

# TP 5

Administration système

Dardor Rochdi

# Rappels sur LDAP

## EXERCICE 5.1 :

Le protocole LDAP (Lightweight Directory Access Protocol) a pour objectif de permettre l'accès et la gestion d'un annuaire centralisé contenant des informations sur les utilisateurs, les groupes et d'autres objets d'une organisation. Il offre un moyen standardisé et efficace d'interroger et de modifier ces données.

## EXERCICE 5.2 :

LDAP est principalement utilisé pour l'authentification centralisée et la gestion des droits d'accès dans un réseau d'entreprise. Il permet de réduire la duplication des comptes et d'assurer une cohérence dans la gestion des identités.

## EXERCICE 5.3 :

LDAP n'est pas limité à l'authentification centralisée. Il peut également être utilisé pour stocker et organiser d'autres types de données comme les noms d'hôtes, les certificats et les répertoires téléphoniques.

## EXERCICE 5.4 :

Lors de l'ajout d'informations dans un annuaire LDAP, il est essentiel de garantir la confidentialité et l'intégrité des données. Cela passe par :

- La définition correcte des droits d'accès.
- L'utilisation de connexions chiffrées (LDAPS).
- La gestion des sauvegardes et de la redondance.

## EXERCICE 5.5 :

Contrairement à une base de données relationnelle comme MySQL, LDAP est conçu pour des lectures rapides et fréquentes. Voici quelques particularités de LDAP :

- Il utilise une structure hiérarchique sous forme d'arbre.
- Les données sont organisées en entrées avec des attributs.
- Il ne supporte pas directement les transactions complexes ou les jointures comme une base SQL.

# Mise en place du serveur

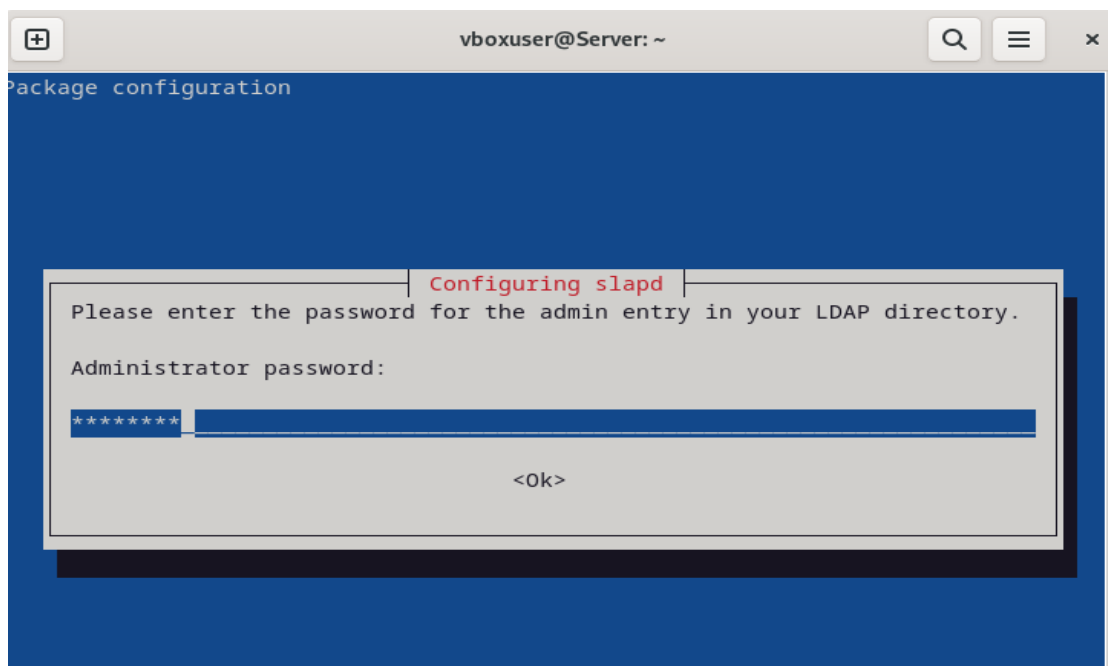
## EXERCICE 5.6 :

Pour installer le serveur LDAP sur ma VM serveur, j'ai exécuté la commande suivante :

```
sudo apt install ldap-utils slapd
```

Lors de l'installation, j'ai configuré le domaine de l'annuaire comme suit :  
dc=istycorp,dc=fr.

```
vboxuser@Server:~$ sudo apt install ldap-utils slapd -y
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
  libodbc2
Suggested packages:
  libsasl2-modules-gssapi-mit | libsasl2-modules-gssapi-heimdal
  odbc-postgresql tdsodbc
The following NEW packages will be installed:
  ldap-utils libodbc2 slapd
0 upgraded, 3 newly installed, 0 to remove and 0 not upgraded.
Need to get 1,730 kB of archives.
After this operation, 5,950 kB of additional disk space will be used.
Ign:1 http://deb.debian.org/debian bookworm/main amd64 libodbc2 amd64 2.3.11-2+d
eb12u1
Ign:2 http://deb.debian.org/debian bookworm/main amd64 slapd amd64 2.5.13+dfsg-5
0% [Working]
```

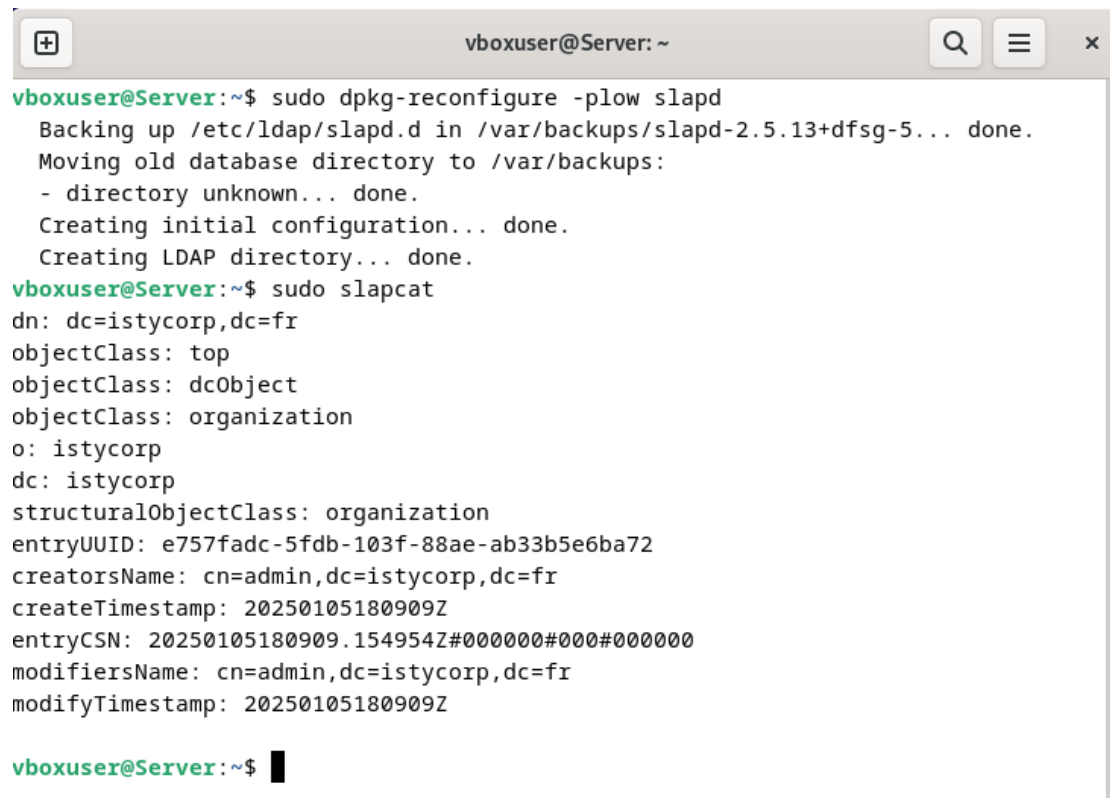


## EXERCICE 5.7 :

J'ai utilisé la commande suivante pour reconfigurer la base de données LDAP :

```
dpkg-reconfigure -plow slapd
```

Ensuite, j'ai vérifié le contenu de la base de données avec slapcat afin d'identifier les éléments importants comme l'entrée admin et les unités organisationnelles.



```
vboxuser@Server: ~  
vboxuser@Server:~$ sudo dpkg-reconfigure -plow slapd  
Backing up /etc/ldap/slapd.d in /var/backups/slapd-2.5.13+dfsg-5... done.  
Moving old database directory to /var/backups:  
- directory unknown... done.  
Creating initial configuration... done.  
Creating LDAP directory... done.  
vboxuser@Server:~$ sudo slapcat  
dn: dc=istycorp,dc=fr  
objectClass: top  
objectClass: dcObject  
objectClass: organization  
o: istycorp  
dc: istycorp  
structuralObjectClass: organization  
entryUUID: e757fadc-5fdb-103f-88ae-ab33b5e6ba72  
creatorsName: cn=admin,dc=istycorp,dc=fr  
createTimestamp: 20250105180909Z  
entryCSN: 20250105180909.154954Z#000000#000#000000  
modifiersName: cn=admin,dc=istycorp,dc=fr  
modifyTimestamp: 20250105180909Z  
  
vboxuser@Server:~$ █
```

## EXERCICE 5.8 :

Pour structurer l'annuaire en deux branches, people et groups, j'ai créé un fichier create-struct.ldiff contenant :

```
dn: ou=people,dc=istycorp,dc=fr
```

```
objectClass: organizationalUnit
```

```
ou: people
```

```
dn: ou=groups,dc=istycorp,dc=fr
```

```
objectClass: organizationalUnit
```

```
ou: groups
```

J'ai ensuite chargé cette structure avec la commande :

```
ldapadd -x -D "cn=admin,dc=istycorp,dc=fr" -f create-struct.ldiff -W
```



```
vboxuser@Server: ~  
vboxuser@Server:~$ nano create-struct.ldiff  
vboxuser@Server:~$ sudo ldapadd -x -D "cn=admin,dc=istycorp,dc=fr" -f create-struct.ldiff -W  
Enter LDAP Password:  
adding new entry "ou=people,dc=istycorp,dc=fr"  
  
adding new entry "ou=groups,dc=istycorp,dc=fr"  
  
vboxuser@Server:~$ cat create-struct.ldiff  
dn: ou=people,dc=istycorp,dc=fr  
objectClass: organizationalUnit  
ou: people  
  
dn: ou=groups,dc=istycorp,dc=fr  
objectClass: organizationalUnit  
ou: groups  
vboxuser@Server:~$ █
```

### EXERCICE 5.9 :

J'ai ajouté un utilisateur nommé rochdi dardor dans la branche people en utilisant le fichier add-user.ldiff suivant :

```
dn: cn=rochdi,ou=people,dc=istycorp,dc=fr  
  
objectClass: top  
  
objectClass: account  
  
objectClass: posixAccount  
  
objectClass: shadowAccount  
  
uid: rochdi  
  
uidNumber: 1001  
  
gidNumber: 1001  
  
userPassword: changemoi  
  
gecos: Rochdi Dardor  
  
loginShell: /bin/bash  
  
homeDirectory: /home/rochdi
```

La commande utilisée pour l'ajouter :

**ldapadd -x -D "cn=admin,dc=istycorp,dc=fr" -f add-user.ldiff -W**

```
vboxuser@Server: ~  
vboxuser@Server:~$ nano add-user.ldiff  
vboxuser@Server:~$ cat add-user.ldiff  
dn: cn=rochdi,ou=people,dc=istycorp,dc=fr  
objectClass: top  
objectClass: account  
objectClass: posixAccount  
objectClass: shadowAccount  
uid: rochdi  
uidNumber: 1001  
gidNumber: 1001  
userPassword: changeme  
gecos: Rochdi Dardor  
loginShell: /bin/bash  
homeDirectory: /home/rochdi  
vboxuser@Server:~$ ldapadd -x -D "cn=admin,dc=istycorp,dc=fr" -W -f add-user.ldiff  
Enter LDAP Password:  
adding new entry "cn=rochdi,ou=people,dc=istycorp,dc=fr"  
  
vboxuser@Server:~$ ldapsearch -x -b "dc=istycorp,dc=fr" "(uid=rochdi)"  
# extended LDIF  
#  
# LDAPv3  
# base <dc=istycorp,dc=fr> with scope subtree  
# filter: (uid=rochdi)  
# requesting: ALL  
#
```

## EXERCICE 5.10 :

J'ai créé un groupe nommé user et y ai ajouté l'utilisateur rochdi :

dn: cn=user,ou=groups,dc=istycorp,dc=fr

objectClass: top

objectClass: posixGroup

cn: user

memberUid: rochdi

gidNumber: 1001

J'ai ensuite chargé ce fichier avec la commande **ldapadd**.

```
vboxuser@Server: ~
vboxuser@Server:~$ nano add-group.ldif
vboxuser@Server:~$ cat add-group.ldif
dn: cn=user,ou=groups,dc=istycorp,dc=fr
objectClass: top
objectClass: posixGroup
cn: user
memberUid: rochdi
gidNumber: 1000
vboxuser@Server:~$ ldapadd -x -D "cn=admin,dc=istycorp,dc=fr" -W -f add-group.ldif
Enter LDAP Password:
adding new entry "cn=user,ou=groups,dc=istycorp,dc=fr"

vboxuser@Server:~$ ldapsearch -x -b "dc=istycorp,dc=fr" "(cn=user)"
# extended LDIF
#
# LDAPv3
# base <dc=istycorp,dc=fr> with scope subtree
# filter: (cn=user)
# requesting: ALL
#
# user, groups, istycorp.fr
dn: cn=user,ou=groups,dc=istycorp,dc=fr
objectClass: top
objectClass: posixGroup
cn: user
memberUid: rochdi
```

### EXERCICE 5.11 :

Pour vérifier que l'utilisateur avait bien été ajouté, j'ai utilisé la commande suivante :

```
ldapsearch -x -D "cn=admin,dc=istycorp,dc=fr" -W -b "ou=people,dc=istycorp,dc=fr"
"(uid=rochdi)"
```

La requête a retourné les informations correctes concernant l'utilisateur rochdi.

```
vboxuser@Server:~$ ldapsearch -x -D "cn=rochdi,ou=people,dc=istycorp,dc=fr" -W -b "cn=rochdi,ou=people,dc=istycorp,dc=fr"
Enter LDAP Password:
# extended LDIF
#
# LDAPv3
# base <cn=rochdi,ou=people,dc=istycorp,dc=fr> with scope subtree
# filter: (objectclass=*)
# requesting: ALL
#
# rochdi, people, istycorp.fr
dn: cn=rochdi,ou=people,dc=istycorp,dc=fr
objectClass: top
objectClass: account
objectClass: posixAccount
objectClass: shadowAccount
uid: rochdi
uidNumber: 1001
gidNumber: 1001
userPassword:: Y2hhbmdlbnV=
gecos: Rochdi Dardor
loginShell: /bin/bash
homeDirectory: /home/rochdi
cn: rochdi

# search result
search: 2
```

### EXERCICE 5.12 :

J'ai changé le mot de passe de l'utilisateur rochdi avec la commande :

```
ldappasswd -x -D 'cn=admin,dc=istycorp,dc=fr' -W -S
'uid=rochdi,ou=people,dc=istycorp,dc=fr'
```

```
vboxuser@Server: ~  
vboxuser@Server:~$ ldappasswd -x -D "cn=rochdi,ou=people,dc=istycorp,dc=fr" -W -S  
New password:  
Re-enter new password:  
Enter LDAP Password:  
vboxuser@Server:~$ ldapsearch -x -D "cn=rochdi,ou=people,dc=istycorp,dc=fr" -W -b "cn=rochdi,ou=people,dc=istycorp,dc=fr"  
Enter LDAP Password:  
# extended LDIF  
#  
# LDAPv3  
# base <cn=rochdi,ou=people,dc=istycorp,dc=fr> with scope subtree  
# filter: (objectclass=*)  
# requesting: ALL  
#  
# rochdi, people, istycorp.fr  
dn: cn=rochdi,ou=people,dc=istycorp,dc=fr  
objectClass: top  
objectClass: account  
objectClass: posixAccount  
objectClass: shadowAccount  
uid: rochdi  
uidNumber: 1001
```

# Gestion graphique : phpldapadmin

## EXERCICE 5.13 :

Pour simplifier la gestion de l'annuaire, j'ai installé l'interface graphique phpLDAPAdmin avec la commande :

```
sudo apt install phpldapadmin php8.2
```

J'ai ensuite configuré l'accès en modifiant le fichier `/etc/phpldapadmin/config.php` afin de pointer vers mon domaine `dc=istycorp,dc=fr`.

```
vboxuser@Server:~$ sudo apt install phpldapadmin
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following NEW packages will be installed:
  phpldapadmin
0 upgraded, 1 newly installed, 0 to remove and 0 not upgraded.
Need to get 702 kB of archives.
After this operation, 3,078 kB of additional disk space will be used.
Get:1 http://deb.debian.org/debian bookworm/main amd64 phpldapadmin all 1.2.6.3-0.3+deb12u1 [702 kB]
Fetched 702 kB in 0s (2,994 kB/s)
Preconfiguring packages ...
Selecting previously unselected package phpldapadmin.
(Reading database ... 185572 files and directories currently installed.)
Preparing to unpack .../phpldapadmin_1.2.6.3-0.3+deb12u1_all.deb ...
Unpacking phpldapadmin (1.2.6.3-0.3+deb12u1) ...
Setting up phpldapadmin (1.2.6.3-0.3+deb12u1) ...

Creating config file /etc/phpldapadmin/config.php with new version
apache2_invoke: Enable configuration phpldapadmin.conf
vboxuser@Server:~$
```

## EXERCICE 5.14 :

Une fois l'installation terminée, j'ai accédé à l'interface via le navigateur à l'adresse <https://192.168.0.4/phpldapadmin>. Après avoir saisi les identifiants administratifs, j'ai pu visualiser et gérer les entrées de l'annuaire

```
GNU nano 7.2 /etc/phpldapadmin/config.php *
$servers->setValue('server','host','127.0.0.1');

/* The port your LDAP server listens on (no quotes). 389 is standard. */
// $servers->setValue('server','port',389);

/* Array of base DN's of your LDAP server. Leave this blank to have phpLDAPadmin
auto-detect it for you. */
$servers->setValue('server','base',array('dc=istycorp,dc=fr'));

/* 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).

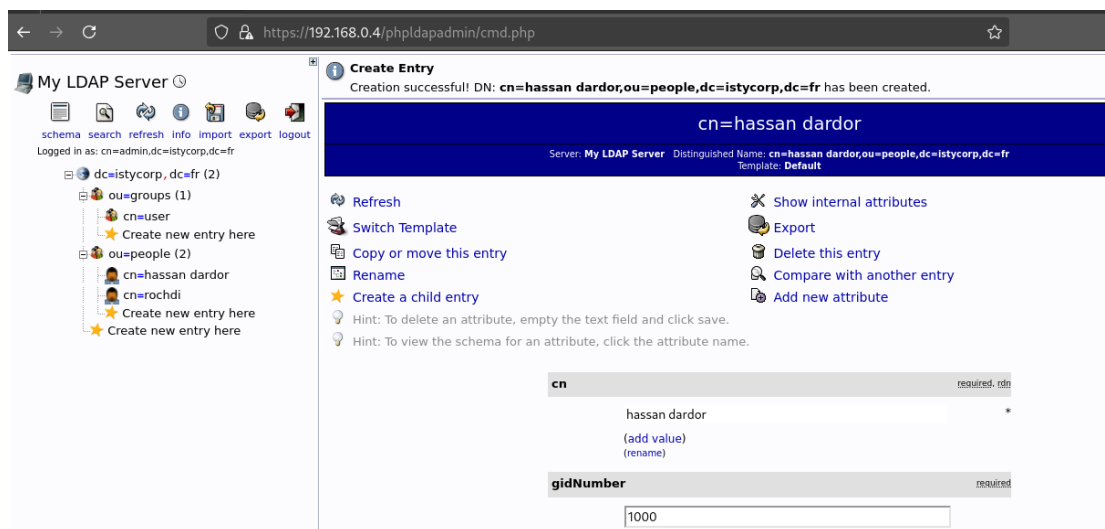
^G Help      ^O Write Out  ^W Where Is   ^K Cut        ^T Execute    ^C Location
^X Exit      ^R Read File  ^N Replace   ^U Paste      ^J Justif     ^_ Go To Line
```

## EXERCICE 5.15 :

J'ai créé un deuxième utilisateur via l'interface phpLDAPadmin en utilisant le modèle Generic: User Account. J'ai rempli les champs nécessaires, notamment :

- **UID** : hassan dardor
- **UID Number** : 1002
- **GID Number** : 1000 (pour l'ajouter au groupe user)
- **Home Directory** : /home/hdardor

Après validation, j'ai vérifié que l'utilisateur apparaissait correctement dans la branche people et qu'il était bien membre du groupe user.



# Intégration à PAM

## EXERCICE 5.16 :

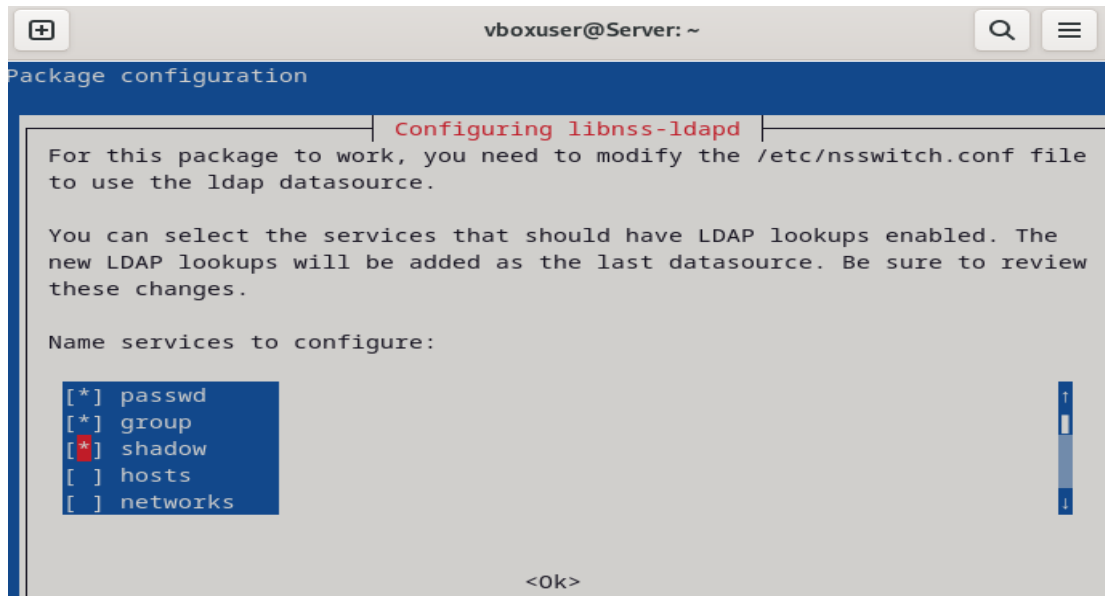
Pour intégrer LDAP dans l'authentification Unix, j'ai installé les paquets nécessaires avec la commande :

```
sudo apt install libpam-ldapd libnss-ldapd
```

Durant l'installation, une interface de configuration s'est affichée, où j'ai spécifié l'URI du serveur LDAP :

```
ldap://192.168.0.4
```

J'ai également renseigné le DN de liaison administrateur et le mot de passe associé.



### EXERCICE 5.17 :

Après installation, j'ai vérifié les fichiers de configuration suivants :

**/etc/nslcd.conf** : contient les paramètres de connexion au serveur LDAP.

**/etc/pam.d/** : j'ai vérifié les lignes relatives à l'intégration LDAP dans les différents services PAM.

```

vboxuser@Server:~$ grep -i ldap /etc/pam.d/*
/etc/pam.d/common-account:account      [success=ok new_authtok_reqd=done ignore
=ignore user_unknown=ignore authinfo_unavail=ignore default=bad]      pam_ldap
.so minimum_uid=1000
/etc/pam.d/common-auth:# (e.g., /etc/shadow, LDAP, Kerberos, etc.). The default
is to use the
/etc/pam.d/common-auth:auth      [success=1 default=ignore]      pam_ldap.so mini
mum_uid=1000 use_first_pass
/etc/pam.d/common-password:password      [success=1 default=ignore]      pam_ldap
.so minimum_uid=1000 try_first_pass
/etc/pam.d/common-session:session      [success=ok default=ignore]      pam_ldap
.so minimum_uid=1000
/etc/pam.d/common-session-noninteractive:session      [success=ok default=igno
re]      pam_ldap.so minimum_uid=1000
vboxuser@Server:~$

```

```
vboxuser@Server: ~
GNU nano 7.2 /etc/nslcd.conf
# /etc/nslcd.conf
# nslcd configuration file. See nslcd.conf(5)
# for details.

# The user and group nslcd should run as.
uid nslcd
gid nslcd

# The location at which the LDAP server(s) should be reachable.
uri ldap://192.168.0.4:389/

# The search base that will be used for all queries.
base dc=istycorp,dc=fr

# The LDAP protocol version to use.
#ldap_version 3

# The DN to bind with for normal lookups.
#binddn cn=anonymous,dc=example,dc=net
#bindpw secret
```

### EXERCICE 5.18:

J'ai modifié le fichier /etc/pam.d/common-session en ajoutant la ligne suivante pour que les dossiers utilisateurs soient créés automatiquement lors de leur première connexion :

```
session required pam_mkhomedir.so skel=/etc/skel umask=0022
```

```
vboxuser@Server: ~
GNU nano 7.2 /etc/pam.d/common-session *
# pam-auth-update to manage selection of other modules. See
# pam-auth-update(8) for details.

# here are the per-package modules (the "Primary" block)
session [default=1] pam_permit.so
# here's the fallback if no module succeeds
session requisite pam_deny.so
# prime the stack with a positive return value if there isn't one already;
# this avoids us returning an error just because nothing sets a success code
# since the modules above will each just jump around
session required pam_permit.so
# and here are more per-package modules (the "Additional" block)
session required pam_unix.so
session [success=ok default=ignore] pam_ldap.so minimum_uid=1000
session optional pam_systemd.so
# end of pam-auth-update config
session required pam_mkhomedir.so skel=/etc/skel umask=0022

^G Help      ^O Write Out ^W Where Is  ^K Cut       ^T Execute  ^C Location
^X Exit      ^R Read File ^\ Replace   ^U Paste     ^J Justify  ^_ Go To Line
```

## EXERCICE 5.19:

Pour vérifier que NSS communique correctement avec le serveur LDAP, j'ai exécuté la commande suivante :

### getent passwd

Cette commande a listé les utilisateurs de l'annuaire LDAP, confirmant le bon fonctionnement.

En cas d'erreur, j'ai utilisé la commande suivante pour lancer le démon NSS en mode debug :

### sudo nslcd -d

```
vboxuser@Server: ~  
vboxuser@Server:~$ 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  
_apt:x:42:65534:/:nonexistent:/usr/sbin/nologin  
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin  
systemd-network:x:998:998:systemd Network Management:/:usr/sbin/nologin  
tss:x:100:107:TPM software stack,,,:/var/lib/tpm:/bin/false  
  
systemd-timesync:x:997:997:systemd Time Synchronization:/:usr/sbin/nologin  
messagebus:x:101:108:/:nonexistent:/usr/sbin/nologin  
avahi-autoipd:x:102:111:Avahi autoip daemon,,,:/var/lib/avahi-autoipd:/usr/sbin/nologin  
usbmux:x:103:46:usbmux daemon,,,:/var/lib/usbmux:/usr/sbin/nologin  
dnsmasq:x:104:65534:dnsmasq,,,:/var/lib/misc:/usr/sbin/nologin  
avahi:x:105:113:Avahi mDNS daemon,,,:/run/avahi-daemon:/usr/sbin/nologin  
speech-dispatcher:x:106:29:Speech Dispatcher,,,:/run/speech-dispatcher:/bin/false  
fwupd-refresh:x:107:116:fwupd-refresh user,,,:/run/systemd:/usr/sbin/nologin  
saned:x:108:118:/:/var/lib/saned:/usr/sbin/nologin  
geoclue:x:109:119:/:/var/lib/geoclue:/usr/sbin/nologin  
polkitd:x:996:996:polkit:/nonexistent:/usr/sbin/nologin  
rtkit:x:110:120:RealtimeKit,,,:/proc:/usr/sbin/nologin  
colord:x:111:121:colord colour management daemon,,,:/var/lib/colord:/usr/sbin/nologin  
gnome-initial-setup:x:112:65534:/:run/gnome-initial-setup:/bin/false  
Debian-gdm:x:113:122:Gnome Display Manager:/var/lib/gdm3:/bin/false  
vboxuser:x:1000:1000:vboxuser,,,:/home/vboxuser:/bin/bash  
vboxadd:x:999:1:/:var/run/vboxadd:/bin/false  
_rpc:x:114:65534:/:run/pcbind:/usr/sbin/nologin  
statd:x:115:65534:/:var/lib/nfs:/usr/sbin/nologin  
sshd:x:116:65534:/:run/sshd:/usr/sbin/nologin  
mysql:x:117:123:MySQL Server,,,:/nonexistent:/bin/false  
tomcat:x:1001:1001:/:opt/tomcat:/bin/false  
openldap:x:118:124:OpenLDAP Server Account,,,:/var/lib/ldap:/bin/false  
nslcd:x:119:125:nslcd name service LDAP connection daemon,,,:/run/nslcd:/usr/sbin/nologin  
rochdi:x:1001:1001:Rochdi Dardor:/home/rochdi:/bin/bash  
hwardor:*:1002:1000:hassan dardor:/home/users/hwardor:  
vboxuser@Server:~$ █
```

## EXERCICE 5.20:

J'ai testé l'authentification d'un utilisateur LDAP en me connectant via SSH et en local sur la VM serveur. L'authentification a fonctionné correctement et le dossier utilisateur a été créé automatiquement.

```
vboxuser@Server:~$ ssh rochdi@192.168.0.4
rochdi@192.168.0.4's password:
Creating directory '/home/rochdi'.
Linux Server 6.1.0-28-amd64 #1 SMP PREEMPT_DYNAMIC Debian 6.1.119-1 (2024-11-22)
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.
rochdi@Server:~$
```

# Intégration à divers services

## EXERCICE 5.21:

Pour intégrer LDAP dans Jenkins, j'ai accédé à l'interface d'administration de Jenkins et activé le plugin LDAP. J'ai configuré les paramètres LDAP comme suit :

- Serveur LDAP : ldap://192.168.0.4
- DN de base : dc=istycorp,dc=fr
- DN de liaison : cn=admin,dc=istycorp,dc=fr

J'ai ensuite configuré un filtre pour restreindre l'accès uniquement aux membres du groupe jenkins.

## EXERCICE 5.22:

J'ai configuré LDAP pour gérer les noms d'hôtes locaux du réseau en suivant les étapes suivantes :

1. Ajout du schéma : J'ai ajouté le schéma nécessaire pour stocker les entrées de type host.
2. Création des entrées : J'ai ajouté les entrées des machines avec leurs adresses IP correspondantes.
3. Configuration de NSS : J'ai modifié le fichier /etc/nsswitch.conf pour inclure LDAP dans la résolution des noms d'hôtes : hosts: files dns ldap

4. Vérification : J'ai utilisé la commande `getent hosts` pour vérifier que les noms d'hôtes étaient correctement résolus via LDAP.

```
vboxuser@Server: ~
GNU nano 7.2 /etc/ldap/ldap.conf *
#
# LDAP Defaults
#
# See ldap.conf(5) for details
# This file should be world readable but not world writable.

BASE    dc=istycorp,dc=fr
URI     ldap://192.168.0.4

#BASE   dc=example,dc=com
#URI    ldap://ldap.example.com ldap://ldap-provider.example.com:666

#SIZELIMIT    12
#TIMELIMIT    15
#DEREF        never

# TLS certificates (needed for GnuTLS)
TLS_CACERT    /etc/ssl/certs/ca-certificates.crt

^G Help      ^O Write Out ^W Where Is  ^K Cut       ^T Execute   ^C Location
^X Exit      ^R Read File ^\ Replace  ^U Paste     ^J Justify   ^_ Go To Line

GNU nano 7.2 /etc/nsswitch.conf *
# /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 systemd ldap
group:       files systemd ldap
shadow:     files systemd ldap
gshadow:     files systemd

hosts:       files myhostname mdns4_minimal [NOTFOUND=return] dns ldap
networks:    files

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

netgroup:    nis

^G Help      ^O Write Out ^W Where Is  ^K Cut       ^T Execute   ^C Location
^X Exit      ^R Read File ^\ Replace  ^U Paste     ^J Justify   ^_ Go To Line
```

```
vboxuser@Server: ~
vboxuser@Server:~$ nano hosts.ldif
vboxuser@Server:~$ cat hosts.ldif
dn: ou=hosts,dc=istycorp,dc=fr
objectClass: organizationalUnit
ou: hosts
vboxuser@Server:~$ ldapadd -x -D "cn=admin,dc=istycorp,dc=fr" -W -f hosts.ldif
Enter LDAP Password:
adding new entry "ou=hosts,dc=istycorp,dc=fr"

vboxuser@Server:~$ nano server.ldif
vboxuser@Server:~$ ldapadd -x -D "cn=admin,dc=istycorp,dc=fr" -W -f server.ldif
Enter LDAP Password:
ldap_bind: Invalid credentials (49)
vboxuser@Server:~$ cat server.ldif
dn: cn=server,ou=hosts,dc=istycorp,dc=fr
objectClass: ipHost
objectClass: device
cn: server
ipHostNumber: 192.168.0.4
vboxuser@Server:~$ ldapadd -x -D "cn=admin,dc=istycorp,dc=fr" -W -f server.ldif
Enter LDAP Password:
adding new entry "cn=server,ou=hosts,dc=istycorp,dc=fr"

vboxuser@Server:~$ █
```

```
vboxuser@Server:~$ getent hosts server
192.168.0.4      server
vboxuser@Server:~$ █
```

### EXERCICE 5.23:

Pour intégrer LDAP dans Redmine, j'ai accédé à l'interface d'administration de Redmine et ajouté un nouvel annuaire LDAP avec les paramètres suivants :

- Nom : LDAP ISTYCORP
- Hôte : 192.168.0.4
- Port : 389
- Compte : cn=admin,dc=istycorp,dc=fr
- Base DN : dc=istycorp,dc=fr

J'ai également activé la synchronisation automatique des utilisateurs.

# Filtrage par groupe dans PAM

J'ai activé le filtrage dans PAM pour n'autoriser l'authentification Unix qu'aux utilisateurs membres du groupe unix. Pour cela, j'ai suivi les étapes décrites dans la documentation Debian :

1. Ajout du filtre dans `/etc/pam.d/common-auth` :

```
auth required pam_group.so group=unix
```

2. Vérification : J'ai testé l'authentification avec un utilisateur membre du groupe unix, qui a réussi, tandis qu'un utilisateur non membre a été refusé.