

1 Création d'un annuaire LDAP

Nous allons configurer la machine virtuelle *Master* de façon à ce qu'elle devienne serveur LDAP, c'est à dire qu'elle fournisse un service d'annuaire LDAP.

- Ouvrir VirtualBox (Menu Applications → Outils Système → Innotek VirtualBox).
- Sélectionner la machine virtuelle *Master* et cliquer sur le bouton *Lancer* (ou menu Machine → Lancer).
- La machine démarre. Sa fenêtre de console apparaît.
- Ouvrir une session en tant que root (password=r00tme)
- Installer le service OpenLDAP (passer toutes les questions avec la touche entrée) :
`apt-get install slapd ldap-utils`
- Stopper le service LDAP : `/etc/init.d/slapd stop`
- Remplacer le fichier de configuration par celui fourni :
`scp tpldap@192.168.1.1:Public/slapd.conf /etc/ldap/slapd.conf`
- Copier le code LDIF de création de l'arborescence ldap et l'intégrer dans l'annuaire :
 - `scp tpldap@192.168.1.1:Public/arbre.ldif /tmp`
 - `slapadd -l /tmp/arbre.ldif`
- Relancer le service LDAP : `/etc/init.d/slapd start`

Il est important d'exécuter la commande *slapadd* uniquement lorsque l'annuaire est hors-ligne. Sinon, il y a risque de corruption de l'annuaire.

L'annuaire LDAP est maintenant opérationnel sur la machine virtuelle *master*, cependant il ne contient aucune entrée.

2 Alimentation et interrogation de l'annuaire

La première façon de dialoguer avec l'annuaire fraîchement installé, est d'utiliser un logiciel tel que GQ. Il est disponible via le menu *Applications* → *Internet* → *GQ LDAP Client*. Il est nécessaire d'ajouter un serveur via le menu *File* → *Preferences* (Onglet *Servers*). Les paramètres à rentrer sont les suivants :

- Name = **Master**
- LDAP Host = **master**
- LDAP Port = **389**
- Base DN = **dc=mathrice,dc=prive**

L'autre technique consiste à utiliser les outils en ligne de commande. Pour cela, nous utilisons la machine virtuelle *Client* :

- Lancer la machine virtuelle et ouvrir une session root (password=r00tme)
- Dans XTerm, installer les outils de recherche OpenLDAP : `apt-get install ldap-utils`
- Une première recherche permettant de lister le contenu de l'annuaire se fait avec : `ldapsearch -x -h master -b dc=mathrice,dc=prive '(objectClass=*)'`

Jusqu'à présent nous utilisons le mode *anonymous* pour interroger l'annuaire. Cependant pour pouvoir ajouter des entrées à l'annuaire il est nécessaire de s'authentifier et de disposer des permissions suffisantes. Nous utilisons donc l'administrateur de l'annuaire, défini par les directives *rootdn* et *rootpw* du fichier *slapd.conf* pour ajouter des entrées (*rootpw* contient la version hashé du mot de passe de l'administrateur de l'annuaire soit *mot2pass*) :

- `scp tpldap@192.168.1.1:Public/user.ldif /tmp`

```
- ldapadd -x -W -D cn=admin,dc=mathrice,dc=prive -h master -f /tmp/user.ldif
```

Pour s'exercer à manipuler les données de l'annuaire :

- Ajouter une entrée dans la branche *people*
- Créer des groupes d'utilisateurs
- Rechercher les personnes dont le nom (attribut uid) commence par NL
- Supprimer une entrée de l'annuaire (cf. `man ldapdelete`).

3 Sécurisation des échanges

Jusqu'à présent, toutes les transactions circulent en clair sur le réseau. Il suffit de mettre en place un `tcpdump` pour, par exemple, intercepter le mot de passe de l'administrateur de l'annuaire.

Nous allons utiliser la couche SSL pour chiffrer les communications. Nous commençons donc par installer, sur la machine virtuelle *master*, les outils nécessaires avec `apt-get install openssl ca-certificates`.

Nous utilisons donc OpenSSL pour générer un certificat X509. Dans la vraie vie, il est recommandé d'utiliser un certificat généré, par exemple, avec l'IGC du CNRS.

- Génération d'un certificat auto-signé :
`/usr/lib/ssl/misc/CA.pl -newcert`
- Suppression de la passphrase dans la clé privée :
`openssl rsa -in newkey.pem -out newkey-unlock.pem`
- Installation du certificat et de sa clé privée
 - `mv newcert.pem /etc/ldap/slapd-crt.pem`
 - `mv newkey-unlock.pem /etc/ldap/slapd-key.pem`
 - `chmod 644 /etc/ldap/slapd-crt.pem`
 - `chmod 600 /etc/ldap/slapd-key.pem`
 - `chown openldap.openldap /etc/ldap/slapd-*.pem`

Il reste ensuite à indiquer, dans le fichier de configuration d'OpenLDAP, où se trouve le certificat et la clé associée. Puis à relancer le service.

```
TLSCipherSuite          HIGH
TLSCertificateFile      /etc/ldap/slapd-crt.pem
TLSCertificateKeyFile   /etc/ldap/slapd-key.pem
```

Il est maintenant possible, depuis la machine virtuelle *client* de demander à ce que les communications soit chiffrées (option `-Z` de `ldapsearch`).

```
ldapsearch -x -Z -h master -b ou=people,dc=mathrice,dc=prive '(givenName=Mel*)'
```

Nous obtenons le message d'erreur ci-dessous. Il indique que le certificat ne peut pas être vérifié.

```
ldap_start_tls: Connect error (-11)
additional info: error:14090086:SSL routines:SSL3_GET_SERVER_CERTIFICATE
:certificate verify failed
```

Le certificat utilisé ne provient pas d'une IGC, nous ne pouvons donc pas configurer la bibliothèque OpenLDAP de façon à ce qu'elle reconnaisse tout les certificats issus de cette autorité. Nous désactivons donc, dans le fichier `/etc/ldap/ldap.conf`, la vérification des certificats en ajoutant la ligne `TLS_REQCERT never`.

Dans le cas où le certificat provient d'une IGC, le fichier pointé par la directive `TLS_CACERT` correspond au certificat racine de l'autorité de certification.

Un nouvel essai de la recherche devrait donner un résultat positif.

A la fin du fichier de configuration du serveur OpenLDAP (*slapd.conf*), sont définis des listes de contrôle d'accès (ACL). Elles spécifient quels utilisateurs peuvent accéder aux différents attributs des entrées de l'annuaire. En s'aidant des deux exemples et de la documentation, écrire une règle autorisant le propriétaire d'une entrée à modifier son adresse électronique (attribut `mail`).

4 Authentification avec un client GNU/Linux

La configuration concerne deux points distinct :

- la résolution des numéros d'utilisateurs en nom (NSS);
- l'authentification (PAM).

Commençons par configurer la résolution des noms d'utilisateurs. Installons les paquets nécessaire ainsi que le fichier de configuration idoine.

- `apt-get install libnss-ldap` (Ignorer les questions avec entrée)
- `mv /etc/libnss-ldap.conf /etc/libnss-ldap.pkg`
- `scp tpldap@192.168.1.1:Public/libnss-ldap.conf /etc`

Il reste ensuite à modifier le fichier */etc/nsswitch.conf* de façon à avoir :

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

La commande `getent passwd` affiche maintenant les utilisateurs enregistrés dans l'annuaire LDAP.

Nous configurons le système PAM de façon à ce que l'ouverture d'une session graphique puisse se faire au moyen d'un compte enregistré dans l'annuaire LDAP. Tous les utilisateurs du fichier *user.ldif* possèdent le même mot de passe, soit `azerty`.

- `apt-get install libpam-ldap`
- `mv /etc/pam_ldap.conf /etc/pam_ldap.pkg`
- `scp tpldap@192.168.1.1:Public/pam_ldap.conf /etc`
- `scp tpldap@192.168.1.1:Public/gdm /etc/pam.d`

A titre d'exercice :

- Configurer PAM de façon à ce que SSH utilise aussi LDAP
- Mettre en oeuvre le changement de mot passe LDAP via PAM (`password`)

5 Replication

Nous allons maintenant mettre en oeuvre une réplication de l'annuaire de la machine *master* sur la machine *replica*. Plusieurs techniques sont proposées par OpenLDAP. Nous utilisons ici *syncrepl* basé sur les *overlays* d'OpenLDAP.

Coté *master*, il faut :

1. Ajouter une entrée pour l'utilisateur de synchronisation (le mot de passe est `mot2pass`)

```
dn: cn=syncuser,dc=mathrice,dc=prive
objectClass: organizationalPerson
cn: syncuser
sn: syncuser
userPassword: {SSHA}7Q7RDtX6PgeC54m85vFYwW4K/4Rbj6pL
```

2. Définir les autorisations pour cet utilisateur (ACL)

```
access to attrs=userPassword,shadowLastChange
  by anonymous auth
  by self write
  by dn="cn=syncuser,dc=mathrice,dc=prive" read
  by * none
```

3. Demander le chargement du module `/usr/lib/ldap/syncprov.so` en ajoutant `moduleload syncprov` dans les options générales de `slapd.conf`.
4. Activer `syncprov` en ajoutant ces lignes dans `slapd.conf`

```
overlay syncprov
syncprov-checkpoint 100 10
syncprov-sessionlog 100
```

Ensuite coté *replica* il est nécessaire de :

- Démarrer la machine virtuelle;
- Installer OpenLDAP (`apt-get install ldap-utils slapd openssl`);
- Créer un certificat avec `/usr/lib/ssl/misc/CA.pl -newcert` et l'installer dans `/etc/ldap` comme indiqué dans la section 3;
- Stopper le service LDAP : `/etc/init.d/slapd stop`
- Installer le fichier du démon OpenLDAP :
`scp tpldap@192.168.1.1:Public/slapd-replica.conf /etc/ldap/slapd.conf`;
- Démarrer le service LDAP : `/etc/init.d/slapd start`

Sur la machine *master*, ouvrir une session administrateur et surveiller le journal syslog avec un `tail -f /var/log/syslog`. Si tout va bien, nous devrions observer une connexion en provenance de 192.168.1.2.

Il est également possible de tester avec `ldapsearch` :

```
ldapsearch -x -h master -Z -D cn=syncuser,dc=mathrice,dc=prive
-W -b dc=mathrice,dc=prive '(objectClass=*)'
```

A l'aide de `ldapsearch`, `ldapdelete` et `ldapadd` comparer le contenu des deux annuaires, après des modifications, après l'arrêt de *master* ou de *replica*.

Sur la machine *client* modifier la directive `uri` dans `/etc/libnss-ldap.conf` et `/etc/pam-ldap.conf` de façon à basculer sur le replica en cas de défaillance du master :

```
hosturi ldap ://192.168.1.2/ ldap :192.168.1.3/
```

Tester la bascule en arrêtant LDAP sur *master*. (`/etc/init.d/slapd stop`).