LDAP User Guide

Version: 1.0

Jul. 2020

Contents

1 Introduction

1.1 Overview

LDAP is short for Lightweight Directory Access Protocol. Here it refers to the simplified edition of the X.500-based Directory Access Protocol (DAP). LDAP exists as an information directory, it can store text data, binary pictures and other information, such as contact lists, personal information, web links, jpeg images, etc. Users and groups are defined only once and shared among multiple machines and applications. In order to access the information stored in the directory, it is necessary to use an access protocol LDAP that running on top of TCP/IP.

1.2 LDAP Information Model

The information in the LDAP directory is organized in a tree structure, and the specific information is stored in the data structure of the entry. The entry is the attribute with the distinguished name DN. The DN is used to reference the entry, and the DN is equivalent to the key in the relational database table. An attribute consists of a type and one or more values. In order to facilitate retrieval, the Type in LDAP can have multiple values. The country (c=CN) or domain name (dc=com) is generally defined at the root of the tree, and one or more organizations or organizational units under it.

1.3 ObjectClass and Attribute in LDAP

LDAP supports setting optional and required attributes for entries, which is implemented by a special attribute called objectClass. The value of this attribute determines some rules that the entry must follow, which stipulates which attributes the entry can and should contain at least.

In LDAP, an entry must contain an objectClass attribute and at least one value must be assigned. Each value will be used as a template for data storage of an LDAP entry; the template contains the attributes and optional attributes that must be assigned to an entry.

The objectClass has a strict hierarchy, the top level is top and alias. For example, the objectClass organizationalPerson belongs to person, and person belongs to top. objectClass can be divided into the following 3 categories:

- Structural: such as person and organizationUnit；
- Auxiliary: such as extensibeObject；
- Abstract: such as top, stract objectClass cannot be used directly.

The following lists some of the required attributes of commonly used objectClass.

- account: userid
- organization: o
- dcobject: dc
- person: cn and sn
- organizationalPerson: same as person
- organizationalRole: cn
- organizationalRole: ou
- organizationalRole: cn and gidNumber
- organizationalRole: cn, gidNumber, homeDirectory, uid, and uidNumber

The attribute is similar to variables in program design and can be assigned values. Common attributes are as follows:

- c: country
- dc: domain component, usually refers to a part of a domain name
- givenName: name of a person, not a family name
- l: a place name, such as the name of a city or other geographical area
- mail: email address
- o: organizationName, name of an organization
- ou: organizationalUnitName, name of an organizational unit
- cn: common name, name of an object. If the object refers to a person, the full name should be used.
- sn: surname, family name of a person
- telephoneNumber: phone number, which should carry the country code
- uid: userid, usually refers to the login name of a user

Note: objectClass is a special type of attribute. It contains other in-use attributes and itself.

1.4 Applicable Models

FIP10, FIP10P, FIP11C, FIP11CP, FIP13G, FIP14G, FIP15G

1.5 Glossary

Keyword	Name	Description
C	Country	Country, such as "CN" and "US"
DC	Domain Component	Domain name, its format is to divide the complete domain name into several parts, such as the domain name winline.com becomes dc= winline, dc=com
O	Organization	Organization name, such as "winline"
OU	Organization Unit	Organizational unit, similar to a subdirectory in the Linux file system, is a container object, and the organization unit can contain various other objects (including other organizational units), such as "test"
UID	User Id	User ID, such as "tom"
CN	Common Name	Common name, such as "Thomas Johansson"
SN	Surname	Last name, such as "Johansson"
DN	Distinguished Name	The unique distinguished name, similar to the absolute path in the Linux file system. Each object has a unique name, such as "Uid=tom,ou=test,dc= winline,dc=com"
RDN	Relative dn	The relative distinguished name, similar to the relative path in the file system. It is a part that has nothing to do with the directory tree structure, such as "uid=tom" or "cn= Thomas Johansson"

2 Build OpenLDAP in windows

2.1 Download and Install OpenLDAP

2.1.1 Download

This section mainly describes how to download and install OpenLDAP in the win10 enterprise edition. OpenLDAP for Windows is free and can be download with the website below:

http://www.userbooster.de/en/download/openldap-for-windows.aspx?l=en

2.1.2 Install

1. Click on the downloaded exe file, the following window will pop up, select Yes.

Figure 2-1-1

2. Click next and keep its default configuration.

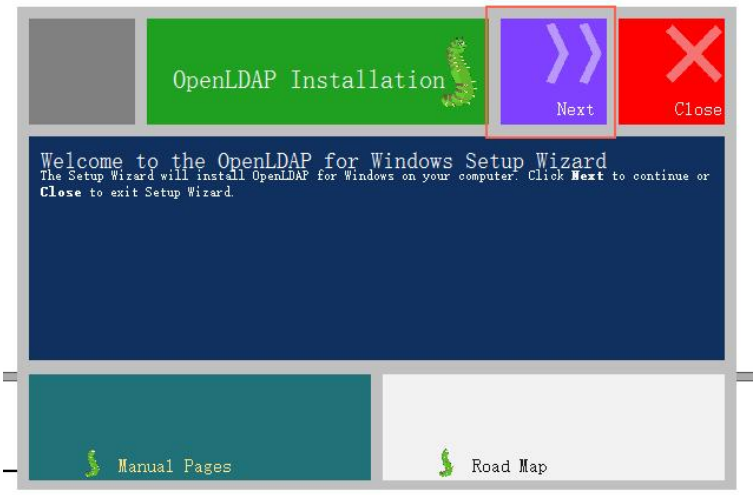

Figure 2-1-2

3. In the dialog box for selecting a path, change the path as required, such as D:\OpenLdap.

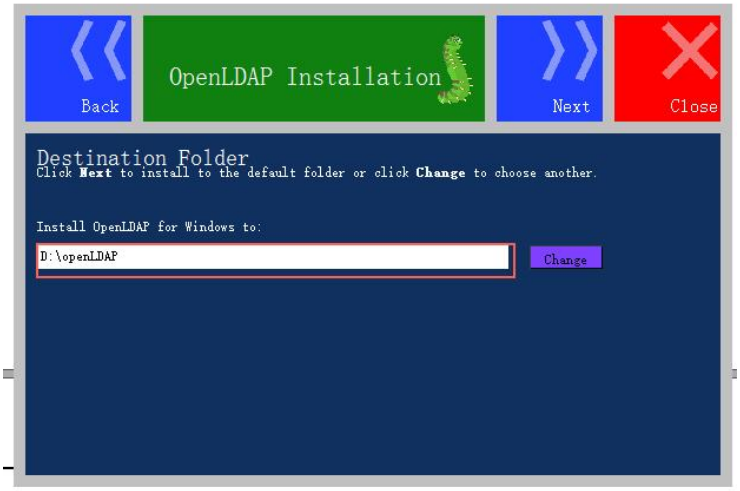

Figure 2-1-3

4. Click the install button to start the installation, click the close button when finished it. If there are any problems during the installation, you can click the link below for the solution.
http://www.userbooster.de/en/support/feature-articles/openldap-for-windows-installation.aspx
During the installation, if the system prompts that gssapi32.dll or gssapi64.dll file is missing, you can download the file online and save it in the installation path of OpenLDAP.

2.2 Configure OpenLDAP Server

2.2.1 Modify the slapd.conf file

Under the installation directory of OpenLDAP, modify the slapd.conf file. Specifically, find related configurations in the file, as shown in Figure 2-2-1.

Suffix “dc = maxcrc, dc = com”
Rootdn “cn = Manager,dc = maxcrc, dc = com”

```
database    mdb
suffix      "dc=maxcrc,dc=com"
rootdn      "cn=Manager,dc=maxcrc,dc=com"
# Cleartext passwords, especially for the rootdn, should
# be avoid.  See slappasswd(8) and slapd.conf(5) for details.
# Use of strong authentication encouraged.
rootpw    {SSHA}G8nIcSW6gSCQ6bKD8eCb4M0dJ/olUDDe
```

Figure 2-2-1

Suffix is a component used to define domain names. Rootdn is used to define administrative users.

We can also change the domain name to flyingvoice.com or other domain names, and the administrator's domain name should also be changed, like the figure below.

Suffix “dc =flyingvoice, dc = com”

Rootdn “cn = Manager, dc = flyingvoice, dc = com”

```
database    mdb
suffix      "dc=flyingvoice,dc=com"
rootdn      "cn=Manager,dc=flyingvoice,dc=com"
# Cleartext passwords, especially for the rootdn, should
# be avoid.  See slappasswd(8) and slapd.conf(5) for details.
# Use of strong authentication encouraged.
rootpw    {SSHA}G8nIcSW6gSCQ6bKD8eCb4M0dJ/olUDDe
```

Figure 2-2-2

If the domain name contains other components, change it as follows

Suffix “dc =flyingvoice, dc = com, dc = cn”

Rootdn “cn = Manager, dc = flyingvoice, dc = com,dc = cn”

```
database    mdb
suffix      "dc=flyingvoice,dc=com,dc=cn"
rootdn      "cn=Manager,dc=flyingvoice,dc=com,dc=cn"
# Cleartext passwords, especially for the rootdn, should
# be avoid.  See slappasswd(8) and slapd.conf(5) for details.
# Use of strong authentication encouraged.
rootpw    {SSHA}G8nIcSW6gSCQ6bKD8eCb4M0dJ/olUDDe
```

Figure 2-2-3

2.2.2 Change the password

1.Disable the LDAP service.

2.Click Start > Run.

3.Type cmd to enter the command line interface, or you can press Windows Key + R Key first, then type cmd.

4.Switch to the installation directory, run slappasswd, enter the new password twice to ensure that the input is correct.

5.Place the obtained secret code in the slapd.conf file, as shown in Figure 2-2-4 and Figure 2-2-5.

6.Restart the LDAP service.

Note: If you cannot copy the secrete code on the CLI, redirect the secret code generated by the slappasswd command to another file, or press Ctrl+M to select the secret code and then press Ctrl+C to copy it.

slappasswd > \home\test.txt

//Place the secret code generated by the slappasswd command to the test.txt file under the home directory.

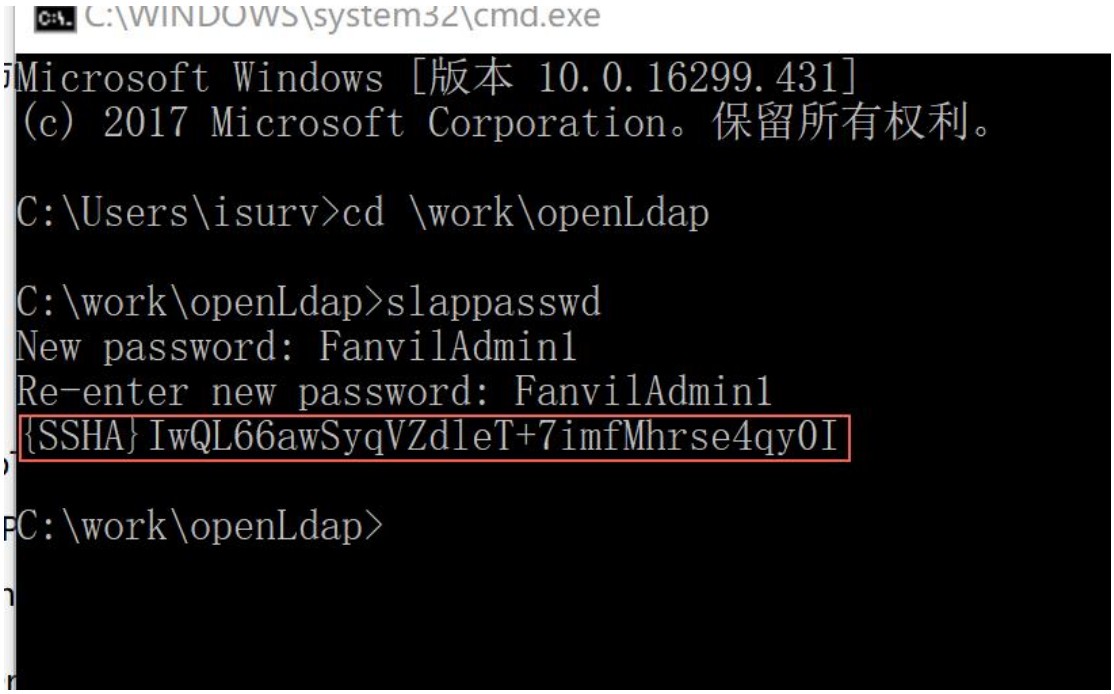

Figure 2-2-4

```
database    mdb
suffix      "dc=flyingvoice,dc=com"
rootdn      "cn=Manager,dc=flyingvoice,dc=com"
# Cleartext passwords, especially for the rootdn, should
# be avoid.  See slappasswd(8) and slapd.conf(5) for details.
# Use of strong authentication encouraged.
rootpw    {SSHA}IwQL66awSyqVZdleT+7imfMhrse4qy0I
```

Figure 2-2-5

2.3 Start the Slapd service

2.3.1 Procedure

Method 1：

1.Click Start > Run.

2.Type cmd to enter the command line interface, or you can press Windows Key + R Key first, then type cmd.

3.Access the LDAP installation path, for example, C:/office software/LDAP and run slapd.exe -d 1 -f ./slapd.conf.

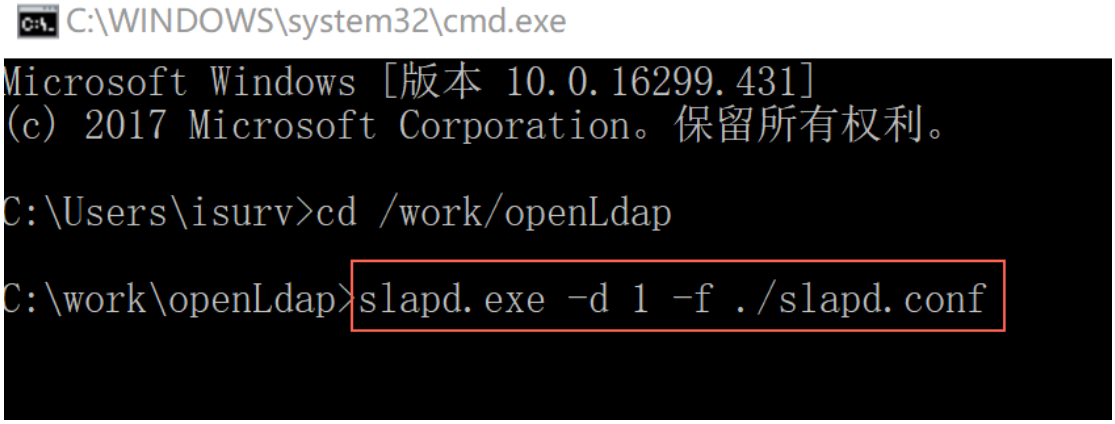

Figure 2-3-1

4.When the service has been started successfully, you will see the field slapd starting.

Note: Do not close the cmd window to ensure the LDAP server keeps running.

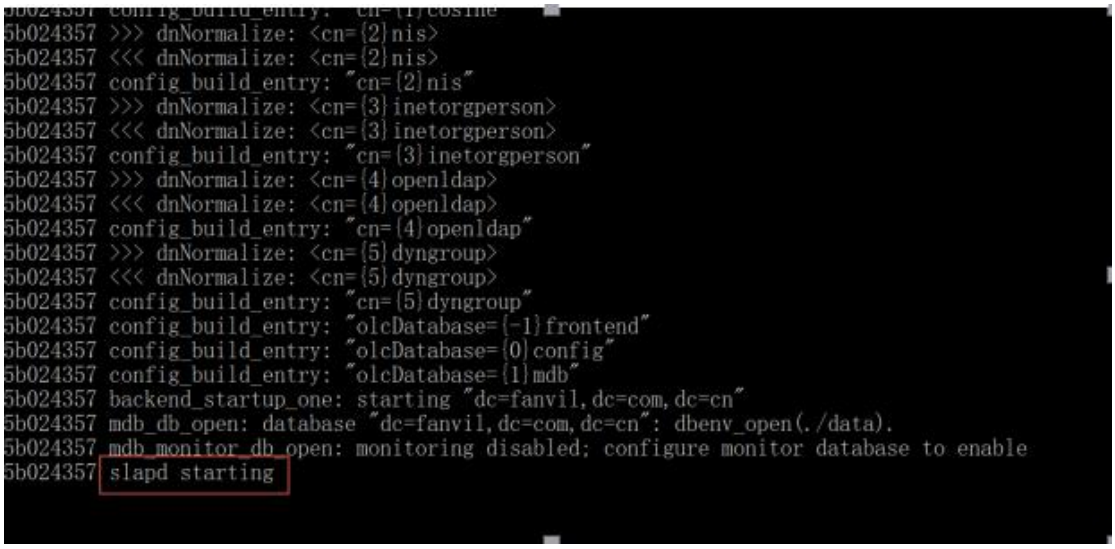

Figure 2-3-2

Method 2：

Enable or disable the LDAP service under My Computer > Management > Services.

2.3.2 Add LDAP entries

Add the file suffix LDIF, store the added empty file in the installation path of OpenLDAP, open the file with a file editor, and fill in the content. For example, right-click an added test.txt file, change its filename extension to ldif (test.ldif), and open the file with a file editor. The following is an example of test.ldif.

```
dn: ou=flyingvoice, dc=beijing,dc=com
ou: flyingvoice
objectClass: organizationalUnit

dn: ou=organizationalRolemun, ou= flyingvoice, dc=beijing,dc=com
ou: organizationalRolemun
objectClass: organizationalUnit

dn: cn=bingwang1,ou=organizationalRolemun, ou= flyingvoice, dc=beijing,dc=com
telephoneNumber: 8231
registeredAddress: WWWEEE
objectClass: organizationalPerson
telexNumber: 8110
```

postalAddress: 332211

sn: bing

street: Zqq

cn: bingwang1

dn:cn=zhangqiang1,ou=organizationalRolemun,ou= flyingvoice, dc=beijing,dc=com

telexNumber: 2000

street: Zqw

sn: zhang

telephoneNumber: 2000

ou: 3ou

objectClass: organizationalPerson

postalAddress: 334411

registeredAddress: ACXCXCCXC

cn: zhangqiang1

dn: cn=sunliang,ou=organizationalRolemun, ou= flyingvoice, dc=beijing,dc=com

telephoneNumber: 123333

registeredAddress: WEEWEWEE

objectClass: organizationalPerson

telexNumber: 6564

sn: sun

cn: sunliang

dn: cn=zhangchao,ou=organizationalRolemun, ou= flyingvoice, dc=beijing,dc=com

telephoneNumber: 7777

registeredAddress: ZZZWWW

objectClass: organizationalPerson

telexNumber: 54646

sn: zhang

street: XAZ

cn: zhangchao

```
dn: cn=xieqian,ou=organizationalRolemun, ou= flyingvoice, dc=beijing,dc=com
telephoneNumber: 3312123
registeredAddress: XXXZZZ
objectClass: organizationalPerson
telexNumber: 242342
postalAddress: 332221
sn: xie
cn: xieqian
```

Note: No space is allowed at the beginning or end of each line. An error will be reported if the format is incorrect.

1. Choose Start > Run.

2. Enter cmd to access the CLI. (If you cannot find Run in Windows 10, enter win + r and then cmd.)

3. Access the LDAP installation path, for example, C:/work/openLdap and run slapadd -v -l ./test.ldif. If conditions allow, it is recommended that LDAP not be installed on drive C and be installed under a pure English path.

Note: The slapadd command can be used to operate only the local LDAP service. Before operation, the local LDAP service must be stopped.

Common LDAP attributes:

DN: The DN is unique under a directory. It is used to identify a node. Its attributes are described as follows:

1. CN=Common Name: user name or server name. The maximum length is 80 characters. It can be in Chinese.

2. OU=Organization Unit: There are a maximum of four levels of organizational units. Each level of organizational unit is 32 characters long at most. It can be in Chinese.

3. DC= Domain Component: directory structure

4. O=Organization: organization name. It is optional and contains 3 to 64 characters.

2.3.3 Schema in LDAP

In LDAP, schema specifies the types of objects contained in a directory and the

mandatory and optional attributes of each objectClass. Therefore, schema is a data model that determines how data is stored and the type of tracked data. A schema needs to be specified in the main configuration file slapd.conf to determine the objectClass to be used in the local directory. The administrator can design a schema, which usually comprises the following parts: AttributeDefinition, ClassDefinition, and SyntaxDefinition.

After creating a schema file, copy it to the schema directory of LDAP. Then modify the slapd.conf file and add the new schema file.

2.4 Graphical management tools

2.4.1 LDAPBrowser Introduction

LDAPBrowser is a graphical LDAP management tool that running on Windows systems. You can browse, modify, and manage contact entry information on LDAP data.

2.4.2 Download and Install LDAPBrowser

Search and download jdk1.4 or jdk1.5 or higher version online, download LdapBrowser with the link below.

http://www.blogjava.net/Files/Unmi/LdapBrowser282.rar

Note: LdapBrowser can be used directly without installation. Click lbe.bat in the installation directory to run LdapBrowser.

2.4.3 Add initial data

After clicking lbe.bat in the installation directory, the following options pop up, select Edit to operate on it or select New to create a new Session List.

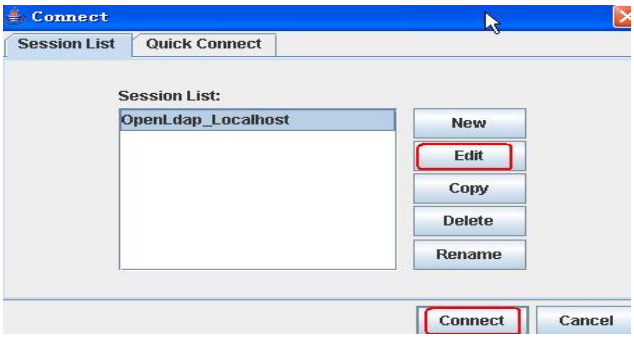

Figure 2-4-1

The following describes the items on the page for creating a session list.

Host: OpenLDAP host name or IP address. Click Fetch DNs to automatically match the root domain of OpenLDAP in slapd.conf.

Port: port reserved by default.

Version: version, which is 3 by default.

Here append base DN must be selected.

User DN: administrator account used during OpenLDAP installation. Here cn=manager is entered.

Password: new password. If the initial password is not changed, the initial password (secret) at installation takes effect by default.

Click Save. On the Connect page, click Connect. To perform anonymous login, select Anonymous bind. It should be noted that an anonymously logged-in user can only view data, as shown in Figure 2-4-2.

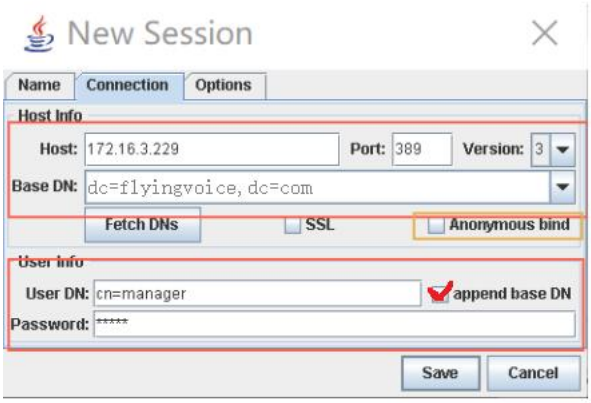

Figure 2-4-2

2.4.4 Add directory attributes

Here is an example of an LDAP with data:

If you need to add Attribute to an element, follow the operations below.

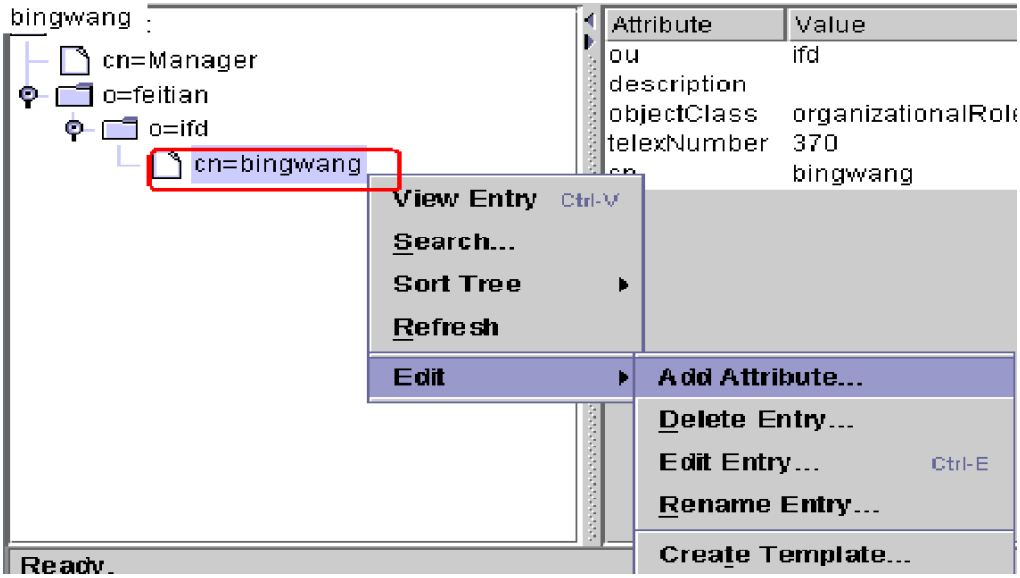

Figure 2-4-3

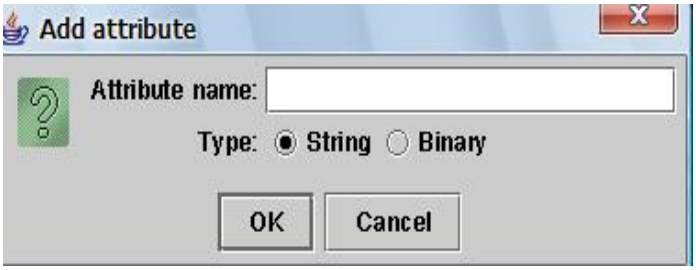

Figure 2-4-4

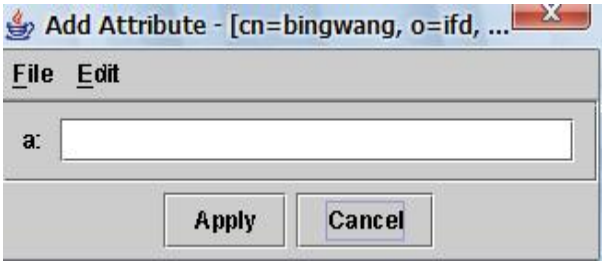

Figure 2-4-5

Click Apply. Added attribute names comply with the LDAP standard or are custom; otherwise, the adding fails. Figure 2-4-5 shows an example of failing to adding attribute a. For details about the default LDAP attribute values, see %openldap_home%\schema\core.schema.

2.4.5 Delete directory attributes

Select the Attribute of an element and delete it. As shown below.

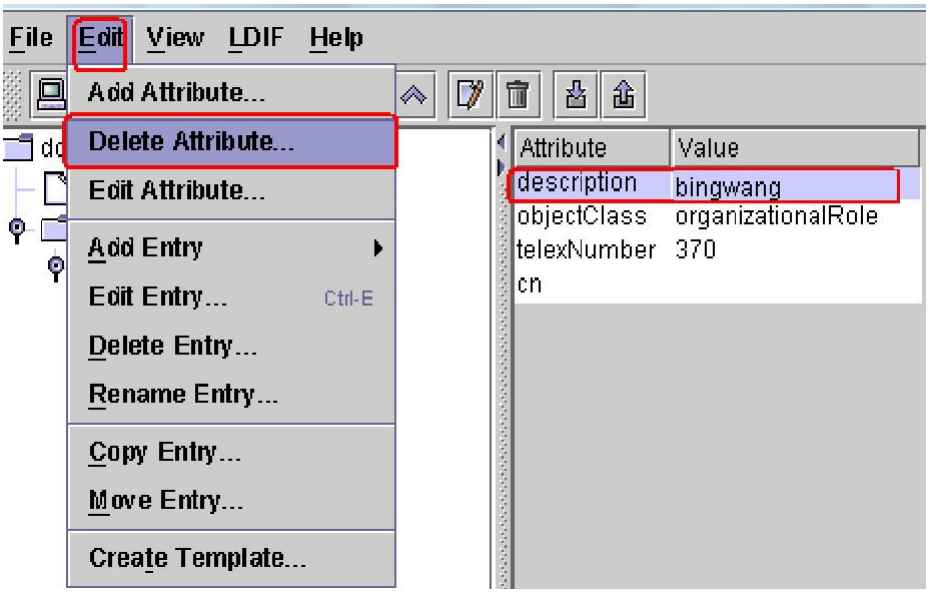

Figure 2-4-6

2.4.6 Modify directory attributes

Double-click on the attribute of the directory to pop up the modification interface, enter the new attribute value and click Apply.

2.4.7 Add a directory

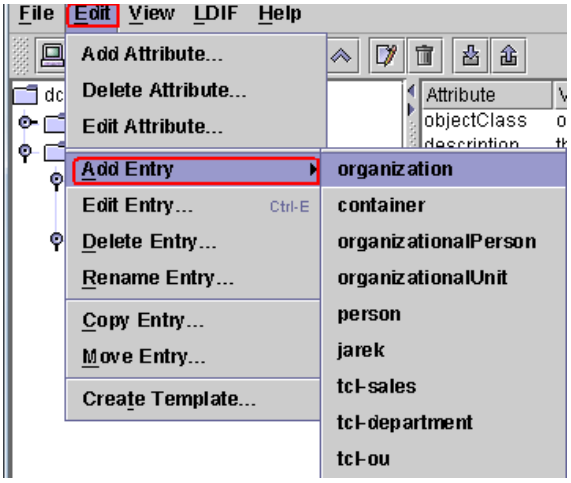

Figure 2-4-7

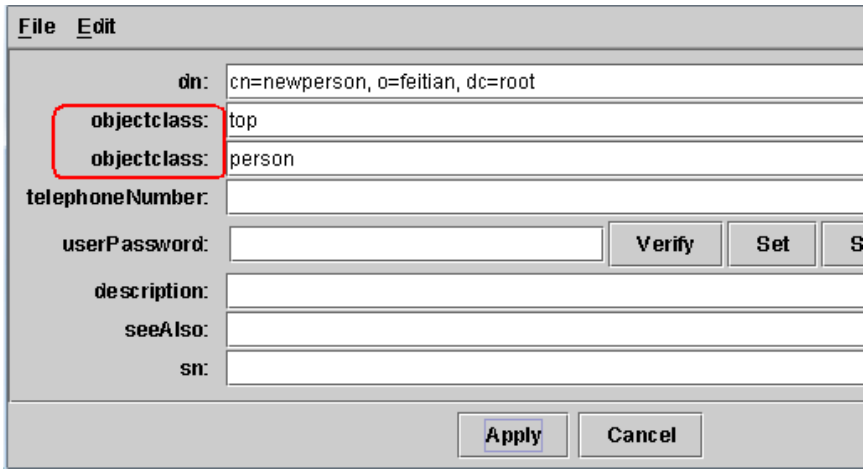

Figure 2-4-8

2.4.8 Modify a directory

Modifying the directory is to modify all the attributes of the directory, you can refer to the above modification directory attribute operation, or refer to the figure below.

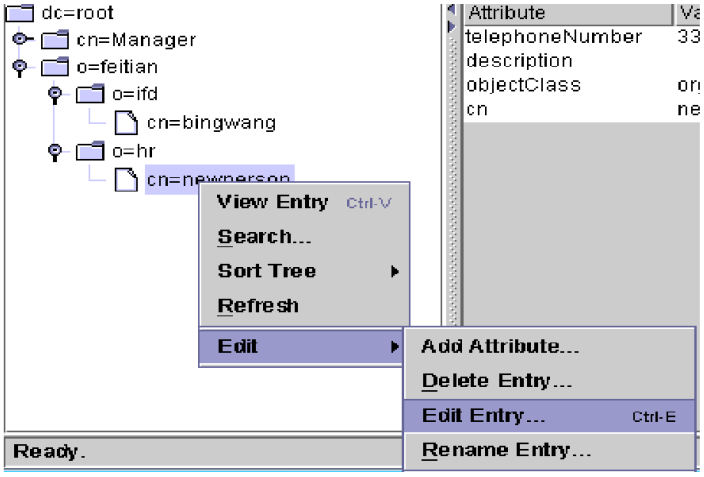

Figure 2-4-9

2.4.9 Delete a directory

Select the directory that you want to delete, then refer to the figure below.

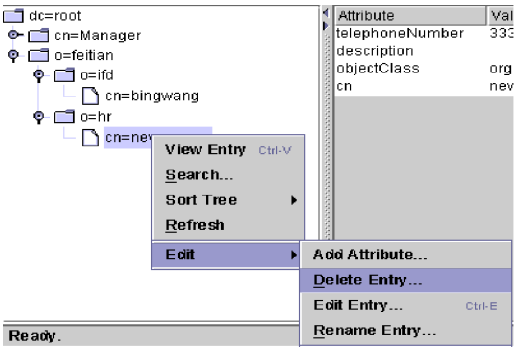

Figure 2-4-10

2.4.10 Example

Here is an example to learn the tree structure of LDAP data.

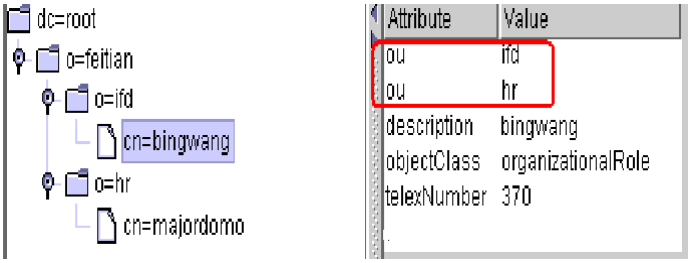

Figure 2-4-11

In Figure above, the entity cn=bingwang is at the end. What is its complete DN?

dn:cn=bingwang,o=ifd,o=feitian,dc=root

The root node at the topmost is at the last of the expression. In addition to the DN, more attributes may be added for a node. For example, a person in an address book is a node and the address and phone number of the person are attributes. Figure 2-4-11 shows various attributes of user bingwang, including two ou attributes, indicating that the user takes a position in the ifd and hr departments. A node may contain multiple identical attributes with different values. Attributes can be fully utilized to describe various information about a node. The following is the content of the ldif file of node cn=bingwang.

```
dn: cn=bingwang, o=ifd, o=feitian, dc=root
ou: ifd
ou: hr
description:bingwang
objectClass: organizationalRole
```

telexNumber: 370

cn: bingwang

3 Build OpenLDAP in Linux

3.1 Overview

In the server with Linux system, openLdap is generally used to build an ldap server. The following is an overview of the required libraries and precautions.

3.1.1 Berkeley DB

Berkeley DB is an open source embedded database management system developed by Sleepycat Software in the United States. It provides scalable, high-performance, transaction-protected data management services for applications. Since openldap requires Berkeley DB to store data, Berkeley DB must be installed first.

Note: Before downloading db.tar, confirm the OpenLDAP version to be downloaded. The two are compatible only under certain versions.

For example, OpenLDAP-2.4.44 is compatible only with Oracle Berkeley 4.4-4.8 or 5.0-5.1.

If any error is reported during the installation of OpenLDAP, the reason may be version incompatibility.

Error：BerkeleyDB version incompatible with BDB/HDB backends

3.1.2 Cyrus -sasl

SASL is short for the Simple Authentication and Security Layer. Its mechanism is to perform verification on the protocol. If a certain service (such as SMTP or the ldap we are going to build now) uses SASL, the code will be shared between applications of this protocol.

3.1.3 OpenLDAP

For details about OpenLDAP, see the preceding sections. OpenLDAP is compatible only with certain Berkeley DB versions. Therefore, check the version to be installed in advance.

3.2 Installation

Here we use Ubuntu 12.04.1, Run the following command to view the Linux VM version:

```
#cat  /etc/issue
```

Perform installation based on the sequence described in this document.

Note: It is recommended that the following installation operations be performed by user root.

3.2.1 Install Cyrus -sasl

Download and install Cyrus SASL. Navigate to the created directory and perform installation.

Here version 2.1.25 is installed.

```
#wget  http://ftp.andrew.cmu.edu/pub/cyrus-mail/cyrus-sasl-2.1.25.tar.gz
```

Note: make sure that the VM connects to the network properly, you will see the error below if put in the incorrect resource.

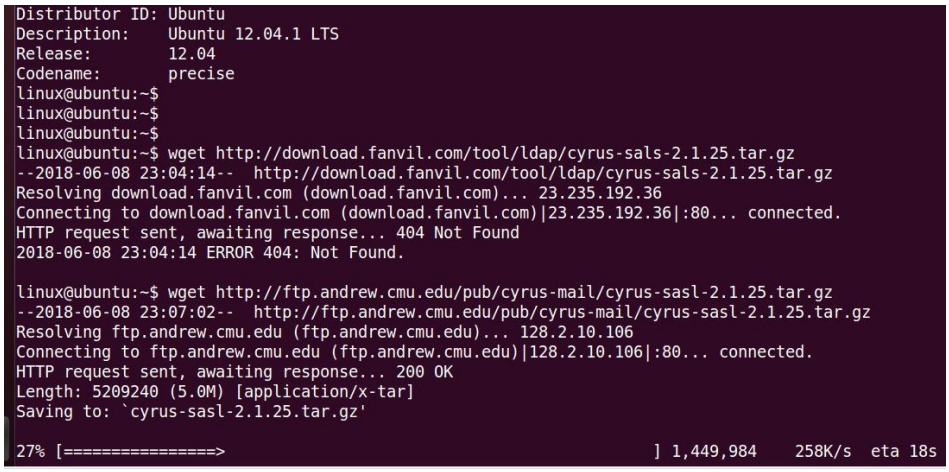

Figure 3-2-1

Run the command below to unzip the installation file downloaded before. You will see as shown on Figure 3-2-2.

```
#tar xzvf cyrus-sasl-2.1.25.tar.gz
```

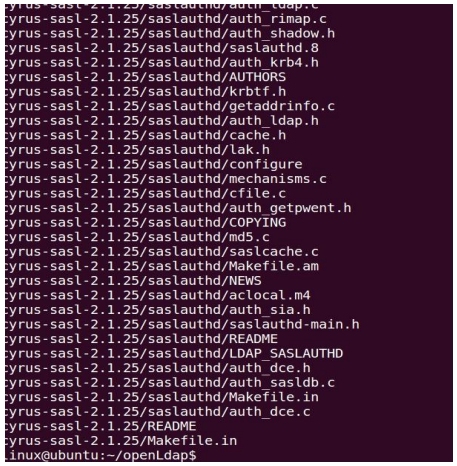

Figure 3-2-2

Open the file you unzipped just now, run the command below to configure it.

```
#cd  cyrus-sasl-2.1.25
#./configure –prefix=/usr/local/sasl2 –with-dblib=no –without-des –with-openssl=
/usr/local/ssl
```

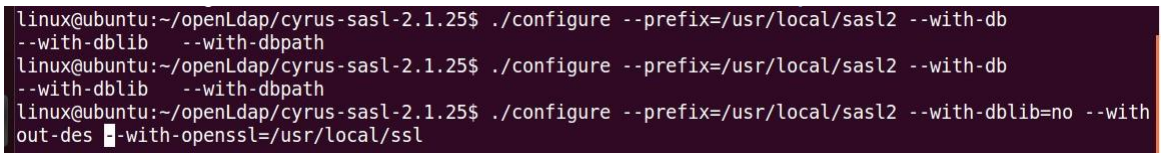

Figure 3-2-3

Input the make below.

```
#make
```

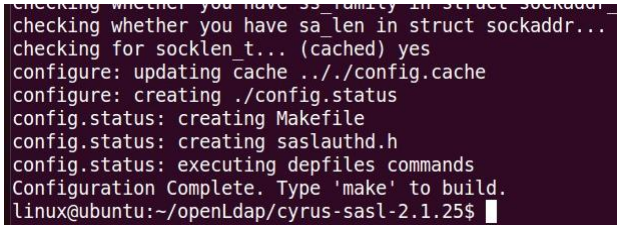

Figure 3-2-4

Input make install.

```
#make install
```

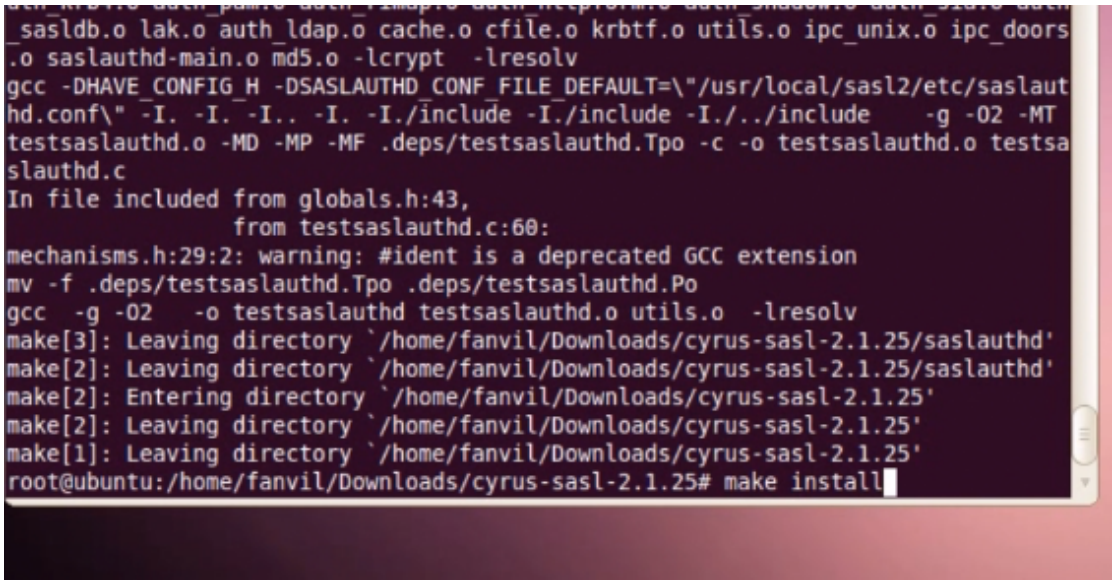

Figure 3-2-5

Configure a library file search path. If this path is not configured, path search may fail when an executable file is executed. The error message is as follows:

```
Error：while loading shared libraries
```

If this error message is displayed, see reference document 2 for a solution.

Run the following commands to configure a library file search path:

```
#echo "/usr/local/sasl2/lib" >> /etc/ld.so.conf
#echo "/usr/local/sasl2/lib/sasl2" >> /etc/ld.so.conf
#ldconfig -v
```

Replace the original SASL file.

```
# cd /usr/lib
# mv libsasl2.so libsasl2.so.OFF
# mv libsasl2.so.2.0.23 libsasl2.so.2.0.23.OFF
# mv lIbsasl2.so.2 libsasl2.so.2.OFF
# ln -s /usr/local/sasl2/lib/* /usr/lib
# ln -s /usr/local/sasl2/lib/sasl2 /usr/lib/sasl2
# ln -s /usr/local/sasl2/lib/libsasl2.so.2.0.23 /usr/lib/libsasl2.so.2
# ln -s /usr/local/sasl2/lib/libsasl2.so /usr/lib/libsasl2.so
```

3.2.2 Install BerkeleyDB

Here we install version 4.6.21. After downloading the installation package, run the following command to decompress the package. Then navigate to the build_unix folder, as shown in Figure 3-2-6

```
#tar xzvf db-4.6.21.tar.gz
#cd db-4.6.21/build_unix
```

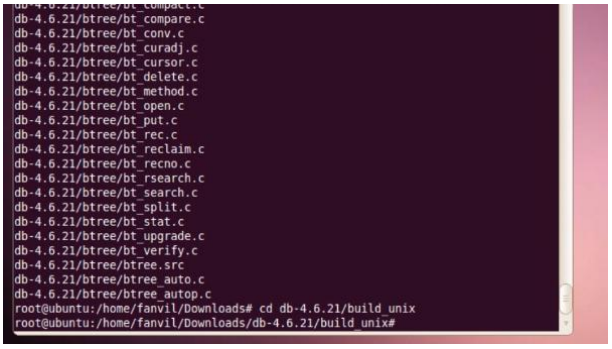

Figure 3-2-6

Configure a dependence environment below.

```
#../dist/configure –prefix=/usr/local/BerkeleyDB
```

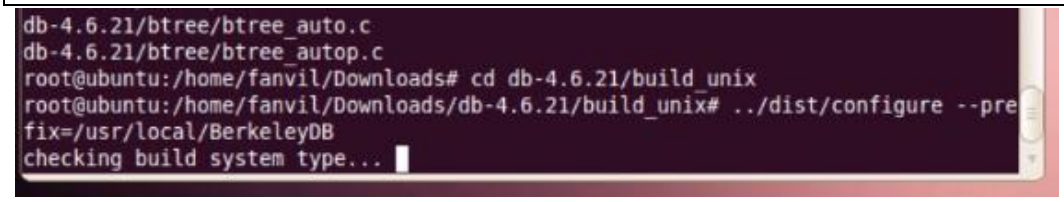

Figure 3-2-7

Figure 3-2-8 shows the configuration result.

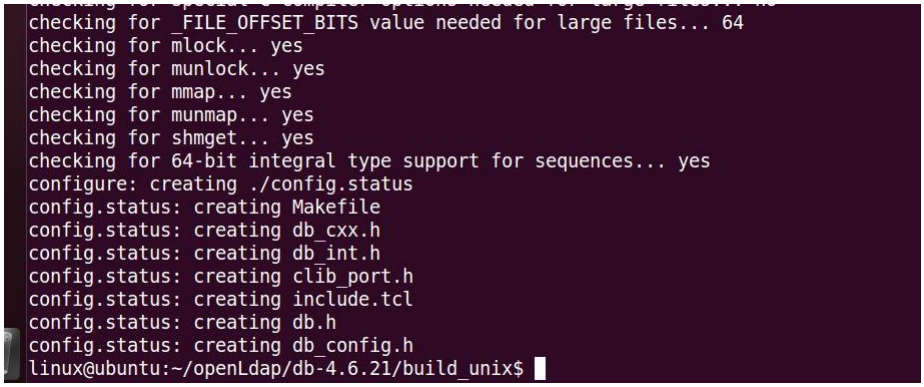

Figure 3-2-8

Input make and the make install.

```
#make
```

```
erify.c  -fPIC -DPIC -o .libs/db_verify.o
 cc -c -I. -I../dist/.. -D_GNU_SOURCE -D_REENTRANT -O3 ../dist/../db_verify/db_v
erify.c -o db_verify.o >/dev/null 2>&1
/bin/sh ./libtool --mode=link cc -O3  -o db_verify  \
           db_verify.lo util_cache.lo util_sig.lo libdb-4.6.la -lpthread
cc -O3 -o .libs/db_verify .libs/db_verify.o .libs/util_cache.o .libs/util_sig.o
 ./.libs/libdb-4.6.so -lpthread  -Wl,--rpath -Wl,/usr/local/BerkeleyDB/lib
creating db_verify
/bin/sh ./libtool --mode=execute true db_verify
root@ubuntu:/home/fanvil/Downloads/db-4.6.21/build_unix# make install
```

Figure 3-2-9

```
#make install
```

If information shown shown in Figure 3-2-10 is displayed, Berkeley DB is in stalled successfully.

```
----------------------------------------------------------------------
Installing DB utilities: /usr/local/BerkeleyDB/bin ...
cp -p .libs/db_archive /usr/local/BerkeleyDB/bin/db_archive
cp -p .libs/db_checkpoint /usr/local/BerkeleyDB/bin/db_checkpoint
cp -p .libs/db_codegen /usr/local/BerkeleyDB/bin/db_codegen
cp -p .libs/db_deadlock /usr/local/BerkeleyDB/bin/db_deadlock
cp -p .libs/db_dump /usr/local/BerkeleyDB/bin/db_dump
cp -p .libs/db_hotbackup /usr/local/BerkeleyDB/bin/db_hotbackup
cp -p .libs/db_load /usr/local/BerkeleyDB/bin/db_load
cp -p .libs/db_printlog /usr/local/BerkeleyDB/bin/db_printlog
cp -p .libs/db_recover /usr/local/BerkeleyDB/bin/db_recover
cp -p .libs/db_stat /usr/local/BerkeleyDB/bin/db_stat
cp -p .libs/db_upgrade /usr/local/BerkeleyDB/bin/db_upgrade
cp -p .libs/db_verify /usr/local/BerkeleyDB/bin/db_verify
Installing documentation: /usr/local/BerkeleyDB/docs ...
linux@ubuntu:~/openLdap/db-4.6.21/build_unix$
```

Figure 3-2-10

Finally, configure a library file search path by running the following comman ds:

```
#echo "/usr/local/BerkeleyDB/lib" >> /etc/ld.so.conf
#ldconfig -v
```

3.2.3 Install OpenLDAP

Download OpenLDAP(version 2.4.40) and run the command below to unzip the file.

```
#tar xzvf openldap-2.4.40.tgz
#cd openldap-2.4.40
```

To avoid an installation failure caused by the incompatibility between OpenLDAP and Berkeley DB, run the following commands first:

```
#exprot LD_LIBRARY_PATH="usr/local/BerkeleyDB/lib"
# export LD_LIBRARY_PATH="xxx/db-4.6.21/build_unix/.libs/"
```

xxx indicates the decompression path of the DB.

Configure the environment.

```
# env CPPFLAGS="-I/usr/local/BerkeleyDB/include" LDFLAGS="-L/usr/local/BerkeleyDB/lib" ./configure --prefix=/usr/local/openldap --enable-ldbm
```

If an incompatibility problem occurs, you will see the error below.

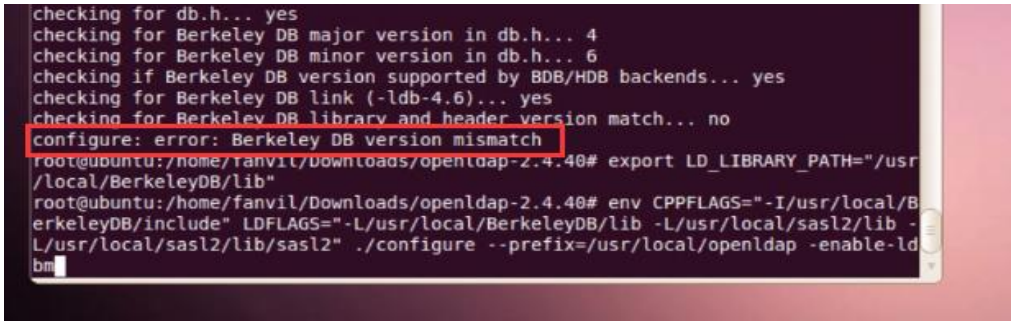

Figure 3-2-11

If the following error occurs.

```
configure: error: BDB/HDB: BerkeleyDB not available
```

Run the command below.

```
#export CPPFLAGS="-I/usr/local/BerkeleyDB/include"
#export LDFLAGS="-L/usr/local/BerkeleyDB/lib"
```

When the message prompting you to enter the make depend command, enter make depend.

```
#make depend
```

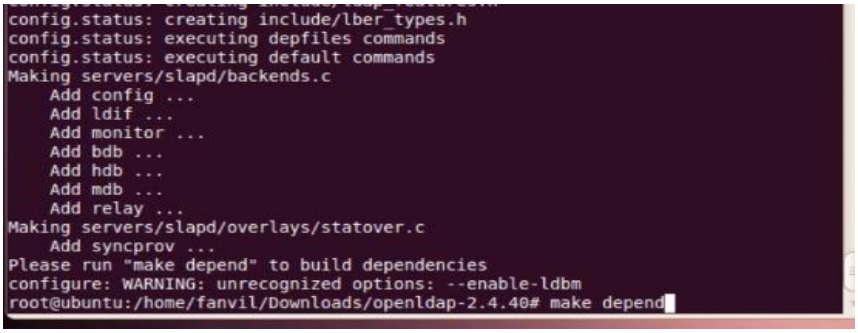

Figure 3-2-12

When the message prompting you to enter the make command, enter make, as shown in Figure 3-2-13.

```
#make
```

Figure 3-2-13

If the message shown in the Figure above, the compilation is successful.

Enter make test to perform a test. The test is not mandatory but can help find problems. The test takes a long time.

Figure 3-2-14

#make test

If no error message is reported during the test, enter make install to start installation, as shown in Figure 3-2-15.

Figure 3-2-15

#make install

If no error is reported, building the server is complete.

3.3 Configuration

The main configuration file of OpenLDAP as follows.

/usr/local/openldap/etc/openldap/slapd.conf

Restart the OpenLDAP service each time you modified the configuration file. After install the OpenLDAP in Linux, create the test.ldif file to import entries as described earlier.

```
# cd /usr/local/openldap/etc/openldap
```

Choose an editing tool based on the system. gedit can be used for a GUI.

```
# gedit slapd.conf
```

Find the following statement:

```
include /usr/local/openldap/etc/openldap/schema/core.schema
```

Add the following statements behind the found statement:

```
include /usr/local/openldap/etc/openldap/schema/corba.schema
include /usr/local/openldap/etc/openldap/schema/cosine.schema
include /usr/local/openldap/etc/openldap/schema/dyngroup.schema
include /usr/local/openldap/etc/openldap/schema/inetorgperson.schema
include /usr/local/openldap/etc/openldap/schema/java.schema
include /usr/local/openldap/etc/openldap/schema/misc.schema
include /usr/local/openldap/etc/openldap/schema/nis.schema
include /usr/local/openldap/etc/openldap/schema/openldap.schema
```

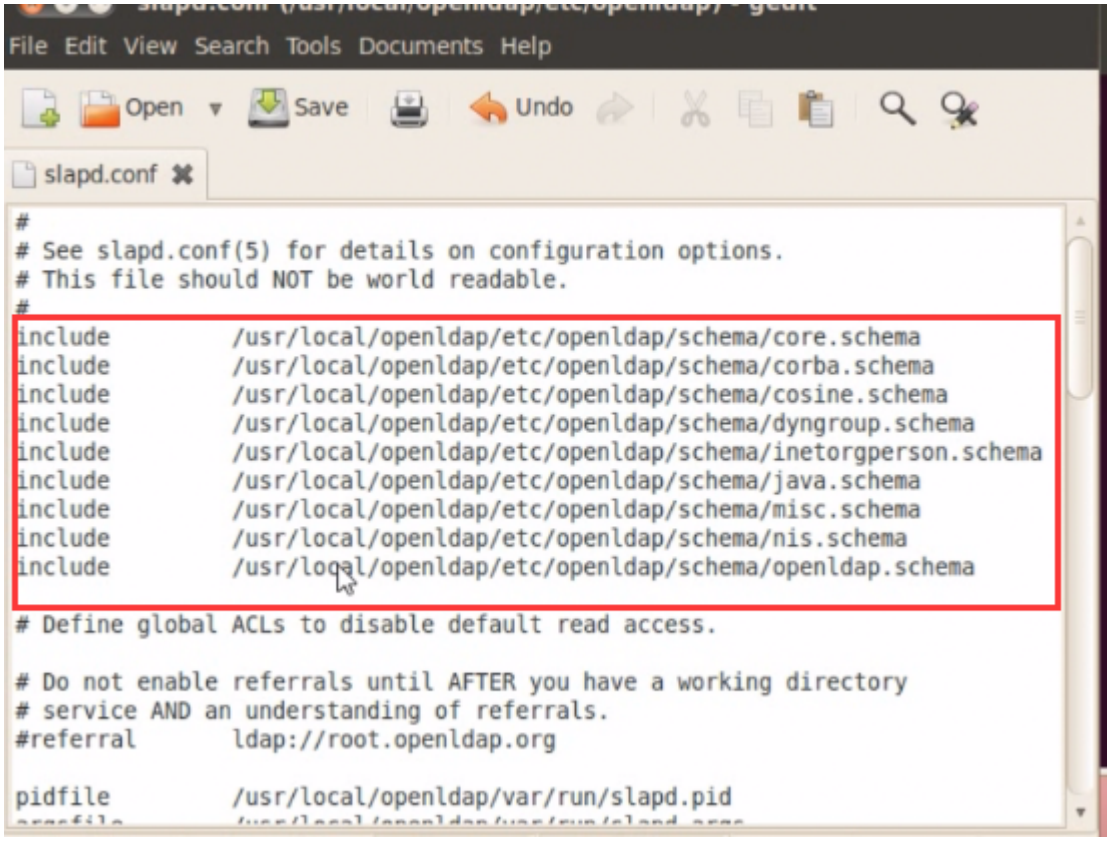

Figure 3-3-1

Set the directory tree.

suffix "dc=my-domain,dc=com"

Change it as follows:

suffix "dc=winline,dc=com"

Note: Here dc=xxx,dc=com can be customized, corresponding to query base in the telephone set settings.

Set the DN of the administrator.

rootdn "cn=Manager,dc=my-domain,dc=com"

Change it as follows:

rootdn "cn=admin,dc= winline,dc=com"

Note: Here cn=xxx,dc=xxx,dc=com can be customized and the latter part must be the same as the suffix.

Set the password of the administrator.

rootpw secret

Change it as follows:

root pw {SSHA}e7BBqjes5EF1grsupjvUfNkNdmZD+F6u

The result is the ciphertext of miracle after being encrypted using the SSHA algorithm. The ciphertext can be obtained as follows:

miracle@miracle-desktop:~$ sudo /usr/local/openldap/sbin/slappasswd

[sudo] password for miracle:

New password:

(Enter your password)

Re-enter new password:

(Enter your password again)

An encrypted key is generated: {SSHA}e7BBqjes5EF1grsupjvUfNkNdmZD+F6u

{SSHA}wZ4AzwiU850mH1F95KwvBh+Dv2S2lDtn

Note: The administrator DN and password are the user name and password for accessing LDAP.

Start the server and enter the following command:

```
#/usr/local/openldap/libexec/slapd
```

LDAP contacts are imported in text format. The file is an .ldif file in UTF-8. The import command is as follows:

/usr/local/openldap/bin/ldapadd -x -D "cn=admin,dc=miracle,dc=com" -W -f test.ldif

Note: In the preceding command, test.ldif is the file to be imported. The command is under the test.ldif folder.

After building OpenLDAP, import the root node.

File format at initial import:

---

dn: dc=winline,dc=com

dc: winline

objectclass: top

objectclass: domain

Note: The file is used to define the root node dc=winline,dc=com. Subsequent directories and contacts are added under this root node.

After the file is imported successfully, edit the file and add directories or contacts based on the actual situation.

---

dn: ou=flyingvoiceShenZhen,dc=winline,dc=com

objectclass: organizationalUnit

ou: flyingvoiceShenZhen

dn: ou=flyingvoiceBeijing,dc=winline,dc=com

objectclass: organizationalUnit

ou: flyingvoiceBeijing

dn: uid=use1,ou= flyingvoiceBeijing, dc=winline,dc=com

objectClass: inetOrgPerson

objectClass: uidObject

cn: user1

sn: user1

telephoneNumber: 112123

mobile: 1234

Import the file again.

Note: When editing a file repeatedly, the previously imported content should be deleted when the file is edited again; otherwise, an error will be reported.

3.4 Graphical management tool

We introduced the manual editing of ldif files to increase users.

For OpenLDAP graphical interface management, open source organizations also provide GUI management OpenLDAP software. Currently, open source products include management tools such as phpLDAPadmin, LDAP Account Manager, Apache Directory Studio, and LDAP Admin. Here we can use the graphical management tools to manage the ldap built under Linux.

4 Use the LDAP Phone Book on the Flyingvoice Phone

4.1 Configuration Description

Item	Description
Enable LDAP	Enable or disable LDAP
LDAP Label	The display name of the LDAP
LDAP Name Filter	Range when searching for name attributes For example: configure (|(cn=%)(sn=%)), search with the letter a, it means to search for all CN or SN attributes beginning with a. For example: configure (&(cn=%)(sn=%)), search with the letter a, it means to search for all CN and SN attributes beginning with a.
LDAP Number Filter	Range when searching for number attributes For example: configure (|(telephoneNumber=%)(mobile=%)(other=%)), input the number 1 when searching, it means to search for all telephoneNumber starting with 1 or all mobile starting with 1 or all other attribute starting with 1.
Server Address	It specifies the LDAP domain name or IP address.
Port	It specifies the LDAP port number, which is 389 by default.
Base	It specifies the search start position of the server.
User Name	Username of the LDAP server.
Password	Password of the LDAP server.
Max Hits (1~1000)	The maximum sample quantity
LDAP Name Attributes	Search the Name with the attribute
LDAP Number Attributes	Specify the number attributes returned by LDAP

LDAP Display Name	Specify the display name of the contact record on the LCD screen. The parameter value must start with the "%".
Protocol	Specify the version of the LDAP server, the default version is 3.
LDAP Lookup For Incoming Call	Enable or disable the incoming call lookup.
LDAP Lookup For Callout	Enable or disable the callout lookup
LDAP Sorting Results	Enable or disable the Sorting results.

4.2 LDAP Settings on the Phone

An example of web configuration is shown in Figure 4-2-1.

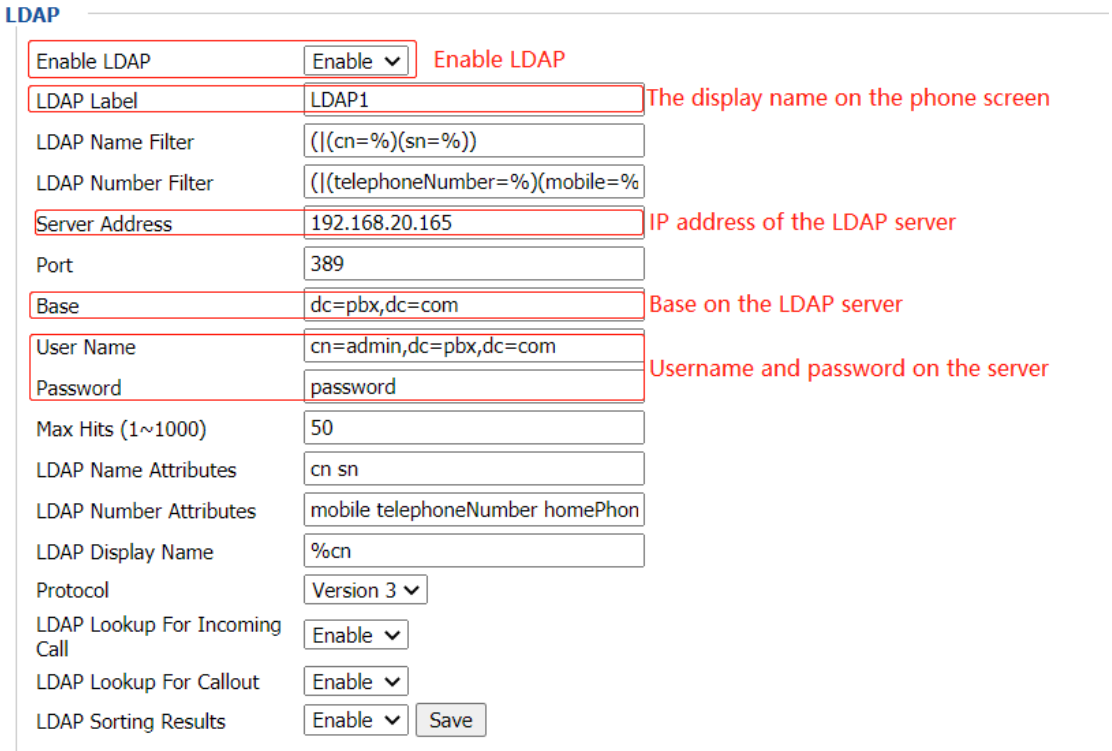

Figure 4-2-1

After configuring as shown in the figure above, you can download the information from the LDAP server in the phone Menu > Directory > LDAP1, and the

downloaded contacts displays on the phone as shown on Figure 4-2-2, you can directly call the contact, add to local contact, add to blacklist or do other operations.

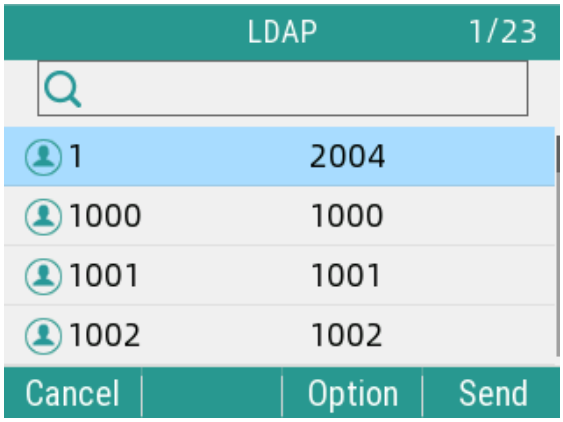

Figure 4-2-2