TP N°2 LDAP

CORRECTION

Master 2 I2L

Année 2009/2010

D'après la version de Jean-Christophe Soulié (2007-2008)

D. Duvivier
LIL – Université du Littoral Côte d'Opale
duvivier@lil.univ-littoral.fr

1 Reprenons au début

Sauvegarder votre fichier `slapd.conf`, nous allons en utiliser un autre. Vous pouvez même détruire les fichiers de la base LDAP après avoir faire une sauvegarde :

```
# /etc/init.d/slapd stop
# mkdir /var/lib/ldap/copie
# cp /var/lib/ldap/* /var/lib/ldap/copie
# rm /var/lib/ldap/*
```

Nous allons maintenant travailler sur le DIT (présenté dans l'énoncé de TP2) relatif à la hiérarchie d'un carnet d'adresse d'une entreprise quelconque…

Dans un premier temps, construisons un fichier `slapd.conf` qui, hormis les déclarations classiques, défini le `dn` de l'arbre (juste ça, pas d'ACLs pour l'instant) :

```
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        255

modulepath      /usr/lib/ldap
moduleload      back_hdb

sizelimit 500
tool-threads 1

backend         hdb
database        hdb
suffix          "dc=exemple,dc=fr"

rootdn          "cn=admin,dc=exemple,dc=fr"
rootpw          "{CRYPT}J9NQ/M7KbU9Ak"

directory       "/var/lib/ldap"
dbconfig set_cachesize 0 16777216 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
```

La base n'existe pas encore, mais nous pouvons tester le fichier de configuration, à condition d'utiliser l'option « -u » de slaptest :

```
# slaptest -u -f /etc/ldap/slapd.conf
config file testing succeeded
```

Dans la commande ci-dessus, n'oubliez pas l'option « -u » sinon une base « incorrecte » est créée (il faudra de nouveau la supprimer) et vous obtenez des messages d'erreur.

Vous pouvez vérifier que tout marche bien avec la commande :

```
# slapd -d 5 -h ldap://localhost:389 -f /etc/ldap/slapd.conf
-----> <CTRL C> pour stopper !
```

Remarque : si la base a été détruire, le fait de relancer le serveur LDAP regénère une base dans /var/lib/ldap, mais elle appartient à root:root. Il faut corriger cela, et on en profite pour générer l'index :

```
# chown openldap:openldap /var/lib/ldap/*
# slapindex
```

Remarque 2 : de manière générale, attention aux copier/coller entre les commandes présentées dans l'énoncé et les shells car le caractère « moins/tiret » (-) est parfois remplacé par un quadratin (–) et ce n'est pas évident à détecter --> en cas d'erreur lors d'un copier/coller, vérfiez si le problème ne vient pas de là !

2 Définition de la structure

Maintenant que le serveur a été initialisé proprement, nous allons définir la structure qui va être utilisée pour rentrer des personnes :

```
dn: dc=exemple,dc=fr
dc: exemple
description: My wonderful company as much text as you want to place
 in this line up to 32K continuation data for the line above must
 have <CR> or <CR><LF> i.e. ENTER works
 on both Windows and *nix system - new line MUST begin with ONE SPACE
objectClass: dcObject
objectClass: organization
o: Example, Inc
```

Stockez ce texte dans un fichier LDIF (structure1.ldif) et ajouter le tout dans la base LDAP (avec `ldapadd`) :

```
# ldapadd -W -D "cn=admin,dc=exemple,dc=fr" -x -H ldap://localhost -f structure1.ldif
Enter LDAP Password:
ldap_sasl_bind(SIMPLE): Can't contact LDAP server (-1)
```

Oups ! Il ne faut pas oublier de lancer le serveur LDAP :

```
# /etc/init.d/slapd start
Starting OpenLDAP: slapd.
# tail /var/log/syslog
  ...
# pidof slapd
  ...
# ldapadd -W -D "cn=admin,dc=exemple,dc=fr" -x -H ldap://localhost -f structure1.ldif
Enter LDAP Password:
adding new entry "dc=exemple,dc=fr"
```

Maintenant, définissez un fichier LDIF (structure2.ldif) qui permet de définir le niveau « `ou` » (Organizational Unit) dans la hiérarchie :

```
dn: ou=people, dc=exemple,dc=fr
ou: people
description: All people in organisation
objectclass: organizationalunit
```

Puis on ajoute à la base :

```
# ldapadd -W -D "cn=admin,dc=exemple,dc=fr" -x -H ldap://localhost -f structure2.ldif
Enter LDAP Password:
adding new entry "ou=people, dc=exemple,dc=fr"
```

Faites une sauvegarde de la base à l'aide de slapcat et après avoir stoppé le serveur (cf. tp1).

3 Ajout de personnes

On peut maintenant ajouter des personnes pour peupler notre annuaire via un fichier LDIF permettant de rentrer les informations suivantes pour les 3 personnes selon les paramètres définis dans l'énoncé de TP2 :

```
## ADD another single entry to people level

dn: cn=Robert Smith,ou=people,dc=exemple,dc=fr
objectclass: inetOrgPerson
cn: Robert Smith
cn: Robert J Smith
cn: bob  smith
sn: smith
uid: rjsmith
userpassword: rJsmitH
carlicense: HISCAR 123
homephone: 555-111-2222
mail: r.smith@exemple.fr
mail: rsmith@exemple.fr
mail: bob.smith@exemple.fr
description: swell guy
ou: Human Resources

## ADD another single entry to people level

dn: cn=John Smith,ou=people,dc=exemple,dc=fr
objectclass: inetOrgPerson
cn: John Smith
cn: John J Smith
sn: Smith
uid: jsmith
userpassword: jSmitH
carlicense: HISCAR 124
homephone: 555-111-2223
mail: j.smith@example.com
mail: jsmith@example.com
mail: john.smith@example.com
ou: Sales

## ADD another single entry to people level

dn: cn=Sheri Smith,ou=people,dc=exemple,dc=fr
objectclass: inetOrgPerson
cn: Sheri Smith
sn: smith
uid: ssmith
userpassword: sSmitH
carlicense: HERCAR 125
homephone: 555-111-2225
mail: s.smith@example.com
mail: ssmith@example.com
mail: sheri.smith@example.com
ou: IT
```

Puis on ajoute à la base :

```
# ldapadd -W -D "cn=admin,dc=exemple,dc=fr" -x -H ldap://localhost -f structure3.ldif
Enter LDAP Password:
adding new entry "cn=Robert Smith,ou=people,dc=exemple,dc=fr"
adding new entry "cn=John Smith,ou=people,dc=exemple,dc=fr"
adding new entry "cn=Sheri Smith,ou=people,dc=exemple,dc=fr"
```

Faites une sauvegarde de la base à l'aide de slapcat et après avoir stoppé le serveur (cf. tp1).

4 Modification

Nous allons maintenant modifier la personne : « Robert Smith » :

- On lui rajoute un nouveau titre : Chef de Département
- On lui rajoute deux nouveaux numéros de téléphone professionnels : 555-555-1212 et 212
- On lui modifie son login en : rjosmith
- On lui remplace ses mails par : robert.smith@exemple.fr et bob.smith@exemple.fr
- Et pour finir, comme il est chef maintenant, on lui enlève sa description, pas très élogieuse il est vrai

Créez les fichiers LDIF associés à chaque modification et vérifiez que tout s'est bien passé. Nous pouvons également aller plus vite en rassemblant les modifications dans un seul fichier LDIF (structure4modif.ldif) :

```
## MODIFY the Robert Smith entry

dn: cn=Robert Smith,ou=people,dc=exemple,dc=fr
changetype: modify
add: title
title: Department Manager
-
add: telephonenumber
telephonenumber: 555-555-1212
telephonenumber: 212
-
replace: uid
uid: rjosmith
-
replace: mail
mail: robert.smith@example.com
mail: bob.smith@example.com
# adds using URL format
#add: jpegphoto
#jpegphoto:< file://path/to/jpeg/file.jpg
-
delete: description
```

On applique les modifications :

```
# ldapmodify -W -D "cn=admin,dc=exemple,dc=fr" -x -H ldap://localhost -f
structure4modif.ldif
Enter LDAP Password:
modifying entry "cn=Robert Smith,ou=people,dc=exemple,dc=fr"
```

Faites une sauvegarde de la base à l'aide de slapcat et après avoir stoppé le serveur (cf. tp1). Vérifiez que la modification est bien effectuée en comparant les bases sauvegardées (avant et après l'appel à ldapmodify). Il est également possible d'effectuer le contrôle via la commande ldapsearch. Nous allons nous simplifier la vie en définissant notre nouvelle base comme base par défaut en modifiant le fichier `/etc/ldap/ldap.conf` :

```
# Configuration des outils clients (voir « man ldap.conf »)
# Racine
BASE dc=exemple,dc=fr
# Nom et port de l'annuaire
URI ldap://localhost:389
```

Ainsi, une interrogation de l'annuaire devient simplement :

```
# ldapsearch -x
```

5 Sécurisation

Pour information, au niveau des ACL utilisées pour le TP1, j'ai ajouté une ACL pour autoriser les accès SASL, cela pourra être utile pour la suite. ATTENTION : il faut adapter ceci à ce TP 2 :

```
# 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
# These access lines apply to database #1 only
access to attrs=userPassword,shadowLastChange
        by dn="cn=admin,dc=i2l250,dc=fr" write
        by anonymous auth
        by self write
        by * none

# Ensure read access to the base for things like supportedSASLMechanisms.  Without this you may
# have problems with SASL not knowing what mechanisms are available and the like. Note that
# this is covered by the 'access to *' ACL below too but if you change that as people are wont
# to do you'll still need this if you want SASL (and possible other things) to work happily.
access to dn.base="" by * read

# The admin dn has full write access, everyone else can read everything.
access to *
        by dn="cn=admin,dc=i2l250,dc=fr" write
        by * read
```

5.1 Politique de sécurisation

Afin de pouvoir mettre en œuvre cette politique, on va devoir modifier le DIT conformément aux indications de l'énoncé de ce TP en utilisant le fichier (structure5.ldif) :

```
# create FIRST Level groups branch

dn: ou=groups,dc=exemple,dc=fr
objectclass:organizationalunit
ou: groups
description: generic groups branch

# create the itpeople entry under groups

dn: cn=itpeople,ou=groups,dc=exemple,dc=fr
objectclass: groupofnames
cn: itpeople
description: IT security group
member: cn=Sheri Smith,ou=people,dc=exemple,dc=fr

# create the hrpeople entry under groups

dn: cn=hrpeople,ou=groups,dc=exemple,dc=fr
objectclass: groupofnames
cn: hrpeople
description: Human Resources group
member: cn=Robert Smith,ou=people,dc=exemple,dc=fr
```

Puis on ajoute à la base :

```
# ldapadd -W -D "cn=admin,dc=exemple,dc=fr" -x -H ldap://localhost -f structure5.ldif
Enter LDAP Password:
adding new entry "ou=groups,dc=exemple,dc=fr"
adding new entry "cn=itpeople,ou=groups,dc=exemple,dc=fr"
adding new entry "cn=hrpeople,ou=groups,dc=exemple,dc=fr"
```

Faites une sauvegarde de la base à l'aide de slapcat et après avoir stoppé le serveur (cf. tp1).

5.2 Modification du fichier slapd.conf

Nous allons définir la politique de sécurisation suivante :

- Le propriétaire d'une entrée dans la hiérarchie doit pouvoir accéder et modifier tous les attributs
- Les ressources humaines doivent pouvoir mettre à jour toutes les entrées, mais pas de lire et modifier les mots de passe
- Les entrées : `carlicence`, `homepostaddress` et `homephone` ne peuvent être lues par personne d'autre que les ressources humaines et le propriétaire
- Tous les utilisateurs doivent s'authentifier (pas d'accès anonyme)

  Les personnes du département IT doivent pouvoir modifier les mots de passe pour tout le monde.

Afin de prendre en compte notre politique, nous devons modifier notre fichier « `slapd.conf` ». Voici une version **incomplète/incorrecte** de ce fichier car les ACL doivent encore être modifiées :

```
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        255

modulepath/usr/lib/ldap
moduleloadback_hdb

sizelimit 500
tool-threads 1

backend        hdb
database        hdb
suffix          "dc=exemple,dc=fr"

rootdn          "cn=admin,dc=exemple,dc=fr"
rootpw          "{CRYPT}J9NQ/M7KbU9Ak"

directory       "/var/lib/ldap"
dbconfig set_cachesize 0 16777216 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
        by dn="cn=admin,dc=exemple,dc=fr" write
        by anonymous auth
        by self write
        by group.exact="cn=itpeople,ou=groups,dc=exemple,dc=fr" write
        by * none

access to dn.base="" by * read

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

Je vous laisse chercher maintenant les autres ACLs à mettre en place pour que notre politique de sécurité soit opérationnelle ! Redémarrez votre démon `slapd`, et « normalement » ça doit repartir !

5.3 Test

Tests préliminaires (connexion en lecture sous différentes identités) :

```
# ldapsearch -x -H ldap://localhost -b "dc=exemple,dc=fr"
     ...
# ldapsearch -W -D "cn=admin,dc=exemple,dc=fr" -x -H ldap://localhost -b
"dc=exemple,dc=fr"
Enter LDAP Password: toto
     ...
# ldapsearch -W -D "cn=Robert Smith, ou=people, dc=exemple, dc=fr" -x -H
ldap://localhost -b "dc=exemple,dc=fr"
Enter LDAP Password: rJsmitH
     ...
```

Testons maintenant notre sécurisation :

- Connectez vous en tant que : `cn=Robert Smith, ou=people, dc=exemple, dc=fr` (mot de passe à retrouver dans ci-dessus) et vérifiez que comme il est « `hrpeople` », il peut modifier toutes les entrées, mais pas les mots de passe (sauf le sien) ;
- Connectez vous en tant que : `cn= Sheri Smith, ou=people, dc=exemple, dc=fr` et vérifiez que comme elle est « `itpeople` », elle peut voir et modifier les mots de passe, mais elle ne peut pas voir les attributs : `carlicense`, `homepostaladdress` et `homephone`, (sauf les siens) ;
- Connectez vous en tant que : `cn=John Smith, ou=people, dc=exemple, dc=fr` et vérifiez qu'il ne peut voir les entrées `carlicense`, `homepostaladdress`, `homephone` and `userpassword` (sauf les siens) ;
- Connectez vous en tant qu'`anonymous`, la connexion doit être refusée ;
- Connectez vous en tant qu'`admin` et vérifiez que vous pouvez faire tout ce que vous voulez !

A VOUS DE JOUER !

5.4 Problème rencontré

Suite à une coupure brutale du serveur, le serveur ldap n'est pas reparti. Voici le message que j'avais au démarrage en mode débugage :

```
# slapd -d 1
bdb_db_open: dbenv_open(/var/lib/ldap)
bdb(dc=mondomaine,dc=com): operation not permitted during recovery
bdb_db_open: db_open(/var/lib/ldap) failed: Invalid argument (22)
backend_startup: bi_db_open failed! (22)
bdb_db_destroy: close failed: Invalid argument (22)
slapd stopped.
```

En fait, c'était la base ldap qui était corrompue et pour régler ce problème, je l'ai simplement ré-indexée avec ces commandes :

```
# /etc/init.d/slapd stop
# slapindex
# /etc/init.d/slapd start
```

5.5 ANNEXE

Informations complémentaires issues de (http://www.coagul.org/article.php3?id_article=172).
La commande suivante permet de générer un fichier .LDIF contenant la base complète :

```
slapcat -l DumpLDAP.ldif -b "dc=mondomaine,dc=com"
```

5.5.1 LDAP Browser

LDAP Browser est un programme en Java, permettant de consulter et de modifier une base LDAP : http://www-unix.mcs.anl.gov/ gawor/ldap/

Liste partielle des attributs de la classe « organization »

Attribut	Description
businessCategory	Activité professionnelle d'une entreprise ou d'une personne
c	Code du pays en deux lettres (respectant le standard ISO 3166)
cn	Nom de l'objet (common name)
description	Description de l'objet
distinguishedName	Nom distingué (utilisé par d'autres attributs par héritage)
facsimileTelephoneNumber	Numéro de fax
givenName	Prénom de la personne
houseIdentifier	Identifiant d'un batiment
initials	Initiales d'une personne
internationalSDNNumber	Numéro ISDN
l	localité de l'objet (géographique)
member	Distinguished Name des membres
name	Nom (utilisé par d'autres attributs par héritage)
o	Nom de l'organisation
objectClass	Classe d'objets
ou	Unité organisationnelle (branche de l'organisation)
owner	Nom du propriétaire de l'objet
postalAddress	Adresse postale (sans le code postal)
postalCode	Code postal
postalOfficeBox	Boîte aux lettres (postale)
presentationAddress	Adresse réseau de la présentation de l'objet (généralement une URL vers la présentation en ligne)
protocolInformation	Attribut complémentaire à presentationAddress pour définir le protocole à utiliser
registeredAddress	Adresse postale pour des envois de courriers recommandés et de colis
seeAlso	DN d'objets complémentaires
serialNumber	Numéro de série de l'objet
sn	Nom de famille de la personne (surname)
st	Etat ou région (state)
streetAddress	Nom de la rue et assimiilé (boulevard, ...)
telephoneNumber	Numéro de téléphone
title	Titre de la personne (différent de fonction)
uid	Identifiant unique de l'objet
userPassword	Mot de passe de l'utilisateur

5.6 Liste partielle des attributs de la classe « inetOrgPerson »

Nom	Sémantique	Mono	Obl	Lecture	Utilisation
cn	nom(s) complet(s) (d'usage) sans accent		O	RI	Ordre : Nom, Prénom. Attention : pas d'accent pour simplifier les recherches. Voir aussi displayName. Exemple : "Bugale Jerome"
displayName	nom complet avec accents				Version accentuée de la valeur principale de cn. Exemple : "Bugalé Jérôme"
employeeType	type de personnel		D ?	RI ?	Définir les grandes familles ?
facsimileTelephoneNumber	Numéro de fax			RI	Format E 123 (cf Références)
givenName	Prénom	M	D	RI	idem sn. Exemple : "Jérôme"
l					localité de l'objet (géographique)
labeledURI	Page personnelle			RI	
mail	adresse mel canonique	M		RI ?	
mobile	numéro de téléphone mobile			RI	Format E 123 (cf Références)
o					Nom de l'organisation
ou					Unité organisationnelle (branche de l'organisation)
postalAddress	Adresse postale			RI	Adresse complète. Attention au format ("$" séparateur, voir RFC2256)
postalCode	Code postal				
preferredLanguage	langue préférée	M		RI	cf RFC2068
sn	Nom		O	RI	Contient le nom d'usage. Il est possible d'ajouter le nom de famille (nom patronymique) en seconde valeur. Tout caractère diacritique. Première lettre en majuscule. Voir aussi cn. Exemple : "Bugalé".
st					Etat ou région (state)
telephoneNumber	numéro de téléphone fixe			RI	Format E 123 (cf Références)
title	titre			RI	Responsabilité ; président, directeur, ... (cf Harpège ?). Code ou intitulé complet ?
uid	identifiant unique	M	D	R	utilisé comme rdn, contenu indifférent mais aussi court que possible
userCertificate	certificat X509			A ?	