

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

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_name_or_IP_address');
```

For the next part, you will need 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 "hidetemplatewarning" attribute. We want to uncomment this line and set the value to "true" to avoid some annoying warnings that are unimportant.

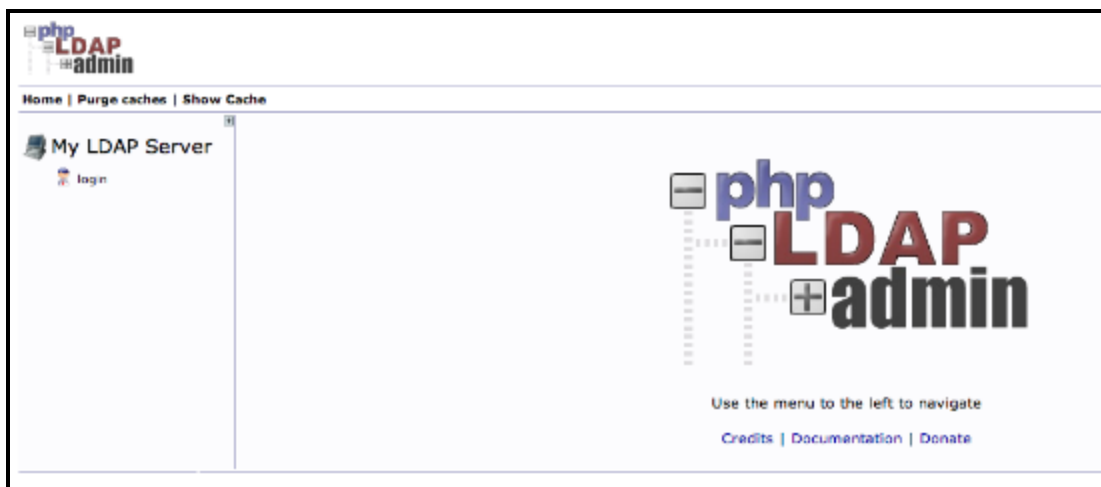
```
$config->custom->appearance['hide_template_warning'] = true;
```

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`



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:



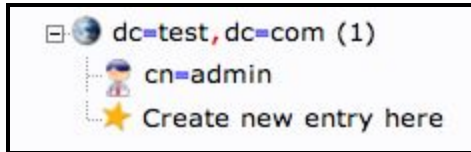
Anonymous ☐

Enter the password you selected during our slapd configuration.

You will be presented with a rather sparse interface initially.



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 *

Create Object

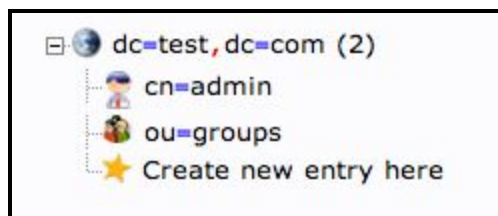
We will then need to commit the changes.

Do you want to create this entry?

Attribute	New Value	Skip
ou=groups,dc=test,dc=com		
objectClass	organizationalUnit	<input type="checkbox"/>
Organisational Unit	groups	<input type="checkbox"/>

Commit Cancel

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



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:

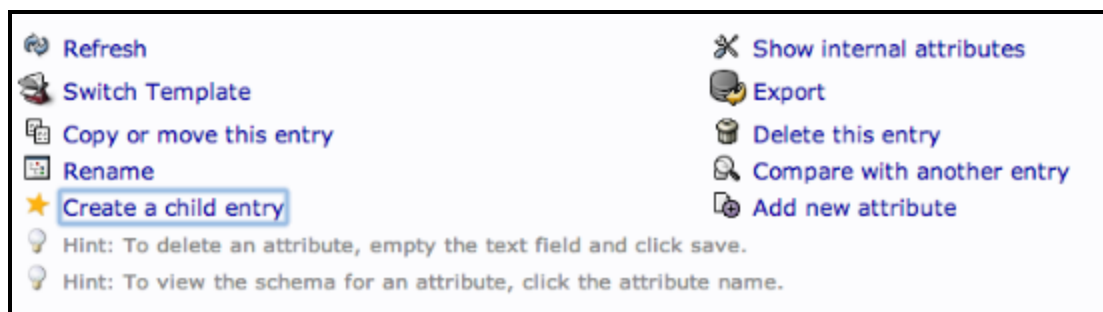


Create Groups

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.



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



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:







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.

<input type="radio"/>		Generic: Simple Security Object
<input type="radio"/>		Generic: User Account
<input type="radio"/>		Kolab: User Entry
<input type="radio"/>		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
<input type="text"/>	*
First name	alias
 <input type="text"/>	
GID Number	alias, required, hint
<input type="text"/>	*
Home directory	alias, required
<input type="text"/>	*
Last name	alias, required
<input type="text"/>	*
Login shell	alias
<input type="text"/>	
Password	alias, hint
 <input type="password"/>	md5 <input type="text"/>
<input type="password"/>	(confirm)
Check password...	

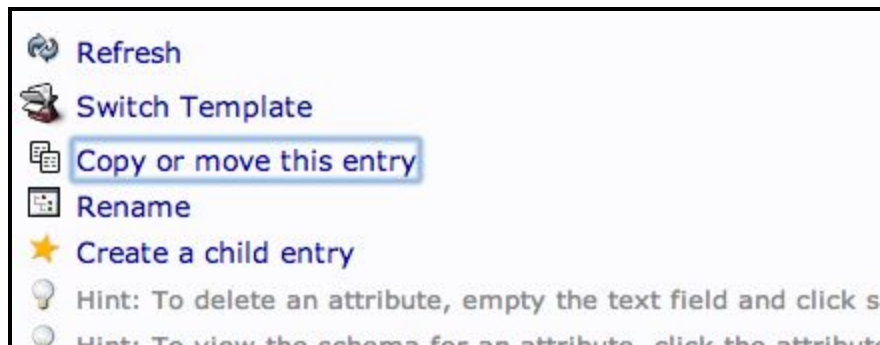
Fill in all of the entries with information that makes sense for your user.

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":



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:

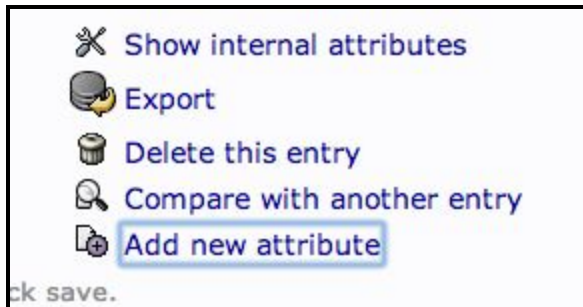
A screenshot of the 'Copy or move this entry' dialog box. It contains the following fields and controls: 'Destination DN:' with a text input field containing 'cn=user2,ou=users,dc=test,dc=com' and a 'browse' button with a magnifying glass icon; 'Destination Server:' with a dropdown menu showing 'My LDAP Server'; 'Delete after copy (move):' with an unchecked checkbox; and a 'Copy' button at the bottom. A hint message at the bottom reads: 'Hint: Copying between different servers only works if there are no schema viola...'. The dialog box has a light blue background and a thin border.

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.

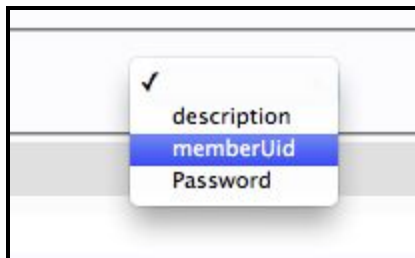
Be sure to adjust the uidNumber. Click the "Create Object" button at the bottom.

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

*

(add value)

(rename)

gidNumber

required

501

objectClass

required

i

posixGroup

(structural)

i

top

(add value)

Update Object

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

Available members

jellingwood

Group members

user2

Add selected >>

Add all >>

<< Remove selected

<< Remove all

Save changes

Conclusion