**LDAP Integrate with Jenkins**

**Pre-Requisites:**

* Install Jenkins
* Install and configure OpenLDAP
* Install and configure LDAP Account Manager on Ubuntu 18.04

**Install and configure OpenLDAP:**

hostnamectl set-hostname ldap.example.com

echo "13.126.172.164 ldap.example.com" | sudo tee -a /etc/hosts

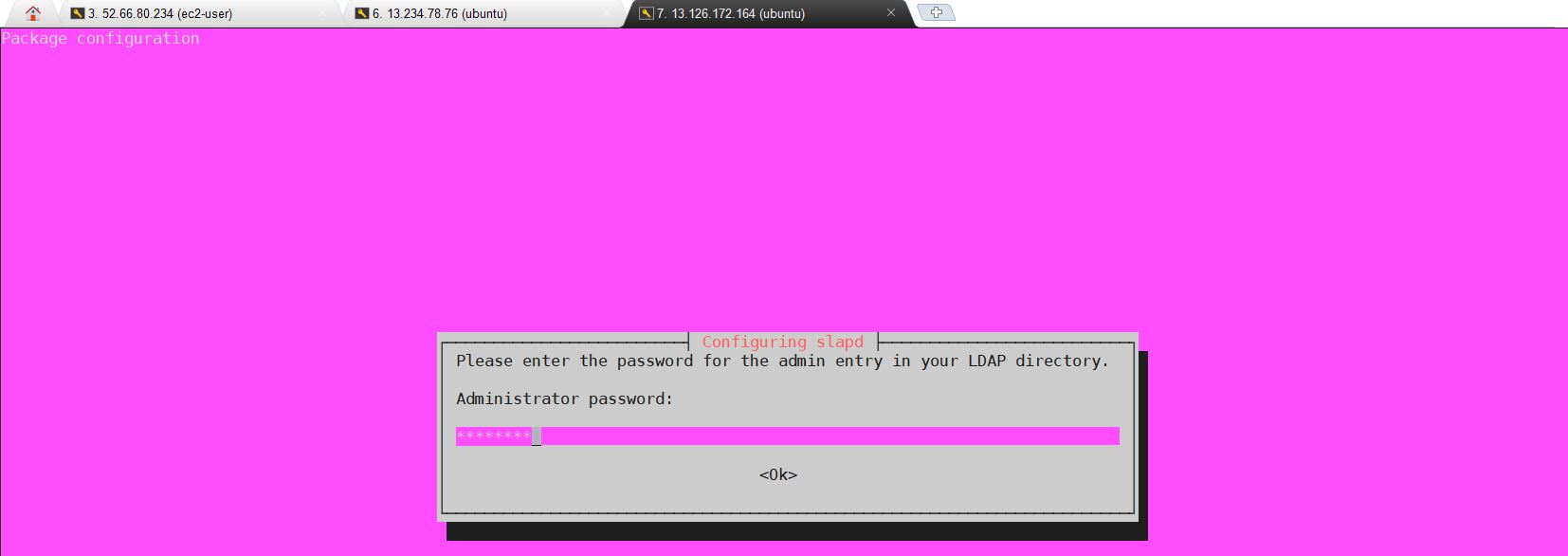
Replace ldap.example.com with your correct hostname/valid domain name.

The OpenLDAP packages are available on Ubuntu 18.04 upstream repositories, and you install them by just firing apt install commands.

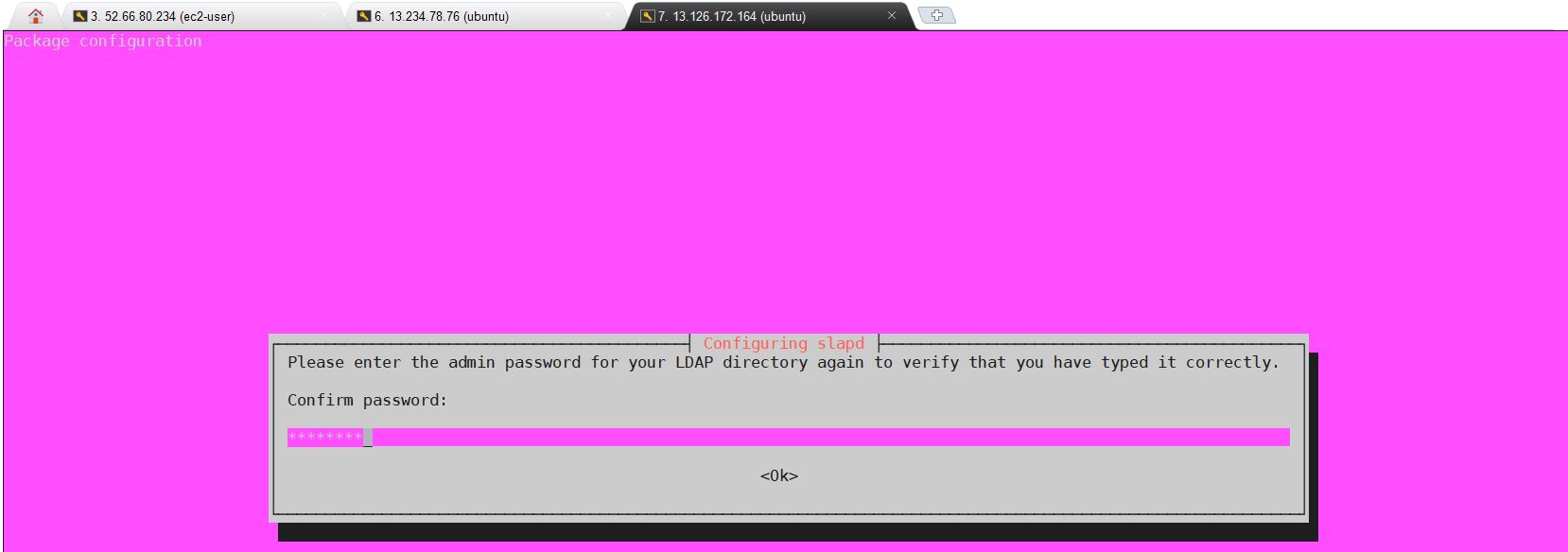
apt update

apt -y install slapd ldap-utils

During the installation, you’ll be prompted to set LDAP admin password, provide your desired password, then press <OK>

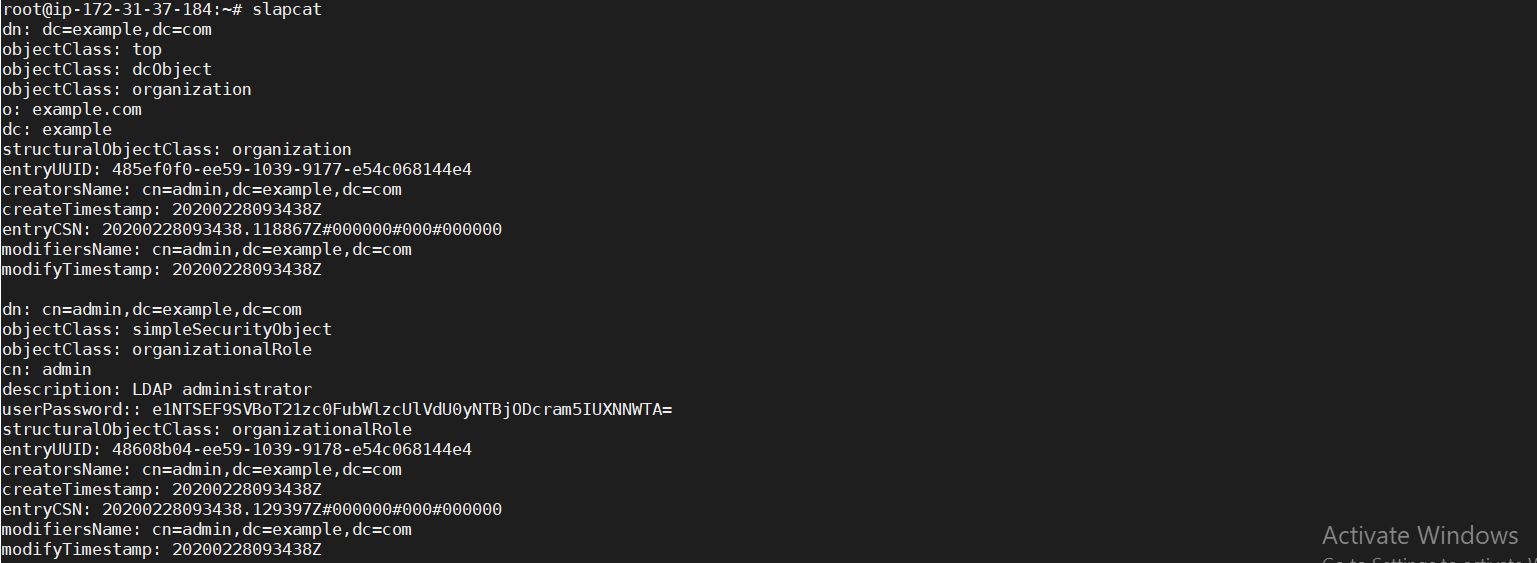


Confirm the password and continue installation by selecting <ok> with TAB key.



You can confirm that your installation was successful using the command slapcat to output SLAPD database contents.

root@ip-172-31-37-184:~# slapcat



Add base dn for Users and Groups:

The next step is adding a base DN for users and groups. Create a file named basedn.ldif with below contents:

vi basedn.ldif

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

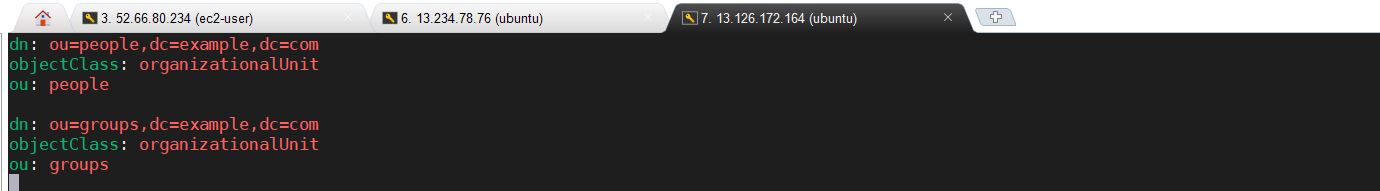
objectClass: organizationalUnit

ou: people

dn: ou=groups,dc=example,dc=com

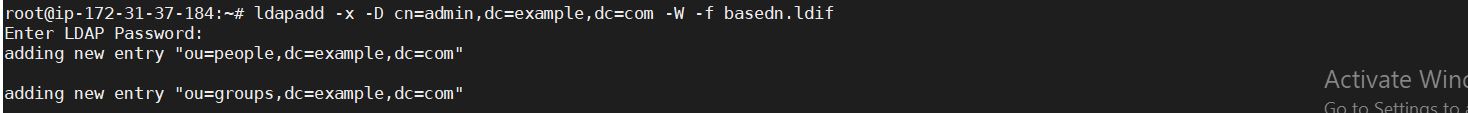
objectClass: organizationalUnit

ou: groups



Now add the file by running the command:

ldapadd -x -D cn=admin,dc=example,dc=com -W -f basedn.ldif



Install Apache Web server & PHP:

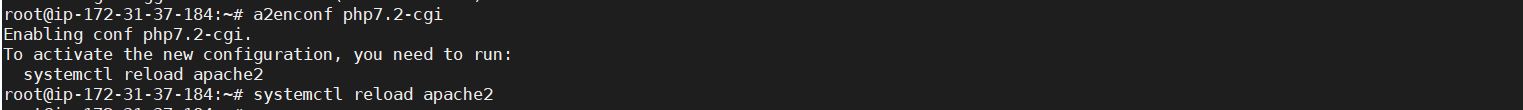
Install PHP and Apache web server by running the commands below on your terminal

apt -y install apache2 php php-cgi libapache2-mod-php php-mbstring php-common php-pear

Then enable php-cgi PHP extension.

a2enconf php7.2-cgi

systemctl reload apache2



**Install LDAP Account Manager:**

LDAP Account Manager package is available on Ubuntu repositories, install it with the command:

apt -y install ldap-account-manager

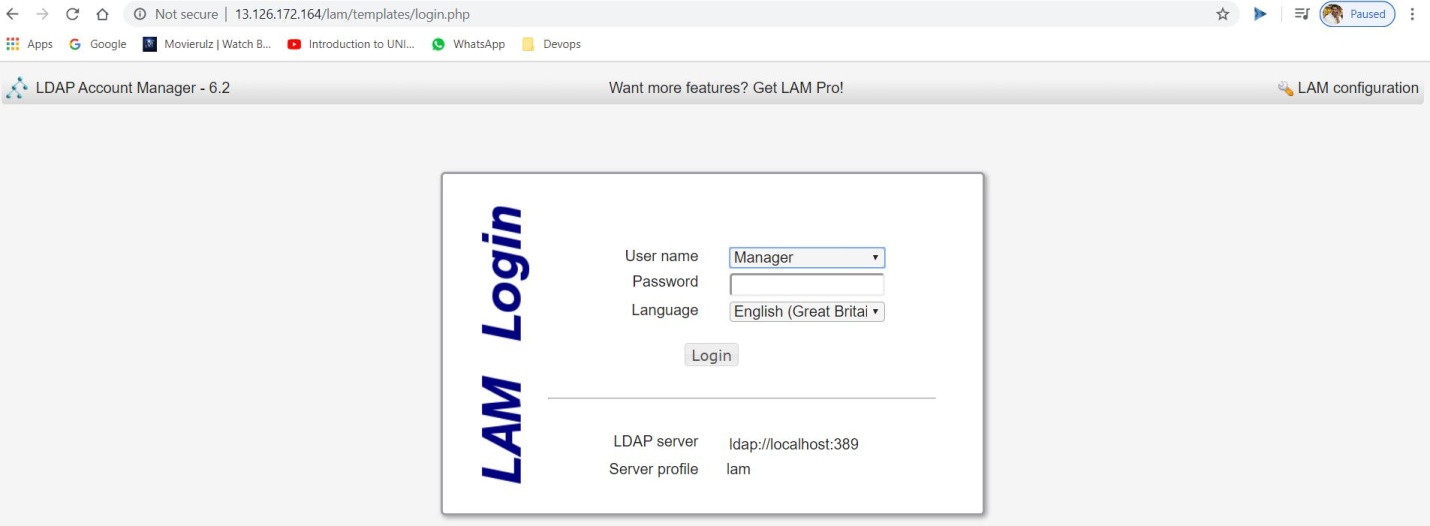
Restart apache web server after making the change:

systemctl restart apache2

Configure LDAP Account Manager:

Access LDAP Account Manager web interface from a trusted machine network on

http://(server’s hostname or IP address)/lam



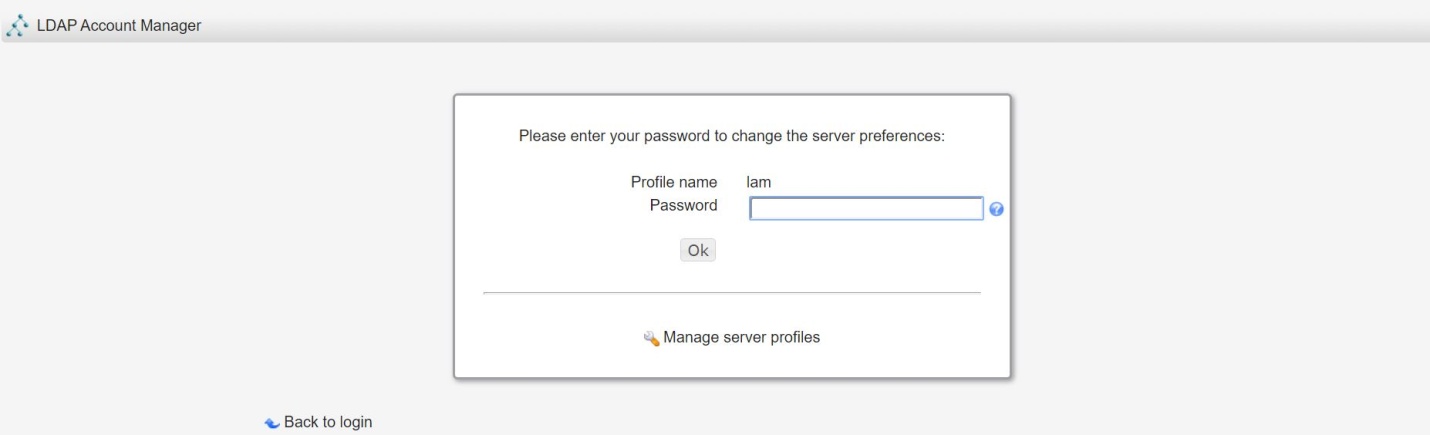
The LDAP Account Manager Login form will be shown. We need to set our LDAP server profile by clicking on[LAM configuration] at the upper right corner.

Then click on,Edit server profiles

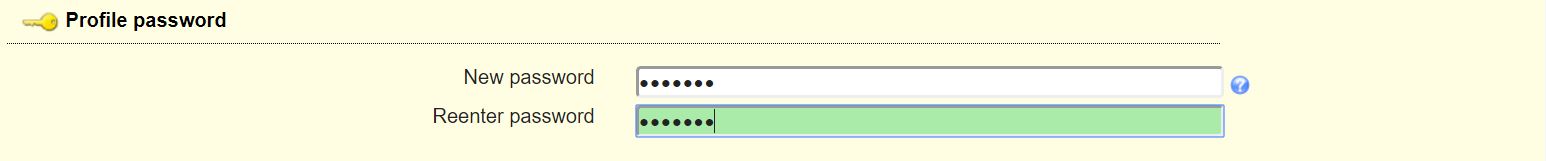


This will ask you for LAM Profile name Password:

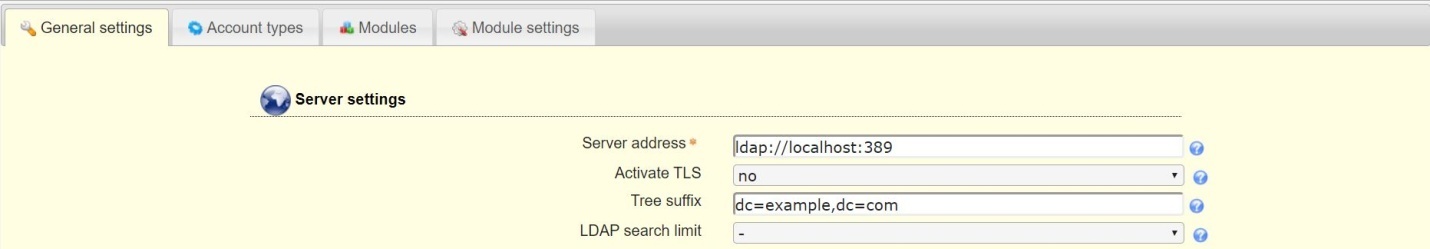
Default password is lam



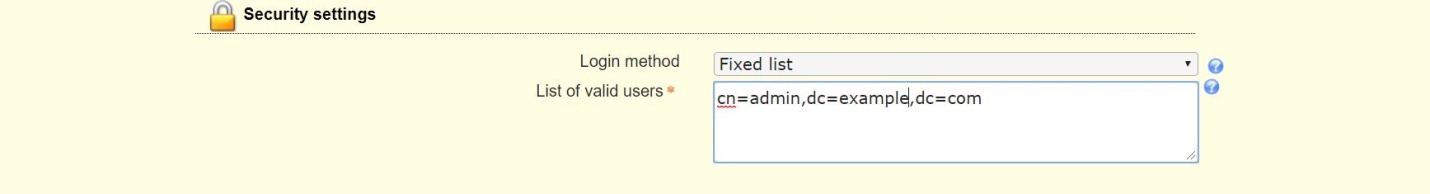
The first thing to change is Profile Password, this is at the end of General Settings page.



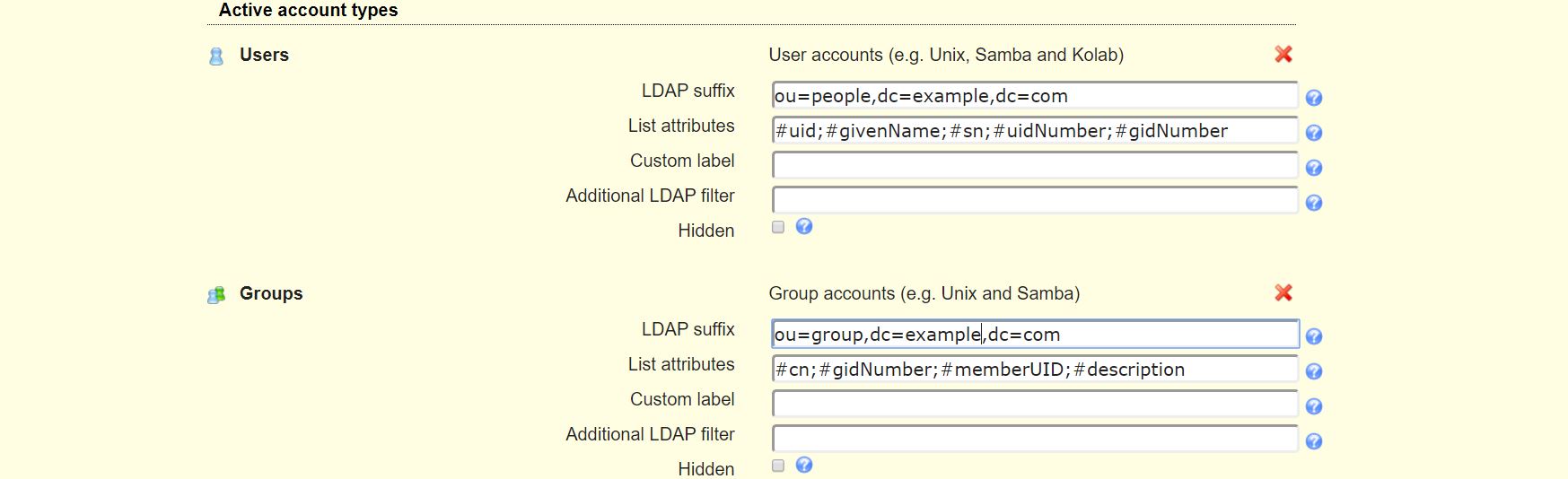
Next is to set LDAP Server address and Tree suffix. Mine looks like below, you need to use your Domain components as set in server hostname.



Set Dashboard login by specifying the admin user account and domain components under “Security settings” section.



Switch to “Account types” page and set Active account types LDAP suffix and List attributes.

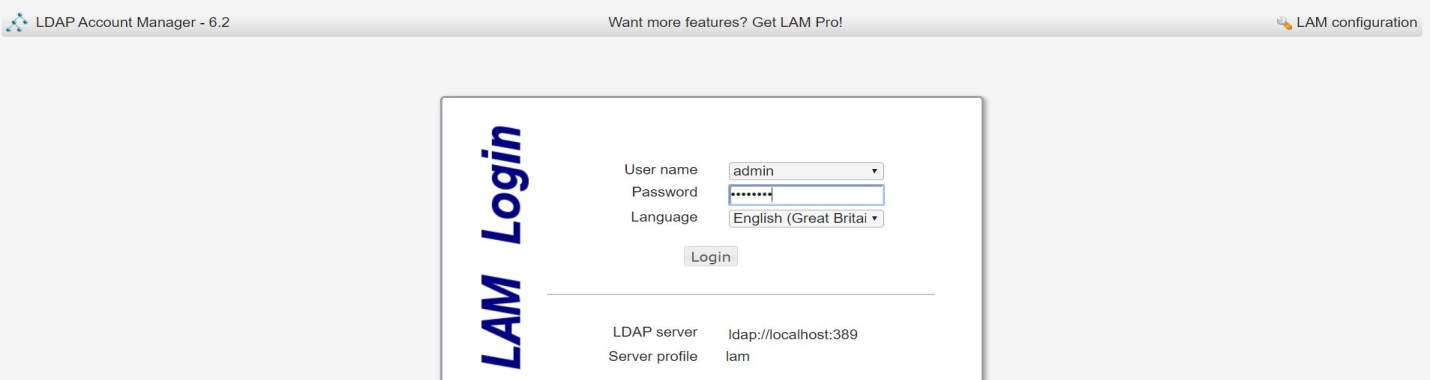


You can also enable other available account types you wish to use. User and Group modules can be enabled and disabled on “Modules” page.

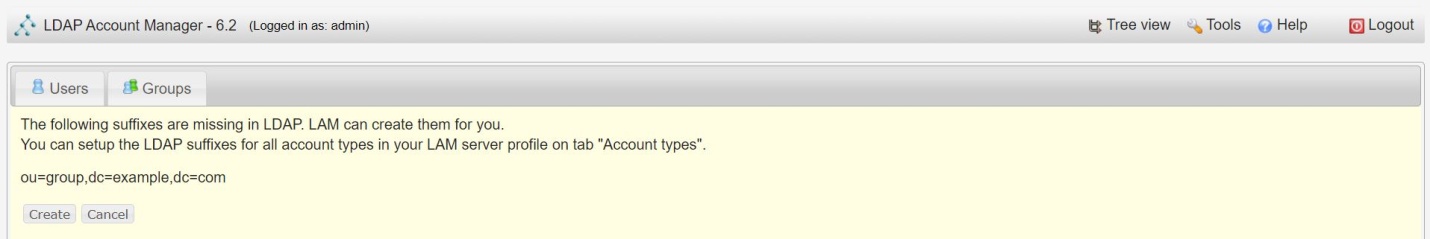
When done with the settings, click the Save button at the bottom of the page.

**Add user accounts and groups with LDAP Account Manager:**

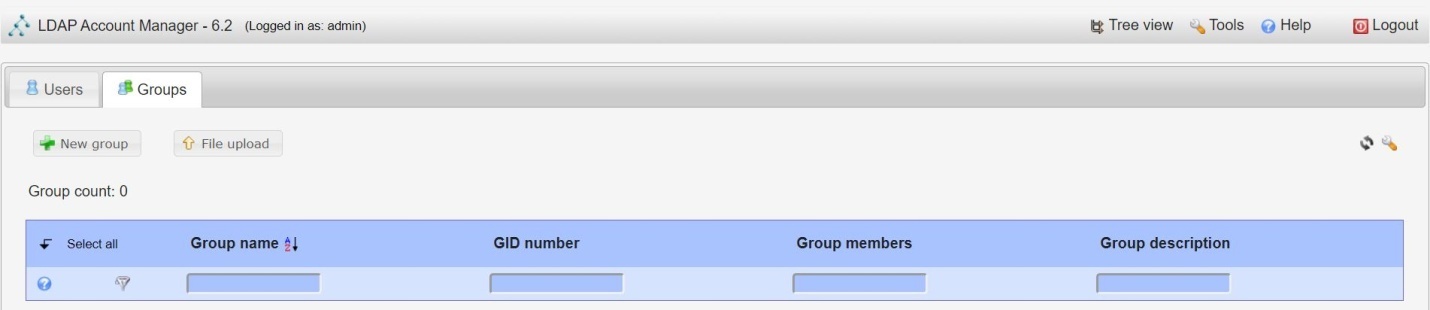
Login with the accountadmin to LAM dashboard to start managing user accounts and groups.



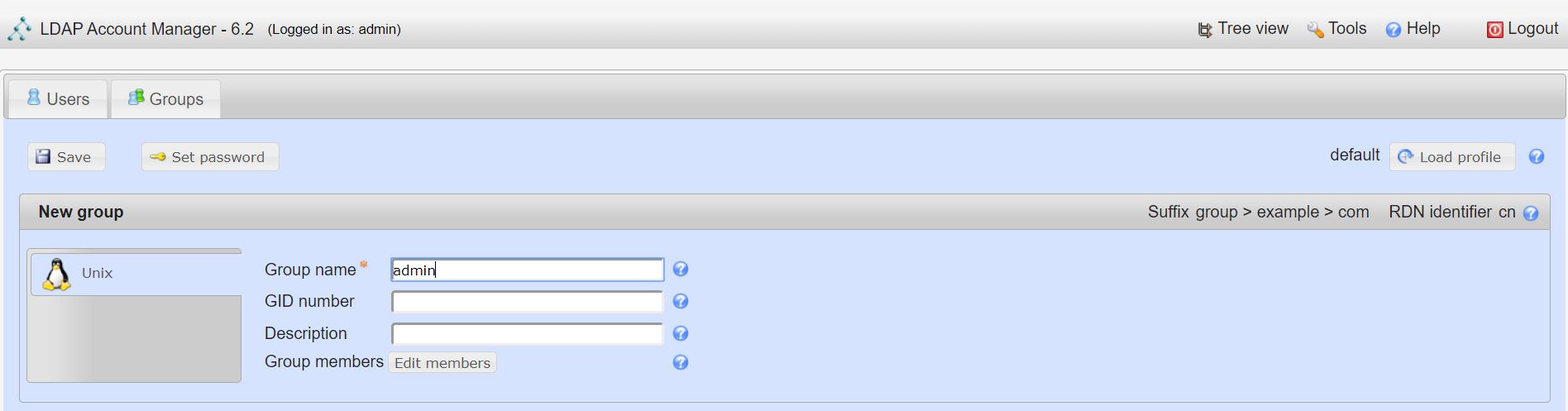
Click on create to create LAM.



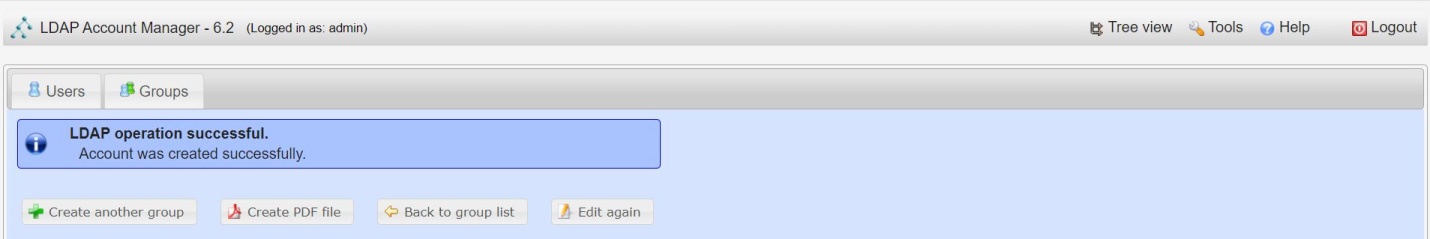
You’ll use the Users and Groups links to manage user accounts and groups.



Give the group a name, optional group ID and description.



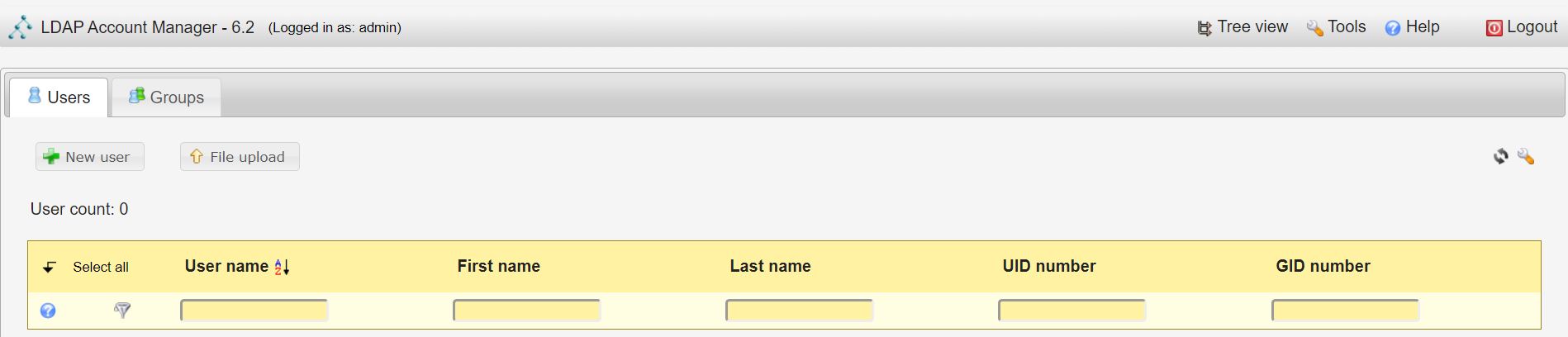
Click on Save button.



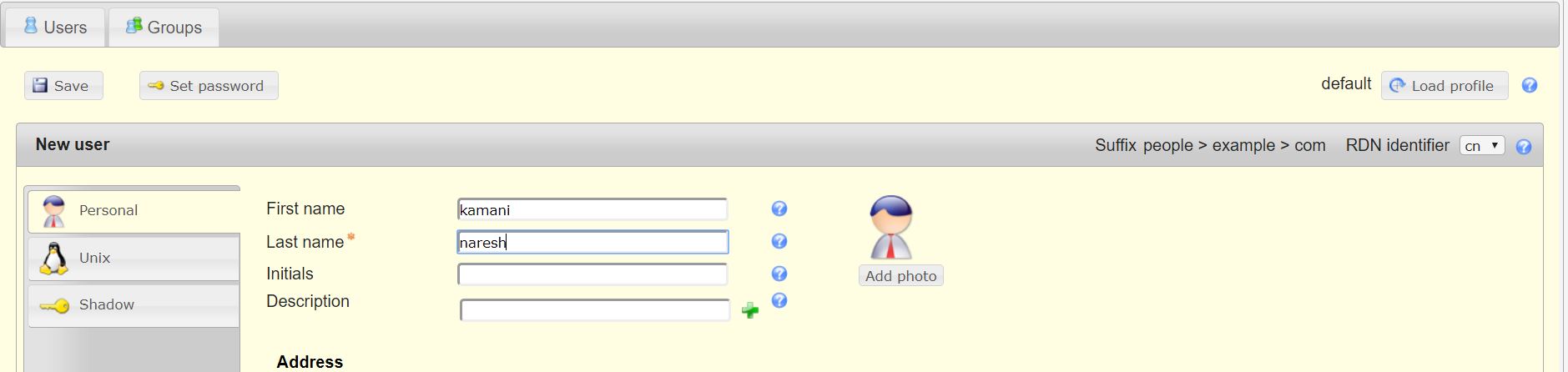
Do the same to add other groups.

Add User Accounts:

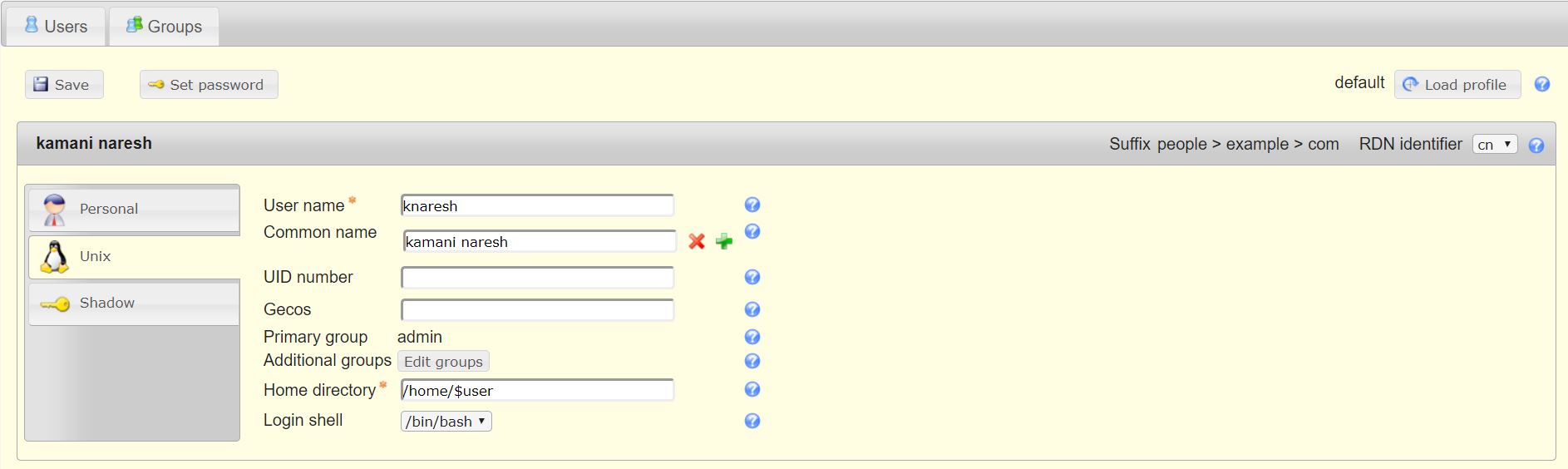
Once you have the groups for user accounts to be added, click on Users > New user to add a new user account to your LDAP server. You have three sections for user management:



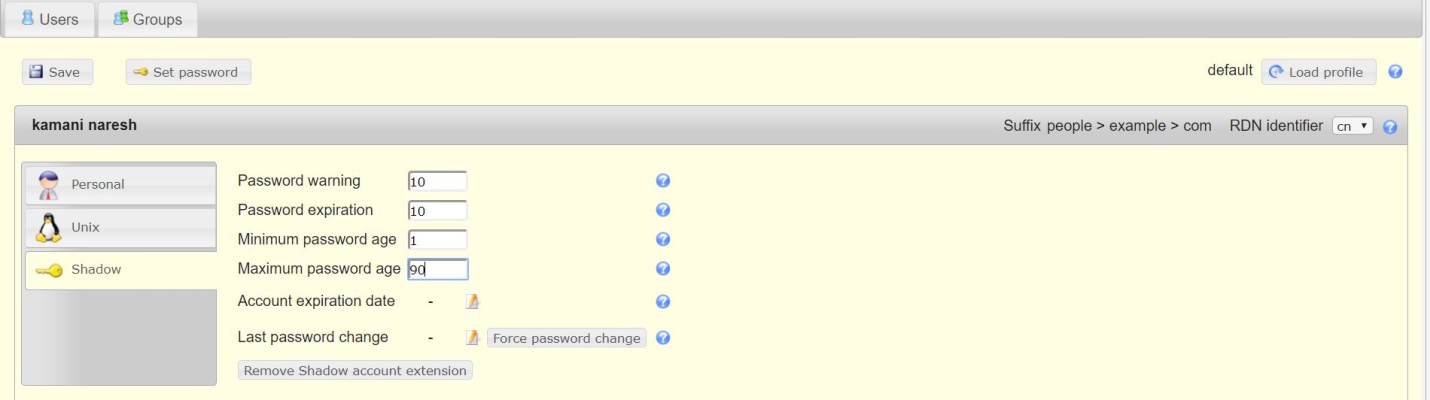
Personal – This contains user’s personal information like the first name, last name, email, phone, department, address e.t.c



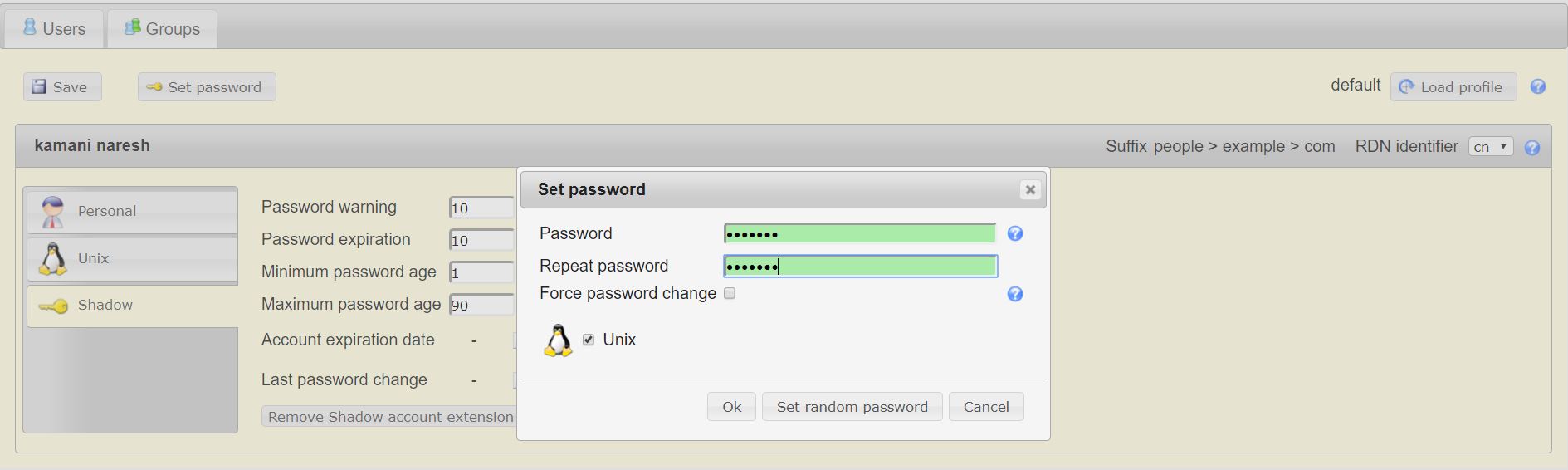
Unix: This section is where you set the Username, Common name, UID number(optional), User comment, User Primary group, and Secondary groups, Home directory and the default Login shell.



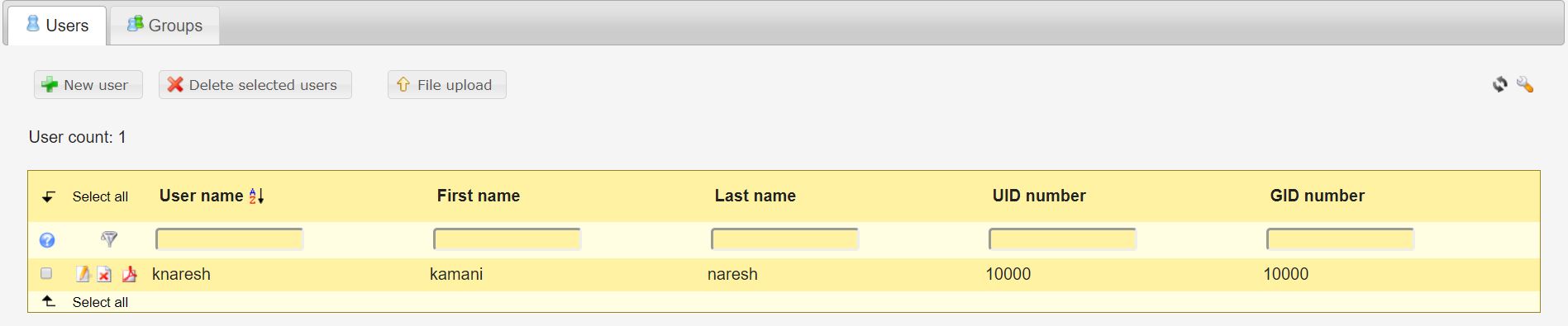
Shadow: This section is where you add Shadow account extension, things related to password aging/expiry.



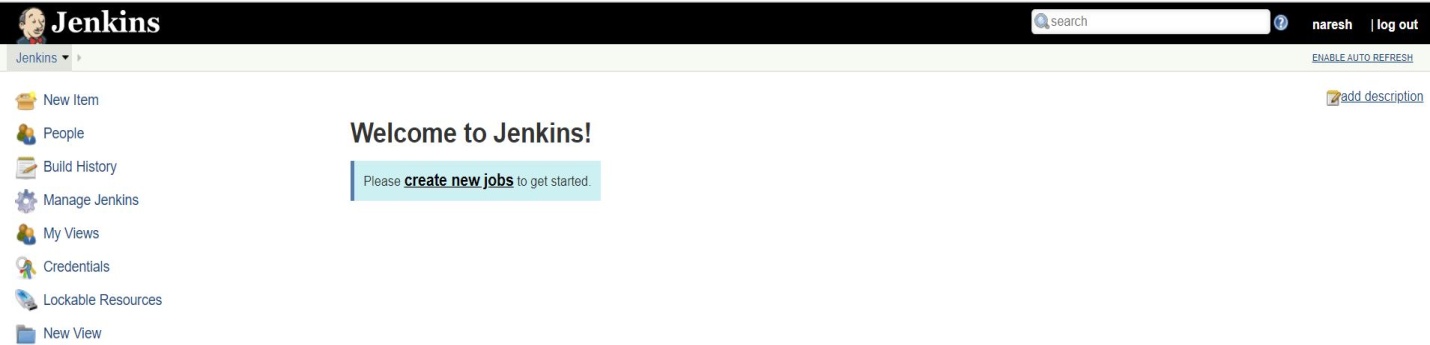
Click on Set password to give password for a user



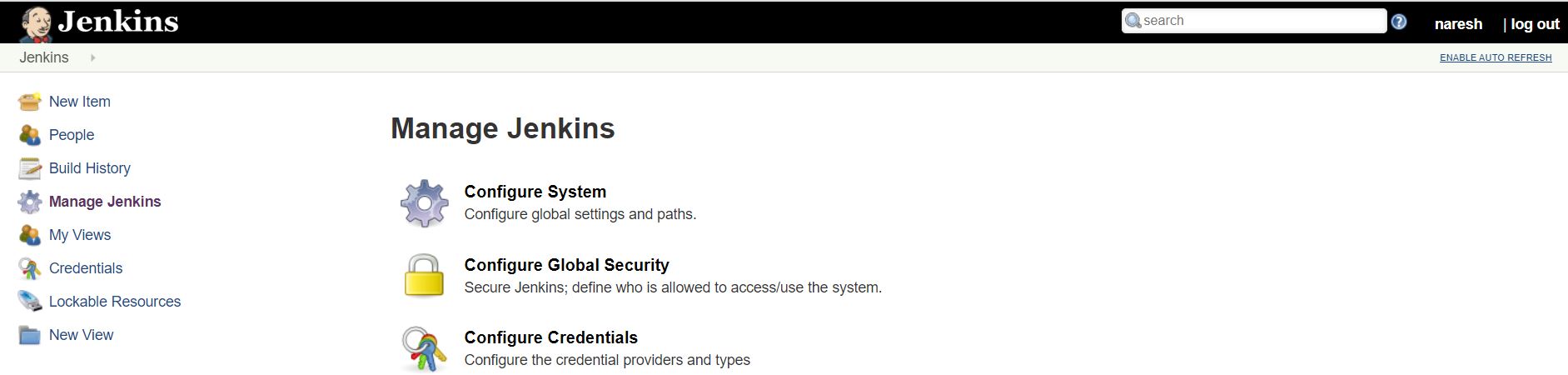
Click on save and check created user.



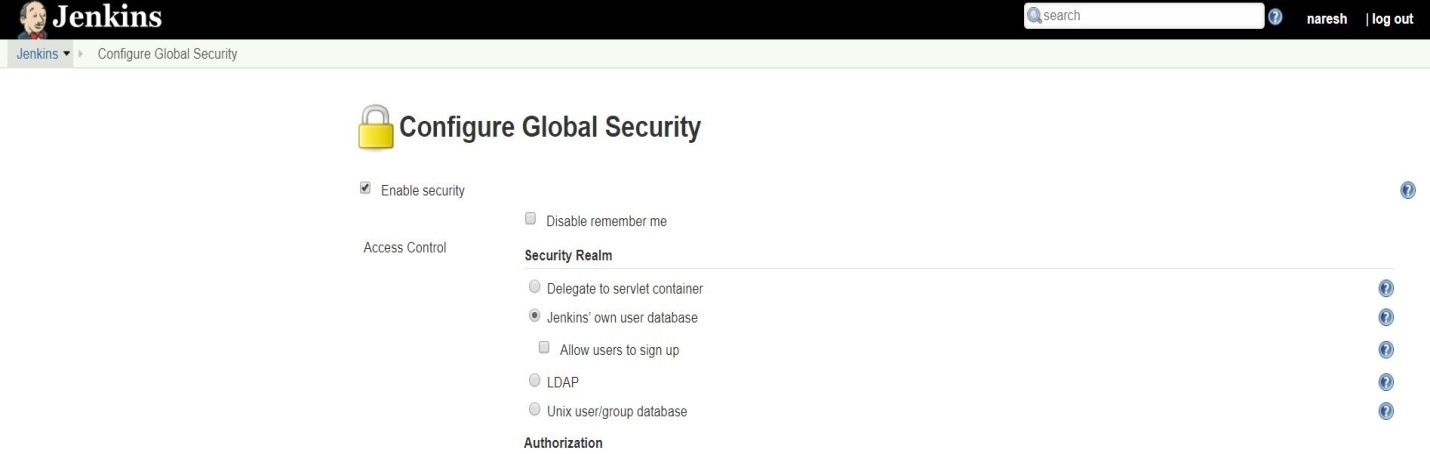
**Open Jenkins on another server:**



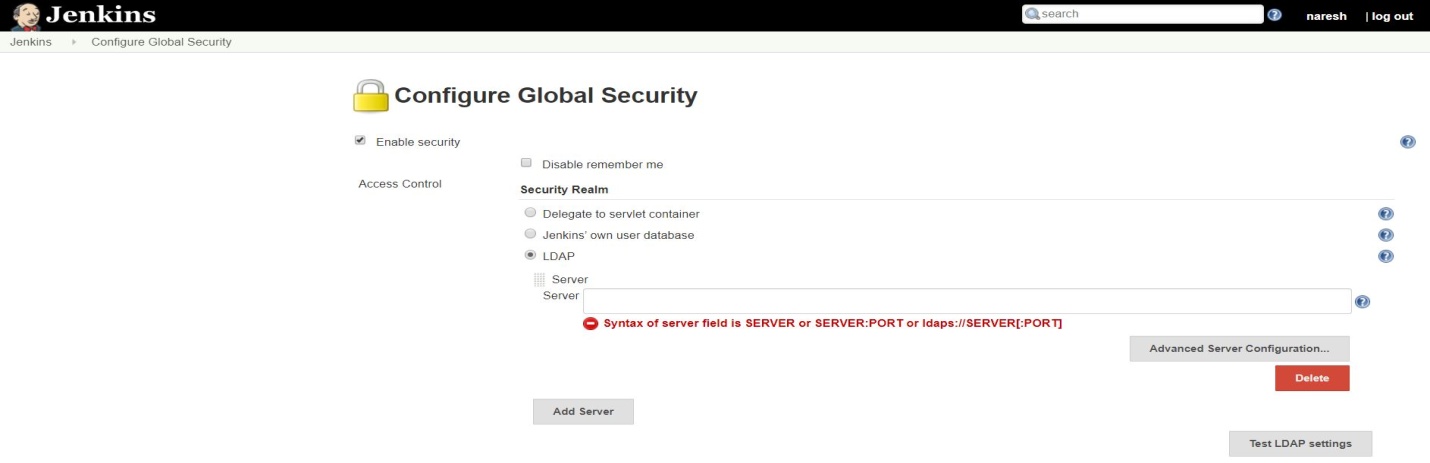
Click on Manage Jenkins



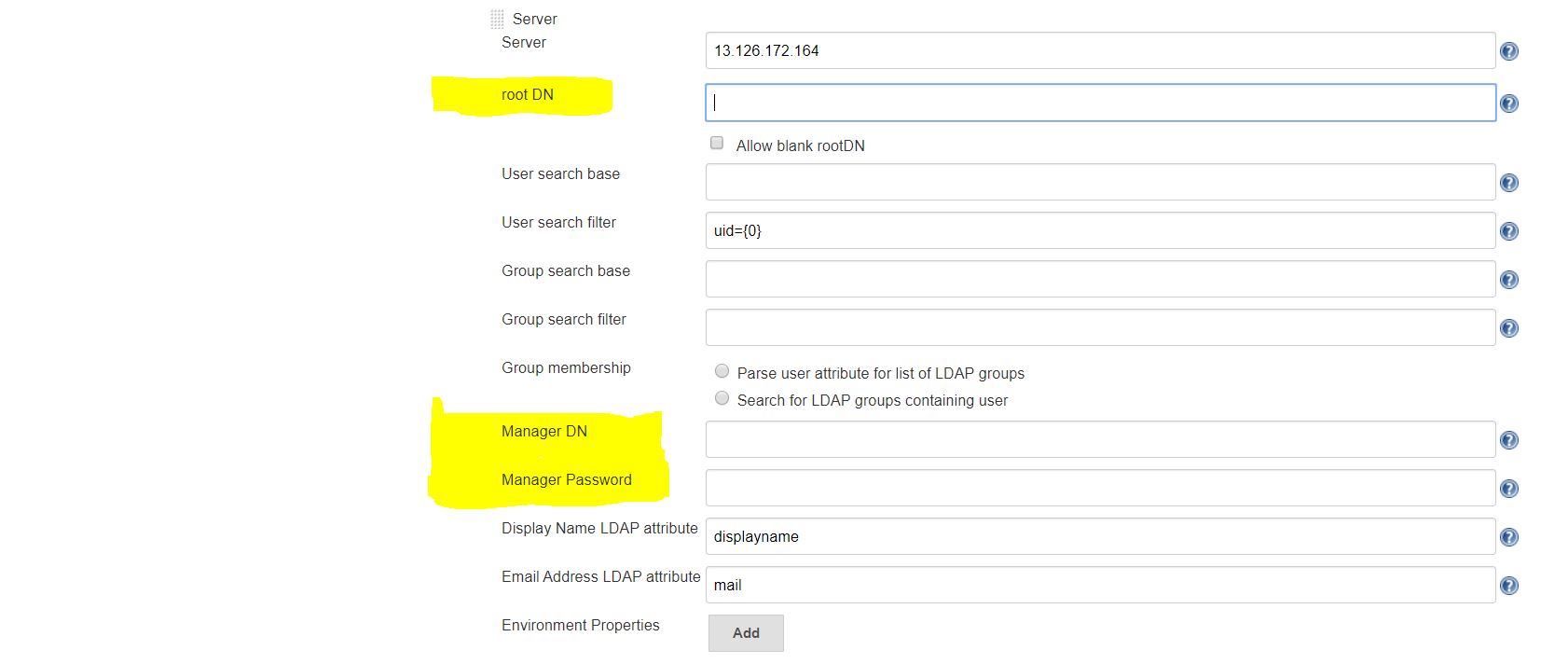
Click on Configure Global Security



Select LDAP with in Configure Global Security



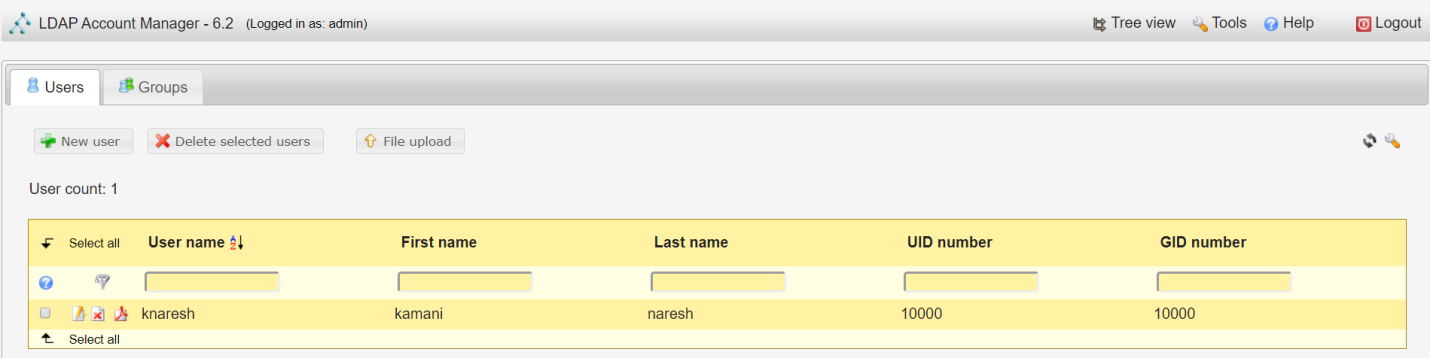
Click on Advanced Server Configuration



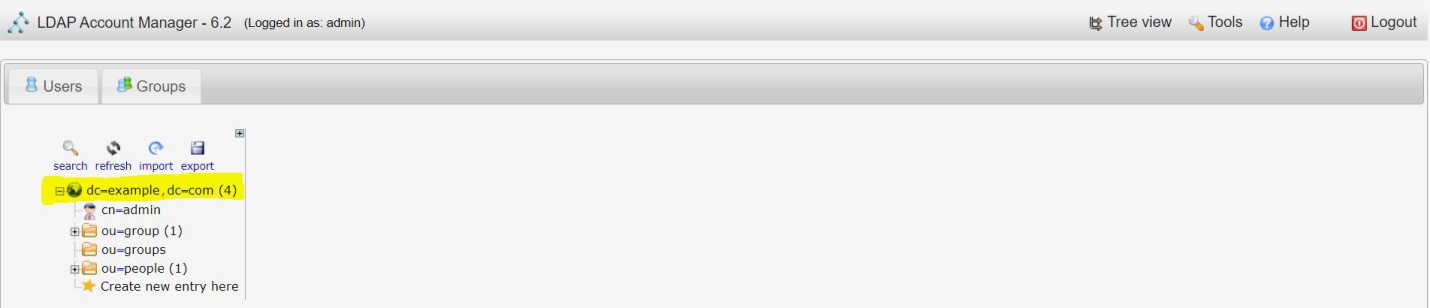
We need to change root DN and Manager DN:

Give server as IP address of Where we installed our LDAP

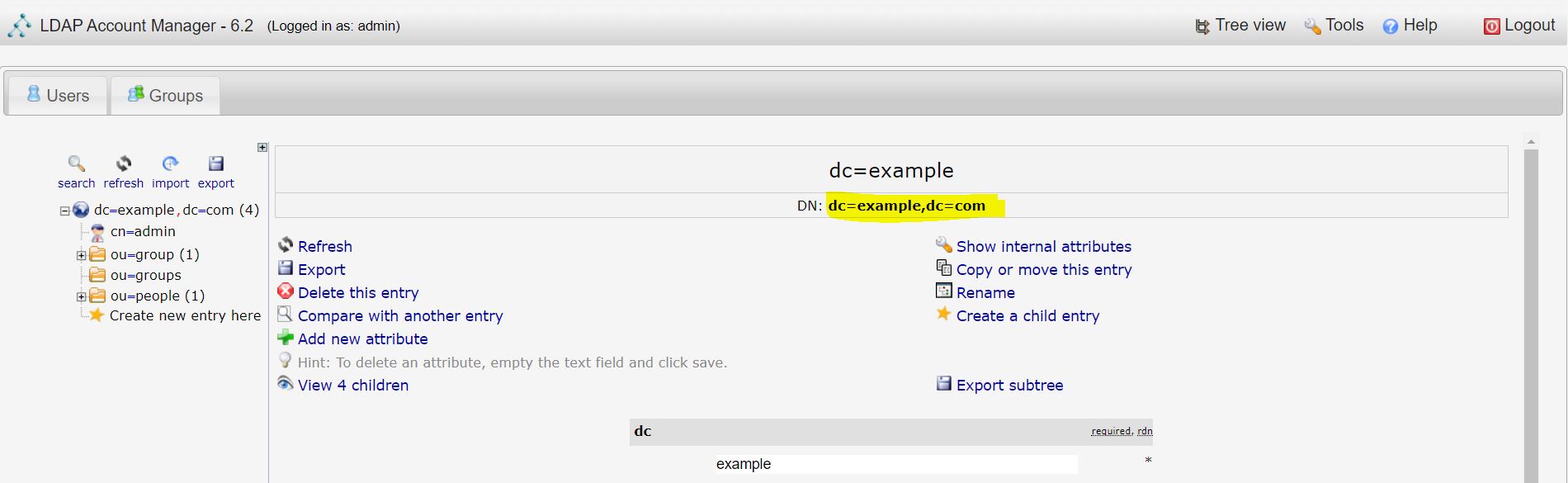
For **root DN** go to LDAP at UI:



Click on Tree view:



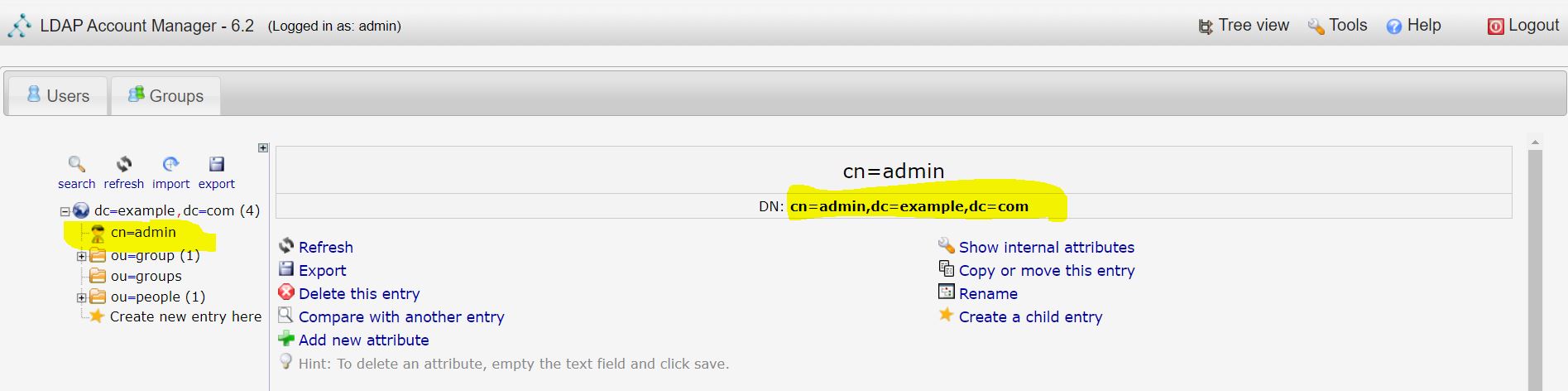
Click on dc=example, dc=com



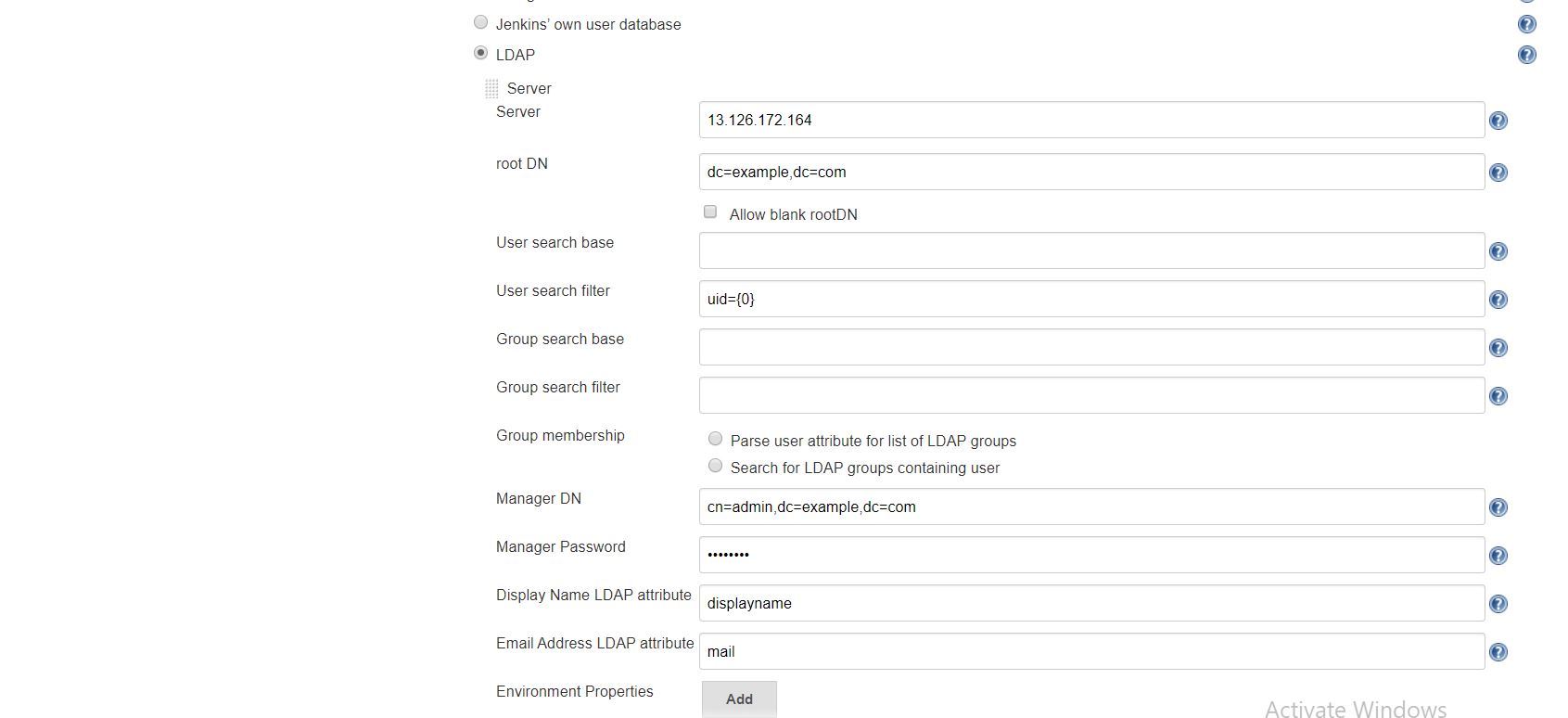
Copy that DN: **dc=example,dc=com**

For **manager DN**:

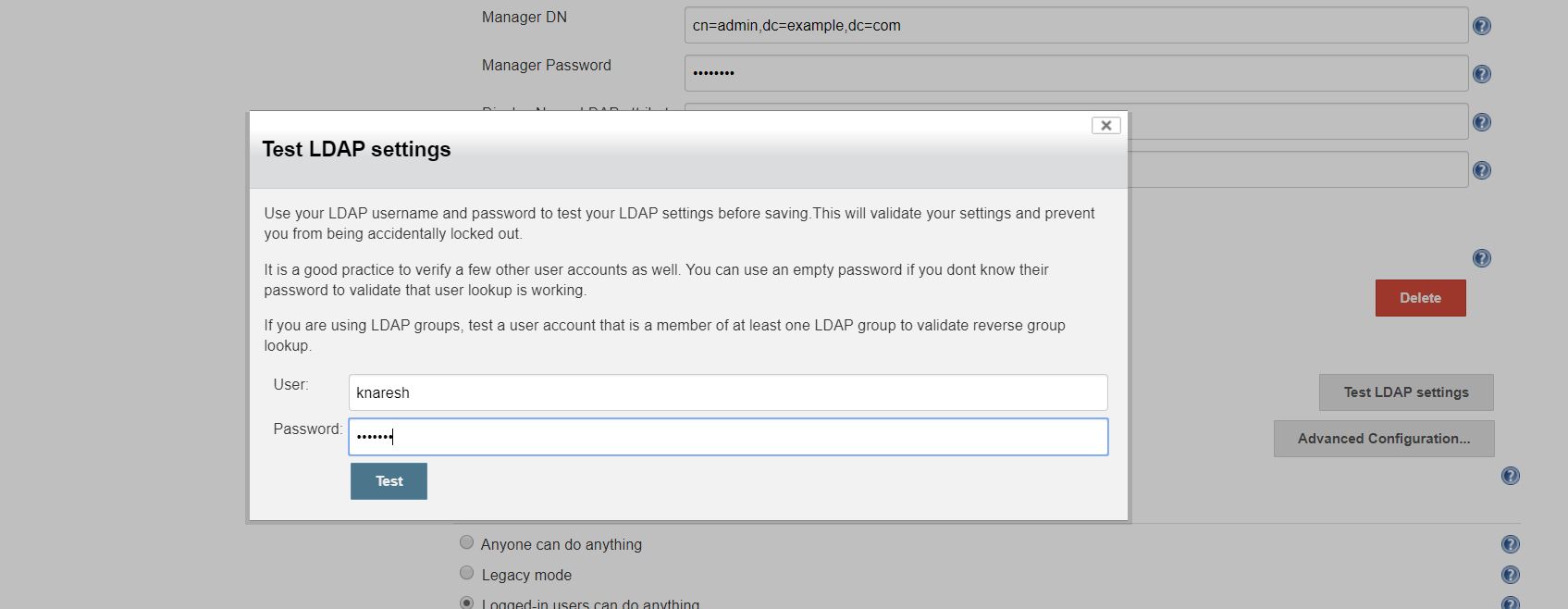
Click on cn=admin and copy DN: **cn=admin,dc=example,dc=com**



See how to fill details in Jenkins:



Click on Test LDAP Settings

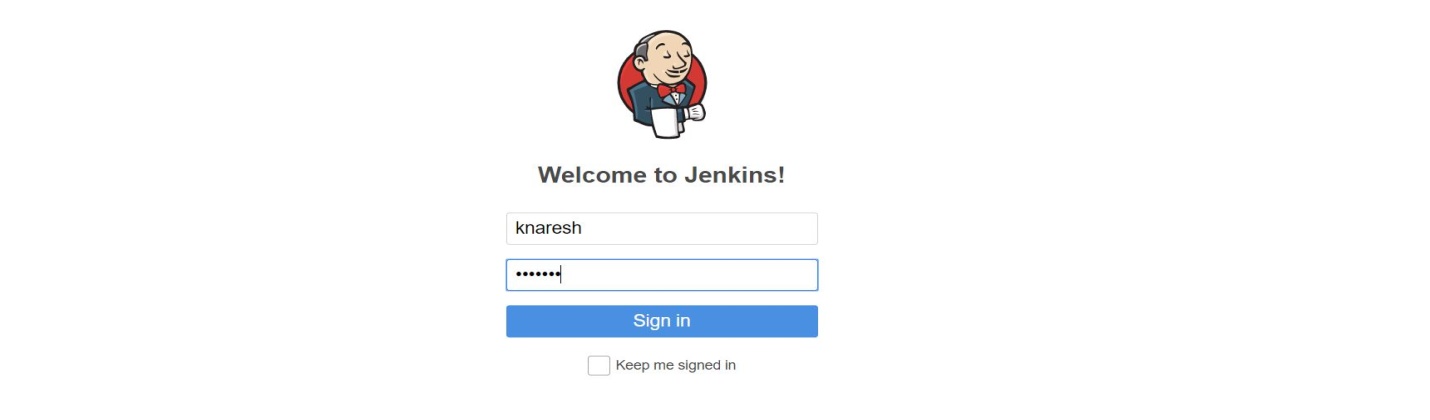


It will show output as:



Now Click on Apply and Save button

Logout out Jenkins terminal and login with new user which we created with LDAP



Check Which user logged In with Jenkins

