Project parveen Servei LDAP

Basic Information

my project is about to explain some basic and adv. function openldap.i am going to explain step by step different function of ldap.

Here i used different docker to make different ldap server and database of ldap.

Also we are going to use as clients how is work connection etc.

we start from basic information and knowledge about opeldap. . . . . thanks

LDAP stands for Lightweight Directory Access Protocol

when to use ldap

- Machine Authentication
- User Authentication
- User/System Groups
- Address book
- Organization Representation
- Telephony Information Store
- E-mail address lookups
- Application Configuration store

ldap workk

LDAP utilizes a client-server model. One or more LDAP servers contain the data making up the directory information tree (DIT)

slapd conf

slapd(8) is an LDAP directory server that runs on many different platforms. You can use it to provide a directory service of your very own. Your directory can contain pretty much anything you want to put in it. You can connect it to the global LDAP directory service, or run a service all by yourself.

Data for ldif

Here i show how is my structure of ldif file all data hbd beacuse of more function we can use

- start with Distinguished Name **dc=edt,dc=org**
- make organization in this data **o=europa,dc=edt,dc=org**
- now make organization unit in my case **ou=usuaris,o=europa,dc=edt,dc=org**
- add new organization unit in my case **ou=group,o=europa,dc=edt,dc=org**
- add new organization unit in my case **ou=usermod,o=europa,dc=edt,dc=org**
- add new organization unit in my case **ou=maquines,o=europa,dc=edt,dc=org**
- now make new organization for another subordinate in my case **o=asia,dc=edt,dc=org**

after this all data will be make another place or docker

- now make organization unit in my case **ou=usuaris,o=asia,dc=edt,dc=org**
- add new organization unit in my case **ou=group,o=asia,dc=edt,dc=org**
- add new organization unit in my case **ou=usermod,o=asia,dc=edt,dc=org**
- add new organization unit in my case **ou=maquines,o=asia,dc=edt,dc=org**

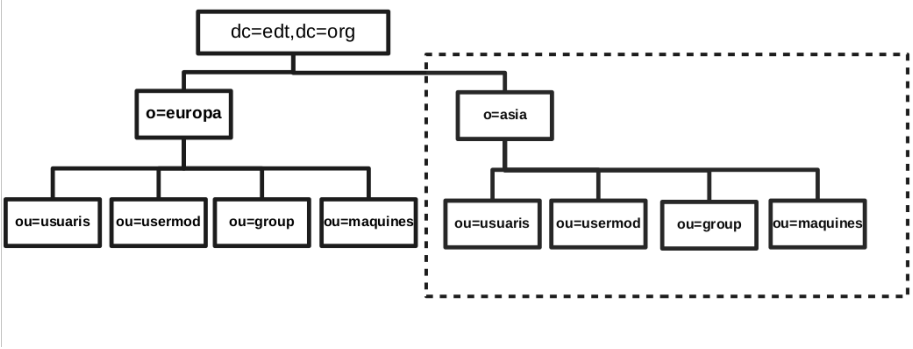

Figure 1: end

Schema Specification

To save data in a readable format in ldap we called schema(this is reason so we can)

different schema make esay to read and write also make fuctionable data in ldif very important to know different type of like photo,dn,cn,binary file etc.

here one simple exemple make by mi

```
# schema add photo and pdf:
#          foto, pdf
# parveen
# Objecte  Auxiliary  (derivat de TOP)
#
attributetype (1.1.2.1.1 NAME 'xfoto'
  DESC 'foto del user jpeg'
  SYNTAX 1.3.6.1.4.1.1466.115.121.1.28)

attributetype (1.1.2.1.2 NAME 'xpdf'
  DESC 'pdf file'
  SYNTAX  1.3.6.1.4.1.1466.115.121.1.5
  SINGLE-VALUE)

objectclass (1.1.2.2.1 NAME 'xuser'
  DESC 'user add foto and pdf'
  SUP TOP
  AUXILIARY
  MUST ( xfoto $ xpdf )
 )
```

docker ldap_schema add photo and pdf

```
docker run --rm --name ldap_schema -h ldap_schema --network project -d parveen1992/ldap_sche
```

avd. serch in ldap

```
ldapsearch -x -LLL -h localhost -D "cn=user01,ou=usermod,o=europa,dc=edt,dc=org" -w user01 '
```

Scripts

here i make some useful scripts /etc/passwd to ldif file

make groop file

```
python group_make_ldif.py groupfile.txt group.ldif
```

make user file

```
python user_make_ldif.py user_file.txt user.ldif
```

some try form outside

```
[root@i03 scripts]# ldapadd -h 172.18.0.2 -D "cn=Manager,dc=edt,dc=org" -w jupiter -f group.
adding new entry "cn=grouplocal01,ou=group,o=europa,dc=edt,dc=org "

adding new entry "cn=grouplocal02,ou=group,o=europa,dc=edt,dc=org "
```

```
adding new entry "cn=grouplocal03,ou=group,o=europa,dc=edt,dc=org "
```

my scripts

```
#! /bin/bash
# description add authomatic all user
rm -rf group.ldif
rm -rf user.ldif

python group_make_ldif.py groupfile.txt group.ldif

python user_make_ldif.py user_file.txt user.ldif

# insisde from network or docker(from out must use ip address)
ldapadd -h ldap_schema -D "cn=Manager,dc=edt,dc=org" -w jupiter -f group.ldif
ldapadd -h ldap_schema -D "cn=Manager,dc=edt,dc=org" -w jupiter -f user.ldif
```

Replication

ldap server backup save called replication

OpenLDAP now supports a wide variety of replication topologies, these terms have been deprecated in favor of provider and consumer: A provider replicates directory updates to consumers; consumers receive replication updates from providers. Unlike the rigidly defined master/slave relationships, provider/consumer roles are quite fluid: replication updates received in a consumer can be further propagated by that consumer to other servers, so a consumer can also act simultaneously as a provider. Also, a consumer need not be an actual LDAP server; it may be just an LDAP client.

but today ldap user ldap provider and consumer server which can we use both as main server and for backup.

here is all configutaion of this server all if you like also use my docker

make new network

```
docker network crete project
```

now start both docker one by one

```
docker run --rm --name ldap_p -h ldap_p --net project -d  parveen1992/ldap_provider
```

```
docker run --rm --name ldap_c -h ldap_c --net project -d  parveen1992/ldap_consumer
```

This is my modify.ldif

```
dn: cn=Pere Pou,ou=usuaris,dc=edt,dc=org
changetype: modify
add: description
description: add by provider
```

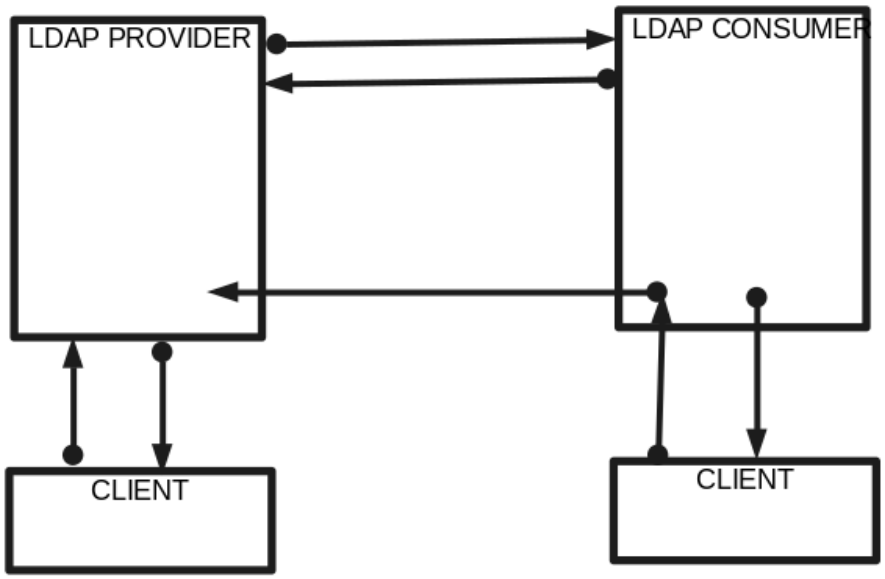

Figure 2: end

But you can change anythings in master or consumer

```
ldapmodify -vx -h ldap_p -D "cn=Manager,dc=edt,dc=org" -w jupiter -f modify.ldif
```

```
ldapmodify -vx -h ldap_c -D "cn=Manager,dc=edt,dc=org" -w jupiter -f modify.ldif
```

```
ldapmodify -vx -h ldap_c -D "cn=user01,ou=usermod,o=europa,dc=edt,dc=org" -w user01 -f modif
```

provider

overlay syncprov

Add in plugin for save all entres later update for consumer

syncprov-checkpoint 50 10

this means update ever 50 operction or 10 mintus

syncprov-sessionlog 100

user log in after 100

consumer

addtion conf. in consumer

```
syncrepl rid=001
  provider=ldap://ldap_p
  type=refreshOnly
  interval=00:00:00:10
  searchbase="dc=edt,dc=org"
  binddn="cn=Manager,dc=edt,dc=org"
  credentials=jupiter
updateref ldap://ldap_p
```

Subordinate and TLS

Subordinate knowledge information may be provided to delegate a subtree. Subordinate knowledge information is maintained in the directory as a special referral object at the delegate point. The referral object acts as a delegation point, gluing two services together. This mechanism allows for hierarchical directory services to be constructed.

NOTE:- if one data str. conf to where we can find iformation about this DSA (another DIT) this is called referral

But we use this referral to server collect all information and send to client

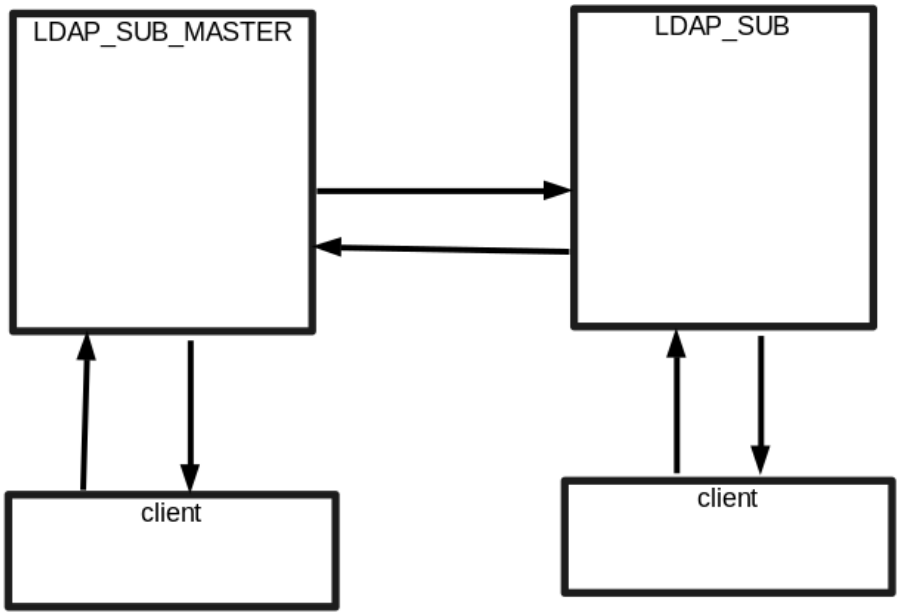

Figure 3: end

docker ldapmaster

```
docker run --rm --name ldap_sub_master -h ldap_sub_master --net project -d parveen1992/ldap_
```

docker ldap_sub

```
docker run --rm --name ldap_sub -h ldap_sub --net project -d  parveen1992/ldap_sub
```

search in both data

```
ldapsearch -M -b "dc=subtree,dc=edt,dc=org" -x "(objectclass=referral)" '*' ref
```

```
[root@ldap_sub_master docker]# ldapsearch -M -LLL -b "o=asia,dc=edt,dc=org" -x "(objectclass
dn: o=asia,dc=edt,dc=org
objectClass: referral
objectClass: extensibleObject
o: asia
ref: ldap://ldap_sub/o=asia,dc=edt,dc=org
```

referrels to find master to by usind sub

try in master

```
[root@ldap_sub_master docker]# ldapsearch -x -LLL -D "cn=Manager,dc=edt,dc=org" -b "o=asia,d
dn: o=asia,dc=edt,dc=org

dn: ou=maquines,o=asia,dc=edt,dc=org

dn: ou=group,o=asia,dc=edt,dc=org

dn: ou=usermod,o=asia,dc=edt,dc=org

dn: ou=usuaris,o=asia,dc=edt,dc=org

dn: cn=Pere Pou,ou=usuaris,o=asia,dc=edt,dc=org

dn: cn=Admin System,ou=usuaris,o=asia,dc=edt,dc=org

dn: cn=user01,ou=usermod,o=asia,dc=edt,dc=org

dn: cn=group01,ou=group,o=asia,dc=edt,dc=org

dn: cn=group02,ou=group,o=asia,dc=edt,dc=org
```

all working

```
[root@ldap_sub docker]# /usr/sbin/slapd -d-1 -u ldap -h "ldap:/// ldaps:/// ldapi:///" && ec
.......
```

```
5ce6432d ==>slap_sasl_authorized: can cn=manager,o=asia,dc=edt,dc=org become cn=pere pou,ou=
5ce6432d <== slap_sasl_authorized: return 0
5ce6432d conn=1002 op=1 PROXYAUTHZ dn="cn=pere pou,ou=usuaris,o=europa,dc=edt,dc=org"
5ce6432d <= get_ctrls: n=1 rc=0 err=""
5ce6432d     attrs: dn
5ce6432d conn=1002 op=1 SRCH base="o=asia,dc=edt,dc=org" scope=2 deref=0 filter="(objectClas
5ce6432d conn=1002 op=1 SRCH attr=dn
5ce6432d ==> limits_get: conn=1002 op=1 self="cn=pere pou,ou=usuaris,o=europa,dc=edt,dc=org'
5ce6432d => hdb_search
5ce6432d bdb_dn2entry("o=asia,dc=edt,dc=org")
5ce6432d => access_allowed: search access to "o=asia,dc=edt,dc=org" "entry" requested
5ce6432d => acl_get: [1] attr entry
5ce6432d => acl_mask: access to entry "o=asia,dc=edt,dc=org", attr "entry" requested
5ce6432d => acl_mask: to all values by "cn=pere pou,ou=usuaris,o=europa,dc=edt,dc=org", (=0)
5ce6432d <= check a_dn_pat: *
5ce6432d <= acl_mask: [1] applying read(=rscxd) (stop)
5ce6432d <= acl_mask: [1] mask: read(=rscxd)
5ce6432d => slap_access_allowed: search access granted by read(=rscxd)
5ce6432d => access_allowed: search access granted by read(=rscxd)
5ce6432d search_candidates: base="o=asia,dc=edt,dc=org" (0x00000001) scope=2
5ce6432d => hdb_dn2idl("o=asia,dc=edt,dc=org")
5ce6432d => bdb_filter_candidates
```

.....

LDAP TLS basic openssl

docker connect to ldap_schema by using tls (ca certificat) or start tls means that can connect normal or if both client and server have conf for tls then start tls

user old cert to my new data working great only change extension must be use same and no project network beacuse of ip adress or add subject alter name

```
docker run --rm --name ldap.edt.org -h ldap.edt.org --network project -it parveen1992/ldaps
```

check point

```
[root@ldaps docker]# ldapsearch -x -LLL -H ldaps://ldap.edt.org -s base -b 'dc=edt,dc=org' d
dn: dc=edt,dc=org

[root@ldaps docker]# cat /etc/hosts
127.0.0.1   localhost
::1 localhost ip6-localhost ip6-loopback
fe00::0 ip6-localnet
ff00::0 ip6-mcastprefix
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters
```

```
172.18.0.2  ldaps.edt.org ldap.edt.org
```

LDAP PAM

here docker ldap_pam connect to ldap_schema and valid to user to login mount of home if not exists then make new one by using pam conf.

pam docker as host

```
docker run --rm --name host -h host --net project --privileged -it parveen1992/ldap_pam
```

check point

```
[root@host docker]# su - pere
Creating directory '/tmp/home/pere'.
reenter password for pam_mount:
[pere@host ~]$ pwd
/tmp/home/pere
[pere@host ~]$ ll
total 0
drwxr-xr-x. 2 pere group01 40 May 19 16:06 test
[pere@host ~]$ su - marta
pam_mount password:
Creating directory '/tmp/home/marta'.
[marta@host ~]$ ll
total 0
[marta@host ~]$ pwd
/tmp/home/marta
```

GRAHICAL VIEW PHP AND HTTPS

my localhost page in httpd

```
<h1> hello everyone </h1>

welcome to my page

page for everyone

<br>

<a href="http://localhost:2080/phpldapadmin">To see photo and data binnary</a>

<br>

<a href="http://localhost:3080">login as ldap user</a>
```

PHP

check by php ldap to look about photo and pdf of user

```
docker run --rm --name ldap_php -h ldap_php --net project -p 2080:80 -it parveen1992/ldap_ph
```

Ldap httpd

** add modul mod_ldap **

conf. like this

```
[root@ldap_httpd docker]# cat ldap_httpd.conf
<VirtualHost *:80>
        ServerAdmin webmaster@localhost
        ServerName ldap_httpd
        DocumentRoot /var/www/ldap
        <Directory /var/www/ldap>
                Options Indexes FollowSymLinks MultiViews
                AllowOverride None
                Order deny,allow
                Deny from All

                AuthType Basic
                AuthBasicProvider ldap
                AuthName "Test OPenLDAP login"
                AuthLDAPURL ldap://ldap_schema/ou=usuaris,o=europa,dc=edt,dc=org?uid
                AuthLDAPBindDN "cn=user01,ou=usermod,o=europa,dc=edt,dc=org"
                AuthLDAPBindPassword "user01"
                Require valid-user
                Satisfy any

        </Directory>
</VirtualHost>
```

check point

```
172.18.0.1 - - [14/May/2019:09:35:34 +0000] "GET / HTTP/1.1" 401 381 "-" "Mozilla/5.0 (X11;
172.18.0.1 - pere [14/May/2019:09:35:45 +0000] "GET / HTTP/1.1" 304 - "-" "Mozilla/5.0 (X11;
172.18.0.1 - pere [14/May/2019:09:35:45 +0000] "GET /favicon.ico HTTP/1.1" 404 209 "http://1
```

docker start and also connect able to ldap_schema

```
docker run --rm --name ldap_httpd -h ldap_httpd --network project -p 3080:80 -d parveen1992/
```

Figure 4: end