# R304 : LDAP

November 21, 2023

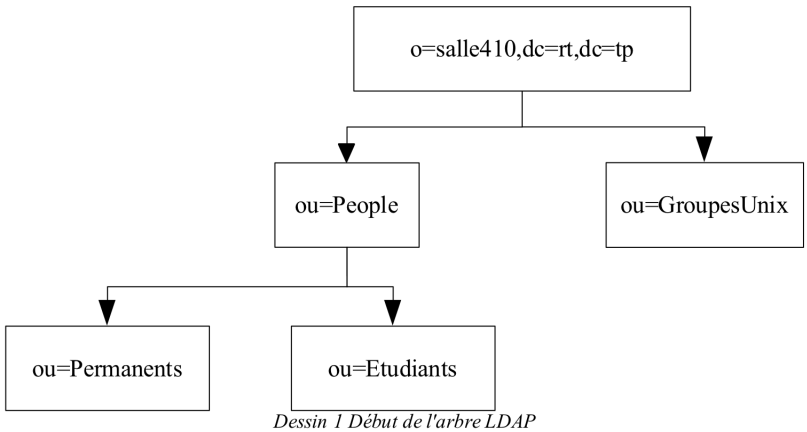
Vous devez envoyer votre rapport électronique au format PDF par mail à l'enseignant en fin de séance.
Buts du TP : à lire IMPERATIVEMENT (votre survie en dépend)
Durant cette manipulation nous allons étudier la création de comptes utilisateurs de façon classique ou via LDAP:

- Nous allons configurer le démon ldap (via son fichier de configuration dans /etc/) avec le bon suffixe (racine de l'arbre) et le bon utilisateur admin à la mode ldap.
- Nous allons ensuite charger une base minimale contenue dans un fichier texte ldif avec 3 objets : le racine, un groupe People et l'admin.
- Ensuite, nous passons en mode graphique. Pour se faire, on utilise phpldapadmin. Ce sont des scripts qui vont interroger le démon ldap (slpad). Pour se faire, il faut configurer le bon suffixe et le bon admin dans le fichier de configuration.
- Une fois tout cela mis en place, vous allez créer un utilisateur dans ldap puis montrer qu'on le voit à côté de ceux définis dans /etc/passwd et enfin, vous allez faire en sorte que des applications comme ssh utilisent la base des utilisateurs ldap.

# 1 LDAP

## 1.1 Structure

Nous allons créer une base d'annuaire. La racine de notre base, le « suffixe » en jargon LDAP, sera : "o=salle410,dc=rt,dc=tp". Ce suffixe correspond à un domaine. Si on gérait unice.fr, on aurait mis "dc=unice,dc=fr". On veut pouvoir identifier des personnes, des machines.
**Important :** tout objet à un dn (distinguished name) qui l'identifie et qui est son chemin dans l'arbre. Par exemple, pour le schéma ci-dessous le dn de People sera "ou=People, o=salle410,dc=rt,dc=tp". Tous les dn devront suivre ce schéma !!!! Faites attention à ne rien oublier



*Dessin 1 Début de l'arbre LDAP*

Figure 1: Début de l'arbre LDAP

Installer le paquet slapd et ldap-utils. Mettre test comme mot de passe root.

La configuration se fait dans le répertoire /etc/ldap/slapd.d/. Ce répertoire contient un fichier cn=config.ldif qui contient la configuration globale (rien à changer) et un répertoire cn=config qui contient une liste de fichiers et de répertoire : Les fichiers olc* sont des *open ldap configuration*.
Les olcDatabase sont les définitions des bases : on en voit 2 la "0" et la "1". La "0" c'est la base config, tous les dn qui la concernent finissent par cn=config. La "-1" aussi dite "frontend" définit toutes les options par défaut de toutes les bases autres que la config (0).

Notre travail de configuration est dans le fichier olcDatabase={1}mdb.ldif. Il faut appliquer ici plusieurs modifications :

- indiquer le « olcSuffix » o=salle410,dc=rt,dc=tp
- modifier le « olcRootDN » cn=admin,o=salle410,dc=rt,dc=tp
- modifier le « olcRootPW » en remplaçant " :: " suivi de la chaine de caractères (qui est codée en base64) par : test

## 1.2 Création d'une base minimale

Pour créer la racine de la base de données, utiliser le fichier lBase-rt-410.ldif qui est accessible à l'adresse : http://www.i3s.unice.fr/~urvoy/docs/M3105/lBase-rt-410.ldif
Le placer dans le répertoire racine de root. Le fichier .ldif est éditable et peut être facilement visualisé.
Combien d'objets contient-il ? Quels sont leur dn (chemin dans l'arbre) ?
Vérifier que les dn sont adaptés au « suffix » que l'on s'est donné et corriger au besoin.
Détruire à la main la base construite à l'installation du logiciel.

```
rm -f /var/lib/ldap/*
```

Il faut alors charger la base de données reconstruite

```
slapadd -l lBase-rt-410.ldif
```

et rétablir les droits pour que l'utilisateur openldap puisse la modifier (vous travailler en root et openldap n'a pas les mêmes droits)

```
chown -R openldap /var/lib/ldap
```

ensuite on démarre le service de ldap

```
service slapd restart
```

Lister la base avec ldapsearch en utilisant l'identifiant de l'administrateur.

```
ldapsearch -x -W -b "o=salle410,dc=rt,dc=tp" -D "cn=admin,o=salle410,dc=rt,dc=tp
   "
```

## 1.3 Création base ldap par interface web

Des accès graphiques peuvent être faits à partir de phpldapadmin. Il faut installer les paquets suivants :

```
apt install  php  apache2 libapache2-mod-php php-xml php-ldap phpldapadmin
```

Il faut ensuite configurer le fichier /etc/phpldapadmin/config.php. Ouvrez ce fichier avec un éditeur et cherchez les lignes qui ne sont pas commentées (en couleur) en mettant le bon **suffixe** et le bon **admin** à la mode LDAP (le bon dn!) On parcourt l'arborescence avec un utilitaire tel que phpldapadmin, à l'adresse: http://localhost/phpldapadmin/.

### 1.4 Annuaire

Créer l'arbre représenté sur le dessin 1 via l'interface graphique phpldapadmin.
Les personnes seront sous la désignation ou=People qui est une OrganisationalUnit.
Au dessous on décompose en permanents et etudiants, qui sont des OrganisationalUnit comme la précédente.
Créér 2 groupes unix que l'on va mettre dans le groupe ldap GroupeUnix.
On créée ensuite un compte utilisateur sous etudiants de type Generic User Account. Il est dans ldap et pas dans /etc/passwd. Choisir un uid/gid qui ne soit pas déjà dans le /etc/passwd, sinon, il y aura des conflits.
Lister la base avec ldapsearch en utilisant l'identifiant de l'administrateur.

```
ldapsearch -x -W -b "o=salle410,dc=rt,dc=tp" -D "cn=admin,o=salle410,dc=rt,dc=tp
   "
```

## 2 Authentification par LDAP

### 2.1 Description de PAM

L'authentification en Linux ainsi qu'en Solaris est faite avec PAM (Pluggable Authentication Module), un ensemble de modules qui rendent l'authentification très versatile (modulaire donc). Les descriptions de ces modules sont dans le répertoire /etc/pam.d. Voir par exemple les fichier login et ssh. Ils comportent au moins quatre étapes

1. auth pour l'authentification : vérification du mot de passe en lien avec le nom d'utilisateur.
2. account pour vérifier que l'utilisateur a les droits sur son compte.
3. session pour mettre en place ce qui doit être fait pour l'environnement de travail dans ce compte.
4. password pour gérer la modification du mot de passe.

Chaque ligne présente un mode de vérification "requisite" "required" "sufficient" "optional" qui indique le niveau de gravité de l'échec de la vérification. Ensuite vient le module proprement dit qui peut être un module écrit par l'administrateur.

### 2.2 Intégration à PAM

Pour que pam puisse utiliser ldap, il faut les modifier.

Commencer par installer les logiciels nécessaires. Installez les 2 packages nécessaires. D'abord

```
apt-get install libnss-ldap
```

Vous devrez remplir le suffixe de la base (suffix) et le DN de l'adminstrateur (rootdn). Faite attention aux questions posés pour l'outil lors de l'installation. Si besoin en cas d'erreur vous pouvez relancer l'assistant de configuration en faisant

```
dpkg-reconfigure libnss-ldap
```

Choisir l'uri ldap://localhost/ (pas de ldapi mais bien ldap!)

```
apt-get install libpam-ldap
```

Idem que pour le paquet précédent.

#### 2.2.1 Obtenir l'information sur le compte

Il faut modifier du fichier /etc/nsswitch.conf en ajoutant "ldap" en fin des lignes passwd, group et shadow.

Surtout ne pas retirer compat sinon la machine ne lira plus les comptes du fichier /etc/passwd et deviendra très instable !!

Redémarrer ensuite le démon nscd qui fournit le cache pour les comptes sous linux. On doit voir votre compte avec la commande

```
getent passwd
```

### 2.2.2 Pouvoir se loger

Vérifiez qu'il y a une ligne avec ldap dans /etc/pam.d/sshd ou dans /etc/pam.d/common-session. Si ce n'est pas le cas, modifier l'un des modules (sshd) pour qu'il utilise ldap. Vous avez dans /usr/share/doc/libpam-ldap/examples/pam.d/ des exemples pour modifier votre /etc/pam.d.
Pour pouvoir se loger il faut configurer le module pam_ldap lui-même, ce qui devrait avoir été fait lors de l'installation. Il est possible de modifier le fichier /etc/pam_ldap.conf à la main. Comme ci-dessus, le faire avec la commande:

```
dpkg-reconfigure libpam-ldap
```

Choisir la même uri que précédement et les mots de passe chiffrés. Il est maintenant possible de se loger sur votre machine par LDAP. Le vérifier avec un ssh votrecompte@localhost. Sur quel répertoire arrive-t-on ?

---

# 3 Partie Bonus

## 3.1 Création du homedir

Vous avez remaqué que l'utilisateur se logeait à la racine car son répertoire home n'avait pas été créé. Pour cela, il faut se loger via su en tant que votre nouvel utilisateur. L'utilitaire su utilise pam et vous devez avoir dans /etc/pam.d soit un fichier su, soit le fichier common-session qui va contenir :

```
session required pam_mkhomedir.so skel=/etc/skel/ umask=0077
```

Vérifiez que vous avez bien la ligne session dans pam.d
Logez vous en tant que l'utilisateur créé sous ldap via pam. Le répertoire home est bien là ?
Est-ce que cela fonctionne en ssh maintenant ?

Ainsi, la création du répertoire home de l'utilisateur sera automatique.

## 3.2 Configuration Apache

On va faire en sorte qu'Apache utilise LDAP pour l'authentification.

Ajouter le module ldap dans apache2 :

```
a2enmod ldap auth_basic authnz_ldap authz_user
```

Modifier AllowOverride None en AllowOverride All dans /etc/apache2/apache2.conf dans la partie <Directory /var/www/>
Créer le fichier .htaccess dans /var/www/html

```
AuthType Basic
AuthName "Restricted Area"
AuthLDAPBindDN "cn=admin,o=salle410,dc=rt,dc=tp"
```

```
AuthLDAPBindPassword "test"
AuthBasicProvider ldap
AuthLDAPURL ldap://127.0.0.1/ou=Etudiants,ou=People,o=salle410,dc=rt,dc=tp
Require valid-user
```

Redémarrer apache2 et montrez que cela fonctionne pour votre utilisateur créé dans PhpLdapAdmin.