**LDAP SERVER INSTALLATION STEPS**

**Document Control**

|  |  |  |  |
| --- | --- | --- | --- |
| Date | Author | Version | Change Reference |
| 02/05/2016 | Kaleem and Naresh | 1.0 | Document Creation |

**Contents**

[**1. Introduction** 3](#_Toc449971730)

[**1.1 LDAP Server:** 3](#_Toc449971731)

[**1.2 LDAP Works:** 3](#_Toc449971732)

[**2. Step by step installation and configuration OpenLDAP server:** 3](#_Toc449971733)

[**3. Steps to perform:** 4](#_Toc449971734)

[**3.1 Step #1.** Requirements 4](#_Toc449971735)

[**3.2 Step #2.** Start the service 4](#_Toc449971736)

[**3.3 Step #3.** Create LDAP root user password. 4](#_Toc449971737)

[**3.4 Step #4.** Update /etc/openldap/slapd.conf for the root password 4](#_Toc449971738)

[**3.5 Step #5.** Apply changes 5](#_Toc449971739)

[**3.6 Step #6.** Create test users 5](#_Toc449971740)

[**3.7 Step #7.** Migrate local users to LDAP 6](#_Toc449971741)

[**3.8 Step #8.** Update default settings on file 6](#_Toc449971742)

[**3.9 Step #9.** Convert passwd. file to ldif(LDAP Data Interchange Format)file 6](#_Toc449971743)

[**3.10 Step #10.** Update root.ldif file for the “Manager” of LDAP Server 7](#_Toc449971744)

[**3.11 Step #11.** Create a domain ldif file 7](#_Toc449971745)

[(/etc/openldap/adminmart.com.ldif) 7](#_Toc449971746)

[**3.12 Step #12.** Import All users in to the LDAP 8](#_Toc449971747)

[**3.13 Step #13.** Apply changes 9](#_Toc449971748)

[**3.14 Step #14.** Test LDAP Server 9](#_Toc449971749)

[**4. Reference:** 9](#_Toc449971750)

[**5. LDAP Browser Installation** 10](#_Toc449971751)

# **1. Introduction**

# **1.1 LDAP Server:**

The **Lightweight Directory Access Protocol** (**LDAP**) is a directory service protocol that runs on a layer above the TCP/IP stack. It provides a mechanism used to connect to, search, and modify Internet directories. The **LDAP** directory service is based on a client-server model.

# **1.2 LDAP Works:**

LDAP directory service is based on a client−server model. One or more LDAP servers contain the data making up the LDAP directory tree or LDAP backend database.

An LDAP client connects to an LDAP server and asks it a question. The server responds with the answer, or with a pointer to where the client can get more information (typically, another LDAP server).

No matter what LDAP server a client connects to, it sees the same view of the directory; a name presented to one LDAP server references the same entry it would at another LDAP server. This is an important feature of a global directory service, like LDAP.

Open the Linux terminal and change the username to “**root “.**  By typing the command **su root**.

# **2. Step by step installation and configuration OpenLDAP server:**

Software:  OS-Cent OS 4.4, openldap 2.2.13-6.4E  
System name:   *ldap.adminmart.com*  
Domain name:   *adminmart.com*  
System IP:     *192.168.6.130*

**Note**: Use your domain name and IP instead of *adminmart*.

Easy steps for adding users:  
    1. Create unix user  
    2. Create unix user's ldap passwd file

3. Convert passwd.file to ldif file  
    4. Add ldap file to LDAP Directory using ldapadd

# **3. Steps to perform:**

# **3.1 Step #1.** Requirements

compat-openldap.i386 0:2.1.30-6.4E   
openldap-clients.i386 0:2.2.13-6.4E   
openldap-devel.i386 0:2.2.13-6.4E   
openldap-servers.i386 0:2.2.13-6.4E   
openldap-servers-sql.i386 0:2.2.13-6.4E

You can install them using the command:

**yum install \*openldap\* -y**

# **3.2 Step #2.** Start the service

To start the service we have to enter the following command.

**[root@ldap ~ ]# chkconfig --levels 235 ldap on  
 [root@ldap ~ ]# service ldap start**

# **3.3 Step #3.** Create LDAP root user password.

To create the LDAP root user password type the following command.

**[root@ldap ~]# slappasswd  
     New password:** enter password **Re-enter new password:** Re enter your password **{SSHA}cWB1VzxDXZLf6F4pwvyNvApBQ8G/DltW  
 [root@ldap ~]#**

# **3.4 Step #4.** Update /etc/openldap/slapd.conf for the root password

To update the root user password type the following command.

**[root@ldap ~]# vi /etc/openldap/slapd.conf**

Update the root password **{SSHA}cWB1VzxDXZLf6F4pwvyNvApBQ8G/DltW** in editor at below mentioned.

**#68 database bdb**

**# 69 suffix “dc=adminmart,dc=com”**

**#70 rootdn “cn=Manager,dc=adminmart,dc=com”**

**#71 rootpw {SSHA}cWB1VzxDXZLf6F4pwvyNvApBQ8G/DltW**

# **3.5 Step #5.** Apply changes

Whenever we apply the changes every time we have to restart the service LDAP.

To restart the service type the following command.

**[root@ldap ~]# service ldap restart**

# **3.6 Step #6.** Create test users

To create the test users and passwords type the following command.

**[root@ldap ~]# useradd test1  
 [root@ldap ~]# passwd test1  
   Changing password for user test1.  
   New UNIX password:   
   Retype new UNIX password:   
    passwd: all authentication tokens updated successfully.  
 [root@ldap ~]# useradd test2   
 [root@ldap ~]# test2  
    Changing password for user test2.  
    New UNIX password:   
    Retype new UNIX password:   
    passwd: all authentication tokens updated successfully.  
 [root@ldap ~]#**

If you want to create more users then repeat the same procedure for rest of the users.

# **3.7 Step #7.** Migrate local users to LDAP

We have to migrate the local users to LDAP, type the following command.

**[root@ldap ~]# grep root /etc/passwd >/etc/openldap/passwd.root  
[root@ldap ~]# grep test1 /etc/passwd > /etc/openldap/passwd.test1  
[root@ldap ~]# grep test2 /etc/passwd > /etc/openldap/passwd.test2**

Repeat same for the rest of the users.

# **3.8 Step #8.** Update default settings on file

To update the default settings on file type the following command.

**/usr/share/openldap/migration/migrate\_common.ph**

set the default mail domain to adminmart.com in the editor.

**#71 $DEFAULT\_MAIL\_DOMAIN =”adminmart.com”;**

**#72 $DEFAULT\_BASE =”dc=adminmart,dc=com”;**

# **3.9 Step #9.** Convert passwd. file to ldif(LDAP Data Interchange Format)file

**[root@ldap ~]# /usr/share/openldap/migration/migrate\_passwd.pl /etc/openldap/passwd.root /etc/openldap/root.ldif**

**[root@ldap ~]# /usr/share/openldap/migration/migrate\_passwd.pl /etc/openldap/passwd.test1 /etc/openldap/test1.ldif**

**[root@ldap ~]# /usr/share/openldap/migration/migrate\_passwd.pl /etc/openldap/passwd.test2 /etc/openldap/test2.ldif**

# **3.10 Step #10.** Update root.ldif file for the “Manager” of LDAP Server

**[root@ldap ~]# vi /etc/openldap/root.ldif**

Update manager to the cn in the vi editor following below

**#1 dn: uid=root,ou=People,dc=adminmart,dc=com**

**#2 uid: root**

**#3 cn: Manager**

**#4 objectClass: account**

# **3.11 Step #11.** Create a domain ldif file

# (/etc/openldap/adminmart.com.ldif)

Create a ldif file domain by following command

**[root@ldap ~]# cat> /etc/openldap/adminmart.com.ldif**

***Enter a blank Line***

**dn: dc=adminmart,dc=com**

**dc: adminmart**

**description: LDAP Admin**

**objectClass: dcObject**

**objectClass: organizationalUnit**

**ou: rootobject**

***Enter a blank Line***

**dn: ou=People, dc=adminmart, dc=com**

**ou: People**

**description: Users of adminmart**

**objectClass: organizationalUnit**

# **3.12 Step #12.** Import All users in to the LDAP

Importing the all user into the LDAP.

Add the Domain ldif file.

**[root@ldap ~]# ldapadd -x -D "cn=Manager,dc=adminmart,dc=com" -W -f  /etc/openldap/adminmart.com.ldif  
    Enter LDAP Password:   
    adding new entry "dc=adminmart,dc=com"  
    adding new entry "ou=People, dc=adminmart,dc=com"  
[root@ldap ~]#**

Add the users

**[root@ldap ~]# ldapadd -x -D "cn=Manager,dc=adminmart,dc=com" -W -f  /etc/openldap/root.ldif  
    Enter LDAP Password:   
    adding new entry "uid=root,ou=People,dc=adminmart,dc=com"  
    adding new entry "uid=operator,ou=People,dc=adminmart,dc=com"  
[root@ldap ~]#  
  
[root@ldap ~]# ldapadd -x -D "cn=Manager,dc=adminmart,dc=com" -W -f  /etc/openldap/test1.ldif  
    Enter LDAP Password:   
    adding new entry "uid=test1,ou=People,dc=adminmart,dc=com"  
[root@ldap ~]#   
  
[root@ldap ~]# ldapadd -x -D "cn=Manager,dc=adminmart,dc=com" -W -f  /etc/openldap/test2.ldif  
    Enter LDAP Password:   
    adding new entry "uid=test2,ou=People,dc=adminmart,dc=com"  
 [root@ldap ~]#**

Repeat the same for rest of the users

# **3.13 Step #13.** Apply changes

Apply changes

Whenever we apply the changes every time we have to restart the service LDAP.

To restart the service type the following command.

**[root@ldap ~]# service ldap restart**

# **3.14 Step #14.** Test LDAP Server

To test the LDAP server type the following command.

**[root@ldap ~]# ldapsearch -x -b 'dc=adminmart,dc=com' '(objectclass=\*)'**

It prints all the user Information.

**Refer the below link for Step by step installation and configuration OpenLDAP.**

# **4. Reference:**

**https://www.howtoforge.com/linux\_openldap\_setup\_server\_client#step-start-the-service**

# **5. LDAP Browser Installation**

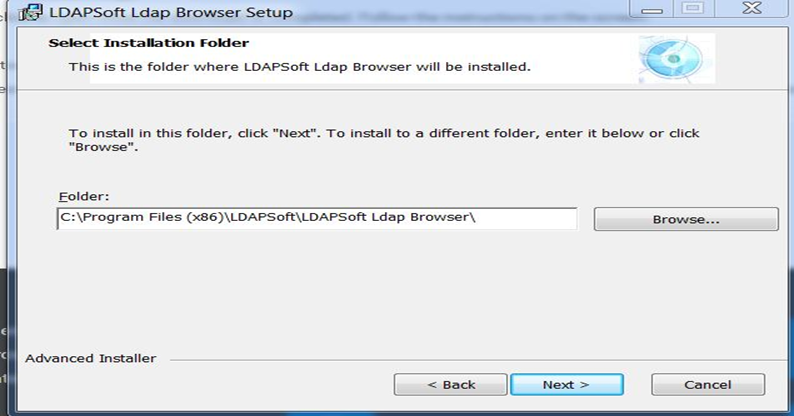
To communicate with the LDAP server we need to install the LDAP Browser.

<https://www.ldapsoft.com/ldapbrowserfree.html>

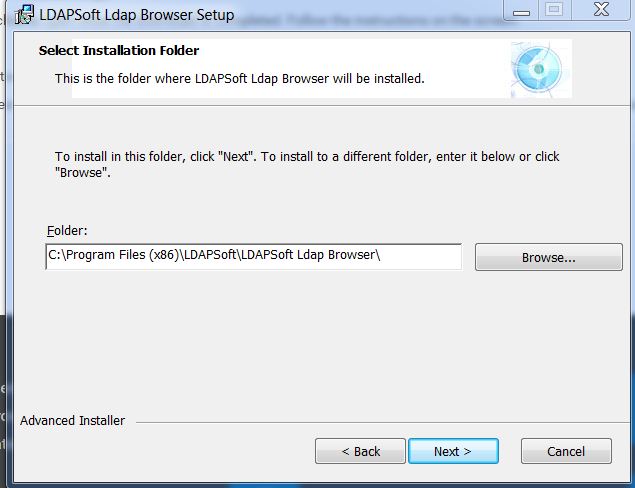
From the above link we can download the setup of LDAP browser.

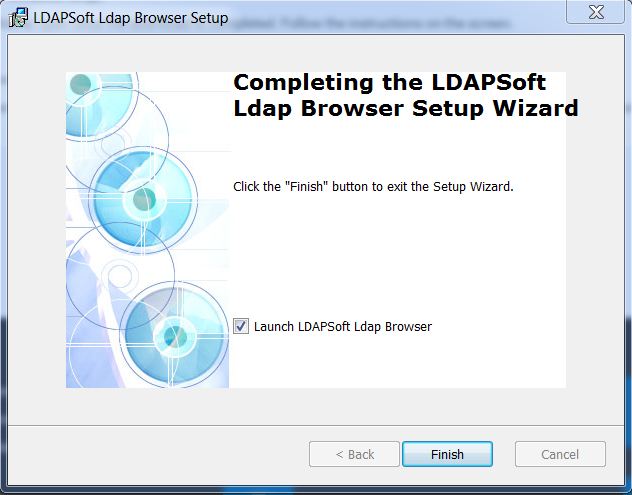
**Perform the following steps to install LDAP brwoser:**

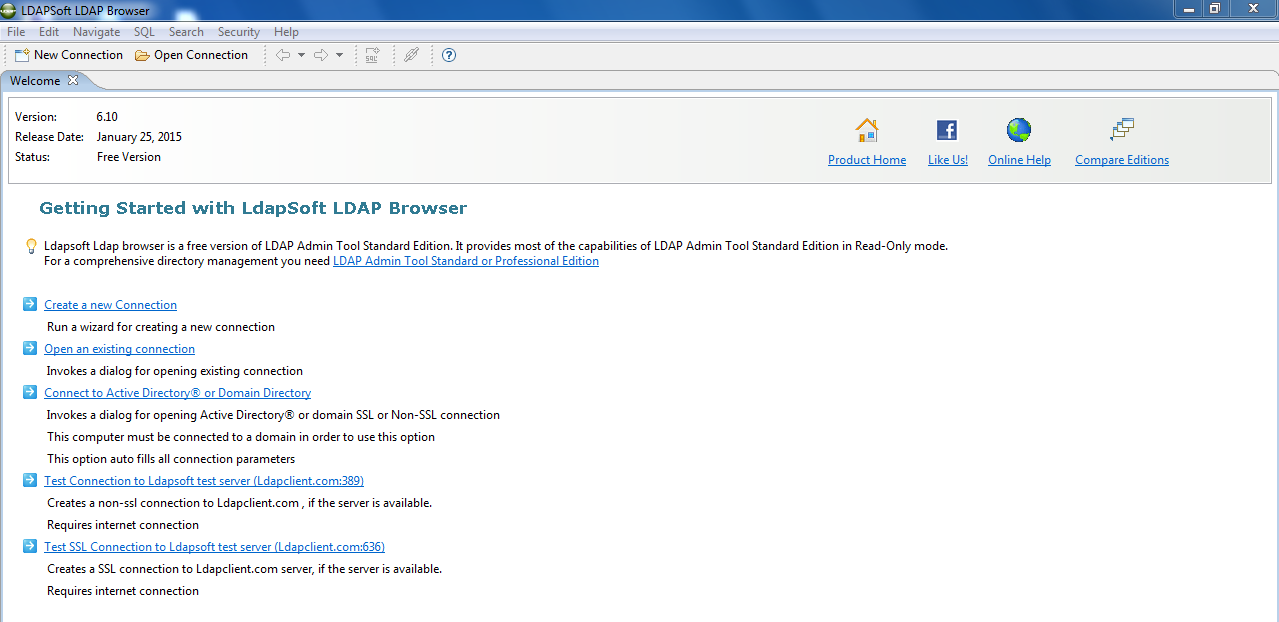




****



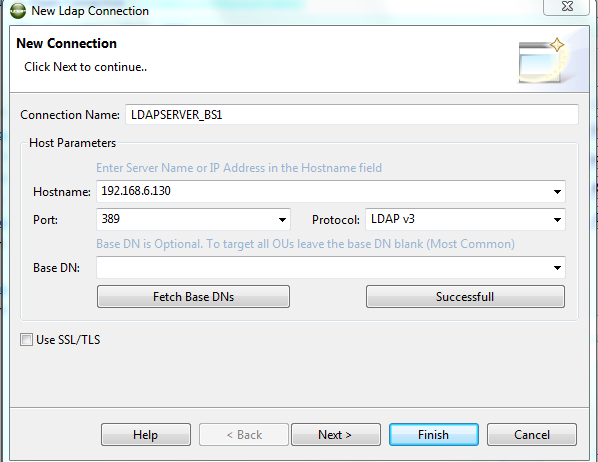




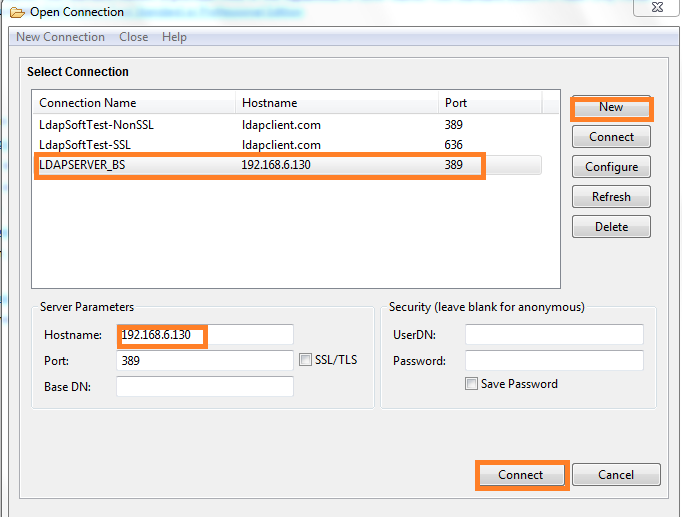
Open an existing connection link to create a new connection.

We need to mention the Connection name, Hostname, port.

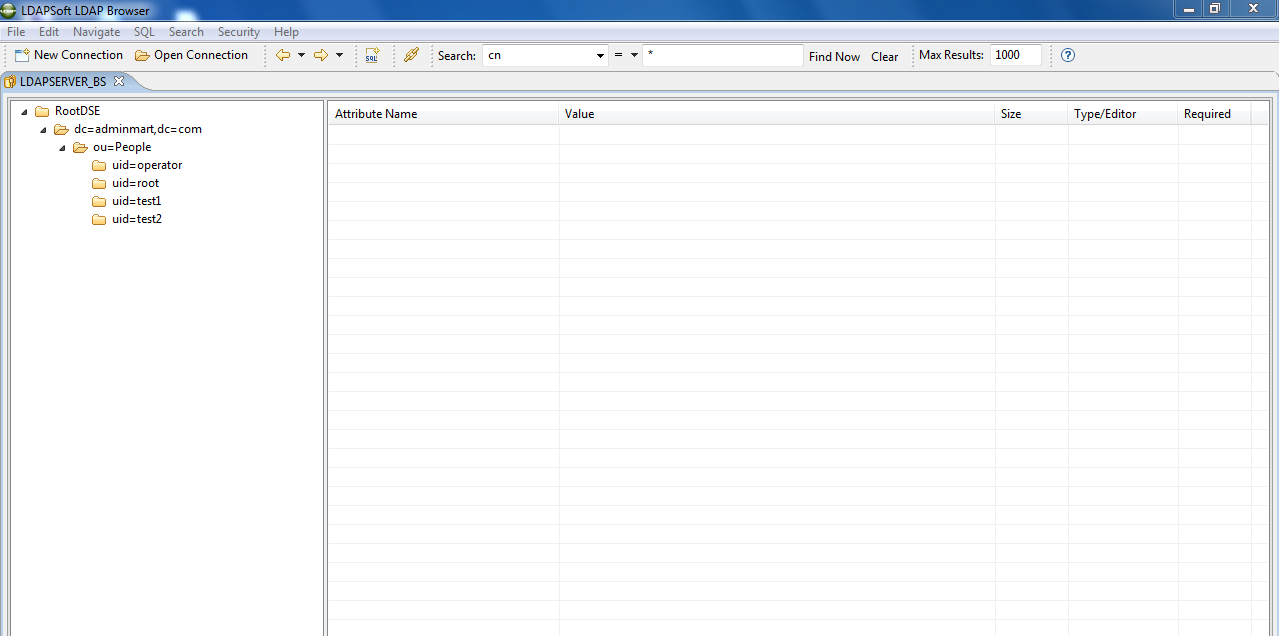
Then we need to test the connection.

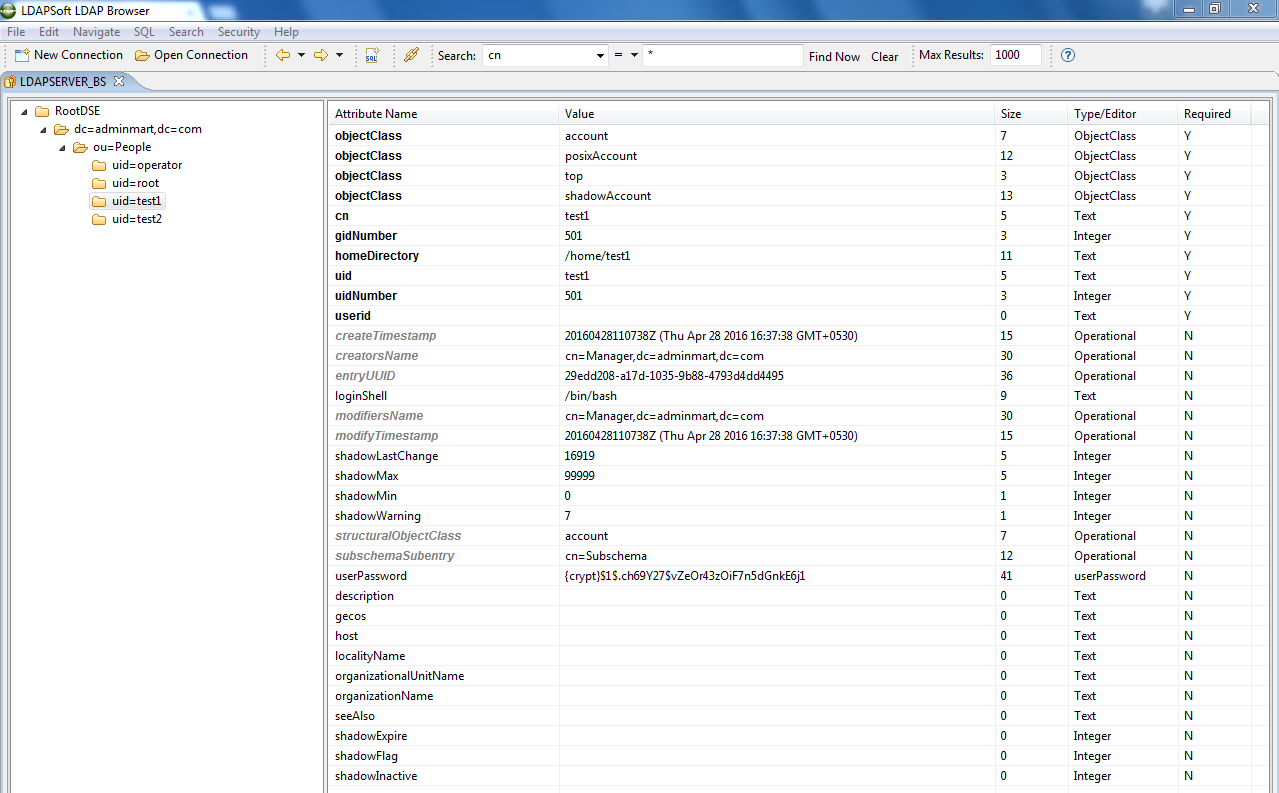


After opening the new connection the window shown below.



We can see the test users that we have created in the LDAP server from browser.





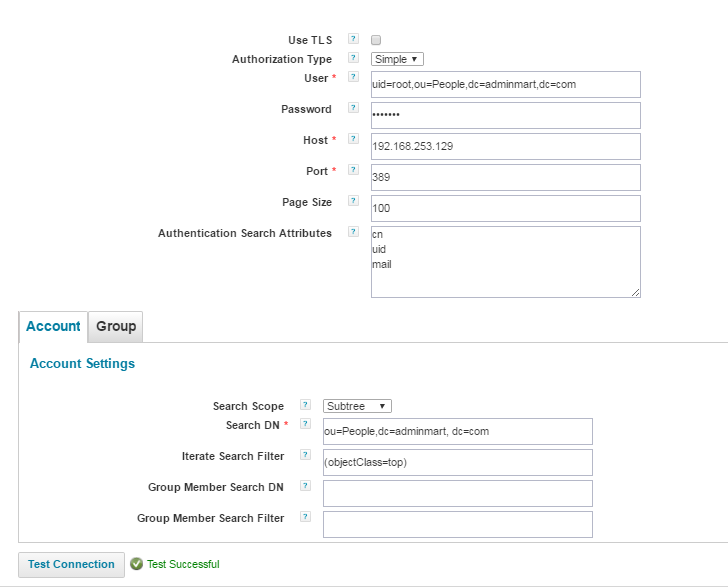
**LDAP Application Onboarding :**

Step 1: After installing the Linux VM with LDAP server open that from VM workstation.

Step2: Open the terminal and give the credentials as **su root** and **root**.

For IP address run the **ifconfig** command in the terminal

Step 3: Now in sailpoint start the LDAP Application Onboarding as below picture.



Here in Iterate Search filter we can configure objectClass=top, \*, posixAccount.

Step 4: In preview the identities which we added in terminal will get reflects in that.

Step 5: Run the aggregation task for the application.

Commands to create group and add users to that in VM terminal :

To display the users in linux terminal : cut -d: -f1 /etc/passwd

create group :

step 1: groupadd groupname

step 2 : Adding user to that group : usermod -G groupname username

step 3: more /etc/passwd

step 4: more /etc/group

the user will add into the group specified and will display as groupname:x:id:username