

## GNU/Linux Administration - Feature #756

### Setup LDAP Authentication for ownCloud

02/25/2016 08:39 PM - Daniel Curtis

<b>Status:</b>	Closed	<b>Start date:</b>	02/25/2016
<b>Priority:</b>	Normal	<b>Due date:</b>	
<b>Assignee:</b>	Daniel Curtis	<b>% Done:</b>	100%
<b>Category:</b>	Authentication	<b>Estimated time:</b>	0.50 hour
<b>Target version:</b>	*nix	<b>Spent time:</b>	1.50 hour

#### Description

This is a guide on how to setup LDAP authentication for users on ownCloud. The LDAP server is OpenLDAP on FreeBSD 9, but should work on any LDAP server.

### Populate the LDAP Server

- Create the People Organizational Unit ldif file:

```
vi ~/people-ou.ldif
```

- And add the following:

```
dn: ou=People,dc=example,dc=com
objectclass: organizationalUnit
ou: People
```

- Import the People OU file into the server:

```
ldapadd -D "cn=Manager,dc=example,dc=com" -W -f ~/people-ou.ldif
```

- Create the bob user ldif file:

```
vi ~/bob.ldif
```

- And add the following:

```
dn: cn=Bob Guy,ou=People,dc=example,dc=com
cn: Bob Guy
givenname: Bob
initials: BG
mail: bob@example.com
objectclass: inetOrgPerson
objectclass: organizationalPerson
objectclass: person
sn: Guy
uid: bob
userpassword: {MD5}X03MO1qnZdYdgyfeuILPmQ==
```

- **NOTE:** The password for bob is **password**.

## Setup LDAP Authentication

**NOTE:** If using LDAP with SSL add the CA certificate used on the LDAP server, or else the connection will not succeed.

- Edit the ldap config file and add the CA certificate used on the LDAP server

```
vi /usr/local/etc/openldap/ldap.conf
```

- And add the following:

```
TLS_CACERT /usr/local/etc/bundle.pem
```

- **NOTE:** Add the CA certificate bundle to the bundle.pem file

---

**NOTE:** Make sure to set the LDAP users *uid* to the group *memberUid* attribute, or else owncloud will not be able to match the LDAP user and groups.

- Log into owncloud admin site, <http://owncloud.example.com/> and go to Apps -> Apps and click on **Not enabled**.
- Locate and enable **LDAP user and group backend**.
- Next go to Username -> Admin and scroll to the LDAP section.
  1. Host: **ldap.example.com**
  2. Port: **389**
  3. User DN: **cn=Manager,dc=example,dc=com**
  4. Password: **SuperSecretPassword**
  5. Base DN: **dc=example,dc=com**
- Click **Continue** and select all of the Object Classes in the Users tab.
- Then click **Continue** and select:
  1. LDAP / AD Username: **[X]**
  2. LDAP / AD Email Address: **[X]**
- Next click the Advanced -> Directory Settings and select **memberUid** from the Group-Member association menu.
- Finally enter in the bob username and test if the connection works. If it does, try logging out and logging into owncloud using the bob user.

**NOTE:** If you are not using Active Directory, then you may not be using the MemberOf attribute. To disable the use of the MemberOf attribute run the following from the owncloud installation directory:

```
sudo -u www ./occ ldap:set-config "" useMemberOfToDetectMembership 0
```

## Resources

- [https://doc.owncloud.org/server/8.2/admin\\_manual/configuration\\_user/user\\_auth\\_ldap.html](https://doc.owncloud.org/server/8.2/admin_manual/configuration_user/user_auth_ldap.html)

---

## History

#1 - 02/25/2016 08:46 PM - Daniel Curtis

- Description updated

- Status changed from New to Resolved

- % Done changed from 0 to 100

**#2 - 02/27/2016 08:59 PM - Daniel Curtis**

- *Description updated*

**#3 - 02/28/2016 01:47 PM - Daniel Curtis**

- *Description updated*

**#4 - 03/12/2016 02:05 PM - Daniel Curtis**

- *Category changed from Web Server to Authentication*

- *Status changed from Resolved to Closed*

**#5 - 05/27/2016 03:17 PM - Daniel Curtis**

- *Description updated*

**#6 - 05/27/2016 03:20 PM - Daniel Curtis**

- *Description updated*