Relecture du TP de Benoit Métrot des rencontres mathrice de Poitiers en mars 2008

Soit un serveur ldap openldap

master$ apt-get install slapd ldap-utils

master$ /etc/init.d/slapd stop

master$ vi /etc/ldap/slapd.conf

```
# This is the main slapd configuration file. See slapd.conf(5) for more
# info on the configuration options.
########################################################################


# Schema and objectClass definition
include         /etc/ldap/schema/core.schema
include         /etc/ldap/schema/cosine.schema
include         /etc/ldap/schema/nis.schema
include         /etc/ldap/schema/inetorgperson.schema

# Where the pid file is put. The init.d script
# will not stop the server if you change this.
pidfile         /var/run/slapd/slapd.pid

# List of arguments that were passed to the server
argsfile        /var/run/slapd/slapd.args

# Read slapd.conf(5) for possible values
loglevel        256

# Where the dynamically loaded modules are stored
modulepath  /usr/lib/ldap
moduleload  back_bdb

# The maximum number of entries that is returned for a search operation
sizelimit 500

# The tool-threads parameter sets the actual amount of cpu's that is used
# for indexing.
tool-threads 1


########################################################################
# Specific Backend Directives for bdb:
# Backend specific directives apply to this backend until another
# 'backend' directive occurs
backend          bdb


########################################################################
# Specific Directives for database #1, of type bdb:
# Database specific directives apply to this databasse until another
# 'database' directive occurs
database        bdb

# The base of your directory in database #1
suffix          "dc=mathrice,dc=prive"
```

```
# rootdn directive for specifying a superuser on the database. This is needed
# for syncrepl.
# Hashed password is generated with slappasswd, here it is mot2pass
rootdn          "cn=admin,dc=mathrice,dc=prive"
rootpw            "{SSHA}7Q7RDtX6PgeC54m85vFYwW4K/4Rbj6pL"

# Where the database file are physically stored for database #1
directory       "/var/lib/ldap"

# For the Debian package we use 2MB as default but be sure to update this
# value if you have plenty of RAM
dbconfig set_cachesize 0 2097152 0

# Sven Hartge reported that he had to set this value incredibly high
# to get slapd running at all. See http://bugs.debian.org/303057
# for more information.

# Number of objects that can be locked at the same time.
dbconfig set_lk_max_objects 1500
# Number of locks (both requested and granted)
dbconfig set_lk_max_locks 1500
# Number of lockers
dbconfig set_lk_max_lockers 1500

# Indexing options for database #1
index           objectClass eq

# Save the time that the entry gets modified, for database #1
lastmod         on

# The userPassword by default can be changed
# by the entry owning it if they are authenticated.
# Others should not be able to see it, except the
# admin entry below
access to attrs=userPassword,shadowLastChange
        by anonymous auth
        by self write
        by * none

# Everyone can read everything else.
access to *
        by * read
```

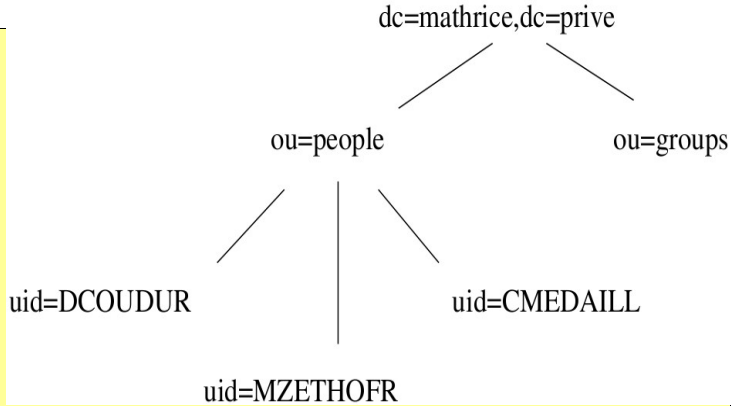
master$ slapadd -l /tmp/arbre.ldif ! slapadd quand slapd est stoppé !

arbre.ldif :

```
dn: dc=mathrice,dc=prive
dc: mathrice
objectClass: dcObject
objectClass: organizationalUnit
ou: mathrice

dn: ou=people,dc=mathrice,dc=prive
ou: people
objectClass: organizationalUnit

dn: ou=groups,dc=mathrice,dc=prive
ou: groups
objectClass: organizationalUnit
```



Soit un client ldap openldap

client$ apt-get install ldap-utils

client$ ldapsearch -x -h master -b dc=mathrice,dc=prive ’(objectClass=*)’

→ Consultation en mode anonymous

Ajout de données

User.ldif : (éventuellement produit avec migration tool

```
dn: uid=anomusu,ou=people,dc=mathrice,dc=prive
objectClass: inetOrgPerson
objectClass: posixAccount
objectClass: shadowAccount
cn: Agtpre.Nomusu
sn: Agtnom
givenName: Agtpre
uid: anomusu
uidNumber: 1001
gidNumber: 300
homeDirectory: /home/anomusu
loginShell: /bin/bash
shadowExpire: 0
userPassword: {SSHA}6gHTLCHTwZjOv/HjT//pTq94ba1HyQq1
mail: Agtpre.Nomusu@domain.tld
mail: anomusu
initials: A. N.

dn: uid=VATERRE,ou=people,dc=mathrice,dc=prive
objectClass: inetOrgPerson
objectClass: posixAccount
objectClass: shadowAccount
cn: Vac.Aterre
sn: Aterre
givenName: Vac
uid: VATERRE
uidNumber: 1002
gidNumber: 300
homeDirectory: /home/vaterre
loginShell: /bin/bash
shadowExpire: 0
userPassword: {SSHA}6gHTLCHTwZjOv/HjT//pTq94ba1HyQq1
mail: Vac.Aterre@domain.tld
mail: VATERRE
initials: V. A.

dn: uid=ZBEBERT,ou=people,dc=mathrice,dc=prive
objectClass: inetOrgPerson
objectClass: posixAccount
objectClass: shadowAccount
cn: Zino.Bebert
sn: Bebert
givenName: Zino
uid: ZBEBERT
uidNumber: 1003
gidNumber: 300
homeDirectory: /home/zbebert
loginShell: /bin/bash
shadowExpire: 0
```

```
userPassword: {SSHA}6gHTLCHTwZjOv/HjT//pTq94ba1HyQq1
mail: Zino.Bebert@domain.tld
mail: ZBEBERT
initials: Z. B.

dn: uid=JBOND,ou=people,dc=mathrice,dc=prive
objectClass: inetOrgPerson
objectClass: posixAccount
objectClass: shadowAccount
cn: James.Bond
sn: Bond
givenName: James
uid: JBOND
uidNumber: 1004
gidNumber: 300
homeDirectory: /home/jbond
loginShell: /bin/bash
shadowExpire: 0
userPassword: {SSHA}6gHTLCHTwZjOv/HjT//pTq94ba1HyQq1
mail: James.Bond@domain.tld
mail: JBOND
initials: J. B.

dn: uid=CBOUKAN,ou=people,dc=mathrice,dc=prive
objectClass: inetOrgPerson
objectClass: posixAccount
objectClass: shadowAccount
cn: Cannotte.Boukan
sn: Boukan
givenName: Cannotte
uid: CBOUKAN
uidNumber: 1005
gidNumber: 300
homeDirectory: /home/cboukan
loginShell: /bin/bash
shadowExpire: 0
userPassword: {SSHA}6gHTLCHTwZjOv/HjT//pTq94ba1HyQq1
mail: Cannotte.Boukan@domain.tld
mail: CBOUKAN
initials: C. B.

dn: uid=CCHANTEU,ou=people,dc=mathrice,dc=prive
objectClass: inetOrgPerson
objectClass: posixAccount
objectClass: shadowAccount
cn: Charme.Chanteur
sn: Chanteur
givenName: Charme
uid: CCHANTEU
uidNumber: 1006
gidNumber: 300
homeDirectory: /home/cchanteu
loginShell: /bin/bash
shadowExpire: 0
userPassword: {SSHA}6gHTLCHTwZjOv/HjT//pTq94ba1HyQq1
mail: Charme.Chanteur@domain.tld
mail: CCHANTEU
initials: C. C.

dn: uid=DCIVET,ou=people,dc=mathrice,dc=prive
objectClass: inetOrgPerson
objectClass: posixAccount
```

```
objectClass: shadowAccount
cn: D'anguilles.Civet
sn: Civet
givenName: D'anguilles
uid: DCIVET
uidNumber: 1007
gidNumber: 300
homeDirectory: /home/dcivet
loginShell: /bin/bash
shadowExpire: 0
userPassword: {SSHA}6gHTLCHTwZjOv/HjT//pTq94ba1HyQq1
mail: D'anguilles.Civet@domain.tld
mail: DCIVET
initials: D. C.

dn: uid=JDARQUE,ou=people,dc=mathrice,dc=prive
objectClass: inetOrgPerson
objectClass: posixAccount
objectClass: shadowAccount
cn: Jeanne.Darque
sn: Darque
givenName: Jeanne
uid: JDARQUE
uidNumber: 1008
gidNumber: 300
homeDirectory: /home/jdarque
loginShell: /bin/bash
shadowExpire: 0
userPassword: {SSHA}6gHTLCHTwZjOv/HjT//pTq94ba1HyQq1
mail: Jeanne.Darque@domain.tld
mail: JDARQUE
initials: J. D.

dn: uid=JDINNE,ou=people,dc=mathrice,dc=prive
objectClass: inetOrgPerson
objectClass: posixAccount
objectClass: shadowAccount
cn: James.Dinne
sn: Dinne
givenName: James
uid: JDINNE
uidNumber: 1009
gidNumber: 300
homeDirectory: /home/jdinne
loginShell: /bin/bash
shadowExpire: 0
userPassword: {SSHA}6gHTLCHTwZjOv/HjT//pTq94ba1HyQq1
mail: James.Dinne@domain.tld
mail: JDINNE
initials: J. D.

dn: uid=HDETOUR,ou=people,dc=mathrice,dc=prive
objectClass: inetOrgPerson
objectClass: posixAccount
objectClass: shadowAccount
cn: Henriette.Detour
sn: Dumans
givenName: Henriette
uid: HDETOUR
uidNumber: 1010
gidNumber: 300
homeDirectory: /home/hdetour
```

```
loginShell: /bin/bash
shadowExpire: 0
userPassword: {SSHA}6gHTLCHTwZjOv/HjT//pTq94ba1HyQq1
mail: Henriette.Detour@domain.tld
mail: HDETOUR
initials: H. D.

dn: uid=HDUMANS,ou=people,dc=mathrice,dc=prive
objectClass: inetOrgPerson
objectClass: posixAccount
objectClass: shadowAccount
cn: Henriette.Dumans
sn: Dumans
givenName: Henriette
uid: HDUMANS
uidNumber: 1011
gidNumber: 300
homeDirectory: /home/hdumans
loginShell: /bin/bash
shadowExpire: 0
userPassword: {SSHA}6gHTLCHTwZjOv/HjT//pTq94ba1HyQq1
mail: Henriette.Dumans@domain.tld
mail: HDUMANS
initials: H. D.

dn: uid=HDUPANNI,ou=people,dc=mathrice,dc=prive
objectClass: inetOrgPerson
objectClass: posixAccount
objectClass: shadowAccount
cn: Hans.Dupannier
sn: Dupannier
givenName: Hans
uid: HDUPANNI
uidNumber: 1012
gidNumber: 300
homeDirectory: /home/hdupanni
loginShell: /bin/bash
shadowExpire: 0
userPassword: {SSHA}6gHTLCHTwZjOv/HjT//pTq94ba1HyQq1
mail: Hans.Dupannier@domain.tld
mail: HDUPANNI
initials: H. D.

dn: uid=RDUPIN,ou=people,dc=mathrice,dc=prive
objectClass: inetOrgPerson
objectClass: posixAccount
objectClass: shadowAccount
cn: Roi.Dupin
sn: Dupin
givenName: Roi
uid: RDUPIN
uidNumber: 1013
gidNumber: 300
homeDirectory: /home/rdupin
loginShell: /bin/bash
shadowExpire: 0
userPassword: {SSHA}6gHTLCHTwZjOv/HjT//pTq94ba1HyQq1
mail: Roi.Dupin@domain.tld
mail: RDUPIN
initials: R. D.

dn: uid=CELPERE,ou=people,dc=mathrice,dc=prive
```

```
objectClass: inetOrgPerson
objectClass: posixAccount
objectClass: shadowAccount
cn: Cecile.Elpere
sn: Elmaquille
givenName: Cecile
uid: CELPERE
uidNumber: 1014
gidNumber: 300
homeDirectory: /home/celpere
loginShell: /bin/bash
shadowExpire: 0
userPassword: {SSHA}6gHTLCHTwZjOv/HjT//pTq94ba1HyQq1
mail: Cecile.Elpere@domain.tld
mail: CELPERE
initials: C. E.

dn: uid=MENC-BOU,ou=people,dc=mathrice,dc=prive
objectClass: inetOrgPerson
objectClass: posixAccount
objectClass: shadowAccount
cn: Monnaie.Enc-bourse
sn: Enc-bourse
givenName: Monnaie
uid: MENC-BOU
uidNumber: 1015
gidNumber: 300
homeDirectory: /home/menc-bou
loginShell: /bin/bash
shadowExpire: 0
userPassword: {SSHA}6gHTLCHTwZjOv/HjT//pTq94ba1HyQq1
mail: Monnaie.Enc-bourse@domain.tld
mail: MENC-BOU
initials: M. E.

dn: uid=OETY,ou=people,dc=mathrice,dc=prive
objectClass: inetOrgPerson
objectClass: posixAccount
objectClass: shadowAccount
cn: Olive.Ety
sn: Ety
givenName: Olive
uid: OETY
uidNumber: 1016
gidNumber: 300
homeDirectory: /home/oety
loginShell: /bin/bash
shadowExpire: 0
userPassword: {SSHA}6gHTLCHTwZjOv/HjT//pTq94ba1HyQq1
mail: Olive.Ety@domain.tld
mail: OETY
initials: O. E.

dn: uid=AFONCTIO,ou=people,dc=mathrice,dc=prive
objectClass: inetOrgPerson
objectClass: posixAccount
objectClass: shadowAccount
cn: Arcive.Fonction
sn: Fonction
givenName: Arcive
uid: AFONCTIO
uidNumber: 1017
```

```
gidNumber: 300
homeDirectory: /home/afonctio
loginShell: /bin/bash
shadowExpire: 0
userPassword: {SSHA}6gHTLCHTwZjOv/HjT//pTq94ba1HyQq1
mail: Arcive.Fonction@domain.tld
mail: AFONCTIO
initials: A. F.

dn: uid=EGAMELLE,ou=people,dc=mathrice,dc=prive
objectClass: inetOrgPerson
objectClass: posixAccount
objectClass: shadowAccount
cn: Etbidon.Gamelle
sn: Gamelle
givenName: Etbidon
uid: EGAMELLE
uidNumber: 1018
gidNumber: 300
homeDirectory: /home/egamelle
loginShell: /bin/bash
shadowExpire: 0
userPassword: {SSHA}6gHTLCHTwZjOv/HjT//pTq94ba1HyQq1
mail: Etbidon.Gamelle@domain.tld
mail: EGAMELLE
initials: E. G.

dn: uid=MGUIDE,ou=people,dc=mathrice,dc=prive
objectClass: inetOrgPerson
objectClass: posixAccount
objectClass: shadowAccount
cn: Moy.Guide
sn: Guide
givenName: Moy
uid: MGUIDE
uidNumber: 1019
gidNumber: 300
homeDirectory: /home/mguide
loginShell: /bin/bash
shadowExpire: 0
userPassword: {SSHA}6gHTLCHTwZjOv/HjT//pTq94ba1HyQq1
mail: Moy.Guide@domain.tld
mail: MGUIDE
initials: M. G.

dn: uid=PINUTILE,ou=people,dc=mathrice,dc=prive
objectClass: inetOrgPerson
objectClass: posixAccount
objectClass: shadowAccount
cn: Present.Inutile
sn: Inutile
givenName: Present
uid: PINUTILE
uidNumber: 1020
gidNumber: 300
homeDirectory: /home/pinutile
loginShell: /bin/bash
shadowExpire: 0
userPassword: {SSHA}6gHTLCHTwZjOv/HjT//pTq94ba1HyQq1
mail: Present.Inutile@domain.tld
mail: PINUTILE
initials: P. I.
```

```
dn: uid=DJOLIVET,ou=people,dc=mathrice,dc=prive
objectClass: inetOrgPerson
objectClass: posixAccount
objectClass: shadowAccount
cn: Dominique.Jolivet
sn: Jolivet
givenName: Dominique
uid: DJOLIVET
uidNumber: 1021
gidNumber: 300
homeDirectory: /home/djolivet
loginShell: /bin/bash
shadowExpire: 0
userPassword: {SSHA}6gHTLCHTwZjOv/HjT//pTq94ba1HyQq1
mail: Dominique.Jolivet@domain.tld
mail: DJOLIVET
initials: D. J.

dn: uid=LJULY,ou=people,dc=mathrice,dc=prive
objectClass: inetOrgPerson
objectClass: posixAccount
objectClass: shadowAccount
cn: Larousse.July
sn: July
givenName: Larousse
uid: LJULY
uidNumber: 1022
gidNumber: 300
homeDirectory: /home/ljuly
loginShell: /bin/bash
shadowExpire: 0
userPassword: {SSHA}6gHTLCHTwZjOv/HjT//pTq94ba1HyQq1
mail: Larousse.July@domain.tld
mail: LJULY
initials: L. J.

dn: uid=RMANAPAN,ou=people,dc=mathrice,dc=prive
objectClass: inetOrgPerson
objectClass: posixAccount
objectClass: shadowAccount
cn: Roche.Manapany
sn: Manapany
givenName: Roche
uid: RMANAPAN
uidNumber: 1023
gidNumber: 300
homeDirectory: /home/rmanapan
loginShell: /bin/bash
shadowExpire: 0
userPassword: {SSHA}6gHTLCHTwZjOv/HjT//pTq94ba1HyQq1
mail: Roche.Manapany@domain.tld
mail: RMANAPAN
initials: R. M.

dn: uid=TNOUNOU,ou=people,dc=mathrice,dc=prive
objectClass: inetOrgPerson
objectClass: posixAccount
objectClass: shadowAccount
cn: Tata.Nounou
sn: Nounou
givenName: Tata
```

```
uid: TNOUNOU
uidNumber: 1024
gidNumber: 300
homeDirectory: /home/tnounou
loginShell: /bin/bash
shadowExpire: 0
userPassword: {SSHA}6gHTLCHTwZjOv/HjT//pTq94ba1HyQq1
mail: Tata.Nounou@domain.tld
mail: TNOUNOU
initials: T. N.

dn: uid=EMIEUT,ou=people,dc=mathrice,dc=prive
objectClass: inetOrgPerson
objectClass: posixAccount
objectClass: shadowAccount
cn: Eva.Mieut
sn: Pabien
givenName: Eva
uid: EMIEUT
uidNumber: 1025
gidNumber: 300
homeDirectory: /home/emieut
loginShell: /bin/bash
shadowExpire: 0
userPassword: {SSHA}6gHTLCHTwZjOv/HjT//pTq94ba1HyQq1
mail: Eva.Mieut@domain.tld
mail: EMIEUT
initials: E. M.

dn: uid=APECHE,ou=people,dc=mathrice,dc=prive
objectClass: inetOrgPerson
objectClass: posixAccount
objectClass: shadowAccount
cn: Augros.Peche
sn: Peche
givenName: Augros
uid: APECHE
uidNumber: 1026
gidNumber: 300
homeDirectory: /home/apeche
loginShell: /bin/bash
shadowExpire: 0
userPassword: {SSHA}6gHTLCHTwZjOv/HjT//pTq94ba1HyQq1
mail: Augros.Peche@domain.tld
mail: APECHE
initials: A. P.

dn: uid=GPLUMIER,ou=people,dc=mathrice,dc=prive
objectClass: inetOrgPerson
objectClass: posixAccount
objectClass: shadowAccount
cn: Gomme.Plumier
sn: Plumier
givenName: Gomme
uid: GPLUMIER
uidNumber: 1027
gidNumber: 300
homeDirectory: /home/gplumier
loginShell: /bin/bash
shadowExpire: 0
userPassword: {SSHA}6gHTLCHTwZjOv/HjT//pTq94ba1HyQq1
mail: Gomme.Plumier@domain.tld
```

```
mail: GPLUMIER
initials: G. P.

dn: uid=RPRECIEU,ou=people,dc=mathrice,dc=prive
objectClass: inetOrgPerson
objectClass: posixAccount
objectClass: shadowAccount
cn: Ridicule.Precieuse
sn: Precieuse
givenName: Ridicule
uid: RPRECIEU
uidNumber: 1028
gidNumber: 300
homeDirectory: /home/rprecieu
loginShell: /bin/bash
shadowExpire: 0
userPassword: {SSHA}6gHTLCHTwZjOv/HjT//pTq94ba1HyQq1
mail: Ridicule.Precieuse@domain.tld
mail: RPRECIEU
initials: R. P.

dn: uid=CQUALIF,ou=people,dc=mathrice,dc=prive
objectClass: inetOrgPerson
objectClass: posixAccount
objectClass: shadowAccount
cn: Contrat.Qualif
sn: Qualif
givenName: Contrat
uid: CQUALIF
uidNumber: 1029
gidNumber: 300
homeDirectory: /home/cqualif
loginShell: /bin/bash
shadowExpire: 0
userPassword: {SSHA}6gHTLCHTwZjOv/HjT//pTq94ba1HyQq1
mail: Contrat.Qualif@domain.tld
mail: CQUALIF
initials: C. Q.

dn: uid=NLAVACHE,ou=people,dc=mathrice,dc=prive
objectClass: inetOrgPerson
objectClass: posixAccount
objectClass: shadowAccount
cn: Normande.Lavache
sn: Quirit
givenName: Normande
uid: NLAVACHE
uidNumber: 1030
gidNumber: 300
homeDirectory: /home/nlavache
loginShell: /bin/bash
shadowExpire: 0
userPassword: {SSHA}6gHTLCHTwZjOv/HjT//pTq94ba1HyQq1
mail: Normande.Lavache@domain.tld
mail: NLAVACHE
initials: N. L.

dn: uid=CMEDAILL,ou=people,dc=mathrice,dc=prive
objectClass: inetOrgPerson
objectClass: posixAccount
objectClass: shadowAccount
cn: Capus.Medaille
```

```
sn: Recompense
givenName: Capus
uid: CMEDAILL
uidNumber: 1031
gidNumber: 300
homeDirectory: /home/cmedaill
loginShell: /bin/bash
shadowExpire: 0
userPassword: {SSHA}6gHTLCHTwZjOv/HjT//pTq94ba1HyQq1
mail: Capus.Medaille@domain.tld
mail: CMEDAILL
initials: C. M.

dn: uid=PREVEREN,ou=people,dc=mathrice,dc=prive
objectClass: inetOrgPerson
objectClass: posixAccount
objectClass: shadowAccount
cn: Pere.Reverend
sn: Reverend
givenName: Pere
uid: PREVEREN
uidNumber: 1032
gidNumber: 300
homeDirectory: /home/preveren
loginShell: /bin/bash
shadowExpire: 0
userPassword: {SSHA}6gHTLCHTwZjOv/HjT//pTq94ba1HyQq1
mail: Pere.Reverend@domain.tld
mail: PREVEREN
initials: P. R.

dn: uid=TPICADOR,ou=people,dc=mathrice,dc=prive
objectClass: inetOrgPerson
objectClass: posixAccount
objectClass: shadowAccount
cn: Torero.Picador
sn: Spania
givenName: Torero
uid: TPICADOR
uidNumber: 1033
gidNumber: 300
homeDirectory: /home/tpicador
loginShell: /bin/bash
shadowExpire: 0
userPassword: {SSHA}6gHTLCHTwZjOv/HjT//pTq94ba1HyQq1
mail: Torero.Picador@domain.tld
mail: TPICADOR
initials: T. P.

dn: uid=STEMPORA,ou=people,dc=mathrice,dc=prive
objectClass: inetOrgPerson
objectClass: posixAccount
objectClass: shadowAccount
cn: Sandrine.Temporaire
sn: Temporaire
givenName: Sandrine
uid: STEMPORA
uidNumber: 1034
gidNumber: 300
homeDirectory: /home/stempora
loginShell: /bin/bash
shadowExpire: 0
```

```
userPassword: {SSHA}6gHTLCHTwZjOv/HjT//pTq94ba1HyQq1
mail: Sandrine.Temporaire@domain.tld
mail: STEMPORA
initials: S. T.

dn: uid=PTEMPS,ou=people,dc=mathrice,dc=prive
objectClass: inetOrgPerson
objectClass: posixAccount
objectClass: shadowAccount
cn: Partiel.Temps
sn: Temps
givenName: Partiel
uid: PTEMPS
uidNumber: 1035
gidNumber: 300
homeDirectory: /home/ptemps
loginShell: /bin/bash
shadowExpire: 0
userPassword: {SSHA}6gHTLCHTwZjOv/HjT//pTq94ba1HyQq1
mail: Partiel.Temps@domain.tld
mail: PTEMPS
initials: P. T.

dn: uid=ATERRIEU,ou=people,dc=mathrice,dc=prive
objectClass: inetOrgPerson
objectClass: posixAccount
objectClass: shadowAccount
cn: Alex.Terrieur
sn: Terrieur
givenName: Alex
uid: ATERRIEU
uidNumber: 1036
gidNumber: 300
homeDirectory: /home/aterrieu
loginShell: /bin/bash
shadowExpire: 0
userPassword: {SSHA}6gHTLCHTwZjOv/HjT//pTq94ba1HyQq1
mail: Alex.Terrieur@domain.tld
mail: ATERRIEU
initials: A. T.

dn: uid=MTILLEUL,ou=people,dc=mathrice,dc=prive
objectClass: inetOrgPerson
objectClass: posixAccount
objectClass: shadowAccount
cn: Medor.Tilleul
sn: Tilleul
givenName: Medor
uid: MTILLEUL
uidNumber: 1037
gidNumber: 300
homeDirectory: /home/mtilleul
loginShell: /bin/bash
shadowExpire: 0
userPassword: {SSHA}6gHTLCHTwZjOv/HjT//pTq94ba1HyQq1
mail: Medor.Tilleul@domain.tld
mail: MTILLEUL
initials: M. T.

dn: uid=DCOUDUR,ou=people,dc=mathrice,dc=prive
objectClass: inetOrgPerson
objectClass: posixAccount
```

```
objectClass: shadowAccount
cn: Drole de.Coudur
sn: Tronche
givenName: Drole de
uid: DCOUDUR
uidNumber: 1038
gidNumber: 300
homeDirectory: /home/dcoudur
loginShell: /bin/bash
shadowExpire: 0
userPassword: {SSHA}6gHTLCHTwZjOv/HjT//pTq94ba1HyQq1
mail: Drole de.Coudur@domain.tld
mail: DCOUDUR
initials: D. C.

dn: uid=MZETHOFR,ou=people,dc=mathrice,dc=prive
objectClass: inetOrgPerson
objectClass: posixAccount
objectClass: shadowAccount
cn: Melanie.Zethofrais
sn: Zethofrais
givenName: Melanie
uid: MZETHOFR
uidNumber: 1039
gidNumber: 300
homeDirectory: /home/mzethofr
loginShell: /bin/bash
shadowExpire: 0
userPassword: {SSHA}6gHTLCHTwZjOv/HjT//pTq94ba1HyQq1
mail: Melanie.Zethofrais@domain.tld
mail: MZETHOFR
initials: M. Z.
```

client$ ldapadd -x -W -D cn=admin,dc=mathrice,dc=prive -h master -f /tmp/user.ldif

Demande le mot de passe du rootdn et ajoute tous les dn

Pour s’exercer à manipuler les données de l’annuaire :

-Ajouter une entrée dans la branche people

-Créer des groupes d’utilisateurs

-Rechercher les personnes dont le nom (attribut uid) commence par NL

-Supprimer une entrée de l’annuaire (cf. man ldapdelete).

Sécurisation des échanges : couche SSL

```
Voir http://islandlinux.org/howto/installing-secure-ldap-openldap-ssl-ubuntu-using-self-signed-certificate
```

master$ apt-get install openssl ca-certificates

Génération d'un certificat auto-signé :

master$ /usr/lib/ssl/misc/CA.pl -newcert

Suppression de la passphrase dans la clé privée :

master$ openssl rsa -in newkey.pem -out newkey-unlock.pem

Installation du certificat et de sa clé privée

master$ mv newcert.pem /etc/ldap/slapd-crt.pem

master$ mv newkey-unlock.pem /etc/ldap/slapd-key.pem

master$ chmod 644 /etc/ldap/slapd-crt.pem

master$ chmod 600 /etc/ldap/slapd-key.pem

master$ chown openldap.openldap /etc/ldap/slapd-*.pem

Ajouter le code suivant à slapd.conf

```
# TLSCipherSuite        HIGH  → Inutile avec Debian Lenny
TLSCertificateFile    /etc/ldap/slapd-crt.pem
TLSCertificateKeyFile /etc/ldap/slapd-key.pem
```

master$ /etc/init.d/slapd restart

Adaptation du client pour qu'il ne vérifie pas le certificat
Client$ vi /etc/ldap/ldap.conf
→ Mettre TLS_REQCERT never
Client$ ldapsearch -x -Z -h master -b ou=people,dc=mathrice,dc=prive '(givenName=Mel*)'
→ Réponses...

Authentification avec un client Linux

-Réglage de NSS
-Configuration de PAM
Client$ apt-get install libnss-ldap
Client$ vi /etc/libnss-ldap.conf

```
#
# This is the configuration file for the LDAP nameservice
# switch library and the LDAP PAM module.
#
# PADL Software
# http://www.padl.com
#


# The distinguished name of the search base.
base dc=mathrice,dc=prive

# Specify your LDAP server
uri ldap://192.168.1.2/

# The LDAP version to use (defaults to 3
ldap_version 3
```

```
# The port.
port 389

# The search scope.
scope sub

# Search timelimit
timelimit 30

# Bind/connect timelimit
bind_timelimit 10

# Reconnect policy:
#  hard_open: reconnect to DSA with exponential backoff if
#             opening connection failed
#  hard_init: reconnect to DSA with exponential backoff if
#             initializing connection failed
#  hard:      alias for hard_open
#  soft:      return immediately on server failure
bind_policy hard

# Connection policy:
#  persist:   DSA connections are kept open (default)
#  oneshot:   DSA connections destroyed after request
nss_connect_policy persist

# Idle timelimit; client will close connections
# (nss_ldap only) if the server has not been contacted
# for the number of seconds specified below.
idle_timelimit 3600

# RFC2307bis naming contexts
# Syntax:
# nss_base_XXX          base?scope?filter
# where scope is {base,one,sub}
# and filter is a filter to be &'d with the default filter.
nss_base_passwd   ou=people,dc=mathrice,dc=prive?sub
nss_base_shadow   ou=people,dc=mathrice,dc=prive?sub
nss_base_group    ou=groups,dc=mathrice,dc=prive?sub

# OpenLDAP SSL mechanism
# start_tls mechanism uses the normal LDAP port, LDAPS typically 636
ssl start_tls
#ssl on
```

Client$ vi /etc/nsswitch.conf

```
passwd: files ldap
group:  files ldap
shadow: files ldap
```

Client$ apt-get install libpam-ldap

Client$ vi /etc/pam_ldap.conf

```
#
# This is the configuration file for the LDAP nameservice
# switch library and the LDAP PAM module.
#
# PADL Software
# http://www.padl.com
#

# The distinguished name of the search base.
base dc=mathrice,dc=prive

# Specify your LDAP server
uri ldap://192.168.1.2/

# The LDAP version to use (defaults to 3
# if supported by client library)
ldap_version 3

# The port
port 389

# The search scope.
scope sub

# Search timelimit
timelimit 30

# Bind/connect timelimit
bind_timelimit 10

# Reconnect policy: hard (default) will retry connecting to
# the software with exponential backoff, soft will fail
# immediately.
bind_policy hard

# Idle timelimit; client will close connections
# (nss_ldap only) if the server has not been contacted
# for the number of seconds specified below.
idle_timelimit 3600

# Filter to AND with uid=%s
pam_filter objectclass=posixAccount

# The user ID attribute (defaults to uid)
pam_login_attribute uid

# Do not hash the password at all; presume
# the directory server will do it, if
# necessary. This is the default.
pam_password crypt

# OpenLDAP SSL mechanism
# start_tls mechanism uses the normal LDAP port, LDAPS typically 636
ssl start_tls
#ssl on
```

Client$ vi /etc/pam.d/gdm

```
#%PAM-1.0
auth  requisite   pam_nologin.so
auth  required    pam_env.so readenv=1
auth  required    pam_env.so readenv=1 envfile=/etc/default/locale
auth    sufficient      pam_ldap.so
auth  required        pam_unix.so nullok_secure try_first_pass

@include common-account
session required        pam_limits.so
session required  pam_mkhomedir.so umask=0022
@include common-session
@include common-password
```

Configuration de PAM pour ssh

Client$ vi /etc/pam.d/ssh

```
# PAM configuration for the Secure Shell service

# Read environment variables from /etc/environment and
# /etc/security/pam_env.conf.
auth       required     pam_env.so # [1]
# In Debian 4.0 (etch), locale-related environment variables were moved to
# /etc/default/locale, so read that as well.
auth       required     pam_env.so envfile=/etc/default/locale

# LDAP Authentication
auth  sufficient  pam_ldap.so

# Standard Un*x authentication.
auth    required        pam_unix.so nullok_secure try_first_pass

# Disallow non-root logins when /etc/nologin exists.
account    required     pam_nologin.so

# Uncomment and edit /etc/security/access.conf if you need to set complex
# access limits that are hard to express in sshd_config.
# account  required     pam_access.so

# Standard Un*x authorization.
@include common-account

# Standard Un*x session setup and teardown.
@include common-session

# Print the message of the day upon successful login.
session    optional     pam_motd.so # [1]

# Print the status of the user's mailbox upon successful login.
session    optional     pam_mail.so standard noenv # [1]

# Set up user limits from /etc/security/limits.conf.
session    required     pam_limits.so

# Set up SELinux capabilities (need modified pam)
# session  required     pam_selinux.so multiple

# Standard Un*x password updating.
@include common-password
```

Changement du mot de passe via PAM

Client$ vi /etc/pam.d/passwd

```
#
# The PAM configuration file for the Shadow `passwd' service
#

password   sufficient pam_ldap.so
password   required   pam_unix.so nullok obscure min=4 max=8 md5
```

Réplication → Utilisation de syncrepl

Ajout d'un utilisateur dédié

Master$ vi ~/syncuser.ldif

```
dn: cn=syncuser,dc=mathrice,dc=prive
objectClass: organizationalPerson
cn: syncuser
sn: syncuser
userPassword: {SSHA}7Q7RDtX6PgeC54m85vFYwW4K/4Rbj6pL
```

Master$ ldapadd -x -Z -W -D cn=admin,dc=mathrice,dc=prive -h master -f ~/syncuser.ldif

Master$ vi /etc/ldap.slapd.conf # pour ajouter ACL

```
access to attrs=userPassword,shadowLastChange
  by anonymous auth
  by self write
  by dn="cn=syncuser,dc=mathrice,dc=prive" read
  by * none
```

Master$ vi /etc/ldap.slapd.conf # pour ajouter syncprov

```
moduleload  syncprov
```

Master$ vi /etc/ldap.slapd.conf # pour activer syncprov

```
overlay syncprov
syncprov-checkpoint 100 10
syncprov-sessionlog 100
```

Configuration du réplica

Replica$ apt-get install ldap-utils slapd openssl

Replica$ /usr/lib/ssl/misc/CA.pl -newcert → L'installer dans /etc/ldap

Suppression de la passphrase dans la clé́ privée :

$ openssl rsa -in newkey.pem -out newkey-unlock.pem

Installation du certificat et de sa clé privée

Replica$ mv newcert.pem /etc/ldap/slapd-crt.pem

Replica$ mv newkey-unlock.pem /etc/ldap/slapd-key.pem

Replica$ chmod 644 /etc/ldap/slapd-crt.pem

Replica$ chmod 600 /etc/ldap/slapd-key.pem

Replica$ chown openldap.openldap /etc/ldap/slapd-*.pem

Ajouter le code suivant à slapd.conf

```
# TLSCipherSuite        HIGH  → Inutile avec Debian Lenny
TLSCertificateFile    /etc/ldap/slapd-crt.pem
TLSCertificateKeyFile /etc/ldap/slapd-key.pem
```

Replica$ /etc/init.d/slapd stop

Replica$ vi /etc/ldap/slapd.conf

```
# This is the main slapd configuration file. See slapd.conf(5) for more
# info on the configuration options.
########################################################################


# Schema and objectClass definition
include         /etc/ldap/schema/core.schema
include         /etc/ldap/schema/cosine.schema
include         /etc/ldap/schema/nis.schema
include         /etc/ldap/schema/inetorgperson.schema

# Where the pid file is put. The init.d script
# will not stop the server if you change this.
pidfile         /var/run/slapd/slapd.pid

# List of arguments that were passed to the server
argsfile        /var/run/slapd/slapd.args

# Read slapd.conf(5) for possible values
loglevel        256

# Where the dynamically loaded modules are stored
modulepath  /usr/lib/ldap
moduleload  back_bdb

# The maximum number of entries that is returned for a search operation
sizelimit 500

# The tool-threads parameter sets the actual amount of cpu's that is used
# for indexing.
tool-threads 1

# TLS Options
TLSCipherSuite           HIGH
TLSCertificateFile       /etc/ldap/slapd-crt.pem
TLSCertificateKeyFile    /etc/ldap/slapd-key.pem


########################################################################
# Specific Backend Directives for bdb:
# Backend specific directives apply to this backend until another
# 'backend' directive occurs
backend          bdb
checkpoint 512 30


########################################################################
# Specific Directives for database #1, of type bdb:
# Database specific directives apply to this databasse until another
# 'database' directive occurs
database        bdb

# The base of your directory in database #1
suffix          "dc=mathrice,dc=prive"
```

```
# rootdn directive for specifying a superuser on the database. This is needed
# for syncrepl.
# Hashed password is generated with slappasswd, here it is mot2pass
rootdn          "cn=admin,dc=mathrice,dc=prive"
rootpw           "{SSHA}7Q7RDtX6PgeC54m85vFYwW4K/4Rbj6pL"

# Where the database file are physically stored for database #1
directory       "/var/lib/ldap"

# For the Debian package we use 2MB as default but be sure to update this
# value if you have plenty of RAM
dbconfig set_cachesize 0 2097152 0

# Sven Hartge reported that he had to set this value incredibly high
# to get slapd running at all. See http://bugs.debian.org/303057
# for more information.

# Number of objects that can be locked at the same time.
dbconfig set_lk_max_objects 1500
# Number of locks (both requested and granted)
dbconfig set_lk_max_locks 1500
# Number of lockers
dbconfig set_lk_max_lockers 1500

# Indexing options for database #1
index           objectClass eq

# Save the time that the entry gets modified, for database #1
lastmod         on

# This directory is a replica
syncrepl rid=123
         provider=ldap://192.168.1.2:389
         type=refreshOnly
         interval=00:00:01:00
         searchbase="dc=mathrice,dc=prive"
         filter="(objectClass=*)"
         scope=sub
         schemachecking=on
         bindmethod=simple
       starttls=yes
         binddn="cn=syncuser,dc=mathrice,dc=prive"
         credentials=mot2pass
updateref ldap://master/

# The userPassword by default can be changed
# by the entry owning it if they are authenticated.
# Others should not be able to see it, except the
# admin entry below
access to attrs=userPassword,shadowLastChange
        by anonymous auth
        by self write
        by * none

# Everyone can read everything else.
access to *
        by * read
```

Replica$ /etc/init.d/slapd start

Client$ vi /etc/pam-ldap.conf → Modifier pour qu'apparaisse

```
uri ldap://192.168.1.2/ ldap://192.168.1.3/
```

Tester le client après arrêt du master....