Rapport TP4 : Configuration LDAP

DRISSI Mohamed Reda
reda-mohamed@isty.uvsq.fr

3 décembre 2018

Table des matières

I Rappels sur LDAP

I.1 Exercice 1

LDAP est un protocole de gestion d'annuaire. Il a cependant évolué pour représenter une norme pour les systèmes d'annuaires, incluant un modèle de données, un modèle de nommage, un modèle fonctionnel basé sur le protocole LDAP, un modèle de sécurité et un modèle de réplication. C'est une structure arborescente dont chacun des nœuds est constitué d'attributs associés à leurs valeurs. LDAP est moins complexe que le modèle X.500 édicté par l'UIT-T.

I.2 Exercice 2

L'annuaire LDAP est utilisé pour centraliser l'authentification des utilisateurs sur les différents services/applications dans le réseau interne où cet annuaire est configuré.

I.3 Exercice 3

LDAP est un protocole qui suit l'esprit du monde UNIX ; il laisse une grande liberté de choix à l'admin sys. Les serveurs peuvent alors supporter une large variété de scénarios.

I.4 Exercice 4

Il faut faire attention à la sécurité de l'annuaire et à la confidentialité des échanges.

I.5 Exercice 5

Une différence majeure entre les annuaires LDAP et les SGBDR est le fait que les attributs puissent être multi-valués. De plus, si un attribut n'a pas de valeur, il est purement et simplement absent de l'entrée. Cependant d'autres annuaires s'appuyent en arrière plan sur un SGBD.

II Mise en place du serveur

II.1 Exercice 6

```
$ aptitude install slapd ldap-utils ldapscripts
```

Le mdp sera `admin`.

II.2 Exercice 7

```
$ dpkg-reconfigure -plow slapd
DNS = istycorp.fr
nom d'organisation = istycorp=fr
```

II.3 Exercice 8

```
$ cat > create-struct.ldif
  dn: ou=people,dc=istycorp,dc=fr
  objectClass: organizationalUnit
  ou: people

  dn: ou=groups,dc=istycorp,dc=fr
  objectClass: organizationalUnit
  ou: groups
$ ldapadd -xWD "cn=admin,dc=istycorp,dc=fr" -f "create-struct.ldif"
$ slapcat
```

II.4 Exercice 9

```
$ cat > user-red.ldif
  dn: cn=red,ou=people,dc=istycorp,dc=fr
  objectClass: top
  objectClass: account
  objectClass: posixAccount
  objectClass: shadowAccount
  uid: julien
  uidNumber: 5671
  gidNumber: 5671
  userPassword: <no need>
  gecos: Reda DRISSI
  loginShell: /bin/bash
  homeDirectory: /home/red
$ ldapadd -xWD "cn=admin,dc=istycorp,dc=fr" -f "user-red.ldif"
$ slapcat
```

II.5 Exercice 10

```
$ cat > group-user.ldif
  dn: cn=user,ou=groups,dc=istycorp,dc=fr
  objectclass: top
  objectclass: posixGroup
  cn: user
  memberUid: red
  gidNumber: 5671
$ ldapadd -xWD "cn=admin,dc=istycorp,dc=fr" -f "group-user.ldif"
$ slapcat
```

II.6 Exercice 11

Nous pouvons chercher les informations de notre utilisateur red en tant que "reda"

```
$ ldapsearch -xWD "cn=reda,ou=people,dc=istycorp,dc=fr" -b "cn=reda,
ou=people,dc=istycorp,dc=fr"
```

II.7 Exercice 12

Nous pouvons changer le mdp du user *red* avec la commande

```
$ ldappasswd -xWSD "cn=reda,ou=people,dc=istycorp,dc=fr"
```

II.8 Exercice 13

phpldapadmin a été abandonné par debian depuis plus de 2 ans. Nous allons donc l'installer manuellement avec dpkg.

```
$ wget http://http.us.debian.org/debian/pool/main/p/phpldapadmin/phpldapadmin_1.2.2
$ dpkg -i phpldapadmin_1.2.2-6.1_all.deb
```

L'application est à présent disponible sur l'adresse "http ://localhost :8080/phpldapadmin/" du hôte.

II.9 Exercice 14

Nous éditons un fichier pour changer le domaine en modifiant une ligne

```
$ vim /etc/phpldapadmin/config.php
la ligne : $servers->setValue('server','base',
array('dc=example,dc=com'));
devient : $servers->setValue('server','base',
array('dc=istycorp,dc=fr'));
```

II.10 Exercice 15

Simple manipulation sur l'interface graphique.

III Intégration à PAM

III.1 Exercice 16

Nous installons les packages

```
$ apt install libpam-ldapd libnss-ldapd
```

Pour `libnss-ldapd` on choisit passwd, group et shadow.

III.2 Exercice 17

```
      $ cat /etc/nslcd.conf
# /etc/nslcd.conf
# nslcd configuration file. See nslcd.conf(5)
# for details.

# The user and group nslcd should run as.
uid nslcd
gid nslcd

# The location at which the LDAP server(s) should be reachable.
uri ldap://127.0.0.1/

# The search base that will be used for all queries.
base dc=istycorp,dc=fr

# The LDAP protocol version to use.
#ldap_version 3

# The DN to bind with for normal lookups.
#binddn cn=annonymous,dc=example,dc=net
#bindpw secret

# The DN used for password modifications by root.
#rootpwmoddn cn=admin,dc=example,dc=com

# SSL options
#ssl off
#tls_reqcert never
tls_cacertfile /etc/ssl/certs/ca-certificates.crt

# The search scope.
#scope sub
```

```
      $ cat /etc/nsswitch.conf
# /etc/nsswitch.conf
#
# Example configuration of GNU Name Service Switch functionality.
# If you have the ‘glibc-doc-reference’ and ‘info’ packages installed, try:
# ‘info libc "Name Service Switch"’ for information about this file.

passwd:         compat ldap
group:          compat ldap
shadow:         compat ldap
gshadow:        files

hosts:          files mdns4_minimal [NOTFOUND=return] dns myhostname
networks:       files

protocols:      db files
services:       db files
ethers:         db files
rpc:            db files

netgroup:       nis
```

```
      $ grep ldap /etc/pam.d/*
etc/pam.d/common-account:account [success=ok new_authtok_reqd=done ignore=ignore user_unk
pam_ldap.so minimum_uid=1000
/etc/pam.d/common-auth:auth [success=1 default=ignore]
pam_ldap.so minimum_uid=1000 use_first_pass
/etc/pam.d/common-password:password
[success=1 default=ignore] pam_ldap.so minimum_uid=1000 try_first_pass
/etc/pam.d/common-session:session [success=ok default=ignore]
pam_ldap.so minimum_uid=1000
/etc/pam.d/common-session-noninteractive:session
[success=ok default=ignore] pam_ldap.so minimum_uid=1000
```

III.3 Exercice 18

— On redémarre les services NSCD et NSLCD avec systemctl restart nscd nslcd
— On change d'utilisateur sur un utilisateur créé dans LDAP (red) avec su - red
— On entre le mot de passe correspondant (red)

— On voit que notre home directory est /
— On sort de la session utilisateur avec exit
— On ajoute la ligne session required pam_mkhomedir.so skel=/etc/skel umask=0022 dans /etc/pam.d/common-session
— On redémarre les services NSCD et NSLCD avec systemctl restart nscd nslcd
— On re-change d'utilisateur sur un utilisateur créé dans LDAP (red) avec su - red
— On entre le mot de passe correspondant (red)
— On voit que notre home directory a maintenant été créé et est /home/red

III.4 Exercice 19

En comparant les résultats avec `vimdiff` entre /etc/passwd et getent passwd. Nous trouvons que les résultats correspondent à ceux entrées dans ldap.

III.5 Exercice 21

```
      $ cat > hosts.ldif
dn: ou=hosts,dc=istycorp,dc=fr
objectClass: organizationalUnit
objectClass: top
ou: hosts

dn: cn=localhost+ipHostNumber=127.0.0.1,ou=hosts,dc=istycorp,dc=fr
objectClass: ipHost
objectClass: device
objectClass: top
cn: localhost
ipHostNumber: 127.0.0.1

dn: cn=router.istycorp.fr+ipHostNumber=192.168.0.1,ou=hosts,dc=istycorp,dc=fr
objectClass: ipHost
objectClass: device
objectClass: top
cn: router.istycorp.fr
ipHostNumber: 192.168.0.1

dn: cn=c2.istycorp.fr+ipHostNumber=192.168.0.2,ou=hosts,dc=istycorp,dc=fr
objectClass: ipHost
objectClass: device
objectClass: top
cn: c2.istycorp.fr
ipHostNumber: 192.168.0.2

dn: cn=c3.istycorp.fr+ipHostNumber=192.168.0.3,ou=hosts,dc=istycorp,dc=fr
objectClass: ipHost
objectClass: device
objectClass: top
cn: c3.istycorp.fr
ipHostNumber: 192.168.0.3

dn: cn=c4.istycorp.fr+ipHostNumber=192.168.0.4,ou=hosts,dc=istycorp,dc=fr
objectClass: ipHost
objectClass: device
objectClass: top
cn: c4.istycorp.fr
ipHostNumber: 192.168.0.4
```

```
dn: cn=c5.istycorp.fr+ipHostNumber=192.168.0.5,ou=hosts,dc=istycorp,dc=fr
objectClass: ipHost
objectClass: device
objectClass: top
cn: c5.istycorp.fr
ipHostNumber: 192.168.0.5

dn: cn=c6.istycorp.fr+ipHostNumber=192.168.0.6,ou=hosts,dc=istycorp,dc=fr
objectClass: ipHost
objectClass: device
objectClass: top
cn: c6.istycorp.fr
ipHostNumber: 192.168.0.6

dn: cn=c7.istycorp.fr+ipHostNumber=192.168.0.7,ou=hosts,dc=istycorp,dc=fr
objectClass: ipHost
objectClass: device
objectClass: top
cn: c7.istycorp.fr
ipHostNumber: 192.168.0.7

dn: cn=c8.istycorp.fr+ipHostNumber=192.168.0.8,ou=hosts,dc=istycorp,dc=fr
objectClass: ipHost
objectClass: device
objectClass: top
cn: c8.istycorp.fr
ipHostNumber: 192.168.0.8

dn: cn=c9.istycorp.fr+ipHostNumber=192.168.0.9,ou=hosts,dc=istycorp,dc=fr
objectClass: ipHost
objectClass: device
objectClass: top
cn: c9.istycorp.fr
ipHostNumber: 192.168.0.9

dn: cn=c10.istycorp.fr+ipHostNumber=192.168.0.10,ou=hosts,dc=istycorp,dc=fr
objectClass: ipHost
objectClass: device
objectClass: top
cn: c10.istycorp.fr
ipHostNumber: 192.168.0.10

dn: cn=server.istycorp.fr+ipHostNumber=192.168.0.11,ou=hosts,dc=istycorp,dc=fr
objectClass: ipHost
objectClass: device
objectClass: top
cn: server.istycorp.fr
ipHostNumber: 192.168.0.11
```

```
    $ ldapadd -xWD "cn=admin,dc=istycorp,dc=fr" -f hosts.ldif
    $ vim /etc/nsswitch.conf
On rajoute le flag "ldap" à la ligne hosts
    $ systemctl restart nscd nslcd
    $ getent hosts
127.0.0.1       localhost
127.0.0.1       localhost ip6-localhost ip6-loopback
127.0.0.1       localhost
192.168.0.1     router.istycorp.fr
192.168.0.2     c2.istycorp.fr
192.168.0.3     c3.istycorp.fr
192.168.0.4     c4.istycorp.fr
192.168.0.5     c5.istycorp.fr
192.168.0.6     c6.istycorp.fr
192.168.0.7     c7.istycorp.fr
192.168.0.8     c8.istycorp.fr
192.168.0.9     c9.istycorp.fr
192.168.0.10    c10.istycorp.fr
192.168.0.11    server.istycorp.fr
```

IV Filtrage par groupe PAM