1. ***Lightweight Directory Access Protocol*** *is an industry standard, lightweight, widely used set of protocols for accessing directory services.*
2. *LDAP is an open-source implementation of Lightweight Directory Access Protocol developed by LDAP project.*
3. *LDAP is an Internet protocol that email and other programs use to look up contact information from a server.*
4. *LDAP is available for all major Linux distributions, AIX, Android, HP-UX, OS X, Solaris, Windows and OS.*
5. *LDAP has unlideeped space to store the information.*
6. *LDAP is also used as a backend database for “single sign-on”.where one password for a user is shared between many services.*

***At server site***

***Give a host entry in a file vi /etc/hosts .***

192.168.72.80 a.deep.com a

192.168.72.81 b.deep.com b

***Now Install LDAP at Server side***

yum -y install openldap compat-openldap openldap-clients openldap-servers openldap-servers-sql openldap-devel

systemctl start slapd

systemctl enable slapd

***Check LDAP***

netstat -antup | grep -i 389

**Give LDAP admin password by command**

slappasswd

Will take a new password

*New password:*

*Re-enter new password:*

{SSHA}H/9vfTXKQLvPhf+eS/IPBxGqcGILgHTS

***Now Configure LDAP server***

OpenLDAP servers configuration files are found in /etc/openldap/slapd.d/. To start with the configuration of LDAP.

**we would need to update the variables “olcSuffix” and “olcRootDN**“.

***1.olcSuffix*** *–* Database Suffix, it is the domain name for which the LDAP server provides the information. OR it should be changed to your domain name.

***2.olcRootDN*** *–* Root Distinguished Name (DN) entry for the user who has the unrestricted access to perform all administration activities on LDAP, like a root user.

***3.olcRootPW*** *–* LDAP admin password for the above RootDN.

***Now create a .ldif file*** *at main page*

vi db.ldif

Replace the encrypted password with the password you generated previous.

dn: olcDatabase={2}hdb,cn=config

changetype: modify

replace: olcSuffix

olcSuffix: dc=deep,dc=com

dn: olcDatabase={2}hdb,cn=config

changetype: modify

replace: olcRootDN

olcRootDN: cn=ldapadm,dc=deep,dc=com

dn: olcDatabase={2}hdb,cn=config

changetype: modify

replace: olcRootPW

olcRootPW: {SSHA}H/9vfTXKQLvPhf+eS/IPBxGqcGILgHTS

***Once entry given to ldif file, send the configuration to the LDAP server.***

ldapmodify -Y EXTERNAL -H ldapi:/// -f db.ldif

***Do not edit manually Make a changes in /etc/openldap/slapd.d/cn=config/olcDatabase={1}monitor.***

***Now crteate a file***

vi monitor.ldif

dn: olcDatabase={1}monitor,cn=config

changetype: modify

replace: olcAccess

olcAccess: {0}to \* by dn.base="gidNumber=0+uidNumber=0,cn=peercred,cn=external, cn=auth" read by dn.base="cn=ldapadm,dc=deep,dc=com" read by \* none

**If done then send the configuration to the LDAP server.**

ldapmodify -Y EXTERNAL -H ldapi:/// -f monitor.ldif

***Now Copy the sample database configuration file to /var/lib/ldap and update the file permissions.***

cp /usr/share/openldap-servers/DB\_CONFIG.example /var/lib/ldap/DB\_CONFIG

chown ldap:ldap /var/lib/ldap/\*

***And Add the cosine and nis LDAP schemas.***

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

***Now Create base.ldif file for your domain and write content inside the file***

vi base.ldif

dn: dc=deep,dc=com

dc: deep

objectClass: top

objectClass: domain

dn: cn=ldapadm ,dc=deep,dc=com

objectClass: organizationalRole

cn: ldapadm

description: LDAP Manager

dn: ou=People,dc=deep,dc=com

objectClass: organizationalUnit

ou: People

dn: ou=Group,dc=deep,dc=com

objectClass: organizationalUnit

ou: Group

***And enter the data by command given belown***

ldapadd -x -W -D "cn=ldapadm,dc=deep,dc=com" -f base.ldif

Enter LDAP Password:

Output:

*adding new entry "dc=deep,dc=com"*

*adding new entry "cn=ldapadm ,dc=deep,dc=com"*

*adding new entry "ou=People,dc=deep,dc=com"*

*adding new entry "ou=Group,dc=deep,dc=com"*

***Now Install and Configure phpLDAPAdmin***

1. *phpLDAPAdmin is a web application for administering LDAP servers. It provides an easy way to manage LDAP servers over a web browser.*
2. *It is a web application, this LDAP browser works on many platforms such as Ubuntu, Debian, Redhat derivatives, Fedora, openSUSE, FreeBSD, OpenBSD, and Solaris.*
3. *phpLDAPAdmin is the perfect tool for LDAP professionals and entry-level administrators.*
4. *phpLDAPAdmin is not available in the main repository, so you need to enable EPEL repository for Redhat based derivatives.*

***Now install repository given below;***

*rpm -ivh https://dl.fedoraproject.org/pub/epel/epel-release-latest-7.noarch.rpm*

*yum -y install epel-release*

*yum install -y phpldapadmin*

***Now change in phpmyadmin configuration file;***

*vi /etc/httpd/conf.d/phpldapadmin.conf*

***Change in the configuration file shown below***

*# Apache 2.4*

*# Require local*

*Require all granted*

*IfModule>*

*<IfModule !mod\_authz\_core.c>*

*# Apache 2.2*

*Order Deny,Allow*

*Deny from all*

*Allow from 127.0.0.1*

*Allow from ::1*

*systemctl restart httpd.service*

***Now change in phpLDAPadmin configuration file.***

*vi /etc/phpldapadmin/config.php*

*$servers->setValue('server','name','Deepak LDAP Server'); (line no. 291)*

*$servers->setValue('server','base',array('dc=deep,dc=com')); (line no. 305)*

*$servers->setValue('login','attr','dn');*

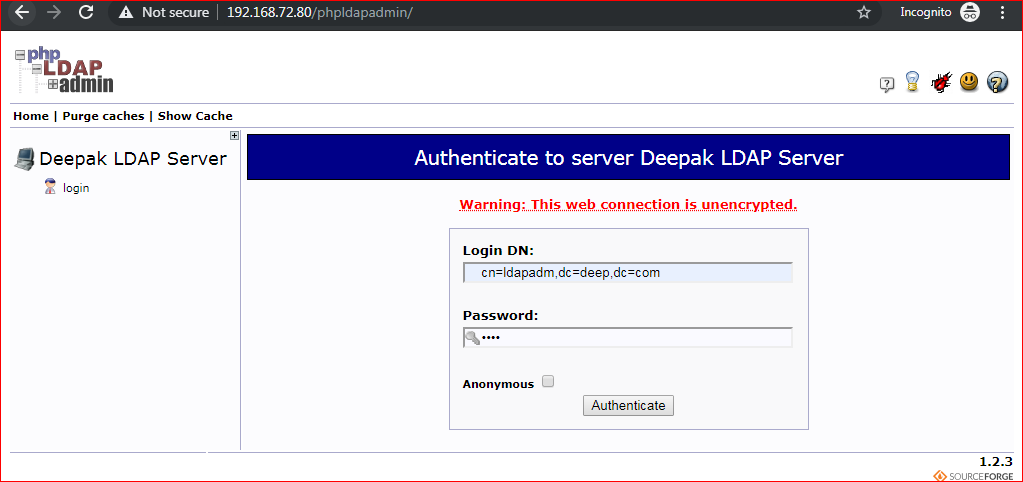
*// $servers->setValue('login','attr','uid');*

***(Uncomment the line 397 and comment out the 398)***

***Stop and Disable the firewall***

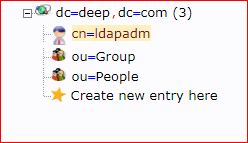
***Open web and type the following URL.***

*http://192.168.72.80/phpldapadmin*

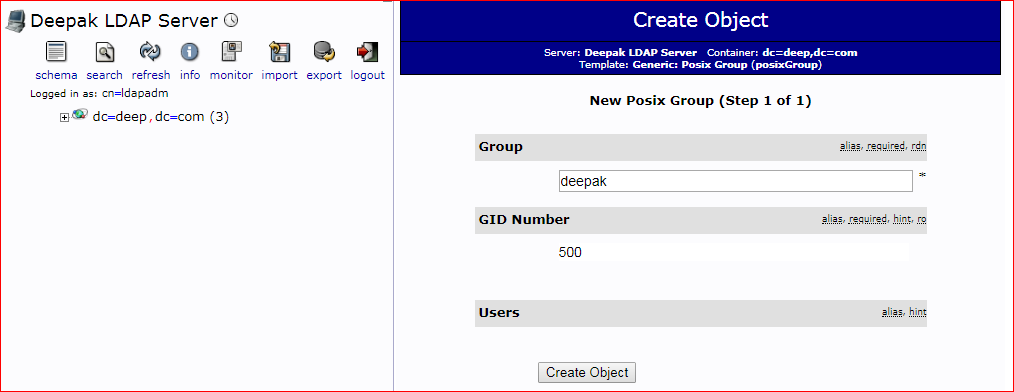


*Now click on (+)*

|  |  |
| --- | --- |
|  |  |

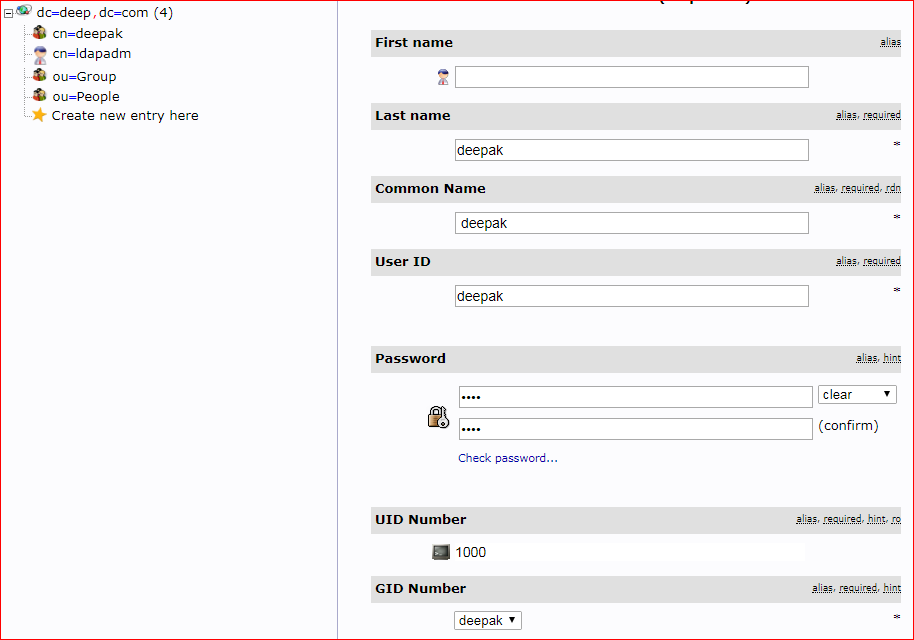


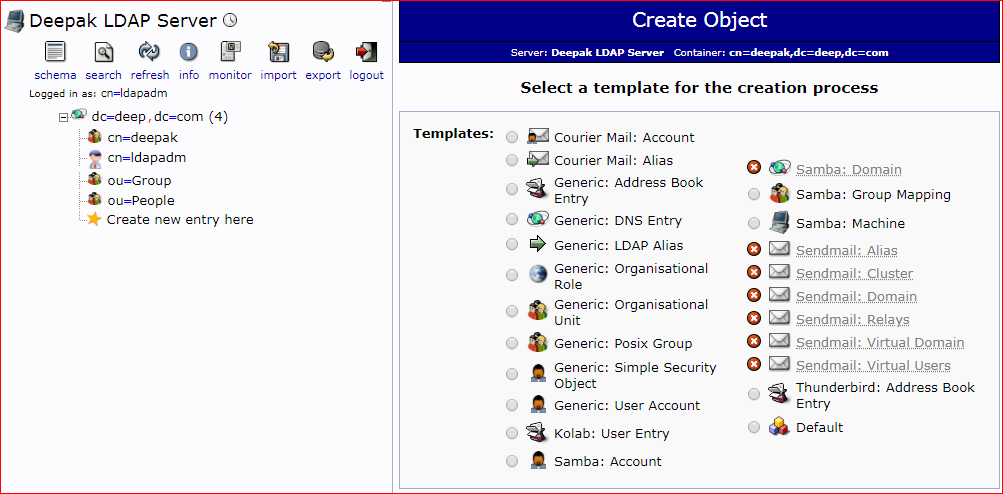
|  |  |  |  |
| --- | --- | --- | --- |
| |  |  | | --- | --- | |  |  | |  |



*Now [->](http://192.168.72.92/phpldapadmin/cmd=template_engine&server_id=1&container=dc=mit,dc=com)*[*Create a child entry here*](http://192.168.72.92/phpldapadmin/cmd.php?cmd=template_engine&server_id=1&container=dc%3Dmit%2Cdc%3Dcom)

|  |  |
| --- | --- |
| *http://192.168.72.92/phpldapadmin/images/default/ldap-user.png* | *Generic: User Account* |





*Now click on user account*

***Now create LDAP user on CLI;***

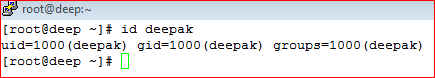
*useradd deepak*

*passwd deepak*

*cat /etc/passwd*

*To* ***check uid or gid of your user***

id deepak



*For a new user deepak Let’s create an LDIF file*

*vi deep.ldif*

*dn: uid=abhi,ou=People,dc=deep,dc=com*

*objectClass: top*

*objectClass: account*

*objectClass: posixAccount*

*objectClass: shadowAccount*

*cn: abhi*

*uid: abhi*

*uidNumber: 1000*

*gidNumber: 1000*

*homeDirectory: /home/deepak*

*loginShell: /bin/bash*

*gecos: deepak [Admin (at) deep]*

*userPassword: temp*

*shadowLastChange: 17058*

*shadowMin: 0*

*shadowMax: 99999*

*shadowWarning: 7*

***Use the ldapadd command with the above file to create a new user called “deep” in OpenLDAP directory.***

*ldapadd -x -W -D "cn=ldapadm,dc=deep,dc=com" -f deep.ldif*

***Now assign a password to the user***

*ldappasswd -s temp -W -D "cn=ldapadm,dc=deep,dc=com" -x "uid=deepak ,ou=People,dc=deep,dc=com"*

***-s*  *specify the password for the username.***

***-x* *username for which the password is changed*.**

***-D* *Distinguished name to authenticate to the LDAP server.***

***Now LDAP client configuration;***

***Install LDAP client packages on the client machine.***

*yum install -y openldap-clients nss-pam-ldapd*

***Now add the client machine to LDAP server for single sign-on.***

*authconfig --enableldap --enableldapauth --ldapserver=192.168.72.80 --ldapbasedn="dc=deep,dc=com" --enablemkhomedir --update*

*systemctl restart nslcd*

***Now check LDAP Login by command "getent passwd deepak" from LDAP Server and output will be same as;***



***Also, We can varify using "su - deepak"***