IV - Configuration de l'authentification linux via LDAP

1. Prérequis

votre serveur openldap doit être configurer et fonctionnel, et il faut activer le service LDAP au démarrage de l'ordinateur pour ne pas avoir de mauvaise surprise.

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

2. Installation des librairies nss_ldap et pam_ldap

Installer les paquets nécessaires

```
# yum install nss_ldap pam_ldap
....
```

Le paquet nss_ldap sera utilisé pour l'annuaire LDAP et le paquet pam_ldap servira pour l'authentification via LDAP

3. Configuration nss_ldap

Éditer le fichier /etc/nss_ldap.conf pour avoir les informations suivantes

```
....
uri ldap://127.0.0.1/
port 389
base dc=esgis,dc=bj
ldap_version 3
rootbinddn cn=admin,dc=esgis,dc=bj
bind_policy soft
....
```

le mot de passe de l'administrateur de l'annuaire LDAP se trouve en clair dans le fichier /etc/ldap.secret

```
# echo votresupermotdepasse > /etc/ldap.secret
```

votresupermotdepasse étant le mot de passe qui a été définit lors de la création de l'annuaire LDAP.

4. Configuration pam_ldap

Éditer le fichier /etc/pam_ldap.conf pour avoir les informations suivantes

```
....
uri ldap://127.0.0.1/
port 389
base dc=esgis,dc=bj
ldap_version 3
rootbinddn cn=admin,dc=esgis,dc=bj
pam_password crypt
....
```

5. Sécurisation des fichiers de configuration nss_ldap et pam_ldap

```
# chmod 600 /etc/nss_ldap.conf
# chmod 600 /etc/pam_ldap.conf
# chmod 600 /etc/ldap.secret
```

6. Configuration nsswitch.conf

Modifier le fichier de configuration /etc/nsswitch.conf pour activer la recherche avec LDAP.

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

7. Configuration nsswitch.conf

La configuration de PAM se fait sous Fedora, pour les options à appliquer sur tout le système, dans le fichier /etc/pam.d/system-auth

Configuration manuelle

```
# vim /etc/pam.d/system-auth

auth        sufficient  pam_ldap.so use_first_pass
account     [default=bad success=ok user_unknown=ignore] pam_ldap.so
password    sufficient  pam_ldap.so use_authtok
session     optional    pam_ldap.so
```

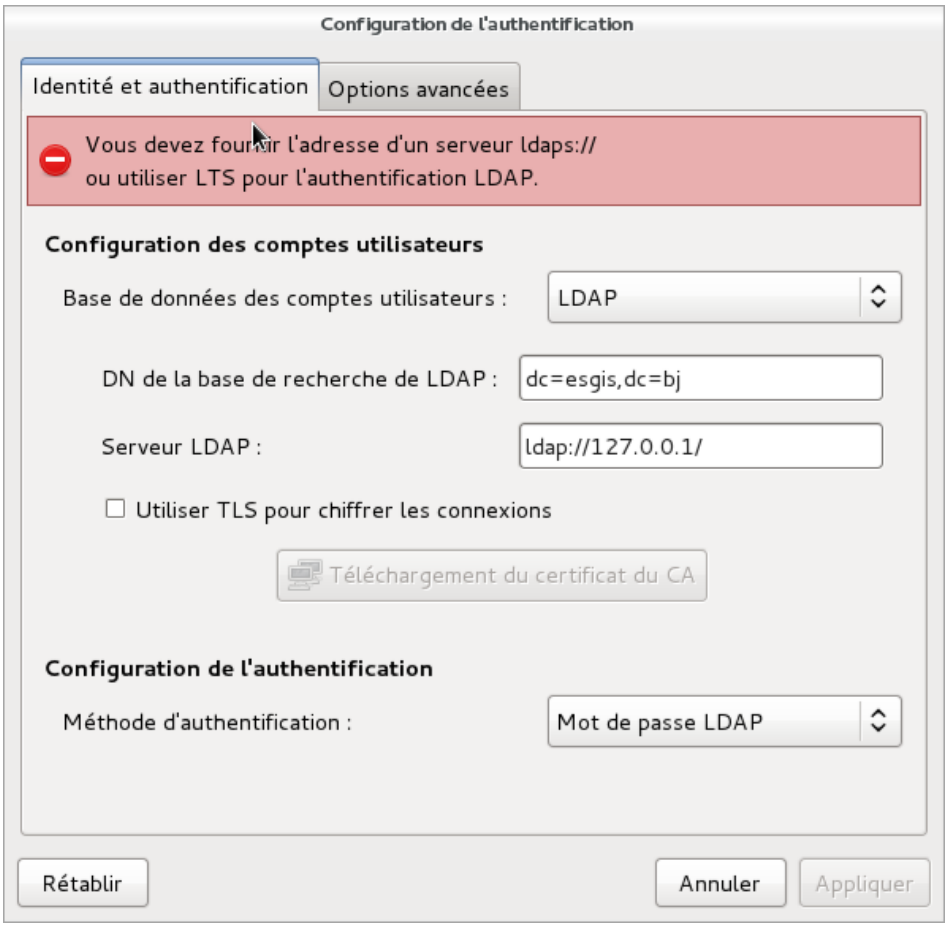
Il faut ajouter les clauses pam_ldap pour chacune des quatres sections (auth, account, password et session)

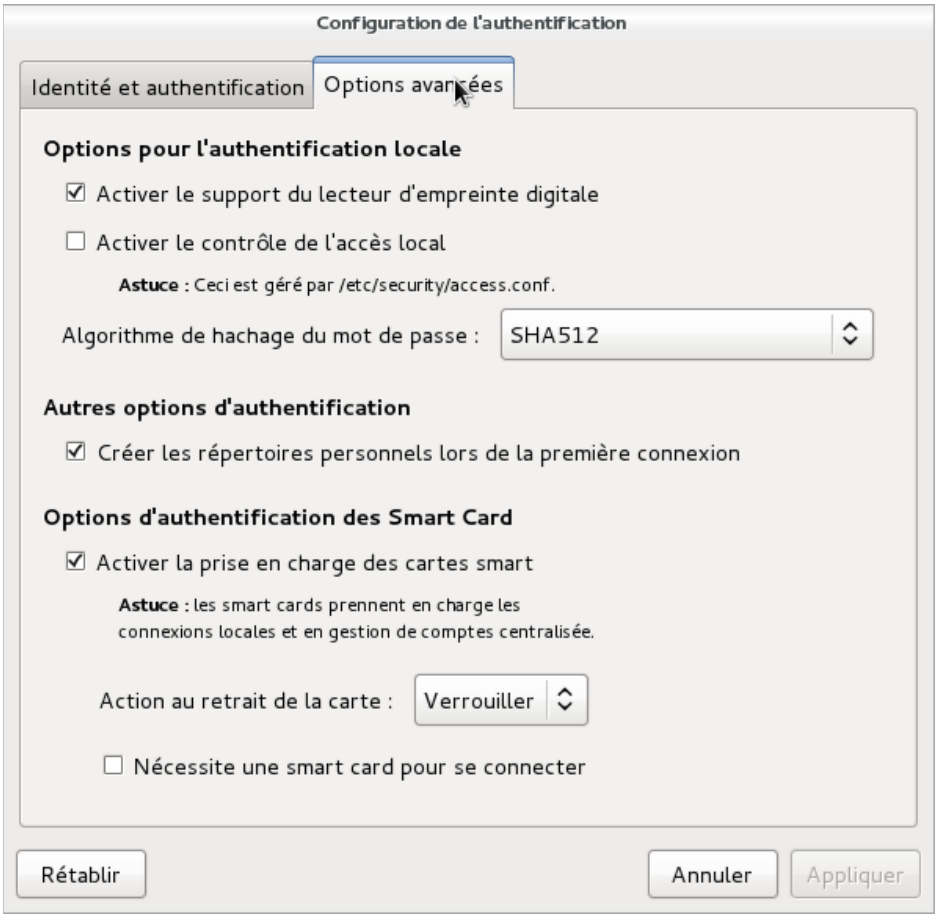
Le fichier doit ressembler à ceci

```
#%PAM-1.0
# This file is auto-generated.
# User changes will be destroyed the next time authconfig is run.
auth        required      pam_env.so
auth        [success=1 default=ignore] pam_succeed_if.so service notin
login:gdm:xdm:kdm:xscreensaver:gnome-screensaver:kscreensaver quiet use_uid
auth        [success=done authinfo_unavail=ignore ignore=ignore default=die] pam_pkcs11.so
card_only
auth        sufficient    pam_fprintd.so
auth        sufficient    pam_unix.so nullok try_first_pass
auth        requisite     pam_succeed_if.so uid >= 1000 quiet
auth        sufficient    pam_ldap.so use_first_pass
auth        required      pam_deny.so

account     required      pam_unix.so broken_shadow
account     sufficient    pam_localuser.so
account     sufficient    pam_succeed_if.so uid < 1000 quiet
account     [default=bad success=ok user_unknown=ignore] pam_ldap.so
account     required      pam_permit.so

password    requisite     pam_cracklib.so try_first_pass retry=3 type=
password    sufficient    pam_unix.so sha512 shadow nullok try_first_pass use_authtok
password    sufficient    pam_ldap.so use_authtok
password    required      pam_deny.so

session     optional      pam_keyinit.so revoke
session     required      pam_limits.so
-session     optional      pam_systemd.so
session     optional      pam_mkhomedir.so
session     [success=1 default=ignore] pam_succeed_if.so service in crond quiet use_uid
session     required      pam_unix.so
session     optional      pam_ldap.so
```

Assistant de configuration graphique PAM (plus simple, plus conviviale)

```
# authconfig-gtk
```





8. Tester la configuration

- Modifier le mot de passe de l'utilisateur joseph via phpldapadmin,
- Fermer la session graphique
- Et tenter connecter au système en tant que l'utilisateur joseph

- ou bien faire un

```
$ su - joseph
```

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
```