LDAP (Lightweight Directory Access Protocol)

A directory is a listing of information about objects arranged in some order that gives details about each object.

Common examples are a city telephone directory and a library card catalog.

In computer terms, a directory is a specialized database, also called a data repository, that stores typed and ordered information about objects.

Directories allow users or applications to find resources that have the characteristics needed for a particular task.

Installing LDAP

1. First Check LDAP Components

   # rpm -qa | grep ldap

2. You should reach to following files.

   If they are not present then you need to install them

   from yum or rpm

   openldap-servers-2.3.27-8.el5_2.4
   openldap-2.3.27-8.el5_2.4
   nss_ldap-253-13.el5_2.1
   python-ldap-2.2.0-2.1
   openldap-clients-2.3.27-8.el5_2.4

Let use LDAP as a phone book or a email directory.

You may want to use and orginazational view like

You can build your own using:

- l= Location
- ou= Organisational Unit
- o= Organisation
- dc= Domain Component
- st= State
- c= Country

For example I am going to use
dc=ax100,
dc=in.

Let us start :

1. Edit the file /etc/openldap/slapd.conf

The only thing that must be edited are
suffix, rootdn and
the two rootpw lines.

Suffix is the high level descriptor you selected above.

The rootdn is who (the user) that owns the server and should start with cn=.

The first root password (rootpw) line should be set to secret.

You can generate an encrypted password for the second rootpw line using the command:

slappasswd

Just cut and paste the output of the slappasswd command into the second rootpw line.

Sample Configuration :

```
database        ldbm
suffix          "dc=ax100,dc=in"
#suffix         "o=My Organization Name,c=US"
rootdn          "cn=Manager,dc=ax100,dc=in"
#rootdn         "cn=Manager,o=My Organization Name,c=US"
# 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          {SSHA}MRNBda83kd9f7d7did902mLA1x0AVOWMRBua
# The database directory MUST exist prior to running slapd AND
```

Now Edit the file /etc/openldap/ldap.conf

This file is very simple. Just add the IP of your server (the localhost in this case) and the your 'Base' suffix.

Sample Configuration :

```
#SIZELIMIT    12
#TIMELIMIT    15
#DEREF        never
HOST 127.0.0.1
BASE dc=ax100,dc=in
```

Now start the server

```
#  service ldap start
```

LDAP Migration tools

PADL Software Ltd. has a collection of tools, written in Perl, that you can use to convert configuration files to the LDIF format.
If you are planning to use your LDAP server to authenticate users you want these tools.

These tools are located in /usr/share/openldap/migration.

You then must edit migrate_common.ph and change the following site-specific variables to reflect your installation:

```
# Default DNS domain
$DEFAULT_MAIL_DOMAIN = ”ax100.in";

# Default base
$DEFAULT_BASE = "dc=ax100,dc=in
```

Create a data file :
(YourOrg.ldif)

Now we need to add the base entries into the LDAP. Here is an example of a new base org. units you may need and a user new user. The file we will create in out example is ax100.in.ldif.

```
dn: dc=ax100,dc=in
objectclass: top
objectclass: organization
o: ax100
description: Top level LDAP for ax100.in
dn: ou=Group,dc=ax100,dc=in
ou: Group
objectClass: top
objectClass: organizationalUnit
```

```
dn: ou=People,dc=ax100,dc=in
ou: People
objectClass: top
objectClass: organizationalUnit

dn: ou=Services,dc=ax100,dc=in
ou: Services
objectClass: top
objectClass: organizationalUnit
```

The simple way to add this stuff is to use the utility

migration_base.pl.

It will create serveral fields you need for things like Services, Mounts and People.

/usr/share/openldap/migration/migrate_base.pl > base.ldif

Importing the first records

Now we need to import the ldif file we just created.

If your ldap server is not running, start it.

Then run this command to import your ldif file. Here is an example.

```
#  ldapadd -a -W -x -D "cn=Manager,dc=ax100,dc=in" -f base.ldif
```

Dumping the all the LDAP data

To test the server we can list the entire contents.
The program to do this is ldapsearch.

We pass it our base orginazation and something to search for.

Every LDAP record has an object class associated with it so we can ask for all object classes to get all records.

```
#   ldapsearch -x -b 'dc=ax100,dc=in' 'objectclass=*'
```

The output of this command should look like the LDIF file we created

Create a test record

Create a file name newrec.ldif and create the needed fields.

```
# Garrett Barnett, < style="font-weight: bold;">ax100, in
dn: uid=gman,ou=People,dc=ax100,dc=in
cn: Garrett Barnett
sn: Barnett
objectClass: top
objectClass: person
objectClass: posixAccount
objectClass: shadowAccount
userPassword: {crypt}$!Z0ksiAKjsKLAsjuwyuAK!jksX
```

uid: gman
    uidNumber: 501
    gidNumber: 501
    loginShell: /bin/bash
    homeDirectory: /home/gman
    shadowLastChange: 10877
    shadowMin: 0
    shadowMax: 999999
    shadowInactive: -1
    shadowWarning: 7
    shadowFlag: 0
    shadowExpire: -1

The dn: record must be uniqe and should include the include your suffix.

Add the record to your LDAP

To add a record to the ldap database we use the command ldapadd.

```
#  ldapadd -W -x -D "cn=Manager,dc=ax100,dc=in" -W -f newrec.ldif
```

Display the record

```
ldapsearch -x -b 'cn=Garrett Barnett,dc=ax100,dc=in'
```

Delete the test record

Now you have a record you need to delete.

```
ldapdelete -W -x -D 'cn=Manager,dc=ax100,dc=in''cn=Garrett Barnett,dc=ax100,dc=in'
```

Migrating /etc/passwd and /etc/group

These tools are very simple to use. After you have installed them

```
/usr/share/openldap/migration/migrate_passwd.pl /etc/passwd > passwd.ldif

ldapadd -W -x -D "cn=Manager,dc=ax100,dc=in" -f passwd.ldif

/usr/share/openldap/migration/migrate_group.pl /etc/group > group.ldif

ldapadd -W -x -D "cn=Manager,dc=ax100,dc=in" -f group.ldif
```

Securing your LDAP

First, if you havn't added an encrypted password to the

/etc/openldap/slapd.conf file

yet, do it now.