Mini-projet : Annuaire des étudiants RT2 de l'IUT

Pouchoulon

Consignes

L'objectif de ce mini-projet est d'implémenter de façon individuelle un annuaire OPENLDAP des étudiants de RT2 et de rattacher dans l'annuaire chaque étudiant à son groupe de TP . La création des entrées LDIF se fera à l'aide d'un script BASH que vous réaliserez. Il se déroule sur deux séances de TP soit cette 1/2 journée. Les livrables à fournir impérativement à 18 heures sont :

- Un script de création en BASH des entrées étudiants et sa sortie au format LDIF (12 points).Le LDIF contiendra toutes les entrées de la promotion RT2.
- Vous rendrez aussi ce soir un fichier ldapout1.log contenant le résultat de la commande suivante :

  ```
  ldapsearch -x -LLL -H ldap:/// -b dc=iutbeziers,dc=fr > ldapout1.log
  ```

- Un fichier dn_groupe.log contenant le résultat de la commande suivante(8 points) et montrant que chaque étudiant est rattaché dynamiquement à un groupe :

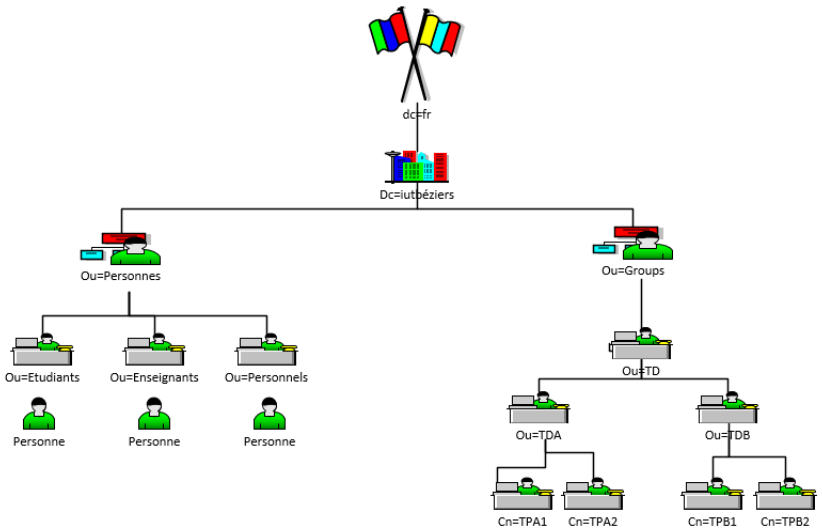
  ```
  ldapsearch -x -LLL -H ldap:/// \
  -b ou=etudiants,ou=personnes,dc=iutbeziers,dc=fr memberof > dn_groupe.log
  ```

  ainsi que l'explication de l'utilité de l'overlay refint.

L'installation de l'annuaire se fera sur une VM en DEBIAN Jessie avec les packages standards.

Entrées du projet et cahier des charges

1. Le schéma suivant montre quel est l'organisation choisie pour le DIT :



   Les entrées enseignants et personnels sont hors du scope de ce TP.

2. Le ldif suivant vous permettra de créer les entrées nécessaires pour les OU et les groupes.

   ```
   dn: ou=groups,dc=iutbeziers,dc=fr
   objectClass: top
   ```

```
objectClass: organizationalunit
ou: groups
description: Branche Groupes

dn: ou=personnes,dc=iutbeziers,dc=fr
objectClass: top
objectClass: organizationalunit
ou: personnes
description: Groupes de personnes

dn: ou=etudiants,ou=personnes,dc=iutbeziers,dc=fr
objectClass: top
objectClass: organizationalunit
ou: etudiants
description: Groupes d'etudiant

dn: ou=TD,ou=groups,dc=iutbeziers,dc=fr
objectClass: top
objectClass: organizationalunit
ou: TD
description: Groupes de TDs

dn: ou=TDA,ou=TD,ou=groups,dc=iutbeziers,dc=fr
objectClass: top
objectClass: organizationalunit
ou: TDA
description: Groupe de TD A

dn: ou=TDB,ou=TD,ou=groups,dc=iutbeziers,dc=fr
objectClass: top
objectClass: organizationalunit
ou: TDB
description: Groupe de TD B
```

3. Le fichier cvs liste_tous.csv stocké sur l'ENT vous permettra de générer des entrées au format ldif L'entrée à générer pour chaque étudiant sera de la forme :

```
dn: uid=aouandhume,ou=etudiants,ou=personnes,dc=iutbeziers,dc=fr
objectClass: inetOrgPerson
objectClass: person
objectClass: organizationalPerson
objectClass: posixAccount
objectClass: shadowAccount
objectClass: top
cn: aouita.andhume
sn: aouita
givenName: andhume
uid: aouandhume
uidNumber: 1001
gidNumber: 1001
homeDirectory: /home/aouandhume
loginShell: /bin/bash
shadowExpire: 0
userPassword: {SSHA}RWK9BASh/NsGzi0k4XLRm1Xt1DoEceJvtB1h1w==
mail: aouita.andhume@iutbeziers.fr
```

L' uid est composé des trois premières lettres du prénom (afin d'éviter les doublons) et du nom. Le password sera le même pour tous. Le mel est au format prénom.nom@iutbeziers.fr. L'uidnumber et le gidnumber seront identiques dans une même entrée et commenceront à 1001. Vous pouvez utilisez

si vous le souhaitez la fonction de création des entrées étudiants suivantes :

```
ecrireEntree() {
 NOM=$(echo $1|tr '[:upper:]' '[:lower:]')
 COMPTEUR=$2
 PRENOM=$(echo $3|tr '[:upper:]' '[:lower:]')
 #echo "$COMPTEUR"
 MYUID=${PRENOM:0:3}${NOM:0:8}
 #echo $MYUID
 SSHA="{SSHA}"
 echo  "dn: uid=${MYUID},ou=etudiants,ou=personnes,dc=iutbeziers,dc=fr"
 echo  "objectClass: inetOrgPerson"
 echo  "objectClass: person"
 echo  "objectClass: organizationalPerson"
 echo  "objectClass: posixAccount"
 echo  "objectClass: shadowAccount"
 echo  "objectClass: top"
 echo  "cn: ${PRENOM}.${NOM}"
 echo  "sn: ${PRENOM}"
 echo  "givenName: ${NOM}"
 echo  "uid: ${MYUID}"
 echo  "uidNumber: ${COMPTEUR}"
 echo  "gidNumber: ${COMPTEUR}"
 echo  "homeDirectory: /home/${MYUID}"
 echo  "loginShell: /bin/bash"
 echo  "shadowExpire: 0"
 echo  "userPassword: ${SSHA}RWK9BASh/NsGzi0k4XLRm1Xt1DoEceJvtB1h1w=="
 echo -e  "mail: ${PRENOM}.${NOM}@iutbeziers.fr\n"
}
```

4. Implémentation de l'Overlay memberof : L'overlay memberof vous permettra de générer dynamiquement pour chaque étudiant la liste de ses groupes dans un attribut multi-valué memberof.

```
ldapsearch -x -LLL -H ldap:/// -b ou=etudiants,ou=personnes,dc=iutbeziers,dc=fr memberof
```

```
dn: ou=etudiants,ou=personnes,dc=iutbeziers,dc=fr

dn: uid=aouandhume,ou=etudiants,ou=personnes,dc=iutbeziers,dc=fr
memberOf: cn=TPA2,ou=TDA,ou=TD,ou=groups,dc=iutbeziers,dc=fr

dn: uid=dimannaix,ou=etudiants,ou=personnes,dc=iutbeziers,dc=fr
memberOf: cn=TPA1,ou=TDA,ou=TD,ou=groups,dc=iutbeziers,dc=fr

dn: uid=khaathie,ou=etudiants,ou=personnes,dc=iutbeziers,dc=fr
memberOf: cn=TPB1,ou=TDB,ou=TD,ou=groups,dc=iutbeziers,dc=fr
```

.... L'intérêt de cet overlay est que le groupe n'est saisi qu'une seule fois dans l'annuaire ou niveau de l'entrée "groupe TP" :

```
dn: cn=TPB1,ou=TDB,ou=TD,ou=groups,dc=iutbeziers,dc=fr
changetype: modify
add: member
member: uid=etidruart,ou=etudiants,ou=personnes,dc=iutbeziers,dc=fr
member: uid=erigodard,ou=etudiants,ou=personnes,dc=iutbeziers,dc=fr
member: uid=valhebert,ou=etudiants,ou=personnes,dc=iutbeziers,dc=fr
member: uid=alejaeg,ou=etudiants,ou=personnes,dc=iutbeziers,dc=fr
```

..... L'overlay memberof s'implémente très simplement dans la configuration de l'annuaire à partir de fichier LDIF. Créez le ldif suivant et ajoutez le au schéma :

```
dn: cn=module,cn=config
cn: module
```

```
objectClass: olcModuleList
olcModuleLoad: memberof
olcModulePath: /usr/lib/ldap

dn: olcOverlay={0}memberof,olcDatabase={1}mdb,cn=config
objectClass: olcConfig
objectClass: olcMemberOf
objectClass: olcOverlayConfig
objectClass: top
olcOverlay: memberof
olcMemberOfDangling: ignore
olcMemberOfRefInt: TRUE
olcMemberOfGroupOC: groupOfNames
olcMemberOfMemberAD: member
olcMemberOfMemberOfAD: memberOf
```

```
ldapadd -Q -Y EXTERNAL -H ldapi:/// -f memberof_load_configure.ldif
```

L'entrée du groupe de TP aura cette forme :

```
objectClass: top
objectClass: groupOfNames
dn: cn=TPB1,ou=TDB,ou=TD,ou=groups,dc=iutbeziers,dc=fr
member: uid=etidruart,ou=etudiants,ou=personnes,dc=iutbeziers,dc=fr
member: uid=erigodard,ou=etudiants,ou=personnes,dc=iutbeziers,dc=fr
member: uid=valhebert,ou=etudiants,ou=personnes,dc=iutbeziers,dc=fr
member: uid=alejaeg,ou=etudiants,ou=personnes,dc=iutbeziers,dc=fr
...
cn: TPB1
description: Groupe TPB1
```

NB : Pour faire apparaitre l'attribut memberof il faut le demander expressement comme attribut lors de votre ldapsearch ou faire apparaître les attributs techniques avec "+". Attention vous utilisez mdb comme backend il faut donc adapter les "how-to".

5. Implémentation de l'Overlay refint
   Créez le ldif suivant :

```
dn: cn=module{1},cn=config
add: olcmoduleload
olcmoduleload: refint
```

```
ldapadd -Q -Y EXTERNAL -H ldapi:/// -f ./1refint.ldif
```

Créez le ldif suivant :

```
dn: olcOverlay={1}refint,olcDatabase={1}mdb,cn=config
objectClass: olcConfig
objectClass: olcOverlayConfig
objectClass: olcRefintConfig
objectClass: top
olcOverlay: {1}refint
olcRefintAttribute: memberof member manager owner
```

```
ldapadd -Q -Y EXTERNAL -H ldapi:/// -f ./2refint.ldif
```

Montrez par un ldapdelete à quoi sert cet overlay :

Des tutos, des liens

— http://www.adimian.com/blog/2014/10/how-to-enable-memberof-using-openldap/
— http://www.zytrax.com/books/ldap/ch11/groups.html
— http://www.openldap.org/doc/admin24/overlays.html