**Contents**

* [1 Introduction](file:///C:\Users\Deepak\Desktop\open%20ldap%20web%20page\ldap%20configure.htm#Introduction)
* [2 The LDAP Directory Structure](file:///C:\Users\Deepak\Desktop\open%20ldap%20web%20page\ldap%20configure.htm#The_LDAP_Directory_Structure)
* [3 Scenario](file:///C:\Users\Deepak\Desktop\open%20ldap%20web%20page\ldap%20configure.htm#Scenario)
* [4 Installing The LDAP Packages](file:///C:\Users\Deepak\Desktop\open%20ldap%20web%20page\ldap%20configure.htm#Downloading_And_Installing_The_LDAP_Packages)
  + [4.1 Required LDAP Server RPMS](file:///C:\Users\Deepak\Desktop\open%20ldap%20web%20page\ldap%20configure.htm#Required_LDAP_Server_RPMS)
  + [4.2 Required LDAP Client RPMS](file:///C:\Users\Deepak\Desktop\open%20ldap%20web%20page\ldap%20configure.htm#Required_LDAP_Client_RPMS)
* [5 Configuring The LDAP Server](file:///C:\Users\Deepak\Desktop\open%20ldap%20web%20page\ldap%20configure.htm#Configuring_The_LDAP_Server)
  + [5.1 Create a database directory](file:///C:\Users\Deepak\Desktop\open%20ldap%20web%20page\ldap%20configure.htm#Create_a_database_directory)
  + [5.2 Create an LDAP "root" password](file:///C:\Users\Deepak\Desktop\open%20ldap%20web%20page\ldap%20configure.htm#Create_an_LDAP_.22root.22_password)
  + [5.3 Create a Test Account Named ldapuser](file:///C:\Users\Deepak\Desktop\open%20ldap%20web%20page\ldap%20configure.htm#Create_a_Test_Account_Named_ldapuser)
  + [5.4 Edit the slapd.conf file](file:///C:\Users\Deepak\Desktop\open%20ldap%20web%20page\ldap%20configure.htm#Edit_the_slapd.conf_file)
  + [5.5 Create Your LDAP Database](file:///C:\Users\Deepak\Desktop\open%20ldap%20web%20page\ldap%20configure.htm#Create_Your_LDAP_Database)
  + [5.6 Test the LDAP database](file:///C:\Users\Deepak\Desktop\open%20ldap%20web%20page\ldap%20configure.htm#Test_the_LDAP_database)
* [6 Configuring The LDAP Client](file:///C:\Users\Deepak\Desktop\open%20ldap%20web%20page\ldap%20configure.htm#Configuring_The_LDAP_Client)
  + [6.1 Edit the ldap.conf configuration file](file:///C:\Users\Deepak\Desktop\open%20ldap%20web%20page\ldap%20configure.htm#Edit_the_ldap.conf_configuration_file)
  + [6.2 Edit the /etc/nsswitch file](file:///C:\Users\Deepak\Desktop\open%20ldap%20web%20page\ldap%20configure.htm#Edit_the_.2Fetc.2Fnsswitch_file)
  + [6.3 Create Home Directories On The LDAP Client](file:///C:\Users\Deepak\Desktop\open%20ldap%20web%20page\ldap%20configure.htm#Create_Home_Directories_On_The_LDAP_Client)
    - [6.3.1 Check if ldapuser is Missing From the /etc/passwd file](file:///C:\Users\Deepak\Desktop\open%20ldap%20web%20page\ldap%20configure.htm#Check_if_ldapuser_is_Missing_From_the_.2Fetc.2Fpasswd_file)
    - [6.3.2 Create The Home Directory For ldapuser On The LDAP Client](file:///C:\Users\Deepak\Desktop\open%20ldap%20web%20page\ldap%20configure.htm#Create_The_Home_Directory_For_ldapuser_On_The_LDAP_Client)
  + [6.4 Testing](file:///C:\Users\Deepak\Desktop\open%20ldap%20web%20page\ldap%20configure.htm#Testing)
* [7 Configuring Encrypted LDAP Communication](file:///C:\Users\Deepak\Desktop\open%20ldap%20web%20page\ldap%20configure.htm#Configuring_Encrypted_LDAP_Communication)
  + [7.1 Using Transport Layer Security (TLS)Encryption](file:///C:\Users\Deepak\Desktop\open%20ldap%20web%20page\ldap%20configure.htm#Using_Transport_Layer_Security_.28TLS.29Encryption)
    - [7.1.1 How TLS Communication Works](file:///C:\Users\Deepak\Desktop\open%20ldap%20web%20page\ldap%20configure.htm#How_TLS_Communication_Works)
    - [7.1.2 Configuring the TLS Server](file:///C:\Users\Deepak\Desktop\open%20ldap%20web%20page\ldap%20configure.htm#Configuring_the_TLS_Server)
    - [7.1.3 Configuring the TLS Client](file:///C:\Users\Deepak\Desktop\open%20ldap%20web%20page\ldap%20configure.htm#Configuring_the_TLS_Client)
* [8 Troubleshooting LDAP Logins](file:///C:\Users\Deepak\Desktop\open%20ldap%20web%20page\ldap%20configure.htm#Troubleshooting_LDAP_Logins)
  + [8.1 Check Your /var/log/messages file](file:///C:\Users\Deepak\Desktop\open%20ldap%20web%20page\ldap%20configure.htm#Check_Your_.2Fvar.2Flog.2Fmessages_file)
  + [8.2 Testing Basic Connectivity](file:///C:\Users\Deepak\Desktop\open%20ldap%20web%20page\ldap%20configure.htm#Testing_Basic_Connectivity)
  + [8.3 Testing Using ldapsearch](file:///C:\Users\Deepak\Desktop\open%20ldap%20web%20page\ldap%20configure.htm#Testing_Using_ldapsearch)
  + [8.4 Use SSH or the Linux console](file:///C:\Users\Deepak\Desktop\open%20ldap%20web%20page\ldap%20configure.htm#Use_SSH_or_the_Linux_console)
  + [8.5 Use the tcpdump Command](file:///C:\Users\Deepak\Desktop\open%20ldap%20web%20page\ldap%20configure.htm#Use_the_tcpdump_Command)
    - [8.5.1 Testing Regular LDAP](file:///C:\Users\Deepak\Desktop\open%20ldap%20web%20page\ldap%20configure.htm#Testing_Regular_LDAP)
    - [8.5.2 Testing Secure LDAP](file:///C:\Users\Deepak\Desktop\open%20ldap%20web%20page\ldap%20configure.htm#Testing_Secure_LDAP)
* [9 Common LDAP Administrative Tasks](file:///C:\Users\Deepak\Desktop\open%20ldap%20web%20page\ldap%20configure.htm#Common_LDAP_Administrative_Tasks)
  + [9.1 Starting and Stopping LDAP](file:///C:\Users\Deepak\Desktop\open%20ldap%20web%20page\ldap%20configure.htm#Starting_and_Stopping_LDAP)
  + [9.2 LDAP users changing their own passwords](file:///C:\Users\Deepak\Desktop\open%20ldap%20web%20page\ldap%20configure.htm#LDAP_users_changing_their_own_passwords)
  + [9.3 LDAP Password Changes by LDAP User "root"](file:///C:\Users\Deepak\Desktop\open%20ldap%20web%20page\ldap%20configure.htm#LDAP_Password_Changes_by_LDAP_User_.22root.22)
  + [9.4 Modifying LDAP users by user "root"](file:///C:\Users\Deepak\Desktop\open%20ldap%20web%20page\ldap%20configure.htm#Modifying_LDAP_users_by_user_.22root.22)
    - [9.4.1 The Modify LDAP User Script](file:///C:\Users\Deepak\Desktop\open%20ldap%20web%20page\ldap%20configure.htm#The_Modify_LDAP_User_Script)
  + [9.5 Adding new LDAP users](file:///C:\Users\Deepak\Desktop\open%20ldap%20web%20page\ldap%20configure.htm#Adding_new_LDAP_users)
    - [9.5.1 Create an LDAP Add User Script](file:///C:\Users\Deepak\Desktop\open%20ldap%20web%20page\ldap%20configure.htm#Create_an_LDAP_Add_User_Script)
    - [9.5.2 Add the User to the Database](file:///C:\Users\Deepak\Desktop\open%20ldap%20web%20page\ldap%20configure.htm#Add_the_User_to_the_Database)
  + [9.6 Deleting LDAP users](file:///C:\Users\Deepak\Desktop\open%20ldap%20web%20page\ldap%20configure.htm#Deleting_LDAP_users)
  + [9.7 LDAP Web Management Tools](file:///C:\Users\Deepak\Desktop\open%20ldap%20web%20page\ldap%20configure.htm#LDAP_Web_Management_Tools)
* [10 Conclusion](file:///C:\Users\Deepak\Desktop\open%20ldap%20web%20page\ldap%20configure.htm#Conclusion)

# Introduction

Many centralized database programs have been developed to allow users to log in on multiple computers using a single password. NIS was one of the first, but it doesn't encrypt the password transaction. It also uses the portmapper daemon, which uses an unpredictable range of TCP ports that are difficult for firewalls to track. LDAP (Lightweight Directory Access Protocol) provides an alternative based on the X.500 standard.

The X.500 standard defines how globally referenced directories of people should be structured. X.500 directories are organized under a common root directory in a tree hierarchy with different levels for each category of information, such as country, state, city, organization, organizational unit, and person. Designed to provide a simpler yet robust implementation of X.500, LDAP was originally used as the backbone of Microsoft's Active Directory Service and Novell's Novell Directory Services (NDS) products. LDAP can also interact with other login programs, such as Remote Authentication Dial-in User Service (RADIUS), which the network equipment of many ISPs uses to manage dialup Internet access.

It was later recognized that LDAP had features that could make it a desirable replacement for NIS in some scenarios. For example, it uses a single TCP port (389) for regular communication and another port (636) for encrypted transactions. LDAP also can interact with many login authentication, authorization, and accounting programs external to Linux and UNIX.

This chapter will first show you how to install and use LDAP on Fedora Linux systems, then go on to explain how LDAP interacts with RADIUS.

# The LDAP Directory Structure

Like X.500, LDAP directory entries are arranged in a tree structure. Under the root, there are branches that represent countries, organizations, organizational units, and people.

In complicated LDAP deployments, in which you have to exchange information with the LDAP databases of other companies, you may want to get a formal organization number from the Internet Assigned Numbers Authority (IANA) to reduce any data conflicts. In the chapter's example this won't be necessary. Because there will be no data sharing, I'll just make up one.

**Scenario**

These concepts are easier to explain when working from an example, so imagine the IT department in a small organization called example.com has many Linux servers it needs to administer.

* The company wants a simple, secure, centralized login scheme for all of the servers.
* It has decided to use the LDAP domain example.com for its LDAP database, in which one domain component (DC) will be example, and the other will be com.
* The database will have only one organizational unit simply called People, which is the LDAP default.
* Each person will have such attributes as a username (User ID or UID), password, Linux home directory, and login shell.
* The Fedora Linux server named bigboy with the IP address 192.168.1.100 will act as the LDAP server containing the database.
* The Fedora Linux server named smallfry will be used to test the system as the LDAP client and has the IP address 192.168.1.102.
* Server bigboy has a special user account named ldapuser that will be used to test the LDAP logins.

# Installing The LDAP Packages

Most RedHat and Fedora Linux software products are available in the RPM format. When searching for the file, remember that the FreeRADIUS RPM's filename usually starts with openldap followed by a version number, as in openldap-servers-2.1.22-8.i386.rpm

Make sure these required LDAP Server RPMs are installed on your LDAP server.

## Required LDAP Server RPMS

You will have to make sure the following packages are installed on your LDAP server.

* openldap
* openldap-clients
* openldap-devel
* nss\_ldap
* openldap-servers

## Required LDAP Client RPMS

You will have to make sure the following packages are installed on your LDAP client.

* openldap
* openldap-clients
* openldap-devel
* nss\_ldap

# Configuring The LDAP Server

The first stage of the project is to correctly configure the LDAP server. To do so, you must create an LDAP database and into which you import the /etc/passwd file. Take a closer look at the steps:

## Create a database directory

Fedora LDAP defaults to putting all databases in the /var/lib/ldap directory. For the example, create a dedicated example.com directory owned by the user ldap. (The ldap user is always created during the RPM installation process.)

[root@bigboy tmp]# mkdir /var/lib/ldap/example.com

[root@bigboy tmp]# chown ldap:ldap /var/lib/ldap/example.com

## Create an LDAP "root" password

Only the LDAP root user can create, import data, and export data into an LDAP database. This user needs an encrypted password. You can create it with the slappasswd command and use the result in the LDAP configuration file.

[root@bigboy tmp]# slappasswd

New password:

Re-enter new password:

{SSHA}v4qLq/qy01w9my60LLX9BvfNUrRhOjQZ

[root@bigboy tmp]#

**Create a Test Account Named ldapuser**

To create the ldapuser account you'll use for testing, type the commands.

[root@bigboy tmp]# useradd -g users ldapuser

[root@bigboy tmp]# passwd ldapuser

Changing password for user ldapuser.

New password:

Retype new password:

passwd: all authentication tokens updated successfully.

[root@bigboy tmp]#

**Edit the slapd.conf file**

The LDAP server's daemon is named slapd and its configuration file is named /etc/openldap/slapd.conf. Update it with:

* A database of the default type bdb using the domain suffix example.com made up of domain components (DCs) example and com.
* The root user with a common name (CN), or nickname, of Manager who, as expected, is part of the example and com DCs.
* The encrypted version of the LDAP root password as well as the location of the LDAP database.

The configuration file syntax to do this is:

database bdb

suffix "dc=pro ,dc=com"

rootdn "cn=Manager,dc=example,dc=com"

rootpw {SSHA}v4qLq/qy01w9my60LLX9BvfNUrRhOjQZ

directory /var/lib/ldap/example.com

## Create Your LDAP Database

This process involves migrating your system’s authentication files to the LDAP database you will need to create. Here’s what you need to do:

1. OpenLDAP is maintained by a company named the PADL Software and they have a number of tools that can be used to migrate your /etc/passwd file into LDAP. Visit their site at <http://www.padl.com>, search for “migration tools” and download the TAR file listed on the relevant page. In this example we do the download using wget and move the files to the /usr/share/openldap/migration/ directory.

[root@bigboy tmp]# wget <http://www.padl.com/download/MigrationTools.tgz>

--2009-07-03 10:59:19-- <http://www.padl.com/download/MigrationTools.tgz>

Resolving www.padl.com... 216.154.215.154

Connecting to www.padl.com|216.154.215.154|:80... connected.

HTTP request sent, awaiting response... 200 OK

Length: 21284 (21K) [application/x-gzip]

Saving to: `MigrationTools.tgz'

100%[=======================================>] 21,284 106K/s in 0.2s

2009-07-03 10:59:19 (106 KB/s) - `MigrationTools.tgz' saved [21284/21284]

[root@bigboy tmp]# tar -xvzf MigrationTools.tgz

MigrationTools-47/

MigrationTools-47/ads/

…

…

[root@bigboy tmp]# mkdir -p /usr/share/openldap/migration/

[root@bigboy tmp]# cd MigrationTools\*

[root@bigboy MigrationTools-47]# cp -rv \* /usr/share/openldap/migration/

`ads' -> `/usr/share/openldap/migration/ads'

…

…

[root@bigboy MigrationTools-47]# cd /tmp

[root@bigboy tmp]#

2. The password conversion script is named migrate\_common.ph. Edit the file and replace all instances of the string “padl” with the string “example”. Padl is the website used by some of the LDAP development team. We need our domain to be “example” instead so it matches our /etc/openldap/slpd.conf file. The migrate\_common.ph file will be used later by the migration script.

[root@bigboy tmp]# vi /usr/share/openldap/migration/migrate\_common.ph

For example, at the vi editor’s : prompt, use the command:

%s/padl/example/g

3. Locate the DB\_CONFIG.example starter file to your LDAP database directory of /var/lib/ldap/example.com. Remember to run the updatedb command so that the locate database is current.

[root@bigboy tmp]# updatedb

[root@bigboy tmp]# locate DB\_CONFIG

/usr/share/doc/openldap-servers-2.4.16/DB\_CONFIG.example

[root@bigboy tmp]# cp /usr/share/doc/openldap-servers-2.4.16/DB\_CONFIG.example \

/var/lib/ldap/example.com/DB\_CONFIG

4. Migrate your system authentication files using the migrate\_all\_offline.sh script that should reside in the same directory as the migrate\_common.ph file.

[root@bigboy tmp]# /usr/share/openldap/migration/migrate\_all\_offline.sh

Creating naming context entries...

Migrating groups...

Migrating hosts...

...

...

...

Preparing LDAP database...

=> bdb\_tool\_entry\_put: id2entry\_add failed: DB\_KEYEXIST: Key/data pair already exists (-30996)

=> bdb\_tool\_entry\_put: txn\_aborted! DB\_KEYEXIST: Key/data pair already exists (-30996)

slapadd: could not add entry dn="cn=raid-am,ou=Services,dc=example,dc=com"

(line=16432): txn\_aborted! DB\_KEYEXIST: Key/data pair already exists (-30996)

Migration failed: saving failed LDIF to /tmp/nis.ldif.E14499

[root@bigboy tmp]#

You may get a key pair error for the raid-am service, but it doesn’t appear to affect functionality.

5. LDAP won’t start unless the files in the database directory are owned by the ldap user. Use the chown command to do this.

[root@bigboy tmp]# chown -R ldap:ldap /var/lib/ldap/example.com

6. Start LDAP and make sure it starts on reboot.

[root@bigboy tmp]# service ldap start

Starting slapd: [ OK ]

[root@bigboy tmp]# chkconfig ldap on

You should be ready to go! The database has been created.

## Test the LDAP database

You can view all the LDAP database entries all at once with the ldapsearch command; this is a good test to make sure you have all the correct functionality.

[root@bigboy tmp]# ldapsearch -x -b 'dc=example,dc=com' \

'(objectclass=\*)'

[root@bigboy tmp]#

# Configuring The LDAP Client

Now that the LDAP server is configured properly, you can turn your attention to configuring and testing the clients.

## Edit the ldap.conf configuration file

LDAP clients are configured using the /etc/openldap/ldap.conf file. You need to make sure that the file refers to the LDAP server's IP address for the domain example.com. The file should look like this:

HOST 192.168.1.100

BASE dc=example,dc=com

## Edit the /etc/nsswitch file

The /etc/nsswitch.conf file defines the order in which the Linux operating system searches login databases for login information.

You want to configure it to first search its /etc/passwd file. If it doesn't find the user password information there, it goes to the LDAP server. The easiest way set this up is to use the /usr/bin/authconfig-tui command:

1. Run /usr/bin/authconfig-tui. The output of this command may be jumbled because your command line shell's language setting may not be compatible. You can usually avoid this problem by placing the string LANG=C in front of the command as shown here.

[root@smallfry tmp]# env LANG=C authconfig-tui

1. Select LDAP.
2. Give the LDAP server's IP address, which is 192.168.1.100 in this case.
3. Give the base DN as dc=example,dc=com
4. Do not select TLS.
5. Use MD5 and shadow passwords.

The screen should look like this:

[\*] Use Shadow Passwords

[\*] Use MD5 Passwords

[\*] Use LDAP [ ] Use TLS

Server: 192.168.1.100

Base DN: dc=example,dc=com

When finished, look at the /etc/nsswitch.conf file and make sure it has references to LDAP.

**Note:** In some Linux versions, the authconfig-tui command is replaced with the authconfig command.

## Create Home Directories On The LDAP Client

You previously created a user named ldapuser in the group users on server bigboy. You now need to make sure that this user has a home directory on the LDAP client smallfry. The example in this section creates the directory and makes ldapuser the owner. As you can see, server smallfry correctly gets its user information about ldapuser from bigboy; the chown command doesn't complain about ldapuser not existing in smallfry's /etc/passwd file.

### Check if ldapuser is Missing From the /etc/passwd file

You can look for ldapuser by searching the /etc/passwd file with the grep command. There should be no response.

[root@smallfry tmp]# grep ldapuser /etc/passwd

[root@smallfry tmp]#

### Create The Home Directory For ldapuser On The LDAP Client

In this phase, you create the home directory, copy a BASH login profile file into it, and modify the ownership of the directory and all the files to user ldapuser.

**Note:** If the chown command fails, it is probably because of an incorrect LDAP configuration in which the LDAP client cannot read the user information from the LDAP server.

In some cases, you may want to use NFS mounts to provide home directories for your users, which will significantly reduce the need to do this step.

[root@smallfry tmp]# mkdir /home/ldapuser

[root@smallfry tmp]# chmod 700 /home/ldapuser/

[root@smallfry tmp]# ll /home

total 2

drwx------ 2 ldapuser users 1024 Aug 4 08:05 ldapuser

[root@smallfry tmp]# cp /etc/skel/.\* /home/ldapuser/

cp: omitting directory `/etc/skel/.'

cp: omitting directory `/etc/skel/..'

cp: omitting directory `/etc/skel/.kde'

[root@smallfry tmp]# chown -R ldapuser:users /home/ldapuser

[root@smallfry tmp]#

# Configuring Encrypted LDAP Communication

There are two commonly mentioned methods of encrypting Linux LDAP communications between clients and servers. One method is through the use of the external stunnel utility that protects the data using SSL. The other method also uses SSL, but it is natively supported in LDAP by using its Transport Layer Security (TLS) option and is therefore easier to implement. This section describes both methods.

## Using Transport Layer Security (TLS)Encryption

TLS is an updated version of the Secure Socket Layer (SSL) protocol used by many web browsers to do shopping cart checkouts. Like most certificate based encryption schemes it allows a client and server to talk in a trusted manner without the use of a password.

TLS will require you to create a certificate authority (CA) for your organization. A CA is a server that will manage the issuance and authentication of new server certificates used by the LDAP server for TLS. In the example that follows, the CA and LDAP servers are the same device, but guidelines are also provided on how the functions can be assigned to separate servers.

**Note:** Unlike the stunnel encryption method described later, TLS runs encrypted on LDAP's TCP port 389.

Before we begin configuration it is important to understand how TLS works. This will be discussed next.

### How TLS Communication Works

There is a sequence of events that occur prior to the creation of an LDAP communication session using TLS. These include the following steps:

1. Both the LDAP server and client need to be configured with a shared copy of a CA certificate beforehand.
2. When the TLS LDAP connection is made, the client and server negotiate their SSL encryption scheme.
3. The LDAP server then sends its public encryption key and its server certificate.
4. The LDAP client inspects the server certificate to make sure that it hasn't expired and takes note of the name and key ID of the CA server that issued it. It then checks this CA information with all the CA certificates in its database to determine whether the server certificate should be trusted.
5. If everything is valid, the LDAP client then creates a random "premaster" secret encryption key that it encrypts with the LDAP server's public key. It then sends the encrypted encryption key to the LDAP server.
6. When public keys are created, a special "private" key is also simultaneously created. Anything encrypted with the public key can only be decrypted with the private key and vice versa. The server then uses its private key to extract the premaster key.
7. The client and server then use the premaster key to generate a master secret that will be the same for both, but will never be transmitted so that a third-party cannot intercept it.
8. The master secret key is then used to create session keys that will be used to encrypt all future communication between client and server for the duration of the TLS session.

Now that you understand the TLS process its time to start configuring secure LDAP.

### Configuring the TLS Server

We are about to create our own CA server to create and sign server certificates. This process is known as creating a self-signed SSL certificate as opposed to having a trusted third party organization, such as Verisign, doing it on your behalf. The latter method is most commonly used by public websites in which the CA certificates of many well known and trusted CA companies already come installed on your PC as part of your Web browser installation. Configuration of the server isn't hard, but there are many steps. Let's go!

1. First you need to edit your /etc/sysconfig/ldap file to make ldap use its secure TCP port 636. Here we turn off regular SLAPD\_LDAP that listens on the unencrypted port 389 and activate secure SLAPD\_LDAPS.

# File: /etc/sysconfig/ldap

#

# Run slapd with -h "... ldap:/// ..."

# yes/no, default: yes

SLAPD\_LDAP=no

#

# Run slapd with -h "... ldapi:/// ..."

# yes/no, default: no

SLAPD\_LDAPI=no

#

# Run slapd with -h "... ldaps:/// ..."

# yes/no, default: no

SLAPD\_LDAPS=yes

2. The certificates are sensitive to the hostname of the LDAP server. We need to know what it is, bigboy.

[root@bigboy tmp]# hostname

bigboy

[root@bigboy tmp]#

3. Enter the /etc/openldap/cacerts/ directory and generate an SSL key with the openssl command. Let’s define the filename as server.pem and give the certificate a lifetime of 10 years, 3650 days. In a business environment, answer as many of the questions as you can. Note: In all cases the host name must be accurately provided. Make sure the hostname is defined in DNS, or listed in all the clients’ /etc/hosts file.

[root@bigboy tmp]# cd /etc/openldap/cacerts/

[root@bigboy cacerts]# openssl req -newkey rsa:1024 \

-x509 -nodes -out server.pem -keyout server.pem -days 3650

Generating a 1024 bit RSA private key

.............++++++

......................++++++

writing new private key to 'server.pem'

-----

You are about to be asked to enter information that will

be incorporated into your certificate request.

What you are about to enter is what is called a

Distinguished Name or a DN.

There are quite a few fields but you can leave some blank

For some fields there will be a default value,

If you enter '.', the field will be left blank.

-----

Country Name (2 letter code) [GB]:

State or Province Name (full name) [Berkshire]:

Locality Name (eg, city) [Newbury]:

Organization Name (eg, company) [My Company Ltd]:

Organizational Unit Name (eg, section) []:

Common Name (eg, your name or your server's hostname) []:bigboy

Email Address []:

[root@bigboy cacerts]#

4. Verify the encrypted server.pem file has been created, it should look like this.

[root@bigboy cacerts]# cat server.pem

-----BEGIN RSA PRIVATE KEY-----

MIICXAIBAAKBgQDj64XGJe1uA1Ybr/1kWTsQcxktU7W9i29OkbmFwI1hc8qYXuO5

qAAGCFHHupInzy9uoXJVvGW3yEw0gasLR6hzyC2+1b8vfG3Eb0yN+Yt4mGp03iiX

c0pzQrEw+HxYcsA0KAUCQDKCo5OTBB0FLpH+ZgTqkeBabt3lNYFphAqEqLyC6q10

+WMlWY/jvLyQYldbvP3ENgahGKlv99SKytSb9MFQlnc=

-----END RSA PRIVATE KEY-----

-----BEGIN CERTIFICATE-----

MIIC+DCCAmGgAwIBAgIJAKhuyXeddEVVMA0GCSqGSIb3DQEBBQUAMFwxCzAJBgNV

BAYTAkdCMRIwEAYDVQQIEwlCZXJrc2hpcmUxEDAOBgNVBAcTB05ld2J1cnkxFzAV

5/ncthk9QyZwLrz1/WEC/9qbST/aYGEz4lOMc8tPu9vKh9CAYI42J6zu51Y=

-----END CERTIFICATE-----

[root@bigboy cacerts]#

5. Each LDAP client will need a copy of the CERTIFICATE part of the file. The grep command can easily extract this information and place it into a file named client.pem.

[root@bigboy cacerts]# grep -A 100 CERTIFICATE \

server.pem > client.pem

6. Next we need to edit the /etc/openldap/slapd.conf file to activate TLS encryption of all incoming connections to the server. In the TLS section make reference to your server.pem file.

# File: /etc/openldap/slapd.conf

TLSCipherSuite HIGH:MEDIUM:+SSLv2:+SSLv3:RSA

TLSCACertificateFile /etc/openldap/cacerts/server.pem

TLSCertificateFile /etc/openldap/cacerts/server.pem

TLSCertificateKeyFile /etc/openldap/cacerts/server.pem

TLSVerifyClient allow

7. Copy the client.pem file to your LDAP client’s /etc/openldap/cacerts/ directory.

[root@bigboy openldap]# scp cacerts/client.pem \

root@smallfry/etc/openldap/cacerts/

root@smallfry's password:

client.pem 100% 1090 1.1KB/s 00:00

[root@bigboy openldap]#

8. The LDAP daemon won’t start properly unless the files in the /etc/openldap/cacerts directory are owned by the ldap user. We need to change this.

[root@bigboy openldap]# chown ldap:ldap cacerts/\*

9. Restart the ldap daemon to make these changes take effect.

[root@bigboy openldap]# service ldap restart

Stopping slapd: [ OK ]

Starting slapd: [ OK ]

[root@bigboy openldap]#

10. Make sure LDAP is listening on the TCP port reserved for secure ldaps. This can be done using the netstat command and you should get a response showing ldaps is listening for new connections like this.

[root@bigboy openldap]# netstat -a | grep ldap

tcp 0 0 \*:ldaps \*:\* LISTEN

[root@bigboy openldap]#

### Configuring the TLS Client

Configuration of the client is much quicker as you will soon see. Here are the steps:

1. Run authconfig-tui and make sure your options match these screens.

-------------------Authentication Configuration -------------------

| |

| User Information Authentication |

| [ ] Cache Information [\*] Use MD5 Passwords |

| [ ] Use Hesiod [\*] Use Shadow Passwords |

| [\*] Use LDAP [\*] Use LDAP Authentication |

| [ ] Use NIS [ ] Use Kerberos |

| [ ] Use Winbind [ ] Use SMB Authentication |

| [ ] Use Winbind Authentication |

| [ ] Local authorization is sufficient |

| |

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

| | Cancel | | Next | |

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

| |

| |

-------------------------------------------------------------------

------------------- LDAP Settings -------------------

| |

| [\*] Use TLS |

| Server: bigboy.my-web-site.org\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |

| Base DN: dc=example,dc=com\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |

| |

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

| | Back | | Ok | |

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

| |

| |

-----------------------------------------------------

2. Review the contents of /etc/ldap.conf and make sure they have the following entries. The host must match the hostname of the certificate.

#

# File: /etc/ldap.conf

#

uri ldaps://bigboy/

#ssl start\_tls

tls\_cacertdir /etc/openldap/cacerts

Note: Comment out the ssl statement as it can cause conflicts which will make remote logins fail while passing all other LDAP tests. 3. Review the contents of /etc/openldap/ldap.conf and make sure they have the following entries. The ldaps:// host must match the hostname of the certificate.

#

# File: /etc/openldap/ldap.conf

#

URI ldaps://bigboy/

BASE dc=example,dc=com

TLS\_CACERTDIR /etc/openldap/cacerts

4. Test to make sure you can get access to the ldap server with the ldapsearch command using the –x flag.

[root@smallfry tmp]# ldapsearch -x

dn: uid=ldapuser,ou=People,dc=example,dc=com

uid: ldapuser

cn: ldapuser

objectClass: account

objectClass: posixAccount

objectClass: top

objectClass: shadowAccount

userPassword:: e2NyeXB0fSQxJDRGL2huRzdjZrV2w5cDA=

shadowLastChange: 13942

shadowMax: 99999

shadowWarning: 7

loginShell: /bin/bash

uidNumber: 504

gidNumber: 100

homeDirectory: /home/ldapuser

[root@smallfry tmp]#

5. A further test is to see whether you can get the LDAP server to send you a copy of its certificate using the openssl command like this.

[root@smallfry tmp]# openssl s\_client -connect bigboy:636 \

-showcerts

CONNECTED(00000003)

depth=0 /C=GB/ST=Berkshire/L=Newbury/O=My Company Ltd/CN=bigboy

verify error:num=18:self signed certificate

verify return:1

---

Certificate chain

0 s:/C=GB/ST=Berkshire/L=Newbury/O=My Company Ltd/CN=bigboy

i:/C=GB/ST=Berkshire/L=Newbury/O=My Company Ltd/CN=bigboy

-----BEGIN CERTIFICATE-----

MIIC+DCCAmGgAwIBAgIJAKhuyXeddEVVMA0GCSqGSIb3DQEBBQUAMFwxCzAJBgNV

BAYTAkdCMRIwEAYDVQQIEwlCZXJrc2hpcmUxEDAOBgNVBAcTB05ld2J1cnkxFzAV

5/ncthk9QyZwLrz1/WEC/9qbST/aYGEz4lOMc8tPu9vKh9CAYI42J6zu51Y=

-----END CERTIFICATE-----

---

Server certificate

subject=/C=GB/ST=Berkshire/L=Newbury/O=My Company Ltd/CN=bigboy

issuer=/C=GB/ST=Berkshire/L=Newbury/O=My Company Ltd/CN=bigboy

---

Acceptable client certificate CA names

/C=GB/ST=Berkshire/L=Newbury/O=My Company Ltd/CN=bigboy

---

SSL handshake has read 1031 bytes and written 343 bytes

---

New, TLSv1/SSLv3, Cipher is AES256-SHA

Server public key is 1024 bit

Compression: NONE

Expansion: NONE

SSL-Session:

Protocol  : TLSv1

Cipher  : AES256-SHA

Key-Arg  : None

Krb5 Principal: None

Verify return code: 18 (self signed certificate)

---

[root@smallfry tmp]#

6. Test logging into your LDAP client using the ldapuser we created earlier when testing insecure LDAP.

[root@smallfry tmp]# ssh -l ldapuser localhost

ldapuser@localhost's password:

Last login: Sat Mar 8 11:01:01 2008 from bigboy-fc8

[ldapuser@smallfry ~]$ exit

[root@smallfry tmp]#

# Troubleshooting LDAP Logins

You can never be certain about the functioning of any application unless you test it. LDAP is fairly complicated to install and should be as thoroughly tested as possible before you deploy it. Here are some steps you can take to help you sleep better at night.

## Check Your /var/log/messages file

The first step is to see what type of error massages you are getting on both the LDAP server and client. Here are some messages that refer to common mistakes:

* You have an unnecessary “ssl start\_tls” statement in your client’s /etc/ldap.conf file.

Mar 8 10:58:50 bigboy slapd[14842]: conn=6 op=0 RESULT oid= err=1 text=TLS already started

## Testing Basic Connectivity

The very first step is to use TELNET to determine whether your LDAP server is accessible on TCP port 389 (LDAP) or 636 (LDAPS).

Lack of connectivity could be caused by a firewall in the path between the LDAP server and client or there could be firewall software running on the servers themselves.

Other sources of failure include LDAP not being started at all, the server could be down, or there could be a network related failure.

## Testing Using ldapsearch

Always run the ldapsearch command on both the LDAP client and server to test your LDAP configuration.

[root@smallfry tmp]# ldapsearch -x -b 'dc=example,dc=com' \

'(objectclass=\*)'

When LDAP is configured correctly, the command sends a full database listing to your screen.

## Use SSH or the Linux console

Try to log in as user ldapuser to the LDAP client Linux system as an alternative test. If it fails, try restarting SSH on the LDAP client so that the /etc/nsswitch.conf file can be reread with the new LDAP information. This step is not required in all versions of Linux.

## Use the tcpdump Command

If the LDAP configuration files appear correct and LDAP still doesn't work, then you should try using the tcpdump command, to see whether your systems can correctly communicate with one another. A failure to communicate could be due to poor routing, misconfigured firewalls along the way, or possibly LDAP being turned off on the server.

### Testing Regular LDAP

On the LDAP server, use the tcpdump command to listen for traffic on the regular LDAP port 389 or ldap. Run the ldapsearch command on the LDAP client.

[root@bigboy tmp]# tcpdump -n tcp port ldap

If everything is configured correctly, you should see bidirectional LDAP packet flows between the LDAP client and server.

**Note:** The insecurity of unencrypted LDAP client communication can also be demonstrated by using network packet capture. In this example, the tethereal command is used with the -x flag to view the ASCII contents of LDAP traffic between client and server. The username, password, UID (100), GID (503), shell (/bin/bash) and home directory (/home/ldapuser) of the ldapuser user can all be clearly seen in clear text. It is always a good practice to add an additional layer of security with LDAP TLS encryption which will eliminate this ASCII visibility.

If you are using the stunnel method you would set the tethereal TCP port to ldaps.

[root@bigboy ~]# tethereal -n -x -i eth0 tcp port ldap

...

...

0050 69 64 3d 6c 64 61 70 75 73 65 72 2c 6f 75 3d 50 id=ldapuser,ou=P

0060 65 6f 70 6c 65 2c 64 63 3d 65 78 61 6d 70 6c 65 eople,dc=example

0070 2c 64 63 3d 63 6f 6d 30 82 01 04 30 11 04 03 75 ,dc=com0...0...u

0080 69 64 31 0a 04 08 6c 64 61 70 75 73 65 72 30 10 id1...ldapuser0.

0090 04 02 63 6e 31 0a 04 08 6c 64 61 70 75 73 65 72 ..cn1...ldapuser

00e0 75 73 65 72 50 61 73 73 77 6f 72 64 31 2b 04 29 userPassword1+.)

00f0 7b 63 72 79 70 74 7d 24 31 24 47 53 77 48 53 54 {crypt}$1$GSwHST

0100 4a 49 24 71 59 4d 65 66 47 32 4f 35 77 6a 7a 70 JI$qYMefG2O5wjzp

0110 77 42 2e 32 4b 70 58 48 31 30 19 04 0a 6c 6f 67 wB.2KpXH10...log

0120 69 6e 53 68 65 6c 6c 31 0b 04 09 2f 62 69 6e 2f inShell1.../bin/

0130 62 61 73 68 30 12 04 09 75 69 64 4e 75 6d 62 65 bash0...uidNumbe

0140 72 31 05 04 03 35 30 33 30 12 04 09 67 69 64 4e r1...5030...gidN

0150 75 6d 62 65 72 31 05 04 03 31 30 30 30 21 04 0d umber1...1000!..

0160 68 6f 6d 65 44 69 72 65 63 74 6f 72 79 31 10 04 homeDirectory1..

0170 0e 2f 68 6f 6d 65 2f 6c 64 61 70 75 73 65 72 ./home/ldapuser

...

...

[root@bigboy ~]#

### Testing Secure LDAP

On the LDAP server, when using stunnel, use the tcpdump command to listen for traffic on the secure LDAP port 636 or ldaps. With TLS you would use the regular LDAP port 389 or ldap with the command. Run the ldapsearch command on the LDAP client and if everything is configured correctly, you should see packet flows such as this one.

[root@bigboy tmp]# tcpdump -n tcp port ldaps

tcpdump: listening on eth0

09:20:02.281257 192.168.1.102.1345 > 192.168.1.100.ldaps: S 1665037104:1665037104(0) win 5840 <mss 1460,sackOK,timestamp 74401362 0,nop,wscale 0> (DF)

09:20:02.281356 192.168.1.100.ldaps > 192.168.1.102.1345: S 1911175072:1911175072(0) ack 1665037105 win 5792 <mss 1460,sackOK,timestamp 20737195 74401362,nop,wscale 0> (DF)

...

...

[root@bigboy tmp]#

**Note:** You can also verify the lack of ACSII strings being sent with LDAP encryption using the tetheral example used previously. Remember to use ldap for TLS encryption and ldaps when using stunnel.

[root@bigboy ~]# tethereal -n -x -i eth0 tcp port ldaps

...

...

0000 00 b0 d0 46 32 71 00 b0 d0 4e f2 18 08 00 45 00 ...F2q...N....E.

0010 01 3e 14 2c 40 00 40 06 a1 11 c0 a8 01 64 c0 a8 .>.,@.@......d..

0020 01 c8 90 ec 01 85 95 c1 c9 95 90 a3 67 01 80 18 ............g...

0030 08 88 3c 2c 00 00 01 01 08 0a 02 3e d3 b9 02 3e ..<,.......>...>

0040 ea 23 17 03 01 00 20 a4 47 5e c4 54 87 66 a2 5a .#.... .G^.T.f.Z

0050 5d ef 24 77 7f 9b c5 57 84 a1 b6 f0 10 ef 3e be ].$w...W......>.

0060 bc 91 ec 31 a2 81 5e 17 03 01 00 e0 ee 34 fc 93 ...1..^......4..

0070 f9 b9 3f ba e7 fb 97 78 3e a0 25 09 77 bf c9 b0 ..?....x>.%.w...

0080 95 30 ca 6a e8 e7 7f cc a5 77 db e5 30 e6 34 ac .0.j.....w..0.4.

0090 e3 d0 84 98 d5 97 1a b5 9f 2b 9c 11 41 b7 ae ed .........+..A...

00a0 0e fc 54 52 89 fd 59 b0 77 42 d4 07 96 83 33 6f ..TR..Y.wB....3o

00b0 fb 85 dd e7 90 dc 83 44 41 1f 8f 1d d3 29 60 28 .......DA....)`(

00c0 58 a7 22 8e 6e 16 01 5f fa f1 4f 69 31 78 1e 6c X.".n..\_..Oi1x.l

00d0 a4 23 9e 89 3a 9c 25 37 da 9d 27 03 d4 17 31 9e .#..:.%7..'...1.

00e0 30 d8 25 d8 95 57 a3 7b 7f 77 20 7b f4 ee cd 7a 0.%..W.{.w {...z

00f0 9e 72 6f 21 80 2d d0 4c 66 f3 6f 40 e0 5d 31 43 .ro!.-.Lf.o@.]1C

0100 20 3c d2 2f 60 30 71 66 a4 7e 4a d2 3b b5 7c eb <./`0qf.~J.;.|.

0110 11 15 06 49 ab 00 46 61 b3 a5 76 7e 2c 37 9d 88 ...I..Fa..v~,7..

0120 6b f9 5e 72 e7 f3 ad 1a 94 cb 81 40 3a 7b d5 cc k.^r.......@:{..

0130 33 23 ad 82 46 29 a8 38 df 48 ba ea 23 87 15 4b 3#..F).8.H..#..K

0140 58 99 88 45 6a 54 e4 5a 54 81 4d bc X..EjT.ZT.M.

...

...

[root@bigboy ~]#

# Common LDAP Administrative Tasks

Here are some explanations of how to do many common LDAP tasks. They are all based on our sample organization with DNs of example and com.

Note: You need to always make sure that there are no entries for regular users in the /etc/passwd files of the LDAP clients. These should only reside on the LDAP server.

## Starting and Stopping LDAP

You can use the chkconfig command to get ldap configured to start at boot:

[root@bigboy tmp]# chkconfig ldap on

To start, stop, or restart ldap after booting, use

[root@bigboy tmp]# service ldap start

[root@bigboy tmp]# service ldap stop

[root@bigboy tmp]# service ldap restart

Remember to restart the ldap process every time you make a change to the LDAP database file for the changes to take effect on the running process.

## LDAP users changing their own passwords

LDAP users can modify their LDAP passwords using the regular passwd command.

[ldapuser@smallfry ldapuser]$ passwd

Changing password for user ldapuser.

Enter login(LDAP) password:

New password:

Retype new password:

LDAP password information changed for ldapuser

passwd: all authentication tokens updated successfully.

[ldapuser@smallfry ldapuser]$

## LDAP Password Changes by LDAP User "root"

The following three commands will reset the password for ldapuser's account. The ldappasswd command automatically generates and sets the password unless run with the -S (prompt for new password) or -s (specify new password) command line options. When prompted for the LDAP password, use the unencrypted version of the root password you created and placed in your slapd.conf file.

[root@smallfry tmp]# ldappasswd -x -W -D cn=Manager,dc=example,dc=com" "uid=ldapuser,ou=People,dc=example,dc=com"

Enter LDAP password:

New password: c06Nb/MA

Result: Success (0)

[root@smallfry tmp]#

[root@smallfry tmp]# ldappasswd -S -x -W -D "cn=Manager,dc=example,dc=com" "uid=ldapuser,ou=People,dc=example,dc=com"

New password:

Re-enter new password:

Enter LDAP password:

Result: Success (0)

[root@smallfry tmp]#

[root@smallfry tmp]# ldappasswd -s NewpasS -x -W –D "cn=Manager,dc=example,dc=com" "uid=ldapuser,ou=People,dc=example,dc=com"

Enter LDAP password:

Result: Success (0)

[root@smallfry tmp]#

## Modifying LDAP users by user "root"

One easy way for the system administrator to manage LDAP users is to modify the regular Linux users' characteristics on the LDAP server in the regular way and then run a script to automatically modify the LDAP database.

### The Modify LDAP User Script

You can use the very simple sample script /usr/local/bin/modifyldapuser to extract a particular user's information from /etc/passwd and import it into your LDAP database.

The script works by using the grep command to extract the /etc/passwd user record to a temporary file. It then runs the migrate\_passwd script on this data and outputs the result to a temporary LDIF file. Next, the script replaces the default padl DC with the example DC and exports this to the final LDIF file. Finally, the ldapmodify command does the update, and then the temporary files are deleted.

#!/bin/bash

grep $1 /etc/passwd > /tmp/modifyldapuser.tmp

/usr/share/openldap/migration/migrate\_passwd.pl \

/tmp/modifyldapuser.tmp /tmp/modifyldapuser.ldif.tmp

cat /tmp/modifyldapuser.ldif.tmp | sed s/padl/example/ \

> /tmp/modifyldapuser.ldif

ldapmodify -x -D "cn=Manager,dc=example,dc=com" -W -f \

/tmp/modifyldapuser.ldif

rm -f /tmp/modifyldapuser.\*

Remember to make the script executable and usable only by user root with the chmod command.

[root@bigboy tmp]# chmod 700 /usr/local/bin/modifyldapuser

[root@bigboy tmp]#

To use the script, modify the Linux user. In this case, modify the password for user ldapuser by running the modifyldapuser script using ldapuser as the argument. You will be prompted for the LDAP root password.

[root@bigboy tmp]# passwd ldapuser

Changing password for user ldapuser.

New password:

Retype new password:

passwd: all authentication tokens updated successfully.

[root@bigboy tmp]# modifyldapuser ldapuser

Enter LDAP Password:

modifying entry "uid=ldapuser,ou=People,dc=example,dc=com"

[root@bigboy tmp]#

## Adding new LDAP users

You can use the short script in this section to add LDAP users to your database. I'll also provide an example of how to use it.

### Create an LDAP Add User Script

You can create a /usr/local/bin/addldapuser script based on the modifyldapuser script you created earlier. For example:

#!/bin/bash

grep $1 /etc/passwd > /tmp/changeldappasswd.tmp

/usr/share/openldap/migration/migrate\_passwd.pl \

/tmp/changeldappasswd.tmp /tmp/changeldappasswd.ldif.tmp

cat /tmp/changeldappasswd.ldif.tmp | sed s/padl/example/ \

> /tmp/changeldappasswd.ldif

ldapadd -x -D "cn=Manager,dc=example,dc=com" -W -f \

/tmp/changeldappasswd.ldif

rm -f /tmp/changeldappasswd.\*

### Add the User to the Database

Adding the user to database takes three steps:

1. Create the Linux user on the LDAP server.

2. Run the addldapuser script with the username as the only argument. This example imports a previously created Linux user named ldapuser. The script prompts you for your LDAP root password.

[root@bigboy tmp]# addldapuser ldapuser

Enter LDAP Password:

adding new entry "uid=ldapuser,ou=People,dc=example,dc=com"

[root@bigboy tmp]#

3. Create home directories for the user on all the LDAP client Linux boxes.

Remember that this script adds existing Linux users to the LDAP database. The creation of Linux users still requires the use of the adduser command.

## Deleting LDAP users

Sometimes you want to get rid of users instead of add them. You can create a /usr/local/bin/deleteldapuser script to delete LDAP users from your database. For example

#!/bin/bash

ldapdelete -x -W -D "cn=Manager,dc=example,dc=com" \

"uid=$1,ou=People,dc=example,dc=com"

To delete the user from the database, run the deleteldapuser script with the username as the only argument. This example below deletes a previously created Linux user named ldapuser. The script prompts you for your LDAP root password.

[root@bigboy tmp]# deleteldapuser ldapuser

Enter LDAP Password:

[root@bigboy tmp]#

## LDAP Web Management Tools

Once you understand the principles behind LDAP management, you may want to use a graphical tool to help with further administration. If the tool misbehaves, at least you'll now know how to try to fix it behind the scenes from the command line.

The LDAP Account Manager (LAM), which is available at <http://lam.sourceforge.net>, is a well known, easy-to-use product. After you feel comfortable enough with the background tasks and concepts outlined in this chapter, you should give it a try.

# Conclusion

LDAP is rapidly becoming a defacto standard for remote authentication and authorization of users, not only in the realm of Linux, but also in that of Windows where it is a key component of Active Directory. Usage of LDAP is also becoming increasingly widespread in wireless networking systems. For example in hot spots, ISPs will sacrifice data security for the sake of convenience by not using encryption, but will use LDAP to restrict access to the Internet to people who have purchased pre-paid access codes with a predefined lifetime.

***REFERENCES:-***

"<http://www.linuxhomenetworking.com/wiki/index.php/Quick_HOWTO_:_Ch31_:_Centralized_Logins_Using_LDAP_and_RADIUS>"

<http://www.linux-tutorial.info/modules.php?name=MContent&pageid=150>

[http://m.sybase.com/content/1026313/SYSD1039LDAP WP.pdf](http://m.sybase.com/content/1026313/SYSD1039LDAP%20WP.pdf)

<http://www.softpanorma.org/NET/Directories/ldap.shtml>