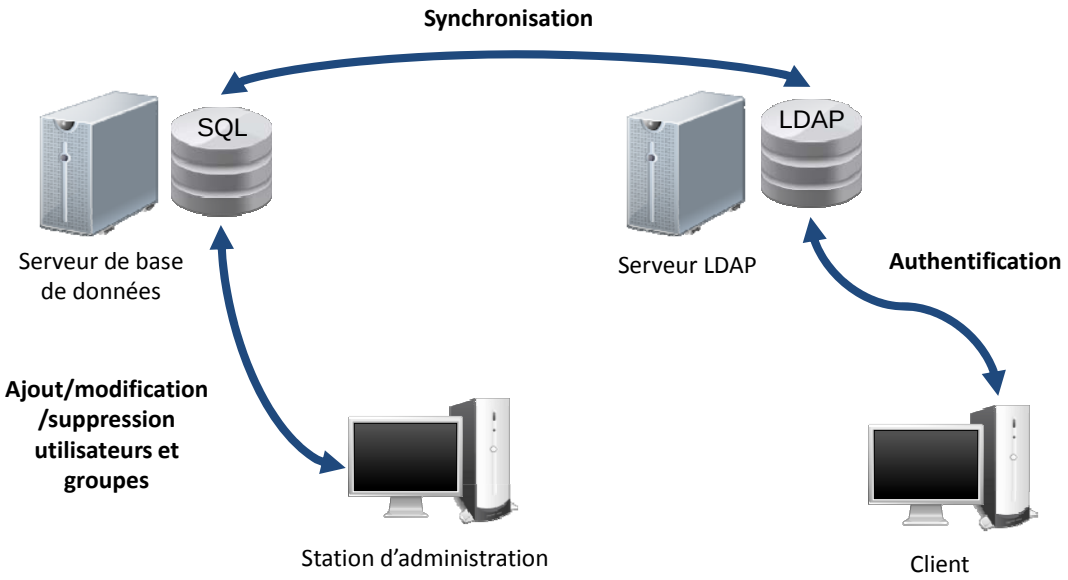
Université Grenoble Alpes
U.F.R. Sciences de l'Homme et de la Société
Master MIASHS – DCISS - WIC

Projet administration système et réseau

Le but de ce projet est de mettre en place une gestion des utilisateurs et des groupes, basée sur un système d'information et sur un annuaire LDAP.

Les données concernant les utilisateurs et les groupes seront stockées dans un système d'information représenté par une base de données MySQL. Les informations présentes dans l'annuaire LDAP seront automatiquement synchronisées sur le serveur de base de données. Toute modification faite dans le système d'information devra être répliquée dans l'annuaire LDAP.

Les clients utiliseront le serveur LDAP pour l'authentification des utilisateurs et leur appartenance aux groupes. Un utilisateur ne doit plus pouvoir se connecter si sa date de fin de séjour est dépassée.



Environnement

Le projet sera réalisé en binôme sous Marionnet.

Vous utiliserez le réseau 192.168.1.0/24 mappé sur le domaine Internet *imss.org*, avec un serveur DNS nommé *ns*, un serveur de base de données nommé *sql*, un serveur LDAP nommé *ldap1*, une passerelle *G1* pour la connectivité Internet. Les serveurs et les passerelles auront les adresses IP suivantes :

- *ns* : 192.168.1.1
- *ldap1* : 192.168.1.100
- *sql* : 192.168.1.101
- *G1* : 192.168.1.2

La machine d'administration qui portera les scripts Perl se nommera *adm*. Le client *m1* devra être configuré pour utiliser l'annuaire LDAP pour la gestion des utilisateurs et des groupes. La machine *adm* et la machine *m1* auront respectivement comme adresses IP 192.168.1.200 et 192.168.1.10.

Utilisez le système « debian-lenny » pour le serveur *sql*[1] et « debian-wheezy » pour toutes les autres machines. Vous pouvez, si vous le souhaitez, partir du TP LDAP.

Format des données

Dans le système d'information, un utilisateur est représenté par :
- un nom
- un prénom
- un identifiant
- un mot de passe
- un numéro d'utilisateur
- un numéro de groupe (groupe primaire)
- une adresse de courriel
- une date de fin de séjour

Un groupe est représenté par :
- un nom
- un numéro de groupe
- une description

Vous utiliserez trois tables MySQL, une table `utilisateurs`, une table `groupes` et une table `groupe_membres` dans la définition du modèle de données.

Dans l'annuaire LDAP, une entrée utilisateur est constitutée des objets suivants :
- `person`
- `organizationalPerson`
- `inetOrgPerson`
- `posixAccount`
- `shadowAccount`

définissant les attributs :
- `uid` : l'identifiant de l'utilisateur
- `cn` : le nom complet de l'utilisateur (au format Prénom Nom)

[1] La procédure d'installation et de configuration de base du service MySQL est indiquée à la fin du document.

- `sn` : le nom de l'utilisateur
- `givenName` : le prénom de l'utilisateur
- `mail` : l'adresse de courriel
- `uidNumber` : le numéro de l'utilisateur
- `gidNumber` : le numéro de groupe de l'utilisateur (groupe primaire)
- `homeDirectory` : le répertoire de login de l'utilisateur (généralement `/home/`*`identifiant`*)
- `loginShell` : le shell de connexion (généralement `/bin/bash`)
- `userPassword` : le mot de passe chiffré
- `shadowExpire` : le nombre de jours depuis le 1er janvier 1970 pendant lesquels le compte est valide. L'ouverture de session n'est plus possible si ce nombre est dépassé.

Un groupe est constitué d'un objet `posixGroup` définissant les attributs :
- `cn` : le nom du groupe
- `gidNumber` : le numéro du groupe
- `description` : la description du groupe
- `memberUid` : l'identifiant d'un utilisateur membre du groupe ; il peut y avoir plusieurs attributs `memberUid` pour un groupe donné.

Fonctionnalités attendues

Depuis la station d'administration, les scripts Perl permettront de gérer les utilisateurs et les groupes. Pour les utilisateurs, cela consiste à :
- lister les utilisateurs présents dans la base de données
- ajouter un utilisateur
- modifier l'adresse de courriel ou la date d'expiration d'un utilisateur
- (re)définir le mot de passe d'un utilisateur
- supprimer un utilisateur

Pour les groupes, cela consiste à :
- afficher la liste des membres d'un groupe
- modifier les membres d'un groupe (ajouter un membre / supprimer un membre)
- supprimer un groupe (à condition qu'il ne contienne plus aucun membre et qu'il ne s'agisse pas du groupe primaire d'un utilisateur)

Installation et configuration de base du service MySQL sur Debian Lenny

Pour installer un paquetage comme `mysql-server` sur *sql* vous devez
1. Editer le fichier `/etc/apt/sources.list` en commentant toutes les lignes (en les préfixant du caractère « # ») et en ajoutant à la fin la ligne :
   ```
   deb http://archive.debian.org/debian/ lenny contrib main non-free
   ```

2. Exécuter la commande `aptitude update` pour recharger la base des paquetages du serveur de dépôt
   ```
   sql:/etc/apt# aptitude update
   Writing extended state information... Done
   Get:1 http://archive.debian.org lenny Release.gpg [1034B]
   Ign http://archive.debian.org lenny/contrib Translation-en_US
   Ign http://archive.debian.org lenny/main Translation-en_US
   Ign http://archive.debian.org lenny/non-free Translation-en_US
   Get:2 http://archive.debian.org lenny Release [99.6kB]
   Ign http://archive.debian.org lenny Release
   Get:3 http://archive.debian.org lenny/contrib Packages [76.2kB]
   Get:4 http://archive.debian.org lenny/main Packages [5191kB]
   ```

```
Get:5 http://archive.debian.org lenny/non-free Packages [100kB]
Get:6 http://archive.debian.org lenny/non-free Packages [100kB]
Fetched 5446kB in 2min14s (40.4kB/s)
Reading package lists... Done
W: GPG error: http://archive.debian.org lenny Release: The following
signatures couldn't be verified because the public key is not
available: NO_PUBKEY AED4B06F473041FA NO_PUBKEY 4D270D06F42584E6
W: You may want to run apt-get update to correct these problems
There are now 543 updates [+543], 22307 new [+22255].
```

Puis faire `aptitude install mysql-server`. L'installation se termine par la configuration du mot de passe de l'administrateur MySQL (root)

3. Par défaut la connexion au service MySQL est restreinte à l'hôte local (127.0.0.1). Pour permettre à la machine *adm* de se connecter au port 3306 du serveur *sql*, éditez sur ce dernier le fichier `/etc/mysql/my.cnf` et commentez la ligne (en la préfixant du caractère « # ») :
   `bind-address = 127.0.0.1`
   puis redémarrez le service avec la commande `/etc/init.d/mysql restart` pour prendre en compte la modification.

4. Autorisez les accès aux bases de données depuis la machine *adm*. Assurez-vous au préalable que la résolution de noms est bien fonctionnelle. Depuis la machine *sql*, connectez-vous à l'interface d'administration de MySQL avec la commande :
   `mysql –u root –p`
   et tapez la commande SQL :
   `GRANT ALL PRIVILEGES ON *.* TO 'root'@'adm.imss.org' IDENTIFIED BY 'password' WITH GRANT OPTION;`
   en remplaçant *password* par le mot de passe que vous avez défini précédemment.

5. Il devrait être possible à présent d'accéder à l'interface d'administration des bases de données depuis la machine *adm* :
   `mysql –h sql.imss.org –u root -p`