Nicolas Yang

LDAP

Contexte :

Le protocole LDAP (Lightweight Directory Access Protocol) est un protocole permettant d'interroger et de modifier un service d'annuaire basé sur X.500 s'exécutant sur TCP / IP.
Ainsi, le protocole LDAP accède aux répertoires LDAP. Voici quelques concepts et termes clés:

1. Un répertoire LDAP est une arborescence d'entrées de données de nature hiérarchique qui est appelée arborescence du répertoire d'information (DIT).
2. Une entrée se compose d'un ensemble d'attributs.
3. Un attribut possède un type (un nom/description) et une ou plusieurs valeurs.
4. Chaque attribut doit être défini dans au moins une classe d'objet.
5. Les attributs et classes d'objets sont définis dans les schémas (une classe d'objet est en fait considérée comme un type particulier d'attribut).
6. Chaque entrée a un identifiant unique: son nom unique (DN ou dn). Celui-ci, à son tour, consiste en un nom distinctif relatif (RDN) suivi du DN de l'entrée parent.
7. Le DN de l'entrée n'est pas un attribut. Il n'est pas considéré comme faisant partie de l'entrée elle-même.

Tutoriel

Installez OpenLDAP

OpenLDAP est un des annuaires les plus répandus. Pour l'installer, vous devrez installer le paquet `slapd` . Installez également le paquet `ldap-utils` qui contient les utilitaires clients pour pouvoir interroger ou modifier votre annuaire.

```
$ sudo apt-get install slapd ldap-utils
```

À l'installation de slapd, on vous demandera d'entrer le mot de passe de l'administrateur de votre annuaire. Pas besoin de le rentrer car vous allez refaire cette opération dans un instant.
Voilà, vous avez installé votre annuaire. Vous allez maintenant utiliser l'outil de configuration debconf de Debian pour définir la configuration de base de votre annuaire :

```
$ sudo dpkg-reconfigure slapd
```

Indiquez :

- No pour la première question afin de pouvoir utiliser l'outil de configuration
- pour nom DNS : mon-entreprise.com
- pour nom d'organisation : mon-entreprise

- le mot de passe administrateur x2
- choisissez le format de base par défaut : mdb
- No pour savoir si la base doit être supprimée quand slapd est purgé
- Yes pour déplacer l'ancienne base de données

Comme votre DNS est mon-entreprise.com, la racine de votre DIT a été configurée à "dc=mon-entreprise,dc=com", vous pouvez utiliser la commande ldapsearch suivante pour visualiser votre DIT :

```
$ sudo ldapsearch -Q -L -Y EXTERNAL -H ldapi:/// -b dc=mon-entreprise,dc=com
version: 1

#
# LDAPv3
# base <dc=mon-entreprise,dc=com> with scope subtree
# filter: (objectclass=*)
# requesting: ALL
#

# mon-entreprise.com
dn: dc=mon-entreprise,dc=com
objectClass: top
objectClass: dcObject
objectClass: organization
o: mon-entreprise
dc: mon-entreprise

# admin, mon-entreprise.com
dn: cn=admin,dc=mon-entreprise,dc=com
objectClass: simpleSecurityObject
objectClass: organizationalRole
cn: admin
description: LDAP administrator

# search result

# numResponses: 3
# numEntries: 2
```

La commande `ldapsearch` sert, comme son nom l'indique à chercher dans un annuaire LDAP. Voici le détail des options utilisées :

-Q	active le mode silencieux pour l'authentification SASL
-Y	indique le mode SASL choisi pour l'authentification. Normalement, EXTERNAL implique une authentification par certificat client mais dans ce cas là ça signifie que l'authentification se fera par l'UID et le GID du compte système. C'est pour ça que vous devez lancer la commande avec "sudo". L'utilisateur root a des passe-droits pour accéder à la base locale LDAP
-L	indique d'afficher le résultat au format LDIF. On aurait pu indiquer `-LLL` pour avoir la même chose sans toutes les lignes commentées.
-H	indique l'URI qu'on veut utiliser pour se connecter. Ici `ldapi:///` dit de se connecter à la socket Unix en local (la communication passe par un fichier local plutôt que par le réseau).
-b	indique le noeud à partir duquel vous voulez faire votre recherche. Ici `dc=mon-entreprise,dc=com` est la racine donc vous recherchez dans tout le DIT. À la suite du noeud, vous auriez pu indiquer des filtres pour votre recherche mais sans filtre vous avez l'affichage le plus complet.

Je vais maintenant vous parler un peu du **format LDIF** utilisé pour afficher la réponse de cette commande.

Nicolas Yang

Mode opératoire :

Recherche dans l'annuaire LDAP

```
$ ldapsearch -x -h localhost -p 389 -LL -b "ou=Users,dc=openstack,dc=org" -D "cn=admin,dc=openstack,dc=org" -w password

## ou

$ ldapsearch -x -H ldap://localhost -LL -b "ou=Users,dc=openstack,dc=org" -D "cn=admin,dc=openstack,dc=org" -w password
version: 1

dn: ou=Users,dc=openstack,dc=org
objectClass: organizationalUnit
ou: Users

dn: cn=Robert Smith,ou=Users,dc=openstack,dc=org
objectClass: inetOrgPerson
cn: Robert Smith
cn: Robert J Smith
cn: bob  smith
sn: smith
uid: rjsmith
userPassword:: ckpzbWl0SA==
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

```

Nicolas Yang

```
dn: cn=Larry Cai,ou=Users,dc=openstack,dc=org
objectClass: inetOrgPerson
cn: Larry Cai
sn: Cai
uid: larrycai
userPassword:: TGFycnlDYWk=
carLicense: HISCAR 123
homePhone: 555-111-2222
mail: larry.caiyu@gmail.com
description: hacker guy
```

Options :

- -b : Base DN, point dans l'arbre LDAP ou l'on se positionne pour commencer la recherche
- -D : Bind DN, utilisateur avec lequel on se connecte à LDAP
- -s : Scope
- -w : Bind Password, on fournit le password dans la ligne de commande
- -W : Bind Password, on sera prompter lors du lancement de la commande
- -v : verbose

Suppression

Unitairement

```
$ ldapdelete -xv  -h localhost -D "cn=admin,dc=openstack,dc=org" -w password "cn=Robert Smith,ou=Users,dc=openstack,dc=org"
```

En masse

```
$ cat delete_masse.txt
cn=Larry Cai,ou=Users,dc=openstack,dc=org
cn=Robert Smith,ou=Users,dc=openstack,dc=org



$ ldapdelete -xv  -h localhost -D "cn=admin,dc=openstack,dc=org" -w password -f ./delete_masse.txt
```

Nicolas Yang

Ajout

```
## Fichier LDIF à ajouter :
$ cat more.ldif
dn: cn=Robert Smith,ou=Users,dc=openstack,dc=org
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

dn: cn=Larry Cai,ou=Users,dc=openstack,dc=org
objectclass: inetOrgPerson
cn: Larry Cai
sn: Cai
uid: larrycai
userpassword: LarryCai
carlicense: HISCAR 123
homephone: 555-111-2222
mail: larry.caiyu@gmail.com
description: hacker guy
ou: Development Department


```

```
$ ldapadd -x -D cn=admin,dc=openstack,dc=org -w password -c -f more.ldif
adding new entry "cn=Robert Smith,ou=Users,dc=openstack,dc=org"

adding new entry "cn=Larry Cai,ou=Users,dc=openstack,dc=org"
```

Note : si une entrée existe déjà elle ne sera pas remplacé ni modifié, il faudra utiliser ldapmodify.

Pour plus de ressources https://www.openldap.org/