* Install OpenLDAP for Windows from <http://www.userbooster.de/en/download/openldap-for-windows.aspx> and follow its [installation instruction.](http://www.userbooster.de/en/support/feature-articles/openldap-for-windows-installation.aspx) Install it on "C:\App\OpenLDAP"
* Accept all the default. Use the **BDB** (Berkley Database) as the **Backend Engine**.
* Your LDAP Server is now running. To see the service just open your Windows Services and search for **OpenLDAP Service**. If you don’t want the service to run automatically every time the Windows restart, just change it to **Manual** from the Properties Dialog.
* Next, install **LDAPExplorerTool** from <http://ldaptool.sourceforge.net/>. And try to connect to your LDAP Server using these settings :
  + Server Name or IP : According to your Computer Name or IP
  + LDAP Port : **389** ; **check** the use default checkbox
  + LDAP SSL Port : **636** ; **check** the use default checkbox
  + Version : **3** (LDAP ver. 3)

User DN : **cn=Manager,dc=maxcrc,dc=com** ; **Uncheck** the anonymous login.

* + Password : **secret**
  + Base DN (Just **click** the **Guess Value** button)
  + For everything else, just accept the default value
  + Click the **Test Connection** button. And after saving it, just click **Open**.
* It should open an empty LDAP directory. Next we will try to add an actual value to it.
* Create a file in **C:\App\OpenLDAP\ldifdata**, name it **step1.ldif**. The contents are :

## DEFINE DIT ROOT/BASE/SUFFIX ####

## uses RFC 2377 format

## replace maxcrc and com as necessary below

## or for experimentation leave as is

## dcObject is an AUXILLIARY objectclass and MUST

## have a STRUCTURAL objectclass (organization in this case)

# this is an ENTRY sequence and is preceded by a BLANK line

dn: dc=maxcrc,dc=com

dc: maxcrc

description: My wonderful company as much text as you want to place

objectClass: dcObject

objectClass: organization

o: Maxcrc, Inc.

## FIRST Level hierarchy - people

## uses mixed upper and lower case for objectclass

# this is an ENTRY sequence and is preceded by a BLANK line

dn: ou=people, dc=maxcrc,dc=com

ou: people

description: All people in organisation

objectclass: organizationalunit

## SECOND Level hierarchy

## ADD a single entry under FIRST (people) level

# this is an ENTRY sequence and is preceded by a BLANK line

# the ou: Human Resources is the department name

dn: cn=291426,ou=people,dc=maxcrc,dc=com

objectclass: inetOrgPerson

cn: 291426

sn: luma

uid:lUma

userpassword: umapassword

mail: [Uma.L2@cognizant.com](mailto:Uma.L2@cognizant.com)

ou: Human Resources

* Save the file. And open a command line and run these command
  + cd C:\App\OpenLDAP\ClientTools
  + ldapmodify.exe -a -x -h localhost -p 389 -D "cn=manager,dc=maxcrc,dc=com" -f d:\App\OpenLDAP\ldifdata\step1.ldif -w secret
* From your **LDAP Explorer Tool** menu, select File -> Open last configuration, and you will find the LDAP Directory is no longer empty and could find user with cn=291426 created in hierarchy level
* We will create one more new user in second level hierarchy. For that create a file with name saravanan.lpdif here **C:\App\OpenLDAP\ldifdata** with below contents

##SECOND Level hierarchy

## ADD a single entry under FIRST (people) level

# this is an ENTRY sequence and is preceded by a BLANK line

# the ou: SOA is the department name

dn: cn=366589,ou=people,dc=maxcrc,dc=com

objectclass: inetOrgPerson

cn: 366589

sn: sakthivelsaravanakumar

uid: saravanan

userpassword: saravananpassword

mail: Saravanakumar.Sakthivel@cognizant.com

ou: SOA

* Save the file. And open a command line and run these command
  + cd C:\App\OpenLDAP\ClientTools
  + ldapmodify.exe -a -x -h localhost -p 389 -D "cn=manager,dc=maxcrc,dc=com" -f d:\App\OpenLDAP\ldifdata\saravanan.ldif -w secret
* From your **LDAP Explorer Tool**menu, select File -> Open last configuration
* As described in above step we can create as many users as needed.
* Please note: Attributes cn, user password, email id are very important in ccap perspective. So please provide values correctly.

Cn=enter networkusername

Userpassword=enter password

Mail=enter mailid

* Changes to be made in ccap properties file on ldap perspective

LDAP\_URL=ldap://10.238.237.43:389

#LDAP system user name. In case of failure, refer with NSS to confirm your area LDAP

LDAP\_SYSTEM\_USER\_NAME=cn=Manager,dc=maxcrc,dc=com

#LDAP system password. In case of failure, refer with NSS to confirm your area LDAP

LDAP\_SYSTEM\_PASSWORD=secret

#LDAP domain search base, usually same across CTS domain, In case of failure, refer with NSS to confirm your area LDAP

LDAP\_SEARCH\_BASE=ou=people,dc=maxcrc,dc=com

* Changes to be made in sonar.properties file on ldap perspective

#-------------------

# Sonar LDAP Plugin

#-------------------

# IMPORTANT : before activation, make sure that one Sonar administrator is defined in the external system

# Activates the plugin. Leave blank or comment out to use default sonar authentication.

sonar.authenticator.class: org.sonar.plugins.ldap.LdapAuthenticator

# Ignore failure at startup if the connection to external system is refused.

# Users can browse sonar but not log in as long as the connection fails.

# When set to true, Sonar will not start if connection to external system fails.

# Default is false.

#sonar.authenticator.ignoreStartupFailure: false

# Automatically create users (available since Sonar 2.0).

# When set to true, user will be created after successful authentication, if doesn't exists.

# The default group affected to new users can be defined online, in Sonar general settings. The default value is "sonar-users".

# Default is false.

sonar.authenticator.createUsers: true

# (omit if you use autodiscovery) URL of the LDAP server.

# If you are using ldaps, then you should install server certificate into java truststore.

# eg. ldap://localhost:10389

ldap.url:ldap://10.238.237.43:389

# (optional) Distinguished Name (DN) of the root node in LDAP from which to search for users,

# eg. “ou=users,o=mycompany”

ldap.baseDn:ou=people,dc=maxcrc,dc=com

# (optional) Bind DN is the username of an LDAP user to connect (or bind) with.

# This is a Distinguished Name of a user who has administrative rights,

# eg. “cn=sonar,ou=users,o=mycompany”. Leave blank for anonymous access to the LDAP directory.

ldap.bindDn:cn=Manager,dc=maxcrc,dc=com

# (optional) Bind Password is the password of the user to connect with.

# Leave blank for anonymous access to the LDAP directory.

ldap.bindPassword:secret

# Login Attribute is the attribute in LDAP holding the user’s login.

# Default is ‘uid’. Set ’sAMAccountName’ for Microsoft Active Directory

ldap.loginAttribute:cn

# Object class of LDAP users.

# Default is 'inetOrgPerson'. Set ‘user’ for Microsoft Active Directory.

ldap.userObjectClass: inetOrgPerson

# (advanced option) See http://java.sun.com/products/jndi/tutorial/ldap/security/auth.html

# Default is 'simple'. Possible values: 'simple', 'CRAM-MD5', 'DIGEST-MD5', 'GSSAPI'.

ldap.authentication: simple

# (advanced option)

# See

# http://java.sun.com/products/jndi/tutorial/ldap/security/digest.html

# http://java.sun.com/products/jndi/tutorial/ldap/security/crammd5.html

# eg. example.org

#ldap.realm:

# (advanced option) Context factory class.

# Default is 'com.sun.jndi.ldap.LdapCtxFactory'.

#ldap.contextFactoryClass: com.sun.jndi.ldap.LdapCtxFactory

* Screen shot of LDAP client.

