Install OpenLDAP

Install the OpenLDAP software as follows:

1. Log in to the appropriate application server as **root**: (e.g. using **dzdo**):

login as: **(your AD user)**  
Red Hat Enterprise Linux Server release 6.7 (Santiago)  
Kernel 2.6.32-573.12.1.el6.x86\_64 on an x86\_64

Last login: Fri Jan 6 12:44:50 2017 from 10.74.1.224  
[duffye@uqscnap730 ~]$ **dzdo su -**  
AD Password: **(your AD password)**  
[root@uqscnap730 ~]#

1. Invoke yum to install the required software:

[root@uqscnap730 ~]# **yum -y install openldap-servers openldap-clients**  
Loaded plugins: product-id, refresh-packagekit, rhnplugin, security, subscription-manager  
This system is receiving updates from RHN Classic or RHN Satellite.  
Setting up Install Process  
Resolving Dependencies  
(...Lots of other output...)

Complete!

Configure LDAP Credentials

Setup the initial configuration of OpenLDAP as follows:

1. We'll set up a root DN user of **ldapadmin**. Pick a password for this user and note it in the usual places. Now encrypt your password:

[root@uqscnap730 ~]# **slappasswd**  
New password: **(your ldapadmin password)**  
Re-enter new password: **(your lpadmin password)**  
{SSHA}XfWiF59FLwEbUPpAxUE8U7zjXaaIlFHe

1. Copy the string returned by the above command (from your system, not the example above) into your paste buffer.
2. Invoke the editor of your choice to open the file **/etc/openldap/slapd.d/cn=config/olcDatabase={2}hdb.ldif**.
3. Make the following changes (near the top of the file):
   1. Modify the **olcSuffix** definiton to read:  
      olcSuffix: dc=localhost
   2. Modify the **olcRootDN** definition to read:  
      olcRootDN: cn=ldapadmin,dc=localhost
   3. Add the following new line below the above one:  
      olcRootPW: (paste encrypted password here)
4. Save the changes to the file and exit

Start the OpenLDAP Service

Perform the following commands to start up the OpenLDAP service and ensure it will auto-start on server reboot:

[root@uqscnap730 ~]# **chkconfig --level 23456 slapd on**  
[root@uqscnap730 ~]# **service slapd start**  
Checking configuration files for slapd:                    [WARNING]  
5874e762 ldif\_read\_file: checksum error on "/etc/openldap/slapd.d/cn=config/olcDatabase={2}bdb.ldif"  
config file testing succeeded  
Starting slapd:                                            [ OK ]

Edit olcDatabase={1}monitor.ldif, to give access for the user (update the user)

olcAccess: {0}to \* by dn.base="gidNumber=0+uidNumber=0,cn=peercred,cn=extern  
al,cn=auth" read by dn.base="**cn=ldapadmin,dc=localhost**" read by \* none

Now add schema, once openldap is started

Now go to /etc/openldap/slapd.d/cn=config and add the following

ldapadd -Y EXTERNAL -H ldapi:/// -f /etc/openldap/schema/java.ldif

ldapadd -Y EXTERNAL -H ldapi:/// -f /etc/openldap/schema/cosine.ldif

ldapadd -Y EXTERNAL -H ldapi:/// -f /etc/openldap/schema/nis.ldif  
ldapadd -Y EXTERNAL -H ldapi:/// -f /etc/openldap/schema/inetorgperson.ldif  
ldapadd -Y EXTERNAL -H ldapi:/// -f /etc/openldap/schema/duaconf.ldif  
ldapadd -Y EXTERNAL -H ldapi:/// -f /etc/openldap/schema/dyngroup.ldif  
ldapadd -Y EXTERNAL -H ldapi:/// -f /etc/openldap/schema/misc.ldif  
ldapadd -Y EXTERNAL -H ldapi:/// -f /etc/openldap/schema/openldap.ldif  
ldapadd -Y EXTERNAL -H ldapi:/// -f /etc/openldap/schema/ppolicy.ldif  
ldapadd -Y EXTERNAL -H ldapi:/// -f /etc/openldap/schema/collective.ldif

Restart the service

service slapd stop

service slapd start

Check your configuration by running the following command:

[root@uqscnap730 ~]# **slaptest -u**  
5874e590 ldif\_read\_file: checksum error on "/etc/openldap/slapd.d/cn=config/olcDatabase={2}bdb.ldif"  
config file testing succeeded

Checksum errors, such as those in the example above, are fine. If any other errors are returned, return to step 1 above and try again.

Add the Initial Structure

We now need to add some structure (OUs) to hold our config. This can be done with the following command:

[root@uqscnap730 ~]# **ldapadd -x -W -D "cn=ldapadmin,dc=localhost"**  
Enter LDAP Password: **(ldapadmin password)**

**If this command gives invalid credentials error please check the password and config files are proper. If everything looks correct try the below command**

**/usr/bin/ldapadd -x -W -D "cn=ldapadmin,dc=localhost"**

The command will now pause, waiting for input. Enter the text in the **Initial structure** code block below, but please note:

1. Copy and pasting from wiki can change the formatting. If this happens, you'll receive the error "ldap\_add: Protocol error (2)". To avoid this problem, paste the text into a text editor, fix the formatting, copy your fixed text then paste it in.
2. If you get still the error , try adding each entry one by one
3. You'll receive various "adding new entry" messages along the way. These are normal.

**Initial structure**

|  |
| --- |
| dn: dc=localhost  objectClass: dcObject  objectClass: organization  o: localhost  dc: localhost    dn: ou=jndi,dc=localhost  objectClass: organizationalUnit  objectClass: top  ou: jndi    dn: ou=users,dc=localhost  objectClass: organizationalUnit  objectClass: top  ou: users    dn: ou=groups,dc=localhost  objectClass: organizationalUnit  objectClass: top  ou: groups |

Finally, press **<Control>-D** to signify end of input. The command will run and you will be returned to the shell prompt.

Run a Test Search

Now run a quick test search to check that the LDAP database looks OK:

[root@uqscnap730 ~]# **ldapsearch -x -b 'ou=jndi,dc=localhost'**  
# extended LDIF  
#  
# LDAPv3  
# base <ou=jndi,dc=localhost> with scope subtree  
# filter: (objectclass=\*)  
# requesting: ALL  
#

# jndi, localhost  
dn: ou=jndi,dc=localhost  
objectClass: organizationalUnit  
objectClass: top  
ou: jndi

# search result  
search: 2  
result: 0 Success

# numResponses: 2  
# numEntries: 1

Check that the output looks similar to that above.