Bài 4: QUẢN LÝ TÀI KHOẢN NGƯỜI DÙNG VÀ NHÓM

Mã bài: MĐCNTT 19.04

Mục tiêu:

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

Nội dung chính:

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

Mục tiêu:

- *Nêu được định nghĩa tài khoản người dùng, tài khoản nhóm.*

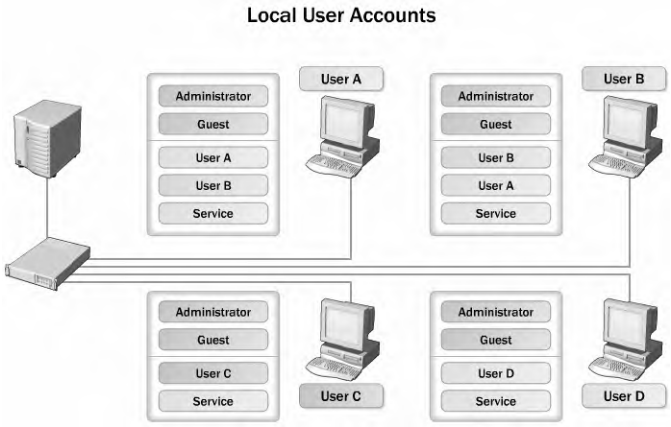
1.1. Tài khoản người dùng

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

1.1.1. Tài khoản người dùng cục bộ

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

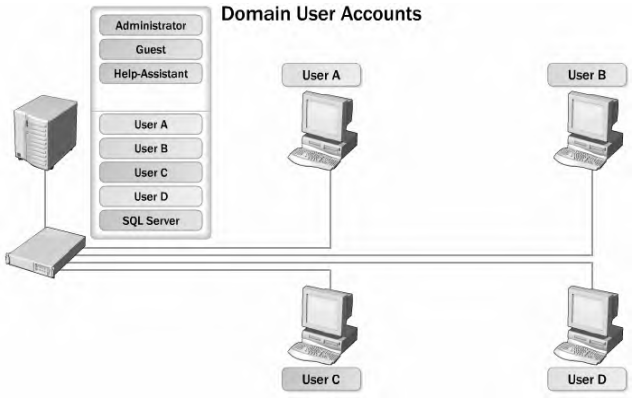
Tập tin SAM này được đặt trongthư mục \Windows\system32\config



1.1.2. Tài khoản người dùng miền

Tài khoản người dùng miền (**domain user account**) là tài khoản người dùng được định nghĩa trên **Active Directory** và được phép đăng nhập (**logon**) vào mạng trên bất kỳ máy trạm nào thuộc vùng. Đồng thời với tài khoản này người

dùng có thể truy cập đến các tài nguyên trên mạng. Bạn tạo tài khoản người dùng miền với công cụ **Active Directory Users and Computer (DSA.MSC)**. Khác với tài khoản người dùng cục bộ, tài khoản người dùng miền không chứa trong các tập tin cơ sở dữ liệu **SAM** mà chứa trong tập tin **NTDS.DIT**, theo mặc định thì tập tin này chứa trong thư mục **\Windows\NTDS**.



1.1.3. Yêu cầu về tài khoản người dùng

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

1.2. Tài khoản nhóm

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

Nhóm bảo mật

Nhóm bảo mật là loại nhóm được dùng để cấp phát các quyền hệ thống (rights) và quyền truy cập (permission). Giống như các tài khoản người dùng, các nhóm bảo mật đều được chỉ định các SID. Có ba loại nhóm bảo mật chính là: local, global và universal. Tuy nhiên nếu chúng ta khảo sát kỹ thì có thể phân thành bốn loại như sau: local, domain local, global và universal.

Local group (nhóm cục bộ) là loại nhóm có trên các máy stand-alone

Server, member server, Win2K Pro hay WinXP. Các nhóm cục bộ này chỉ có ý nghĩa và phạm vi hoạt động ngay tại trên máy chứa nó thôi.

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

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

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

Nhóm phân phối

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

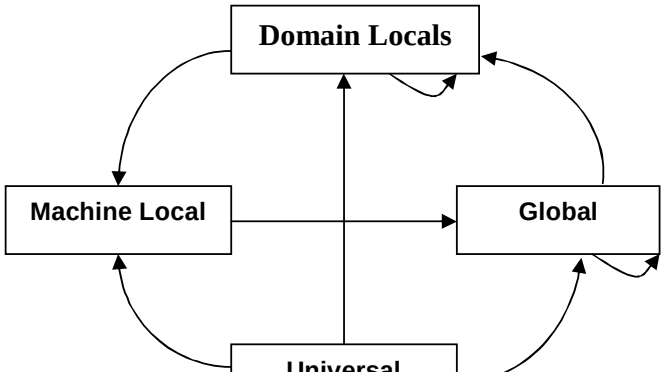
Qui tắc gia nhập nhóm

Tất cả các nhóm Domain local, Global, Universal đều có thể đặt vào trong nhóm Machine Local.

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

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

Nhóm Global có thể đặt vào trong nhóm Universal.



2. Chứng thực và kiểm soát truy cập

2.1. Giao thức chứng thực và phân quyền truy cập mạng (AAA)

Ngày nay, việc sử dụng giao thức chứng thực và phân quyền (AAA) trong vấn đề bảo mật và điều khiển truy cập dữ liệu trong mạng có dây (cable) và mạng không dây (wifi) rất cần thiết.

Các nhà quản trị mạng phải điều khiển việc truy cập cũng như giám sát thông tin mà người dùng đầu cuối đang thao tác vào hệ thống mạng. Những việc làm đó có thể đưa đến sự mất mát dữ liệu của công ty. Với ý tưởng đó, AAA là cách thức tốt nhất để giám sát những gì mà người dùng đầu cuối có thể làm trên mạng. Ta có thể xác thực, định danh (authentication) người dùng, phân quyền (authorization) cho người dùng, cũng như tập hợp được những thông tin như thời gian bắt đầu hay kết thúc của người dùng (accounting), tài nguyên người dùng đã truy cập. Như ta thấy, bảo mật là vấn đề rất quan trọng.

Với mức độ điều khiển, thật dễ dàng để cài đặt bảo mật và quản trị mạng. Ta có thể định nghĩa các vai trò (role) đưa ra cho user những lệnh mà họ cần để hoàn thành nhiệm vụ của họ và theo dõi những thay đổi trong mạng. Với khả năng hệ thống ghi log lại các sự kiện, ta có thể có những sự điều chỉnh thích hợp với từng yêu cầu đặt ra. Tất cả những thành phần này là cần thiết để duy trì tính an toàn, bảo mật cho mạng. Với thông tin thu thập được, ta có thể dự đoán việc cập nhật cần thiết theo thời gian. Ví dụ : 1 user bình thường sẽ truy cập vào tài nguyên hệ thống trong giờ làm việc (từ 8h sáng đến 5h chiều), hôm nay thấy truy cập bất thường từ 1h sáng đến 3h sáng.

Yêu cầu bảo mật dữ liệu, giám sát các vấn đề trên mạng… tất cả đều có thể tìm thấy trên dịch vụ AAA.

2.1.1. Tổng quan AAA:

AAA cho phép nhà quản trị mạng biết được các thông tin quan trọng về tình hình cũng như mức độ an toàn trong mạng. Nó cung cấp việc xác thực(authentication) người dùng nhằm bảo đảm có thể nhận dạng đúng người dùng, đúng họ và tên nhân viên, đúng phòng ban. Một khi đã nhận dạng người dùng, ta có thể giới hạn phân quyền(authorization) mà người dùng có thể tương tác vào hệ thống. Khi người dùng sử dụng mạng, ta cũng có thể giám sát tất cả những gì mà họ làm. AAA với ba thành phần xác thực (authentication), phân quyền(authorization), tính cước(accounting) là các phần riêng biệt mà ta có thể sử dụng trong dịch vụ mạng, cần thiết để mở rộng và bảo mật mạng.

AAA có thể dùng để tập hợp thông tin từ nhiều thiết bị trên mạng. Ta có thể bật các dịch vụ AAA trên router, switch, firewall, các thiết bị VPN, server…

Theo kiến trúc thiết kế bảo mật, chúng ta thường đặt các câu hỏi như sau:

- Authentication

  Who are you?

  I am user student and my password validateme proves it.

- Authorization

What can you do? What can you access?

User student can access host serverXYZ using Telnet.

- Accounting

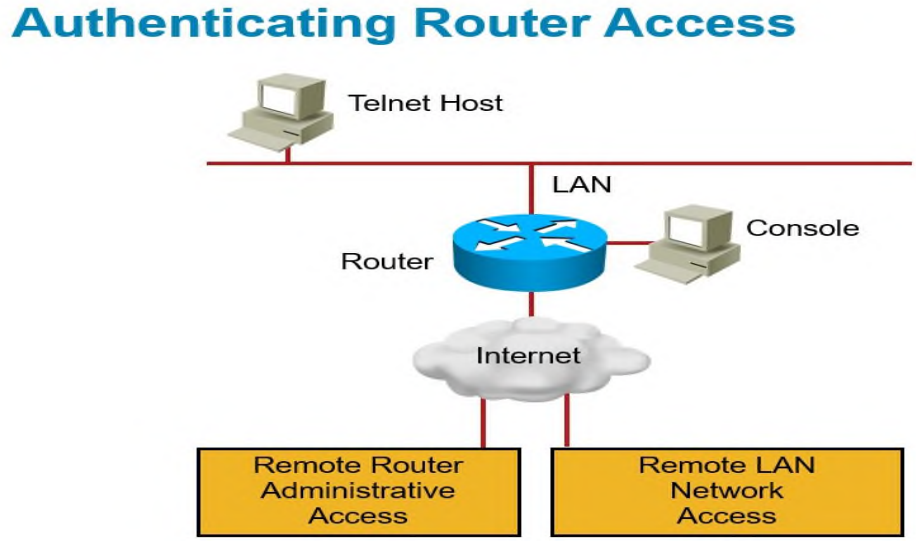
What did you do? How long did you do it?

How often did you do it?

User student accessed host serverXYZ using Telnet for 15 minutes.

2.1.2. Định nghĩa AAA:

Các dịch vụ AAA được chia thành ba phần: xác thực (authentication), phân quyền (accounting), tính cước (accounting). Ta sẽ tìm hiểu sự khác nhau của ba phần này và cách thức chúng làm việc như thể nào.



2.1.3. Xác thực người dùng (Authentication user):

Xác thực dùng để định danh, nhận dạng (identify user) người dùng. Trong suốt quá trình xác thực, username và password của người dùng được kiểm tra và đối chiếu với cơ sở dữ liệu lưu trong AAA Server hoặc external database. Tất nhiên, tùy thuộc vào giao thức mà AAA hỗ trợ mã hóa đến đâu, ít nhất thì cũng mã hóa username và password. Xác thực sẽ xác định người dùng là ai.

Ví dụ: Người dùng có username và mật khẩu trong hệ thống, sẽ là hợp lệ và được xác thực thành công với hệ thống. Sau khi xác thực thành công thì người dùng đó có thể truy cập được vào mạng. Tiến trình này chỉ là một trong các thành phần để điều khiển người dùng với AAA. Một khi username và password được chấp nhận, AAA có thể dùng để định nghĩa phân quyền mà người dùng được phép làm trong hệ thống.

2.1.4. Phân quyền người dùng (Authorization user):

Authorization cho phép nhà quản trị điều khiển việc cấp quyền trong một khoảng thời gian, hay trên từng thiết bị, từng nhóm, từng người dùng cụ thể hay trên từng giao thức. AAA cho phép nhà quản trị tạo ra các thuộc tính mô tả các chức năng của người dùng được phép làm. Do đó, người dùng phải được xác thực trước khi cấp quyền cho người đó.

AAA Authorization làm việc giống như một tập các thuộc tính mô tả những gì mà người dùng đã được xác thực có thể có. Ví dụ: 1 người dùng là nhân viên thuộc phòng nhân sự, truy cập vào hệ thống, sẽ được phân quyền theo chúc năng của phòng nhân sự, người dùng là khách của công ty, sẽ được phân quyền tối thiểu để truy cập internet, không truy cập vào tài nguyên hệ thống được. Những thuộc tính này được so sánh với thông tin chứa trong cơ sở dữ liệu của người dùng đó và kết quả được AAA trả về để xác định khả năng cũng như giới hạn thực tế của người đó. Điều này yêu cầu cơ sở dữ liệu phải giao tiếp liên tục với AAA server trong suốt quá trình kết nối đến thiết bị truy cập từ xa.

3.Các tài khoản tạo sẵn

Mục tiêu: Trình bày được các tài khoản tạo sẵn.

3.1. Tài khoản người dùng tạo sẵn

Tài khoản người dùng tạo sẵn (**Built-in**) là những tài khoản người dùng mà khi ta cài đặt **Windows Server 2003** thì mặc định được tạo ra. Tài khoản này là hệ thống nên chúng ta không có quyền xóa đi nhưng vẫn có quyền đổi tên (chú ý thao tác đổi tên trên những tài khoản hệ thống phức tạp một chút so với việc đổi tên một tài khoản bình thường do nhà quản trị tạo ra). Tất cả các tài khoản người dùng tạo sẵn này đều nằng trong **Container Users** của công cụ **Active Directory User and Computer**. Sau đây là bảng mô tả các tài khoản người dùng được tạo sẵn:

Tên tài khoản	Mô tả
Administrator	**Administrator** là một tài khoản đặc biệt, có toàn quyền trên máy tính hiện tại. Bạn có thể đặt mật khẩu cho tài khoản này trong lúc cài đặt **Windows Server 2003**. Tài khoản này có thể thi hành tất cả các tác vụ như tạo tài khoản người dùng, nhóm, quản lý các tập tin hệ thống và cấu hình máy in.
Guest	Tài khoản **Guest** cho phép người dùng truy cập vào các máy tính nếu họ không có một tài khoản và mật mã riêng. Mặc định là tài khoản này không được sử dụng, nếu được sử dụng thì thông thường nó bị giới hạn về quyền, ví dụ như là chỉ được truy cập **Internet** hoặc in ấn.
ILS_Anonymous_User	Là tài khoản đặc biệt được dùng cho dịch vụ **ILS**. **ILS** hỗ trợ cho các ứng dụng điện thoại có các đặc tính như: **caller ID**, **video conferencing**, **conference calling**, và **faxing**. Muốn sử dụng **ILS** thì dịch vụ **IIS** phải được cài đặt.
IUSR_computer- name	Là tài khoản đặc biệt được dùng trong các truy cập giấu tên trong dịch vụ **IIS** trên máy tính có cài **IIS**.
IWAM_computer- name	Là tài khoản đặc biệt được dùng cho **IIS** khởi động các tiến trình của các ứng dụng trên máy có cài **IIS**.
Krbtgt	Là tài khoản đặc biệt được dùng cho dịch vụ trung tâm phân phối khóa (**Key Distribution Center**)

TSInternetUser	Là tài khoản đặc biệt được dùng cho **Terminal Services**.

3.2. Tài khoản nhóm Domain Local tạo sẵn

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

Tên nhóm	Mô tả
Administrators	Nhóm này mặc định được ấn định sẵn tất cả các quyền hạn cho nên thành viên của nhóm này có toàn quyền trên hệ thống mạng. Nhóm **Domain Admins** và **Enterprise Admins** là thành viên mặc định của nhóm **Administrators**.
Account Operators	Thành viên của nhóm này có thể thêm, xóa, sửa được các tài khoản người dùng, tài khoản máy và tài khoản nhóm. Tuy nhiên họ không có quyền xóa, sửa các nhóm trong **container Built-in** và **OU**.
Domain Controllers	Nhóm này chỉ có trên các **Domain Controller** và mặc định không có thành viên nào, thành viên của nhóm có thể đăng nhập cục bộ vào các **Domain Controller** nhưng không có quyền quản trị các chính sách bảo mật.
Backup Operators	Thành viên của nhóm này có quyền lưu trữ dự phòng (**Backup**) và phục hồi (**Retore**) hệ thống tập tin. Trong trường hợp hệ thống tập tin là **NTFS** và họ không được gán quyền trên hệ thống tập tin thì thành viên của nhóm này chỉ có thể truy cập hệ thống tập tin thông qua công cụ **Backup**. Nếu muốn truy cập trực tiếp thì họ phải được gán quyền.
Guests	Là nhóm bị hạn chế quyền truy cập các tài nguyên trên mạng. Các thành viên nhóm này là người dùng vãng lai không phải là thành viên của mạng. Mặc định các tài khoản **Guest** bị khóa
Print Operator	Thành viên của nhóm này có quyền tạo ra, quản lý và xóa bỏ các đối tượng máy in dùng chung trong Active Directory.
Server Operators	Thành viên của nhóm này có thể quản trị các máy server trong miền như: cài đặt, quản lý máy in, tạo và quản lý thư mục dùng chung, backup dữ liệu, định dạng đĩa, thay đổi giờ…

Users	Mặc định mọi người dùng được tạo đều thuộc nhóm này, nhóm này có quyền tối thiểu của một người dùng nên việc truy cập rất hạn chế.
Replicator	Nhóm này được dùng để hỗ trợ việc sao chép danh bạ trong **Directory Services**, nhóm này không có thành viên mặc định.
Incoming Forest Trust Builders	Thành viên nhóm này có thể tạo ra các quan hệ tin cậy hướng đến, một chiều vào các rừng. Nhóm này không có thành viên mặ định.
Network Configuration Operators	Thành viên nhóm này có quyền sửa đổi các thông số **TCP/IP** trên các máy **Domain Controller** trong miền.
Pre-Windows 2000 Compatible	Nhóm này có quyền truy cập đến tất cả các tài khoản người dùng và tài khoản nhóm trong miền, nhằm hỗ trợ cho các hệ thống **WinNT** cũ.
Remote Desktop User	Thành viên nhóm này có thể đăng nhập từ xa vào các **Domain Controller** trong miền, nhóm này không có thành viên mặc định
Performace Log Users	Thành viên nhóm này có quyền truy cập từ xa để ghi nhận lại những giá trị về hiệu năng của các máy **Domain Controller**, nhóm này cũng không có thành viên mặc định.
Performace Monitor Users	Thành viên nhóm này có khả năng giám sát từ xa các máy **Domain Controller**.

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

3.3. Tài khoản nhóm Global tạo sẵn

Tên nhóm	Mô tả
Domain Admins	Thành viên của nhóm này có thể toàn quyền quản trị các máy tính trong miền vì mặc định khi gia nhập vào miền các **member server** và các máy trạm (**Win2K Pro, WinXP**) đã đưa nhóm **Domain Admins** là thành viên của nhóm cục bộ **Administrators** trên các máy này.
Domain Users	Theo mặc định mọi tài khoản người dùng trên miền đều là thành viên của nhóm này. Mặc định nhóm này là thành viên của nhóm cục bộ **Users** trên các máy **server** thành viên và máy trạm.

Group Policy Creator Owners	Thành viên nhóm này có quyền sửa đổi chính sách nhóm của miền, theo mặc định tài khoản **administrator** miền là thành viên của nhóm này.
Enterprise Admins	Đây là một nhóm **universal**, thành viên của nhóm này có toàn quyền trên tất cả các miền trong rừng đang xét. Nhóm này chỉ xuất hiện trong miền gốc của rừng thôi. Mặc định nhóm này là thành viên của nhóm **administrators** trên các **Domain Controller** trong rừng.
Schema Admins	Nhóm **universal** này cũng chỉ xuất hiện trong miền gốc của rừng, thành viên của nhóm này có thể chỉnh sửa cấu trúc tổ chức (**schema**) của **Active Directory**.

3.4. Các nhóm tạo sẵn đặc biệt

Ngoài các nhóm tạo sẵn đã trình bày ở trên, hệ thống **Windows Server 2003** còn có một số nhóm tạo sẵn đặt biệt, chúng không xuất hiện trên cửa sổ của công cụ **Active Directory User** and **Computer**, mà chúng chỉ xuất hiện trên các **ACL** của các tài nguyên và đối tượng. Ý nghĩa của nhóm đặc biệt này là:

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

4.Quản lý tài khoản người dùng và nhóm cục bộ

Mục tiêu:

- Sử dụng được các công cụ tạo và quản trị tài khoản người dùng và nhóm cục bộ.

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

Muốn tổ chức và quản lý người dùng cục bộ, ta dùng công cụ **Local Users**

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

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

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

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

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

3.Nhấp chuột vào nút Add để mở hộp thoại Add Standalone Snap-in. Chọn Local Users and Groups và nhấp chuột vào nút Add. Hộp thoại Choose Target Machine xuất hiện, ta chọn Local Computer và nhấp chuột vào nút Finish để trở lại hộp thoại Add Standalone Snap-in.

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

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

6.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.

7.Nếu máy tính của bạn không có cấu hình MMC thì cách nhanh nhất để truy cập công cụ Local Users and Groups thông qua công cụ Computer Management. Nhấp phải chuột vào My Computer và chọn Manage từ pop-up menu và mở cửa sổ Computer Management. Trong mục System Tools, ta sẽ nhìn thấy mục Local Users and Groups

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

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

4.2.1. Tạo tài khoản mới

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

4.2.2. Xóa tài khoản

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

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

4.2.3 Khóa tài khoản

Khi một tài khoản không sử dụng trong thời gian dài bạn nên khóa lại vì lý do bảo mật và an toàn hệ thống. Nếu bạn xóa tài khoản này đi thì không thể phục

hồi lại được do đó ta chỉ tạm khóa. Trong công cụ **Local Users and Groups**, nhấp đôi chuột vào người dùng cần khóa, hộp thoại **Properties** của tài khoản xuất hiện.

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

4.2.4 Đổi tên tài khoản

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

4.2.5 Thay đổi mật khẩu

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

5.Quản lý tài khoản người dùng nhóm trên Active Directory

Mục tiêu:

- Sử dụng được các công cụ tạo và quản trị tài khoản người dùng và nhóm cục bộ.

5.1. Tạo mới tài khoản người dùng

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

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

Cửa sổ Active Directory Users and Computers xuất hiện, bạn nhấp phải chuột vào mục Users, chọn New \ User

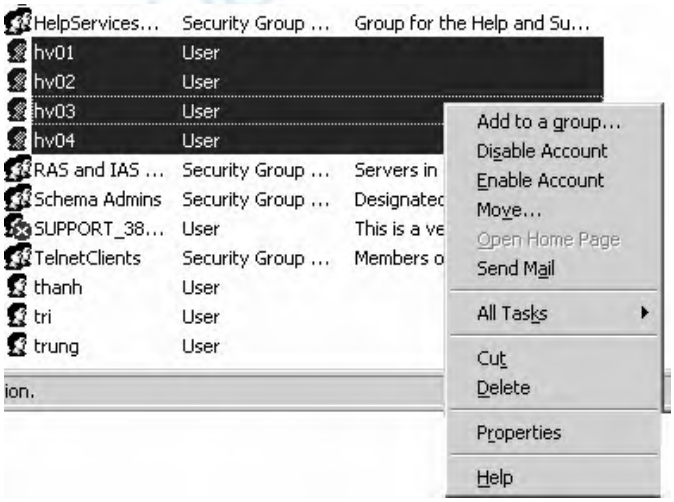
Hộp thoại New Object-User xuất hiện như hình sau, bạn nhập tên mô tả người dùng, tên tài khoản logon vào mạng. Giá trị Full Name sẽ tự động phát sinh khi bạn nhập giá trị First Name và Last Name, nhưng bạn vẫn có thể thay đổi được. Chú ý: giá trị quan trọng nhất và bắt buộc phải có là logon name (username). Chuỗi này là duy nhất cho một tài khoản người dùng theo như định nghĩa trên phần lý thuyết. Trong môi trường Windows 2000 và 2003, Microsoft đưa thêm một khái niệm hậu tố UPN (Universal Principal Name), trong ví dụ này là "@netclass.edu.vn". Hậu tố UPN này gắn vào sau chuỗi username dùng để tạo thành một tên username đầy đủ dùng để chứng thực ở cấp rừng hoặc chứng thực ở một miền khác có quan hệ tin cậy với miền của người dùng đó, trong ví dụ này thì tên username đầy đủ là tuan@netclass.edu.vn". Ngoài ra trong hộp thoại này cũng cho phép chúng ta đặt tên username của tài khoản người dùng phục vụ cho hệ thống cũ (pre-Windows 2000). Sau khi việc nhập các thông tin hoàn thành bạn nhấp chuột vào nút Next để tiếp tục.

Hộp thoại thứ hai xuất hiện, cho phép bạn nhập vào mật khẩu (password) của tài khoản người dùng và đánh dấu vào các lựa chọn liên quan đến tài khoản như: cho phép đổi mật khẩu, yêu cầu phải đổi mật khẩu lần đăng nhập đầu tiên hay khóa tài khoản. Các lựa chọn này chúng ta sẽ tìm hiểu chi tiết ở phần tiếp theo.

Hộp thoại cuối cùng xuất hiện và nó hiển thị các thông tin đã cấu hình cho người dùng. Nếu tất cả các thông tin đã chính xác thì bạn nhấp chuột vào nút Finish để hoàn thành, còn nếu cần chỉnh sửa lại thì nhấp chuột vào nút Back để trở về các hộp thoại trước.

5.2. Các thuộc tính của tài khoản người dùng

Muốn quản lý các thuộc tính của các tài khoản người ta dùng công cụ Active Directory Users and Computers (bằng cách chọn Start\ Programs\ Administrative Tools\ Active Directory Users and Computers), sau đó chọn thư mục Users và nhấp đôi chuột vào tài khoản người dùng cần khảo sát. Hộp thoại Properties xuất hiện, trong hộp thoại này chứa 12 Tab chính, ta sẽ lần lượt khảo sát các Tab này. Ngoài ra bạn có thể gom nhóm (dùng hai phím Shift, Ctrl) và hiệu chỉnh thông tin của nhiều tài khoản người dùng cùng một lúc.



5.2.1 Các thông tin mở rộng của người dùng

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

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

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

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

5.2.2 Tab Account

Tab **Account** cho phép bạn khai báo lại username, quy định giờ logon vào mạng cho người dùng, quy định máy trạm mà người dùng có thể sử dụng để vào mạng, quy định các chính sách tài khoản cho người dùng, quy định thời điểm hết

hạn của tài khoản...

Điều khiển giờ logon vào mạng: bạn nhấp chuột vào nút Logon Hours, hộp thoại Logon Hours xuất hiện. Mặc định tất cả mọi người dùng đều được phép truy cập vào mạng 24 giờ mỗi ngày, trong tất cả 7 ngày của tuần. Khi một người dùng logon vào mạng thì hệ thống sẽ kiểm tra xem thời điểm này có nằm trong khoảng thời gian cho phép truy cập không, nếu không phù hợp thì hệ thống sẽ không cho vào mạng và thông báo lỗi Unable to log you on because of an account restriction. Bạn có thể thay đổi quy định giờ logon bằng cách chọn vùng thời gian cần thay đổi và nhấp chuột vào nút lựa chọn Logon Permitted, nếu ngược lại không cho phép thì nhấp chuột vào nút lựa chọn Logon Denied. Sau đây là hình ví dụ chỉ cho phép người dùng làm việc từ 7h sáng đến 5h chiều, từ thứ 2 đến thứ 6.

Chú ý: mặc định người dùng không bị logoff tự động khi hết giờ đăng nhập nhưng bạn có thể điều chỉnh điều này tại mục Automatically Log Off Users When Logon Hours Expire trong Group Policy phần Computer Configuration\ Windows Settings\Security Settings\ Local Policies\ Security Option. Ngoài ra bạn cũng có cách khác để điều chỉnh thông tin logoff này bằng cách dùng công cụ Domain Security Policy hoặc Local Security Policy tùy theo bối cảnh.

Chọn lựa máy trạm được truy cập vào mạng: bạn nhấp chuột vào nút Log On To, bạn sẽ thấy hộp thoại Logon Workstations xuất hiện. Hộp thoại này cho phép bạn chỉ định người dùng có thể logon từ tất cả các máy tính trong mạng hoặc giới hạn người dùng chỉ được phép logon từ một số máy tính trong mạng. Ví dụ như người quản trị mạng làm việc trong môi trường bảo mật nên tài khoản người dùng này chỉ được chỉ định logon vào mạng từ một số máy tránh tình trạng người dùng giả dạng quản trị để tấn công mạng. Muốn chỉ định máy tính mà người dùng được phép logon vào mạng, bạn nhập tên máy tính đó vào mục Computer Name và sau đó nhấp chuột vào nút Add

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

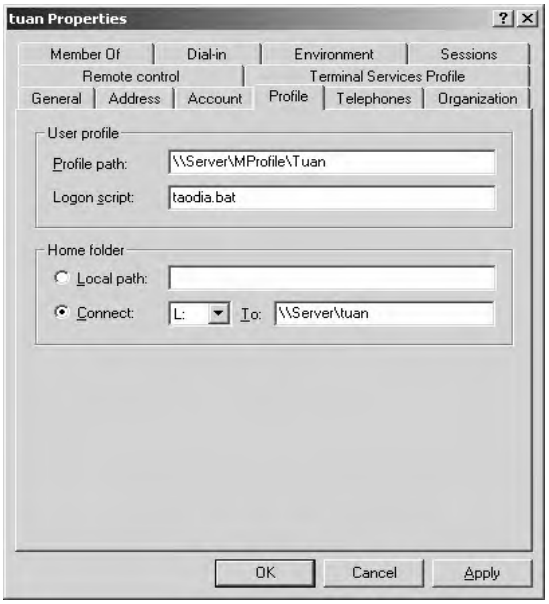
Tùy chọn	Ý nghĩa
User must change password at next logon	Người dùng phải thay đổi mật khẩu lần đăng nhập kế tiếp, sau đó mục này sẽ tự động bỏ chọn.
User cannot change password	Nếu được chọn thì ngăn không cho người dùng tùy ý thay đổi mật khẩu.
Password never expires	Nếu được chọn thì mật khẩu của tài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

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

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

5.2.3 Tab Profile

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



Trước tiên chúng ta hãy tìm hiểu khái niệm **Profile**. **User Profiles** là một thư mục chứa các thông tin về môi trường của **Windows Server 2003** cho từng

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

Mặc định khi người dùng đăng nhập vào mạng, một **profile** sẽ được mở cho người dùng đó. Nếu là lần đăng nhập lần đầu tiên thì họ sẽ nhận được một **profile** chuẩn. Một thư mục có tên giống như tên của người dùng đăng nhập sẽ được tạo trong thư mục **Documents and Settings**. Thư mục **profile** người dùng được tạo chứa một tập tin **ntuser.dat**, tập tin này được xem như là một thư mục con chứa các liên kết thư mục đến các biểu tượng nền của người dùng. Trong **Windows Server 2003** có ba loại **Profile**:

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

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

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

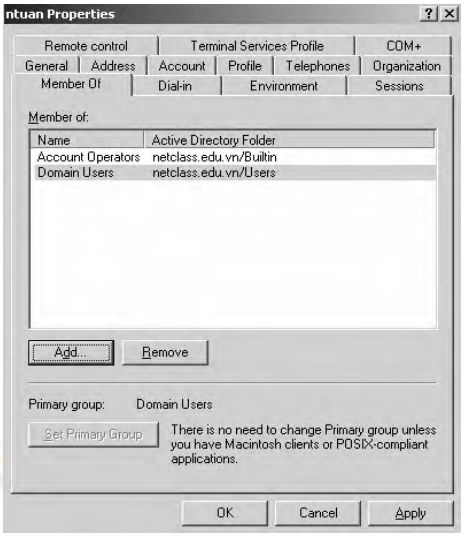
Kịch bản đăng nhập (**logon script** hay **login script**) là những tập tin chương trình được thi hành mỗi khi người dùng đăng nhập vào hệ thống, với chức năng là cấu hình môi trường làm việc của người dùng và phân phát cho họ những tài nguyên mạng như ổ đĩa, máy in (được ánh xa từ **Server**). Bạn có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

Đối với **Windows Server 2003** thì có hai cách để khai báo **logon script** là: khai báo trong thuộc tính của tài khoản người dùng thông qua công cụ **Active Directory User and Computers**, khai báo thông qua **Group Policy**. Nhưng chú ý trong cả hai cách, các tập tin **script** và mọi tập tin cần thiết khác phải được đặt trong thư mục chia sẻ **SYSVOL**, nằm trong **\Windows\SYSVOL\sysvol**, nếu các tập tin script này phục vụ cho các máy tiền **Win2K** thì phải đặt trongthư mục **\Windows\Sysvol\sysvol\domainname\scripts**. Để các tập tin **script** thi hành được bạn nhớ cấp quyền cho các người dùng mạng có quyền **Read** và **Excute** trên các tập tin này.

Thư mục cá nhân (**home folder hay home directory**) là thư mục dành riêng cho mỗi tài khoản người dùng, giúp người dùng có thể lưu trữ các tài liệu và tập tin riêng, đồng thời đây cũng là thư mục mặc định tại dấu nhắc lệnh. Muốn tạo một thư mục nhân cho người dùng thì trong mục **Connect** bạn chọn ổ đĩa hiển thị trên máy trạm và đường dẫn mà đĩa này cần ánh xạ đến (chú ý là các thư mục dùng chung đảm bảo đã chia sẻ). Trong ví dụ này bạn chỉ thư mục cá nhân cho tài khoản Tuan là "\\server\tuan", nhưng bạn có thể thay thế tên tài khoản bằng biến môi trường người dùng như: "\\server\%username%".

5.2.4 Tab Member Of

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

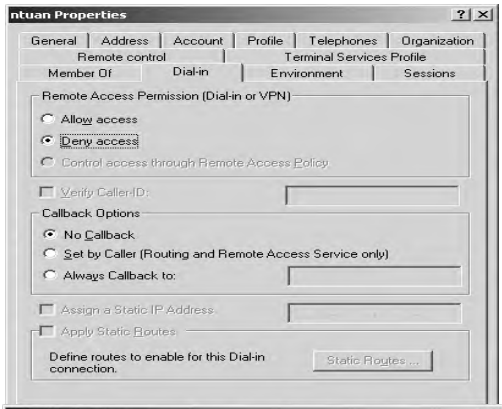


Trong hộp thoại chọn nhóm, nếu bạn nhớ tên nhóm thì có thể nhập trực tiếp tên nhóm vào và sau đó nhấp chuột vào nút **Check Names** để kiểm tra có chính xác không, bạn có thể nhập gần đúng để hệ thống tìm các tên nhóm có liên quan. Đây là tính năng mới của **Windows Server 2003** tránh tình trạng tìm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

Nếu bạn muốn tài khoản người dùng hiện tại thoát ra khỏi một nhóm nào đó thì bạn chọn nhóm sau đó nhấp chuột vào nút **Remove**.

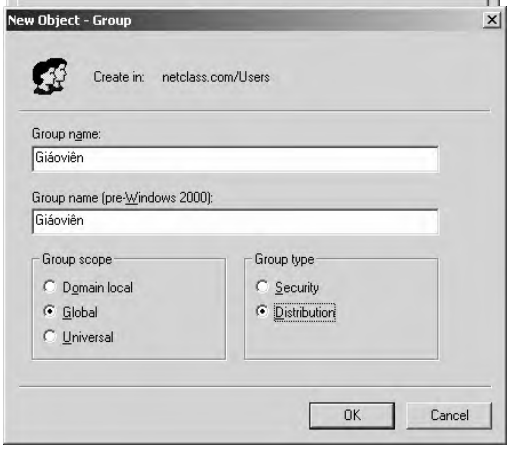
5.2.5 Tab Dial-in

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



5.3. Tạo mới tài khoản nhóm

Bạn tạo và quản lý tài khoản nhóm trên Active Directory thông qua công cụ Active Directory Users and Computers. Trước khi tạo nhóm bạn phải xác định loại nhóm cần tạo, phạm vi hoạt động của nhóm như thế nào. Sau khi chuẩn bị đầy đủ các thông tin bạn thực hiện các bước sau:



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

Hộp thoại New Object – Group xuất hiện, bạn nhập tên nhóm vào mục Group name, trường tên nhóm cho các hệ điều hành trước Windows 2000 (pre-

Windows 2000) tự động phát sinh, bạn có thể hiệu chỉnh lại cho phù hợp.

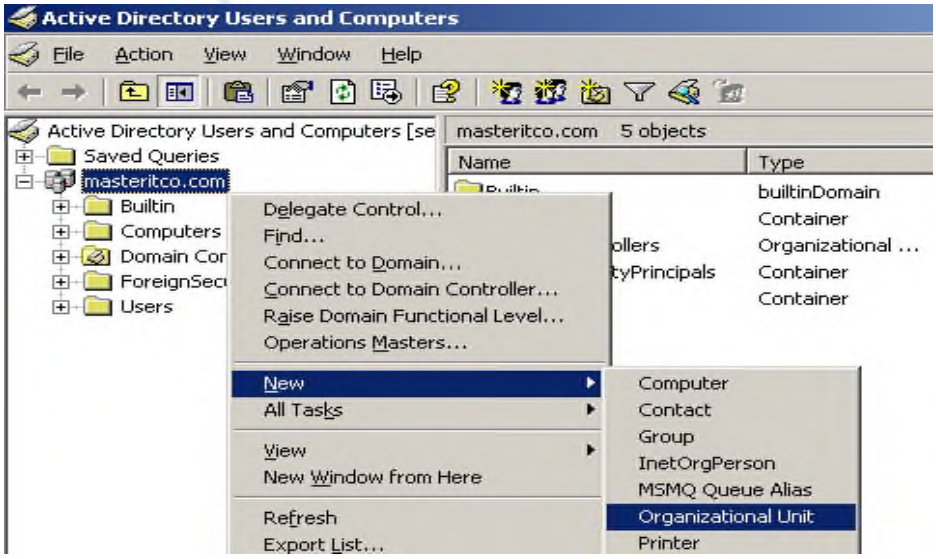
Bài tập thực hành của học viên

1. Trên máy Domain Controller tạo OU có tên HCM.
2. Trong OU HCM tạo 2 nhóm có tên là Ke Toan và Nhan Su.
3. Trong mỗi nhóm tạo 3 user.
4. Tìm kiếm, di chuyển và khóa một vài tài khoản người dùng bất kỳ.
5. Chỉ cho phép các user logon vào mạng từ 7:00am-6:00pm.
6. Tạo Home Folder cho các user.
7. Cho phép user chỉ lưu trữ 500MB trên Home Folder.
8. Thực hiện Account Lock-Out(cho phép user nhập sai 2 lần)
9. Cài đặt Adminpak.msi xuống máy client.

Hướng dẫn thực hiện:

Tạo OU có tên HCM:

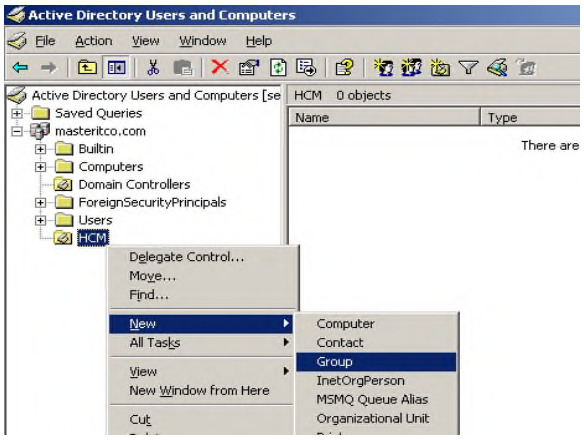
F Tại server: Start / Programs / Administrative Tools / Active Directory Users and Computers/ click nút phải chuột trên biểu tượng server / New / Organizational Unit

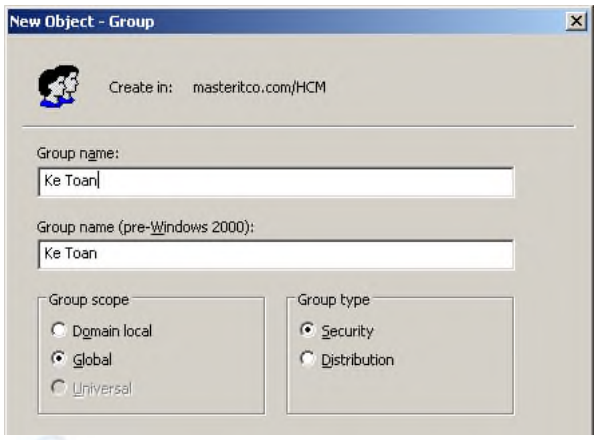


F **Đặt tên cho OU**

Trong OU HCM tạo 2 nhóm có tên là Ke Toan và Nhan Su:

F Click nút phải chuột trên OU HCM / New / Group





Group Name: Ke Toan /Group scope: Global /Group type: Security

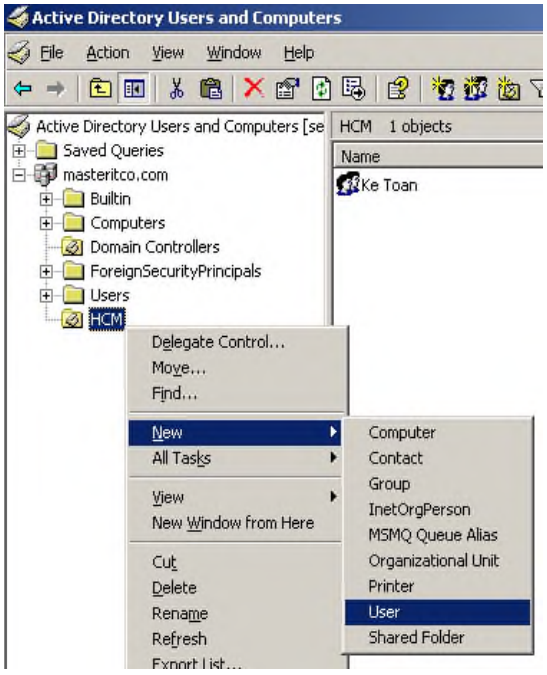
F **Tương tự tạo Group "Nhan Su"**

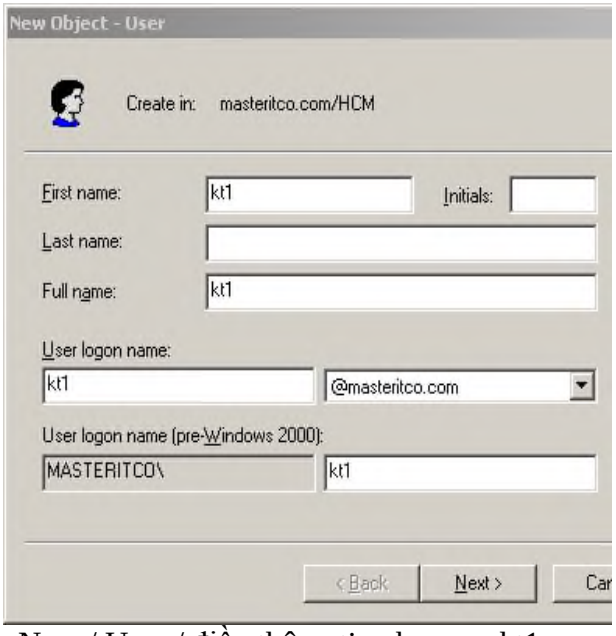
Trong mỗi nhóm tạo 3 user:

-Tạo Users

(Chú ý: Sau khi tạo xong các User hãy nhập các thông tin về các User đó như: Số điện thoại, địa chỉ, email, địa chỉ Web, nhập tên người quản lý....)

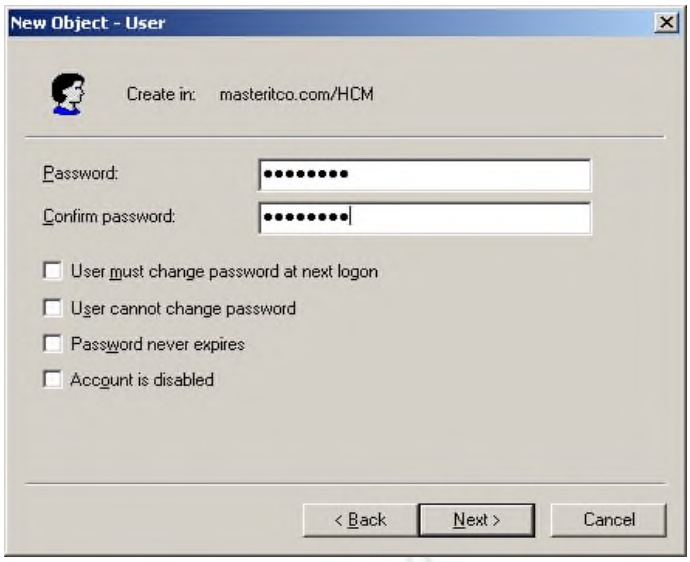
F Click nút phải chuột trên OU HCM /





New / User / điền thông tin cho user kt1

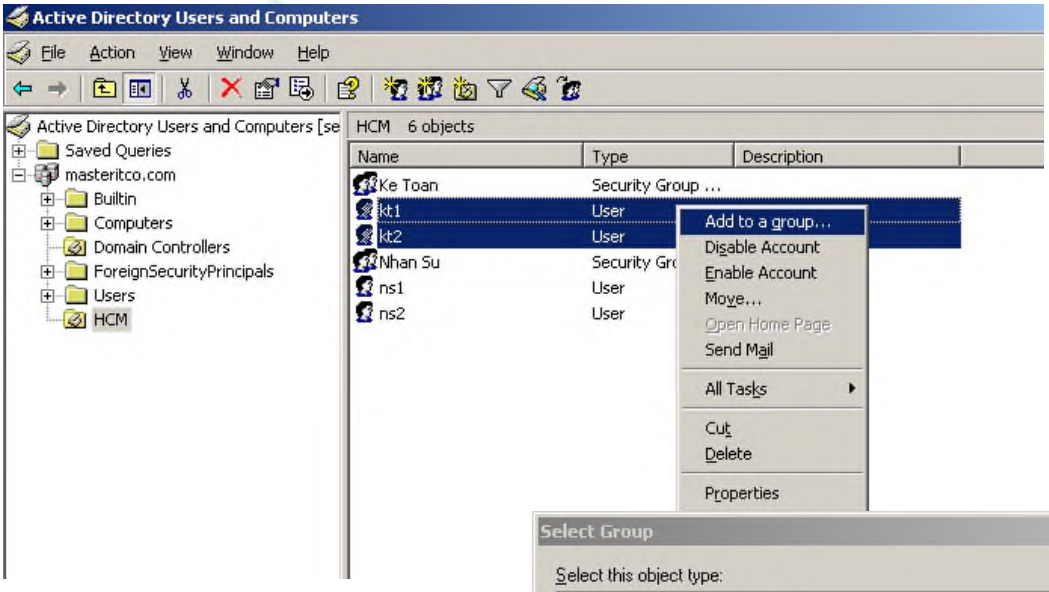
F Đặt password cho user, đánh dấu mục Password never expires

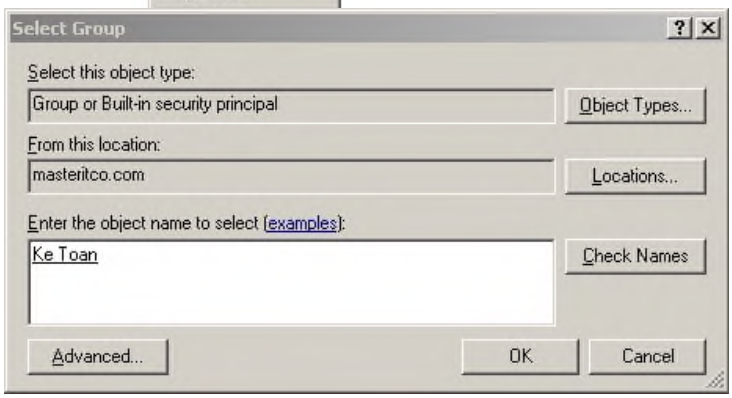


F Lặp lại tương tự cho các user KT2, KT3, NS1, NS2, NS3

-Thiết lập Users thuộc Group:

F Chọn 3 user KT1, KT2 và KT3 / click nút phải chuột trên 3 user / Add to a group





F Gõ tên nhóm "Ke Toan" / Check Names / xuất hiên gạch chân trên group "Ke Toan"

- **Thông báo kết quả**
- **Làm tương tự với các user NS1, NS2 và NS3 để đưa vào nhóm "Nhan Su"**