãng nào thì ngăn bên phải (Printers) sẽ hiện danh sách các trình điều khiển in ứng với các kiểu máy in vật lý. Theo mặc định Windows server sẽ dùng các trình điều khiển in của riêng nó. Nếu ta có một bộ trình điều khiển in mới hơn từ đĩa mà nhà chế tạo cung cấp, thì nhấn nút **Have Disk** rồi cho biết đường dẫn của nơi chứa bộ trình điều khiển in đó. Sau khi chọn song trình điều khiển in, ta nhấn nút **Next** để đặt tên cho máy in trong cửa sổ Hình 5.32. Tên của máy in gồm các ký tự bất kỳ và có thể dài đến 80 ký tự. Tiếp theo chọn **Next** để hiện ra cửa sổ như Hình 5.33.



Hình 5.31: Cửa sổ chọn trình điều khiển in

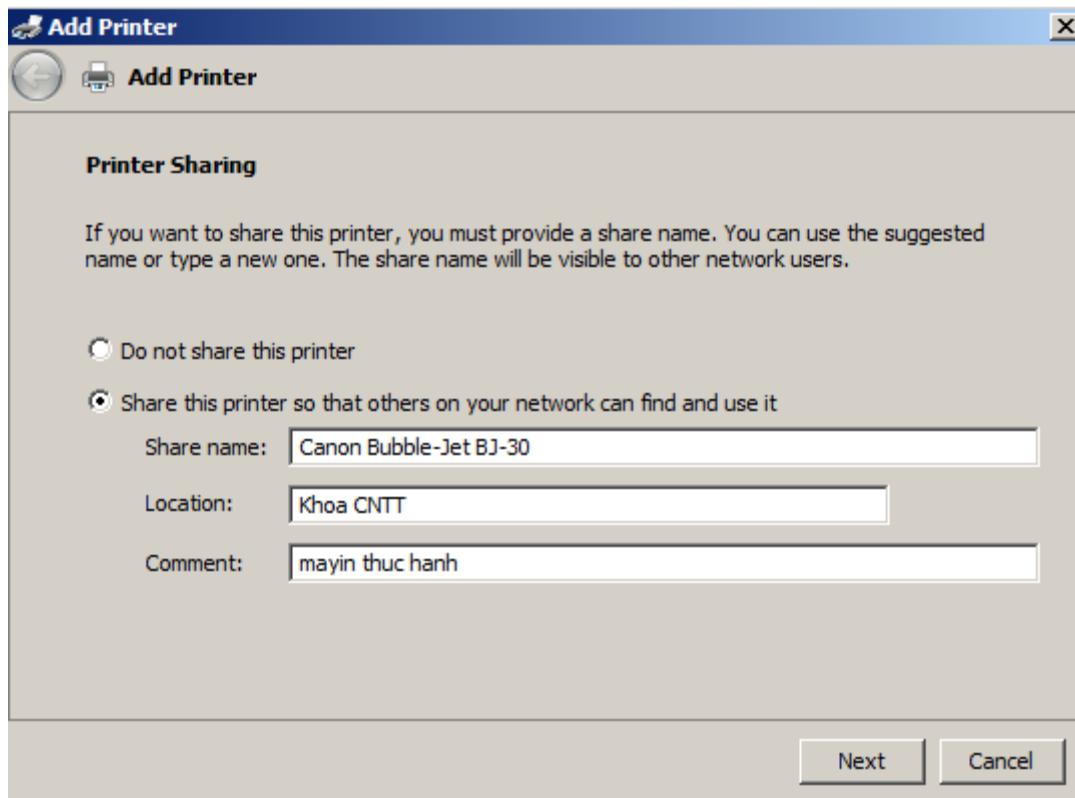


Hình 5.32: **Đặt tên cho máy in cục bộ**



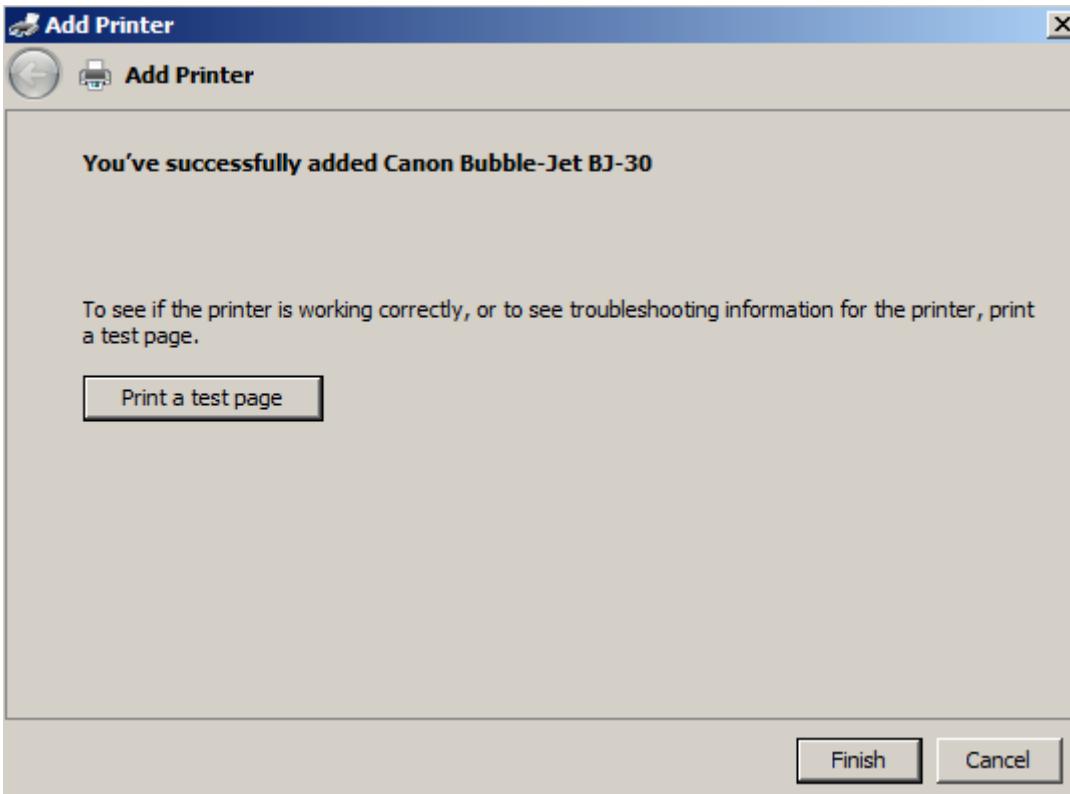
Hình 5.33: **Cửa sổ chọn chia sẻ máy in cục bộ**

Nếu ta muốn chia sẻ ngay máy in cục bộ này thì chọn **Share as** và gõ vào một tên chia sẻ. Nếu không chia sẻ ở đây, sau này ta vẫn có thể chia sẻ nó bằng cách nhấn nút phải chuột tại tên của nó trong cửa sổ Printers, rồi chọn Sharing. Sau khi chọn **Next** ta có cửa sổ như Hình 5.34.



Hình 5.34: Vào những thông tin mô tả về máy in cục bộ này

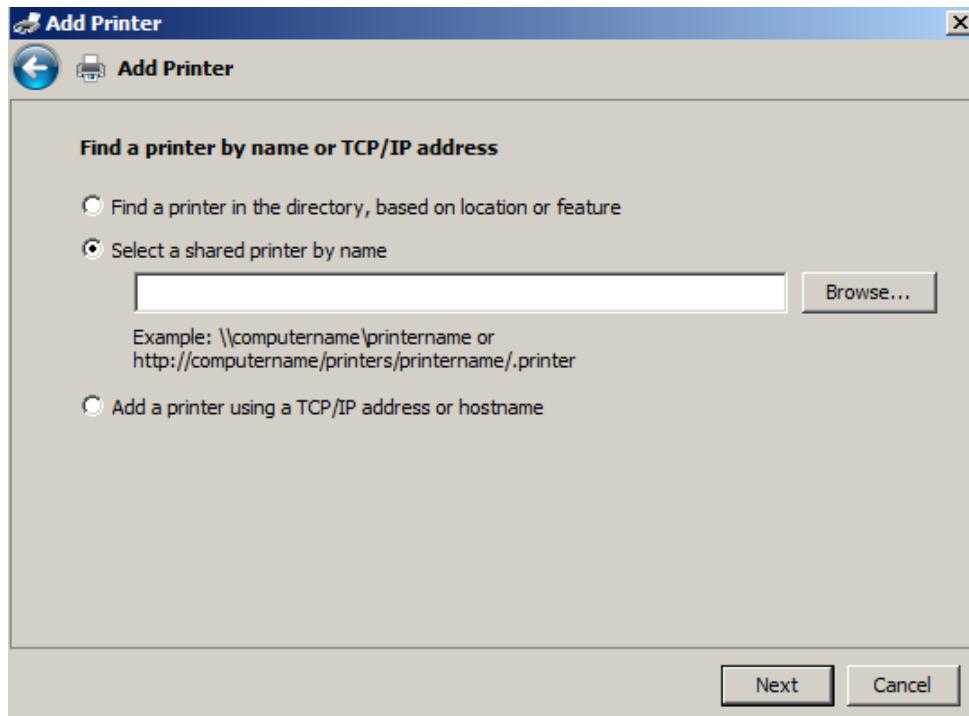
Màn hình trên dùng để mô tả về máy in vật lý được gắn với máy in logic này. Những thông tin ở đây sẽ giúp ích cho việc tìm kiếm và nhận diện các máy in trên mạng, nhưng nếu thấy không cần thiết thì có thể không cần nhập. Khi nhấn **Next**, cửa sổ kế tiếp sẽ hỏi ta có muốn in một trang thử nghiệm hay không (Do you want to print a test page ?), chọn: **Yes** – nếu có, **No** – nếu không, rồi nhấn **Next**, để hiện ra cửa sổ cuối cùng như Hình 5.35. Cửa sổ này hiện ra những thông tin mà ta đã khai báo ở các bước trước. Nếu không thấy còn phải sửa thông tin nào thì ta nhấn nút **Finish** để bắt đầu quá trình cài đặt các tập tin cần thiết và kết thúc. Còn nếu muốn quay lại các bước trước để chỉnh sửa thì nhấn nút **Back**.



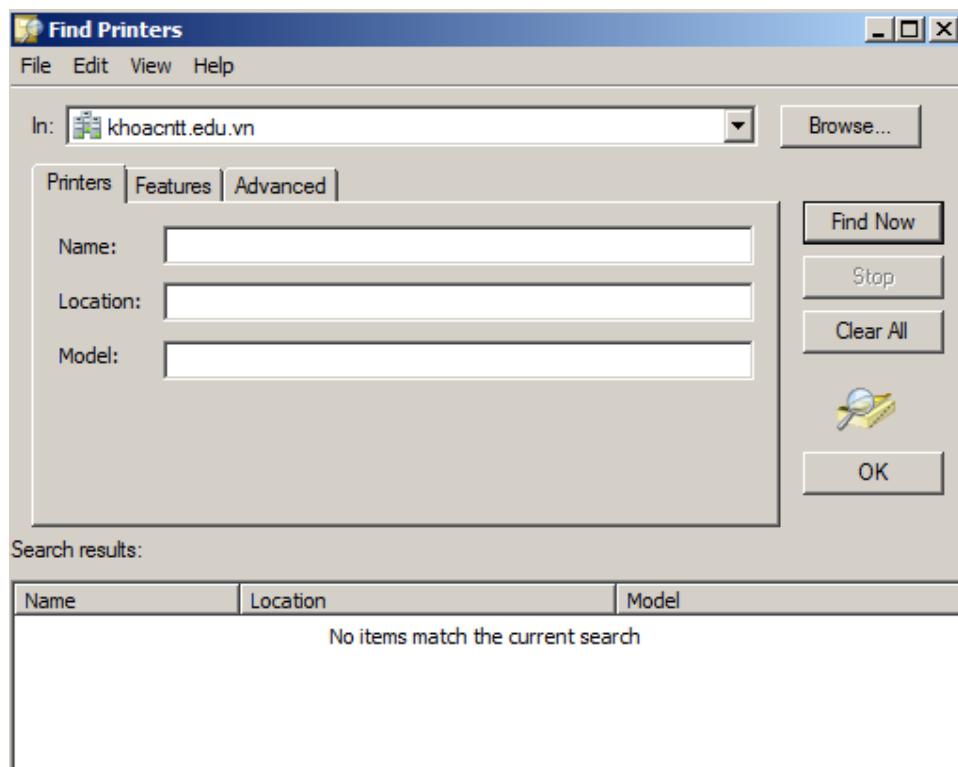
Hình 5.35: Cửa sổ xác nhận những thông tin đã khai báo về máy in cục bộ

5.3.3. Kết nối máy in cục bộ đã chia sẻ

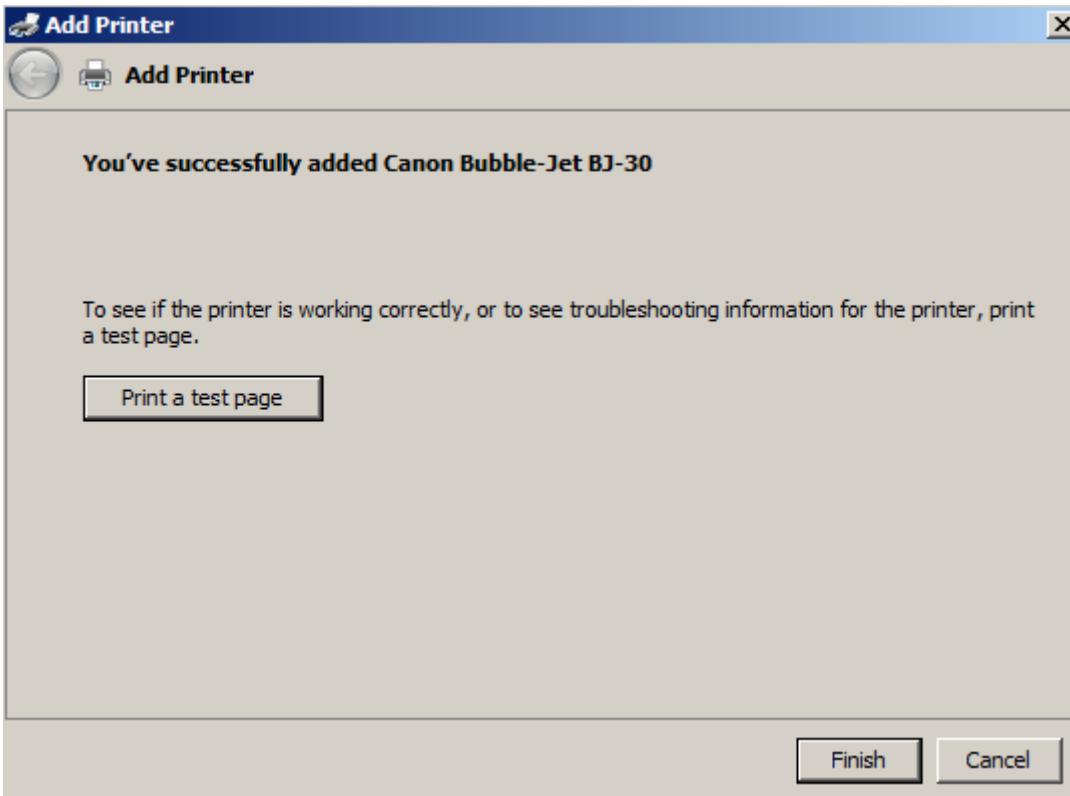
Muốn kết nối với một máy in đã chia sẻ để tạo ra máy in mạng, ta cũng vào cửa sổ **Printers** và nhấn đúp chuột tại mục **Add printer**, chọn **Next**. Khi đó màn hình sẽ hiện ra cửa sổ như Hình 5.29, chọn **Network printer** từ cửa sổ này để tạo máy in mạng, chọn **Next**. Tiếp theo ta có một số cách chọn các máy in đã chia sẻ để kết nối, ở đây ta chọn cách thứ hai như Hình 5.36. Với cách này ta có thể gõ vào tên máy in chia sẻ, hoặc chọn **Next** để duyệt tìm trên mạng. Sau đó ta chọn máy tính có máy in chia sẻ, rồi chọn máy in chia sẻ của máy tính đó, như Hình 5.37 ta thấy máy in chia sẻ vừa tạo ở trên nằm trên MAYCHU1. Khi chọn xong máy in chia sẻ, nhấn **Next**. Cửa sổ tiếp theo hỏi ta có muốn chọn máy in mạng này làm máy in mặc định mà các chương trình sẽ in ra hay không, chọn: **Yes** – nếu có, **No** – nếu không, rồi nhấn **Next** để chuyển đến cửa sổ cuối cùng hiện ra các thông tin đã khai báo về máy in này như Hình 5.35. Nếu đồng ý với những thông tin này, ta nhấn nút **Finish**, ngược lại có thể chọn **Next** để quay về sửa các bước tiếp theo.



Hình 5.36: Chọn cách tìm các máy in đã chia sẻ



Hình 5.37: Tìm các máy in đã chia sẻ để kết nối



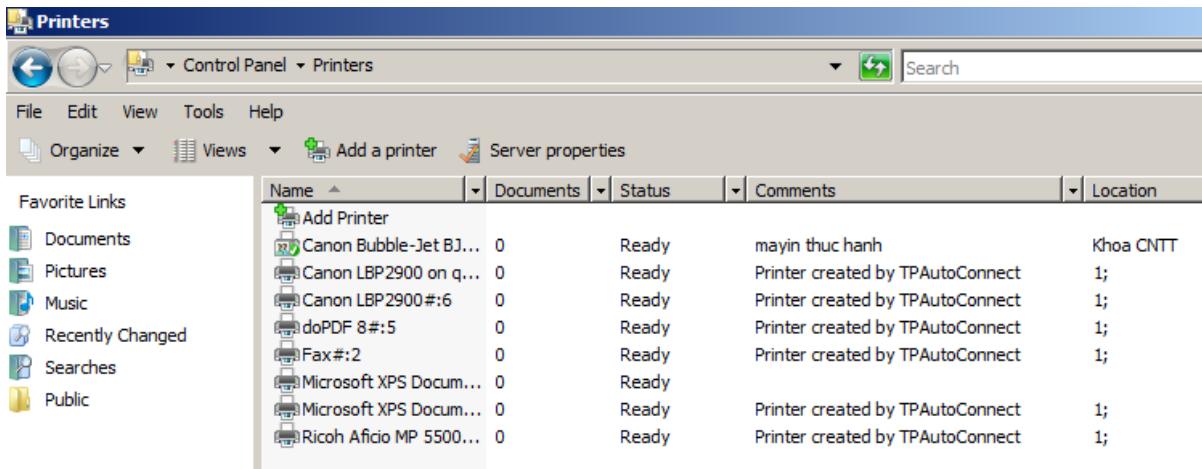
Hình 5.38: Cửa sổ xác nhận những thông tin đã khai báo về máy in mạng

Khi kết thúc các bước trên, màn hình Printers bây giờ có nội dung như Hình 3.38. Trong đó: những máy in mạng được phân biệt bởi biểu tượng có đoạn dây dẫn ở bên dưới, tên của máy in mạng có chỉ cho biết là được kết nối với máy in cục bộ trên máy tính nào; các máy in cục bộ đã chia sẻ sẽ có thêm hình tượng bàn tay ở bên dưới; máy in được chọn mặc định có thêm ký hiệu duyệt chọn ở đầu.

Nếu muốn đặt máy in nào đó là mặc định, ta nhấn nút phải chuột tại máy in đó, rồi chọn **Set as Default Printer**.

Để xoá một máy in, ta chọn nó rồi bấm phím **Delete** và xác nhận **Yes**.

Trong chức năng in của hầu hết các ứng dụng, ta có thể chọn máy in cần in ra (máy in được chọn có thể là máy in cục bộ hoặc máy in mạng), nếu ta không chọn máy in thì được hiểu là chọn máy in mặc định.



Hình 5.39: Các loại máy in trong cửa sổ Printers

5.3.4. Một số thiết định về máy in

Windows server có rất nhiều thiết định về cấu hình và bảo mật cho máy in để đáp ứng nhiều nhu cầu sử dụng máy in khác nhau trên mạng. Trong phạm vi giáo trình này chỉ giới thiệu hai thiết định thông dụng là: tạo và sử các trang phân cách, và thiết lập chế độ bảo mật cho máy in.

5.3.4.1. Tạo và sử dụng các trang phân cách (separator pages)

Khi nhiều người dùng cùng in ra một máy in, rõ ràng là rất dễ nhầm lẫn các bản in của mỗi người. Để khắc phục điều đó, Windows server cho phép ta tạo ra một trang phân cách để ghi những thông tin nhận diện văn bản của mỗi người, sau đó cài đặt trang phân cách này vào máy in. Khi đó trang phân cách này sẽ được tự động in ra trước khi in các trang văn bản của mỗi người.

5.3.4.1.1. Tạo ra trang phân cách mới

Trang phân cách phải được tạo trên máy print server để cài đặt cho các máy in cục bộ của máy này thì mới có tác dụng. Nó được tạo ra dưới dạng các tập tin văn bản đơn giản có phần đuôi là .SEP, do vậy ta có thể tạo chúng bằng **Notepad**. Tuy nhiên để ghi được với phần đuôi .SEP, thì trong mục **Save as type** ta phải chọn là **All files**. Cấu trúc của trang phân cách như sau:

- Dòng đầu tiên chỉ gõ vào một ký tự duy nhất được gọi là *ký tự thoát* (escape character). Ký tự nào cũng có thể được dùng làm ký tự thoát, nhưng nên là những ký tự đặc biệt để không trùng với các ký tự diễn đạt nội dung (thông thường ta

nên dùng ký tự # hoặc \$). Ký tự thoát sẽ được dùng làm dấu hiệu để Windows server biết là sắp thực hiện một hàm sau đó, chứ không phải là nhập vào văn bản.

- Sau khi đã chọn một ký tự thoát, ta có thể biến đổi trang phân cách theo ý riêng bằng các ký tự tuỳ chọn được viết ngay sau ký tự thoát. Các ký tự tuỳ chọn này khi đứng ngay sau ký tự thoát sẽ trở thành các lời gọi hàm, do vậy ta có thể gọi chúng là các hàm. Có khá nhiều hàm tuỳ chọn, bảng 3.2 chỉ trình bày những hàm thông dụng nhất.

Bảng 5.2. Một số hàm thông dụng được dùng trong trang phân cách

Hàm	Chức năng
D	In ngày công việc in được in ra
L	In tất cả các ký tự sau
N	In tên đăng nhập của người có công việc in
n	n là một số nguyên từ 0 – 9, để nhảy bỏ n dòng. Nếu n=0 có nghĩa là chỉ chuyển xuống dòng kế tiếp.
T	In giờ công việc in được in ra

Chú ý: Các trang phân cách khi in ra sẽ không hiển thị được font tiếng Việt, mặc dù trong Notepad có thể soạn thảo được bằng font tiếng Việt. Do vậy ta chỉ nên soạn thảo văn bản không dấu trong trang phân cách.

Ví dụ: Với trang phân cách có nội dung như sau:

\$

\$L Day la trang phan cach

\$L Nguoi In: \$N

\$1

\$L Thoi gian In: \$T \$L ngay \$D

Giả sử người gửi in văn bản là administrator. Khi đó nội dung trang phân cách được in ra sẽ có dạng:

Day la trang phan cach

Nguoi in: administrator

Thoi gian: 10:19:55 AM ngay 28/12/2014

5.3.4.1.2. Sử dụng trang phân cách

Để sử dụng được trang phân cách ta phải gắn nó vào một máy in cụ thể, bằng cách nhấn nút phải chuột tại máy in cần gắn từ cửa sổ **Printers**, chọn **Properties** để mở cửa sổ đặc tính của máy in. Sau đó chọn trang **Advance**, rồi chọn **Separator Page**, để hiện ra cửa sổ như Hình 5.40. Tại đây ta có thể gõ vào tên và đường dẫn của tập tin lưu trang phân cách tại vị trí con trỏ, hoặc nhấn nút **Browse** để tìm trên đĩa. Cuối cùng nhấn **OK**.



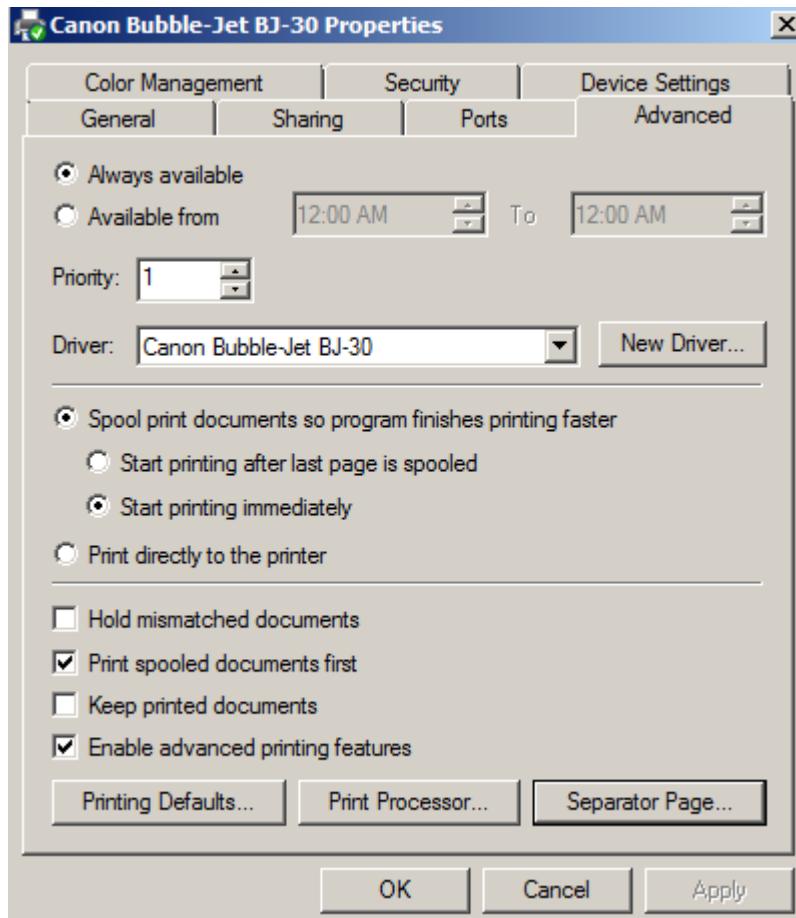
Hình 5.40: Cửa sổ chọn trang phân cách

5.3.4.2. Thiết lập chế độ bảo mật cho máy in

Theo mặc định, mỗi máy in đều cho phép mọi người dùng có thể in và in vào mọi thời điểm trong ngày. Nhưng với những máy in quý hiếm trên mạng, để tránh lãnh phí và cũng để thuận tiện trong việc quản lý, ta nên hạn chế số người và thời gian có thể in, bằng cách thiết lập những chế độ bảo mật do Windows server cung cấp.

5.3.4.2.1. Ấn định số giờ khả dụng của máy in

Để thực hiện công việc này ta mở cửa sổ đặc tính của máy in, rồi chọn trang **Advanced**. Sau đó nếu chọn mục **Always available**, thì sẽ in được mọi giờ trong ngày. Còn mục bên dưới cho ta chọn phạm vi giờ có thể dùng được, như trên Hình 5.41, ta chọn từ 9 giờ sáng đến 5 giờ chiều.



Hình 5.41: Qui định những giờ dùng được máy in

5.3.4.2.2. Ẩn định các quyền truy cập máy in

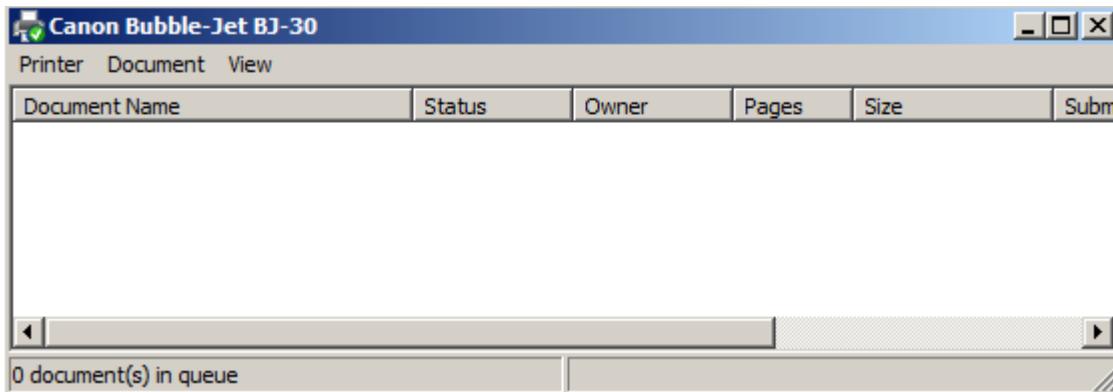
Cách trao quyền truy cập máy in cũng tương tự như trao quyền truy cập file và thư mục. Có ba quyền truy cập cơ bản về máy in là:

Print: Người dùng có quyền này sẽ được phép gửi các công việc in đến máy in để in.

Manage Printers: Quyền này cho phép thay đổi các đặc tính và đặt lại quyền truy cập máy in.

Manage Documents: Người dùng có thể kiểm soát các thiết định đặc trưng cho các công việc in, tạm dừng, tiếp tục, khởi động lại, hoặc xoá đi các công việc in đã được gửi đến máy in và đang chờ trong *hàng đợi in* (mỗi máy in logic đều có một *hàng đợi in* (print queue) để nhận các công việc in được gửi về máy in, và nằm chờ ở đây cho đến khi chúng được in ra).

Để xem các công việc in đang chờ trong hàng đợi của máy in nào, ta nhấp đúp chuột tại máy in đó trong cửa sổ **Printers**. Như Hình 5.42, hàng đợi của máy in **Canon BLP 3260** đang có 1 công việc in.



Hình 5.42: Nội dung hàng đợi của máy in HP LaserJet 5L

Nếu muốn tạm dừng một công việc in nào, ta chọn nó rồi chọn **Document/Pause**.

Nếu muốn bỏ trạng thái tạm dừng để tiếp tục một công việc in nào đó, ta chọn nó rồi chọn **Document/Resume**.

Nếu muốn khởi động lại một công việc in nào đó (bắt đầu in lại từ trang đầu nếu nó đang in dở), ta chọn nó rồi chọn **Document/Restart**.

Nếu muốn xoá bỏ công việc in nào ra khỏi hàng đợi in, ta chọn nó, rồi chọn **Document/Cancel**.

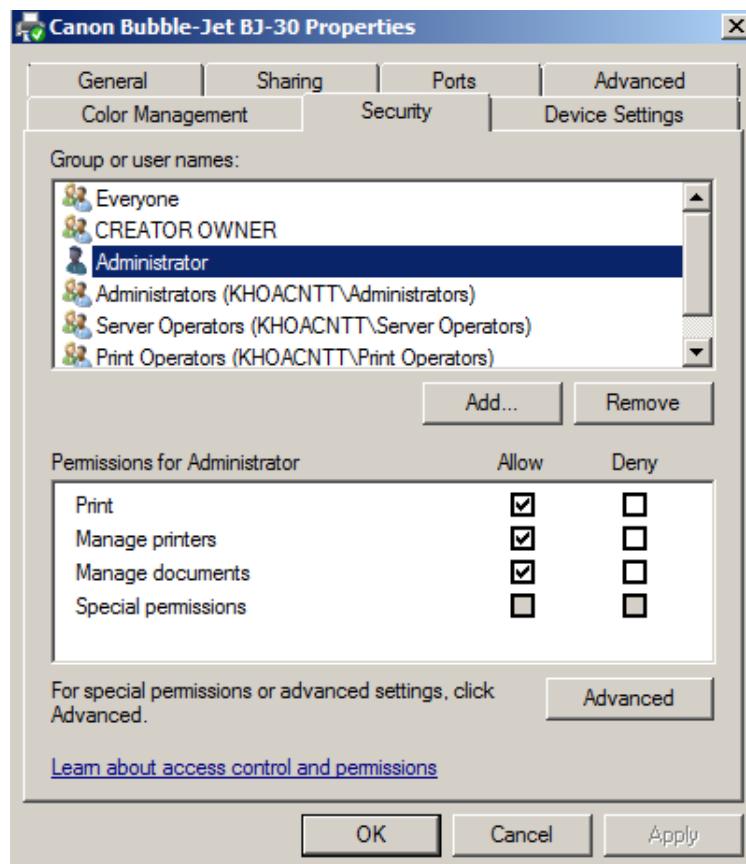
Để ấn định các quyền truy cập máy in, ta chọn trang **Security** trong cửa sổ đặc tính của máy in. Như được minh họa trong Hình 5.43, ta thấy ban đầu nhóm **Everyone** có quyền **Print**, vì quyền này được duyệt tại ô **Allow**. Như vậy mọi người đều có thể in được ra máy in này. Để ngăn cấm không tương minh một quyền nào đó, thì ta không duyệt ở cả hai ô **Allow** và **Deny**, còn muốn ngăn cấm tương minh một quyền nào đó thì ta duyệt vào ô **Deny**.

Để thay đổi các quyền truy cập máy in của đối tượng nào, thì ta chọn đối tượng đó trong phần **Name**, rồi duyệt hoặc bỏ duyệt tại những ô thích hợp trong phần **Permissions**.

Để thêm các đối tượng mới vào khung **Name**, ta nhấn nút **Add**, rồi chọn các đối tượng cần thêm.

Để loại bỏ đối tượng nào đó ra khỏi khung **Name**, ta chọn nó rồi nhấn nút **Remove**.

Khi một người dùng là thành viên của nhiều nhóm, thì quyền truy cập máy in của họ sẽ là tổng hợp tất cả các quyền truy cập trong các nhóm chứa người dùng này, cùng với quyền truy cập riêng của người đó, trừ ra những quyền bị cấm tường minh. Ví dụ: đối với máy in P, nhóm N1 bị cấm tường minh quyền Print, trong khi nhóm N2 có quyền này, A là người sử dụng nằm trong cả hai nhóm N1 và N2. Khi đó người dùng A không thể in trên máy in P, vì tổng hợp lại thì A không có quyền Print đối với máy in P. Tuy nhiên nếu nhóm N1 bị ngăn cấm không tường minh quyền Print, thì A sẽ có quyền Print đối với máy in P, nên có thể in ra trên máy in này.



Hình 5.43: Cửa sổ thay đổi quyền truy cập máy in

5.4. SAO LƯU VÀ PHỤC HỒI

5.4.1. Khái niệm sao lưu và phục hồi dữ liệu

Nhiệm vụ sao lưu đơn giản là sao chép dữ liệu một cách đều đặn để nếu như thiết bị lưu trữ bị hư hỏng hoặc phá hủy và dữ liệu trên đó bị mất, 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 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, thõ vẫn cần phải có một giải pháp sao lưu cho mõnh.

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 vỡ cù 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 có thể sử dụng mạng để truy cập đến các máy chủ cần sao lưu, điều này cho phép sử dụng một thiết bị sao lưu để bảo vệ rất nhiều máy tính.

Giải pháp 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 sử dụng để lưu các dữ liệu sao lưu. Quyết định chọn lựa tùy thuộc vào phần cứng và phần mềm sao lưu đồng thời các chính sách quản trị mà người quản trị sử dụng, tùy thuộc vào dung lượng dữ liệu cần sao lưu, thời gian sao lưu và mức bảo vệ cần áp dụng.

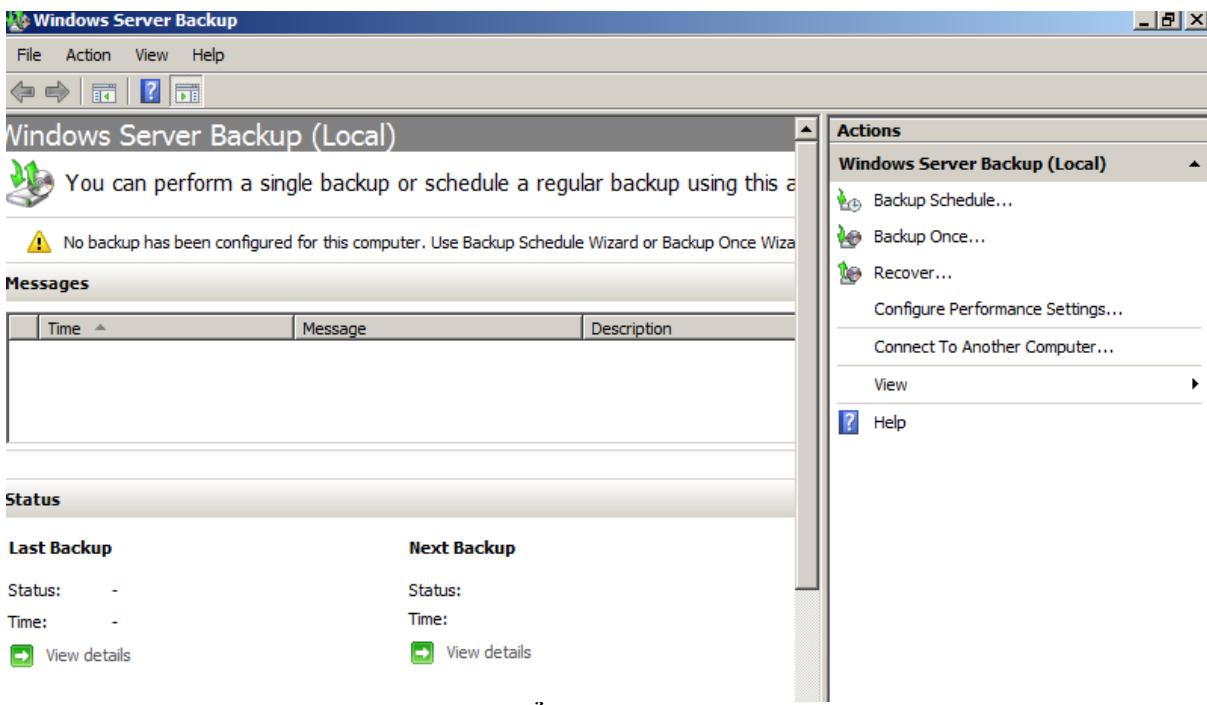
Một giải pháp sao lưu mạng bao gồm hai thành phần sau đây:

- Phần cứng sao lưu: yêu cầu về tốc độ, dung lượng và chi phí
- 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 người dùng cần. Ở đây chỉ đề cập tới giải pháp sử dụng phần mềm sao lưu được hỗ trợ trong Windows Server là Windows Server Backup

5.4.2. Sử dụng Windows Server Backup

Công cụ sao lưu trong windows server thường được quy vào bằng cái tên của nó có thể thực hiện được Windows Server Backup , vào Start/Administrative tool/Windows Server Backup, giao diện backup dữ liệu như Hình 5.44:

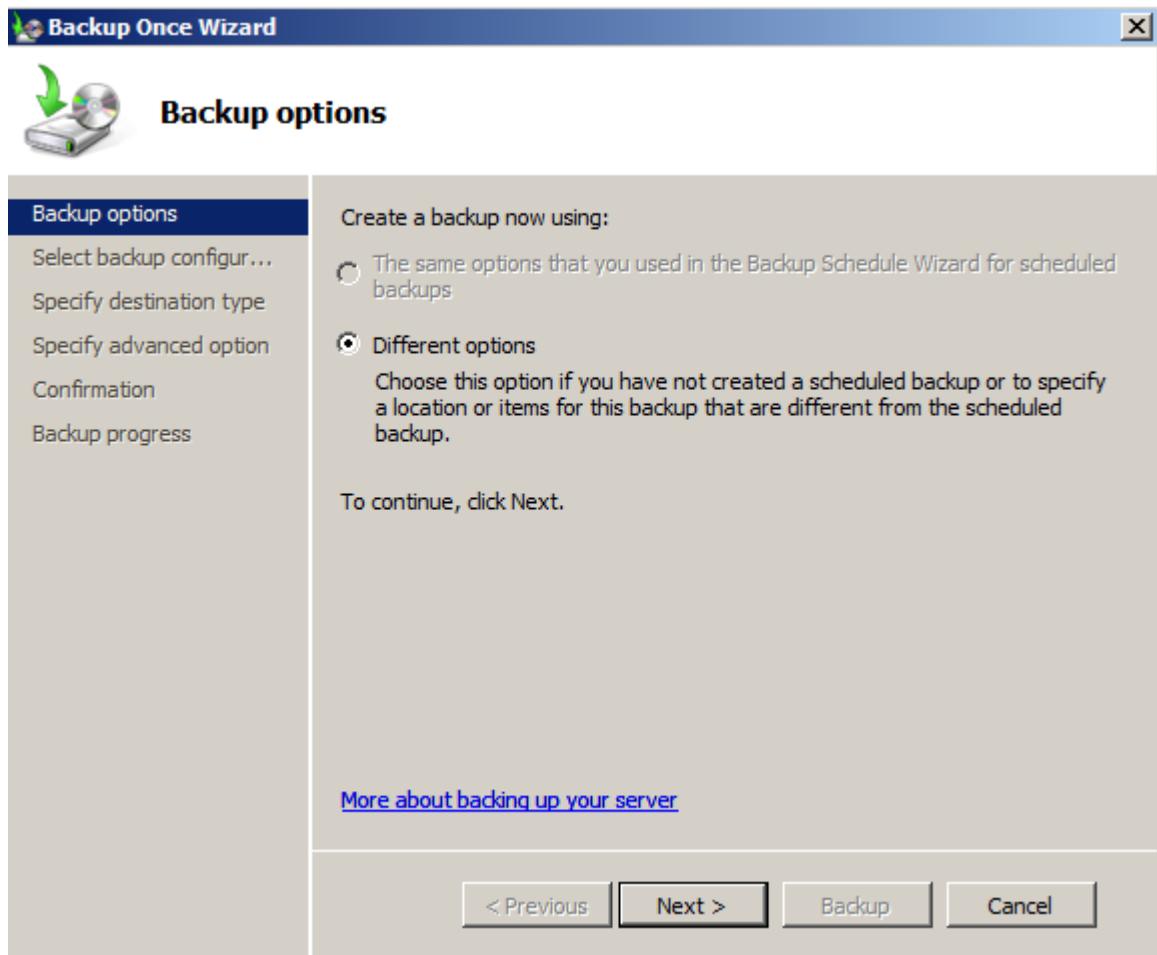


Hình 5.44: Cửa sổ Windows Server Backup

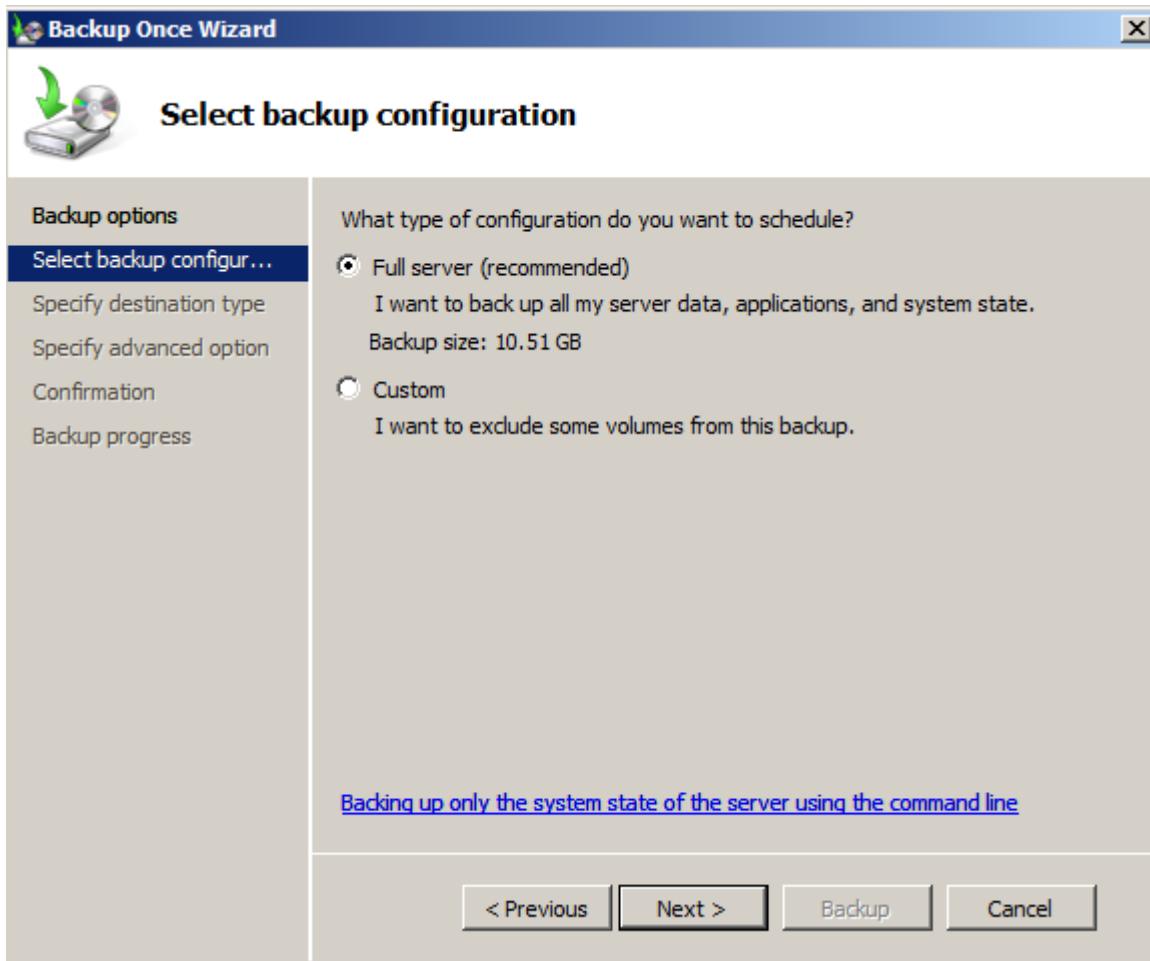
Trong đó **Backup Schedule** là quá trình thiết lập hệ thống tự động tiến hành sao lưu dữ liệu theo yêu cầu của người dùng. **Backup Once** là quá trình backup những dữ liệu mà người dùng khi cần thiết mới tiến hành sao lưu

5.4.2.1. Backup Once

Quá trình này cho phép tiến hành sao lưu dữ liệu toàn bộ máy tính hoặc một phần dữ liệu trên máy tính. Từ giao diện như trong hình 5.30 chọn Backup Once, thấy xuất hiện giao diện như trong Hình 5.45 chọn Next để thực hiện việc cấu hình sao lưu dữ liệu như Hình 5.46



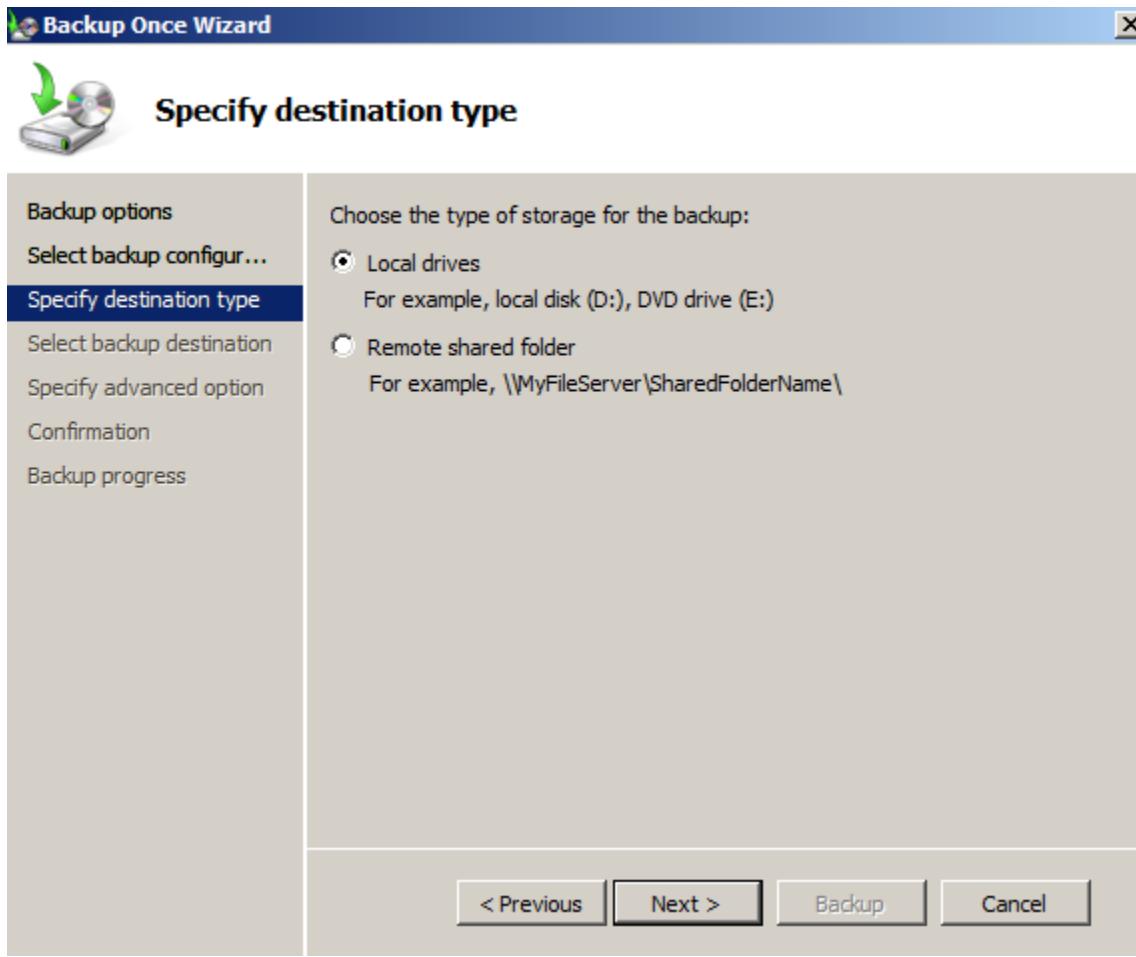
Hình 5.45: Giao diện lựa chọn chế độ sao lưu



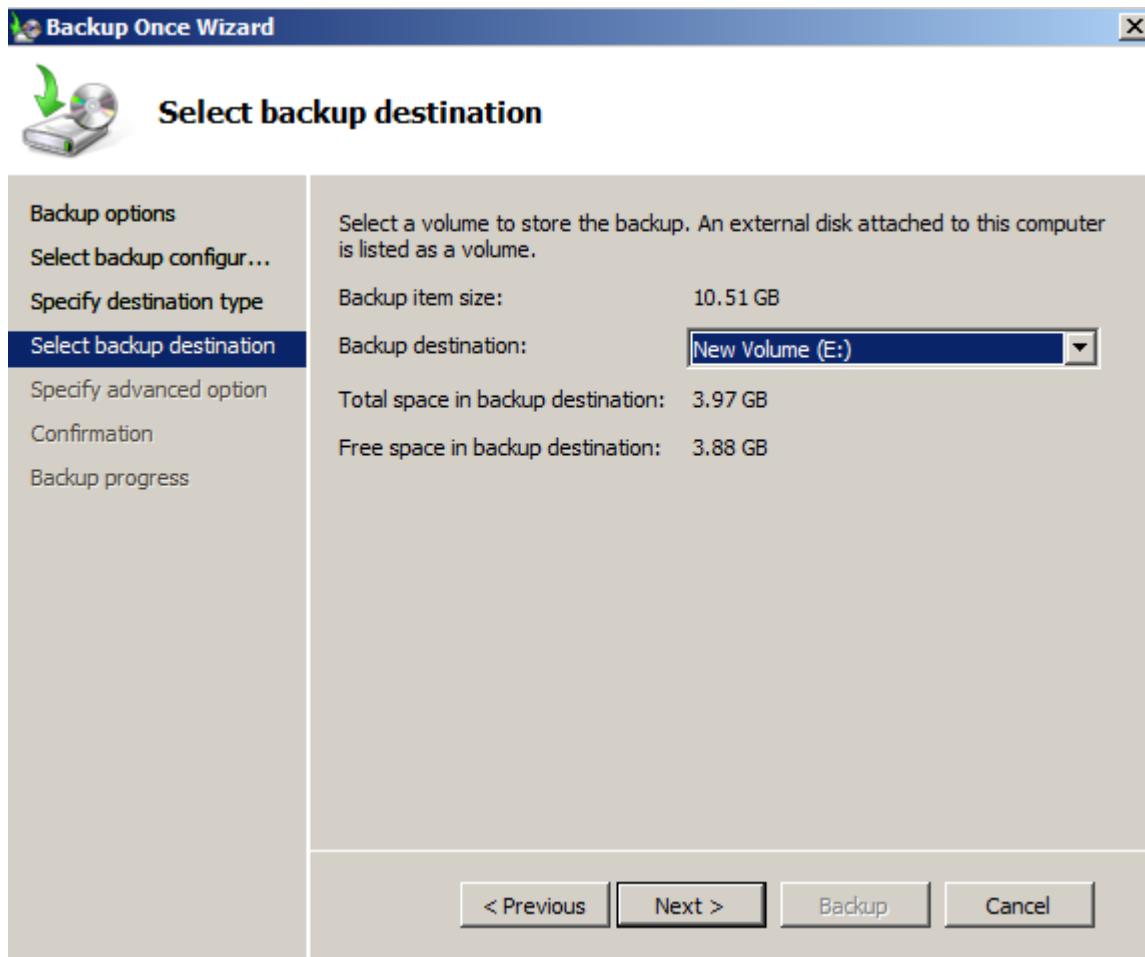
Hình 5.46: giao diện chọn cách thức sao lưu

1. Full Server là chế độ sao lưu toàn bộ hệ thống
2. Custom là chế độ chọn lựa sao lưu những dữ liệu mà người dùng cần

Chọn nơi lưu trữ file sao lưu trên ổ đĩa hay trên thư mục được chia sẻ trên mạng như giao diện Hình 5.47

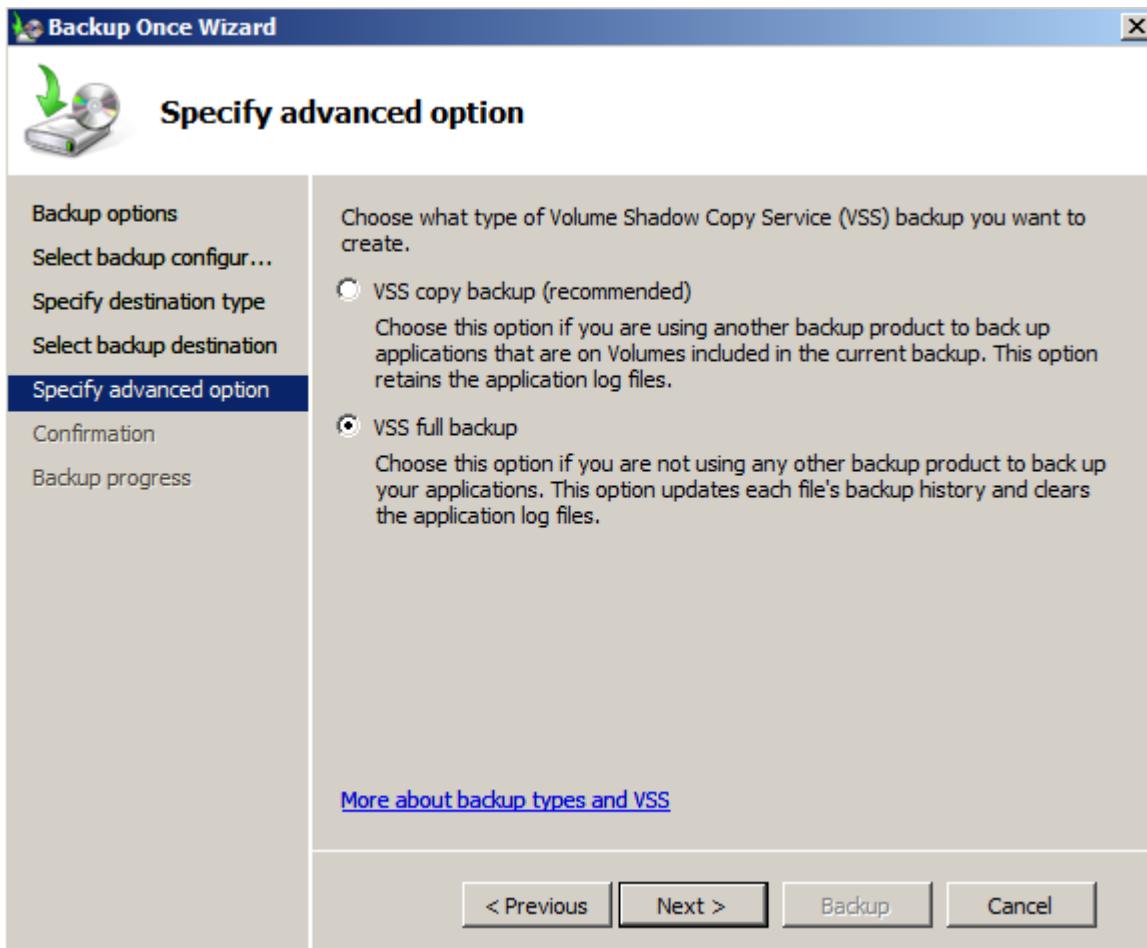


Hình 5.47: Giao diện lựa chọn nguồn lưu trữ



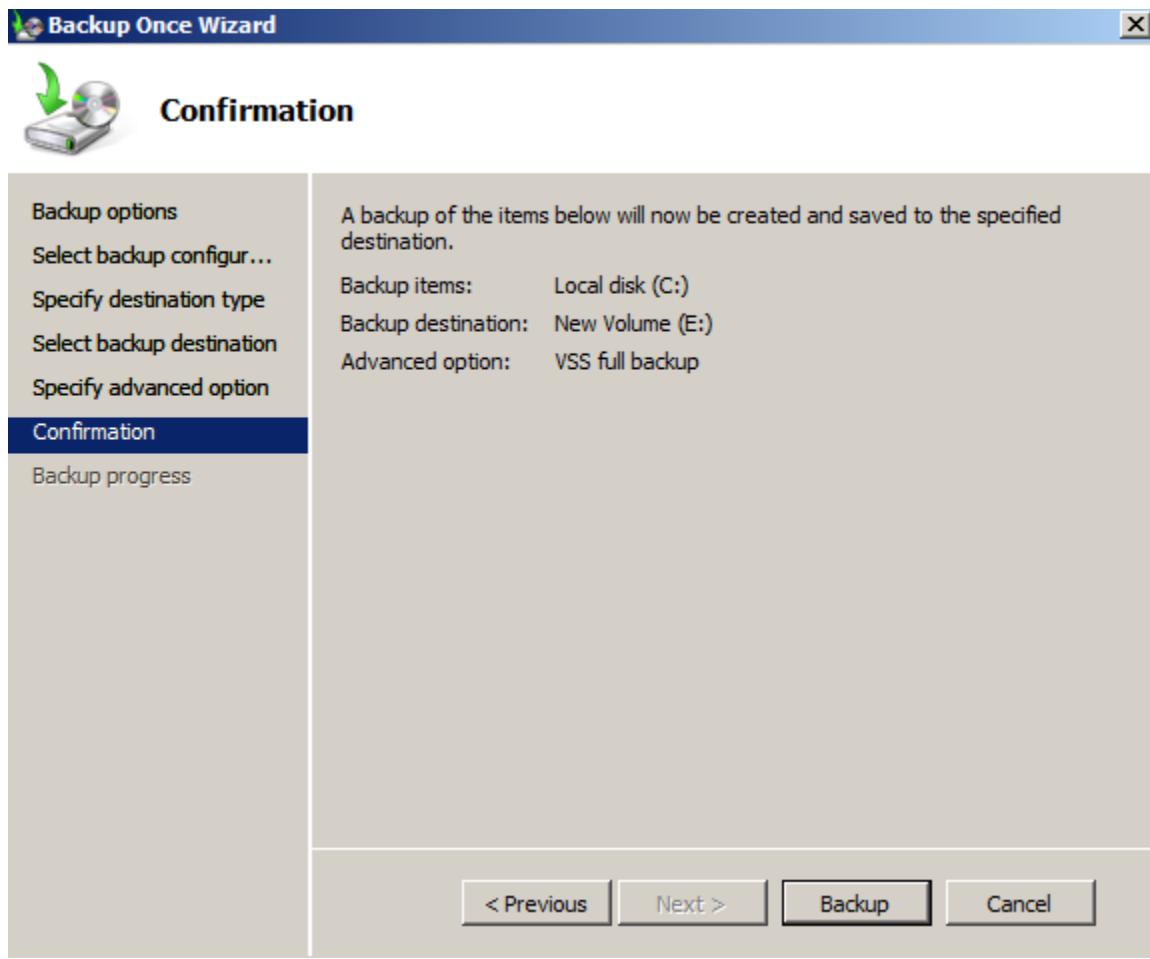
Hình 5.48: Cửa sổ thông tin nguồn lưu trữ

Chọn chế độ sao lưu cho tiến trình như giao diện Hình 5.49



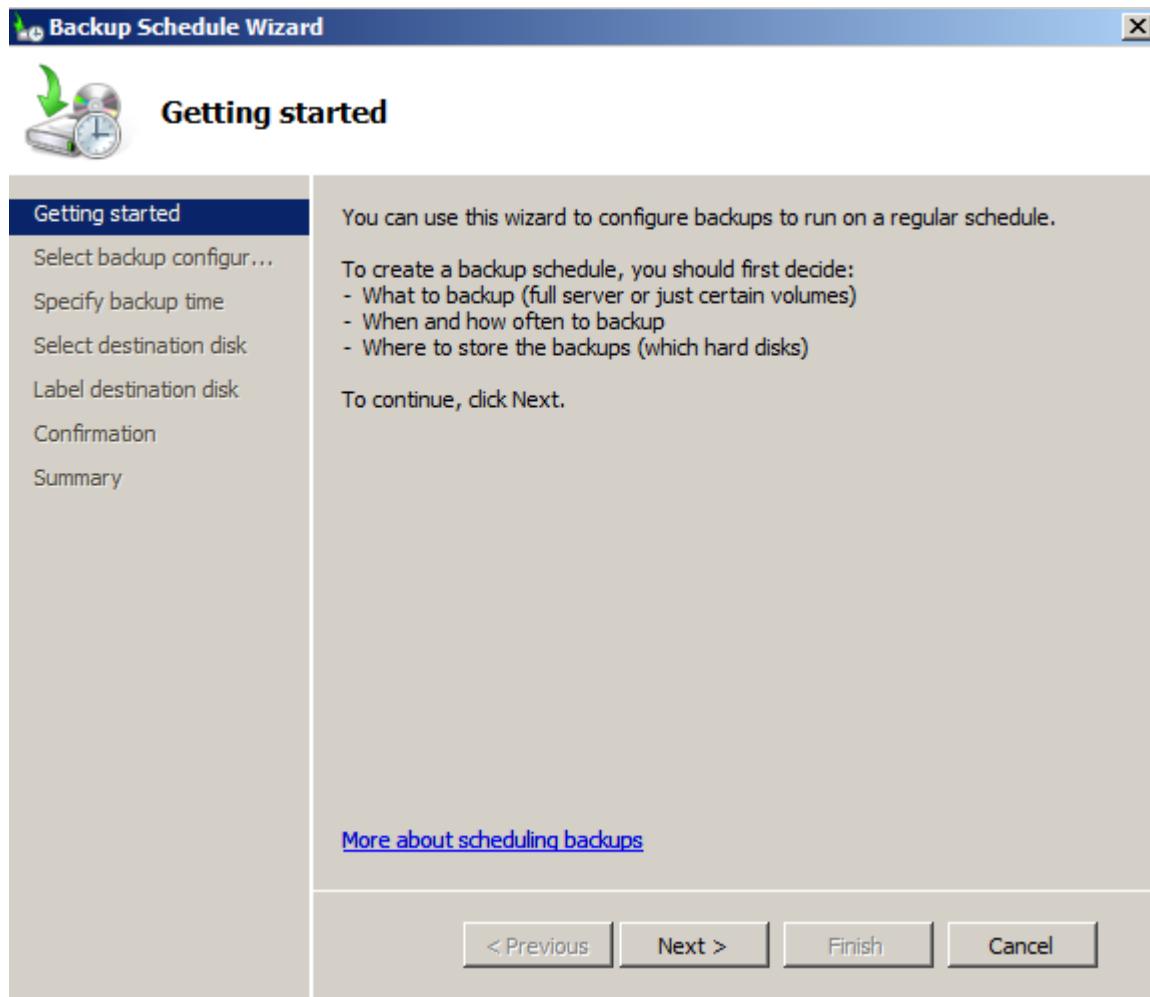
Hình 5.49: Cửa sổ chọn chế độ sao lưu

Sau khi cấu hình xong hệ thống sẽ hiện thị thông tin cấu hình, người dùng kiểm tra lại thông tin và kích vào Backup để bắt đầu quá trình sao lưu



5.4.2.2. Schedule Backup

Quá trình này cho phép tiến hành sao lưu dữ liệu toàn bộ máy tính hoặc một phần dữ liệu trên máy tính. Từ giao diện như trong Hình 5.44 chọn Schedule Backup, thấy xuất hiện giao diện như trong Hình 5.50 chọn Next để thực hiện việc cấu hình sao lưu dữ liệu như Hình 5.51



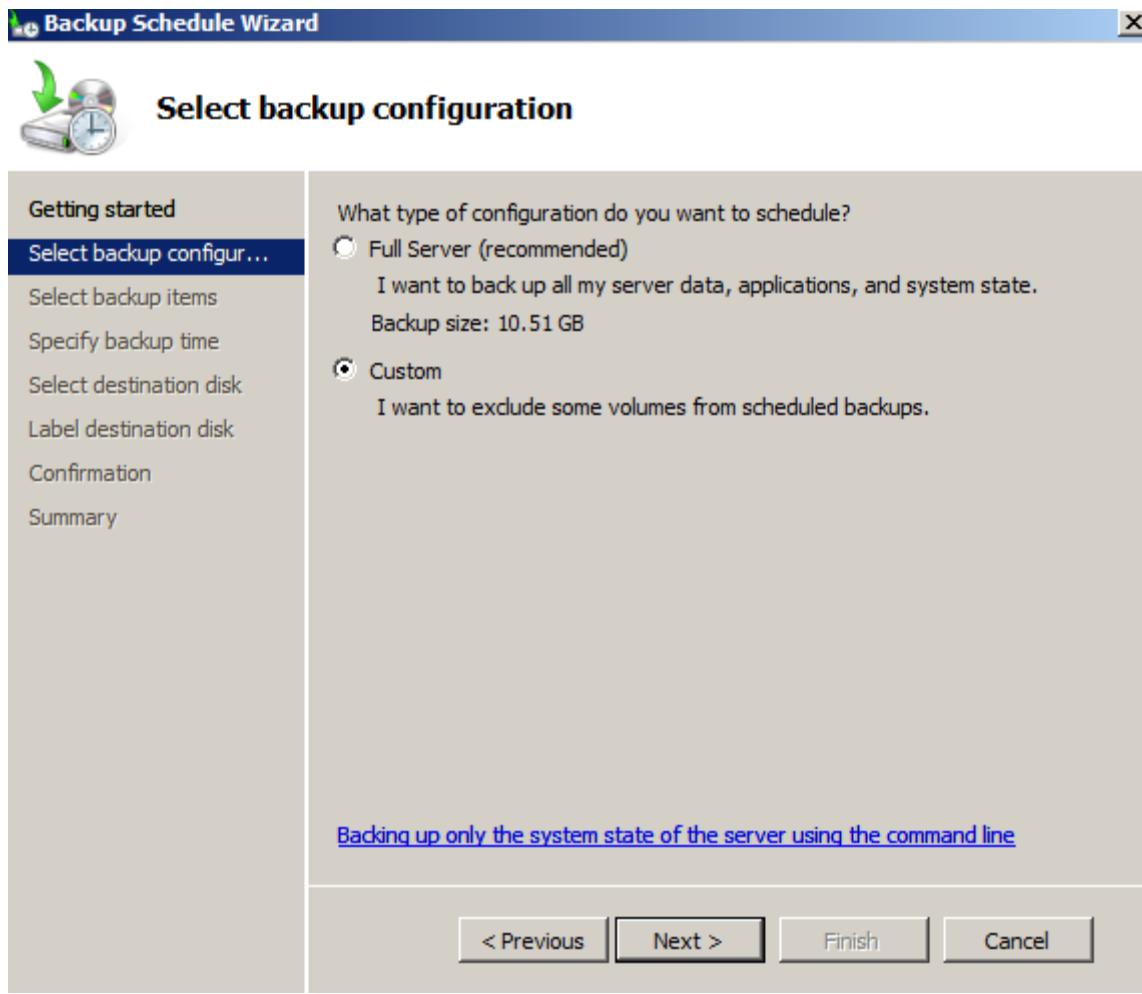
Hình 5.50: **Màn hình** Getting Started

- Màn hình **Select backup configuration**, có 2 tùy chọn:

+ **Full Server**: Backup toàn bộ các ổ đĩa à file backup này sẽ rất lớn

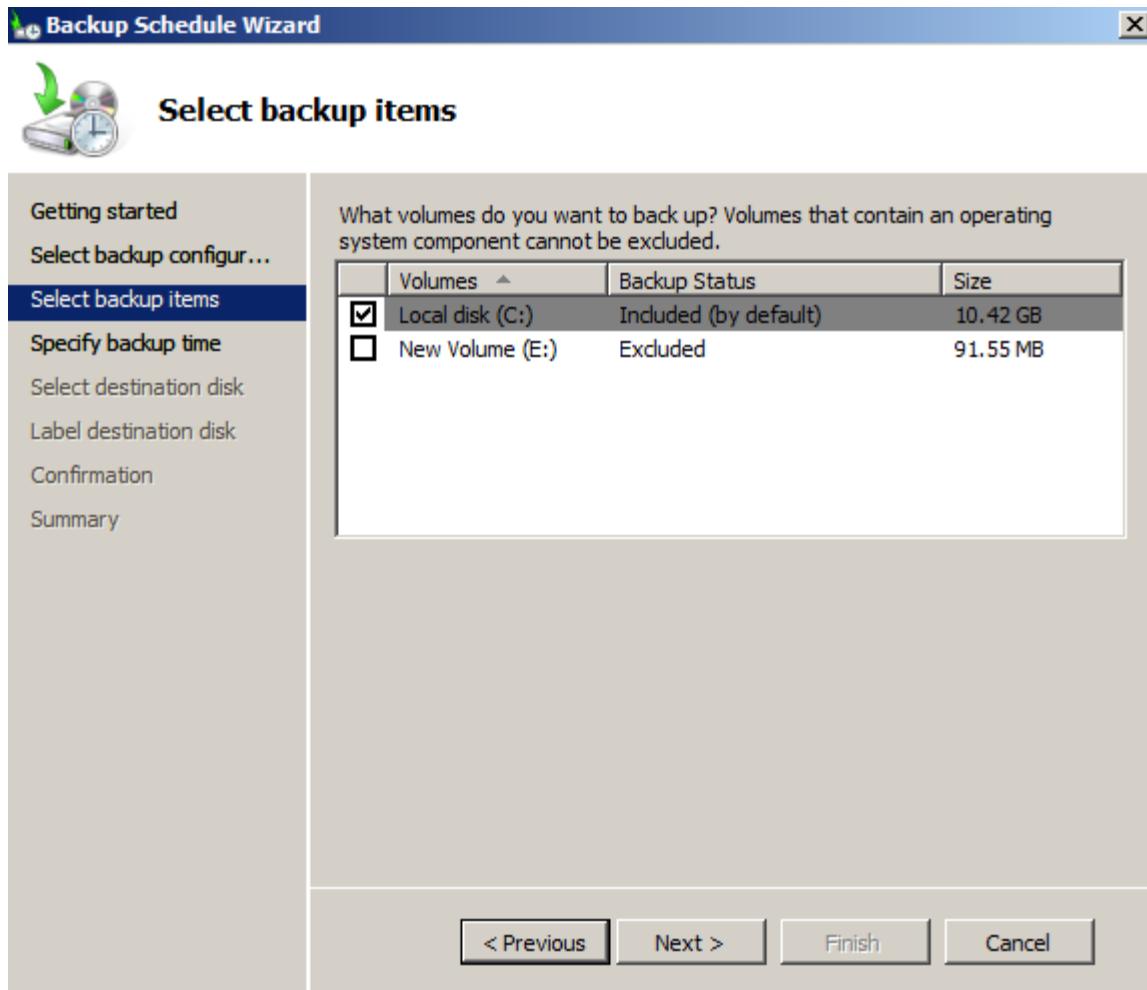
+ **Custom**: bạn có thể chọn các ổ đĩa mà bạn muốn Backup

Ở đây vì các user lưu dữ liệu vào 2 ổ C: và D: nên Tèo không cần phải Backup toàn bộ mà chọn Custom, sau đó nhấn **Next**



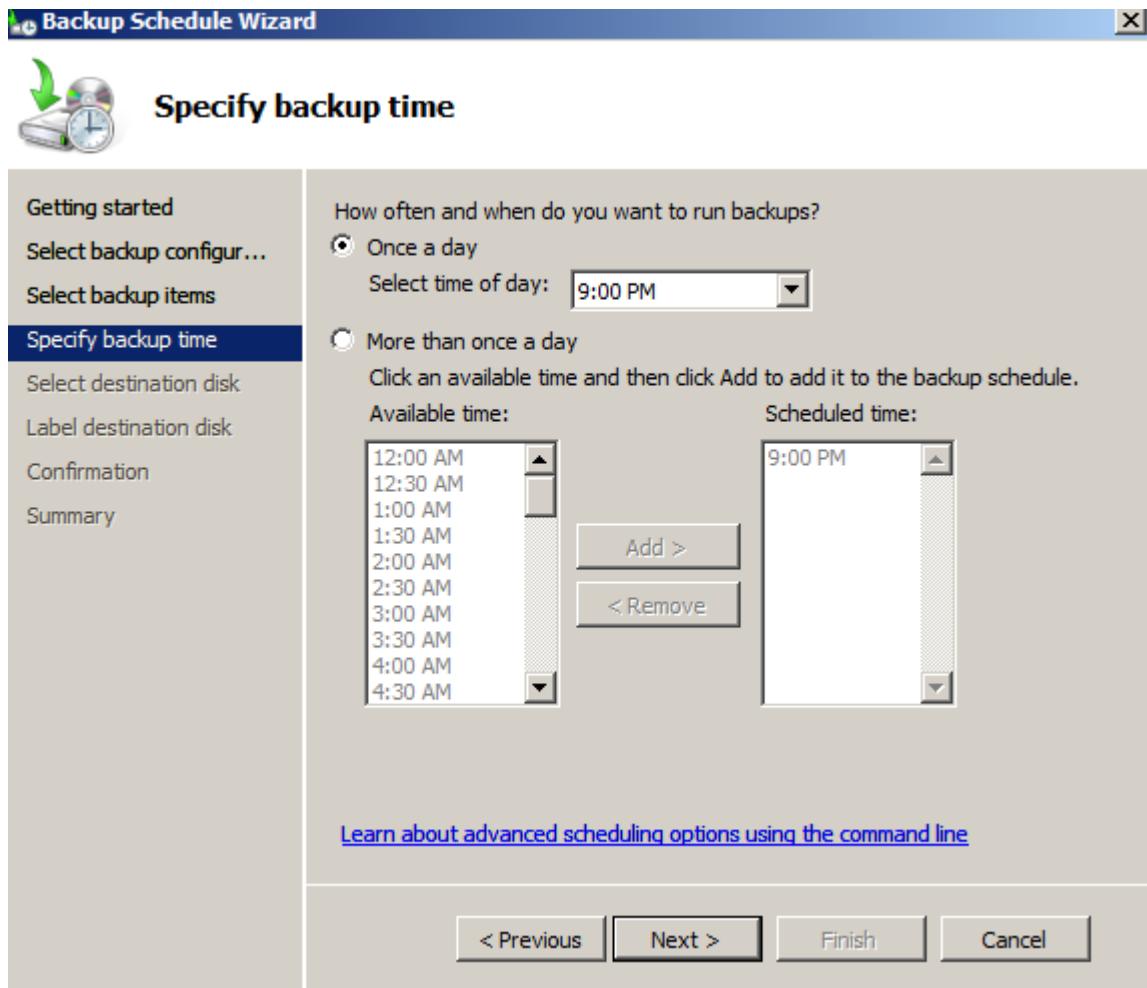
Hình 5.51: màn hình Select Backup Items

- Màn hình **Select Backup Items**, đánh dấu chọn **Custom**, sau đó nhấn **Next**



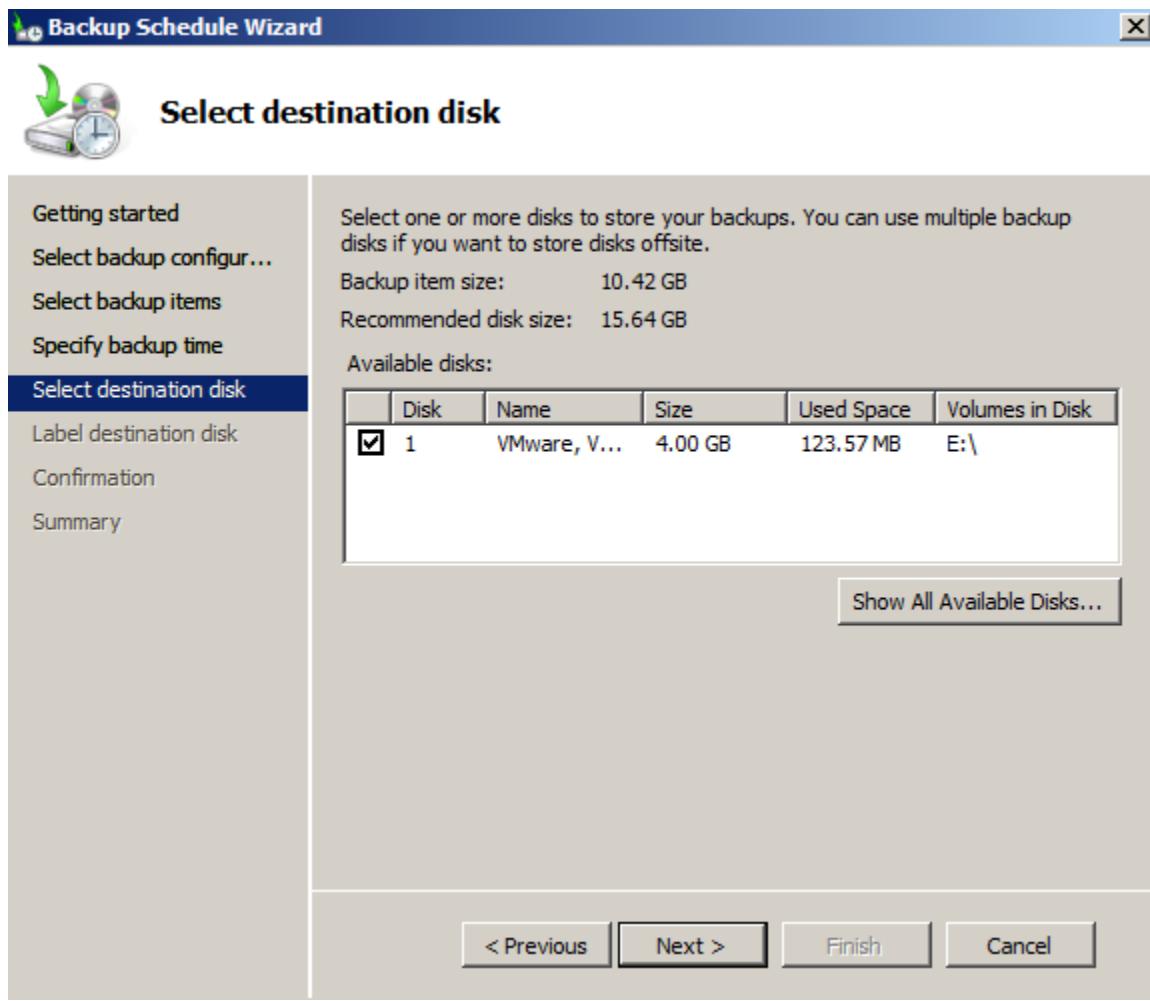
Hình 5.52: Màn hình chọn nguồn Backup

- Màn hình **Specify backup time**, ta có thể chọn nhiều giờ để Backup hoặc chỉ chọn 1 giờ để Backup. Chọn **Once a day** vào lúc 12:00 PM. Sau đó nhấn **Next**



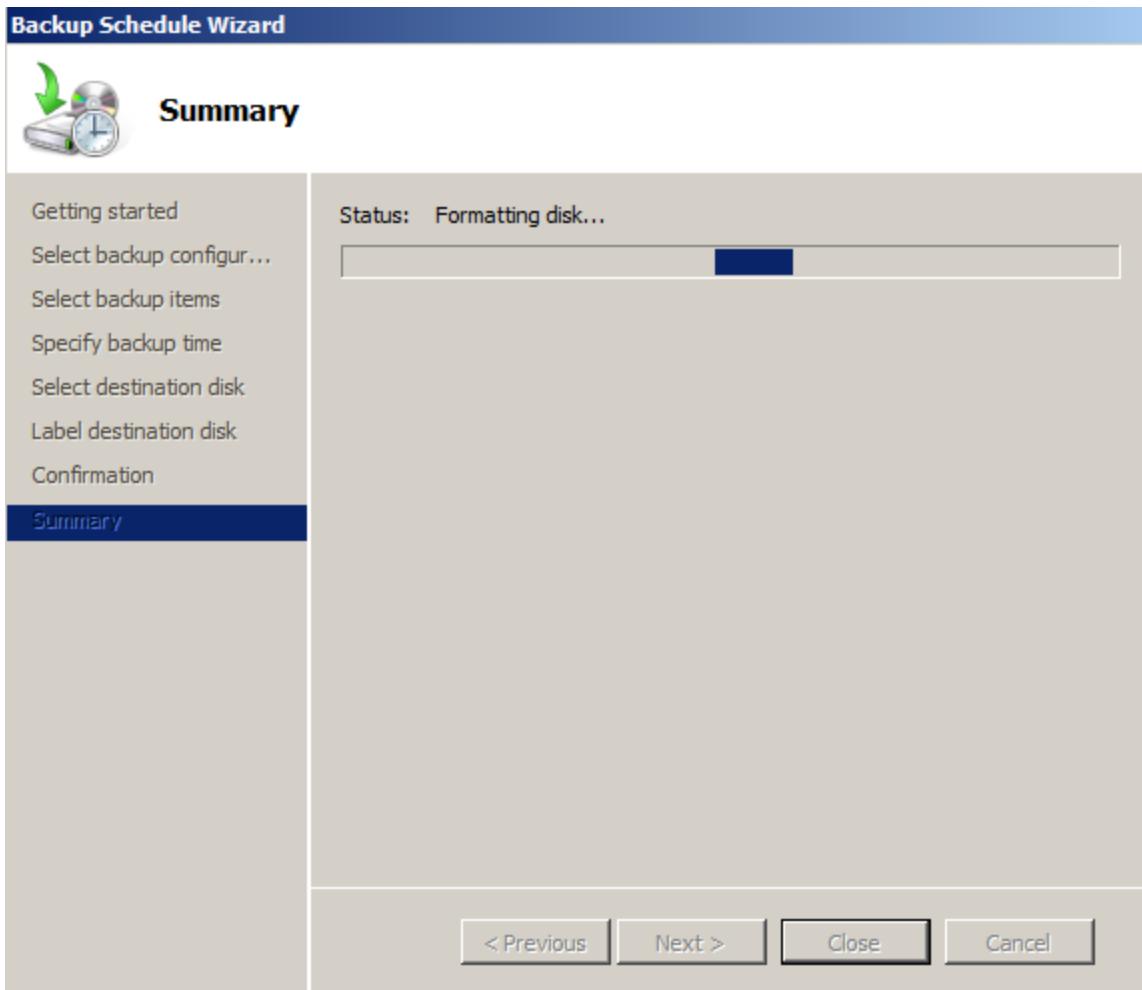
Hình 5.53: Màn hình setup lập lịch Backup

- Màn hình **Select destination disk**, nhấn **Show All Available Disk...**, chọn ổ đĩa E:, toàn bộ file Backup sẽ được lưu vào ổ E:



Hình 5.54: Chọn nơi lưu trữ file backup

- Quá trình cài đặt còn lại diễn ra như mặc định. Cuối cùng màn hình **Summary**, nhấn **Close**

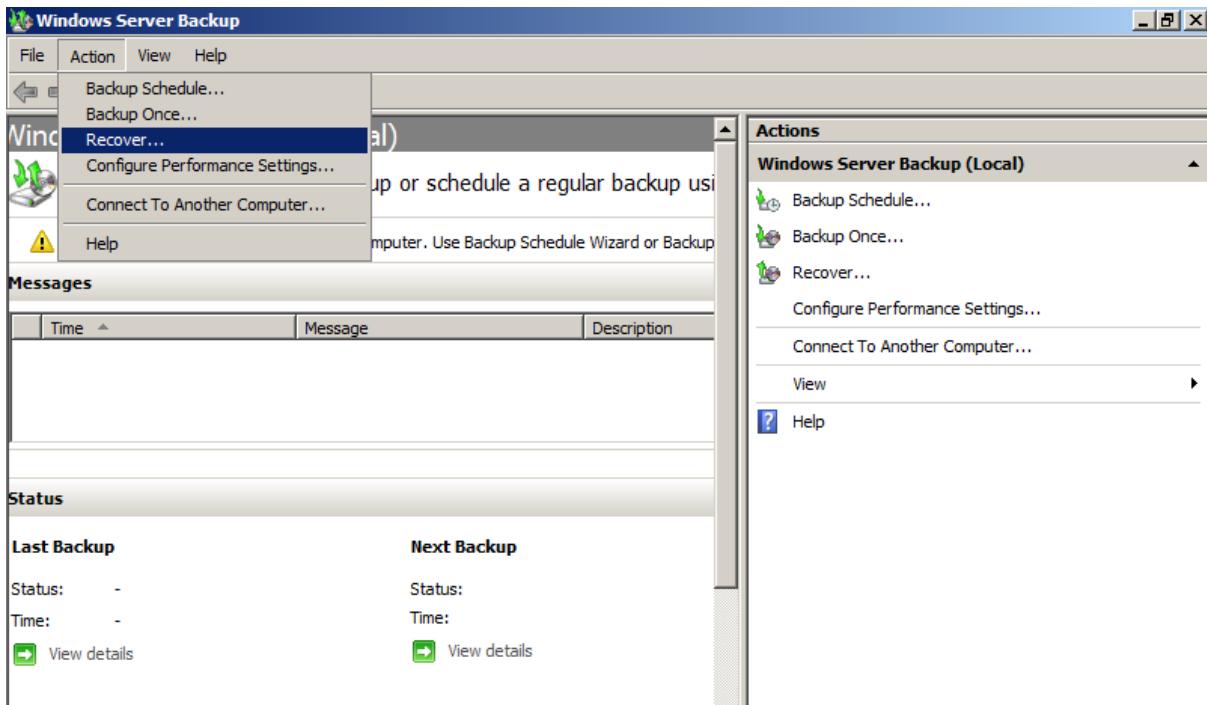


Hình 5.55: Lưu lại cấu hình cho tiến trình lập lịch

Như vậy cứ 9:00 AM mỗi ngày thì chương trình Backup sẽ tự động làm việc. Sau đó để cho chắc chắn, ta vào menu Action, chọn Backup Once (Backup ngay lập tức), Backup lại trước 1 bản để dự phòng. Bản Backup được thực hiện **vào lúc 11:24 AM ngày 30/12/2014**

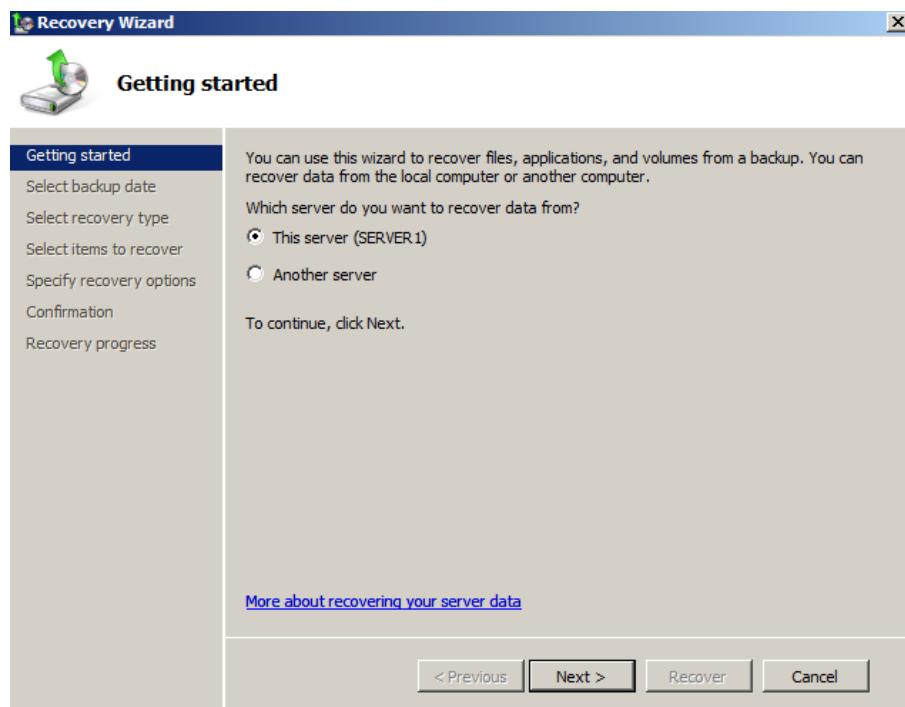
5.4.3. Phục hồi dữ liệu

- Mở chương trình **Windows Server Backup**, vào menu **Action**, chọn **Recover**



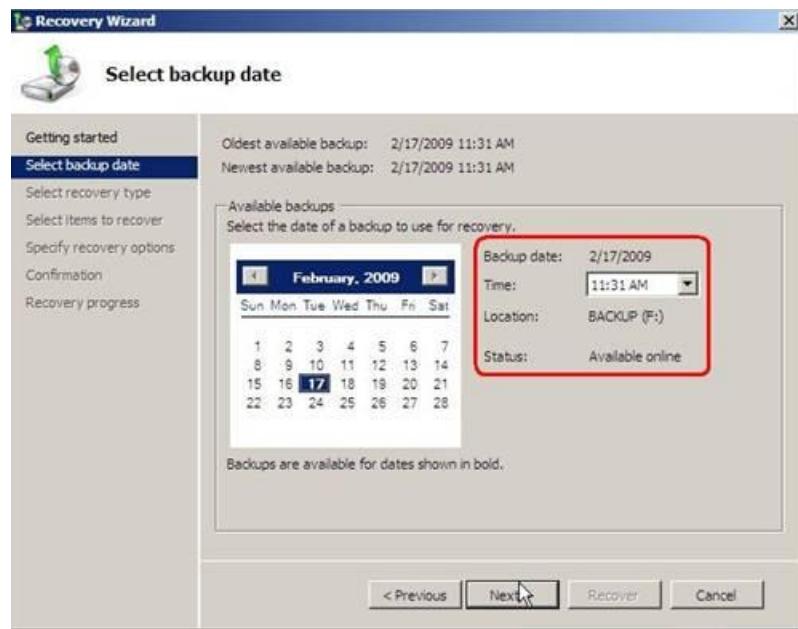
Hình 5.56: Khởi động quá trình khôi phục dữ liệu

- Màn hình **Getting Started**, chọn **This Server**, nhấn **Next**



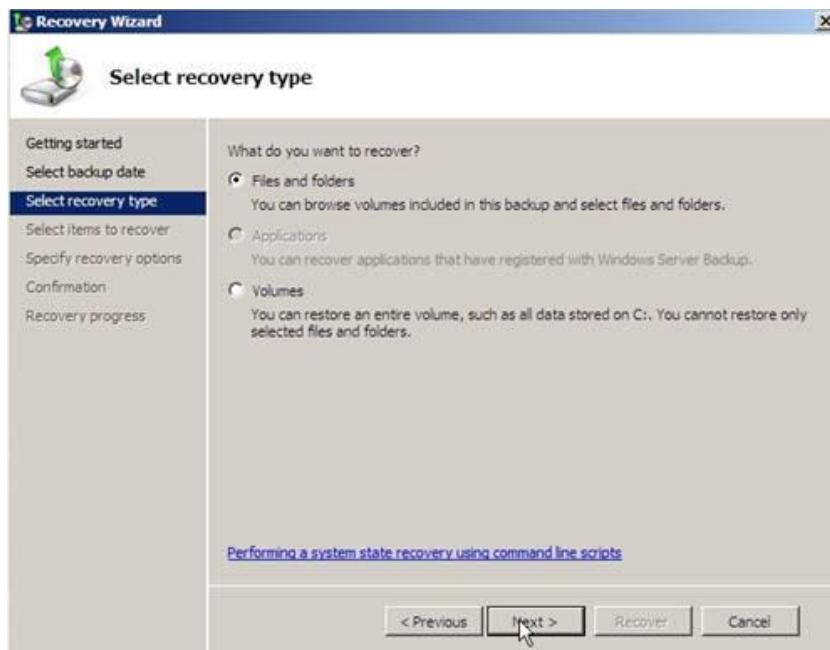
Hình 5.57: Chọn chế độ khôi phục trên máy tính cục bộ hay khôi phục qua mạng

- Màn hình **Select backup date**, Ta chọn ngày mình thực hiện Backup, tự động sẽ show ra thời gian mà ta đã Backup, rất tiện lợi, sau đó nhấn **Next**



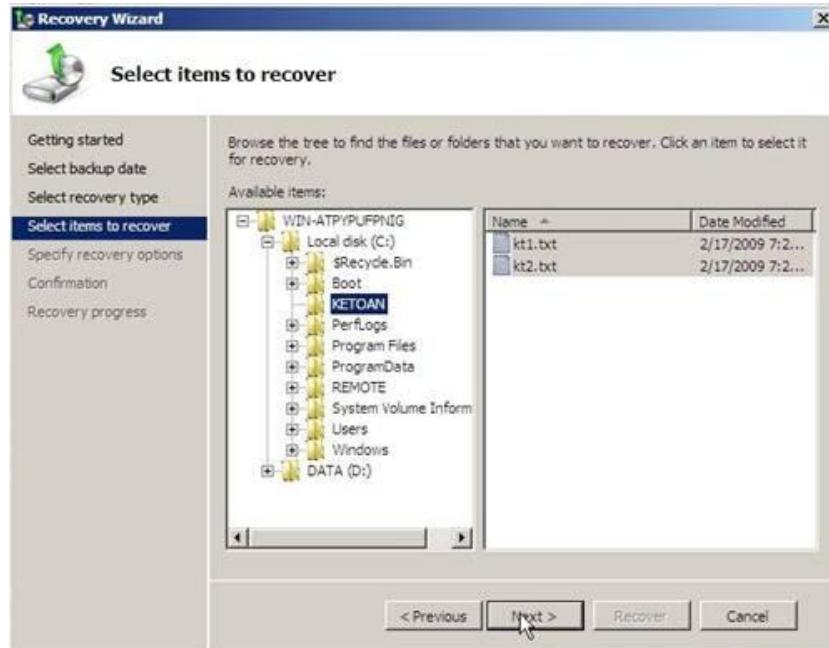
Hình 5.58: Chọn thời gian tiến hành backup

- Màn hình **Select recovery type**, chọn **File and Folder**, nhấn **Next**



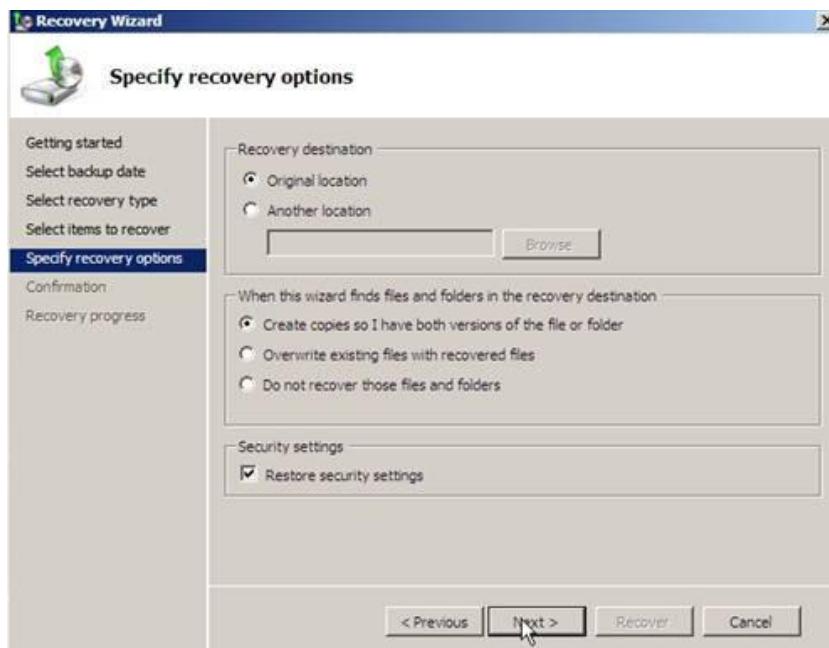
Hình 5.59: Chọn kiểu khôi phục dữ liệu

- Muốn restore thư mục **KETOAN** nên chọn thư mục **KETOAN**, sau đó nhấn **Next**



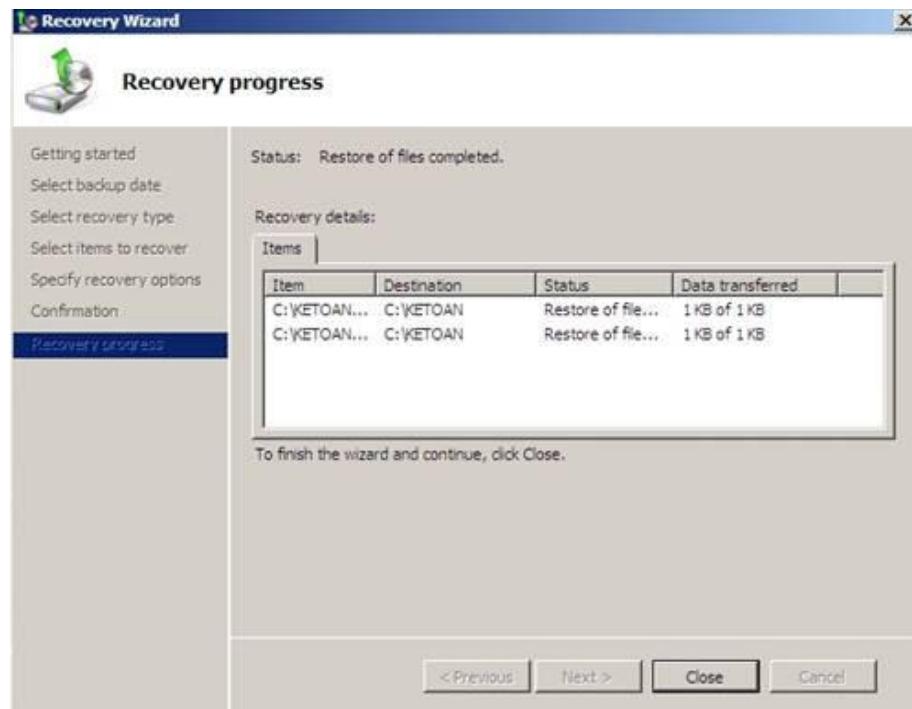
Hình 5.60: Chọn dữ liệu cần khôi phục

- Màn hình **Specify recovery options**, giữ nguyên như mặc định, nhấn **Next**

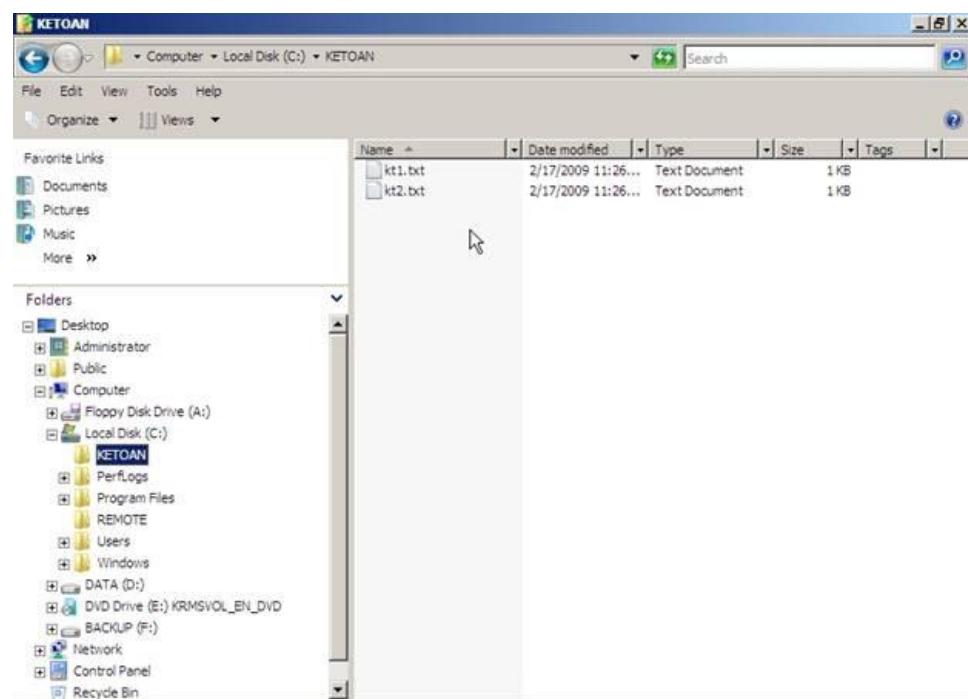


Hình 5.61: Chọn lựa khôi phục dữ liệu tối đâu

- Chờ chừng vài phút là khôi phục thành công. Sau khi khôi phục xong, nhấn **Close**



- Kiểm tra, đã thấy thư mục **KETOAN** được khôi phục trên SERVER



5.5. TỔNG KẾT CHƯƠNG

Nội dung chương này đã trình bày chi tiết các nghiệp vụ quản lý tài nguyên trong hệ thống mạng. Hoạt động quản lý tài nguyên trong hệ thống mạng bao gồm: quản lý hệ thống file và thư mục, quản lý ổ đĩa, dịch vụ in trên mạng và sao lưu, phục hồi.

Trong quản lý hệ thống file và thư mục cần nắm rõ các định dạng file như FAT, NTFS, v.v. vì mỗi định dạng file sẽ hỗ trợ các chế độ bảo mật khác nhau. FAT chỉ hỗ trợ quyền truy cập mà không hỗ trợ quyền cục bộ còn NTFS hỗ trợ cả quyền cục bộ và quyền truy cập từ xa. Nội dung phần này tập trung trình bày vấn đề chia sẻ, trao quyền truy cập từ xa và trao quyền truy cập cục bộ, chiếm quyền sở hữu và cách tổng hợp quyền truy cập.

Vấn đề quản lý ổ đĩa gồm các hoạt động chính là cấu hình đĩa lưu trữ, sử dụng tiện ích quản lý ổ đĩa, nén dữ liệu trên ổ đĩa và thiết lập hạn ngạch ổ đĩa. Ổ đĩa lưu trữ có thể được cấu hình tĩnh/ động. Tiện ích quản lý ổ đĩa cho phép thống kê thông tin ổ đĩa, sửa/ loại bỏ các phân vùng hoặc thêm phân vùng mới. Hạn ngạch đĩa được dùng để chỉ định lượng không gian đĩa tối đa mà một người dùng có thể sử dụng trên một volume NTFS. Có thể áp dụng hạn ngạch đĩa cho tất cả người dùng hoặc chỉ đối với từng người dùng riêng biệt.

Dịch vụ in trên mạng được triển khai và quản trị theo các bước: cài đặt và chia sẻ máy in cục bộ, kết nối với máy in cục bộ đã chia sẻ, cấu hình máy in mạng. Dữ liệu in không được đưa trực tiếp ra máy in vật lý mà được đưa từ ứng dụng ra máy in lô-gic. Máy in lô-gic được quản lý bởi hệ điều hành. Nhiều máy in lô-gic có thể ánh xạ đến một máy in vật lý. *Máy in vật lý* là thiết bị in được gắn với một máy tính để in các công việc in do các máy in logic gửi đến. Mỗi máy in lô-gic trong máy tính gọi là máy in cục bộ. Máy in cục bộ này được chia sẻ và cấu hình để sử dụng trong hệ thống mạng.

Sao lưu và phục hồi là một hoạt động thiết yếu trong hệ thống mạng. Hoạt động này đảm bảo tính an toàn của hệ thống cũng như hỗ trợ giải quyết nhanh

các sự cố. Có thể sử dụng tiện ích **Windows Server Backup** để sao lưu và phục hồi dữ liệu.

CÂU HỎI VÀ BÀI TẬP THỰC HÀNH

Câu 1. Trình bày nội dung 05 kiểu sao lưu: copy, daily, normal, differential và incremental.

Câu 2. Những user nào có khả năng sao lưu và phục hồi dữ liệu?

Câu 3. Giải thích ý nghĩa 03 permission trên một printer: print, manage printer và manage document.

Câu 4. Trình bày cách cấu hình để print job của một user luôn luôn được thực hiện trước print job của các user khác.

Câu 5. Trình bày cách cấu hình cân tải (chia đều print job) tự động trên 05 print device HP Laser 2000.

Câu 6. Trình bày cách áp đặt giá trị disk quota giống nhau lên mọi volume trên một server.

Câu 7. Trình bày cách cấu hình một hardware profile.

Câu 8. Khi truy cập tài nguyên qua mạng, người dùng phải chịu các loại permission nào, kết quả tổng hợp là gì?

Câu 9. Trên thư mục ABC, permission được thiết lập: Shared permission: Everyone allow read; NTFS permission: KT1 allow write. Cho biết KT1 có quyền gì khi truy cập ABC qua mạng.

Câu 10. Trình bày cách thiết lập quyền giữa NTFS permission và Share permission trên tài nguyên sao cho NTFS permission được bảo toàn trong cả 2 trường hợp truy cập tại chỗ và truy cập qua mạng.

Câu 11. Share Permission có bao nhiêu lựa chọn?

Câu 12. Trình bày câu lệnh tạo ổ đĩa mạng.

Câu 13. Liệt kê tất cả shared folder và vị trí của chúng trên một server.

Câu 14. Trình bày cách hủy inheritable NTFS permission trên một tài nguyên.

Câu 15. Trình bày cách áp NTFS permission của một thư mục lên mọi tài nguyên trong thư mục đó.

Câu 16. Liệt kê các standard NTFS permission

Bài thực hành 1. Thiết lập quyền người dùng trên thư mục dùng chung
Trên File Server có tài khoản người dùng và nhóm như sau:

- Nhóm BanGiamDoc gồm: Hung, Trong
- Nhóm NhanVien gồm: Diep, Tuan, Tung.

Anh/Chị hãy tạo cấu trúc thư mục như hình sau.



Sau đó, Anh/Chị hãy cấp quyền truy cập cho người dùng theo yêu cầu sau:
Mỗi người dùng có toàn quyền trên thư mục dành riêng của mình. Trưởng phòng của mỗi phòng ban sẽ đọc được dữ liệu của các thành viên khác trong phòng. Trưởng phòng là tài khoản đầu tiên trong danh sách của mỗi nhóm. Thư mục Public là thư mục dùng chung, mọi người có thể ghi dữ liệu lên đó nhưng chỉ xóa được những dữ liệu cho mình tạo ra. Mọi người có thể truy cập thư mục Public từ máy cục bộ hoặc từ một máy khác trong hệ thống mạng

Bài thực hành 2. Trên hệ thống mạng đang có, các tài nguyên chia sẻ nằm rải rác trên các máy Server khác nhau.

Trên máy File Server đang chia sẻ thư mục Public. Trên máy Tuan đang chia sẻ thư mục Software. Trên máy Diep đang chia sẻ thư mục Music. Anh/Chị muốn người dùng truy cập vào một tài nguyên chia sẻ trên máy Server có địa chỉ IP 192.168.1.250. Từ đó, mọi người có thể truy cập các tài nguyên trên. Anh/Chị hãy cấu hình hệ thống theo yêu cầu trên.

Bài thực hành 3. Dùng máy ảo xây dựng hệ thống mạng như trên mô hình và thực hiện các yêu cầu sau:

Tiến hành backup hệ thống từ máy server sang máy chủ dự phòng IBM.

Trên máy PC/Laptop có rất nhiều dữ liệu quan trọng cần được backup thường xuyên vậy bạn hãy tiến hành lập lịch backup cho các dữ liệu đó. Toàn bộ dữ liệu backup sẽ được lưu trực tiếp trên server IBM

CHƯƠNG 6. DỊCH VỤ DNS VÀ DHCP

Chương này tập trung trình bày hai dịch vụ quan trọng và phổ biến trong các hệ thống mạng máy tính là dịch vụ phân giải tên miền (DNS – Domain Name System) và dịch vụ cấp phát địa chỉ IP động theo giao thức DHCP (). *Mục 6.1* trình bày về dịch vụ DNS gồm các vấn đề: khái niệm, các loại bản ghi, triển khai DNS trên máy chủ và cấu hình DNS trên máy trạm. *Mục 6.2* trình bày về giao thức DHCP, cài đặt dịch vụ DHCP trên máy chủ, cấu hình DHCP phía máy trạm. *Mục 6.3* tổng kết các nội dung của chương.

6.1. DỊCH VỤ DNS

6.1.1. Một số khái niệm

Dịch vụ phân giải tên miền DNS (Domain Name System) được tích hợp trong Active Directory dùng để phân giải các tên máy như Client1.khoacntt.edu.vn thành các địa chỉ IP khó nhớ như 172.67.1.10. Một máy chủ có cài dịch vụ này được gọi là DNS Server (máy chủ phân giải tên), ta cũng có thể cho máy chủ DC kiêm cả chức năng DNS Server.

Zone (khu vực): được hiểu là phạm vi các địa chỉ IP mà DNS Server phải quan tâm. Các DNS Server không chứa thông tin tên của các miền, mà chỉ những thông tin của các zone. Một DNS Server có thể phụ trách nhiều zone.

Forward Lookup Zones (khu vực tra cứu xuôi): là khu vực để tra cứu địa chỉ IP của một tên máy (chuyển một tên máy thành một địa chỉ IP). Thông tin về khu vực này có thể được lưu trữ trong Active Directory hoặc lưu trữ trong một file gọi là *zone file* tra cứu xuôi. Mỗi một miền có một *zone file* riêng.

Mỗi một miền chỉ có một khu vực tra cứu xuôi, được đặt tên chính là tên miền. Còn tên *zone file* tra cứu xuôi được đặt bằng các ghép thêm đuôi .dns vào sau tên zone.

Ví dụ: Với miền khoacntt.edu.vn, thì tên zone tra cứu xuôi sẽ chính là: khoacntt.edu.vn, còn tên zone file là: khoacntt.edu.vn.dns

Reverse Lookup Zones (khu vực tra cứu ngược): là khu vực để tra cứu tên máy của một địa chỉ IP (chuyển một địa chỉ IP thành một tên máy).

Qui tắc đặt tên zone tra cứu ngược không liên quan gì đến tên miền, mà liên quan đến địa chỉ mạng IP. Mỗi một mạng (hay lô địa chỉ IP có) có một zone tra cứu ngược tương ứng. Thông tin về khu vực này cũng có thể được lưu trữ trong Active Directory hoặc lưu trữ trong một file gọi là *zone file* tra cứu ngược. Mỗi một mạng có một *zone file* tra cứu ngược riêng.

Tên của zone tra cứu ngược được đặt bằng các đảo ngược các nhóm của địa chỉ mạng, rồi ghép thêm vào cuối cụm “.in-addr.arpa”. Còn tên *zone file* tra cứu ngược cũng được đặt bằng các ghép thêm đuôi .dns vào sau tên zone.

Ví dụ: Với mạng 172.67.1, thì tên zone tra cứu ngược sẽ là: 1.67.172.in-addr.arpa, còn tên zone file là: 1.67.172.in-addr.arpa.dns

6.1.2. Những loại bản ghi phổ biến trong DNS

Mỗi một dòng được lưu trữ trong DNS được gọi là một bản ghi. Cơ sở dữ liệu DNS không chỉ chứa các bản ghi để phân giải các tên và địa chỉ IP, mà còn chứa một số loại bản ghi khác mà ta sẽ tìm hiểu ngay dưới đây.

a. Bản ghi A (Address), tức là bản ghi Host

Là những bản ghi để tra cứu xuôi, như trong Hình 6.1 ta thấy máy tính Client1 có địa chỉ IP là 172.67.1.10.

b. Bản ghi SOA (Start of Authority)

Mỗi miền đều có một bản ghi SOA (chỗ bắt đầu chịu trách nhiệm), đây là bản ghi dành cho tên của DNS server chính của miền, như trên Hình 6.1 ta thấy máy đó là server1.khoacntt.edu.vn. Con số [76] của bản ghi SOA này cho biết rằng kể từ khi được thiết lập đã có 76 lần thay đổi (có thể là thêm bản ghi mới hoặc xoá bản ghi đã có). Các DNS server phụ sẽ dựa vào thông tin này để biết dữ liệu trên server chính đã thay đổi hay chưa, từ đó xác định là có cần lấy những thông tin đã cập nhật từ DNS server chính hay không.

Name	Type	Data	Timestamp
_msdcsv	Start of Authority (SOA)	[76], server1.khoacontt.edu....	11/2/20
_sites	Name Server (NS)	server1.khoacontt.edu.vn.	11/2/20
_tcp	Host (A)	172.67.1.1	11/2/20
_udp	IPv6 Host (AAAA)	2002:ac43:0101:0000:0000...	11/2/20
DomainDnsZones	(same as parent folder)		
ForestDnsZones	(same as parent folder)		
Client1	Host (A)	172.67.1.10	11/3/20
Client1	IPv6 Host (AAAA)	2002:ac43:010a:0000:0000...	11/3/20
ftp	Alias (CNAME)	www.khoacontt.edu.vn	static
server1	Host (A)	172.67.1.1	11/3/20
server1	IPv6 Host (AAAA)	2002:ac43:0101:0000:0000...	11/3/20
Server2	Host (A)	172.67.1.200	static
WIN-TMVMRBAVAFN	IPv6 Host (AAAA)	2002:ac43:010a:0000:0000...	11/3/20
www	Host (A)	172.67.1.1	static
email	Host (A)	172.67.1.2	
email	Mail Exchanger (MX)	[10] email.khoacontt.edu.vn	

Hình 6.1: Các loại bản ghi thuộc zone tra cứu xuôi

c. Bản ghi NS (Name Server)

Các bản ghi NS dùng để qui định tên các DNS server trong miền, như trên hình 6.1 ta thấy có một máy dùng làm DNS server là server1.khoacontt.edu.vn.

d. Bản ghi CNAME (Canonical Name)

Bản ghi CNAME hay còn gọi là bản ghi bí danh dùng để đặt một tên khác cho một máy, thường được dùng khi một máy chủ kiêm nhiều dịch vụ trên đó. Trên Hình 6.1 ta thấy máy web server www.khoacontt.edu.vn kiêm luôn dịch vụ FTP, nên phải có bản ghi bí danh là:

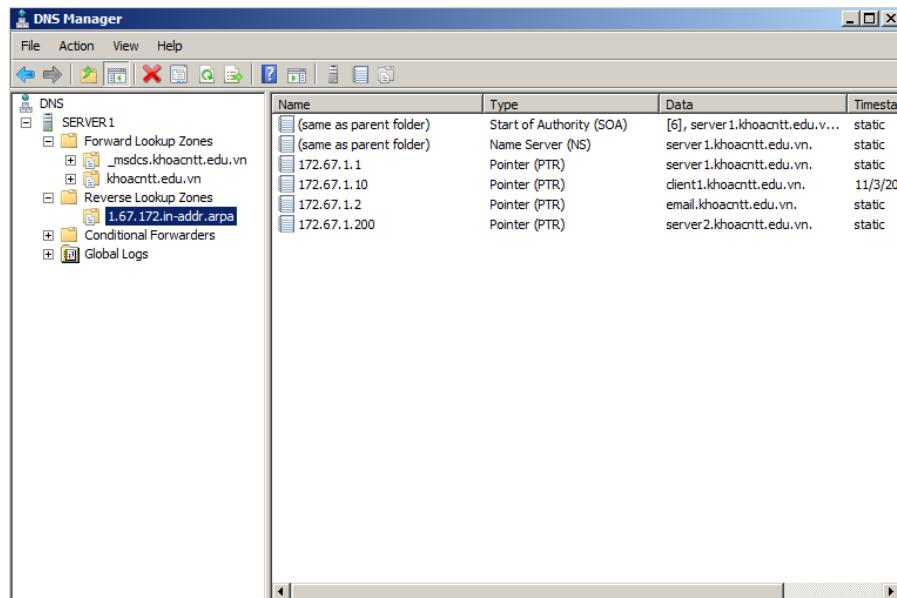
ftp	Alias	www. khoacontt.edu.vn
-----	-------	-----------------------

e. Bản ghi MX (Mail Exchange)

Bản ghi này dùng để xác định miền của thư điện tử được chuyển về máy mail server (máy chủ thư) nào. Trên Hình 6.1 đó là máy email.khoacontt.edu.vn, con số [10] chỉ sự ưu tiên. Khi có nhiều hơn một bản ghi MX đối với miền đã định, tức là có thể có nhiều mail server để dự phòng trong trường hợp một mail server nào đó bị hỏng hóc, thì máy mail server nào có số ưu tiên nhỏ hơn sẽ được ưu tiên để nhận thư.

f. Bản ghi PTR (Pointer)

Bản ghi PTR (bản ghi con trỏ), hay còn gọi là bản ghi Reverse host. Bản ghi PTR cũng tương tự như bản ghi A, chỉ khác là bản ghi A để tra cứu địa chỉ IP được liên kết với một tên máy, trong khi bản ghi PTR cho phép ta tra cứu một tên máy được liên kết với một địa chỉ IP cụ thể. Trong Hình 6.2 ta thấy địa chỉ IP 172.67.1.10 được gắn cho máy: Client1.khoacntt.edu.vn.



Hình 6.2: Các bản ghi PTR thuộc zone tra cứu ngược

6.1.3. Cài đặt DNS server

Chỉ các máy có cài đặt Windows server mới cài đặt được dịch vụ DNS. Khi máy chủ có cài đặt dịch vụ này thì nó được gọi là DNS server. Các bước để cài đặt dịch vụ DNS cũng tương tự như các bước để cài đặt các dịch vụ khác, nên ta có thể tóm tắt một số bước như sau:

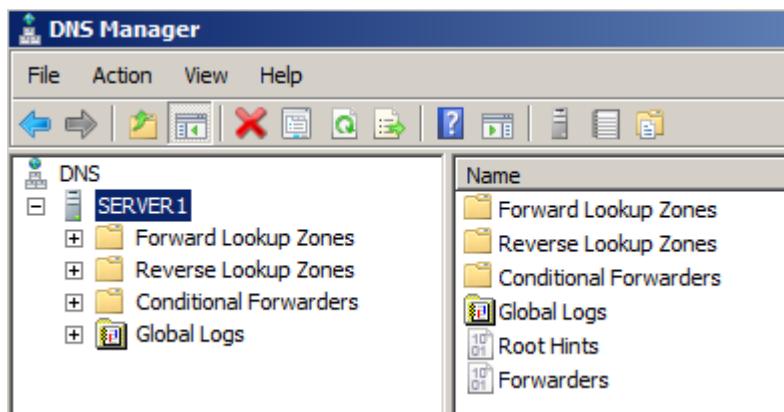
1. Chọn **Start > Programs > Administrative Tools > Server Manager**.
2. Tại cửa sổ **Server Manager**, chọn mục **Roles**, chọn mục **Add Roles**.
3. Tại cửa sổ **Before You Begin**, chọn **Next**.
4. Tại cửa sổ **Select Server Roles**, chọn **DNS Server**, chọn **Next**.

5. Tại cửa sổ **DNS Server**, chọn **Next**. Quá trình cài đặt sẽ diễn ra...Sau khi cài đặt xong, nhấn **Close** để kết thúc quá trình cài đặt.
6. Nhấn **OK** để quay về cửa sổ Windows Components Wizard.
7. Tại cửa sổ **Confirm Installation Selections**, chọn **Install** để tiến hành cài đặt.
8. Quá trình cài đặt sẽ diễn ra...Sau khi cài đặt xong, nhấn **Close** để kết thúc quá trình cài đặt.

6.1.4. Tạo ra các Zone

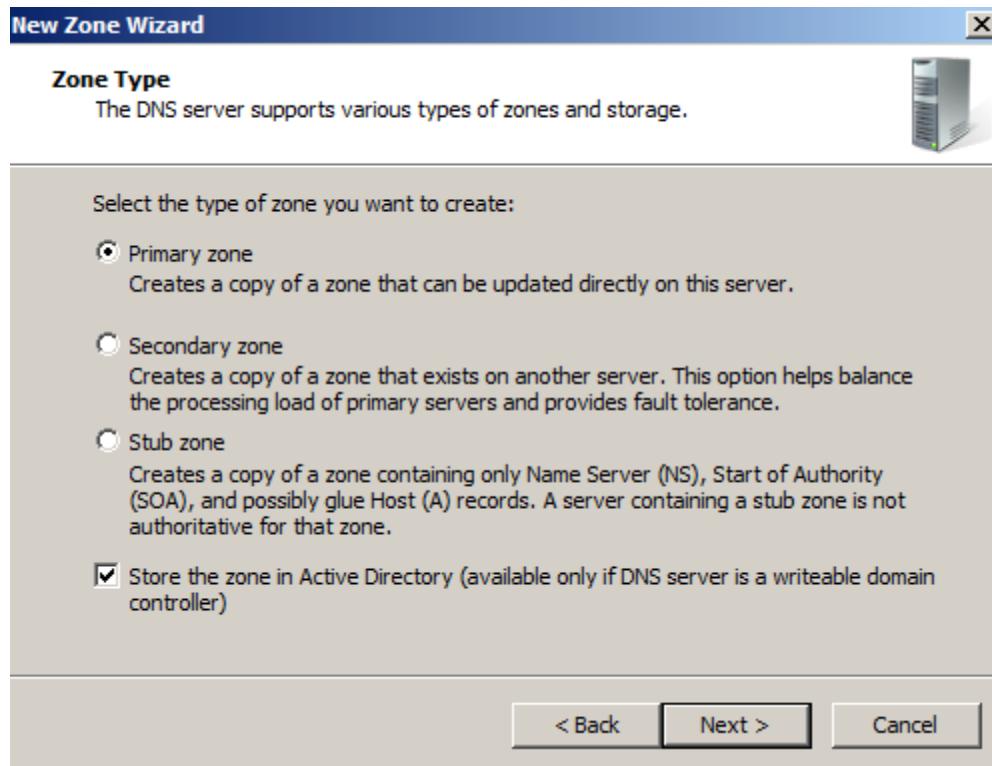
a. Tạo Zone tra cứu xuôi

Khi cài đặt xong dịch vụ DNS, ta không cần khởi động lại máy mà vẫn có thể khởi động luôn dịch vụ DNS để tạo ra các zone bằng cách chọn Start/Administrative Tools/DNS để hiện ra cửa sổ như hình sau:



Hình 6.3: Cửa sổ bắt đầu dịch vụ DNS

Để tạo zone tra cứu xuôi cho miền khoatin.org, ta nhấp chuột phải tại Forward Lookup Zones, chọn New Zone, nhấn Next để hiện ra cửa sổ chọn loại zone như Hình 6.4.



Hình 6.4:Cửa sổ chọn loại zone

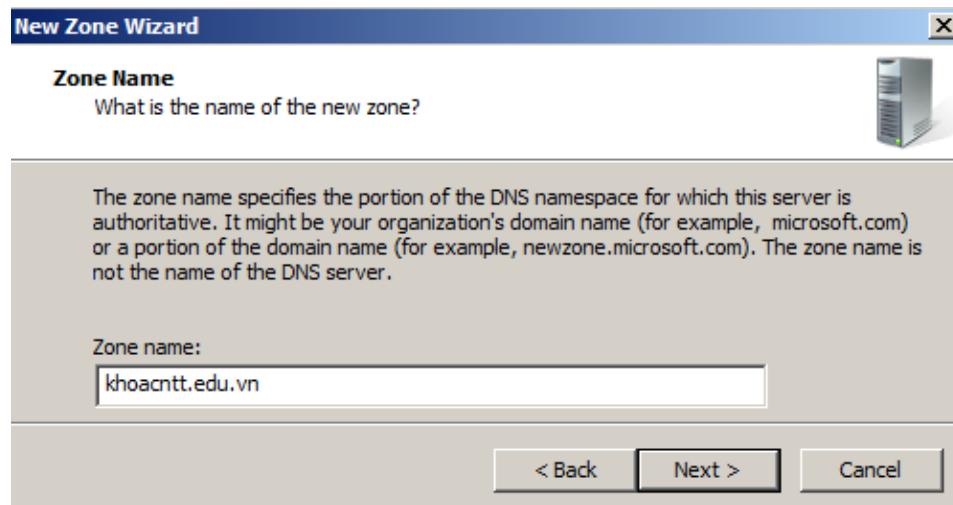
ý nghĩa của các loại zone trong cửa sổ trên như sau:

Active Directory-integrated: zone với các bản ghi sẽ lưu trữ trong cơ sở dữ liệu Active Directory.

Standard primary: zone dành cho máy DNS server chính, với các bản ghi sẽ lưu trữ trong một zone file dạng text.

Standard secondary: zone dành cho máy DNS server dự phòng, sẽ tạo ra bản copy của một zone đã tồn tại trên máy DNS server chính.

ở đây ta chọn loại Active Directory-integrated. Nhấn Next để nhìn thấy cửa sổ như Hình 6.5.

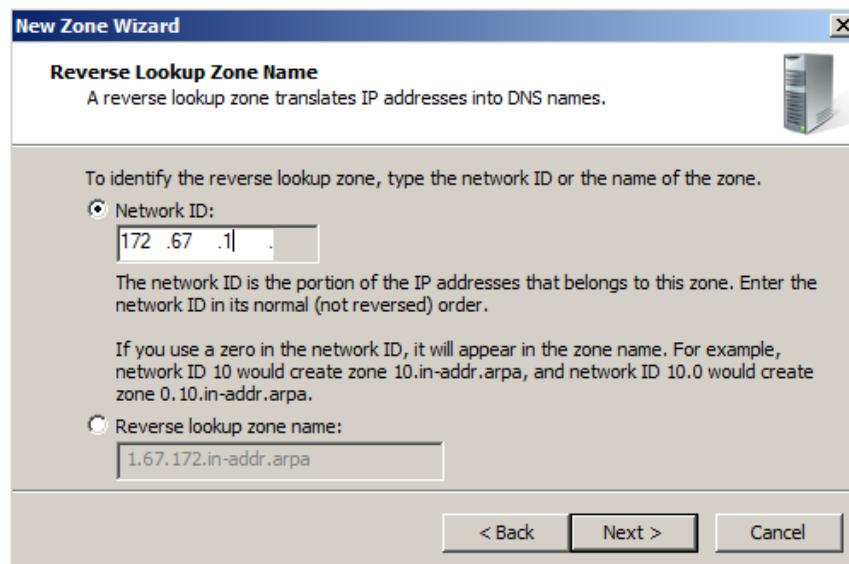


Hình 6.5: Cửa sổ đặt tên cho zone

Cửa sổ trên dùng để đặt tên cho zone, tên này phải trùng với tên miền. Tiếp theo nhấn Next, rồi nhấn nút Finish để kết thúc.

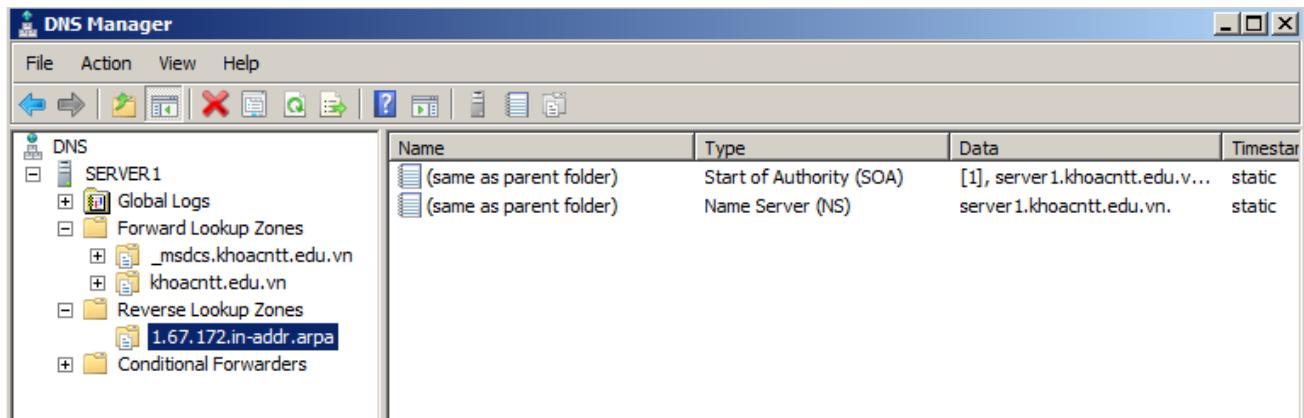
b. Tạo Zone tra cứu ngược

Để tạo zone tra cứu ngược cho địa chỉ mạng 172.67.1, ta nhấp chuột phải tại Reverse Lookup Zones, chọn New Zone, nhấp Next để hiện ra cửa sổ như Hình 6.6. Nhập địa chỉ mạng vào ô Network ID, ta thấy tên zone tra cứu ngược sẽ được tự đặt trong ô Reverse lookup zones name.



Hình 6.6: Cửa sổ đặt tên cho zone

Khi các zone được tạo xong, cửa sổ DNS có dạng như Hình 6.7.

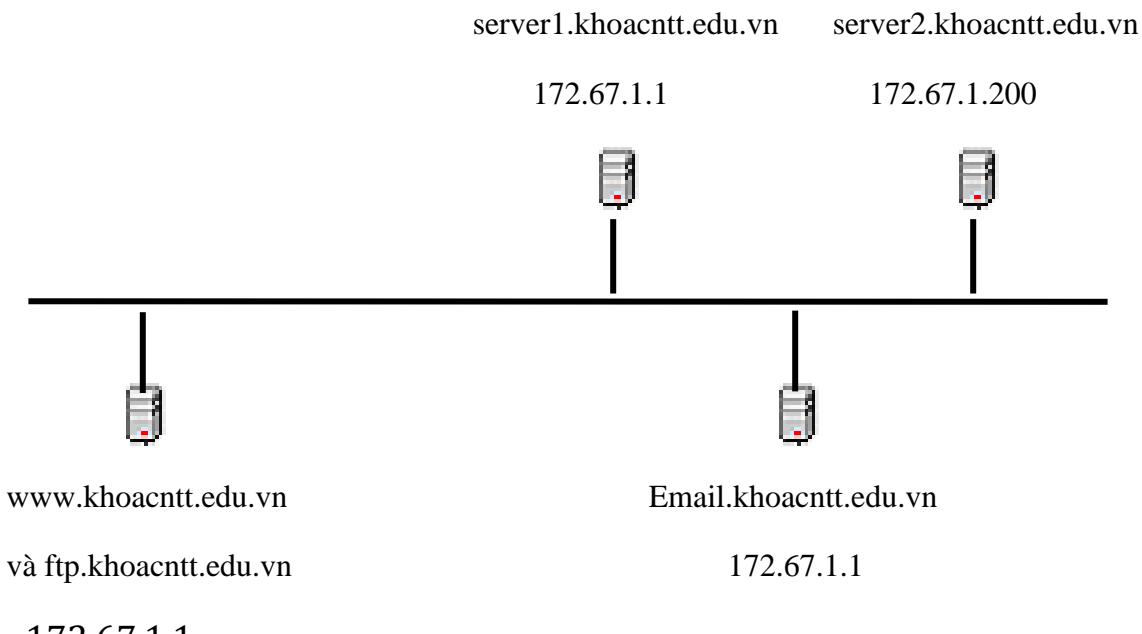


Hình 6.7: Cửa sổ DNS khi đã tạo ra các Zone

6.1.5. Tạo các bản ghi

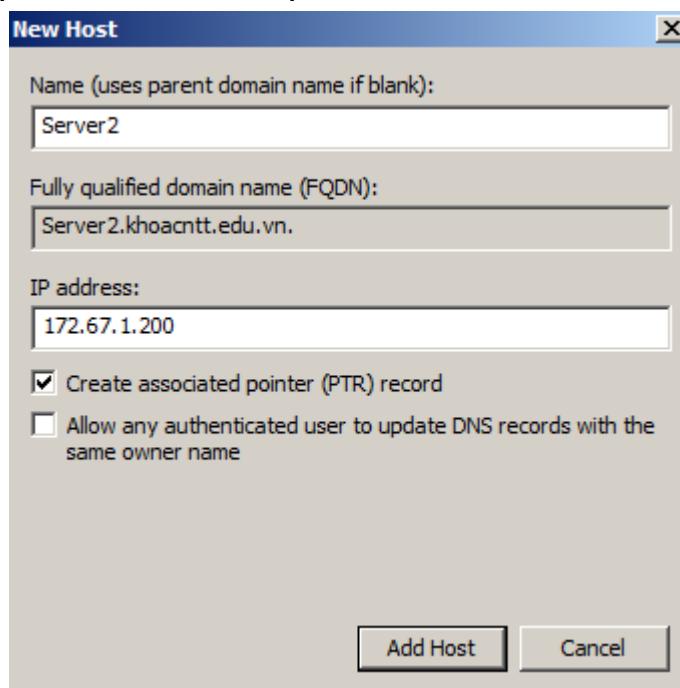
a. Tạo các bản ghi Host (bản ghi A)

DNS server của Windows server có khả năng tự cập nhật các bản ghi Host, nên ta không cần phải nhập các bản ghi host cho từng máy. Tuy nhiên ta vẫn cần nhập một số bản ghi host cho các máy server hoặc router.



Hình 6.8: Các server của miền khoacntt.edu.vn

Giả sử miền khoacntt.edu.vn có các máy chủ như Hình 6.8. Khi đó để tạo ra các bản ghi host cho mỗi máy chủ, ta nhấn phải chuột vào tên zone khoacntt.edu.vn, chọn New Host để hiện ra cửa sổ như Hình 6.9.



Hình 6.9: Cửa sổ New Host

Trong cửa sổ trên, các mục:

Name: để nhập vào tên host

IP address: để nhập địa chỉ IP của host

Create associated pointer (PTR) record: nếu được chọn sẽ tự tạo ra bản ghi PTR ứng với bản ghi host này.

Nhấn nút Add Host để tạo, rồi tiếp tục tạo các host khác, để có được kết quả như cửa sổ Hình 6.10.

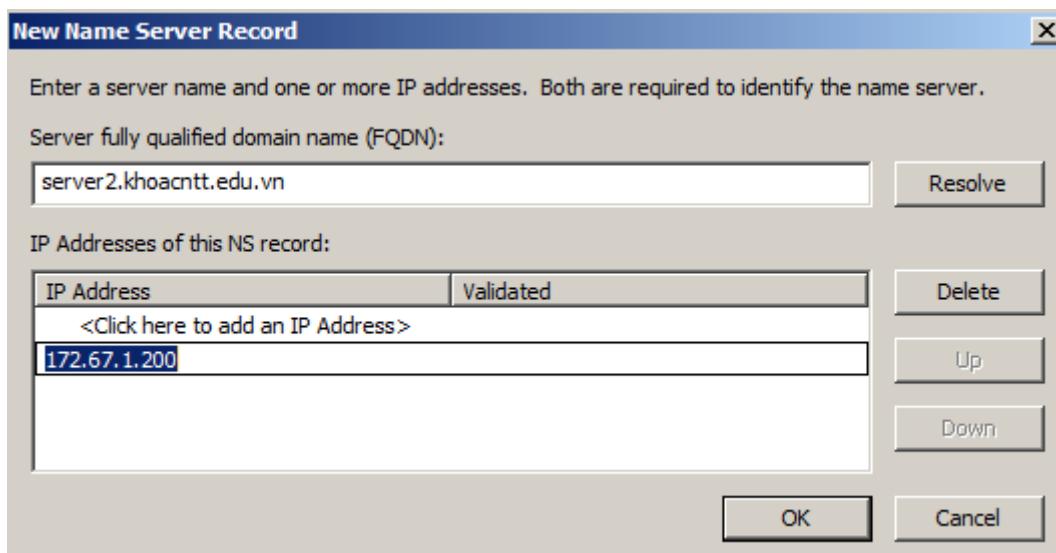
The screenshot shows the Windows DNS Manager window. On the left, a tree view displays the DNS structure under SERVER.1, including Global Logs, Forward Lookup Zones (with _msdcs.khoacntt.edu.vn selected), Reverse Lookup Zones (with 1.67.172.in-addr.arpa), and Conditional Forwarders. The main pane on the right lists hosts in a table with columns: Name, Type, Data, and Timestamp. The table includes entries for Start of Authority (SOA), Name Server (NS), Host (A), and IPv6 Host (AAAA) records for various clients and servers like Client1, server1, and Server2.

Name	Type	Data	Timestamp
_msdcs			
_sites			
_tcp			
_udp			
DomainDnsZones			
ForestDnsZones			
(same as parent folder)	Start of Authority (SOA)	[67], server1.khoacntt.edu....	11/2/20
(same as parent folder)	Name Server (NS)	server1.khoacntt.edu.vn.	11/2/20
(same as parent folder)	Host (A)	172.67.1.1	11/2/20
(same as parent folder)	IPv6 Host (AAAA)	2002:ac43:0101:0000:0000...	11/2/20
Client1	Host (A)	172.67.1.10	11/3/20
Client1	IPv6 Host (AAAA)	2002:ac43:010a:0000:0000...	11/3/20
server1	Host (A)	172.67.1.1	11/3/20
server1	IPv6 Host (AAAA)	2002:ac43:0101:0000:0000...	11/3/20
WIN-TMVMRBAVAFN	IPv6 Host (AAAA)	2002:ac43:010a:0000:0000...	11/3/20
Server2	Host (A)	172.67.1.200	

Hình 6.10: Cửa sổ hiện các host cần tạo

b. Chỉ định name server thứ hai

Nhấn phải chuột vào khoang chứa khoatin.org, chọn Properties, chọn trang Name Servers, nhấn nút Add để hiện ra cửa sổ như Hình 6.11.

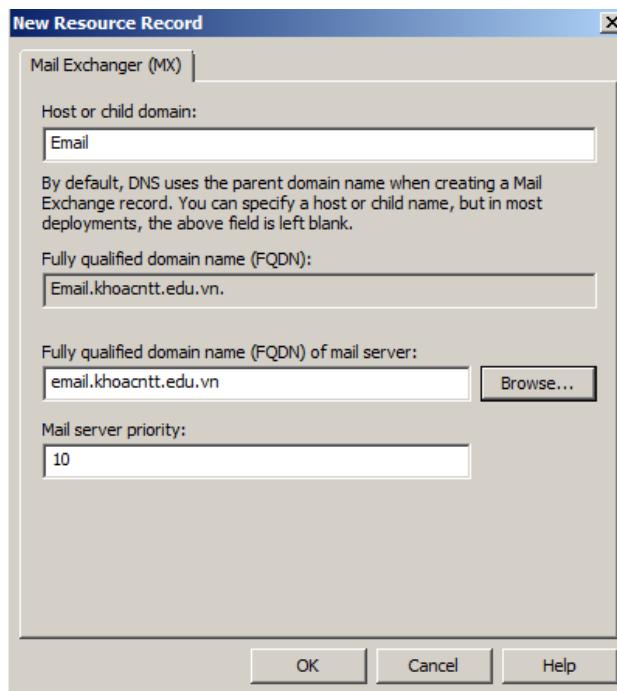


Hình 6.11 : Cửa sổ quy định máy server2 là một DNS server

Khi nhập xong các thông tin, ta nhấn Add, rồi nhấn OK để kết thúc.

c. Tạo bản ghi MX

Nhấn phải chuột vào khoang chứa khoatin.org, chọn New Mail Exchanger, khi đó ra cửa sổ như Hình 6.12 sẽ hiện ra. Ta nhập tên đầy đủ cho server Email tại hộp Mail server. Ô Mail server priority để nhập vào giá trị ưu tiên nhận thư, giá trị này chỉ có tác dụng khi trên miền có nhiều Mail server. Để kết thúc tạo bản ghi này ta nhấn OK.

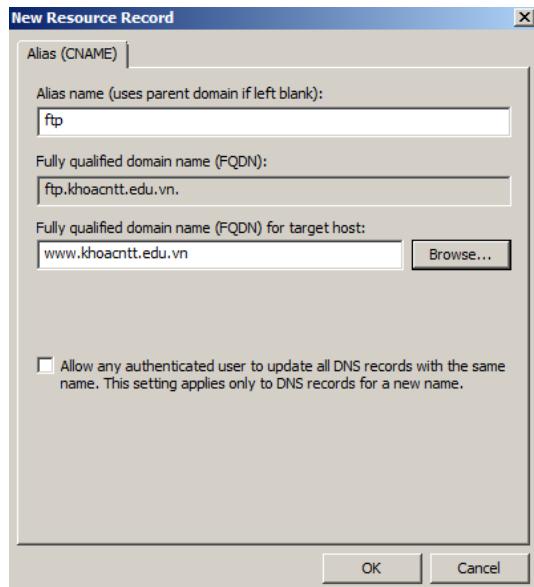


Hình 6.12: Cửa sổ biến máy EMail thành một Mail server

d. Tạo bản ghi CNAME

Ta thấy máy www đang đóng vai trò là một Web server. Để máy này cũng đóng vai trò là một FTP server thì ta phải cho www một cái tên thứ hai là ftp, bằng cách tạo ra bản ghi CNAME (hay Alias) như sau:

Nhấn phải chuột tại khoatin.org, chọn New Alias để hiện ra cửa sổ như Hình 6.13. Sau đó nhập bí danh vào ô: Alias name, nhập tên server gốc tại ô: Fully qualified name for target host, rồi nhấn OK.



Hình 6.13: Cửa sổ tạo bí danh cho máy Web server

Cửa sổ DNS khi đã tạo xong các bản ghi có dạng như hình 6.14.

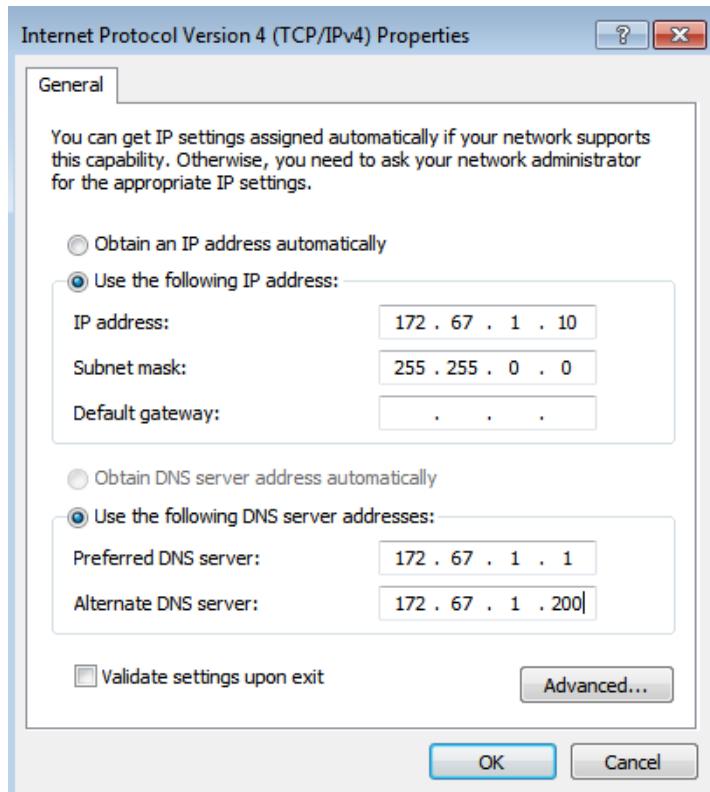
Name	Type	Data	Timestamp
_msdcsv	Start of Authority (SOA)	[76], server1.khoacntt.edu....	11/2/20
_sites	Name Server (NS)	server1.khoacntt.edu.vn.	11/2/20
_tcp	Host (A)	172.67.1.1	11/2/20
_udp	IPv6 Host (AAAA)	2002:ac43:0101:0000:0000...	11/2/20
DomainDnsZones	Host (A)	172.67.1.10	11/3/20
ForestDnsZones	IPv6 Host (AAAA)	2002:ac43:010a:0000:0000...	11/3/20
(same as parent folder)	Host (A)	172.67.1.1	11/3/20
(same as parent folder)	IPv6 Host (AAAA)	2002:ac43:0101:0000:0000...	11/3/20
(same as parent folder)	Host (A)	172.67.1.200	static
Client1	Host (A)	172.67.1.10	11/3/20
Client1	IPv6 Host (AAAA)	2002:ac43:010a:0000:0000...	11/3/20
ftp	Alias (CNAME)	www.khoacntt.edu.vn	static
server1	Host (A)	172.67.1.1	11/3/20
server1	IPv6 Host (AAAA)	2002:ac43:0101:0000:0000...	11/3/20
Server2	Host (A)	172.67.1.200	static
WIN-TMVMRBAVAFN	IPv6 Host (AAAA)	2002:ac43:010a:0000:0000...	11/3/20
www	Host (A)	172.67.1.1	static
email	Host (A)	172.67.1.2	static
email	Mail Exchanger (MX)	[10] email.khoacntt.edu.vn	

Hình 6.14: Cửa sổ DNS khi đã tạo ra các loại bản ghi

Để xoá một zone nào đó ta chỉ việc chọn nó rồi bấm phím Delete.

6.1.6. Cấu hình dịch vụ DNS trên máy khách

Trên các máy khách, nếu muốn cấu hình tĩnh dịch vụ DNS, thì ta lại mở cửa sổ thiết lập cấu hình TCP/IP như Hình 6.15. Sau đó nhập địa chỉ IP của máy DNS server chính vào ô: Preferred DNS server, nhập địa chỉ IP của máy DNS server phụ nếu có vào ô: Alternate DNS server.



Hình 6.15:Cửa sổ thiết lập cấu hình tĩnh dịch vụ DNS

6.2. DỊCH VỤ DHCP

Dịch vụ DHCP (Dynamic Host Configuration Protocol) dùng để tự cấp địa chỉ IP cho mỗi máy khi đăng nhập vào mạng. Như vậy, với một máy chủ có cài đặt dịch vụ này trên mạng theo mô hình miền, ta không cần phải đặt địa chỉ IP tĩnh cho từng máy như trong mô hình mạng ngang hàng.

6.2.1. Cài đặt DHCP server

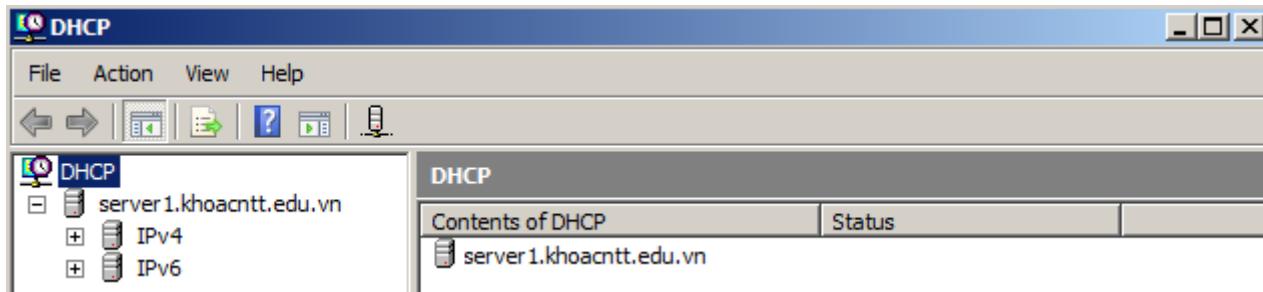
Chỉ các máy có cài đặt Windows server mới cài đặt được dịch vụ DHCP. Khi máy chủ có cài đặt dịch vụ này thì nó được gọi là DHCP server. Các bước để cài đặt

dịch vụ DHCP cũng tương tự như các bước để cài đặt dịch vụ DNS ở trên, gồm một số bước chính sau:

1. Chọn **Start > Programs > Administrative Tools > Server Manager**.
2. Tại cửa sổ **Server Manager**, chọn mục **Roles**, chọn mục **Add Roles**.
3. Tại cửa sổ **Before You Begin**, chọn **Next**.
4. Tại cửa sổ **Select Server Roles**, chọn **DHCP Server**, chọn **Next**.
5. Nếu không có địa chỉ IP tĩnh được gán trên máy chủ thì sẽ gặp một cảnh báo, cảnh báo này thông báo rằng không nên cài đặt DHCP với một địa chỉ IP động.
6. Tiếp theo, hệ thống sẽ yêu cầu các thông tin về IP mạng, thông tin về phạm vi và các thông tin DNS. Nếu chỉ cài đặt DHCP server mà không cần cấu hình các phạm vi và các thiết lập, chỉ cần kích **Next** xuyên suốt các chất vấn trong quá trình cài đặt.
7. Tiếp đến hệ thống sẽ hỏi “what interface do you want to provide DHCP services on?” tức là “giao diện bạn muốn cung cấp cho các dịch vụ DHCP là gì?” Chọn mặc định và kích **Next**.
8. Tiếp đến, nhập vào **Parent Domain**, **Primary DNS Server**, và **Alternate DNS Server** và kích **Next**.
9. Lựa chọn NOT để sử dụng WINS trên mạng của mình và kích **Next**.
10. Hệ thống sẽ chuyển tới bảng cấu hình DHCP scope cho DHCP Server mới. Hãy cấu hình scope mới sau kích **OK**. Quay trở lại màn hình Add Scope, kích **Next** để cập nhập scope mới cho server
11. Chọn **Disable DHCPv6 stateless mode** cho máy chủ này và kích **Next**.
- 12. Xác nhận DHCP Installation Selections của server và kích **Install**.**
13. DHCP Server sẽ được cài đặt. Kích **Close** để đóng cửa sổ cài đặt sau khi kết thúc quá trình cài đặt

6.2.2. Trao quyền hoạt động cho DHCP server

Khi cài đặt xong dịch vụ DHCP, ta không cần khởi động lại máy mà vẫn có thể khởi động luôn dịch vụ DHCP để tạo ra các zone bằng cách chọn Start/Administrative Tools/DHCP. Cửa sổ ban đầu của dịch vụ này được hiện ra như cửa sổ như Hình 6.16.

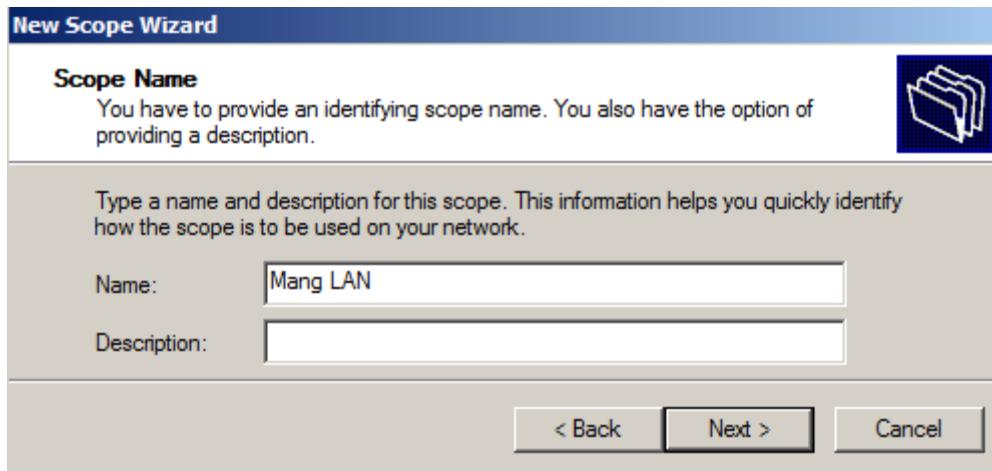


Hình 6.16: Cửa sổ DHCP ban đầu

Ta thấy tại biểu tượng máy chủ server1 có dấu mũi tên màu đỏ trỏ xuống dưới để cho biết là máy DHCP server chưa được trao quyền hoạt động. Để trao quyền hoạt động cho máy này, ta nhấn chuột phải vào nó rồi chọn Authorize. Sau đó lại nhấn phải chuột tại máy chủ đó, chọn Refresh để xem màn hình mới. Khi đó sẽ thấy dấu mũi tên chuyển sang màu xanh và hướng lên trên để cho biết là máy DHCP server đã được trao quyền hoạt động.

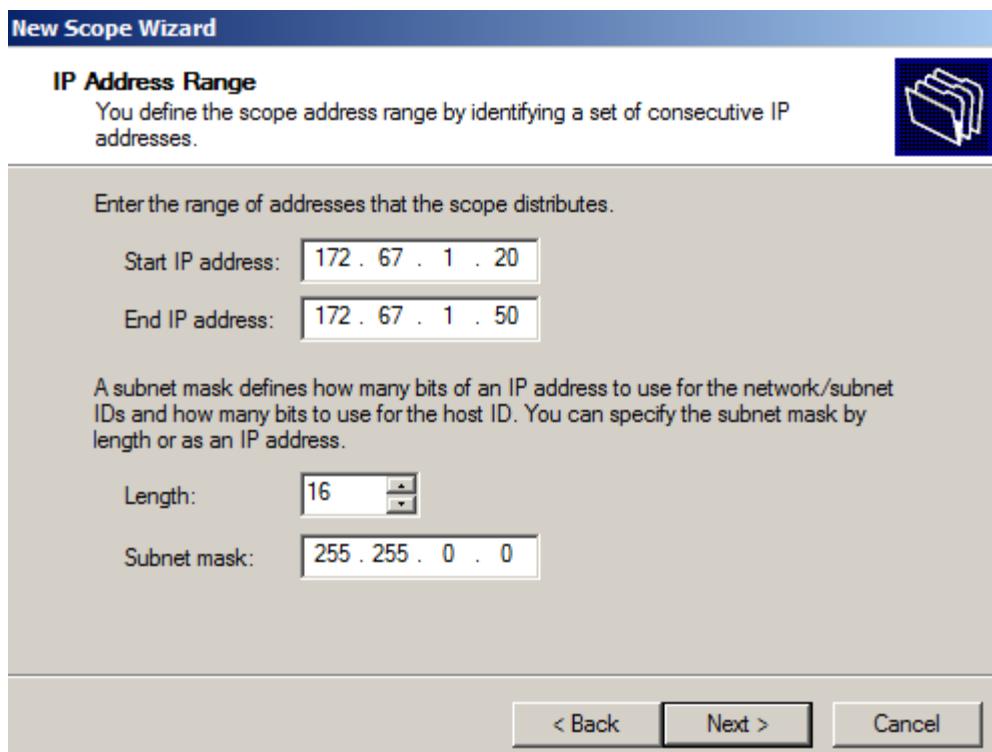
6.2.3. Tạo ra một scope (tầm)

Để DHCP server trao được các địa chỉ IP cho các máy, nó phải biết rõ về phạm vi địa chỉ mà nó có thể trao, phạm vi này được gọi là *scope (tầm)*. Một máy DHCP server có thể phục vụ nhiều scope. Để tạo ra một tầm, ta nhấn phải chuột vào biểu tượng máy chủ, chọn New Scope, nhấn Next, cửa sổ Hình 6.17 hiện ra để đặt tên cho tầm tại ô Name và một lời mô tả nếu có tại ô Description.



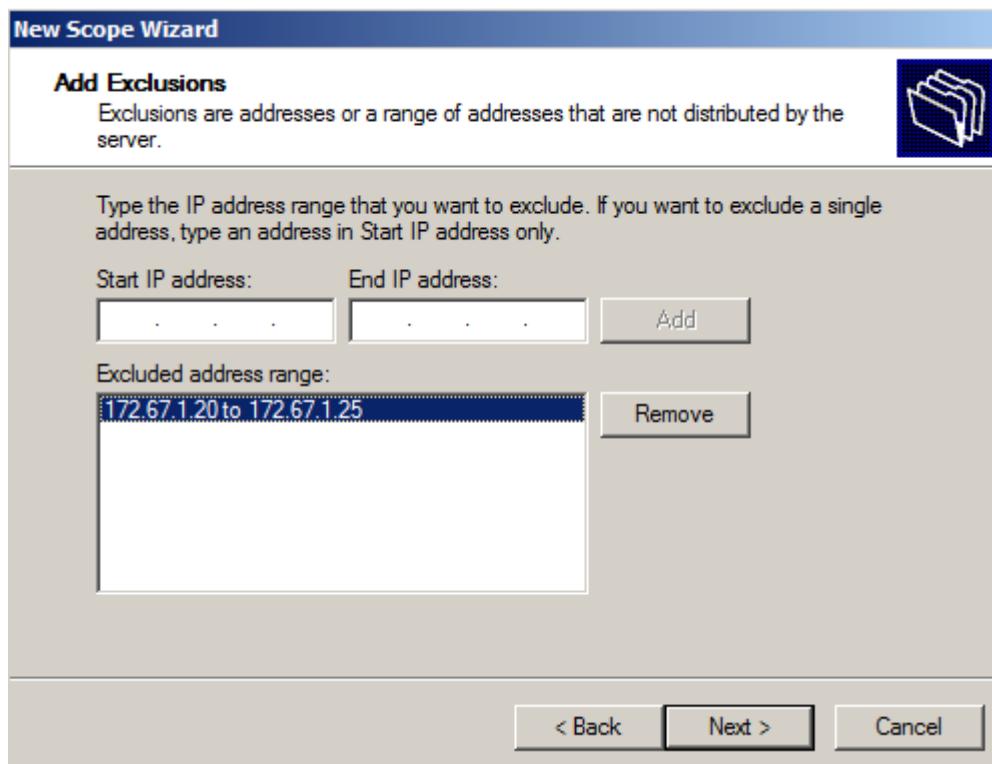
Hình 6.17: Cửa sổ đặt tên cho tầm

Nhấn Next, cửa sổ Hình 6.18 hiện ra để nhập vào phạm vi địa chỉ IP của tầm, từ địa chỉ tại ô: Start IP address đến địa chỉ tại ô: End IP address. Ô Length dùng để nhập số bit của Subnet mask.



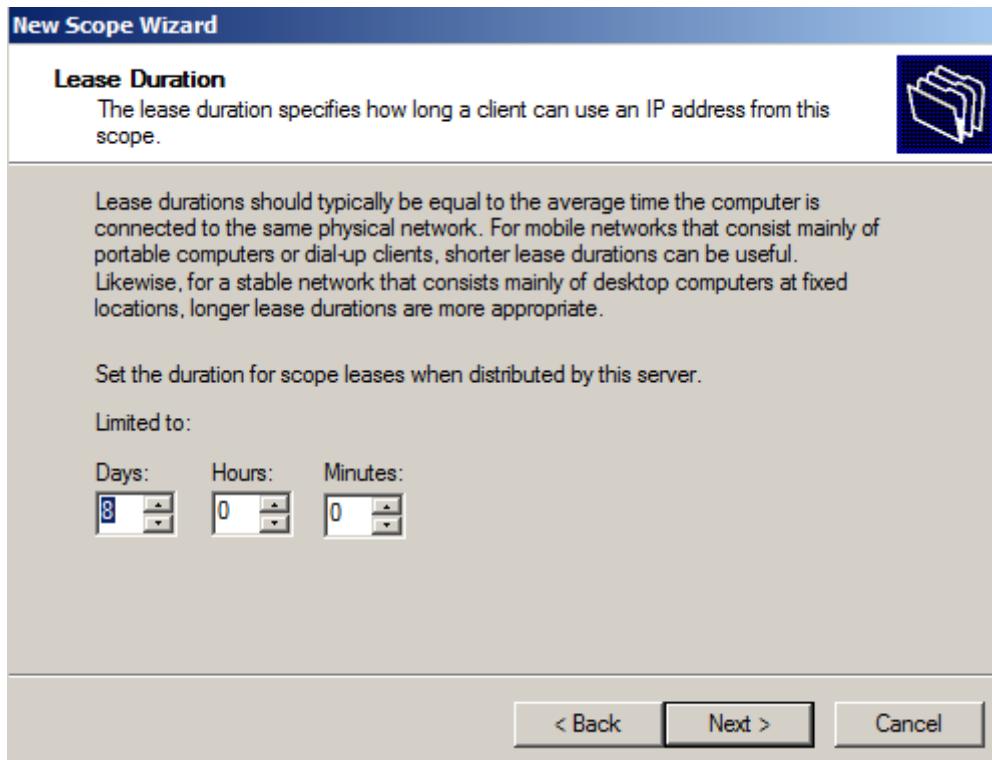
Hình 6.18: Cửa sổ qui định phạm vi địa chỉ IP

Nhấn Next, cửa sổ Hình 6.19 hiện ra cho phép loại ra các địa chỉ IP đã được cấp tĩnh cho một số địa chỉ.



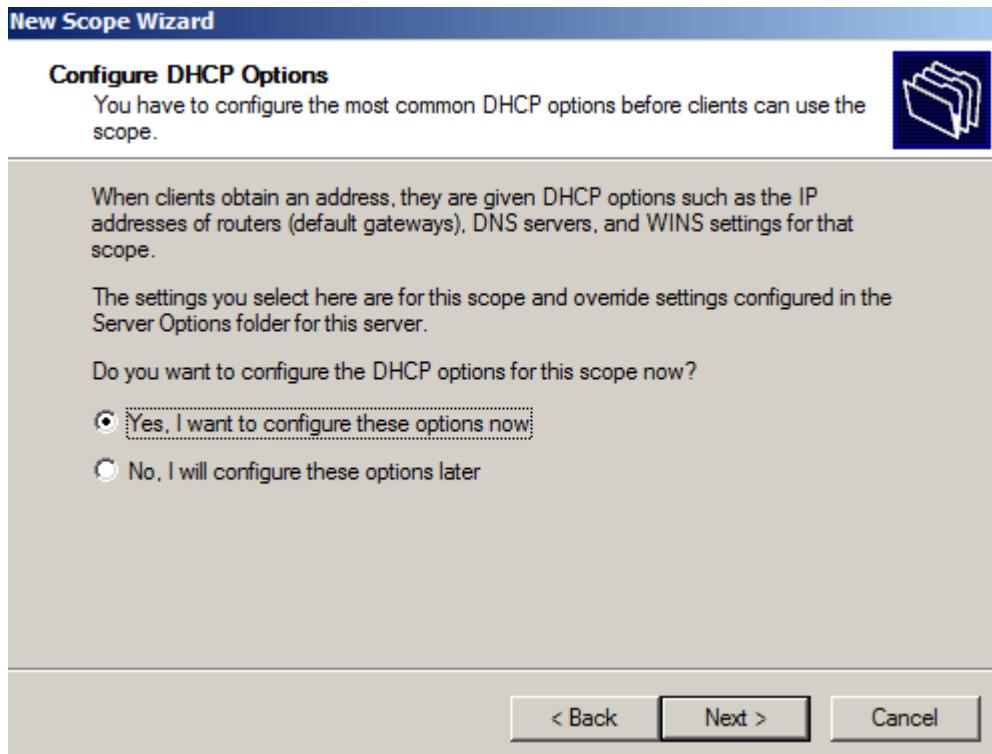
Hình 6.19: Cửa sổ cho phép loại ra phạm vi địa chỉ IP nào đó

Nhấn Next, cửa sổ Hình 6.20 hiện ra cho phép ta ấn định thời gian thuê bao (lease duration) các địa chỉ IP.



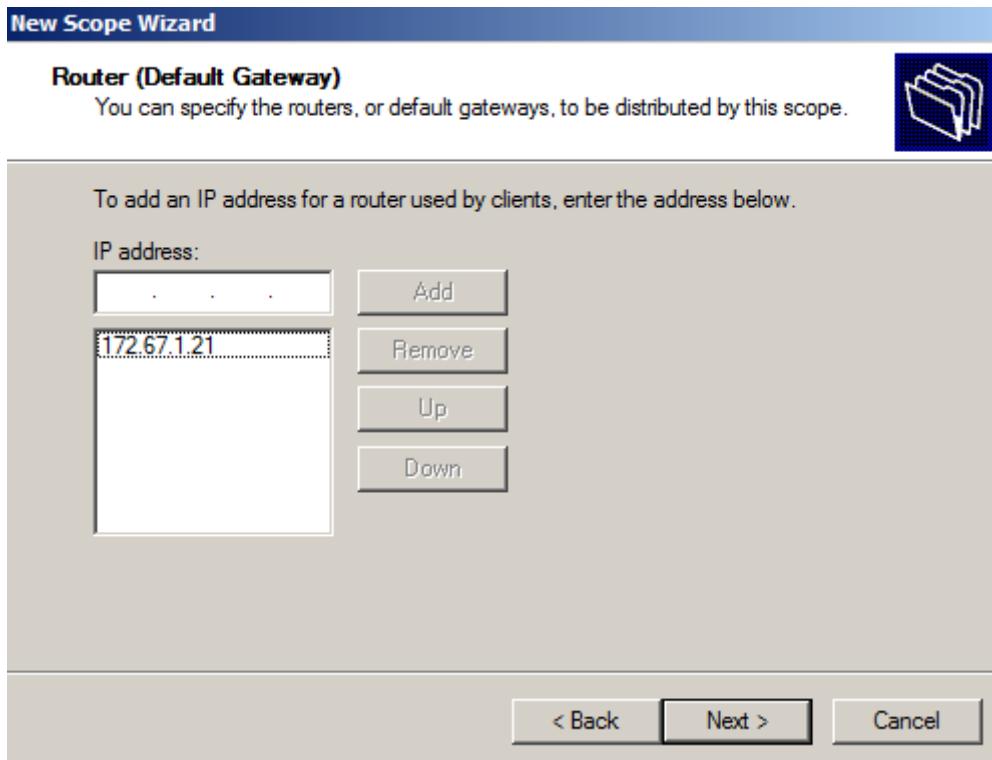
Hình 6.20: Cửa sổ ấn định thời gian thuê bao các địa chỉ IP

Nhấn Next, cửa sổ Hình 6.21 hiện ra cho phép ta ấn định các tuỳ chọn cấu hình mặc định DHCP trên máy khách.



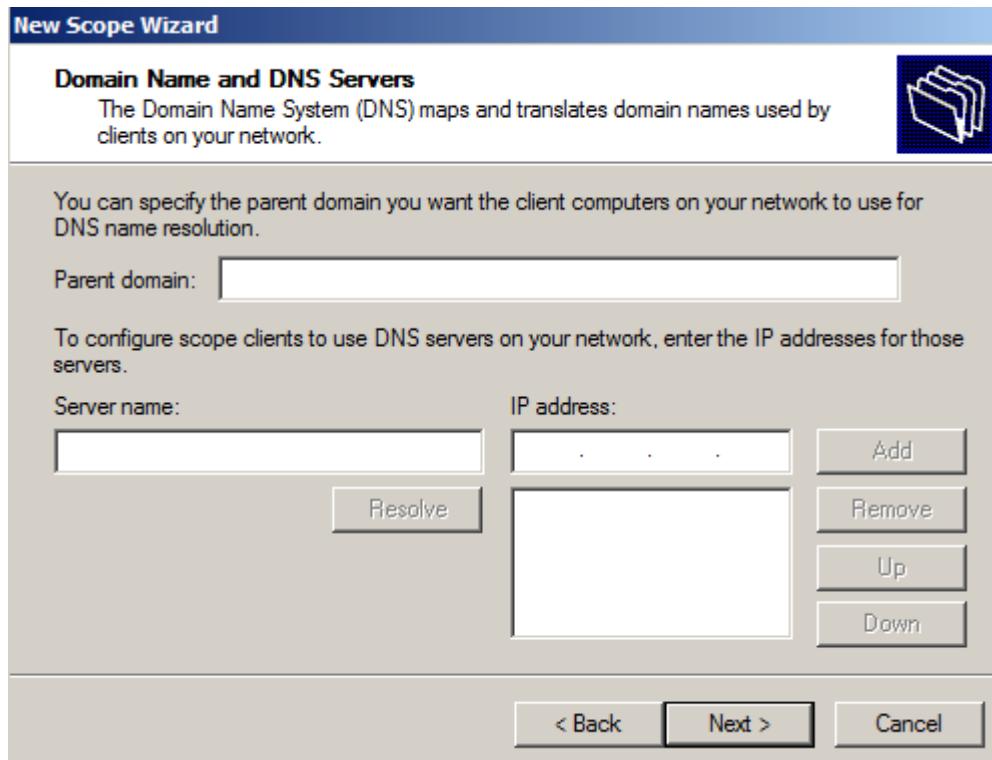
Hình 6.21: Cửa sổ ấn định các tùy chọn mặc định DHCP trên máy khách

Tại đây ta chọn Yes rồi nhấn Next, màn hình tiếp theo như Hình 6.22 hiện ra cho phép ta ấn định địa chỉ IP Default gateway cho các máy khách.

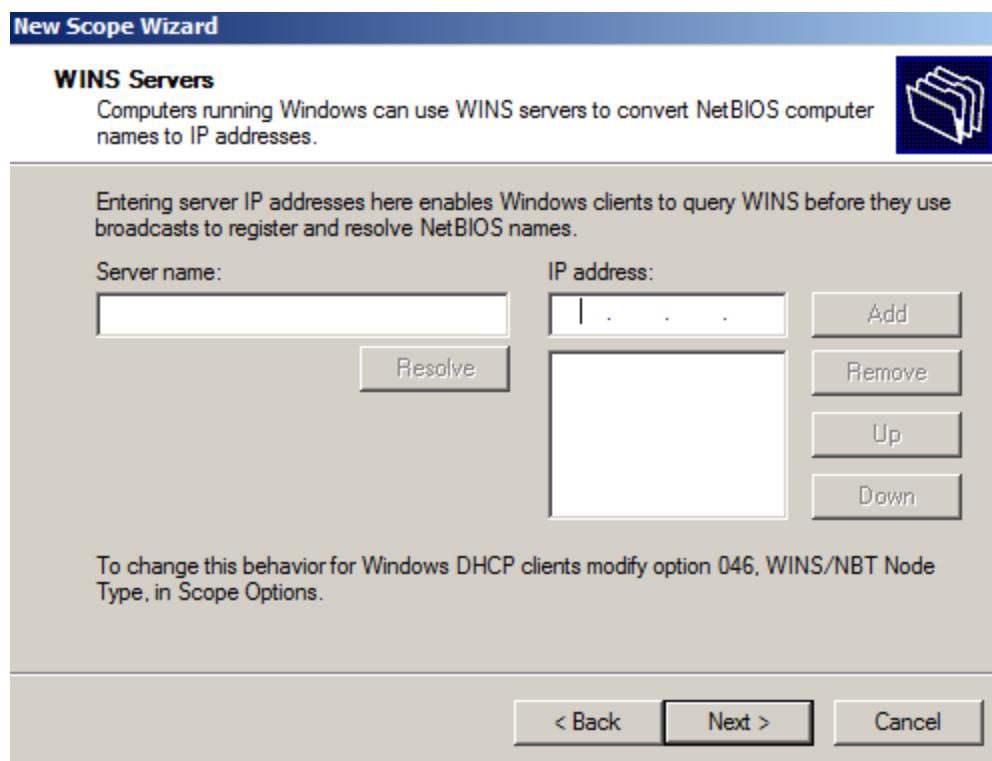


Hình 6.22: Cửa sổ ấn định địa chỉ IP Default gateway cho các máy khách

Nhấn Next, cửa sổ Hình 6.23 hiện ra cho phép ta nhập vào địa chỉ IP của các DNS server, các địa chỉ này sẽ báo cho DHCP server biết rằng, mỗi khi nó cho một máy khách thuê bao một địa chỉ IP từ scope này, thì nó cũng nên ấn định các địa chỉ IP của các DNS server cho máy khách đó chính là các địa chỉ IP của các DNS server được khai báo ở đây. Tuy nhiên cách này chỉ có tác dụng cho một scope đang tạo, dưới đây ta sẽ biết cách làm để có tác dụng cho tất cả các scope. Do vậy ở đây ta không cần đặt gì cả, nhấn Next để chuyển sang cửa sổ Hình 6.24.

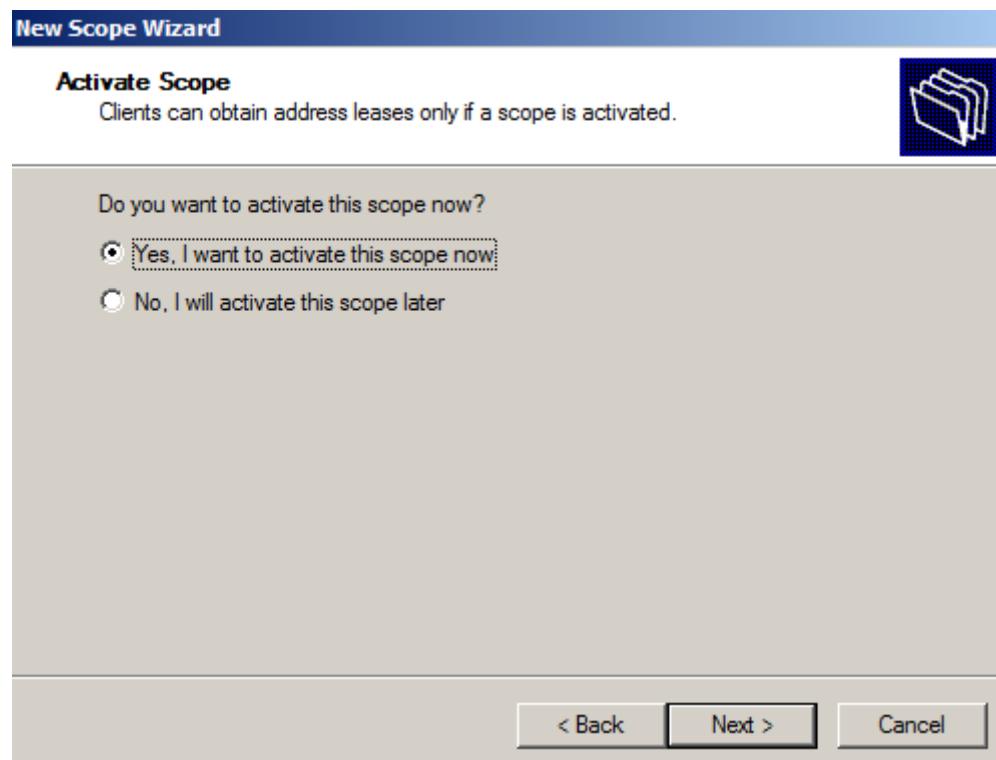


Hình 6.23: Cửa sổ xác định các DNS server



Hình 6.24: Cửa sổ xác định các WINS server

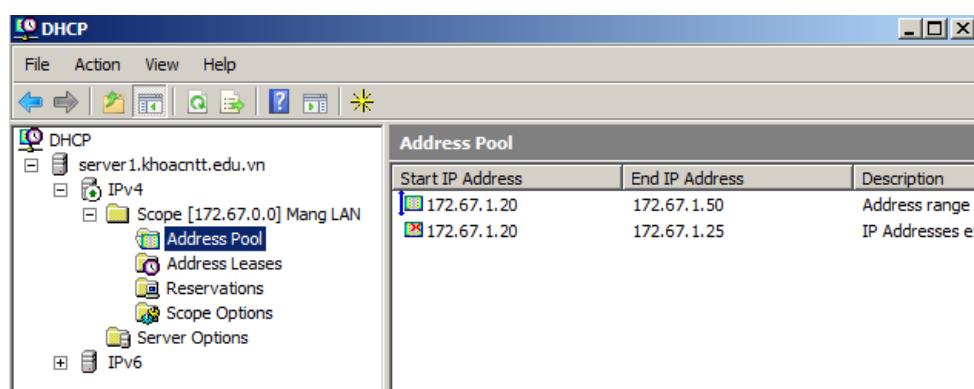
Đây là nơi báo cho các máy khách biết nơi cần tìm các WINS Server, trong trường hợp mạng còn có máy chủ NT. Tại đây ta không nhập gì, nhấn Next để chuyển đến cửa sổ Hình 6.25 cho phép chọn có đưa tầm vào hoạt động hay không.



Hình 6.25: Cửa sổ DHCP ban đầu

Tại đây ta chọn Yes, nhấn Next, rồi nhấn Finish tại cửa sổ cuối cùng để kết thúc việc tạo ra một tầm.

Cửa sổ DHCP khi có một tầm được tạo ra có dạng như hình sau:



Hình 6.26: Cửa sổ DHCP với một scope được kích hoạt

Ta thấy mỗi một tầm sẽ có bốn mục với ý nghĩa như sau:

Address Pool: cho biết phạm vi địa chỉ IP của tầm tại dòng có biểu tượng , còn các dòng có biểu tượng  là phạm vi những địa chỉ IP bị loại ra trong khi cấp động.

Address Leases: cho biết các địa chỉ IP đã được cấp.

Reservations: dùng để giữ chỗ trước các địa chỉ IP để cấp động cho các máy cụ thể.

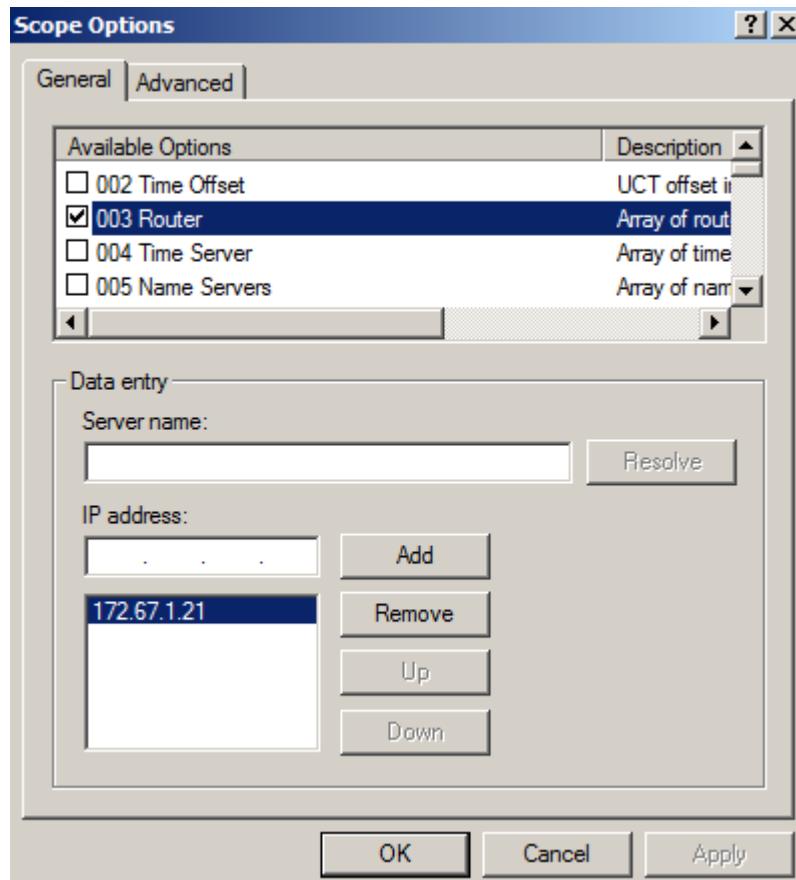
Scope Option: chứa các ấn định tùy chọn cấu hình mặc định DHCP trên máy khách.

Khi đã có các scope, để xoá một scope nào đó ta chỉ việc chọn nó rồi bấm phím Delete.

6.2.4. Ấn định các thông số tùy chọn cho tất cả các scope

Có rất nhiều thông số tùy chọn có thể ấn định cho tất cả các scope, ở đây ta chỉ đề cập tới cách ấn định các máy DNS server như đã nói đến ở Hình 6.23. Cách thực hiện như sau:

Nhấn phải chuột tại mục Server Options, chọn Configure Options để hiện ra cửa sổ sau:

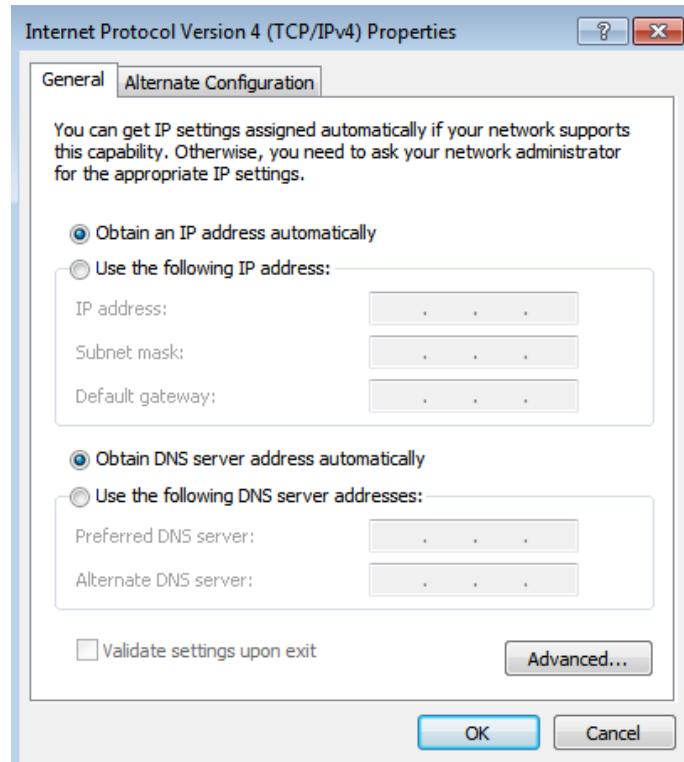


Hình 6.27: Cửa sổ Server Options

Tại đây ta đánh dấu tùy chọn 006 DNS Servers, rồi nhập vào địa chỉ IP của các máy DNS Servers tại ô: IP address.

6.2.5. Cấu hình dịch vụ DHCP bên máy khách

Trên các máy khách, nếu muốn cấu hình dịch vụ DHCP, thì ta lại mở cửa sổ thiết lập cấu hình TCP/IP. Sau đó chọn mục: Obtain an IP address automatically. Nếu địa chỉ IP của các DNS server đã được nhập trong cửa sổ 6.23 hoặc 6.27, thì ta cũng không cần nhập vào địa chỉ IP cho các máy này tại đây, mà chỉ cần chọn mục: Obtain an DNS server address automatically. Khi đó, mỗi khi DHCP server cho một máy khách thuê bao một địa chỉ IP, nó sẽ tự biết ấn định các địa chỉ IP của các DNS server đã được nhập trong cửa sổ 6.23 hoặc 6.27 cho máy khách đó.



Hình 6.28. Cửa sổ thiết lập cấu hình dịch vụ DHCP

6.2.6. Các bước nhận một địa chỉ IP từ DHCP server

Một máy khách có thiết lập cấu hình DHCP sẽ nhận một địa chỉ IP từ một DHCP server theo bốn bước sau:

1. Máy khách loan truyền khắp nơi một gói thỉnh cầu (request) DHCPDISCOVER đến tất cả các DHCP server trong tầm truyền của nó, thỉnh cầu được cấp một địa chỉ IP.
2. Các DHCP server hồi đáp bằng một gói đề nghị DHCPOFFER, chứa thông tin về các địa chỉ IP và thời gian cho thuê.
3. Máy khách chọn đề nghị nào hấp dẫn nhất, rồi truyền trả lại một gói DHCPREQUEST để xác nhận là muốn dùng địa chỉ ấy.
4. DHCP server đã đề nghị địa chỉ IP ấy sẽ trao địa chỉ IP ấy, rồi hoàn tất thủ tục bằng cách gửi trả lại một gói DHCPACK, tức là một gói chấp nhận yêu cầu đó.

6.3. TỔNG KẾT CHƯƠNG

Cài đặt, cấu hình, vận hành các dịch vụ mạng là một nghiệp vụ mà người quản trị cần hiểu kỹ và làm chủ. Các dịch vụ mạng phổ biến như dịch vụ DNS, dịch vụ DHCP, dịch vụ thư điện tử, dịch vụ Web, v.v. Trong phạm vi giáo trình, chương này đã tập trung trình bày hai dịch vụ là DNS và DHCP.

DNS là dịch vụ phân giải tên miền, có chức năng phân giải tên miền thành địa chỉ IP hoặc tìm kiếm tên khi biết địa chỉ IP. Có thể triển khai dịch vụ DNS trên một máy chủ riêng hoặc trên máy chủ điều khiển miền. DNS quản lý theo các dải địa chỉ IP gọi là các vùng (Zone). Mỗi DNS có thể có nhiều vùng tra cứu xuôi – tìm địa chỉ IP của tên và chỉ có một vùng tra cứu ngược – tìm tên tương ứng với địa chỉ IP. Trong DSN có các loại bản ghi phổ biến như: bản ghi địa chỉ (host), bản ghi tên máy chủ, bản ghi bí danh, v.v. Các hoạt động quản trị DNS bao gồm: cài đặt máy chủ DNS, tạo và quản lý các vùng, tạo và quản lý các bản ghi trong vùng, cấu hình dịch vụ DNS trên máy khách.

Dịch vụ DHCP cho phép cấp phát địa chỉ IP động khi các máy khách tham gia hệ thống mạng. Các hoạt động chính trong dịch vụ này bao gồm: cài đặt máy chủ DHCP, trao quyền hoạt động cho máy chủ DHCP, tạo phạm vi địa chỉ, cấu hình DHCP trên máy khách. Để quản lý tốt dịch vụ này, người quản trị cũng cần hiểu rõ quy trình yêu cầu và cấp phát địa chỉ IP động.

CÂU HỎI VÀ BÀI TẬP THỰC HÀNH

Câu 1. Để một DHCP domain member server có thể cấp phát thông số IP thì cần phải thực hiện hành động gì trước tiên, với quyền hạn của ai?

Câu 2. Trên một DHCP scope, khi nào cần khai báo các địa chỉ loại trừ (exclusion)?

Câu 3. Liệt kê code, name của 03 (ba) DHCP option. Scope từ 192.168.1.1 đến 192.168.1.200 có thể nhận các giá trị scope thế nào?

Câu 4. Trình bày quá trình giao tiếp giữa DHCP client và DHCP server để DHCP client nhận được thông số IP.

Câu 5. Administrator vừa cấu hình thêm 01 (một) option tại DHCP server. Cách đơn giản nhất để một máy trạm nhận được thông số mới?

Câu 6. Xác định ưu thế giữa 3 cấp option: reservation, server và scope.

Câu 7. Phân tích phát biểu này: “Không nên cấu hình option 003 ở cấp server option.”

Câu 8. Khi nào cần triển khai DHCP relay agent?

Câu 9. Trình bày quá trình giao tiếp giữa DHCP client – DHCP relay agent - DHCP server để DHCP client nhận được thông số IP.

Câu 10. Trình bày ý nghĩa của ô Preferred DNS Server.

Câu 11. Trình bày sự khác biệt giữa 2 loại DNS record: Start Of Authority(SOA) và Name Server(NS)

Câu 12. Trình bày sự khác biệt giữa 2 loại DNS record: Host(A) và Alias(CNAME)

Câu 13. Công dụng của Pointer (PTR) record?

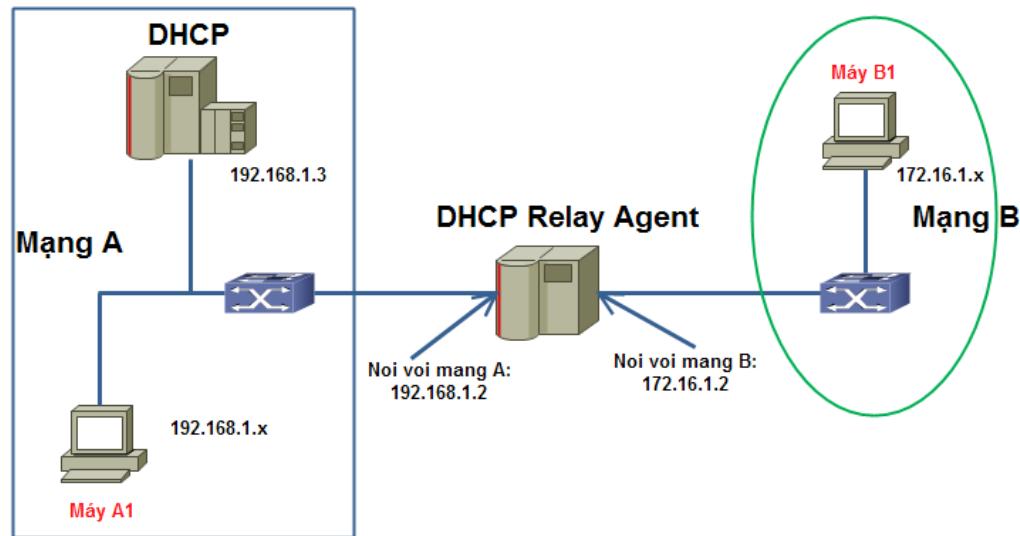
Câu 14. Công dụng của Mail Exchanger(MX) record?

Câu 15. Trình bày cách truy vấn để biết được tên và địa chỉ IP các DNS server của một domain.

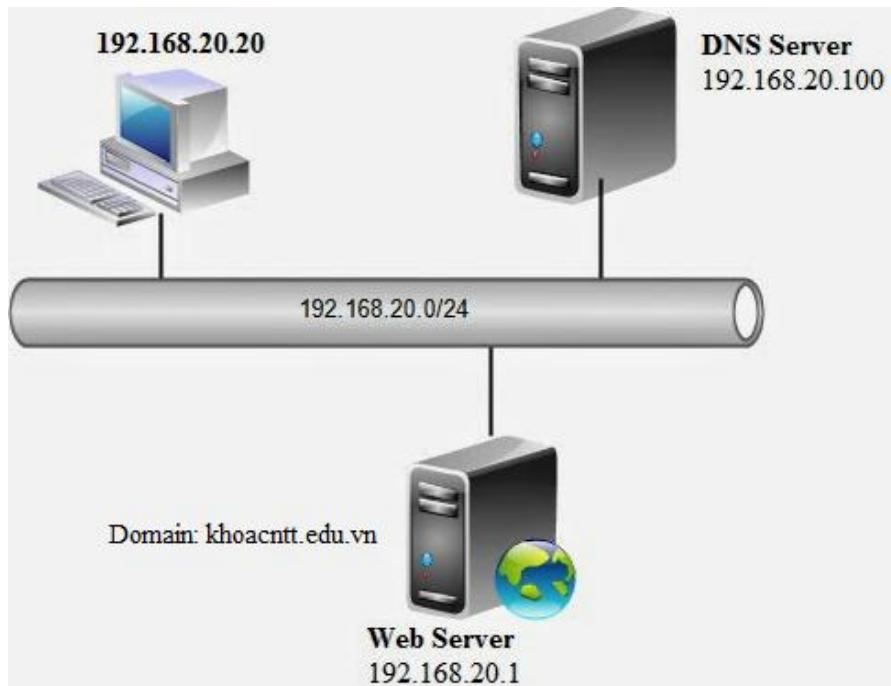
Câu 16. Trình bày cách truy vấn để biết được tên và địa chỉ IP primary DNS server của một domain.

Câu 17. Trình bày cách truy vấn để biết được tên và địa chỉ IP SMTP mail server của một domain.

Bài thực hành 1. Triển khai hệ thống mạng trên máy ảo và cấu hình DHCP theo mô hình sau:



Bài thực hành 2. Triển khai hệ thống mạng trên máy ảo và cấu hình DNS để phân giải tên miền + tên máy tính trong hệ thống theo mô hình sau.



CHƯƠNG 7.GIÁM SÁT HỆ THỐNG

Hệ thống mạng có thể hoạt động với khả năng cao ngay sau khi triển khai, tuy nhiên hiệu năng của mạng có thể giảm dần vì rất nhiều nguyên nhân. Để quản trị hệ thống tốt phải giám sát hiệu năng của máy chủ thường xuyên đều đặn để nhận biết và phát hiện các sự cố có thể ảnh hưởng đến hiệu năng cũng như các vấn đề an toàn, an ninh mạng. Chương này sẽ tập trung trình bày các hoạt động giám sát hệ thống trong quản trị mạng với các nội dung cụ thể sau: *Mục 7.1* trình bày về các kỹ năng giám sát máy chủ, *Mục 7.2* mô tả việc sử dụng tiện ích Task Manager trong giám sát mạng, *Mục 7.3* trình bày tiện ích Event Viewer, *Mục 7.4* mô tả cách sử dụng tiện ích Performance Console, và *Mục 7.5* tổng hợp các nội dung của chương.

7.1. CÁC KỸ NĂNG GIÁM SÁT MÁY CHỦ

Các công cụ giám sát hiệu năng máy chủ có trong Windows Server cho phép người quản trị có thể kiểm tra rất nhiều các tham số hệ thống theo rất nhiều cách khác nhau. Cách thức sử dụng các công cụ phụ thuộc vào các tài nguyên muốn giám sát... 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. Phương pháp này cung cấp các thông tin gần với hiện tại nhất.
- **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.

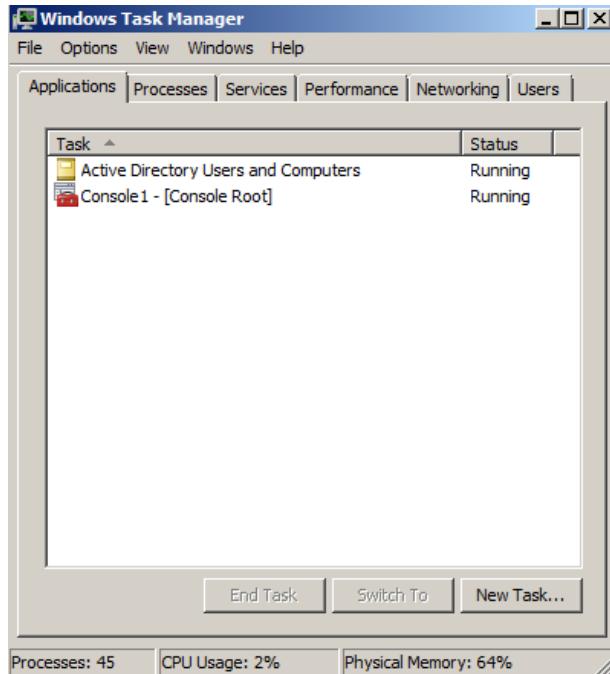
Cách thức sử dụng của việc giám sát thời gian thực và giám sát bằng nhật ký không có tính chất loại trừ nhau.

7.2. SỬ DỤNG TASK MANAGER

Task Manager (Trình Quản lý Tác vụ) là một ứng dụng quan trọng của Windows, 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.

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).

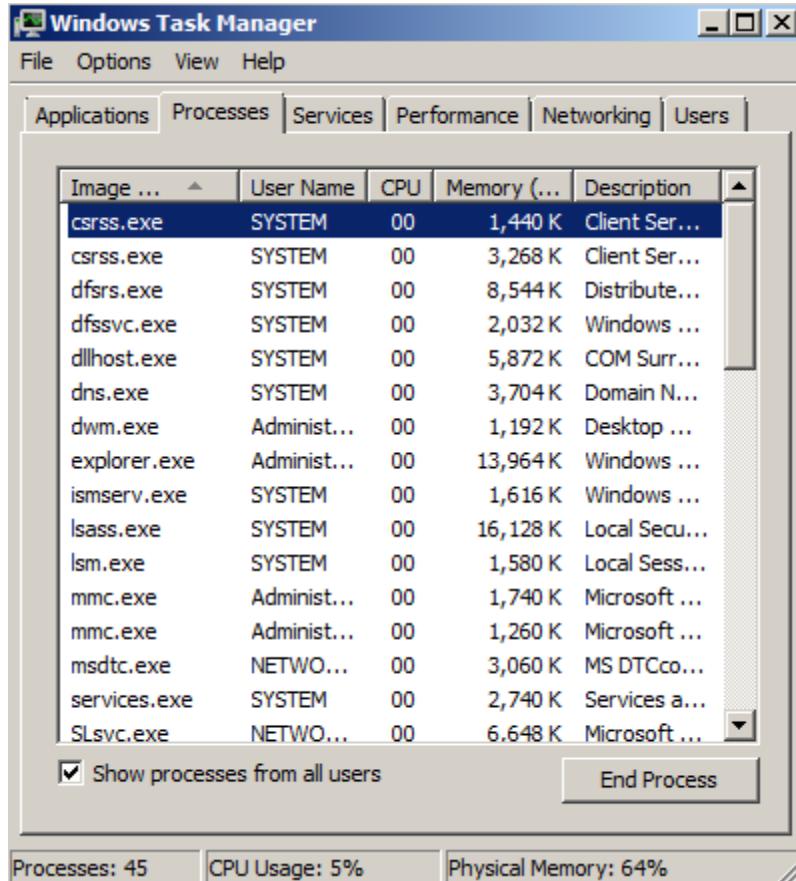
Làm việc với các ứng dụng: Thẻ Application chỉ ra trạng thái của các chương trình mức người dùng đang chạy trong hệ thống. Các dịch vụ và ứng dụng hệ thống chạy trong các ngữ cảnh khác với người dùng đang đăng nhập sẽ không hiển thị. Đối với các ứng dụng liệt kê ở đây, cột Status (Trạng thái) sẽ chỉ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



Hình 7.1: Giao diện thẻ ứng dụng

Thẻ Processes: liệt kê tất cả các tiến trình của các người dùng hiện tại đang chạy trên máy tính. Khi 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



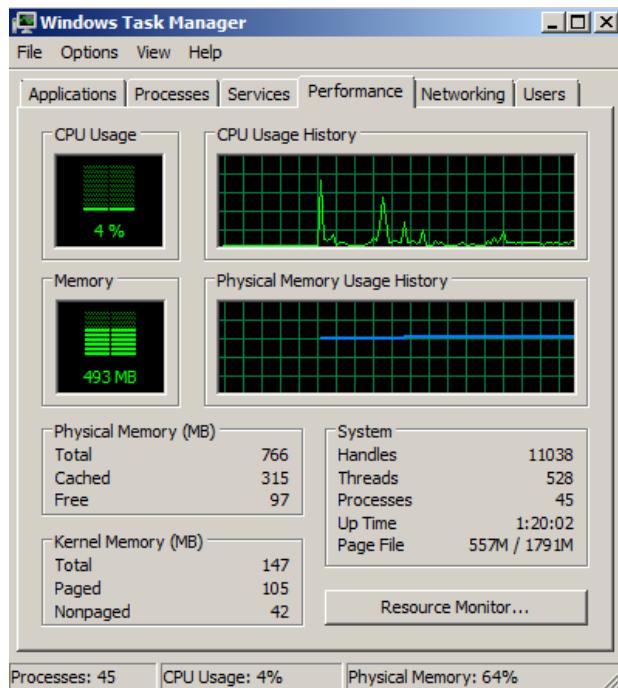
Hình 7.2: Giao diện thẻ Properties

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

- **Set Priority (Thiết lập mức ưu tiên):** Chính 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 Processor Afinity (Thiết lập mối quan hệ vi xử lý):** Chỉ định người dùng muốn chạy tiến trình bằng bộ vi xử lý nào trên một hệ thống máy tính có nhiều bộ vi xử lý.
- **End Process (Kết thúc tiến trình):** Dừng tiến trình ngay lập tức.
Mọi tài nguyên chưa lưu sẽ bị mất

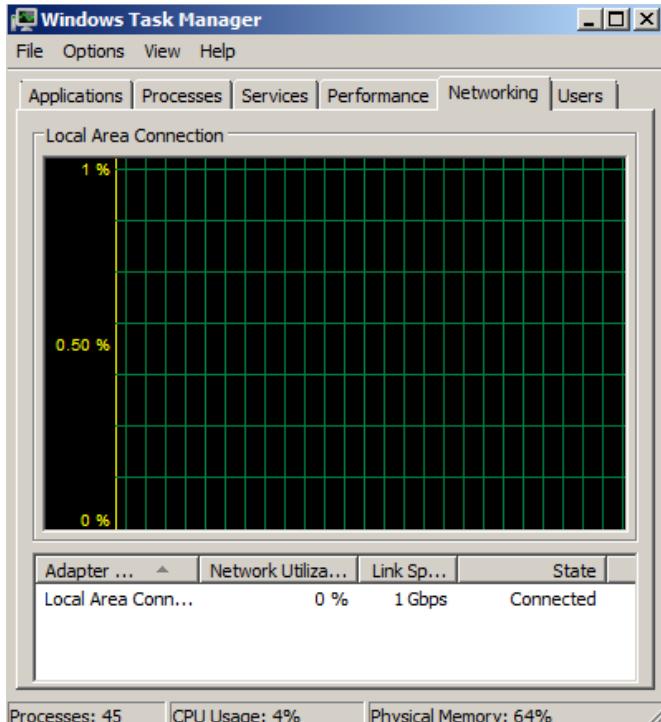
- **End Process Tree (Kết thúc cây tiến trình):** Dừng mọi tiến trình và các tiến trình con hoặc tiến trình liên quan ngay lập tức. Mọi dữ liệu chưa lưu sẽ bị mất.
- **Debug (Gỡ lỗi):** Tạo ra một trường hợp ngoại lệ để ngắt tiến trình và gắn nó với một trình gỡ lỗi được cài đặt trong hệ thống.

Thẻ Performance: 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.



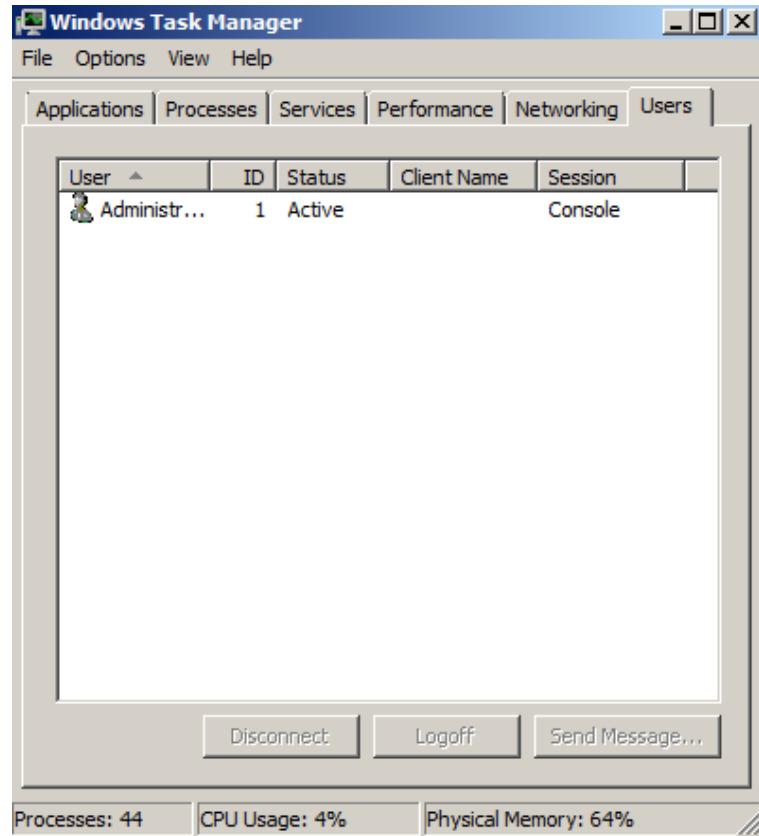
Hình 7.3: Giao diện thẻ Performance

Thẻ Networking: 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.



Hình 7.4: Giao diện thẻ Networking

Thẻ User: 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, có thể đăng xuất người dùng đó, ngắt kết nối của họ đến máy tính hoặc gửi thông báo cho họ.



Hình 7.5: Giao diện thẻ User

7.3. SỬ DỤNG EVENT VIEWER

Windows Server duy trì rất nhiều nhật ký chứa các thông tin về các tiến trình đang chạy. Để xem các nhật ký này, sử dụng snap-in Event Viewer (Trình xem sự kiện) trong MMC.

a. Các nhật ký trong Event Viewer

Khi nạp ứng dụng Event Viewer, 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 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 sinh ra, ví dụ như các dịch vụ hoặc trình điều khiển thiết bị.

- **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 (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, 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 người dùng 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.

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 (Directory 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.

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 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 có thể mở bằng bất kỳ trình soạn thảo văn bản nào.

b. Các kiểu sự kiện

Khi lựa chọn một trong các nhật ký liệt kê trong khung Phạm vi của snap-in Event Viewer, 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:

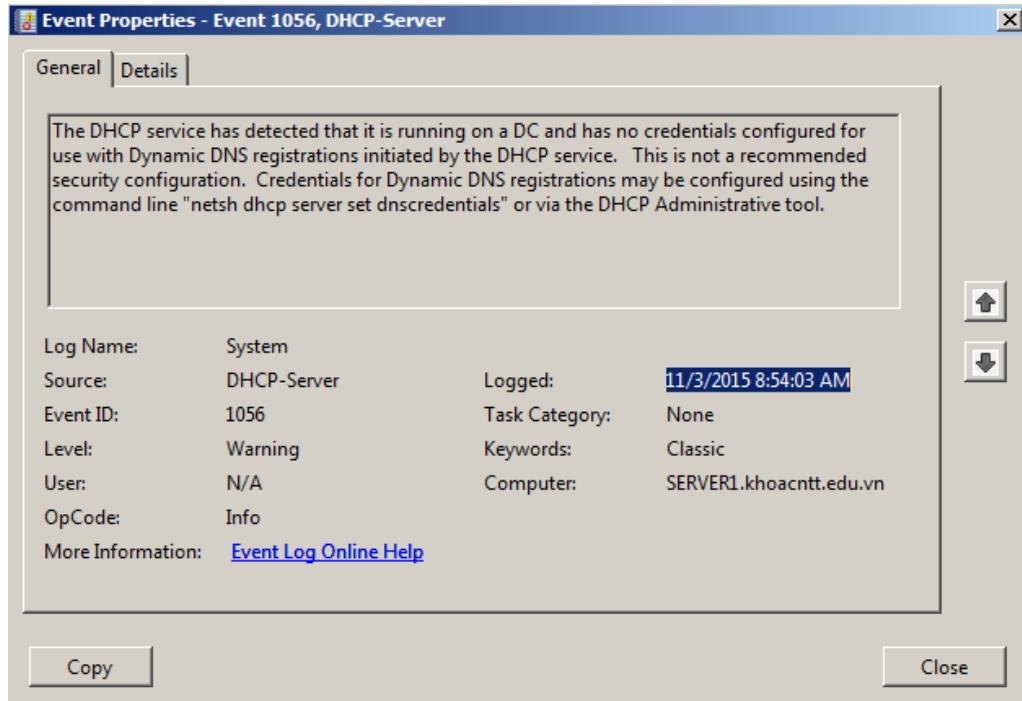
Kiểu sự kiện	Biểu tượng	Mô tả
Lỗi		Một sự cố có ý nghĩa quan trọng, ví dụ như mất dữ liệu hoặc sai chức năng
Cảnh báo		Một sự kiện có thể không có ý nghĩa nhưng có thể thể hiện một sự cố trong tương lai
Thông tin		Một sự kiện mô tả hoạt động thành công của một ứng dụng, trình điều khiển hoặc dịch vụ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

Hình 7.6: Một số kiểu sự kiện

Nhấn đúp vào một sự kiện trong khung Chi tiết của Event Viewer sẽ hiển thị hộp thoại thuộc tính của sự kiện đó, 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

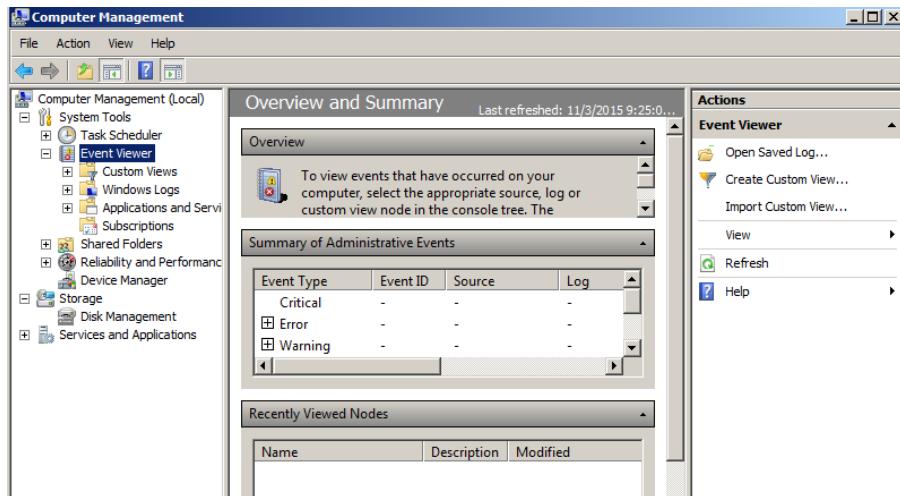
- Category (Hạng mục): Sự phân loại của sự kiện này, được định nghĩa bởi tiến trình nguồn
- Event ID (Mã số của sự kiện): Một giá trị đơn nhất để nhận biết sự kiện cụ thể này.
- Description (Mô tả): Một thông báo văn bản mô tả bản chất của sự kiện, được tạo ra bởi tiến trình nguồn
- Data (Dữ liệu): Dữ liệu nhị phân sinh ra bởi sự kiện



Hình 7.7:Dữ liệu sự kiện

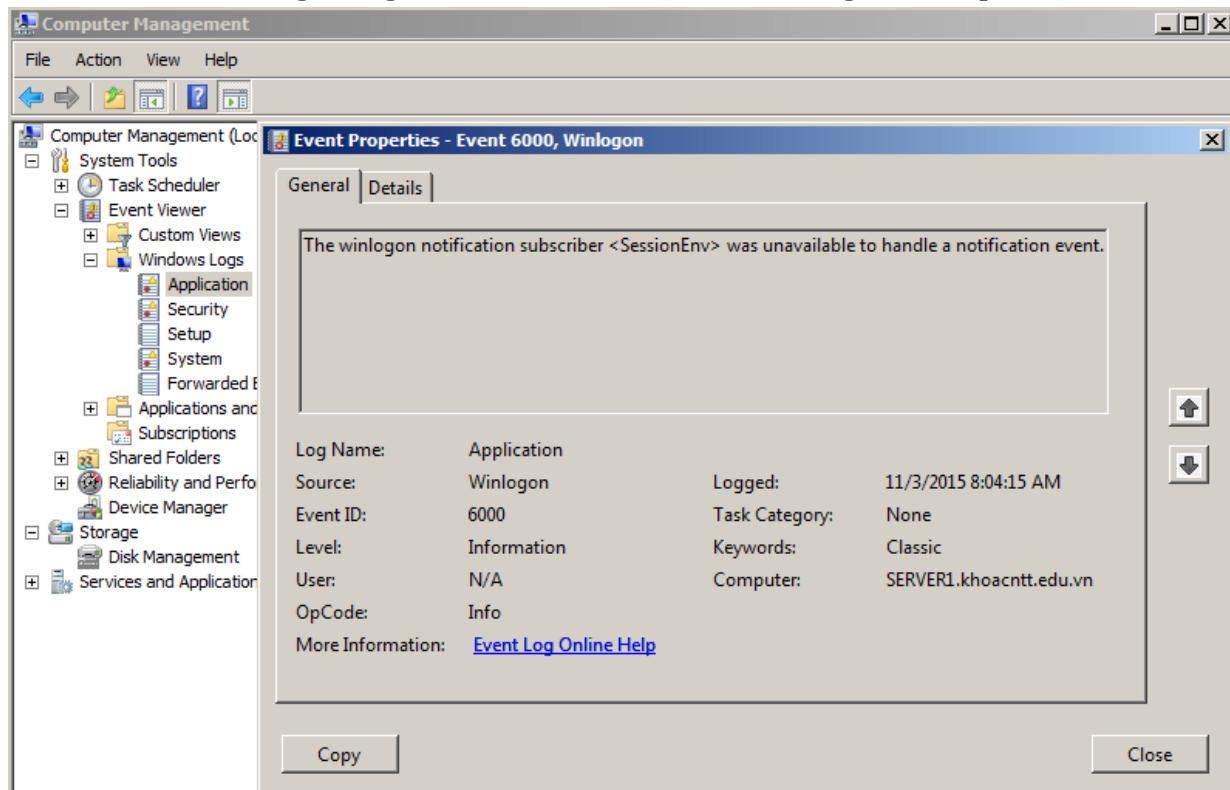
c. Phân tích file LOG

Cấu Trong Event viewer đã phân vùng các sự kiện riêng biệt cho từng ứng dụng, một máy chủ cài đặt mặc định sẽ có ba phân vùng trong event viewer: Application, Security và System.



Hình 7.8:Liệt kê các sự kiện

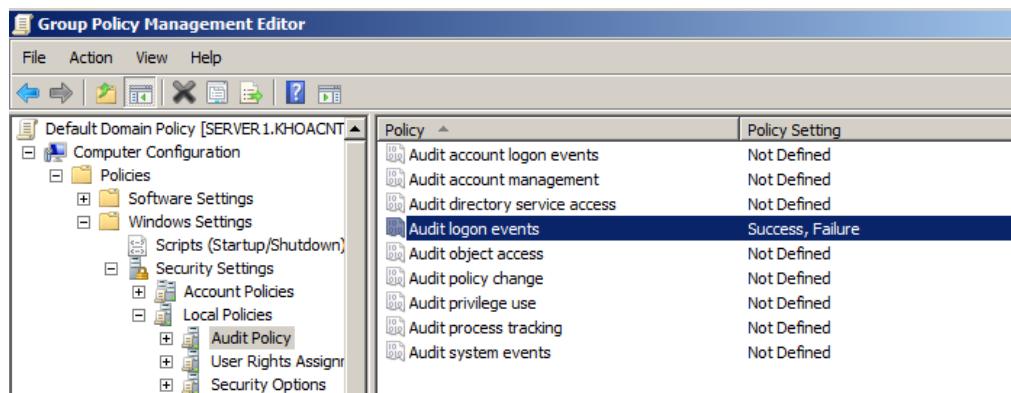
Application log: ghi lại sự kiện của các ứng dụng khác từ các nhà sản xuất khác như symantec hay các ứng dụng mail... Thường thiết lập trong application là mặc định của các ứng dụng nên chỉ có thể đọc mà không thiết lập được.



Hình 7.9:Nhật ký ứng dụng

Security log: Đây là một trong những log quan trọng nhất trong hệ thống, ghi lại toàn bộ các thiết lập audit trong group policy. Nhưng trong các thiết lập

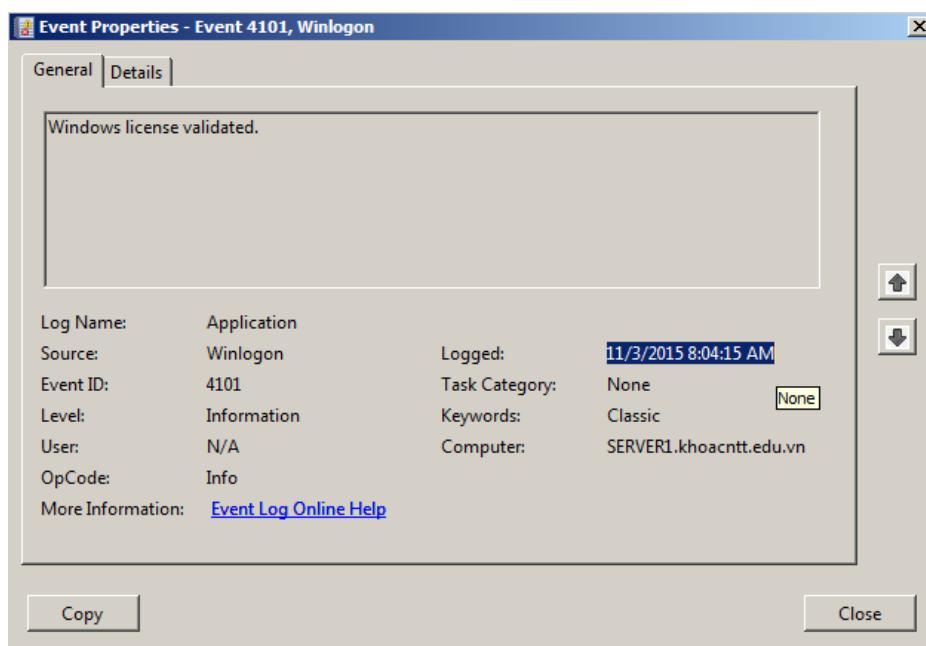
group policy quan trọng nhất là thiết lập giám sát quá trình login vào hệ thống, truy cập dữ liệu.



Hình 7.10:Nhật ký về an toàn

Ví dụ: Trong thiết lập này chỉ thiết lập giám sát quá trình truy cập login log-off hệ thống. Nếu với thiết lập như trên toàn bộ người dùng logon hay logoff vào hệ thống đều được ghi lại sau khi thiết lập trong group policy thì nên logoff hoặc restart lại máy bởi các thông tin chỉnh trong group policy bẩn chất là chỉnh các thông số trong registry.

Giờ đăng xuất và đăng nhập sẽ được ghi lại trong security log.



Hình 7.11:Nhật ký truy cập

Sau khi logon vào máy tính mở event viewer ra xem và phát hiện hệ thống đã lưu lại thông tin đăng nhập

Mục đích của việc xem lại log này là gì: Nếu dữ liệu trong máy của bạn đã bị mất và trong log ghi lại là đã được xoá lúc 12h đêm vậy cần quy trách nhiệm đó cho ai, file log sẽ cho biết trong thời điểm đó những ai đang online và logon, logoff trong thời gian đó.

Thiết lập giám sát một folder dữ liệu quan trọng, với yêu cầu đặt ra là giám sát toàn bộ các quá trình truy cập các action cụ thể với folder này. Trong ổ E có thư mục quan trọng DATA việc cần thiết của là đưa ra các thiết lập giám sát toàn bộ truy cập vào folder này.

Bước 1: thiết lập audit object access trong group policy ở cả chế độ success và fails

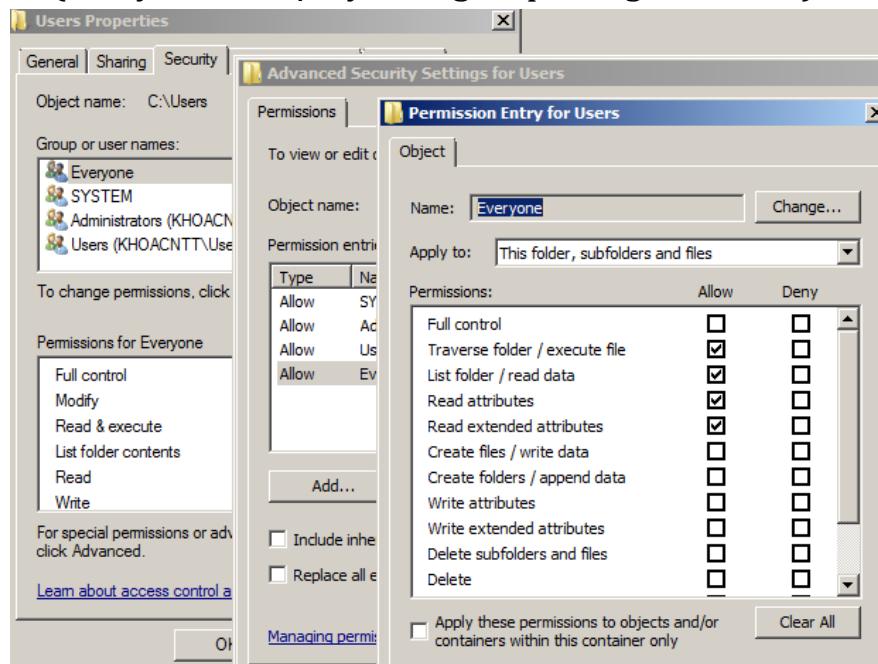


Hình 7.12: Thiết lập an toàn cục bộ

Với thiết lập trong group policy có nghĩa là chỉ enable tính năng cho phép hệ thống ghi lại mà thôi, mặc định hệ thống sau khi thiết lập này sẽ ghi lại event với các đối tượng hệ thống như registry... Còn muốn một quá trình truy cập vào folder mà được lưu lại thì phải thiết lập trên folder đó.

Bước 2: thiết lập audit trên folder

Nhấn chuột phải vào folder chọn properties sang tab security chọn advanced, chuyển sang tab audit chọn trong cửa sổ add tiến hành add group với tên là everyone (everyone là một system group trong Windows).

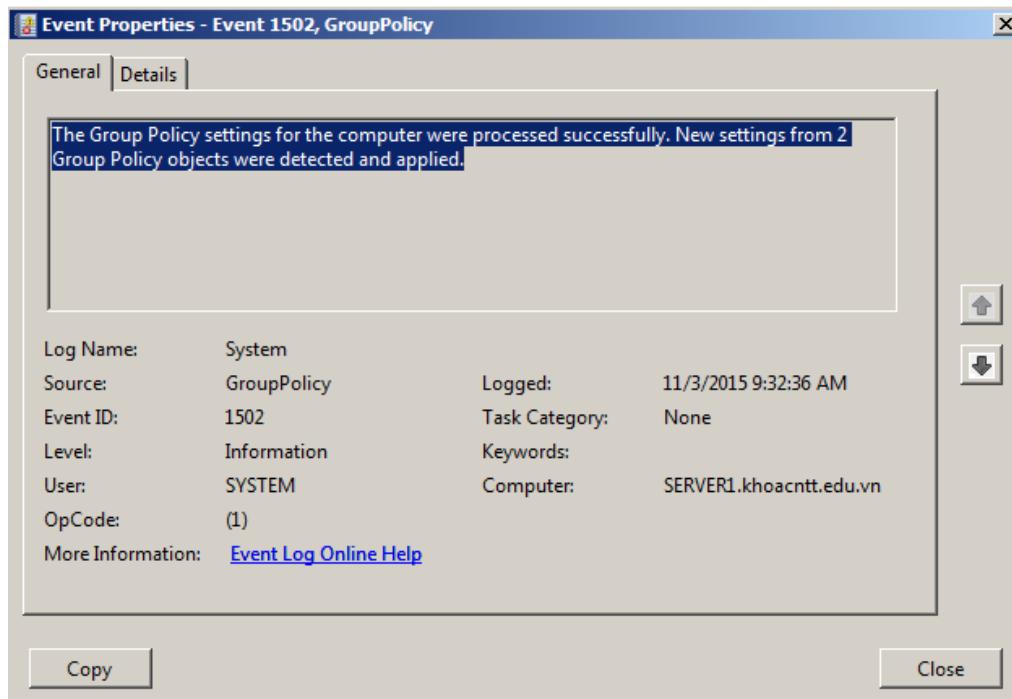


Hình 7.13: Thiết lập kiểm toán

Sau khi thiết lập restart lại máy và thử truy cập vào folder này xem trong event viewer có ghi các sự kiện với folder này không.

System Log: System log được thiết lập mặc định của hệ thống giúp người quản trị xem lại các sự kiện: Bật, tắt, pause, disable, enable các services của hệ thống.

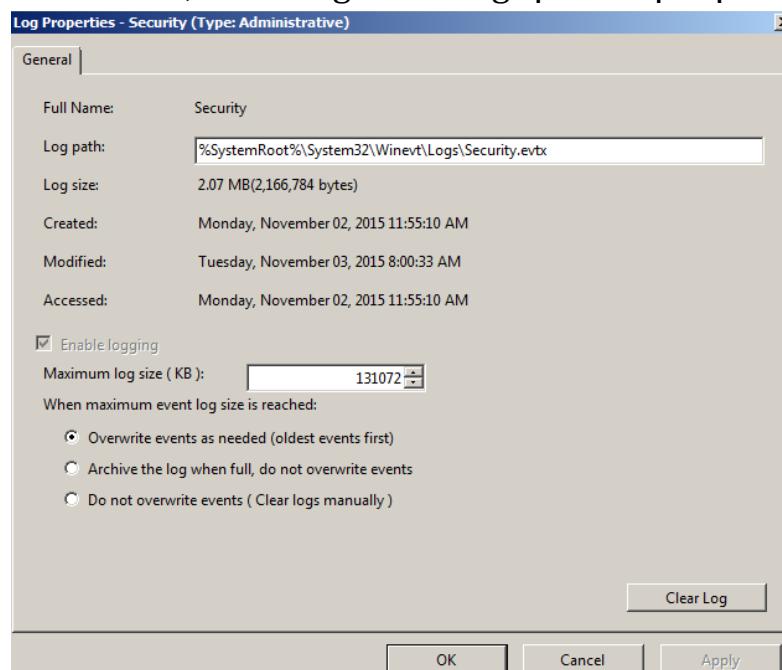
Ví như một service bật bị lỗi trong thời điểm nào nó sẽ ghi lại trong system log của event viewer.



Hình 7.14: Thông tin sự kiện

d. Log properties

Log properties giúp người quản trị cấu hình dung lượng file log, cách xoá các event cũ đi như thế nào, và những tính năng lọc các sự kiện.

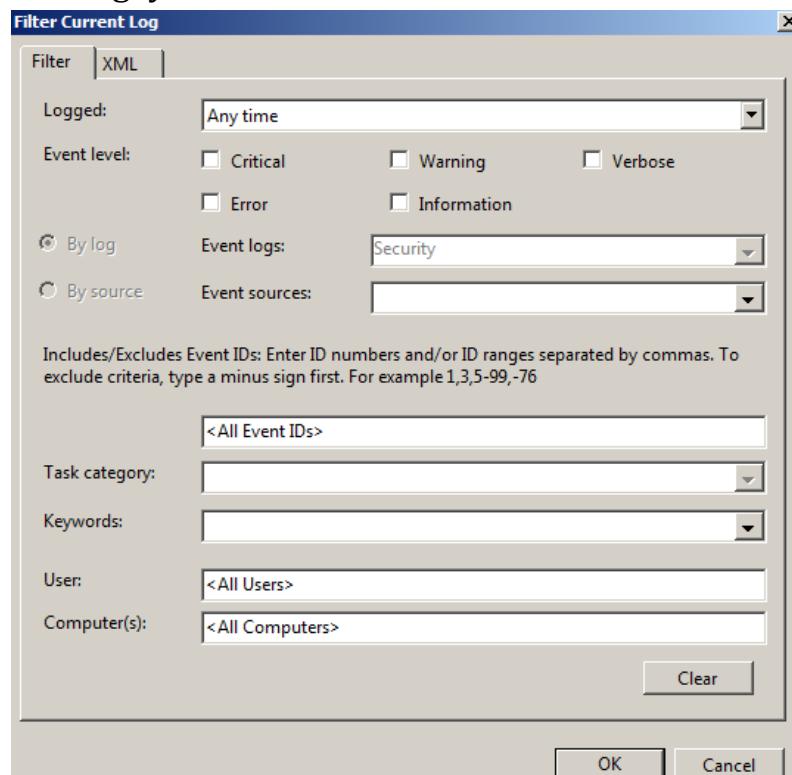


Hình 7.15: Thuộc tính nhật ký

Đây là thiết lập cho security properties: Với file log tên là gì và ở đâu: C:\Windows\System32\Config\SecEvent.Evt

Dung lượng tối đa cho file log này là 131072 KB, có thể cấu hình lại lớn hơn hoặc nhỏ hơn, nếu dung lượng file log lớn hơn 131072 KB hệ thống sẽ tự xoá các sự kiện cũ theo thuật toán First in First out

Nếu dung lượng chưa được 131072KB nhưng với thiết lập mặc định các event sẽ bị xoá sau 7 ngày.

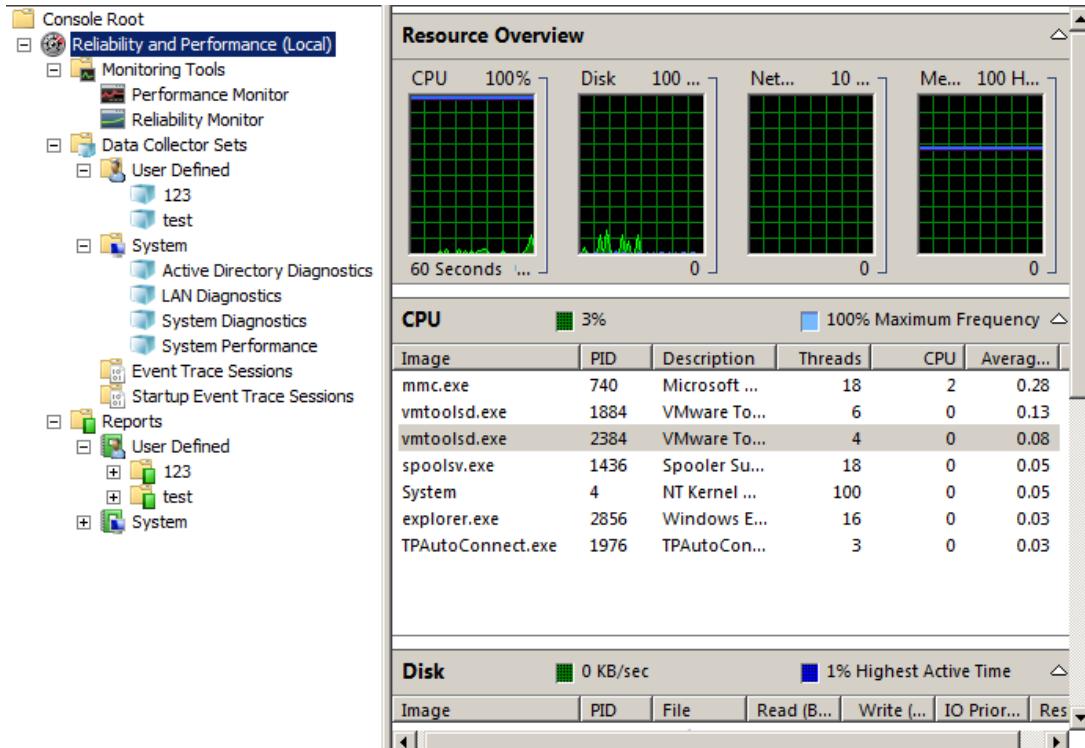


Hình 7.16:Thuộc tính an toàn

Trong tab này với khi chưa cấu hình lọc mặc định sẽ hiển thị toàn bộ các sự kiện bạn có thể lọc chỉ hiển thị theo "event types: như information, waring, erro, success audit, hay failure audit". Hoặc có thể thiết lập lọc các sự kiện theo thời gian và ID của các sự kiện.

7.4. SỬ DỤNG PERFORMANCE CONSOLE

Performance console (Bảng điều khiển hiệu năng) là một trong những công cụ giám sát mạnh nhất trong Windows Server. Bảng điều khiển này cho phép giám sát hiệu năng làm việc của hệ thống



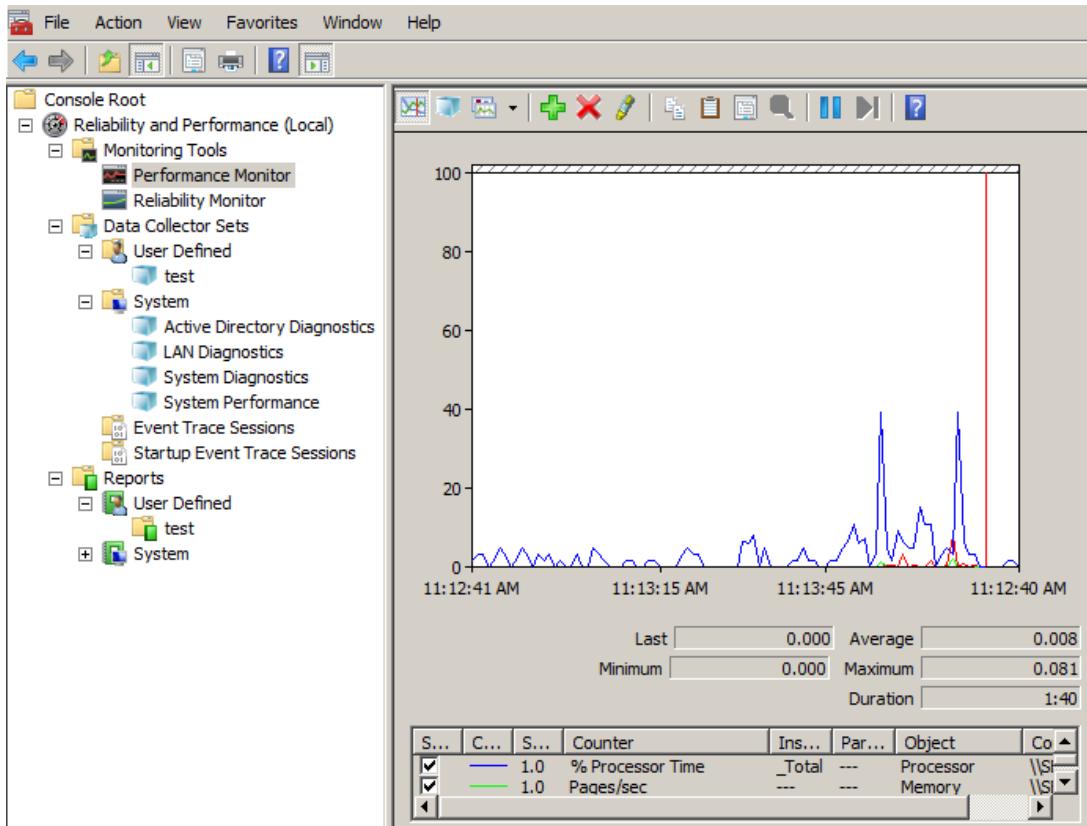
Hình 7.17: Thông tin theo dõi hiệu năng làm việc của hệ thống

a. Sử dụng Monitoring Tools (Giám sát hoạt động)

Khi mở Bảng điều khiển Performance, theo mặc định thì snap-in System Monitor (Giám sát hệ thống) xuất hiện. Khung Chi tiết của snap-in có một đồ thị dạng đường, được cập nhật theo thời gian thực, cho 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 xảy 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 (working 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.

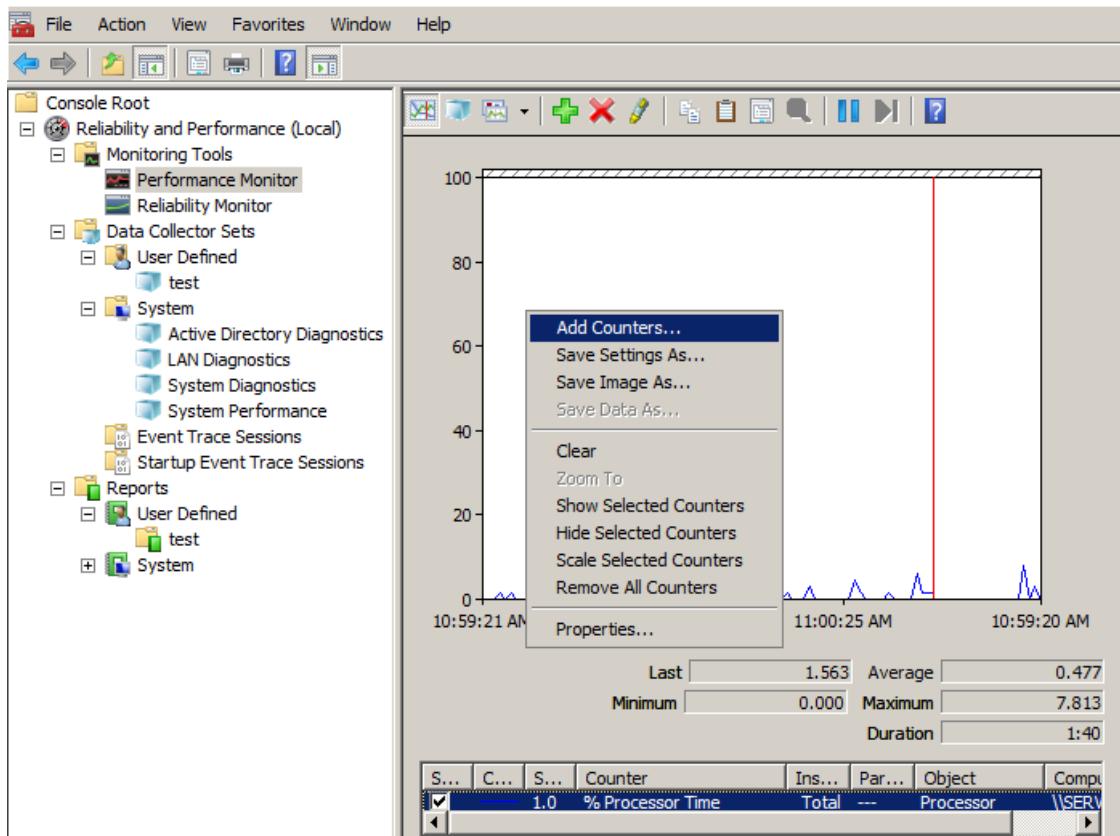


Hình 7.17: Thông tin hiệu năng

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.

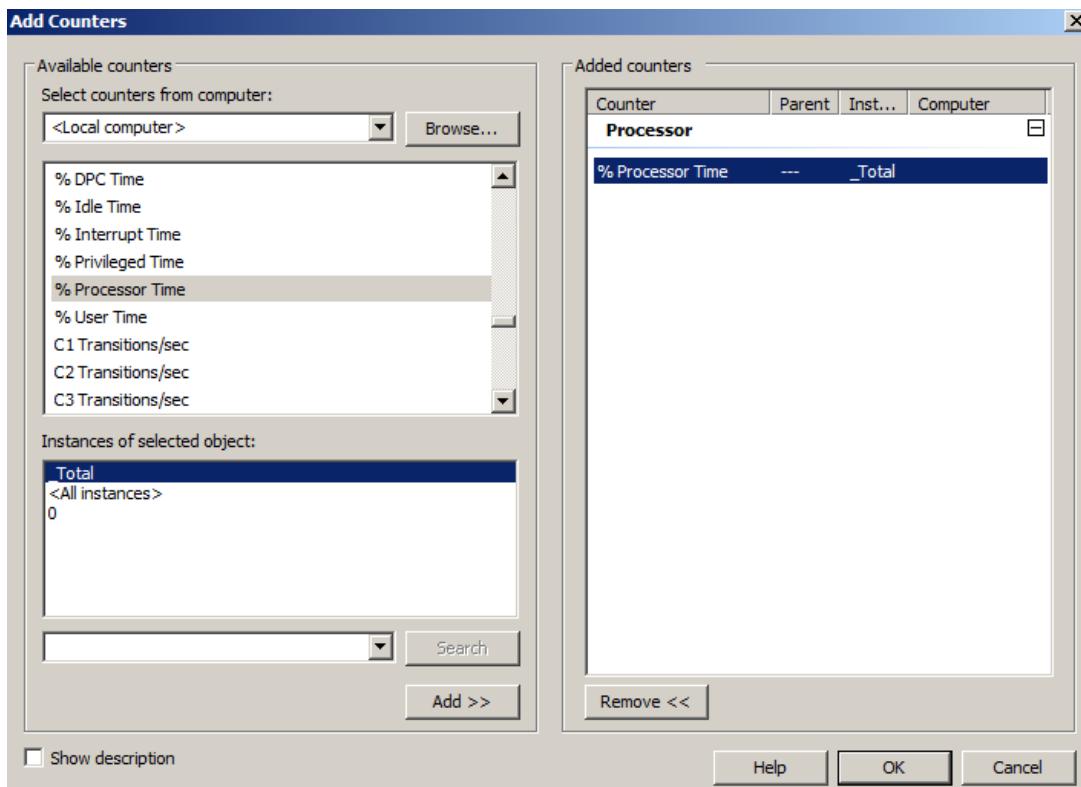
b. Counter Logs (Nhật ký các biến đếm).

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. Counter log ngoài việc cho người dùng giám sát trực tiếp counter của đối tượng cụ thể mà còn cho phép ghi lại với những thiết lập cụ thể, cửa sổ counter log nhấn New Log Setting.



Hình 7.18:Nhật ký biến đếm

Sau khi tạo ra một log file bạn thiết lập add các counter, như tên của log này là Log %Processor time của CPU nên nhấp vào add counter trong cửa sổ log setting. Nếu chọn vào add object thì hệ thống tự động add toàn bộ các counter của object đó.



Hình 7.19:Cấu hình nhật ký

7.5. TỔNG KẾT CHƯƠNG

Nghiệp vụ giám sát hệ thống đóng vai trò quan trọng trong quản trị mạng. Các thông tin về người dùng, tài nguyên, hệ thống, v.v. là cơ sở để người quản trị phân tích, đánh giá để thực hiện các hoạt động duy trì tính ổn định của hệ thống, cải thiện hiệu năng, đảm bảo an toàn và an ninh mạng. Nội dung chương này đã trình bày các hoạt động chính trong nghiệp vụ giám sát hệ thống là sử dụng tiện ích Task Manager, sử dụng Event Viewer và Performance Console.

Windows Server cho phép người quản trị thực hiện hai kỹ năng giám sát máy chủ là giám sát thời gian thực và giám sát nhật ký.

Trình quản lý tác vụ Task Manager là một tiện ích quan trọng của Windows, cho phép thống kê và quản lý thông tin các đối tượng trong hệ thống như: các chương trình (applications), các tiến trình (processes), hiệu năng hệ thống, hoạt động mạng và người dùng.

Tiện ích Event Viewer hoạt động như một trình quản lý nhật ký sự kiện của toàn bộ hệ thống. Các lỗi, các cảnh báo, thông tin truy xuất, v.v. đều được Event Viewer thống kê, quản lý. Tiện ích lưu nhật ký sự kiện liên quan đến ba vấn đề chính là ứng dụng, hệ thống và các vấn đề bảo mật. Đồng thời, tiện ích cũng có chức năng phân tích nhật ký (log) giúp việc giám sát hiệu quả hơn.

Tiện ích Performance Console hoạt động như một bảng điều giám sát và điều khiển hiệu năng. Tiện ích này có hai chức năng chính là: giám sát hệ thống – thống kê và quản lý mọi thông tin liên quan đến hiệu năng như CPU, bộ nhớ, và các tài nguyên khác; phân tích nhật ký và cảnh báo hiệu năng.

CÂU HỎI VÀ BÀI TẬP THỰC HÀNH

Câu 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?

Câu 2. 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?

Câu 3. Tại sao một số các Biến đếm hiệu năng trong **Monitoring Tools** lại có nhiều trường hợp riêng (*instance*) khác nhau?

Bài thực hành 1. Giám sát thao tác người dùng trên một tập tin/thư mục Trên ổ đĩa D: của máy File Server, Anh/Chị đã có chia sẻ thư mục Public cho mọi người dùng. Anh/Chị cần giám sát các thao tác xóa dữ liệu của người dùng TRONG trên thư mục này.

TÀI LIỆU THAM KHẢO

I. Sách tham khảo

1. "Configuring Windows Server 2008 Active Directory"; Dan Holme, Nelson Ruest, Danielle Ruest; 2008.
2. "Configuring Windows Server 2008 Network Infrastructure"; J.C. Mackin and Tony Northrup; 2008.
3. "Configuring Windows Server 2008 Applications Infrastructure"; J.C. Mackin and Anil Desai; 2008.
4. "Windows Server 2008_ Server Administrator"; Ian McLean and Orin Thomas; 2008.
5. "Windows Server 2008_ Enterprise Administrator"; Orin Thomas, John Policelli, Ian McLean, J.C. Mackin, Paul Mancuso, and David R. Miller, with GrandMasters; 2008
6. "Configuring Microsoft Windows Vista Client"; Ian McLean and Orin Thomas; 2008
7. "Giáo trình Quản trị Windows Server 2003"; Trần Văn Thành – Đại học Quốc Gia Tp.HCM.

II. Website tham khảo

1. <http://www.nhatnghe.com>
2. <http://www.athena.com.vn>
3. <http://www.netpro.com.vn>
4. <http://www.microsoft.com>

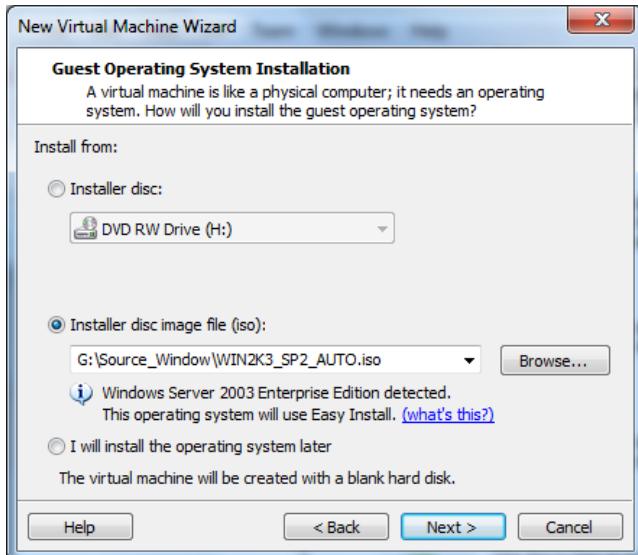
PHỤ LỤC A. TRIỂN KHAI HỆ THỐNG MẠNG TRÊN CÁC MÁY ẢO

A.1. Tạo máy ảo với VMWare

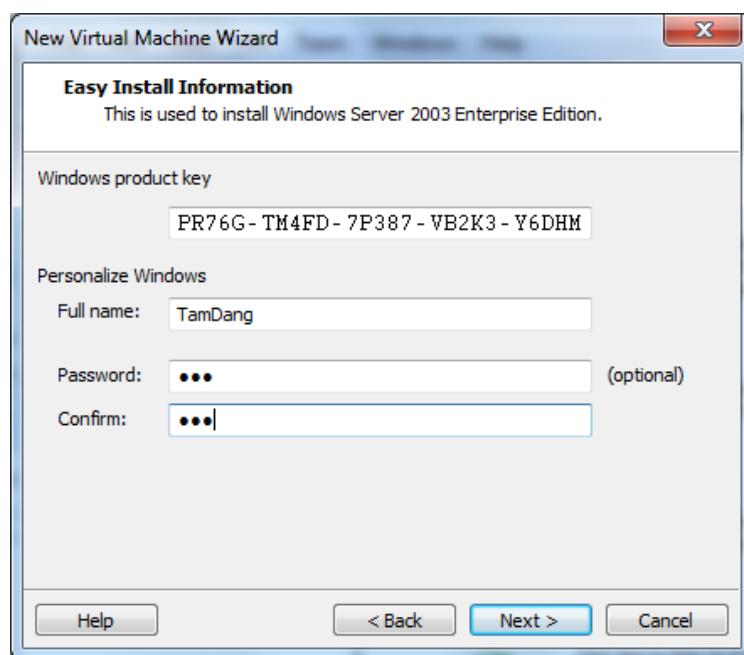
Trang HOME> New Virtual Machine



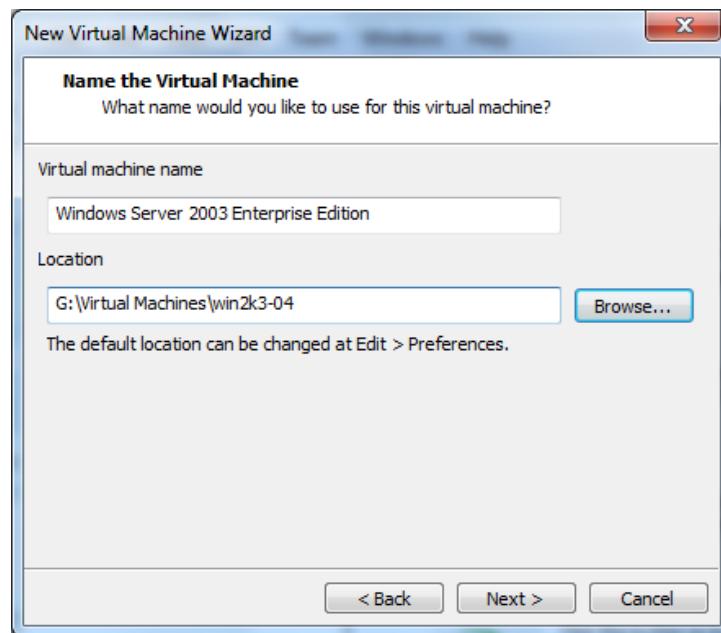
Nếu các hệ điều hành dự định cài đặt lên máy ảo thuộc loại phổ dụng thì VMWare hỗ trợ cài đặt không giám sát bằng cách chọn Typical rồi điền các thông số vào cần thiết vào trước.



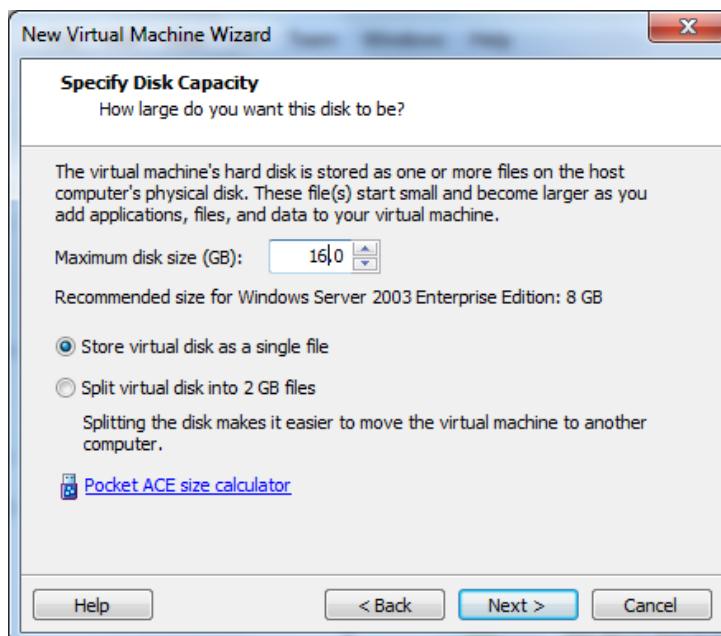
Số CD-Key

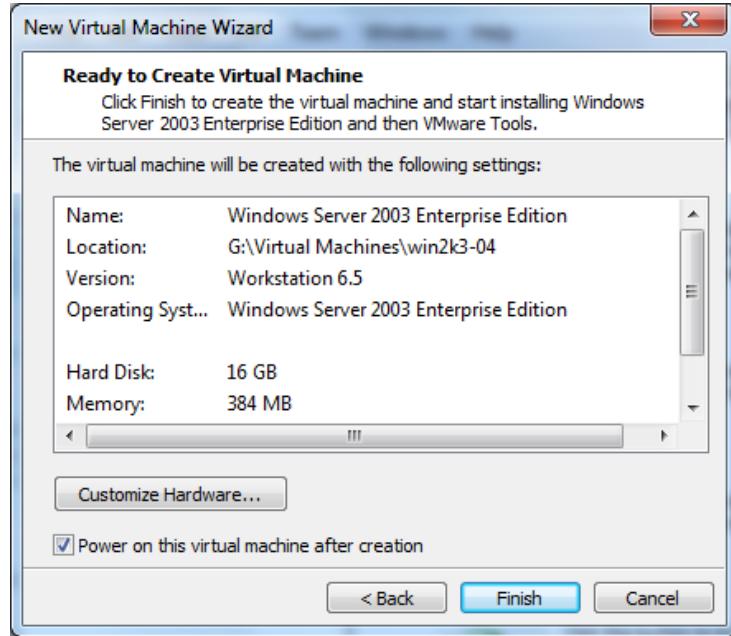


Chọn nơi lưu



Định dung lượng ổ đĩa. Nếu dung lượng đĩa hơn 2 GB, có thể lựa chọn lưu thành 1 file để dễ quản lý.



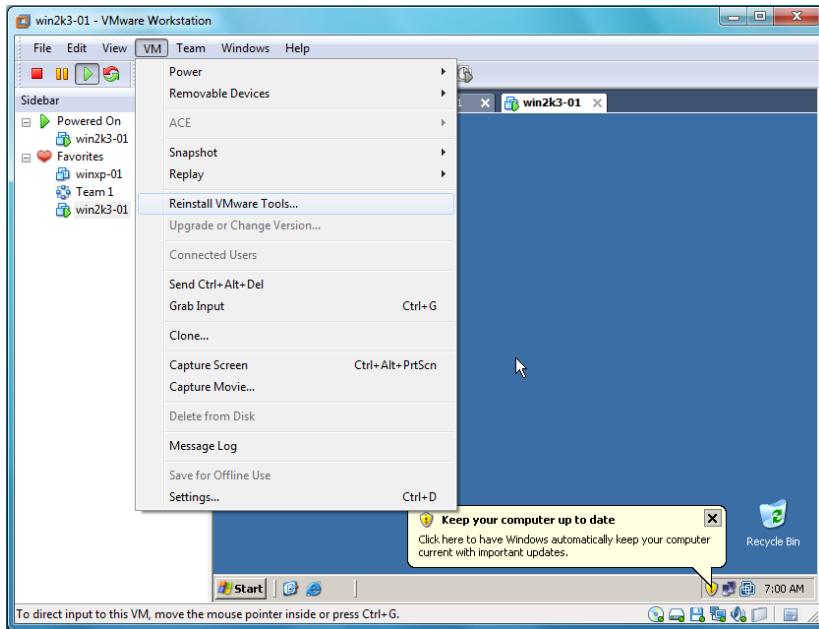


Trong trường hợp hệ điều hành cài đặt không thuộc loại phổ dụng thì nên chọn phần Custom rồi thiết lập các thông số cấu hình phù hợp cho máy ảo.

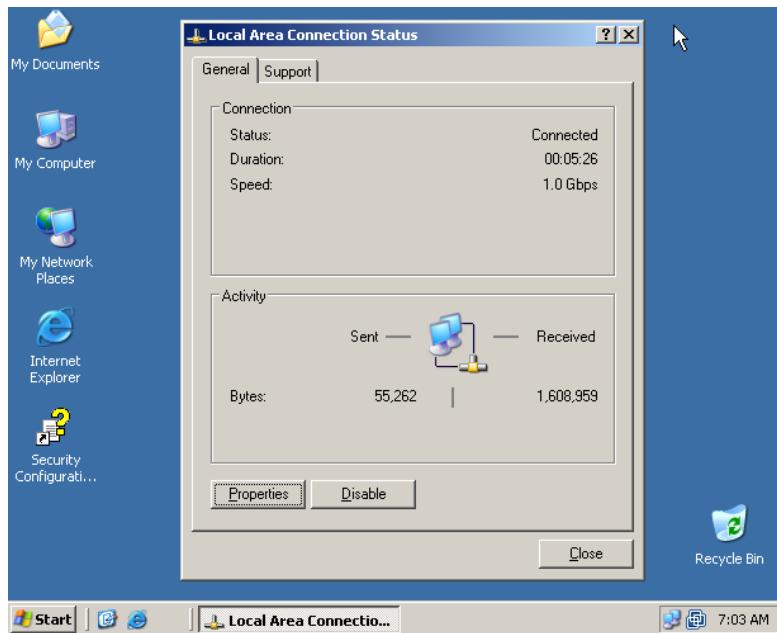
Với máy ảo VMWare, các phím thao tác được quy định như máy thật. Ví dụ muốn hiện của sổ Logon trong Windows Server trong máy ảo cũng nhấn Ctrl + Alt+ Del như máy thật.

A.2. Quản lý cấu hình phần cứng

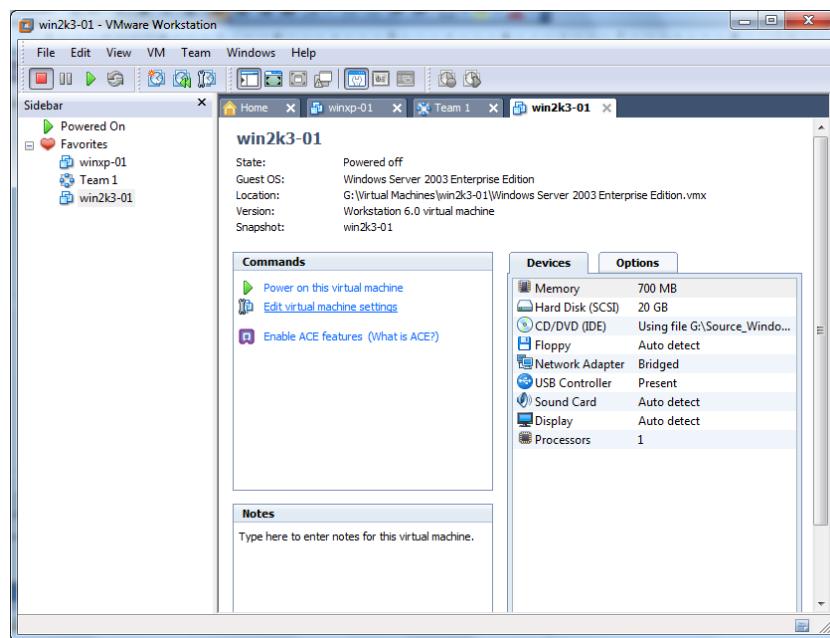
Để máy ảo hoạt động tối ưu hơn, sau khi cài đặt hệ điều hành cho máy ảo xong nên cài vào máy ảo bộ công cụ VMWare Tool. Khởi động máy ảo lên, chọn vào menu **VM** chọn **Install VMWare Tool**



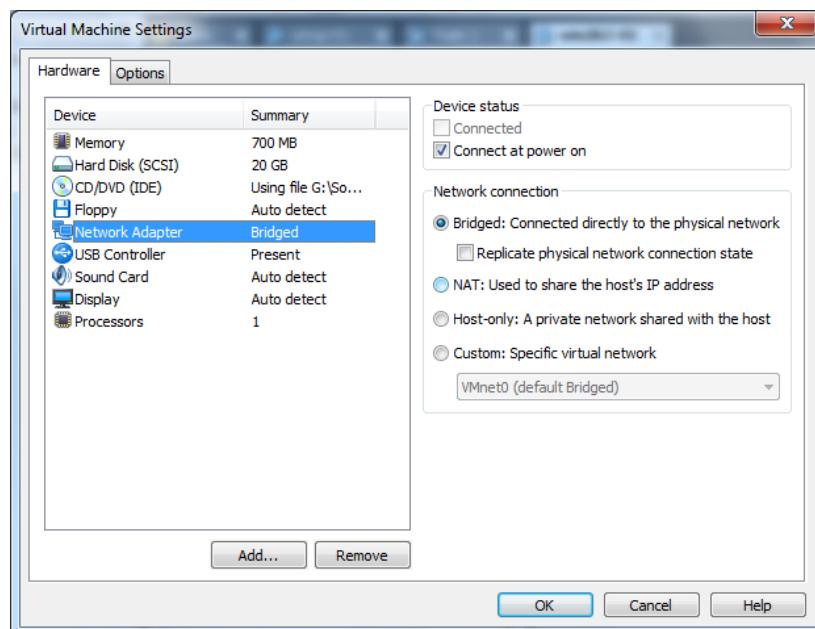
Cài đặt xong góc dưới bên tay phải của màn hình máy ảo sẽ có biểu tượng VMWare Tool. Các phần cứng đã được tối ưu dựa theo cấu hình phần cứng máy thật (card mạng tốc độ lên 1.0 Gbps)



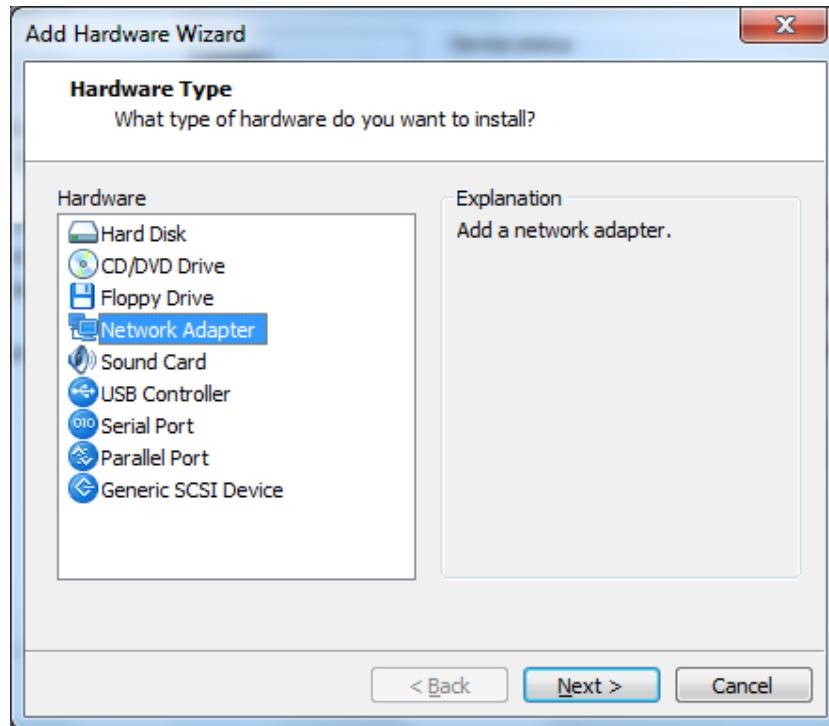
Ngoài ra trong máy ảo, các bạn có thể chỉnh sửa cấu hình phần cứng như thêm card mạng, ổ đĩa cứng v.. v.. Nhưng trong quá trình chỉnh sửa bạn phải tắt máy ảo, trong cửa sổ máy ảo bạn chọn Edit Virtual machine setting.



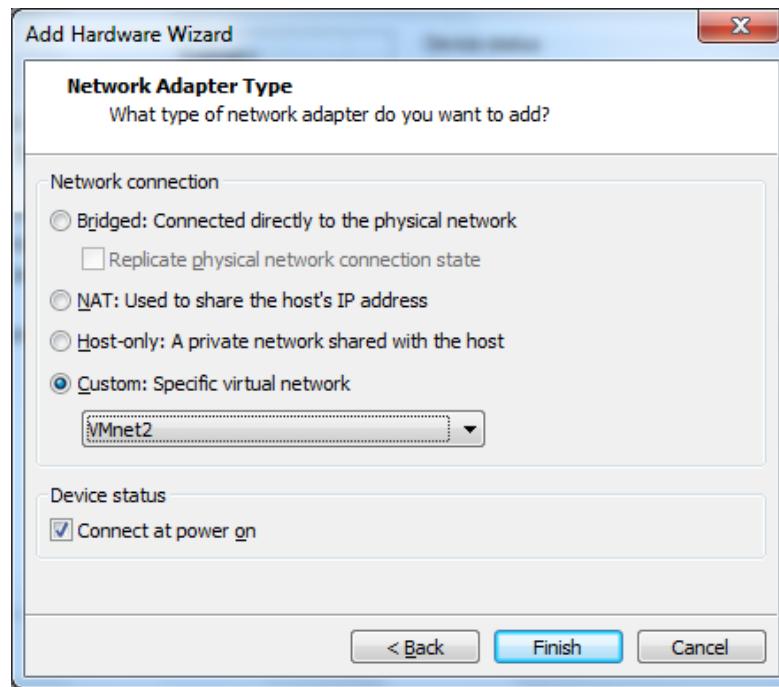
Giả sử trong trường hợp này ta muốn thêm card mạng. Trong cửa sổ Virtual Machine Settings> tab Hardware> Add



Chọn Network Adapter

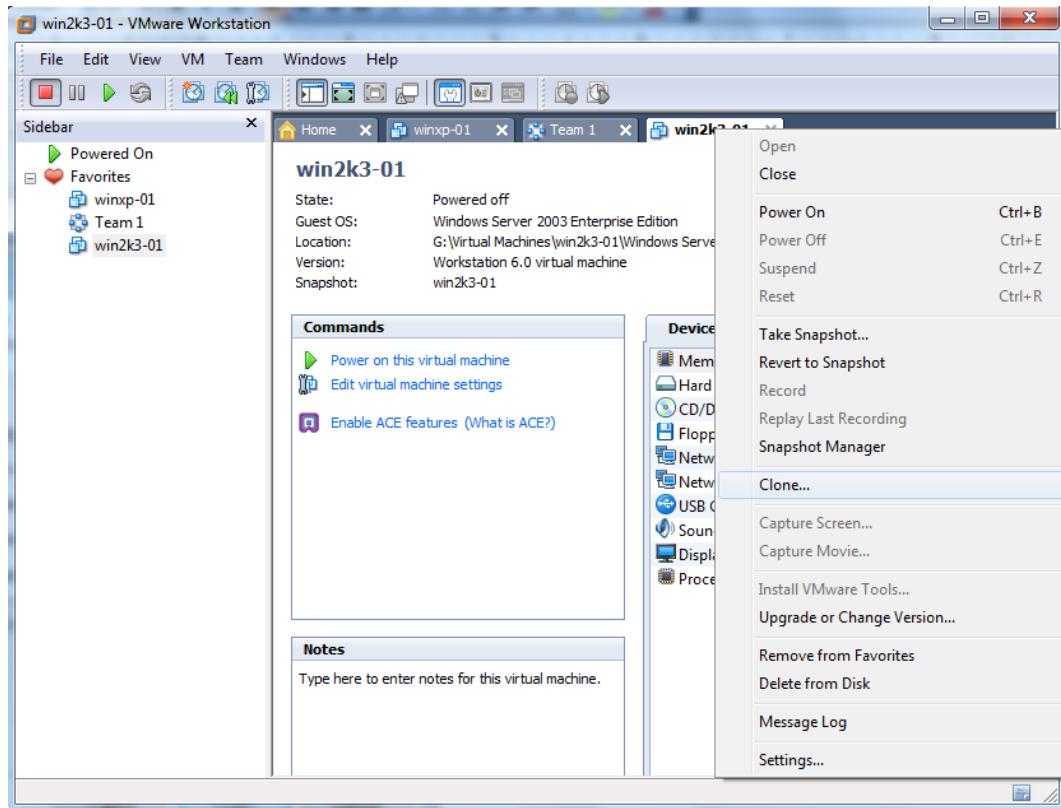


Chọn VMnet muốn kết nối và Finish



A.3. Nhân bản máy ảo

Khi cần nhiều máy ảo để xây dựng mô hình mạng máy tính, mà các máy ảo cấu hình và hệ điều hành tương tự nhau thì có thể lựa chọn nhân bản máy ảo đã cấu hình và cài đặt phần mềm đầy đủ thay vì phải cài đặt lại 1 máy ảo mới hoàn toàn. Để thực hiện chọn vào máy ảo đã có, click phải chọn **Clone**.

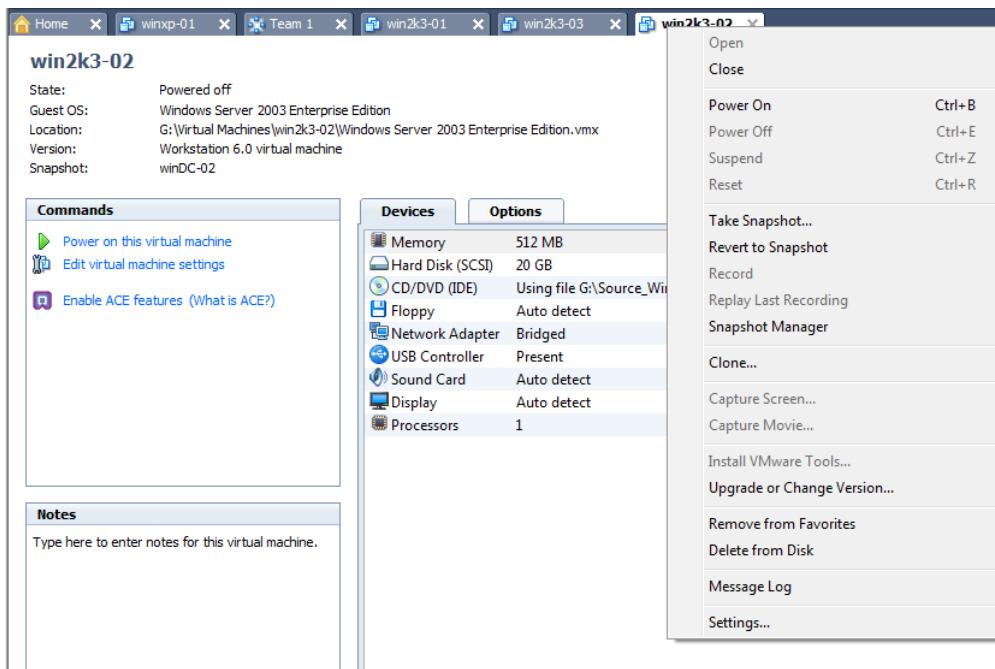


Chọn nơi đặt bản sao lưu. Máy nhân bản hoạt động như máy gốc, nhưng cần chú ý phải đổi computername và IP để tránh xung đột với máy gốc. trong trường hợp muốn join cả 2 máy vào domain thì cần phải đổi số SID của máy nhân bản cho khác máy gốc.

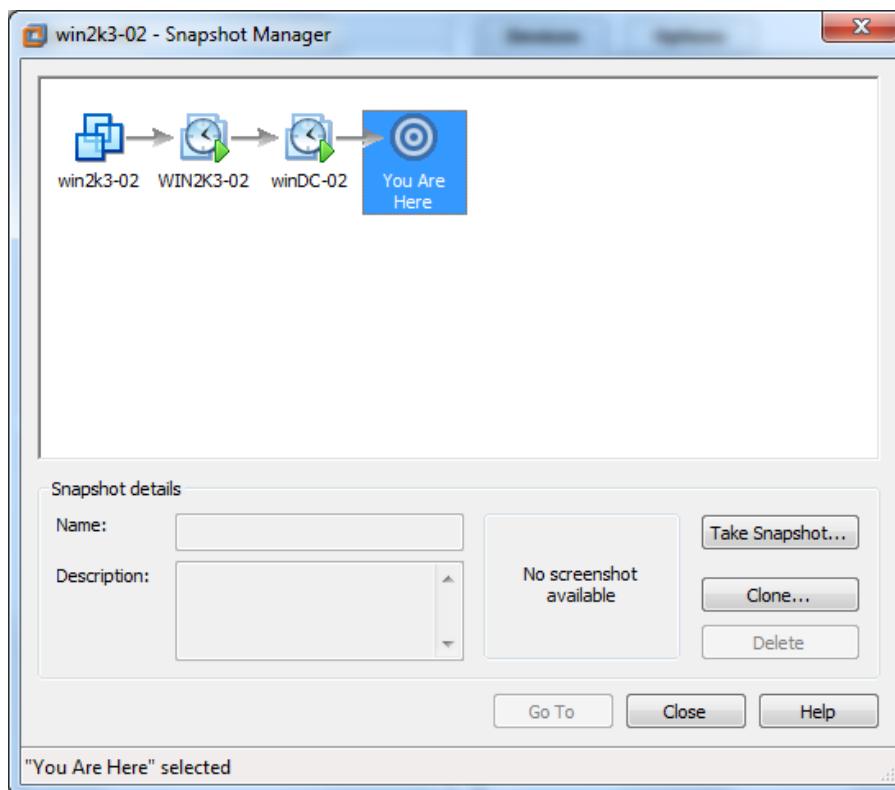
A.4. Tạo điểm phục hồi

Trên máy thật, mỗi khi cần lưu lại thông số cấu hình hiện tại, phải sử dụng các chương trình sao lưu và phục hồi. Nhưng trong máy ảo có chức năng Snapshot để tạo các điểm giúp phục hồi về trạng thái định trước mà không cần bất kì chương trình sao lưu nào.

Để tạo bản Snapshot, trong cửa sổ máy ảo click phải, chọn **Take Snapshot**.



Các bản Snap Shoot được quản lý trong Snapshot Manager

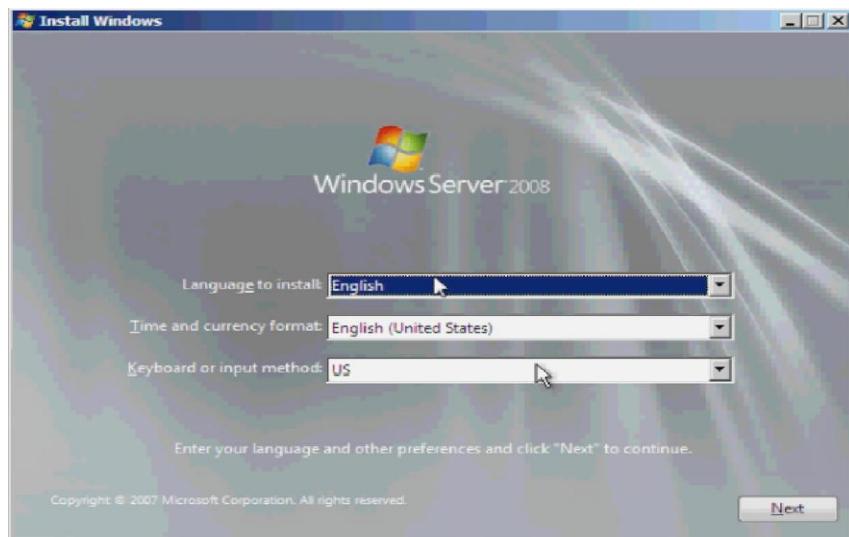


Khi muốn quay lại trạng thái cấu hình máy trước đó, chọn bản Snapshoot rồi click vào nút Go To.

PHỤ LỤC B. CÀI ĐẶT WINDOWS SERVER 2008

Để triển khai hệ thống mạng Windows theo mô hình miền, cần phải cài đặt hệ điều hành Windows Server trên máy điều khiển miền. Việc cài đặt hệ điều hành Windows Server có một số khó khăn và đặc thù so với các hệ điều hành trên máy trạm. Phụ lục B này sẽ trình bày cụ thể vấn đề cài đặt Windows Server 2008 trên máy chủ điều khiển miền. Các bước cài đặt cụ thể được tiến hành sau đây.

Đặt đĩa CD vào ổ đĩa, khởi động lại máy tính và bắt đầu tiến hành quá trình cài đặt (Hình B.1).



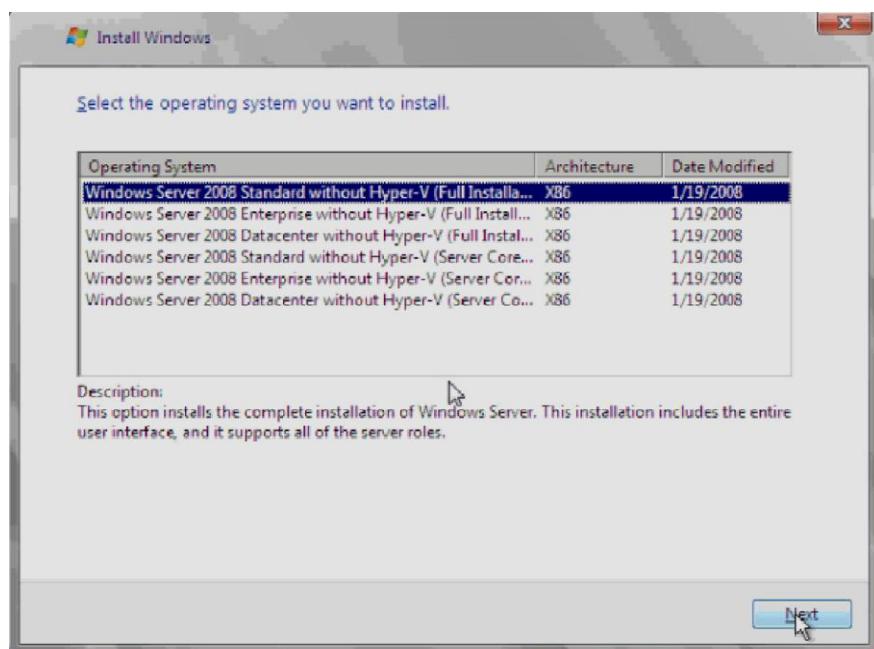
Hình B.1: Giao diện bắt đầu cài đặt Windows Server 2008

- **Language to install** : Chọn ngôn ngữ muốn hiển thị.
- **Time and currency format** : Định dạng thời gian và tiền tệ.
- **Keyboard or input method** : Định dạng bàn phím và phương thức nhập chữ. Sau khi lựa chọn, click **Next** để tiếp tục cài đặt. Kết quả như trong Hình B2.



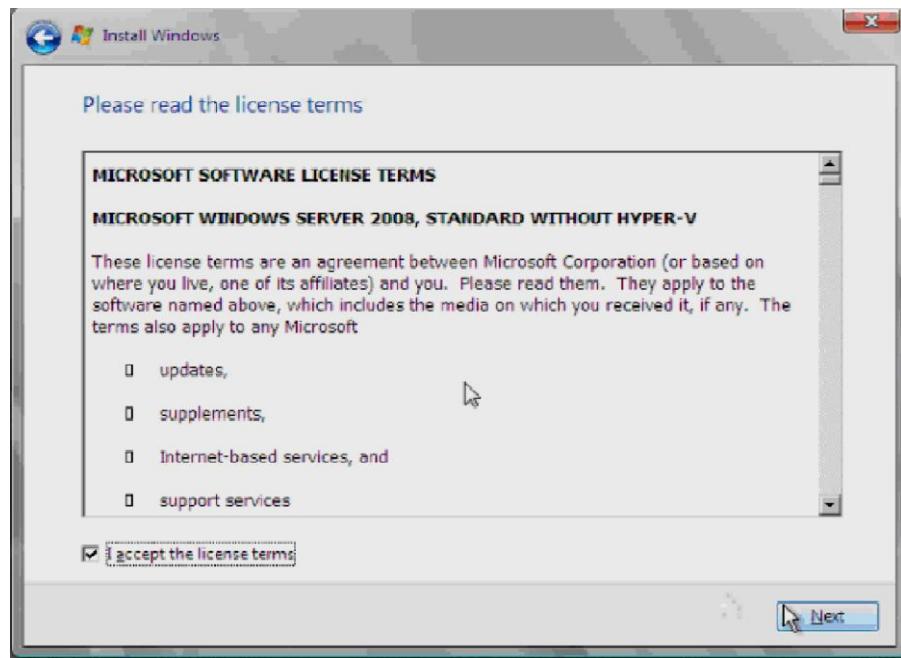
Hình B.2: Lựa chọn cài đặt

Click **Install now** để bắt đầu cài đặt (Hình B.3).



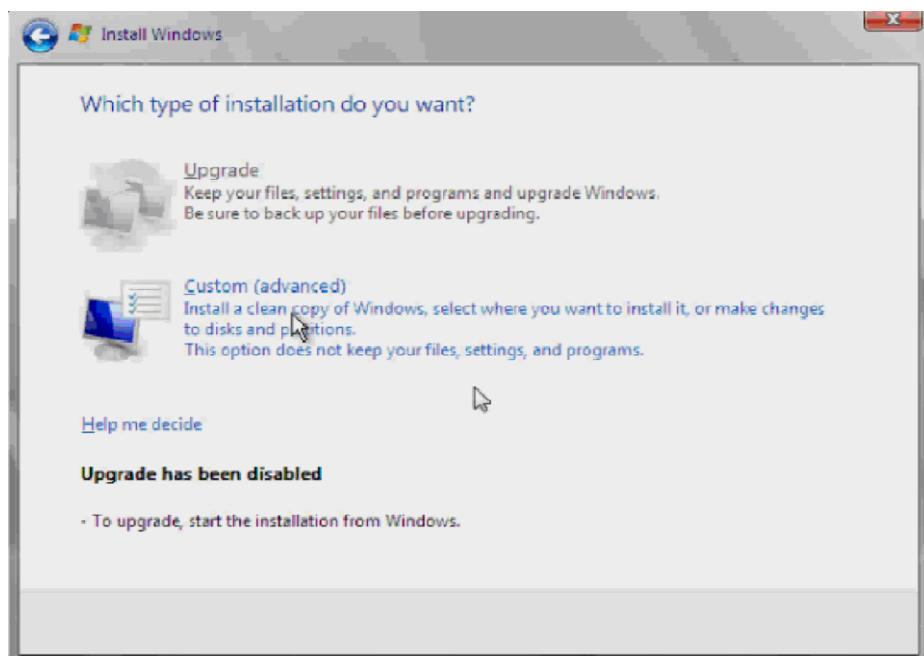
Hình B.3: Lựa chọn phiên bản

Lựa chọn phiên bản Windows Server thích hợp. Click **Next** để tiếp tục (Hình B.4).



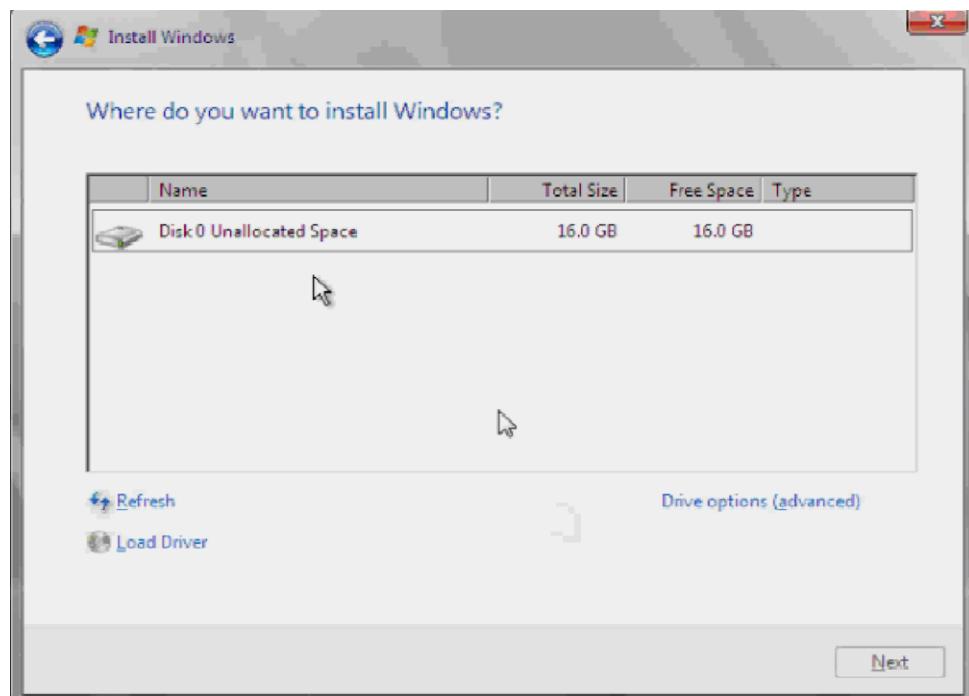
Hình B.4: Thông tin License

Tại bảng MICROSOFT PRE-RELEASE SOFTWARE LICENSE TERMS là những điều khoản sử dụng sản phẩm của Microsoft. Đánh dấu chọn **vào I accept the license terms** để chấp nhận những điều khoản đó và click **Next** để tiếp tục (Hình B.5).



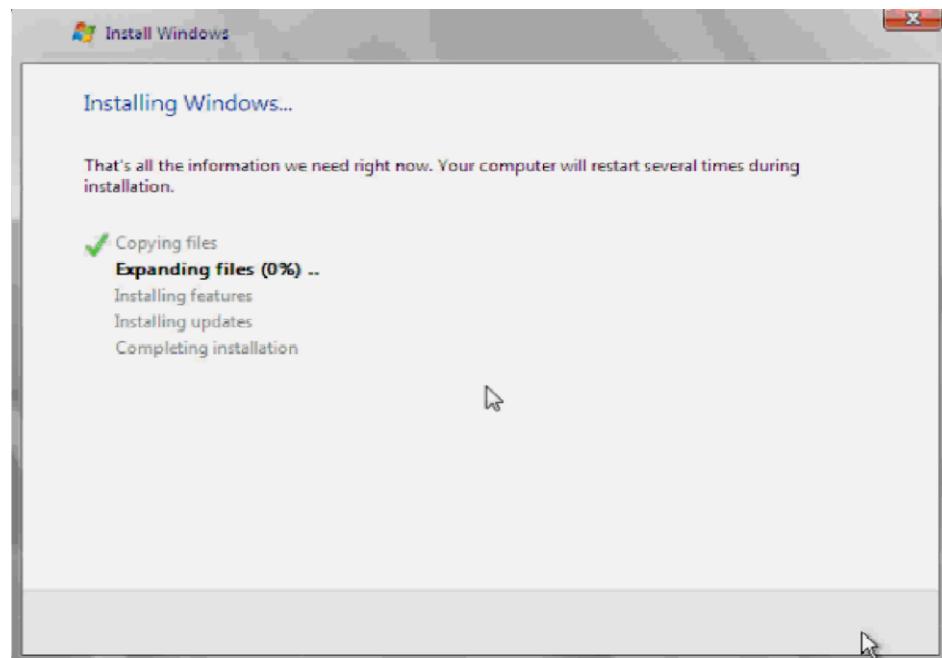
Hình B.5: Lựa chọn kiểu cài đặt

Chọn **Custom (advaneced)** để tiến hành cài đặt tùy chọn (Hình B.6).



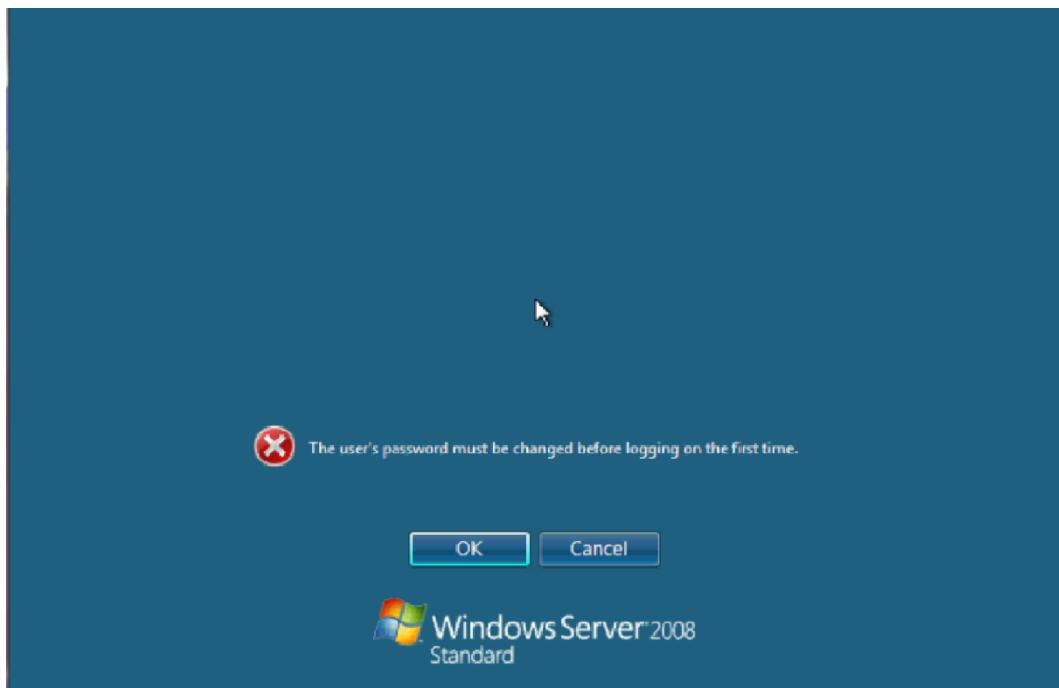
Hình B.6: Lựa chọn phân vùng cài đặt

Tiếp theo là chọn ổ đĩa để cài đặt Windows. Tiếp tục click **Next** sau khi đã chọn ổ đĩa cài đặt (Hình B.7).



Hình B.7: Giao diện đang cài đặt Windows Server 2008

Sau khi hệ thống hoàn tất cài đặt sẽ tự động đăng nhập với tài khoản Administrator, tuy nhiên mật khẩu đang ở trạng thái trống (blank) vì thế cần phải thiết lập mật khẩu ở lần đăng nhập đầu tiên (Hình B.8).



Hình B.8: Thiết lập mật khẩu

Click OK để tiến hành thay đổi mật khẩu. Sau đó đăng nhập vào bằng mật khẩu vừa thay đổi. Đến đây quá trình cài đặt kết thúc.

PHỤ LỤC C. QUẢN TRỊ MẠNG TRONG LINUX

Hiện nay, nhu cầu về các chuyên viên vi tính đặc biệt là chuyên viên quản trị hệ thống thành thạo hệ thống Linux ngày càng nhiều, nhất là khi Việt Nam đã trở thành thành viên thứ 150 của tổ chức WTO thì vấn đề chi phí bản quyền phần mềm làm cho nhiều doanh nghiệp chuyển đổi hệ thống của mình từ dựa trên nền tảng Windows sang Linux để tiết kiệm chi phí.

Các hệ thống mạng Linux cũng như số lượng người dùng Linux cũng gia tăng nhanh chóng. Có nhiều bản phân phối hệ điều hành dựa trên Linux như Cent OS, redhat, Fedora, Suse, Ubuntu... Mỗi sản phẩm sẽ có những mặt mạnh và yếu riêng nhưng theo thống kê và đánh giá thì Ubuntu là một trong những lựa chọn tốt nhất cho người dùng cuối khi chuyển từ Windows sang Linux, còn đối với phiên bản server thì có thể chọn Fedora hoặc Cent OS, v.v.

Phụ lục này sẽ trình bày những vấn đề cơ bản, cốt lõi để có thể triển khai, quản trị hệ thống mạng Linux dựa trên Fedora. Đây là một hệ điều hành mạng họ Linux được dùng phổ biến và dễ tiếp cận đối với người quản trị đã quen môi trường Windows.

Trong phần này, nghiệp vụ quản trị mạng trong môi trường Linux tập trung vào các hoạt động chính sau:

- Cài đặt hệ điều hành Fedora
- Cấu trúc thư mục và hệ thống tập tin
- Quản lý người dùng và nhóm
- Cấu hình mạng và xây dựng DHCP Server trên Linux
- Xây dựng DNS Server trên Linux
- Xây dựng Samba Server trên Linux (máy chủ File).

C.1. GIỚI THIỆU CHUNG VỀ LINUX

Linux là một hệ điều hành máy tính giống Unix (Unix-Like) được phát triển và phân phối theo mô hình “Phần mềm tự do” và việc phát triển phần mềm mã nguồn mở. Thành phần cơ bản của Linux là nhân Linux, là nhân hệ

điều hành được phát triển bởi Linus Torvalds được công bố lần đầu tiên vào tháng 9 năm 1991 với phiên bản 0.01.

C.1.1. Lịch sử phát triển của Linux

Ngày 5/4/1991, Linus Torvalds, sinh viên trường Đại học Helsinki, Phần Lan bắt đầu viết hệ điều hành Linux.

Ngày 14/3/1994, Torvalds cho ra mắt phiên bản hoàn thiện đầu tiên, Linux 1.0 với 176.250 dòng lệnh. 1 năm sau đó, phiên bản 1.2 ra mắt với 310.950 dòng lệnh.

Ngày 3/11/1994, Red Hat Linux, phiên bản 1.0 được giới thiệu. Đây là một trong những hệ điều hành được thương mại hóa đầu tiên dựa trên Linux.

Năm 2007, hàng loạt hãng sản xuất máy tính lớn như HP, ASUS, Dell, Lenovo bắt đầu bán ra các sản phẩm laptop được cài đặt sẵn Linux.

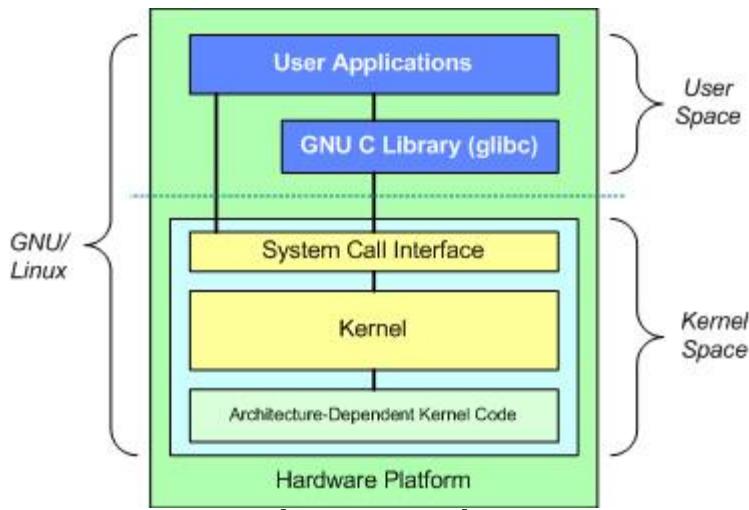
Tính đến thời điểm hiện tại, Linux đã có rất nhiều biến thể và phiên bản khác nhau, được xây dựng và phát triển riêng biệt bởi các công ty phần mềm và các cá nhân. Nổi bật trong số đó chính là hệ điều hành di động Android của Google, hiện là một trong những hệ điều hành thông dụng nhất hiện nay.

Đến tháng 1/2009, số người dùng Linux trên toàn cầu đạt mốc 10 triệu người.

Hiện nay, sau 20 năm tồn tại và phát triển, Linux được sử dụng rộng rãi trên toàn thế giới, trên các máy tính cá nhân, các máy chủ, đến các thiết bị di động, máy nghe nhạc, máy tính bảng, các máy ATM và thậm chí trên cả các siêu máy tính.

C.1.2. Kiến trúc của Linux

Một hệ điều hành GNU/Linux có thể phân thành hai vùng: vùng người dùng (User Space) gồm các thư viện C và các phần mềm ứng dụng (soạn văn bản, ...); vùng nhân (Kernel Space) gồm ba thành phần chính như trong Hình C.1.



Hình C.1: Kiến trúc hệ điều hành Linux

Trên cùng là lớp các ứng dụng của người dùng (User Applications). Bên dưới là lớp các thư viện C (GNU C Library). Lớp thư viện phục vụ cho giao diện các lời gọi hệ thống tạo liên kết giữa các ứng dụng và nhân Linux. Giao diện này quan trọng vì nhân Linux và các ứng dụng chiếm các vùng địa chỉ bộ nhớ được bảo vệ khác nhau. Mỗi ứng dụng có vùng địa chỉ ảo riêng còn nhân có một vùng địa chỉ duy nhất.

Nhân Linux có thể chia thành ba lớp. Trên cùng là giao diện các lời gọi hệ thống thực hiện các chức năng cơ bản như đọc, ghi. Bên dưới là phần mã nhân hệ điều hành (kernel code) hoặc chính xác hơn là mã nhân độc lập với kiến trúc vi xử lý (processor). Các mã lệnh trong lớp này dùng chung cho mọi loại processor mà Linux hỗ trợ. Lớp dưới cùng là các mã lệnh phụ thuộc vào kiến trúc từng loại processor (x86, x86-64, v.v.).

C.1.3. Các bản phân phối hệ điều hành họ Linux

Linux hiện nay có nhiều bản phân phối khác nhau, một phần là bởi vì tính chất nguồn mở của nó. Sau đây là một số bản phân phối chủ yếu, danh sách được cập nhật vào 05/09/2015:

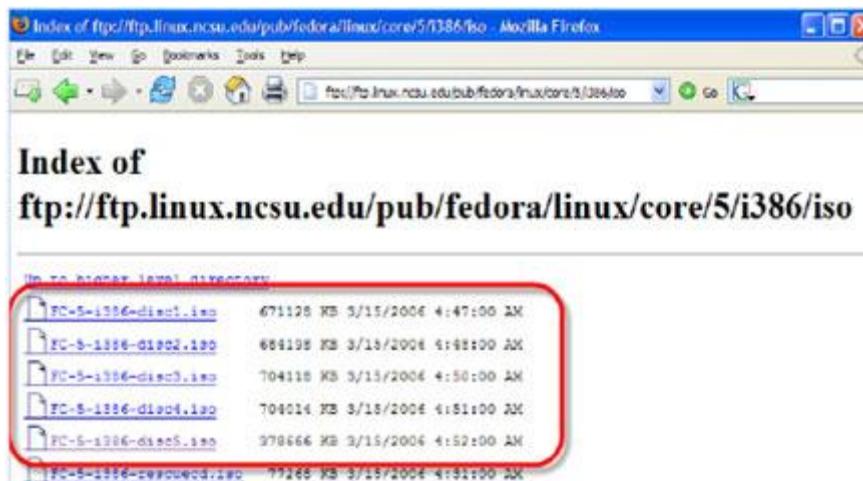
Tên bản phân phối	Phiên bản mới nhất	Trang web chính thức	Các bản dẫn xuất
Ubuntu	15.04	http://www.ubuntu.com/	Kubuntu, Xubuntu, Edubuntu, Ubuntu Studio, Lubuntu

Tên bản phân phối	Phiên bản mới nhất	Trang web chính thức	Các bản dẫn xuất
Debian GNU/Linux	8	http://www.debian.org/	
Elementary OS	0.3.1	http://www.elementaryos.org/	
Ultimate Edition	4.4	http://ultimateedition.info/	
Red Hat Enterprise Linux	6.5	http://www.redhat.com/rhel/	
Chrome Linux	2.4.1290	http://getchrome.eu/	
Fedora	22	http://www.fedoraproject.org/	
SUSE Linux Enterprise Desktop	13.2	http://vi.opensuse.org/	OpenSUSE 11.4, Mono 2.10.4
Linux Mint	17.2	http://linuxmint.com/	
Knoppix	7.4.2	http://www.knoppix.org/	
PCLinuxOS	2014	http://wwwpclinuxos.com/	
Mandrake	2011	http://www.mandriva.com	Mandriva
CentOS	7	http://www.centos.org/	
Gentoo	20140415	http://www.gentoo.org/	
Slackware	14.1	http://www.slackware.com/	
SLAX	7.0.8	http://www.slax.org/	
Sabayon	14.01	http://www.sabayon.org/	
Dreamlinux	5	http://www.dreamlinux.info/	
OpenSolaris	11.1	http://www.opensolaris.org/	
Hồng kỳ linux	6.0 SP3	http://www.redflag-linux.com/	
Puppy linux	5.7	http://puppylinux.org/	
Hacao Linux	2011	http://www.hacao.com/	
Asianux	4.5	http://www.asianux.vn/	Asianux

Tên bản phân phối	Phiên bản mới nhất	Trang web chính thức	Các bản dẫn xuất
			Server
SliTaz	5.0 RC 3	http://www.slitaz.org/	GNU/Linux
Linpus	2.2	http://www.linpus.com/	Linpus Linux
Back Track	5r3	http://www.backtrack-linux.org/	Back Track - Linux, Kali Linux
Kali linux	2.0.0	http://www.kali.org/	Kali - Linux, Back Track
Backbox	4.3	http://www.backbox.org	Backbox, linux
Super Ubuntu	11.10	http://superubuntu.linuxfreedom.com/download.html	Ubuntu, Zorin OS, Linux Mint,
Zorin OS	10	http://zorin-os.com/	Ubuntu, Super Ubuntu, Linux Mint

C.2. CÀI ĐẶT VÀ SỬ DỤNG HỆ THỐNG FEDORA

Trước khi cài đặt, cần tải một phiên bản Fedora phù hợp từ website như trong Hình C.2. Lựa chọn i386 trừ khi sử dụng hệ thống 64bit.



Hình C.2: Website download Fedora

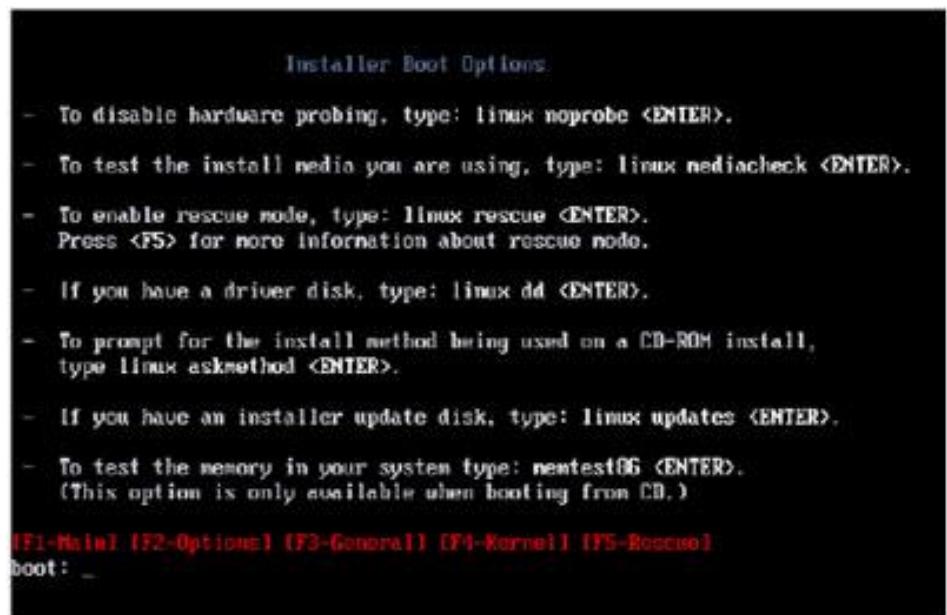
Tải về về tất cả các file iso, sau đó hãy sử dụng chương trình burn image như nero burn để ghi các ảnh trên thành CD/DVD cài đặt và tiến hành khởi động từ CD/DVD. Sau đây là tóm tắt các bước cài đặt hệ thống:

Bước 1. Chọn chế độ khởi động từ CD/DVD (thiết lập trong cmos), đưa cd cài đặt vào ổ CD/DVD sẽ thấy xuất hiện giao diện như Hình C.3 sau:



Hình C.3: Giao diện bắt đầu cài đặt Fedora

Bước 2. Nhấn F2 sẽ thấy một số tùy chọn nâng cao (Hình C.4)



Hình C.4: Một số tùy chọn nâng cao

Bước 3. Nhấn enter để tiến hành cài đặt như Hình C.5. [Có thể chọn skip](#) để bỏ qua quá trình kiểm tra đĩa.



Hình C.5: Lựa chọn kiểm tra ổ đĩa

Bước 4. Sau khi chọn skip tiến trình cài đặt Fedora sẽ thực thi, màn hình sẽ chuyển từ độ phân giải 640x480 sang 800x600 (Hình C.6).



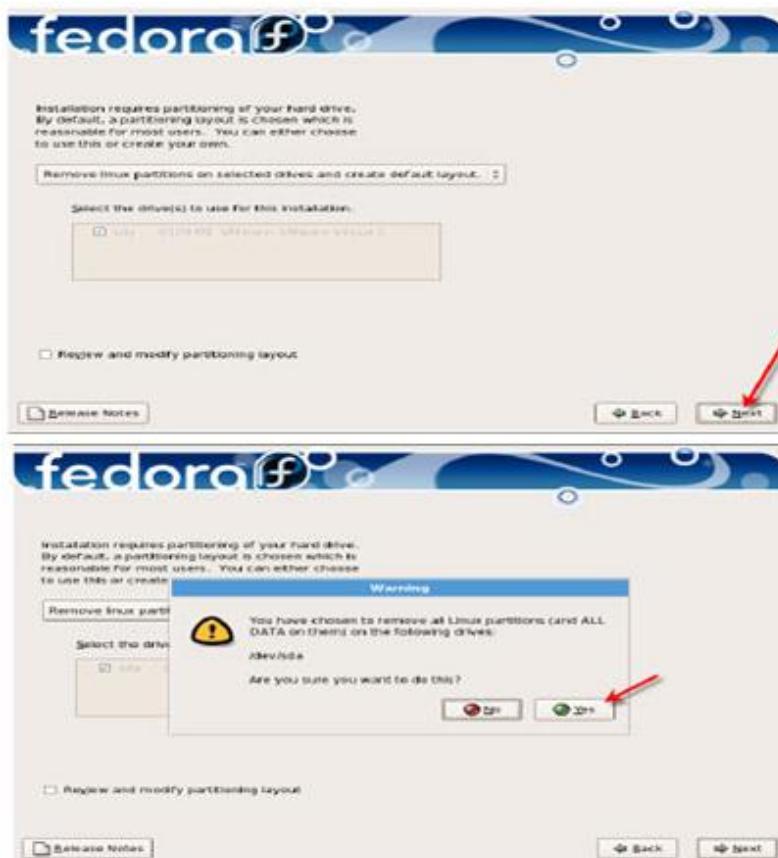
Hình C.6: Giao diện Fedora chuyển độ phân giải

Bước 5. Tiếp theo là một số tùy chọn về ngôn ngữ hiển thị, kiểu bàn phím và chuột, có thể chọn các giá trị mặc định và click Next, trong trường hợp muốn hiển thị ngôn ngữ là việt nam hãy chọn Vietnamese tuy nhiên có thể thay đổi điều này dễ dàng sau khi hoàn tất cài đặt hệ thống (Hình C.7).



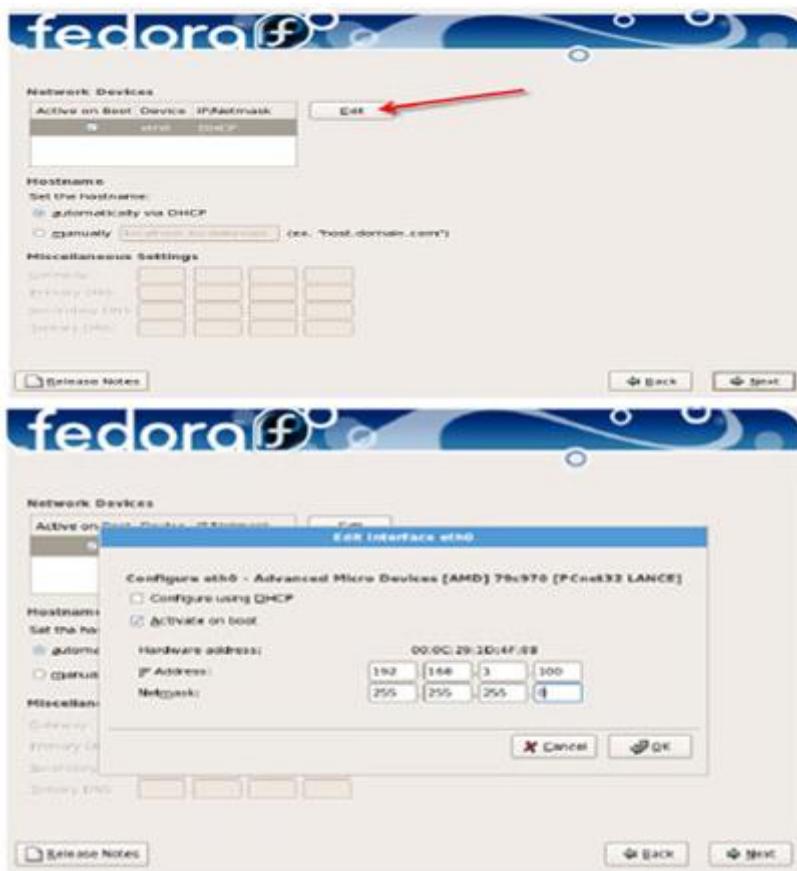
Hình C.7: Lựa chọn ngôn ngữ

Bước 6. Chọn Next để chuyển sang màn hình chia partition cho hệ thống Linux, có một số tùy chọn. Có thể để hệ thống tự phân chia trên partition trống, hoặc chọn xóa toàn bộ partition Linux đang tồn tại trên đĩa cứng cũng hay xóa toàn bộ partition trên đĩa cứng (nên cẩn thận khi chọn tùy chọn này vì nó sẽ xóa toàn bộ dữ liệu trên máy tính, hãy tiến hành backup dữ liệu cẩn thận) (Hình C.8).



Hình C.8: Lựa chọn phân vùng cài đặt

Bước 7. Sau khi chọn YES, sẽ cấu hình TCP/IP cho máy tính Linux của mình, có thể chọn lấy IP từ DHCP hoặc nhập vào thông tin IP tĩnh cho máy tính (192.168.1.100/24) (Hình C.9).



Hình C.9: Cấu hình địa chỉ IP

Bước 8. Quay trở lại màn hình chính, hãy nhập vào tên host cho máy tính và các địa chỉ DNS cần thiết như Hình C.10.



Hình C.10: Lựa chọn tên host và địa chỉ DNS

Trong đó, Primary DNS và Seconadry có thể chọn 210.245.31.130 và 203.162.4.181, v.v.

Bước 9. Click Next để chuyển sang màn hình chọn giờ. Hãy chọn múi giờ thích hợp (Hình C.11) và click Next.



Hình C.11: Lựa chọn múi giờ

Bước 10. Trên màn hình tiếp theo ta nhập vào mật mã của tài khoản root (giống tài khoản super administrator trên windows).



Hình C.12: Đặt và xác nhận mật khẩu

Bước 11. Tiếp theo sẽ chọn các gói cần cài đặt, hãy chọn Customize now và chọn Next (Hình C.13).



Hình C.13: Lựa chọn các gói cài đặt cần thiết

Bước 12. Bây giờ, sẽ chọn các dịch vụ cần thiết cho hệ thống của mình, hãy đánh dấu vào các ô check box (Hình C.14) tương ứng như sau:

Servers:

- DNS Name Server
- FTP Server
- Network Servers
- Printing Support
- Server Configuration Tools
- Web Server
- Windows File Server

Base System:

- System Tools



Hình C.14: Lựa chọn cài đặt các dịch vụ trên máy chủ

Bước 13. Click Next để bắt đầu cài đặt, trong quá trình cài đặt sẽ cần thay đổi các cdrom theo thứ tự cần thiết. Reboot để khởi động lại máy tính sau khi hoàn tất (Hình C.15).



Hình C.15: Giao diện bắt đầu cài đặt và lựa chọn khởi động lại máy

Bước 14. Trong lần khởi động đầu tiên cần xác định một số tham số như sau:

Chọn **Forward** trên màn hình welcome (Hình C.16)



Hình C.16: Giao diện lần khởi chạy đầu tiên

Có thể chọn **disable Firewall** (Hình C.17).



Hình C.17: Vô hiệu Firewall

Trên màn hình thiết lập cơ chế bảo mật nâng cao hãy chọn **permissive** (Hình C.18).



Hình C.18: Thiết lập cơ chế bảo mật nâng cao

Xác lập ngày giờ cho hệ thống và chọn Forward (Hình C.19).



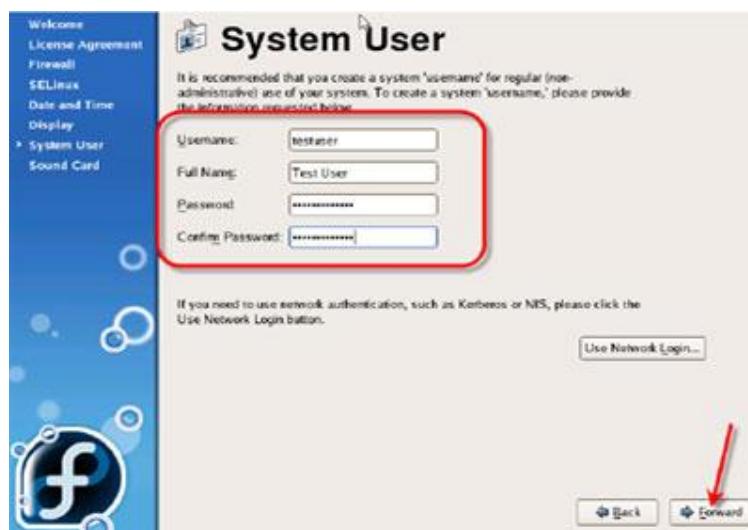
Hình C.19: Xác lập ngày giờ

Xác định độ phân giải màn hình (tùy thuộc vào card màn hình trên hệ thống) và click forward (Hình C.20).



Hình C.20: Xác định độ phân giải màn hình

Tạo tài khoản đăng nhập đầu tiên cho hệ thống và click forward (Hình C.21).



Hình C.21: Tạo tài khoản đầu tiên

Kiểm tra card âm thanh trên máy tính và click Finish (Hình C.22).



Hình C.22: Kiểm tra card âm thanh

Bây giờ có thể đăng nhập vào hệ thống Linux server của mình với tài khoản root và mật mã đã xác định (Hình C.23). Màn hình giao diện sau khi đăng nhập thành công như trong Hình C.24.



Hình C.23: Màn hình đăng nhập hệ thống



Hình C.24: Giao diện đăng nhập thành công

Một số thành phần chính của hệ thống Linux

- **GNOME** và **KDE** là hai giao diện đồ họa được sử dụng nhiều nhất trên các hệ thống Linux.
- **Terminal**: dùng để thực thi các dòng lệnh, giống với command prompt của hệ thống Windows
- **Root**: tài khoản quản trị trên hệ thống Linux tương tự như tài khoản Administrator trên Windows.
- **Panel**: khung điều khiển với nhiều chức năng thường xuất hiện dưới đáy của màn hình.
- **SU (switch user)**: khi đăng nhập hệ thống với user thường có thể sử dụng lệnh **su** để chuyển qua quyền root khi cần tiến hành các lệnh và dịch vụ cần thực hiện dưới quyền này, gần giống với lệnh runas trên hệ thống Windows.
- **Man page**: trang hướng dẫn.

Một số lệnh cơ bản trên hệ Thống Linux

Lệnh	Mô tả
/	Root directory.
./	Current directory.
../	Parent directory.
Cat	Hiển thị nội dung tập tin. Sử dụng: cat <filename>
Cd	Chuyển thư mục, sử dụng : cd <directory_name>
Cp	Copy file/folder, sử dụng : cp <source_filename><destination_filename>
echo \$PATH	xem các biến đường dẫn hiện tại.
Export	Xem các biến môi trường.
History	Xem các lệnh đã được thực hiện ví dụ: history 10 là liệt kê 10 lệnh được sử dụng gần nhất.

ifconfig	xem cấu hình TCP/IP (như ipconfig trên Windows).
Kill	kết thúc tiến trình: kill <PID>
Ls	Liệt kê các file và folder của thư mục: ls <directory_name>
Mkdir	Tạo thư mục: mkdir <directory_name>
Mv	Di chuyển thư mục hoặc file: mv <current_filename><new_filename>
passwd	Thay đổi password.
Ps	Xem các tiến trình đang chạy trên hệ thống.
Pwd	Hiển thị thư mục hiện hành.
Rm	Xóa file :: rm <filename>
Rmdir	Xóa thư mục : rmdir <directory_name>
shutdown	Tắt hệ thống
Touch	Tạo file: touch <filename>

Một số phím tắt thông dụng

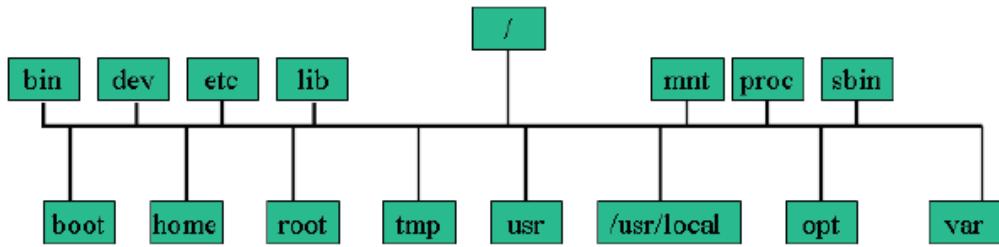
- **Ctrl+Alt+Backspace:** tắt giao diện đồ họa đang sử dụng và trở ra màn hình log in.
- **Ctrl+Alt+Delete:** Shut down và reboot hệ thống.
- **Ctrl+D:** log out khỏi một terminal hay console session.
- **Ctrl+Alt+Fx:** Chuyển màn hình.

C.3. HỆ THỐNG TỆP TIN VÀ THƯ MỤC

C.3.1. Hệ thống tệp tin và thư mục trong Linux

Cấu trúc của hệ thống tệp tin (file)

Mỗi hệ thống file được tổ chức theo cấu trúc cây thư mục như Hình C.25. Mỗi phân vùng khi được tạo ra đều có thể có một điểm kết nối (mount point). Công việc này thường được thi hành trong quá trình cài đặt.



The base directories

boot home root tmp usr /usr/local opt var

Directories that can be mount points for separate devices

Hình C.25: Cấu trúc thư mục trong Linux

Trong hình trên, gốc của kiến trúc phân cấp này là thư mục gốc “/”. Nó gần tương tự như “C:\” trong DOS ngoại trừ việc “C:\” chính là phân vùng đầu tiên của đĩa cứng đầu tiên, trong khi thư mục gốc “/” của Linux có thể là ánh xạ của bất kỳ phân vùng nào.

Thư mục gốc:

Các thư mục cơ sở là những thư mục con cấp 1 nằm ngay dưới thư mục gốc “/”. Tiến trình khởi động sẽ ánh xạ thư mục gốc đầu tiên nhằm giúp đỡ tất cả các thao tác tiếp theo như kiểm tra phân vùng, nạp module cho nhân...vv vì khi ánh xạ thư mục gốc xong thì các chương trình như: fsck, insmod hay mount mới có thể được sử dụng.

Để đảm bảo cho quá trình khởi động diễn ra chính xác, các thư mục **/dev**, **/bin**, **/sbin**, **/etc** và **/lib** bắt buộc phải là thư mục con của “/” và không thể là ánh xạ của bất kỳ phân vùng nào khác.

Sau đây là một số thư mục cơ sở và giải thích ngắn gọn ý nghĩa của chúng:

/bin và **/sbin**: Chứa những file cần thiết cho quá trình khởi động và những lệnh thiết yếu để duy trì hệ thống.

/dev: Chứa các định danh ánh xạ của thiết bị hoặc những file đặc biệt.

/etc: Chứa các file cấu hình của hệ thống và nhiều chương trình tiện ích.

/lib: Chứa các thư viện dùng chung cho các lệnh nằm trong /bin và /sbin. Và thư mục này cũng chứa các module của nhân.

/mnt hoặc **/media:** Mount point mặc định cho những hệ thống file kết nối bên ngoài.

/proc: Lưu các thông tin của nhân, chỉ có thể ghi được nội dung trong thư mục

/proc/sys và **/boot:** Chứa nhân Linux để khởi động và các file system maps cũng như các file khởi động giai đoạn hai.

/home (tùy chọn): Thư mục dành cho người dùng khác root. Thông tin khởi tạo thư mục mặc định của người dùng được đặt trong **/etc/skel/**

/root (tùy chọn): Thư mục mặc định của người dùng root.

/tmp: Thư mục chứa các file tạm thời.

/usr: Thư mục chứa những file cố định hoặc quan trọng để phục vụ tất cả người dùng.

/usr/local hoặc **/opt** (tùy chọn): Thư mục chứa các phần mềm cài thêm.

/var/www, /var/ftp/ hoặc **/srv** (Suse): Thư mục chứa thông tin của các dịch vụ WEB hay FTP.

/var: Thư mục chứa các thông tin hay thay đổi như: spool và log

Hệ thống file chuẩn ext2

Để có thể lưu trữ và quản lý dữ liệu, mỗi phân vùng trên đĩa cứng đều phải được tạo ra một hệ thống file. Ngay trước khi khởi tạo, bao giờ người thiết lập cũng phải chỉ định kiểu định dạng của hệ thống file mới cần tạo.

Hiện nay, nhân Linux hỗ trợ rất nhiều kiểu định dạng của hệ thống file. Trong đó, kiểu hệ thống file **ext2** được coi là mặc định trong các hệ

thống của Linux “Linux Native” (Trong nhiều hệ thống **ext3** được coi là mặc định nhưng thực tế **ext3** chính là **ext2** kèm thêm chức năng journal)

The Second Extended File System

Ext2 là kiểu định dạng hệ thống file được thiết kế dựa trên việc quản lý các khối dữ liệu có kích thước 1KB (1024 byte), đây là kích thước mặc định và có thể thay đổi được. Có 3 loại khối như trên được định nghĩa trong ext2:

Superblocks

Lặp lại sau mỗi 8193 khối. Khối này chứa thông tin như: block-size, free inodes, last mounted time, v.v.

Inodes

Chứa các con trỏ trỏ đến khối dữ liệu. 12 khối dữ liệu đầu tiên được truy cập trực tiếp từ con trỏ này. Nếu dữ liệu > 12KB thì các inodes gián tiếp sẽ được sử dụng.

Mỗi inode bao gồm 256 byte và chứa các thông tin về user, group, permissions và time stamp của dữ liệu mà nó quản lý.

Khối dữ liệu

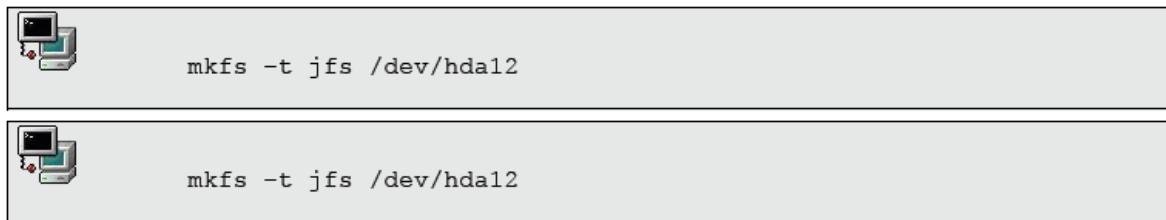
Có thể là file hoặc thư mục với nội dung thật được chứa trong các khối này.

Tiện ích định dạng

Do nhân Linux chỉ có thể đọc được các hệ thống file đã được định dạng từ trước nên để lưu trữ và quản lý dữ liệu trên các phân vùng mới, cần phải định dạng một hệ thống file trên đó thông qua các công cụ định dạng.

Để định dạng một phân vùng có kiểu hệ thống file là **ext2** bằng lệnh **mkfs.ext2** hay **mke2fs**. Tương tự như vậy với kiểu hệ thống file **xfs** (của Silicon Graphics) với lệnh **mkfs.xfs**.

Lệnh **mkfs** thực chất là một chương trình kiểm tra yêu cầu định dạng và lựa chọn đúng lệnh để thi hành. Cú pháp của mkfs như minh họa trong Hình C.26.



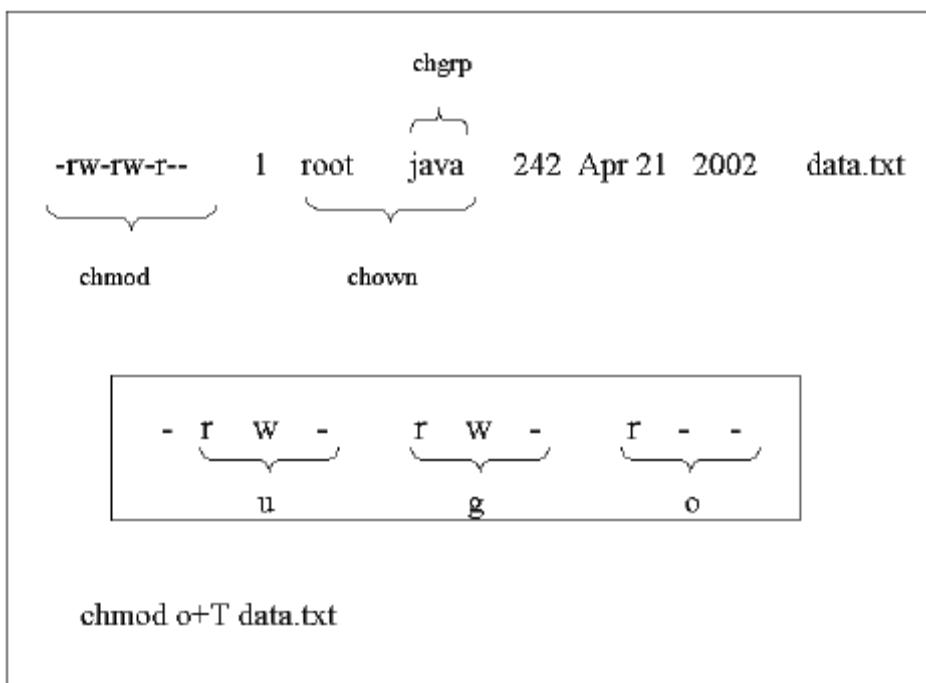
```
mkfs -t jfs /dev/hda12
```

```
mkfs -t jfs /dev/hda12
```

Hình C.26: Cú pháp mkfs

C.3.2. Quyền truy nhập thư mục và file

Quyền truy cập thư mục và file được tổng quát như trong Hình C.27.



Hình C.27: Tổng thể về quyền truy cập trong Linux

Thay đổi quyền truy xuất và chủ sở hữu

Quyền truy xuất file, thư mục và chủ sở hữu được định nghĩa để quy định cách thức truy cập dữ liệu trong hệ thống. Để thay đổi quyền truy cập, sử dụng lệnh **chmod**. Có ba nhóm đối tượng chính được tác động bởi quyền truy cập là:

- *u* Người dùng sở hữu
- *g* Nhóm người dùng sở hữu

- Không thuộc hai đối tượng trên

Ví dụ (Hình C.28):

-rw-rw-r-- 1 jade sales 24880 Oct 25 17:28 libcgic.a

```
chmod g=r,o-r libcgic.a
chmod g+w libcgic.a

chown root libcgic.a
chgrp apache libcgic.a
```

Hình C.28: Minh họa thay đổi quyền truy xuất

Tùy chọn hay dùng với chmod, chown và chgrp là -R cho phép thay đổi trong cả các thư mục, file bên trong thư mục chỉ định.

Ngoài cách sử dụng ký tự đại diện cho các quyền: read=r, write=w, execute=x, chmod cho phép sử dụng một bộ số hệ bát phân để thay đổi quyền theo Hình C.29 sau:

<i>read</i>	4	
<i>write</i>	2	
<i>execute</i>	1	
user	group	other
<i>rwx</i>	<i>r-x</i>	<i>rw-</i>
<i>4+2+1=7</i>	<i>4+1=5</i>	<i>4+2=6</i>

Hình C.29: Tổng hợp quyền

Quyền truy xuất chuẩn

Các hệ thống UNIX tạo ra file và thư mục với quyền truy xuất chuẩn như sau:

<i>Files</i>	666	-rw-rw-rw-
<i>Directories</i>	777	-rwxrwxrwx

umask

Là khái niệm được thiết lập để chỉ định quyền truy xuất mặc định cho các file và thư mục mới tạo **đối với mỗi người dùng**. umask là một mặt nạ gồm một bộ các số hệ bát phân. Khi đó, quyền truy xuất mặc định của các file và thư mục đối với mỗi người dùng được tính theo công thức sau:

$$\text{Final Permissions} = \text{Standard Permissions} \text{ (logical AND)} \\ (\text{NOT})\text{Umask}$$

Quyền truy cập SUID

Là quyền truy cập được thiết lập bởi root cho phép người dùng bình thường có thể thi hành một lệnh như là root. Quyền này được thiết lập với tên là s (nằm ở vị trí x của nhóm u) và được gán số hệ bát phân là 4000.

Quyền truy cập SGID

Là quyền truy cập cho phép người dùng thuộc nhóm sở hữu có thể thi hành lệnh mà không cần dùng **newgrp** để chuyển nhóm. Quyền này được thiết lập với tên là s (nằm ở vị trí x của nhóm g) và được gán số hệ bát phân là 2000. Tại thư mục được thiết lập SGID, tất cả các file, thư mục tạo bên trong sẽ có nhóm sở hữu mặc định là nhóm sở hữu của thư mục cha.

Bit đánh dấu (The sticky bit)

Quyền này được thiết lập với tên là t (nằm ở vị trí x của nhóm o) và được gán số hệ bát phân là 1000. Quyền này được thiết lập để:

- Cho phép các thư mục cấm người dùng xóa file trừ phi họ là chủ sở hữu.
- Cho phép file được thi hành hoặc nạp vào bộ nhớ nhanh hơn.

C.4. QUẢN LÝ TÀI KHOẢN NGƯỜI DÙNG VÀ NHÓM

Muốn bổ sung thêm người dùng, hoặc nhóm người dùng, cho hệ thống, có thể dùng chương trình **Users And Groups**, trong thực đơn **System -> Administration -> Users and Groups**.

Để bổ sung một người dùng mới, ấn chuột vào **Add user**, điền các thông tin cần thiết rồi ấn chuột vào nút ghi **OK**. Để chỉnh lại các thuộc tính

của từng người dùng, có thể ấn chuột vào nút ghi **Properties** có trong cửa sổ chính của Users.

Để bổ sung một nhóm người dùng mới, chọn tab Groups tab và ấn chuột vào **Add group**. Xác định tên của nhóm mới và nếu muốn có thể thay đổi số ấn định cho nhóm (Group ID). Nếu định dùng một số Group ID đã dùng rồi, hệ thống sẽ có thông báo.

Để bổ sung người dùng cho nhóm vừa mới được tạo ra, chỉ cần chọn một người dùng từ danh sách bên trái và ấn vào nút ghi **Add**. Muốn loại trừ một người dùng ra khỏi một nhóm cũng đơn giản bằng việc bổ sung: sau khi đã chọn tên người dùng trong cửa sổ bên phải, ấn chuột vào nút đã ghi.

Remove. Khi nào xong, ấn vào nút **OK** để kết thúc và thực sự tạo ra nhóm người dùng mới, cùng những người dùng thuộc nhóm đó.

Muốn sửa lại các thuộc tính của một nhóm người dùng, chọn tên của một nhóm trong cửa sổ Groups và ấn chuột vào nút đã ghi **Properties**.

Để xoá hoàn toàn một người dùng, hoặc một nhóm người dùng, từ hệ thống, chọn tên người dùng hoặc tên nhóm người dùng muốn xoá và ấn chuột vào nút đã ghi **Delete**.

Tương tự hệ thống Windows, khi cài đặt Linux (FC Core) sẽ tạo ra một tài khoản có quyền quản trị hệ thống và có thể dùng để tạo ra các tài khoản khác, đây là tài khoản cao cấp nhất có tên gọi là root. Để cấp quyền truy cập hệ thống cần tạo ra các tài khoản người dùng, và mỗi tài khoản người dùng được gán một UID. Các tài khoản có chung thuộc tính sẽ được xếp vào các nhóm như trên hệ thống Windows và mỗi nhóm sẽ có các GID riêng.

Trên hệ thống Linux có thể xem các User hiện có thông qua nội dung của tập tin */etc/passwd* như hình dưới đây:

```

root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/bin/sh
bin:x:2:2:bin:/bin/sh
sys:x:3:3:sys:/dev/bin/sh
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/bin/sh
man:x:6:12:man:/var/cache/man:/bin/sh
lp:x:7:7:lp:/var/spool/lpd:/bin/sh
mail:x:8:8:mail:/var/mail:/bin/sh
news:x:9:9:news:/var/spool/news:/bin/sh
uucp:x:10:10:uucp:/var/spool/uucp:/bin/sh
proxy:x:13:13:proxy:/bin:/bin/sh
www-data:x:33:33:www-data:/var/www:/bin/sh
backup:x:34:34:backup:/var/backups:/bin/sh
list:x:38:38:Mailing List Manager:/var/list:/bin/sh
irc:x:39:39:ircd:/var/run/ircd:/bin/sh
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/bin/sh
nobody:x:65534:65534:nobody:/nonexistent:/bin/sh
libuuid:x:100:101:/var/lib/libuuid:/bin/sh
syslog:x:101:103::/home/syslog:/bin/false
mysql:x:102:105:MySQL Server,,,:/nonexistent:/bin/false
postfix:x:103:109:/var/spool/postfix:/bin/false
dovecot:x:104:111:Dovecot mail server,,,:/usr/lib/dovecot:/bin/false
sshd:x:105:65534:/var/run/sshd:/usr/sbin/nologin
landscape:x:106:113:/var/lib/landscape:/bin/false
eric:x:1000:1000:mixeduperic,,,:/home/eric:/bin/bash
jim:x:1001:1001:/home/jim:/bin/bash
bob:x:1002:1002:/home/bob:/bin/bash
tony:x:1003:1003:Tony Smith,,,:/home/tony:/bin/bash
'/etc/passwd' 29L, 1257C

```

29,1

All

Trong tập tin passwd này thấy có nhiều record với các field khác nhau như:

User Account Name: login name của tài khoản người dùng.

Password: login password của tài khoản người dùng. Nếu chỉ thấy kí tự x trong ô này thì mật mã đã được mã hóa và bảo vệ trong tập tin shadow password.

User ID: số hiệu của user (UID)

Group ID: số hiệu Group mà người dùng này là thành viên (GID).

Full Name: tên đầy đủ của người dùng.

Home Directory: thư mục chủ của người dùng sau khi đăng nhập.

Shell: trình diễn dịch lệnh, ví dụ bash.

Khi một tài khoản mới được tạo nó sẽ được gán 1 UID, bắt đầu từ 500 trở đi và tăng dần khi các tài khoản mới được tạo ra.

Cũng như trên hệ điều hành Windows, sau khi cài đặt một số tài khoản và group mặc định sẽ được tạo như:

User	UID	GID	Home Directory	Shell
Root	0	0	/root	/bin/bash
Bin	1	1	/bin	/sbin/nologin
Daemon	2	2	/sbin	/sbin/nologin
Adm	3	3	/var/adm	/sbin/nologin
Shutdown	6	6	/sbin	/sbin/shutdown
Mail	8	8	/var/spool/mail	/sbin/nologin
News	9	9	/var/spool/news	
ftp	14	14	/var/ftp	/sbin/nologin

Các default user

Group	GID	Default Members
Root	0	Root
Bin	1	Root, Bin, Daemon
Daemon	2	Root, Bin, Daemon
Adm	4	Root, Bin, Daemon
Mail	12	Mail
News	13	News
ftp	50	

Các default group

Tạo User và Group

Có thể tạo tài khoản người dùng trên Linux bằng dòng lệnh hoặc giao diện đồ họa. Để tạo tài khoản người dùng Linux1 bằng dòng lệnh hãy thực hiện như sau:

useradd -g Users Linux1

passwd Linux1

New password: qwerty

Retype new password: qwerty

Nếu muốn xác định home folder và shell cho user khi tạo có thể sử dụng tùy chọn **-d** và **-s**

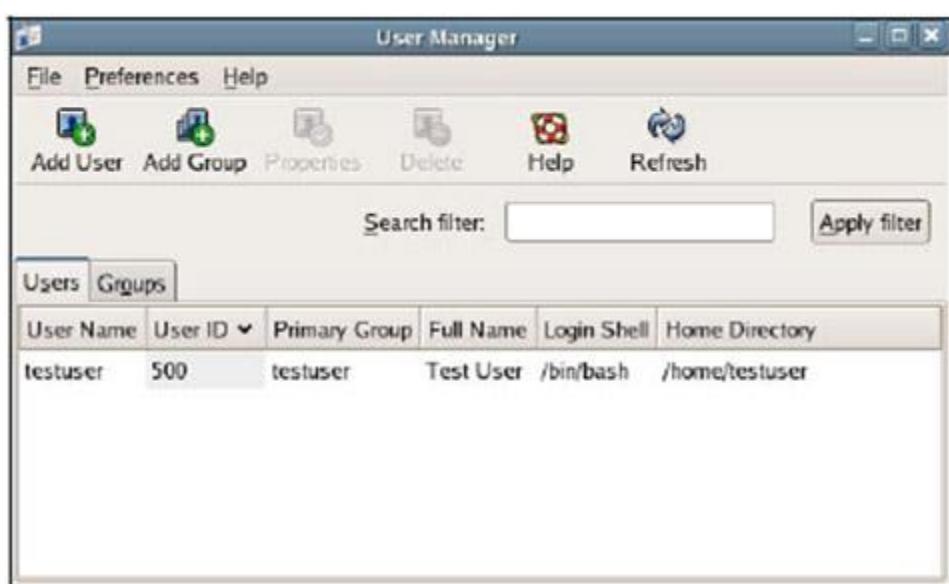
Ví dụ sau sẽ tạo ra 1 group với GID là 1024 (tùy chọn -g dùng để xác định GID, nếu không sử dụng tùy chọn này thì hệ thống sẽ tự động xác định GID cho group theo thứ tự tăng dần).

Add Linux User và Group

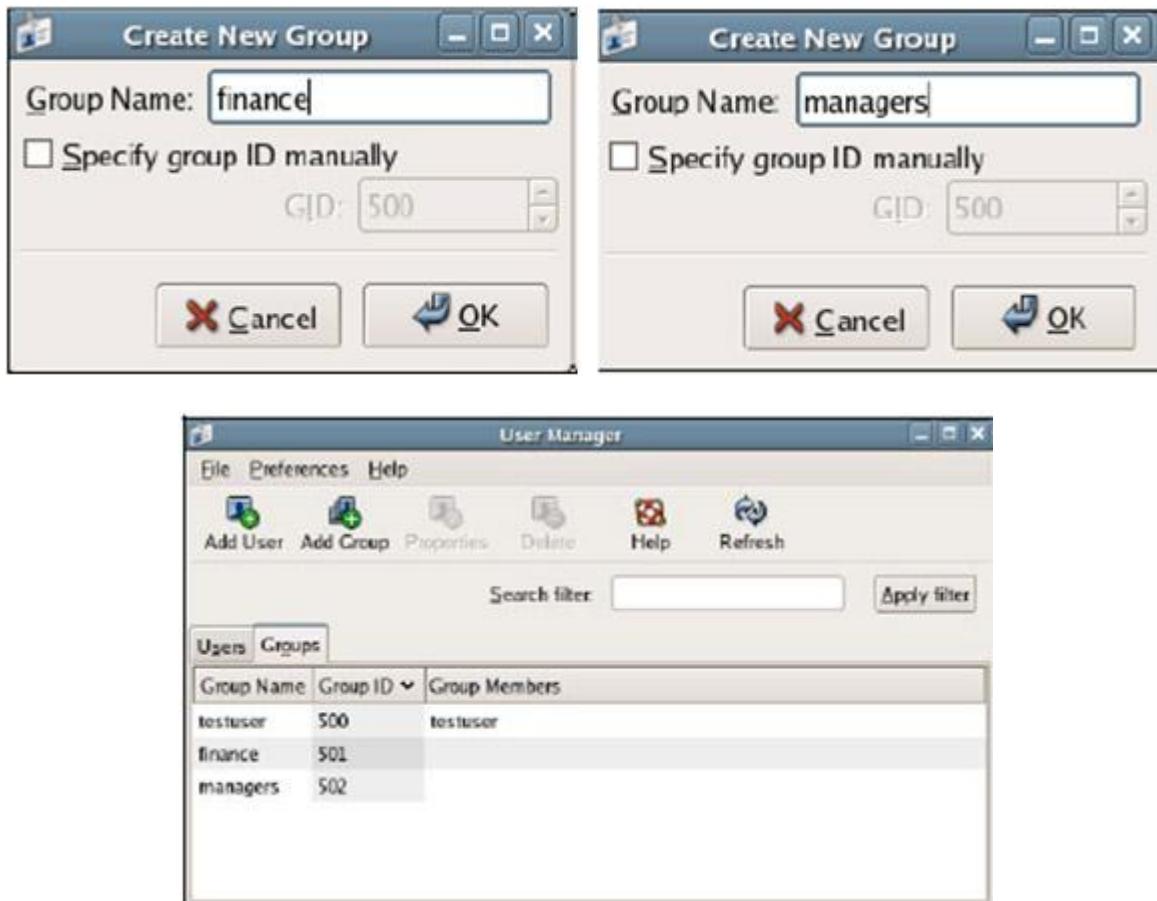
1. Để Add một User mới trên hệ thống Linux hãy click **System => Administration => Users and Groups**.



2. Giao diện quản lý user như sau:



3. Click **Add Group** trên thanh toolbar sau đó tạo 2 group finance và managers như hình sau:



4. Hãy chọn tab **Users** và chọn **Add User** để tạo các tài khoản *Sam Randolph* với các thông tin như sau:

User Name **srandolph**

Full Name **Sam Randolph**

Password **Fishing123**

Confirm Password **Fishing123**

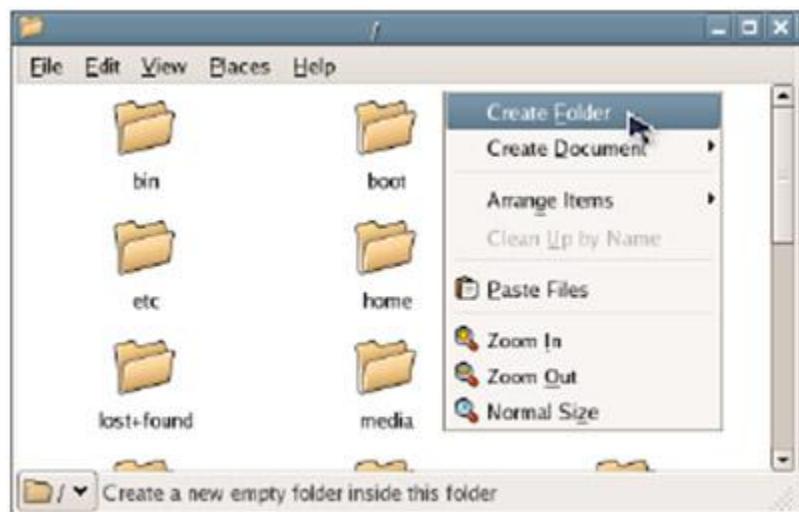


Click OK hoàn tất



Gán quyền trên các File và Folder

1.Tạo một folder tên là *Share* bằng cách nhấn đúp vào icon **Computer** sau đó mở **File System**. Nhấn chuột phải và chọn **Create Folder**.



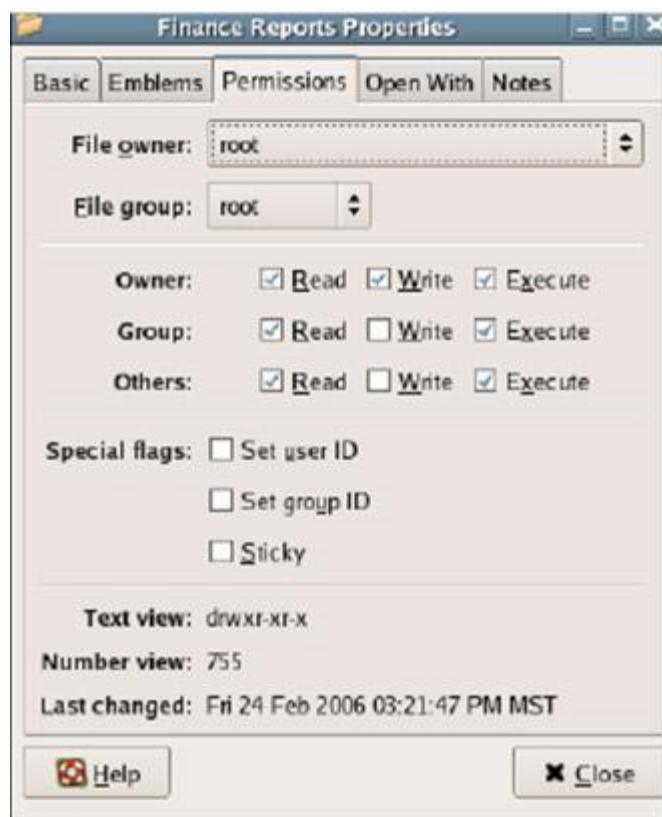
2. Nhập vào tên folder là *Shares* và nhấn **Enter**.



3. Tiếp theo tạo 2 folder con là **Finance Reports** và **Managers** trong **Shares Folder**



4. Bây giờ sẽ gán các quyền tương ứng cho người dùng trên những folder vừa tạo ra, hãy click chuột phải lên folder *Finance Reports* và chọn **Properties**. Trên cửa sổ thuộc tính chọn tab **Permissions** (nếu không thấy tab Permissions hãy restart lại hệ thống)



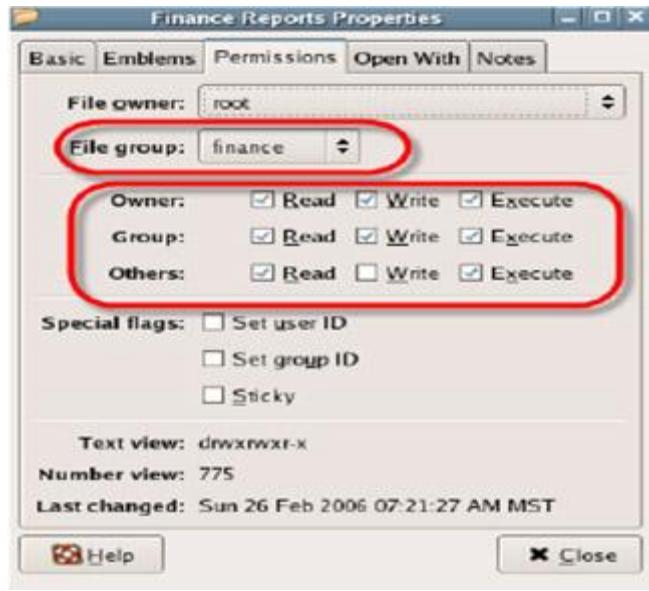
5. Thay đổi các quyền trên folder này như sau:

File Group = **finance**

Group Permissions = **Read, Write, và Execute**

Other Permissions = **Read only** (nếu muốn duyệt thư mục phải chọn Read & Execute)

Sau khi gán quyền như trên group Finance có thể truy cập folder này còn các user khác chỉ có quyền Read.



6. Tương tự hãy gán quyền cho folder Managers như sau:

File Group = managers

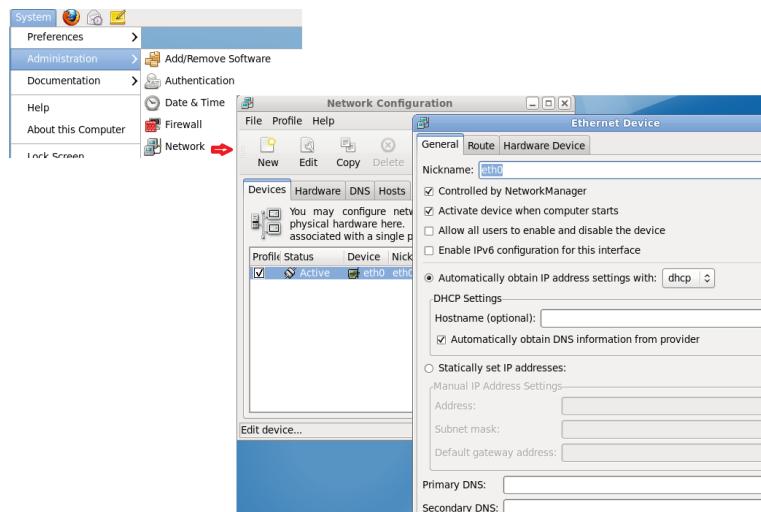
Group Permissions = Read, Write, và Execute

Other Permissions = (none)

Để kiểm tra kết quả của việc gán quyền cho các folder và group hãy đăng nhập bằng các tài khoản tương ứng và tiến hành các thao tác tạo file, folder, đọc hay xóa file...

C.5. CẤU HÌNH MẠNG VÀ XÂY DỰNG MÁY CHỦ DHCP TRÊN FEDORA

Cấu hình địa chỉ IP: Thiết lập địa chỉ IP máy tính



Cấu hình dịch vụ cấp phát IP động:

Thành phần của một DHCP server bao gồm bốn mục chính sau :

<i>Thành phần</i>	<i>Chức năng</i>
Options	Dùng để cung cấp các yếu tố cho phía client như địa chỉ IP, địa chỉ subnet mask, địa chỉ Gateway, địa chỉ DNS .v.v...
Scope	Một đoạn địa chỉ được quy định trước trên DHCP server sẽ dùng để gán cho các máy client.
Reservation	Là những đoạn địa chỉ dùng để “để dành” trong một scope đã quy định ở trên.
Lease	Thời gian “cho thuê” địa chỉ IP đối với mỗi client.

Cài đặt:

Để sử dụng được dịch vụ DHCP này, phải cài đặt vào hệ thống thông thường bằng gói dịch vụ có sẵn trên đĩa CD có phần đuôi mở rộng là *.rpm*, ngoài ra có thể cài đặt package ở dạng *source code* và tải gói này về từ trang web của GNU. Quá trình cài đặt bao gồm những bước sau đây :

- Ở dạng phần đuôi mở rộng là *.rpm*, ta chạy lệnh:
rpm -ivh dhcp-.rpm*

- Ở dạng source code, ta biên dịch như sau :
tar -xzvf dhcp-.tar.gz*

*cd dhcp-**

./configure

make

make install

Sau khi hoàn tất xong quá trình cài đặt, kế tiếp sẽ cấu hình để dịch vụ này có thể hoạt động theo ý muốn của bằng cách tạo và sửa đổi file */etc/dhcpd.conf*. Tập tin này sẽ có những nội dung sau :

```

deny client-updates;
ddns-update-style interim;

subnet 192.168.0.0 netmask 255.255.255.0 {
    range dynamic-bootp 192.168.0.190 192.168.0.240;

    option routers 192.168.0.10;
    option subnet-mask 255.255.255.0;

    option nis-domain "mydomain.com";
    option domain-name "mydomain.com";
    option domain-name-servers 192.168.0.20;
    option netbios-name-servers 192.168.0.100;
    option ntp-servers 192.168.0.25;
    option smtp-server 192.168.0.35;

    default-lease-time 360000;
    max-lease-time 259200;
}

```

Client-definitions

```

host big-daddy {
    hardware ethernet 00:a0:d9:cb:94:8a;
    fixed-address 192.168.0.18;
}

```

Các dòng trên có ý nghĩa như sau :

- Hai dòng đầu tiên sẽ không cho phép DHCP Server cập nhật động DNS.
- Dòng kế tiếp là đoạn địa chỉ cần cung cấp cho hệ thống các máy con, bao gồm địa chỉ NET IDs và một đoạn địa chỉ. (Như ở trên Server sẽ cấp cho phía máy con một đoạn địa chỉ chạy từ 192.168.0.190 đến 192.168.0.240)
 - Option routers cung cấp cổng gateway mặc định.
 - Option subnet-mask Subnet mask mặc định cho phía client.
 - Option nis-domain cung cấp tên NIS Domain Server

- Option domain-name cung cấp tên domain mặc định nếu sử dụng FQDN
 - Option domain-name-servers cung cấp name-servers cho mạng.
 - Option netbios-name-servers cung cấp địa chỉ mặc định của WINS-server
 - Option ntp-servers cung cấp địa chỉ timeserver.
 - Option smtp-server cung cấp địa chỉ smtp-server (**đuy nhất chỉ 1 server**)
- Dòng cuối cùng là nếu dự định cấp một địa chỉ cố định cho một máy nào đó thì cần phải khai báo địa chỉ MAC của máy đó và IP tương ứng

Trước khi khởi động DHCP Server lên thì phải tạo một tập tin cuối cùng dùng để xem xét việc cấp phát các địa chỉ IP cho phía client:

```
touch /etc/dhcpd.lease
```

Để bật/tắt dịch vụ DHCP thì chạy hai script tương ứng như sau:

```
/etc/init.d/dhcpd start
```

```
/etc/init.d/dhcpd stop
```

C.6. XÂY DỰNG MÁY CHỦ DNS TRÊN FEDORA

DNS là dịch vụ cho phép ánh xạ, chuyển đổi tên của một hệ thống nối Internet ra địa chỉ IP của nó. Nguyên nhân của sự tồn tại của DNS là do con người có thói quen đặt tên cho các trang thiết bị mà các trang thiết bị thì lại chỉ có thể dùng số để liên lạc với nhau. Vào những thời kỳ đầu tiên của Internet, người ta lập bảng về mối liên hệ giữa tên và địa chỉ IP và cài đặt trên một máy tính để tất cả cùng tham khảo. Nhưng với sự phát triển quá nhanh của Internet, bảng này phát triển nhanh chóng và không một máy nào có thể hoàn thành nổi nhiệm vụ tuy đơn giản nhưng lại rất quan trọng này. Hơn nữa, mỗi thay đổi dù ở đâu cũng phải thông qua server trung tâm. Điều này trở nên không thể chấp nhận được vì luôn có thay đổi trên Internet. Một giải pháp được cộng đồng Internet chấp nhận là chia toàn bộ không gian các địa chỉ IP và tên ra thành các nhóm logic nhỏ hơn. Mỗi nhóm có quyền tổ chức thông tin của các máy của mình.

Như vậy bước đầu tiên, một máy nối vào Internet, không phụ thuộc vào việc nó có chạy hay không DNS server, phải được cấu hình resolver, tức là chỉ ra cách thức hành động khi có yêu cầu phân giải địa chỉ. Resolver được cấu hình qua tập tin **/etc/host.conf**:

```
[root@priser tuanql]# more /etc/host.conf
```

```
order hosts,bind
```

```
multi on
```

- Dòng thứ nhất của **/etc/host.conf** cho biết khi có yêu cầu phân giải tên, resolver sẽ xem xét đầu tiên tập tin **/etc/hosts** sau đó đến sử dụng DNS server (**bind**).
- Dòng thứ hai cho phép một host có nhiều địa chỉ IP trong tập tin **/etc/hosts**.

Tập tin **/etc/hosts** chính là tiền thân của dịch vụ DNS. Hiện nay, **/etc/hosts** chỉ còn thường lưu các địa chỉ của mạng nội bộ hay dùng tới nhất đối với một máy. Khi yêu cầu phân giải vượt qua khả năng trả lời của **/etc/hosts** từ khóa **bind** chỉ ra cần phải sử dụng dịch vụ DNS. BIND là viết tắt của Berkeley Internet Name Domain và một triển khai rộng rãi nhất của dịch vụ DNS hiện nay.

Khi đó, resolver cần thông tin tiếp theo về DNS server. Thông tin này lưu trữ trong tập tin **/etc/resolv.conf**. Tập tin này kiểm tra cách resolver sử dụng DNS để phân giải địa chỉ. Nó quyết định DNS server cụ thể cần phải truy vấn và cách bổ sung phần domain cho phần tên của máy. Ví dụ một tập tin **/etc/resolv.conf**.

```
[root@Priser root]# more /etc/resolv.conf
```

```
search hcmutrans.edu.vn
```

```
nameserver 192.168.2.10
```

```
[root@priser root]#
```

Dòng đầu tiên cho phép resolver không chỉ phân giải tên như chương trình client yêu cầu, mà trong trường hợp phân giải không thành công, tiếp tục thử phân giải tên với phần domain tiếp nối sau. Ví dụ muốn tìm địa chỉ máy ITdep . Nếu quá trình phân giải ITdep không thành công, resolver sẽ thử phân giải *Itdep.hcmutrans.edu.vn*. Dòng tiếp theo là địa chỉ của name server cần phải truy vấn. Nhớ rằng địa chỉ của name server là số IP chứ

không phải là tên, vì nếu ngược lại, ai sẽ là người phân giải tên cho máy làm nhiệm vụ phân giải tên?

Bây giờ sẽ chuyển qua xem xét đến cấu hình của bản thân name server. Chương trình server của DNS name server là một chương trình daemon named (đọc là nêm đê). Named thường được khởi động ngay từ đầu cùng với khởi động của hệ thống. Thường thì named được chạy thông qua một script trong /etc/rc.d/rc3.d/named . Trong quá trình khởi động named đọc các tập tin dữ liệu rồi chờ các yêu cầu phân giải qua cổng xác định trong tập tin /etc/service (thông thường là cổng 53). Named dùng đầu tiên là giao thức UDP để phân giải tên, nếu phân giải bằng UDP không có kết quả, named sẽ dùng TCP sau đó.

Tập tin đầu tiên được named tham chiếu là /etc/named.conf. Nội dung tập tin này của Linux Redhat 7.3 được cài mặc định là :

```
options {  
    directory "/var/named";  
};  
  
zone "." {  
    type hint;  
    file "root.hints";  
};  
  
zone "0.0.127.in-addr.arpa" {  
    type master;  
    file "pz/127.0.0";  
};
```

Mở đầu là từ khóa **options** cho phép nhập các tùy chọn (options) toàn cục. *directory "/var/named"*; cho biết là các tập tin sau đây sẽ là tương đối đối với thư mục này.

Ta có thể bổ sung thêm trong phần *options* dòng lệnh :

```
forwaders {203.162.4.1 ; 203.162.0.11;};
```

Khi đó, DNS server sẽ tham chiếu các name server **203.162.4.1**; **203.162.0.11** mỗi khi nó không tìm thấy câu trả lời trong dữ liệu mà nó có . Sau phần tham số toàn cục options, ta thấy các khối zone “tên_zone “ { type master (hoặc slave hoặc hint); file “tên_tập_tin”; }; liên tiếp nhau.

Đối với mỗi domain, cần 2 tập tin dữ liệu. Tập tin thứ nhất lưu trữ các dữ liệu liên quan đến phân giải “xuôi “ từ name sang IP và tập tin thứ hai để phân giải “ngược“ từ IP ra name. Trừ miền “.” có tính chất giúp đỡ là có tập tin cache đặc biệt

; There might be opening comments here if you already have this file.

; If not don't worry.

;

. 6D IN NS G.ROOT-SERVERS.NET.

. 6D IN NS J.ROOT-SERVERS.NET.

. 6D IN NS K.ROOT-SERVERS.NET.

. 6D IN NS L.ROOT-SERVERS.NET.

. 6D IN NS M.ROOT-SERVERS.NET.

. 6D IN NS A.ROOT-SERVERS.NET.

. 6D IN NS H.ROOT-SERVERS.NET.

. 6D IN NS B.ROOT-SERVERS.NET.

. 6D IN NS C.ROOT-SERVERS.NET.

. 6D IN NS D.ROOT-SERVERS.NET.

. 6D IN NS E.ROOT-SERVERS.NET.

. 6D IN NS I.ROOT-SERVERS.NET.

. 6D IN NS F.ROOT-SERVERS.NET.

G.ROOT-SERVERS.NET. 5w6d16h IN A 192.112.36.4

J.ROOT-SERVERS.NET. 5w6d16h IN A 198.41.0.10

K.ROOT-SERVERS.NET. 5w6d16h IN A 193.0.14.129

L.ROOT-SERVERS.NET. 5w6d16h IN A 198.32.64.12

M.ROOT-SERVERS.NET. 5w6d16h IN A 202.12.27.33

A.ROOT-SERVERS.NET. 5w6d16h IN A 198.41.0.4
H.ROOT-SERVERS.NET. 5w6d16h IN A 128.63.2.53
B.ROOT-SERVERS.NET. 5w6d16h IN A 128.9.0.107
C.ROOT-SERVERS.NET. 5w6d16h IN A 192.33.4.12
D.ROOT-SERVERS.NET. 5w6d16h IN A 128.8.10.90
E.ROOT-SERVERS.NET. 5w6d16h IN A 192.203.230.10
I.ROOT-SERVERS.NET. 5w6d16h IN A 192.36.148.17
F.ROOT-SERVERS.NET. 5w6d16h IN A 192.5.5.241

Đây thực chất là địa chỉ IP của các name server gốc (root) của Internet.

Ví dụ như đối với miền hcmutrans.edu.vn ta cần có :

```
zone "hcmutrans.edu.vn" {  
    type master;  
    file "db.hcmutrans.edu.vn";  
};  
zone "1.16.172.in-addr.arpa" {  
    type master;  
    file "db.172.16.1";
```

Chú ý các viết cú pháp *1.16.172.in-addr.arpa* cho tên của miền phân giải ngược IP ra name.

Sau đây ta sẽ xem xét đến cấu trúc tập tin
/var/named/db.hcmutrans.edu.vn

```
@ IN SOA hcmutrans.edu.vn. root.hcmutrans.edu.vn. (  
199609206 ; serial, todays date + todays serial #  
8H ; refresh, seconds  
2H ; retry, seconds  
1W ; expire, seconds  
1D ) ; minimum, seconds
```

NS hcmutrans.edu.vn.

MX 10 hcmutrans.edu.vn. ; Primary Mail Exchanger

TXT "MCSEVIETNAM Corporation"

localhost A 127.0.0.1

hcmutrans.edu.vn. A 172.16.1.1

linuxsrv A 172.16.1.1

www A 172.16.1.1

ftp CNAME hcmutrans.edu.vn.

mail CNAME hcmutrans.edu.vn.

news CNAME hcmutrans.edu.vn.

Ký tự “@” đầu tiên thay cho miền *hcmutrans.edu.vn*; IN là Internet ; SOA là Start Of Authority; tiếp nối bởi tên miền và địa chỉ người chịu trách nhiệm. Chú ý là trong địa chỉ email của người chịu trách nhiệm, dấu @ quen thuộc được thay bằng dấu chấm “.”. Sau các tên miền có dấu chấm “.” ở cuối. Trong tất cả các tập tin dữ liệu của DNS, những tên không kết thúc bởi dấu chấm sẽ được DNS server thêm vào tên miền tương ứng của tập tin đó. Ví dụ đây là tập tin ứng với miền *hcmutrans.edu.vn*, **ITdep** sẽ được bổ sung thêm thành *ITdep.hcmutrans.edu.vn*.

Sau phần ngoặc đơn với 5 số miêu tả số serie và các thông số thời gian của thông tin, bắt đầu các dòng (record) dữ liệu. **Khoảng trắng** ở đầu dòng tương đương với tên miền (như dấu @), **NS** ám chỉ record dạng nameserver. **MX** là mail exchange, dùng để chỉ ra máy chịu trách nhiệm nhận thư điện tử cho domain này. Số 10 là mức độ ưu tiên cho mail server này. Độ ưu tiên sẽ càng cao nếu số càng nhỏ . **A** là viết tắt của Address, sẽ tiếp theo bởi một địa chỉ IP. **CNAME** là canonical name . Với CNAME ta có thể gán cho máy biệt danh tùy ý tiện cho việc sử dụng. Các dòng bắt đầu bởi ; là các chú thích.

Ví dụ tập tin dùng cho phân giải ngược **/var/named/db.172.16.1**

@ IN SOA hcmutrans.edu.vn. root.hcmutrans.edu.vn. (

199609206 ; Serial

28800 ; Refresh

7200 ; Retry

```

604800 ; Expire

86400) ; Minimum TTL

NS hcmutrans.edu.vn.

;

; Servers

;

1 PTR simbahcm.hcmutrans.edu.vn.

2 PTR trantungbre.hcmutrans.edu.vn.

3 PTR hungden.hcmutrans.edu.vn.

;

```

Cấu trúc tập tin **/var/named/db.172.16.1** có phần đầu giống hệt như tập tin phân giải xuôi. Chỉ có từ khóa **PTR = Pointer** là khác.

Việc cấu hình các dữ liệu của name server cần rất thận trọng vì nhiều khi lỗi của nó rất khó tìm. Mỗi khi thay đổi dữ liệu, cần phải khởi động lại named bằng cách sử dụng kill -9 named_PID để dừng named rồi khởi động lại bằng cách nhập dòng lệnh named. Tập tin */var/log/messages* có thể giúp đỡ nhiều để tìm ra lỗi nếu named không hoạt động theo muốn. Để thử hoạt động của quá trình phân giải tên, Linux có lệnh **nslookup** với nhiều tính năng rất mạnh. Xem manpage của nslookup để biết cách sử dụng.

C.7. XÂY DỰNG MÁY CHỦ FILE – SAMBA

Khái niệm:

Ngày nay nhu cầu chia sẻ tài nguyên trong mạng nội bộ là không thể thiếu. Chia sẻ đĩa, chia sẻ thư mục, máy in dùng chung trong mạng nội bộ. Trong bài này hướng dẫn nối mạng Linux với Windows sử dụng giao thức *Server Message Block (SMB)*, hay còn gọi là *Session Message Block* để giao tiếp và chia sẻ tập tin, máy in lẫn nhau. Sử dụng chương trình Samba để đáp ứng nhu cầu trên. Biểu tượng Linux PC xuất hiện trong Windows Network Neighborhood.

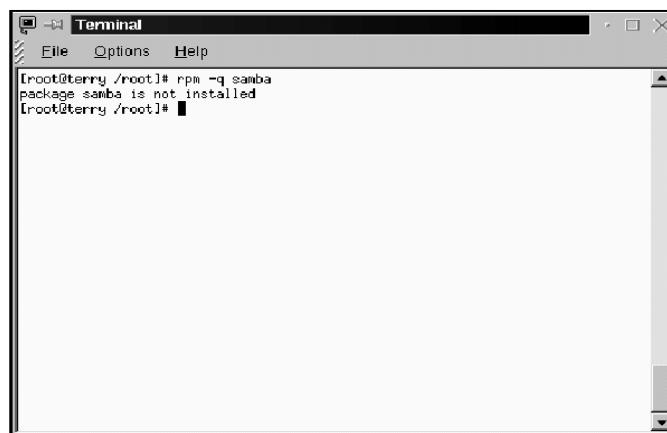
Samba: giao thức *Server Message Block (SMB)*, hay còn gọi là *Session Message Block*.

Giao thức SMB được dùng để chia sẻ dữ liệu và máy in cho Microsoft Windows 3.11, NT và 95/98. Sử dụng công cụ Samba trên Linux có thể chia sẻ tài nguyên của Linux cho Windows. Bốn điều cơ bản Samba có thể làm:

- Chia sẻ dữ liệu Linux cho Windows
- Chia sẻ SMB với máy Linux
- Chia sẻ máy in trên Linux cho Windows
- Chia sẻ máy in trên Windows cho Linux

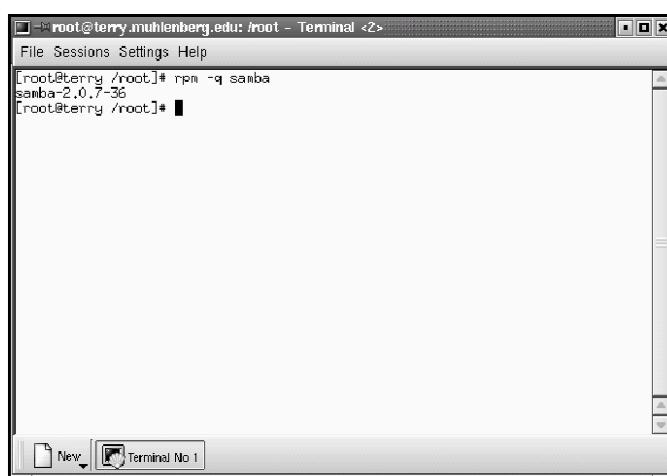
Cài đặt và cấu hình Samba

- Kiểm tra xem Samba đã cài chưa: dùng lệnh rpm -q samba
 - + Nếu chưa cài thì màn hình terminal sẽ trả về



```
[root@terry /root]# rpm -q samba  
package samba is not installed  
[root@terry /root]#
```

- + Nếu đã cài màn hình terminal sẽ trả về



```
[root@terry /root]# rpm -q samba  
samba-2.0.7-36  
[root@terry /root]#
```

Thư mục cài Samba

Directory	Miêu tả
/usr/local/samba	Thư mục chính
/usr/local/samba/bin	Binaries
/usr/local/samba/lib	smb.conf, lmhosts, configuration files, etc.
/usr/local/samba/man	Tài liệu hướng dẫn Samba
/usr/local/samba/private	File password đã mã hóa
/usr/local/samba/swat	Files SWAT
/usr/local/samba/var	Samba log files, lock files, browse list info, shared memory files, process ID files

Nếu chưa cài Samba, có thể vào website www.samba.org theo hướng dẫn của trang web để tải tập tin RPM.

Để cài đặt dùng lệnh rpm -i samba

Từ Version 2.0 trở đi Samba kèm theo tên ích Swat (công cụ quản trị Samba qua giao diện Web), công cụ này cho phép cấu hình Samba một cách dễ dàng. Swat cho phép bạn dùng trình duyệt web thay đổi trực tiếp lên tập tin cấu hình chính của Samba /etc/smb.conf

File cấu hình chính Samba /etc/samba/smb.conf

```
# Samba config file created using SWAT
# from localhost (127.0.0.1)
# Date: 2000/05/25 10:29:40
# Global parameters
```

[global]

```
workgroup = ONE
netbios name = TERRY
server string = Samba Server
security = SHARE
log file = /var/log/samba/log
max log size = 50
socket options = TCP_NODELAY SO_RCVBUF=8192 SO_SNDBUF=8192
wins support = Yes
hosts allow = 192.168.1.
hosts deny = all
```

[homes]

```
comment = Home Directories
read only = No
[printers]
comment = All Printers
path = /var/spool/samba
guest ok = Yes
print ok = Yes
browseable = Yes
```

[test]

```
path = /tmp/sambatest
valid users = test
read only = no
guest ok = no
browseable = yes
```

[global]

[Global] là phần đầu tiên của smb.conf, mỗi phần trong smb.conf gồm lựa chọn và giá trị định dạng: option = values .Bạn có hàng trăm lựa chọn và giá trị định dạng khác nhau. Dưới đây là những định dạng chung nhất

Workgroup = TuanQL tên của workgroup xuất hiện trong network properties trên máy windows

Netbios name = Linux là tên mà Samba server sẽ được biết bởi máy windows

Server string = Samba Server là tên của Samba server

Security = SHARE mức độ quyền trên Server, các mức độ khác: User , Default, Domain, Server. Sử dụng Share sẽ dễ dàng tạo chia sẻ cho anonymous, không cần chứng thực.

Log_file = /var/log/samba/log thư mục chứa tập tin log

max log size = 50 dung lượng tối đa của tập tin log tính bằng KB

socket options = TCP_NODELAY SO_RCVBUF=8192 SO_SNDBUF=8192 tối ưu hóa server

wins support = Yes samba server đóng vai trò là Wins Server

hosts allow = 192.168.1. chỉ cho phép yêu cầu từ network này

hosts deny = all không nhận yêu cầu từ tất cả các host

Lựa chọn này cho phép người dùng nhanh chóng truy nhập vào thư mục home của họ

comment = Home Directories ghi chú

read only = No người dùng có toàn quyền trong thư mục home của họ

Thiết lập lựa chọn máy in

Path = /var/spool/samba thư mục của máy in

Guest ok = Yes cho phép guest truy cập vào máy in

Print ok = Yes cho phép người dùng sử dụng máy in

Browsable = Yes biểu tượng máy in sẽ xuất hiện trong browse list

[test]

Cấu hình chia sẻ thư mục test trên Linux

Path = /tmp/sambatest đường dẫn thư mục chia sẻ

Valid users = test chỉ định người dùng sử dụng thư mục này

Read only = No cho phép quyền ghi trên thư mục

Guest ok = No không cho guest quyền truy nhập

read only = No người dùng có toàn quyền trong thư mục home của họ

Browsable = Yes thư mục share sẽ xuất hiện trong browse list

Sử dụng Swat: Trước khi có thể sử dụng Swat cần thay đổi 2 tập tin để bật tiện ích này lên.

+ Thêm vào /etc/services

Swat 901/tcp

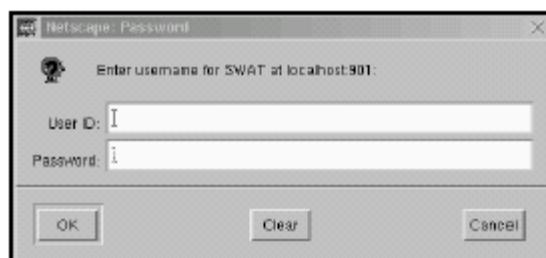
+ Thêm vào /etc/inetd.conf

Swat stream tcp nowait.400 root /usr/sbin/swat swat

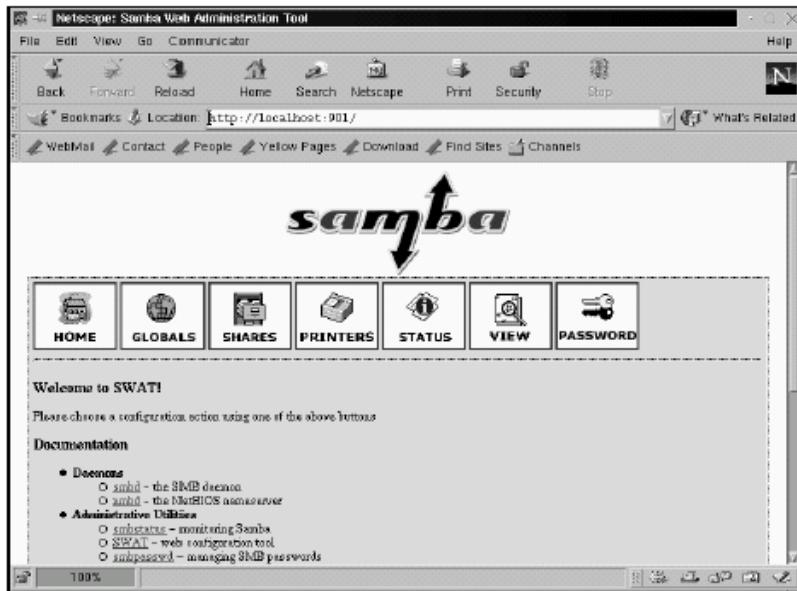
+ khởi động lại Inetd

killall -HUP inetd

Sử dụng trình duyệt web để chạy Swat <http://localhost:901>. Hộp thoại yêu cầu nhập User ID và mật khẩu xuất hiện, đăng nhập với quyền root:



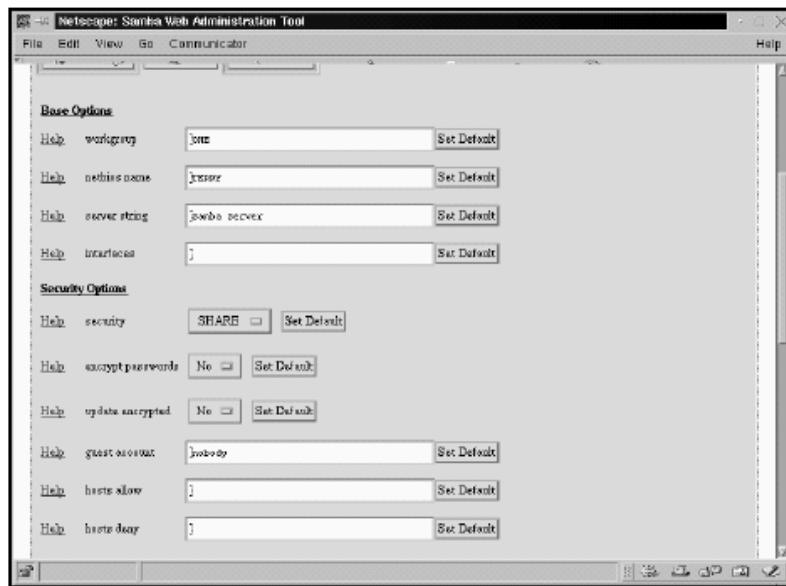
Đầu tiên bạn phải cấu hình [globals] bằng cách bấm vào biểu tượng GLOBALS



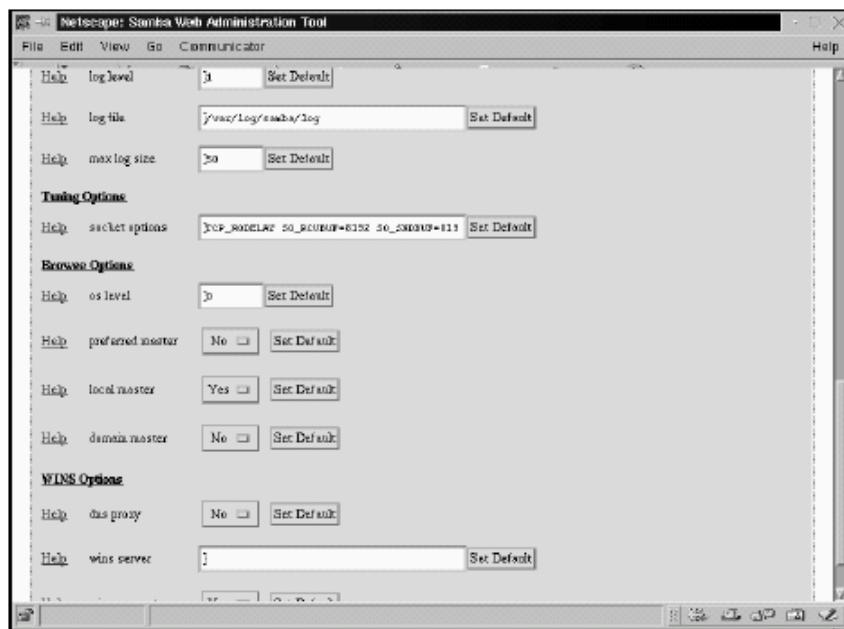
Những biến Global xuất hiện. Giá trị này là giá trị file smb.conf



Trang Global Variables cho phép người quản trị dễ cấu hình [Globals] trong file smb.conf. Trang Global Variables chia thành 6 lựa chọn: Base Options, Security Options, Logging Options, Tuning Options, Browse Options, WINS Options.



Base và Security Options



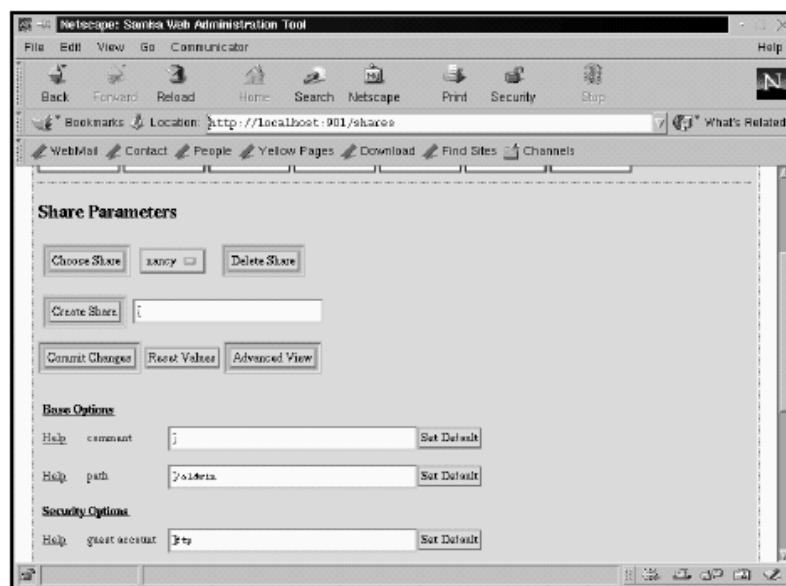
Log, tuning, browse, và WINS options

Sau khi điền vào những giá trị cần thiết, bấm vào Commit Changes để lưu thay đổi. Tiếp theo chọn biểu tượng SHARES để mở trang Share Parameters

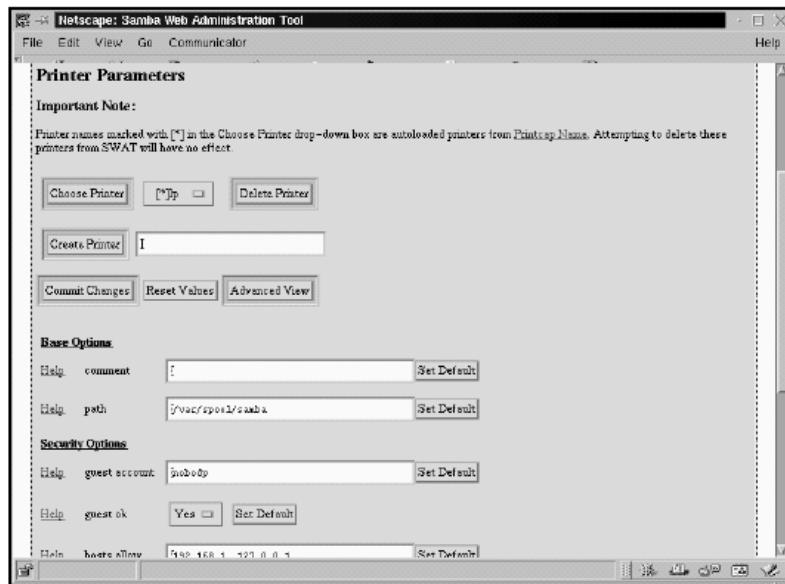


Trang Share Parameters

Để tạo chia sẻ điền vào tên share và nhấn nút Create Share



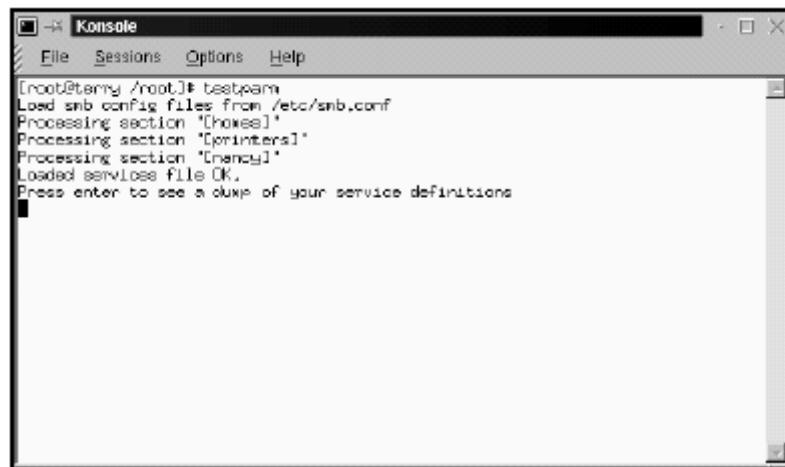
Điền vào những thông tin cấu hình để Windows có thể truy cập vào Samba server. Sau khi hoàn tất nhấn Commit Changes để lưu vào file smb.conf. Tiếp theo chia sẻ máy in cho máy Windows sử dụng. Chọn biểu tượng PRINTERS.



Hiển thị tên máy in đã chọn

Để tạo mới chọn Create Printer, nếu bạn đã có sẵn máy in bạn có thể chọn từ menu Drop-down. Chú ý nếu bạn đã cài sẵn máy in trong RedHat, nó sẽ được sử dụng như máy in mặc định trong samba và không thể xóa. Nhấn vào Commit Changes để lưu lại vào smb.conf.

Sau khi đã hoàn tất sử dụng tiện ích testparm để kiểm tra lại. Từ màn hình dòng lệnh gõ vào: testparm



Tiện ích testparm kiểm tra lỗi tập tin smb.conf

Sau khi thay đổi file smb.conf, bạn phải khởi động lại samba. Khởi động Samba bằng dòng lệnh: /usr/sbin/samba start hoặc /etc/init.d/samba start . Để khởi động Samba bằng Swat chọn biểu tượng STATUS. 2 dịch vụ smbd và nmbd phải được khởi động.



Trang Server Status cho biết hiện trạng của samba server

Sau khi Samba khởi động, dùng lệnh smbclient trên localhost để thấy thông tin cấu hình samba: smbclient -L localhost

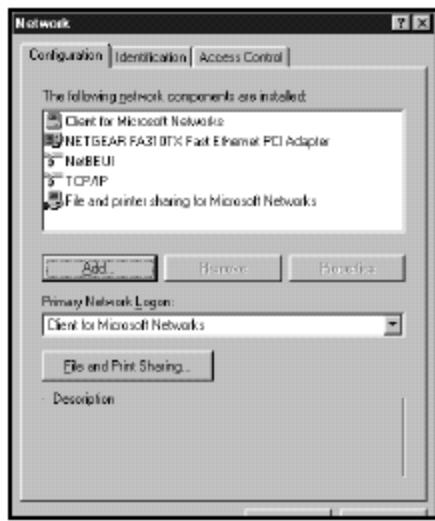
```

[root@terry ~root]# smbclient -L localhost
Password:
Domain=[CNE] OS=[Unix] Server=[Samba 2.0.5a]
[Sharename      Type      Comment]
[homes          Disk      Home Directories]
[nancyd         Disk      ]
[IPC$           IPC       IPC Service (Samba Server)]
[lp              Printer   ]
[Server          Comment   ]
[TERRY          Samba Server]
[Workgroup      Master    ]
[CNE            TERRY     ]

```

Cấu hình Samba Client

Trên máy Windows Client phải được cài “Client for Microsoft Network” và “File and printer sharing for Microsoft Networks”, Hộp thoại Network Properties:



Kiểm tra Samba server

Trên máy Windows -> Network Neighborhood .Trong cửa sổ Network Neighborhood, có thể thấy được danh sách máy Windows, những thư mục chia sẻ, cũng sẽ thấy Linux Server. Trên máy Linux cũng có thể truy cập vào thư mục Windows bằng lệnh smbclient: smbclient //tên máy tính/tên thư mục

MỤC LỤC

CHƯƠNG 1. KHÁI QUÁT VỀ QUẢN TRỊ MẠNG	1
1.1. MỤC TIÊU, QUY TRÌNH VÀ CÁC HOẠT ĐỘNG QUẢN TRỊ MẠNG	1
1.1.1. Các đối tượng quản trị	3
1.1.2. Chính sách hệ thống.....	5
1.1.3. Quản lý tài nguyên	6
1.1.4. Giám sát hệ thống.....	7
1.2. MÔI TRƯỜNG VÀ CÔNG CỤ QUẢN TRỊ	7
1.2.1. Các môi trường mạng	7
1.2.2. Các mô hình mạng trong môi trường Microsoft	8
1.2.3. Giới thiệu Active Directory.....	9
1.2.4. Các công cụ quản trị.....	15
1.3. TỔNG KẾT CHƯƠNG	20
CHƯƠNG 2. CÀI ĐẶT VÀ THIẾT LẬP MẠNG WINDOWS	23
2.1. THIẾT LẬP MẠNG NGANG HÀNG	23
2.1.1. Thiết lập cấu hình TCP/IP	23
2.1.2. Xây dựng Workgroup	26
2.2. CÀI ĐẶT VÀ THIẾT LẬP MẠNG KHÁCH/CHỦ.....	29
2.2.1. Cài đặt máy chủ.....	29
2.2.2. Xây dựng cấu trúc Active Directory.....	31
2.2.3. Gia nhập miền cho máy tính trạm	40
2.2. TỔNG KẾT CHƯƠNG	42
CÂU HỎI VÀ BÀI TẬP THỰC HÀNH	44
CHƯƠNG 3. QUẢN LÝ ĐỐI TƯỢNG	45
3.1. QUẢN LÝ CÁC OU	45
3.1.1. Tạo các OU	45
3.1.2. Đổi tên OU	47
3.1.3. Xoá OU	48
3.2. QUẢN LÝ TÀI KHOẢN NGƯỜI DÙNG	48
3.2.1. Quản lý tài khoản người dùng của máy	48
3.2.2. Quản lý tài khoản người dùng của miền	51
3.2.3. Thay đổi các thiết định về tài khoản người dùng	56
3.3. QUẢN LÝ CÁC TÀI KHOẢN NHÓM	60
3.3.1. Khái niệm nhóm	60
3.3.2. Các loại nhóm bảo mật	62
3.3.3. Các nhóm cục bộ được tạo sẵn	64
3.3.4. Các nhóm toàn miền và nhóm toàn rừng được tạo sẵn	68
3.3.5. Các nhóm đặc biệt	70
3.3.6. Tạo và quản lý tài khoản nhóm của miền	70
3.3.7. Tạo và quản lý tài khoản nhóm của máy.....	74
3.4. CÁC QUYỀN HẠN NGƯỜI DÙNG	75

3.5. ỦY THÁC QUYỀN QUẢN LÝ OU.....	80
3.6. TỔNG KẾT CHƯƠNG	85
CÂU HỎI VÀ BÀI TẬP THỰC HÀNH.....	87
CHƯƠNG 4. CHÍNH SÁCH NHÓM	89
4.1. CHỨC NĂNG, PHÂN LOẠI VÀ SỬ DỤNG CHÍNH SÁCH NHÓM.....	89
4.2. TẠO CÁC ĐỐI TƯỢNG CHÍNH SÁCH NHÓM	92
4.3. ỦY THÁC QUYỀN QUẢN TRỊ CHÍNH SÁCH NHÓM	101
4.4. TÍNH NĂNG CÀI ĐẶT GÓI PHẦN MỀM CỦA CHÍNH SÁCH NHÓM	106
4.4.1. Quảng bá và phân bổ gói phần mềm	108
4.5. QUẢN LÝ GÓI PHẦN MỀM ĐÃ PHÂN BỐ HOẶC QUẢNG BÁ.....	113
4.5.1. Thay đổi một số đặc tính của gói phần mềm	113
4.5.2. Triển khai lại một gói phần mềm	115
4.5.3. Gỡ bỏ một gói phần mềm	115
4.6. TỔNG KẾT CHƯƠNG	116
CÂU HỎI VÀ BÀI TẬP THỰC HÀNH.....	117
CHƯƠNG 5. QUẢN LÝ TÀI NGUYÊN MẠNG	119
5.1. QUẢN LÝ FILE VÀ THƯ MỤC	119
5.1.1. Chế độ bảo mật của NTFS	119
5.1.2. Chia sẻ và quản lý quyền truy cập từ xa	124
5.1.3. Trao quyền truy cập cục bộ.....	131
5.1.4. Lấy quyền sở hữu	137
5.1.5. Tổng hợp các quyền truy cập	139
5.2. QUẢN LÝ Ổ ĐĨA.....	141
5.2.1. Cấu hình hệ thống tập tin	141
5.2.2. Cấu hình đĩa lưu trữ	141
5.2.3. Sử dụng chương trình disk Manager	142
5.2.4. Quản lý việc nén dữ liệu.....	150
5.2.5. Thiết lập hạn ngạch đĩa (Disk Quota)	152
5.3. DỊCH VỤ IN TRÊN MẠNG	155
5.3.1. Quá trình in trên mạng	155
5.3.2. Cài đặt và chia sẻ máy in cục bộ.....	157
5.3.3. Kết nối máy in cục bộ đã chia sẻ	162
5.3.4. Một số thiết định về máy in	165
5.4. SAO LUU VÀ PHỤC HỒI.....	171
5.4.1. Khái niệm sao lưu và phục hồi dữ liệu	171
5.4.2. Sử dụng Windows Server Backup	171
5.4.3. Phục hồi dữ liệu	184
5.5. TỔNG KẾT CHƯƠNG	189
CÂU HỎI VÀ BÀI TẬP THỰC HÀNH.....	190
CHƯƠNG 6. DỊCH VỤ DNS VÀ DHCP.....	193

6.1. DỊCH VỤ DNS	193
6.1.1. Một số khái niệm	193
6.1.2. Những loại bản ghi phổ biến trong DNS	194
6.1.3. Cài đặt DNS server	196
6.1.4. Tạo ra các Zone	197
6.1.5. Tạo các bản ghi	200
6.1.6. Cấu hình dịch vụ DNS trên máy khách	205
6.2. DỊCH VỤ DHCP	205
6.2.1. Cài đặt DHCP server	205
6.2.3. Tạo ra một scope (tầm)	207
6.2.4. ấn định các thông số tùy chọn cho tất cả các scope	215
6.2.5. Cấu hình dịch vụ DHCP bên máy khách	216
6.2.6. Các bước nhận một địa chỉ IP từ DHCP server	217
6.3. TỔNG KẾT CHƯƠNG	218
CÂU HỎI VÀ BÀI TẬP THỰC HÀNH.....	219
CHƯƠNG 7.GIÁM SÁT HỆ THỐNG.....	222
7.1. CÁC KỸ NĂNG GIÁM SÁT MÁY CHỦ	222
7.2. SỬ DỤNG TASK MANAGER	223
7.3. SỬ DỤNG EVENT VIEWER	228
7.4. SỬ DỤNG PERFORMANCE CONSOLE	237
7.5. TỔNG KẾT CHƯƠNG	241
CÂU HỎI VÀ BÀI TẬP THỰC HÀNH.....	243
TÀI LIỆU THAM KHẢO	244
PHỤ LỤC A. TRIỂN KHAI HỆ THỐNG MẠNG TRÊN CÁC MÁY ẢO	245
A.1. Tạo máy ảo với VMWare	245
A.2. Quản lý cấu hình phần cứng	248
A.3. Nhận bản máy ảo	252
A.4. Tạo điểm phục hồi.....	252
PHỤ LỤC B. CÀI ĐẶT WINDOWS SERVER 2008	254
PHỤ LỤC C. QUẢN TRỊ MẠNG TRONG LINUX.....	259
C.1. GIỚI THIỆU CHUNG VỀ LINUX.....	259
C.1.1. Lịch sử phát triển của Linux	260
C.1.2. Kiến trúc của Linux	260
C.1.3. Các bản phân phối hệ điều hành họ Linux	261
C.2. CÀI ĐẶT VÀ SỬ DỤNG HỆ THỐNG FEDORA	263
C.3. HỆ THỐNG TẾP TIN VÀ THƯ MỤC	276
C.3.1. Hệ thống tệp tin và thư mục trong Linux.....	276
C.3.2. Quyền truy nhập thư mục và file	280

C.4. QUẢN LÝ TÀI KHOẢN NGƯỜI DÙNG VÀ NHÓM	282
C.5. CẤU HÌNH MẠNG VÀ XÂY DỰNG MÁY CHỦ DHCP TRÊN FEDORA.....	291
C.6. XÂY DỰNG MÁY CHỦ DNS TRÊN FEDORA	294
C.7. XÂY DỰNG MÁY CHỦ FILE – SAMBA	300
BẢNG THUẬT NGỮ.....	v
DANH MỤC HÌNH VẼ	vii

BẢNG THUẬT NGỮ

STT	Ký hiệu	Thuật ngữ
1	OU	Organizational Unit
2	AD	Active Directory
3	DC	Domain Controller
4	NTFS	New Technology File System
5	CSDL	Cơ sở dữ liệu
6	HDH	Hệ điều hành
7	GUI	Graphical User Interface
8	SAM	Security Accounts Manager
9	PDC	Primary Domain Controller
10	DNS	Domain Name System
11	MMC	Microsoft Management Console
12	RDC	Remote Desktop Connection
13	TCP	Transmission Control Protocol
14	IP	Internet Protocol
15	SID	Security Identifier
16	ACL	Access Control List
17	GPO	Group Policy Object
18	SI	Software Installation
19	MSI	MicroSoft Installer
20	CD	Compact Disc
21	EFS	Encrypting File System
22	FAT	File Allocation Table

23	DHCP	Dynamic Host Configuration Protocol
----	------	-------------------------------------

DANH MỤC HÌNH VẼ

Hình 1.1: Công việc và quy trình quản trị mạng	3
Hình 1.2: Cấu trúc các OU trong miền HVKTMM.COM	12
Hình 1.4: Rừng của các cây	15
Hình 1.5: Cửa sổ MMC trống	16
Hình 1.6: Cửa sổ thêm/loại bỏ các Snap-in hoặc thư mục	17
Hình 1.7: Lựa chọn chỉnh sửa phần mở rộng	18
Hình 1.8: Cửa sổ console sau khi hoàn tất	19
Hình 1.9: Cửa sổ console Hardware sau khi hoàn tất	19
Hình 1.10: Kết nối quản trị từ xa	20
Hình 2.1: Lựa chọn kết nối mạng để cấu hình	23
Hình 2.2: Lựa chọn giao thức TCP/IP	24
Hình 2.3: Cấu hình địa chỉ IP	25
Hình 2.4: Kiểm tra cấu hình IP	26
Hình 2.6: Tìm kiếm thiết lập workgroup trên Windows 8	27
Hình 2.7: Tìm kiếm thiết lập workgroup trên Windows 7	27
Hình 2.8: Lựa chọn thay đổi các thiết lập cho workgroup	28
Hình 2.9: Thay đổi Workgroup	28
Hình 2.10: Thiết lập Workgroup mới	29
Hình 2.11: Các yêu cầu phần cứng cho Windows Server 2008	30
Hình 2.12: Các tính năng chính theo các phiên bản của Windows Server 2008	31
Hình 2.13: Giao diện quản lý role	31
Hình 2.14: Thông báo chuẩn bị cài đặt	32
Hình 2.15: Các thư viện yêu cầu để chạy dcpromo	32
Hình 2.16: Giao diện cài đặt thành công	33
Hình 2.17: Lựa chọn cài đặt dcpromo	33

Hình 2.18: Bắt đầu cài đặt dcpromo	34
Hình 2.19: Lựa chọn để tạo một rừng mới	34
Hình 2.20: Nhập tên miền	35
Hình 2.21: Lựa chọn tên miền tương thích với NetBIOS	35
Hình 2.22: Thiết lập chức năng mức rừng	36
Hình 2.23: Giao diện lựa chọn máy chủ DNS	37
Hình 2.24: Cảnh báo khi tạo máy chủ DNS đầu tiên	37
Hình 2.25: Định vị các thư mục cho DNS	38
Hình 2.26: Mật khẩu và xác nhận mật khẩu	38
Hình 2.27: Xác nhận thông tin về DNS	39
Hình 2.28: Lựa chọn khởi động lại khi cài đặt thành công	40
Hình 2.29: Lựa chọn thiết lập địa chỉ IP	40
Hình 2.30: Lựa chọn Change để gia nhập miền	41
Hình 2.31: Lựa chọn tên miền muốn gia nhập	42
Hình 2.32: Lựa chọn khởi động lại máy sau khi gia nhập miền	42
Hình 2.33: Khởi động lại	42
Hình 3.1: Cửa sổ Active Directory Users and Computers	45
Hình 3.2: Cửa sổ khai báo OU mới	46
Hình 3.3: Cửa sổ Active Directory Users and Computers sau khi tạo thêm OU PTHUCHANH	47
Hình 3.4: Đổi tên OU	47
Hình 3.5: Xóa OU	48
Hình 3.6: Cửa sổ Computer Management	49
Hình 3.7: Cửa sổ tạo tài khoản người dùng của máy	50
Hình 3.8: Cửa sổ Active Directory Users and Computers	51
Hình 3.9: Cửa sổ tạo tài khoản người dùng của miền	52
Hình 3.10: Cửa sổ ấn định các tùy chọn về mật khẩu và tài khoản	53
Hình 3.11: Cửa sổ xác nhận thông tin của tài khoản người dùng trước khi tạo	54

Hình 3.12: Cửa sổ Active Directory Users and Computers sau khi tạo thêm tài khoản người dùng mới Nguyen Thu Ha	55
Hình 3.13: Cửa sổ chọn nơi chứa mới của tài khoản người dùng	55
Hình 3.14: Cửa sổ đổi mật khẩu mới của tài khoản người dùng	56
Hình 3.15: Cửa sổ đặc tính của tài khoản người dùng	57
Hình 3.16: Trang Account của cửa sổ đặc tính	58
Hình 3.17: Cửa sổ ấn định ngày, giờ đăng nhập vào mạng	59
Hình 3.18: Cửa sổ ấn định người dùng được phép đăng nhập từ máy nào	60
Hình 3.19: Các nhóm cục bộ được tạo sẵn của máy	64
Hình 3.20: Các nhóm cục bộ được tạo sẵn của miền	66
Hình 3.21: Các nhóm toàn miền và nhóm toàn rừng được tạo sẵn	68
Hình 3.22: Cửa sổ tạo nhóm mới	71
Hình 3.23: Cửa sổ đặc tính của nhóm với trang General	72
Hình 3.24: Cửa sổ thêm thành viên mới cho nhóm	73
Hình 3.25: Cửa sổ chọn thành viên mới	73
Hình 3.26: Cửa sổ tạo nhóm mới	74
Hình 3.27: Danh sách các quyền hạn người dùng	76
Hình 3.28: Thêm bớt đối tượng được cấp quyền hạn người dùng	77
Hình 3.29: Cửa sổ chọn đối tượng mới để cấp quyền hạn người dùng	77
Hình 3.30: Giao diện ủy thác quản lý OU	81
Hình 3.31: Các quyền hạn ủy thác	82
Hình 3.32: Cửa sổ Active Directory Users and Computers ở chế độ xem Advanced Features	83
Hình 3.33: Trang Security của OU được chọn	84
Hình 3.34: Những thiết định chi tiết của OU được chọn	84
Hình 3.35: Các quyền hạn có thể trao cho đối tượng	85
Hình 4.1: Giao diện Group Policy Management	92
Hình 4.2: Giao diện tạo Group Policy Object	92

Hình 4.3: Cửa sổ đặc tính của một GPO	94
Hình 4.4: Danh sách các đối tượng được phép truy cập một GPO	94
Hình 4.5: Việc tháo gỡ một GPO ra khỏi danh sách các GPO liên kết với OU hiện tại	95
Hình 4.6: Các GPO có sẵn có thể liên kết với OU hiện tại	96
Hình 4.7: Giao diện cấu hình GPO	97
Hình 4.8: Cửa sổ đặt các thiết định của một chính sách nhóm	97
Hình 4.10: Các thiết định về chính sách khoá chặt tài khoản	100
Hình 4.15: Những thiết định chi tiết của OU được chọn	105
Hình 4.16: Các quyền hạn có thể trao cho đối tượng	106
Hình 4.17: Việc sao chép Skype vào một thư mục chia sẻ	109
Hình 4.18: Đặt tên cho GPO mới	110
Hình 4.19: Áp dụng GPO này cho hai nhóm Domain Admins và Enterprise Admins	110
Hình 4.20: Đưa gói phần mềm vào một GPO	111
Hình 4.21: Chọn gói phần mềm để đưa vào GPO	112
Hình 4.22: Chọn phương thức quảng bá gói phần mềm	113
Hình 4.23: Gói công cụ quản trị đã được đưa vào GPO với tên gọi Windows Server Administration Tools	113
Hình 4.24: Cửa sổ thay đổi một số đặc tính của gói phần mềm	114
Hình 4.25: Lựa chọn các xử lý các bản đã được cài đặt	115
Hình 5.1: Minh họa cho quyền truy cập Traverse folder	123
Hình 5.2: Cửa sổ thay đổi các đặc tính của thư mục dùng chung	125
Hình 5.3: Cửa sổ trao quyền truy cập từ xa của thư mục cho các đối tượng	126
Hình 5.4: Cửa sổ đặt thiết định đệm trữ cho thư mục chia sẻ	128
Hình 5.5: Dùng giao diện Explorer để truy nhập tài nguyên mạng	129
Hình 5.6: Cửa sổ định nghĩa ổ đĩa mạng	130
Hình 5.7: Xem các ổ đĩa mạng	131
Hình 5.8: Cửa sổ trao quyền truy cập cục bộ cho các đối tượng	134
Hình 5.9: Những lựa chọn trước khi ngăn không cho thừa hưởng những thiết định đã có	134

Hình 5.10: Cửa sổ đặt những thiết định truy cập cao cấp	136
Hình 5.11: Cửa sổ trao quyền truy cập mức thấp	137
Hình 5.12: Cửa sổ xem/lấy quyền sở hữu	139
Hình 5.13: Cửa sổ chương trình Disk Management	143
Hình 5.13: Thuộc tính thông tin ổ đĩa	144
Hình 5.14: Thuộc tính Volume của ổ đĩa	145
Hình 5.15: Cửa sổ ban đầu tạo Partition	146
Hình 5.16: Cửa sổ chọn kích thước ổ đĩa	147
Hình 5.17: Cửa sổ chọn ký tự định danh cho ổ đĩa	148
Hình 5.18: Chọn định dạng ổ đĩa	148
Hình 5.19: Xem lại các thuộc tính đã chọn cho ổ đĩa	149
Hình 5.20: Xóa ổ đĩa	149
Hình 5.21: Chuyển đổi cơ chế lưu trữ ổ đĩa	150
Hình 5.22: Cửa sổ nén dữ liệu	151
Hình 5.23: Lựa chọn cách thức nén dữ liệu	152
Hình 5.24: Thiết lập hạng ngạch đĩa	153
Hình 5.25: Cửa sổ Quota Entries	154
Hình 5.26: Thay đổi giá trị các hạn ngạch	155
Hình 5.27: Quá trình in trên mạng	156
Hình 5.28: Cửa sổ Printer dùng để quản lý các máy in logic	157
Hình 5.29: Cửa sổ chọn cài đặt máy in cục bộ hay máy in mạng	158
Hình 5.30: Cửa sổ chọn cổng máy in	158
Hình 5.31: Cửa sổ chọn trình điều khiển in	159
Hình 5.32: Đặt tên cho máy in cục bộ	160
Hình 5.33: Cửa sổ chọn chia sẻ máy in cục bộ	160
Hình 5.34: Vào những thông tin mô tả về máy in cục bộ này	161
Hình 5.35: Cửa sổ xác nhận những thông tin đã khai báo về máy in cục bộ	162

Hình 5.36: Chọn cách tìm các máy in đã chia sẻ	163
Hình 5.37: Tìm các máy in đã chia sẻ để kết nối	163
Hình 5.38: Cửa sổ xác nhận những thông tin đã khai báo về máy in mạng	164
Hình 5.39: Các loại máy in trong cửa sổ Printers	165
Hình 5.40: Cửa sổ chọn trang phân cách	167
Hình 5.41: Qui định những giờ dùng được máy in	168
Hình 5.42: Nội dung hàng đợi của máy in HP LaserJet 5L	169
Hình 5.43: Cửa sổ thay đổi quyền truy cập máy in	170
Hình 5.44: Cửa sổ Windows Server Backup	172
Hình 5.45: Giao diện lựa chọn chế độ sao lưu	173
Hình 5.46: giao diện chọn cách thức sao lưu	174
Hình 5.47: Giao diện lựa chọn nguồn lưu trữ	175
Hình 5.48: Cửa sổ thông tin nguồn lưu trữ	176
Hình 5.49: Cửa sổ chọn chế độ sao lưu	177
Hình 5.50: Màn hình Getting Started	179
Hình 5.51: màn hình Select Backup Items	180
Hình 5.52: Màn hình chọn nguồn Backup	181
Hình 5.53: Màn hình setup lập lịch Backup	182
Hình 5.54: Chọn nơi lưu trữ file backup	183
Hình 5.55: Lưu lại cấu hình cho tiến trình lập lịch	184
Hình 5.56: Khởi động quá trình khôi phục dữ liệu	185
Hình 5.57: Chọn chế độ khôi phục trên máy tính cục bộ hay khôi phục qua mạng	185
Hình 5.58: Chọn thời gian tiến hành backup	186
Hình 5.59: Chọn kiểu khôi phục dữ liệu	186
Hình 5.60: Chọn dữ liệu cần khôi phục	187
Hình 5.61: Chọn lựa khôi phục dự liệu tới đâu	187
Hình 6.1: Các loại bản ghi thuộc zone tra cứu xuôi	195

Hình 6.2: Các bản ghi PTR thuộc zone tra cứu ngược	196
Hình 6.3: Cửa sổ bắt đầu dịch vụ DNS	197
Hình 6.4: Cửa sổ chọn loại zone	198
Hình 6.5: Cửa sổ đặt tên cho zone	199
Hình 6.6: Cửa sổ đặt tên cho zone	199
Hình 6.7: Cửa sổ DNS khi đã tạo ra các Zone	200
Hình 6.8: Các server của miền khoacntt.edu.vn	200
Hình 6.9: Cửa sổ New Host	201
Hình 6.10: Cửa sổ hiện các host cần tạo	202
Hình 6.11 : Cửa sổ quy định máy server2 là một DNS server	202
Hình 6.12: Cửa sổ biến máy EMail thành một Mail server	203
Hình 6.13: Cửa sổ tạo bí danh cho máy Web server	204
Hình 6.14: Cửa sổ DNS khi đã tạo ra các loại bản ghi	204
Hình 6.15: Cửa sổ thiết lập cấu hình tĩnh dịch vụ DNS	205
Hình 6.16: Cửa sổ DHCP ban đầu	207
Hình 6.17: Cửa sổ đặt tên cho tầm	208
Hình 6.18: Cửa sổ qui định phạm vi địa chỉ IP	208
Hình 6.19: Cửa sổ cho phép loại ra phạm vi địa chỉ IP nào đó	209
Hình 6.20: Cửa sổ ấn định thời gian thuê bao các địa chỉ IP	210
Hình 6.21: Cửa sổ ấn định các tùy chọn mặc định DHCP trên máy khách	211
Hình 6.22: Cửa sổ ấn định địa chỉ IP Default gateway cho các máy khách	212
Hình 6.23: Cửa sổ ấn định các DNS server	213
Hình 6.24: Cửa sổ ấn định các WINS server	213
Hình 6.25: Cửa sổ DHCP ban đầu	214
Hình 6.26: Cửa sổ DHCP với một scope được kích hoạt	214
Hình 6.27: Cửa sổ Server Options	216
Hình 6.28. Cửa sổ thiết lập cấu hình dịch vụ DHCP	217

Hình 7.1: Giao diện thẻ ứng dụng	224
Hình 7.2: Giao diện thẻ Properties	225
Hình 7.3: Giao diện thẻ Performance	226
Hình 7.4: Giao diện thẻ Networking	227
Hình 7.5: Giao diện thẻ User	228
Hình 7.6: Một số kiểu sự kiện	230
Hình 7.7: Dữ liệu sự kiện	231
Hình 7.8: Liệt kê các sự kiện	232
Hình 7.9: Nhật ký ứng dụng	232
Hình 7.10: Nhật ký về an toàn	233
Hình 7.11: Nhật ký truy cập	233
Hình 7.12: Thiết lập an toàn cục bộ	234
Hình 7.13: Thiết lập kiểm toán	235
Hình 7.14: Thông tin sự kiện	236
Hình 7.15: Thuộc tính nhật ký	236
Hình 7.16: Thuộc tính an toàn	237
Hình 7.17: Thông tin theo dõi hiệu năng làm việc của hệ thống	238
Hình 7.18: Thông tin hiệu năng	239
Hình 7.19: Nhật ký biến đổi	240
Hình 7.20: Cấu hình nhật ký	241
Hình B.1: Giao diện bắt đầu cài đặt Windows Server 2008	254
Hình B.2: Lựa chọn cài đặt	255
Hình B.3: Lựa chọn phiên bản	255
Hình B.4: Thông tin License	256
Hình B.5: Lựa chọn kiểu cài đặt	256
Hình B.6: Lựa chọn phân vùng cài đặt	257
Hình B.7: Giao diện đang cài đặt Windows Server 2008	257

Hình B.8: Thiết lập mật khẩu	258
Hình C.1: Kiến trúc hệ điều hành Linux	261
Hình C.2: Website download Fedora	264
Hình C.3: Giao diện bắt đầu cài đặt Fedora	264
Hình C.4: Một số tùy chọn nâng cao	265
Hình C.5: Lựa chọn kiểm tra ổ đĩa	266
Hình C.6: Giao diện Fedora chuyển độ phân giải	266
Hình C.7: Lựa chọn ngôn ngữ	267
Hình C.8: Lựa chọn phân vùng cài đặt	267
Hình C.9: Cấu hình địa chỉ IP	268
Hình C.10: Lựa chọn tên host và địa chỉ DNS	268
Hình C.11: Lựa chọn múi giờ	269
Hình C.12: Đặt và xác nhận mật khẩu	269
Hình C.13: Lựa chọn các gói cài đặt cần thiết	270
Hình C.14: Lựa chọn cài đặt các dịch vụ trên máy chủ	270
Hình C.15: Giao diện bắt đầu cài đặt và lựa chọn khởi động lại máy	271
Hình C.16: Giao diện lần khởi chạy đầu tiên	272
Hình C.17: Vô hiệu Firewall	272
Hình C.18: Thiết lập cơ chế bảo mật nâng cao	272
Hình C.19: Xác lập ngày giờ	273
Hình C.20: Xác định độ phân giải màn hình	273
Hình C.21: Tạo tài khoản đầu tiên	273
Hình C.22: Kiểm tra card âm thanh	274
Hình C.23: Màn hình đăng nhập hệ thống	274
Hình C.24: Giao diện đăng nhập thành công	274
Hình C.25: Cấu trúc thư mục trong Linux	277