

Chapter 2.

Triển khai dịch vụ **Active Directory Domain**

NGUYỄN THÀNH THỦY

BM. Tin học quản lý

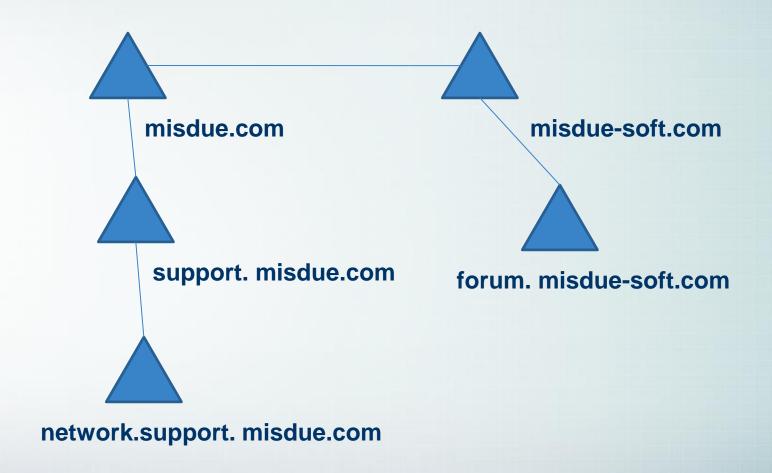
Trường Đại học Kinh tế, Đại học Đà Nẵng

Email: thuynt@due.edu.vn

2.1. Giới thiệu về dịch vụ Active Directory

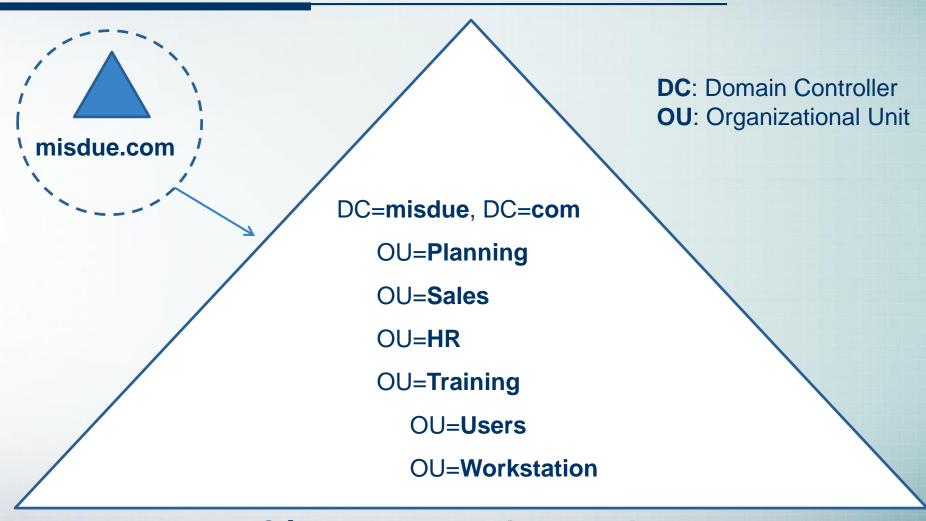
- Active Directory (AD) còn gọi là dịch vụ thư mục (directory service)
- Là nơi lưu trữ thông tin về các đối tượng như: users, groups, computers, ... trong hệ thống mạng.
- AD được tổ chức theo cấu trúc phân cấp, gồm:
 - AD forest: được tạo ra từ một nhóm gồm 2 hay nhiều domain tree có quan hệ tin cậy với nhau.
 - Các domain tree
 - Các Organizational Unit (OU)

2.1. Giới thiệu về dịch vụ Active Directory



Một Active Directory forest

2.1. Giới thiệu về dịch vụ Active Directory



Các OU trong một Domain

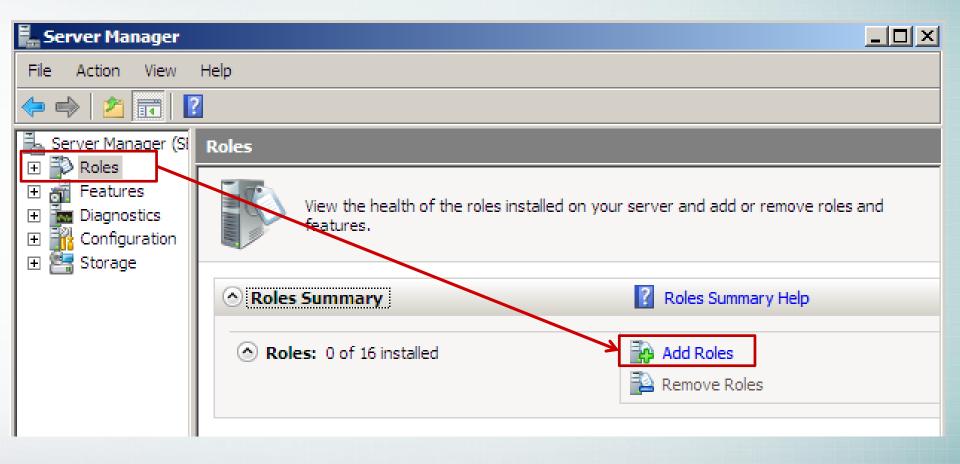
2.2. Cài đặt AD

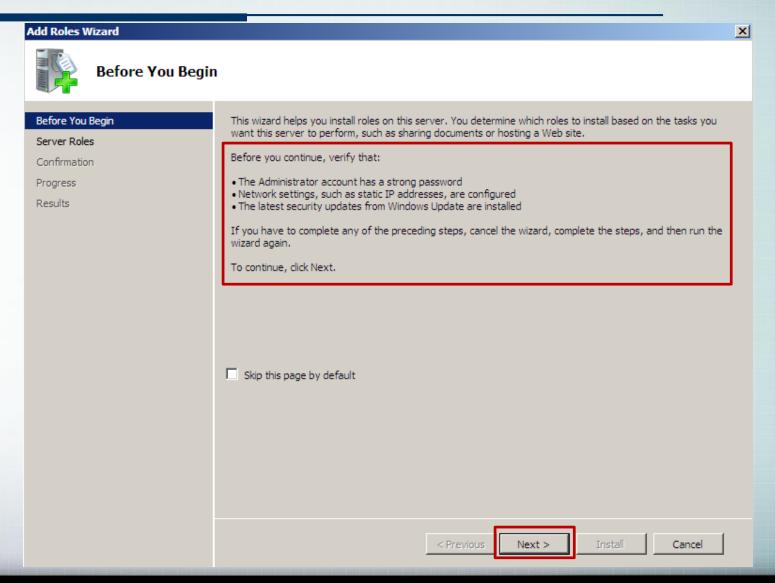
Yêu cầu trước khi cài đặt:

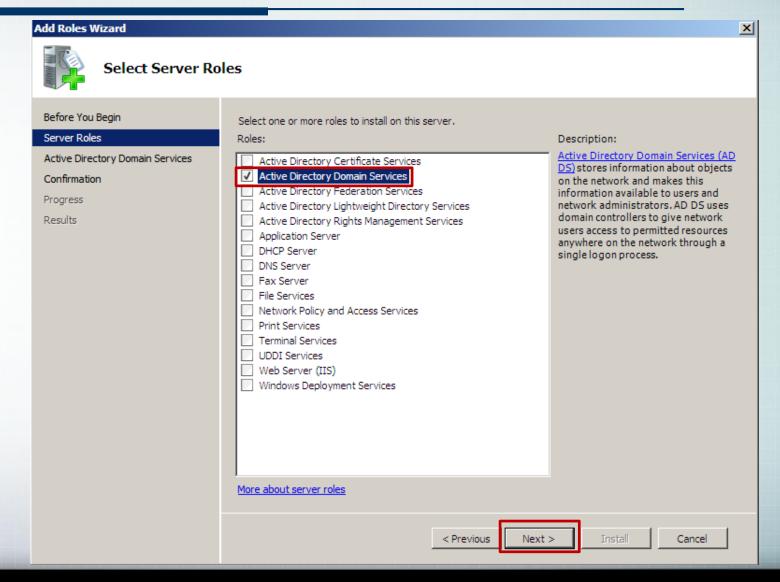
- Thiết lập địa chỉ IP cho card mạng của server
- Thiết lập tên (PC Name) cho server

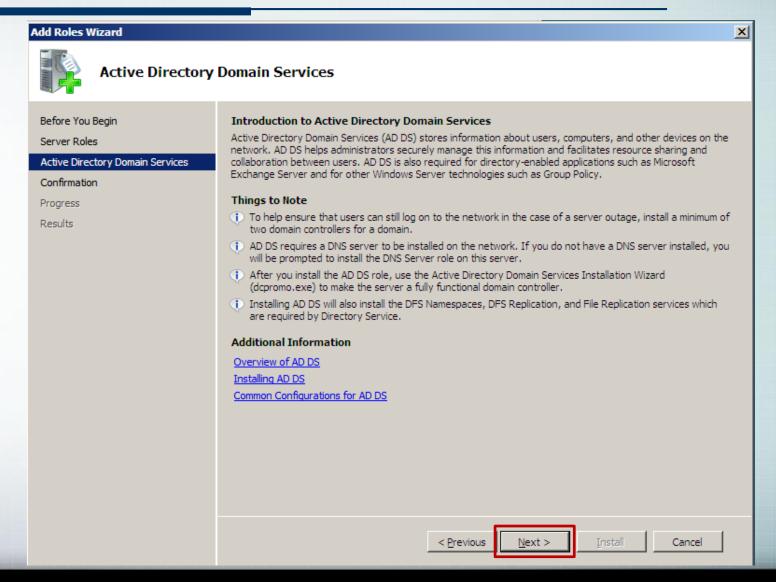
Các bước cài đặt:

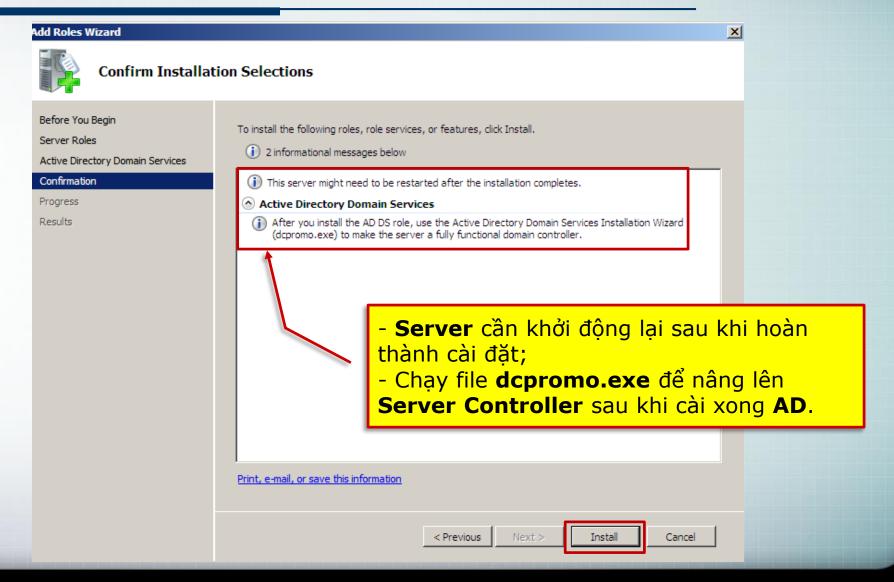
 Vào Server Manager → Trong Roles Summary chọn Add Roles.

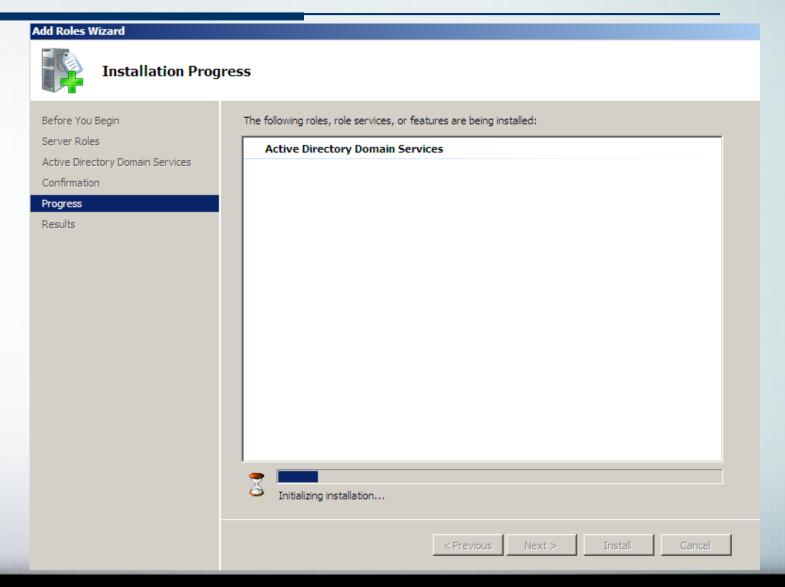


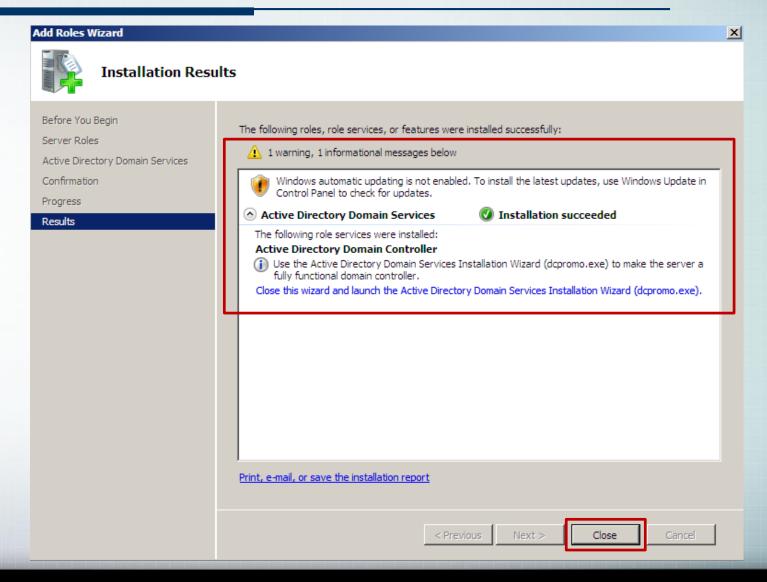


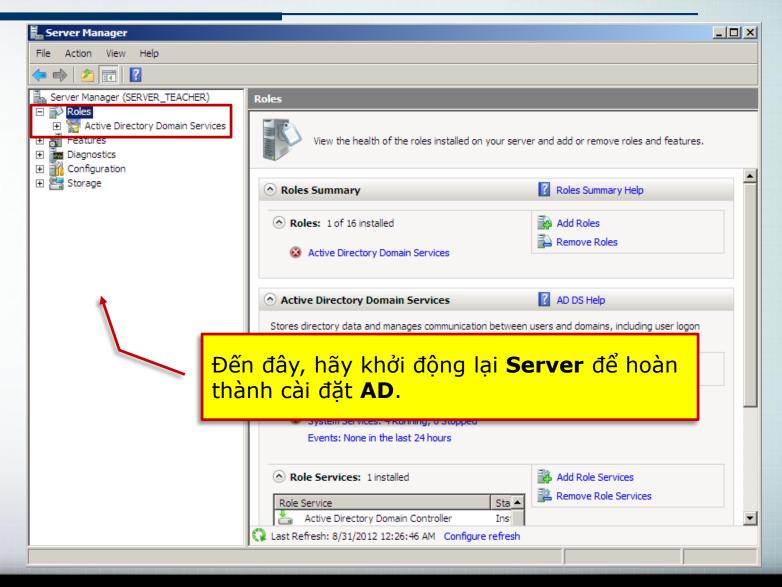


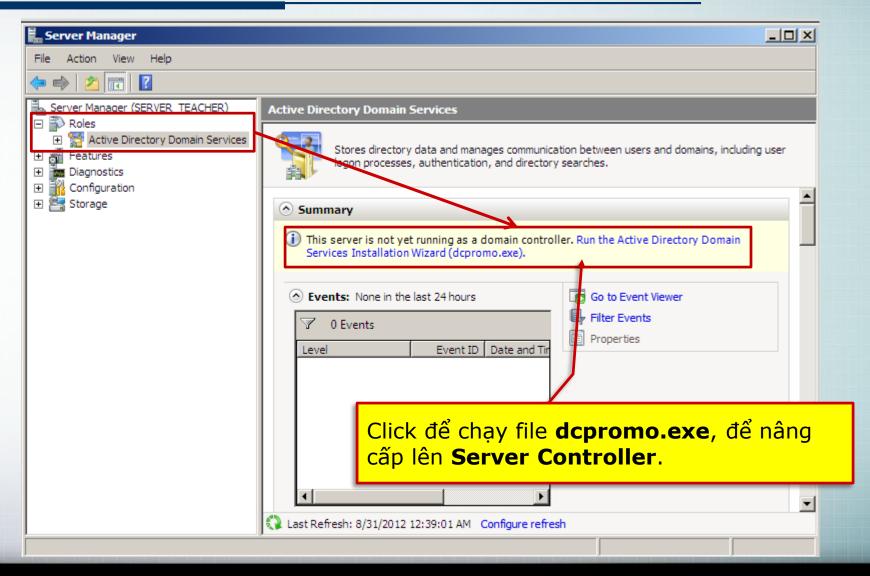




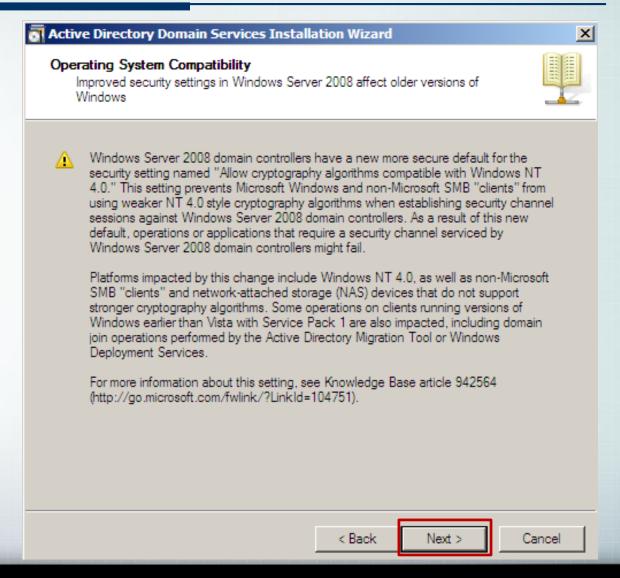


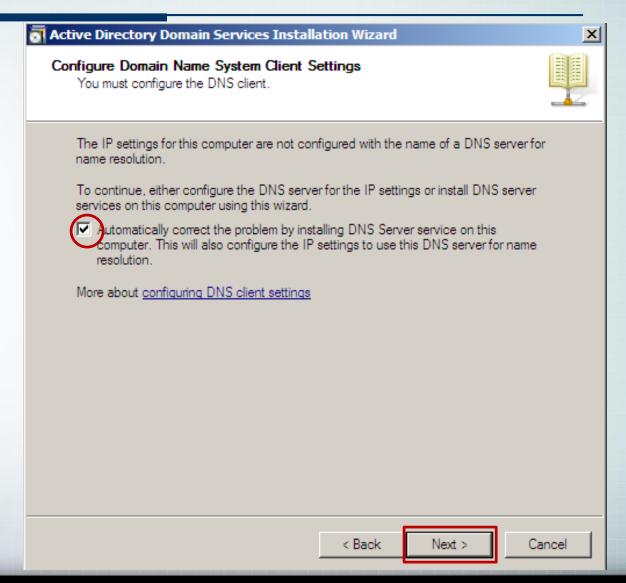


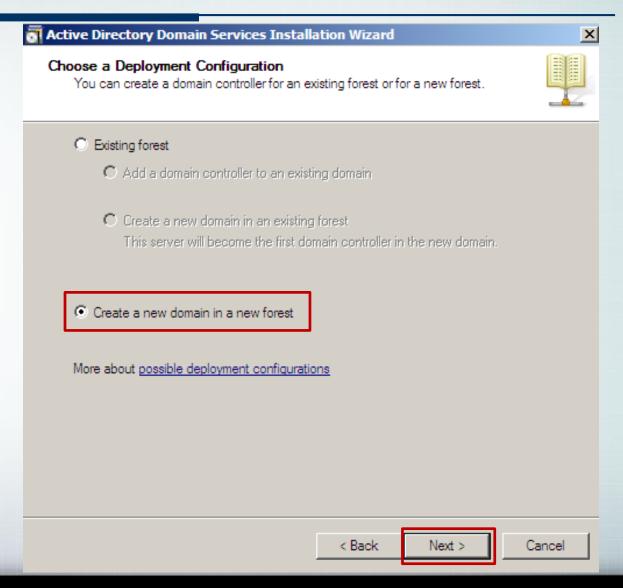


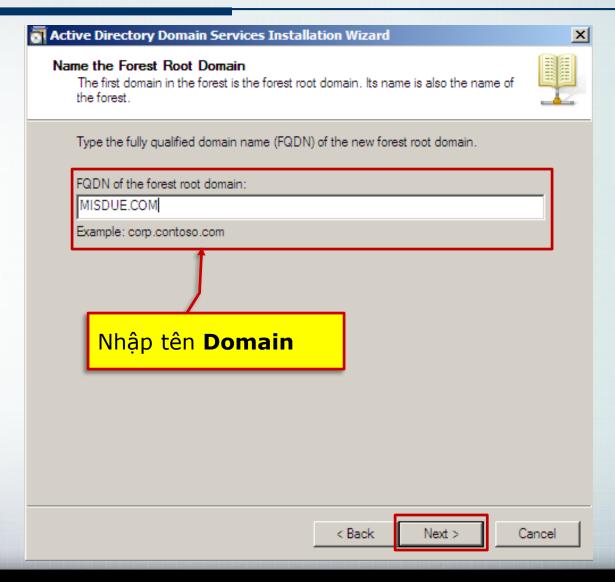


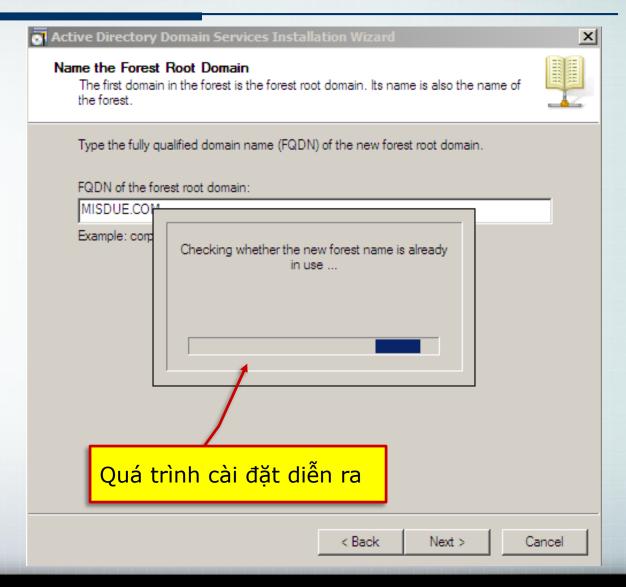


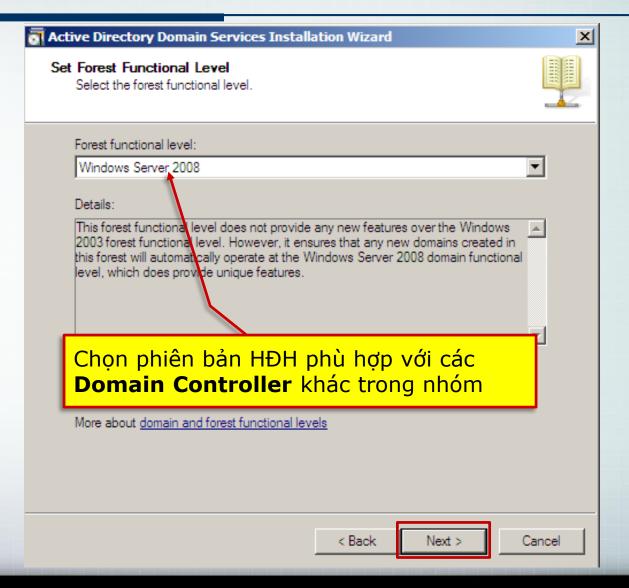


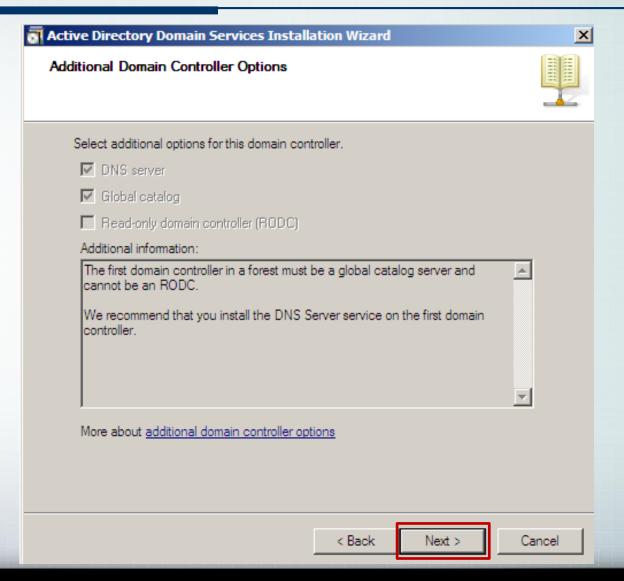


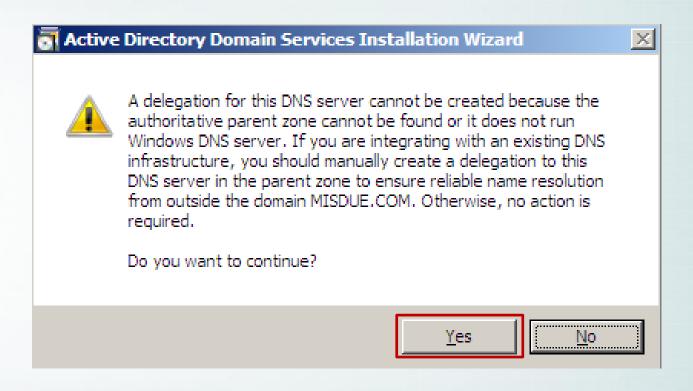


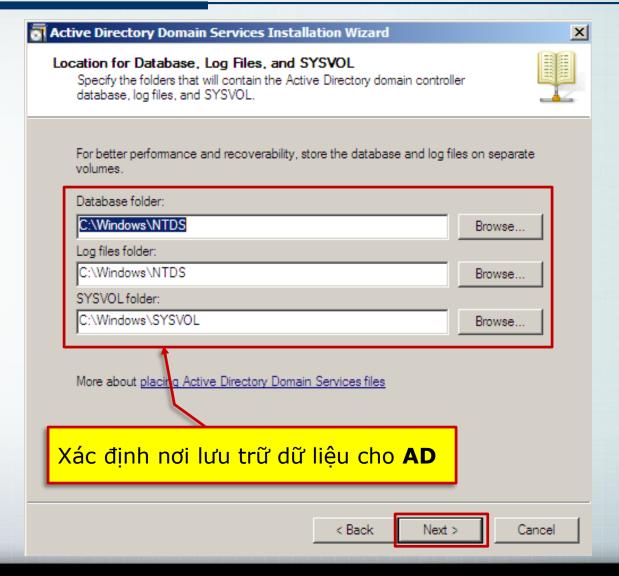


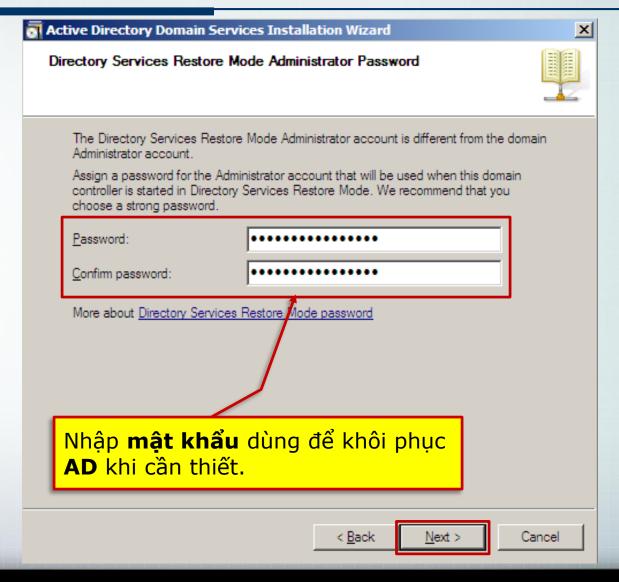


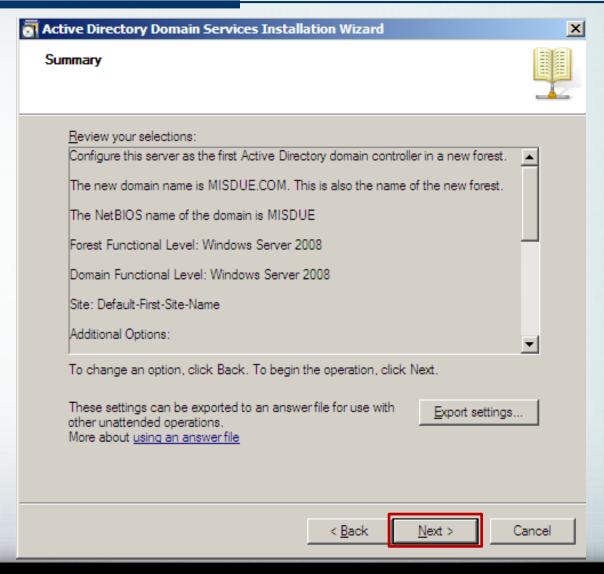


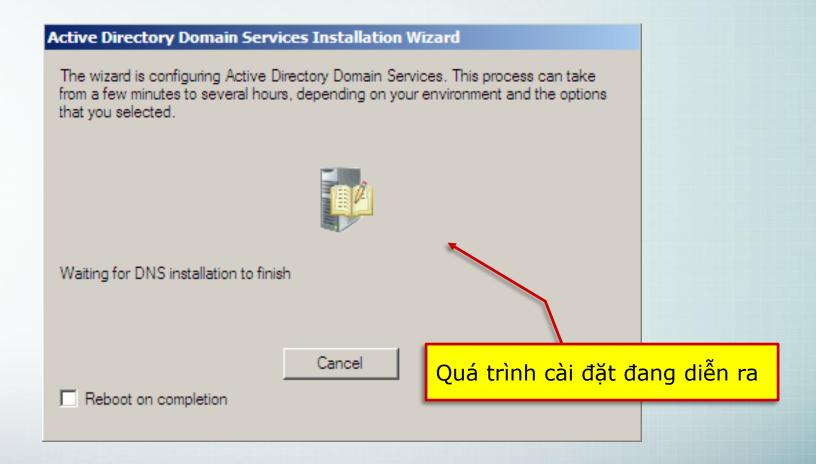


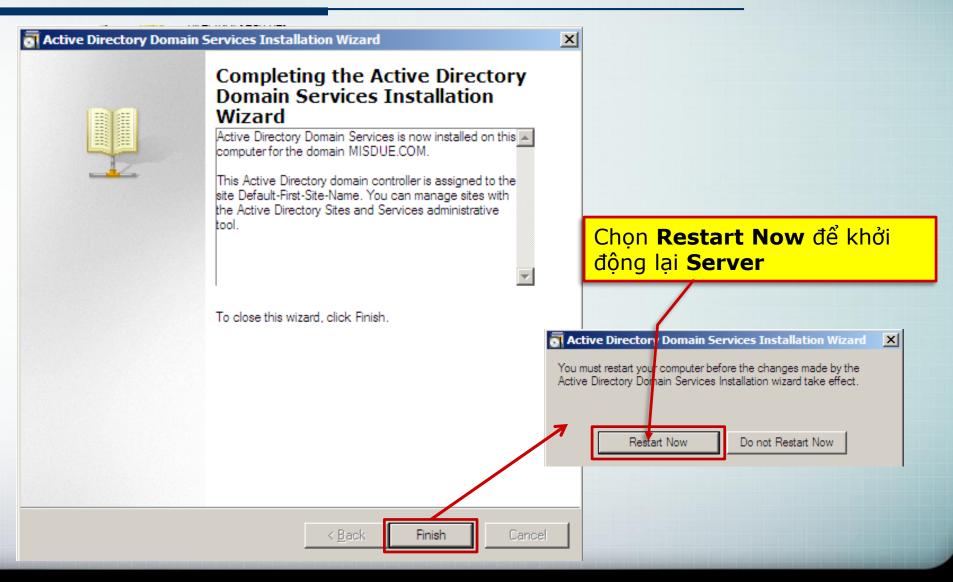


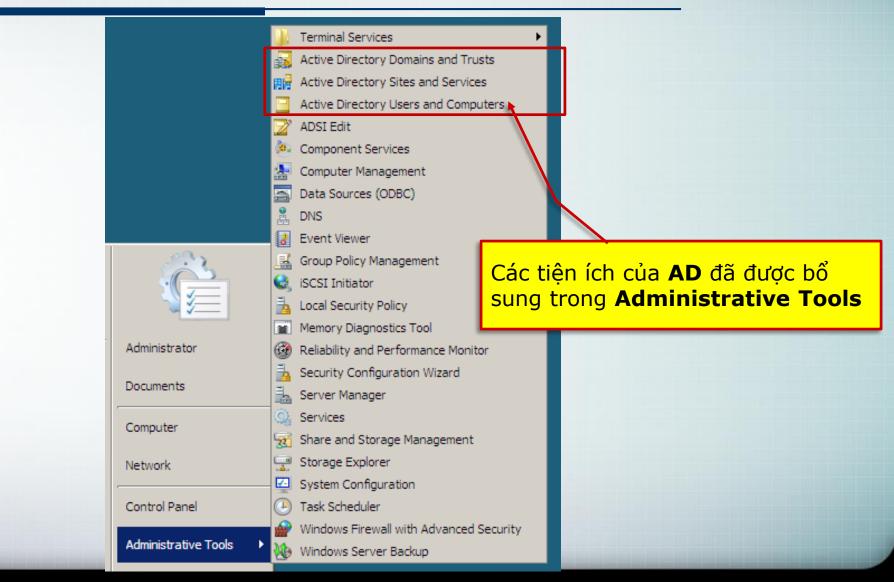












2.3 Quản lý User, Group, Computer và OU

*2.3.1 Quản lý User

- Mục đích: Cho phép quản trị tài khoản người dùng trong mạng.
- Thực hiện:
 - Trong cửa sổ Server Manager → Mục Roles → Active Directory Domain Services → Active Directory Users and Computers → Chọn Domain → User
 - Hoặc vào Start → Programs → Administrative
 Tools → Active Directory Users and Computers

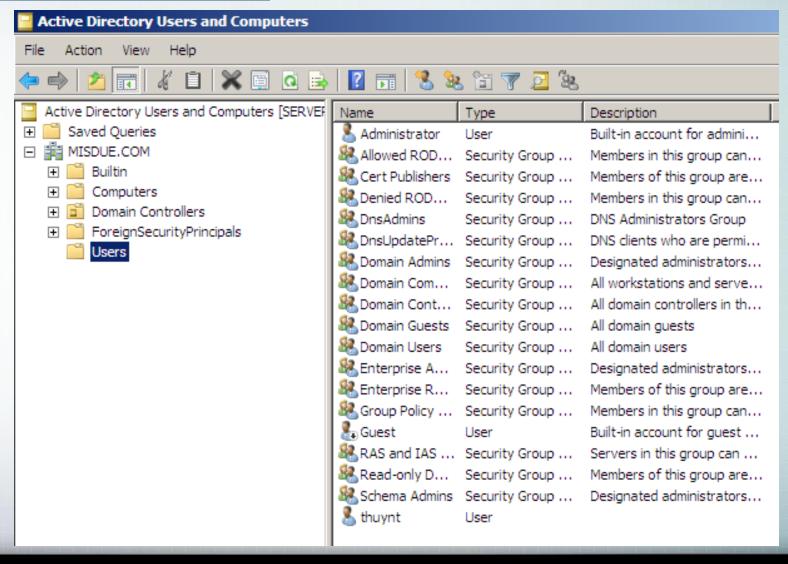
2.3.1 Quản lý User

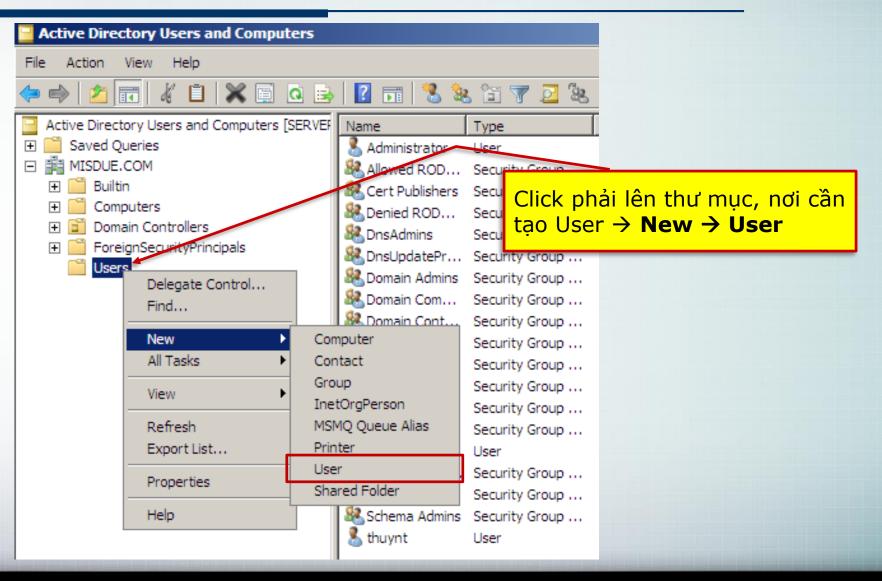
Các hoạt động cơ bản khi quản trị User

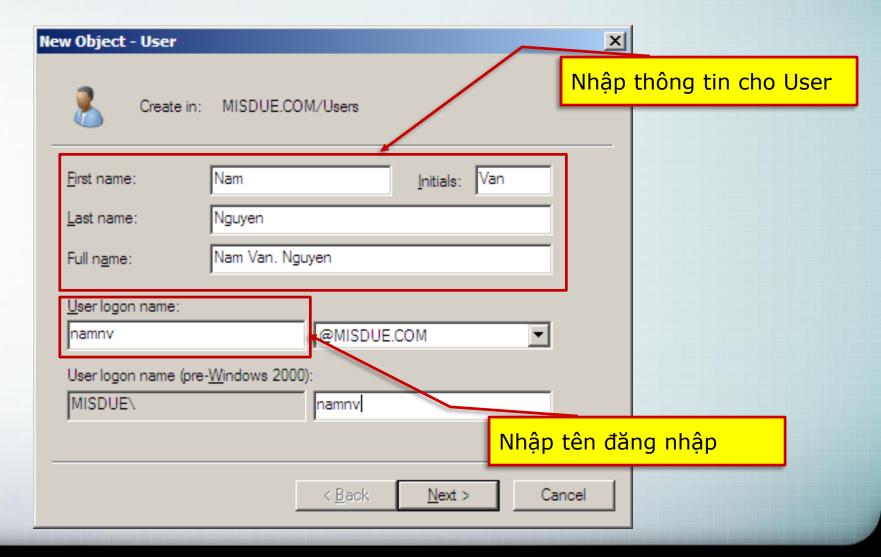
- Tạo mới tài khoản
- Cấu hình thuộc tính cho tài khoản
 - Quy định chế độ đổi mật khẩu
 - Hạn sử dụng của tài khoản
 - Chỉ định thời gian cho phép đăng nhập mạng của tài khoản
 - Chỉ định máy tính mà tài khoản được phép đăng nhập

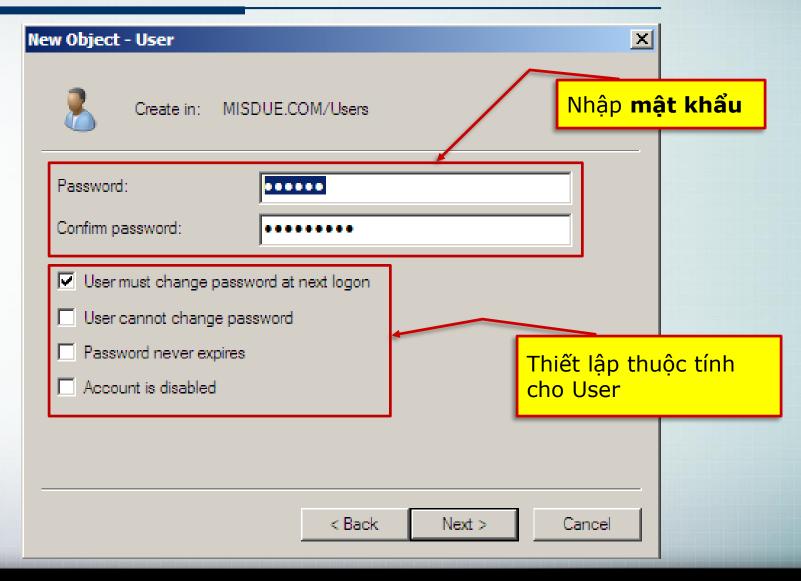
– ...

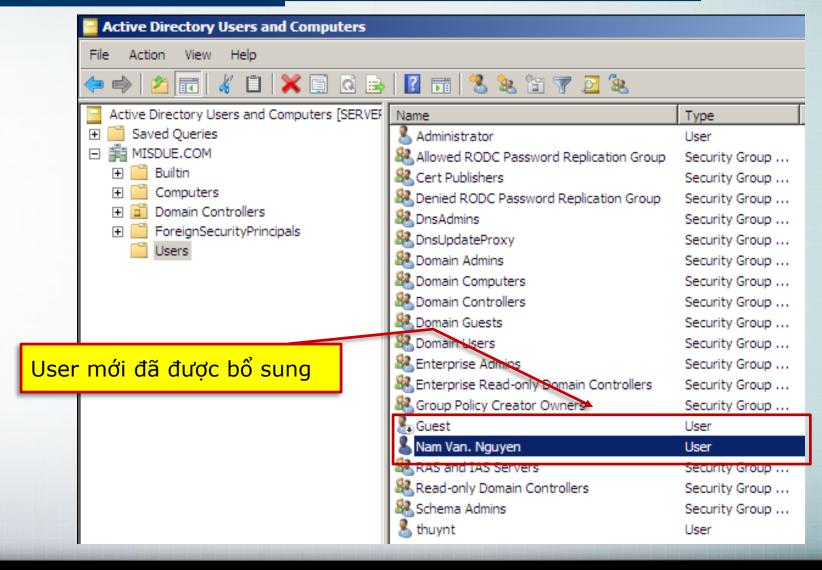
2.3.1 Quản lý User

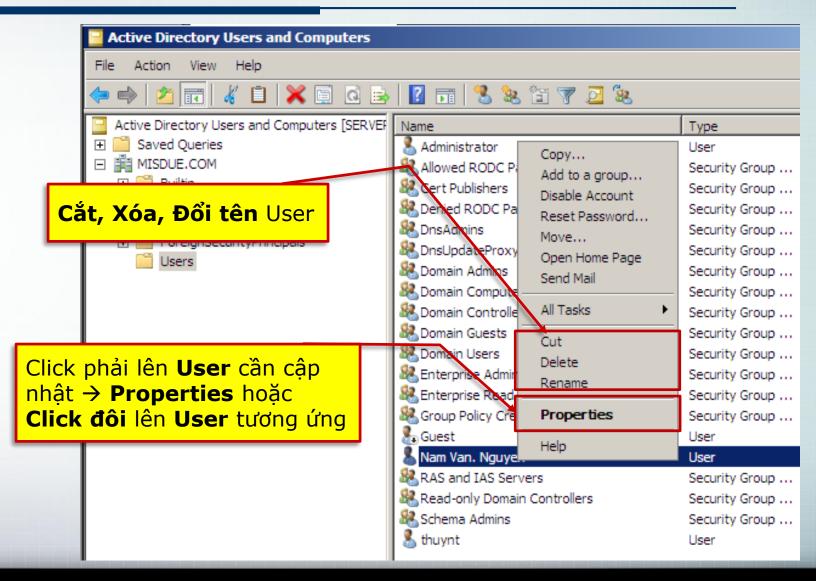


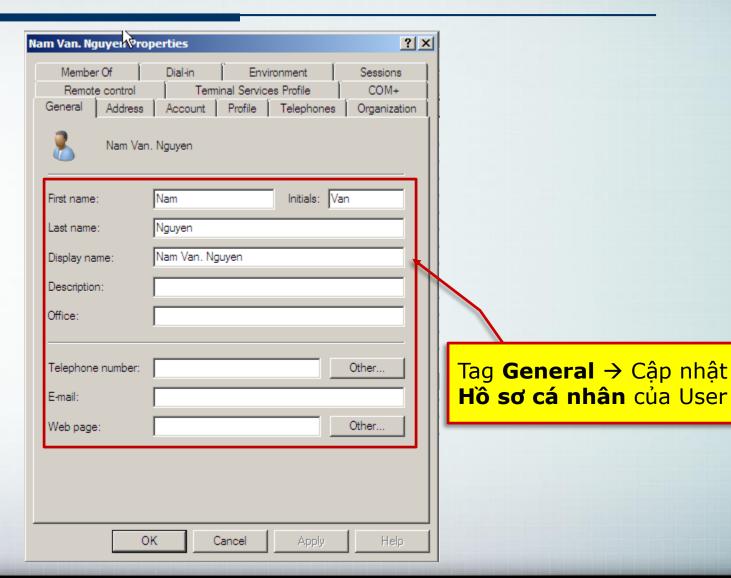


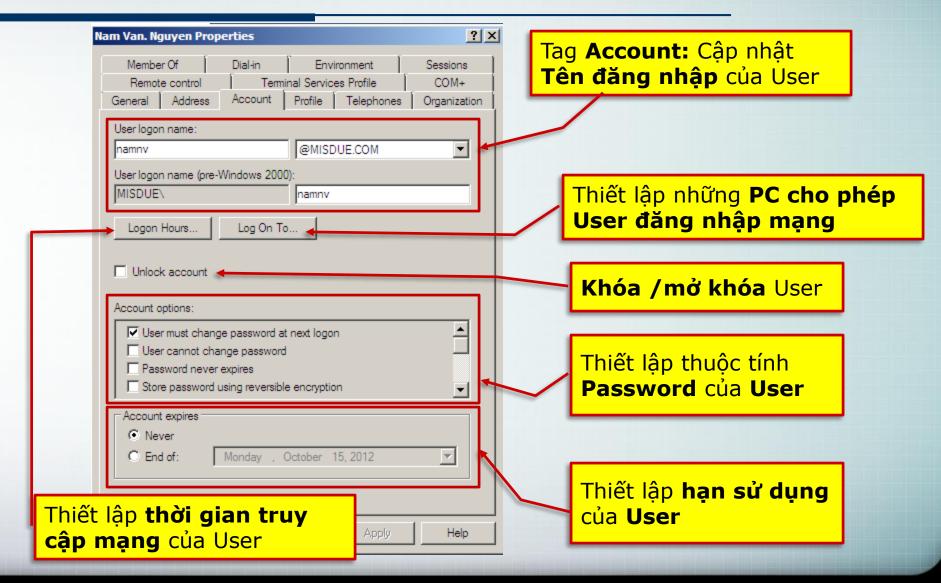


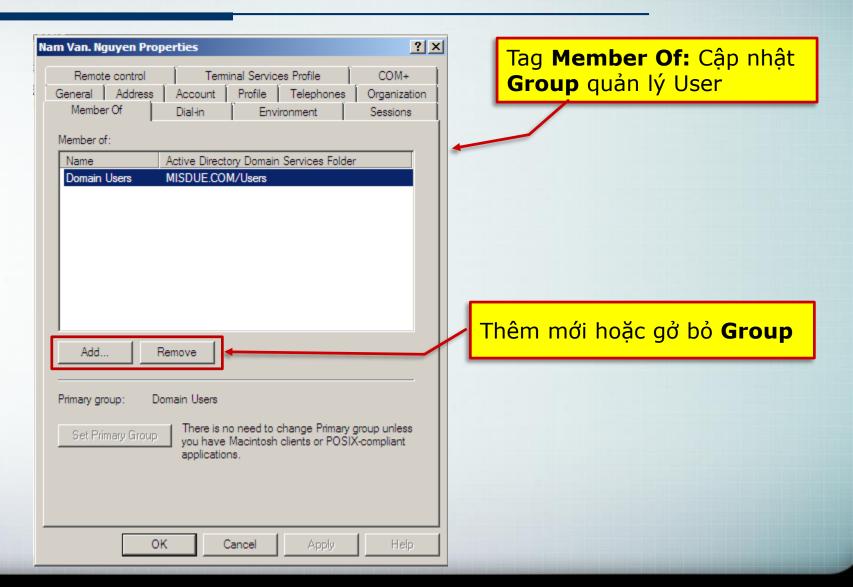










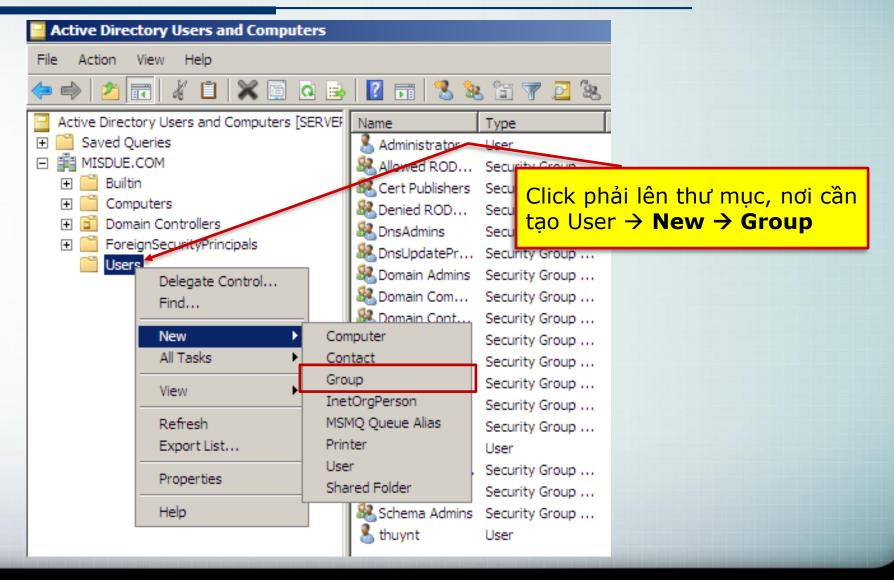


2.3 Quản lý User, Group, Computer và OU

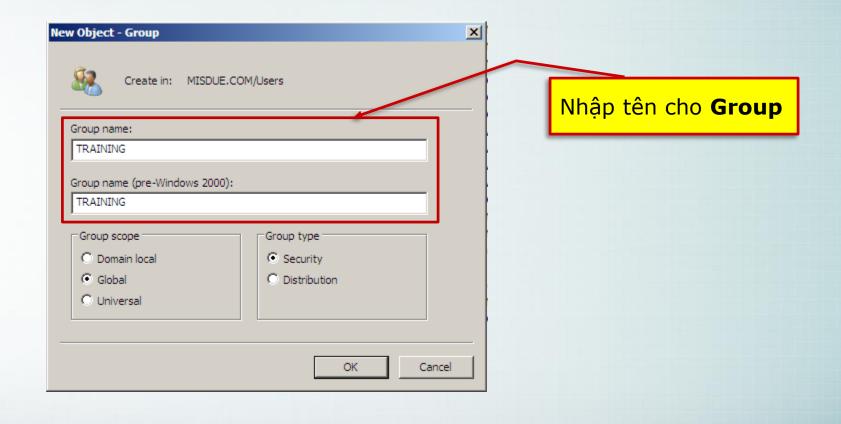
* 2.3.2 Quản lý Group

- Mục đích: Cho phép quản trị nhóm người dùng trong mạng.
- Thực hiện:
 - Tạo mới group
 - Cập nhật thông tin group
 - Xóa nhóm group

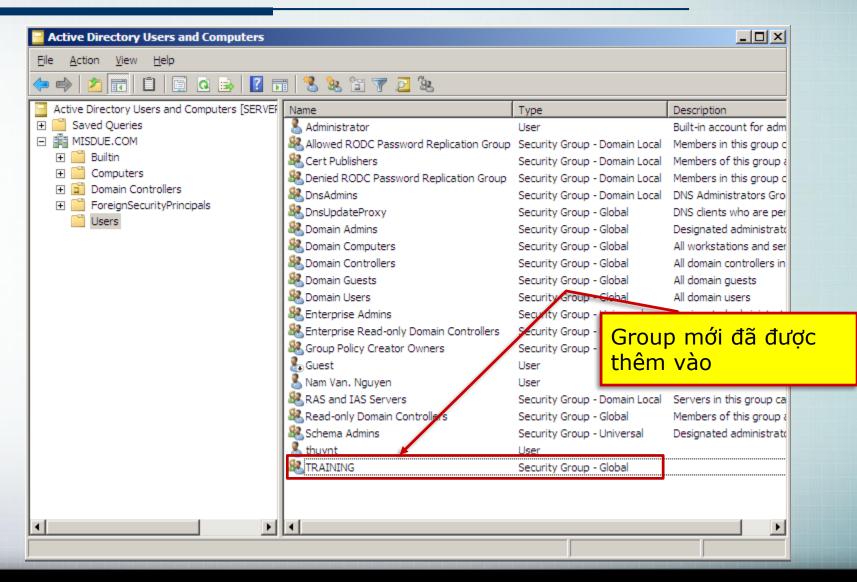
a. Tạo mới Group



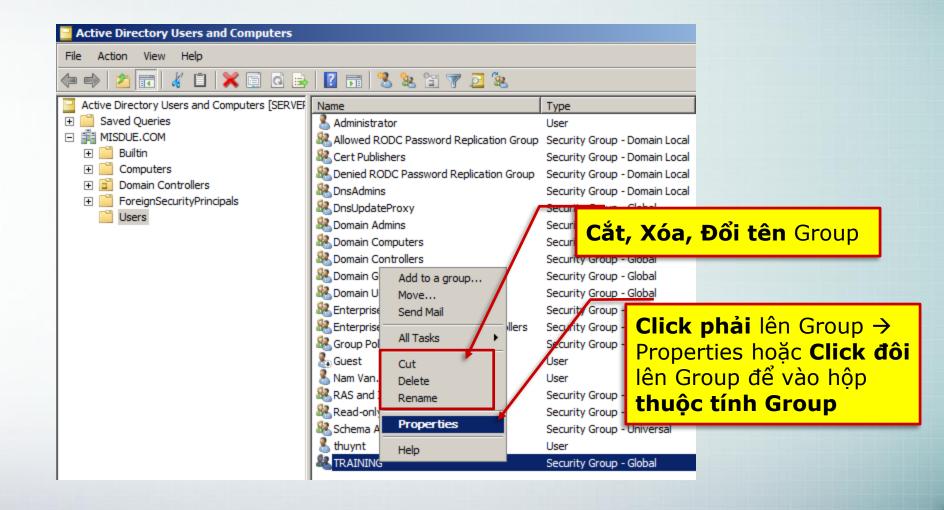
a. Tạo mới Group



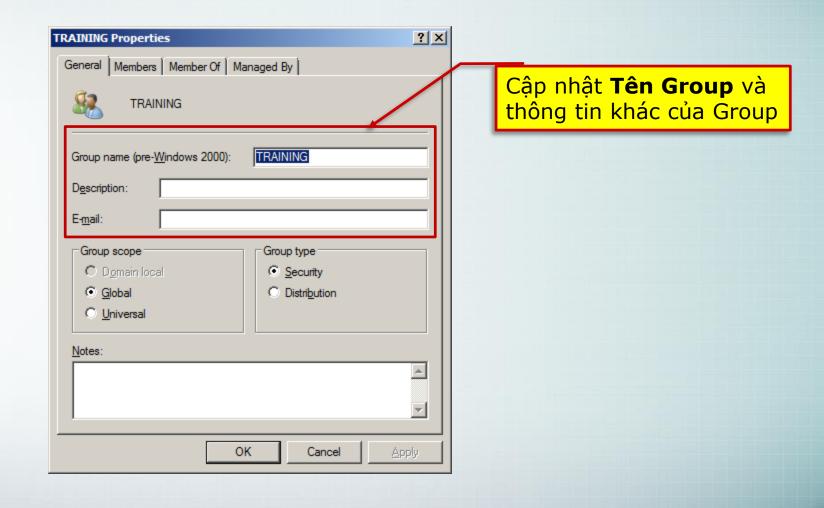
a. Tạo mới Group



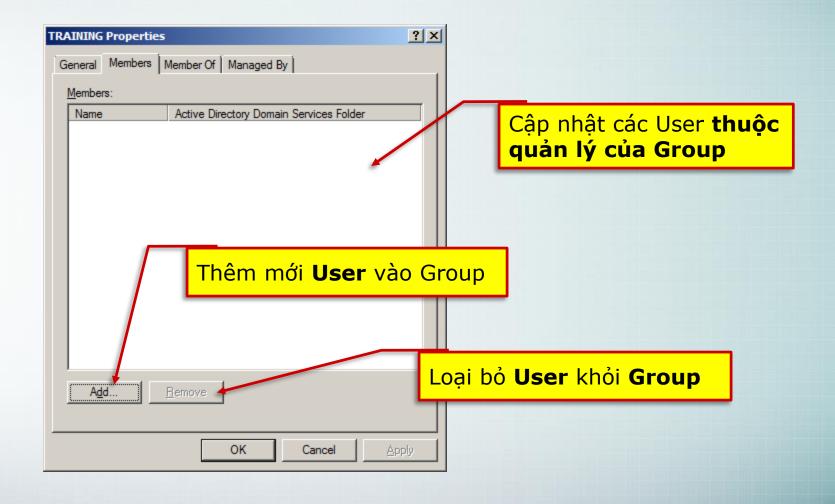
a. Cập nhật thuộc tính của Group



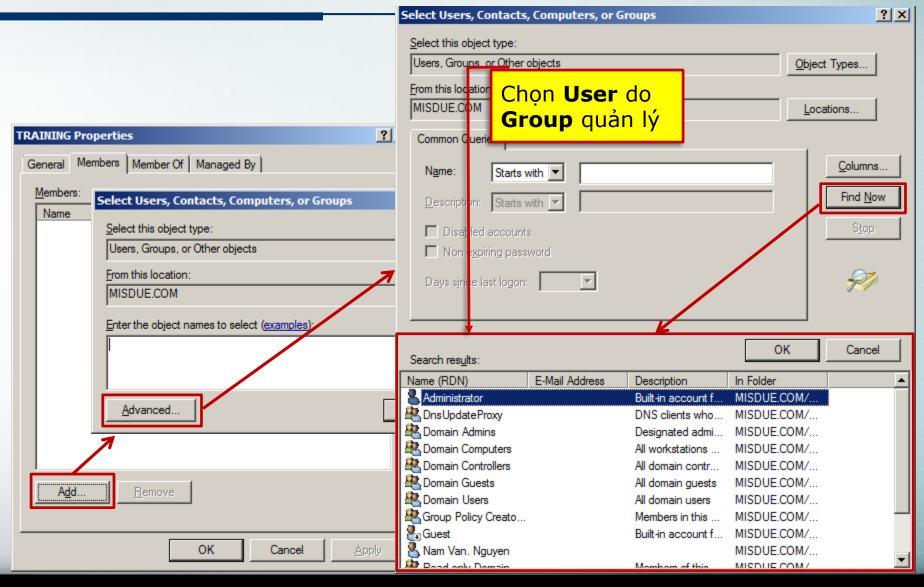
a. Cập nhật thuộc tính của Group → General



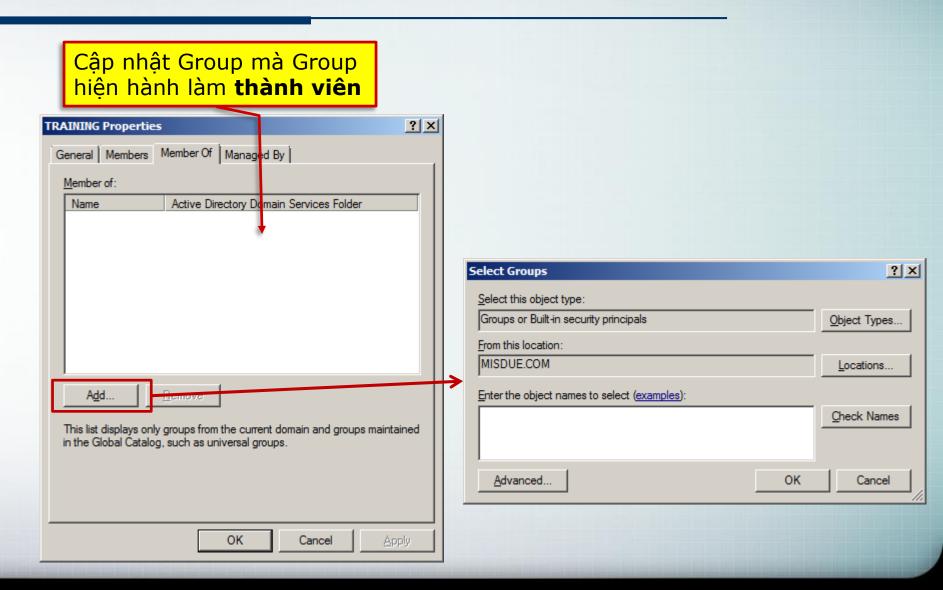
a. Cập nhật thuộc tính của Group → Members



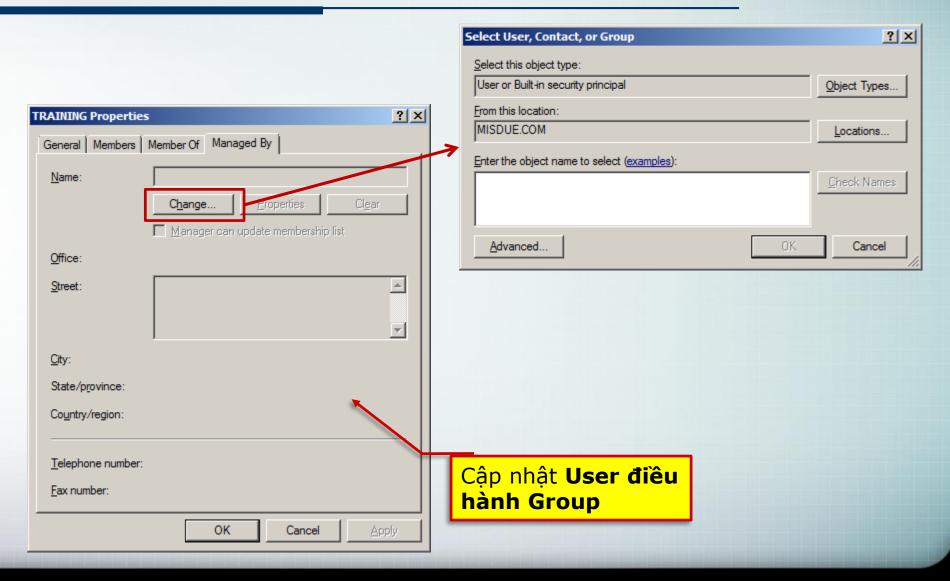
a. Cập nhật thuộc tính của Group → Members



a. Cập nhật thuộc tính của Group → Member Of



a. Cập nhật thuộc tính của Group → Managed By

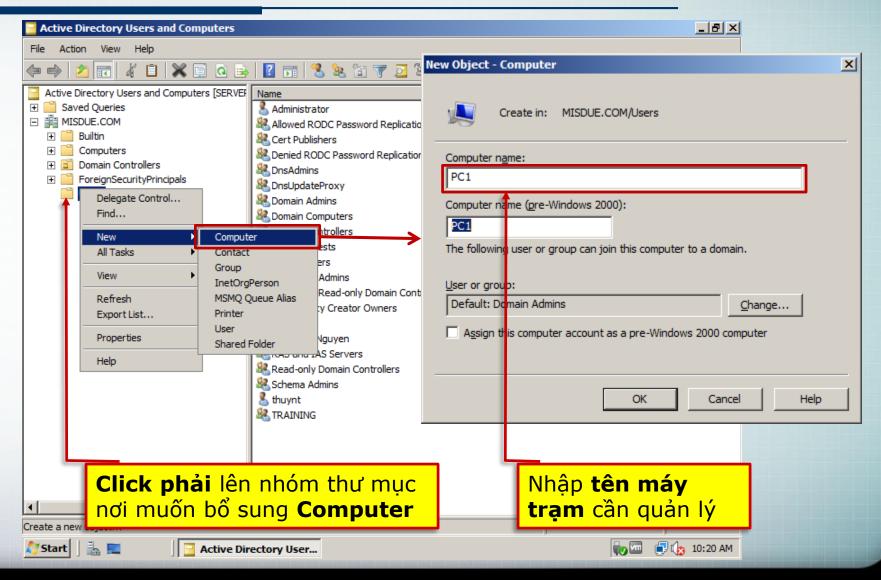


2.3 Quản lý User, Group, Computer và OU

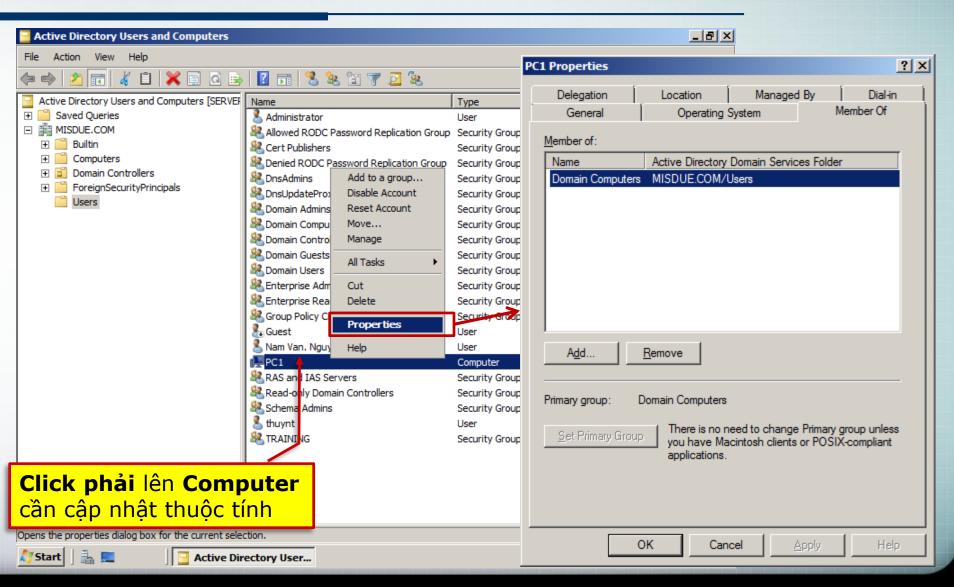
2.3.3 Quản lý Computer

- Mục đích: thực hiện quản trị các Computer (máy trạm) làm việc trong nhóm tổ chức.
- Các hoạt động cơ bản trong quản lý Computer:
 - Tạo mới, xóa computer.
 - Quản trị: nhóm làm việc, cấu hình hệ thống máy trạm từ xa,...

a. Thêm mới Computer



b. Cập nhật thuộc tính cho Computer

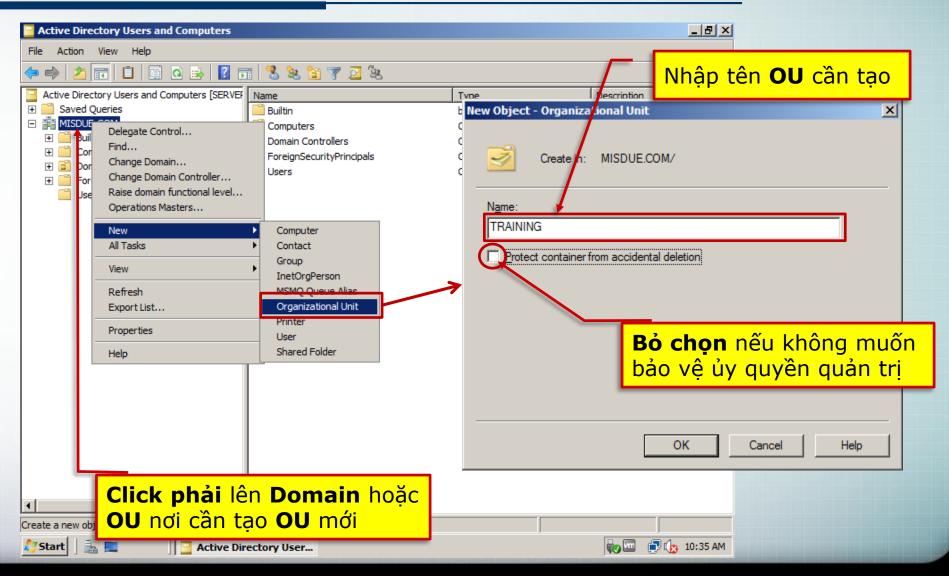


2.3 Quản lý User, Group, Computer và OU

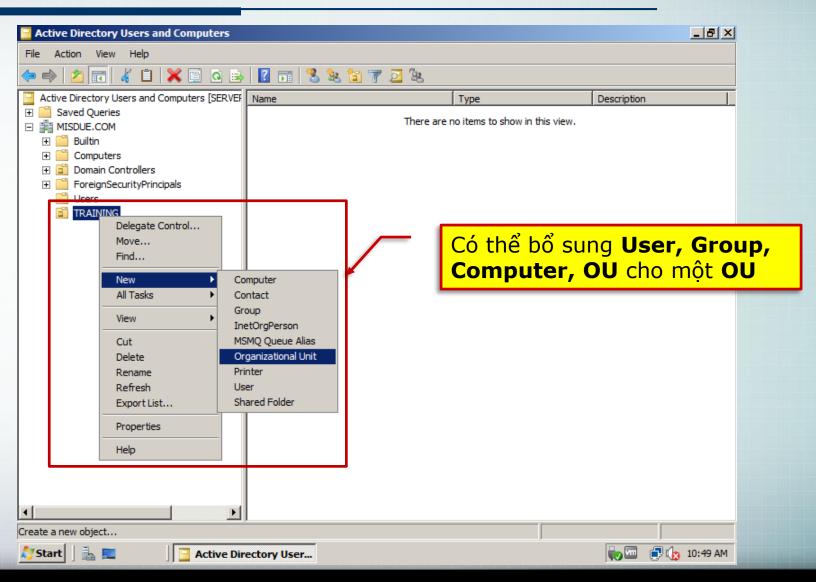
2.3.4 Quản lý OU (Organization Unit)

- Muc đích:
 - Cho phép quản trị các OU (nhóm tổ chức) trong mạng.
 - Trong một OU có thể bao gồm nhiều OU con, các Computer, User và Group.
- Các hoạt động cơ bản trong quản lý OU
 - Tạo mới, xóa OU
 - Quản trị: tạo mới các OU con, bổ sung các Computer, Group và User thuộc tổ chức.

a. Tạo mới OU



b. Cập nhật, bổ sung User, Group, Computer, OU cho OU



56

2.4 Kết nối máy trạm vào Domain

Muc đích

Kết nối các máy trạm trên mạng vào Domain (Join Domain), giúp Domain có thể nhận diện và kiểm soát các máy trạm khi vào mạng.

Các bước thực hiện:

- Tại Server: tạo User, tạo Group, tạo Computer
- Tại Client: Cấu hình mạng, tiến hành đăng nhập vào Domain từ máy trạm

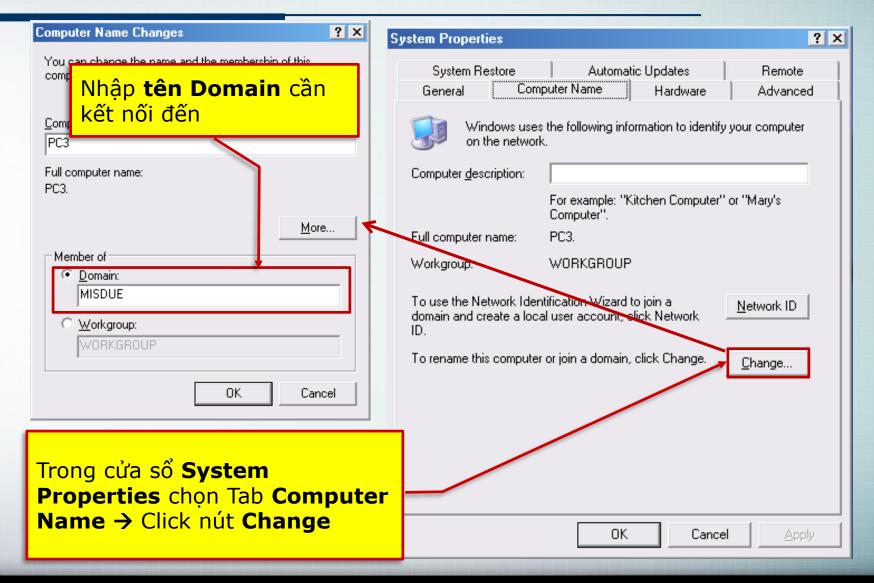
(Hướng dẫn cài đặt kết nối mạng giữa các máy ảo)

a. Cấu hình mạng ở máy trạm

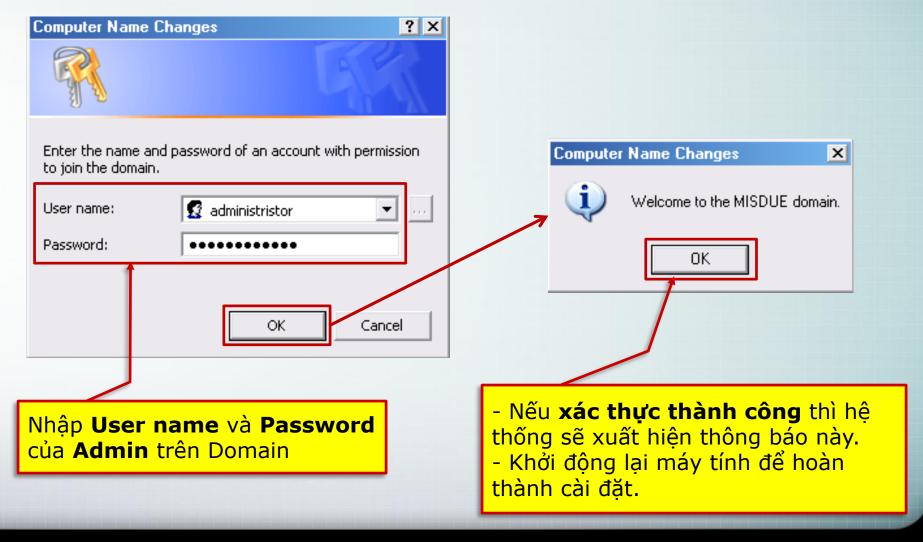


- Login vào máy trạm với quyền
 Administrator
- Click phải lên biểu tượng My Computer trên Desktop → Properties

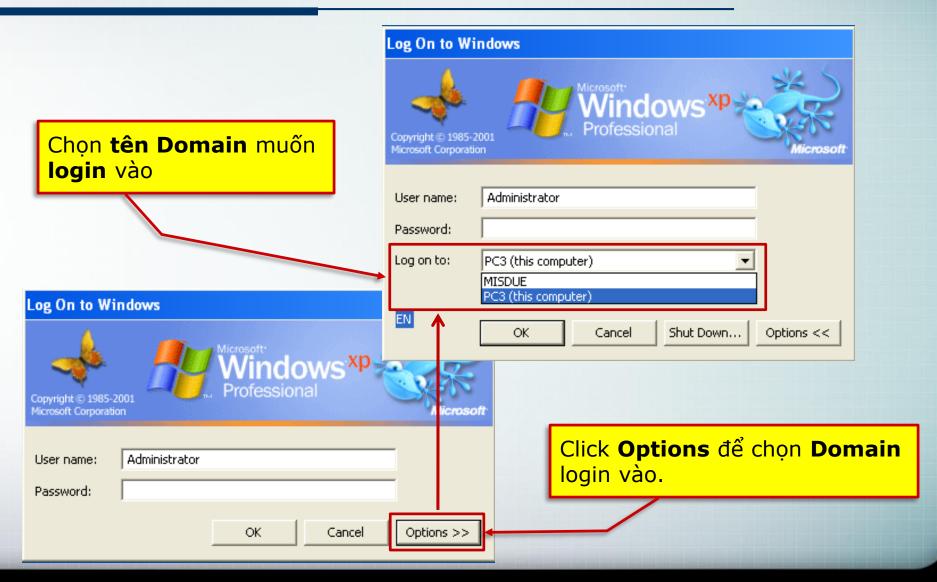
a. Cấu hình mạng ở máy trạm



a. Cấu hình mạng ở máy trạm



b. Login vào Domain



Share và phân quyền truy cập tài nguyên

Muc đích:

- Nhằm share một thư mục/ổ đĩa logic/thiết bị phần cứng (gọi chung là tài nguyên) trên Server hoặc từ các Client, để các user có thể khai thác trực tuyến từ Client;
- Để đảm bảo yếu tố bảo mật, người quản trị mạng có thể thực hiện thiết lập quyền/mức độ khai thác tài nguyên (gọi chung là **phân quyền**) cho từng đối tượng cu thể đối với tài nguyên đó

Share và phân quyền truy cập tài nguyên

Phương pháp

 Các quyền (mức độ) user được phép khai thác tài nguyên:

Quyền	Mô tả
Full control	Toàn quyền (đọc, sửa, xóa,)
Read	Chỉ đọc
Change	Được thay đổi (sửa, xóa)
Modify	Được thay đổi (sửa, xóa)
Read & Execute	Đọc và thực thi
List folder contents	Hiển thị danh sách các thư mục/tập tin
Write	Được sửa
Special permissions	Các quyền theo giới hạn cụ thể nào đó

Share và phân quyền truy cập tài nguyên

* Thực hành:

- Share và bỏ share thư mục
- Phân quyền (nâng cao) truy cập tài nguyên

64

Muc đích:

- MAP (ánh xạ) nhằm tạo shortcut đường dẫn truy cập của thư mục đã được share trên server xuống máy trạm.
- Đường dẫn sẽ hiển thị như một ổ đĩa logic trên máy trạm, nhưng dữ liệu thực tế được lưu trên server.



Phương pháp:

- MAP tự động
 - Trên Server, sử dụng AD để cấu hình cho 1 hoặc nhiều user
 - Khi user login vào mạng từ Client (bất kỳ client nào), hệ thống sẽ tự động MAP thư mục xuống máy trạm đó → ổ đĩa mạng

MAP thủ công

- Trên 1 Client cụ thể, thực hiện MAP thư mục đã chia sẻ trên Server → ổ đĩa mạng
- Ở đĩa mạng chỉ MAP xuống Client đã cấu hình, không tự MAP khi user login ở Client khác

* Thực hành:

- MAP ổ đĩa mạng tự động và bỏ MAP (video)
- MAP ổ đĩa mạng thủ công và bỏ MAP (video)

BÀI TẬP KẾT THÚC CHƯƠNG

LAB 2.1. Thông mạng Client và Server

- Cài đặt Client Server thông mạng với nhau
- Kiểm tra thông mạng Client Server

LAB 2.2. Kết nối Client vào Server

- Cài đặt Join domain
- Đăng nhập domain từ client

BÀI TẬP KẾT THÚC CHƯƠNG

LAB 2.3. Phân quyền khai thác thư mục mạng

- Tạo tài khoản người dùng, nhóm người dùng, tổ chức thư mục, ... trên Server
- Phân quyền truy cập thư mục

LAB 2.4. MAP thư mục mạng

- MAP thủ công
- MAP tự động
- Login từ Client để kiểm tra lại kết quả

LAB 2.5. Cấp quota dung lượng ổ đĩa mạng cho user

- Mỗi User (trong bài LAB2.3) được cấp tối đa 1GB dữ liệu trên thư mục cá nhân.

BÀI TẬP NÂNG CAO

- 1. Tạo Roaming Profiles cho tài khoản người dùng. (tên tài khoản: STT1_STT2)
- 2. Add nhiều User tự động bằng script
- 3. Map ổ đĩa mạng tự động bằng script cho nhiều User
- 4. Phân quyền khai thác thư mục cho nhiều User

BÀI TẬP NÂNG CAO

Cách để kiểm tra kết quả Tạo Roaming Profile cho tài khoản người dùng:

- Tạo 1 tài khoản người dùng (vd: namnv)
- Cấu hình Profiles cho tài khoản namnv trên Server 2008
- Tạo 2 máy ảo Windows XP/7
- Kết nối 2 máy ảo vào Windows Server 2008
- Từ máy ảo PC1, login vào server với tài khoản namnv --> tạo thử 1 file đặt tên FileMau.txt trên desktop --> logoff
- Từ máy ảo PC2, login vào server với tài khoản namnv --> kiểm trên trên desktop ở PC2 có file FileMau.txt hay không?
- --> nếu có file này nghĩa là cấu hình Profiles thành công.