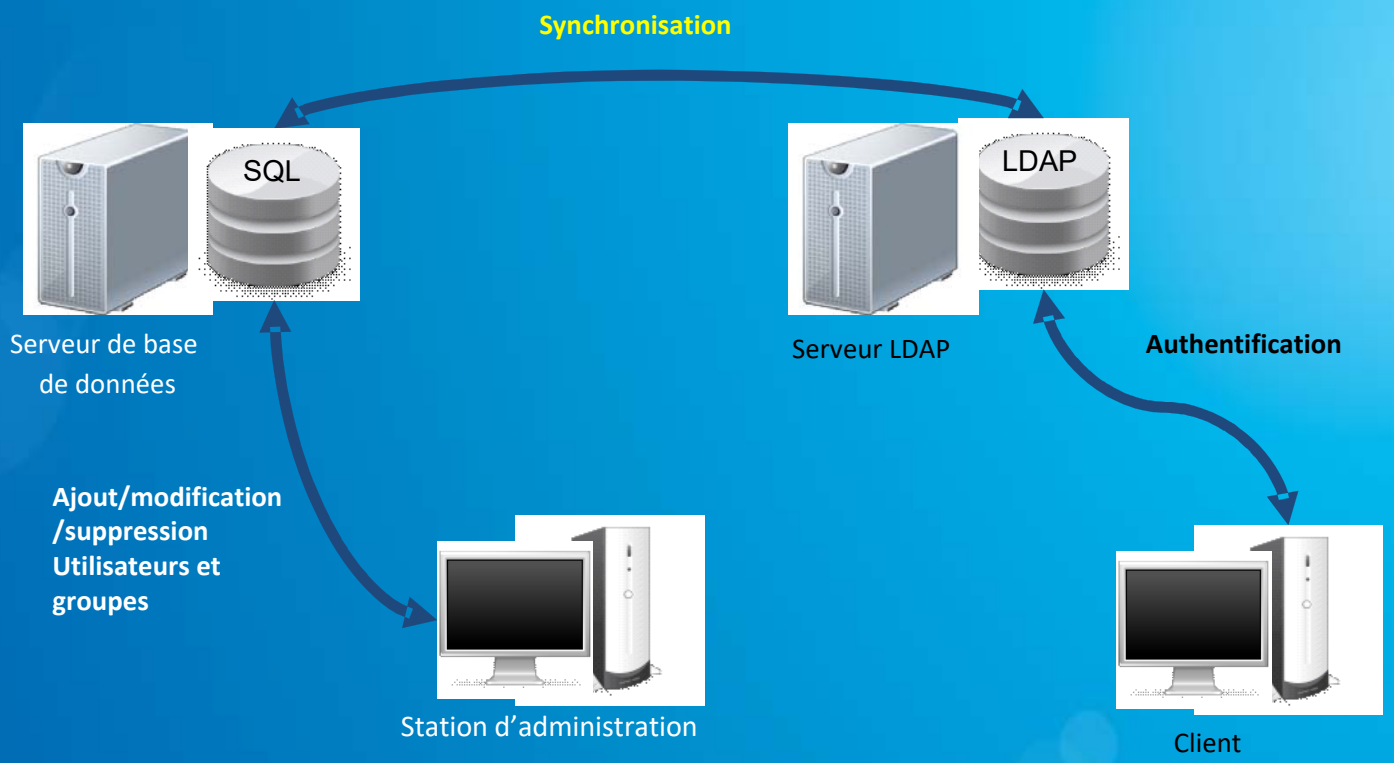
Projet Administration système et réseau

Objectif

- Mettre en place une gestion d'utilisateurs et de 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 effectuée dans le système d'information devra être répliquée dans l'annuaire LDAP.

Schéma général



- 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 de travail

- Projet sera réalisé en binôme sous Marionnet.
- Utilisation du réseau mis en place dans le TP LDAP :
  - *ns* : 192.168.1.1
  - *ldap1* : 192.168.1.100
  - *sql* : 192.168.1.101
  - *G1* : 192.168.1.2
- Pour les machines utiliser le système « debian-wheezy »
- La machine d'administration qui portera les scripts Perl se nommera *adm* : 192.168.1.200
- Le client *m1* sera configuré pour utiliser l'annuaire LDAP pour la gestion des utilisateurs et des groupes : 192.168.1.10

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

Système d'information

- La base de données comprendra 3 tables MySQL :
  - Table utilisateurs
  - Table groupes
  - Table groupe_membres
- Dans l'annuaire LDAP une entrée utilisateur est constituée des objets suivants :
  - person
  - organizationalPerson
  - inetOrgPerson
  - posixAccount
  - shadowAccount

Annuaire LDAP

Attributs définis pour un utilisateur :

- uid : l'identifiant de l'utilisateur
- cn : le nom complet de l'utilisateur (au format Prénom Nom)
- 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.

Annuaire LDAP

Exemple de fichier .ldif définissant un utilisateur :

```
dn: uid=moraneb,ou=users,dc=imss,dc=org
givenName: Bob
objectClass: top
objectClass: inetOrgPerson
objectClass: person
objectClass: organizationalPerson
objectClass: posixAccount
userPassword: {MD5}y9t+Kx7VZs63lq8t8HIFow==
uid: moraneb
mail: bob.morane@imss.org
uidNumber: 999001
cn: Bob Morane
loginShell: /bin/bash
gidNumber: 999000
homeDirectory: /home/moraneb
sn: Morane
shadowExpire: 18262
```

31/12/2019 à 23:59:59

Annuaire LDAP

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

Fonctionnalités attendues

Depuis la station d'administration, les scripts Perl permettront de gérer les utilisateurs et les groupes.

- 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
- Lors des modifications, une synchronisation assurant la cohérence entre la base de données et l'annuaire sera réalisée

Evaluation du projet

- Date prévue pour l'évaluation des projets :
  le 2 mai 2019
- Soutenance :
  - Présentation du projet réalisé
  - Description des différentes parties développées
- Démonstration
  - Présentation du projet Marionnet développé

Aide au développement du projet

- Un module perl facilitant la gestion de l'annuaire LDAP
- TP perl LDAP
- TP mettant en œuvre une base de données MySQL depuis un programme Perl

Module ldap_lib.pm

- Utilise le module Net::LDAP
- Exporte des procedures pour
  - Se connecter à un annuaire LDAP
  - Lire des entrées
  - Détrure des entrées
  - Créer, détruire, modifier des attributs
  - Récupérer la liste des utilisateurs
  - Récupérer la liste des groupes
  - Récupérer la liste des membres d'un groupe
  - Ajouter un utilisateur, un groupe, un groupe POSIX
  - Etc.