DigitalOcean

MENU

How To Install and Configure a Basic LDAP Server on an Ubuntu 12.04 VPS

TAGGED IN: UBUNTU, APACHE, PHP, SECURITY, NETWORKING, SYSTEM TOOLS

SHARE

AUTHOR: JUSTIN ELLINGWOOD • PUBLISHED: OCT 1, 2013 • UPDATED: JUN 17, 2014

Introduction

LDAP, or Lightweight Directory Access Protocol, is a protocol for managing related information from a centralized location through the use of a file and directory hierarchy.

It functions in a similar way to a relational database in certain ways, and can be used to organize and store any kind of information. LDAP is commonly used for centralized authentication.

In this guide, we will cover how to install and configure an OpenLDAP server on an Ubuntu 12.04 VPS. We will populate it with some users and groups. In a later tutorial, authentication using LDAP will be covered.

Install LDAP

The OpenLDAP server is in Ubuntu's default repositories under the package "slapd", so we can install it easily with apt-get. We will also install some additional utilities:

```
sudo apt-get update
sudo apt-get install slapd ldap-utils
```

You will be asked to enter and confirm an administrator password for the administrator LDAP account.

Reconfigure slapd

When the installation is complete, we actually need to reconfigure the LDAP package. Type the following to bring up the package configuration tool:

```
sudo dpkg-reconfigure slapd
```

You will be asked a series of questions about how you'd like to configure the software.

- Omit OpenLDAP server configuration? **No**

- DNS domain name?

  - This will create the base structure of your directory path. Read the message to understand how it works.
  - There are no set rules for how to configure this. If you have an actual domain name on this server, you can use that. Otherwise, use whatever you'd like.
  - In this article, we will call it **test.com**

- Organization name?

  - Again, this is up to you
  - We will use **example** in this guide.

- Administrator password?

  - Use the password you configured during installation, or choose another one

- Database backend to use? **HDB**
- Remove the database when slapd is purged? **No**
- Move old database? **Yes**
- Allow LDAPv2 protocol? **No**

Install PHPldapadmin

We will be administering LDAP through a web interface called PHPldapadmin. This is also available in Ubuntu's default repositories.

Install it with this command:

```
sudo apt-get install phpldapadmin
```

That will install all of the required web server and PHP dependencies.

Configure PHPldapadmin

We need to configure some values within the web interface configuration files before trying it out.

Open the configuration file with root privileges:

```
sudo nano /etc/phpldapadmin/config.php
```

Search for the following sections and modify them accordingly.

Change the red value to the way you will be referencing your server, either through domain name or IP address.

```
$servers->setValue('server','host','domain_nam_or_IP_address');
```

For the next part, you will neec to reflect the same value you gave when asked for the DNS domain name when we reconfigured "slapd".

You will have to convert it into a format that LDAP understands by separating each domain component. Domain components are anything that is separated by a dot.

These components are then given as values to the "dc" attribute.

For instance, if your DNS domain name entry was "imaginary.lalala.com", LDAP would need to see "dc=imaginary,dc=lalala,dc=com". Edit the following entry to reflect the name you selected (ours is "test.com" as you recall):

```
$servers->setValue('server','base',array('dc=test,dc=com'));
```

The next value to modify will use the same domain components that you just set up in the last entry. Add these after the "cn=admin" in the entry below:

```
$servers->setValue('login','bind_id','cn=admin,dc=test,dc=com');
```

Search for the following section about the "hide*template*warning" attribute. We want to uncomment this line and set the value to "true" to avoid some annoying warnings that are unimportant.

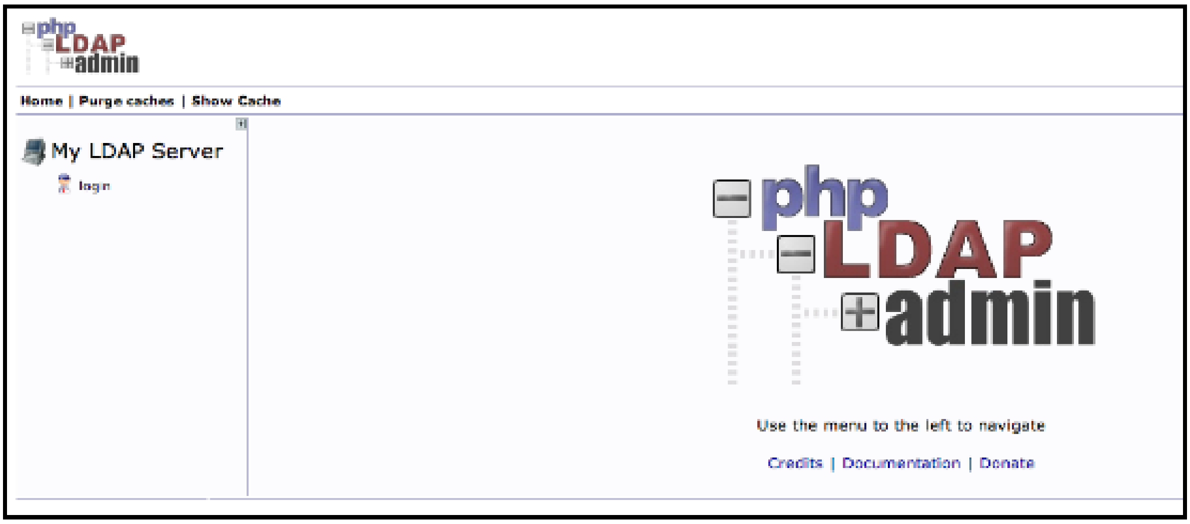
```
$config->custom->appearance['hide_template_warning'] = true;
```

Save and close the file.

Log Into the Web Interface

You can access by going to your domain name or IP address followed by "/phpldapadmin" in your web browser:

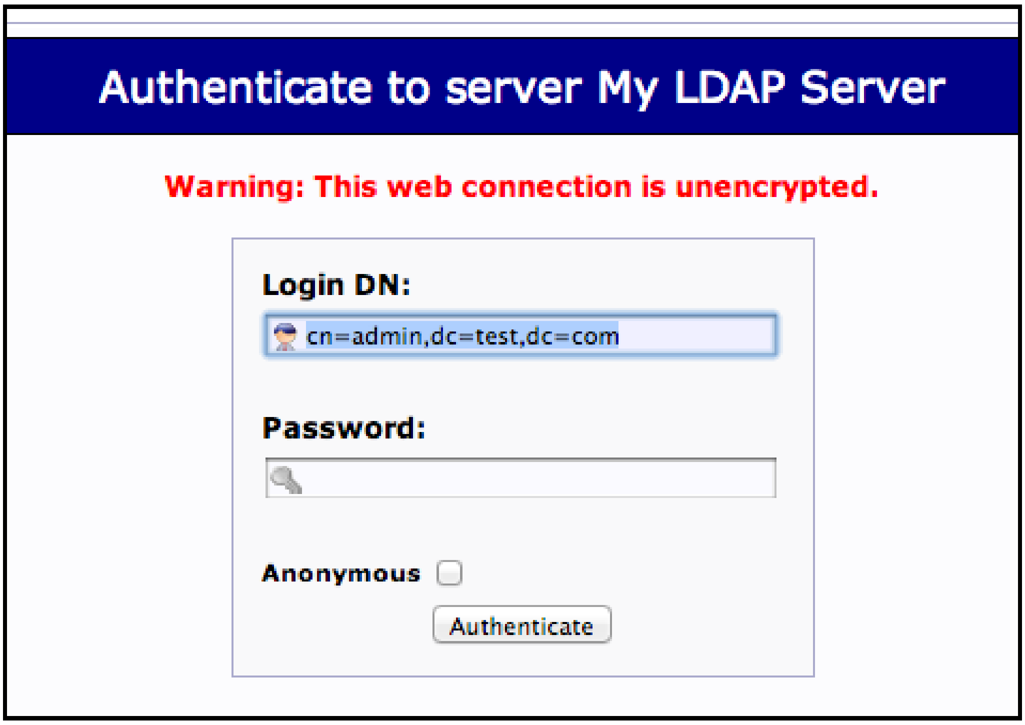
```
domain_name_or_IP_address/phpldapadmin
```


phpLDAPadmin
Home | Purge caches | Show Cache
My LDAP Server
login
Credits | Documentation | Donate

Use the menu to the left to navigate

Click on the "login" link on the left-hand side.

You will receive a login prompt. The correct Login DN (distinguished name) should be pre-populated if you configured PHPldapadmin correctly. In our case, this would be "cn=admin,dc=test,dc=com".



Authenticate to server My LDAP Server

Warning: This web connection is unencrypted.

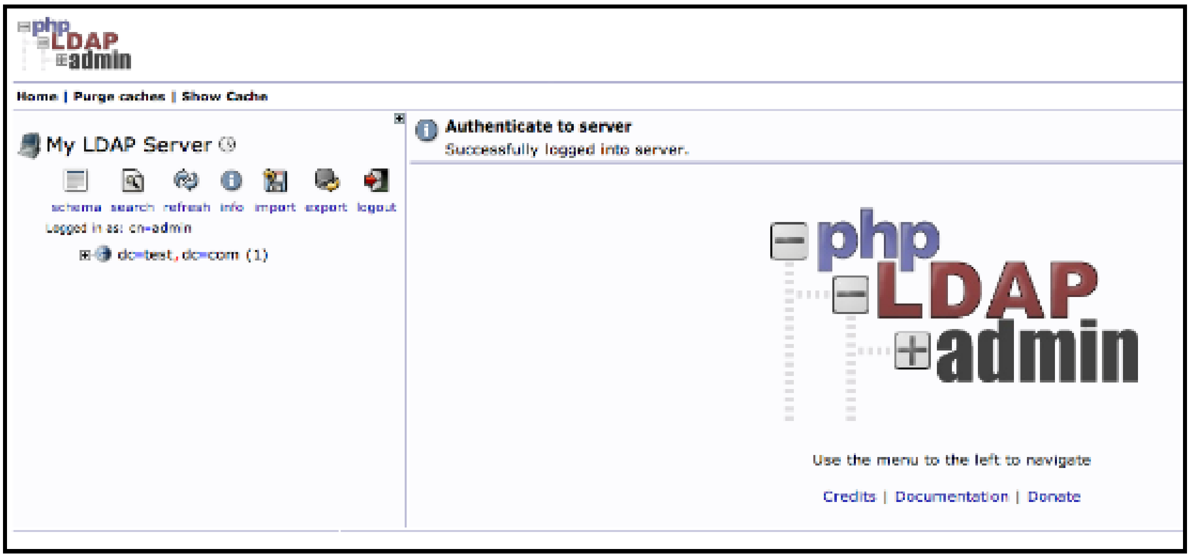
Login DN: cn=admin,dc=test,dc=com

Password:

Anonymous □

Enter the password you selected during our slapd configuration.

You will be presented with a rather sparse interface initially.



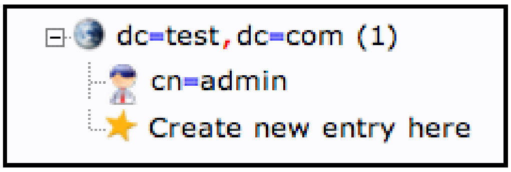
Logged in as: cn=admin

Authenticate to server

Successfully logged into server.

Use the menu to the left to navigate

If you click on the "plus" next to the domain components (dc=test,dc=com), you will see the admin login we are using.



Add Organizational Units, Groups, and Users

LDAP is very flexible. You can create hierarchies and relationships in many different ways, depending on what kind of information you need accessible and what kind of use case you have.

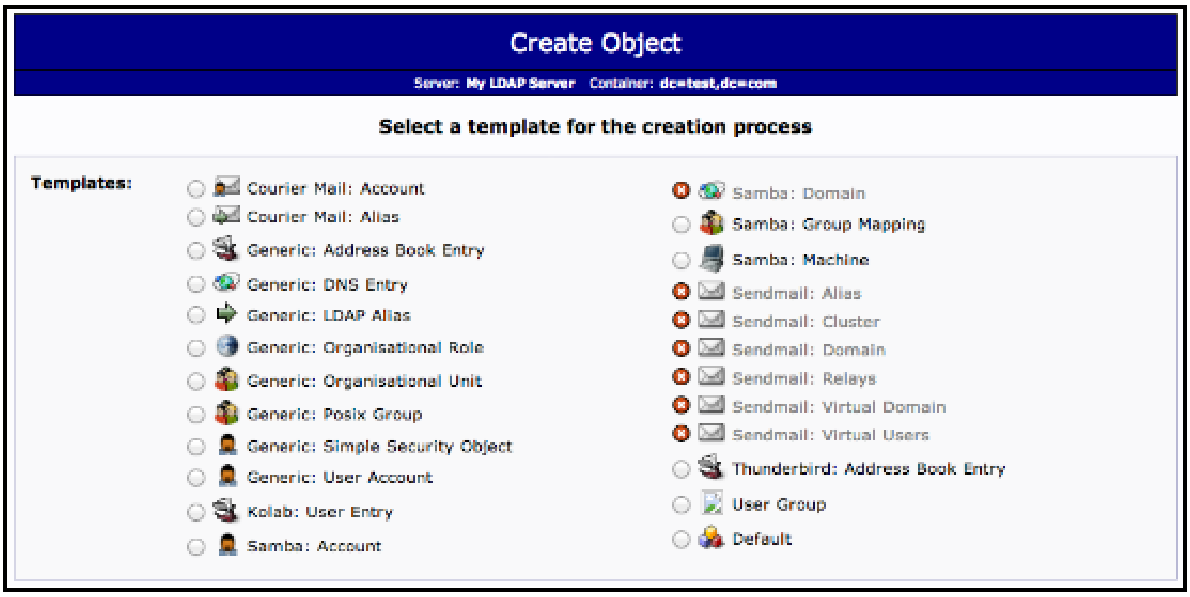
We will create some basic structure to our information and then populate it with information.

Create Organizational Units

First, we will create some categories of information where we will place the later information. Because this is a basic setup, we will only need two categories: groups and users.

Click on the "Create new entry here" link on the left-hand side.

Here, we can see the different kinds of entries we can create.



Create Object

Server: My LDAP Server Container: dc=test,dc=com

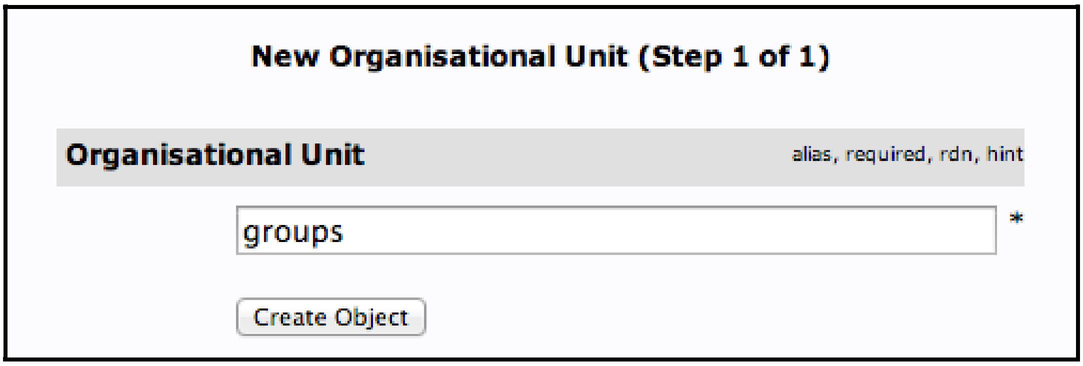
Select a template for the creation process

Templates:

- ○ Courier Mail: Account
- ○ Courier Mail: Alias
- ○ Generic: Address Book Entry
- ○ Generic: DNS Entry
- ○ Generic: LDAP Alias
- ○ Generic: Organisational Role
- ○ Generic: Organisational Unit
- ○ Generic: Posix Group
- ○ Generic: Simple Security Object
- ○ Generic: User Account
- ○ Kolab: User Entry
- ○ Samba: Account
- ☒ Samba: Domain
- ○ Samba: Group Mapping
- ○ Samba: Machine
- ☒ Sendmail: Alias
- ☒ Sendmail: Cluster
- ☒ Sendmail: Domain
- ☒ Sendmail: Relays
- ☒ Sendmail: Virtual Domain
- ☒ Sendmail: Virtual Users
- ○ Thunderbird: Address Book Entry
- ○ User Group
- ○ Default

Because we are only using this as an organizational structure, rather than an information-heavy entry, we will use the "Generic: Organizational Unit" template.

We will be asked to create a name for our organizational unit. Type "groups":

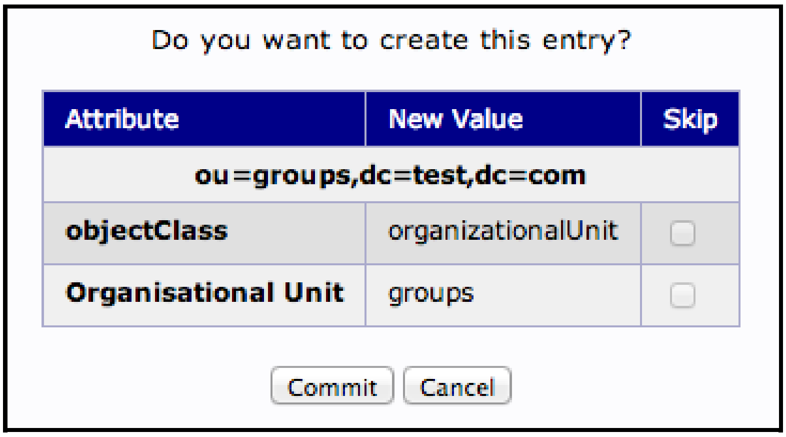


New Organisational Unit (Step 1 of 1)

Organisational Unit — alias, required, rdn, hint

groups *

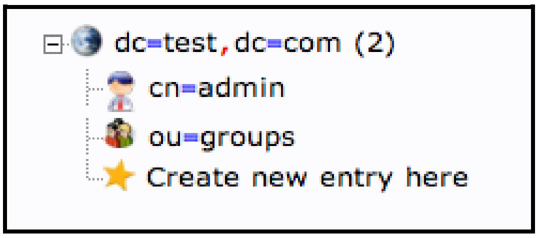
We will then need to commit the changes.



Do you want to create this entry?

Attribute	New Value	Skip
ou=groups,dc=test,dc=com		
objectClass	organizationalUnit	□
Organisational Unit	groups	□

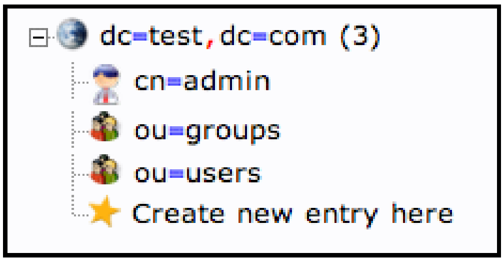
When this is complete, we can see a new entry on the left-hand side.



dc=test,dc=com (2)
cn=admin
ou=groups
Create new entry here

We will create one more organizational structure to get ourselves going. Repeat the procedure, but this time, use the name "users".

When you are done, you should have something that looks like this:



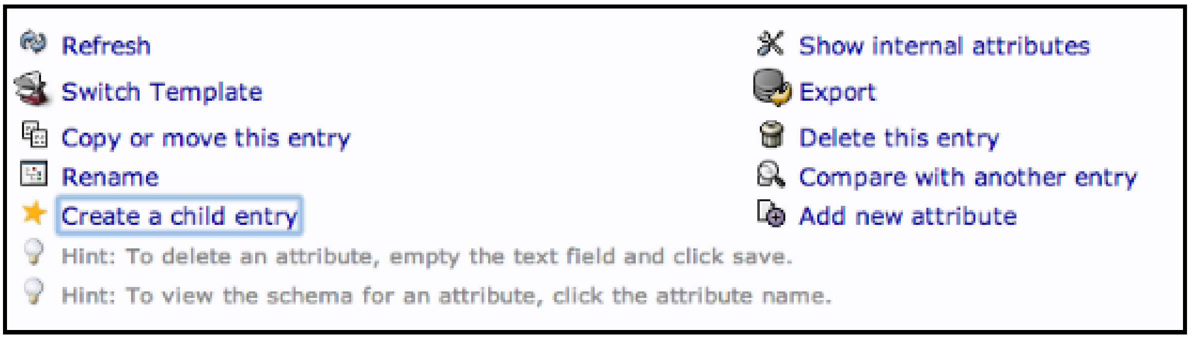
dc=test,dc=com (3)
cn=admin
ou=groups
ou=users
Create new entry here

Create Groups

We will be creating three different groups that could be used to organize users into different "access" groups based on the privileges they require.

We will create an "admin" group, an "irc" group, and a "user" group. We could then allow members of different groups to authenticate if we set up client LDAP authentication.

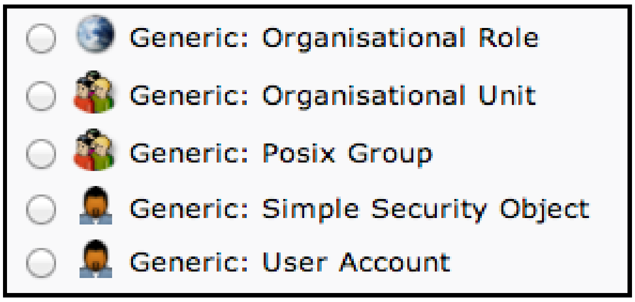
We want to create the groups within the "groups" organizational unit. Click on the "groups" category we created. In the main pane, click on the "Create a child entry" within the groups category.



Hint: To delete an attribute, empty the text field and click save.

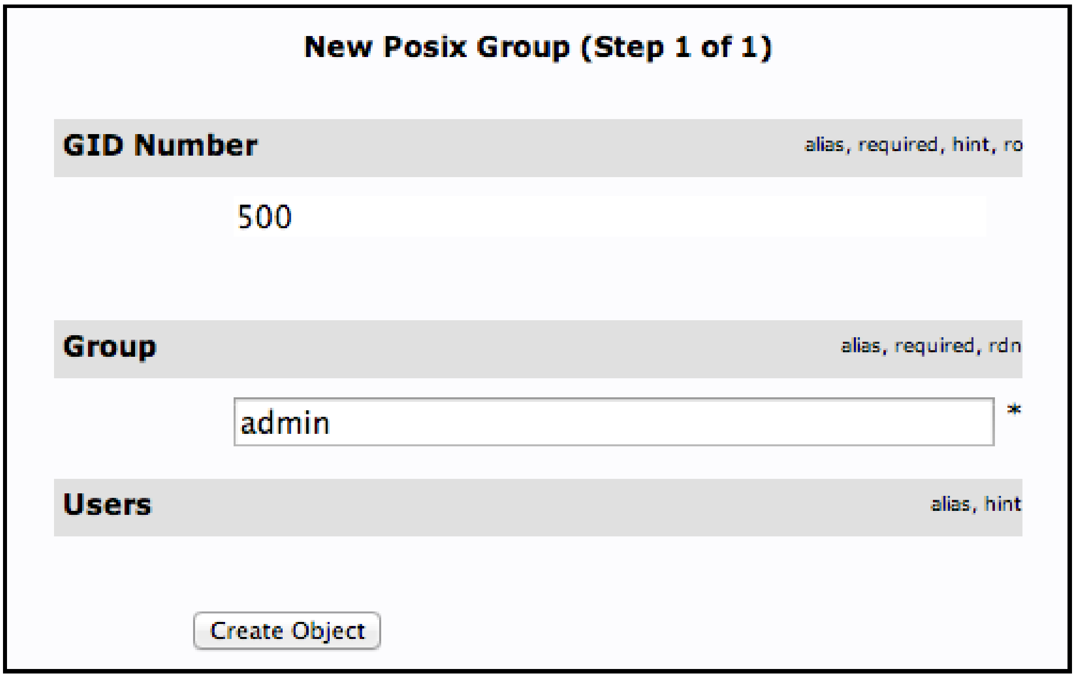
Hint: To view the schema for an attribute, click the attribute name.

This time, we will choose the "Generic: Posix Group" category.



- ○ Generic: Organisational Role
- ○ Generic: Organisational Unit
- ○ Generic: Posix Group
- ○ Generic: Simple Security Object
- ○ Generic: User Account

Fill in "admin" as the group name. Click "Create Object" and then confirm on the next page.



New Posix Group (Step 1 of 1)

GID Number alias, required, hint, ro

500

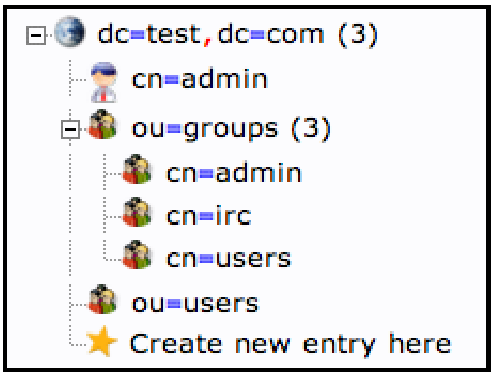
Group alias, required, rdn

admin *

Users alias, hint

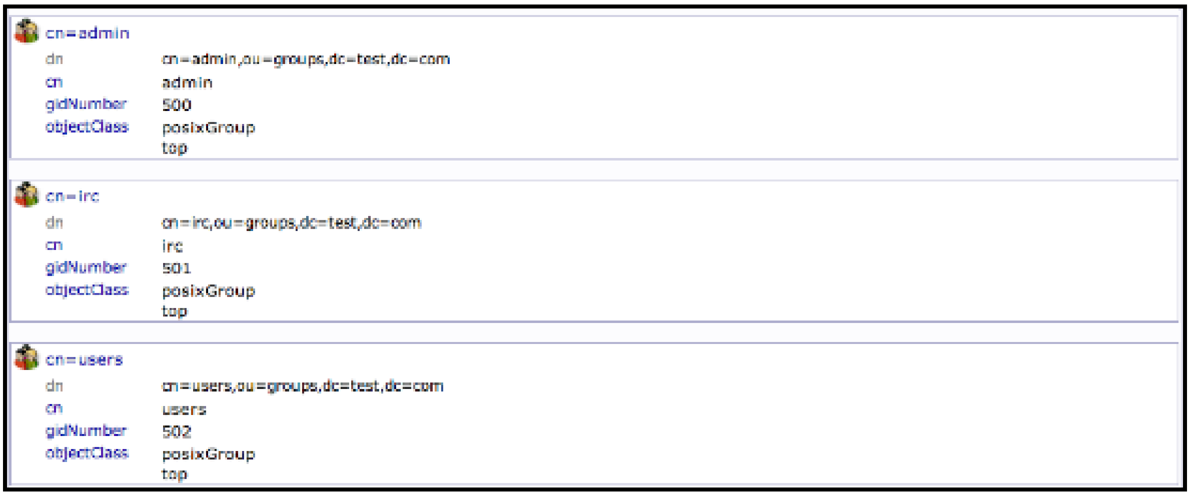
Repeat the process, but simply replace the "admin" name with "irc" and "user". Be sure to re-click the "ou=groups" entry before creating child entries, or else you may create entries under the wrong category.

You should now have three groups in the left-hand panel:



dc=test,dc=com (3)
- cn=admin
- ou=groups (3)
  - cn=admin
  - cn=irc
  - cn=users
- ou=users
- Create new entry here

You can see an overview of the entries in the "ou=groups" category by clicking on that entry, and then clicking on "View 3 children":

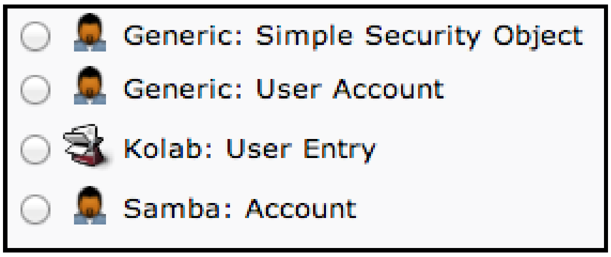


```
cn=admin
dn           cn=admin,ou=groups,dc=test,dc=com
cn           admin
gidNumber    500
objectClass  posixGroup
             top

cn=irc
dn           cn=irc,ou=groups,dc=test,dc=com
cn           irc
gidNumber    501
objectClass  posixGroup
             top

cn=users
dn           cn=users,ou=groups,dc=test,dc=com
cn           users
gidNumber    502
objectClass  posixGroup
             top
```

Create Users

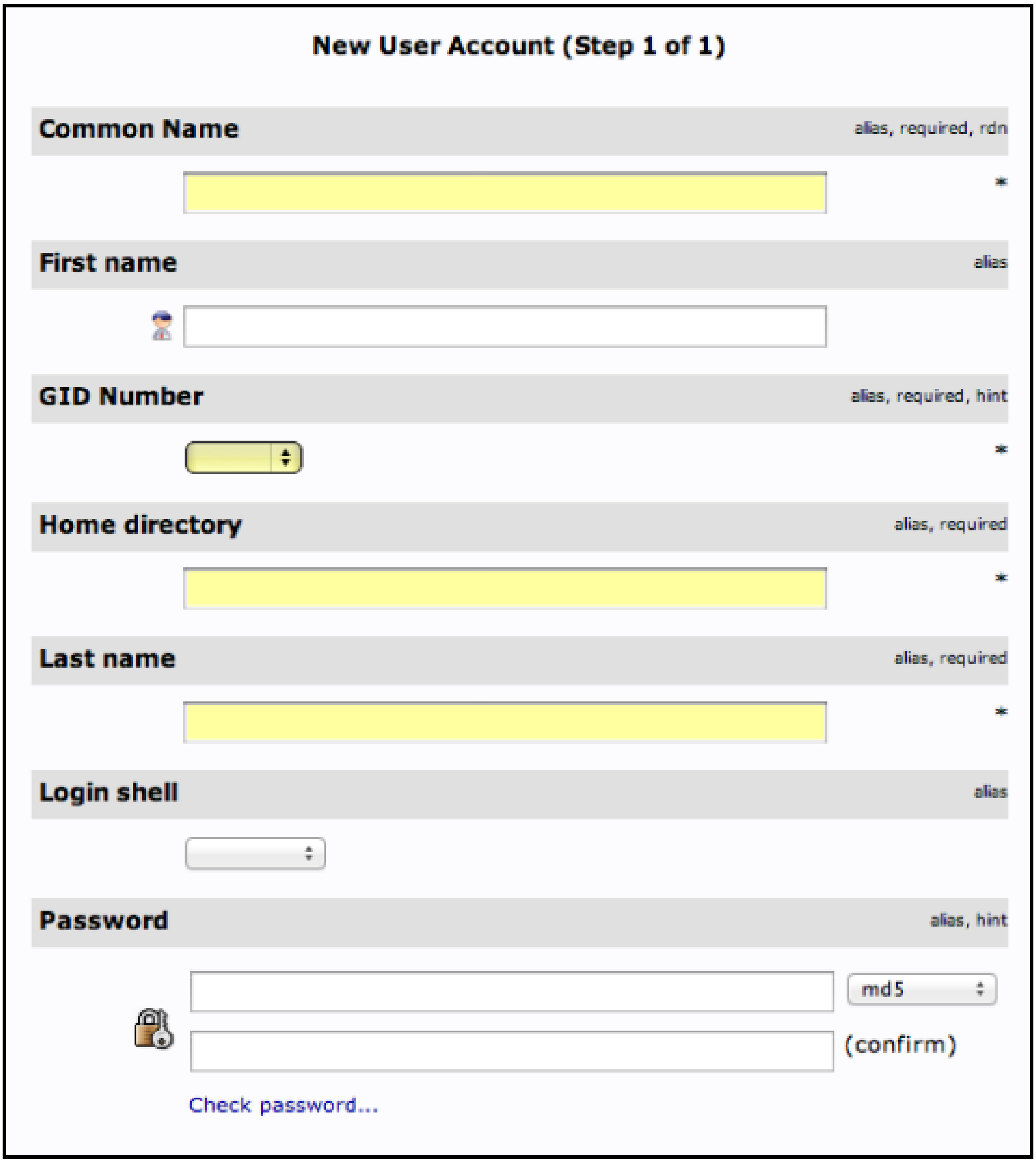
Next, we will create users to put in these groups. Start by clicking the "ou=users" category. Click on "Create a child entry".

We will choose "Generic: User Account" for these entries.



○ Generic: Simple Security Object
○ Generic: User Account
○ Kolab: User Entry
○ Samba: Account

We will be given a lot of fields to fill out:



New User Account (Step 1 of 1)

Common Name alias, required, rdn

*

First name alias

GID Number alias, required, hint

*

Home directory alias, required

*

Last name alias, required

*

Login shell alias

Password alias, hint

md5

(confirm)

Check password...

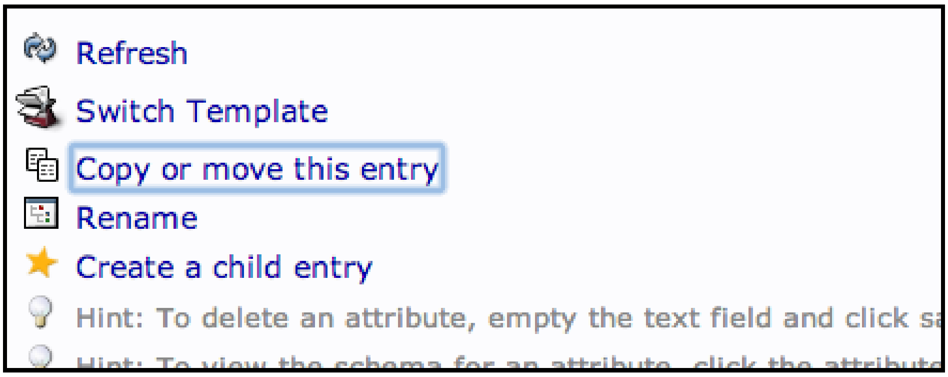
Fill in all of the entries with information that makes sense for your user.

Something to keep in mind is that the "Common Name" needs to be unique for each entry in a category. So you may want to use a username format instead of the default "FirstName LastName" that is auto-populated.

Click "Create Object" at the bottom and confirm on the following page.

To create additional users, we will take advantage of the ability to copy entries.

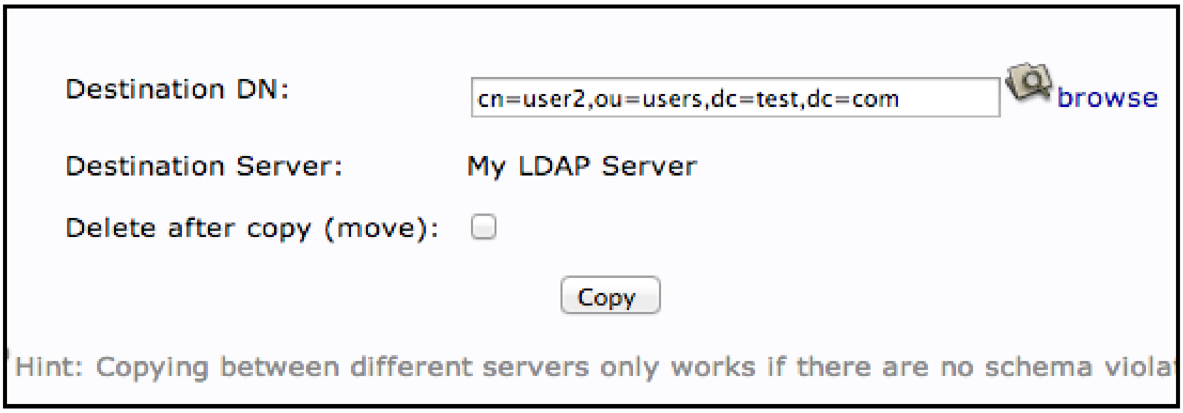
Click on the user you just created in the left-hand panel. In the main pane, click "Copy or move this entry":



Hint: To delete an attribute, empty the text field and click sa

Hint: To view the schema for an attribute, click the attribute

Adjust the "cn=user" portion of the entry to point it to the common name you'd like to use for the new entry. Click "Copy" at the bottom:



Destination DN: cn=user2,ou=users,dc=test,dc=com

Destination Server: My LDAP Server

Delete after copy (move): □

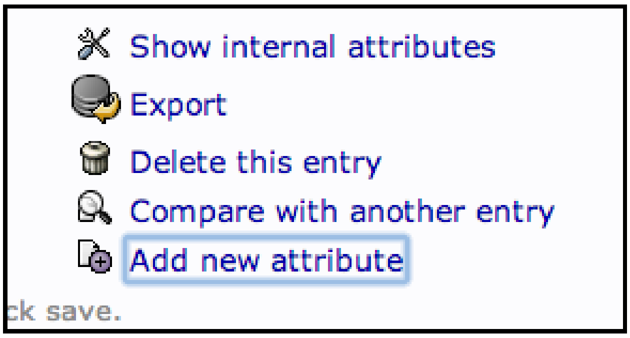
Hint: Copying between different servers only works if there are no schema viola

You will be given the next page populated with your first users data. You will need to adjust it to match the new users information.

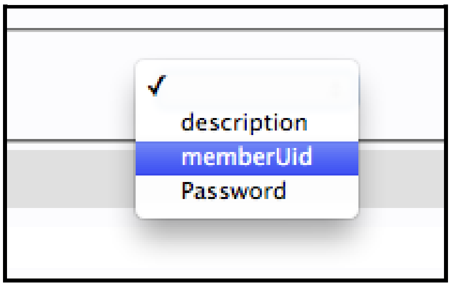
Be sure to adjust the uidNumber. Click the "Create Object" button at the bottom.

Add Users to Groups

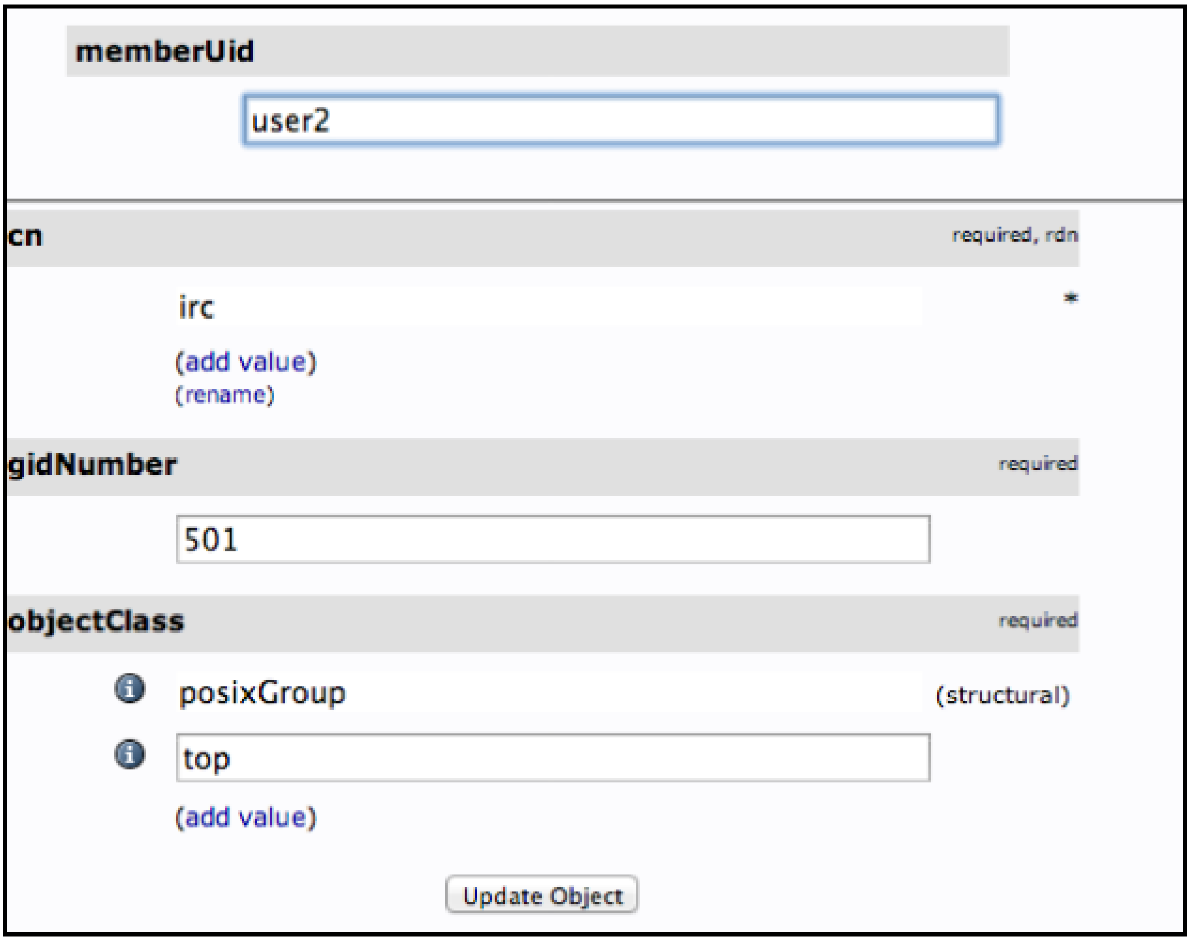
We can add users to various groups by clicking on the group in question. In the main pane, select "Add new attribute":



Select "memberUid" from the drop down menu:



In the text field that populates, enter the first user you'd like to add. Click "Update Object" at the bottom:



memberUid

user2

cn required, rdn

irc *

gidNumber required

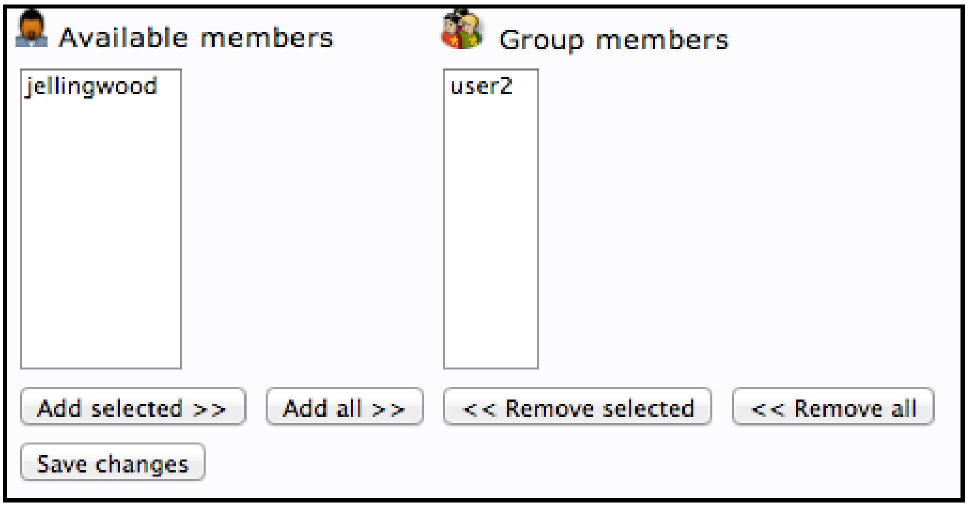
501

objectClass required

posixGroup (structural)

top

You can then add more members by clicking "modify group members" and selecting them from the available choices:



Conclusion

You should now have a basic LDAP server set up with a few users and groups. You can expand this information and add all of the different organizational structures to replicate the structure of your business.

We will cover in another section how to authenticate using the LDAP credentials for various services.

By Justin Ellingwood

Related Tutorials

How To Share PHP Sessions on Multiple Memcached Servers on Ubuntu 14.04

How To Install Linux, Nginx, MySQL, PHP (LEMP) stack On CentOS 7

How To Create an ECC Certificate on Nginx for Debian 7

How To Install Linux, Apache, MySQL, PHP (LAMP) stack On CentOS 7

An Introduction to OAuth 2

21 Comments

andrew *January 2, 2014*

I would suggest changing the link in

We will cover in another section 'how to authenticate using the LDAP credentials' for various services.
which is,
"https://www.digitalocean.com/community/articles/how-to-use-pam-to-configure-authentication-on-an-ubuntu-12-04-vps "
to
"https://www.digitalocean.com/community/articles/how-to-authenticate-client-computers-using-ldap-on-an-ubuntu-12-04-vps"

Justin Ellingwood *January 2, 2014*

andrew: Thanks for the heads up. That was the intended link, and I've updated the article to reflect your suggestion.

Let me know if you see anything else! Thanks!

---

andrew *January 3, 2014*

The link at the top of the article should also be changed

Kamal Nasser *January 5, 2014*

Thanks, andrew! I've updated the article.

---

mssurajkaiga *January 6, 2014*

Hi, I am getting the following error when trying to create a user.

Could not add the object to the LDAP server.
LDAP said: No such object
Error number: 0x20 (LDAP_NO_SUCH_OBJECT)

Description: That object does not exist.

josephrushdoony *January 11, 2014*

I am in the process of migration a Centos5 OpenLDAP server over to Ubuntu 12.04, and I am running in to an issue with the initial configuration. I am trying to replication the structure that was setup by the admin a couple of years back (who is no longer around), but I have been unsuccessful at it. I am hoping that someone could point me in the right direction. The structure of the original install is as follows:

First the login:
Login DN: cn=Manager,o=sun

Structure:
The top structure only has “o=sun”, no “dc=sun, dc=net”. Then: “ou=Groups, o=sun”,“ou=Users, o=sun”, “sambaDomainName=SUNSERVER”, and “Create new entry here”.

I am new to OpenLDAP, I have been using the following how-to, successfully, but I have not been able to achieve the desired results.

http://ideasnet.wordpress.com/2012/10/31/ideas-server-how-to-install-and-set-openldap-in-ubuntu-12-04lts-server-edition-part-1/

Thanks in advance,
Joe

daniellago85 *February 14, 2014*

The best I've seend. Congratulations.

lordnynex *March 1, 2014*

This is a fantastic article. It should be noted though that this article required some additional steps if you're installing on Ubuntu 13.10 as phpLDAPadmin requires a fair bit of patching due to the php5.5 version that 13.10 selects.

http://sourceforge.net/u/nihilisticz/phpldapadmin/ci/7e53dab990748c546b79f0610c3a7a584

and
http://stackoverflow.com/questions/20673186/getting-error-for-setting-password-feild-when-creating-generic-user-account-phpl

will get you through.

---

gilles *March 3, 2014*

Hello,
and thank you for this great article.

When i try to connect to My_IP_address/phpldapadmin the browser suggest me to download the file with this message "Vous avez choisir d'ouvrir "application/x-httpd-php" à partir de http://IP.............

I have this configuration PHP Version => 5.4.4-14+deb7u7

I tried several things but didn't find the right way to solve it....
Can you help me ?
Thanks in advance
Gilles

Kamal Nasser *March 3, 2014*

@gilles: What version of Ubuntu are you using?

---

gilles *March 4, 2014*

Thanks for your reply.
I am using a Debian 7.
Gilles

---

msajjadaslam *March 13, 2014*

how to join windows client in Open Ldap domain, its not working for windows clients.

---

celio.mello *April 22, 2014*

LDAP said: No such object Error number: 0x20 (LDAP_NO_SUCH_OBJECT) Description: That object does not exist.

---

ping2praveenr *May 2, 2014*

Hello,
Thank you for great article.
after successful installation of LDAP and phpldapadmin
while logging using IP_address/phpldapadmin
it says :
Unable to connect to LDAP server My LDAP Server
Error: Can't contact LDAP server (-1) for login
error Failed to Authenticate to server
Invalid Username or Password.

Thanks in advance,

---

ping2praveenr *May 2, 2014*

sorry forgot to mention the os Ubuntu 12.04

Andrew SB *May 2, 2014*

@ping2praveenr: Make sure that the password that you are entering match the ones set when you installed slapd. Also make sure the DNS name that you entered, matches the values you used in /etc/phpldapadmin/config.php

If you want to reset your slapd configuration, run:

```
sudo dpkg-reconfigure slapd
```

luckypur *May 23, 2014*

same problem...

Unable to connect to LDAP server My LDAP Server

Error: Can't contact LDAP server (-1) for user

error Failed to Authenticate to server

Invalid Username or Password.

Kamal Nasser *May 28, 2014*

@luckypur: Make sure the LDAP server's IP address is set properly and that all the necessary ports are open.

martin *June 20, 2014*

same problem... Unable to connect to LDAP server My LDAP Server Error: Can't contact LDAP server (-1) for user error Failed to Authenticate to server Invalid Username or Password.

oyeeinfotech *June 25, 2014*

Good work. is it possible and how to get it setup on windows in specific windows 8.1 thanks

afsin *July 6, 2014*

Thank you! A very good work! It works for Ubuntu 14.04 too!

Note that a very small fix mentioned in http://stackoverflow.com/questions/20673186/getting-error-for-setting-password-feild-when-creating-generic-user-account-phpl needed.

Log In to comment

B I

Leave a comment...

SUBMIT COMMENT >

Proudly Made in NY

Terms, Privacy, & Copyright
Security

COMMUNITY

Dashboard

Overview

Tutorials

Questions

Projects

Tutorial Suggestions

Get Paid to Write

2,152,440 DROPLETS LAUNCHED