TP N°2 LDAP

Master 2 I2L

Année 2009/2010

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

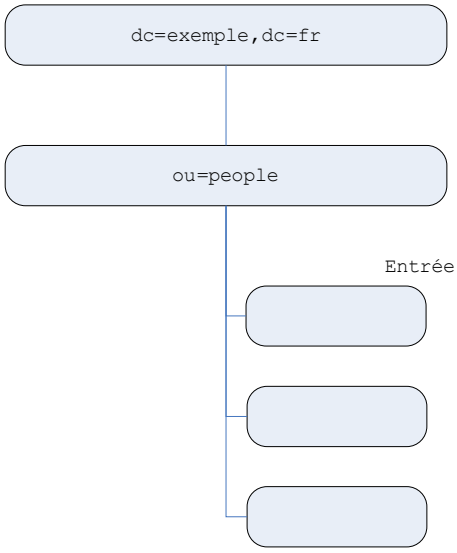
D. Duvivier
LIL – Université du Littoral Côte d'Opale
duvivier@lil.univ-littoral.fr

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 :

```
# /etc/init.d/slapd stop
# rm -fr /var/lib/ldap/*
```

Nous allons maintenant travailler sur le DIT suivant :



Cette structure représente la hiérarchie d'un carnet d'adresse d'une entreprise quelconque…

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

Vous pouvez vérifier que tout marche bien avec :

```
# slapd -d 5 -h ldap://localhost:389 -f /etc/ldap/slapd.conf
```

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 :

```
## dcObject est un objectClass AUXILIARY et doit
## avoir un objectClass STRUCTURAL (organization dans ce cas)

dn: dc=exemple,dc=fr
dc: exemple
description: La description de ce que vous voulez décrire,
 c'est comme vous voulez
 les nouvelles lignes commencent avec un espace
objectClass: dcObject
objectClass: organization
o: Exemple, SA.
```

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

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

3 Ajout de personnes

On peut maintenant ajouter des personnes pour peupler notre annuaire. On va utiliser un objet de type : `inetOrgPerson`.

Définir un fichier LDIF permettant de rentrer les informations suivantes pour les 3 personnes :

- Robert Smith (ou Robert J Smith, ou bob smith), Surnom : smith, Login : rjsmith, Mot de Passe : rJsmitH, Tel perso : 555-111-2222, Mail : r.smith@exemple.fr et rsmith@exemple.fr et bob.smith@exemple.fr, Description : grincheux, Organisation : Ressources humaines
- John Smith (ou John J Smith), Surnom : Smith, Login : jsmith, Mot de Passe : jSmitH, Tel perso : 555-111-2223, Mail : j.smith@exemple.fr et jsmith@exemple.fr et john.smith@exemple.fr, Organisation : Ventes
- Sheri Smith, Surnom : smith, Login : ssmith, Mot de Passe : sSmitH, Tel perso : 555-111-2225, Mail : s.smith@exemple.fr et ssmith@exemple.fr et sheri.smith@exemple.fr, Organisation : IT

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.

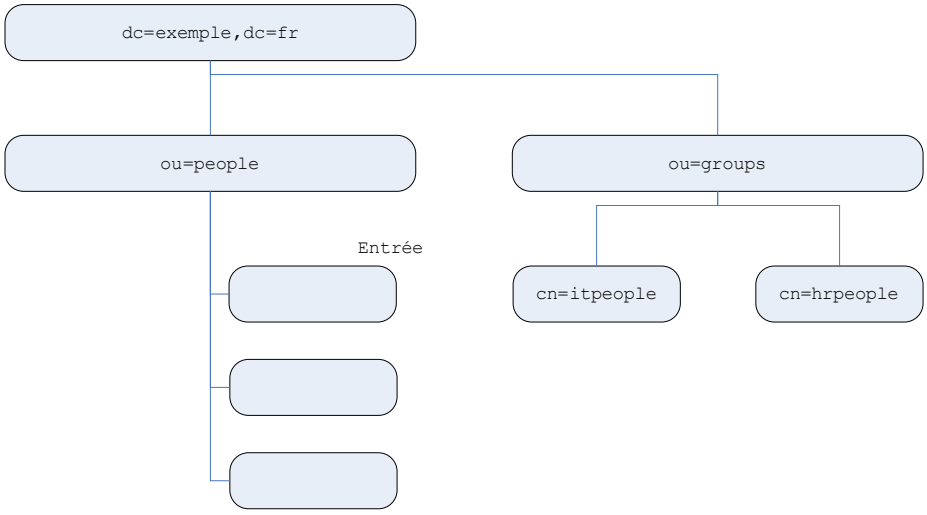
5 Sécurisation

5.1 Politique de sécurisation

Nous allons définir la politique de sécurisation suivante :

- Le propriétaire d'une entrée dans la hiérarchie doit pouvoir accéder et modifier tous les attributs (même les mots de passe)
- 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 pouvoir mettre en œuvre cette politique, on va devoir modifier le DIT afin qu'il devienne comme ceci :



Le premier nouveau élément « `ou=groups` » va être créé via un fichier LDIF de la même manière que pour l'élément « `ou=people` ». On mettra juste une description du style : Branche pour les groupes.

Par contre, les éléments « `cn=itpeople` » et « `cn=hrpeople` » vont être utilisés avec un objectclass de type « `groupofnames` ». Ce type définit un attribut : « `member:` » dans lequel on va placer qui est membre de ce groupe (il faut mettre le `dn` de la personne !).

Afin de créer les éléments « `cn=itpeople` » et « `cn=hrpeople` », on va passer (comme d'habitude !) par un fichier LDIF. Ce fichier va contenir les éléments suivants :

- Pour « `cn=itpeople` », Description : Groupe de Sécurité IT et le membre de ce groupe est : Sheri Smith
- Pour « `cn=hrpeople` », Description : Groupe des Ressources Humaines et le membre de ce groupe est : Robert Smith

5.2 Modification du fichier slapd.conf

Afin de prendre en compte notre politique, nous devons modifier notre fichier « `slapd.conf` ». Voici la première ACL à ajouter (juste après `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
```

Je vous laisse chercher maintenant les autres ACLs (il y en a 2 autres dans mon fichier « `slapd.conf` »)à mettre en place pour que notre politique de sécurité soit opérationnelle !

Redémarrez votre démon `slapd`, et « normalement » ça doit repartir !

5.3 Test

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 !