**1. Steps for installing Symas OpenLDAP**

* 1. Install SymasOpenLdap Silver version by double clicking on “symas-openldap-silver-win.NT\_i686-2.4.33.20121128.exe” and during the installation provide the exact location, where you want to install the OpenLdap server.

e.g.

SymasOpenLdap can be installed at below location

“J:\OpenLdap\LDAP\_Server\symas-openldap”

* 1. Once the installation is finished, complete the steps outlined below.
     1. Copy the file “J:\OpenLdap\LDAP\_Server\symas-openldap\etc\openldap\slapd.conf.default” to “J:\OpenLdap\LDAP\_Server\symas-openldap\etc\openldap\slapd.conf”
     2. Copy the file “J:\OpenLdap\LDAP\_Server\symas-openldap\ etc\openldap\ldap.conf.default ” to “J:\OpenLdap\LDAP\_Server\symas-openldap\etc\openldap\ldap.conf”
     3. Edit the “slapd.conf” file to suit your needs.
     4. Edit the “ldap.conf” file to suit your needs.
  2. Add “startSlapd.cmd” file under “J:\OpenLdap\LDAP\_Server\symas-openldap” with below contents.

echo 'Starting OpenLDAP...'

@rem cd J:\OpenLdap\LDAP\_Server\symas-openldap

slapd.exe -f J:\OpenLdap\LDAP\_Server\symas-openldap\etc\openldap\slapd.conf

* 1. Add “stopSlapd.cmd” file under “J:\OpenLdap\LDAP\_Server\symas-openldap” with below contents.

echo 'Stopping OpenLDAP...'

#slapd.exe -f J:\OpenLdap\LDAP\_Server\symas-openldap\etc\openldap\slapd.conf

set prgId=type slapd.pid

set prgName=slapd.exe

taskkill -F /IM slapd.exe

@rem taskkill -F -pid %prgId%

* 1. Double click on “startSlapd.cmd” file to start the SymasOpenLdap Server.

* 1. Double click on “stopSlapd.cmd” file to stop the SymasOpenLdap Server.
  2. We can use ApacheDirectoryStudio as well to check the connection and to browse the SymasOpenLdap with below credentials:

Host 192.168.24.131 (localhost)

Port 389

Domain name dc=example, dc=com

Password secret

1. **Steps for creating the schema over Symas OpenLDAP**
   1. Create one “ xxxx.schema ” file with all your need and save under below location

J:\OpenLdap\LDAP\_Server\symas-openldap\etc\openldap\schema

e.g.

Created one “user.schema” file for a userEntry object whose attributes are name, userName, userPassword and telephoneNumber.

and saved this file at “J:\OpenLdap\LDAP\_Server\symas-openldap\etc\openldap\schema\user.schema”

Structure of “user. schema”

objectclass ( 1.4.7.2.5.2.49199.3.3 NAME 'userEntry'

DESC 'a user'

SUP ( top ) STRUCTURAL

MUST ( sn $ cn )

MAY ( userPassword $ telephoneNumber ) )

objectclass ( 1.4.7.2.5.2.49199.3.4 NAME 'rootUser'

DESC 'root for the user'

SUP top STRUCTURAL

MUST ( cn ) )

* 1. Add one entry in the “slapd.conf” for this newly created “xxxx.schema” file as given below,

e.g.

include "etc/openldap/schema/user.schema"

* 1. Add one parent entry into the “OpenLdap Server” so that the child entry could be added. Follow below steps,
     1. Change the suffix and rootdn both as “cn=user,dc=example,dc=com” in the “slapd.conf” file.
     2. Create one “99user.ldif” file under “J:\OpenLdap\LDAP\_Server\symas-openldap” with below contents,

dn: cn=user,dc=example,dc=com

changetype: add

objectClass: rootUser

cn: user

* + 1. Open command prompt at “J:\OpenLdap\LDAP\_Server\symas-openldap” and execute the below command.

J:\OpenLdap\LDAP\_Server\symas-openldap>ldapadd -x -D "cn=user,dc=example,dc=com" -W -f 99user.ldif

* + 1. Provide the LDAP Password as “secret”
    2. After successful execution we’ll get the below message,

adding new entry "cn=user,dc=example,dc=com"

1. **Steps for adding the entry into Symas OpenLDAP**

To add one entry into the OpenLdapServer through command prompt use below steps

* 1. Create one “99user.ldif” file under “J:\OpenLdap\LDAP\_Server\symas-openldap” with below contents,

dn: cn=Test1,cn=user,dc=example,dc=com

objectClass: userEntry

cn: Test1

sn: Test1

telephoneNumber: +91 999-995-5555

userPassword: Test1

* 1. Open command prompt at “J:\OpenLdap\LDAP\_Server\symas-openldap” and execute the below command.

J:\OpenLdap\LDAP\_Server\symas-openldap>ldapadd -x -D "cn=user,dc=example,dc=com" -W -f 99user.ldif

* 1. Enter LDAP Password as “secret”.
  2. After successful execution we’ll get the below message,

adding new entry "cn=Test1,cn=user,dc=example,dc=com"

1. **Steps to write the java program for POC**
   1. Create a java project in the eclipse and add below jars into the classpath,

spring-ldap-1.2.1.jar

spring-beans-2.5.6.jar

spring-context-2.5.6.jar

spring-core-2.5.6.jar

spring-dao-2.0-rc1.jar

commons-logging-1.1.1.jar

commons-lang-2.1.jar

* 1. Add below bean definitions into the spring configuration file.

<bean id=*"userDAO"* class=*"com.crimsonlogic.ldappoc.dao.UserDAOImpl"*>

<property name=*"ldapTemplate"* ref=*"ldapTemplate"* />

</bean>

<bean id=*"ldapTemplate"* class=*"org.springframework.ldap.core.LdapTemplate"*>

<constructor-arg ref=*"contextSource"* />

</bean>

<bean id=*"contextSource"* class=*"org.springframework.ldap.core.support.LdapContextSource"*>

<property name=*"url"* value=*"ldap://192.168.24.131:389"* />

<property name=*"base"* value=*"cn=user,dc=example,dc=com"* />

<property name=*"userName"* value=*"cn=user,dc=example,dc=com"* />

<property name=*"password"* value=*"secret"* />

</bean>

* 1. Use below piece of code to add entry into the OpenLdap.

DistinguishedName dn = **new** DistinguishedName();

dn.add("cn", "Test1" );

Attributes attrs = **new** BasicAttributes();

BasicAttribute ocattr = **new** BasicAttribute("objectclass");

ocattr.add("top");

ocattr.add("userEntry");

attrs.put(ocattr);

attrs.put("cn", "Test1");

attrs.put("sn", "Test1");

attrs.put("userPassword", "Test1");

attrs.put("telephoneNumber", "+91 999-995-5555");

ldapTemplate.bind(dn, **null**, attrs);

* 1. Use below piece of code to modify entry into the OpenLdap.

DistinguishedName dn = **new** DistinguishedName();

dn.add("cn", "Test1" );

Attributes attrs = **new** BasicAttributes();

BasicAttribute ocattr = **new** BasicAttribute("objectclass");

ocattr.add("top");

ocattr.add("userEntry");

attrs.put(ocattr);

attrs.put("cn", "Test1");

attrs.put("sn", "Test1");

attrs.put("userPassword", "Test1");

attrs.put("telephoneNumber", "+91 999-996-6666");

ldapTemplate.rebind(dn, **null**, attrs);

* 1. Use below piece of code to delete the entry from the OpenLdap.

DistinguishedName dn = **new** DistinguishedName();

dn.add("cn", "Test1" );

ldapTemplate.unbind(dn);

4.6 Use below piece of code to write the authentication logic.

DistinguishedName dn = **new** DistinguishedName();

dn.add("cn", userName);

ldapTemplate.lookup(dn, getContextMapper());

**protected** ContextMapper getContextMapper() {

return new UserContextMapper();

}

**private** **static** **class** UserContextMapper **implements** ContextMapper {

**public** Object mapFromContext(Object ctx) {

DirContextAdapter context = (DirContextAdapter) ctx;

UserTO uto = **new** UserTO();

uto.setUsername(context.getStringAttribute("cn"));

uto.setPassword(context.getStringAttribute("sn"));

uto.setTelephone(

context.getObjectAttribute("telephoneNumber").toString());

**return** uto;

}

}

1. **References:**

|  |  |
| --- | --- |
| Installation of “symas-openldap-silver-win.NT\_i686-2.4.33.20121128.exe” | www.symas.com |
| Installation of “ApacheDirectoryStudio” | <http://directory.apache.org/studio/download/download-windows.html>  <http://directory.apache.org/studio/installation-in-eclipse.html> |
| OpenLDAP software documentation | http://www.openldap.org/doc/admin24  <http://symas.com/>  <http://www.rfc-editor.org/rfc/rfc4519.txt>  <http://www.zytrax.com/books/ldap> |