

# **Open LDAP Server Installation and Configuration**

**( Prepared by Sijeesh Kunnotharamal )**

## Reference Link :

<https://medium.com/how-to-config/how-to-install-and-configure-openldap-and-phpldapadmin-on-an-centos-server-6-5-df8ac08e33b1>

### Install epel packages

```
yum -y install epel-release  
( You may need to cd /etc/yum.repos.d/ edit epel*.repo files disable  
gpgcheck and comment out all lines starting with mirrorlist and  
uncomment all lines with baseurl )
```

### Install Open LDAP Packages

```
yum -y install openldap*
```

### Execute the following commands

```
cp /usr/share/openldap-servers/DB_CONFIG.example /var/lib/ldap/DB_CONFIG  
chown ldap. /var/lib/ldap/DB_CONFIG  
service slapd start
```

Use the command **slappasswd** to generate encrypted password.

**Create a file setrootpass.ldif add the following lines , replace the highlighted password field with password created**

```
dn: olcDatabase={0}config,cn=config  
changetype: modify  
add: olcRootPW  
olcRootPW: {SSHA}7ncqfmnkUw1CxVqklKk7tQRP1ptOW4fX
```

Execute ldapadd command with following options.

```
ldapadd -Y EXTERNAL -H ldapi:/// -f setrootpass.ldif
```

Create domain.ldif and add following lines , replace the example with the domain name.

```
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=Manager,dc=example,dc=com" read by * none

dn: olcDatabase={2}bdb,cn=config
changetype: modify
replace: olcSuffix
olcSuffix: dc=example,dc=com

dn: olcDatabase={2}bdb,cn=config
changetype: modify
replace: olcRootDN
olcRootDN: cn=Manager,dc=example,dc=com

dn: olcDatabase={2}bdb,cn=config
changetype: modify
add: olcRootPW
olcRootPW: {SSHA}0rK0gKVn13Ith2oFH9Bvm2InMBYnpwjv

dn: olcDatabase={2}bdb,cn=config
changetype: modify
add: olcAccess
olcAccess: {0}to attrs=userPassword,shadowLastChange by
  dn="cn=Manager,dc=example,dc=com" write by anonymous auth by self
write by * none
olcAccess: {1}to dn.base="" by * read
olcAccess: {2}to * by dn="cn=Manager,dc=server,dc=world" write by *
read
```

Execute the bellow line

```
ldapmodify -Y EXTERNAL -H ldapi:/// -f domain.ldif
```

**Create file basedomain.ldif and add bellow lines**

```
dn: dc=example,dc=com
objectClass: top
objectClass: dcObject
objectclass: organization
o: example
dc: example
```

```
dn: cn=Manager,dc=example,dc=com
objectClass: organizationalRole
cn: Manager
description: Directory Manager
```

```
ldapadd -x -D cn=Manager,dc=example,dc=com -W -f basedomain.ldif
```

**Can use ldapsearch command to make sure our LDAP service is properly working.**

```
ldapsearch -D cn="Manager,dc=example,dc=com"(bind user) -W -b
"dc=example,dc=com" objectClass=*
```

**Installation of php-ldapadmin tool**

```
yum install phpldapadmin
```

Open the file /etc/phpldapadmin/config.php and do the following changes.

**in line 305 add this**

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

**On line 397: uncomment, line 398: comment out**

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

**Line 332**

```
$servers->setValue('login','bind_id','cn=Manager,dc=example,dc=com');
```

Open the file /etc/httpd/conf.d/phpldapadmin.conf edit allow and deny IP addresses

open web browser and access the URL [http://LDAP\\_SERVER/ldapadmin](http://LDAP_SERVER/ldapadmin)

### **On Linux client machines**

```
yum install nss-pam-ldapd
```

```
authconfig --enableldap --enablemkhomedir --ldapserver=ldap://LDAP_Server_IP:389 \  
--ldapbasedn="dc=example,dc=com" --update
```

Or use authconfig-tui command.