M1 - Outils de l'Internet (Année 2010/2011)

Gold is Where You Find It

L'objet de ce dernier TD est de comprendre le système de répertoire LDAP, d'être capable d'écrire des requêtes pour un serveur LDAP, et de comprendre les problèmes liés à la conception et à l'organisation d'un tel serveur.

1 Introduction

LDAP (Lightweight Directory Access Protocol) est le standard de système de répertoires ; un système de répertoire permet d'organiser une base de donnée selon une direction privilégiée.
– La liste des RFCs régissant LDAP : `http://tools.ietf.org/html/rfc4510`
– OpenLDAP en est l'implémentation libre de référence : `http://www.openldap.org/`

2 Les entrées LDIF par l'exemple

LDIF est le standard décrivant comment afficher les entrées d'un répertoire LDAP de manière lisible par l'être humain. LDIF peut servir à décrire des entrées LDAP, ou des directives devant s'appliquer à un système de répertoire LDAP pour le modifier. Voici un exemple d'entrées LDAP écrites en LDIF :

```
version: 1

dn: dc=example,dc=com
dc: example
description: My wonderful company whose name is incredibly large
 and requires two lines and a blank space.
objectClass: dcObject
objectClass: organization
o: Example, Inc.

dn: ou=people, dc=example,dc=com
ou: people
description: All people in organisation
objectclass: organizationalunit

dn: cn=Robert Smith,ou=people,dc=example,dc=com
objectclass: inetOrgPerson
cn: Robert Smith
cn: Robert J Smith
cn: bob  smith
sn: smith
uid: rjsmith
userpassword: rJsmitH
carlicense: HISCAR 123
homephone: 555-111-2222
```

```
mail: r.smith@example.com
mail: rsmith@example.com
mail: bob.smith@example.com
description: swell guy
ou: Human Resources
```

3 Directives LDIF : accéder LDAP en écriture

3.1 Ajouter une entrée ou la supprimer

```
dn: cn=Robert Smith,ou=people,dc=example,dc=com
changetype: add
objectclass: inetorgperson
cn: Robert smith
cn: Robert J Smith
cn: Bob Smith
telephonenumber: 123-111

dn: cn=Robert Smith,ou=people,dc=example,dc=com
changetype: delete
```

3.2 Changer le nom ou l'emplacement d'une entrée et créer une copie ou non

```
dn: cn=Robert Ssmith,ou=people,dc=example,dc=com
changetype: modrdn
newrdn: Robert Smith
deleteoldrdn: 1


dn: cn=Robert Smith,ou=people,dc=example,dc=com
changetype: modrdn
newrdn: Robert Smith
deleteoldrdn: 1
newsuperior: ou=expeople,dc=example,dc=com


dn: cn=Robert Smith,ou=people,dc=example,dc=com
changetype: modrdn
newrdn: Robert Smith
deleteoldrdn: 0
newsuperior: ou=expeople,dc=example,dc=com
```

3.3 Ajouter un attribut et des valeurs, ou les effacer

```
dn: cn=Robert Smith,ou=people,dc=example,dc=com
changetype: modify
add: telephonenumber
telephonenumber: 123-111
```

```
dn: cn=Robert Smith,ou=people,dc=example,dc=com
changetype: modify
add: telephonenumber
telephonenumber: 555-123-1111
telephonenumber: 111

dn: cn=Robert Ssmith,ou=people,dc=example,dc=com
changetype: modify
delete: telephonenumber
telephonenumber: 123-111
telephonenumber: 111

dn: cn=Robert Ssmith,ou=people,dc=example,dc=com
changetype: modify
delete: telephonenumber
```

3.4 Changer les valeurs d'un attribut

```
dn: cn=Robert Smith,ou=people,dc=example,dc=com
changetype: modify
# replaces ALL telephonenumber attributes
# with 555-111-1212
replace: telephonenumber
telephonenumber: 555-111-1212

# to replace a single value of a multi attribute value
# delete then add

dn: cn=Robert Smith,ou=people,dc=example,dc=com
changetype: modify
# first delete the required attribute
delete: telephonenumber
telephonenumber: 555-111-1212
# SEPARATOR line essential
-
# add new value
add: telephonenumber
telephonenumber: 555
```

4 Requêtes par l'exemple

Une requête a plein de paramètres
– L'endroit de l'arbre ou commence la recherche
– La profondeur de la recherche
– Le filtre de recherche
– Les attributs que l'on veut connaître
La profondeur de la recherche peut valoir `base` (juste un noeud), `onelevel search` (le niveau suivant), `subtree` (le sous-arbre).

Il y a plein de façons de faire une requête. On présente ici uniquement les URIs LDAP. Elles sont de la forme `ldap://host/base_dn?attr?scope?filter`. Ces paramètres correspondent (mais pas dans l'ordre) aux quatre paramètres cités précédemment.
Le filtre de recherche, qu'on met toujours entre parenthèses, est formé ainsi
- `(attr=name)` pour chercher les entrées dont l'attribut `attr` existe et vaut `name`. Les wildcard ($\star$) sont acceptées.
- `(&(a)(b)(c))` pour les entrées qui vérifient les trois sous-filtres a,b,c.
- `(|(a)(b)(c))` et `{!(a)}` pour ce qu'on pense.

1. Écrire une requête qui cherche le nom de l'utilisateur rjsmith.

2. Écrire une requête qui renvoie tous les logins.

5 ACL

LDAP supporte deux méthodes d'accès aux données d'un annuaire : le mode authentifié, et le mode anonyme.
On restreint les droits grâce aux ACL (Access control lists). L'ordre des ACL est significatif : les règles s'appliquent dans l'ordre.
Les différents droits sont les suivants :
- read : permet de lire la valeur d'un attribut
- search : permet de lire et de faire une recherche sur cet attribut
- write : permet de modifier l'attribut
- plein d'autres

3. Comprendre les ACLs suivantes :

```
access     to dn.subtree="ou=people,dc=example,dc=com" attr=userPassword
     by self write
     by dn="ou=Manager,dc=example,dc=com" write
     by anonymous auth
access     to dn.subtree="ou=people,dc=example,dc=com"
     by self write
     by dn="ou=Manager,dc=example,dc=com" write
     by users read
access     to *
     by *  read
```