Ldap

Table des matières

1 Installation

- http://www.openldap.org/doc/admin24/quickstart.html
- https://www.digitalocean.com/community/tutorials/how-to-install-and-configure-a-basic-ldap-server-on-an-ubuntu-12-04-vps
- intro
- quickstart
- liste

```
slapd - OpenLDAP server (slapd)
ldap-utils - OpenLDAP utilities
ldap-git-backup - Back up LDAP database in an Git repository

# apt-get install slapd ldap-utils

# ps -ef | grep slapd
openldap 15103     1  0 01:44 ?        00:00:00 \
 /usr/sbin/slapd -h ldap:/// ldapi:/// -g openldap -u openldap \
 -F /etc/ldap/slapd.d

# slapcat

# find /etc/ldap/slapd.d/
/etc/ldap/slapd.d/
/etc/ldap/slapd.d/cn=config
/etc/ldap/slapd.d/cn=config/cn=schema
/etc/ldap/slapd.d/cn=config/cn=schema/cn={3}inetorgperson.ldif
/etc/ldap/slapd.d/cn=config/cn=schema/cn={1}cosine.ldif
/etc/ldap/slapd.d/cn=config/cn=schema/cn={0}core.ldif
/etc/ldap/slapd.d/cn=config/cn=schema/cn={2}nis.ldif
/etc/ldap/slapd.d/cn=config/olcDatabase={1}mdb.ldif
/etc/ldap/slapd.d/cn=config/olcBackend={0}mdb.ldif
/etc/ldap/slapd.d/cn=config/cn=module{0}.ldif
/etc/ldap/slapd.d/cn=config/cn=schema.ldif
/etc/ldap/slapd.d/cn=config/olcDatabase={0}config.ldif
/etc/ldap/slapd.d/cn=config/olcDatabase={-1}frontend.ldif
/etc/ldap/slapd.d/cn=config.ldif

# ls /var/lib/ldap/data.mdb
```

2 Configuration

```
# dpkg-reconfigure -plow slapd ?
$ ldapsearch -x -b '' -s base '(objectclass=*)' namingContexts
dn:
namingContexts: dc=narval,dc=fr,dc=eu,dc=org

$ cat > tmp.ldif <<EOF
dn: dc=narval,dc=fr,dc=eu,dc=org
objectclass: dcObject
objectclass: organization
o: mdtx
dc: narval

dn: cn=Manager,dc=narval,dc=fr,dc=eu,dc=org
objectclass: organizationalRole
cn: Manager
EOF

# ldapadd -x -D "cn=Manager,dc=narval,dc=fr,dc=eu,dc=org" -W -f tmp.ldif
Enter LDAP Password:

# ldapadd -Y external -H ldapi:/// -f tmp.ldif ?
# slappasswd ?

# /etc/init.d/slapd stop
# slapd -h ldap://localhost -d 481
5816a86a mdb_db_open: database "dc=narval,dc=fr,dc=eu,dc=org": dbenv_open(/var/lib/ldap).

# slapcat -n0 | grep olcRootDN
# ldapadd -x -D "cn=admin,dc=narval,dc=fr,dc=eu,dc=org" -W -f tmp.ldif
Enter LDAP Password:

$ ldapsearch -x -b 'dc=example,dc=com' '(objectclass=*)'
```

»»»> 07dfbc288a1e7dbc828a4537e299f6471bf66765

3 2ème essai

... schema
Configuration globale

```
# apt-get install slapd
> mot de passe admin ldap :

# dpkg-reconfigure slapd
```

Configuration client

```
# vi /etc/ldap/ldap.conf
BASE    dc=narval,dc=fr,dc=eu,dc=org
URI     ldap://127.0.0.1

$ ldapsearch -x
$ slapcat

# apt-get install lat
```

Configuration détaillée

```
# apt-get install ldap-utils

$ ldapsearch -Y EXTERNAL -H ldapi:/// -b "cn=config"
```

Ldap via le browser ?

```
# vi /etc/default/slapd
SLAPD_SERVICES="ldap://127.0.0.1:389/ ldaps:/// ldapi:///"

ldap://127.0.0.1:389

$ cat >test.ldif <<EOF
dn: ou=collections,o=mediatex,dc=narval,dc=fr,dc=eu,dc=org
objectClass: organizationalUnit
ou: collections

dn: ou=users,o=mediatex,dc=narval,dc=fr,dc=eu,dc=org
objectClass: organizationalUnit
ou: users
EOF

# /etc/init.d/slapd stop
# slapadd -c -v -l test.ldif
# /etc/init.d/slapd start

$ cat >user.ldif <<EOF
dn: cn=nroche,ou=users,dc=narval,dc=fr,dc=eu,dc=org
cn: nroche
gidNumber: 20000
objectClass: top
objectClass: posixGroup

dn: uid=nroche,ou=users,dc=narval,dc=fr,dc=eu,dc=org
uid: nroche
uidNumber: 20000
gidNumber: 20000
cn: nroche
sn: nroche
objectClass: top
objectClass: person
objectClass: posixAccount
objectClass: shadowAccount
loginShell: /bin/bash
homeDirectory: /home/nroche
EOF

$ ldapadd -c -x -D cn=admin,dc=narval,dc=fr,dc=eu,dc=org -W -f user.ldif
$ ldappasswd -x -D cn=admin,dc=narval,dc=fr,dc=eu,dc=org -W -S uid=nroche,ou=users,dc=narval,dc=fr,dc=eu,dc=org
$ ldapsearch -x uid=nroche
```

**Apache
Configuration Apache

```
# a2enmod ldap auth_basic authnz_ldap authz_user
# /etc/init.d/apache2 restart

# vi /etc/apache2/sites-enabled/000-default.conf
<Directory /var/www/html/prologuei>
        AuthType Basic
        AuthName "Restricted Area"
```

```
        AuthLDAPBindDN "cn=admin,dc=narval,dc=fr,dc=eu,dc=org
        AuthLDAPBindPassword "totoro00"
        AuthBasicProvider ldap
        AuthLDAPURL ldap://127.0.0.1/ou=users,dc=narval,dc=fr,dc=eu,dc=org
        Require valid-user
</Directory>
```

Etendre le schema : /etc/ldap/schema/custom-user.schema

```
objectClass     ( 1.3.6.1.4.1.4203.666.1.100
    NAME 'user'
        DESC 'User login'
    STRUCTURAL
        MAY  ( uid $ userPassword )
        )

dn: cn=toto,ou=users,dc=narval,dc=fr,dc=eu,dc=org
cn: toto
objectClass: top
objectClass: user

dn: uid=toto,ou=users,dc=narval,dc=fr,dc=eu,dc=org
uid: toto
cn: toto
sn: toto
objectClass: top
objectClass: user
EOF

$ ldapadd -c -x -D cn=admin,dc=narval,dc=fr,dc=eu,dc=org -W -f user.ldif
// ne marche pas :(
```

TODO :

- connection chiffrée
- connection distante

En fait, on n'a pas besoin de LDAP pour faire ce que je veux. Pour les logins : http ://the-dance.net/ roth/TECHBLOG/openid.html http ://stackoverflow.com/questions/28588/how-do-you-set-up-an-openid-provider-server-in-ubuntu

On veut réécrire "http ://narval.fr.eu.org/ mdtx-COLL" en "http ://DN.narval.fr.eu.org/ mdtx-COLL" rewrite url : RewriteMap

/etc/bind/db.narval.fr.eu.org

```
; round-robin
rr01    IN      A       5.135.154.197
rr01    IN      A       79.143.250.133

dn01    IN      CNAME   rr01.narval.fr.eu.org.

cat >map.txt <<EOF
galoupinou dn01
demo dn01
paies dn02
bof dn02
toto dn03
EOF
# httxt2dbm -i map.txt -o map.map
# chown www-data. map.*
```

```
# mkdir /var/www/html/dn01
# echo "coucou" > /var/www/html/dn01/mdtx-coll1.html
# chown -R www-data. /var/www/html/dn01
```

/etc/apache2/sites-enabled/000-default.conf

```
## redirection d'URL pour avoir mediatex reparti sur plusieurs machines
RewriteEngine On
RewriteCond %{HTTP_HOST}   ^www\.(.+)$ [NC]
RewriteMap dn "dbm:/etc/apache2/map.map"
RewriteRule "/~mdtx-([^/]*)(.*)" "http://${dn:$1}.%1/~mdtx-$1$2"

# a retirer pour la prod (ralenti)
LogLevel alert rewrite:trace3
```

Rq : le `%1` s'applique aux parenthèses du `RewriteCond`. Ici le `RewriteCond` est requis car `RewriteRule` ne travaille (premier champ) que sur le path. Le `$1` s'applique aux parenthèses du `RewriteRule`.

```
# tail -f /var/log/apache2/error.log

[rewrite:trace2]  init rewrite engine with requested uri /~mdtx-galoupinou/index/
[rewrite:trace3]  applying pattern '/~mdtx-([^/]*)' to uri '/~mdtx-galoupinou/index/'
[rewrite:trace2]  rewrite '/~mdtx-galoupinou/index/' -> 'http://dn01.narval.fr.eu.org/~mdtx-galoupinou'
[rewrite:trace2]  implicitly forcing redirect (rc=302) with http://dn01.narval.fr.eu.org/~mdtx-galoupinou
[rewrite:trace1]  escaping http://dn01.narval.fr.eu.org/~mdtx-galoupinou for redirect
[rewrite:trace1]  redirect to http://dn01.narval.fr.eu.org/~mdtx-galoupinou [REDIRECT/302]
[rewrite:trace2]  init rewrite engine with requested uri /~mdtx-galoupinou
[rewrite:trace3]  applying pattern '/~mdtx-([^/]*)' to uri '/~mdtx-galoupinou'
[rewrite:trace1]  pass through /~mdtx-galoupinou
[rewrite:trace2]  init rewrite engine with requested uri /~mdtx-galoupinou/
[rewrite:trace3]  applying pattern '/~mdtx-([^/]*)' to uri '/~mdtx-galoupinou/'
[rewrite:trace1]  pass through /~mdtx-galoupinou/
[rewrite:trace2]  init rewrite engine with requested uri /~mdtx-galoupinou/index.shtml
[rewrite:trace3]  applying pattern '/~mdtx-([^/]*)' to uri '/~mdtx-galoupinou/index.shtml'
[rewrite:trace1]  pass through /~mdtx-galoupinou/index.shtml
[rewrite:trace2]  init rewrite engine with requested uri /favicon.ico
[rewrite:trace3]  applying pattern '/~mdtx-([^/]*)' to uri '/favicon.ico'
[rewrite:trace1]  pass through /favicon.ico
[rewrite:trace2]  init rewrite engine with requested uri /~mdtx-galoupinou/index
[rewrite:trace3]  applying pattern '/~mdtx-([^/]*)' to uri '/~mdtx-galoupinou/index'
[rewrite:trace1]  pass through /~mdtx-galoupinou/index
[rewrite:trace2]  init rewrite engine with requested uri /favicon.ico
[rewrite:trace3]  applying pattern '/~mdtx-([^/]*)' to uri '/favicon.ico'
[rewrite:trace1]  pass through /favicon.ico
[rewrite:trace2]  init rewrite engine with requested uri /~mdtx-galoupinou/index/
[rewrite:trace3]  applying pattern '/~mdtx-([^/]*)' to uri '/~mdtx-galoupinou/index/'
[rewrite:trace1]  pass through /~mdtx-galoupinou/index/
[rewrite:trace2]  init rewrite engine with requested uri /~mdtx-galoupinou/index/index.shtml
[rewrite:trace3]  applying pattern '/~mdtx-([^/]*)' to uri '/~mdtx-galoupinou/index/index.shtml'
[rewrite:trace1]  pass through /~mdtx-galoupinou/index/index.shtml
[rewrite:trace2]  init rewrite engine with requested uri /~mdtx-galoupinou/indexHeader.shtml
[rewrite:trace3]  applying pattern '/~mdtx-([^/]*)' to uri '/~mdtx-galoupinou/indexHeader.shtml'
[rewrite:trace1]  pass through /~mdtx-galoupinou/indexHeader.shtml
[rewrite:trace2]  init rewrite engine with requested uri /~mdtx-galoupinou/readme.html
[rewrite:trace3]  applying pattern '/~mdtx-([^/]*)' to uri '/~mdtx-galoupinou/readme.html'
[rewrite:trace1]  pass through /~mdtx-galoupinou/readme.html
[rewrite:trace2]  init rewrite engine with requested uri /~mdtx-galoupinou/footer.html
```

```
[rewrite:trace3]  applying pattern '/~mdtx-([^/]*)' to uri '/~mdtx-galoupinou/footer.html'
[rewrite:trace1]  pass through /~mdtx-galoupinou/footer.html
```