

LDAP

Giới thiệu chung

MỤC LỤC

1	Giới thiệu	3
1.1	Mục đích	3
1.2	Định nghĩa từ viết tắt	3
1.3	Tài liệu tham khảo	4
2	Giới thiệu chung về LDAP	5
2.1	Giới thiệu cơ bản	5
2.1.1	LDAP - Lightweight Directory Access Protocol	5
2.1.2	Phương thức hoạt động của LDAP	6
2.1.3	Cấu trúc file Ldif	9
2.2	Mô hình LDAP	12
2.2.1	Mô hình thông tin Ldap (LDAP information model)	13
2.2.2	Mô hình đặt tên Ldap (LDAP naming model)	14
2.2.3	Mô hình chức năng Ldap (LDAP function model)	15
2.2.4	Mô hình bảo mật Ldap (LDAP Security model)	18
2.3	Chứng thực trong LDAP	19
2.4	Một số dịch vụ sử dụng nghi thức LDAP	20
3	Áp dụng vào khoa CNTT	23
3.1	Xây dựng CSDL ban đầu	23
3.2	Sơ đồ	23
3.3	Nội dung file Ldif	24
4	Giới thiệu các LDAP server thường dùng	25
4.1	Bản miễn phí	25
4.2	Bản thương mại	25
4.3	Cài đặt OpenLDAP và cấu hình jXplorer kết nối vào OpenLDAP	25

1 Giới thiệu

1.1 Mục đích

Giới thiệu chung về công nghệ Ldap dùng để chứng thực tập trung, các mô hình làm việc của nó và xây dựng mô hình phù hợp với khoa CNTT.

1.2 Định nghĩa từ viết tắt

STT	Tên	Mô tả
1	Ldap	Lightweight Directory Access Protocol : giao thức truy nhập nhanh dịch vụ thư mục.
2	Ldif	LDAP Data Interchange Format : định nghĩa ra khuôn dạng để trao đổi dữ liệu ở dạng thức văn bản dùng để mô tả thông tin về thư mục . LDIF còn có thể mô tả một tập hợp các thư mục hay các cập nhật có thể được áp dụng trên thư mục.
3	RDN	Relative Distinguished Name : là thuộc tính của DN làm cho đối tượng là duy nhất trong ngữ cảnh đó.
4	DIT	Directory Information Tree : cây thông tin thư mục
5	OID	Object Identifier : là một số duy nhất trên toàn cầu xác định đối tượng.
6	SSL	Secure Sockets Layer - là một giao thức thường được sử dụng để quản lý an ninh của một truyền tin trên Internet.
7	TSL	Transport Layer Security - là một giao thức đảm bảo sự riêng tư (private) giữa các ứng dụng truyền thông và người dùng của họ trên Internet.
8	SASL	Simple Authentication and Security Layer

1.3 Tài liệu tham khảo

- Lightweight Directory Access Protocol - Wikipedia, the free encyclopedia.htm
- Understanding LDAP design and Implementation, IBM redbooks (sg244986.pdf).
- <http://www.ust.hk/itsc/ldap/understand.html>
- <http://www.zytrax.com/books/ldap/>

2 Giới thiệu chung về LDAP

2.1 Giới thiệu cơ bản

- Hiện nay, để xây dựng các hệ thống lớn, điều tối quan trọng là phải làm cách nào để có thể tích hợp dữ liệu để từ đó có thể dùng chung giữa các hệ thống khác nhau. Trong đó, tích hợp tài khoản của người sử dụng là vấn đề cần thiết nhất trong những cái "tối quan trọng" trên.
- Hãy tưởng tượng một hệ thống với khoảng 5 - 6 mô đun khác nhau, mỗi mô đun lại được thiết kế trên một nền tảng khác nhau (Có người thì dùng Oracle + AS Portal, có người thì dùng DB2 với WebSphere, người khác thì dùng MySQL với phpnuke, người thì dùng Window, người thì cài Linux), do đó cần có một hệ thống người dùng khác nhau. Vậy thì với mỗi mô đun, người sử dụng cần phải có một User Name, một mật khẩu khác nhau, đó là điều không thể chấp nhận được. Người dùng chẳng mấy chốc mà chán ghét hệ thống.
- Làm cách nào để có thể tích hợp được người dùng giữa các hệ thống trên? Câu trả lời đó là LDAP. Vậy LDAP là gì?

2.1.1 LDAP - Lightweight Directory Access Protocol

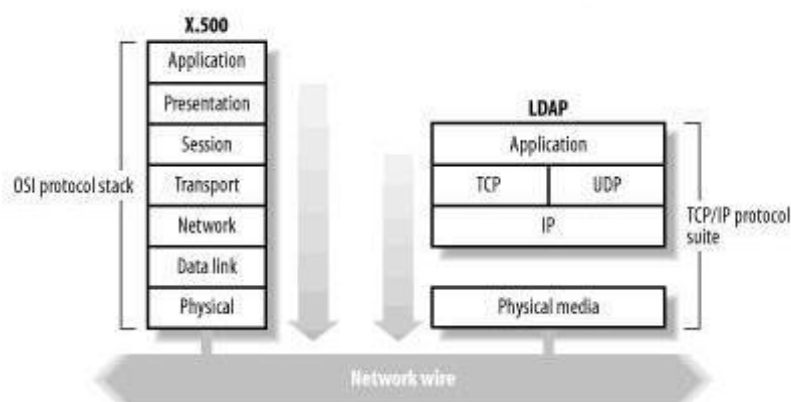
Định nghĩa về LDAP

- LDAP** (Lightweight Directory Access Protocol) – là giao thức truy cập nhanh các dịch vụ thư mục - là một chuẩn mở rộng cho nghi thức truy cập thư mục.
- LDAP** là một giao thức tìm, truy nhập các thông tin dạng thư mục trên server. Nó dùng giao thức dạng Client/Server để truy cập dịch vụ thư mục.
- LDAP** chạy trên TCP/IP hoặc các dịch vụ hướng kết nối khác.
- Ngoài ra, LDAP được tạo ra đặc biệt cho hành động "đọc". Bởi thế, xác thực người dùng bằng phương tiện "lookup" LDAP nhanh, hiệu suất, ít tốn tài nguyên, đơn giản hơn là query 1 user account trên CSDL.
- Có các **LDAP** Server như: OpenLDAP, OPENDS, Active Directory, ...

Giải thích cụm từ "Lightweight Directory Access Protocol"

1. Lightweight

- Tại sao LDAP được coi là lightweight? Lightweight được so sánh với cái gì? Để trả lời những câu hỏi này, bạn cần tìm hiểu nguồn gốc của LDAP.
- Bản chất của LDAP là một phần của dịch vụ thư mục X.500. LDAP thực chất được thiết kế như một giao thức nhẹ nhàng, dùng như gateway trả lời những yêu cầu của X.500 server.
- X500 được biết như là một heavyweight, là một tập các chuẩn. Nó yêu cầu client và server liên lạc với nhau sử dụng theo mô hình OSI. Mô hình 7 tầng của OSI - mô hình chuẩn phù hợp trong thiết kế với giao thức mạng, nhưng khi so sánh với chuẩn TCP/IP thì nó trở nên không còn hợp lý.
- LDAP được so sánh với lightweight vì nó sử dụng gói tin overhead thấp, nó được xác định chính xác trên lớp TCP (mặc định là cổng 389) của danh sách các giao thức TCP/IP. Còn X.500 là một lớp giao thức ứng dụng, nó chứa nhiều thứ hơn, ví dụ như các network header được bao quanh các gói tin ở mỗi layer trước khi nó được chuyển đi trong mạng.

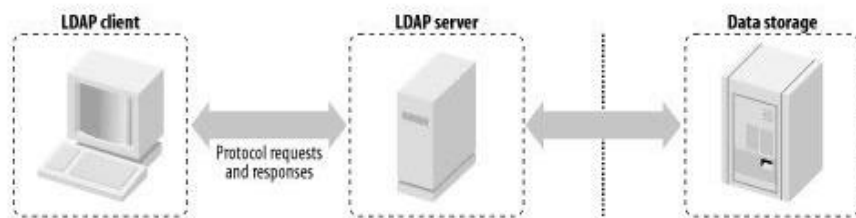


Hình 1. X.500 thông qua mô hình OSI – LDAP thông qua TCP/IP

- Tóm lại, LDAP được coi là *lightweight* bởi vì nó đã lược bỏ rất nhiều những phương thức ít được dùng của X.500.

2. Directory

- Dịch vụ thư mục không được nhằm với một cơ sở dữ liệu. Thư mục được thiết kế để đọc nhiều hơn là để ghi vào, còn đối với cơ sở dữ liệu, nó phù hợp với cả công việc đọc và ghi một cách thường xuyên và lặp đi lặp lại.
- LDAP chỉ là một giao thức, nó là một tập những thông tin cho việc xử lý các loại dữ liệu. Một giao thức không thể biết dữ liệu được lưu trữ ở đâu. LDAP không hỗ trợ sự xử lý và những đặc trưng khác như của cơ sở dữ liệu.
- Client sẽ không bao giờ thấy được hoặc biết rằng có một bộ máy lưu trữ backend. Vì lý do này, LDAP client cần liên tác với LDAP server theo mô hình chuẩn sau:



Hình 2. Mối quan hệ giữa LDAP client, LDAP server và nơi chứa dữ liệu

3. Access Protocol

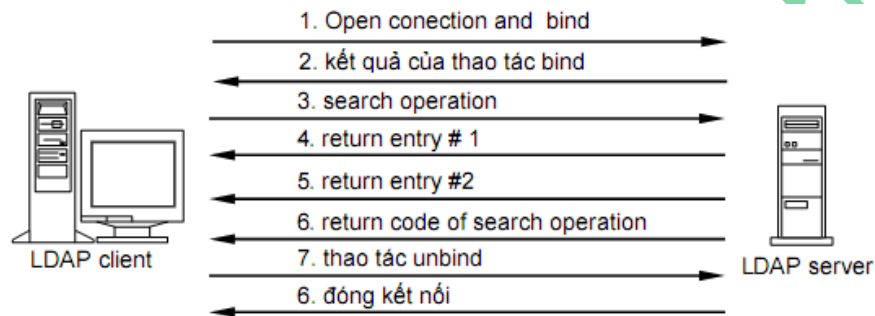
- LDAP là một giao thức truy cập. Nó đưa ra mô hình dạng cây của dữ liệu, và mô hình dạng cây này được nhắc tới khi bạn truy cập một LDAP server.
- Giao thức truy cập client/server của LDAP được định nghĩa trong RFC, một client có thể đưa ra một loạt những yêu cầu và những trả lời cho những yêu cầu đó lại được trả lời theo những cách sắp xếp khác nhau.

2.1.2 Phương thức hoạt động của LDAP

Ldap dùng giao thức giao tiếp client/sever

- Giao thức giao tiếp client/sever là một mô hình giao thức giữa một chương trình client chạy trên một máy tính gửi một yêu cầu qua mạng đến cho một máy tính khác đang chạy một chương trình sever (phục vụ).
- Chương trình server này nhận lấy yêu cầu và thực hiện sau đó nó trả lại kết quả cho chương trình client
- Ý tưởng cơ bản của giao thức client/server là công việc được gán cho những máy tính đã được tối ưu hoá để thực hiện công việc đó.
- Một máy server LDAP cần có rất nhiều RAM(bộ nhớ) dùng để lưu trữ nội dung các thư mục cho các thao tác thực thi nhanh và máy này cũng cần đĩa cứng và các bộ vi xử lý ở tốc độ cao.

Đây là một tiến trình hoạt động trao đổi LDAP client/server :

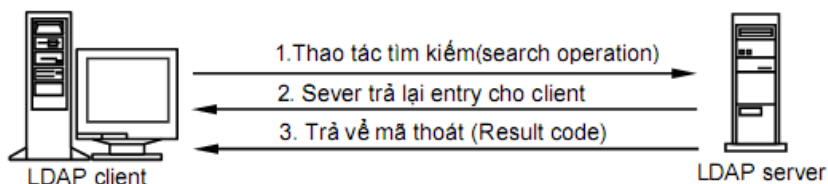


Hình 3. Mô hình kết nối giữa client/server

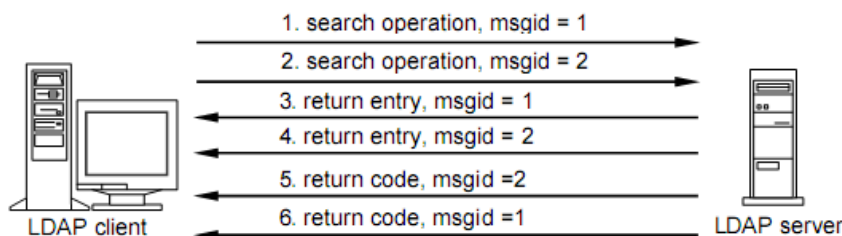
- Client mở một kết nối TCP đến LDAP server và thực hiện một thao tác bind. Thao tác bind bao gồm tên của một directory entry ,và uỷ nhiệm thư sẽ được sử dụng trong quá trình xác thực, uỷ nhiệm thư thông thường là password nhưng cũng có thể là chứng chỉ điện tử dùng để xác thực client.
- Sau khi thư mục có được sự xác định của thao tác bind, kết quả của thao tác bind được trả về cho client. Client phát ra các yêu cầu tìm kiếm.
- Server thực hiện xử lý và trả về kết quả cho client.
- Server gửi thông điệp kết thúc việc tìm kiếm.
- Client phát ra yêu cầu unbind, với yêu cầu này server biết rằng client muốn huỷ bỏ kết nối.
- Server đóng kết nối.

LDAP là một giao thức hướng thông điệp

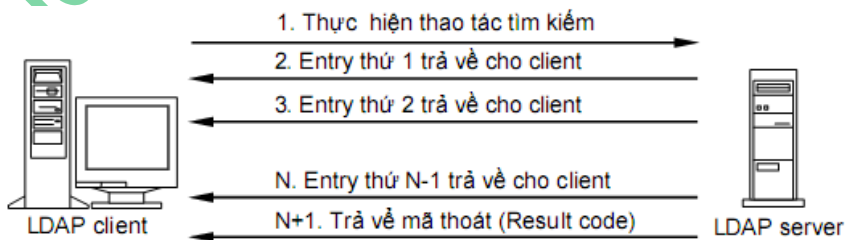
- Do client và sever giao tiếp thông qua các thông điệp, Client tạo một thông điệp (LDAP message) chứa yêu cầu và gửi nó đến cho server. Server nhận được thông điệp và xử lý yêu cầu của client sau đó gửi trả cho client cũng bằng một thông điệp LDAP.
- Ví dụ: Khi LDAP client muốn tìm kiếm trên thư mục, client tạo LDAP tìm kiếm và gửi thông điệp cho server. Server tìm trong cơ sở dữ liệu và gửi kết quả cho client trong một thông điệp LDAP.

**Hình 4. Thao tác tìm kiếm cơ bản**

- Nếu client tìm kiếm thư mục và nhiều kết quả được tìm thấy, thì các kết quả này được gửi đến client bằng nhiều thông điệp

**Hình 5. Những thông điệp Client gửi cho server**

- Do nghi thức **LDAP** là giao thức hướng thông điệp nên client được phép phát ra nhiều thông điệp yêu cầu đồng thời cùng một lúc. Trong **LDAP**, message ID dùng để phân biệt các yêu cầu của client và kết quả trả về của server.

**Hình 6. Nhiều kết quả tìm kiếm được trả về**

- Việc cho phép nhiều thông điệp cùng xử lý đồng thời làm cho **LDAP** linh động hơn các nghi thức khác.
- Ví dụ như HTTP, với mỗi yêu cầu từ client phải được trả lời trước khi một yêu cầu khác được gửi đi, một HTTP client program như là Web browser muốn tải xuống cùng lúc

nhều file thì Web browser phải thực hiện mở từng kết nối cho từng file, LDAP thực hiện theo cách hoàn toàn khác, quản lý tất cả thao tác trên một kết nối.

2.1.3 Cấu trúc file Ldif

Khái niệm LDIF

- **LDIF** (LDAP Interchange Format) được định nghĩa trong RFC 2849, là một chuẩn định dạng file text lưu trữ những thông tin cấu hình LDAP và nội dung thư mục.
- File LDIF thường được sử dụng để import dữ liệu mới vào trong directory của bạn hoặc thay đổi dữ liệu đã có. Dữ liệu trong file LDIF cần phải tuân theo một luật có trong schema của LDAP directory.
- Schema là một loại dữ liệu đã được định nghĩa từ trước trong directory của bạn. Mọi thành phần được thêm vào hoặc thay đổi trong directory của bạn sẽ được kiểm tra lại trong schema để đảm bảo sự chính xác. Lỗi vi phạm schema sẽ xuất hiện nếu dữ liệu không đúng với các luật đã có.
- Giải pháp Import dữ liệu lớn vào LDAP. Nếu dữ liệu được lưu trong excel khoảng vài chục ngàn mẫu tin, viết tool chuyển thành định dạng trên rồi import vào LDAP Server.

Cấu trúc tập tin Ldif

- Thông thường một file LDIF sẽ theo khuôn dạng sau:
 - Mỗi một tập entry khác nhau được phân cách bởi một dòng trắng
 - Sự sắp đặt "tên thuộc tính : giá trị"
 - Một tập các chỉ dẫn cú pháp để làm sao xử lý được thông tin
- Những yêu cầu khi khai báo nội dung file LDIF :
 - Lời chú giải trong file LDIF được gõ sau dấu # trong một dòng
 - Thuộc tính được liệt kê phía bên trái của dấu (:) và giá trị được biểu diễn bên phải. Dấu đặc biệt được phân cách với giá trị bằng dấu cách trắng
 - Thuộc tính dn định nghĩa duy nhất một DN xác định trong entry đó

- Dưới đây là ví dụ về cấu trúc một file Ldif:



- Chú ý:** Những tên trường mà đằng sau có dấu “::” thì giá trị của nó được mã hóa theo chuẩn BASE64 Encoding, với charset UTF-8. Nếu gõ tiếng việt thì khi import vào LDAP Server sẽ không hiểu, vì thế bắt buộc ta phải mã hóa theo chuẩn BASE64.
 - Ví dụ: cn:Phạm Thị Thùy → cn:: VHLhuqduIFRow6FplExvbmc= (dấu “::” cho biết trường này sử dụng basecode64)

Nội dung một entry thư mục ở dạng Ldif:

- Dưới đây là nội dung một entry trong tập tin Ldif.

```

dn: uid=tuanh,ou=Teacher,o=it,dc=hcmuaf,dc=edu,dc=vn
objectClass: person
objectClass: inetOrgPerson
objectClass: organizationalPerson
objectClass: top
givenName: tuanh
uid: tuanh
cn: tuanh
telephoneNumber: 125698742
sn: tuanh
userPassword: {SSHA}WixBYpdCo4bEZPRPwUriImctcWZ9sDgQQ/WElg==
mail: tuanh
facsimileTelephoneNumber: 5426
entryUUID: bc95b0ee-6e3e-480d-83c1-2c1e13c89dc9
createTimestamp: 20100326001110Z
creatorsName: cn=Directory Manager,cn=Root DNs,cn=config
pwdChangedTime: 20100326001110.323Z

```

- Một **entry** là tập hợp của các thuộc tính, từng thuộc tính này mô tả một nét đặt trưng tiêu biểu của một đối tượng. Một entry bao gồm nhiều dòng :
 - **dn** : distinguished name - là tên của entry thư mục, tất cả được viết trên một dòng.
 - Sau đó lần lượt là các thuộc tính của entry, thuộc tính dùng để lưu giữ dữ liệu. Mỗi thuộc tính trên một dòng theo định dạng là " kiểu thuộc tính : giá trị thuộc tính".
 - Thứ tự các thuộc tính không quan trọng, tuy nhiên để dễ đọc được thông tin chúng ta nên đặt các giá trị objectclass trước tiên và nên làm sao cho các giá trị của các thuộc tính cùng kiểu ở gần nhau.
- Một số các thuộc tính cơ bản trong file Ldif:

STT	Tên	Mô tả
1	dn	Distinguished Name : tên gọi phân biệt
2	c	country – 2 kí tự viết tắt tên của một nước
3	o	organization – tổ chức
4	ou	organization unit – đơn vị tổ chức

STT	Tên	Mô tả
5	objectClass	Mỗi giá trị objectClass hoạt động như một khuôn mẫu cho các dữ liệu được lưu giữ trong một entry. Nó định nghĩa một bộ các thuộc tính phải được trình bày trong entry (Ví dụ : entry này có giá trị của thuộc tính objectClass là eperson, mà trong eperson có quy định cần có các thuộc tính là tên, email, uid ,...thì entry này sẽ có các thuộc tính đó), còn bộ các thuộc tính tùy chọn có thể có hoặc có thể không có mặt.
6	givenName	tên
7	uid	id người dùng
8	cn	common name – tên thường gọi (thường là givenName + sn)
9	telephoneNumber	số điện thoại
10	sn	surename – họ
11	userPassword	mật khẩu người dùng
12	mail	địa chỉ email
13	facsimileTelephoneNumber	số fax
14	createTimestamp	thời gian tạo ra entry này
15	creatorsName	tên người tạo ra entry này
16	pwdChangedTime	thời gian thay đổi mật khẩu
17	entryUUID	id của entry
18	description	mô tả người dùng
19	dc	Domain component – Một thành phần của domain

2.2 ♦ Mô hình LDAP

LDAP còn định nghĩa ra bốn mô hình, các mô hình này cho phép linh động trong việc sắp đặt các thư mục:

- Mô hình **LDAP** information - xác định cấu trúc và đặc điểm của thông tin trong thư mục.
- Mô hình **LDAP** Naming - xác định cách các thông tin được tham chiếu và tổ chức.

- Mô hình **LDAP** Functional - định nghĩa cách mà bạn truy cập và cập nhật thông tin trong thư mục của bạn.
- Mô hình **LDAP** Security - định nghĩa ra cách thông tin trong thư mục của bạn được bảo vệ tránh các truy cập không được phép.

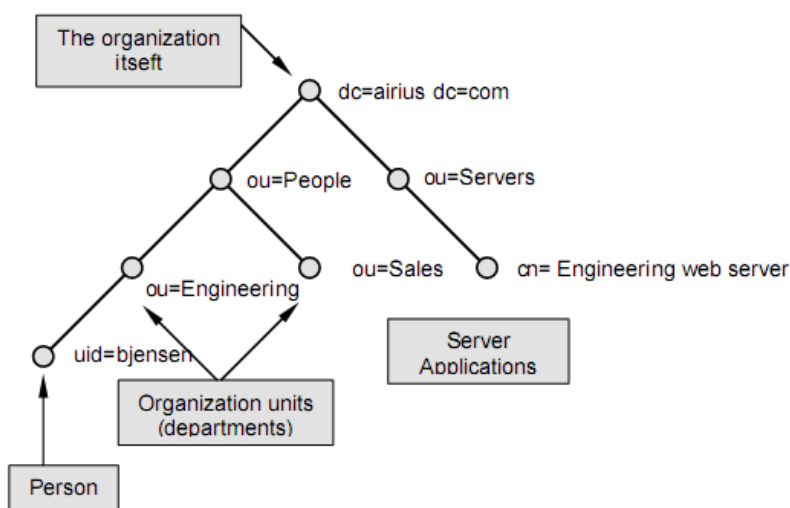
2.2.1 Mô hình thông tin Ldap (LDAP information model)

Khái niệm

- Mô hình LDAP Information định nghĩa ra các kiểu của dữ liệu và các thành phần thông tin cơ bản mà bạn có thể chứa trong thư mục. Hay nó mô tả cách xây dựng ra các khối dữ liệu mà chúng ta có thể sử dụng để tạo ra thư mục.

Mô hình thông tin Ldap

- Thành phần cơ bản của thông tin trong một thư mục gọi là **entry**. Đây là tập hợp chứa các thông tin về đối tượng (Object).



Hình 7. Một cây thư mục với các entry là các thành phần cơ bản

Attribute type	Attribute values
cn :	Barbara jensen Bads jensen
sn :	jensen
telephone number :	+1 408 555 1212
mail :	bads@arius.com

Hình 8. Một entry với các thuộc tính cơ bản

- Thông tin mô tả dữ liệu được lưu trữ theo cấu trúc trong tập tin *.ldif. Cấu trúc file Ldif đã được giới thiệu ở phần trên.

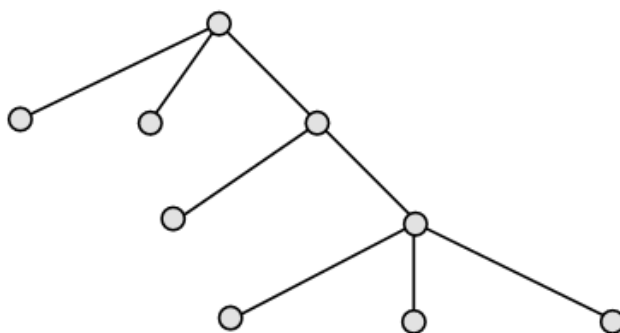
2.2.2 Mô hình đặt tên Ldap (LDAP naming model)

Khái niệm

- Mô hình LDAP Naming định nghĩa ra cách để chúng ta có thể sắp xếp và tham chiếu đến dữ liệu của mình.
- Hay có thể nói mô hình này mô tả cách sắp xếp các entry vào một cấu trúc có logic, và mô hình LDAP Naming chỉ ra cách để chúng ta có thể tham chiếu đến bất kỳ một entry thư mục nào nằm trong cấu trúc đó.
- Mô hình LDAP Naming cho phép chúng ta có thể đặt dữ liệu vào thư mục theo cách mà chúng ta có thể dễ dàng quản lý nhất.

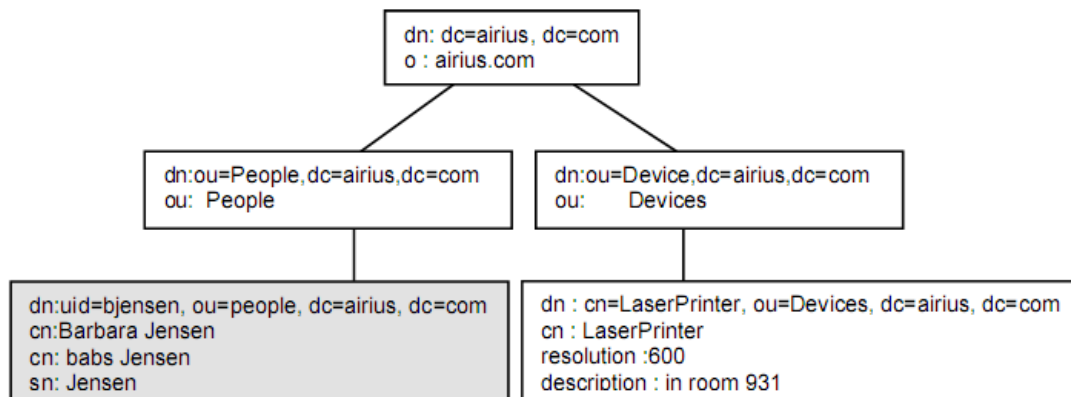
Cách sắp xếp dữ liệu

- Ví dụ như chúng ta có thể tạo ra một container chứa tất cả các entry mô tả người trong một tổ chức(o), và một container chứa tất cả các group của bạn, hoặc bạn có thể thiết kế entry theo mô hình phân cấp theo cấu trúc tổ chức của bạn. Việc thiết kế tốt cần phải có những nghiên cứu thoả đáng.



Hình 9. Một cây thư mục LDAP

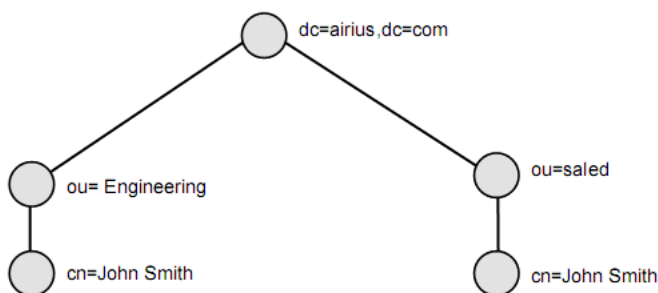
- Ta có thể thấy rằng entry trong thư mục có thể đồng thời là tập tin và là thư mục.



Hình 10. Một phần thư mục LDAP với các entry chứa thông tin

- Giống như đường dẫn của hệ thống tập tin, tên của một entry **LDAP** được hình thành bằng cách nối tất cả các tên của từng entry cấp trên (cha) cho đến khi trở lên root.
- Như hình trên ta thấy node có màu đậm sẽ có tên là `uid=bjensen, ou=people, dc=airius, dc=com`, nếu chúng ta đi từ trái sang phải thì chúng ta có thể quay ngược lại đỉnh của cây, chúng ta thấy rằng các thành phần riêng lẻ của cây được phân cách bởi dấu “,”.

- Với bất kỳ một **DN**, thành phần trái nhất được gọi là relative distinguished name (**RDN**), như đã nói **DN** là tên duy nhất cho mỗi entry trên thư mục, do đó các **entry** có cùng cha thì **RDN** cũng phải phân biệt.

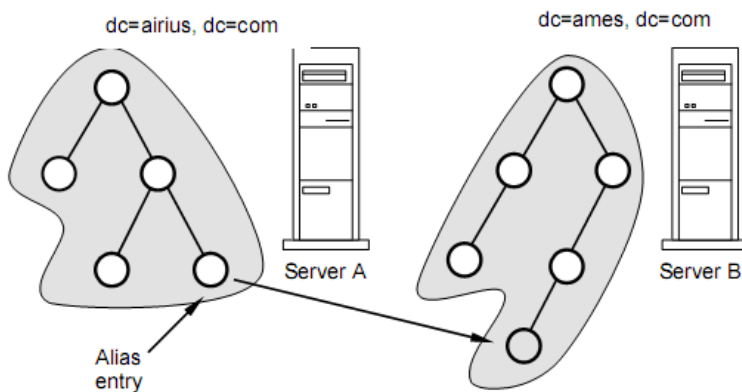


Hình 11.

- Ví dụ như hình trên, mặc dù hai entry có cùng RDN **cn=John Smith** nhưng hai entry ở hai nhánh khác nhau.

Bí danh (Aliases) – cách tham chiếu đến dữ liệu

- Những entry bí danh (Aliases entry) trong thư mục **LDAP** cho phép một entry chỉ đến một entry khác.
- Chúng ta có thể xây dựng ra cấu trúc mà thứ bậc không còn chính xác nữa, khái niệm Aliases entry giống như khái niệm symbolic links trong **UNIX** hay shortcuts trên **Windows9x/NT**.
- Để tạo ra một alias entry trong thư mục trước tiên bạn phải tạo ra một entry với tên thuộc tính là *aliasedObjectName* với giá trị thuộc tính là **DN** của entry mà chúng ta muốn alias entry này chỉ đến.
- Hình dưới đây cho ta thấy được một aliases entry trỏ đến một **entry** thật sự.



Hình 12. LDAP với Alias entry

- Nhưng không phải tất cả các LDAP Directory Server đều hỗ trợ Aliases. Bởi vì một alias entry có thể chỉ đến bất kỳ một entry nào, kể cả các entry LDAP server khác. Và việc tìm kiếm khi gặp phải một bí danh có thể phải thực hiện tìm kiếm trên một cây thư mục khác nằm trên các server khác, do đó làm tăng chi phí cho việc tìm kiếm, đó là lý do chính mà các phần mềm không hỗ trợ alias.

2.2.3 Mô hình chức năng Ldap (LDAP function model)

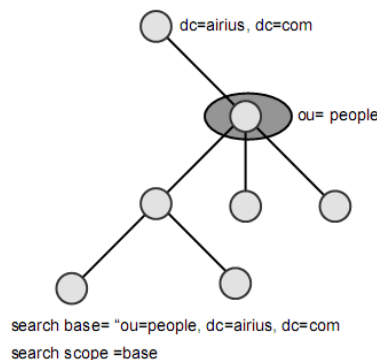
Khái niệm

- Đây là mô hình mô tả các thao tác cho phép chúng ta có thể thao tác trên thư mục.
- Mô hình LDAP Functional chứa một tập các thao tác chia thành 3 nhóm:
 - Thao tác thăm tra (interrogation) cho phép bạn có thể search trên thư mục và nhận dữ liệu từ thư mục.
 - Thao tác cập nhật (update): add, delete, rename và thay đổi các entry thư mục.
 - Thao tác xác thực và điều khiển (authentication and control) cho phép client xác định mình đến chỗ thư mục và điều khiển các hoạt động của phiên kết nối.
- Với version 3 nghi thức LDAP ngoài 3 nhóm thao tác trên, còn có thao tác LDAP extended, thao tác này cho phép nghi thức LDAP sau này có thể mở rộng một cách có tổ chức và không làm thay đổi đến nghi thức.

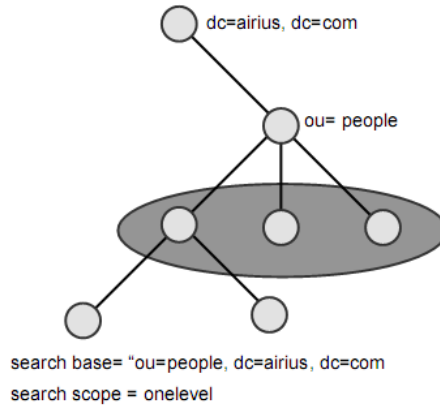
Mô tả các thao tác

1. Thao tác thăm tra (LDAP Interrogation)

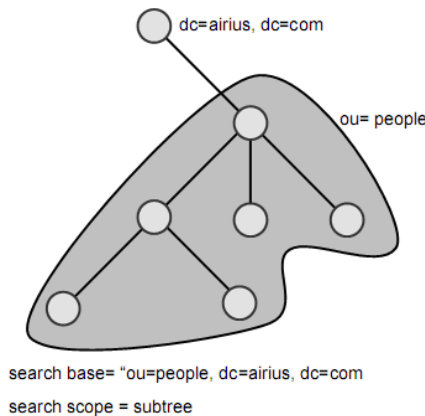
- Cho phép client có thể tìm và nhận lại thông tin từ thư mục.
- Thao tác tìm kiếm (LDAP search operation) yêu cầu 8 tham số (Ví dụ: search ("o=people,dc=airius,dc=com","base","derefInSearching",10,60,Filter,ArrayAttribute))
 - **Tham số đầu tiên** là đối tượng cơ sở mà các thao tác tìm kiếm thực hiện trên đó, tham số này là DN chỉ đến đỉnh của cây mà chúng ta muốn tìm.
 - **Tham số thứ hai** là phạm vi cho việc tìm kiếm, chúng ta có 3 phạm vi thực hiện tìm kiếm:
 - Phạm vi "base" chỉ ra rằng bạn muốn tìm ngay tại đối tượng cơ sở.
 - Phạm vi "onelevel" thao tác tìm kiếm diễn ra tại cấp dưới (con trực tiếp của đối tượng cơ sở)
 - Phạm vi "subtree" thao tác này thực hiện tìm hết trên cây mà đối tượng cơ sở là đỉnh.



Hình 13. Thao tác tìm kiếm với phạm vi base



Hình 14. Thao tác tìm kiếm với phạm vi onellevel



Hình 15. Thao tác tìm kiếm với phạm vi subtree

- **Tham số thứ ba** `derefAliases`, cho server biết rằng liệu bí danh aliases có bị bỏ qua hay không khi thực hiện tìm kiếm, có 4 giá trị mà `derefAliases` có thể nhận được:
 - `noverDerefAliases` - thực hiện tìm kiếm và không bỏ qua bí danh (aliases) trong lúc thực hiện tìm kiếm và áp dụng với cả đối tượng cơ sở.
 - `derefInsearching` - bỏ qua các aliases trong trong các entry cấp dưới của đối tượng cơ sở, và không quan tâm đến thuộc tính của đối tượng cơ sở.
 - `derefFindingBaseObject` - tìm kiếm sẽ bỏ qua các aliases của đối tượng cơ sở, và không quan tâm đến thuộc tính của các entry thấp hơn đối tượng cơ sở.
 - `derfAlways` - bỏ qua cả hai nếu việc tìm kiếm thấy đối tượng cơ sở hay là các entry cấp thấp là các entry aliases.
- **Tham số thứ bốn** cho server biết có tối đa bao nhiêu entry kết quả được trả về.
- **Tham số thứ năm** qui định thời gian tối đa cho việc thực hiện tìm kiếm.
- **Tham số thứ sáu:** `attrOnly` – là tham số kiểu bool, nếu được thiết lập là true, thì server chỉ gọi các kiểu thuộc tính của entry cho client, nhưng sever không gọi giá trị của các thuộc tính đi, điều này là cần thiết nếu như client chỉ quan tâm đến các kiểu thuộc tính chứa trong.

- **Tham số thứ bảy** là bộ lọc tìm kiếm(search filter) đây là một biểu thức mô tả các loại entry sẽ được giữ lại.
- **Tham số thứ tám**: danh sách các thuộc tính được giữ lại với mỗi entry.

2. Thao tác cập nhật (update)

Chúng ta có 4 thao tác cập nhật đó là add, delete, rename(modify DN), và modify

- Add
- Delete
- Rename
- Update

3. Thao tác xác thực và điều khiển (authentication and control)

Thao tác xác thực gồm: thao tác bind và unbind:

- Bind : cho phép client tự xác định được mình với thư mục, thao tác này cung cấp sự xác nhận và xác thực chứng thực
- Unbind : cho phép client huỷ bỏ phân đoạn làm việc hiện hành

Thao tác điều khiển chỉ có abandon:

- Abandon : cho phép client chỉ ra các thao tác mà kết quả client không còn quan tâm đến nữa.

4. Các thao tác mở rộng

Ngoài 9 thao tác cơ bản, LDAP version 3 được thiết kế mở rộng thông qua 3 thao tác :

- Thao tác mở rộng LDAP (LDAP extended operations)
 - Đây là một nghi thức thao tác mới. Trong tương lai nếu cần một thao tác mới, thì thao tác này có thể định nghĩa và trở thành chuẩn mà không yêu cầu ta phải xây dựng lại các thành phần cốt lõi của LDAP.
 - Ví dụ một thao tác mở rộng là StartTLS, nghĩa là báo cho sever rằng client muốn sử dụng transport layer security(TLS) để mã hoá và tùy chọn cách xác thực khi kết nối.
- LDAP control
 - Là những phần của thông tin kèm theo cùng với các thao tác LDAP, thay đổi hành vi của thao tác trên cùng một đối tượng.
- Xác thực đơn giản và tầng bảo mật (Simple Authentication and Security Layer SASL)
 - Là một mô hình hỗ trợ cho nhiều phương thức xác thực.
 - Bằng cách sử dụng mô hình SASL để thực hiện chứng thực, LDAP có thể dễ dàng thích nghi với các phương thức xác thực mới khác.
 - SASL còn hỗ trợ một mô hình cho client và server có thể đàm phán trên hệ thống bảo mật diễn ra ở các tầng thấp (dẫn đến độ an toàn cao).

2.2.4 Mô hình bảo mật Ldap (LDAP Security model)

- Vấn đề cuối cùng trong các mô hình LDAP là việc bảo vệ thông tin trong thư mục khỏi các truy cập không được phép.

- Khi thực hiện thao tác bind dưới một tên DN hay một người vô danh thì với mỗi user có một số quyền thao tác trên thư mục entry. Và những quyền nào được entry chấp nhận tất cả những điều trên gọi là truy cập điều khiển (access control).
- Hiện nay LDAP chưa định nghĩa ra một mô hình Access Control, các điều kiện truy cập này được thiết lập bởi các nhà quản trị hệ thống bằng các server software.

2.3 Chứng thực trong LDAP

- Việc xác thực trong một thư mục LDAP là một điều cần thiết và không thể thiếu. Các quá trình xác thực được sử dụng để thiết lập các quyền của khách hàng cho mỗi lần sử dụng.
- Tất cả các công việc như tìm kiếm, truy vấn, vv... được sự kiểm soát bởi các mức ủy quyền của người được xác thực.
- Khi xác nhận một người dùng của LDAP cần tên người dùng được xác định như là một DN (ví dụ cn = tuanh, o = it, dc = nlu, dc = info) và mật khẩu tương ứng với DN đó.

Một số phương thức xác thực người dùng

- Xác thực người dùng chưa xác định (Anonymous Authentication)
 - Xác thực người dùng chưa xác định là một xử lý ràng buộc đăng nhập vào thư mục với một tên đăng nhập và mật khẩu là rỗng. Cách đăng nhập này rất thông dụng và được thường xuyên sử dụng đối với ứng dụng client.
- Xác thực người dùng đơn giản (Simple Authntication)
 - Đối với xác thực người dùng đơn giản, tên đăng nhập trong DN được gửi kèm cùng với một mật khẩu dưới dạng clear text tới máy chủ LDAP.
 - Máy chủ sẽ so sánh mật khẩu với giá trị thuộc tính userPassword hoặc với những giá trị thuộc tính đã được định nghĩa trước trong entry cho DN đó.
 - Nếu mật khẩu được lưu dưới dạng bị băm(mã hoá), máy chủ sẽ sử dụng hàm băm tương ứng để biến đổi mật khẩu đưa vào và so sánh với giá trị đó với giá trị mật khẩu đã mã hoá từ trước.
 - Nếu cả hai mật khẩu trùng nhau, việc xác thực client sẽ thành công.
- Xác thực đơn giản qua SSL/TLS
 - Nếu việc gửi username và mật khẩu của bạn qua mạng khiến bạn không cảm thấy yên tâm về tính bảo mật, sẽ là an toàn hơn khi truyền thông tin trong một lớp truyền tải được mã hóa.
 - LDAP sẽ vượt qua lớp truyền tải đã được mã hóa này trước khi thực hiện bất cứ hoạt động kết nối nào. Do đó, tất cả thông tin người dùng sẽ được đảm bảo an toàn (ít nhất là trong suốt session đó)
 - Có hai cách sử dụng SSL/TSL với LDAPv3

1. LDAP với SSL

- LDAP với SSL (LDAPs-tcp/636) được hỗ trợ bởi rất nhiều bởi các máy chủ LDAP (cả phiên bản thương mại và mã nguồn mở). Mặc dù được sử dụng thường xuyên, nó vẫn không chấp nhận quá trình mở rộng LDAP với StartTLS.
- *SSL sử dụng một lớp chương trình nằm giữa các lớp của Internet Hypertext Transfer Protocol (HTTP) và Transport Control Protocol (TCP).*

- Trong điều khoản của layman, dữ liệu được mã hóa trong trình duyệt web của người dùng, sử dụng một khóa mật mã mà thuộc về trang web.
- Dữ liệu được chuyển từ trình duyệt web vào trang web ở định dạng đã được mã hóa. Điều này đảm bảo rằng thông tin cá nhân của người sử dụng không được chuyển giao trong định dạng có thể đọc được cho bất cứ ai để nắm bắt và đọc khi nó truyền trên Internet.

2. LDAP với TLS

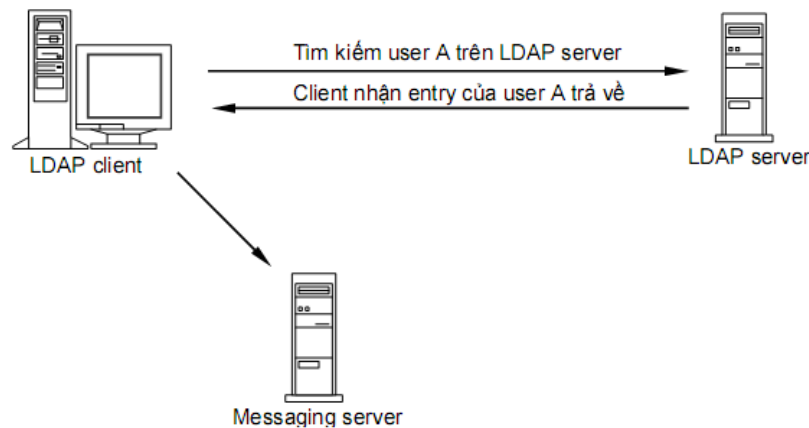
- RFC 2830 đưa ra một phương thức mở rộng đối với LDAPv3 cho việc xử lý TLS qua cổng tiêu chuẩn tcp/389.
- Phương thức này được biết đến như là một StartTLS, giúp cho máy chủ có thể hỗ trợ các việc mã hóa và giải mã các phiên giao dịch trên cùng một cổng.
- Khi máy chủ và máy khách giao tiếp, TLS đảm bảo rằng không có bên thứ ba có thể nghe trộm hoặc giả mạo tin nhắn bất kỳ.
- TLS cho phép các máy chủ và khách hàng để xác thực lẫn nhau và để thương lượng một thuật toán mã hóa và khóa mã hóa trước khi dữ liệu được trao đổi.
- TLS là sự kế thừa của Secure Sockets Layer (SSL), và dựa trên công nghệ đó. Bằng cách này, có thể nói rằng SSL đã phát triển thành các giao thức TLS.

2.4 Một số dịch vụ sử dụng nghi thức LDAP

Bằng cách kết hợp các thao tác LDAP đơn giản này. Thư mục client có thể thực hiện các thao tác phức tạp như các ví dụ sau đây.

1. Mô hình lưu trữ dữ liệu

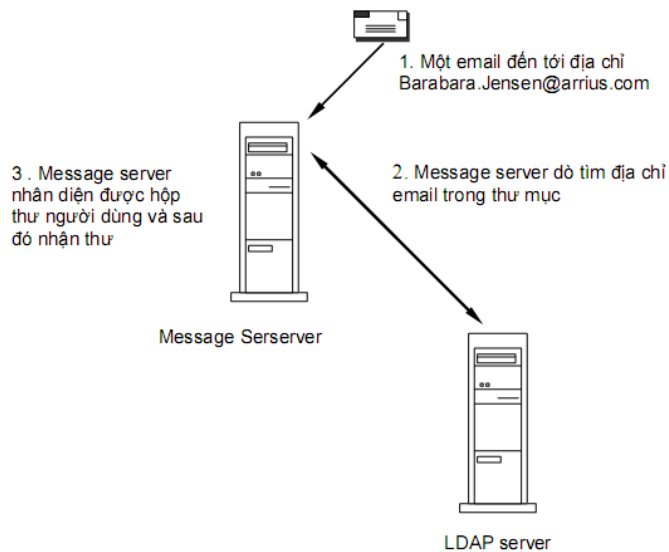
- Một chương trình mail có thể thực hiện dùng chứng chỉ điện tử chứa trong thư mục trên server LDAP để ký, bằng cách gửi yêu cầu tìm kiếm cho LDAP server.
- LDAP server gửi lại cho client chứng chỉ điện tử của nó.
- Sau đó chương trình mail dùng chứng chỉ điện tử để ký và gửi cho Message sever.
- Nhưng ở góc độ người dùng thì tất cả quá trình trên đều hoạt động một cách tự động và người dùng không phải quan tâm.



Hình 16. Một mô hình lưu trữ đơn giản

2. Quản lý thư

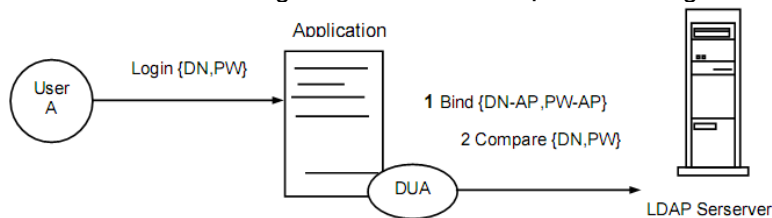
- Netscape Message server có thể sử dụng LDAP directory để thực hiện kiểm tra các mail.
- Khi một mail đến từ một địa chỉ, message server tìm kiếm địa chỉ email trong thư mục trên LDAP server lúc này Message server biết được hộp thư người sử dụng có tồn tại.



Hình 17. Dùng LDAP để quản lý thư

3. Xác thực dùng LDAP

- Dùng LDAP xác thực một user đăng nhập vào một hệ thống qua chương trình thẩm tra, chương trình thực hiện như sau :
 - Đầu tiên chương trình thẩm tra tạo ra một đại diện để xác thực với LDAP thông qua (1)
 - Sau đó so sánh mật khẩu của user A với thông tin chứa trong thư mục. Nếu so sánh thành công thì user A đã xác thực thành công.



Hình 18. Xác thực dùng LDAP

3 Áp dụng vào khoa CNTT

3.1 Xây dựng CSDL ban đầu

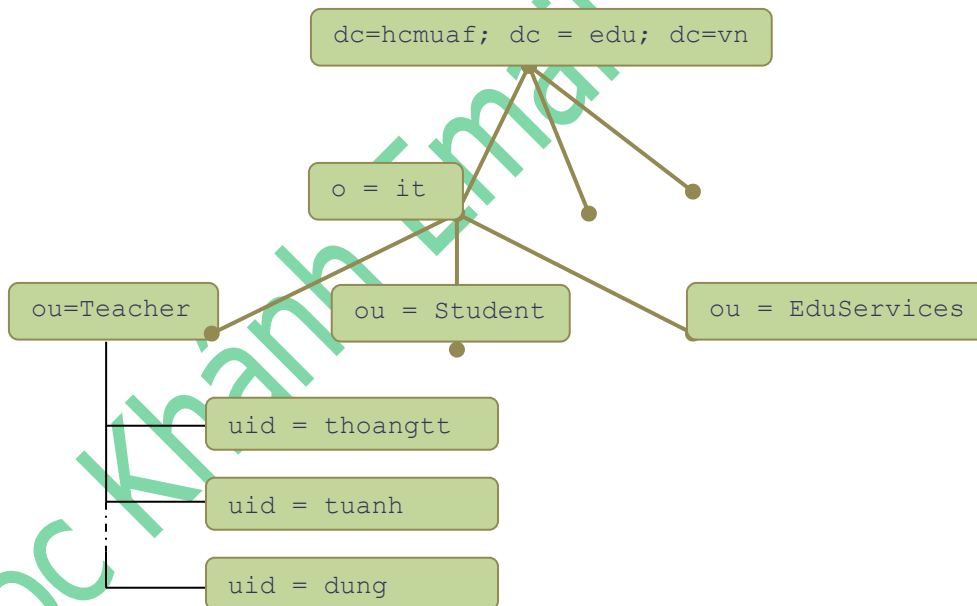
- LDAP tổ chức dữ liệu dạng cây. Do đó trong CSDL phải có một cơ sở, các nhánh, các nhánh của nhánh và các nút lá (các entries trong CSDL).
- Trong ứng dụng với khoa CNTT ta sẽ xây dựng CSDL có cấu trúc như sau:
Cơ sở (base): dc=hcmuaf, dc = edu, dc=vn

Nhánh của khoa CNTT:

```
o = it : khoa công nghệ thông tin
ou=Teacher : lưu trữ thông tin về giáo viên
ou=Student : lưu trữ thông tin về sinh viên
ou= EduServices : lưu trữ thông tin về giáo vụ khoa
```

3.2 Sơ đồ

- Với cơ sở dữ liệu có cấu trúc như trên ta có thể biểu diễn thành sơ đồ sau:



- Ứng với cơ sở và mỗi nhánh sẽ có một người có toàn quyền quản lý. Và do LDAP tổ chức dữ liệu kiểu cây cho nên người ở mức cao hơn sẽ có quyền cao hơn.

3.3 Nội dung file Ldif

- Với mô hình và cấu trúc cơ sở dữ liệu như trên, tương ứng với nội dung trong file Ldif là:

```
dn: dc=hcmuaf,dc=edu,dc=vn
objectClass: domain
objectClass: top
dc: hcmuaf
entryUUID: a1255ce5-2710-388c-95a6-3c030a59a8d3

dn: o=it,dc=hcmuaf,dc=edu,dc=vn
objectClass: top
objectClass: organization
description: information technology
o: it
entryUUID: fbc85d5-e17c-494e-a36d-5932fb503125
createTimestamp: 20100326000527Z
creatorsName: cn=Directory Manager,cn=Root DNs,cn=config

dn: ou=student,o=it,dc=hcmuaf,dc=edu,dc=vn
objectClass: organizationalUnit
objectClass: top
ou: student
entryUUID: a05481a4-f448-44a0-902f-a1f0cc6ee63f
createTimestamp: 20100326000608Z
creatorsName: cn=Directory Manager,cn=Root DNs,cn=config

dn: ou=Teacher,o=it,dc=hcmuaf,dc=edu,dc=vn
objectClass: organizationalUnit
objectClass: top
ou: Teacher
entryUUID: 675d5e04-fa4f-40fe-98fb-79fba17e2ba8
createTimestamp: 20100326000638Z
creatorsName: cn=Directory Manager,cn=Root DNs,cn=config

dn: ou=EduServices,o=it,dc=hcmuaf,dc=edu,dc=vn
objectClass: organizationalUnit
objectClass: top
ou: EduServices
entryUUID: 8150807d-d796-475d-968b-3fc1fcf231ff
createTimestamp: 20100326000705Z
creatorsName: cn=Directory Manager,cn=Root DNs,cn=config
```

- Trong phần dữ liệu ở trên thì account Directory Manager được tạo ra để quản lý toàn bộ CSDL và người dùng được tạo ra để cho phép các máy client kết nối được vào server để đọc được thông tin trong CSDL của LDAP nhằm phục vụ cho việc đăng nhập.
- Sau này thì ta sẽ dùng account Directory Manager để thay đổi, thêm vào thông tin người dùng hay account tùy theo yêu cầu.

4 Giới thiệu các LDAP server thường dùng

4.1 Bản miễn phí

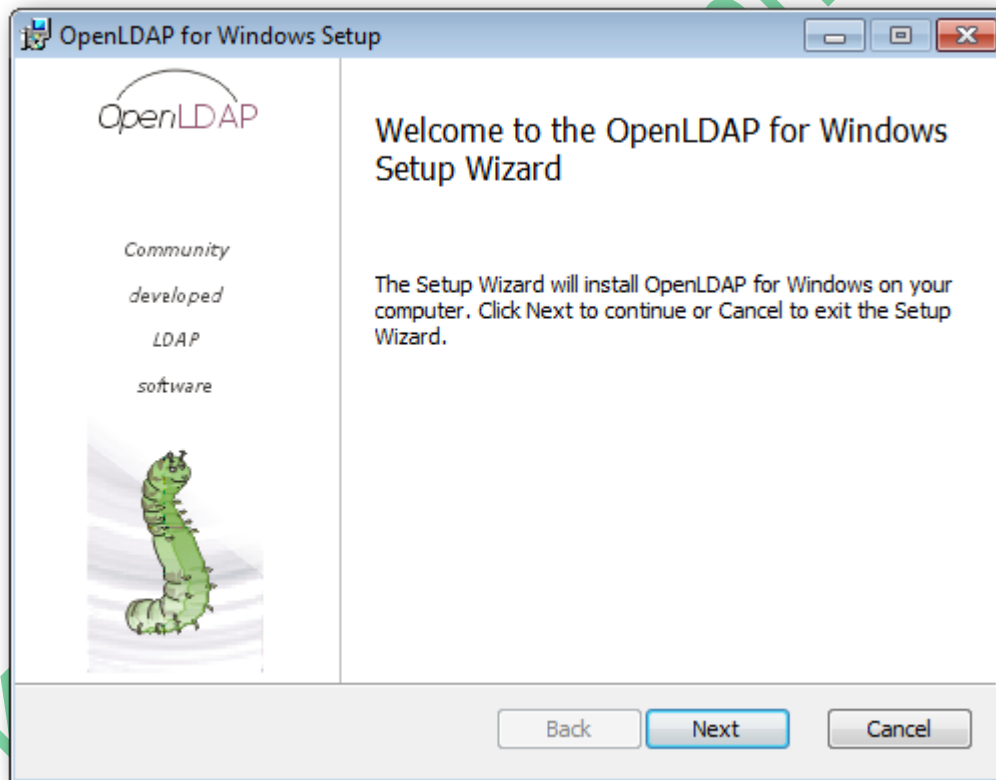
- Open LDAP
- Apache Director Server
- Open DS

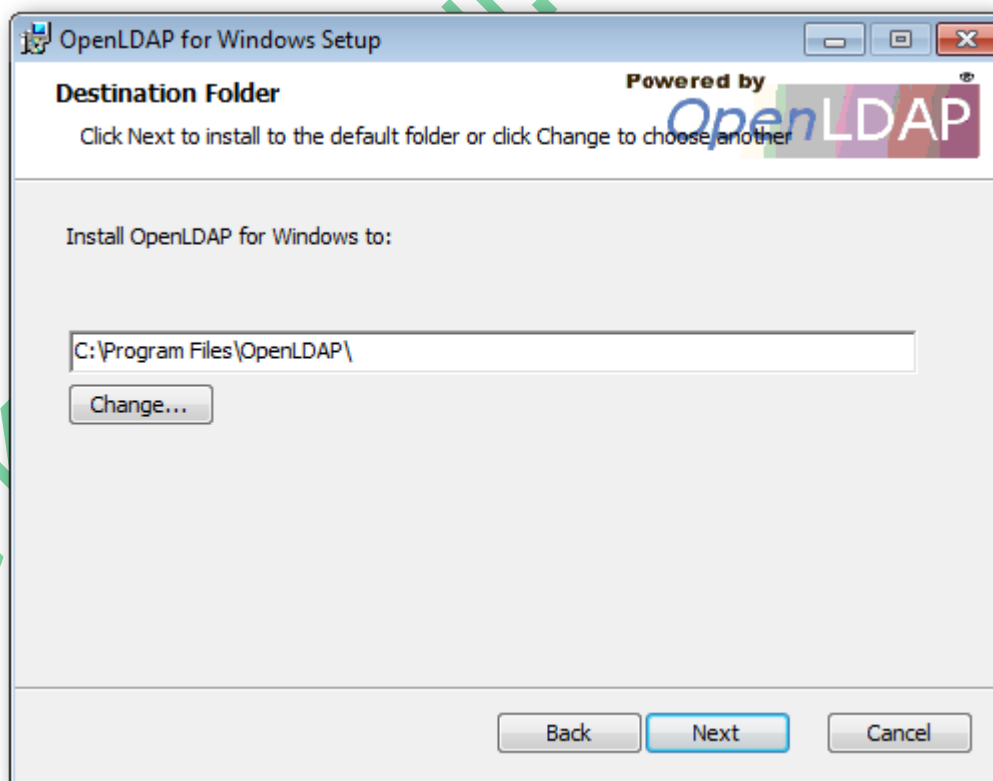
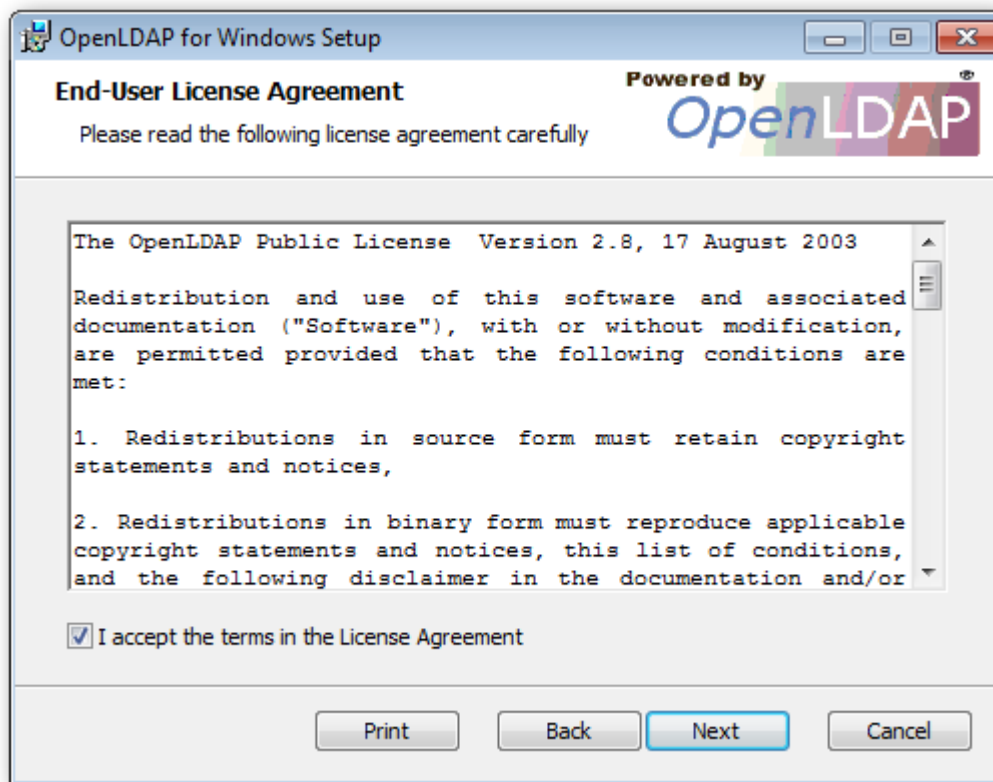
4.2 Bản thương mại

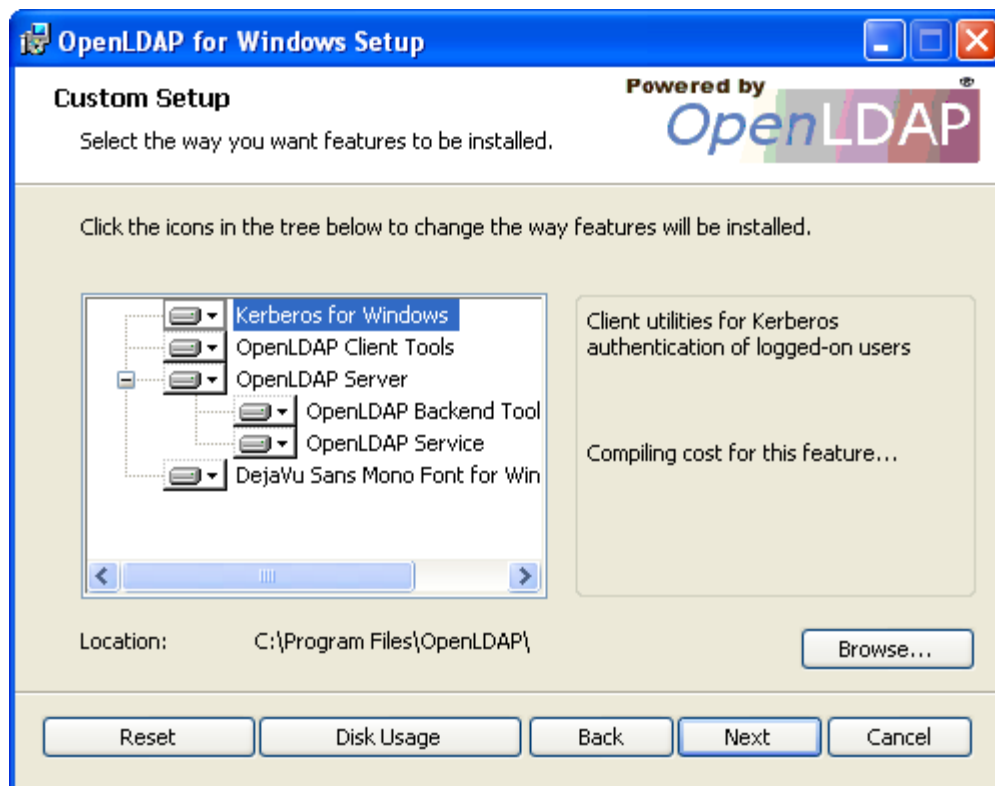
- Active Director

4.3 Cài đặt OpenLDAP và cấu hình jXplorer kết nối vào OpenLDAP

- Cài đặt OpenLDAP
- Tải về bản cài đặt cho Windows từ địa chỉ:
<http://www.userbooster.de/downloadablecontent/freeware/openldap-for-windows.msi>
- Cài đặt từ file: openldap-for-windows.msi. Mặc định chương trình sẽ được cài vào C:\Program Files\OpenLDAP.







- The below table contains the features and prerequisites and their descriptions.

Feature/Prerequisite	Optional	Description
VC Redistribution Package	No	Microsoft Visual C++ 2005 Redistributable Installer Package
OpenLDAP Client Tools	No	Command line utilities (ldapsearch, ldapcompare, ldapexop, etc.) for working with LDAP entries
OpenLDAP Server	Yes	OpenLDAP server components with different backend modules like LDIF, BDB, SQL DATABASE, etc.
BDB Backend Tools	No	Berkley Database tools
OpenLDAP Service	Yes	Configures and starts the OpenLDAP daemon
DejaVu Sans Mono Font for Windows Console	Yes	Installs a DejaVu Sans Mono font and adds it to the list of fonts available to the console. The font provides a wide range of Unicode characters.

OpenLDAP for Windows Setup

Powered by **OpenLDAP**

Additional Settings
Server Properties (optional)

The server components to be installed require a server name (IP address), a regular port and an SSL port to be assigned. You can leave or modify the default values below.

IP-Address, OpenLDAP Port and OpenLDAP SSL-Port for the OpenLDAP Backend are:

Servername / IP-Address:

Port: SSL-Port:

Back Next Cancel

OpenLDAP for Windows Setup

Powered by **OpenLDAP**

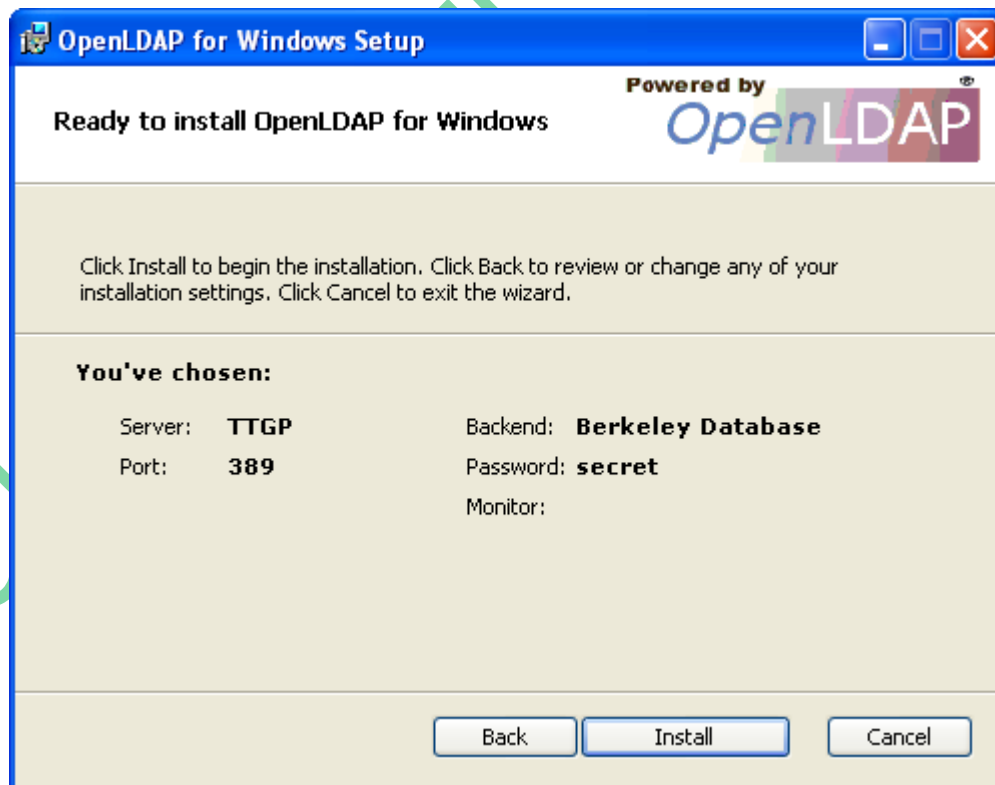
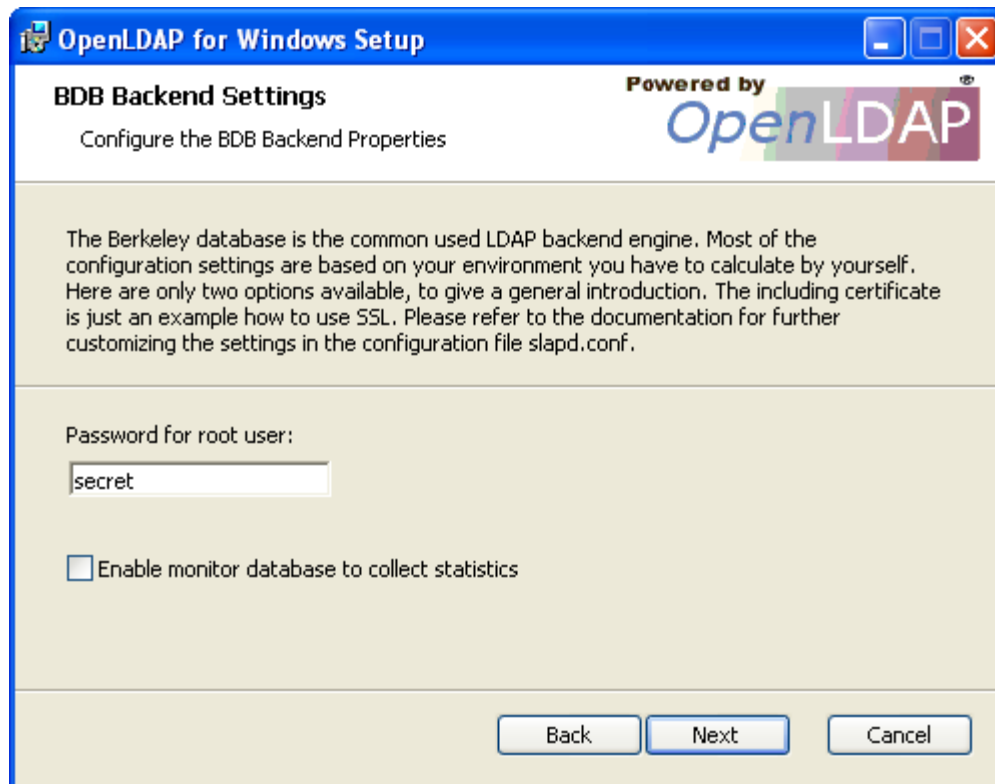
Backend Configuration
Select Backend Engine

OpenLDAP supports many backends. This package offers the most popular Berkeley Database (BDB) and the standard OpenLDAP backend (LDAP) running out of the box. Please select the desired backend and click Next to configure it.

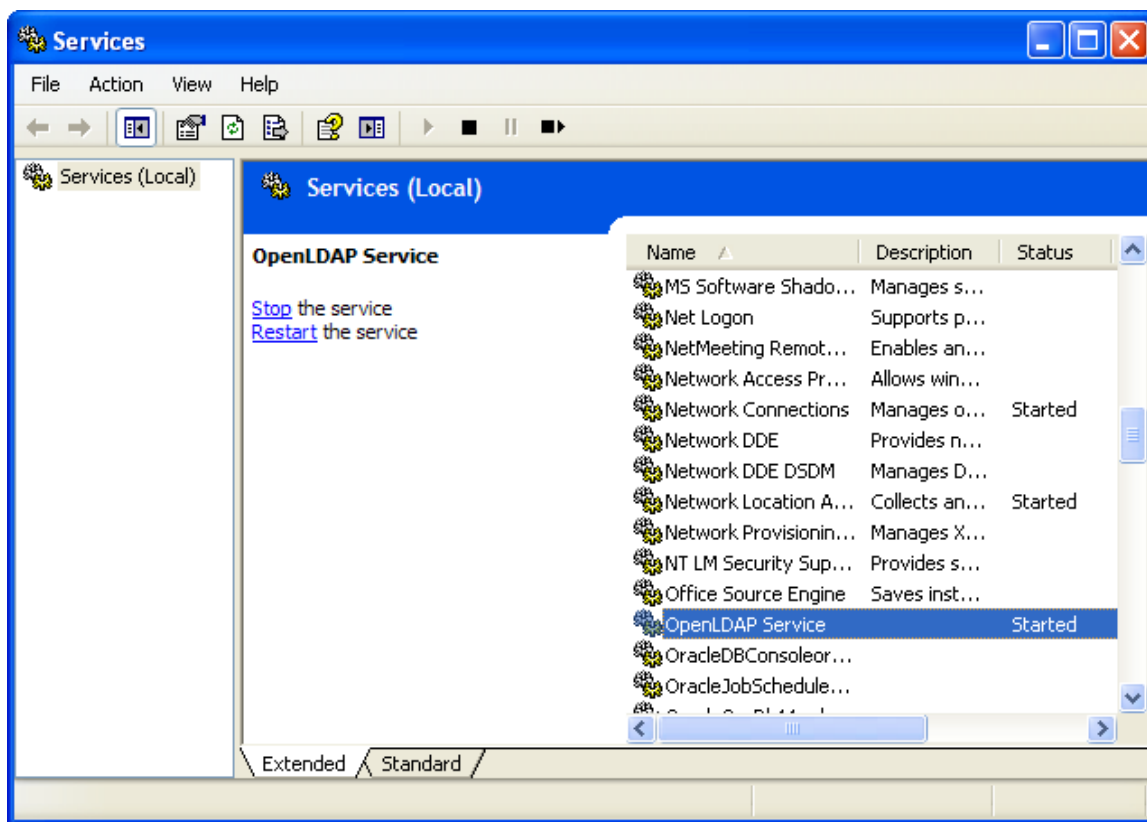
Please select Berkely Database Backend or LDAP Backend

☒ **BDB**
☐ **LDAP**

Back Next Cancel



- Để kiểm tra OpenLDAP service đã start hay chưa: (Start > Run > services.msc hoặc vào Start > Settings->Control Panel, double click Administrative Tools > Services)



- Tạo mật khẩu cho rootdn

C:\Program Files\OpenLDAP>slappasswd.exe

New password:

Re-enter new password: {SSHA}XelybaVBI/PM1O6XO0XXbMexpHEbSg1f

copy paste {SSHA}XelybaVBI/PM1O6XO0XXbMexpHEbSg1f vào slapd.conf của

rootpw

- Sau khi cài đặt vào file: C:\Program Files\OpenLDAP\slapd.conf

```
# BDB Backend configuration file
# See slapd.conf(5) for details on configuration options.
# This file should NOT be world readable.
ucdata-path      ./ucdata
include           ./schema/core.schema
include           ./schema/cosine.schema
include           ./schema/nis.schema
include           ./schema/inetorgperson.schema
include           ./schema/openldap.schema
include           ./schema/dyngroup.schema

pidfile          ./run/slapd.pid
argsfile          ./run/slapd.args

# Enable TLS if port is defined for ldaps

TLSVerifyClient  never
TLSCipherSuite   HIGH:MEDIUM:-SSLv2
TLSCertificateFile ./secure/certs/server.pem
```

```

TLSCertificateKeyFile ./secure/certs/server.pem
TLSCACertificateFile ./secure/certs/server.pem
#####
# bdb database definitions
#####

```

```

database bdb
suffix          "dc=example"
rootdn          "cn=Manager,dc=example"
# Cleartext passwords, especially for the rootdn, should
# be avoid. See slapd.conf(5) for details.
# Use of strong authentication encouraged.
rootpw         {SSHA}XelybaVBI/PMl06X00XXbMexpHEbSg1f
# The database directory MUST exist prior to running slapd AND
# should only be accessible by the slapd and slap tools.
# Mode 700 recommended.
directory      ./data
dirtyread
searchstack 20
# Indices to maintain
index mail pres,eq
index objectclass pres
index default eq,sub
index sn eq,sub,subinitial
index telephonenumber
index cn

```

- Kiểm tra server:
Stop openldap service:

```
net stop openldap-slapd
ldapsearch -x -s base (objectclass=*) namingContexts
```

 Thông báo: Can't contact LDAP server (-1)
 Start openldap service:

```
net start openldap-slapd
ldapsearch -x -s base (objectclass=*) namingContexts
```

 Cho kết quả: namingContexts=dc=example

- Tạo file C:\Program File\OpenLDAP\init.ldif

```

version: 1
dn: dc=example
objectClass: dcObject
objectClass: organization
dc: example
o: Example Company

dn: cn=0001cn,dc=example
objectClass: person
objectClass: organizationalPerson
objectClass: inetOrgPerson
objectClass: top
cn: 0001
description: No comment 1
givenName: 0001gn
mail: user01@hipt.com

```

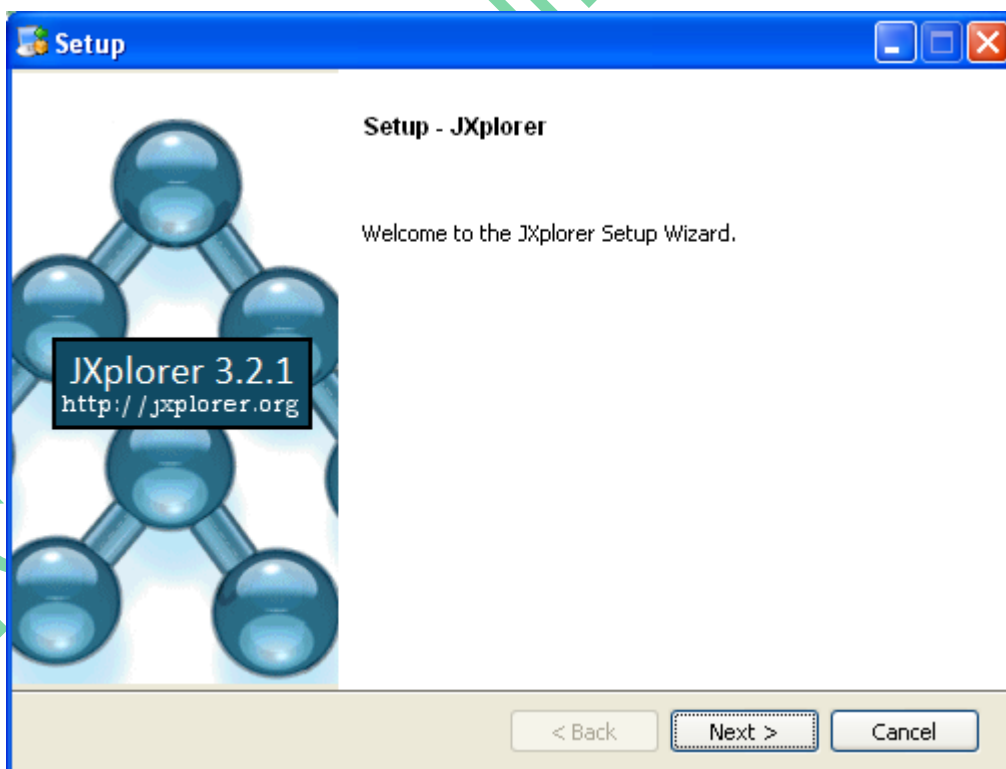
```
mobile: 0987654321  
sn: 0001sn  
uid: 0001  
userPassword: 123456
```

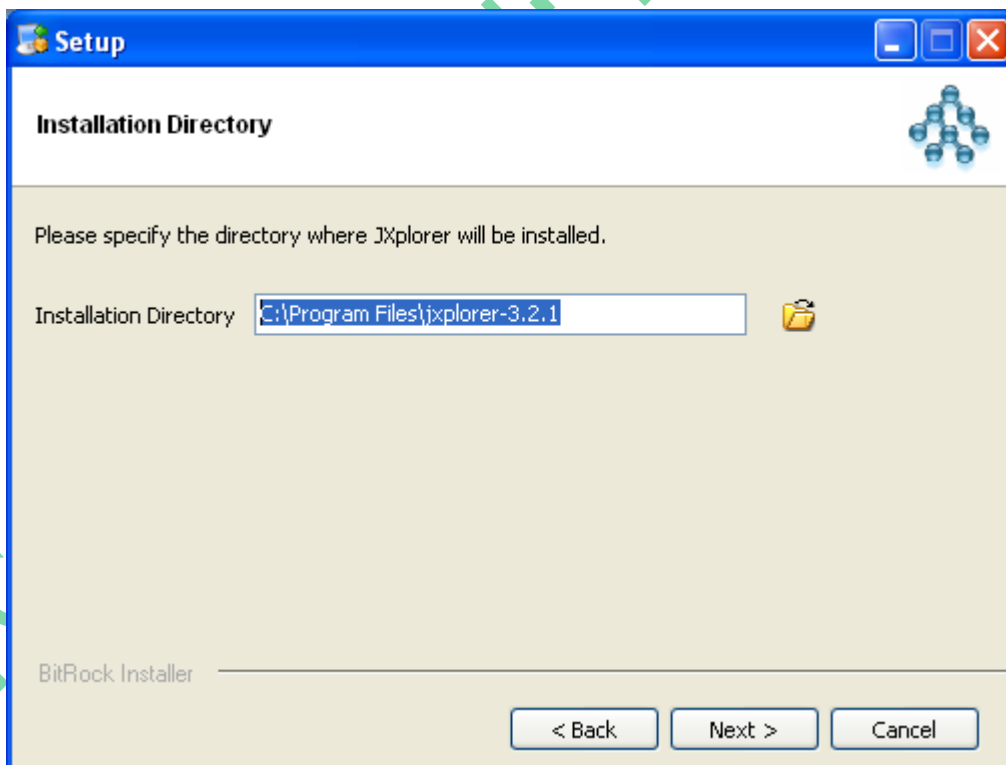
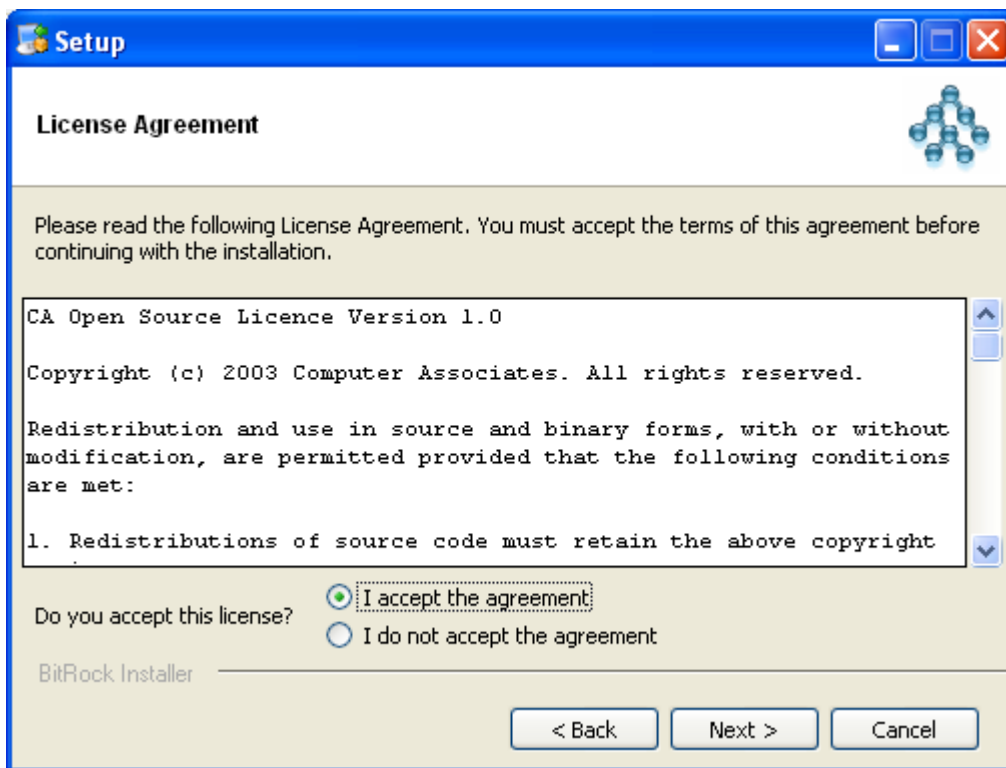
```
dn: cn=0002cn,dc=example  
objectClass: person  
objectClass: organizationalPerson  
objectClass: inetOrgPerson  
objectClass: top  
cn: 0002cn  
description: No comment 2  
givenName: 0002gn  
mail: user02@hipt.com  
sn: 0002sn  
uid: 0002  
userPassword: 123456
```

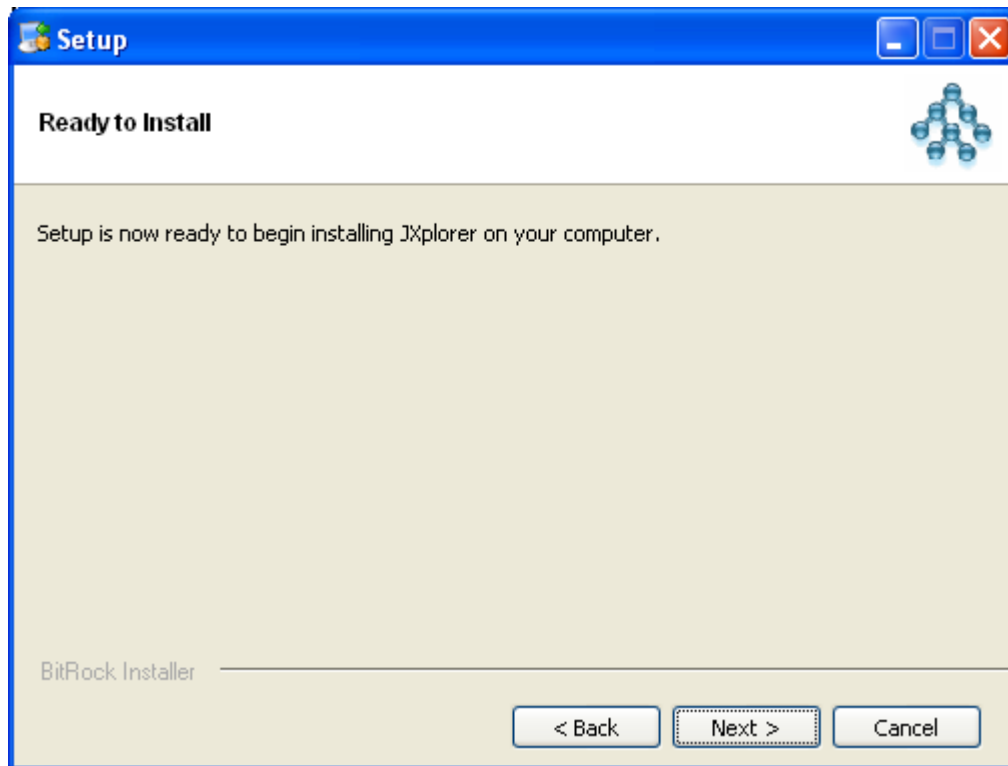
Import LDIF file vào LDAP:

```
C:\Program Files\OpenLDAP>ldapadd -H ldap://localhost:389 -x -D  
"cn=Manager,dc=example" -f init.ldif -w secret  
adding new entry dc=example  
adding new entry cn=0001cn,dc=example  
adding new entry cn=0002cn,dc=example
```

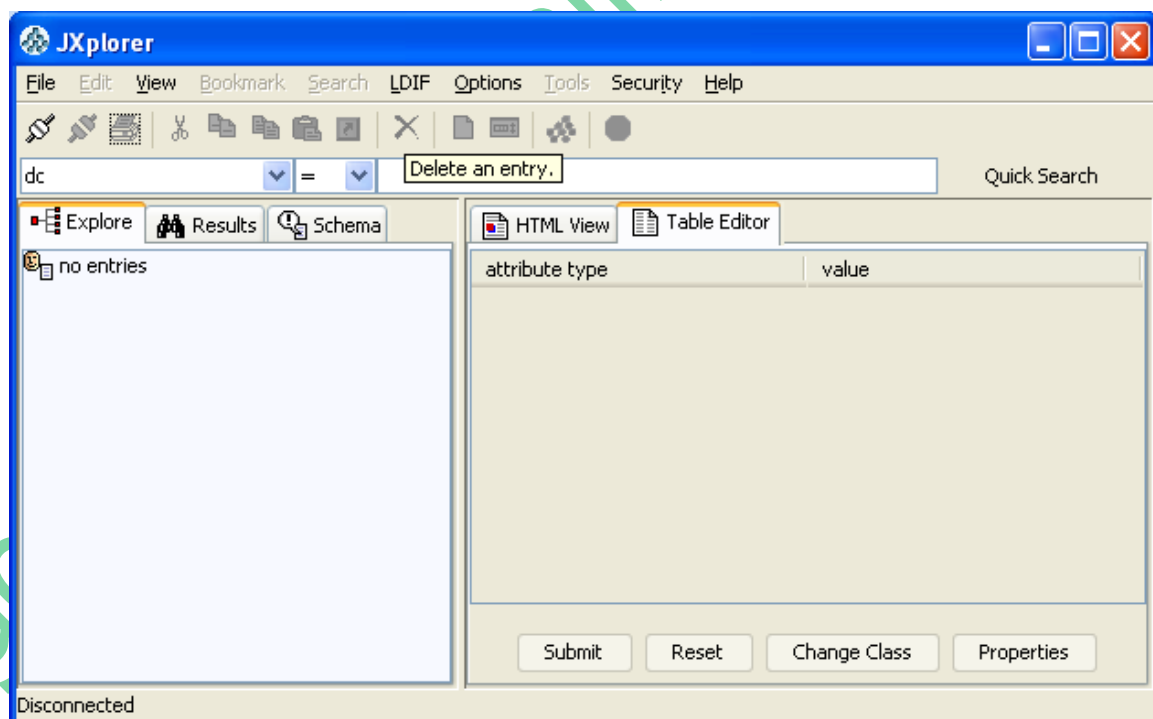
- Cài đặt jxplorer: C:\Program Files\jxplorer-3.2.1



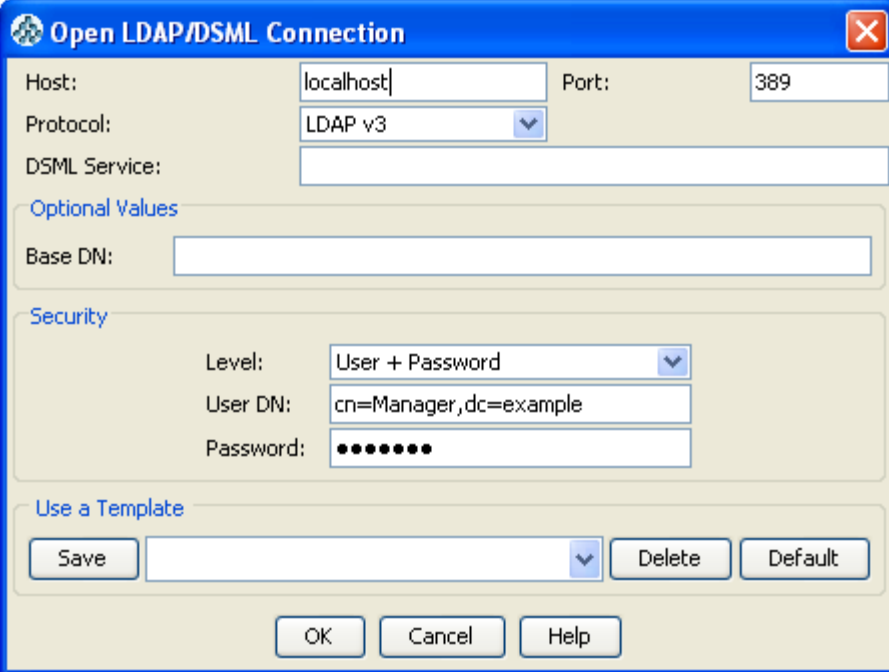




- Sau khi cài đặt, khởi động jxplorer



Chọn File > Connect:



Open LDAP/DSML Connection

Host: localhost Port: 389

Protocol: LDAP v3

DSML Service:

Optional Values

Base DN:

Security

Level: User + Password

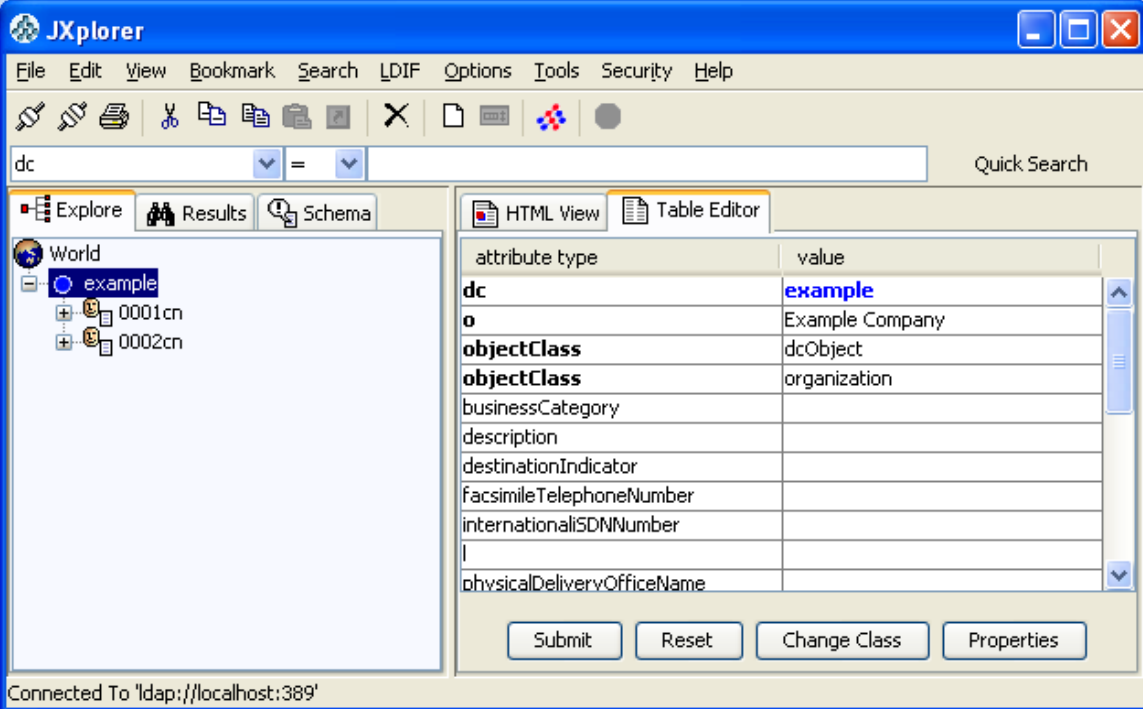
User DN: cn=Manager,dc=example

Password:

Use a Template

Save Delete Default

OK Cancel Help



JXplorer

File Edit View Bookmark Search LDIF Options Tools Security Help

dc = Quick Search

Explore Results Schema

World

- example
 - 0001cn
 - 0002cn

HTML View Table Editor

attribute type	value
dc	example
o	Example Company
objectClass	dcObject
objectClass	organization
businessCategory	
description	
destinationIndicator	
facsimileTelephoneNumber	
internationalSDNNumber	
physicalDeliveryOfficeName	

Submit Reset Change Class Properties

Connected To 'ldap://localhost:389'