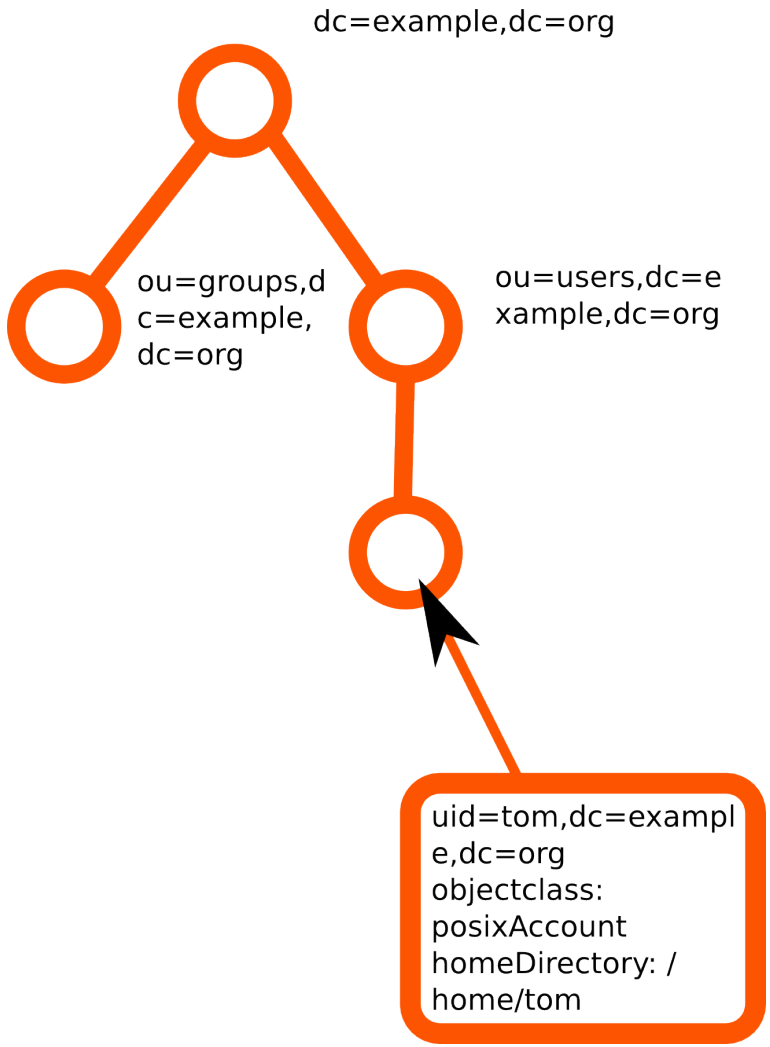
LDAP

DIT


dc=example,dc=org
ou=groups,dc=example,dc=org
ou=users,dc=example,dc=org
uid=tom,dc=example,dc=org
objectclass: posixAccount
homeDirectory: /home/tom

LDIF

```
dn: cn=admin,dc=example,dc=org
objectClass: person
cn: admin
description: admin Ldap
```

```
structuralObjectClass: inetOrgPerson
entryUUID: af1b6df8-981f-103f-9b15-9
    b59b2406d23
creatorsName: cn=manager,dc=od
createTimestamp: 20250318083525Z
entryCSN: 20250318170815.057879Z#
    000000#000#000000
modifiersName: cn=manager,dc=od
modifyTimestamp: 20250318170815Z
entryDN: uid=tom,ou=opendoor.fr,dc=
    od
subschemaSubentry: cn=Subschema
hasSubordinates: FALSE
```

LDIF pour modification

```
dn: cn=admin,dc=example,dc=org
changetype: modify
replace: description
description: Administrateur de l'
 annuaire

```

slapd.conf

```
include         /etc/ldap/schema/core.schema
include         /etc/ldap/schema/cosine.schema
include         /etc/ldap/schema/nis.schema
include         /etc/ldap/schema/inetorgperson.schema

pidfile         /var/run/slapd/slapd.pid
argsfile        /var/run/slapd/slapd.args
loglevel        none

modulepath      /usr/lib/ldap
moduleload      back_hdb

sizelimit 500
tool-threads 1

backend         hdb
database        hdb

suffix          "dc=maison,dc=opendoor,dc=fr"
directory       "/var/lib/ldap"

dbconfig set_cachesize 0 2097152 0
dbconfig set_lk_max_objects 1500
dbconfig set_lk_max_locks 1500
dbconfig set_lk_max_lockers 1500
index           objectClass eq

lastmod         on
checkpoint      512 30

access to attrs=userPassword,shadowLastChange
```

Index

index objectclass eq

eq(uality)	uid=tconstans
approx	dc=˜epsi
pre(sence)	attribut présent ou pas
sub(string)	ou=*group*

ACL

```
access to attrs=userPassword,
    shadowLastChange
        by dn="cn=admin,dc=maison,dc=
            opendoor,dc=fr" write
        by anonymous auth
        by self write
        by * none

access to dn.base="" by * read

access to *
        by dn="cn=admin,dc=maison,dc=
            opendoor,dc=fr" write
        by * read
```

Journalisation

valeur de *loglevel*

0	aucun
8	gestion des connexions
32	gestion des index
64	directives de configuration
128	ACL
256	Statistiques sur les connexions, les opérations et leur résultat
-1	tout

Codes d'erreur

13	NoSuchAttribute	attribut inconnnu
32	NoSuchObject	objet introuvable ou base de recherche incorrecte
49	InvalidCredentials	authentification incorrecte
50	InsufficientAccessRight	Les acl ne permettent pas l'opération
52	Unavailable	problème d'accès au serveur
65	ObjectClassViolation	les nouvelles données ne respectent pas la classe de l'entrée.

ldap.conf

```
BASE        dc=maison,dc=opendoor,dc=fr
URI         ldap://cafeine
TLS_CACERT          /etc/ldap/certs/cacert.pem
TLS_REQCERT         demand
```

Options commune au client ldap

-D dn pour l'authentification

-W demande du mot de passe

-x authentification simple

-d niveau de debug

-H ldap uri

-b base de la recherche

Recherche

```
ldapsearch –x ’(|(objectclass=person)(objectclass=group))’
```

Recherche

```
ldapsearch –x ’(|(objectclass=person)(objectclass=group))’
ldapsearch –xWD cn=admin,dc=example,dc=org ’(&(objectclass=account)(
passwordAge>365))’
```

Modification

1. Création d'un fichier LDIF :

```
dn: ou=utilisateurs,dc=example,dc=
    org
objectClass: organizationalUnit
objectClass: top
ou: utilisateurs
```

2. Application :

   ldapadd option –f fichier.ldif

Modification

1. Création du fichier LDIF :

```
dn: cn=admin,dc=example,dc=org
changetype: modify
replace: description
description: l'admin■DIT
add:■title
title:■Da■Boss
■■■■■■
```

2. Application :

   ldapmodify option –f fichier.ldif

Gestion du mot de passe

1. Offline à l'aide de slappasswd
2. Online à l'aide de :

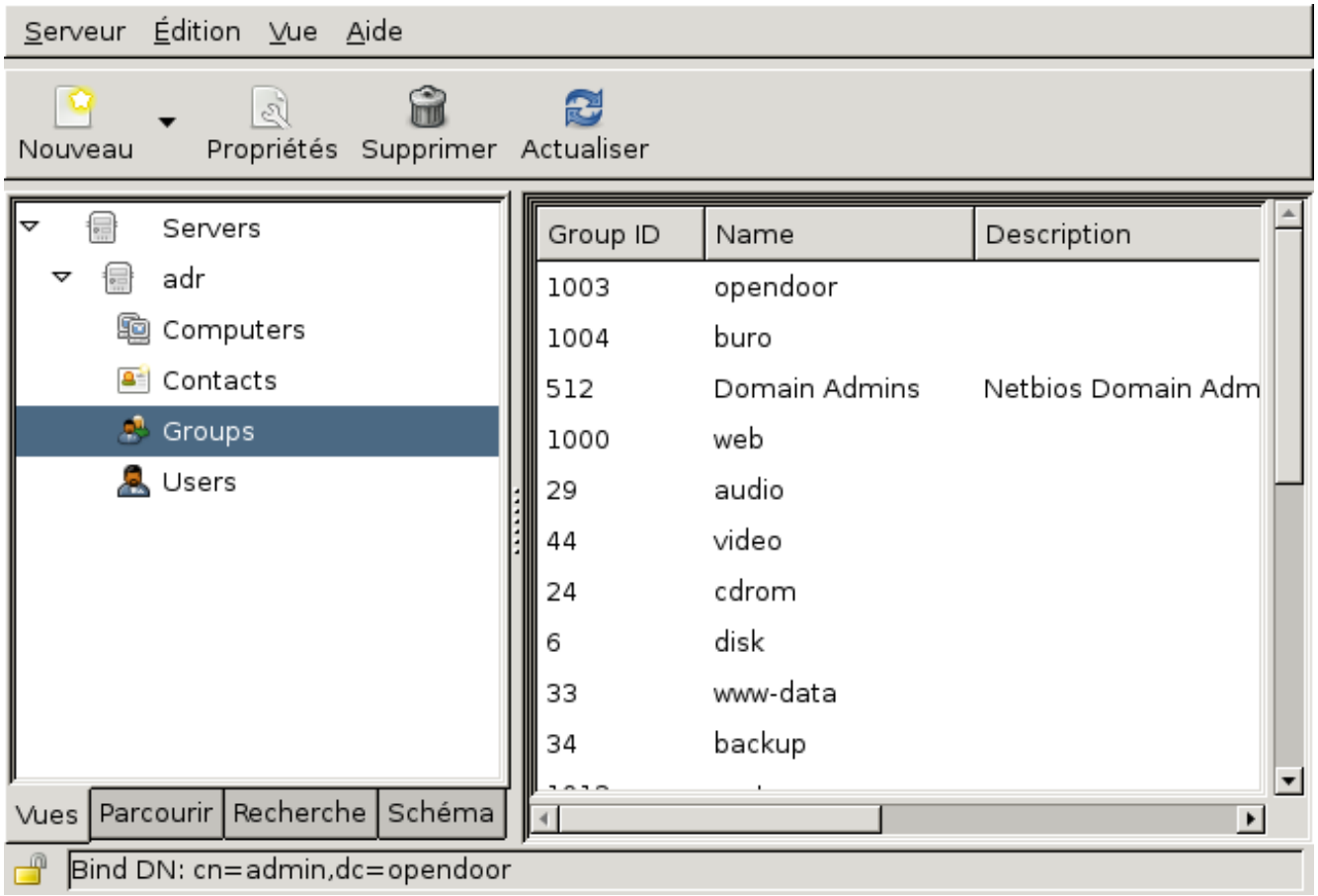
   ldappasswd options –D binddn DN

Les options peuvent être :

-A demande l'ancien mot de passe

-S demande le nouveau mot de passe

Autres clients



Interface de programmation

```
use Net::LDAP;
$ldap = Net::LDAP->new ( "ldap.opendoor.fr" ) or die "$@";
$mesg = $ldap->bind ( version => 3 );
$mesg = $ldap->bind ( "cn=admin,dc=opendoor",
          password => "zdezm",
         version => 3 );
 my $result = $ldap->search ( base    => "dc=opendoor",
                              scope   => "sub",
                              filter  => "(objectclass=person)",
                              attrs   =>  uid
                            );
          ...
```

Intégration avec Apache

Utilisation de ldap pour l'authentification :

1. Activer le module : a2enmod mod_authnz_ldap
2. Rajouter les directives :

```
AuthLDAPURL ldap://adresse:
    port?base?attribut?etendue
    ?filtre
AuthLDAPGroupAttribute (par
    defaut member |
    uniquemember)
AuthLDAPGroupAttributeIsDN on|
    off
Require valid-user | ldap-user
      | ldap-group
```

3. Relancer apache : apache2ctl graceful