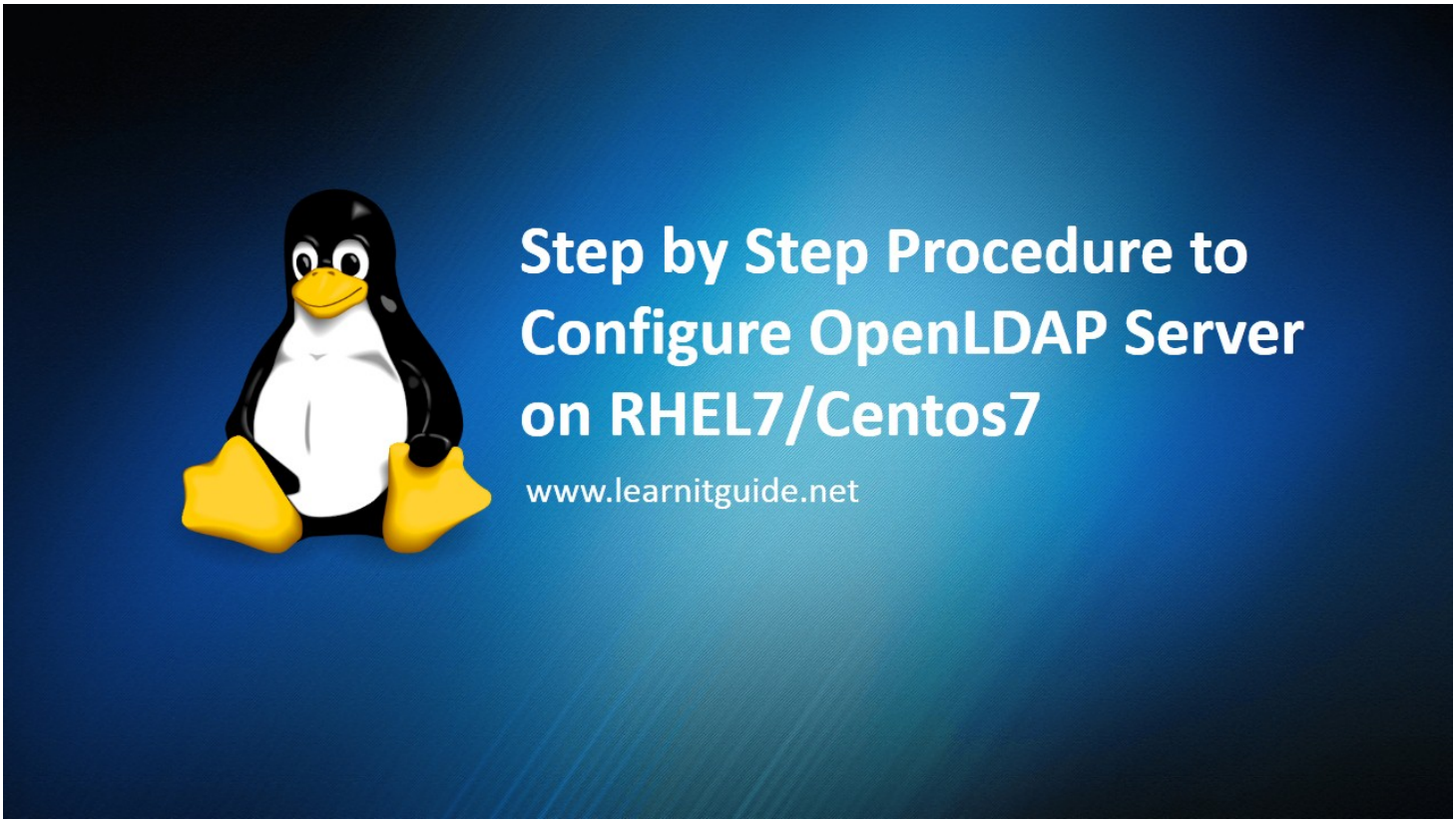


Step by Step OpenLDAP Server Configuration on RHEL7/Centos7

January 08, 2016

OpenLDAP Server Configuration on RHEL7/Centos7

This Tutorial describes you Step by Step Procedure to install and configure an OpenLDAP server and Client on RHEL7/CentOS7. Also watch the tutorial video below.

LDAP, or Lightweight Directory Access Protocol, is a protocol for managing related information from a centralized location through the use of a file and directory hierarchy. It functions in a similar way to a relational database in certain ways, and can be used to organize and store any kind of information. LDAP is commonly used for centralized authentication.

Our Lab Setup

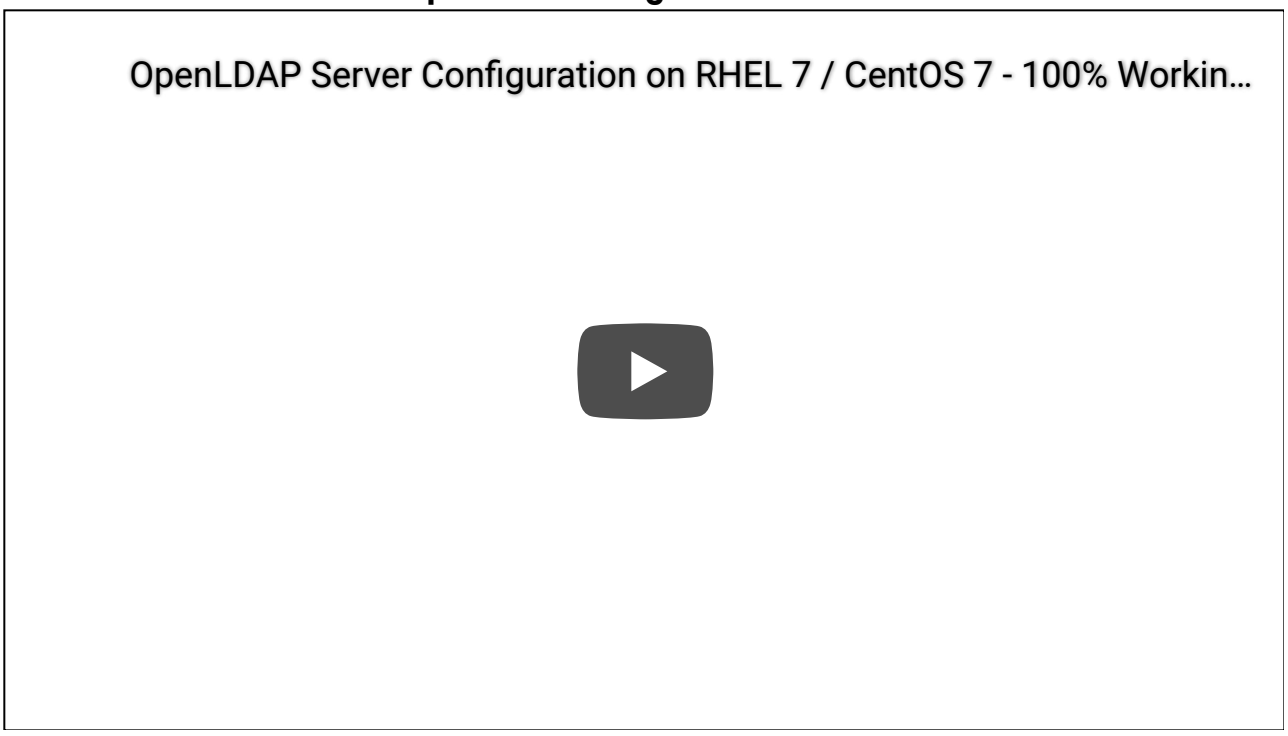
Description	Server Information	Client Information
Operating System	RHEL7 - 64 Bit	RHEL7 - 64 Bit
Host Name	linux1.learnitguide.net	linux2.learnitguide.net
IP Address	192.168.2.10	192.168.2.20

Use the following instructions to install and configure the LDAP Server and Ldap Client on Centos7/RHEL7.

Prerequisites:

1. Make sure both server Linux1(192.168.2.10) and client(192.168.2.20) are accessible.
2. Make an entry of each host in /etc/hosts for name resolution or Configure it in DNS to resolve the IP, if you use server name instead of IP address. Read also How to Configure DNS Server on RHEL7 But we use IP Address for reference.

Watch this OpenLDAP Configuration Video on YouTube



Server end configuration

Login into the server linux1 192.168.2.10 and do the following steps to configure OpenLDAP Server.

1. Install the required LDAP Packages "Openldap"

Install the appropriate LDAP packages "openldap" and "migrationtools" using yum to avoid dependencies issue. if yum is not configured, please refer the link Yum Configuration on Linux

```
[root@linux1 ~]# yum -y install openldap* migrationtools
```

2. Create a LDAP root passwd for administration purpose.

```
[root@linux1 ~]# slappasswd
New password:
Re-enter new password:
{SSHA}bHSiwuPJEypHS6zHSE2Uy7M69sQjmkPL
```

Copy the encrypted the passwd from the above output "{SSHA}bHSiwuPJEypHS6zHSE2Uy7M69sQjmkPL". Replace with your password and keep it aside.

3. Edit the OpenLDAP Server Configuration

OpenLDAP server Configuration files are located in **/etc/openldap/slapd.d/**.
Go to **cn=config** directory under **/etc/openldap/slapd.d/** and edit the **"olcDatabase={2}hdb.ldif"** for changing the configuration.

```
[root@linux1 ~]# cd /etc/openldap/slapd.d/cn=config
[root@linux1 cn=config]# vi olcDatabase={2}hdb.ldif
```

Change the variables of "**olcSuffix**" and "**olcRootDN**" according to your domain as below.

```
olcSuffix: dc=learnitguide,dc=net
olcRootDN: cn=Manager,dc=learnitguide,dc=net
```

Add the below three lines additionally in the same configuration file.

```
olcRootPW: {SSHA}bHSiwuPJEypHS6zHSE2Uy7M69sQjmkPL
olcTLSCertificateFile: /etc/pki/tls/certs/learnitguideldap.pem
olcTLSCertificateKeyFile: /etc/pki/tls/certs/learnitguideldapkey.pem
```

Replace the "olcRootPW" value with your copied passwd. Now Save and exit the configuration file.

The suffix line names the domain for which the LDAP server provides information and should be changed to your domain name. The rootdn entry is the Distinguished Name (DN) for a user who is unrestricted by access controls or administrative limit parameters set for operations on the LDAP directory. The rootdn user can be thought of as the root user for the LDAP directory. In the configuration file, change the rootdn line from its default value as above.

4. Provide the Monitor privileges

Open the file **/etc/openldap/slapd.d/cn=config/olcDatabase={1}monitor.ldif** and go to the line start with **olcAccess.** Replace the value **"dc=my-domain,dc=com"** to **"dc=learnitguide,dc=net"** as below.

```
[root@linux1 cn=config]# vi olcDatabase={1}monitor.ldif
olcAccess: {0}to * by dn.base="gidNumber=0+uidNumber=0,cn=peercred,cn=external,
cn=auth" read by dn.base="cn=Manager,dc=learnitguide,dc=net" read by * none
```

Note: If no olcAccess directives are specified, the default access control policy, to * by * read, allows all users (both authenticated and anonymous) read access.
Note: Access controls defined in the frontend are appended to all other databases' controls.

Verify the configuration

```
[root@linux1 cn=config]# slaptest -u
56abba86 ldif_read_file: checksum error on
"/etc/openldap/slapd.d/cn=config/olcDatabase={1}monitor.ldif"
56abba86 ldif_read_file: checksum error on
"/etc/openldap/slapd.d/cn=config/olcDatabase={2}hdb.ldif"
config file testing succeeded
```

Ignore the Checksum errors as of now.

5. Enable and Start the SLAPD service

```
[root@linux1 cn=config]# systemctl start slapd
[root@linux1 cn=config]# systemctl enable slapd
```

```
[root@linux1 cn=config]# netstat -lt | grep ldap
tcp        0      0 0.0.0.0:ldap            0.0.0.0:*               LISTEN
tcp6       0      0 [::]:ldap               [::]:*                  LISTEN
```

6. Configure the LDAP Database

Copy the Sample Database Configuration file, change the file permisions as below.

```
[root@linux1 cn=config]# cp /usr/share/openldap-servers/DB_CONFIG.example
/var/lib/ldap/DB_CONFIG
[root@linux1 cn=config]# chown -R ldap:ldap /var/lib/ldap/
```

Add the following LDAP Schemas

```
[root@linux1 cn=config]# ldapadd -Y EXTERNAL -H ldapi:/// -f
/etc/openldap/schema/cosine.ldif
[root@linux1 cn=config]# ldapadd -Y EXTERNAL -H ldapi:/// -f
/etc/openldap/schema/nis.ldif
[root@linux1 cn=config]# ldapadd -Y EXTERNAL -H ldapi:/// -f
/etc/openldap/schema/inetorgperson.ldif
```

7. Create the self-signed certificate

In Step 3, We have specified our certificate locations. But we have not created yet, Lets create the self signed certificate,

```
[root@linux1 cn=config]# openssl req -new -x509 -nodes -out
/etc/pki/tls/certs/learnitguideldap.pem -keyout
/etc/pki/tls/certs/learnitguideldapkey.pem -days 365
```

Provide your company details to generate the certificate as below.

```
Country Name (2 letter code) [XX]:IN
State or Province Name (full name) []:Chennai
Locality Name (eg, city) [Default City]:Chennai
Organization Name (eg, company) [Default Company Ltd]:Learnitguide
Organizational Unit Name (eg, section) []:DCOPS
Common Name (eg, your name or your server's hostname) []:linux1.learnitguide.net
Email Address []:root@linux1.learnitguide.net
```

Verify the created certificates under the location /etc/pki/tls/certs/

```
[root@linux1 cn=config]# ll /etc/pki/tls/certs/*.pem
-rw-r--r--. 1 root root 1704 Jan  8 14:52 /etc/pki/tls/certs/learnitguideldapkey.pem
-rw-r--r--. 1 root root 1497 Jan  8 14:52 /etc/pki/tls/certs/learnitguideldap.pem
```

8. Create base objects in OpenLDAP

To create base objects in OpenLDAP, we need migration tools to be installed. We have already installed the migrationtools in the step 1 itself. So You will see lot of files and scripts under /usr/share/migrationtools/.

We need to change some predefined values in the file "migrate_common.ph" according to our domain name, for that do the following:

```
[root@linux1 cn=config]# cd /usr/share/migrationtools/
[root@linux1 migrationtools]# vi migrate_common.ph
```

Go to Line Number 71 and change your domain name

```
$DEFAULT_MAIL_DOMAIN = "learnitguide.net";
```

Go to line number 74 and change your base name

```
$DEFAULT_BASE = "dc=learnitguide,dc=net";
```

Go to line number 90 and change your EXTENDED_SCHEMA from "0" to "1"

```
$EXTENDED_SCHEMA = 1;
```

Finally Save and Exit the file.

9. Generate a base.ldif file for your Domain

```
[root@linux1 migrationtools]# touch /root/base.ldif
```

Copy the below lines and paste inside the file /root/base.ldif.

```
dn: dc=learnitguide,dc=net
objectClass: top
objectClass: dcObject
objectclass: organization
o: learnitguide net
dc: learnitguide
```

```
dn: cn=Manager,dc=learnitguide,dc=net
objectClass: organizationalRole
cn: Manager
description: Directory Manager

dn: ou=People,dc=learnitguide,dc=net
objectClass: organizationalUnit
ou: People

dn: ou=Group,dc=learnitguide,dc=net
objectClass: organizationalUnit
ou: Group
```

Replace with your domain name instead of **learnitguide.net**, Save and exit the file.

10. Create a Local Users

Lets create some local users and groups, then we will migrate to LDAP. For testing purpose, I create three users as below.

```
[root@linux1 migrationtools} # useradd ldapuser1
[root@linux1 migrationtools} # useradd ldapuser2
[root@linux1 migrationtools] # echo "redhat" | passwd --stdin ldapuser1
[root@linux1 migrationtools] # echo "redhat" | passwd --stdin ldapuser2
```

Filter out these user from /etc/passwd to another file:

```
[root@linux1 migrationtools]# grep ":10[0-9][0-9]" /etc/passwd > /root/passwd
```

Filter out user group from /etc/group to another file:

```
[root@linux1 migrationtools]# grep ":10[0-9][0-9]" /etc/group > /root/group
```

Now Convert the Individual Users file to LDAP Data Interchange Format (LDIF)
Generate a ldif file for users

```
[root@linux1 migrationtools]# ./migrate_passwd.pl /root/passwd /root/users.ldif
```

Generate a ldif file for groups

```
[root@linux1 migrationtools]# ./migrate_group.pl /root/group /root/groups.ldif
```

11. Import Users in to the LDAP Database.

Lets update these ldif file to LDAP Database.

```
[root@linux1 migrationtools]# ldapadd -x -W -D "cn=Manager,dc=learnitguide,dc=net" -f /root/base.ldif
[root@linux1 migrationtools]# ldapadd -x -W -D "cn=Manager,dc=learnitguide,dc=net" -f /root/users.ldif
[root@linux1 migrationtools]# ldapadd -x -W -D "cn=Manager,dc=learnitguide,dc=net" -f /root/groups.ldif
```

NOTE: It will ask for a password of "Manager", you have to type the password which you generated in encrypted format.

12. Test the configuration.

To test the configuration, search for the user **"ldapuser1"** in LDAP as below.

```
[root@linux1 migrationtools]# ldapsearch -x cn=ldapuser1 -b dc=learnitguide,dc=net
```

It prints all the user information:

```
[root@linux1 migrationtools]# ldapsearch -x -b 'dc=learnitguide,dc=net' '(objectclass=*)'
```

13. Stop Firewalld to allow the connection.

```
[root@linux1 migrationtools]# systemctl stop firewalld
```

LDAP Configuration is done, but we need to share the LDAP Users Home Directories via NFS. So Users who logged in the client servers will also be able to save their data remotely on LDAP Server. If not they will get an error as **"Home Directory not found".** If you wish to export the Home directory using autofs instead of making an entry in fstab file, please refer the link Mounting the NFS Filesystem using autofs. Here we use simple fstab entry for testing purpose also watch this demo on youtube, how to configure Linux Clients for LDAP Authentication to OpenLDAP Server.

14. NFS Configuration to export the Home Directory.

Edit the file /etc/exports and add an entry as below to export the home directory.

```
[root@linux1 ~]# vi /etc/exports
/home *(rw,sync)
```

Save and Exit the file.

Enable and restart rpcbind and nfs service.

```
[root@linux1 ~]# yum -y install rpcbind nfs-utils
[root@linux1 ~]# systemctl start rpcbind
[root@linux1 ~]# systemctl start nfs
[root@linux1 ~]# systemctl enable rpcbind
[root@linux1 ~]# systemctl enable nfs
```

Test the NFS Configuration

```
[root@linux1 ~]# showmount -e
Export list for linux1.learnitguide.net:
/home *
```

Client end configuration

Login into the server linux2 192.168.2.20

1. Ldap Client Configuration to use LDAP Server

```
[root@linux2 ~]# yum install -y openldap-clients nss-pam-ldapd
[root@linux2 ~]# authconfig-tui
```

Steps to follow for LDAP Authentication:

1. Put '*' Mark on "Use LDAP"
2. Put '*' Mark on "Use LDAP Authentication"
3. Select "Next" and Enter.
4. Enter the server field as "ldap://linux1.learnitguide.net/"
5. Enter the Base DN Field as "dc=learnitguide,dc=net"
6. Select "OK" and Enter

2. Test the Client Configuration.

Search the ldap user using the below command and check the output. If you get output, then our LDAP Configurations are working properly.

```
[root@linux2 ~]# getent passwd ldapuser1
ldapuser1:x:1000:1000:ldapuser1:/home/ldapuser1:/bin/bash
```

3. Mount the LDAP Users Home Directory.

Add the below entry to mount the LDAP Users home directory in the file /etc/fstab as below.

```
linux1.learnitguide.net:/home   /home   auto  defaults 0 0
```

If you would like to automount the Home Directories over NFS, please refer the link Automount home directories over NFS using autofs. Configure OpenLDAP Server on RHEL7/Centos7, linux openldap server setup, Linux ldap configuration, openldap server configuration, Step by step OpenLDAP Configuration, install openldap server in centos7, ldap server configuration

Thats all from client end. Now login using the LDAP User to ensure the authentication. Also refer How to Create a LDAP Users and Groups using LDIF file

ldap client configuration, ldap installation and configuration, ldap server configuration in linux, ldap configuration in linux, linux ldap server configuration, ldap configuration linux, ldap server installation and configuration in linux

Thanks for reading our post. share with your friends. We appreciate your feedback, Leave your comments if any. ldap configuration in linux step by step, ldap client configuration in linux, linux ldap configuration, ldap configuration example, redhat ldap configuration, ldap server configuration in ubuntu step by step, ldap server linux, ldap in linux

We have more articles to be updated soon. To not miss any updates, Follow us on social networking sites and Subscribe us on our Youtube channel. linux ldap, ldap configuration in linux, ldap server configuration in linux, ldap linux server, how to configure ldap server in linux, what is ldap in linux, ldap on linux, linux ldap server, ldap for linux, ldap tutorial linux, linux ldap configuration, ldap server for linux, linux ldap tutorial, openldap linux, openldap for linux, linux ldap tutorial for beginners, openldap server configuration on rhel7, openldap server configuration on centos7

Tags Linux 87 Linux Howto 68 Linux Server Configuration 23 Linux Tutorials 27 Linux Videos 5 Videos 51

Next
Automount Home Directories Over NFS in RHEL7/CentOS7 (https://www.learnitguide.net/2016/01/automount-home-directories-over-nfs-linux.html)

Previous
What is Openstack Opensource Cloud Computing for Beginners (https://www.learnitguide.net/2015/12/what-is-openstack-opensource-cloud.html)

POST A COMMENT

Disqus Facebook Blogger