Chapter 6: Network Administration

ACTIVE DIRECTORY

Lecturer: Nguyễn Thị Thanh Vân – FIT - HCMUTE

Nội dung

I. Các mô hình mạng trong môi trường Microsoft.
II. Active Directory.
III. Cài đặt và cấu hình Active Directory

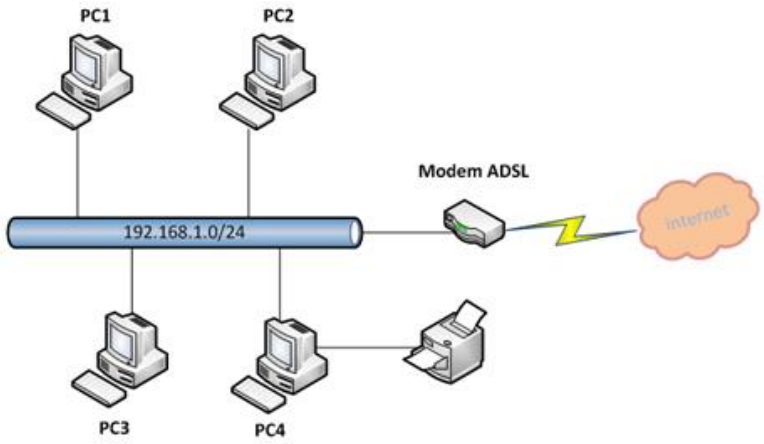
I. Các mô hình mạng trong môi trường Microsoft

1. Mô hình Workgroup
2. Mô hình Domain. ....

1. Mô hình Workgroup

- Còn gọi là mô hình mạng peer-to-peer,
- Đặc điểm:
  - Các máy tính có vai trò như nhau được nối kết với nhau.
  - Các dữ liệu và tài nguyên được lưu trữ phân tán tại các máy cục bộ,
  - Các máy tự quản lý tài nguyên cục bộ của mình.
  - Không có máy tính chuyên cung cấp dịch vụ và quản lý hệ thống mạng.
- Mô hình này chỉ phù hợp với các mạng nhỏ, dưới mười máy tính và yêu cầu bảo mật không cao.
- Thông tin người dùng trong một tập tin SAM (Security Accounts Manager) ngay chính trên máy tính cục bộ và được mã hóa
- Thông tin này bao gồm:
  - username ,
  - fullname,
  - password,
  - description…

1. Mô hình Workgroup

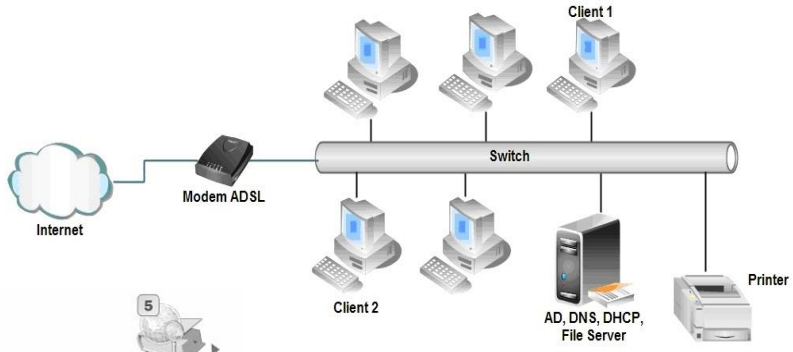


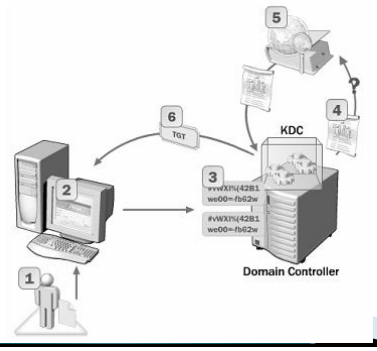
Hình 8: Mô hình Workgroup dùng để chia sẻ dữ liệu, máy in, truy cập Internet

2. Mô hình Domain

- Hoạt động theo cơ chế client-server,
- Có ít nhất một máy tính làm chức năng điều khiển vùng (Domain Controller): lưu trữ các thông tin người dùng tập trung (dịch vụ AD).
- Tệp lưu trữ là NTDS.DIT, có thể lưu trữ hàng triệu người dùng (tổ chức giống MS Access)
- Việc quản lý tài nguyên mạng được tập trung tại các Server trong miền.
- Mô hình này được áp dụng cho các công ty vừa và lớn.

2. Mô hình Domain





- Việc chứng thực người dùng đăng nhập vào mạng được tập trung và do máy điều khiển vùng chứng thực.

II. Active Directory

1. Directory Services.
   a. Giới thiệu Directory Services
   b. Các thành phần trong Directory Services
2. Giới thiệu Active Directory.
3. Chức năng của Active Directory.
4. Kiến trúc của Active Directory.
   a. Kiến trúc vật lý
   b. Kiến trúc logic.

1. Directory Services.

a. Giới thiệu Directory Services (dịch vụ danh bạ)

- Directory là một mô hình tổ chức thông tin, dữ liệu mà trong đó các thông tin dữ liệu có mối quan hệ chặt chẽ với nhau (danh sách các đối tượng và thuộc tính)
- Cung cấp một phương tiện hỗ trợ việc lưu trữ các thông tin, dữ liệu theo kiến trúc tổ chức Directory và quản lí tập trung các đối tượng, đơn giản hóa việc truy xuất Resource.
- Là một dịch vụ hoạt động như một tổng đài (switchboard) chính trong các OS máy chủ, nó hỗ trợ các nguồn Resources độc lập và phân tán có thể làm việc với nhau, có thể kết nối với nhau
- Là một dịch vụ cơ sở làm nền tảng để hình thành một hệ thống Active Directory.
- được chứa trong NTDS.DIT và các chương trình quản lý, khai thác tập tin này.

1. Directory Services.

b. Các thành phần trong Directory Services

- Object (đối tượng).
- Attribute (thuộc tính).
- Schema (cấu trúc tổ chức).
- Container (vật chứa).
- Global Catalog.

Object, Attribute

b. Các thành phần trong Directory Services

❖ Object (đối tượng).

- Bao gồm các máy in, người dùng mạng, các server, các máy trạm, các thư mục dùng chung, dịch vụ mạng, …
- Đối tượng chính là thành tố căn bản nhất của dịch vụ danh bạ.

❖ Attribute (thuộc tính).

- Một thuộc tính mô tả một đối tượng.
- Các đối tượng khác nhau có danh sách thuộc tính khác nhau, tuy nhiên, các đối tượng khác nhau cũng có thể có một số thuộc tính giống nhau.

  Ví dụ như một máy in và một máy trạm cả hai đều có một thuộc tính là địa chỉ IP.

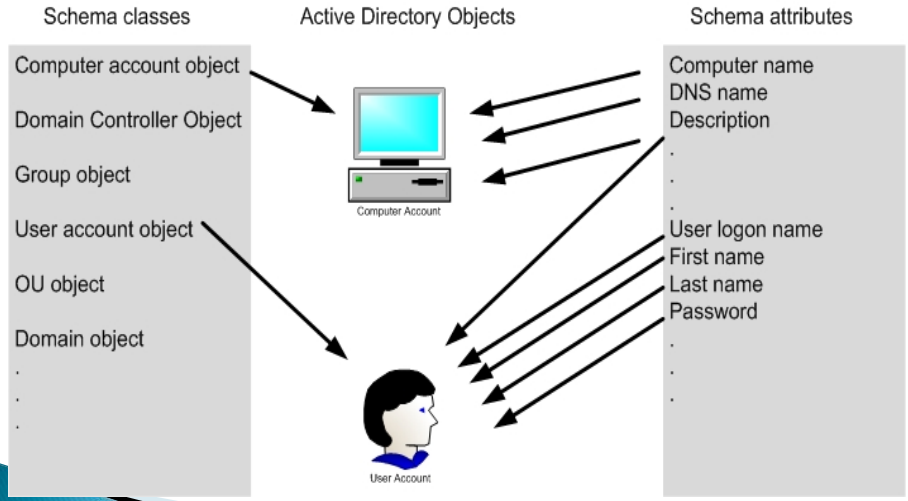
Schema

b. Các thành phần trong Directory Services

❖ Schema (cấu trúc tổ chức).

- Một schema định nghĩa danh sách các thuộc tính dùng để mô tả một loại đối tượng nào đó.
- Schema classes: định nghĩa các kiểu đối tượng được lưu trữ trong AD
- Schema attributes: định nghĩa các thông tin về kiểu của từng đối tượng trong AD
- Schema có đặc tính là tuỳ biến được - các thuộc tính dùng để định nghĩa một lớp đối tượng có thể sửa đổi được.
- Schema có thể xem là một danh bạ của cái danh bạ AD

Schema



Container

b. Các thành phần trong Directory Services

- Container (vật chứa).

- Một vật chứa có thể chứa các đối tượng và các vật chứa khác. (khái niệm thư mục trong Window)
- Vật chứa cũng có các thuộc tính như đối tượng mặc dù vật chứa không thể hiện một thực thể thật sự nào đó như đối tượng.
- Có ba loại vật chứa là:
  - Domain: khái niệm này được trình bày chi tiết ở phần sau.
  - Site: một site là một vị trí. Site được dùng để phân biệt giữa các vị trí cục bộ và các vị trí xa xôi.
    - Ví dụ: các chi nhánh của 1 công ty
  - OU (Organizational Unit): gồm người dùng, nhóm, máy tính và những OU khác.
    - Một OU không thể chứa các đối tượng nằm trong domain khác.

    -> ta có thể xây dựng một mô hình thứ bậc của các vật chứa để mô hình hoá cấu trúc của một tổ chức bên trong một domain.
    - Ta nên sử dụng OU để giảm thiểu số lượng domain cần phải thiết lập trên hệ thống.

Global Catalog

- Global Catalog.
- Dịch vụ Global Catalog dùng để xác định thông tin, vị trí của một đối tượng mà người dùng được cấp quyền truy cập.
  - định vị được đối tượng bằng tên và
  - có thể bằng cả những thuộc tính của đối tượng.
- Khi một đối tượng được tạo mới trong AD, đối tượng được gán một con số GUID (Global Unique Identifier):
  - luôn cố định cho dù ta có di chuyển đối tượng đi đến khu vực khác.
- Cung cấp dịch vụ xác thực khi user truy nhập vào từ một domain khác
- Xác nhận việc tìm kiếm thông tin khi có yêu cầu từ Exchange hoặc các ứng dụng khác
- Việc tạo bản sao của server DC trong 1 forest được cấu hình là DC đầu tiên trong forest được tự động gán là global catalog server

2. Giới thiệu Active Directory

- Active Directory là một cơ sở dữ liệu của các tài nguyên trên mạng (Objects) cũng như các thông tin liên quan đến các đối tượng đó.
- Giống Directory Service của Novell, LANManager trên Windows NT 4.0.
- Active Directory giúp quản lý được hệ thống mạng lớn, cung cấp một mức độ ứng dụng mới cho môi trường xí nghiệp:
  - Phân chia thành nhiều domain, dịch vụ thư mục trong mỗi domain có thể lưu trữ hơn mười triệu đối tượng, đủ để phục vụ mười triệu người dùng
  - Thiết lập các mối quan hệ uỷ quyền thích hợp.

3.Chức năng của Active Directory

- Lưu giữ: username, password, computer
- Cung cấp một Server đóng vai trò chứng thực (authentication server) hoặc Server quản lý đăng nhập (logon Server), còn gọi là domain controller (máy điều khiển vùng).
- Duy trì một bảng hướng dẫn hoặc một bảng chỉ mục (index) giúp dò tìm nhanh tài nguyên trên các máy tính khác trong vùng.
- Cho phép tạo ra những tài khoản người dùng với những mức độ quyền (rights) khác nhau như:
  - toàn quyền trên hệ thống mạng,
  - chỉ có quyền backup dữ liệu hay
  - shutdown Server từ xa…
- Cho phép chia nhỏ miền của mình ra thành các miền con (subdomain) hay các đơn vị tổ chức OU (Organizational Unit).

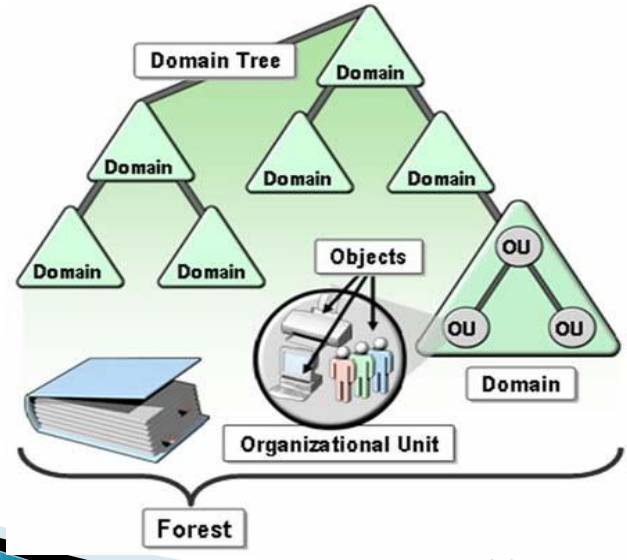
  Sau đó chúng ta có thể ủy quyền cho các quản trị viên bộ phận quản lý từng bộ phận nhỏ.

4. Kiến trúc của Active Directory.

- Logical structure
  - Makes it possible to pattern the directory service's look and feel after the organization in which it runs
    - Objects.
    - Organizational Units
    - Domain
    - Domain Tree.
    - Forest
- Physical structure
  - Consists of sites and servers configured as domain controllers
    - Sites
    - Domain controller

Kiến trúc logic của AD

Kiến trúc logic của AD:



23/05/2020 19

Kiến trúc logic của AD: Object

- Object:
- Objects have attributes depending on object type
- Objects are searchable by attributes

ColorPrinter1	
Attributes	Values
IP address	172.16.0.0
Name	ColorPrinter1
Building	117
Location	1342

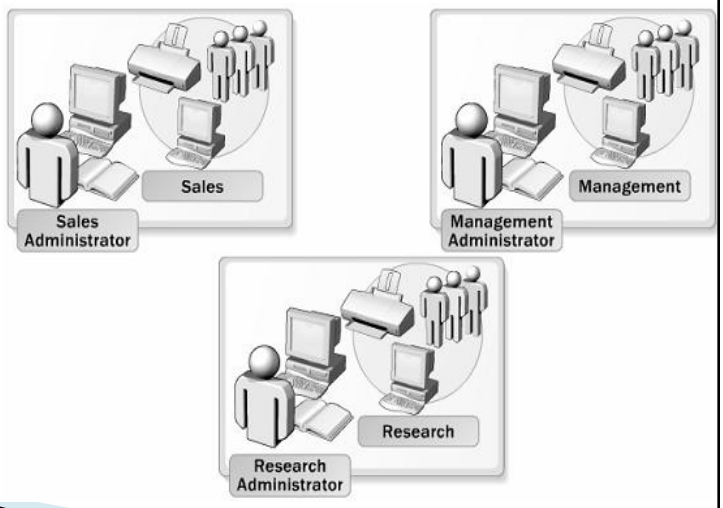
KimYoshida	
Attributes	Values
Name	Kim Yoshida
Building	117
Floor	1

PC1	
Attributes	Values
IP address	172.16.0.2
Name	PC1
Building	200
Location	Sale

23/05/2020 20

Kiến trúc logic của AD: OU

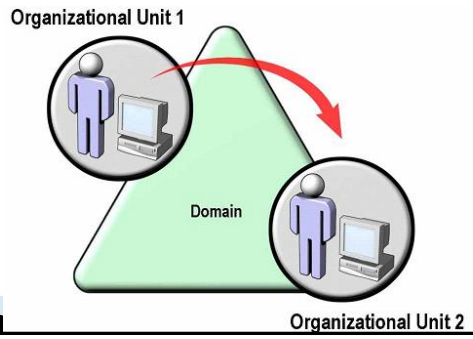
- OU:
  - User accounts
  - Groups
  - Computer accounts
  - Printers
  - Shared folders
  - Applications
  - Servers
  - Domain controll



Kiến trúc logic của AD: OU

Đặc điểm của OU

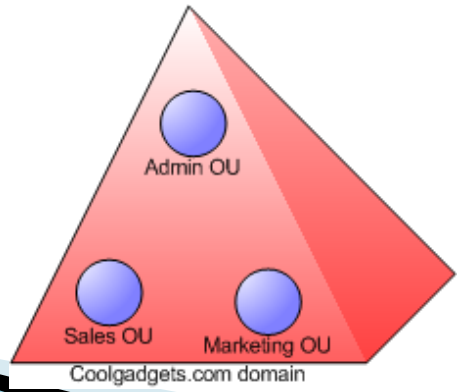
- Tổ chức các objects theo nhóm quản trị và thiết lập các chính sách theo nhóm (GPO).
- Ủy quyền (Delegation) kiểm soát một tập hợp các đối tượng cho sub-administrator
  -> giảm bớt công tác quản trị cho administrator
- Dễ dàng thay đổi cấu trúc các OU: di chuyển…



Kiến trúc logic của AD: Domain

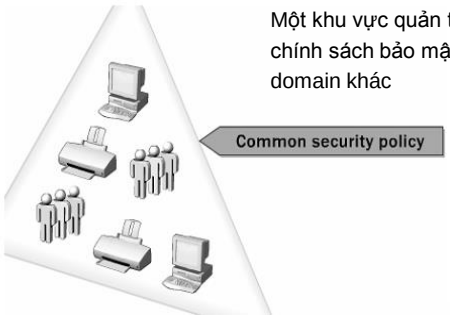
Domain

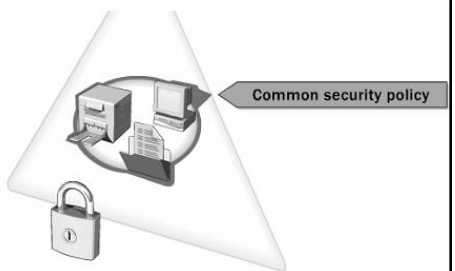
- là đơn vị chức năng nòng cốt của cấu trúc logic AD
- Nó là phương tiện để qui định một tập hợp những người dùng, máy tính, tài nguyên chia sẻ có những qui tắc bảo mật giống nhau từ đó giúp cho việc quản lý các truy cập vào các Server dễ dàng hơn.



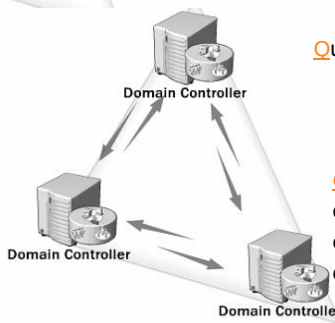
Kiến trúc logic của AD: Domain

Một khu vực quản trị (administrative boundary): các chính sách bảo mật, các quan hệ ủy quyền với các domain khác





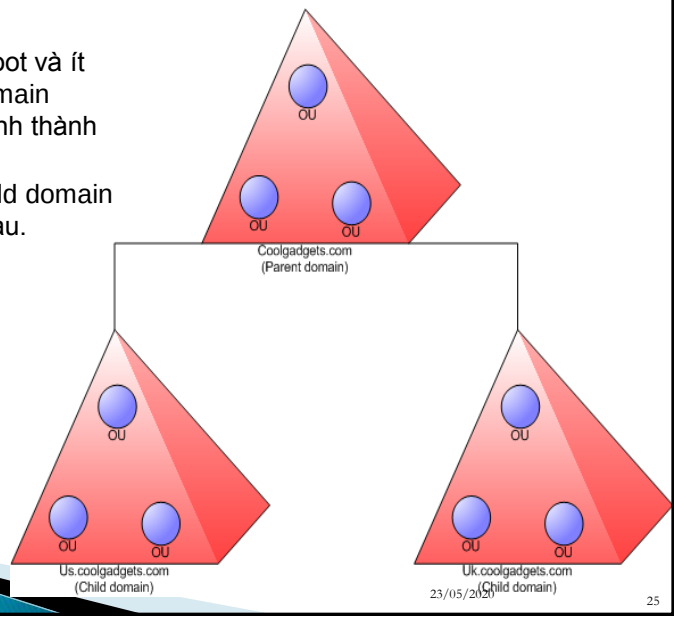
Quản lý bảo mật các các tài nguyên chia sẻ



Cung cấp các Server dự phòng làm chức năng điều khiển vùng (domain controller), đồng thời đảm bảo các thông tin trên các Server này được được đồng bộ với nhau.

Kiến trúc logic của AD: Domain Tree

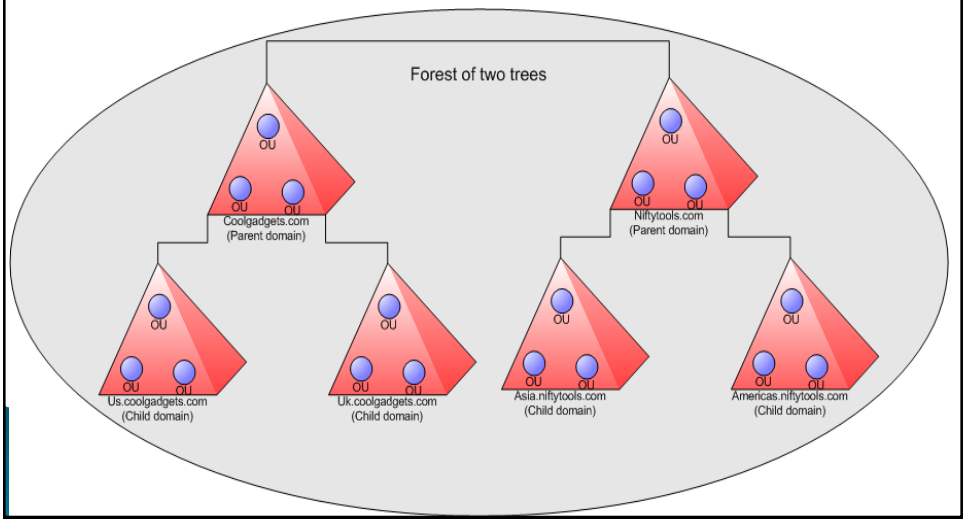
- Domain tree
  - Khi một domain root và ít nhất một child domain được tạo ra thì hình thành một domain tree
  - Tên của các child domain phải khác biệt nhau.



Kiến trúc logic của AD: Forest

- Forest

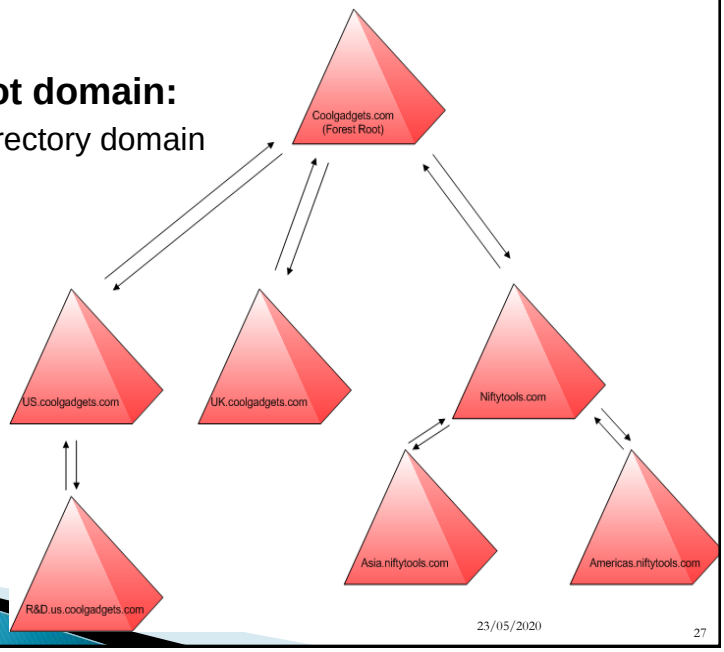
là tập hợp các Domain Tree có thiết lập quan hệ và ủy quyền cho nhau



Kiến trúc logic của AD: Forest

- **Forest root domain:**

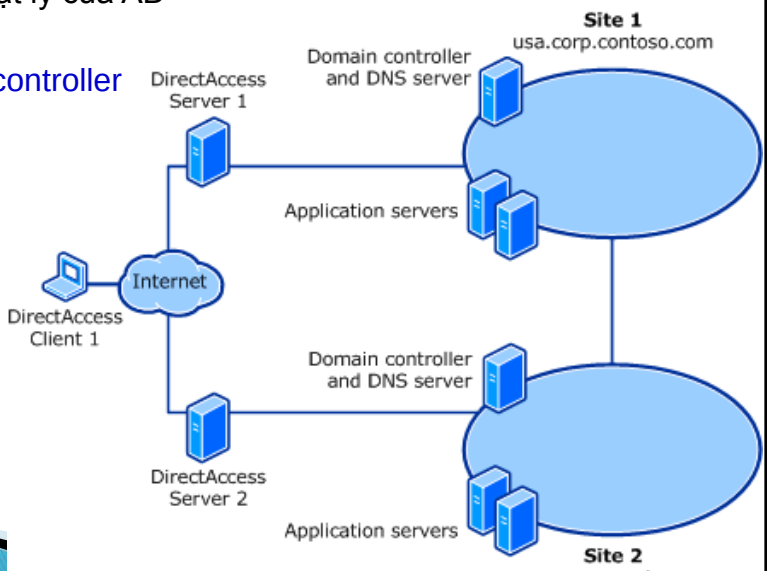
First Active Directory domain



Kiến trúc vật lý của AD

Kiến trúc vật lý của AD

- Site
- Domain controller

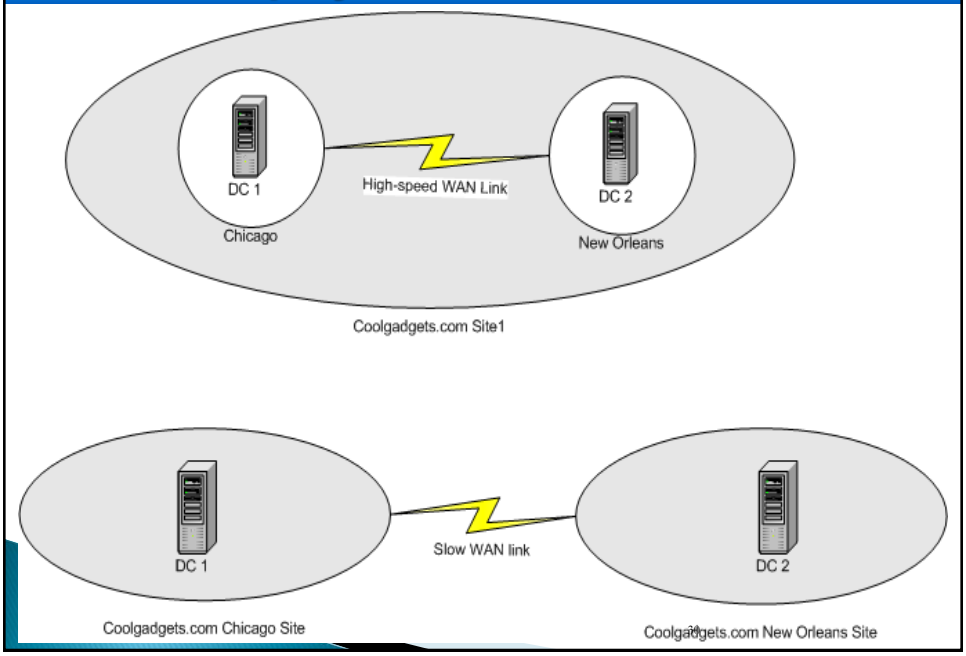


Kiến trúc vật lý của AD: Site

- Site biểu diễn vị trí địa lý đặt các domain controller và các chính sách nhóm được áp dụng
- Các user tại site nào sẽ được xác thực bởi DC tại vị trí site đó.
- First DC of a forest creates a site named Default-First-Site-Name once installed
- Three main reasons for establishing multiple sites:
  - Authentication efficiency
  - Replication efficiency
  - Application efficiency
- Sites are created using Active Directory Sites and Services

29

Kiến trúc vật lý của AD: Site



30

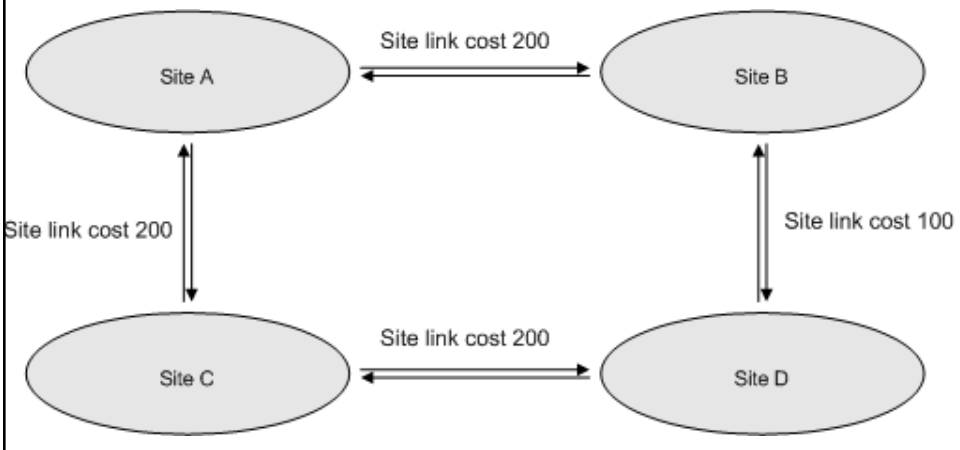
Kiến trúc vật lý của AD: Site

Các thành phần của site:

- Subnets
  - Site: là tổ hợp một hoặc nhiều mạng con sử dụng giao thức IP. Gồm máy tính và các thiết bị nối mạng
- Site Links
  - A site link dùng để kết nối 2 hoặc nhiều sites
  - Xác định thời gian và tần số đồng bộ giữa 2 sites
- Bridgehead Servers
  - Việc đồng bộ trong site xảy ra giữa các server đầu cầu
  - 1 DC được thiết kế như 1 Inter-Site topology Generator (ISTG), mà sau đó chỉ định một máy chủ đầu cầu để xử lý các bản sao cho mỗi phân vùng thư mục

31

Kiến trúc vật lý của AD: Site



Topo nhân bản liên site được xác định theo giá trị chi phí liên quan với các liên kết site

32

Kiến trúc vật lý của AD: Domain Controller

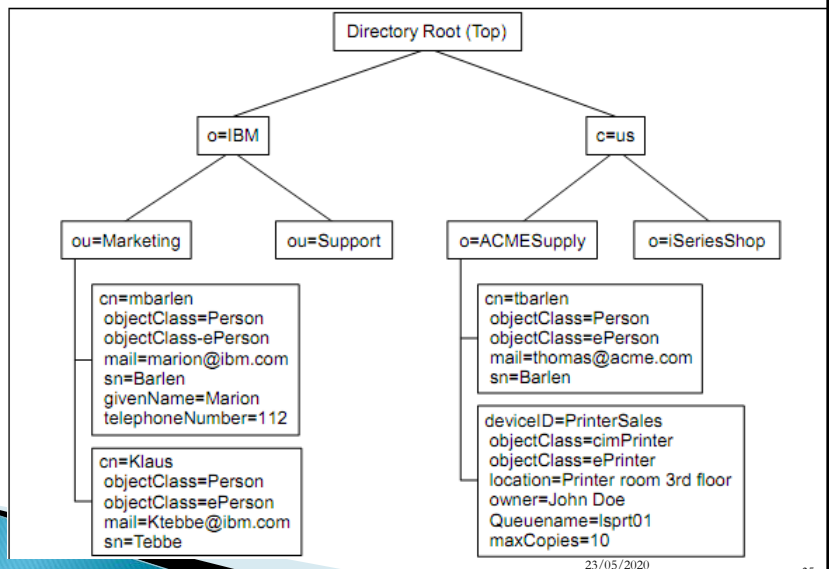
- Domain controller (DC)
  - Active Directory yêu cầu 1 hoặc nhiều domain để hoạt động
  - Một miền phải có 1 hoặc nhiều máy domain controller (DC)
  - Các DC hoạt động ngang hàng (không dùng PDC, BDC)
  - Mỗi DC chứa thông tin về AD của Domain, tự động sao chép thông tin cho các DC khác (đồng bộ).
  - DC quản lý tất cả các tương tác của user trên Domain: tìm kiếm trên AD, duy trì các chính sách và cung cấp sự thẩm định cho các đăng nhập vào Domain
  - Sử dụng nhiều DC giúp giảm tải (trong việc chứng thực), tăng khả năng chịu lỗi (khi 1 DC bị lỗi)

AD và LDAP

- LDAP (Lightweight Directory Access Protocol) là một phần của Active Directory,
- là một giao thức phần mềm cho phép định vị các tổ chức, cá nhân hoặc các tài nguyên khác như file và thiết bị trong mạng, dù là mạng Internet hay mạng nội bộ trong công ty.
- Thư mục LDAP được tổ chức theo một kiến trúc cây đơn giản gồm có các mức dưới đây:
  - **Thư mục gốc - Top:** có các nhánh con
  - **Country - C**, mỗi Country lại có các nhánh con
  - **Organizations - O**, mỗi Organization lại có các nhánh con
  - **Organizational units - OU** (các phòng ban,…), OU có các nhánh
  - **Common Name – CN:** gồm các user, file và tài nguyên chia sẻ, chẳng hạn như printer)

AD và LDAP

- LDAP.

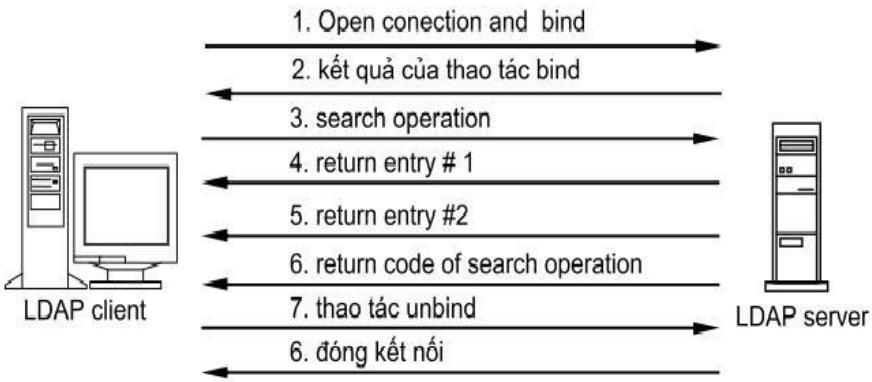


AD và LDAP

- Một thư mục LDAP có thể được phân phối giữa nhiều máy chủ. Mỗi máy chủ có thể có một phiên bản sao của thư mục tổng thể và được đồng bộ theo chu kỳ.
- Các quản trị viên cần phải hiểu LDAP khi tìm kiếm các thông tin trong Active Directory, cần tạo các truy vấn LDAP hữu dụng khi tìm kiếm các thông tin được lưu trong cơ sở dữ liệu Active Directory

AD và LDAP

- LDAP: hoạt động them client/server



Hình 5 - 4 Mô hình kết nối giữa client /server

III. Cài đặt và cấu hình AD

1. Nâng cấp Server thành Domain Controller.
   a. Giới thiệu.
   b. Các bước cài đặt.
2. Gia nhập máy trạm vào Domain.
   a. Giới thiệu.
   b. Các bước cài đặt.
3. Xây dựng các Domain Controller đồng hành.
   a. Giới thiệu
   b. Các bước cài đặt.
4. Xây dựng Subdomain
5. Xây dựng Organizational Unit.
6. Công cụ quản trị các đối tượng trong Active Directory

Nâng cấp Server thành DC

- Các bước cơ bản:
  - Cài đặt standalone Server (server độc lập)
  - Nâng cấp standalone Server thành một máy DC
- Nếu muốn chuyển ngược lại:
  - Giáng cấp một máy DC thành một Server bình thường

39

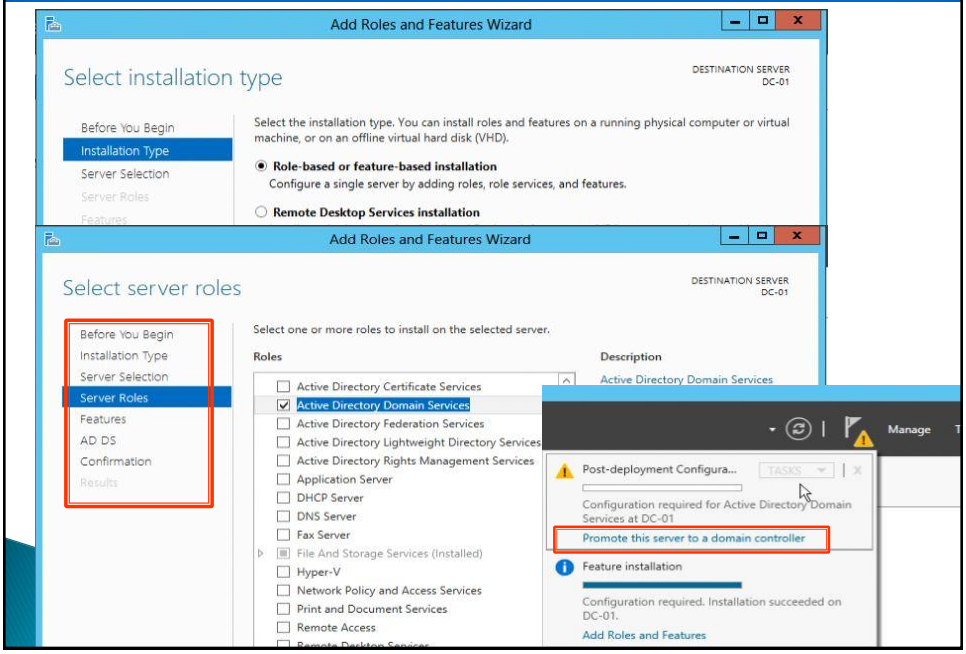
Nâng cấp Server thành DC

Yêu cầu:

- Khai báo đầy đủ các thông số TCP/IP,
- Khai báo DNS Server có địa chỉ chính là địa chỉ IP của Server cần nâng cấp. Nên cấu hình dịch vụ trước khi nâng cấp Server,
  Hoặc cài đặt DNS tự động trong quá trình nâng cấp.
- Thực hiện:
  - Dùng tiện ích Manage Your Server trong Administrative Tools
  - Hoặc DCPROMO.
  - Với windows server 2012, chọn:
    Promote this server to a domain controller

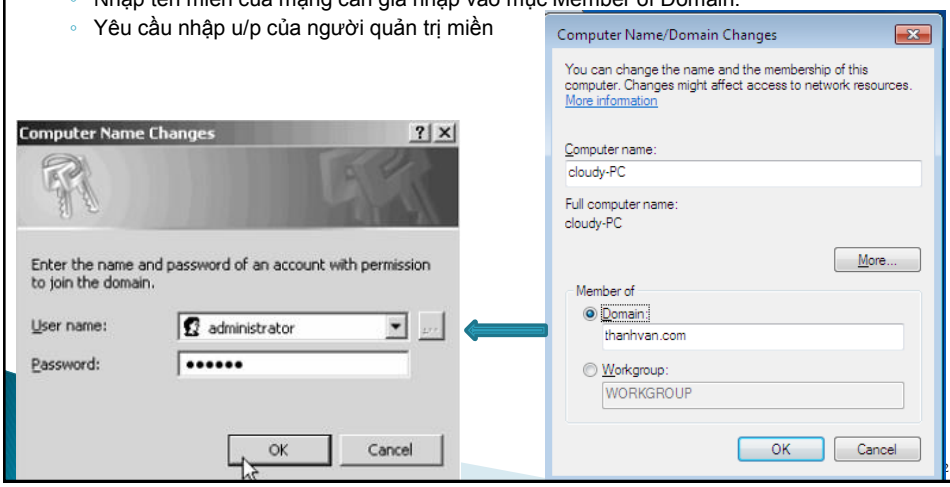
40

cài đặt gói Active Directory Domain Services.



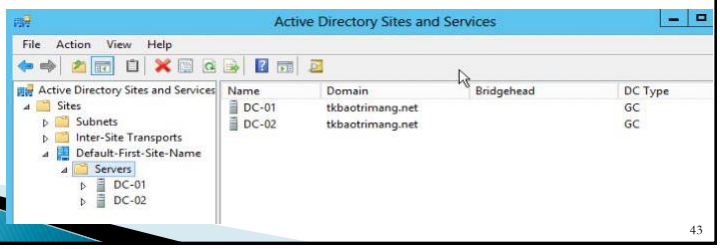
Gia nhập máy trạm vào Domain

- Máy client: có IP, trỏ tới DNS server
- Đăng nhập cục bộ vào máy trạm với vai trò người quản trị (administrator).
- Right click My Computer, chọn Properties, Tab Computer Name\ Change:
  - Nhập tên miền của mạng cần gia nhập vào mục Member of Domain.
  - Yêu cầu nhập u/p của người quản trị miền



Xây dựng các DC đồng hành

- Chọn 1 server muốn cài DC đồng hành
- Cài AD và nâng cấp DC
  - Domain Controller Type:
    Additional domain cotroller for an existing domain
  - xác thực bạn phải là người quản trị cấp miền thì mới có quyền tạo các DC
  - nhập Full DNS Name của miền mà bạn cần tạo thêm DC
  - Chỉ định thư mục chứa cơ sở dữ liệu của AD
  - Transaction Log và thư mục Sysvol.
  - Quá trinh đồng bộ dữ liệu AD giữa hai DC cũ và mới
  - Retart máy



43

Xây dựng các DC đồng hành

- Chuyển Server DC đồng hành (DC2) thành DC Master:
  - Cách 1: Máy Master đang bật

Thao tác trên máy Master (DC1.abc.com)
Change Domain Controller
Trust..: change (3)
..Schema (2)

  - Cách 2: Máy Master bị tắt (hỏng)

Thao tác trên máy DC2:

- Ntdsutil
- Role
- Connections
- Connect to server <name> (ex: DC2.abc.com)

44

Xây dựng Subdomain

- DC đầu tiên quản lý miền (là một gốc của rừng hoặc Domain Tree đầu tiên)
- Từ DC đầu tiên, có thể tạo thêm các subdomain cho hệ thống.
- Thực hiện:
  - Tại member server, chạy dcpromo
  - Domain Controller Type: **Domain Controller for a New Domain**
  - Create new domain:
    - Domain in new forest: tạo domain đầu tiên trong một rừng mới,
    - Child domain in an existing domain tree: tạo ra một domain con dựa trên một cây domain có sẵn => chọn mục này để tạo subdomain
    - Domain tree in an existing forest: tạo ra một cây domain mới trong một rừng đã có sẵn.
  - Network Credenrial: xác nhận là người quản trị cấp domain tree.
  - Nhập tên của domain tree hiện có và tên của child domain cần tạo.
  - ….Next/ Restart máy
- Kiểm tra: cây DNS của hệ thống trên Server quản lý gốc rừng có tạo thêm một child domain không

45

Xây dựng Organizational Unit

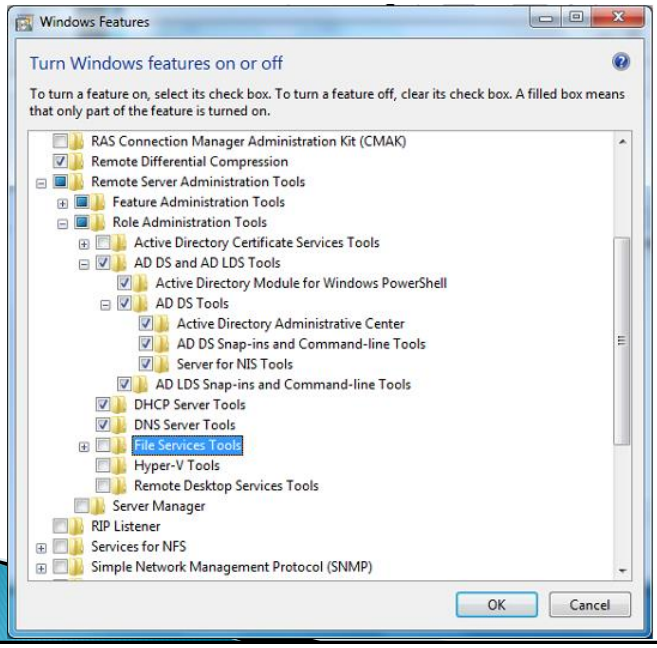
- OU là một nhóm tài khoản người dùng, máy tính và tài nguyên mạng được tạo ra nhằm mục đích:
  - Dễ dàng quản lý hơn và
  - Ủy quyền cho các quản trị viên địa phương giải quyết các công việc đơn giản.
  - Thông qua OU chúng ta có thể áp đặt các giới hạn phần mềm và giới hạn phần cứng thông qua các Group Policy.
- Thực hiện:
  - Chọn menu Start ¤ Programs ¤ Administrative Tools ¤ Active Directory User and Computer
  - Right click trên tên miền và chọn New-Organizational Unit.

46

Công cụ quản trị các đối tượng trong AD

- Có thể quản trị các đối tượng trong AD ở các máy trạm (win7)
- Kích hoạt bộ cài đặt Remote Server Administration Tool
- Kích hoạt Remote Server Administrative Tool: Start \ Control Panel \ Program And Features \ Turn On or Off Program and Features \ đánh dấu chọn các công cụ như hình minh họa \ OK

47



481