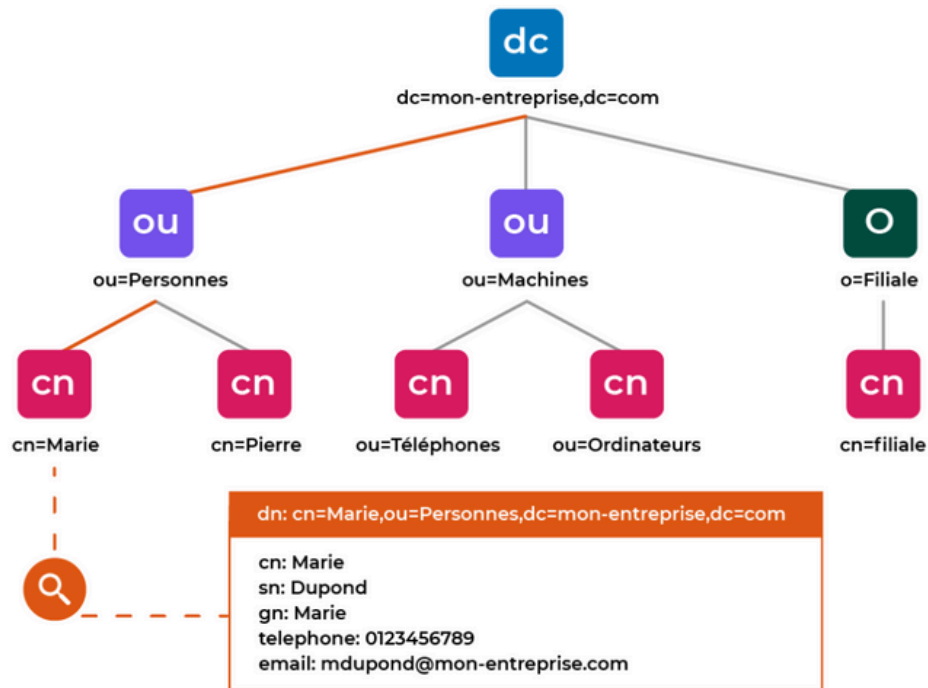


**LDAP Lightweight Directory Access Protocol** permet de gérer des annuaires.

L'annuaire LDAP permet de référencer différentes ressources utilisateurs, ordi/imprimantes , groupes)

Un **annuaire** est **ensemble d'entrées** qui **possèdent** :

- **Identifiant unique, GUID** ( Globl Unique IDentificateur)
  - **Nom unique, DN** (Distinguished Name), c'est le **chemin complet qui identifie l'objet**
- Organisées** de manière **hiérarchique** sous forme d'un arbre appelé **DIT**  
(Directory Information Tree)



Les **communications LDAP** s'effectuent sur le **port 389 (636chiffré)**

Attribut	Abréviation	Origine de l'abréviation
Nom commun	cn	<i>Common name</i>
Adresse e-mail	mail	E-mail
Unité organisationnelle	ou	<i>Organization unit</i>
Nom de famille	sn	<i>Surname</i>

partie d'un nom DNS

dc

domain component

ex : pour mon.entreprise.com , dc= mon-entreprise,dc=com

**cn=Marie Dupond,ou=Personnes,dc=mon-entreprise,dc=com"**

# Installation DLAP

## 1. Installation

```
valdeb@LDAP:~$ sudo apt install slapd ldap-utils
[sudo] Mot de passe de valdeb :
Lecture des listes de paquets... Fait
Construction de l'arbre des dépendances... Fait
Lecture des informations d'état... Fait
Les paquets supplémentaires suivants seront installés :
  libltdl7 libodbc2
Paquets suggérés :
  libsasl2-modules-gssapi-mit
  | libsasl2-modules-gssapi-heimdal odbc-postgresql tdsodbc
Les NOUVEAUX paquets suivants seront installés :
```

```
Configuration de slapd
Veuillez indiquer le mot de passe de l'administrateur de
l'annuaire LDAP.

Mot de passe de l'administrateur :

<Ok>
```

```
valdeb@LDAP:~$ sudo dpkg-reconfigure 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.
```

```
Configuration de slapd
Le nom de domaine DNS est utilisé pour établir le nom
distinctif de base (« base DN » ou « Distinguished
Name ») de l'annuaire LDAP. Par exemple, si vous
indiquez « toto.example.org » ici, le nom distinctif de
base sera « dc=toto, dc=example, dc=org ».

Nom de domaine :

valdomaine.com
<Ok>
```

```
Configuration de slapd
Veuillez indiquer la valeur qui sera utilisée comme nom
d'entité (« organization ») dans le nom distinctif de
base de l'annuaire LDAP.

Nom d'entité (« organization ») :

valdomaine
<Ok>
```

```
Configuration de slapd
Veuillez entrer à nouveau le mot de passe de
l'administrateur de l'annuaire LDAP afin de vérifier
qu'il a été saisi correctement.

Mot de passe de l'administrateur :

****
<Ok>
```

```
Configuration de slapd
Des fichiers présents dans /var/lib/ldap vont
probablement provoquer l'échec de la procédure de
configuration. Si vous choisissez cette option, les
scripts de configuration déplaceront les anciens
fichiers des bases de données avant de créer une
nouvelle base de données.

Faut-il déplacer l'ancienne base de données ?

<Oui> <Non>
```

Vérification de la bonne installation avec  
**slapcat**

```
valdeb@LDAP:~$ sudo slapcat
dn: dc=valdomaine,dc=com
objectClass: top
objectClass: dcObject
objectClass: organization
o: valdomaine
dc: valdomaine
structuralObjectClass: organization
entryUUID: 99b0f66e-774e-103f-89c8-65e8a06e5034
creatorsName: cn=admin,dc=valdomaine,dc=com
createTimestamp: 20250204141807Z
entryCSN: 20250204141807.743623Z#000000#000#000000
modifiersName: cn=admin,dc=valdomaine,dc=com
modifyTimestamp: 20250204141807Z
```

## 2.1 Créer et configurer le fichier groups sudo nano ldapgroups.ldif

```
GNU nano 7.2                                ldapgroups.ldif *
#création des groups
dn: ou=groups,dc=valdomaine,dc=com
objectClass: organizationalUnit
ou: groups

dn: cn=dev,ou=groups,dc=valdomaine,dc=com
objectClass: posixGroup
cn: dev
gidNumber: 223

dn: cn=admin,ou=groups,dc=valdomaine,dc=com
objectClass: posixGroup
cn: admin
gidNumber: 224

dn: cn=user,ou=groups,dc=valdomaine,dc=com
objectClass: posixGroup
cn:people
gidNumber: 225
```

## 2.2 # On insère le group dans le LDAP

ldapadd -x -D cn=admin,dc=valdomaine,dc=com -W -f ldapgroups.ldif

```
valdeb@LDAP:~$ ldapadd -x -D "cn=admin,dc=valdomaine,dc=com" -W
-f ldapgroups.ldif
Enter LDAP Password:
adding new entry "ou=groups,dc=valdomaine,dc=com"

adding new entry "cn=dev,ou=groups,dc=valdomaine,dc=com"

adding new entry "cn=admin,ou=groups,dc=valdomaine,dc=com"

adding new entry "cn=user,ou=groups,dc=valdomaine,dc=com "
```

### 3.1 Créer et configurer le fichier Utilisateurs `sudo nano ldapusers.ldif`

```
GNU nano 7.2      ldapusers.ldif
#config Utilisateurs
dn: ou=people,dc=valdomaine,dc=com
objectClass: organizationalUnit
ou: people

dn: uid=alice,ou=people,dc=valdomaine,dc=com
objectClass: inetOrgPerson
objectClass: posixAccount
objectClass: shadowAccount
cn: Alice
sn: Alice
uid: alice
uidNumber: 112
gidNumber: 223
homeDirectory: /home/alice
loginShell: /bin/bash
userPassword: {SSHA}mLy/hzapHJjqvn/QS0itnkSY92sYLZBA

dn: uid=bob,ou=people,dc=valdomaine,dc=com
objectClass: inetOrgPerson
objectClass: posixAccount
objectClass: shadowAccount
cn: Bob
sn: Bob
uid: bob
uidNumber: 113
gidNumber: 224
homeDirectory: /home/bob
```

### 3.2 # On insère l'utilisateur dans le LDAP `ldapadd -x -D cn=admin,dc=valdomaine,dc=com -W -f ldapusers.ldif`

### 3.3 Créer un **mdp haché** avec `sudo slappasswd`

```
valdeb@LDAP:~$ sudo slappasswd
[sudo] Mot de passe de valdeb :
New password:
Re-enter new password:
{SSHA}pUexFrENQm4yr0MKw1Jb+LLyL8azyxVS
```

### 3.4 Rentrer dans un fichier ldif ce **mdp haché**

```
GNU nano 7.2      mdp.ldif
#ce fichier sert à intégrer le chiffrement du mdp

dn: uid=alice,ou=people;dc=valdomaine,dc=com
changetype: modify
replace: userPassword
userPassword: {SSHA}mLy/hzapHJjqvn/QS0itnkSY92sYLZBA
```

## 4.1 Vérification que l'utilisateur est bien créé et que son MDP fonctionne

```
valdeb@LDAP:~$ ldapwhoami -x -D "uid=bob,ou=people,dc=valdomaine,dc=com" -W
Enter LDAP Password:
dn:uid=bob,ou=people,dc=valdomaine,dc=com
```

```
valdeb@LDAP:~$ sudo apt-get install libnss-ldap libpam-ldap
```

```
Configuration de nslcd
Veuillez indiquer l'URI (« Uniform Resource Identifier ») du serveur LDAP à utiliser. Il s'agit d'une adresse de la forme
« ldap://<nom de machine ou IP>:<port>/ ». Des adresses sous la forme « ldaps:// » et « ldapi:// » peuvent aussi être
utilisées. Le numéro de port est facultatif.

Lorsque le protocole utilisé est « ldap » ou « ldaps », il est recommandé d'utiliser une adresse IP plutôt qu'un nom d'hôte
afin de réduire les risques d'échec en cas d'indisponibilité du service de noms.

Des adresses multiples peuvent être indiquées, séparées par des espaces.

URI du serveur LDAP :
ldap://192.168.110.128:389/

<Ok> <Annuler>
```

```
Configuration de nslcd
Veuillez indiquer le nom distinctif (« DN ») de la base de recherche du serveur LDAP. Beaucoup de sites utilisent les
éléments composant leur nom de domaine à cette fin. Par exemple, le domaine « example.net » utiliserait
« dc=example,dc=net ».

Base de recherche du serveur LDAP :
dc=valdomaine,dc=com

<Ok> <Annuler>
```

```
Configuration de libnss-ldapd
Le fichier /etc/nsswitch.conf doit être modifié (afin d'utiliser la source de données « ldap ») pour rendre ce paquet
fonctionnel.

Vous pouvez aussi choisir les services qui doivent être activés ou désactivés pour les requêtes LDAP. Les nouvelles requêtes
LDAP seront ajoutées sous dernière source possible. Il est important de bien contrôler ces modifications.

Services de nom à configurer :
[*] passwd
[*] group
[*] shadow
[*] hosts
[ ] networks
[ ] ethers
[ ] protocols
[ ] services
[ ] rpc
[ ] netgroup
[ ] aliases

<Ok>
```

```
GNU nano 7.2 /etc/nsswitch.conf *
# /etc/nsswitch.conf
#
# Example configuration of GNU Name Service Switch
# If you have the 'glibc-doc-reference' and 'info' utilities, you can run:
# `info libc "Name Service Switch"' for information about this file.

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

hosts:           files dns
networks:        files

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

netgroup:        nis
```

```
valdeb@ldap2:~/LDAP$ ssh alice@192.168.110.130
alice@192.168.110.130's password:
Linux ldap2 6.1.0-30-amd64 #1 SMP PREEMPT_DYNAMIC Debian 6.1.124-1 (2025-01-12) 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: Sun Feb  9 22:27:32 2025 from ::1
Could not chdir to home directory /home/alice: No such file or directory
alice@ldap2:/$
```

## Difficultés rencontrées:

Difficulté à comprendre le fonctionnement Ldap add / Ldap modif. Lorsqu'on ajoute (user ou group) dans ldap avec ldapadd, on ne peut pas utiliser ldapadd pour modifier ce fichier ldif, ce que l'on a ajouté précédemment ne sera pas modifié.

Si on doit faire une modification sur un utilisateur ou group, il ne faut pas la faire dans le fichier utilisateur ou group, il faut la faire dans un nouveau fichier ldapmodify.ldif puis "push" la modif avec la commande ldapmodify.

On peut aussi supprimer avec ldapdelete.

```
GNU nano 7.2                                modify.ldif
# Ajout du groupe dev
dn: cn=dev,ou=groups,dc=valdomaine,dc=com
changetype: add
objectClass: posixGroup
cn: dev
gidNumber: 223
```

```
valdeb@LDAP:~$ ldapmodify -x -D "cn=admin,dc=valdomaine,dc=com" -W -f modify.ldif
```

J'ai modifié le fichier su, après cela mon mdp admin ne fonctionnait plus, j'en ne pouvais rien faire, j'ai dû retourner sur un snapshot avant installation de ldap.