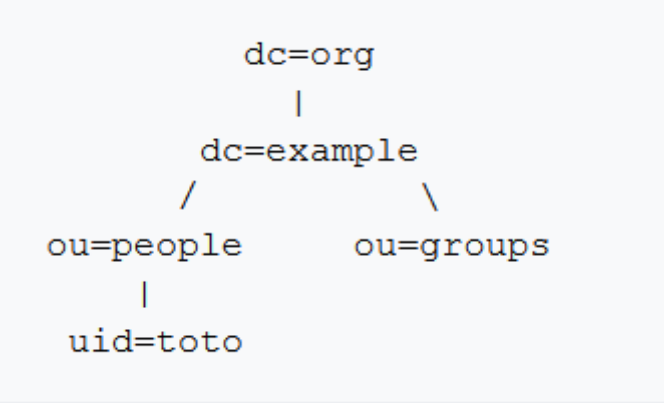
M3105 : Supervision réseau et application LDAP

Introduction :

LDAP pour Lightweight Directory Access Protocol est un protocole permettant de gérer des annuaires, c'est-à-dire d'accéder à des bases d'informations sur les utilisateurs d'un réseau par l'intermédiaire de protocoles TCP/IP. C'est une solution incontournable dans les entreprises qui a été normalisée par IETF (Internet Engineering Task Force).
LDIF est un format de données intelligibles utilisé par LDAP mais les données sont stockées dans la base LDAP sous forme différente (binaire). Il y possibilité de convertir dans les deux sens : Base de données ↔ LDIP.
Un annuaire est un arbre d'entrées.



Arbre d'entrée LDAP

Les entrées LDAP sont organisées de manière hiérarchique avec un **identifiant unique** par entrée appelé **dn** (distinguished name). Le **dn** d'une entrée est le chemin absolu depuis la racine. Une entrée est constituée d'un ensemble d'attributs. Le **dn** est le nom d'une entrée, ce n'est pas un attribut.
Un attribut possède un nom, un type et une ou plusieurs valeurs.

Exemple d'une entrée formatée en LDIF :

```
dn: cn=John Doe, dc=example, dc=org
cn: John Doe
givenName: John
sn: Doe
telephoneNumber: +1 555 6789
telephoneNumber: +1 555 1234
mail: john@example.com
manager: cn=Barbara Doe, dc=exemple, dc=com
objectClass: inetOrgPerson
objectClass: organizationalPerson
objectClass: person
objectClass: top
```

Entrée formatée en LDIF

Type d'attributs : **cn** (common name), **sn** (surname), **dc** (domain components), **ou** (organizational units), **uid** (user identifier) etc.

1. Définition d'utilisateurs UNIX

Le fichier /etc/passwd définit tous les utilisateurs

```
rt@rt410p102:~$ cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
systemd-timesync:x:100:102:systemd Time Synchronization,,,:/run/systemd:/bin/false
systemd-network:x:101:103:systemd Network Management,,,:/run/systemd/netif:/bin/false
systemd-resolve:x:102:104:systemd Resolver,,,:/run/systemd/resolve:/bin/false
_apt:x:104:65534::/nonexistent:/bin/false
Debian-exim:x:105:109::/var/spool/exim4:/bin/false
rtkit:x:106:111:RealtimeKit,,,:/proc:/bin/false
avahi-autoipd:x:108:112:Avahi autoip daemon,,,:/var/lib/avahi-autoipd:/bin/false
messagebus:x:109:113::/var/run/dbus:/bin/false
usbmux:x:110:46:usbmux daemon,,,:/var/lib/usbmux:/bin/false
speech-dispatcher:x:111:29:Speech Dispatcher,,,:/var/run/speech-dispatcher:/bin/false
sshd:x:112:65534::/run/sshd:/usr/sbin/nologin
lightdm:x:113:117:Light Display Manager:/var/lib/lightdm:/bin/false
pulse:x:114:118:PulseAudio daemon,,,:/var/run/pulse:/bin/false
avahi:x:115:121:Avahi mDNS daemon,,,:/var/run/avahi-daemon:/bin/false
colord:x:116:122:colord colour management daemon,,,:/var/lib/colord:/bin/false
saned:x:117:123::/var/lib/saned:/bin/false
hplip:x:118:7:HPLIP system user,,,:/var/run/hplip:/bin/false
rt:x:1000:1000:rt,,,:/home/rt:/bin/bash
vboxadd:x:999:1::/var/run/vboxadd:/bin/false
clamav:x:107:125::/var/lib/clamav:/bin/false
dovecot:x:119:126:Dovecot mail server,,,:/usr/lib/dovecot:/bin/false
dovenull:x:120:127:Dovecot login user,,,:/nonexistent:/bin/false
geoclue:x:121:128::/var/lib/geoclue:/bin/false
mysql:x:122:130:MySQL Server,,,:/nonexistent:/bin/false
postfix:x:123:131::/var/spool/postfix:/bin/false
statd:x:125:65534::/var/lib/nfs:/bin/false
_rpc:x:103:65534::/run/rpcbind:/usr/sbin/nologin
systemd-coredump:x:998:998:systemd Core Dumper:/:/usr/sbin/nologin
tcpdump:x:124:134::/nonexistent:/usr/sbin/nologin
rt@rt410p102:~$
```

Exemple de /etc/paswd

Le fichier /etc/shadow contient entre autres les mots de passe chiffrés.
Il n'est accessible qu'en sudo.

```
root@rt410p102:~# cat /etc/shadow
root:$6$aUwA5ts9$3/3BAlKYBE3m2iD3LICONt14njpDSO785AnKrJuYeBUDUDnbnpAkisgE/EbvuGsq0TbJFEiexlIRjzbQQ9mP7.:17339:0:99999:7:::
daemon:*:17339:0:99999:7:::
bin:*:17339:0:99999:7:::
sys:*:17339:0:99999:7:::
sync:*:17339:0:99999:7:::
games:*:17339:0:99999:7:::
man:*:17339:0:99999:7:::
lp:*:17339:0:99999:7:::
mail:*:17339:0:99999:7:::
news:*:17339:0:99999:7:::
uucp:*:17339:0:99999:7:::
proxy:*:17339:0:99999:7:::
www-data:*:17339:0:99999:7:::
backup:*:17339:0:99999:7:::
list:*:17339:0:99999:7:::
irc:*:17339:0:99999:7:::
gnats:*:17339:0:99999:7:::
nobody:*:17339:0:99999:7:::
systemd-timesync:*:17339:0:99999:7:::
systemd-network:*:17339:0:99999:7:::
systemd-resolve:*:17339:0:99999:7:::
_apt:*:17339:0:99999:7:::
Debian-exim:!:17339:0:99999:7:::
rtkit:*:17339:0:99999:7:::
avahi-autoipd:*:17339:0:99999:7:::
messagebus:*:17339:0:99999:7:::
usbmux:*:17339:0:99999:7:::
speech-dispatcher:!:17339:0:99999:7:::
sshd:*:17339:0:99999:7:::
lightdm:*:17339:0:99999:7:::
pulse:*:17339:0:99999:7:::
avahi:*:17339:0:99999:7:::
colord:*:17339:0:99999:7:::
saned:*:17339:0:99999:7:::
hplip:*:17339:0:99999:7:::
rt:$6$0stLZQzu$tcD8o2H9OttkgJafFaTT5geKBqNNJMr1mW7PWldMpaddwGNi4UK.ozYwrWyFm1GzvuwG6cFXy/BX1CXV5wafK0:17339:0:99999:7:::
vboxadd:!:17339:::::
clamav:!:17342:0:99999:7:::
dovecot:*:17342:0:99999:7:::
dovenull:*:17342:0:99999:7:::
geoclue:*:17342:0:99999:7:::
mysql:!:17342:0:99999:7:::
postfix:*:17342:0:99999:7:::
statd:*:17342:0:99999:7:::
_rpc:*:18708:0:99999:7:::
systemd-coredump:!!:18709::::::
tcpdump:*:18879:0:99999:7:::
root@rt410p102:~#
root@rt410p102:~#
```

Exemple de fichier /etc/shadow

Pour ajouter l'utilisateur machin avec un uid de 2510 on fait :

```
root@rt410p102:~# adduser --uid 2510 machin
Ajout de l'utilisateur « machin » ...
Ajout du nouveau groupe « machin » (2510) ...
Ajout du nouvel utilisateur « machin » (2510) avec le groupe « machin » ...
Le répertoire personnel « /home/machin » existe déjà.  Rien n'est copié depuis « /etc/skel ».
Nouveau mot de passe :
Retapez le nouveau mot de passe :
passwd: password updated successfully
Changing the user information for machin
Enter the new value, or press ENTER for the default
        Full Name []:
        Room Number []:
        Work Phone []:
        Home Phone []:
        Other []:
Cette information est-elle correcte ? [O/n]
```

Ajout d'un utilisateur grâce à adduser

On regarde maintenant les fichiers /etc/passwd et /etc/shadow et on voit que machin y est :

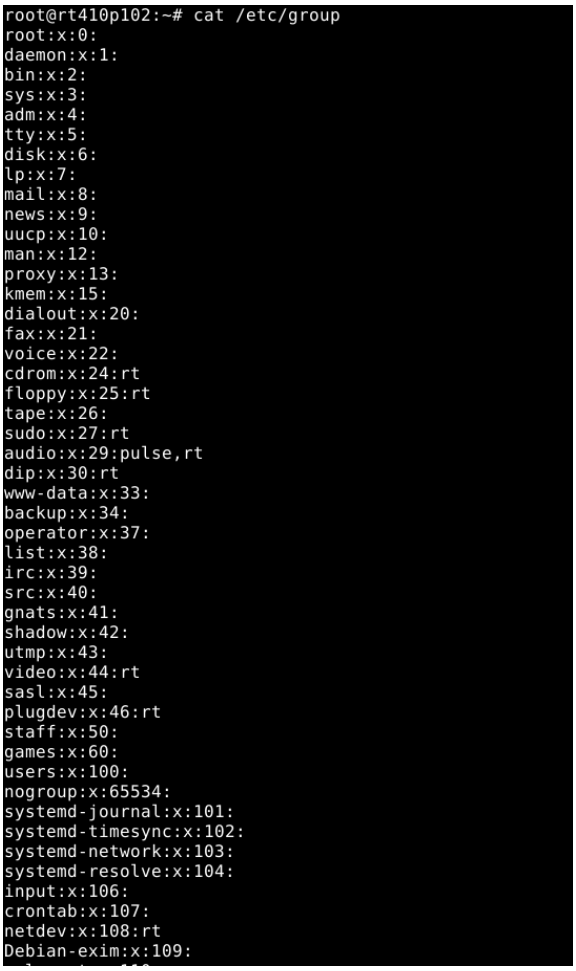
```
root@rt410p102:~# cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
systemd-timesync:x:100:102:systemd Time Synchronization,,,:/run/systemd:/bin/false
systemd-network:x:101:103:systemd Network Management,,,:/run/systemd/netif:/bin/false
systemd-resolve:x:102:104:systemd Resolver,,,:/run/systemd/resolve:/bin/false
_apt:x:104:65534::/nonexistent:/bin/false
Debian-exim:x:105:109::/var/spool/exim4:/bin/false
rtkit:x:106:111:RealtimeKit,,,:/proc:/bin/false
avahi-autoipd:x:108:112:Avahi autoip daemon,,,:/var/lib/avahi-autoipd:/bin/false
messagebus:x:109:113::/var/run/dbus:/bin/false
usbmux:x:110:46:usbmux daemon,,,:/var/lib/usbmux:/bin/false
speech-dispatcher:x:111:29:Speech Dispatcher,,,:/var/run/speech-dispatcher:/bin/false
sshd:x:112:65534::/run/sshd:/usr/sbin/nologin
lightdm:x:113:117:Light Display Manager:/var/lib/lightdm:/bin/false
pulse:x:114:118:PulseAudio daemon,,,:/var/run/pulse:/bin/false
avahi:x:115:121:Avahi mDNS daemon,,,:/var/run/avahi-daemon:/bin/false
colord:x:116:122:colord colour management daemon,,,:/var/lib/colord:/bin/false
saned:x:117:123::/var/lib/saned:/bin/false
hplip:x:118:7:HPLIP system user,,,:/var/run/hplip:/bin/false
rt:x:1000:1000:rt,,,:/home/rt:/bin/bash
vboxadd:x:999:1::/var/run/vboxadd:/bin/false
clamav:x:107:125::/var/lib/clamav:/bin/false
dovecot:x:119:126:Dovecot mail server,,,:/usr/lib/dovecot:/bin/false
dovenull:x:120:127:Dovecot login user,,,:/nonexistent:/bin/false
geoclue:x:121:128::/var/lib/geoclue:/bin/false
mysql:x:122:130:MySQL Server,,,:/nonexistent:/bin/false
postfix:x:123:131::/var/spool/postfix:/bin/false
statd:x:125:65534::/var/lib/nfs:/bin/false
_rpc:x:103:65534::/run/rpcbind:/usr/sbin/nologin
systemd-coredump:x:998:998:systemd Core Dumper:/:/usr/sbin/nologin
tcpdump:x:124:134::/nonexistent:/usr/sbin/nologin
machin:x:2510:2510:,,,:/home/machin:/bin/bash
root@rt410p102:~#
root@rt410p102:~#
```

/etc/passwd après ajout de machin

```
root@rt410p102:~# cat /etc/shadow
root:$6$aUwA5ts9$3/3BAlKYBE3m2iD3LICONt14njpDSO785AnKrJuYeBUDUDnbnpAkisgE/EbvuGsq0TbJFEiexlIRjzbQQ9mP7.:17339:0:99999:7:::
daemon:*:17339:0:99999:7:::
bin:*:17339:0:99999:7:::
sys:*:17339:0:99999:7:::
sync:*:17339:0:99999:7:::
games:*:17339:0:99999:7:::
man:*:17339:0:99999:7:::
lp:*:17339:0:99999:7:::
mail:*:17339:0:99999:7:::
news:*:17339:0:99999:7:::
uucp:*:17339:0:99999:7:::
proxy:*:17339:0:99999:7:::
www-data:*:17339:0:99999:7:::
backup:*:17339:0:99999:7:::
list:*:17339:0:99999:7:::
irc:*:17339:0:99999:7:::
gnats:*:17339:0:99999:7:::
nobody:*:17339:0:99999:7:::
systemd-timesync:*:17339:0:99999:7:::
systemd-network:*:17339:0:99999:7:::
systemd-resolve:*:17339:0:99999:7:::
_apt:*:17339:0:99999:7:::
Debian-exim:!:17339:0:99999:7:::
rtkit:*:17339:0:99999:7:::
avahi-autoipd:*:17339:0:99999:7:::
messagebus:*:17339:0:99999:7:::
usbmux:*:17339:0:99999:7:::
speech-dispatcher:!:17339:0:99999:7:::
sshd:*:17339:0:99999:7:::
lightdm:*:17339:0:99999:7:::
pulse:*:17339:0:99999:7:::
avahi:*:17339:0:99999:7:::
colord:*:17339:0:99999:7:::
saned:*:17339:0:99999:7:::
hplip:*:17339:0:99999:7:::
rt:$6$0stLZQzu$tcD8o2H9OttkgJafFaTT5geKBqNNJMr1mW7PWldMpaddwGNi4UK.ozYwrWyFm1GzvuwG6cFXy/BX1CXV5wafK0:17339:0:99999:7:::
vboxadd:!:17339::::::
clamav:!:17342:0:99999:7:::
dovecot:*:17342:0:99999:7:::
dovenull:*:17342:0:99999:7:::
geoclue:*:17342:0:99999:7:::
mysql:!:17342:0:99999:7:::
postfix:*:17342:0:99999:7:::
statd:*:17342:0:99999:7:::
_rpc:*:18708:0:99999:7:::
systemd-coredump:!!:18709::::::
tcpdump:*:18879:0:99999:7:::
machin:$y$j9T$U1ahQK1CcxmVwb4AvsYQt1$q1EWgSkkPANdehViVQQnphTYEbioZiggWyWSmL7T6K0:18950:0:99999:7:::
root@rt410p102:~#
```

/etc/shadow après ajout de machin

On liste les groupes existants en allant lire le fichier /etc/group

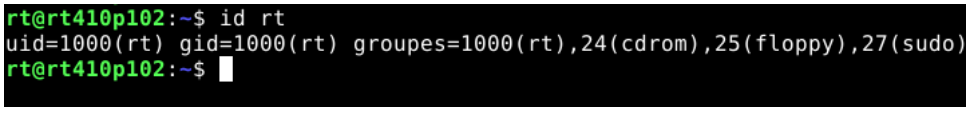


Contenu du fichier /etc/group

Et on ajoute rt au groupe sudo en faisant :

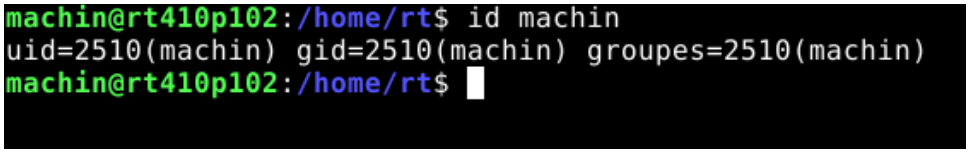
Ajout de l'utilisateur rt au groupe sudo par la commande usermod

On vérifie que ça a bien été pris en compte en faisant :



Liste des groupes auxquels rt appartient avec la commande id

L'utilisateur rt appartient bien au groupe sudo, entre autres.
Dans le même temps en vérifie à le bon uid :



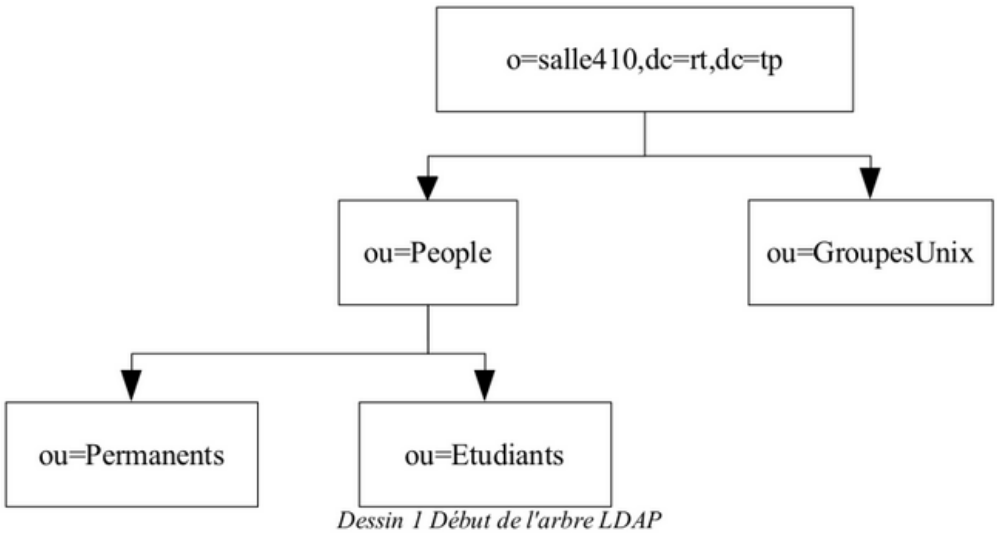
Liste des groupes auxquels machin appartient avec la commande id

Tout est bon.

2. LDAP

2.1 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

Dans un premier temps, il nous faut les paquets slapd et ldap-utils. Donc :

```
#apt update
#apt install slapd
#apt install ldap-utils
```

Lors de l'installation de slapd, on va pouvoir choisir le mot de passe administrateur. On choisira test.

Dans un second temps on va modifier le fichier olcDatabase={1}mdb.ldif dans le répertoire /etc/ldap/slapd.d/cn=config tel que :

```
# AUTO-GENERATED FILE - DO NOT EDIT!! Use ldapmodify.
# CRC32 ba4a7dd1
dn: olcDatabase={1}mdb
objectClass: olcDatabaseConfig
objectClass: olcMdbConfig
olcDatabase: {1}mdb
olcDbDirectory: /var/lib/ldap
olcSuffix: o=salle410,dc=rt,dc=tp
olcAccess: {0}to attrs=userPassword by self write by anonymous auth by * non
 e
olcAccess: {1}to attrs=shadowLastChange by self write by * read
olcAccess: {2}to * by * read
olcLastMod: TRUE
olcRootDN: cn=admin,o=salle410,dc=rt,dc=tp
olcRootPW: test
olcDbCheckpoint: 512 30
olcDbIndex: objectClass eq
olcDbIndex: cn,uid eq
olcDbIndex: uidNumber,gidNumber eq
olcDbIndex: member,memberUid eq
olcDbMaxSize: 1073741824
structuralObjectClass: olcMdbConfig
entryUUID: c9fcf3c0-df23-103b-9c5b-a91f0651fbd6
creatorsName: cn=admin,cn=config
createTimestamp: 20211121143350Z
entryCSN: 20211121143350.657596Z#000000#000#000000
modifiersName: cn=admin,cn=config
modifyTimestamp: 20211121143350Z
```

Les champs modifiés sont olcSuffix, olcRootDN et olcRootPW.

2.2 Création d'une base minimale

Maintenant que la configuration minimale a été faite, nous allons télécharger une racine de base de données déjà faite à cette adresse que nous placerons à la racine de root.
Dans ce fichier on peut voir 4 dn donc il y a 4 objets.

```
dn: o=salle410,dc=rt,dc=tp
objectClass: top
objectClass: organization
o: salle410
structuralObjectClass: organization

dn: cn=admin,o=salle410,dc=rt,dc=tp
objectClass: simpleSecurityObject
objectClass: organizationalRole
cn: admin
description: LDAP administrator
userPassword: test
structuralObjectClass: organizationalRole

dn: ou=People,o=salle410,dc=rt,dc=tp
ou: People
objectClass: top
objectClass: organizationalUnit
structuralObjectClass: organizationalUnit

dn: cn=groupe1001, o=salle410,dc=rt,dc=tp
cn: groupe1001
gidNumber: 1001
objectClass: top
objectClass: posixGroup
```

Contenu du fichier lBase-rt-410.ldif

Le dn des 4 objets correspond bien au suffixe que l'on a choisi car tous les dn finissent par o=salle410,dc=rt,dc=tp (le suffix).

Maintenant on supprime la base déjà existante grâce à :

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

Puis charger la nôtre :

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

Et là, ça ne marche pas. Pourquoi ? parce qu'on a modifié le fichier cn=config à la main alors qu'il est bien spécifié de ne PAS le modifier à la main et d'utiliser la commande ldapmodify. Bref, cela à fait que la somme de contrôle de ce fichier n'est plus bonne, il faut donc la recalculer.
On installe un paquet qui nous permet de calculer le checksum en CRC32

```
# apt install libarchive-zip-perl
```

On fait une petite commande maison qui va recalculer le checksum et le mettre à la fin du fichier posant problème :

```
# tail -n +3 olcDatabase\=\{1\}mdb.ldif > /tmp/new.ldif ; crc32
/tmp/new.ldif >> olcDatabase\=\{1\}mdb.ldif
```

Puis on édite le fichier et on remplace le checksum en début de fichier par celle en fin de fichier.
Une fois le checksum changé, il faut supprimer celle qui se trouve en fin de fichier.
Ce n'est surement pas la meilleure solution mais ça marche.
On refait :

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

Puis :

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

Et là ça marche
On donne les droits à l'utilisateur openldap :

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

Et on démarre le service :

```
# service slapd start
```

2.3 Création d'une base LDAP par interface web

On veut maintenant une interface web, il nous faut les paquets suivants :

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

Ainsi que :

```
# wget
ftp.us.debian.org/debian/pool/main/p/phpldapadmin/phpldapadmin_1.2.2-
6.3_all.deb
```

Que l'on installe à la main :

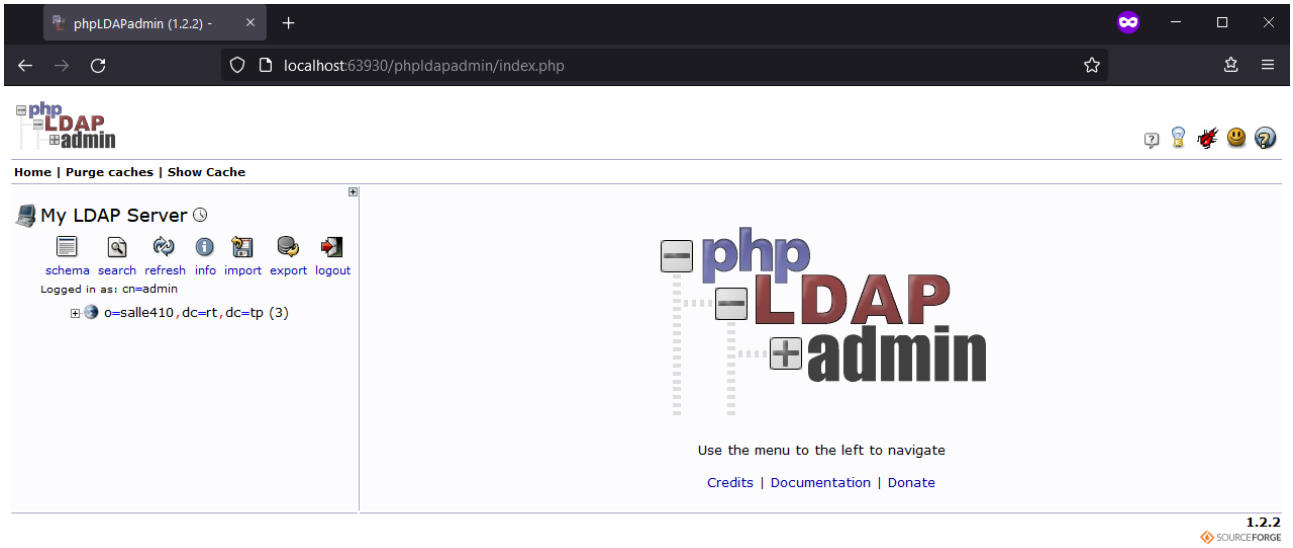
```
# dpkg -i phpldapadmin_1.2.2-6.3_all.deb
```

On adapte le fichier /etc/phpldapadmin/config.php en avec les bon DN :

```
$servers->setValue('server','base',array('o=salle410,dc=rt,dc=tp'));

/* Five options for auth_type:
   1. 'cookie': you will login via a web form, and a client-side cookie will
      store your login dn and password.
   2. 'session': same as cookie but your login dn and password are stored on the
      web server in a persistent session variable.
   3. 'http': same as session but your login dn and password are retrieved via
      HTTP authentication.
   4. 'config': specify your login dn and password here in this config file. No
      login will be required to use phpLDAPadmin for this server.
   5. 'sasl': login will be taken from the webserver's kerberos authentication.
      Currently only GSSAPI has been tested (using mod_auth_kerb).

   Choose wisely to protect your authentication information appropriately for
   your situation. If you choose 'cookie', your cookie contents will be
   encrypted using blowfish and the secret your specify above as
   session['blowfish']. */
$servers->setValue('login','auth_type','session');

/* The DN of the user for phpLDAPadmin to bind with. For anonymous binds or
   'cookie','session' or 'sasl' auth_types, LEAVE THE LOGIN_DN AND LOGIN_PASS
   BLANK. If you specify a login_attr in conjunction with a cookie or session
   auth_type, then you can also specify the bind_id/bind_pass here for searching
   the directory for users (ie, if your LDAP server does not allow anonymous
   binds. */
$servers->setValue('login','bind_id','cn=admin,o=salle410,dc=rt,dc=tp');
#  $servers->setValue('login','bind_id','cn=Manager,dc=example,dc=com');
```

Lignes modifiées dans /etc/phpldapadmin/config.php

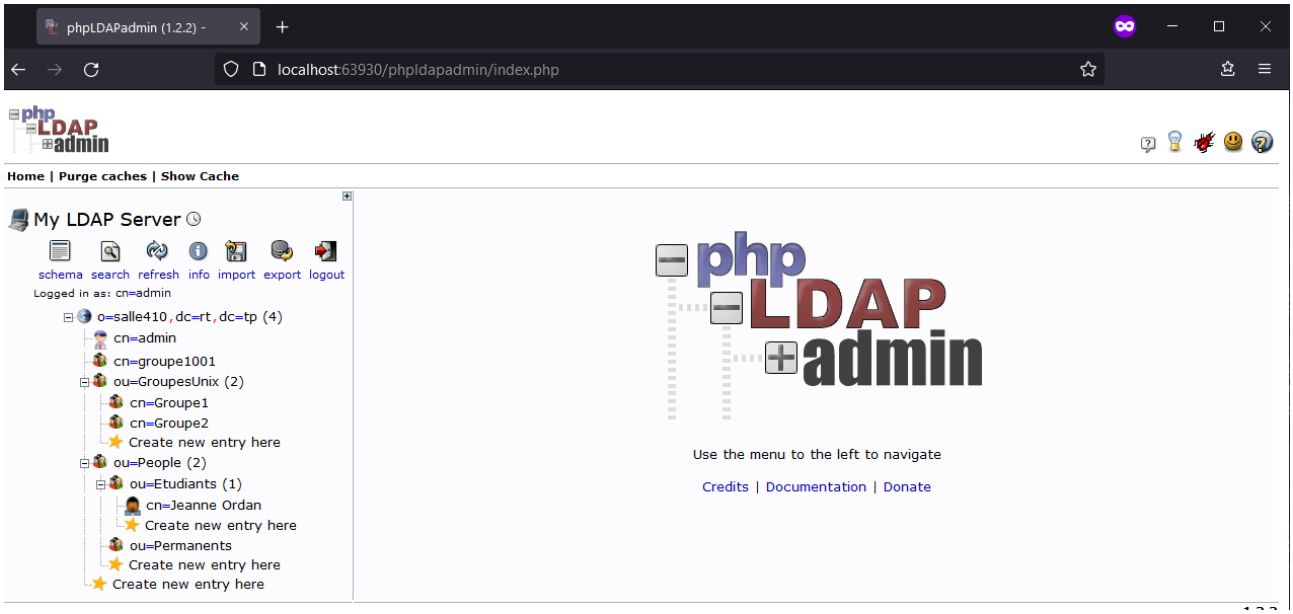
On démarre le service apache si ce n'est pas déjà le cas puis on accède à la page de configuration à l'adresse http://localhost/phpldapadmin/



Page de configuration phpldapadmin

2.4 Annuaire

On ajoute les entrées comme demandé en utilisant l'interface web, pour obtenir :



Page de configuration phpldapadmin une fois les entrées ajoutées

On peut vérifier que tout ait bien été pris en compte grâce à la commande :

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

Qui donne le résultat suivant :

```
root@7716b5e8f3ac:~# ldapsearch -x -W -b "o=salle410,dc=rt,dc=tp"
-D "cn=admin,o=salle410,dc=rt,dc=tp"
Enter LDAP Password:
# extended LDIF
#
# LDAPv3
# base <o=salle410,dc=rt,dc=tp> with scope subtree
# filter: (objectclass=*)
# requesting: ALL
#

# salle410, rt.tp
dn: o=salle410,dc=rt,dc=tp
objectClass: top
objectClass: organization
o: salle410

# admin, salle410, rt.tp
dn: cn=admin,o=salle410,dc=rt,dc=tp
objectClass: simpleSecurityObject
objectClass: organizationalRole
cn: admin
```

```
description: LDAP administrator
userPassword:: dGVzdA==

# People, salle410, rt.tp
dn: ou=People,o=salle410,dc=rt,dc=tp
ou: People
objectClass: top
objectClass: organizationalUnit

# groupe1001, salle410, rt.tp
dn: cn=groupe1001,o=salle410,dc=rt,dc=tp
cn: groupe1001
objectClass: posixGroup
objectClass: top
gidNumber: 1001

# GroupesUnix, salle410, rt.tp
dn: ou=GroupesUnix,o=salle410,dc=rt,dc=tp
objectClass: organizationalUnit
objectClass: top
ou: GroupesUnix

# Etudiants, People, salle410, rt.tp
dn: ou=Etudiants,ou=People,o=salle410,dc=rt,dc=tp
objectClass: organizationalUnit
objectClass: top
ou: Etudiants

# Permanents, People, salle410, rt.tp
dn: ou=Permanents,ou=People,o=salle410,dc=rt,dc=tp
objectClass: organizationalUnit
objectClass: top
ou: Permanents

# Jeanne Ordan, Etudiants, People, salle410, rt.tp
dn: cn=Jeanne Ordan,ou=Etudiants,ou=People,o=salle410,dc=rt,dc=tp
cn: Jeanne Ordan
givenName: Jeanne
gidNumber: 500
homeDirectory: /home/users/jordan
sn: Ordan
loginShell: /bin/sh
objectClass: inetOrgPerson
objectClass: posixAccount
objectClass: top
userPassword:: e01ENX1DaW1UK0FmS3dsdHd0V2NNM1c4UTlBPT0=
uid: jordan
uidNumber: 1234

# Groupe1, GroupesUnix, salle410, rt.tp
dn: cn=Groupe1,ou=GroupesUnix,o=salle410,dc=rt,dc=tp
cn: Groupe1
objectClass: posixGroup
```

```
objectClass: top
gidNumber: 500

# Groupe2, GroupesUnix, salle410, rt.tp
dn: cn=Groupe2,ou=GroupesUnix,o=salle410,dc=rt,dc=tp
gidNumber: 501
cn: Groupe2
objectClass: posixGroup
objectClass: top

# search result
search: 2
result: 0 Success

# numResponses: 11
# numEntries: 10
root@7716b5e8f3ac:~#
```

Résultat de la commande ldapsearch -x -W -b "o=salle410,dc=rt,dc=tp" -D "cn=admin,o=salle410,dc=rt,dc=tp"

3. Authentification par LDAP

3.2 Intégration à PAM

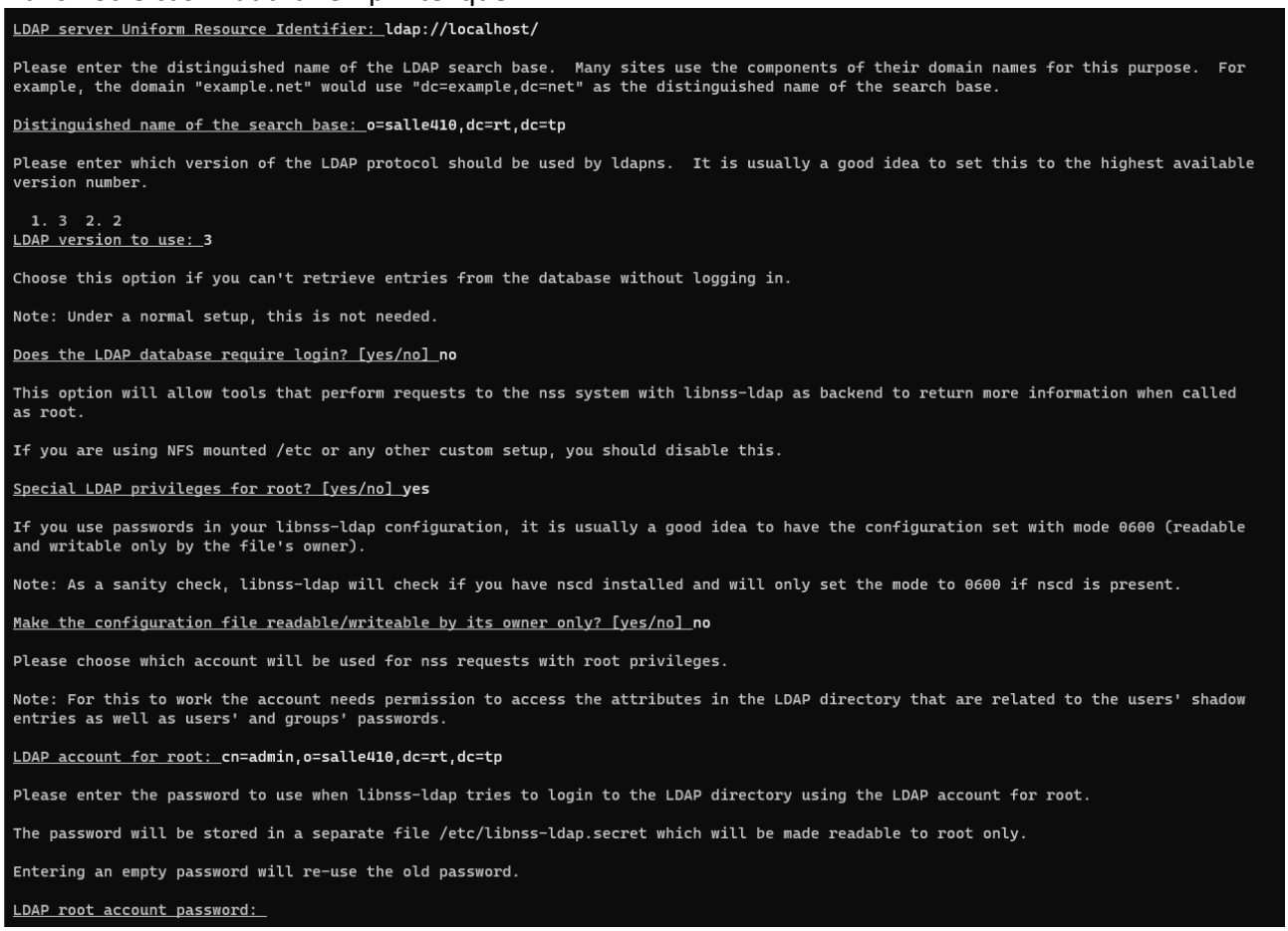
Pour pouvoir utiliser PAM, il faut installer le paquet suivant :

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

Lors de son installation il faut correctement configurer les champs demandés. Si l'on se trompe lors de l'installation, on peut reconfigurer grâce à la commande :

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

Dans notre cas il faudra remplir tel que :



3.2.1 Obtenir l'information sur le compte

Une fois fait, on dit à l'OS d'aller fournir les fichiers passwd, group et shadow via LDAP.
Pour ce faire on édite le fichier /etc/nsswitch.conf tel que :

```
# /etc/nsswitch.conf
#
# Example configuration of GNU Name Service Switch functionality.
# If you have the `glibc-doc-reference' and `info' packages installed, try:
# `info libc "Name Service Switch"' for information about this file.

passwd:         files ldap
group:          files ldap
shadow:         files ldap
gshadow:        files

hosts:          files dns
networks:       files

protocols:      db files
services:       db files
ethers:         db files
rpc:            db files

netgroup:       nis
~
```

Contenu du fichier /etc/nsswitch.conf après modification

Enfin, on redémarre le démon nscd pour recharger le cache des comptes sous linux et on peut tester si la base LDAP est bien importé localement en faisant :

```
#getent passwd
```

```
root@7716b5e8f3ac:/# getent passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
_apt:x:100:65534::/nonexistent:/usr/sbin/nologin
openldap:x:101:101:OpenLDAP Server Account,,,:/var/lib/ldap:/bin/false
Debian-exim:x:102:104::/var/spool/exim4:/usr/sbin/nologin
jordan:*:1234:500:Jeanne Ordan:/home/users/jordan:/bin/sh
root@7716b5e8f3ac:/#
```

3.2.2 Pouvoir se loger

Ça marche, l'utilisateur créé tout à l'heure apparait bien ici (jordan).

Maintenant on aimerait bien pourvoir se logger.
Pour ça :
On reconfigure le paquet libpam-ldap un peu comme libnss-ldap

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

Tel que :

```
root@7716b5e8f3ac:/# dpkg-reconfigure libpam-ldap
debconf: unable to initialize frontend: Dialog
debconf: (No usable dialog-like program is installed, so the dialog based
frontend cannot be used. at /usr/share/perl5/Debconf/FrontEnd/Dialog.pm line
78.)
debconf: falling back to frontend: Readline
Configuring libpam-ldap
----------------------

Please enter the Uniform Resource Identifier of the LDAP server. The format is
'ldap://<hostname_or_IP>:<port>/'. Alternatively,
'ldaps://' or 'ldapi://' can be used. The port number is optional.

Using an IP address is recommended to avoid failures when domain name services
are unavailable.

LDAP server URI: ldap://localhost/

Please enter the distinguished name of the LDAP search base. Many sites use
the components of their domain names for this purpose. For
example, the domain "example.net" would use "dc=example,dc=net" as the
distinguished name of the search base.

Distinguished name of the search base: o=salle410,dc=rt,dc=tp

Please choose the version of the LDAP protocol that should be used by ldapns.
Using the highest available version number is recommended.

  1. 3  2. 2
LDAP version to use: 3

This option will allow password utilities that use PAM to change local
passwords.

The LDAP admin account password will be stored in a separate file which will
be made readable to root only.

If /etc is mounted by NFS, this option should be disabled.

Allow LDAP admin account to behave like local root? [yes/no] yes

Please choose whether the LDAP server enforces a login before retrieving
entries.

Such a setup is not usually needed.

Does the LDAP database require login? [yes/no] no

Please enter the name of the LDAP administrative account.
```

```
This account will be used automatically for database management, so it must
have the appropriate administrative privileges.

LDAP administrative account: cn=admin,o=salle410,dc=rt,dc=tp

Please enter the password of the administrative account.

The password will be stored in the file /etc/pam_ldap.secret. This will be
made readable to root only, and will allow libpam-ldap to
carry out automatic database management logins.

If this field is left empty, the previously stored password will be re-used.

LDAP administrative password:

The PAM module can encrypt the password locally when changing it, which is
recommended:
 * clear: no encryption. This should be chosen when LDAP servers
   automatically encrypt the userPassword entry;
 * crypt: make userPassword use the same format as the flat
   local password database. If in doubt, you should choose this option;
 * nds: use Novell Directory Services-style updating. The old
   password is first removed, then updated;
 * ad: Active Directory-style. This creates a Unicode password and
   updates the unicodePwd attribute;
 * exop: use the OpenLDAP password change extended operation to update the
   password.

  1. clear  2. crypt  3. nds  4. ad  5. exop  6. md5
Local encryption algorithm to use for passwords: 2

PAM configuration
-----------------

Pluggable Authentication Modules (PAM) determine how authentication,
authorization, and password changing are handled on the system, as
well as allowing configuration of additional actions to take when starting
user sessions.

Some PAM module packages provide profiles that can be used to automatically
adjust the behavior of all PAM-using applications on the
system.  Please indicate which of these behaviors you wish to enable.

  1. Unix authentication  3. Register user sessions in the systemd control
group hierarchy  5. Inheritable Capabilities Management
  2. LDAP Authentication  4. Create home directory on login
6. none of the above

(Enter the items or ranges you want to select, separated by spaces.)

PAM profiles to enable: 1 2 3 5
```

Le texte en gras sont les paramètres entrés.

On vérifie que ça marche en faisant :
Un ssh sur nous même mais avec le nom de l'utilisateur LDAP

```
root@7716b5e8f3ac:/# ssh jordan@localhost
The authenticity of host 'localhost (127.0.0.1)' can't be established.
ECDSA key fingerprint is SHA256:k0yjTsoOa4obE9bBQSwFB+JL1s0I9ZDqOvdL6Xx0fTE.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added 'localhost' (ECDSA) to the list of known hosts.
jordan@localhost's password:
Linux 7716b5e8f3ac 5.10.16.3-microsoft-standard-WSL2 #1 SMP Fri Apr 2 22:23:49 UTC 2021 x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Could not chdir to home directory /home/users/jordan: No such file or directory
$
$ pwd
/
$ whoami
jordan
$
```

Ça marche !
On arrive sur la racine.

3.2.3 Création du homedir

Si maintenant on veut arriver dans un répertoire personnel type /home/users/<non_user>
Il faut relancer la configuration de ce paquet et spécifier "create home directory on login" comme ceci :

```
Pluggable Authentication Modules (PAM) determine how authentication, authorization, and password changing are handled on the system, as
well as allowing configuration of additional actions to take when starting user sessions.

Some PAM module packages provide profiles that can be used to automatically adjust the behavior of all PAM-using applications on the
system.  Please indicate which of these behaviors you wish to enable.

  1. Unix authentication  3. Register user sessions in the systemd control group hierarchy  5. Inheritable Capabilities Management
  2. LDAP Authentication  4. Create home directory on login                                  6. none of the above

(Enter the items or ranges you want to select, separated by spaces.)

PAM profiles to enable: 1 2 3 4 5
```

Et donc on obtient un home directory :

```
root@7716b5e8f3ac:/etc/pam.d# ssh jordan@localhost
jordan@localhost's password:
Creating directory '/home/users/jordan'.
Linux 7716b5e8f3ac 5.10.16.3-microsoft-standard-WSL2 #1 SMP Fri Apr 2 22:23:49 UTC 2021 x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Thu Nov 25 15:53:27 2021 from 127.0.0.1
$ ls
$ pwd
/home/users/jordan
$
$
$ ^C
$ exit
Connection to localhost closed.
root@7716b5e8f3ac:/etc/pam.d# ssh jordan@localhost
```

3.2.4 Configuration Apache

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

On ajoute le module ldap dans apache2 :

```
# a2enmod ldap auth_basic authnz_ldap authz_user
```

On redémarre le service apache2 :

```
# service apache2 restart
```

On modifie le fichier /etc/apache2/apache2.conf pour autoriser l'override partour dans le répertoire /var/www/, tel que :

```
<Directory /var/www/>
        Options Indexes FollowSymLinks
        AllowOverride All
        Require all granted
</Directory>
```

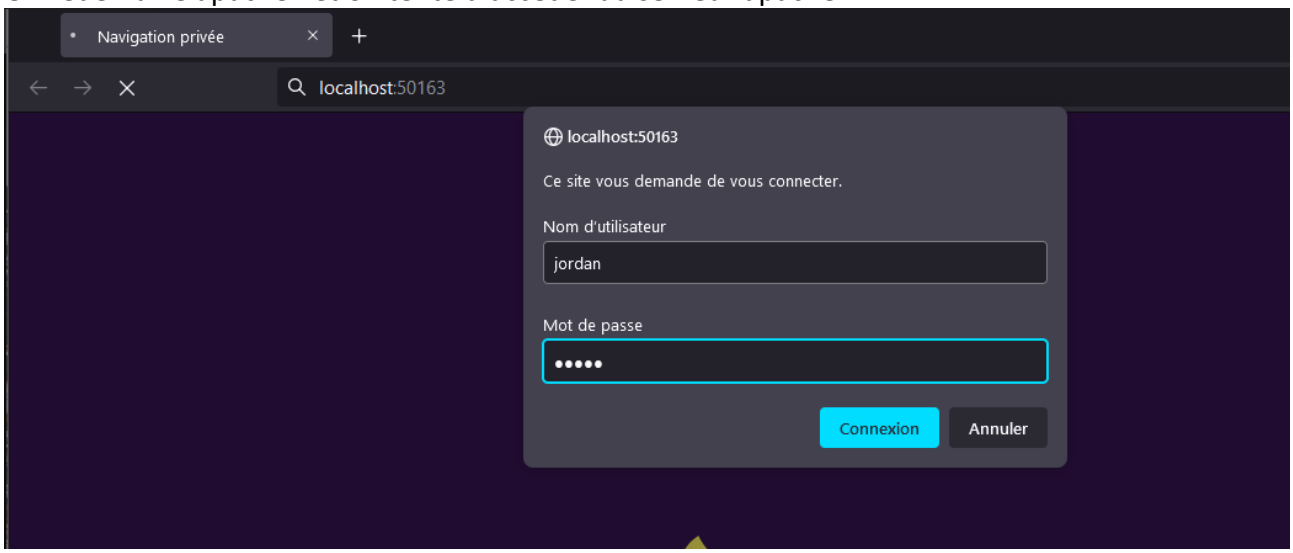
Partie du fichier /etc/apache2/apache2.conf

On crée le fichier /var/www/html/.htaccess et on le remplie de la sorte :

```
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
```

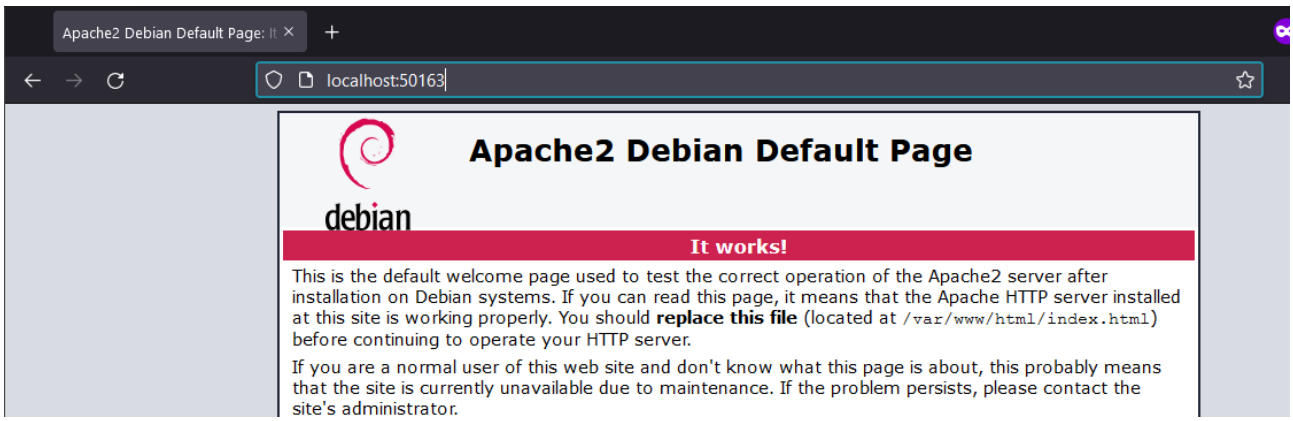
Fichier /var/www/html/.htaccess

On redémarre apache2 et on tente d'accéder au serveur apache :



Demande de connexion de la part de apache

Il nous demande de nous authentifier, on le fait avec l'utilisateur créé, et ça marche :



Connexion réussie et accès à la page par défaut de apache