

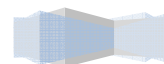
Bài 10

QUẢN LÝ TÀI KHOẢN NGƯỜI DÙNG VÀ NHÓM

Tóm tắt

Lý thuyết 4 tiết - Thực hành 10 tiết

Mục tiêu	Các mục chính	Bài tập bắt buộc	Bài tập làm thêm
Kết thúc bài học này cung cấp học viên kiến thức về tài khoản người dùng, nhóm, các thuộc tính của tài khoản người dùng, các nhóm tạo sẵn ...	<ul style="list-style-type: none"> I. Định nghĩa tài khoản người dùng và tài khoản nhóm. II. Chứng thực và kiểm soát truy cập. III. Các tài khoản tạo sẵn. IV. Quản lý tài khoản người dùng và nhóm cục bộ. V. Quản lý tài khoản người dùng và nhóm trên Active Directory. 	Dựa vào bài tập môn Quản trị Windows Server 2003.	Dựa vào bài tập môn Quản trị Windows Server 2003.



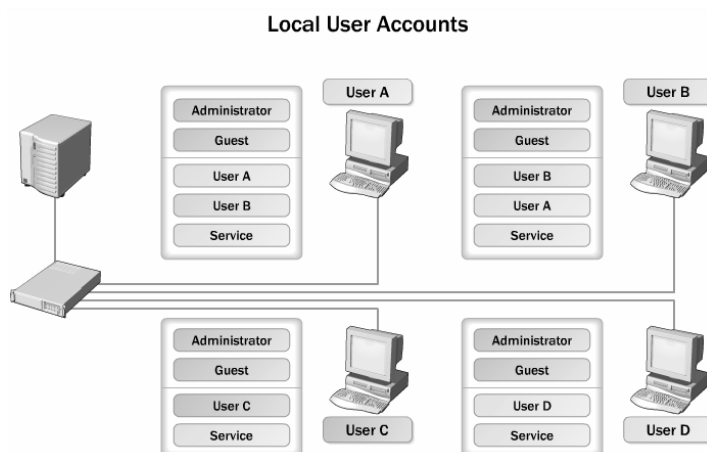
I. ĐỊNH NGHĨA TÀI KHOẢN NGƯỜI DÙNG VÀ TÀI KHOẢN NHÓM.

I.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.

I.1.1 Tài khoản người dùng cục bộ.

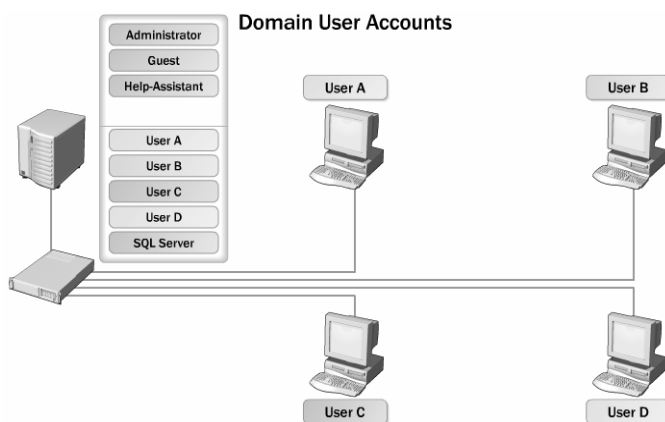
Tài khoản người dùng cục bộ (**local user account**) là tài khoản người dùng được định nghĩa trên máy cục bộ và chỉ được phép **logon**, truy cập các tài nguyên trên máy tính cục bộ. Nếu muốn truy cập các tài nguyên trên mạng thì người dùng này phải chứng thực lại với máy **domain controller** hoặc máy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



Hình 3.1: lưu trữ thông tin tài khoản người dùng cục bộ

I.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**.



Hình 3.2: lưu trữ thông tin tài khoản người dùng miền.

I.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.

I.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**).

I.2.1 Nhóm bảo mật.

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

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

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

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

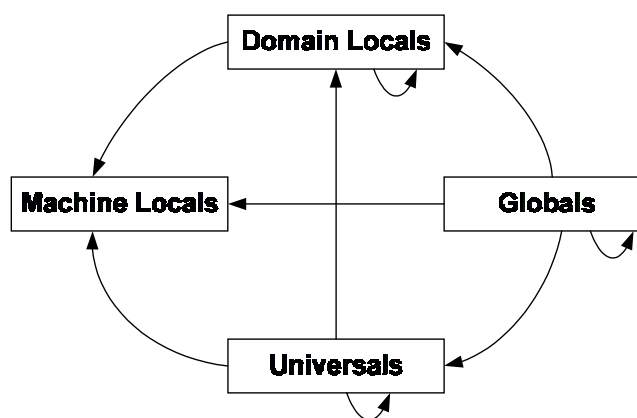
Universal group (nhóm phổ quát) là loại nhóm có chức năng giống như **global group** nhưng nó dùng để cấp quyền cho các đối tượng trên khắp các miền trong một rừng và giữa các miền có thiết lập quan hệ tin cậy với nhau. Loại nhóm này tiện lợi hơn hai nhóm **global group** và **local group** vì chúng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

1.2.2 Nhóm phân phối.

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

1.2.3 Qui tắc gia nhập nhóm.

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



Hình 3.3: khả năng gia nhập của các loại nhóm.

II. CHỨNG THỰC VÀ KIỂM SOÁT TRUY CẬP.

II.1. Các giao thức chứng thực.

Chứng thực trong **Windows Server 2003** là quy trình gồm hai giai đoạn: đăng nhập tương tác và chứng thực mạng. Khi người dùng đăng nhập vùng bằng tên và mật mã, quy trình đăng nhập tương tác sẽ phê chuẩn yêu cầu truy cập của người dùng. Với tài khoản cục bộ, thông tin đăng nhập được chứng thực cục bộ và người dùng được cấp quyền truy cập máy tính cục bộ. Với tài khoản miền, thông tin đăng nhập được chứng thực trên **Active Directory** và người dùng có quyền truy cập các tài nguyên trên mạng. Như vậy với tài khoản người dùng miền ta có thể chứng thực trên bất kỳ máy tính nào trong miền. **Windows 2003** hỗ trợ nhiều giao thức chứng thực mạng, nổi bật nhất là:

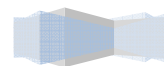
- **Kerberos V5**: là giao thức chuẩn **Internet** dùng để chứng thực người dùng và hệ thống.
- **NT LAN Manager (NTLM)**: là giao thức chứng thực chính của **Windows NT**.
- **Secure Socket Layer/Transport Layer Security (SSL/TLS)**: là cơ chế chứng thực chính được dùng khi truy cập vào máy phục vụ **Web** an toàn.

II.2. Số nhận diện bảo mật SID.

Tuy hệ thống **Windows Server 2003** dựa vào tài khoản người dùng (**user account**) để mô tả các quyền hệ thống (**rights**) và quyền truy cập (**permission**) nhưng thực sự bên trong hệ thống mỗi tài khoản được đặc trưng bởi một con số nhận dạng bảo mật **SID (Security Identifier)**. **SID** là thành phần nhận dạng không trùng lặp, được hệ thống tạo ra đồng thời với tài khoản và dùng riêng cho hệ thống xử lý, người dùng không quan tâm đến các giá trị này. **SID** bao gồm phần **SID** vùng cộng thêm với một **RID** của người dùng không trùng lặp. **SID** có dạng chuẩn "**S-1-5-21-D1-D2-D3-RID**", khi đó tất cả các **SID** trong miền đều có cùng giá trị **D1**, **D2**, **D3**, nhưng giá trị **RID** là khác nhau. Hai mục đích chính của việc hệ thống sử dụng **SID** là:

- Dễ dàng thay đổi tên tài khoản người dùng mà các quyền hệ thống và quyền truy cập không thay đổi.
- Khi xóa một tài khoản thì **SID** của tài khoản đó không còn giá trị nữa, nếu chúng ta có tạo một tài khoản mới cùng tên với tài khoản vừa xóa thì các quyền cũ cũng không sử dụng được bởi vì khi

tạo tài khoản mới thì giá trị **SID** của tài khoản này là một giá trị mới.



II.3. Kiểm soát hoạt động truy cập của đối tượng.

Active Directory là dịch vụ hoạt động dựa trên các đối tượng, có nghĩa là người dùng, nhóm, máy tính, các tài nguyên mạng đều được định nghĩa dưới dạng đối tượng và được kiểm soát hoạt động truy cập dựa vào bộ mô tả bảo mật **ACE**. Chức năng của bộ mô tả bảo mật bao gồm:

- Liệt kê người dùng và nhóm nào được cấp quyền truy cập đối tượng.
- Định rõ quyền truy cập cho người dùng và nhóm.
- Theo dõi các sự kiện xảy ra trên đối tượng.
- Định rõ quyền sở hữu của đối tượng.

Các thông tin của một đối tượng **Active Directory** trong bộ mô tả bảo mật được xem là mục kiểm soát hoạt động truy cập **ACE (Access Control Entry)**. Một **ACL (Access Control List)** chứa nhiều **ACE**, nó là danh sách tất cả người dùng và nhóm có quyền truy cập đến đối tượng. **ACL** có đặc tính kế thừa, có nghĩa là thành viên của một nhóm thì được thừa hưởng các quyền truy cập đã cấp cho nhóm này.

III. CÁC TÀI KHOẢN TẠO SẴN.

III.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 nằm 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 .

III.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 vắng 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 mặc 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 Access	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.

III.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 .

III.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 đặc 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 hữu 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**.

IV. QUẢN LÝ TÀI KHOẢN NGƯỜI DÙNG VÀ NHÓM CỤC BỘ.

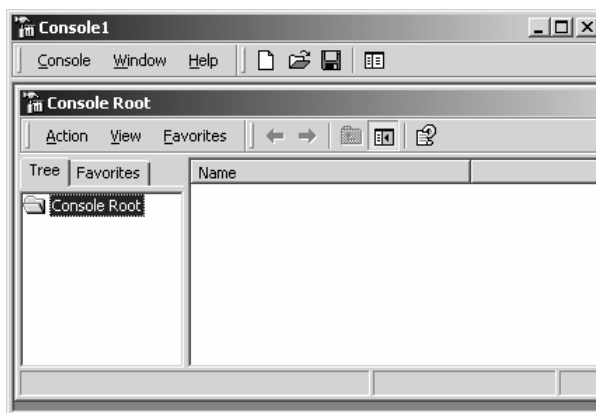
IV.1. Công cụ quản lý tài khoản người dùng cục bộ.

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

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

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

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



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

Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | <http://www.adminviet.net>

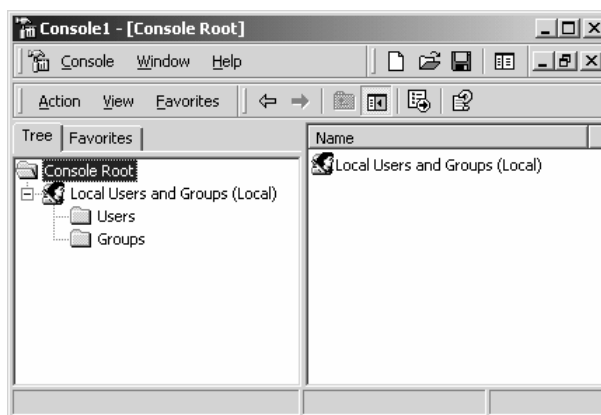
Nhấp chuột vào nút **Add** để mở hộp thoại **Add Standalone Snap-in**.

Chọn **Local Users and Groups** và nhấp chuột vào nút **Add**.

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

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

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



Lưu **Console** bằng cách chọn **Console** ⌚ **Save**, sau đó ta nhập đường dẫn và tên file cần lưu trữ. Để tiện lợi cho việc quản trị sau này ta có thể lưu **console** ngay trên **Desktop**.

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

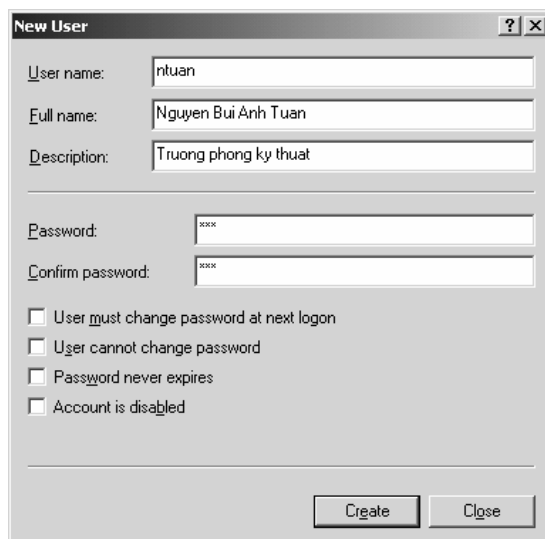


Cách khác để truy cập đến công cụ **Local Users and Groups** là vào **Start** ⌚ **Programs** ⌚ **Administrative Tools** ⌚ **Computer Management**.

IV.2. Các thao tác cơ bản trên tài khoản người dùng cục bộ.

IV.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**.

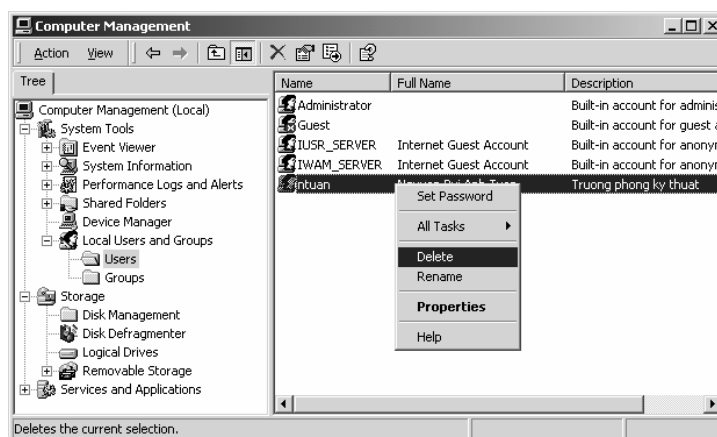


The 'New User' dialog box contains the following fields and options:

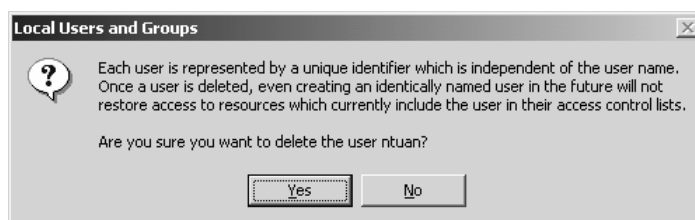
- User name:** ntuan
- Full name:** Nguyen Bui Anh Tuan
- Description:** Truong phong ky thuat
- Password:** (masked with 'x')
- Confirm password:** (masked with 'x')
- ☐ User must change password at next logon
- ☐ User cannot change password
- ☐ Password never expires
- ☐ Account is disabled
- Create** button
- Close** button

IV.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**.

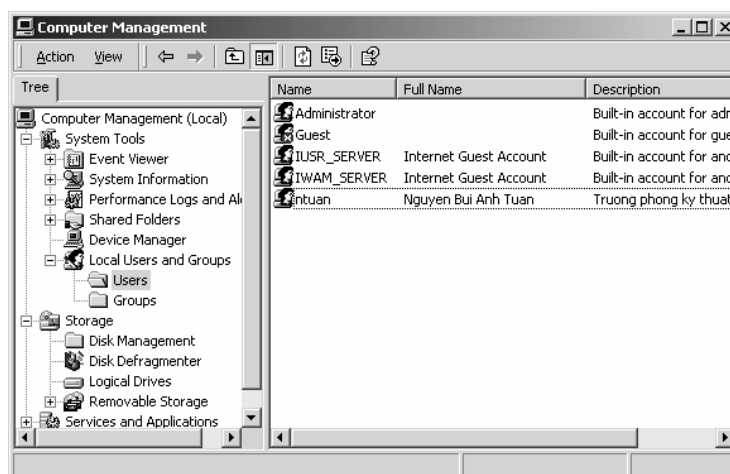


Chú ý: khi chọn **Delete** thì hệ thống xuất hiện hộp thoại hỏi bạn muốn xóa thật sự không vì tránh trường hợp bạn xóa nhầm. Bởi vì khi đã xóa thì tài khoản người dùng này không thể phục hồi được.

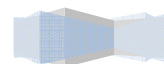


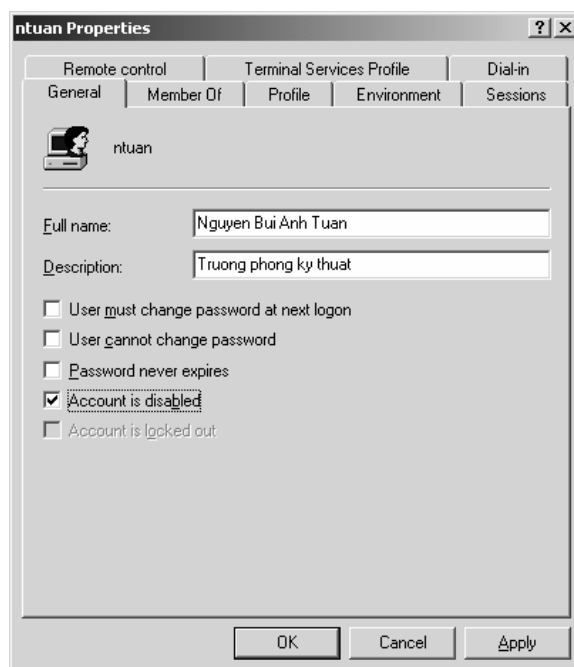
IV.2.3 Khóa tài khoản.

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**.





IV.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**.

IV.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**.

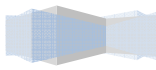
V. QUẢN LÝ TÀI KHOẢN NGƯỜI DÙNG VÀ NHÓM TRÊN ACTIVE DIRECTORY.

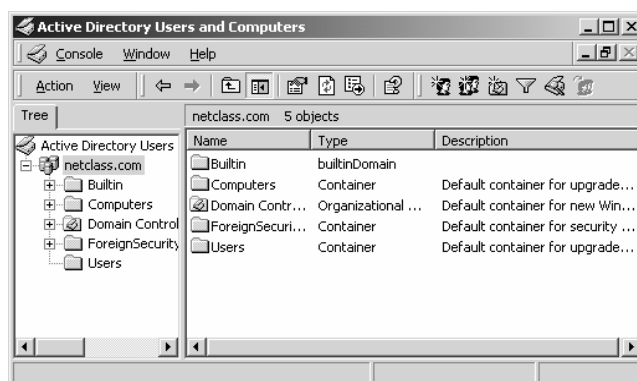
V.1. Tạo mới tài khoản người dùng.

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:

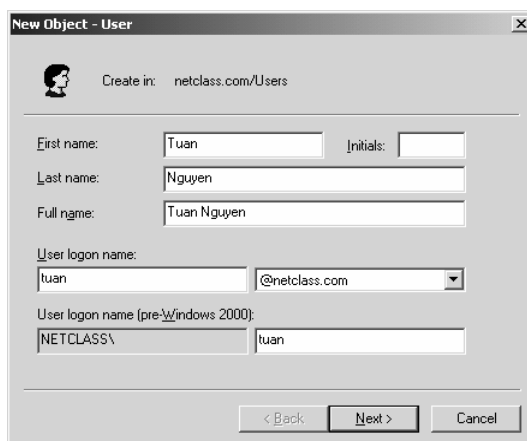
Chọn **Start** ⌚ **Programs** ⌚ **Administrative Tools** ⌚ **Active Directory Users and Computers**.

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





Hộp thoại **New Object-User** xuất hiện như hình sau, bạn nhập tên mô tả người dùng, tên tài khoản login 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.

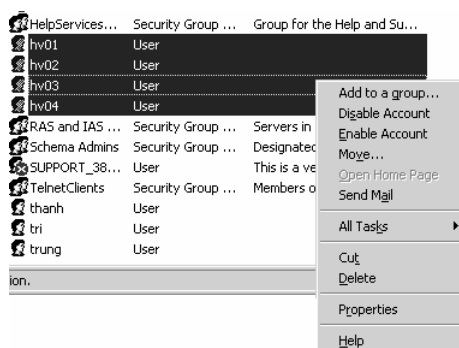


Hộp thoại thứ hai xuất hiện, cho phép bạn nhập vào mật khẩu (**password**) của tài khoản người dùng và đánh dấu vào các lựa chọn liên quan đến tài khoản như: cho phép đổi mật khẩu, yêu cầu phải đổi mật khẩu lần đăng nhập đầu tiên hay khóa tài khoản. Các lựa chọn này chúng ta sẽ tìm hiểu chi tiết ở phần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

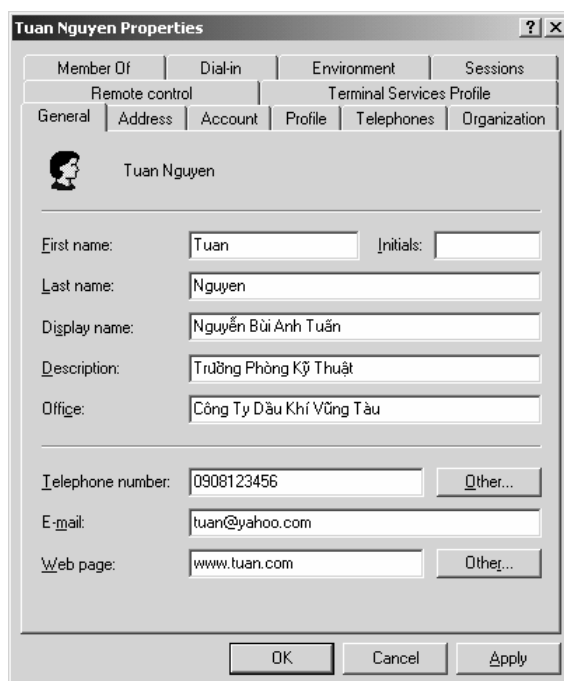
V.2. Các thuộc tính của tài khoản người dùng

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.

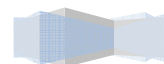


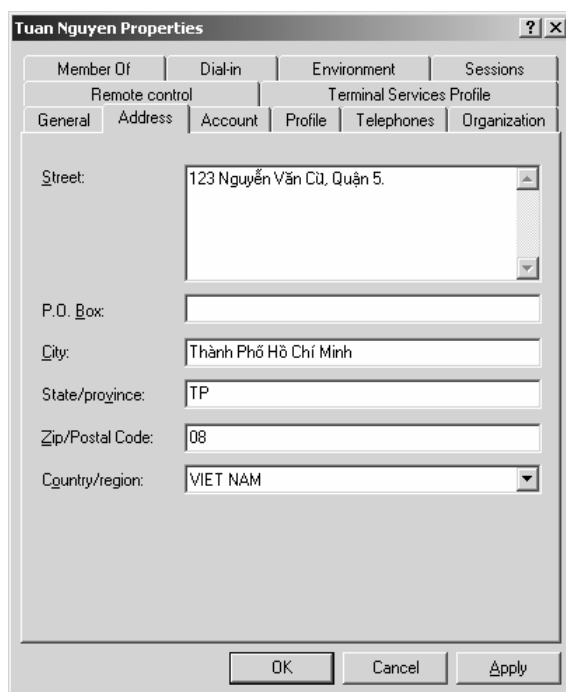
V.2.1 Các thông tin mở rộng của người dùng

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...





Tuan Nguyen Properties

Member Of: Dial-in: Environment: Sessions:

Remote control: Terminal Services Profile:

General Address Account Profile Telephones Organization

Street: 123 Nguyễn Văn Cù, Quận 5.

P.O. Box:

City: Thành Phố Hồ Chí Minh

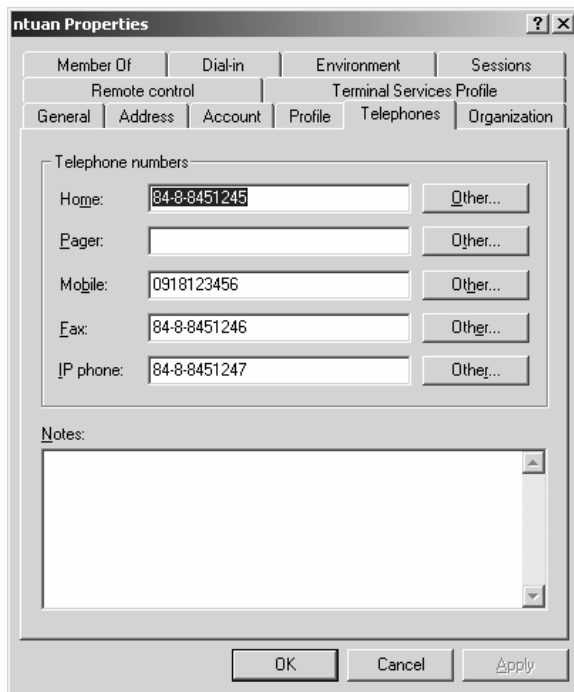
State/province: TP

Zip/Postal Code: 08

Country/region: VIET NAM

OK Cancel Apply

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



ntuan Properties

Member Of: Dial-in: Environment: Sessions:

Remote control: Terminal Services Profile:

General Address Account Profile Telephones Organization

Telephone numbers:

Home: 84-8-8451245 Other...

Pager: Other...

Mobile: 0918123456 Other...

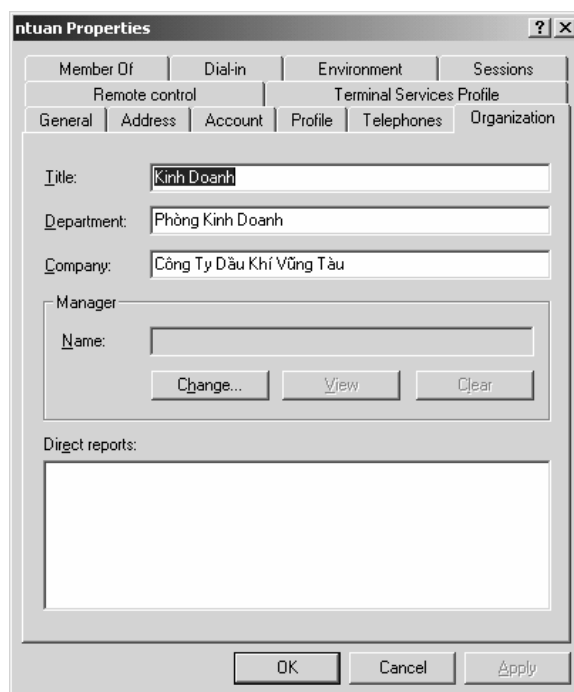
Fax: 84-8-8451246 Other...

IP phone: 84-8-8451247 Other...

Notes:

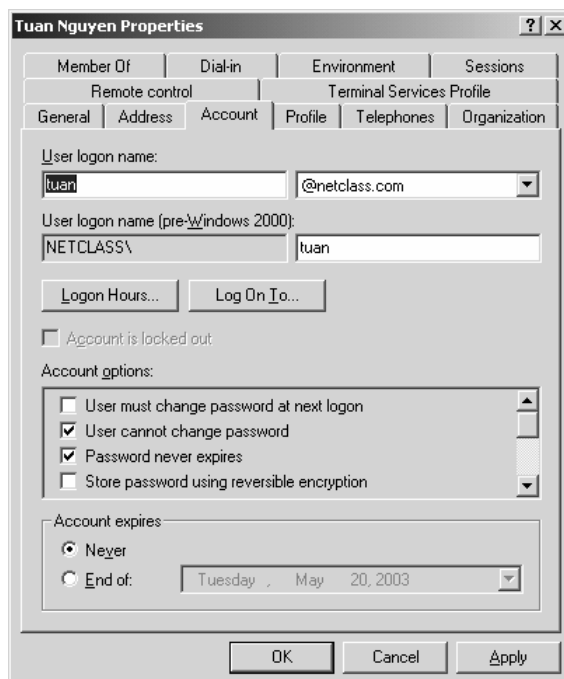
OK Cancel Apply

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 ...

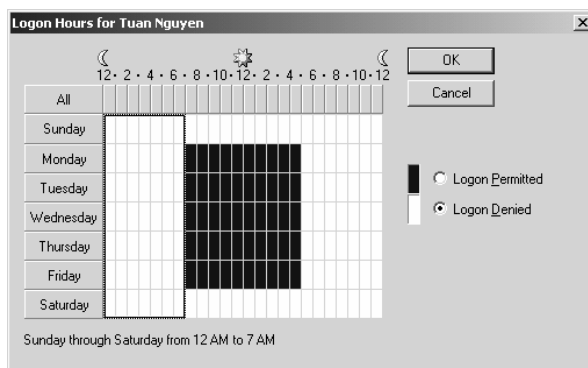


V.2.2 Tab Account.

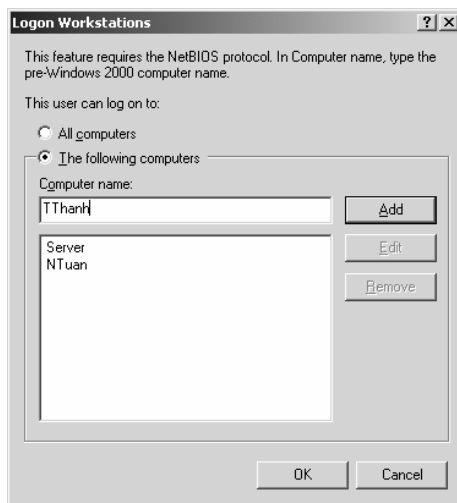
Tab **Account** cho phép bạn khai báo lại **username**, quy định giờ **logon** vào mạng cho người dùng, quy định máy trạm mà người dùng có thể sử dụng để vào mạng, quy định các chính sách tài khoản cho người dùng, quy định thời điểm hết hạn của tài khoản...



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**.



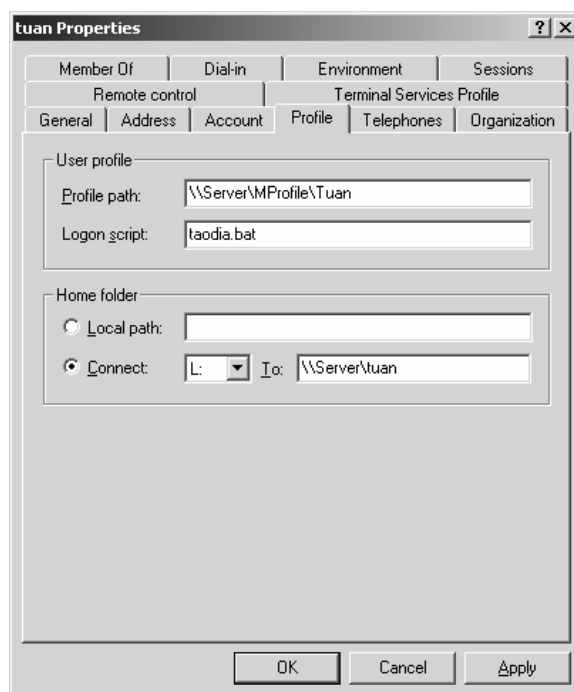
Bảng mô tả chi tiết các tùy chọn liên quan đến tài khoản người dùng:

Tùy Chọn	Ý Nghĩa
User must change password at next login	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 trusted for delegation	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 vắng 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.

V.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 xạ từ **Server**). Bạn có thể dùng nhiều ngôn ngữ kịch bản để tạo ra **logon script** như: lệnh **shell** của **DOS/NT/Windows**, **Windows Scripting Host (WSH)**, **VBScript**, **Jscript**...

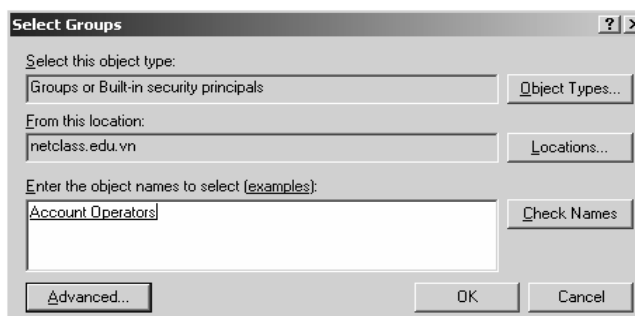
Đối với **Windows Server 2003** thì có hai cách để khai báo **logon script** là: khai báo trong thuộc tính của tài khoản người dùng thông qua công cụ **Active Directory User and Computers**, khai báo thông qua **Group Policy**. Nhưng chú ý trong cả hai cách, các tập tin **script** và mọi tập tin cần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

```
@echo off
rem Taodia.bat Version 1.0
rem neu nguoi dung logon ngay tai server thi khong lam gi ca.
ff %computername%.== tvthanh. goto END
rem xoa cac o dia anh xa dang ton tai
net use h: /delete >nul
net use j: /delete >nul
rem anh xa o dia h va j
net use h: \\tvthanh\users /yes >nul
net use j: \\tvthanh\apps /yes >nul
rem dong bo thoi gian voi Server
net time \\tvthanh /set /yes
:END
```

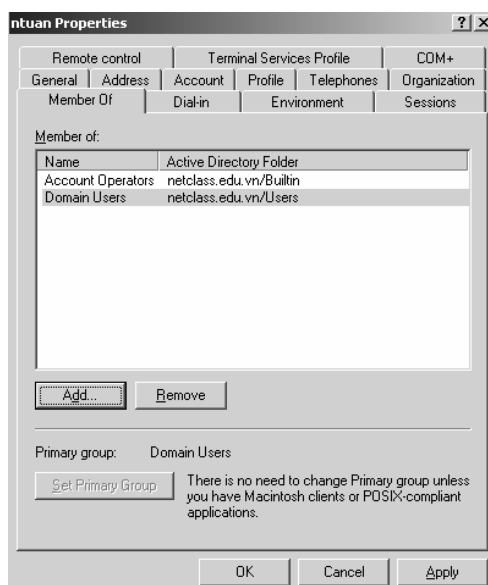
Thư mục cá nhân (**home folder hay home directory**) là thư mục dành riêng cho mỗi tài khoản người dùng, giúp người dùng có thể lưu trữ các tài liệu và tập tin riêng, đồng thời đây cũng là thư mục mặc định tại dấu nhắc lệnh. Muốn tạo một thư mục nhân cho người dùng thì trong mục **Connect** bạn chọn 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%”.

V.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.



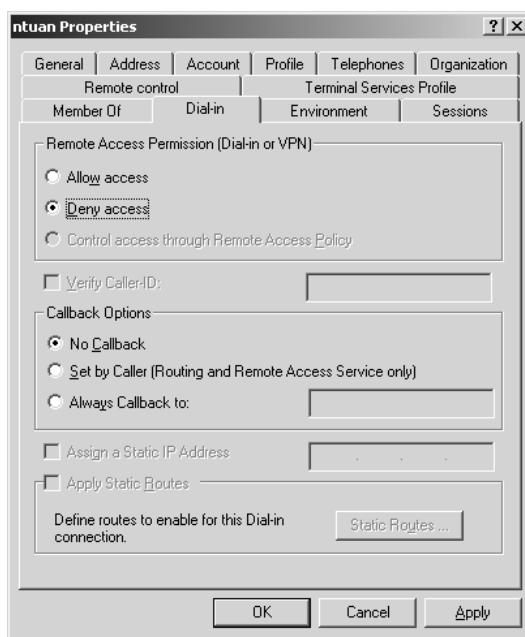
Trong hộp thoại chọn nhóm, nếu bạn nhớ tên nhóm thì có thể nhập trực tiếp tên nhóm vào và sau đó nhấp chuột vào nút **Check Names** để kiểm tra có chính xác không, bạn có thể nhập gần đúng để hệ thống tìm các tên nhóm có liên quan. Đây là tính năng mới của **Windows Server 2003** tránh tình trạng tìm 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**.

V.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**.



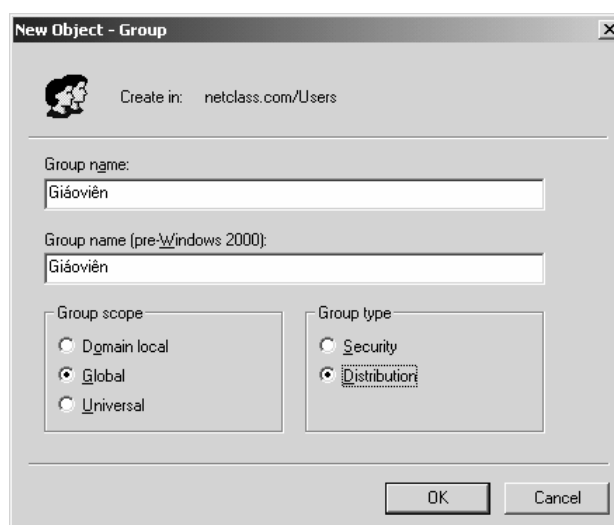
V.3. Tạo mới tài khoản nhóm.

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.



Nhấp chuột vào nút **OK** để hoàn tất và đóng hộp thoại.

V.4. Các tiện ích dòng lệnh quản lý tài khoản người dùng và tài khoản nhóm.

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

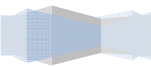
V.4.1 Lệnh net user.

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

Cú pháp:

```
net user [username [password | *] [options]] [/domain]
```

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



net user username [/delete] [/domain]

Ý nghĩa các tham số:

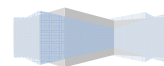
- Không tham số: dùng để hiển thị danh sách của tất cả các tài khoản người dùng trên máy tính
- **[Username]**: chỉ ra tên tài khoản người dùng cần thêm, xóa, hiệu chỉnh hoặc hiển thị. Tên của tài khoản người dùng có thể dài đến 20 ký tự.
- **[Password]**: ấn định hoặc thay đổi mật mã của tài khoản người dùng. Một mật mã phải có chiều dài tối thiểu bằng với chiều dài quy định trong chính sách tài khoản người dùng. Trong **Windows 2000** thì chiều dài của mật mã có thể dài đến 127 ký tự, nhưng trên hệ thống **Win9X** thì chỉ hiểu được 14 ký tự, do đó nếu bạn đặt mật mã dài hơn 14 ký tự thì có thể tài khoản này không thể **login** vào mạng từ máy trạm dùng **Win9X**.
- **[/domain]**: các tác vụ sẽ thực hiện trên máy điều khiển vùng. Tham số này chỉ áp dụng cho **Windows 2000 Server** là **primary domain controller** hoặc **Windows 2000 Professional** là thành viên của máy **Windows 2000 Server domain**.
- **[/add]**: thêm một tài khoản người dùng vào trong cơ sở dữ liệu tài khoản người dùng.
- **[/delete]**: xóa một tài khoản người dùng khỏi cơ sở dữ liệu tài khoản người dùng.
- **[/active:{no | yes}]**: cho phép hoặc tạm khóa tài khoản người dùng. Nếu tài khoản bị khóa thì người dùng không thể truy cập các tài nguyên trên máy tính. Mặc định là cho phép (**active**).
- **[/comment:"text"]**: cung cấp mô tả về tài khoản người dùng, mô tả này có thể dài đến 48 ký tự.
- **[/countrycode:nnn]**: chỉ định mã quốc gia và mã vùng.
- **[/expires:{date | never}]**: quy định ngày hết hiệu lực của tài khoản người dùng.
- **[/fullname:"name"]**: khai báo tên đầy đủ của người dùng.
- **[/homedir:path]**: khai báo đường dẫn thư mục cá nhân của tài khoản, chú ý đường dẫn này đã tồn tại.
- **[/passwordchg:{yes | no}]**: chỉ định người dùng có thể thay đổi mật mã của mình không, mặc định là có thể.
- **[/passwordreq:{yes | no}]**: chỉ định một tài khoản người dùng phải có một mật mã, mặc định là có mật mã.
- **[/profilepath:[path]]**: khai báo đường dẫn **Profile** của người dùng, nếu không hệ thống sẽ tự tạo một profile chuẩn cho người dùng lần **login** đầu tiên.
- **[/scriptpath:path]**: khai báo đường dẫn và tập tin **login script**. Đường dẫn này có thể là đường dẫn tuyệt đối hoặc đường dẫn tương đối (ví dụ: %systemroot%\System32\Repl\Import\Scripts).
- **[/times:{times | all}]**: quy định giờ cho phép người dùng login vào mạng hay máy tính cục bộ. Các thứ trong tuần được đại diện bởi ký tự : M, T, W, Th, F, Sa, Su. Giờ ta dùng AM, PM để phân biệt buổi sáng hoặc chiều. Ví dụ sau chỉ cho phép người dùng làm việc trong giờ hành chính từ thứ 2 đến thứ 6: "M,7AM-5PM; T,7AM-5PM; W,7AM-5PM; Th,7AM-5PM; F,7AM-5PM;"
- **[/workstations:{computername[,...] | *}]**: chỉ định các máy tính mà người dùng này có thể sử dụng để login vào mạng. Nếu **/workstations** không có danh sách hoặc danh sách là ký tự '*' thì người dùng có thể sử dụng bất kỳ máy nào để vào mạng.

V.4.2 Lệnh net group.

Chức năng: tạo mới thêm, hiển thị hoặc hiệu chỉnh nhóm toàn cục trên **Windows 2000 Server**

Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | <http://www.adminviet.net>

domains, lệnh này chỉ có hiệu lực khi dùng trên máy **Windows 2000 Server Domain Controllers**.



Cú pháp:

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

Ý nghĩa các tham số:

- Không tham số: dùng để hiển thị tên của Server và tên của các nhóm trên Server đó.
- **[Groupname]**: chỉ định tên nhóm cần thêm, mở rộng hoặc xóa.
- **[/comment:"text"]**: thêm thông tin mô tả cho một nhóm mới hoặc có sẵn, nội dung này có thể dài đến 48 ký tự.
- **[/domain]**: các tác vụ sẽ thực hiện trên máy điều khiển vùng. Tham số này chỉ áp dụng cho **Windows 2000 Server** là **primary domain controller** hoặc **Windows 2000 Professional** là thành viên của máy **Windows 2000 Server domain**.
- **[username[...]]**: danh sách một hoặc nhiều người dùng cần thêm hoặc xóa ra khỏi nhóm, các tên này cách nhau bởi khoảng trắng.
- **[/add]**: thêm một nhóm hoặc thêm một người dùng vào nhóm.
- **[/delete]**: xóa một nhóm hoặc xóa một người dùng khỏi nhóm.

V.4.3 Lệnh net localgroup.

Chức năng: thêm, hiển thị hoặc hiệu chỉnh nhóm cục bộ.

Cú pháp:

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

Ý nghĩa các tham số:

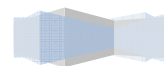
- Không tham số: dùng để hiển thị tên server và tên các nhóm cục bộ trên máy tính hiện tại.
- **[Groupname]**: chỉ định tên nhóm cần thêm, mở rộng hoặc xóa.
- **[/comment:"text"]**: thêm thông tin mô tả cho một nhóm mới hoặc có sẵn, nội dung này có thể dài đến 48 ký tự.
- **[/domain]**: các tác vụ sẽ thực hiện trên máy điều khiển vùng. Tham số này chỉ áp dụng cho **Windows 2000 Server** là **primary domain controller** hoặc **Windows 2000 Professional** là thành viên của máy **Windows 2000 Server domain**.
- **[name [...]]**: danh sách một hoặc nhiều tên người dùng hoặc tên nhóm cần thêm vào hoặc xóa khỏi nhóm cục bộ. Các tên này cách nhau bởi khoảng trắng.
- **[/add]**: thêm tên một nhóm toàn cục hoặc tên người dùng vào nhóm cục bộ.
- **[/delete]**: xóa tên một nhóm toàn cục hoặc tên người dùng khỏi nhóm cục bộ.

V.4.4 Các lệnh hỗ trợ dịch vụ Active Directory trong môi trường Windows Server 2003.

Trên hệ thống **Windows Server 2003**, **Microsoft** phát triển thêm một số lệnh nhằm hỗ trợ tốt hơn cho dịch vụ **Directory** như: **dsadd**, **dsrm**, **dsmove**, **dsget**, **dsmod**, **dsquery**. Các lệnh này thao tác chủ

Download tài liệu này tại diễn đàn quản trị mạng và quản trị hệ thống | <http://www.adminviet.net>

yếu trên các đối tượng **computer, contact, group, ou, user, quota**.



- **Dsadd**: cho phép bạn thêm một **computer**, **contact**, **group**, **ou** hoặc **user** vào trong dịch vụ **Directory**.
- **Dsrm**: xóa một đối tượng trong dịch vụ **Directory**.
- **Dsmove**: di chuyển một đối tượng từ vị trí này đến vị trí khác trong dịch vụ **Directory**.
- **Dsget**: hiển thị các thông tin lựa chọn của một đối tượng **computer**, **contact**, **group**, **ou**, **server** hoặc **user** trong một dịch vụ **Directory**.
- **Dsmod**: chỉnh sửa các thông tin của **computer**, **contact**, **group**, **ou** hoặc **user** trong một dịch vụ **Directory**.
- **Dsquery**: truy vấn các thành phần trong dịch vụ **Directory**.
- Ví dụ:
- Tạo một **user** mới: `dsadd user "CN=hv10, CN=Users, DC=netclass, DC=edu, DC=vn" -samid hv10 -pwd 123`
- Xóa một **user**: `dsrm "CN=hv10, CN=Users, DC=netclass, DC=edu, DC=vn"`
- Xem các **user** trong hệ thống: ***dsquery user***
- Gia nhập **user** mới vào nhóm: `dsmod group "CN=hs, CN=Users, DC=netclass, DC=edu, DC=vn" -addmbr "CN=hv10, CN=Users, DC=netclass, DC=edu, DC=vn"`

