



Linux và phần mềm mã nguồn mở:

TÌM HIỂU VÀ TRIỂN KHAI LDAP

Sinh viên: Nguyễn Thế Tuyển

Lớp: 59^{Th3}

MSV: 175A071418

LDAP là gì?

- **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.
- Có các LDAPServer như: OpenLDAP, OPENDS, Active Directory, ...

Chức năng cụ thể của LDAP

- Mô hình lưu trữ dữ liệu
- Quản lý thư
- Xác thực

Một số thuộc tính cơ bản trong file ldif

Tên	Mô tả
dn	Distinguished Name : tên gọi phân biệt
c	country – 2 kí tự viết tắt tên của một nước
o	organization – tổ chức
ou	organization unit – đơn vị tổ chức
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)
givenName	tên
uid	id người dùng
cn	common name – tên thường gọi

Một số thuộc tính cơ bản trong file ldif (tiếp)

Tên	Mô tả
telephoneNumber	số điện thoại
sn	surname – họ
userPassword	mật khẩu người dùng
mail	địa chỉ mail
facsimileTelephoneNumber	số phách
createTimestamp	thời điểm tạo ra entry này
creatorsName	tên người tạo ra entry này
pwdChangedTime	thời gian thay đổi mật khẩu
entryUUID	id của entry

Mô hình LDAP

- 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.

Hướng dẫn cài đặt

Bước 1: cập nhật hệ thống

```
sudo apt-get update
```

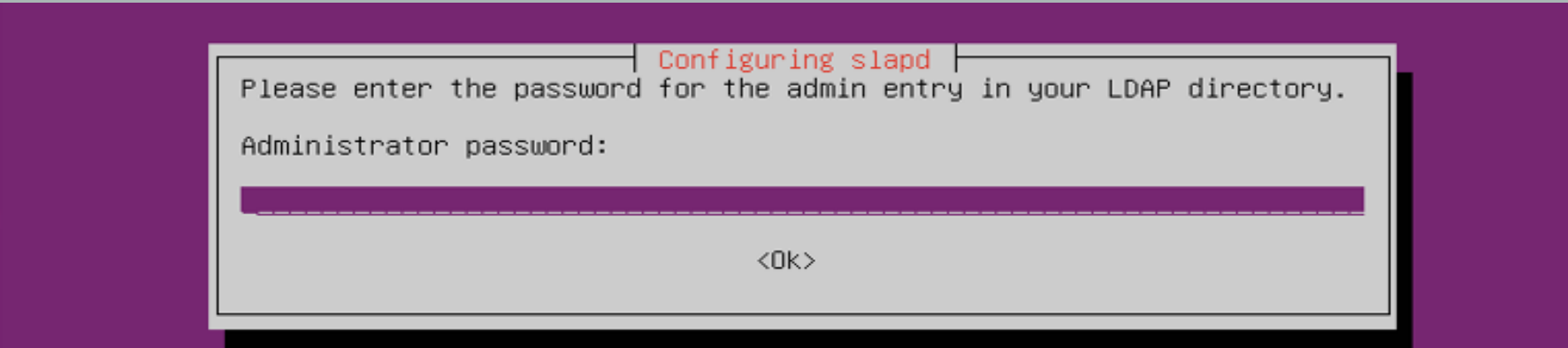
```
thetuyen@ubuntu:~$ sudo apt-get update
```

Bước 2: cài đặt LDAP

```
sudo apt-get install slapd ldap-utils
```

```
thetuyen@ubuntu:~$ sudo apt-get install slapd ldap-utils
```

Cập nhật mật khẩu cho Admin



Configuring slapd

Please enter the password for the admin entry in your LDAP directory.

Administrator password:

<Ok>

Cấu hình LDAP

Sử dụng lệnh: `sudo dpkg-reconfigure slapd`

```
nttuyen@ubuntu-ldap:~$ sudo dpkg-reconfigure slapd
```


Configuring slapd

If you enable this option, no initial configuration or database will be created for you.
Omit OpenLDAP server configuration?

<Yes>

<No>

Configuring slapd

The DNS domain name is used to construct the base DN of the LDAP directory. For example, 'foo.example.org' will create the directory with 'dc=foo, dc=example, dc=org' as base DN.

DNS domain name:

opldap.net

<Ok>

Configuring slapd

Please enter the name of the organization to use in the base DN of your LDAP directory.

Organization name:

opldap

<Ok>

Sử dụng file ldif để thêm entry

```
dn: ou=KhoaCNTT,dc=opldap,dc=net
objectClass: organizationalUnit
ou: KhoaCNTT

dn: ou=KhoaCT,dc=opldap,dc=net
objectClass: organizationalUnit
ou: KhoaCT

dn: ou=Users,dc=opldap,dc=net
objectClass: organizationalUnit
ou: Users

dn: ou=Groups,dc=opldap,dc=net
objectClass: organizationalUnit
ou: Groups

dn: cn=Students,ou=Groups,dc=opldap,dc=net
objectclass: posixGroup
cn: Students
gidNumber: 5000

dn: cn=Teachers,ou=Groups,dc=opldap,dc=net
objectclass: posixGroup
cn: Teachers
gidNumber: 2001

dn: uid=sv1,ou=Users,dc=opldap,dc=net
objectClass: inetOrgPerson
objectClass: posixAccount
objectClass: shadowAccount
uid: sv1
sn: Nguyen Van
givenName: A
cn: Nguyen Van A
displayName: Nguyen Van A
uidNumber: 3000
```

Sử dụng file ldif để thêm entry (tiếp)

Dùng lệnh `ldapadd -x -D "cn=admin,dc=opldap,dc=net" -W -f <tên file ldif>`

```
thetuyen@ubuntusv:~$ ldapadd -x -D cn=admin,dc=opldap,dc=net -W -f taodc.ldif
Enter LDAP Password:
adding new entry "ou=KhoaCNTT,dc=opldap,dc=net"

adding new entry "ou=KhoaCT,dc=opldap,dc=net"

adding new entry "ou=Users,dc=opldap,dc=net"

adding new entry "ou=Groups,dc=opldap,dc=net"

adding new entry "cn=Students,ou=Groups,dc=opldap,dc=net"

adding new entry "cn=Teachers,ou=Groups,dc=opldap,dc=net"

adding new entry "uid=sv1,ou=Users,dc=opldap,dc=net"
```

Xem kết quả bằng Ldap admin

Connection properties

Connection name: opldap

General Options Attributes

Connection:

Host: 192.168.1.77 Port: 389 Version: 3

Base: dc=opldap,dc=net Fetch DN's

☒ Simple authentication ☐ SSL ☐ TLS
☐ GSS-API ☐ SASL

Account

Username:

Password:

☒ Anonymous connection

Test connection OK Cancel

- ou=Groups
 - cn=Students
 - cn=Teachers
 - ou=KhoaCNTT
 - ou=KhoaCT
 - ou=Users
 - uid=sv1
 - cn=admin

Tìm kiếm entry

```
thetuyen@ubuntusever:~$ ldapsearch -x -LLL -b dc=opldap,dc=net "uid=sv1"
dn: uid=sv1,ou=Users,dc=opldap,dc=net
objectClass: inetOrgPerson
objectClass: posixAccount
objectClass: shadowAccount
uid: sv1
sn: Nguyen Van
givenName: A
cn: Nguyen Van A
displayName: Nguyen Van A
uidNumber: 3000
loginShell: /bin/bash
homeDirectory: /home/sv1/
gidNumber: 5000
```


Sửa thông tin entry

Tạo file chứa thông tin cần sửa

```
dn: uid=sv1,ou=Users,dc=opldap,dc=net
changetype: modify
replace: givenName
givenName: Tuyen
-
replace: cn
cn: Nguyen The Tuyen
-
replace: displayName
displayName: The Tuyen
```

Chạy file

```
thetuyen@ubuntusever:~$ ldapmodify -x -D cn=admin,dc=opldap,dc=net -W -f ch.ldif
Enter LDAP Password:
modifying entry "uid=sv1,ou=Users,dc=opldap,dc=net"
```

Sử dụng giao diện web với phpLDAPAdmin

Cài đặt phpLDAPAdmin

```
thetuyen@ubuntusv:~$ sudo apt-get install phpldapadmin
```

Sửa file config

```
thetuyen@ubuntusv:~$ sudo nano /etc/phpldapadmin/config.php
```

Đổi tên tại dòng 286

```
$servers->setValue('server','name','My LDAP Server');
```

Đổi domain tại dòng 300

```
$servers->setValue('server','base',array('dc=opldap,dc=net'));
```

Đổi tên đăng nhập mặc định tại dòng 326

```
$servers->setValue('login','bind_id','cn=admin,dc=opldap,dc=net');
```

Uncomment và đổi giá trị thành true tại dòng 161


```
$config->custom->appearance['hide_template_warning'] = true;
```

My LDAP Server

[schema](#) [search](#) [refresh](#) [info](#) [import](#) [export](#) [logout](#)

Logged in as: cn=admin

- dc=opldap,dc=net (5)
 - cn=admin
 - ou=Groups (2)
 - ou=KhoaCNTT
 - ou=KhoaCT
 - ou=Users (1)
 - Create new entry here



Use the menu to the left to navigate

[Credits](#) | [Documentation](#) | [Donate](#)

Thêm entry mới

Home | Purge caches | Show Cache

My LDAP Server

schema search refresh info import export logout

Logged in as: cn=admin

dc=opldap,dc=net (5)

cn=admin

ou=Groups (2)

ou=KhoaCNTT

ou=KhoaCT

ou=Users (1)

uid=sv1

Create new entry here

Create new entry here

ou=Users

Server: My LDAP Server Distinguished Name: ou=Users,dc=opldap,dc=net
Template: Default

Refresh

Switch Template

Copy or move this entry

Rename

Create a child entry

Hint: To delete an attribute, empty the text field and click save.

View 1 child

Hint: To view the schema for an attribute, click the attribute name.

Show internal attributes

Export

Delete this entry

Compare with another entry

Add new attribute

Export subtree

objectClass

organizationalUnit (structural)
(add value)

ou

required, rdn

Users

*
























(add value)
(rename)

Update Object

Thêm entry mới




- Chọn object

Templates:

- ☐  Courier Mail: Account
- ☐  Courier Mail: Alias
- ☐  Generic: Address Book Entry
- ☐  Generic: DNS Entry
- ☐  Generic: LDAP Alias
- ☐  Generic: Organisational Role
- ☐  Generic: Organisational Unit
- ☐  Generic: Posix Group
- ☐  Generic: Simple Security Object
- ☐  Generic: User Account
- ☐  Kolab: User Entry
- ☐  Samba: Account
- ☒  Samba: Domain
- ☐  Samba: Group Mapping
- ☐  Samba: Machine
- ☒  Sendmail: Alias
- ☒  Sendmail: Cluster
- ☒  Sendmail: Domain
- ☒  Sendmail: Relays
- ☒  Sendmail: Virtual Domain
- ☒  Sendmail: Virtual Users
- ☐  Thunderbird: Address Book Entry
- ☐  Default

Thêm entry mới

- Nhập dữ liệu

Common Name	alias, required, rdn
<input type="text" value="C Nguyen Van"/>	*
First name	alias
 <input type="text" value="C"/>	
GID Number	alias, required, hint
<input type="text" value="Teachers"/>	*
Home directory	alias, required
<input type="text" value="/home/users/Teachers"/>	*
Last name	alias, required
<input type="text" value="Nguyen Van"/>	*
Login shell	alias
 <input type="text" value="/bin/sh"/>	
Password	alias, hint
 <input type="password" value="..."/>	md5
<input type="password" value="..."/>	(confirm)

Thêm entry mới

- Xác nhận

Create LDAP Entry

Server: **My LDAP Server** Container: **ou=Users,dc=opldap,dc=net**

Do you want to create this entry?

Attribute	New Value	Skip
cn=C Nguyen Van,ou=Users,dc=opldap,dc=net		
Common Name	C Nguyen Van	<input type="checkbox"/>
First name	C	<input type="checkbox"/>
GID Number	2001	<input type="checkbox"/>
Home directory	/home/users/Teachers/chers-c	<input type="checkbox"/>
Last name	Nguyen Van	<input type="checkbox"/>
Login shell	/bin/sh	<input type="checkbox"/>
objectClass	inetOrgPerson posixAccount	<input type="checkbox"/>
Password	*****	<input type="checkbox"/>
UID Number	1000	<input type="checkbox"/>
User ID	Teachers-c	<input type="checkbox"/>

Commit

Cancel

Cấu hình ldap client để sử dụng account ldap

- Cài đặt libnss-ldap libpam-ldap ldap-utils

```
thetuyen@ubuntusv:~$ sudo apt install libnss-ldap libpam-ldap ldap-utils
```

- Nhập tên miền

Configuring ldap-auth-config

Please enter the URI of the LDAP server to use. This is a string in the form of ldap://<hostname or IP>:<port>/. ldaps:// or ldapi:// can also be used. The port number is optional.

Note: It is usually a good idea to use an IP address because it reduces risks of failure in the event name service problems.

LDAP server Uniform Resource Identifier:

ldapi:///ubuntusv.opldap.net

<Ok>

- Nhập tên phân biệt (dn)

Configuring ldap-auth-config

Please enter the distinguished name of the LDAP search base. Many sites use the components of their domain names for this purpose. For example, the domain "example.net" would use "dc=example,dc=net" as the distinguished name of the search base.

Distinguished name of the search base:

dc=opldap,dc=net

<Ok>

- Chọn phiên bản của giao thức LDAP

Configuring ldap-auth-config

Please enter which version of the LDAP protocol should be used by ldapns. It is usually a good idea to set this to the highest available version.

LDAP version to use:

3

2

<Ok>

- Chọn cái nào bạn muốn

Configuring ldap-auth-config	
<p>This option will allow you to make password utilities that use pam to behave like you would be changing local passwords.</p> <p>The password will be stored in a separate file which will be made readable to root only.</p> <p>If you are using NFS mounted /etc or any other custom setup, you should disable this.</p> <p>Make local root Database admin:</p>	
<input checked="" type="radio"/> <Yes>	<input type="radio"/> <No>

Configuring ldap-auth-config	
<p>Choose this option if you are required to login to the database to retrieve entries.</p> <p>Note: Under a normal setup, this is not needed.</p> <p>Does the LDAP database require login?</p>	
<input type="radio"/> <Yes>	<input checked="" type="radio"/> <No>

- Xác định tài khoản admin

Configuring ldap-auth-config

This account will be used when root changes a password.

Note: This account has to be a privileged account.

LDAP account for root:

cn=admin,dc=example,dc=net

<Ok>

- Thay đổi mật khẩu tài khoản root nếu muốn (để trống nếu muốn sử dụng mật khẩu cũ)

Configuring ldap-auth-config

Please enter the password to use when ldap-auth-config tries to login to the LDAP directory using the LDAP account for root.

The password will be stored in a separate file /etc/ldap.secret which will be made readable to root only.

Entering an empty password will re-use the old password.

LDAP root account password:

<Ok>

Config

- File `/etc/nsswitch.conf`

```
thetuyen@ubuntusv:~$ sudo vi /etc/nsswitch.conf
# line 7: add
passwd:      compat systemd ldap
group:       compat systemd ldap
shadow:      compat
```

- File `/etc/pam.d/common-password`

```
thetuyen@ubuntusv:~$ sudo vi /etc/pam.d/common-password
# line 26: change ( remove [use_authok] )
password      [success=1 user_unknown=ignore default=die]      pam_ldap.so try_first_pass
```

- File `/etc/pam.d/common-session`

```
thetuyen@ubuntusv:~$ sudo vi /etc/pam.d/common-session
# add to the end if need (create home directory automatically at initial login)
session optional      pam_mkhomedir.so skel=/etc/skel umask=077
```