Bài 4: QUẢN LÝ TÀI KHOẢN NGƯỜI DÙNG VÀ NHÓM
Mã bài: MĐ 04.04.

Giới thiệu:

Quản lý tài nguyên người dùng và nhóm cung cấp cho người học những kiến thức về tài khoản người dùng và nhóm, các thuộc tính của tài khoản người dùng , các nhóm tạo sẵn. Bài này được trình bày thành các mục chính được sắp xếp như sau:

- Định nghĩa tài khoản người dùng và tài khoản nhóm.
- Các tài khoản tạo sẵn.
- Quản lý tài khoản người dùng và nhóm cục bộ.

Mục tiêu

- *Hiểu được tài khoản người dùng, tài khoản nhóm*
- *Tạo và quản trị được tài khoản người dùng, tài khoản nhóm.*
- *Tính chính xác, đúng đắn khi ra những quyết định quản trị.*

NỘI DUNG CHÍNH

1. Giới thiệu

Mục tiêu.

- Biết đăng nhập vào hệ thống

- Tạo được tài khoản người dùng cục bộ và tài khoản người dùng miền.

1.1. Quá trình đăng nhập vào hệ thống

Nếu bạn không muốn nhập tên người dùng và mật khẩu mỗi khi truy cập vào sản phẩm Google ưa thích của mình, bạn có thể chọn tuỳ chọn 'Duy trì trạng thái đăng nhập' trên trang đăng nhập của Tài khoản Google ở ngay phía trên nút **Đăng nhập**.

Nếu bạn chọn tuỳ chọn này và đăng nhập vào Tài khoản Google của bạn thành công, hệ thống của chúng tôi sẽ không yêu cầu bạn đăng nhập lại trong tối đa 2 tuần, trừ khi bạn đăng xuất.

1.2. Tài khoản người dùng cục bộ

Tài khoản người dùng cục bộ (**local user account**) là tài khoản người dùng được định nghĩa trên máy cục bộ và chỉ được phép **logon**, truy cập các tài nguyên trên máy tính cục bộ. Nếu muốn truy cập các tài nguyên trên mạng thì người dùng này phải chứng thực lại với máy **domain controller** hoặc máy tính chứa tài nguyên chia sẻ. Bạn tạo tài khoản người dùng cục bộ với công cụ **Local Users and Group** trong **ComputerManagement (COMPMGMT.MSC)**. Các tài khoản cục bộ tạo ra trên máy **stand-alone server** , **member server** hoặc các máy trạm đều được lưu trữ trong tập tin cơ sở dữ liệu **SAM** (**Security Accounts Manager**). Tập tin **SAM n**ày được đặt trong thư mục **\Windows \system32\config.**

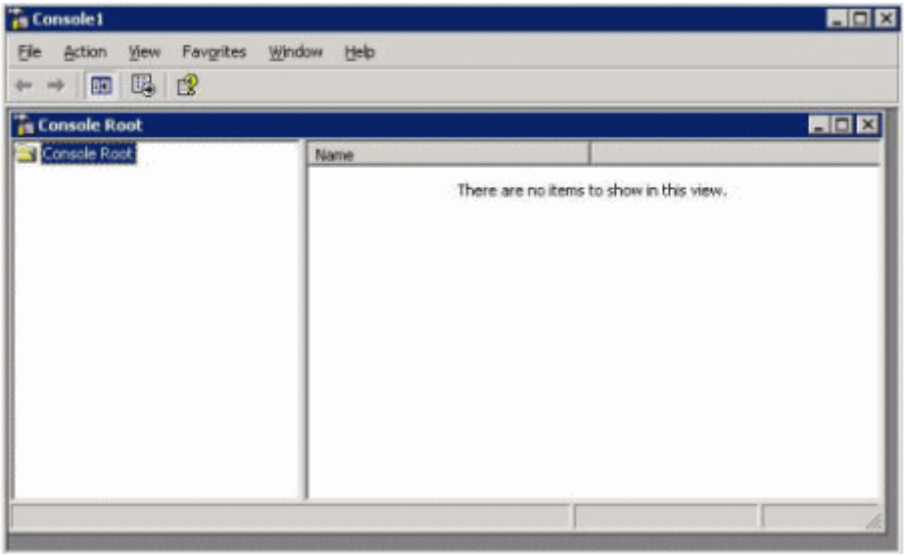
Để tổ chức và quản lý như tạo, xóa, sửa, thay đổi mật khẩu tài khoản người dùng cục bộ, bạn sử dụng công cụ Local Users ang Groups.

Có 3 cách truy cập Local Users and Groups :

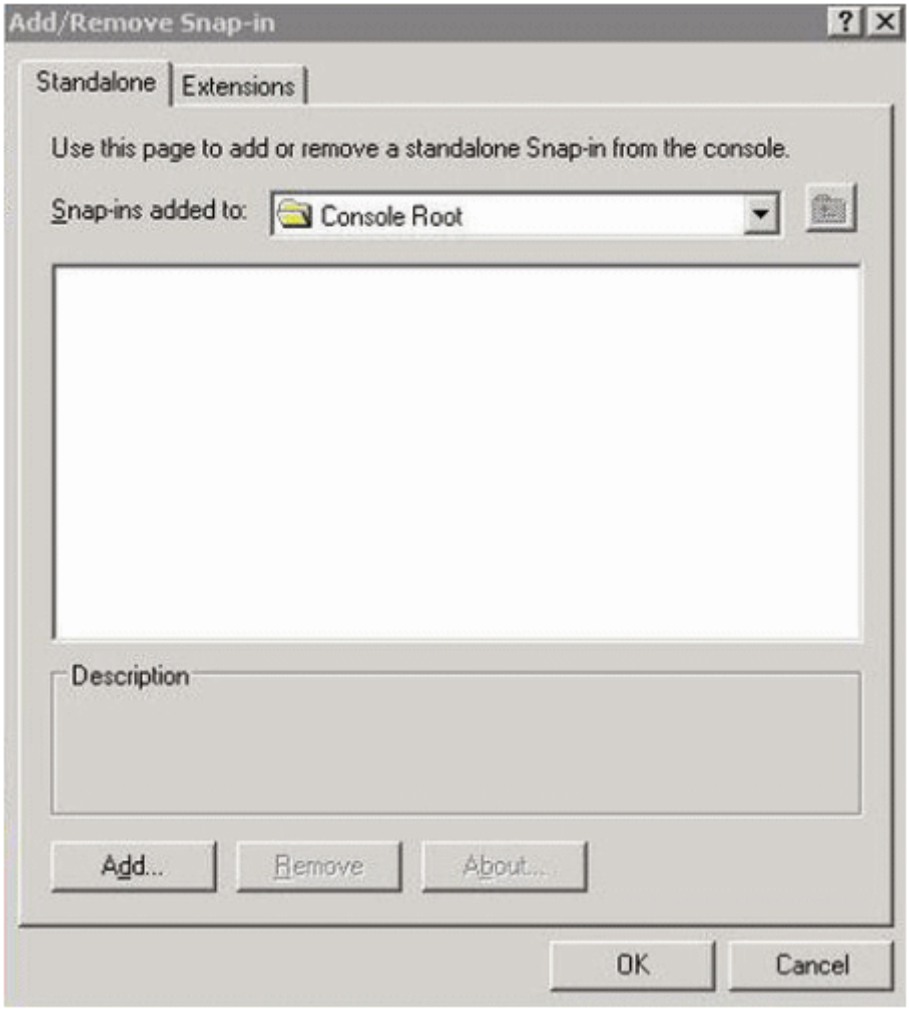
- Cách 1:

Chèn Local Users and Groups snap-in vào MMC (Microsoft Management Console) bằng cách:

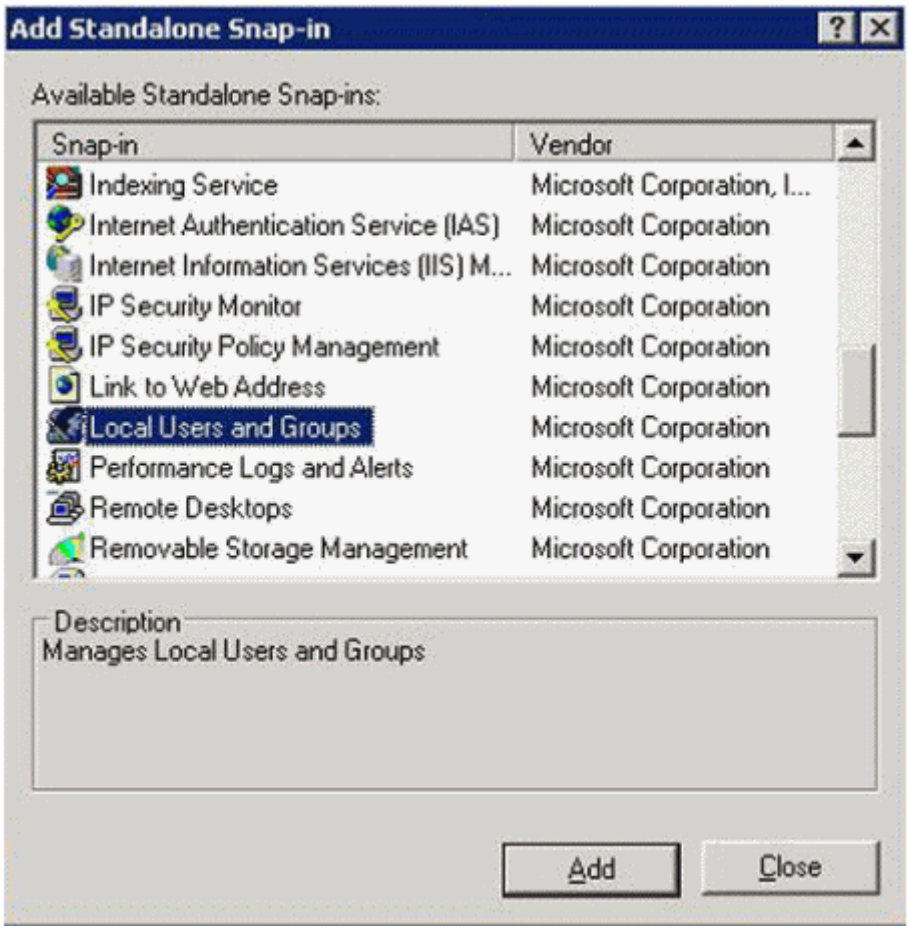
Chọn Start --> Run, nhập vào MMC --> nhấn Enter. Xuất hiện cửa sổ :



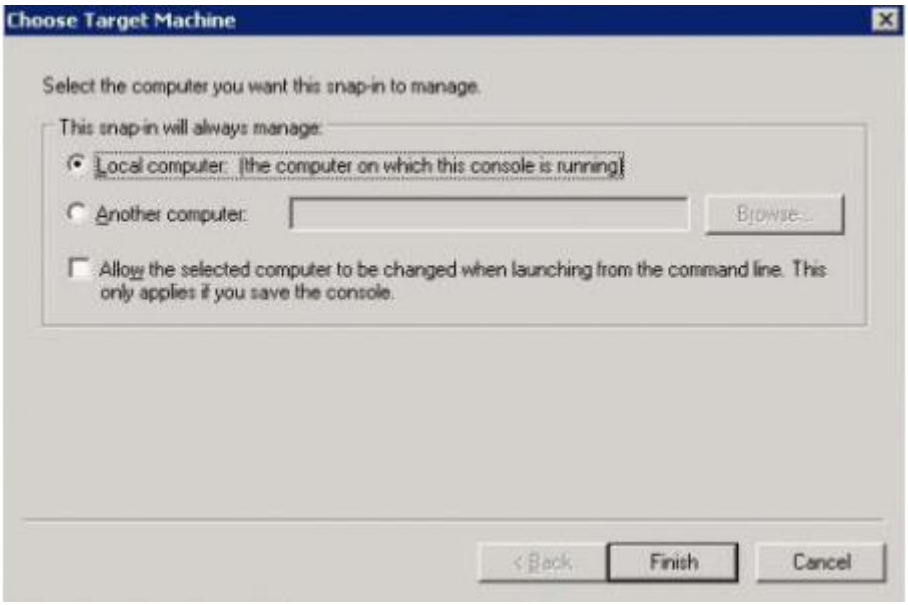
Chọn File --> Add/Remove Snap-in, xuất hiện hộp hội thoại :



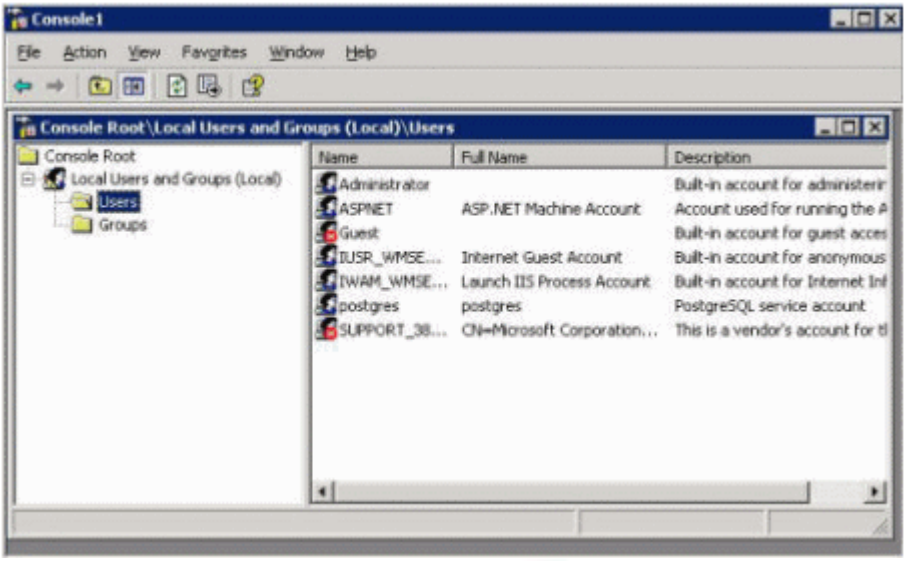
Chọn Add, xuất hiện hộp hội thoại :



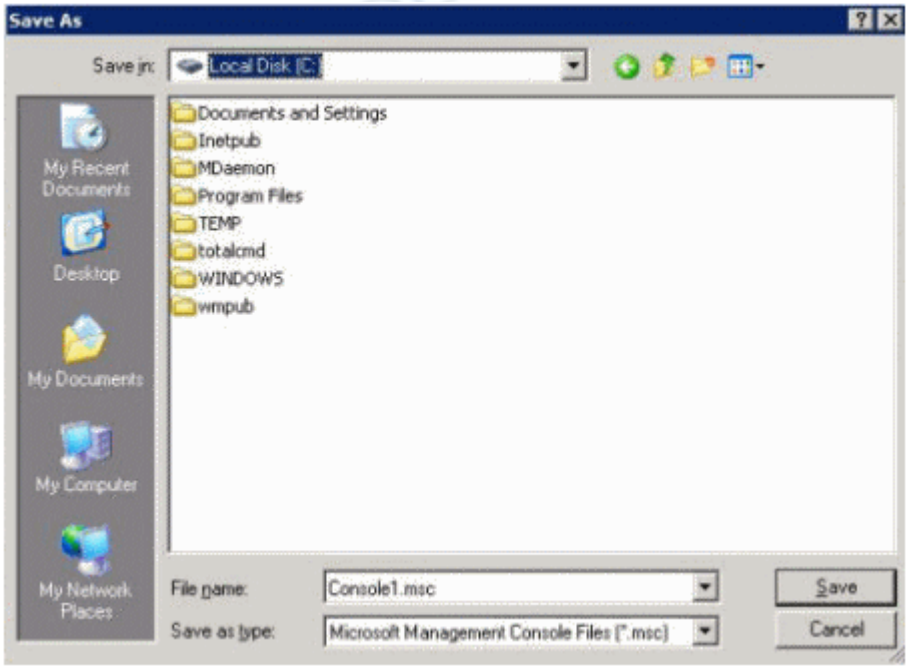
Chọn Local Users and Groups --> chọn Add, xuất hiện hộp hội thoại :



Chọn Finish --> chọn Close --> chọn OK để hoàn tất việc chèn Local Users and Groups snap-in vào MMC. Cửa sổ console xuất hiện :



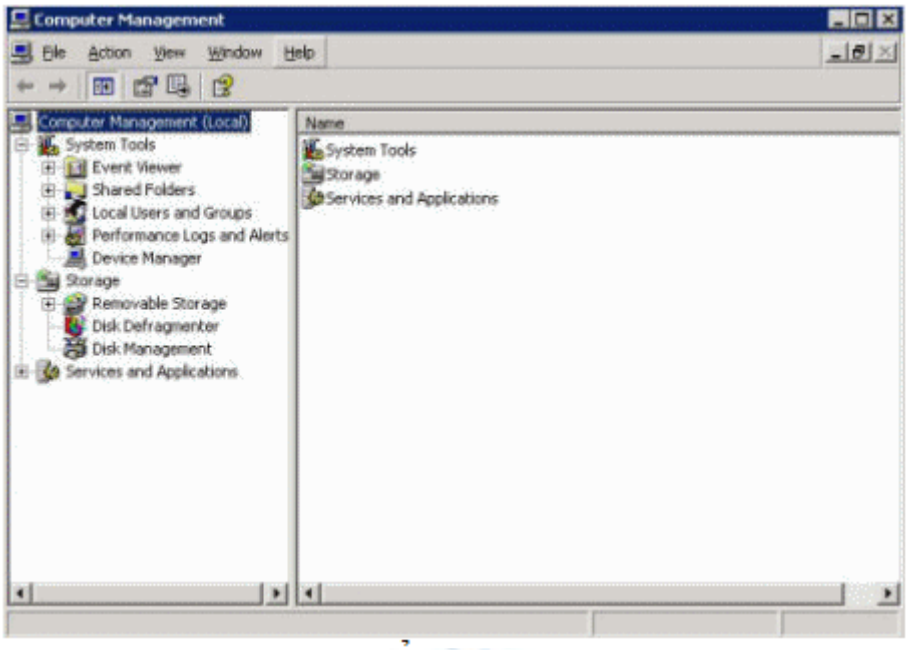
Để lưu console, bạn chọn File --> Save, xuất hiện hộp hội thoại :



Chọn đường dẫn và đặt tên để lưu file *.msc, ví dụ là console1.msc.
Khi cần sử dụng công cụ Local Users and Groups, bạn mở file console1.msc.

- Cách 2 :

Sử dụng công cụ Computer Management bằng cách :
Click chuột phải tại biểu tượng của My Computer trên desktop, chọn Manege, xuất hiện cửa sổ :



Bên khung cửa sổ bên phải, chọn và mở Local Users and Groups.

- Cách 3 :

Chọn Start --> Programs --> Administrative Tools --> Computer Management, xuất hiện cửa sổ như hình trên

1.3. Tài khoản người dùng miền.

Tài khoản người dùng miền (domain user account) là tài khoản người dùng được định nghĩa trên **Active Directory** và được phép đăng nhập (**logon**) vào mạng trên bất kỳ máy trạm nào thuộc vùng. Đồng thời với tài khoản này người dùng có thể truy cập đến các tài nguyên trên mạng. Bạn tạo tài khoản người dùng miền với công cụ **ActiveDirectory Users and Computer (DSA.MSC)**. Khác với tài khoản người dùng cục bộ, tài khoản người dùng miền không chứa trong các tập tin cơ sở dữ liệu **SAM** mà chứa trong tập tin**NTDS.DIT**, theo mặc định thì tập tin này chứa trong thư mục**\Windows\NTDS**

2. Tài khoản người dùng.

Mục tiêu.

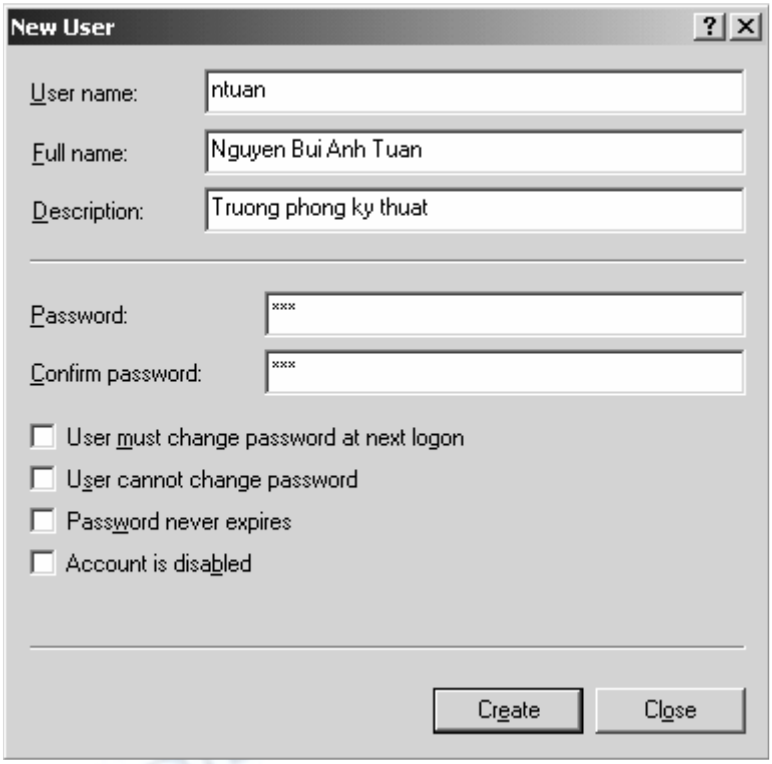
- Biết tạo tài khoản người dùng

- Phân biệt được tạo tài khoản người dùng bằng giao diện và dòng điện

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

2.1. Tạo tài khoản người dùng bằng giao diện

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

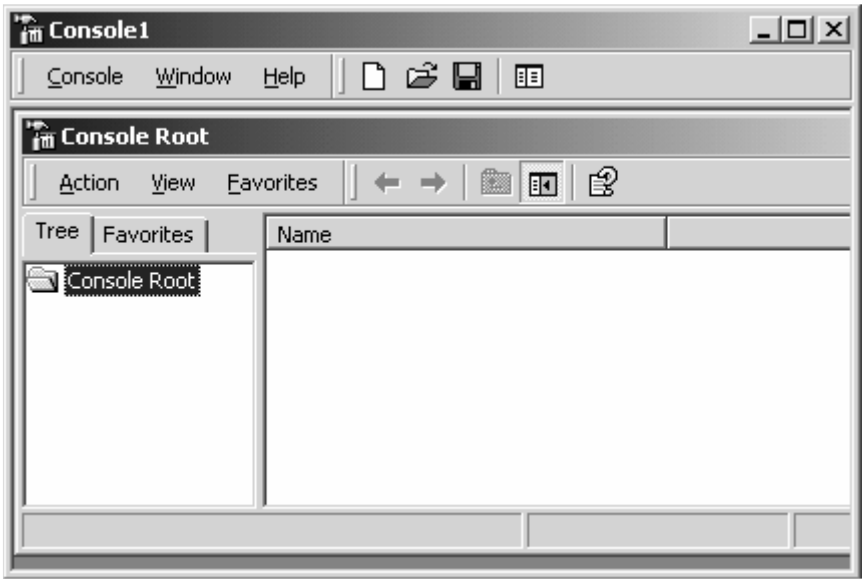


2.2. Tạo tài khoản người dùng bằng dòng lệnh

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

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

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



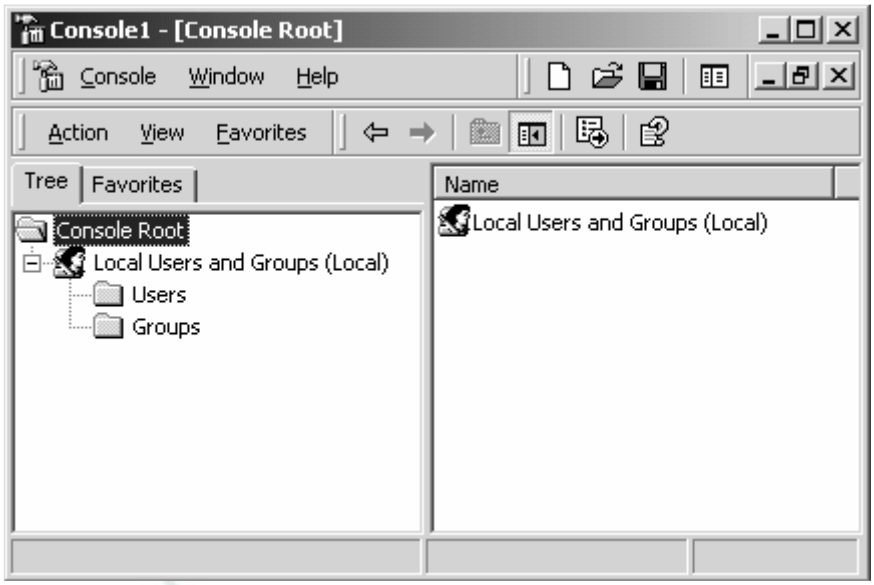
Chọn **Console / Add/Remove Snap-in** để mở hộp thoại **Add/Remove Snap-in**.

Nhấp chuột vào nút **Add** để mở hộp thoại **Add Standalone Snap-in**. Chọn **Local Users and Groups** và nhấp chuột vào nút **Add**. Hộp thoại **Choose Targe**t

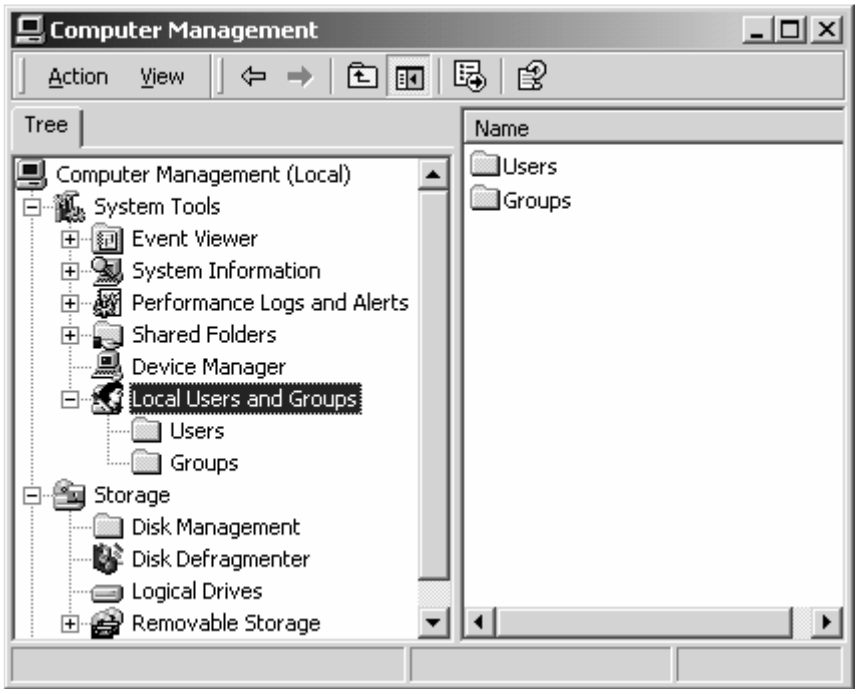
Machine xuất hiện, ta chọn **Local Computer** và nhấp chuột vào nút **Finish** để trở lại hộp thoại **Add Standalone Snap-in**.

Nhấp chuột vào nút **Close** để trở lại hộp thoại **Add/Remove Snap-in**.

Nhấp chuột vào nút **OK**, ta sẽ nhìn thấy **Local Users and Groups snap-in** đã chèn vào **MMC** như hình sau.



Lưu **Console** bằng cách chọn **Console / Save**, sau đó ta nhập đường dẫn và tên file cần lưu trữ. Để tiện lợi cho việc quản trị sau này ta có thể lưu **console** ngay trên **Desktop**. Nếu máy tính của bạn không có cấu hình **MMC** thì cách nhanh nhất để truy cập công cụ **Local Users and Groups** thông qua công cụ **Computer Management**. Nhấp phải chuột vào **My Computer** và chọn M**anage** từ **pop-up menu** và mở cửa sổ **Computer Management**. Trong mục **System Tools**, ta sẽ nhìn thấy mục **Local Users and Groups**



Cách khác để truy cập đến công cụ **Local Users and Groups** là vào **Start / Programs /Administrative Tools / Computer Management**.

3. Tài khoản nhóm.

Mục tiêu.

- Nắm được ý nghĩa của group scope và ý nghĩa của group type.

- Phân biệt được 2 ý nghĩa này.

3.1. Ý nghĩa của group scope

Phạm vi của một nhóm xác định hai đặc điểm:

Nó xác định mức độ ứng dụng bảo mật cho một nhóm xác định mà người dùng có thể được thêm vào một nhóm. Windows Server 2003 hỗ trợ các phạm vi sau đây: Domain Local: Các nhóm domain địa phương được sử dụng để gán quyền truy cập địa phương nguồn tài nguyên như file và máy in. Các thành viên có thể đến từ tên miền bất kỳ. toàn cầu: Các thành viên của nhóm này có thể truy cập tài nguyên trong phạm vi bất kỳ. Các thành viên chỉ có thể đến từ các miền địa phương. giới: Các thành viên có thể được thêm vào từ bất kỳ tên miền trong rừng. Các thành viên có thể truy cập tài nguyên từ tên miền bất kỳ. Các nhóm Universal group được sử dụng cho quản lý an ninh trên các tên miền. Các nhóm Universal group cũng có thể chứa toàn cầu nhóm. Universal group là chỉ có sẵn trong các lĩnh vực có mức chức năng Windows 2000 có nguồn gốc hoặc Windows Server 2003.

3.2. Ý nghĩa của group type

Nhóm các loại

Nhóm được sử dụng để thu thập các tài khoản người dùng, tài khoản máy tính, và nhóm tài khoản khác vào đơn vị quản lý. Làm việc với các nhóm thay vì với người dùng cá nhân giúp đơn giản hóa việc bảo trì mạng và quản trị.

Có hai loại của các nhóm trong Active Directory: nhóm phân phối và các nhóm bảo mật. Bạn có thể sử dụng các nhóm phân phối để tạo ra danh sách phân phối e-mail và các nhóm bảo mật để gán quyền truy cập tài nguyên chia sẻ.

Phân phối các nhóm

Nhóm phân phối có thể được sử dụng chỉ với các ứng dụng e-mail (chẳng hạn như Exchange) để gửi e-mail cho các bộ sưu tập của người sử dụng. Nhóm phân phối không phải là an ninh cho phép, có nghĩa là họ không thể được liệt kê trong danh sách kiểm soát truy cập tùy ý (DACLs). Nếu bạn cần một nhóm để kiểm soát truy cập vào tài nguyên chia sẻ, tạo ra một nhóm bảo mật.

An ninh nhóm

Được sử dụng với việc chăm sóc, nhóm an ninh cung cấp một cách hiệu quả để gán quyền truy cập tài nguyên trên mạng của bạn. Sử dụng các nhóm bảo mật, bạn có thể:

- **Chỉ định quyền người dùng để nhóm bảo mật trong Active mục**

Quyền của người dùng được gán cho nhóm bảo mật để xác định những gì các thành viên của nhóm đó có thể làm trong phạm vi của một tên miền (hoặc rừng). Quyền người dùng được tự động gán cho một số nhóm bảo mật Active Directory được cài đặt để giúp các quản trị viên xác định vai trò quản lý của một người trong miền. Ví dụ, một người dùng được thêm vào nhóm nhà khai thác sao lưu trong Active Directory có khả năng sao lưu và khôi phục lại các tập tin và thư mục nằm trên mỗi bộ điều khiển miền trong miền này có thể bởi vì theo mặc định, các quyền người dùng Back up files và thư

mục Khôi phục các tập tin và thư mục được tự động gán cho nhóm Nhà điều hành sao lưu. Vì vậy, các thành viên của nhóm này kế thừa các quyền người dùng được gán cho nhóm đó. Để biết thêm thông tin về các quyền của người sử dụng, quyền tài . Để biết thêm thông tin về người sử dụng quyền được giao cho các nhóm bảo mật, nhìn thấy các nhóm mặc định . Bạn có thể gán quyền người dùng để nhóm bảo mật bằng cách sử dụng Group Policy để giúp các nhiệm vụ đại biểu cụ thể. Bạn nên luôn luôn sử dụng theo ý mình khi giao nhiệm vụ được giao vì một người sử dụng chưa qua đào tạo được giao quyền quá nhiều vào một nhóm bảo mật có khả năng có thể gây ra thiệt hại đáng kể cho mạng của bạn. Để biết thêm thông tin, xem Delegating quản lý. Để biết thêm thông tin về người sử dụng quyền giao cho các nhóm, xem Gán quyền người dùng cho một nhóm trong Active Directory .

- **Gán quyền truy cập cho các nhóm an ninh về tài nguyên**

  Không nên nhầm lẫn với quyền người dùng. Quyền được giao cho nhóm bảo mật trên các nguồn tài nguyên chia sẻ. Quyền xác định những người có thể truy cập tài nguyên và mức độ truy cập, chẳng hạn như kiểm soát toàn. Một số điều khoản trên các đối tượng miền được tự động chỉ định để cho phép mức độ khác nhau truy cập cho các nhóm bảo mật mặc định như nhóm Account Operator hoặc các nhóm Domain Admins. Để biết thêm thông tin về quyền truy cập, xem Truy cập kiểm soát trong Active Directory . nhóm an ninh đang được liệt kê trong DACLs xác định các quyền truy cập vào tài nguyên và các đối tượng. Khi phân quyền truy cập cho nguồn tài nguyên (chia sẻ file, máy in, và như vậy), các quản trị viên nên chỉ định những quyền truy cập vào một nhóm bảo mật hơn là người dùng cá nhân. Các điều khoản được giao một lần cho nhóm, thay vì nhiều lần để mỗi người dùng cá nhân. Mỗi tài khoản được thêm vào một nhóm nhận được các quyền được giao cho nhóm đó trong Active Directory và các điều khoản quy định cho nhóm đó nguồn tài nguyên.

  Giống như các nhóm phân phối, các nhóm bảo mật cũng có thể được sử dụng như một thực thể e-mail. Gửi một tin nhắn e-mail cho nhóm gửi tin nhắn cho tất cả các thành viên của nhóm.

  Chuyển đổi giữa an ninh và các nhóm phân phối

  Một nhóm có thể được chuyển đổi từ một nhóm bảo mật để một nhóm phân phối, và ngược lại, bất cứ lúc nào, nhưng nếu mức độ miền chức năng được thiết lập để bản địa Windows 2000 hoặc cao hơn. Chưa có nhóm nào có thể được chuyển đổi trong khi mức độ miền chức năng được thiết lập để Windows 2000 trộn lẫn. Đối với thông tin thủ tục cụ thể, chuyển đổi một nhóm đến một loại nhóm . Đối với thông tin về chức năng miền, tên miền và chức năng rừng.

CÂU HỎI VÀ BÀI TẬP

1- Nêu các định nghĩa về tài khoản người dùng?

2- Phân biệt sự khác nhau giữa tài khoản người dùng cục bộ và tài khoản người dùng miền.

Bài 5: QUẢN LÝ TÀI NGUYÊN DÙNG CHUNG
Mã bài: MĐ 04.05.

Giới thiệu:

Quản lý tài nguyên dùng chung là một trong những công việc tạo nên thành công việc chia sẻ và phân quyền truy suất tài nguyên. Bài này sẽ cung cấp cho sinh viên các kiến thức cần thiết để chia sẻ thư mục, máy in, quyền NTFS và những vấn đề liên quan đến quyền. Được trình bày thành các mục chính được sắp xếp như sau:

- Quyền truy xuất tài nguyên
- Triển khai dịch vụ file – DFS
- Quyền quản lý File - NTFS
- Cài đặt và quản trị máy in mạng

Mục tiêu:

- *Giải thích được việc chia sẻ và phân quyền truy xuất tài nguyên*
- *Trình bày được các quyền chia sẻ thư mục, máy in, quyền NTFS và những vấn đề liên quan đến quyền*
- *Chia sẻ thư mục, phân quyền truy xuất cho User bởi công cụ đồ họa hay dòng lệnh*
- *Triển khai dịch vụ chia sẻ tập tin DFS*
- *Triển khai máy in cục bộ, máy in mạng*
- *Xử lý các sự cố thông dụng về quyền và in ấn.*
- *Tính chính xác, đúng đắn khi ra những quyết định quản trị.*

NỘI DUNG CHÍNH

1. Tổng quan về quyền truy xuất tài nguyên.

Mục tiêu

- Nắm được khái niệm quyền truy xuất: File (Shared, NTFS), Print, Services.

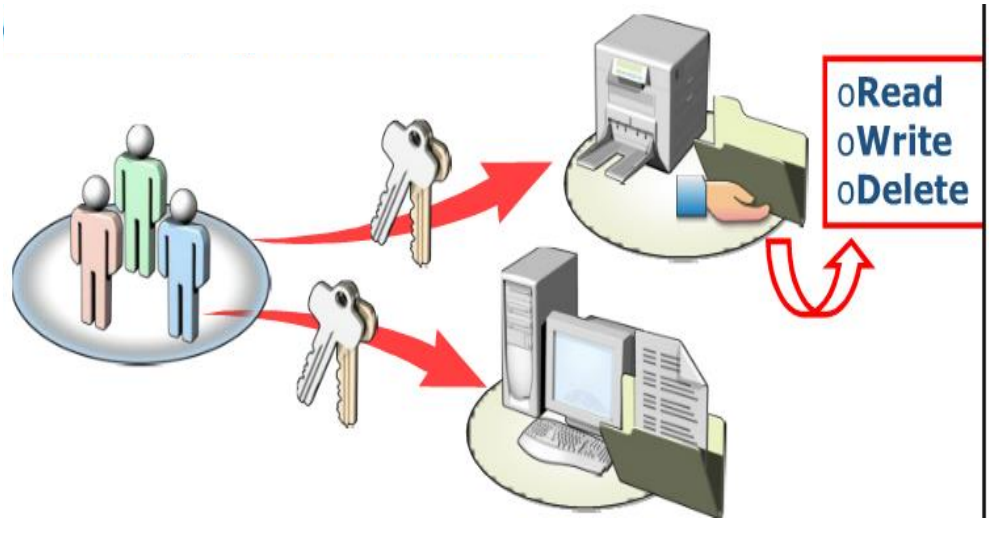
- Nắm được quản lý tài khoản (SID, ACE, DACL).

Khi người dùng truy xuất đến các tài nguyên hệ thống thì phải có một tài khoản nhất định, mỗi tài khoản có một mức độ truy cập nhất định, còn gọi là Premission.

Permission là quyền hạn truy xuất tài nguyên của người dùng.

Permission đươc dùng để gán cho các đối tượng muốn bảo mật: File, Folder, Printer.

Permission được áp dụng cho user và group hay Computer trên Activer Directory hay Local on Computer.



1.1. Khái niệm quyền truy xuất: File (Shared, NTFS), Print, Services

Quyền truy xuất tài nguyên: người dùng muốn sử dụng tài nguyên hệ thống mạng: PC, Foder, File, Printer phải có một tài khoản nhất định

Tài khoản còn gọi là username, được tạo ra và có một ID nhất định trên toàn hệ thống

Khi người dùng truy xuất tài nguyên sẽ có xác thực của hệ thống.

Để xác thực quyền truy xuất tài nguyên của người dùng hệ thống dựa vào: SID, DACL, ACL.

1.2. Quản lý tài khoản (SID, ACE, DACL)

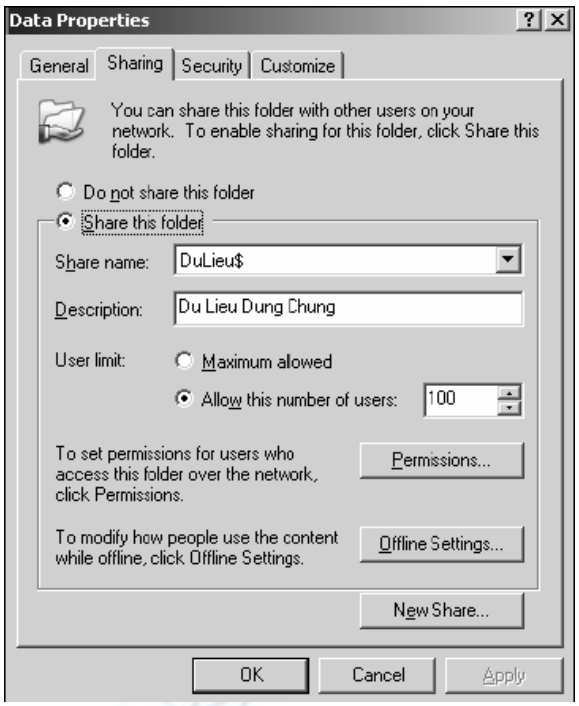
- SID (Security Identifier): Số nhận dạng bảo mật. Thành phần nhận dạng không trùng lặp được hệ thống tạo ra với tài khoản và dùng cho hệ thống nhận dạng.
- DACL: (Discretionary Access Control List): Danh sách điều khiển truy cập của chủ sở hữu, chủ sở hữu đối tượng có quyền thay đổi nội dung danh sách này. Cho phép hoặc không cho phép truy cập đối tượng.
- ACL: Một danh sách liên kết, chứa nhiều ACE là các phần tử. Mỗi ACE chứa một một số bảo mật SID của người dùng hoặc nhóm người dùng, danh sách quy định người dùng được phép hay không được phép truy cập đến đối tượng gọi là Access Mask.

2. Quyền chia sẻ thư mục – Shared folder.

Mục tiêu.

- Biết được các chia sẻ quản trị, quyền thực hiện chia sẻ và các bước thực hiện chia sẻ và các bước quảng bá thư mục chia sẻ Domain.

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



2.1. Chia sẻ quản trị: Drive$, Admin$, Netlogon, Sysvol

Shared Folder được dùng để cung cấp cho người dùng mạng các truy nhập đến các tài nguyên file. Khi một folder được chia sẻ, người dùng có thể kết nối đến folder qua mạng và đạt được truy nhập đến file mà nó chứa. Tuy nhiên, để đạt được truy nhập đến các files, người dùng cần phải có giấy phép (permission) để truy nhập đến Shared folder đó.

a. Shared foder permission

Một shared folder có thể chứa các ứng dụng, dữ liệu hoặc dữ liệu cá nhân của người dùng (home folder). Mỗi kiểu dữ liệu có thể đòi hỏi các giấy phép trên share dfolder khác nhau. Shared folder permisson có đặc điểm chung sau: Shared folder permisson áp dụng cho folder, chứ không cho file cụ thể. Từ đó bạn có thể áp dụng Shared folder permisson chỉ cho toàn thể shared folder và không áp dụng đến các file cụ thể hoặc các subfolders trong cùng shared folder đó, sharedfolder permission cung cấp ít chi tiết hơn NTFS permission.Shared folder permission không hạn chế tuy nhập đối với các người dùng màcó được truy nhập đến folder đó tại máy tính nơi folder được lưu. Chúng áp dụng chỉcho các người dùng kết nối đến folder qua mạng.Shared folder permission là cách thức duy nhất để bảo mật tài nguyên mạngtrên một FAT volume. NTFS permission không có trên FAT volumeDefault shared folder permission là Full Controll và nó được gán đến nhómEveryone khi bạn chia sẻ folder Để điều khiển cách thức người dùng có được truy nhập đến một shared folder, bạn phải gán shared folder permision. Mỗi shared folder permission cho phép ngườidùng thực hiệnRead: Người dùng có thể xem folder name, filenames, file data và attributes;chạy các file chương trình, và di chuyển đến các subfoder bên trong shared folder. Change: Người dùng có thể tạo folders, thêm file vào foldes, thay đổi dữ liệutrong các files, thêm dữ liệu vào file, thay đổi file attributes, xoá folder và files, thự chiện các hành động cho phép bởi Read permission. Full Control: Người dùng có thể thay đổi file permissions, lấy quyền sở hữu (take ownership) của các files, và thực hiện tất cả các tác vụ cho phép bởi Change permission.

Bạn có thể cho phép hoặc huỷ bỏ shared folder permission đối với cá nhân cụthể hoặc đối với cả nhóm.

b. Áp dụng Shared folder permission

Việc áp dụng shared permission đối với user account và group ảnh hưởng đến truy nhập đối với một shared folder. Việc huỷ bỏ permission được ưu tiên (ghi đè) qua các permission mà bạn cho phép. Nhiều Permission. Một người dùng có thể là thành viên của nhiều nhóm, mỗi nhóm với các permission khác nhau mà cung cấp các mức truy nhập khác nhau đến shared folder. Khi gán một permission đến một người dùng cho một shared folder; đồng thời ngườidùng đó là thành viên của một nhóm và bạn gái các permission khác đến nhóm này, permission tổng hợp có tác động đến người dùng đó là tổ hợp user permission và group permission. Ví dụ, nếu người dùng có Read permission và là thành viên của một nhóm có Change permission, permission có hiệu quả của người dùng là change, mà bao hàm ReadDeny ghi đè các permission khác Denied permission lấy ưu tiên (take precedence) qua bất kỳ permission nào mà bạn có thể cho phép trái lại cho các user và group account. Nếu bạn huỷ bỏ bất kỳ shared folder permission với một người dùng, người dùng sẽ không thể có permission đó, thậm chí nếu bạn cho phép permission cho một nhóm mà người dùng đó là thành viên. NTFS permission Shared folder permission là đủ để đạt được truy nhập đến các file và folders trên một FAT volume nhưng không là giải pháp tốt nhất cho một NTFS partition. Trên một FAT partition, người dùng có thể đạt được truy nhập đến một shared folder trong đó họ có các permission, tương tự như đến tất cả nội dung của folders. Khi người dùng có được truy nhập đến một shared folder trên NTFS partition, bạn nên dùng quyền chia sẻ (share right) hoặc NTFS permission nhưng không nên cả hai. NTFS permission là thích hợp khi permission có thể thiết lập trên cả hai file và folder. Nếu quyền chia sẻ được cấu hình cho một folder và các NTFS permission được cấu hình cho các folders hoặc file bên trong một folders, quyền hạn chế nhất sẽ trở thành quyền có tác dụng với người dùng. Điều này tăng một cách đáng kể độ phức tạp của việc giải quyết quyền truy nhập cho các tài nguyên mạng. Sao chép hoặc di chuyển các shared folder Khi bạn sao chép một shared folder, shared folder ban đầu vẫn còn được chia sẻ, nhưng bản coppy thì không. Khi bạn di chuyển một shared folder, nó không được chia sẻ nữa.

c. Chia sẻ thư mục

Các đòi hỏi cho việc chia sẻ thư mụcTrong Windows 2003, thành viên của nhóm built-in Administrators, Server Operators và Power Users có khả năng phụ thuộc vào việc máy tính thuộc domain hoặc workgroup và kiểu của máy trên đó shared folder định vị. Trong Windows 2003 domain, nhóm Adminisstrator và Server Operators cóthể chia sẻ các folder nằm trên bất kỳ máy nào trong domain. Nhóm Power User lànhóm cục bộ (local group) và chỉ có thể chia sẻ folders nằm trên stand - alone server

Trong một workgroup, nhóm Adminisstrator và Power Shared Objects có thể tạo ra các shared folder trên máy tính nơi quyền này được gán. Chia sẻ một folder. Khi bạn chia sẻ một folder, bạn có thể gán cho nó:- Share name- Lời chú thích (comments) để mô tả về folder và nội dung của nó- Hạn chế số người dùng có quyền truy nhập đến fofders, gán các permissions- Chia sẻ một folder nhiều lần. Để chia sẻ một thư mục, nhấn chuột phải folder bạn muốn và nhấn Sharing. Để gán permission cho các user hoặc group, bạn có thể nhấn nút Permission rồi gán. Thay đổi các thuộc tính chia sẻ. Để thay đổi thuộc tính của một tài nguyên chia sẻ, bạn phải đăng nhập vàonhư là một thành viên của các nhóm Administrators hoặc Server Operators. Bạn có thể lựa chọn một tài nguyên đã chia sẻ và tạo ra các thay đổi cho các thuộc tính của nó.

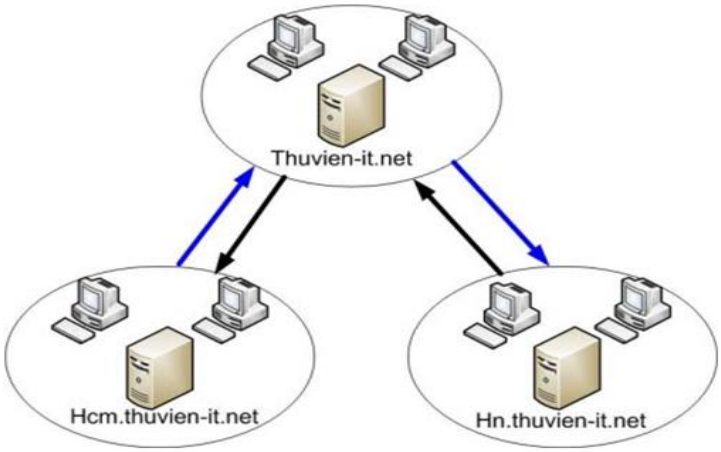
Dùng hộp thoại share Properties để thay đổi đường dẫn thư mục, thêm lời chú thích, thay đổi số người dùng cho phép kết nối đến share tại một thời điểm. Nhấn Permissions để xem danh sách người dùng và nhóm mà được phép dùng share và thay đổi sự cho phép. Dừng việc chia sẻ thư mục. Khi bạn dừng việc chia sẻ thư một thư mục, nó không được tồn tại lâu hơn nữa trên mạng. Để dừng việc chia sử một thư mục, bạn cần phải đăng nhập như thành viên của nhóm Administrators hoặc Server Operators. Hộp thoại Shared Directory trình bày các thư mục chia sẻ bạn tạo ra cũng nhưcác thư mục chia sẻ tạo bởi hệ thống. Nhìn chung, bạn không nên dừng việc chia sẻ tạo bởi hệ thống. Các shares dành cho việc quản trị mà đã bị xoá sẽ được tạo lại mộtcách tự động lần tiếp theo sau khi dịch vụ Server được khởi động.

Chú ý: Nếu quyết định dừng việc chia sẻ một thư mục trong khi người dùngđang kết nối, người dùng có thể mất dữ liệu. Dùng Window Explorer để dừng việcchia sẻ một thư mục. Kết nối đến một thư mục chia sẻ. Có một vài cách để kết nối đến thư mục chia sẻ bạn có thể dùng lện Find trên Start menu để kết nối đến bất kỳ máy tính hoặc thư mục chia sẻ nào trên mạng, hoặc nhấn đúp một máy tính trong My Network Places.

2.2. Quyền thực hiện chia sẻ Local (Administrators, Power Users Group); Domain (Administrators, Server Operators).

Quyền thực hiện chia sẻ Domain, giúp người quản trị dễ chia nhỏ việc ra nhiều phần, mỗi phần đó sẽ có 1 máy quản lý riêng, giúp hệ thống quản lý tên miền hoạt động linh hoạt hơn.

Mô hình



Các bước triển khai

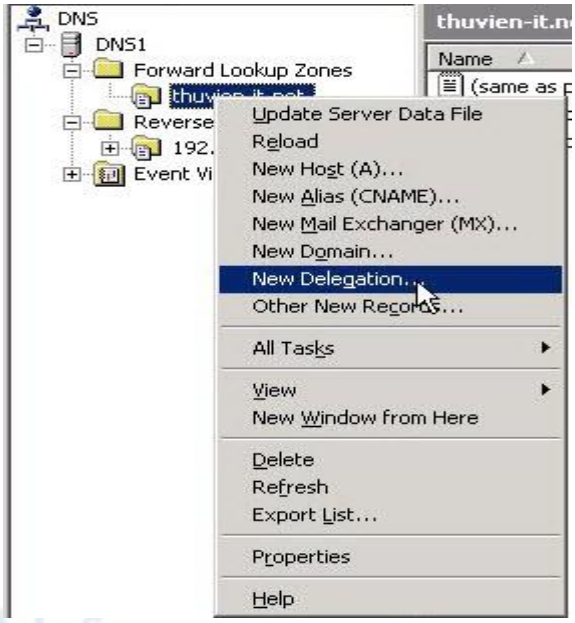
Thực hiện việc ủy quyền trên máy DNS có tên miền là "thuvien-it.net.". Trên máy DNS đang quản lý tên miền hcm.thuvien-it.net thực hiện việc Forwarder đến máy DNS tên miền thuvien-it.net.

Thực hành:

Thông số IP như sau:

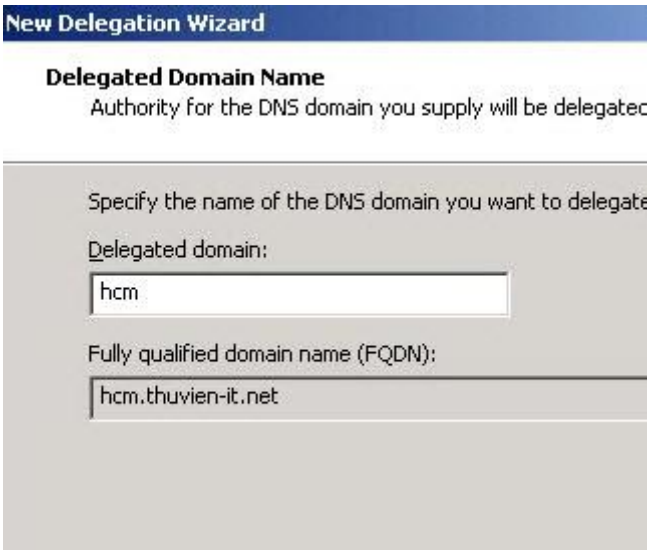
Miền	Thuvien-it.net	Hcm.thuvien-it.net
IP address:	192.168.1.5	192.168.1.50
Subnet mask:	255.255.255.0	255.255.255.0
Preferred DNS:	192.168.1.5	192.168.1.50

Thực hiện việc ủy quyền trên máy DNS có tên miền là "thuvien-it.net.". Vào Run gõ **dnsmgmt.msc** để truy xuất vào hộp thoại quản lý DNS. Click phải vào miền thuvien-it.net chọn **New Delegation**…



Hình 1 : New Delegation.

Tại hộp thoại New Delegation ta tạo tên mới để ủy quyền vídu: "hcm".

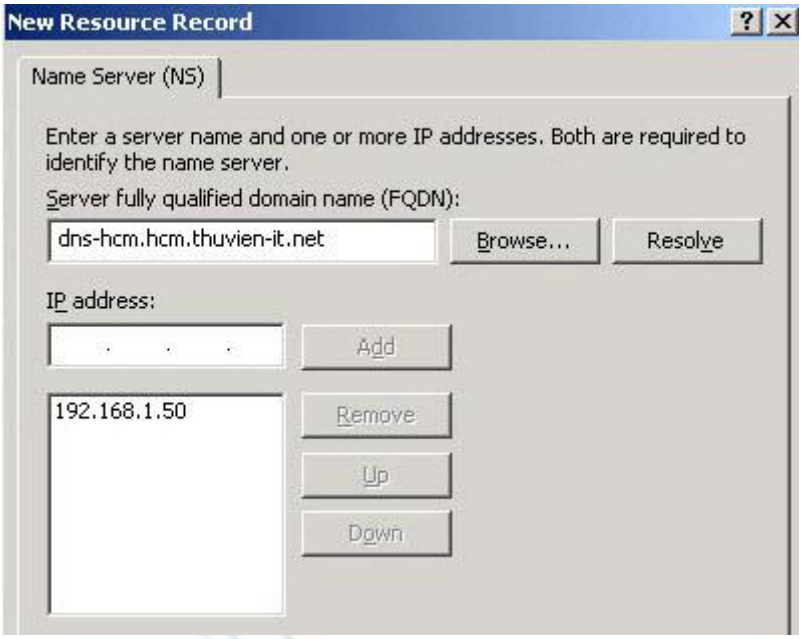


Hình 2 : Tạo tên để quản lý .

Tại hộp thoại Name server : bấm vào nút **Add** tại ô Text **Server fully qualified domain name** điền chính tên của máy DNS đang quản lý tên miền hcm.thuvien-it.net và địa chỉ Ip của máy.

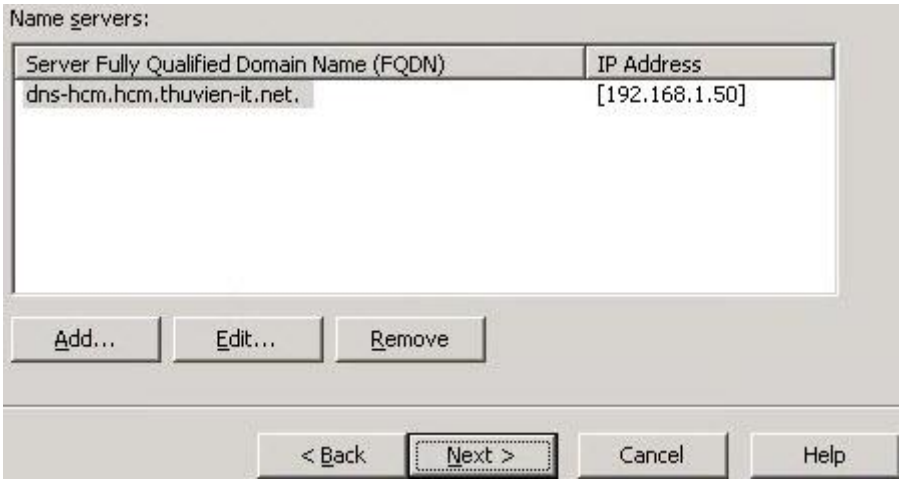
Ví dụ : DNS.HCM.hcm.thuvien-it.net

DNS.HCM là tên của máy DNS có tên miền hcm.thuvien-it.net



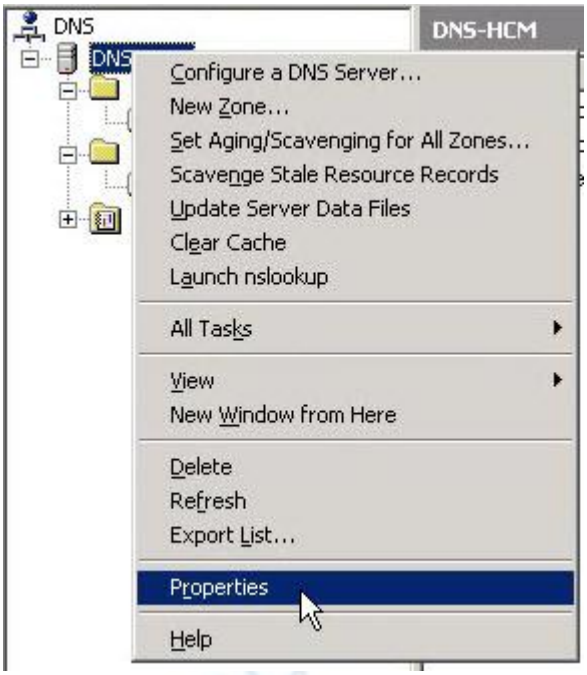
Hình 3 : Khai báo tên máy và Ip muốn ủy quyền sang.

Sau khi điền đầy đủ thông tin -> Next



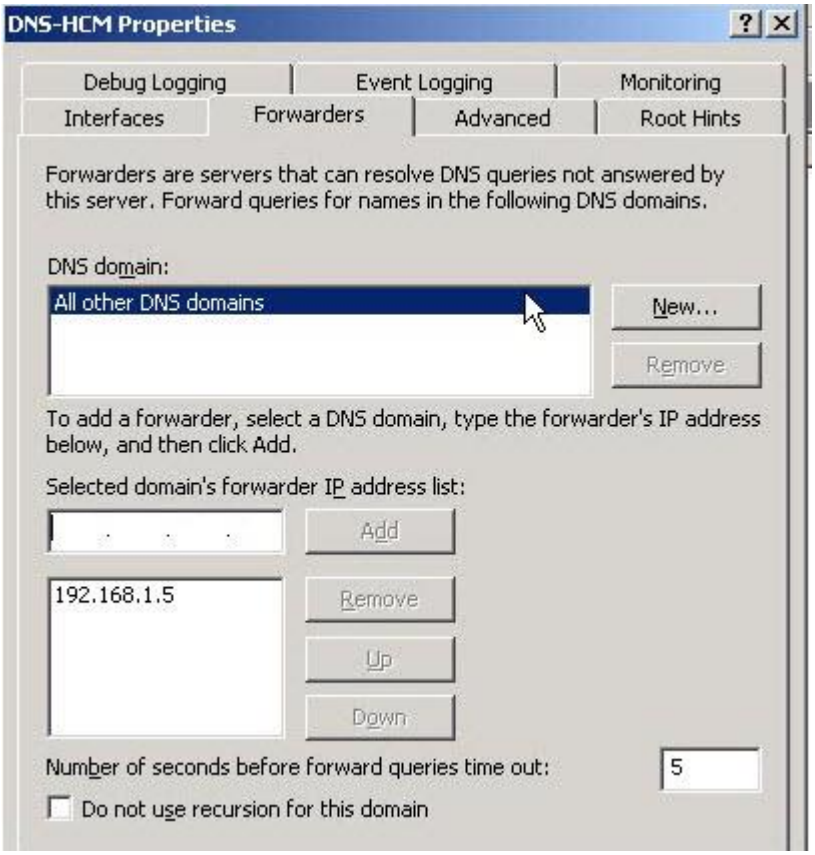
Hình 4 : Hộp thoại Name server.

Trên máy DNS đang quản lý tên miền "hcm.thuvien-it.net" thực hiện việc Forwarder đến máy DNS miền thuvien-it.net. Trong hộp thoại quản lý DNS click phải vào tên máy có tên **DNS-HCM** chọn **properties**.



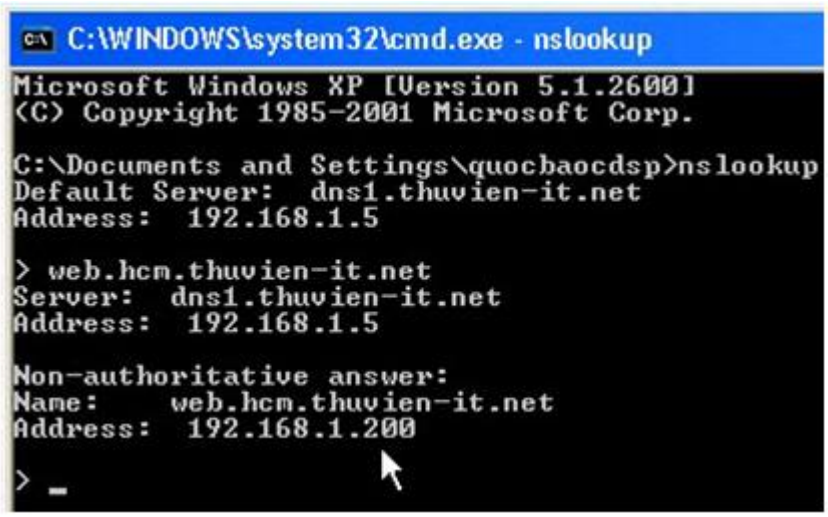
Hình 5 : Hộp thoại quản lý tên miền.

Tại tab **Forwarders** tại ô điền Ip ta điền Ip của máy DNS đang quản lý tên miền thuvien-it.net. Sau đó nhấn OK.



Hình 6 : Chỉ định việc truyền thông tin tới máy có IP.

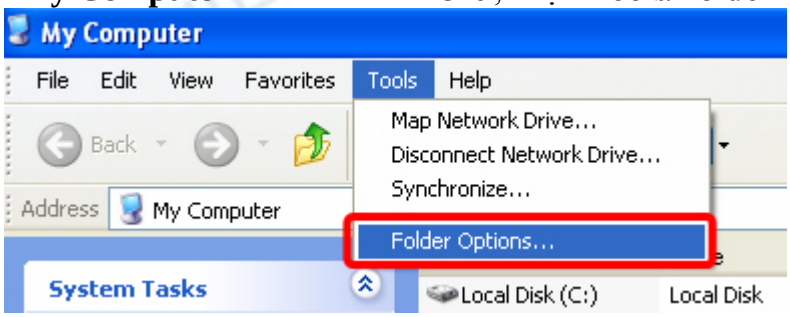
Kiểm tra lại việc vừa cấu hình trên máy Client Xp.



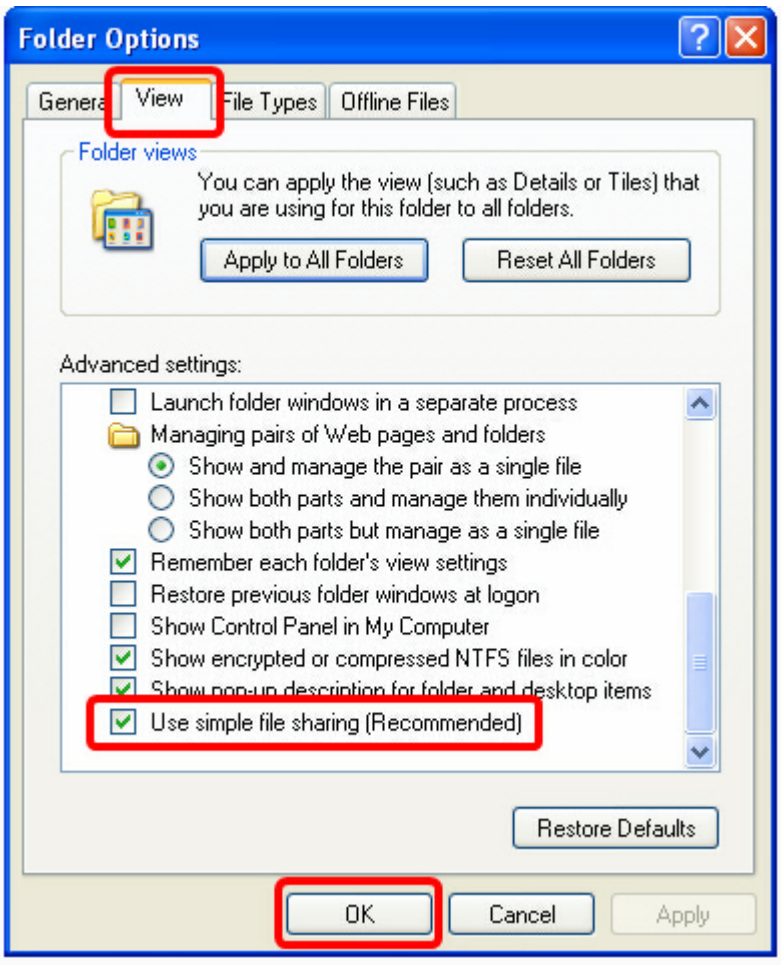
Hình 7 : kiểm tra hoạt động giữa các máy.

2.3. Các bước thực hiện chia sẻ: Computer Management, My Computer; Net Share.

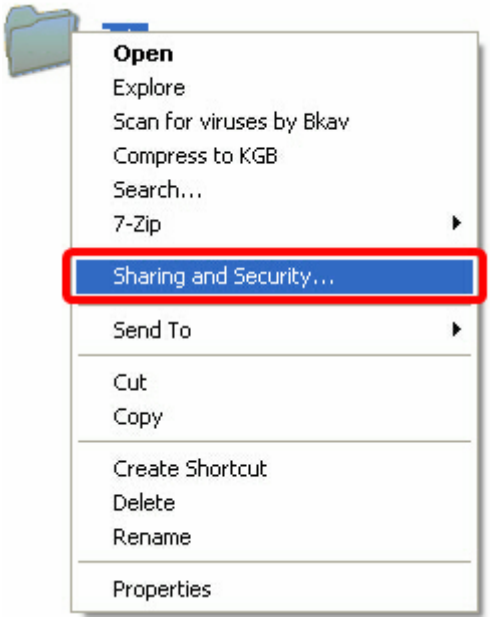
Bước 1: Mở **My Computer**. Trên thanh **Menu**, chọn **Tools/Folder Options…**



Bước 2: Trong cửa sổ **Folder Options**, bạn chọn**View,** kéo thanh cuộn xuống dưới cùng, tick chọn**Use simple file sharing (Recommended)** như hình dưới và bấm **OK.**



Bước 3: Trên cửa sổ **My Computer**, bạn di chuyển tới thư mục muốn chia sẻ. Bấm chuột phải lên thư mục này, chọn**Sharing and Security…**



Bước 4: Nếu tính năng chia sẻ lần đầu tiên được sử dụng trên máy tính, cửa sổ mới xuất hiện có nội dung mục **Network sharing and security** như trong hình. Bạn bấm vào dòng **If you understand the security risks but want to share files**

without running the wizard, click here. Nếu tính năng chia sẻ đã từng được sử dụng, bạn có thể bỏ qua bước này và chuyển đến **Bước 5**.

Cửa sổ **Enable File Sharing**, bạn chọn **Just enable file sharing** và bấm **OK**.

Bước 5: Trong cửa sổ mới xuất hiện, bạn chọn **Share this folder on the network**, sau đó bấm **OK** để hoàn tất việc chia sẻ thư mục trên mạng nội bộ.