Step by Step OpenLDAP Server Configuration on CentOS 7 / RHEL 7

[By **Raj**](https://www.itzgeek.com/author/admin) Last updated **Apr 3, 2018**

[**OpenLDAP**](https://www.itzgeek.com/tag/openldap) is an open-source implementation of Lightweight Directory Access Protocol developed by OpenLDAP project. LDAP is an Internet protocol that email and other programs use to look up contact information from a server. It is released under OpenLDAP public license; it is available for all major 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.

In this tutorial, we will configure OpenLDAP for centralized login where the users use the single account to log in to multiple servers.

This post covers only the OpenLDAP configuration without SSL. If you would like to configure OpenLDAP with SSL, then follow the below link after you complete this post.

**READ**:

## **Environment**

|  |  |  |  |
| --- | --- | --- | --- |
| **Host Name** | **IP Address** | **OS** | **Purpose** |
| server.itzgeek.local | 192.168.1.10 | CentOS 7 | LDAP Server |
| client.itzgeek.local | 192.168.1.20 | CentOS 7 | LDAP Client |

## **Prerequisites**

1. Make sure both LDAP server **“server.itzgeek.local” (192.168.1.10)** and LDAP client **“client.itzgeek.local” (192.168.1.20)** are accessible.

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

192.168.1.10 server.itzgeek.local server

192.168.1.20 client.itzgeek.local client

**OR**

If you plan to use a hostname instead of IP address, then configure DNS server using the article on [**How to Configure DNS Server on CentOS 7 / RHEL 7**](https://www.itzgeek.com/how-tos/linux/centos-how-tos/configure-dns-bind-server-on-centos-7-rhel-7.html).

Here I will use IP address for all the configuration.

If you are planning to Build LDAP server with Replication, then skip this tutorial and visit [**Configure OpenLDAP Multi-Master Replication on Linux**](https://www.itzgeek.com/how-tos/linux/centos-how-tos/configure-openldap-multi-master-replication-linux.html).

## **Install OpenLDAP Packages**

Install the following LDAP RPM packages on LDAP server (**server.itzgeek.local**).

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

Start the LDAP service and enable it for the auto start of service on system boot.

systemctl start slapd

systemctl enable slapd

Verify the LDAP.

netstat -antup | grep -i 389

**Output:**

tcp 0 0 0.0.0.0:389 0.0.0.0:\* LISTEN 1520/slapd

tcp6 0 0 :::389 :::\* LISTEN 1520/slapd

**READ**: **[netstat command not found on CentOS 7 / RHEL 7 – Quick Fix](https://www.itzgeek.com/how-tos/mini-howtos/netstat-command-not-found-on-centos-7-rhel-7-quick-fix.html)**

## **Setup LDAP admin password**

Run below command to create an LDAP root password. We will use this LDAP admin (root) password throughout this article.

Replace ldppassword with your password.

slappasswd -h {SSHA} -s ldppassword

The above command will generate an encrypted hash of entered password which you need to use in LDAP configuration file. So make a note of this and keep it aside.

**Output:**

{SSHA}d/thexcQUuSfe3rx3gRaEhHpNJ52N8D3

## **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**“.

**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.

**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.

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

The above entries need to be updated in /etc/openldap/slapd.d/cn=config/olcDatabase={2}hdb.ldif file. Manually edit of LDAP configuration is not recommended as you will lose changes whenever you run ldapmodify command.

Please create a **.ldif** file.

vi db.ldif

Add the below entries.

**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=itzgeek,dc=local

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

changetype: modify

replace: olcRootDN

olcRootDN: cn=ldapadm,dc=itzgeek,dc=local

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

changetype: modify

replace: olcRootPW

olcRootPW: **{SSHA}d/thexcQUuSfe3rx3gRaEhHpNJ52N8D3**

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

Use the below information.

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=itzgeek,dc=local" 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.example /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

Use the below information. You can modify it according to your requirement.

dn: dc=itzgeek,dc=local

dc: itzgeek

objectClass: top

objectClass: domain

dn: cn=ldapadm ,dc=itzgeek,dc=local

objectClass: organizationalRole

cn: ldapadm

description: LDAP Manager

dn: ou=People,dc=itzgeek,dc=local

objectClass: organizationalUnit

ou: People

dn: ou=Group,dc=itzgeek,dc=local

objectClass: organizationalUnit

ou: Group

Build the directory structure.

ldapadd -x -W -D "cn=ldapadm,dc=itzgeek,dc=local" -f base.ldif

The ldapadd command will prompt you for the password of ldapadm (LDAP root user).

**Output:**

Enter LDAP Password:

adding new entry "dc=itzgeek,dc=local"

adding new entry "cn=ldapadm ,dc=itzgeek,dc=local"

adding new entry "ou=People,dc=itzgeek,dc=local"

adding new entry "ou=Group,dc=itzgeek,dc=local"

## **Create LDAP user**

Instead of creating a new user, [**you can migrate the local users to LDAP**](https://www.itzgeek.com/how-tos/linux/centos-how-tos/migrate-local-users-ldap-accounts.html). Let’s create an LDIF file for a new user called raj.

vi raj.ldif

Paste the below lines to above LDIF file.

dn: uid=raj,ou=People,dc=itzgeek,dc=local

objectClass: top

objectClass: account

objectClass: posixAccount

objectClass: shadowAccount

cn: raj

uid: raj

uidNumber: 9999

gidNumber: 100

homeDirectory: /home/raj

loginShell: /bin/bash

gecos: Raj [Admin (at) ITzGeek]

userPassword: {crypt}x

shadowLastChange: 17058

shadowMin: 0

shadowMax: 99999

shadowWarning: 7

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

ldapadd -x -W -D "cn=ldapadm,dc=itzgeek,dc=local" -f raj.ldif

**Output: – Enter ldapadm password.**

Enter LDAP Password:

adding new entry "uid=raj,ou=People,dc=itzgeek,dc=local"

Assign a password to the user.

ldappasswd -s password123 -W -D "cn=ldapadm,dc=itzgeek,dc=local" -x "uid=raj,ou=People,dc=itzgeek,dc=local"

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.

Verify LDAP entries.

ldapsearch -x cn=raj -b dc=itzgeek,dc=local

**Output:**

# extended LDIF

#

# LDAPv3

# base <dc=itzgeek,dc=local> with scope subtree

# filter: cn=raj

# requesting: ALL

#

# raj, People, itzgeek.local

dn: uid=raj,ou=People,dc=itzgeek,dc=local

objectClass: top

objectClass: account

objectClass: posixAccount

objectClass: shadowAccount

cn: raj

uid: raj

uidNumber: 9999

gidNumber: 100

homeDirectory: /home/raj

loginShell: /bin/bash

gecos: Raj [Admin (at) ITzGeek]

shadowLastChange: 17058

shadowMin: 0

shadowMax: 99999

shadowWarning: 7

userPassword:: e1NTSEF9MkE2eUhIS0pJQVRnMHBCdkpVWjR5Q3JvTkJLTzdBTWY=

# search result

search: 2

result: 0 Success

# numResponses: 2

# numEntries: 1

To delete an entry from LDAP (**Optional**).

ldapdelete -W -D "cn=ldapadm,dc=itzgeek,dc=local" "uid=raj,ou=People,dc=itzgeek,dc=local"

## **Firewall**

Add the LDAP service to the firewall (TCP 389).

firewall-cmd --permanent --add-service=ldap

firewall-cmd --reload

## **Enable LDAP logging**

Configure Rsyslog to log LDAP events to log file /var/log/ldap.log.

vi /etc/rsyslog.conf

Add below line to /etc/rsyslog.conf file.

local4.\* /var/log/ldap.log

Restart the rsyslog service.

systemctl restart rsyslog

## **LDAP client configuration to use LDAP Server**

Install the necessary LDAP client packages on the client machine.

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

Execute the below command to add the client machine to LDAP server for single sign-on. Replace **“192.168.1.10”** with your LDAP server’s IP address or hostname.

authconfig --enableldap --enableldapauth --ldapserver=**192.168.1.10** --ldapbasedn="dc=itzgeek,dc=local" --enablemkhomedir --update

Restart the LDAP client service.

systemctl restart nslcd

## **Verify LDAP Login**

Use the getent command to get the LDAP entries from the LDAP server.

getent passwd raj

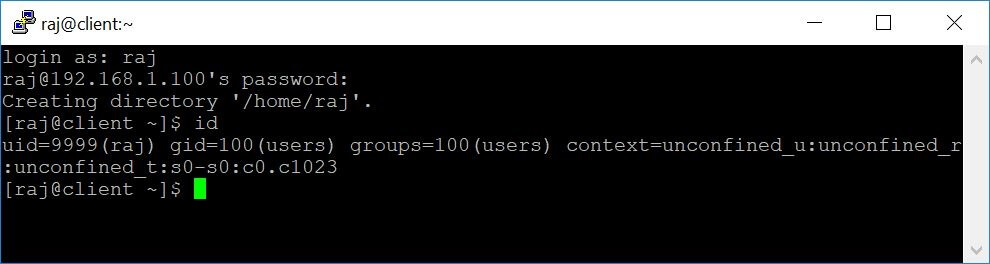
**Output:**

raj:x:9999:100:Raj [Admin (at) ITzGeek]:/home/raj:/bin/bash

**Screenshot:**

OpenLDAP Server Configuration on CentOS 7 - Verify LDAP LoginOpenLDAP Server Configuration on CentOS 7 – Verify LDAP Login

To verify the LDAP, log in using the LDAP user “**raj**” on the client machine.

OpenLDAP Server Configuration on CentOS 7 – LDAP User login on the Client machine

That’s All.