xCAT 2 LDAP How-To

6/27/2008

Table of Contents

1.0 Introduction: Scalable User Authentication with LDAP

WARNING: LDAP security is not addressed. Consult your local LDAP expert (or become one). At a minimum consider `hosts.allow` and `hosts.deny`. LDAP performance is not addressed. You may need to investigate LDAP setup options for performance enhancements.

> **NOTE**: If you really want to understand LDAP, then pick up the text *Mastering OpenLDAP*, by Matt Butcher.

LDAP is a client/server directory service that can be used to distribute just about anything of interest. In the case of authentication we are only concerned about users, groups, and passwords.

LDAP may be configured as flat (one-to-many), i.e. all LDAP clients will use the same LDAP server. Or, LDAP may be configured as hierarchical (one-to-many, many-to-many), i.e. all LDAP clients can use the primary LDAP server or a shadow (replicated) LDAP server. The 2nd option increases scalability.

Throughout this document the primary LDAP server will be referred to as the *management* node. Shadow (or replication) LDAP servers will be referred to as *service* nodes. All LDAP client nodes will be referred to as *compute*, *user*, or *head* nodes.

There are four configuration files that need to be maintained (not all nodes need all configuration files):

- `/etc/ldap.conf`: This LDAP configuration file is used only by nodes that require user (not root) authentication, i.e. *compute*, *user*, and *head* nodes. Do not setup users on nodes that users should not be on, i.e. *management* and *service* nodes.
- `/etc/openldap/ldap.conf`: This LDAP configuration file is used by the `ldap*` client commands, e.g. `ldapsearch`, `ldappasswd`, etc… All nodes should have this setup for testing and troubleshooting.
- `/etc/openldap/slapd.conf`: This LDAP configuration file is used by nodes that need to provide LDAP services to clients, i.e. *management* and *service* nodes.
- `/etc/nsswitch`. This system configuration file is used by anything that needs to resolve users, groups, or passwords, i.e. authentication, direction listings, etc... This file should only be setup on nodes that will need to resolve user information (e.g. username from user ID). More on this later.

1.1 LDAP Installation Requirements

All nodes should have the LDAP clients installed (i.e. the `ldap*` commands):

```
openldap-clients-*
```

Only the management and service nodes need to have the LDAP servers installed:

```
openldap-*
openldap-servers-*
```

NSS support for LDAP should only be installed on nodes that require user, group, and password name services (e.g. *compute*, *user*, *head*, and *login* nodes):

```
nss_ldap-*
```

NOTE: You may wish or find it easier to install all the RPMs on all nodes and then configure them properly.

2.0 Setup LDAP on Primary Server

2.1 Install LDAP

```
yum install openldap-servers
```

or download from:

http://download.fedora.redhat.com/pub/fedora/linux/releases/8/Everything/x86_64/os/Packages/

The following rpms should be installed:

```
openldap-*
openldap-devel-*
openldap-clients-*
openldap-servers-*

If using LDAP 2.4  also install :

migrationtools-*
```

2.2 Configure LDAP on the Primary Server

Throughout this document the LDAP suffix **dc=cluster,dc=net** will be used. You can use any value you like. The convention is to match your domain name. e.g. `foo.bar.org` becomes `dc=foo,dc=bar,dc=org`.

All nodes should have `/etc/openldap/ldap.conf` defined. This LDAP client configuration file tells the `ldap*` commands what node is the LDAP server. This file requires the following two lines:

```
BASE    dc=cluster,dc=net
URI      ldap://ldap_server_hostname
```

The `BASE` is the default suffix and the `URI` is the location of the LDAP server.

For nodes that run as LDAP servers (e.g. service and management) then `URI` should be set to `ldap://127.0.0.1`. This setup will aid with troubleshooting server problems, i.e. if you cannot talk to yourself, then nobody can talk to your either.

For client nodes the `URI` should be point to a service or management node. For our example, our management node is mn20, our service node is rrra000. ldap://mn20.

1.1.1 Edit /etc/openldap/ldap.conf

On LDAP primary Server or master node , edit /etc/openldap/ldap.conf as follows:

```
BASE    dc=cluster,dc=net
URI      ldap://127.0.0.1
```

Backup /etc/openldap/slapd.conf.

```
cp /etc/openldap/slapd.conf  /etc/openldap/slapd.conf.ORIG
```

The following `/etc/openldap/slapd.conf` is a good base for the LDAP primary server node, i.e. the node that will manage the LDAP data. Create a new /etc/openldap/slapd.conf file containing the following lines:

```
include /etc/openldap/schema/core.schema
include /etc/openldap/schema/cosine.schema
include /etc/openldap/schema/inetorgperson.schema
include /etc/openldap/schema/nis.schema
include /etc/openldap/schema/misc.schema

pidfile /var/run/openldap/slapd.pid
argsfile /var/run/openldap/slapd.args
loglevel 0

database  hdb
suffix  "dc=cluster,dc=net"
rootdn  "cn=root,dc=cluster,dc=net"
rootpw {SSHA}SHdbpFVBnX7qreNL+DYPsqqlrJWq/W16
directory /var/lib/ldap
index objectclass,entryCSN,entryUUID    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
password-hash {SSHA}
access to attrs=userPassword
    by dn="uid=admin,ou=People,dc=cluster,dc=net" write
    by anonymous auth
    by self write
    by * none
access to attrs=shadowLastChange
    by dn="uid=admin,ou=People,dc=cluster,dc=net" write
    by self write
    by * read

###sync provider
modulepath      /usr/lib64/openldap
moduleload      syncprov
overlay syncprov
syncprov-checkpoint 100 10
```

```
syncprov-sessionlog 100
###sync
```

The values in **bold** should be changed to match your environment. With the exception of the LDAP `rootpw`, the changes are limited to the suffix.

The big picture explanation for this LDAP server configuration file:

1. loglevel 0 means log nothing. loglevel 4 will give good debug, loglevel -1 will give all debug
2. Use the `hdb` database format and store my stuff in `/var/lib/ldap`.
3. Index a bunch of stuff to increase performance.
4. Declare the LDAP root password using the SSHA hash algorithm. Use the `slappasswd` command to generate this. e.g. slappasswd prompts for new password and gives encrypted string which is placed in the slapd.conf file for rootpw attribute. Our password is **cluster,** which will be used in later client configuration file and when running ldap commands.

   ```
   [root@xcat20RRmn ~]# slappasswd
   New password:
   Re-enter new password:
   {SSHA}SHdbpFVBnX7qreNL+DYPsqqlrJWq/W16
   ```
5. Allow root to change any password.
6. Allow users to change their own passwords.
7. Become a sync provider to allow service nodes to replicate.

NOTE: The lines under `access to` must be indented. Indented lines in `slapd.conf` indicate an extension of the previous line.

NOTE: The last section (`sync provider`) can be removed if you have no plans to add service nodes to help with large scale-out environments. However it will not hurt to leave it there for future use.

2.2.1 Setup LDAP tuning options

For openldap earlier than 2.4:

```
cp /etc/openldap/DB_CONFIG.example /var/lib/ldap/DB_CONFIG
```

If using openLDAP 2.4 or later:

```
vi /var/lib/ldap/DB_CONFIG and add the following lines:
```

```
set_cachesize 0 268435456 1
set_lg_regionmax 262144
```
set_lg_bsize 2097152

2.2.2 Start LDAP on the Primary Server

Make ldap userid id the owner and group for the /var/lib/ldap directory . This is the location of your database and other ldap files.

```
cd /var/lib
chown ldap.ldap ldap
```

start ldap to make sure "OK"

```
service ldap start
```

Check the syntax of your slapd.conf file

```
slaptest -v -f /etc/openldap/slapd.conf
may get hdb_monitor_db_open: monitoring disabled; configure monitor database to
   enable  - ignore
config file testing succeeded
```

2.2.3 Migrate Users on the Master Node into LDAP

The following new user id can be setup for testing the migration

1. export /home (rw) for testing

```
 echo '/home *(rw,no_root_squash,sync)' >> /etc/exports
 exportfs -a
```

2. add a test userid "ibm" which will be added to the LDAP database

```
useradd ibm
mkdir ~ibm/.ssh
mkdir ~ibm/.pbs_spool
```

3. Assign a password

```
passwd ibm
```

4. Generate root ssh keys for mn20 and give ibm id root ssh authority

```
ssh-keygen -t rsa -q -N "" -f ~ibm/.ssh/id_rsa
cp ~ibm/.ssh/id_rsa.pub ~ibm/.ssh/authorized_keys

vi  ~ibm/.ssh/config
```

Add the following lines:

```
ForwardX11 yes
StrictHostKeyChecking no
FallBackToRsh no
BatchMode yes
ConnectionAttempts 5
UsePrivilegedPort no
Compression no
Cipher blowfish
UserKnownHostsFile /dev/null
CheckHostIP no
```

5. Set permissions :

```
chown -R ibm.ibm ~ibm
chmod 700 ~ibm/.ssh
chmod 600 ~ibm/.ssh/*
```

Note: openLDAP 2.4 and above package the migration tools are in the migrationtools* rpm; make sure this is installed. See .

For openLDAP 2.4 :

```
cd /usr/share/migrationtools/migration
```

For openLDAP 2.3 (or earlier)

```
cd /usr/share/openldap/migration
```

6. Migrate :

```
cp migrate_common.ph migrate_common.ph.save
```

Edit migrate_common.ph and change the following lines to be:

```
vi migrate_common.ph
$DEFAULT_MAIL_DOMAIN = "cluster.net";
$DEFAULT_BASE = "dc=cluster,dc=net";
$EXTENDED_SCHEMA = 1;
```

Run:

```
./migrate_base.pl >/tmp/base.ldif
./migrate_passwd.pl /etc/passwd >>/tmp/base.ldif
./migrate_group.pl /etc/group >>/tmp/base.ldif
cd /var/lib/ldap
service ldap stop
slapadd -l /tmp/base.ldif
chown ldap.ldap *
service ldap start
```

7. Test the database by searching for a the user ibm:

```
ldapsearch -x -v -D  "cn=root,dc=cluster,dc=net" -w cluster  -b
   "ou=People,dc=cluster,dc=net" "uid=ibm"
```

Output should be as follows:

```
ldap_initialize( <DEFAULT> )
filter: uid=ibm
requesting: All userApplication attributes
# extended LDIF
#
# LDAPv3
# base <ou=People,dc=cluster,dc=net> with scope subtree
# filter: uid=ibm
# requesting: ALL
#

# ibm, People, cluster.net
dn: uid=ibm,ou=People,dc=cluster,dc=net
uid: ibm
cn: ibm
sn: ibm
mail: ibm@cluster.net
objectClass: person
objectClass: organizationalPerson
objectClass: inetOrgPerson
objectClass: posixAccount
objectClass: top
objectClass: shadowAccount
userPassword:: e2NyeXB0fSEh
shadowLastChange: 13998
shadowMax: 99999
shadowWarning: 7
loginShell: /bin/bash
uidNumber: 501
gidNumber: 501
homeDirectory: /home/ibm

# search result
search: 2
result: 0 Success

# numResponses: 2
# numEntries: 1
```

2.2.4 Add a User to LDAP

Setup a new user adduser.ldif file with the following contents:

```
dn: uid=ibm4,ou=People,dc=cluster,dc=net
uid: ibm4
cn: ibm4
sn: ibm4
mail: ibm4@cluster.net
objectClass: person
objectClass: organizationalPerson
```

```
objectClass: inetOrgPerson
objectClass: posixAccount
objectClass: top
objectClass: shadowAccount
shadowLastChange: 13998
shadowMax: 99999
shadowWarning: 7
loginShell: /bin/bash
uidNumber: 504
gidNumber: 504
homeDirectory: /home/ibm4
```

Run:

```
   ldapadd -x -c -D  "cn=root,dc=cluster,dc=net" -w cluster -f adduser.ldif

adding new entry "uid=ibm4,ou=People,dc=cluster,dc=net"
```

Verify:

```
ldapsearch -x -v -D  "cn=root,dc=cluster,dc=net" -w cluster  -b
   "ou=People,dc=cluster,dc=net" "uid=ibm4"
```

2.2.5 Modify a User in LDAP

Setup a new user moduser.ldif file with the following contents:

```
dn: uid=ibm4,ou=People,dc=cluster,dc=net
uid: ibm4
cn: ibm4
sn: ibm4
mail: ibm4@cluster.net
objectClass: person
objectClass: organizationalPerson
objectClass: inetOrgPerson
objectClass: posixAccount
objectClass: top
objectClass: shadowAccount
shadowLastChange: 13998
shadowMax: 99999
shadowWarning: 7
loginShell: /bin/bash
uidNumber: 504
gidNumber: 504
homeDirectory: /home/ibm44 <---- modification
```

Run:

```
ldapmodify -x -c -D  "cn=root,dc=cluster,dc=net" -w cluster -f moduser.ldif

modifying entry "uid=ibm4,ou=People,dc=cluster,dc=net"
```

Verify:

```
ldapsearch -x -v -D  "cn=root,dc=cluster,dc=net" -w cluster  -b
   "ou=People,dc=cluster,dc=net" "uid=ibm4"
```

2.2.6 Set LDAP Userid Password

Root sets the password to ibm4

```
ldappasswd -x -w cluster -D 'cn=root,dc=cluster,dc=net' -s ibm4
   'uid=ibm4,ou=People,dc=cluster,dc=net'
Result: Success (0)
```

User sets the password to ibm4

```
ldappasswd -x -w ibm4 -D 'uid=ibm4,ou=People,dc=cluster,dc=net' -s ibm4
   'uid=ibm4,ou=People,dc=cluster,dc=net'
Result: Success (0)
```

3.0 Setup Hierarchical LDAP

If you do not plan to use Hierarchical LDAP with shadow LDAP Servers you can skip to Setup LDAP Client.

For Hierarchical LDAP the Service Node(s) will be set as a shadow server(s) to the LDAP Master server on the Master Node. The process will describe putting the configuration changes into the diskless image. If you are using diskfull service nodes, then make the same configuration changes on the installed service nodes.

3.1 Setup Service node(s) as LDAP Shadow Server

The installation and setup of LDAP on the service nodes described below will be either done into the diskless image or on the service node files, if using diskfull installation. For diskfull, you may choose to create the appropriate edited files on the Primary Server in a temporary directory and then xdcp them to the Service node (s), since the files will be the same for all shadow servers.

3.1.1 Install required LDAP rpms and dependencies

For diskless install the rpms into the image:

yum --installroot=/install/netboot/fedora8/x86_64/service/rootimg \

```
  install openldap-clients nss_ldap nfs-utils vi openldap-devel openldap-
servers
```

For diskfull install these same rpms on the service node (s) which will be LDAP shadow servers.

3.1.2 Update the LDAP Configuration in Service Node image

For diskless:

```
Export SNIMAGE=/install/netboot/fedora8/x86_64/service/rootimg
```

3.1.2.1 Edit /etc/openldap/ldap.conf

For diskless:

edit $SNIMAGE/etc/openldap/ldap.conf as follows:

For diskfull:

edit /etc/openldap/ldap.conf as follows:

```
BASE    dc=cluster,dc=net
URI      ldap://127.0.0.1
```

3.1.2.2 Edit slapd configuration file

Backup /etc/openldap/slapd.conf.

For diskless:

Edit $SNIMAGE/etc/openldap/slapd.conf file:

For diskfull:

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

`sldap.conf` looks similar to the management or primary LDAP server configuration (see Configure LDAP on the Primary Server) with `access to` and `sync provider` omitted, but with a `syncrepl` section added:

```
include         /etc/openldap/schema/core.schema
include         /etc/openldap/schema/cosine.schema
```

```
include         /etc/openldap/schema/inetorgperson.schema
include         /etc/openldap/schema/nis.schema
include         /etc/openldap/schema/misc.schema

pidfile         /var/run/openldap/slapd.pid
argsfile        /var/run/openldap/slapd.args
loglevel        0

database        hdb
suffix          "dc=cluster,dc=net"
rootdn          "cn=root,dc=cluster,dc=net"
rootpw          {SSHA}AW/VeGc+5csvRZoayPl+FnRGluxDJyaJ
directory       /var/lib/ldap
index objectclass,entryCSN,entryUUID    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
password-hash {SSHA}

###sync consumer
syncrepl rid=NNN
    provider=ldap://management_node
    type=refreshOnly
    interval=00:00:01:00
    searchbase="dc=cluster,dc=net"
    binddn="cn=root,dc=cluster,dc=net"
    credentials=cluster
###sync consumer
```

The fields in **bold** should be customized for your environment. Most should be obvious with the exception of `credentials` and `rid`. `rid` should be a unique number per service node. `credentials` should be the plain text (ouch!) rootpw password. Make sure `ldap` owns this file and the permissions are 600.

The last two configurations files (`/etc/ldap.conf` and `/etc/nsswitch`) go hand-in-hand. Nodes that require user, group, and password name services will need both files setup (e.g. *compute, user*, *head*, and *login* nodes).

3.1.2.3 Edit /etc/ldap.conf

Edit the $SNIMAGE/etc/ldap.conf file or /etc/ldap.conf for diskfull.

The following `ldap.conf` should provide anonymous access to *`ldap_server`*.

```
host ldap_server
base dc=cluster,dc=net
timelimit 120
bind_timelimit 120
idle_timelimit 3600
nss_base_passwd ou=People,dc=cluster,dc=net
nss_base_shadow ou=People,dc=cluster,dc=net
nss_base_group ou=Group,dc=cluster,dc=net
nss_initgroups_ignoreusers
root,ldap,named,avahi,haldaemon,dbus,radvd,tomcat,radiusd,news,mailman,nscd
```

The fields in `bold` should be customized for your environment.

3.1.2.4 Edit /etc/nsswitch

$SNIMAGE`/etc/nsswitch` or /etc/nsswitch for diskfull should have the following lines updated to include `ldap`:

```
passwd:     files ldap
shadow:     files
group:      files ldap
```

`shadow` was explicitly skipped. Most cluster environments do not allow users to login to nodes with password authentication. However *user* and *head* nodes often allow this.

3.1.2.5 Setup user password authentication

In the case where you require that users access nodes with password authentication update $SNIMAGE`/etc/nsswitch` or /etc/nsswitch for diskfull with:

```
shadow:    files ldap
```

And append to $SNIMAGE/etc/ldap.conf or /etc/ldap.conf for diskfull:

```
pam_filter objectclass=People
pam_login_attribute uid
pam_lookup_policy yes
pam_password md5
```

Make ldap userid id the owner and group for the /var/lib/ldap directory

```
cd $SNIMAGE/var/lib or /var/lib
chown ldap.ldap ldap
```

3.1.2.6 Setup LDAP tuning options

Copy the configuration tuning file into the image or on the Service Node

For openldap earlier than 2.4:

For diskless:

```
  cp $SNIMAGE/etc/openldap/DB_CONFIG.example $SNIMAGE/var/lib/ldap/DB_CONFIG

For diskfull:
  cp /etc/openldap/DB_CONFIG.example /var/lib/ldap/DB_CONFIG
```

If using openLDAP 2.4 or later:

```
For diskles:
  vi $SNIMAGE/var/lib/ldap/DB_CONFIG and add the following lines:
For diskfull:
  vi /var/lib/ldap/DB_CONFIG and add the following lines:


set_cachesize 0 268435456 1
set_lg_regionmax 262144
set_lg_bsize 2097152
```

3.1.3 Build the Service Node diskless image and install

Set to start LDAP in the servicenode table after install , if not already set.

```
chtab node=service servicenode.ldapserver=1

cd /opt/xcat/share/xcat/netboot/fedora
./geninitrd -i eth0 -n tg3,bnx2,sunrpc,lockd,nfs,nfs_acl -o fedora8 -p service

nodeset rra000 netboot
rpower rra000 boot
```

3.1.4 Install the Service Node diskfull

Set to start LDAP in the servicenode table after install , if not already set.

```
chtab node=service servicenode.ldapserver=1


nodeset rra000 install
rpower rra000 reset
```

3.1.5 Test the Shadow Server

Add a userid (e.g. Ibm6) to the database on the Master Node:
See section 2.2.4, Add a User to LDAP.

Go to the Service Node and search the database for the new user id.
Run:

```
ldapsearch -x -v -D  "cn=root,dc=cluster,dc=net" -w cluster  -b
   "ou=People,dc=cluster,dc=net" "uid=ibm6"
```

4.0 Setup LDAP Client

4.1.1 Setup LDAP on the Compute Nodes

Note: if using diskless image the LDAP this setup will be added the configuration file changes needed to that image before the install. If the compute nodes are diskfull, just add the changes to the LDAP configuration files on the installed node. For example, you can create an updated LDAP configuration file in a tmp space on the Management Node and then xdcp it to all the diskfull nodes.

All nodes should have the LDAP clients installed (i.e. the `ldap*` commands):

```
openldap-clients-*
```

NSS support for LDAP should only be installed on nodes that require user, group, and password name services (e.g. *compute*, *user*, *head*, and *login* nodes):

```
nss_ldap-*
```

NOTE: The lazy (or efficient) may wish to install all the RPMs on all nodes and then configure them properly.

For diskless, install need ldap rpms and dependencies into the image:

```
yum --installroot=/install/netboot/fedora8/x86_64/compute/rootimg \
        install openldap-clients nss_ldap nfs-utils vi
```

For diskfull, install additional rpms on the compute nodes.

4.1.2 Update the LDAP Configuration

For diskless:
export CPIMAGE=/install/netboot/fedora8/x86_64/compute/rootimg

```
cd $CPIMAGE/etc/openldap
```

For diskfull:

```
cd /etc/openldap
```

Note: there are two files /etc/ldap.conf and /etc/openldap/ldap.conf to edit

4.1.2.1 Update /etc/openldap/ldap.conf

All nodes should have **`/etc/openldap/ldap.conf`** defined or $CPIMAGE/etc/openldap/ldap.conf if diskless. This LDAP client configuration file tells the `ldap*` commands what LDAP server to communicate with. This file requires the following two lines:

If non-hierarchical:

```
BASE    dc=cluster,dc=net
URI     ldap://mn20
```

If hierarchical:

```
BASE    dc=cluster,dc=net
URI     ldap://rra000
```

The `BASE` is the default suffix and the `URI` is the location of the LDAP server. In our example the server is mn20. For client nodes the `URI` should be point to a management node or the service node of the client, if using hierarchy.

4.1.2.2 Update /etc/ldap.conf

The last two configurations files (`/etc/ldap.conf` and `/etc/nsswitch`) go hand-in-hand. Nodes that require user, group, and password name services will need both files setup (e.g. compute, user, head, and login nodes).

The following `/etc/ldap.conf` should provide anonymous access to *`ldap_server`*. This is sufficient, if using hierarchical xCAT support for LDAP and the Service Node is setup as a shadow server with anonymous access to the LDAP server. See Setup Hierarchical LDAP.

If diskless:

Create $CPIMAGE/etc/ldap.conf with the following lines:

If diskfull

Create /etc/ldap.conf with the following lines:

```
host <management_node or Service node>
base dc=cluster,dc=net
timelimit 120
bind_timelimit 120
idle_timelimit 3600
nss_base_passwd ou=People,dc=cluster,dc=net
nss_base_shadow ou=People,dc=cluster,dc=net
nss_base_group ou=Group,dc=cluster,dc=net
nss_initgroups_ignoreusers
root,ldap,named,avahi,haldaemon,dbus,radvd,tomcat,radiusd,news,mailman,nscd
```

But if you are not using a Service Node with anonymous access ,that is the nodes use the management node for LDAP the following lines should also be be added to `/etc/ldap.conf` or `$CPIMAGE/etc/ldap.conf` for diskless.

```
binddn cn=root,dc=cluster,dc=net
bindpw cluster
rootbinddn cn=root,dc=cluster,dc=net
```

This is because the management node setup above is not setup for anonymous access. The service node setup for anonymous access because it is read-only replica of the management node. The fields in **`bold`** should be customized for your environment.

4.1.2.3 Update /etc/nsswitch

Last but not least `/etc/nsswitch` or $CPIMAGE/etc/nsswitch should have the following lines updated to include `ldap`:

```
passwd:     files ldap
shadow:     files
group:      files ldap
```

`shadow` was explicitly skipped. Most cluster environments do not allow users to login to nodes with password authentication. However *user* and *head* nodes often allow this.

4.1.2.4 Setup user password authentication with LDAP

In the case where you require that users access nodes with password authentication then update `/etc/nsswitch` on the node or in the image with:

```
shadow:     files ldap
```

And append to `/etc/ldap.conf`:

```
pam_filter objectclass=People
pam_login_attribute uid
pam_lookup_policy yes
pam_password md5
```

Add to fstab to Mount /home for testing:

```
mn20:/home /home nfs timeo=14,intr 1 2
```

4.1.3 Install and test

Add the following rpms for testing. Note: the order of modules in the geninitrd command is important!

```
bnx2,sunrpc,lockd,nfs,nfs_acl
```

If using diskless:

```
cd /opt/xcat/share/xcat/netboot/fedora
./geninitrd -i eth0 -n tg3,bnx2,sunrpc,lockd,nfs,nfs_acl -o fedora8 -p compute
packimage -o fedora8 -p compute -a x86_64
nodeset rra001a netboot
rpower rra001a boot
```

If diskfull:

```
nodesetup rra0001a install
rpower rra001a reset
```

4.1.4 Test LDAP Client

```
ssh to rra001a
```

Run:

```
ldapsearch -x -v -D  "cn=root,dc=cluster,dc=net" -w cluster  -b
   "ou=People,dc=cluster,dc=net" "uid=ibm"
```

Check to see if you get output from the LDAP server as in section 2.2.3, Migrate Users on the Master Node into LDAP.

Now authenticate the ibm users from LDAP by changing it's password and su to ibm.

```
passwd ibm
su – ibm
```

2.0 Other Documentation Available

- xCAT man pages: http://xcat.sf.net/man1/xcat.1.html
- xCAT DB table descriptions: http://xcat.sf.net/man5/xcatdb.5.html
- Installing xCAT on iDataPlex: http://xcat.svn.sourceforge.net/svnroot/xcat/xcat-core/trunk/xCAT-client/share/doc/xCAT-iDpx.pdf
- xCAT2.0 Cookbook: http://xcat.svn.sourceforge.net/svnroot/xcat/xcat-core/trunk/xCAT-client/share/doc/xCAT2.pdf
- Monitoring Your Cluster with xCAT: http://xcat.svn.sourceforge.net/svnroot/xcat/xcat-core/trunk/xCAT-client/share/doc/xCAT2-Monitoring.pdf
- xCAT on AIX Cookbook: http://xcat.svn.sourceforge.net/svnroot/xcat/xcat-core/trunk/xCAT-client/share/doc/xCAT2onAIX.pdf

- xCAT wiki: http://xcat.wiki.sourceforge.net/
- xCAT mailing list: http://xcat.org/mailman/listinfo/xcat-user
- xCAT bugs: https://sourceforge.net/tracker/?group_id=208749&atid=1006945
- xCAT feature requests: https://sourceforge.net/tracker/?group_id=208749&atid=1006948
- Mastering *OpenLDAP*, by Matt Butcher.