Wiki Enseignement

admin:tp7

TP7 (LDAP)

NIS c'est un peu démodé… Aujourd'hui, on préfère utiliser LDAP.

1) Configuration du serveur LDAP

On configure le serveur LDAP sur la machine *immortal*. Les autres machines servent de client.

```
immortal$ adduser tutu
immortal$ adduser titi
```

Création d'un password pour l'admin LDAP:

```
immortal$ slappasswd
  New password: admin
  Re-enter new password: admin
  {SSHA}XSd0QXLAiNz734f/8QGpaujkMdK5BxWp
```

Editer le fichier /etc/ldap/sldap.conf (attention, pas d'espace en début de ligne) :

```
# nom du domaine LDAP
suffix          "dc=mydomain,dc=fr"

# nom de l'admin
rootdn          "cn=admin,dc=mydomain,dc=fr"

# ajout d'un mot de passe admin
rootpw          "{SSHA}XSd0QXLAiNz734f/8QGpaujkMdK5BxWp"
```

Attention : Ne pas oublier de corriger le nom de domaine pour les ACLs en fin de fichier ! En gros, il faut remplacer tous les @XXXXXXXXX@ !

Nota Bene : dc = domain component

Dans le fichier /etc/default/slapd, modifiez :

```
SLAPD_CONF="/etc/ldap/slapd.conf"
```

Démarrage du serveur LDAP :

```
immortal$ /etc/init.d/slapd start
```

On vérifie que le démon a démarré !

```
immortal$ ps aux |grep slapd
```

2) Ajout des comptes dans le serveur LDAP

On va utiliser un script pour peupler automatiquement la base LDAP avec les comptes des utilisateurs (et d'autres trucs). Editer le fichier /etc/migrationtools/migrate_common.ph, et mettre à jour votre nom de domaine :

```
# Default DNS domain
$DEFAULT_MAIL_DOMAIN = "mydomain.fr";

# Default base
$DEFAULT_BASE = "dc=mydomain,dc=fr";
```

Ensuite, il faut lancer le script :

```
  immortal$ cd /usr/share/migrationtools      # Important : il faut dans ce répertoire...
  immortal$./migrate_all_online.sh            # ... pour lancer le script !

Enter the X.500 naming context you wish to import into: [dc=mydomain,dc=fr]
Enter the hostname of your LDAP server [ldap]: localhost
Enter the manager DN: [cn=admin,dc=mydomain,dc=fr]:
Enter the credentials to bind with:            <-- mot de passe de l'admin !!!
Do you wish to generate a DUAConfigProfile [yes|no]? no

Importing into dc=mydomain,dc=fr...

Creating naming context entries...
Migrating groups...
Migrating hosts...
Migrating networks...
Migrating users...
Migrating netgroups...
Migrating netgroups (by user)...
Migrating netgroups (by host)...
Importing into LDAP...
adding new entry "dc=mydomain,dc=fr"
...
adding new entry "cn=root,ou=Group,dc=mydomain,dc=fr"
...
adding new entry "cn=toto,ou=Group,dc=mydomain,dc=fr"
adding new entry "cn=tutu,ou=Group,dc=mydomain,dc=fr"
adding new entry "cn=titi,ou=Group,dc=mydomain,dc=fr"
...
adding new entry "cn=localhost,ou=Hosts,dc=mydomain,dc=fr"
adding new entry "cn=cinder.localdomain,ou=Hosts,dc=mydomain,dc=fr"
...
adding new entry "uid=toto,ou=People,dc=mydomain,dc=fr"
adding new entry "uid=tutu,ou=People,dc=mydomain,dc=fr"
adding new entry "uid=titi,ou=People,dc=mydomain,dc=fr"
```

En cas d'erreur

Bon, si ça ne marche pas, on fait le ménage :

```
$/etc/init.d/slapd stop
$ rm -rf /var/lib/ldap/*
```

On vérifie ses configs et on recommence !!!

```
$/etc/init.d/slapd start
```

Test du serveur LDAP

On effectue une recherche sur toutes les entrées “objectclass=*”

```
immortal$ ldapsearch -x -b "dc=mydomain,dc=fr" -D "cn=admin,dc=mydomain,dc=fr" "(uid=*)" -W
grave$ ldapsearch -x -h @immortal -b "dc=mydomain,dc=fr" -D "cn=admin,dc=mydomain,dc=fr" "(uid=*)" -W
```

ou plus simplement si tout le monde peut consulter le serveur LDAP (cf. ACL) :

```
immortal$ ldapsearch -x "(uid=*)"
```

Comparer le nombre de répondes avec /etc/passwd sur le serveur :

```
  immortal$ wc -l /etc/passwd
```

L'ajout manuel d'une entrée se fait via un fichier LDIF (cf. manuel) :

```
immortal$ grep tutu /etc/passwd > tutu
immortal$ migrate-passwd.pl tutu > tutu.ldif
immortal$ ldapadd -x -D "cn=admin,dc=mydomain,dc=fr" -W -f tutu.ldif
```

3) Configuration d'un client LDAP

Nota Bene : Il n'y a pas de démon côté client!

Editer le fichier /etc/ldap/ldap.conf sur la machine cliente :

```
BASE    dc=mydomain,dc=fr
URI     ldap://192.168.0.1   <--- IP du serveur LDAP !
```

Un petit test sur le client (pas besoin de mettre l'option -b)

```
$ ldapsearch -x -D "cn=admin,dc=mydomain,dc=fr" "(objectclass=account)" -W
```

4) Authentification via LDAP

Dans le fichier /etc/nsswitch.conf, ajouter ldap

```
passwd:         files ldap
group:          files ldap
shadow:         files ldap
```

Attention : Ne pas oublier *files*, sinon mieux vaut que *ldap* fonctionne du premier coup !!!

```
$ /etc/init.d/nscd restart
```

A partir d'ici, les comptes LDAP sont visibles, mais l'authentification ne marche pas encore, car il faut encore configurer PAM, pour y authoriser l'authentification via LDAP.

On lance la commande suivante et on sélectionne Unix + LDAP.

```
$ pam-auth-update
```

Ensuite :

```
$ dpkg-reconfigure libpam-ldap
$ dpkg-reconfigure libnss-ldapd
```

Attention, il faut saisir ldap://192.168.0.1 [ldap://192.168.0.1] (ET NON ldapi !)

Pour finir :

```
$ dpkg-reconfigure nslcd
```

A vous de jouer… on peut ajouter le serveur NFS !

Test LDAP de UBX

Au CREMI uniquement, vous pouvez interrogez l'annuaire complet. Voici une requête qui interroge le sereur LDAP *cresus* et lui demande des infos sur l'UID *auesnard* (le mien) :

```
ldapsearch -h cresus -x -b "DC=cremi,DC=emi,DC=u-bordeaux1,DC=fr" "(uid=auesnard)"
```

Pour afficher la leste des enseignants :

```
ldapsearch -h cresus -x -LLL -b "DC=cremi,DC=emi,DC=u-bordeaux1,DC=fr" cn=teacher member
```

admin/tp7.txt · Last modified: 2016/03/18 12:20 by orel