Seminar

OpenLDAP - Giải pháp xác thực tập trung

1. **GIỚI THIỆU**
   - Tổng quan về LDAP
   - Giới thiệu các ứng dụng sử dụng ldap làm backend
   - Các công cụ quản trị LDAP
   - Giới thiệu OpenLDAP

2. **DEMO:**
   - Cài đặt OpenLDAP trên Ubuntu Server.
   - Sử dụng phpldapadmin để quản trị OpenLDAP
   - Sử dụng OpenLDAP xác thực các dịch vụ: CMS (Drupal), LMS (Moodle), Forum (phpBB3), FTP (Proftpd).

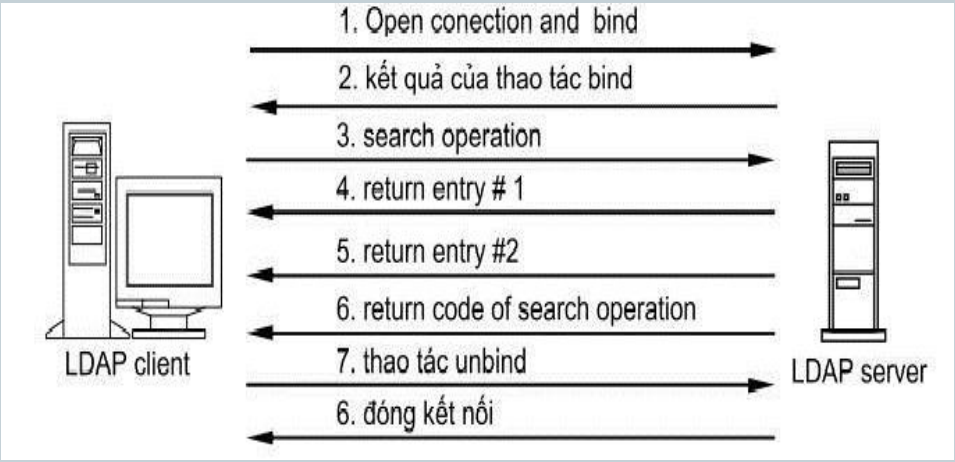
Tổng quan về thư mục và dịch vụ thư mục

LDAP: Lightweight Directory Access Protocol

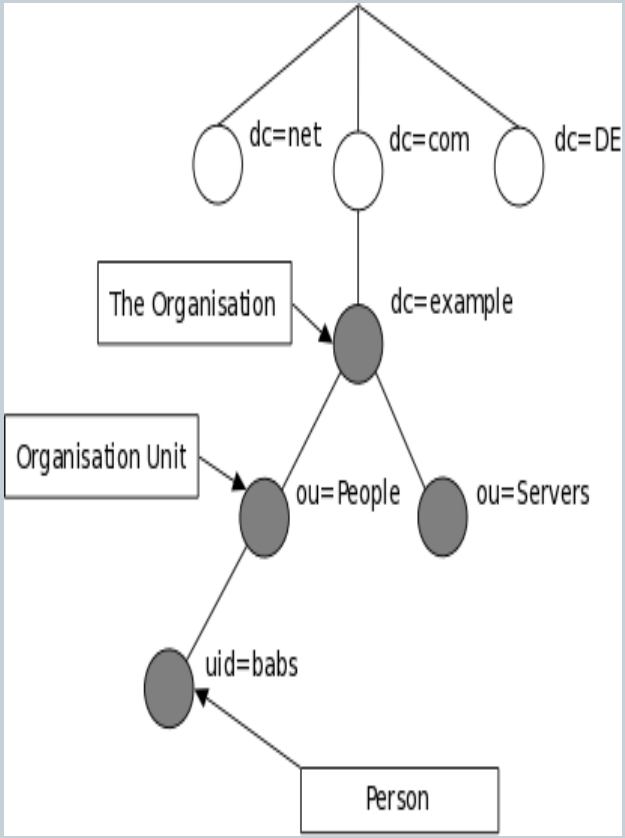
- **Thư mục (Directory)**: là nơi dùng để chứa danh sách thông tin về các đối tượng, được sắp xếp một cách chi tiết cho phép thực hiện các thao tác truy xuất thông tin nhanh chóng.
- **Dịch vụ thư mục (Directory Service)**: Là một dạng CSDL đặc biệt, có tính mô tả cao, được thiết kế để tối ưu hóa cho việc tìm kiếm, đọc và duyệt dữ liệu.
- **Các dịch vụ thư mục thường thấy hiện nay:**
  - Active Directory (Microsoft)
  - eDirectory (Novell)
  - Red Hat Directory Server
  - ApacheDS
  - OPenDS
  - OpenLDAP
  - ...

Tổng quan về LDAP

- Là giao thức truy cập nhanh các dịch vụ thư mục.
- Được phát triển dựa trên X-500 (DAP).
- Là giao thức dạng Client – Server
- Hoạt động trên mô hình TCP/IP.



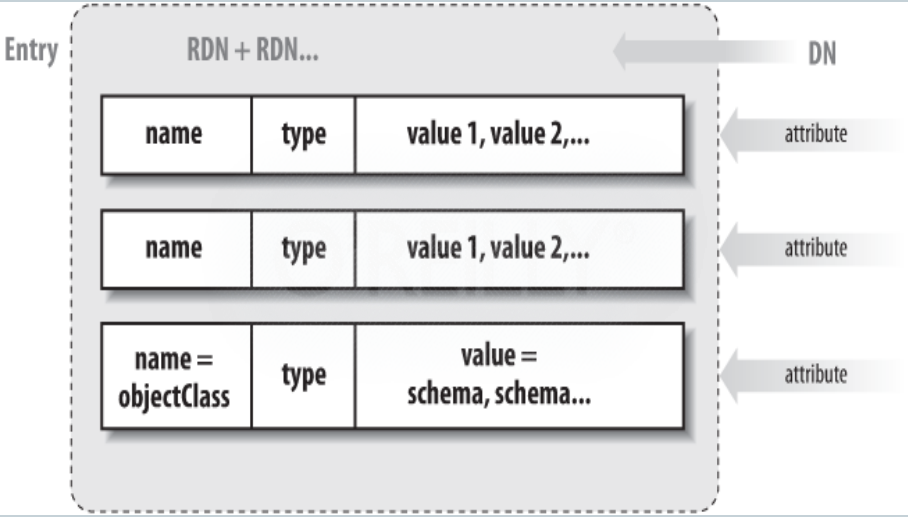
Mô hình kết nối giữa Client/Server



Mô hình cây thư mục LDAP

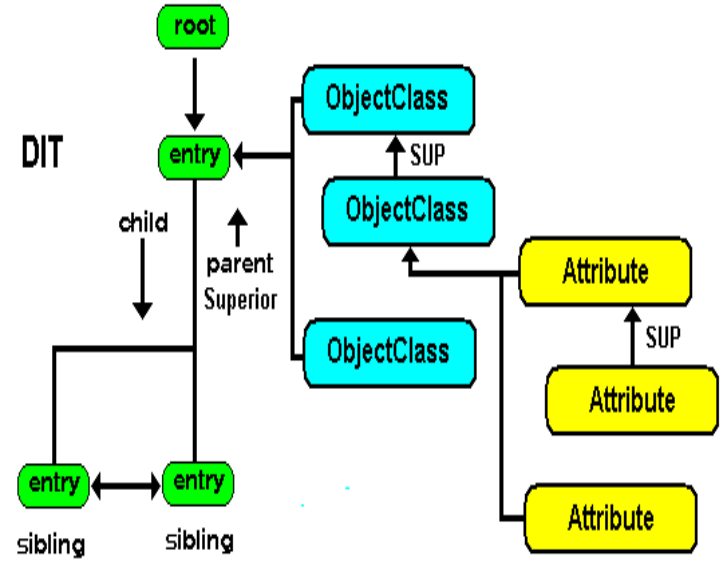
Các mô hình của LDAP (LDAP Models)

- **LDAP hoạt động dựa trên 4 mô hình (LDAP Models)**
  - Mô hình thông tin (Information model)
  - Mô hình đặt tên (Naming model)
  - Mô hình chức năng (Functional Model)
  - Mô hình bảo mật (Security Model)



dn: uid=cict,ou=People,dc=cict,dc=local
objectclass: top
objectclass: person
objectclass: inetOrgPerson
cn: cict
sn: cict_agu
uid: cict
mail: cict@cict.local
userpassword: cict_password

Schema, Objectclass, Attribute



Schema:

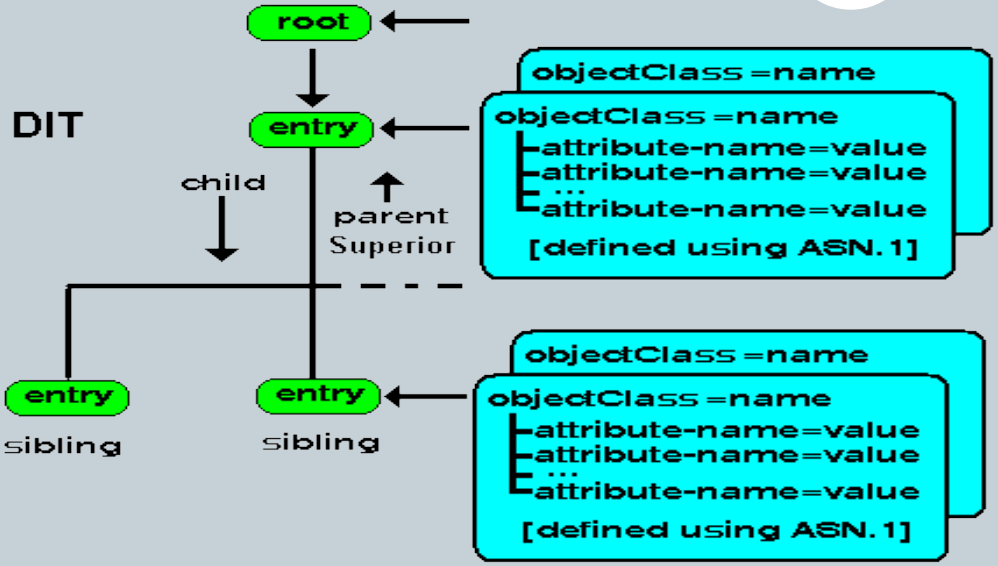
- Là một tập hợp các quy tắc (rule) để điều khiển các loại thông tin mà máy chủ thư mục có thể tổ chức.
- Một Attribute được định nghĩa trong schema này có thể được sử dụng bởi một Objectclass được định nghĩa trong schema khác.

Objectclass:

- Là một nhóm thiết lập của các thuộc tính (Attribute).

- Objecclass có thể được tổ chức phân cấp, khi đó nó sẽ được thừa hưởng thuộc tính của các cấp cao hơn.
- Mỗi Objectclass đều định nghĩa các thuộc tính bắt buộc và các thuộc tính tùy chọn.

Schema, Objectclass, Attribute



Attribute:

- Chứa các dữ liệu, mỗi thuộc tính đều có tên và giá trị của nó.
- Một Attribute có thể bao gồm trong 1 hoặc nhiều Objectclass.
- Mỗi Attribute có thể có 1 hoặc nhiều giá trị.
- Attribute cũng có thể được tổ chức theo dạng phân cấp.

Các ứng dụng sử dụng LDAP làm Backend

- BIND9
- SQUID PROXY
- POSTFIX, ZIMBRA, EXIM
- SAMBA
- OPENVPN
- RADIUS
- WEB
- ...

OpenLDAP

- Website: http://www.openldap.org/
- Phiên bản hiện tại: **2.4.31**
- OpenLDAP là phần mềm nguồn mở, miễn phí sử dụng để tạo một máy chủ thư mục LDAP.
- Thành phần quan trọng nhất trong Openldap là deamon slapd, nó có tác dụng tạo ra 1 máy chủ thư mục.
- Ngoài ra còn có các thư viện hỗ trợ người dùng tương tác với LDAP.
- OpenLDAP cung cấp và hỗ trợ đầy đủ các yêu cầu cần thiết cho 1 máy chủ thư mục.

Một số công cụ quản trị LDAP

LDAP Admin

- Website: http://www.ldapadmin.org/
- Giới thiệu: Là 1 LDAP client miễn phí chạy trên môi trường Windows , dùng để quản trị thư mục LDAP, nó cho phép duyệt, tìm kiếm, chỉnh sửa, xóa ... các đối tượng trên máy chủ LDAP.

PhpLdapAdmin

- Website: http://phpldapadmin.sourceforge.net
- Giới thiệu: Là một LDAP client miễn phí chạy trên môi trường web, dùng để quản trị máy chủ LDAP.

DEMO