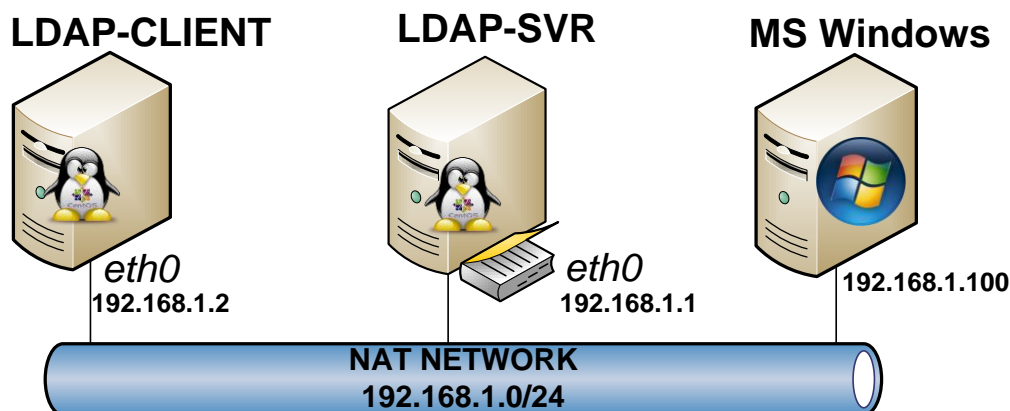


Bài thực hành

Cài đặt và cấu hình OpenLDAP - PAM

Trong bài thực hành này, bạn cần sử dụng 02 máy ảo Linux và máy thật Windows kết nối theo mô hình bên dưới



Bài thực hành này bao gồm các nội dung sau đây:

- Cài đặt và cấu hình dịch vụ LDAP trên máy LDAP-SVR sử dụng OpenLDAP.
- Tạo LDAP Domain với tên **ipmac.lab** và tạo các đối tượng quản trị (user, group...) trong domain này.
- Cài đặt công cụ quản trị LDAP Admin trên máy Windows và tìm hiểu các tính năng của công cụ này.
- Cấu hình LDAP-CLIENT để xác thực người dùng thông qua dịch vụ LDAP

I. Cài đặt và khởi tạo dịch vụ LDAP trên LDAP Server

Bước 1. [Trên LDAP Server] Cấu hình các interface trên theo mô hình trên

```
[root@LDAP-SVR]# ifconfig eth0 192.168.1.1/24 up
[root@LDAP-SVR]# service iptables stop
```

Bước 2. [Trên LDAP Server] Kiểm tra package **openldap-servers** và **openldap-clients** đã được cài đặt hay chưa. Nếu chưa cần tiến hành cài đặt package này qua **yum** hoặc **rpm**

```
[root@LDAP-SVR]# rpm -qa | grep openldap
openldap-devel-2.3.43-12.el5
openldap-2.3.43-12.el5
[root@LDAP-SVR]# yum install openldap-servers openldap-clients
[root@LDAP-SVR]# rpm -qa | grep openldap
openldap-devel-2.3.43-12.el5
openldap-clients-2.3.43-12.el5
openldap-2.3.43-12.el5
openldap-servers-2.3.43-12.el5
```

Bước 3. Mở file cấu hình tổng thể của **OpenLDAP Server** (*/etc/openldap/slapd.conf*) và xem các thông tin cấu hình chính

```
[root@LDAP-SVR]# less /etc/openldap/slapd.conf
...
#Các file schema được sử dụng mặc định
include          /etc/openldap/schema/core.schema
include          /etc/openldap/schema/cosine.schema
include          /etc/openldap/schema/inetorgperson.schema
include          /etc/openldap/schema/nis.schema
...
#####
# ldbm and/or bdb database definitions
#####
#Các thông tin về base, rootdn và manager password
database         bdb
suffix           "dc=my-domain,dc=com"
rootdn           "cn=Manager,dc=my-domain,dc=com"
# Cleartext passwords, especially for the rootdn, should
# be avoided. See slappasswd(8) and slapd.conf(5) for details.
# Use of strong authentication encouraged.
# rootpw         secret
# rootpw         {crypt}ijFYncSNctBYg

# The database directory MUST exist prior to running slapd AND
# should only be accessible by the slapd and slap tools.
# Mode 700 recommended.
directory        /var/lib/ldap

# Indices to maintain for this database
index objectClass          eq,pres
index ou,cn,mail,surname,givenname      eq,pres,sub
index uidNumber,gidNumber,loginShell    eq,pres
index uid,memberUid          eq,pres,sub
index nisMapName,nisMapEntry    eq,pres,sub
```

Bước 4. [Trên LDAP Server] Chạy lệnh **slappasswd** để sinh password dạng encrypt để quản trị OpenLDAP. Copy lại password đã được encrypt

```
[root@LDAP-SVR]# slappasswd
New password:
Re-enter new password:
{SSHA}ffhPJKASQXjwhRb0ANI9z7V0WTH+9xYA
```

Bước 5. [Trên LDAP Server] Sửa lại các dòng trong **/etc/openldap/slapd.conf** và đưa thông tin về password quản trị (sinh ra ở bước 4).

```
[root@LDAP-SVR]# vi /etc/openldap/slapd.conf
...
#####
# ldbm and/or bdb database definitions
#####

database            bdb
suffix               "dc=ipmac,dc=lab"
rootdn              "cn=Manager,dc=ipmac,dc=lab"
# Cleartext passwords, especially for the rootdn, should
# be avoided.  See slappasswd(8) and slapd.conf(5) for details.
# Use of strong authentication encouraged.
# rootpw                secret
# rootpw                {crypt}ijFYnCSNctBYg
rootpw              {SSHA}ffhPJKASQXjwhRb0ANI9z7V0WTH+9xYA

# The database directory MUST exist prior to running slapd AND
# should only be accessible by the slapd and slap tools.
# Mode 700 recommended.
directory            /var/lib/ldap

# Indices to maintain for this database
index objectClass          eq,pres
index ou,cn,mail,surname,givenname  eq,pres,sub
index uidNumber,gidNumber,loginShell eq,pres
index uid,memberUid        eq,pres,sub
index nisMapName,nisMapEntry eq,pres,sub
```

Bước 6. [Trên LDAP Server] Khởi động dịch vụ LDAP

```
[root@LDAP-SVR]# service ldap start
Checking configuration files for slapd:  config file testing succeeded
                                           [ OK ]
Starting slapd:                          [ OK ]
```

II. Tự viết file LDIF để xây dựng kiến trúc cho LDAP Server

Bước 7. [Trên LDAP Server] Soạn file */tmp/ipmac.lab.ldif* với thông tin như bên dưới.

```
[root@LDAP-SVR]# vi /tmp/ipmac.lab.ldif
dn: dc=ipmac,dc=lab
dc: ipmac
o: IPMac Lab
description: Root LDAP entry for ipmac.lab
objectClass: dcObject
objectClass: organization

dn: ou=People, dc=ipmac, dc=lab
ou: People
description: All the people in our domain
objectClass: organizationalUnit

dn: cn=testuser, ou=People, dc=ipmac, dc=lab
cn: testuser
objectClass: organizationalRole
```

Bước 8. [Trên LDAP Server] Đưa nội dung của file *ipmac.lab.ldif* vào kiến trúc của LDAP server bằng lệnh **ldapadd**

```
[root@LDAP-SVR]# ldapadd -x -D "cn=Manager,dc=ipmac,dc=lab" \
-W -f /tmp/ipmac.lab.ldif
Enter LDAP Password:
adding new entry "dc=ipmac,dc=lab"

adding new entry "ou=People, dc=ipmac, dc=lab"

adding new entry "cn=testuser, ou=People, dc=ipmac, dc=lab"
```

Bước 9. [Trên LDAP Server] Xem và tìm kiếm các nội dung vừa được import bằng lệnh **ldapsearch**

```
[root@LDAP-SVR]# ldapsearch -x -b "dc=ipmac,dc=lab" "(objectclass=*)"
Enter LDAP Password:
...
# ipmac.lab
dn: dc=ipmac,dc=lab
dc: ipmac
o: IPMac Lab
description: Root LDAP entry for ipmac.lab
objectClass: dcObject
objectClass: organization

# People, ipmac.lab
dn: ou=People,dc=ipmac,dc=lab
ou: People
description: All the people in our domain
objectClass: organizationalUnit

# testuser, People, ipmac.lab
```

```
dn: cn=testuser,ou=People,dc=ipmac,dc=lab
cn: testuser
objectClass: organizationalRole
...
[root@LDAP-SVR]# ldapsearch -x -LLL -b "dc=ipmac,dc=lab" "(cn=testuser)"
dn: cn=testuser,ou=People,dc=ipmac,dc=lab
cn: testuser
objectClass: organizationalRole
```

Bước 10. [Trên LDAP Server] Xóa user **testuser** bằng lệnh **ldapdelete**

```
[root@LDAP-SVR]# ldapdelete -x -W -D "cn=Manager,dc=ipmac,dc=lab" \
"cn=testuser,ou=People,dc=ipmac,dc=lab"
Enter LDAP Password:
[root@LDAP-SVR]# ldapsearch -x -LLL -b "dc=ipmac,dc=lab" "(cn=testuser)"
```

III. Xây dựng kiến trúc LDAP Server dựa trên thông tin có sẵn của hệ thống sử dụng các migration script

Bước 11. [Trên LDAP Server] Chuyển đến thư mục chứa các migration script (*/usr/share/openldap/migration*) và chỉnh sửa file cấu hình chung *migrate_common.ph*

```
[root@LDAP-SVR]# cd /usr/share/openldap/migration
[root@LDAP-SVR]# vi migrate_common.ph
...
# Default DNS domain
$DEFAULT_MAIL_DOMAIN = "ipmac.lab";

# Default base
$DEFAULT_BASE = "dc=ipmac,dc=lab";
...
```

Bước 12. [Trên LDAP Server] Chạy script *migrate_base.pl* để tạo file LDIF chứa thông tin về base mới. Xem nội dung file này.

```
[root@LDAP-SVR]# ./migrate_base.pl > /tmp/base.ldif
[root@LDAP-SVR]# less /tmp/base.ldif
...
```

Bước 13. [Trên LDAP Server] Đưa nội dung file *base.ldif* vào kiến trúc của LDAP bằng *ldapadd* và kiểm tra kết quả với *ldapsearch*

```
[root@LDAP-SVR]# ldapadd -c -x -D "cn=Manager,dc=ipmac,dc=lab" \
-W -f /tmp/base.ldif
Enter LDAP Password:
adding new entry "dc=ipmac,dc=lab"
ldapadd: Already exists (68)
adding new entry "ou=Hosts,dc=ipmac,dc=lab"
adding new entry "ou=Rpc,dc=ipmac,dc=lab"
adding new entry "ou=Services,dc=ipmac,dc=lab"
adding new entry "nisMapName=netgroup.byuser,dc=ipmac,dc=lab"
adding new entry "ou=Mounts,dc=ipmac,dc=lab"
adding new entry "ou=Networks,dc=ipmac,dc=lab"
adding new entry "ou=People,dc=ipmac,dc=lab"
ldapadd: Already exists (68)
adding new entry "ou=Group,dc=ipmac,dc=lab"
adding new entry "ou=Netgroup,dc=ipmac,dc=lab"
adding new entry "ou=Protocols,dc=ipmac,dc=lab"
adding new entry "ou=Aliases,dc=ipmac,dc=lab"
adding new entry "nisMapName=netgroup.byhost,dc=ipmac,dc=lab"

[root@LDAP-SVR]# ldapsearch -x -LLL -b "dc=ipmac,dc=lab" "(objectclass=*)"
...
dn: dc=ipmac,dc=lab
dc: ipmac
o: IPMac Lab
description: Root LDAP entry for ipmac.lab
objectClass: dcObject
objectClass: organization

dn: ou=People,dc=ipmac,dc=lab
```

```
ou: People
description: All the people in our domain
objectClass: organizationalUnit

dn: ou=Hosts,dc=ipmac,dc=lab
ou: Hosts
objectClass: top
objectClass: organizationalUnit
...
```

Bước 14. [Trên LDAP Server] Chạy script *migrate_passwd.pl* để tạo file LDIF chứa danh mục user cho LDAP dựa trên danh sách các user hiện có trên hệ thống (chứa trong file */etc/passwd*). Xem nội dung file LDIF .

```
[root@LDAP-SVR]# pwd
/usr/share/openldap/migration
[root@LDAP-SVR]# ./migrate_passwd.pl /etc/passwd > /tmp/allusers.ldif
[root@LDAP-SVR]# less /tmp/allusers.ldif
...
```

Bước 15. [Trên LDAP Server] Đưa nội dung file *allusers.ldif* vào kiến trúc của LDAP bằng *ldapadd* và kiểm tra kết quả với *ldapsearch*

```
[root@LDAP-SVR]# ldapadd -c -x -D "cn=Manager,dc=ipmac,dc=lab" \
-W -f /tmp/allusers.ldif
Enter LDAP Password:
adding new entry "uid=root,ou=People,dc=ipmac,dc=lab"
adding new entry "uid=bin,ou=People,dc=ipmac,dc=lab"
adding new entry "uid=daemon,ou=People,dc=ipmac,dc=lab"
...
adding new entry "uid=user,ou=People,dc=ipmac,dc=lab"
adding new entry "uid=named,ou=People,dc=ipmac,dc=lab"
adding new entry "uid=squid,ou=People,dc=ipmac,dc=lab"
adding new entry "uid=ipmac,ou=People,dc=ipmac,dc=lab"

[root@LDAP-SVR]# ldapsearch -x -LLL -b "dc=ipmac,dc=lab" "(uid=root)"
dn: uid=root,ou=People,dc=ipmac,dc=lab
uid: root
cn: root
objectClass: account
objectClass: posixAccount
objectClass: top
objectClass: shadowAccount
userPassword:: e2NyeXB0fSQxJG1Qem1jbHFOJDFxL25UMWpzRnpkYWxQYmtxdWxvNC8=
shadowLastChange: 15020
shadowMin: 0
shadowMax: 99999
shadowWarning: 7
loginShell: /bin/bash
uidNumber: 0
gidNumber: 0
homeDirectory: /root
gecos: root
```

Bước 16. [Trên LDAP Server] Tạo mới một account có tên **ldapuser** trên hệ thống và đưa account này vào LDAP.

```
#Tạo một user tên là ldapuser, thuộc nhóm users và đặt password cho user này
[root@LDAP-SVR]# useradd -g users ldapuser
[root@LDAP-SVR]# passwd ldapuser
Changing password for user ldapuser.
New UNIX password:
Retype new UNIX password:
passwd: all authentication tokens updated successfully.

#Lấy thông tin về "ldapuser" từ /etc/passwd và ghi ra /tmp/ldapuser.info
[root@LDAP-SVR]# grep "ldapuser" /etc/passwd | tee /tmp/ldapuser.info
ldapuser:x:502:100::/home/ldapuser:/bin/bash

#Kiểm tra thư mục hiện tại để đảm bảo đang ở /usr/share/openldap/migration
[root@LDAP-SVR]# pwd
/usr/share/openldap/migration

#Dùng script migrate_passwd.pl để tạo LDIF file từ /tmp/ldapuser.info
[root@LDAP-SVR]# ./migrate_passwd.pl /tmp/ldapuser.info > /tmp/ldapuser.ldif
[root@LDAP-SVR]# less /tmp/ldapuser.ldif
...

#Đưa thông tin về user ldapuser trong LDIF file vào kiến trúc của LDAP
[root@LDAP-SVR]# ldapadd -c -x -D "cn=Manager,dc=ipmac,dc=lab" \
-W -f /tmp/ldapuser.ldif
Enter LDAP Password:
adding new entry "uid=ldapuser,ou=People,dc=ipmac,dc=lab"

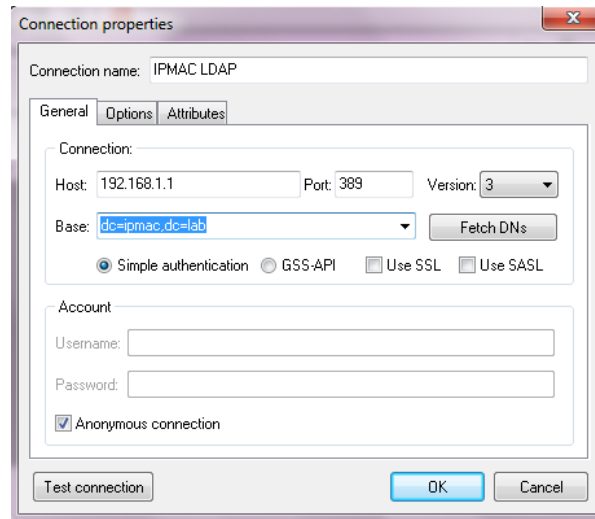
#Kiểm tra thông tin về user ldapuser trong kiến trúc của LDAP
[root@LDAP-SVR]# ldapsearch -x -LLL -b "dc=ipmac,dc=lab" "(uid=ldapuser)"
dn: uid=ldapuser,ou=People,dc=ipmac,dc=lab
uid: ldapuser
cn: ldapuser
objectClass: account
objectClass: posixAccount
objectClass: top
objectClass: shadowAccount
userPassword:: e2NyeXB0fSQxJEN5RH55ajQvJG1Ya0RWbz1IRFZwSURnbjZteTJhdC4=
shadowLastChange: 15058
shadowMin: 0
shadowMax: 99999
shadowWarning: 7
loginShell: /bin/bash
uidNumber: 502
gidNumber: 100
homeDirectory: /home/ldapuser
```


IV. Cấu hình LDAP Server sử dụng công cụ LDAP Admin

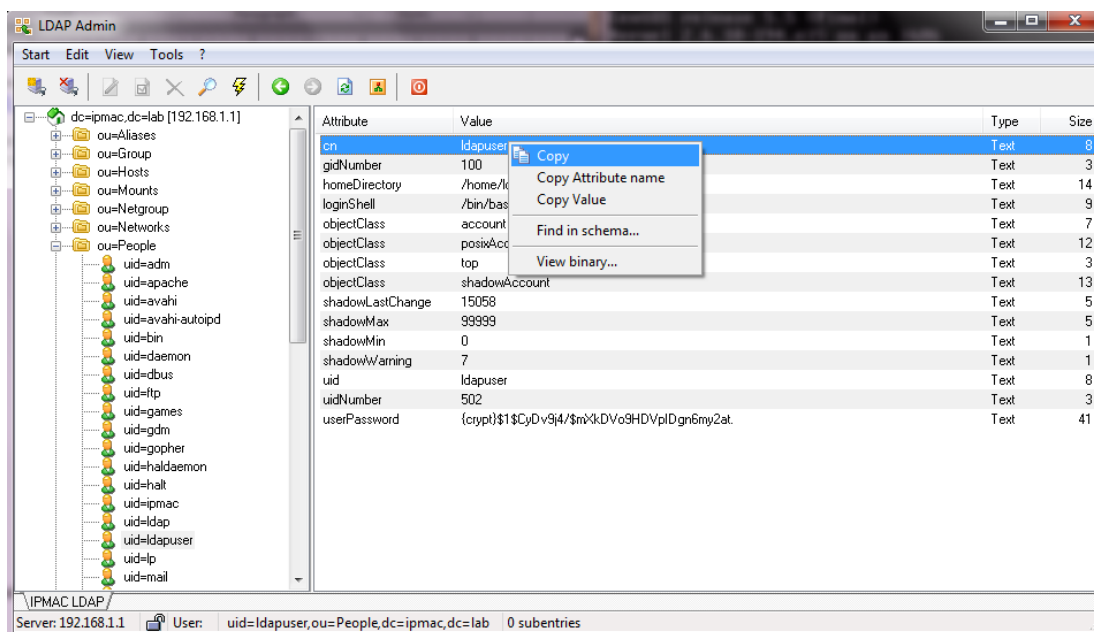
Bước 17. [Trên máy thật Windows] Download công cụ LDAP Admin tại địa chỉ
<http://nchc.sourceforge.net/project/ldapadmin/ldapadmin/1.1/LdapAdminExe-1.1.zip>

Bước 18. [Trên máy thật Windows] Chạy LDAP Admin. Vào **Start > Connect... > New Connection** và điền thông tin kết nối đến LDAP Server. Click **OK** để hoàn tất.

Chú ý: Sau khi điền địa chỉ IP của Host có thể click **Fetch DNs** để công cụ tự động lấy các thông tin về Base.



Bước 19. [Trên máy thật Windows] Double click vào kết nối vừa tạo và nhập password (nếu yêu cầu) để kết nối đến LDAP Server. Sau khi kết nối thành công, tìm hiểu giao diện và các tính năng mà công cụ LDAP Admin cung cấp.



V. Cấu hình Client để xác thực qua LDAP Server

Bước 20. [Trên LDAP Client] Cấu hình địa chỉ IP cho client trên theo mô hình trên, kiểm tra việc kết nối giữa LDAP Client và LDAP Server

```
[root@LDAP-CLIENT]# ifconfig eth0 192.168.1.2/24 up
[root@LDAP-CLIENT]# service iptables stop
[root@LDAP-CLIENT]# ping 192.168.1.1
PING 192.168.1.1 (192.168.1.1) 56(84) bytes of data.
64 bytes from 192.168.1.1: icmp_seq=1 ttl=64 time=1.370 ms
64 bytes from 192.168.1.1: icmp_seq=2 ttl=64 time=0.179 ms
```

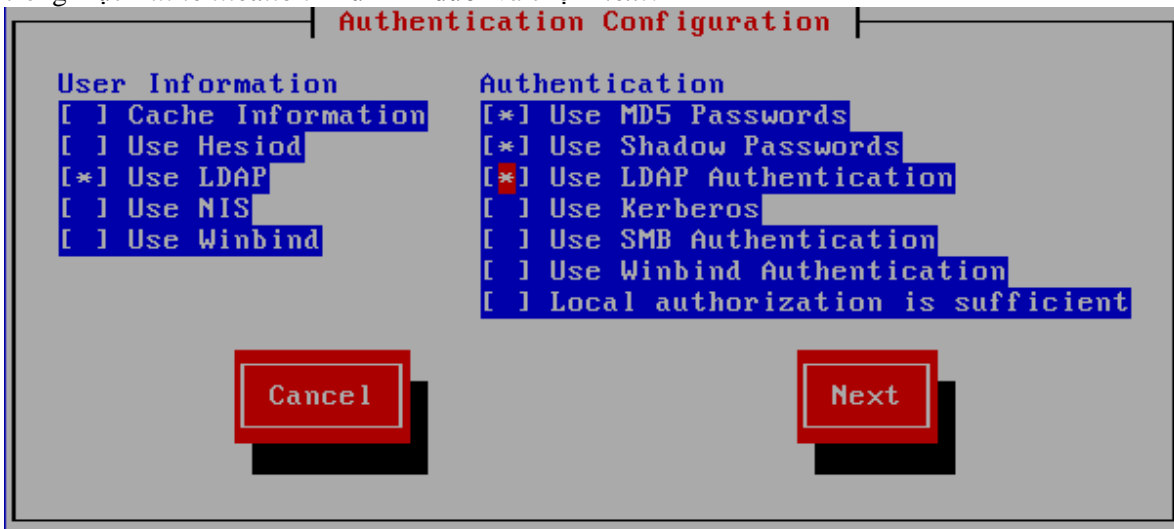
Bước 21. [Trên LDAP Client] Kiểm tra thông tin về account **ldapuser** trên client để đảm bảo chưa có user này

```
[root@LDAP-CLIENT]# finger ldapuser
finger: ldapuser: no such user.
```

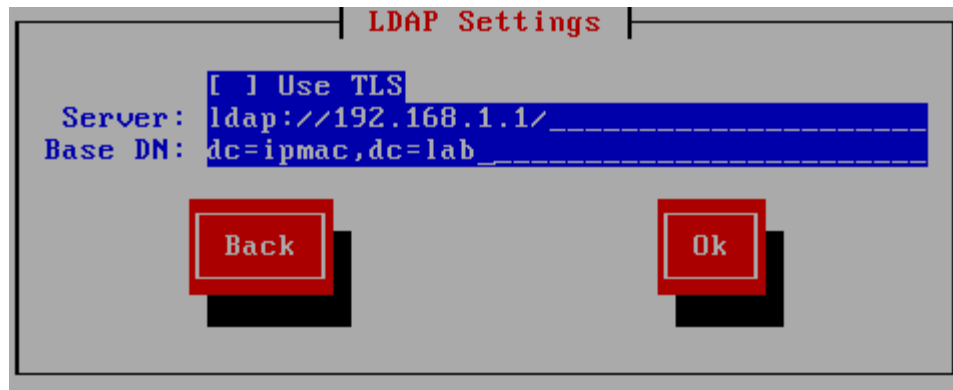
Bước 22. [Trên LDAP Client] Kiểm tra file */etc/nsswitch.conf* và các file trong */etc/pam.d/* để thấy việc tìm kiếm thông tin user (User Information) và xác thực cho user (Authentication) chưa được cấu hình để sử dụng LDAP

```
[root@LDAP-CLIENT]# cat /etc/nsswitch.conf
...
passwd:      files
shadow:      files
group:       files
...
[root@LDAP-CLIENT]# grep "ldap" /etc/pam.d/*
```

Bước 23. [Trên LDAP Client] Chạy lệnh **authconfig-tui** để mở chương trình **Authentication Configuration**. Chọn **Use LDAP** trong mục **User Information** và **Use LDAP Authentication** trong mục **Authentication** như hình dưới và chọn **Next**.



Nhập thông tin về LDAP *Server* và *Base DN* và chọn **OK**



Bước 24. [Trên LDAP Client] Kiểm tra lại các file */etc/nsswitch.conf* và */etc/pam.d/system-auth* để thấy việc tìm kiếm thông tin user (User Information) và xác thực cho user (Authentication) đã được cấu hình để sử dụng LDAP

```
[root@LDAP-CLIENT]# grep "ldap" /etc/nsswitch.conf
passwd:      files ldap
shadow:      files ldap
group:       files ldap
...
[root@LDAP-CLIENT]# grep "ldap" /etc/pam.d/system-auth
auth         sufficient    pam_ldap.so use_first_pass
account      [default=bad  success=ok user_unknown=ignore] pam_ldap.so
password     sufficient    pam_ldap.so use_authtok
session      optional     pam_ldap.so
```

Bước 25. [Trên LDAP Client] Kiểm tra lại thông tin về account **ldapuser**. Chú ý rằng thư mục *\$HOME* của **ldapuser** (*/home/ldapuser*) chưa được tạo sẵn.

```
[root@LDAP-CLIENT]# finger ldapuser
Login: ldapuser                      Name: ldapuser
Directory: /home/ldapuser            Shell: /bin/bash
Never logged in.
No mail.
No Plan.
[root@LDAP-CLIENT]# cd /home/ldapuser
-bash: cd: /home/ldapuser: No such file or directory
```

Bước 26. [Trên LDAP Client] Cấu hình thêm cho PAM để tự động tạo thư mục *\$HOME* cho các user khi login lần đầu tiên vào hệ thống

```
[root@LDAP-CLIENT]# ls /lib/security | grep pam_mkhomedir
pam_mkhomedir.so
[root@LDAP-CLIENT]# vi /etc/pam.d/system-auth
...
#Chèn vào cuối cùng của file
session      optional     pam_mkhomedir.so skel=/etc/skel/ umask=0022
```

Bước 27. [Trên LDAP Client] Chuyển sang một terminal khác (*Ctrl+Alt+F3*) và thử login sử dụng account **ldapuser**. Kiểm tra để thấy thư mục *\$HOME* của account này đã được tự động tạo ra trên hệ thống

```
LDAP-CLIENT release 5.5 (Final)
Kernel 2.6.18-194.el5 on an i686
```

```
LDAP-CLIENT login: ldapuser  
Password:  
Creating directory '/home/ldapuser'  
Creating directory '/home/ldapuser/.mozilla'  
Creating directory '/home/ldapuser/.mozilla/plugins'  
Creating directory '/home/ldapuser/.mozilla/extensions'  
[ldapuser@LDAP-CLIENT ~]$ pwd  
/home/ldapuser
```