**Ldap(openldap) install and configuration on centos 7**

**OpenLDAP is an open-source implementation of Lightweight Directory Access Protocol developed byOpenLDAP project. LDAP is an Internet protocol that email and other programs use to look up contactinformation from a server. It is released under OpenLDAP public license; it is available for allmajor Linux distributions, AIX, Android, HP-UX, OS X, Solaris, Windows and z/OS.**

**It functions as a relational database in certain ways and can be used to store any information.**

**LDAP is not limited to store the information; it is also used as a backend database for “single sign-on”.where one password for a user is shared between many services.**

**MY ENVIRONMENT SETUP:**

**HostName IP Address OS Purpose**

server.mit.com 192.168.72.92 centos 7 LDAP Server

client.mit.com 192.168.72.95 centos 7 LDAP Client

OR

**Make an host entry on each machine in vi /etc/hosts for name resolution.**

192.168.72.92 server.mit.com server

192.168.72.95 client.mit.com client

**Install OpenLDAP Packages**

**For server configuration:**

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

**Start the LDAP service and enable.....!!!**

systemctl start slapd

systemctl enable slapd

**Verify the LDAP.......!!!!**

netstat -antup | grep -i 389

**Setup LDAP admin password**

slappasswd

New password:

Re-enter new password:

{SSHA}H/9vfTXKQLvPhf+eS/IPBxGqcGILgHTS

**Configure OpenLDAP 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. In simple words,

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 administrationactivities on LDAP, like a root user.

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

**Please create a .ldif file**.

vi db.ldif

**Replace the encrypted password ({SSHA}d/thexcQUuSfe3rx3gRaEhHpNJ52N8D3) with the password you generated in the previous step.**

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

changetype: modify

replace: olcSuffix

olcSuffix: dc=mit,dc=com

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

changetype: modify

replace: olcRootDN

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

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

changetype: modify

replace: olcRootPW

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

**Once you are done with the ldif file, send the configuration to the LDAP server.**

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

**Make a changes to /etc/openldap/slapd.d/cn=config/olcDatabase={1}monitor.ldif (Do not edit manually) file to restrict the**

**monitor access only to ldap root (ldapadm) user not to others.**

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=mit,dc=com" read by \* none

**Once you have updated the file, send the configuration to the LDAP server.**

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

**Set up LDAP database**

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

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

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

**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

**Generate base.ldif file for your domain.**

vi base.ldif

dn: dc=mit,dc=com

dc: mit

objectClass: top

objectClass: domain

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

objectClass: organizationalRole

cn: ldapadm

description: LDAP Manager

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

objectClass: organizationalUnit

ou: People

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

objectClass: organizationalUnit

ou: Group

**Build the directory structure.**

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

Output:

Enter LDAP Password:

adding new entry "dc=mit,dc=com"

adding new entry "cn=ldapadm ,dc=mit,dc=com"

adding new entry "ou=People,dc=mit,dc=com"

adding new entry "ou=Group,dc=mit,dc=com"

**Install and Configure phpLDAPAdmin**

**phpLDAPAdmin (aka PLA) is a web application for administering LDAP servers. It provides an easy way to manage LDAP servers over a web browser. It is written in PHP language and is licensed under the GNU GPL.**

**Since it is a web application, this LDAP browser works on many platforms such as Ubuntu, Debian, Redhat derivatives, Fedora, openSUSE, FreeBSD, OpenBSD, and Solaris.**

**phpLDAPAdmin is the perfect tool for LDAP professionals and entry-level administrators.**

**phpLDAPAdmin is not available in the main repository, so you need to enable EPEL repository for Redhat based derivatives.**

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

yum -y install epel-release

yum install -y phpldapadmin

**In CentOS 7, web access is managed by mod\_authz\_core.c module; so regular allow or deny rules won’t work even if you modify.**

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

**(Update the configuration file shown like below. Hash out the Red and Add the Green one.)**

Alias /phpldapadmin /usr/share/phpldapadmin/htdocs

Alias /ldapadmin /usr/share/phpldapadmin/htdocs

usr/share/phpldapadmin/htdocs>

<IfModule mod\_authz\_core.c>

# 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

</IfModule>

</Directory>

systemctl restart httpd.service

**Now, setup phpLDAPadmin by modifying some of its configuration values.**

vi /etc/phpldapadmin/config.php

$servers->setValue('server','name',' Abhis LDAP Server');

$servers->setValue('server','base',array('dc=mit,dc=com'));

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

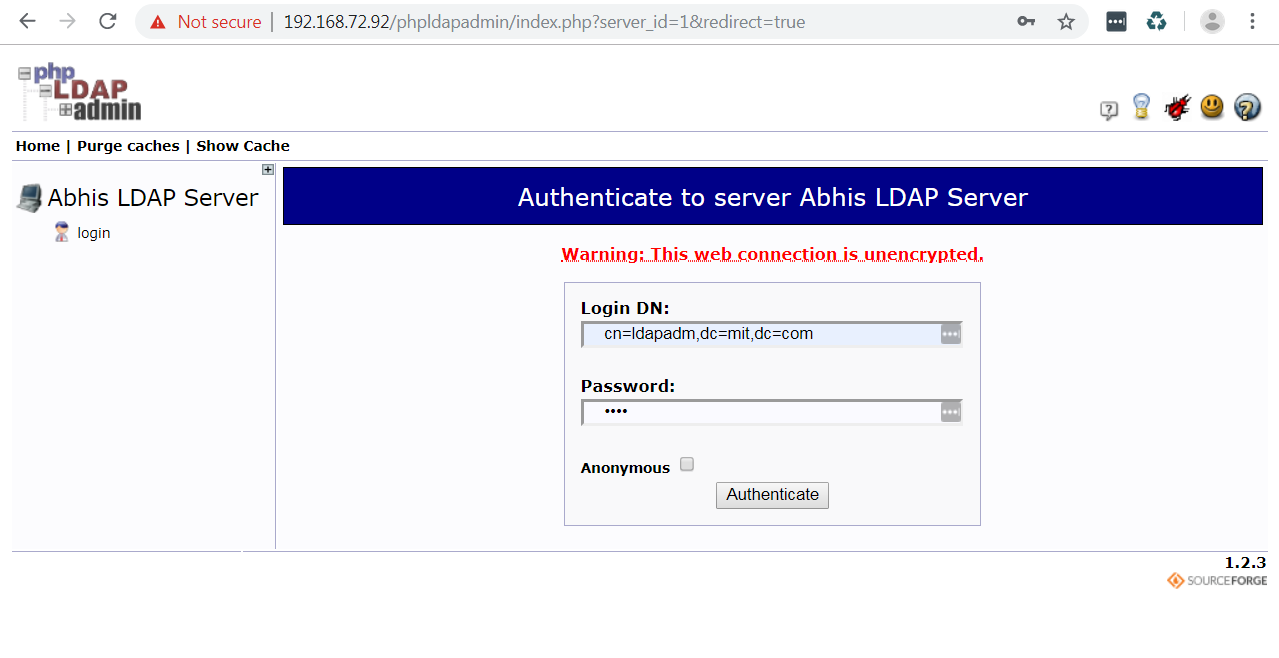
// $servers->setValue('login','attr','uid');

**(Uncomment the line 397 and comment out the 398, like above.)**

**Open up the web browser and navigate it to the following URL.**

http://192.168.72.92/phpldapadmin

now login in ladpaadmin



click on +

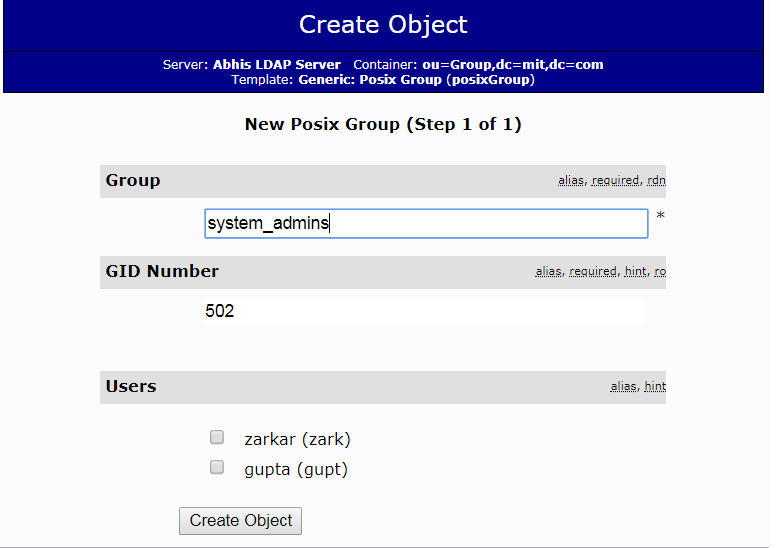
|  |  |
| --- | --- |
|  | [+-](http://192.168.72.92/phpldapadmin/cmd.php?server_id=1&redirect=true)[->](http://192.168.72.92/phpldapadmin/cmd.php?cmd=template_engine&server_id=1&dn=dc=mit,dc=com) [dc**=**mit**,**dc**=**com (6)](http://192.168.72.92/phpldapadmin/cmd.php?cmd=template_engine&server_id=1&dn=dc%3Dmit%2Cdc%3Dcom) |

[->](http://192.168.72.92/phpldapadmin/cmd.php?cmd=template_engine&server_id=1&dn=ou=Group,dc=mit,dc=com) [ou**=**Group (1)](http://192.168.72.92/phpldapadmin/cmd.php?cmd=template_engine&server_id=1&dn=ou%3DGroup%2Cdc%3Dmit%2Cdc%3Dcom)

create

|  |  |
| --- | --- |
| Create | [Create a child entry](http://192.168.72.92/phpldapadmin/cmd.php?cmd=template_engine&server_id=1&container=ou%3DGroup%2Cdc%3Dmit%2Cdc%3Dcom) |

|  |  |  |  |
| --- | --- | --- | --- |
| |  |  | | --- | --- | | http://192.168.72.92/phpldapadmin/images/default/ldap-ou.png | Generic:PosixGroup | |  |

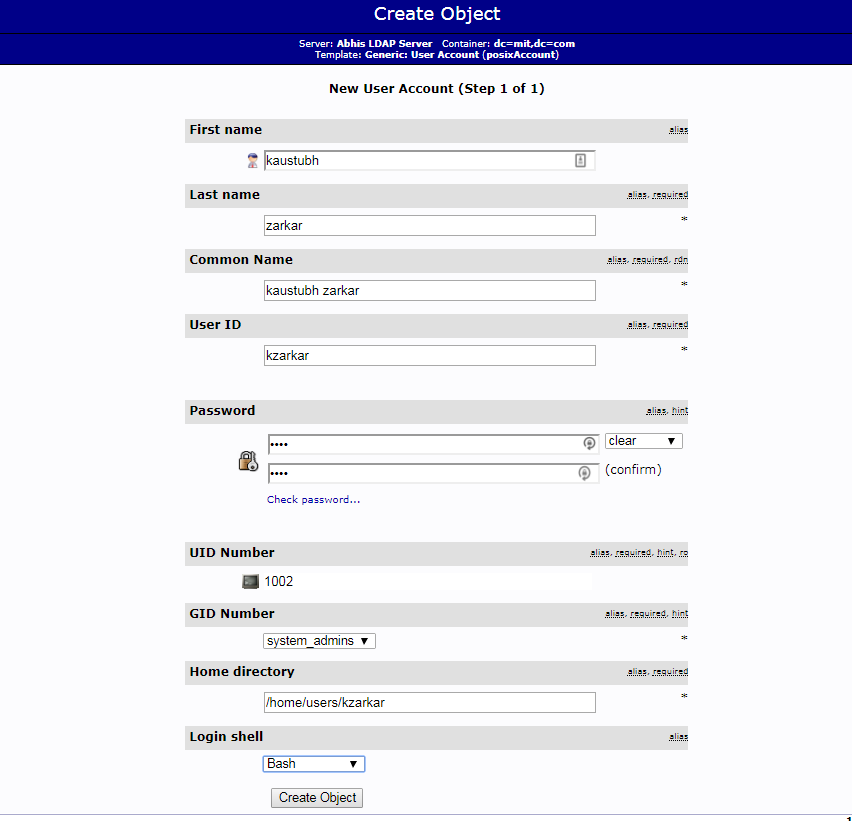


**after that commit and update**

now you can create user

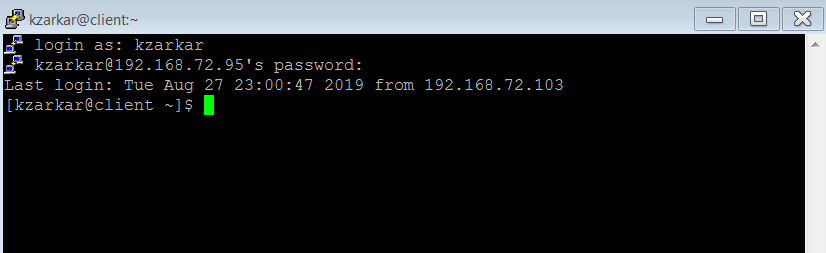
[->](http://192.168.72.92/phpldapadmin/cmd=template_engine&server_id=1&container=dc=mit,dc=com) [Create new entry here](http://192.168.72.92/phpldapadmin/cmd.php?cmd=template_engine&server_id=1&container=dc%3Dmit%2Cdc%3Dcom)

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



then create object and commit

now we can login any ladap client server



(NOTE: First you have to configure ldap client, this proceed mention below )

**Create LDAP user On Command Line Inteface**

useradd abhi

cat /etc/passwd

**Command to check uid or gid of your user.....!!!!**

id abhi

uid=1000(abhi) gid=1000(abhi) groups=1000(abhi)

Let’s create an LDIF file for a new user called abhi.

vi abhi.ldif

dn: uid=abhi,ou=People,dc=mit,dc=com

objectClass: top

objectClass: account

objectClass: posixAccount

objectClass: shadowAccount

cn: abhi

uid: abhi

uidNumber: 1000

gidNumber: 1000

homeDirectory: /home/abhi

loginShell: /bin/bash

gecos: abhi [Admin (at) mit]

userPassword: temp

shadowLastChange: 17058

shadowMin: 0

shadowMax: 99999

shadowWarning: 7

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

ldapadd -x -W -D "cn=ldapadm,dc=mit,dc=com" -f abhi.ldif

**Output: – Enter ldapadm password.**

Enter LDAP Password:

adding new entry "uid=abhi,ou=People,dc=mit,dc=com"

**Assign a password to the user.....!!!!!**

ldappasswd -s temp -W -D "cn=ldapadm,dc=mit,dc=com" -x "uid=abhi,ou=People,dc=mit,dc=com"

**Where,**

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

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

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

**LDAP client configuration to use LDAP Server**

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

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

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

authconfig --enableldap --enableldapauth --ldapserver=192.168.72.92 --ldapbasedn="dc=mit,dc=com" --enablemkhomedir --update

**Restart the LDAP client service...**

systemctl restart nslcd

**Verify or Testing LDAP Login**

**getent command to get the LDAP entries from the LDAP server**

getent passwd abhi

Output: abhi:x:1000:1000:abhi [Admin (at) mit]:/home/abhi:/bin/bash

getent passwd kzarkar

kzarkar:\*:1002:502:kaustubh zarkar:/home/users/kzarkar:/bin/bash

You can see Groups also by using belows comman

getent group

To verify the LDAP, log in using the LDAP user “abhi” "kzarkar"on the client machine.

sudo su - abhi

Output:

Creating directory '/home/abhi'.

/usr/bin/id: cannot find name for group ID 1000

[abhi@fresh ~]$

........finished....!!!!!!!!