TD - LDAP

Résumé Le but de ce TP est de mettre en place un mécanisme d'authentification utilisant le protocole LDAP.

Récupérez l'archive `/net/stockage/aguermou/AR/images/archive_tp7.tgz` et utiliser la procédure habituelle pour la mise en place des fichier cow (le script à lancer pour ce TP est `/net/stockage/aguermou/AR/TP/7/demo-gterm`). À partir de maintenant, nous allons configurer les machines de la manière suivante :

- la machine `immortal`, sur laquelle tournera le serveur LDAP.
- la machine `grave`, qui jouera le rôle de client.

1 Configuration du serveur LDAP

Sur la machine `immortal`, vous devez suivre les étapes suivantes :

1. Créez un compte utilisateur sur `immortal`.
2. Éditez le fichier `/etc/ldap/slapd.conf` (fichier de configuration du serveur LDAP) pour y configurer :
   (a) le nom de domaine LDAP (`suffix "dc=toto,dc=fr"`)
   (b) le nom de l'administrateur (`rootdn "cn=admin,dc=toto,dc=fr"`)
   (c) et le mot de passe de l'administrateur. Ceci devra être fait en ajoutant (`rootpw xxxx`) où `xxxx` est le résultat de la commande slappasswd (cette dernière vous renvoie le mot de passe que vous avez saisi en crypté).
   (d) remplacer tous les champs commençant par @ par la valeur correspodante (i.e. @BACKEND@ par hdb, @SUFFIX@ par "dc=toto,dc=fr", etc ...)
   (e) N'oubliez pas de nettoyer les différentes ACL présents à la fin du fichier pour qu'elles utilisent le nom de votre domaine LDAP.
3. Lancez le serveur LDAP avec la commande `/etc/init.d/slapd start` et vérifiez que ce dernier est bien lancé.
4. Une fois la configuration minimale opérationnelle, il faut remplir l'annuaire LDAP avec par exemple les comptes/informations du serveur. L'ajout d'entrées dans la base se fait via des fichiers textes au format ldif. Ce dernier n'étant pas très pratique à manipuler, l'utilisation du script `/usr/share/migrationtools/migrate_all_online.sh` vous permettra d'utiliser une procédure automatique. Il faut alors :
   (a) Editer le fichier `/etc/migrationtools/migrate_common.ph` et y modifier les entrées `$DEFAULT_MAIL_DOMAIN` et `$DEFAULT_BASE` pour qu'elles soient conformes au nom de votre domaine LDAP.
   (b) Aller dans le dossier `/usr/share/migrationtools` et lancer le script `migrate_all_online.sh`. Le script va tout d'abord va vous demander certaines informations (typiquement le nom du serveur LDAP, le mot de passe administrateur, etc ...)

Une fois cette opération effectuée, le serveur LDAP est opérationnel. Pour voir si les étapes précédentes ont bien fonctionné, il suffit de faire une requête au serveur LDAP avec la commande ldapsearch. L'ajout d'une nouvelle entrée (typiquement un nouvel utilisateur) dans la base LDAP se fait en créant un fichier ldif puis en ajoutant ce dernier à la base avec la commande ldapadd. Il est à noter qu'en général, on utilise des scripts (qui existent pour la majorité) pour automatiser l'opération.

Nous allons nous intéresser maintenant à la configuration de la machine cliente (en l'occurrence `grave`).

1. Éditez le fichier `/etc/ldap/ldap.conf` (qui représente le fichier de configuration du client LDAP) et mettez y les informations concernant l'adresse du serveur et le nom du domaine LDAP.

2. Testez la communication entre le client et le serveur à l'aide de la commande ldapsearch.

Une fois les configurations du client et du serveur opérationnelles, nous allons nous intéresser à la mise en place des mécanismes d'authentification au-dessus de LDAP. Tout le travail doit être fait sur la machine cliente en utilisant la commande `pam-auth-update`.

1. Éditez le fichier `/etc/nsswitch.conf` pour y ajouter ldap

2. Configurer PAM pour qu'il utilise LDAP à l'aide de la commande : `dpkg-reconfigure libpam-ldap`

3. Configurer NSS pour qu'il utilise LDAP à l'aide de la commande : `dpkg-reconfigure libnss-ldap`

Validez votre configuration en essayant de vous "loguer" en tant qu'un utilisateur qui n'existe qu'au niveau du serveur LDAP.

2 Sécurisation des transactions

Pour les plus avancés, nous allons nous intéresser à la sécurisation des communications entre les clients LDAP et le serveur à l'aide de TLS.

Nous allons commencer par la configuration du serveur :

1. Sur immortal, Allez dans `/tmp` et exécutez les commandes suivantes :

```
certtool --generate-privkey --outfile ca-key.pem

certtool --generate-self-signed --load-privkey ca-key.pem --outfile \
   ca-cert.pem

certtool --generate-privkey --outfile key.pem

certtool --generate-certificate --load-privkey key.pem --outfile \
   cert.pem --load-ca-certificate ca-cert.pem  --load-ca-privkey \
   ca-key.pem
```

Les deux premières commandes servent à créer le couple clé privée/certificat (le certificat étant une clé publique avec des informations à coté) pour notre propre autorité de certification qui est nécessaire au bon fonctionnement de TLS/SSL. Ensuite, les deux autres commandes servent à créer un couple clé privée/certificat qui seront ceux de notre serveur LDAP (c'est à dire immortal). Le certificat d'immortal est "signé" par l'autorité de certification ce qui lui permet d'être utilisable (il y a une notion de confiance quand il s'agit de certificats).

Remarque : À chaque fois qu'on vous demande un nom dans les étapes précédentes, il faut que vous saisissiez le nom de la machine immortal (i.e. `immortal.metal.fr`)

2. Il faut maintenant stocker les fichiers générés à un endroit qui n'est accessible que par `root` et à l'utilisateur openLDAP sur le serveur. Nous allons donc créer un dossier `/etc/ldap/ssl/`. Il faut ensuite exécuter les commandes suivantes :
   ```
   mv /tmp/ca-cert.pem /etc/ldap/ssl/cacert.pem
   mv /tmp/cert.pem /etc/ldap/ssl/servercrt.pem
   mv /tmp/key.pem /etc/ldap/ssl/serverkey.pem
   ```

3. Changer les droits du dossier `/etc/ldap/ssl` et de son contenu pour qu'ils ne soient accessibles qu'à l'utilisateur `openldap` en lecture/écriture seulement.

4. Ajoutez les lignes suivantes au fichier de configuration du serveur de manière à spécifier à ce dernier où sont les fichiers contenant les certificats et les clés.
   ```
   TLSCertificateFile /etc/ldap/ssl/servercrt.pem
   TLSCertificateKeyFile /etc/ldap/ssl/serverkey.pem
   TLSCACertificateFile /etc/ldap/ssl/cacert.pem
   ```

5. Modifiez le fichier `/etc/default/slapd` de telle sorte que le serveur ldap ne reponde qu'aux requêtes arrivant sur le port ldaps.

Nous allons maintenant configurer le client :

1. Copiez les fichiers `/etc/ldap/ssl/cacert.pem` et `/etc/ldap/ssl/servercrt.pem` à partir du serveur et le mettre dans `/etc/ldap/ssl` côté client.

2. Modifiez le fichier `ldap.conf` pour lui faire utiliser le protocole LDAP sécurisé et pour lui spécifier le fichier contenant le certificat. Cette dernière opération se fera par l'ajout de la ligne :
   ```
   TLS_CACERT /etc/ldap/ssl/cacert.pem
   ```

3. Testez votre configuration à l'aide de la commande ldapsearch.