TP N°2 LDAP

CORRECTION 2

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

5 Sécurisation

5.7 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` » :

```
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.pid
loglevel   5
modulepath /usr/lib/ldap
moduleload back_bdb
sizelimit  500
tool-threads     1
backend          bdb
database bdb
suffix "dc=exemple,dc=fr"

# ACL1
access to attr=userpassword
       by self       write
       by anonymous  auth
       by group.exact="cn=itpeople,ou=groups,dc=exemple,dc=fr"  write
       by *          none

# ACL2
access to attr=carlicense,homepostaladdress,homephone
       by self       write
       by group.exact="cn=hrpeople,ou=groups,dc=exemple,dc=fr"  write
       by *          none

# ACL3
access to *
       by self       write
       by group.exact="cn=hrpeople,ou=groups,dc=exemple,dc=fr"  write
       by users      read
       by *          none

rootdn     "cn=admin,dc=exemple,dc=fr"
rootpw     toto

directory  /var/lib/ldap/

index uid  eq
index cn,gn,mail eq,sub
index sn eq,sub
index ou eq
index telephonenumber  eq,sub

cachesize 10000
checkpoint 128 15
```

Bien évidemment après avoir modifié ce fichier il faut relancer le serveur (par exemple, via /etc/init.d/slapd restart) et vérifier qu'il est bien lancé via les commandes suivantes :

```
# echo `pidof slapd` `cat /var/run/slapd/slapd.pid`
# lsof -i :389
# tail /var/log/syslog
# ldapsearch -x -h localhost -b 'dc=exemple,dc=fr' '(objectClass=inetOrgPerson)' dn
# ldapsearch -x -h 192.168.0.13 -b 'dc=exemple,dc=fr' '(objectClass=inetOrgPerson)' homePhone
```

Remarque : le même genre de requêtes peut être effectué (avec modération !) sur le serveur ldap gérant les salles informatiques :

```
# ldapsearch -x -H ldap://192.168.22.61:389 -b  'dc=calais,dc=fr'
```