# 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

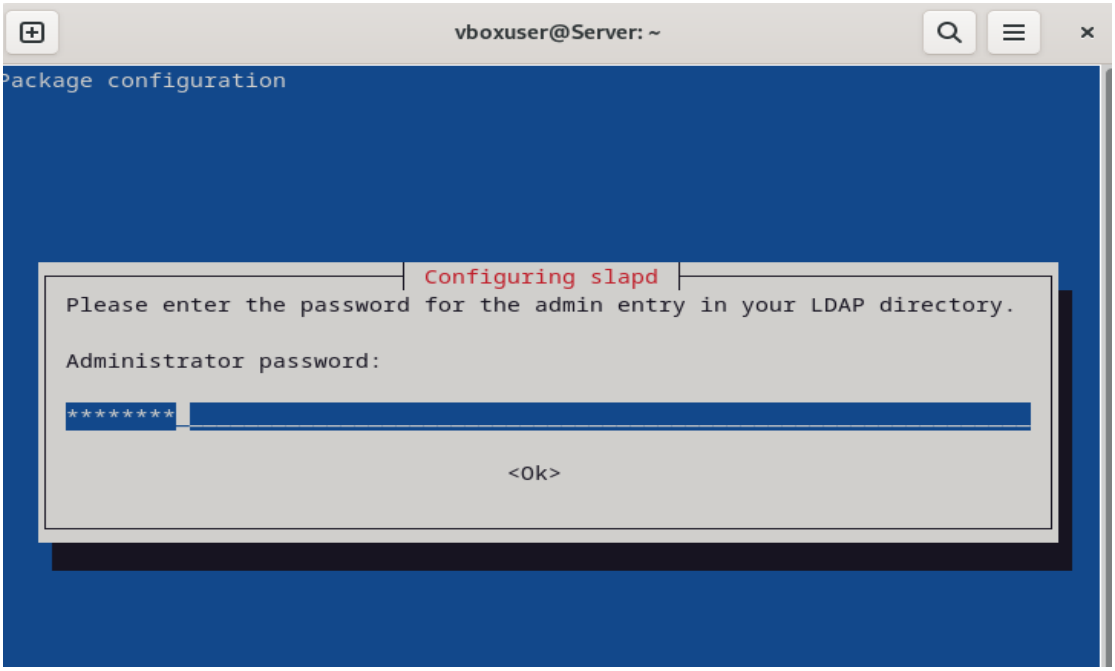
## EXERCICE 5.6 :

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]
```

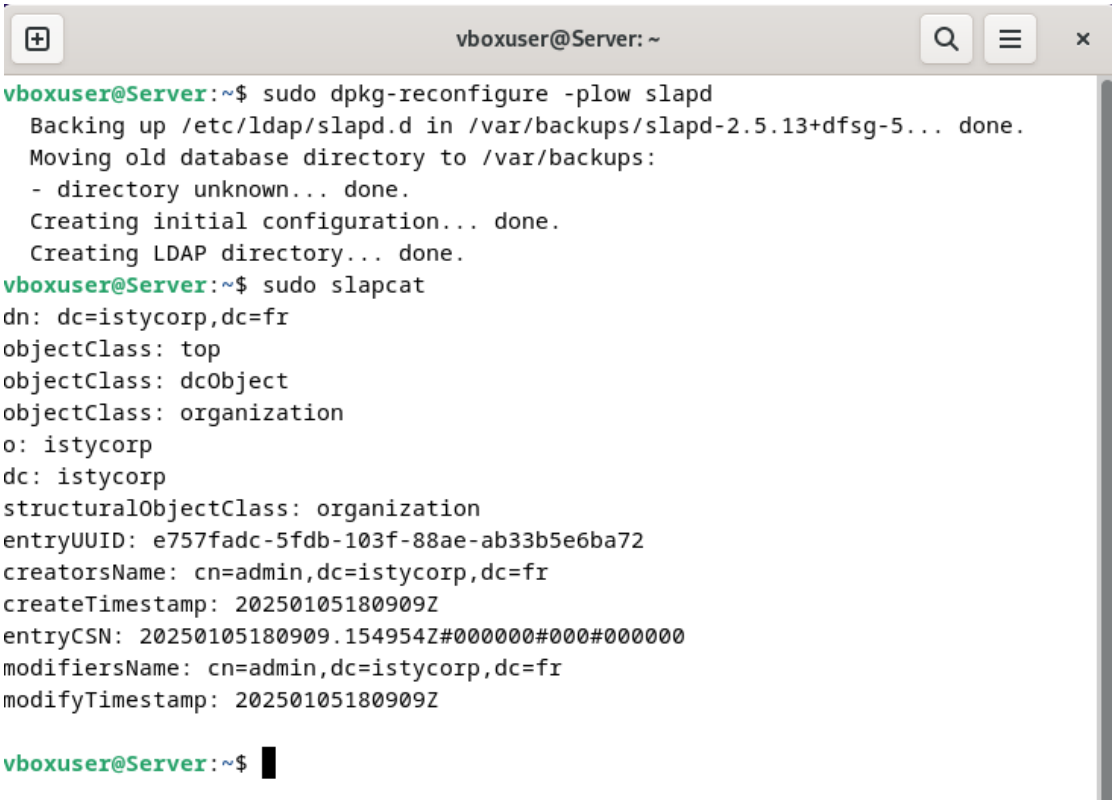


## EXERCICE 5.7 :

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.




## 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**


## 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

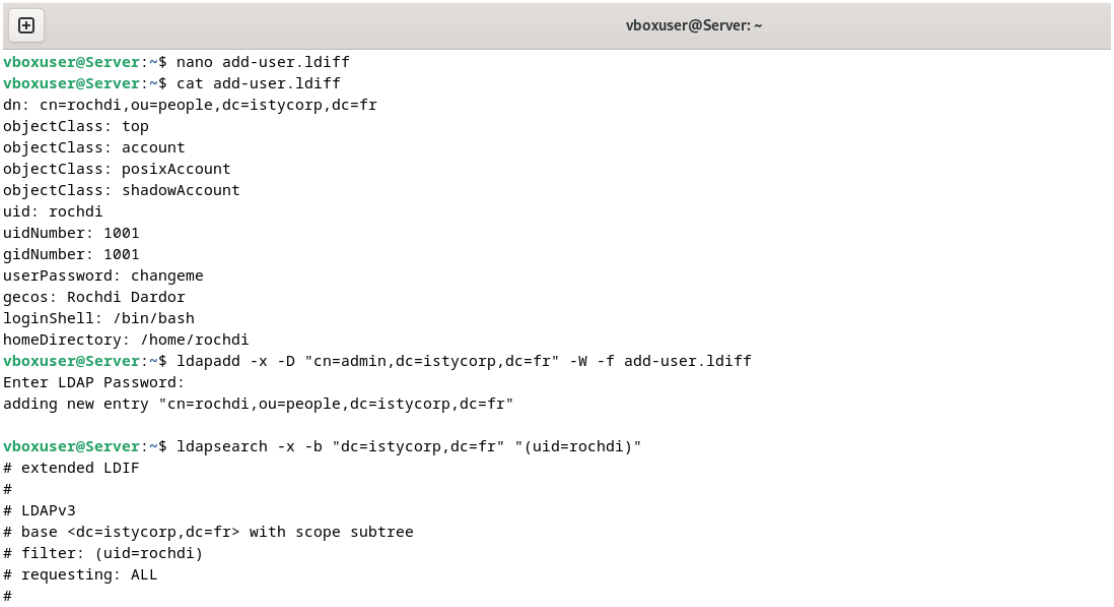
gecos: Rochdi Dardor

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**




## 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:: Y2hhbmdlbWU=
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'


# 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

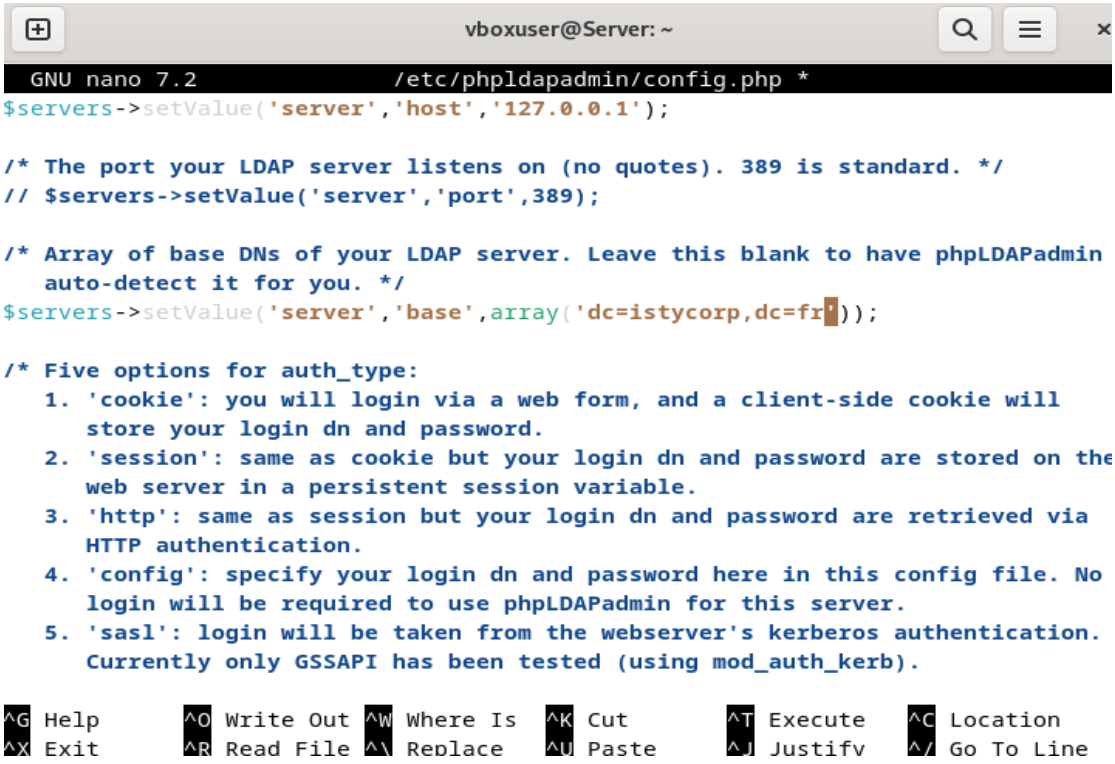
J'ai ensuite configuré l'accès en modifiant le fichier /etc/phpldapadmin/config.php afin de pointer vers mon domaine dc=istycorp,dc=fr.

```
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

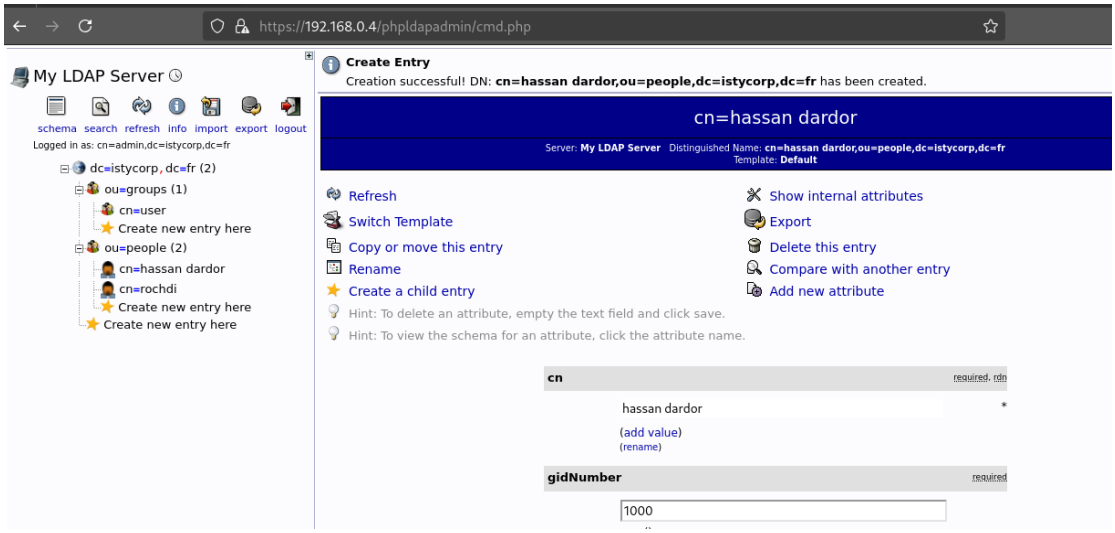


### EXERCICE 5.15 :

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 :

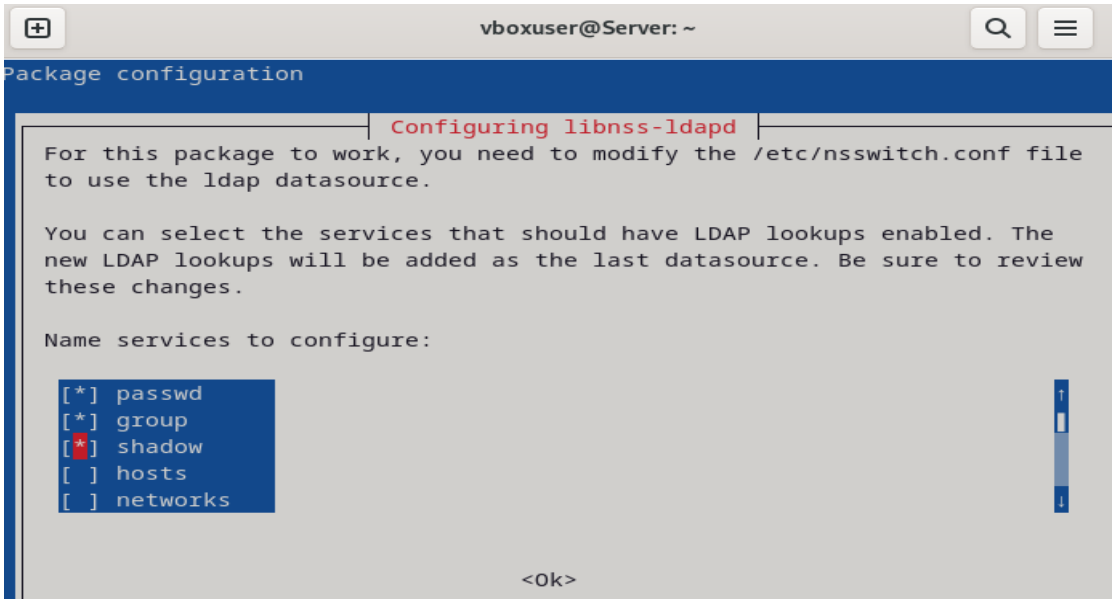
Pour intégrer LDAP dans l'authentification Unix, j'ai installé les paquets nécessaires avec la commande :

**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.

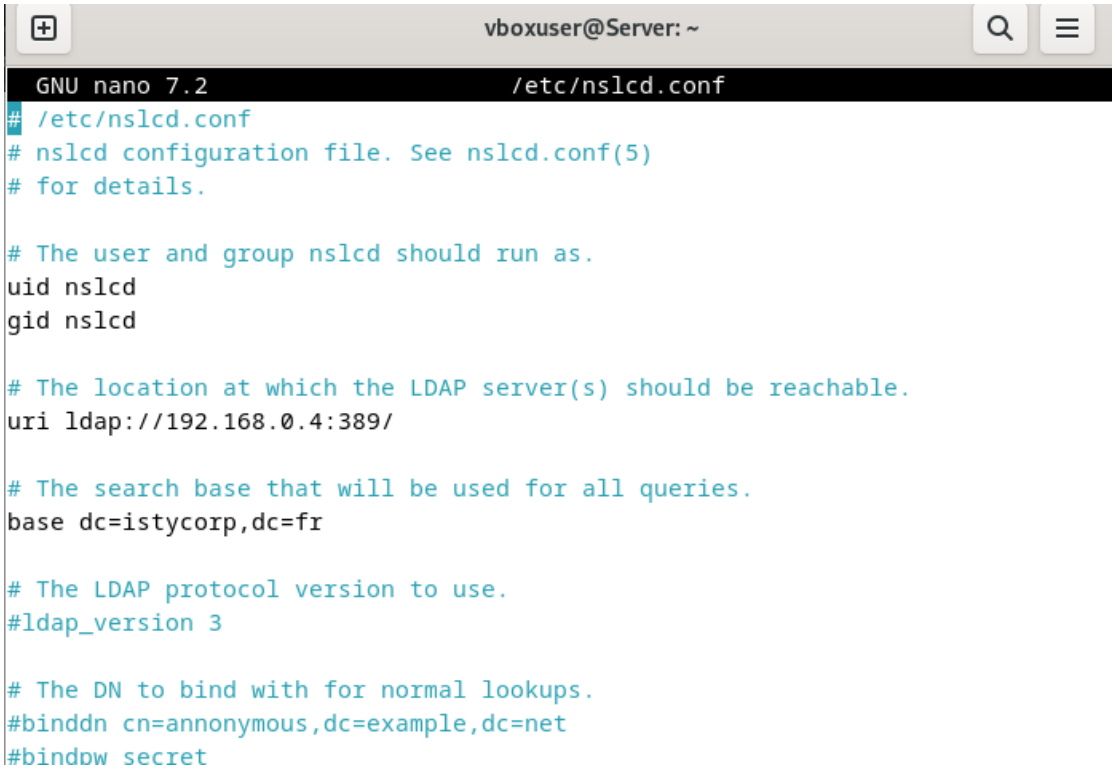



EXERCICE 5.17 :
Après installation, j'ai vérifié les fichiers de configuration suivants :

**/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.

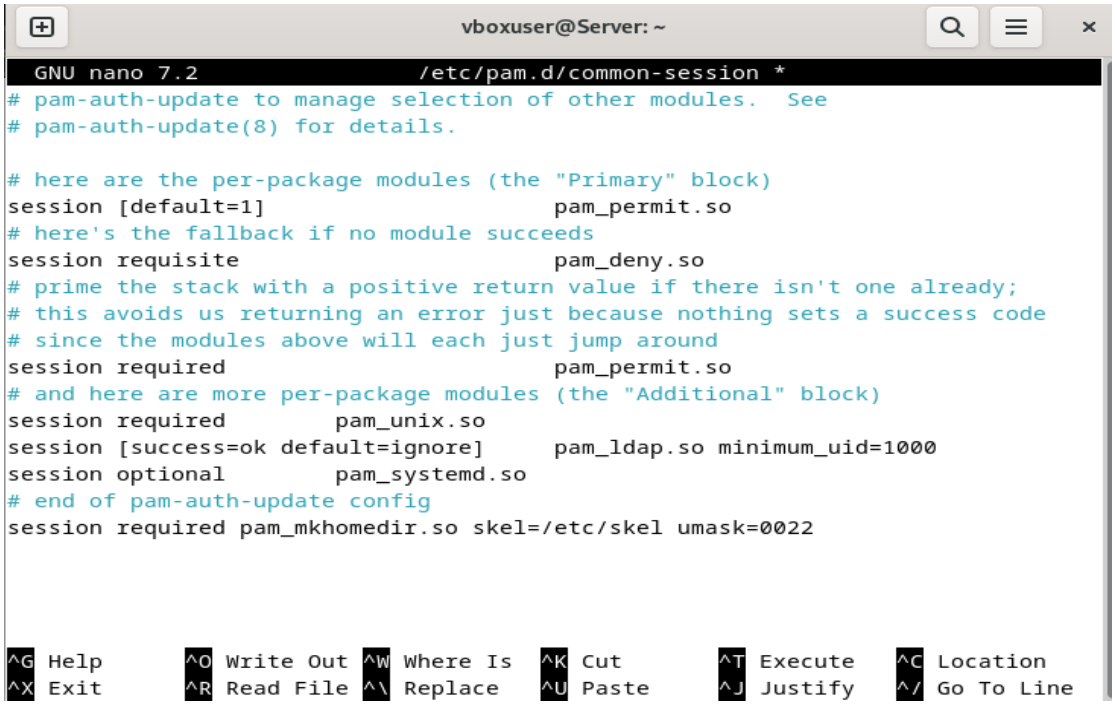
```
vboxuser@Server:~$ grep -i ldap /etc/pam.d/*
/etc/pam.d/common-account:account       [success=ok new_authtok_reqd=done ignore
=ignore user_unknown=ignore authinfo_unavail=ignore default=bad]        pam_ldap
.so minimum_uid=1000
/etc/pam.d/common-auth:# (e.g., /etc/shadow, LDAP, Kerberos, etc.).  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:~$
```




## 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



## EXERCICE 5.19:

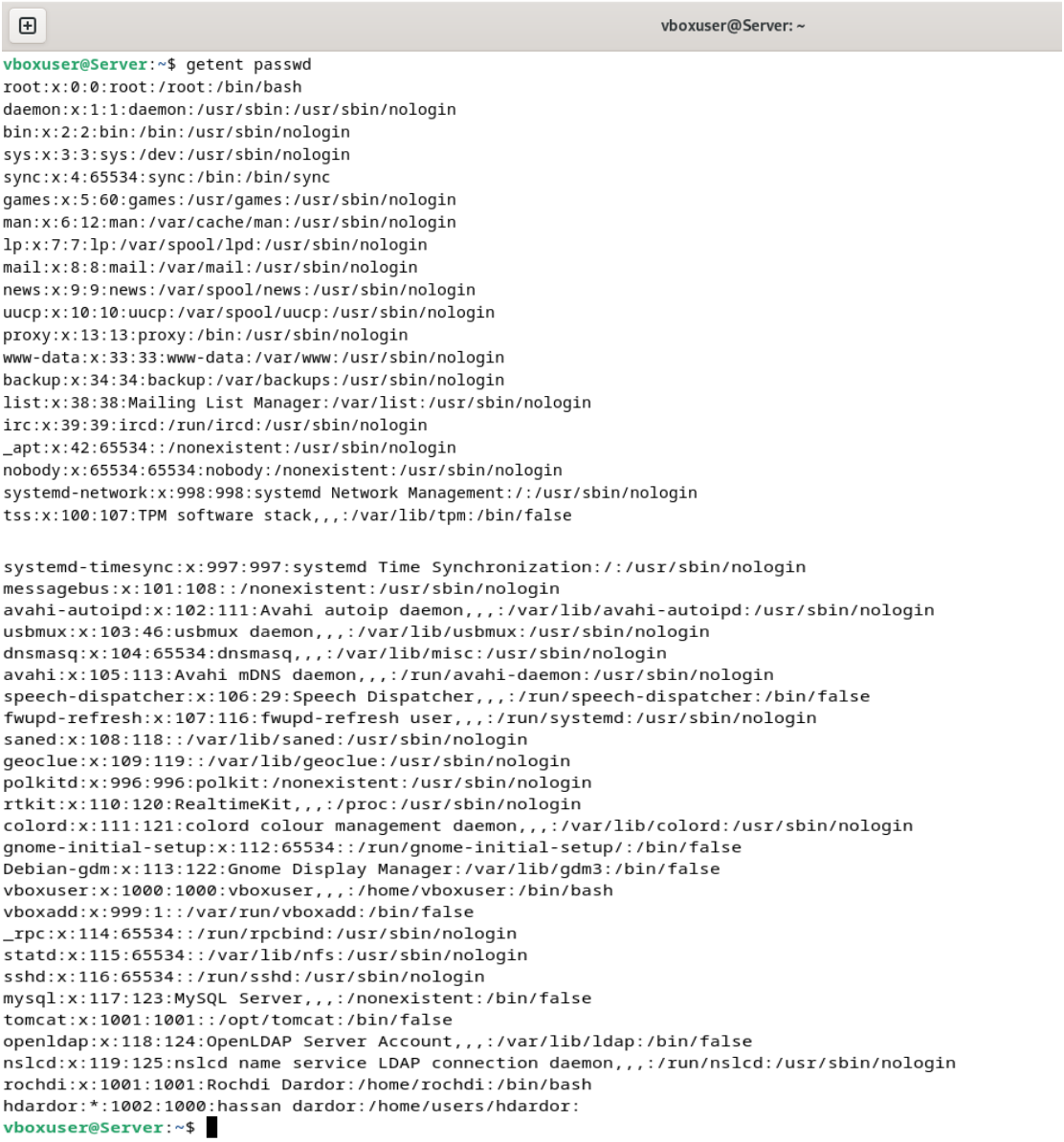
Pour vérifier que NSS communique correctement avec le serveur LDAP, j'ai exécuté la commande suivante :

**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**



### 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

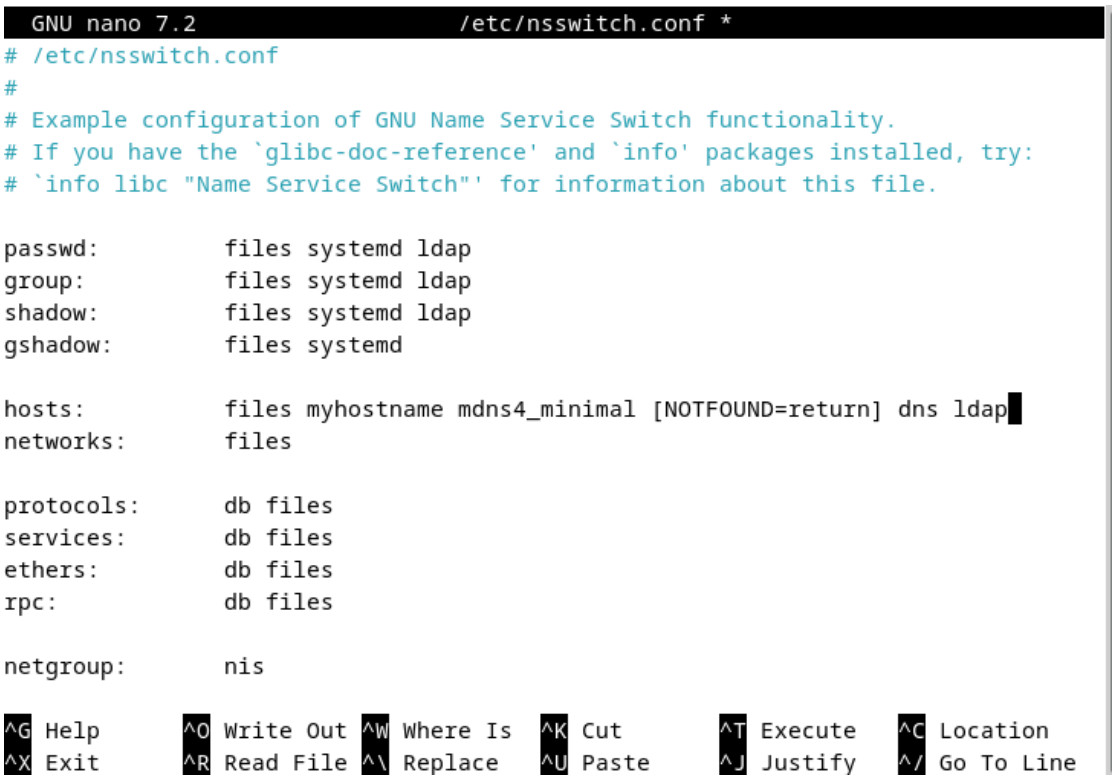
J'ai ensuite configuré un filtre pour restreindre l'accès uniquement aux membres du groupe jenkins.

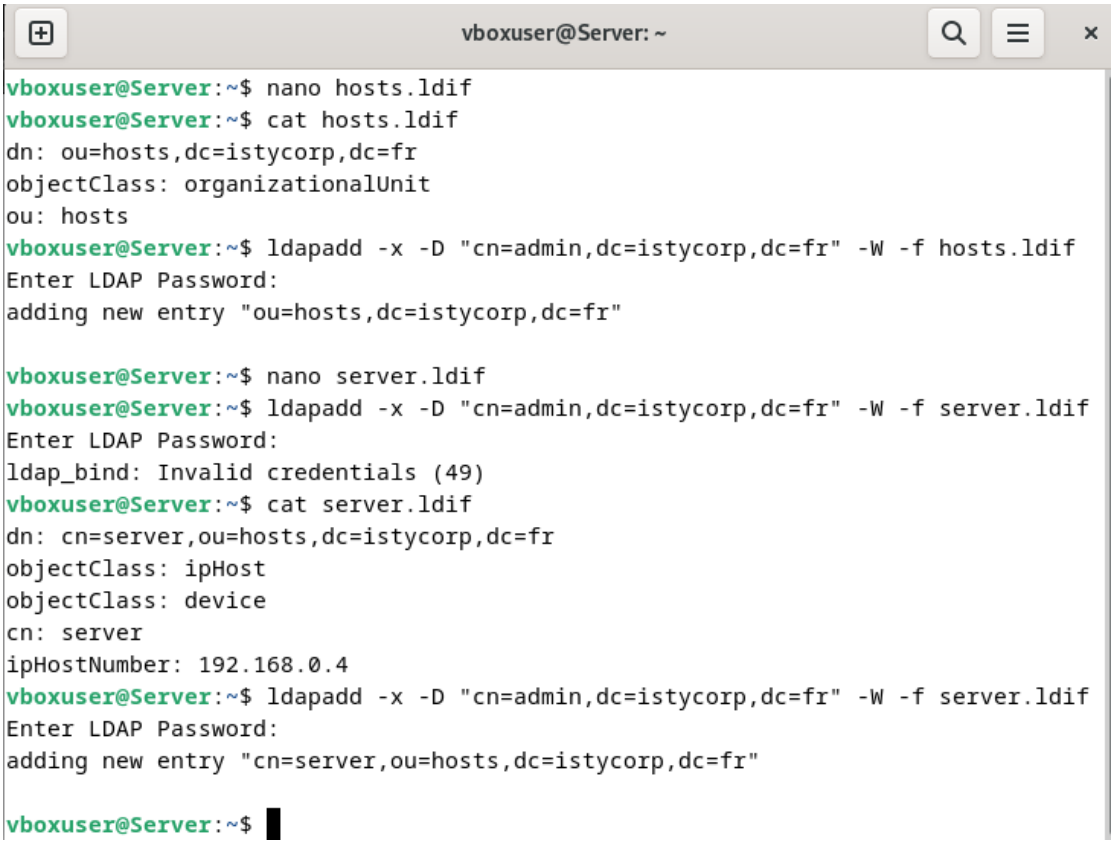
### EXERCICE 5.22:

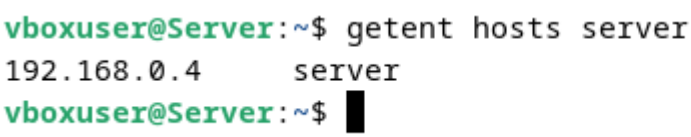
J'ai configuré LDAP pour gérer les noms d'hôtes locaux du réseau en suivant les étapes suivantes :

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.




## 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.