TP 2 LDAP Search Complement

La commande *ldapsearch* est composée principalement de quatre paramètres importants

- L'URI d'accès réseaux à l'annuaire
- Login et Mot de passe (-D -W ou -w).
- DN de recherche (-b) spécifie la base de recherche. Il s'agit du nœud racine à partir duquel commencera la recherche dans toutes les sous branches (le point de départ de la recherche). Tous les nœuds (entrées) au-dessous de ce niveau dans l'arbre sont recherchés. Il faut spécifier un DN de base correcte pour obtenir les résultats souhaités.
- Le filtre qui représente une chaîne de requête qui filtre les entrées d'un annuaire LDAP et génère les enregistrements correspondants. Il est possible de créer des filtres complexes en utilisant une combinaison des symboles suivants : & (AND), | (OU) ! (PAS), caractères jokers, () parenthèses pour l'imbrication

Pour maitriser la création de chaînes de filtres LDAP, reportez-vous aux livres LDAP et aux ressources en ligne, y compris la norme LDAP, RFC 2254, *The String Representation of LDAP Search Filters.*

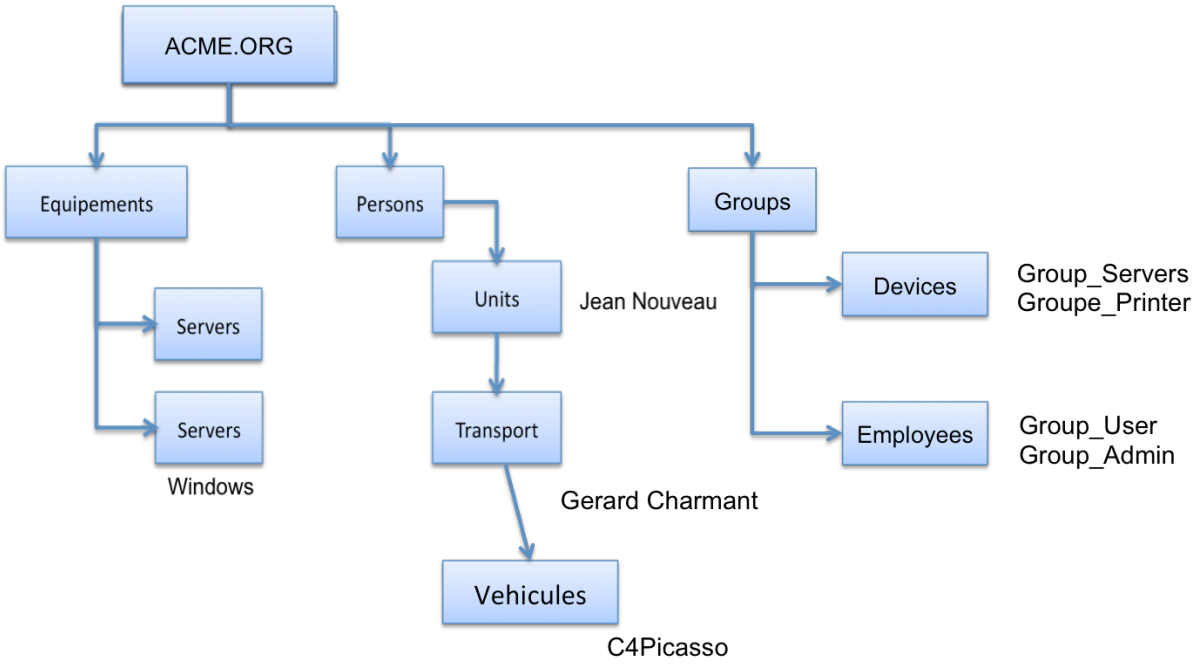
Quelques exemples de commandes :

```
ldapsearch -x -s base (objectclass=*) namingContexts


ldapsearch \
    -x -h localhost \
    -D " cn=admin,dc=company,dc=local" \
    -W \
    -b "dc=company,dc=local" \
    -s sub "(cn=*)" cn mail sn
ldapsearch \
    -x -h localhost \
    -D "cn=admin,dc=company,dc=local" \
    -W \
    -b "dc=company,dc=local" "cn=James Brown"\
    -s sub "(cn=*)" cn mail sn
```

Partie 1 : Création de l'annuaire ACME.ORG

Dans une machine virtuelle linux, il faut installer les packages slapd et ldap-utils. Utilisant la commande dpkg-reconfigure, il faut créer une instance d'un annuaire dont le domaine est ACME.ORG et le nom de l'organisation est « Entreprise ACME ». En utilisant le client windows LDAPAdmin, il faut configurer un accès à l'annuaire ACME.ORG et créer les objets donnés dans le schéma suivant. Vous devez réutiliser les fichiers ldif crées dans les séances de TPs précédentes mais en modifiant les valeurs des attributs pour que ça correspond à l'annuaire ci-dessus.



Point de Contrôle N°1

Appelez le responsable pour vérifier l'avancement de votre travail

Partie 2 : Recherches simples

Retourner toutes les entrées de l'annuaire

La commande suivante renvoi toutes les entrées sur l'hôte RT108-02 via le port 389 avec renvoi de tous les attributs et de toutes les valeurs (sous réserve des limites de taille et de temps configurées dans les paramètres systèmes du serveur annuaire) :

```
ldapsearch -D "cn=admin,…,dc=ACME,dc=CORP" -w vitrygtr -p 389 -h RT108-02 -b "dc=ACME,dc=CORP" -s sub "(objectclass=*)"
```

"objectclass=*" est un filtre de recherche qui correspond à n'importe quelle entrée de l'annuaire puisque chaque entrée doit avoir une classe d'objets et que l'attribut objectclass est toujours indexé. Il s'agit d'un filtre de recherche utile pour retourner toutes les entrées.

Question 1 : Donner la commande ldapsearch permettant de chercher tous les objets de l'annuaire. Combien d'objets retournés dans le résultat.

Il est possible d'écrire la requête ci-dessus d'une manière simplifiée.

```
ldapsearch -h RT108-02 "(objectclass=*)"
```

Un autre exemple d'une requête simplifié qui renvoi les noms d'attributs uniquement

```
ldapsearch -A -h RT108-02 "(objectclass=*)"
```

Un autre exemple d'une requête simplifié qui renvoi seulement les attributs mail, cn, sn, givenname

```
ldapsearch -h RT108-02 "(objectclass=*)" mail cn sn givenname
```

Question 2 : Donner la commande ldapsearch permettant de chercher tous les objets de l'annuaire et renvoyer seulement les attributs cn et objectclass.

Opération 2 : Spécification d'un niveau de recherche

L'option -s (Scope) spécifie le périmètre de recherche. Il s'agit d'une option différente du DN de recherche qui spécifie le point de départ de la recherche. L'attribut Scope indique le niveau de profondeur auquel la recherche est effectuée.
Il est possible de spécifier deux niveaux de profondeur :

- One Level (Un seul niveau) : indique que la recherche de toutes les entrées sera effectué à un niveau sous le DN de base, mais n'inclut pas le DN de base lui-même.
- Sub-Tree Level (sous-arbre) : indique que la recherche de toutes les entrées sera effectué à tous les niveaux sous le DN de base, y compris le DN de base lui-même.

L'exemple suivant concerne une requête simplifié qui renvoie toutes les entrées de l'annuaire via le port 389 avec affichage de tous les attributs et de toutes les valeurs

```
ldapsearch -s onelevel -h RT108-02 "(objectclass=*)"
```

Question 3 : Donner la commande ldapsearch permettant de chercher tous les objets de l'annuaire ACME à partir de la racine et en se limitant à un seul niveau. Le résultat de la commande doit renvoyer seulement les attributs cn, ou et objectclass.

Question 4 : Donner la commande ldapsearch permettant de chercher tous les objets de l'annuaire ACME à partir de la racine et en se limitant à un seul niveau. Le résultat de la commande doit renvoyer seulement les attributs cn, ou et objectclass.

Point de Contrôle N°2

Appelez le responsable pour vérifier l'avancement de votre travail

Partie 2 : Recherches avec des filtres

Spécification des filtres de recherche sur les attributs des objets
La requête suivante inclut un filtre de recherche sur les valeurs des attributs. Le filtre est spécifié directement en ligne de commande comme paramètre de ldapsearch. Le filtre est entouré de guillemets ("cn=etudiant1234"). Ce dernier permet de chercher tout objet dont la valeur du cn est exactement etudiant1234.

```
ldapsearch -D "cn=admin,…,dc=ACME,dc=CORP" -w vitrygtr -p 389 -h RT108-02 -b "dc=ACME,dc=CORP" -s sub "cn=etudiant1234"
```

Question 5 : Donner la commande ldapsearch permettant de chercher tous les objets de l'annuaire ACME ayant apartenant à la classe « InetOrgPerson » et en utilisant comme racine de recherche la branche « OU=Units, OU=Persons, … ». Vous devez limiter la recherche à un seul niveau. Le résultat de la commande doit renvoyer seulement les attributs cn, sn, uid, et objectclass.

Spécification des filtres de recherche à l'aide d'un fichier
Les filtres de recherche peuvent être saisis dans un fichier au lieu d'être saisis sur la ligne de commande. Dans ce cas, spécifiez chaque filtre de recherche sur une ligne distincte du fichier. La commande ldapsearch exécute chaque recherche dans l'ordre dans lequel elle apparaît dans le fichier.

Prenons comme exemple le fichiers persons.txt ci-dessous

```
sn=Francis

givenname=Richard
```

ldapsearch trouve d'abord toutes les entrées avec l'attribut sn « Surname » égal à Francis, puis toutes les entrées avec l'attribut givenname égal à Richard. Si une entrée correspondant aux deux critères de recherche est trouvée, l'entrée est retournée deux fois.

L'ensemble des attributs retournés ici peut être limité en spécifiant les noms des attributs à la fin de la ligne de recherche. Par exemple, la commande ldapsearch suivante effectue les deux recherches mais retourne uniquement le DN et les attributs prénom et sn de chaque entrée :

```
ldapsearch -D "cn=admin,…,dc=ACME,dc=CORP" -w vitrygtr -p 389 -h RT108-02 -b "dc=ACME,dc=CORP" -f persons.txt sn givenname
```

Question 6 : Donner la commande ldapsearch permettant de chercher tous les objets de l'annuaire ACME et en utilisant comme racine de recherche la branche « OU=Units,

OU=Persons, … ». La recherche doit utiliser un objectclass = InetOrgPerson et sn=Ch*. La recherche doit parcourir tous les noeuds sous la branche OU=Units. Le résultat de la recherche doit renvoyer seulement les attributs cn, sn, uid, et objectclass.

Spécification de filtres contenant des caractères jokers

Le filtre fait référence à une sous-chaîne « substring » qui désigne toute valeur de chaîne de caractères. Un filtre de recherche peut contenir des caractères Jokers (Wildcards). La forme de la comparaison, par exemple, sensible ou non à la casse est définie par la règle SUBSTR dans la définition des attributs.

Question 7 : Donner les commandes ldapsearch permettant de chercher les objets de l'annuaire ACME correspondants au filtres donnés dans le listing ci-dessous.

```
(mail=*) # retourne toutes les entrées qui ont un attribut mail
(mail=*@*) # retourne les entrées ayant une adresse mail RFC822 valide
(sn=Nouveau) # retourne les entrées ayant un attribut sn avec une valeur qui correspond exactement à Nouveau
(sn=G*) # retourne les entrées avec des attributs sn commençant par s ou S
(cn=*u*a*) # retourne les entrées avec des noms communs (attribut cn) contenant a et i n'importe où
(telephonenumber=*555) # retourne les entrées avec des numéros de téléphone qui se terminent par 555
(objectclass=person) # retourne les entrées qui sont crées avec la classe d'objets person
```

Point de Contrôle N°3

Appelez le responsable pour vérifier l'avancement de votre travail

Spécification de filtres avec les opérateurs logiques

Il est possible de définir des filtres complexes en combinant ou imbriquant plusieurs expressions en utilisant des opérateurs logiques & (AND), ! (NOT) and | (OR).

Question 8 : Donner les commandes ldapsearch permettant de chercher les objets de l'annuaire ACME correspondants au filtres donnés dans le listing ci-dessous. Expliquer le rôle de chaque filtre.

Le listing ci-dessous donne des exemples de filtres complexes avec des opérateurs logiques et des caractères jokers.

```
a) (&(mail=*)(cn=*u)(sn=N*)) #
b) (|(sn=a*)(sn=b*)(sn=c*)) #
c) (!(sn=a*)) #
d) (&(!(sn=a*))(!(sn=b*))) #
e) (&amp;(sn=*a)(!(sn=s*))) #
```

```
f)   (&(sn=a*)(sn=b*)(sb=c*)) #
```

Question 9 : Certains filtres dans le listing ci-dessus ne donner aucun résultat. Pour y remédier merci de créer ou mettre à jours pour chaque filtre un ou plusieurs objets dans l'annuaire pour faire en sorte que la recherche devient fructueuse.

Spécification de filtres pour chercher des caractères spéciaux

Il est possible de rechercher des objets dont les valeurs des attributs contiennent un ou plusieurs caractères spéciaux (*) (\ ou NULL). Pour ce faire il faut utiliser le code hexadécimal du caractère spécial représentant ce dernier dans le codage ASCII. De même, toute valeur binaire peut être recherchée en utilisant sa valeur hexadécimale.

Le listing ci-dessous donne des exemples de codes des caractères spéciaux

```
\2a replaces or escapes *
\28 replaces or escapes (
\29 replaces or escapes )
\5c replaces or escapes \
\00 replaces or escapes NUL
\xx search for hexadecimal value
    where xx lies in range 00 - FF
```

Question 10 : Donner les commandes ldapsearch permettant de chercher les objets de l'annuaire ACME correspondants au filtres donnés dans le listing ci-dessous. Expliquer le rôle de chaque filtre. Certains filtres dans le listing ci-dessus ne donner aucun résultat. Pour y remédier merci de créer ou mettre à jours pour chaque filtre un ou plusieurs objets dans l'annuaire pour faire en sorte que la recherche devient fructueuse.

```
(homedir=/home/etudiant) #
(description=*\28*\29) #
(group=\5b\04) #
```

Point de Contrôle N°4

Appelez le responsable pour vérifier l'avancement de votre travail

Partie 3 : Recherches techniques pour l'administration de l'annuaire

Spécification de requêtes de recherche avec des DN qui contiennent des virgules

Lorsqu'un DN dans une requête de recherche contient le caractère virgule comme faisant partie de sa valeur, la virgule doit être pris en compte avec une barre oblique inverse (\). Par

exemple, pour trouver tout le monde qui se trouve sous la branche l=*Bolivia, S.A,dc= dc=ACME,dc=CORP* utilisez la commande suivante :

```
ldapsearch -D "cn=admin,…,dc=ACME,dc=CORP" -w vitrygtr -p 389 -h RT108-02 -b "l=Bolivia\,S.A.,dc=ACME,dc=CORP" "objectclass=*"
```

Question 11 : Donner les commandes ldapsearch permettant de chercher les objets qui sont membres du groupe Groupe_User ou du groupe Groupe_Admin. Attention vous devez utiliser le filtre sur l'attribut member. Ce dernier est utilisé pour relier un objet utilisateur avec un ou plusieurs objets groupes. Par conséquent cette attribut doit avoir comme valeurs des dn.

Recherche de l'entrée DSE racine
Le DSE racine est une entrée spéciale qui contient une liste de tous les suffixes des dns des objets enregistrés dans l'annuaire. Cette entrée spéciale peut être recherchée avec la commande ldapsearch en fournissant une base de recherche vide avec l'option -b et un champ de recherche de type base, et le filtre "objectclass=*".

```
ldapsearch -D "cn=admin,…,dc=ACME,dc=CORP" -w vitrygtr -p 389 -h RT108-02 -b "" -s base "objectclass=*"
```

Question 12 : Donner le résultat de la commande ldapsearch pour afficher l'entrée DSE de l'annuaire ACME.

Recherche d'une entrée donnée dans le schéma de l'annuaire
Directory Server stocke tous les schémas du serveur ldap dans l'entrée spéciale cn=schema. Cette entrée contient les descriptions de chaque classe d'objets et les attribut de ses dernières. La commande suivante permet d'afficher toutes les classes définies sous l'entrée cn=schema

```
ldapsearch -D "cn=admin,…,dc=ACME,dc=CORP" -w vitrygtr -p 389 -h RT108-02 -b "cn=schema" -s base "objectclass=*"
```

Question 13 : Donner la commande ldapsearch pour afficher la description de la classe Account et la classe InetOrgPerson. Quel est le type de ces deux classes (Structural ou Auxiliary).

Rechercher des attributs opérationnels

Les attributs opérationnels sont des attributs spéciaux définis par le serveur d'annuaire lui-même. Ces attributs sont utilisés par le serveur d'annuaire pour effectuer des tâches de contrôle et de maintien de l'annuaire comme par exemple le contrôle d'accès. Ces attributs sont des informations spécifiques comme l'heure de la création initiale de l'objet et le nom de l'utilisateur qui l'a créée, etc. En général, les attributs opérationnels ne font pas parti de la classe de l'objet et peuvent être utilisés pour chaque entrée d'annuaire.
Les attributs opérationnels ne sont pas retournés dans les résultats de la requête ldapsearch. Pour retourner les attributs opérationnels, ces derniers doivent être soit explicitement spécifiés dans la requête. L'utilisation du + permet en revanche de retourner toute la liste des objets et attributs opérationnels.

```
ldapsearch -D "cn=admin,…,dc=ACME,dc=CORP" -w vitrygtr -p 389 -h RT108-02 -b "dc=ACME,dc=CORP" -s sub "(objectclass=*)" creatorsName createTimestamp modifiersName modifyTimestamp
```

Question 14 : Donner la commande ldapsearch pour trouver à quel moment l'objet Jean Nouveau a été créé et par qui.

La commande suivante permet de retourner tous les objets et les attributs opérationnels de l'annuaire

```
ldapsearch -D "cn=admin,…,dc=ACME,dc=CORP" -w vitrygtr -p 389 -h RT108-02 -b "dc=ACME,dc=CORP" -s sub "(objectclass=*)" +
```

ou d'une manière plus simple

```
ldapsearch  -h RT108-02 -x -s base -b "" +
```

Question 15 : Donner le résultat de commande ldapsearch ci-dessus sur l'annuaire ACME. Combien existe-il d'objets opérationnels dans l'annuaire ACME ?

Il est possible aussi de faire la recherche du schéma des objets et des attributs opérationnels dans le schéma de l'annuaire suivant cette commande
"cn=subschema"

```
ldapsearch  -h RT108-02 -x -s base -b "" "cn=subschema" objectclasses
```

Question 16 : Donner le résultat de commande ldapsearch ci-dessus sur l'annuaire ACME. Combien existe-il de classes opérationnels dans l'annuaire ACME ?

Question 17 : Donner la requête ldapserach permettant de retourner la description de la classe « account »

```
objectClasses: ( 0.9.2342.19200300.100.4.5 NAME 'account'
  SUP top STRUCTURAL
  MUST userid
  MAY ( description $ seeAlso $ localityName $ organizationName
  $ organizationalUnitName $ host ) )
```

Point de Contrôle N°5

Appelez le responsable pour vérifier l'avancement de votre travail