Utils

- OpenLDAP + phpLDAPAdmin Docker
  - Tags: osixia/openldap:1.2.1
  - Latest release: 1.2.1 - OpenLDAP 2.4.44
  - Readme:github
  - docker-compose.yml
- OpenLDAP Backup https://github.com/osixia/docker-openldap-backup
- Apache Directory Studio
- LDAP Account Manager
  - Docker: https://hub.docker.com/r/mwaeckerlin/lam/
  - ```
    docker run -d -p 8123:80 --name lam mwaeckerlin/lam
    ```
    - goto **LAM configuration** / **Edit general settings**, login with default password **lam** and Change master password. Then go back and still with password lam go to Edit server profiles to setup your OpenLDAP
    - user: Manager, password: lam

cn=config

Historically OpenLDAP has been statically configured, that is, to make a change to the configuration the slapd.conf file was modified and slapd stopped and started. In the case of larger users this could take a considerable period of time and had become increasingly unacceptable as an operational method.

Typically in your OpenLDAP installation you have at least two trees:

- One is the DIT (“data information tree”) where you enter your nodes
  - access by “cn=admin,dc=example,dc=org”
  - default password “admin”
- One is **cn=config**, where the configuration information is put (which can be manipulated with just the same LDAP commands, as itself is setup as a DIT!).
  - access by “cn=admin,cn=config”
  - default password “config”
  - **BaseDN: 'cn=config'** - use Apache Directory Studio to connect

ACL

https://www.openldap.org/doc/admin24/access-control.html

Order matters in ACL rules. LDAP will stop looking on the first match. So new acl entries should be inserted before default ones.

Default entries:
    ```

```
olcAccess: {0}to attrs=userPassword,shadowLastChange by self write by
dn="cn=admin,dc=example,dc=org" write by anonymous auth by * none
olcAccess: {1}to * by self read by dn="cn=admin,dc=example,dc=org" write by
* none
```

- olcAccess: {0}to attrs=userPassword,shadowLastChange
  - by self write
  - by dn=“cn=admin,dc=example,dc=org” write
  - by anonymous auth
  - by * none
- olcAccess: {1}to *
  - by self read
  - by dn=“cn=admin,dc=example,dc=org” write
  - by * none

Giving user: **uid=nextcloudsystemuser,ou=it,dc=grinn-global,dc=com** rights:

- Entry to edit: **olcDatabase={1}mdb,cn=config**
- Attribute to add: **olcAccess**
- to by dn.exact=“uid=nextcloudsystemuser,ou=it,dc=grinn-global,dc=com” read

Examples

```
olcAccess: {1}to dn.base="" by * read
```

- Give user access to modify photo: <code>olcAccess: to attrs=jpegPhoto by self write by * read</codE>