

Les commandes ldap

Les commandes que nous pouvons effectuer sur OpenLDAP peuvent se diviser en deux grandes catégories. Cette division va vous aider à mieux comprendre leurs utilités et pourquoi ces commandes semblent parfois en double. Nous les diviserons donc comme suit:

- Les outils de gestion de la base de données;
- Les outils de manipulation de l'annuaire LDAP.

Débutons par les commandes de manipulation de l'annuaire LDAP. Toutes ces commandes débutent par le préfixe **ldap**. Ce sont des commandes qui permettent de faire les mêmes tâches que les autres outils de gestion.

ldapadd

La commande *ldapadd* est en fait un "*hard link*" sur l'outil *ldapmodify*. Lorsque vous exécutez *ldapadd*, ce dernier appelle en réalité *ldapmodify* avec le commutateur *-a* (qui permet d'ajouter une nouvelle entrée).

Vous utiliser cette commande, pour ajouter un objet par l'intermédiaire d'un fichier LDIF.

Exemple:

```
ldapadd -x -D "cn=ldapadmin,dc=cybiolab,dc=lan" -W -f test.ldif
```

Enter LDAP Password:

Adding new entry "cn=ldapadmin,dc=cybiolab,dc=lan"

où le fichier LDIF pourrait ressembler à ceci pour la création d'un utilisateur posix. N'utilisez surtout pas cet exemple pour créer des utilisateurs sur votre domaine. Consulter plutôt le prochain module.

```
dn: cn=test,dc=cybiolab,dc=lan
givenName: test
sn: test
uid: ttest
userPassword: {SSHA}$1$3GJcvfb6$VXikf.bp7RXFVGE6x9JBd0
uidNumber: 1025
gidNumber: 513
homeDirectory: /home/test
loginShell: /bin/bash
```

NOTES



```
objectClass: inetOrgPerson
objectClass: posixAccount
objectClass: top
cn: test
displayName : test
```

NOTES



Voici la description des commutateurs utilisés par cet exemple.

| Commutateur | Description |
|------------------|---|
| -f | Permet de spécifier un fichier réponse, généralement en format LDIF. |
| -x | Utilise l'authentification simple au lieu de SASL. |
| -D <i>binddn</i> | Utilise ce DN pour se lier à l'annuaire LDAP. Généralement pour l'administration utiliser toujours votre compte administrateur de l'annuaire. |
| -W | Permet d'afficher un invite pour entrer votre mot de passe. |

Idapcompare

L'outil *Idapcompare* permet d'ouvrir une connexion vers un serveur LDAP spécifique, de se lier, et effectuer une comparaison selon des paramètres que vous avez spécifiés.

Comme dans le prochain exemple, nous allons vérifier que le sn a la valeur test dans l'entrée cn=test,dc=cybiolab,dc=lan.

Exemple:

```
Idapcompare -x -D "cn=ldapadmin,dc=cybiolab,dc=lan" -W
"cn=test,dc=cybiolab,dc=lan" sn:test
```

```
Enter LDAP Password:
TRUE
```

Idapmodify

L'outil *Idapmodify* permet d'ouvrir une connexion vers un serveur LDAP spécifique, de se lier, et modifier ou ajouter une ou plusieurs entrées.

Cet outil est sûrement le plus intéressant et le plus important de tous les outils de manipulation de l'annuaire LDAP.

Le prochain exemple, va nous permettre d'ajouter une entrée dans l'annuaire LDAP comme l'aurait fait la commande `ldapadd`.

Exemple:

```
ldapmodify -a -x -D "cn=ldapadmin,dc=cybiolab,dc=lan" -W -f testmod.ldif
```

```
Enter LDAP Password:  
modifying entry "cn=test,dc=cybiolab,dc=lan"
```

Mais comme son nom l'indique, cette commande va nous permettre d'ajouter, modifier ou supprimer des attributs et objets dans une entrée LDAP.

Dans le prochain exemple, nous allons ajouter l'attribut `description`, modifier l'attribut `loginShell` et supprimer l'attribut `displayName`.

| Commutateur | Description |
|-------------|---|
| -a | Permet d'ajouter une nouvelle entrée. Par défaut <code>ldapmodify</code> permet seulement de modifier un élément déjà existant. |

Exemple:

```
dn: cn=test,dc=cybiolab,dc=lan  
changetype:modify  
add:description  
description:allo  
-  
delete:displayName  
-  
replace:loginShell  
loginShell:/bin/false
```

Faites attention que votre syntaxe soit parfaite, un espace de trop après un attribut ou un espace entre les lignes et plus rien fonctionne.

NOTES



veut associer à l'utilisateur. Le mot de passe LDAP est celui qui nous permet de nous lier à l'annuaire LDAP.

Exemple:

```
ldappasswd -x -D "cn=ldapadmin,dc=cybiolab,dc=lan" -W -S
"cn=test,dc=cybiolab,dc=lan"
```

New password:

Re-enter new password:

Enter LDAP Password:

| Commutateur | Description |
|-------------|---|
| -S | Permet d'afficher un invite pour entrer votre nouveau mot de passe. |

ldapsearch

Cet outil est sûrement le second en important de tous les outils de manipulation de l'annuaire LDAP, mais le plus utilisé.

Exemple:

```
ldapsearch -x -b "dc=cybiolab,dc=lan" -D
"cn=ldapadmin,dc=cybiolab,dc=lan" -W cn=test
```

ou encore

```
ldapsearch -x -LLL -b "dc=cybiolab,dc=lan" -D
"cn=ldapadmin,dc=cybiolab,dc=lan" -W cn=test
```

| Commutateur | Description |
|-------------|---|
| -b | Définit la base pour la recherche dans l'arborescence de l'annuaire LDAP. |
| -L | Le résultat des recherches sera affiché en format LDIF. Un second -L supprime les commentaires. Un troisième -L supprime l'affichage de la version de LDIF. |

Le prochain exemple permet de faire une recherche dans les entrées comprenant l'attribut UID et dont l'attribut description est égale à allo.

NOTES



Exemple:

```
ldapsearch -x -LLL -b "dc=cybiolab,dc=lan" -D  
"cn=ldapadmin,dc=cybiolab,dc=lan" -W "(uid=*)" description:allo
```

Nous n'avons donnée qu'une faible possibilité que renferme cet outil. Nous vous conseillons de regarder son man page pour plus d'information.

Idapwhoami

L'équivalent de la commande whoami sur votre système. Sûrement utile pour les scripts.

Idapdelete

L'outil *ldapdelete* permet d'ouvrir une connexion vers un serveur LDAP spécifique, de se lier, et de supprimer un ou plusieurs objets ou attributs de l'annuaire LDAP.

Exemple:

```
ldapdelete -x -D "cn=root,dc=cybiolab,dc=lan" -W cn=test,  
dc=cybiolab,dc=lan
```

Enter LDAP Password:

Les commandes slap

Passons aux commandes de gestion de la base de données. Ces commandes ne permettent pas de modifier l'annuaire LDAP, mais bien son service slapd. Toutes ces commandes débutent par le préfixe **slap**, justement en référence au service slapd.

slapacl

Permet de vérifier la liste des accès des attributs. L'exemple qui suit va nous donner les ACLs sur l'entrée de l'unité organisationnel Users dans la base cybiolab.lan.

Exemple:

NOTES



```
slapacl -f /etc/openldap/slapd.conf -v -U test -b  
"dc=cybiolab,dc=lan" "ou/read:Users"
```

ajouter -u après la commande slapacl si vous utiliser encore le type de base de données ldbm.

slapadd

L'outil *slapadd* permet d'ajouter une entrée dans l'annuaire LDAP (un peu comme *ldapadd*). Il ne vérifie cependant pas si les entrées supérieures de l'arborescence existe avant d'ajouter l'entrée, il ne fait pas de vérification de tous les utilisateurs et du schéma. Et ne fait pas suivre les attributs opérationnel, tel que *createTimeStamp* ou *modifiersName*.

Exemple:

```
slapadd -l test.ldif
```

slapauth

L'outil *slapauth* permet de faire la vérification du comportement du service slapd dans l'authentification et les autorisations pour un utilisateur selon le fichier de configuration slapd.conf. La réponse sera donnée par un Ok ou un Failed.

Exemple:

```
slapauth -f /etc/openldap/slapd.conf -U ldapadmin -X u:test  
ID: <root>  
authcDN: <uid=ldapadmin,cn=auth>  
authzDN: <uid=test,cn=auth>  
authorization OK
```

slapcat

L'outil *slapcat* permet de générer un fichier au format LDIF (LDAP Directory Interchange Format) selon les éléments de la base de données utilisé par OpenLDAP.

Cet outil est indispensable pour faire une sauvegarde de notre annuaire DLAP.

NOTES



Exemple:

```
slapcat -b "dc=cybiolab,dc=lan" -l cybiolab.ldif
```

ou encore

```
slapcat -b "dc=cybiolab,dc=lan" > /root/cybiolab.ldif
```

Remarquer que dans l'exemple nous spécifions le suffixe, car votre service d'annuaire LDAP peut contenir plusieurs base de donnée. Donc il peut être intéressant de spécifier lequel de ces base de donnée que l'ont désire sauvegarder.

Il se peut qu'avec la base de données ldbm vous ayez l'erreur suivante.

```
ldbm_back_db_open: database already in use
backend_startup_one: bi_db_open failed! (-1)
slap_startup failed
```

Vous devez arrêter le service slapd, faire la sauvegarde et redémarrer le service.

slapdn

L'outil *slapdn* permet de vérifier la conformité d'un DN en fonction du schéma du serveur. N'a pas vraiment d'interaction avec le service slapd et est sûrement plus utile pour les scripts.

Exemple:

```
slapdn -f /etc/openldap/slapd.conf cn=test,dc=cybiolab,dc=lan
```

slapindex

L'outil *slapindex* permet de régénérer l'indexation des bases de données et fait la mise à jour de toutes les valeurs de chacun des attributs des éléments identifié pour l'indexation.

Les valeurs définies pour l'indexation sont déclarées dans le fichier de configuration slapd.conf

Lors de l'utilisation de l'outil slapindex, **votre service slapd ne doit pas fonctionner**. Cette commande s'avère longue et peut nuire

NOTES



considérablement les performances de votre serveur si elle est mal utilisé.

Exemple:

```
slapindex -b dc=cybiolab,dc=lan
```



ATTENTION: Il est absolument important que votre service slapd soit arrêté avant de procéder à la régénération de l'indexation des bases de données LDAP.

NOTES



slappasswd

Déjà décrit dans le module sur OpenLDAP, L'outil *slappasswd* permet de générer des mots de passe selon le type de cryptage désiré.

Les types hachages acceptés peuvent être en texte clair, MD5, SMD5, CRYPT, SHA, SSHA.

Exemple:

```
slappasswd -h {SSHA}  
New password:  
Re-enter new password:  
{SSHA}YnvgpdmGIRgA2
```

slaptest

Vérifie la syntaxe de votre fichier slapd.conf. Après avoir modifié le fichier slapd.conf, il est une bonne habitude d'exécuter cet outil avant de redémarrer votre service.

Exemple:

```
slaptest  
config file testing succeeded
```

