……..o0o……..


# Mạng máy tính và viễn thông

Khoa Công nghệ Thông tin – Đại học Khoa học tự nhiên

Bộ môn Mạng máy tính và Viễn thông

---

Môn: Mạng máy tính nâng cao

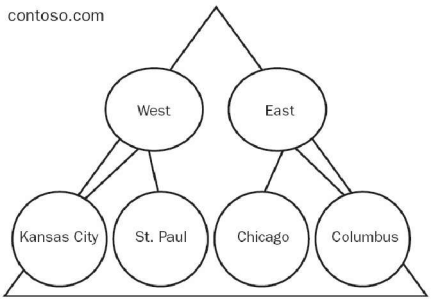
Bài thực hành số 6:Active Directory

1. GIỚI THIỆU ACTIVE DIRECTORY
   1.1. Directory Service: cung cấp chức năng lưu trữ, xác định (locating), quản lý tập trung các tài nguyên trên như máy in, thư mục dữ liệu chia sẻ trên mạng, các tài khoản về người dùng, nhóm người dùng …
   1.2. Domain: Nhóm các máy tính (servers và workstations) sử dụng chung cơ sở dữ liệu về các tài khoản người dùng.
   1.3. Active Directory là directory service của hệ điều hành mạng Windows 2000/2003. Máy tính chạy AD được gọi là domain controller.
   1.4. Các objects trong Active Directory: Thông tin về các tài nguyên mạng được tổ chức thành các object. *Ví dụ thông tin về user, computer.*
      1.4.1. User Account
         1. Local User Account: chỉ có ý nghĩa trên máy tính mà account đó được tạo ra.
         2. Domain User Account: được tạo ra trong Active Directory. Account này có ý nghĩa trên tất cả các tài nguyên mạng trong cùng domain.
      1.4.2. Computer
      1.4.3. Group: Các user account được nhóm lại thành group để tiện cho việc quản lý. Trong AD có 2 loại group: security group (được sử dụng chủ yếu trong những tác vụ liên quan đến security, vd: phân quyền truy cập các tài nguyên trong AD) và distribution group (được sử dụng chỉ trong những tác vụ không liên quan đến bảo mật, vd: gửi mail đến một nhóm người dùng).Security group có đầy đủ các chức năng của một distribution group.

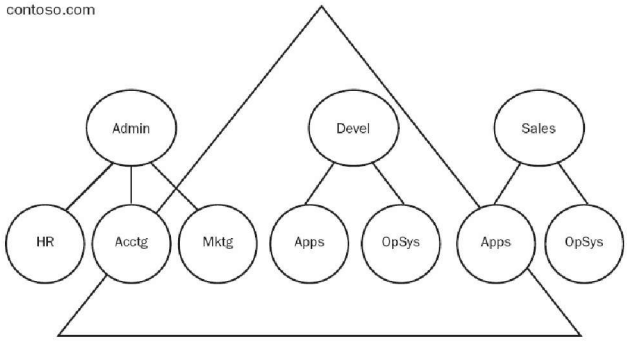
| | Membership | Resource Access |
|---|---|---|
| Global | Local domain | Any domain |
| Domain local | Any domain | Local domain |
| Universal | Any domain | Any domain |

   1.5. DNS:AD có cùng cấu trúc với DNS. AD client sử dụng DNS để xác định domain controller. Trong trường hợp hệ thống cho phép ra Internet, việc chọn tên cho domain cần phải cân nhắc để tránh việc trùng tên với DNS domain ở ngoài.
   1.6. OU(organizational unit): Để tiện lợi cho việc quản lý, các objects trong domain được tổ chức vào các OUs.

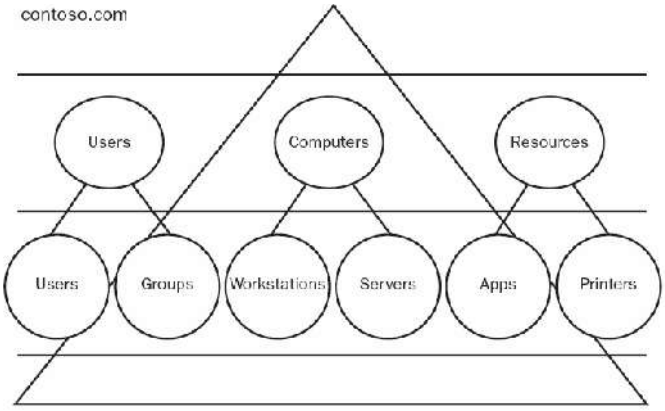
   OU được tổ chức dựa trên vị trí địa lý.




OU được tổ chức dựa trên chức năng công việc



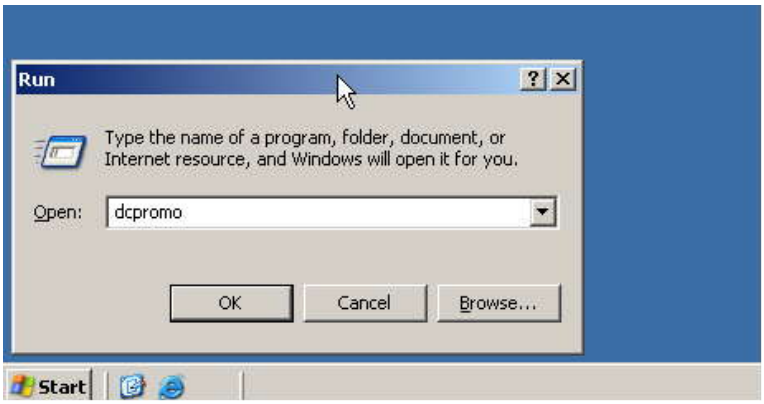

OU được tổ chức dựa trên loại tài nguyên



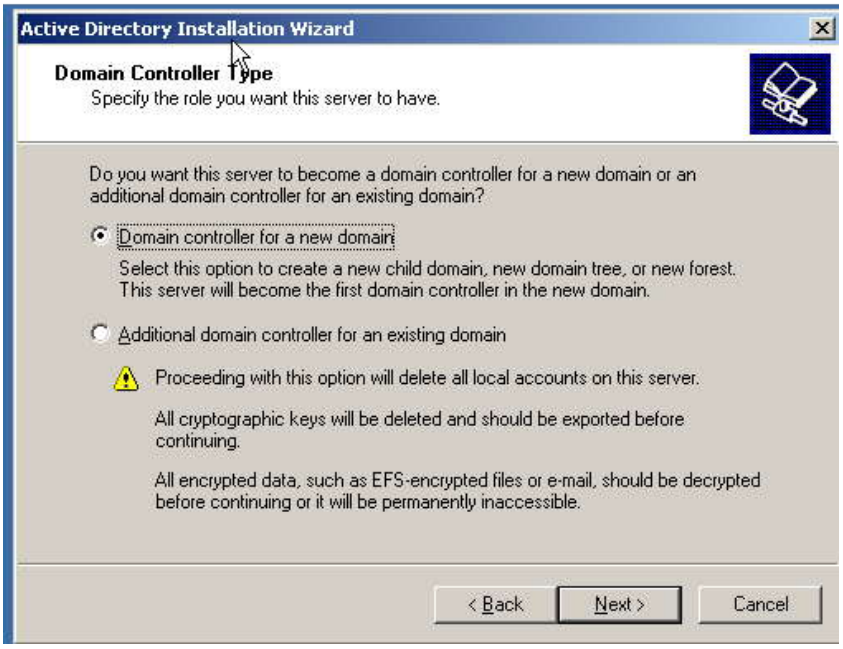

## 2. MỘT SỐ THAO TÁC TRÊN ACTIVE DIRECTORY

### 2.1. Cài đặt Active Directory

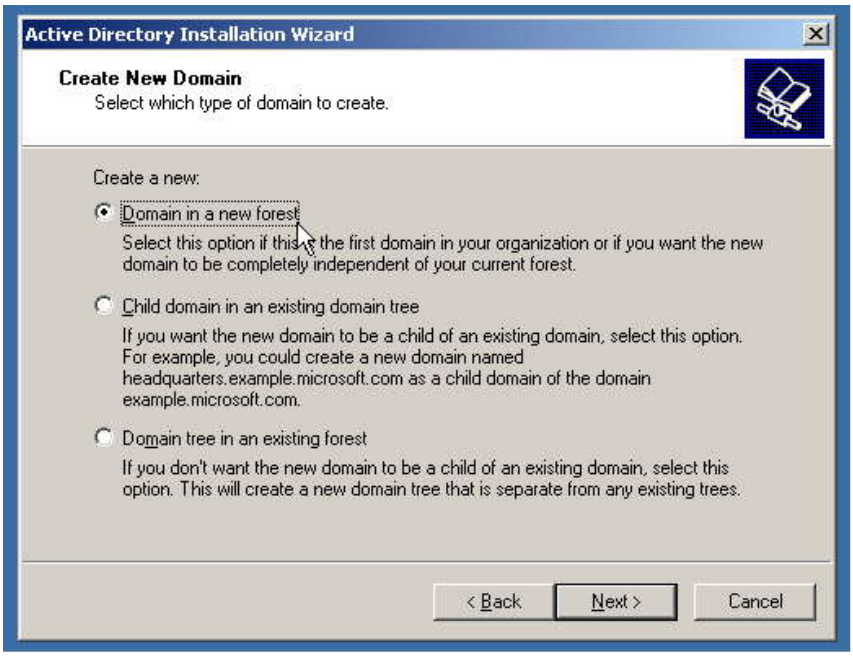
1. Gọi lệnh dcpromo



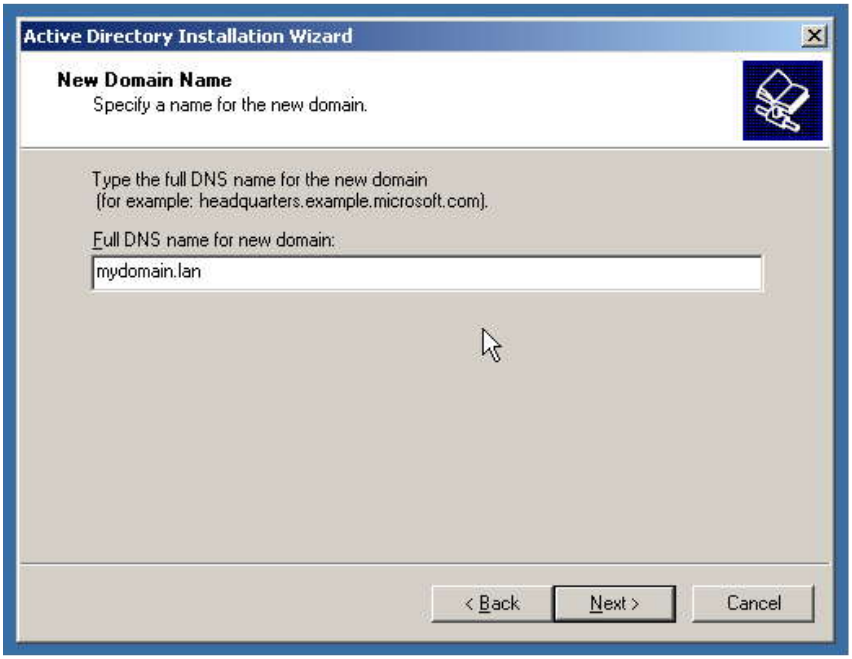

2. Chọn cài đặt domain controller cho domain mới



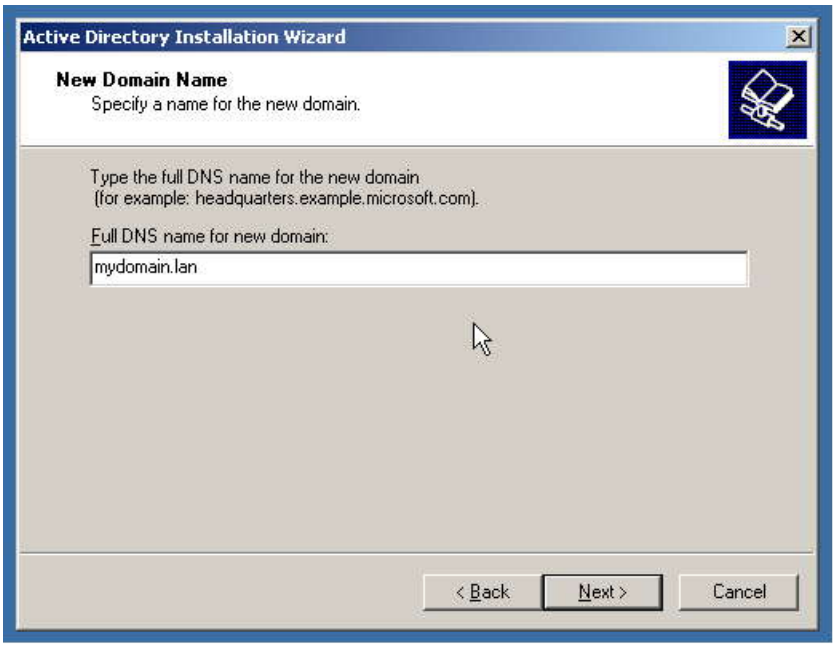

3. Chọn tạo root domain cho một forest mới.



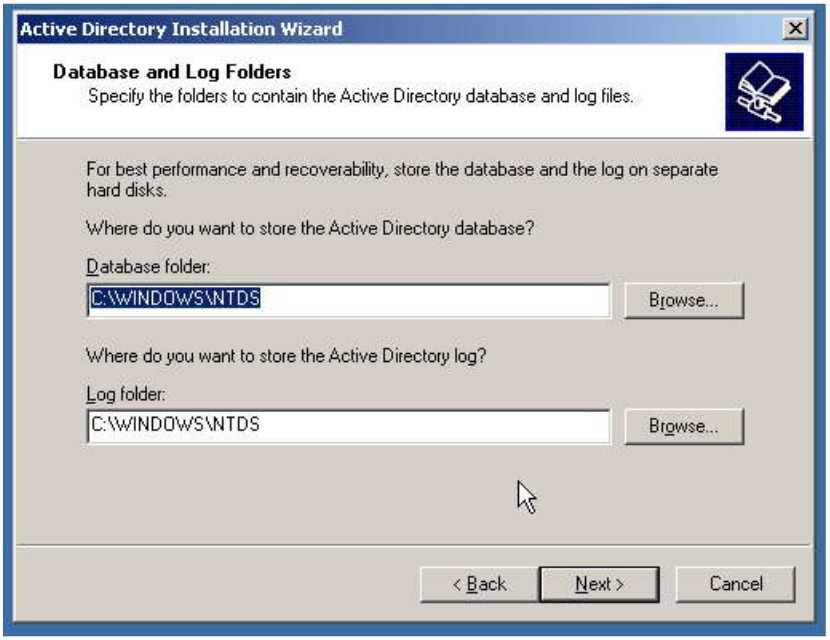

4. Đặt tên cho domain



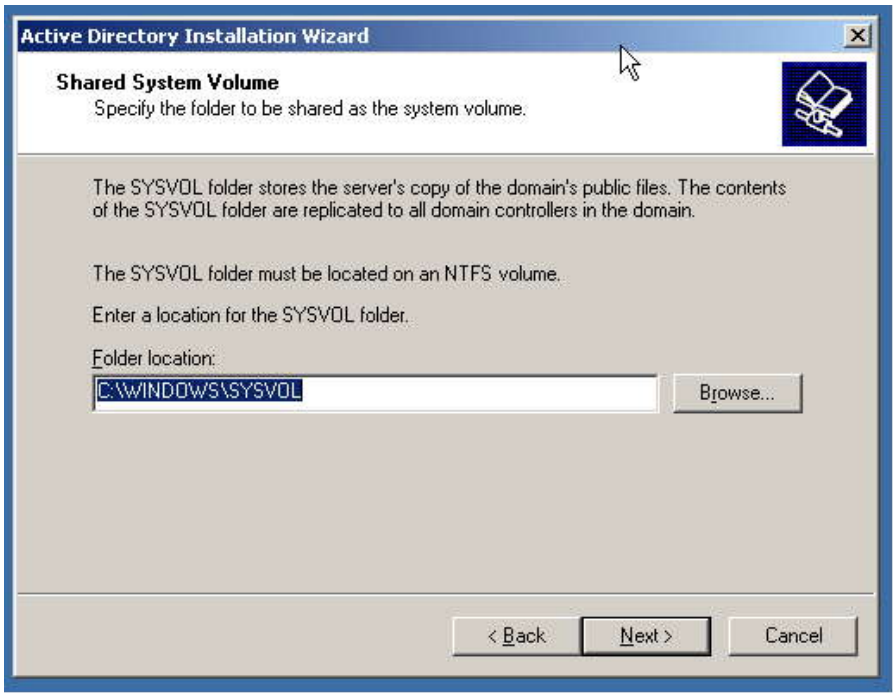

5. Chọn NETBIOS name cho domain



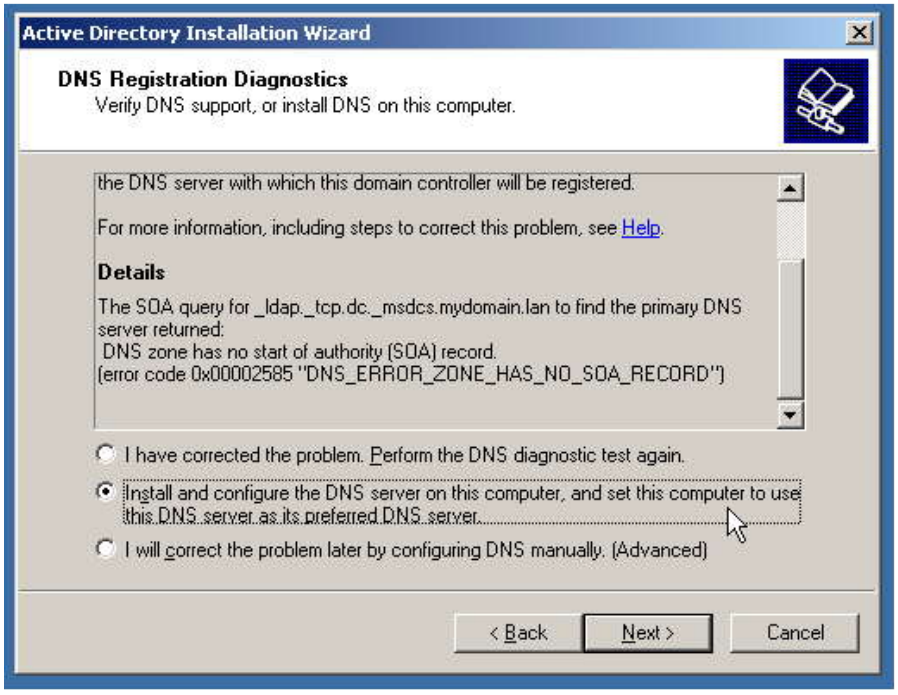

6. Chọn vị trí lưu database và log file của Active Directory




7. Chọn vị trí lưu thông tin do AD publish

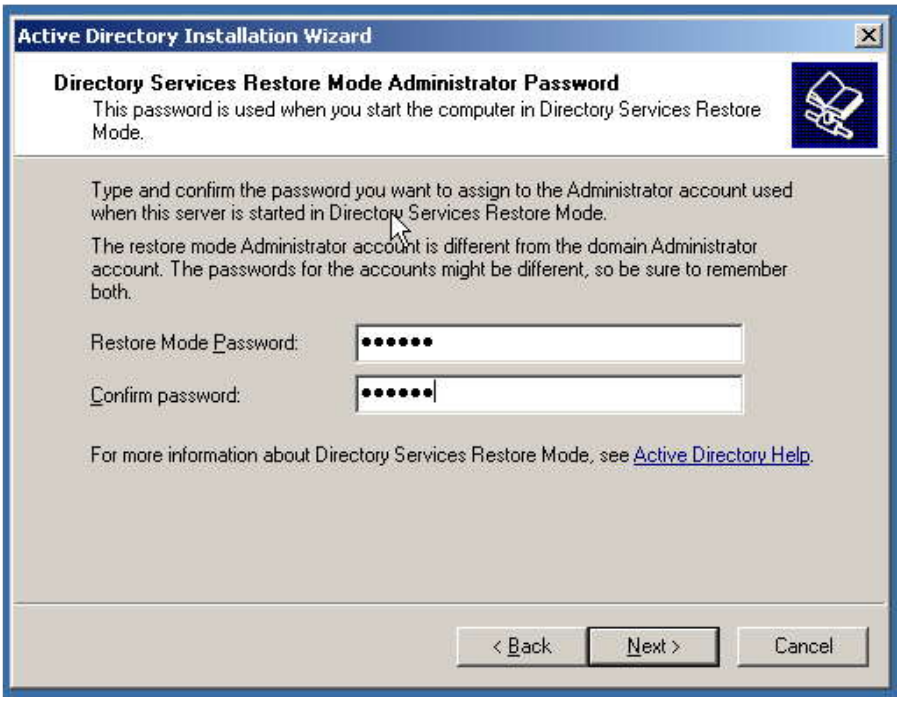



8. Cấu hình DNS phục vụ cho AD. Chọn AD Installation Wizard tự động cài đặt DNS và cấu hình domain controller sử dụng DNS server này.



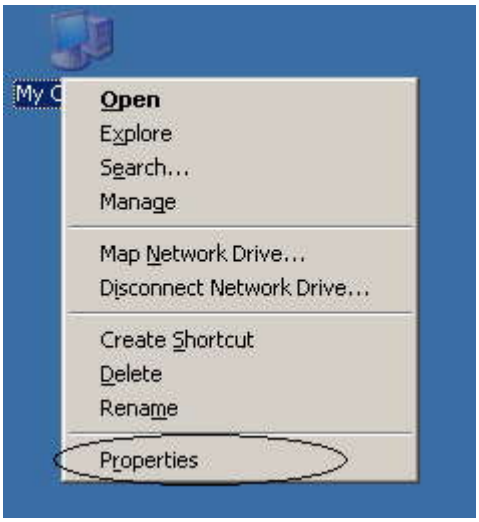

9. Chọn permission mặc định cho


10. Chọn password cho account Administrator dùng trong trường hợp doman controller chạy ở mode restore hoặc khi gỡ bỏ AD directory khỏi domain cotroller.

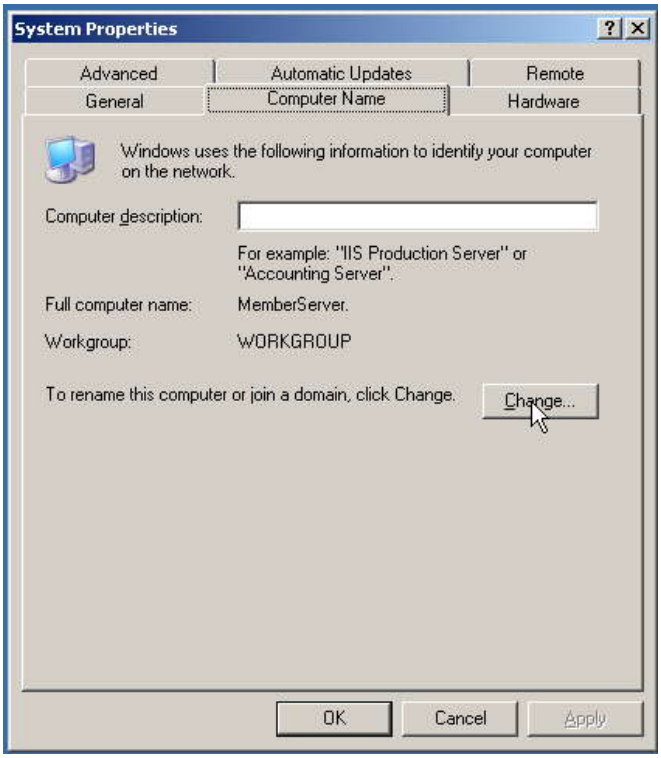



2.2. Thêm một máy tính vào domain (join domain)

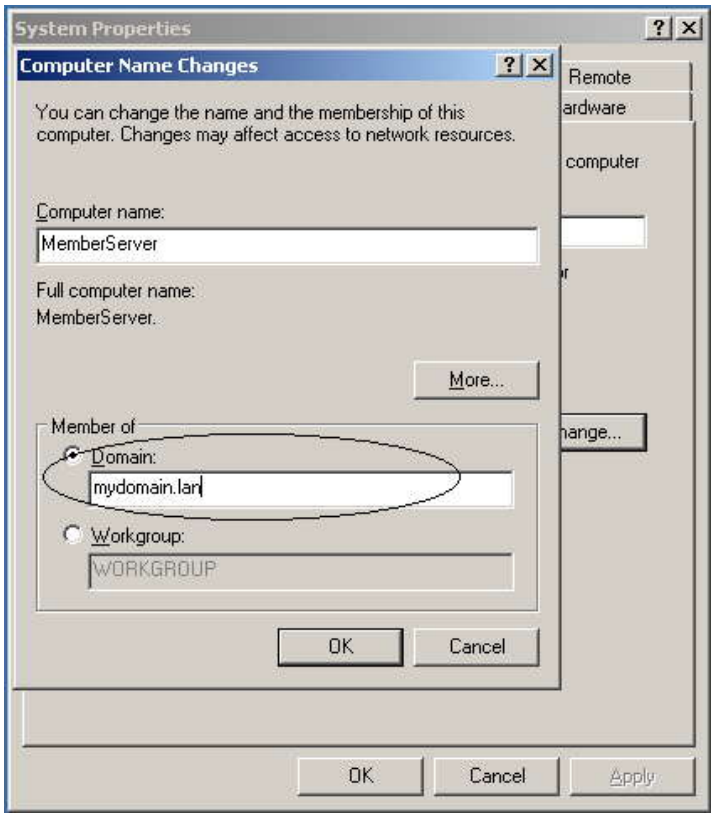
1. Chọn property của My computer




2. Chọn change computer name or join a domain trong tab Computer name.




3. Nhập tên của domain máy tính muốn gia nhập vào.




4. Nhập user name và password của account được phép join máy tính vào domain


2.3. User: Roaming user profile

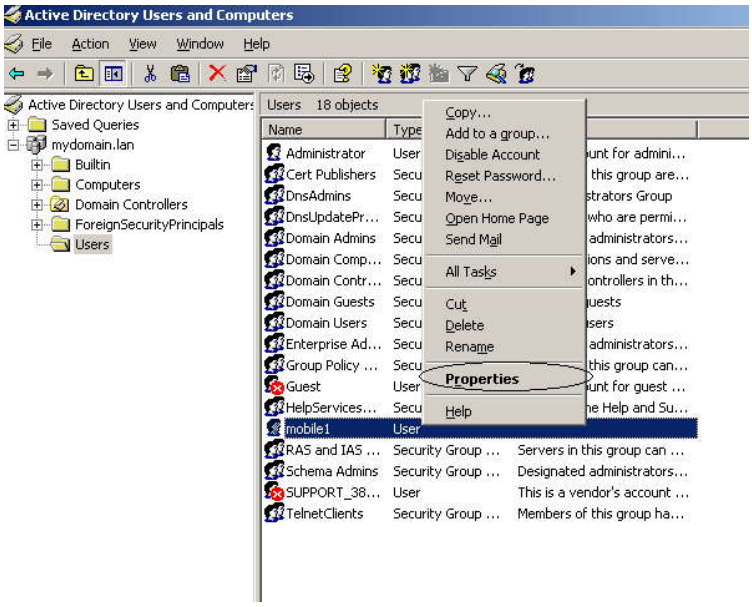
User profile: Chứa thông tin về tùy chọn của người dùng. VD: Desktop, application settings, những network connection đã được thiết lập (chẳng hạn mapped network drive).

Mặc định, khi một user log on vào một máy tính, profile của user sẽ được tạo ra trên máy tính đó (local user profile).

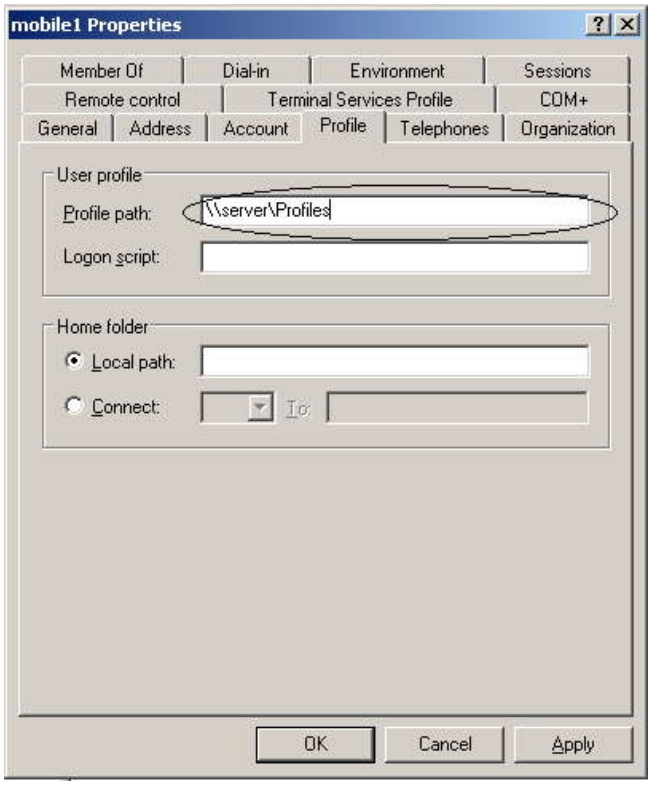
Roaming user profile: cho phép user nhận được profile như nhau bất kể user đó log on vào máy tính nào trong domain. Để thực hiện điều này, các profile sẽ được lưu tập trung trên một thư mục shared.

1. Share một thư mục để chứa profiles.
2. Chọn Active Directory Users and Computer console.


3. Chọn Properties của roaming user.

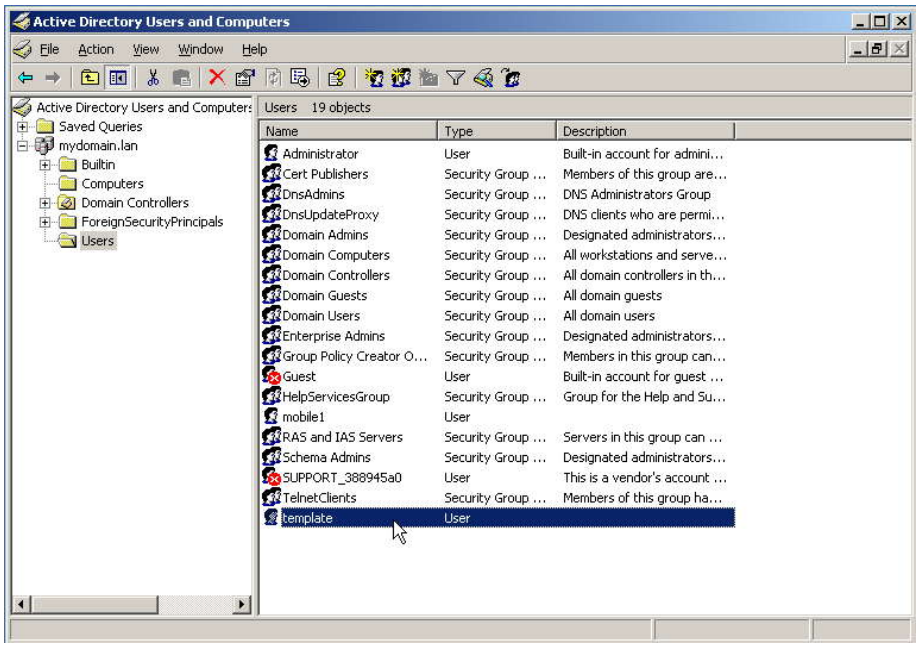



4. Chỉ ra vị trí lưu profile cho user:\\server\Profiles\%username%



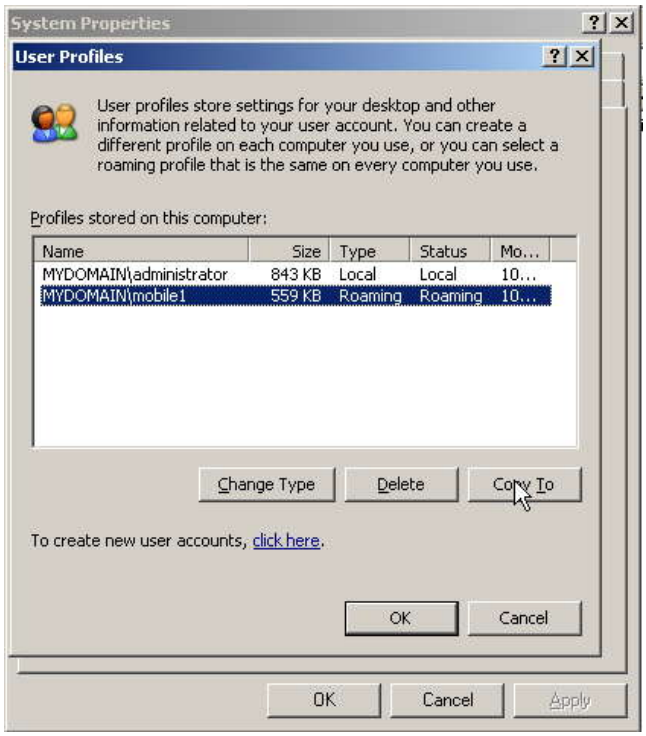

2.4. Mandatory User Profile:

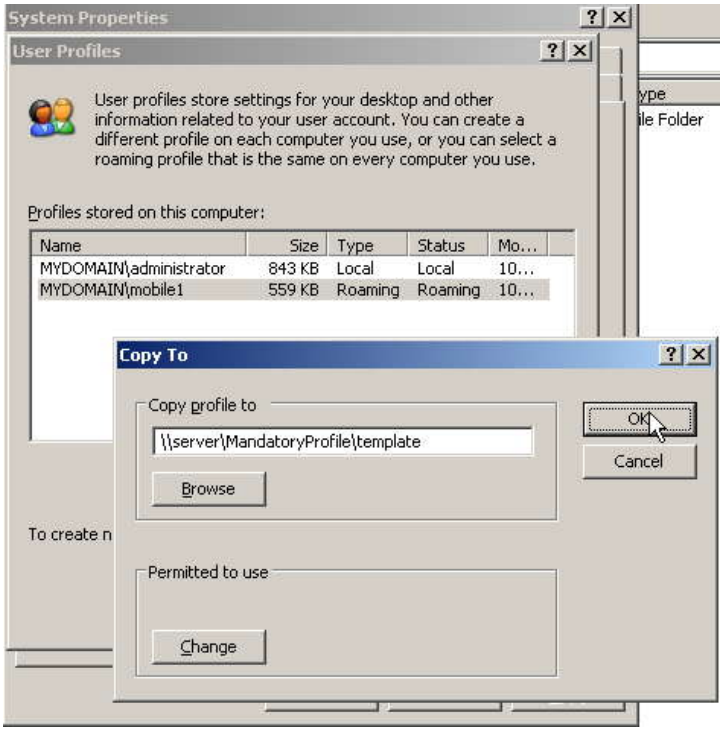
1. Tạo một account để làm mẫu (các mandatory user profile được tạo sau này sẽ giống như profile của user mẫu này).



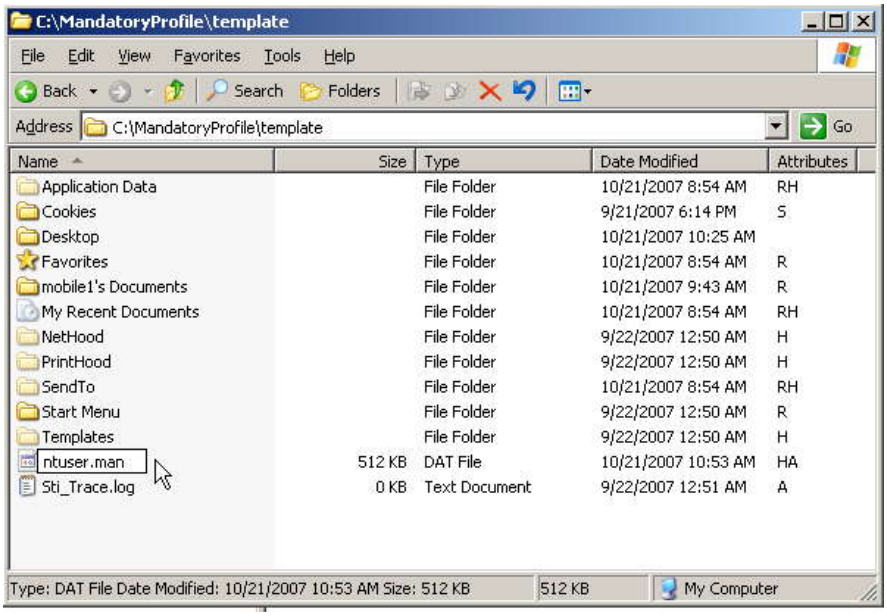

2. Log on vào vào domain controller bằng account mẫu vừa tạo. Điều chỉnh profile theo ý muốn (tạo shortcuts, map network drive…)

3. Vào properties của máy tính ở bước 2. Chọn Settings của phần User Profile ở tab Advanced. Copy profile của account mẫu vào thư mục share đã được tạo.

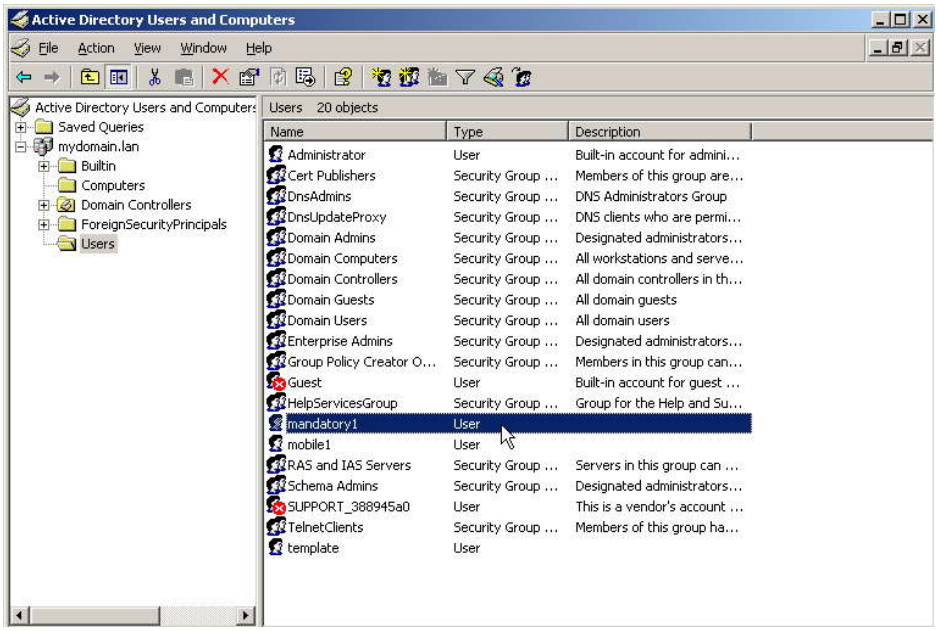




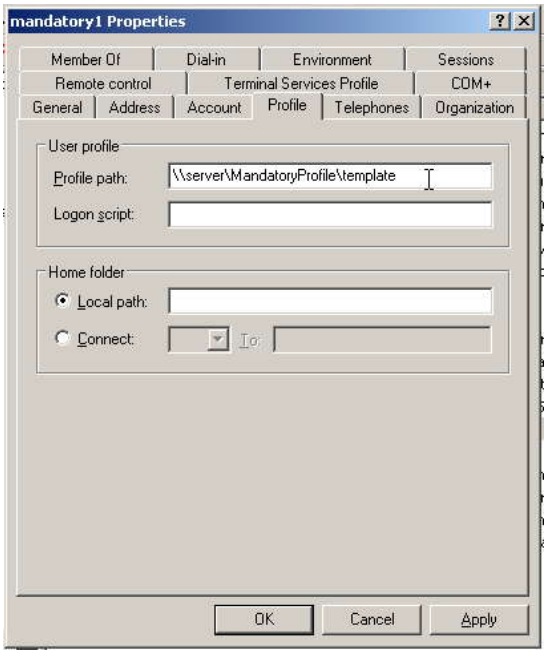

4. Tại vị trí lưu profile mẫu vừa được copy ở bước 3. Tìm và đổi tên file ntuser.dat thành ntuser.man (Lưu ý file này có thuộc tính ẩn).




5. Tạo ra account sử dụng manatory profile




6. Cấu hình profile của mandatory account là profile mẫu được copy ở bước 3.




2.4.2. Home folder:

Thư mục mà người dùng có thể lưu trữ dữ liệu. Home folder có thể đặt ở local hoặc đặt trên một thư mục share trên mạng. Home folder không phải là một bộ phận của profile nên trong trường hợp home folder và user profile được đặt tại một thư mục share trên mạng, home folder không cần phải tải về khi user log on.

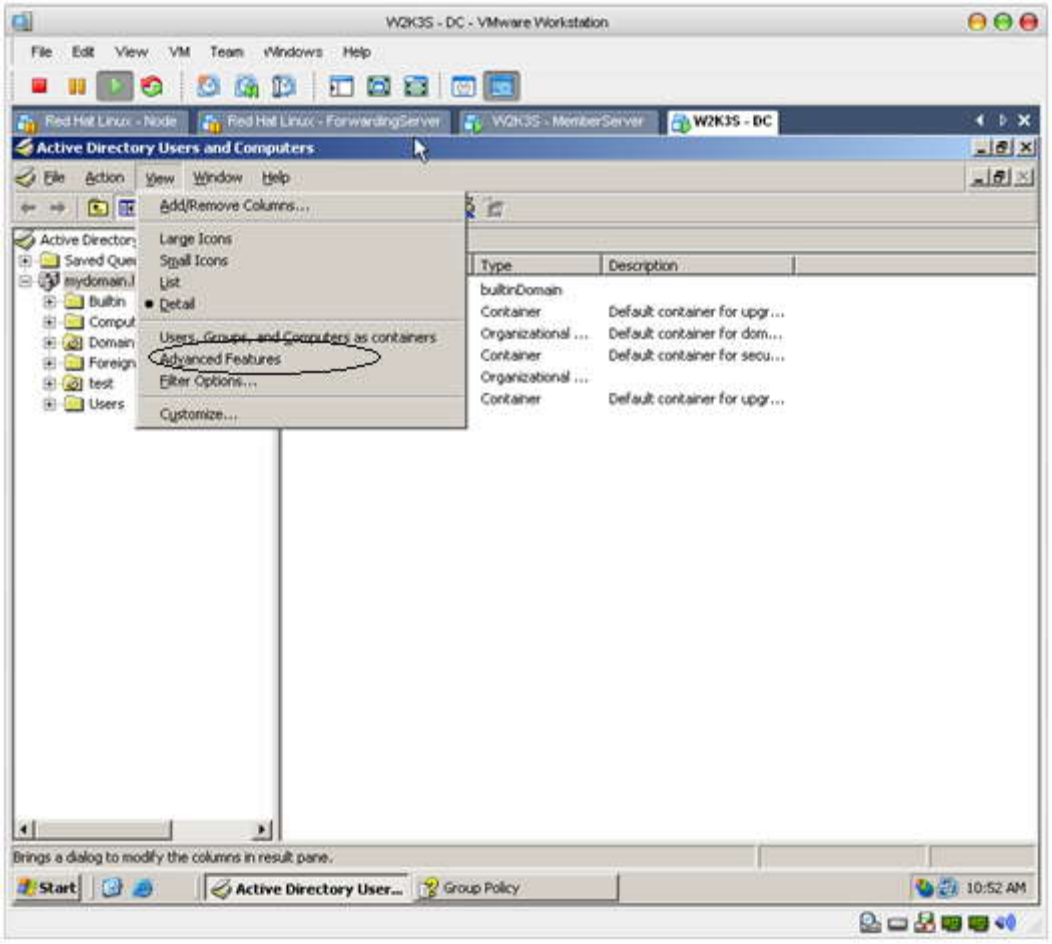
2.4.3. Log on script:

Script được chạy mỗi khi user log on vào máy tính.

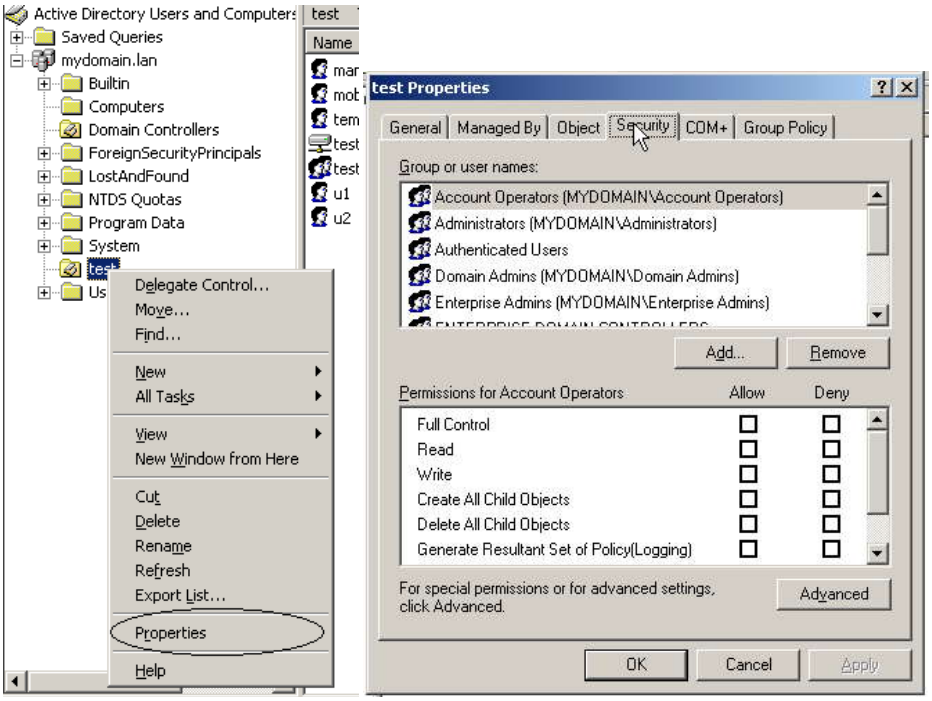
## 2.5. Control access to AD

Việc kiểm soát các thao tác (operation) lên những resources trong AD có thể được thực hiện theo cơ chế tương tự như NTFS permission. Mỗi resource có 1 ACL (Access Control List) để kiểm soát ai có thể thực hiện những hành động gì lên chính resource đó. Việc này được thực hiện bằng Active Directory Users and Computers Snap-in.

Để hiện thị chức năng Control Access, ta chọn chức năng Advanced Features

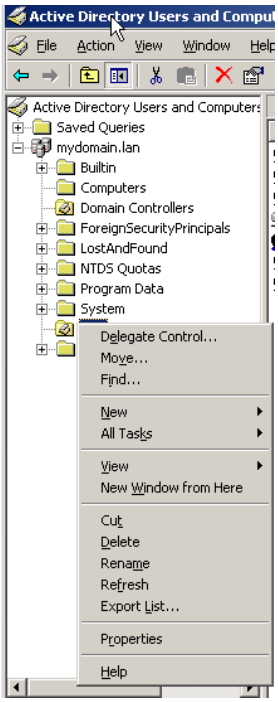



ACL của các objects trong AD được truy cập thông qua tab Security.




## 2.6. Delegate Control

Các object như domain, OU các access permission được tổ chức thành từng nhóm thuận tiện cho việc phân quyền. Việc phân quyền trên các nhóm permission này được thực hiện thông qua Delegate Control Wizard.

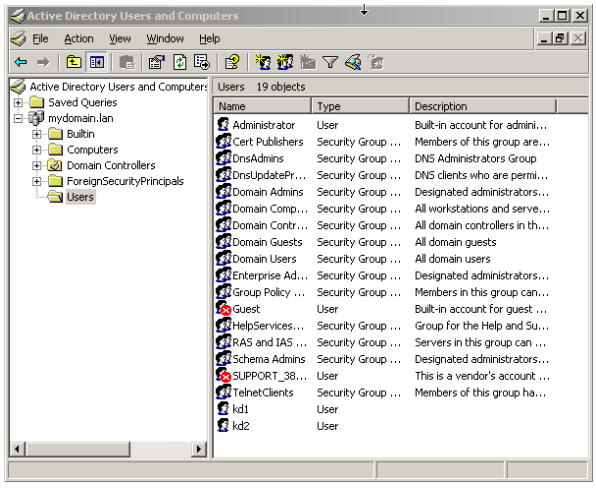


## 2.7. Sử dụng Group Policy.

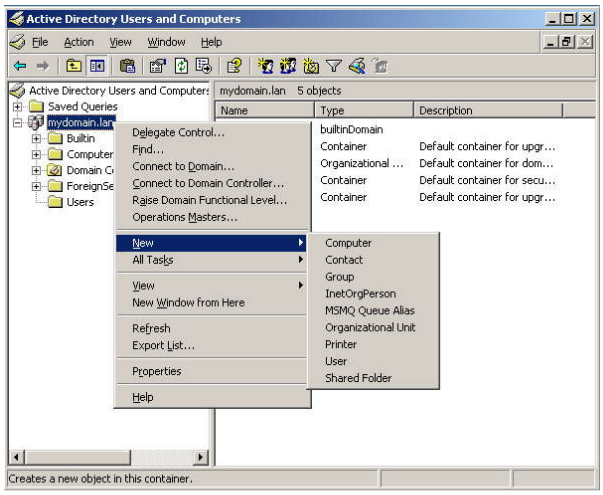
Để thuận tiện cho việc quản lý một hệ thống lớn, Active Directory cung cấp công cụ Group Policy cho phép áp đặt những chính sách lên toàn bộ hệ thống. Các chính sách có thể áp đặt dựa trên máy tính hoặc người dùng (khi người dùng logon/logoff, khi máy tính khởi động lên/hoặc tắt sẽ phải thực hiện một số công việc nào đó được quy định trong Group Policy). *Tham khảo tài liệu về Group Policy để thấy được các khả năng được cung cấp bởi Group Policy*.
Ta có thể áp dụng Group Policy trên một số đối tượng (máy tính/ người dùng) được lựa chọn thông qua OU. Các người dùng (máy tính) cần phải thực hiện một số yêu cầu giống nhau nào đó sẽ được đặt vào một OU, Group Policy sẽ được áp đặt lên OU này.

Trong ví dụ minh họa sau, ta sẽ áp đặt Group Policy cho một số người dùng được lựa chọn.
Giả sử: các nhân viên trong phòng Kinh doanh cần áp đặt một số chính sách nào đó (Ví dụ, cấm những nhân viên này không được sử dụng command line và Control Panel). Account của các nhân viên này cần được đặt trong một OU và các Group Policy cần thiết sẽ được áp đặt lên OU này.

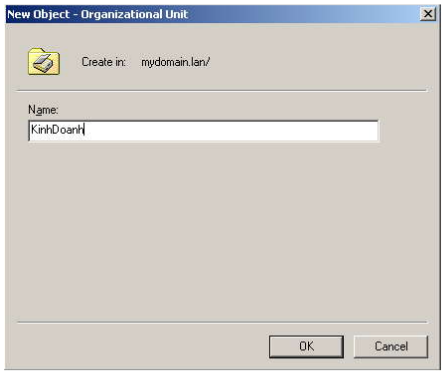
B0.Giả sử đã có các account của nhân viên phòng Kinh doanh: kd1, kd2




B1.Tạo OU KinhDoanh để chứa các account này.
Right-click lên domain muốn tạo OU, chọn 'New', chọn 'Organizational Unit'.

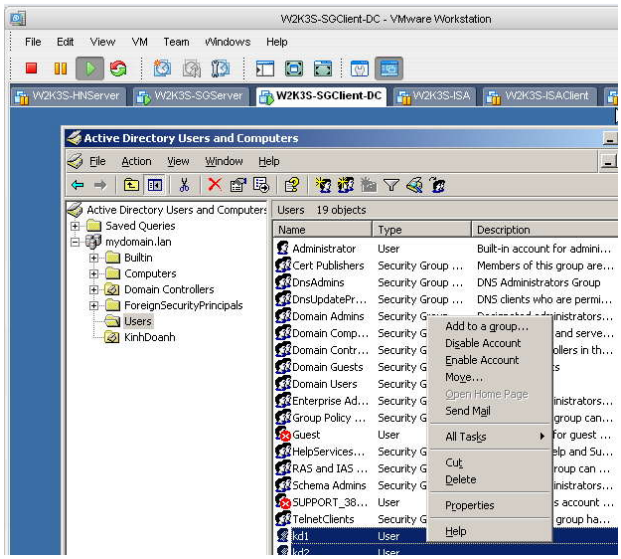



B2.Đặt tên cho OU.

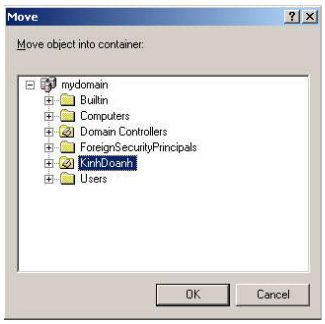



B3.Di chuyển các account kd1, kd2 vào OU KinhDoanh.

Right-click lên các account muốn di chuyển, chọn 'Move'.

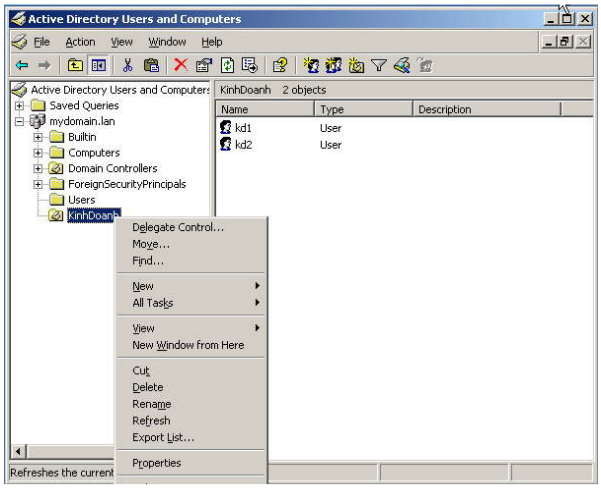



B4.Chọn vị trí muốn di chuyển đến (OU KinhDoanh).

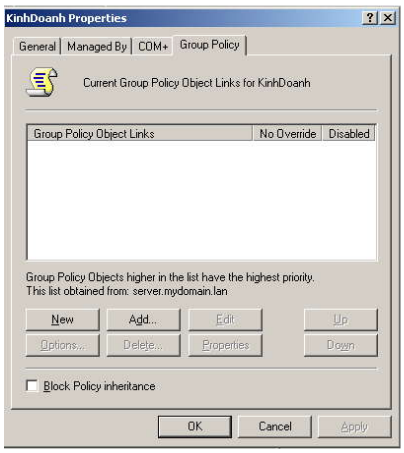



B5.Cấu hình Group Policy cho OU KinhDoanh.

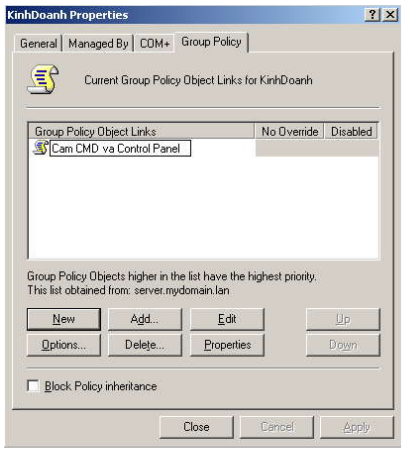
Right-click lên đối tượng muốn tạo Group Policy, chọn Properties




B6.Chọn tab Group Policy, chọn nút 'New'.

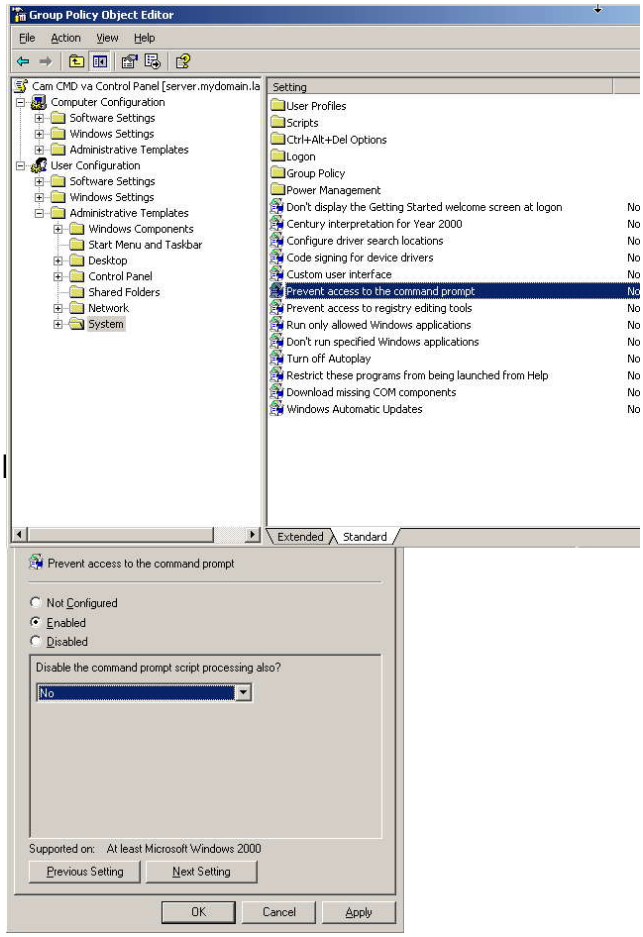



B7.Đặt tên lại cho Group Policy, chọn 'Edit'.



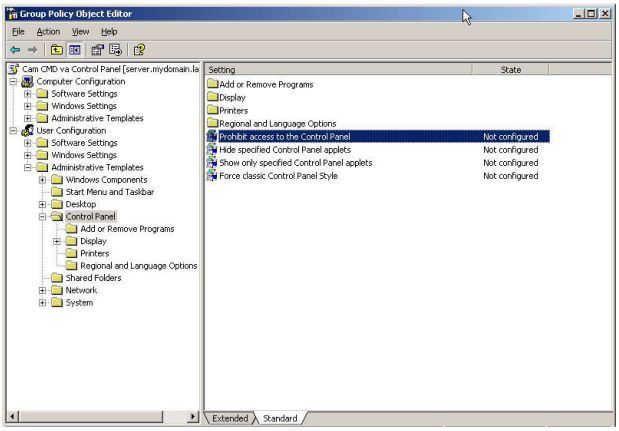

B8.Chỉnh sửa lại Group Policy theo yêu cầu. Cấm không cho người dùng sử dụng command line.

Chọn User Configuration/Administrative Templates/System/; double-click 'Prevent access to the command prompt'.

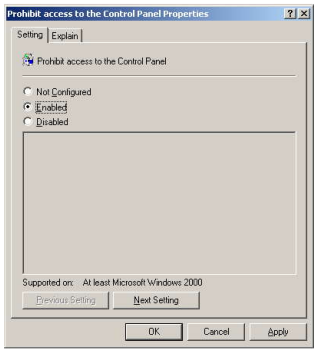



B10.Cấu hình cấm người dùng truy cập Control Panel.

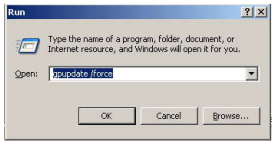
Chọn  User Configuration/Administrative Templates/System/; double-click 'Prohibit access to the Control Panel'.




B11.Chọn 'Enabled'

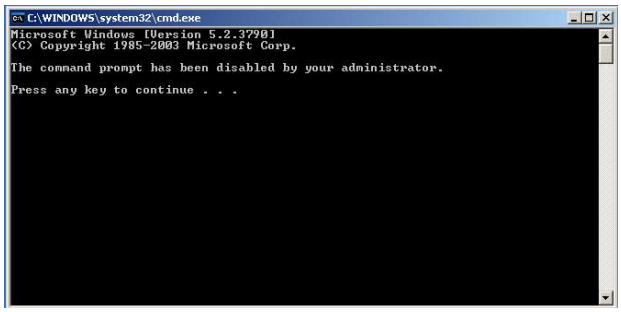



B12. Vào Start/Run gõ gpupdate /force để cập nhật các Policies.

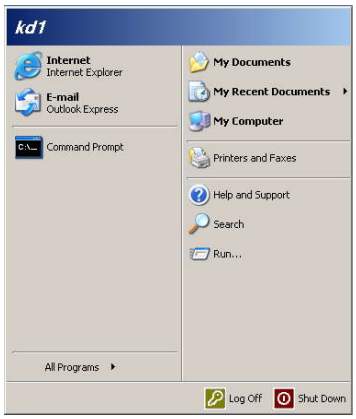



B13.Kiểm tra: đăng nhập bằng account kd1 vào một máy tính nằm trong domain.


B14.Sử dụng command line sẽ bị cấm.




B15.Không sử dụng được Control Panel.




Bài tập:

1.Thực hiện lại những ví dụ đã được minh họa.

2.Thực hiện chức năng Triển khai phần mềm bằng Group Policy. (Software Deployment).