

I - Installation et configuration d'openldap

1. Installation d'openldap

Passer en root

```
$ su -
```

Installer les paquets nécessaires

```
# yum install openldap openldap-servers openldap-clients migrationtools vim
....
```

Le paquet migrationtools sera utilisé après pour la migration des users de /etc/passwd à ldap

Le paquet vim servira pour l'édition du fichier de configuration (vim est plus convivial que vi)

2. Configuration d'openldap

Générer un mot de passe crypté de l'administrateur de la base ldap

```
# slappasswd
New password:
Re-enter new password:
{SSHA}MP0BeMJzmCoCi5o1BhwcRDYJaGBFgN5K
```

Copier le mot de passe crypté généré pour la prochaine étape (*{SSHA}MP0BeMJzmCoCi5o1BhwcRDYJaGBFgN5K*)

Effacer le répertoire slapd.d (sinon Fedora ne pourra pas prendre en compte notre configuration)

```
# rm -Rf /etc/openldap/slapd.d/
```

Créer un fichier de configuration slapd.conf à partir d'un fichier template

```
# cp /usr/share/openldap-servers/slapd.conf.obsolete /etc/openldap/slapd.conf
```

Éditer le fichier de configuration slapd.conf avec vim par exemple

```
# vim /etc/openldap/slapd.conf
```

Modifier dans le fichier slapd.conf pour avoir les informations suivantes

```
access to *
by dn.exact="cn=admin,dc=esgis,dc=bj" read
by * none
...
suffix "dc=esgis,dc=bj"
rootdn "cn=admin,dc=esgis,dc=bj"
...
rootpw {SSHA}MP0BeMJzmCoCi5o1BhwcRDYJaGBFgN5K
```

Sauvegarder et quitter le fichier de configuration

```
:x
```

3. Vérifier la configuration d'openldap

Démarrer le service ldap (slapd)

```
# service slapd start
Starting slapd (via systemctl): [ OK ]
```

Tester la configuration

```
# slaptest -u
config file testing succeeded
```

4. Peupler l'annuaire ldap

le fichier ldif se trouve par exemple dans /home/mathias/fic1.ldif

```
# ldapadd -x -D cn=admin,dc=esgis,dc=bj -W -H ldapi:/// -f /home/mathias/fic1.ldif
Enter LDAP Password:
....
```

Précautions

- SELinux est un module de sécurité inclus dans Fedora et qui pourrait empêcher la bonne exécution du serveur ldap (problème de permission étendue sur le fichier slapd.conf créé auparavant). Il faut avant de démarrer le service ldap, configurer SELinux en mode permissive qui est moins strict que le mode enforcing ; mais cette manipulation est temporaire.

```
# setenforce 0
```

- Si vous souhaitez rendre accessible à d'autres machines du réseaux votre serveur ldap, il faut configurer le pare-feux (iptables) de Fedora qui par défaut n'autorise que le port SSH (port 22). Pour le faire il faut rendre accessible le port LDAP (port 389) de l'extérieur

```
# iptables -t filter -A INPUT -m tcp -p tcp --dport 389 -j ACCEPT
```

Ressources

- Tutorial openldap sous fedora - <http://blog.christophersmart.com/articles/openldap-how-to-fedora/>
- Survie sous vi et vim - <http://mathias.houngbo.net/node/30>
- En savoir plus sur SELinux - <http://doc.fedora-fr.org/wiki/SELinux>
- En savoir plus sur le Parefeux - <http://doc.fedora-fr.org/wiki/Parefeu> - [firewall](#) - [netfilter](#) - [iptables](#)