



# LAN

## INTRODUCTION :

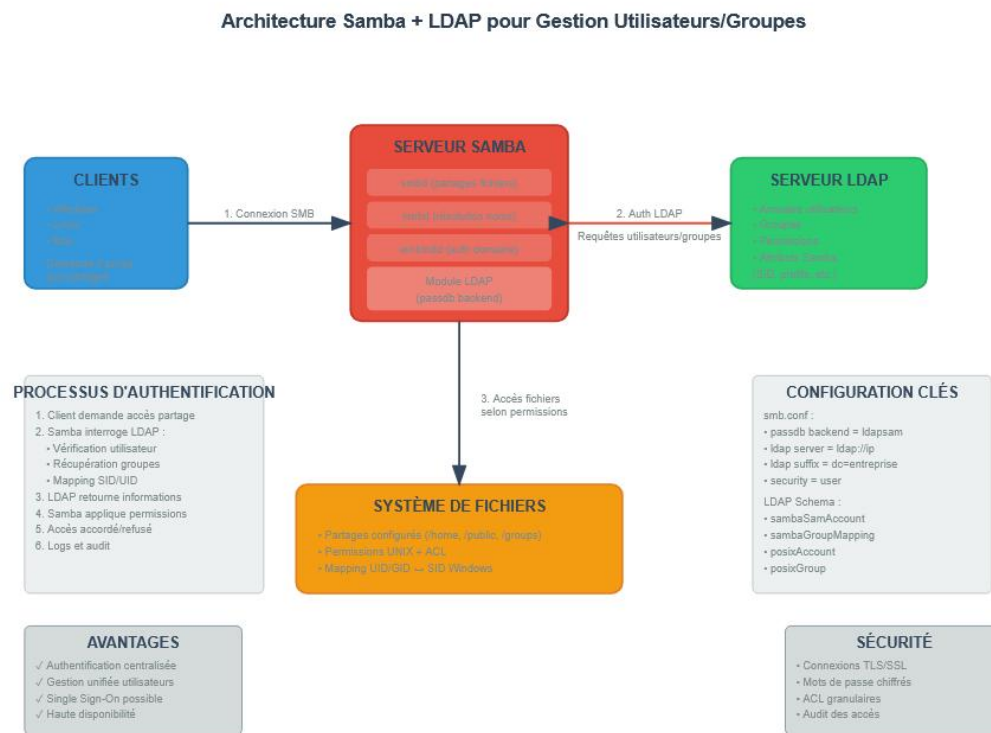
Le LAN (Local Area Network) représente le cœur du réseau interne de l'entreprise SMARTTECH.

Il regroupe les services essentiels tels que le serveur Nextcloud, la base de données, le serveur de fichiers et les outils collaboratifs.

Ces services sont accessibles uniquement aux utilisateurs authentifiés via LDAP/Kerberos, garantissant une sécurité et une gestion centralisée.

## 1. Serveur de fichiers (Samba/NFS) :

### Schema Expliquatif :



Le serveur de fichiers permet de partager des répertoires entre plusieurs machines du réseau local. Dans ce projet, nous utilisons **Samba** pour offrir un accès aux fichiers aux utilisateurs authentifiés via LDAP.

On installe Samba

```
phone1@Nextcloud:~$ sudo apt update && sudo apt install samba -y
```

Puis on crée un répertoire Partage

```
phone1@Nextcloud:~$ sudo mkdir -p /srv/samba/Partage
```

On définit les permissions du dossier partagé pour que seuls les membres du groupe aient accès en lecture/écriture, avec héritage du groupe.

```
phone1@Nextcloud:~$ sudo chmod 2770 /srv/samba/Partage
phone1@Nextcloud:~$ sudo nano /etc/samba/smb.conf
```

On édite le fichier de configuration de Samba pour déclarer le partage réseau.

```
GNU nano 7.2 /etc/samba/smb.conf
path = /var/lib/samba/printers
browseable = yes
read only = yes
guest ok = no
# Uncomment to allow remote administration of Windows print drivers.
# You may need to replace 'lpadmin' with the name of the group your
# admin users are members of.
# Please note that you also need to set appropriate Unix permissions
# to the drivers directory for these users to have write rights in it
; write list = root, @lpadmin

[projets]
path = /srv/samba/projets
browsable = yes
writable = yes
valid users = @partageprojet
create mask = 0660
directory mask = 0770
force group = partageprojet
```

On ajoute une **section [projets]** dans le fichier de configuration de Samba pour définir le partage réseau.

Le dossier **/srv/samba/projets** est accessible uniquement aux membres du groupe **partageprojet**, avec des droits adaptés à un usage collaboratif.

```
[global]
```

On configure les paramètres globaux de Samba pour l'intégrer à l'**annuaire LDAP** de l'entreprise.

Le serveur utilise **security = user** pour permettre une authentification basée sur les comptes utilisateurs LDAP.

Le backend **ldapsam** indique que la base des mots de passe est gérée via un annuaire LDAP distant (**ici ldap.tp.local**).

```
workgroup = TP
server string = Samba Server
netbios name = kdc
security = user
# realm = TP.LOCAL
passdb backend = ldapsam:ldap://ldap.tp.local
```

On précise les **suffixes LDAP** utilisés pour les **utilisateurs, groupes et machines** afin que Samba puisse interroger correctement l'annuaire.

L'administrateur Samba est défini avec son **DN** complet pour les opérations nécessitant des droits élevés.

La communication LDAP utilise **StartTLS** pour **sécuriser les échanges**, et la **synchronisation des mots de passe Unix** avec Samba est activée pour garder la cohérence des comptes.

```
ldap suffix = dc=tp,dc=local
ldap user suffix = ou=people
ldap group suffix = ou=groups
ldap machine suffix = ou=machines
ldap admin dn = uid=sambaadmin,ou=people,dc=tp,dc=local

ldap ssl = start_tls
ldap passwd sync = yes
log file = /var/log/samba/log.%m
max log size = 1000
unix password sync = yes
obey pam restrictions = yes
```

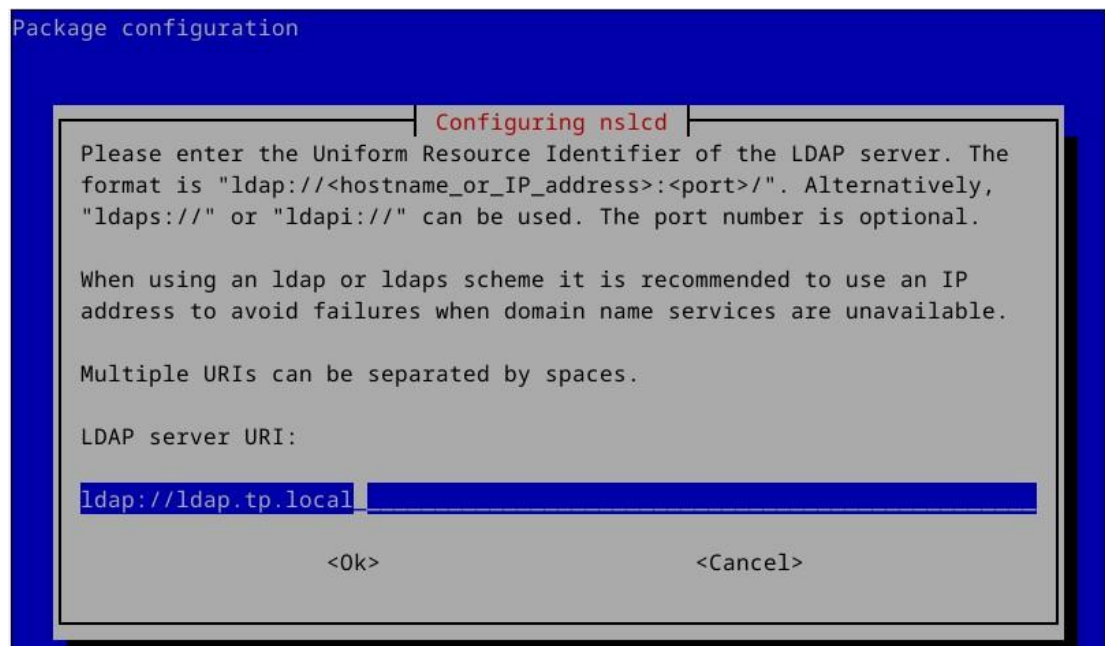
On installe les paquets nécessaires pour intégrer le serveur aux services LDAP et gérer l'authentification centralisée.

**sssd** facilite la gestion des identités et des accès, tandis que **libnss-ldap** et **libpam-ldap** permettent la résolution des utilisateurs et l'authentification via LDAP.

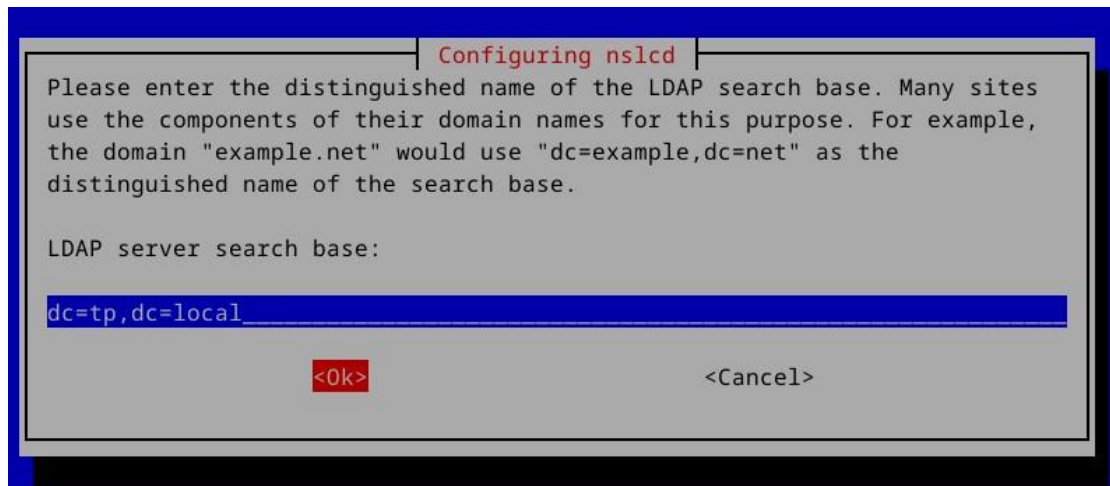
**ldap-utils** fournit des outils en ligne de commande pour interagir avec l'annuaire LDAP.

```
phone1@Nextcloud:~$ sudo apt install sssd libnss-ldap libpam-ldap ldap-utils
```

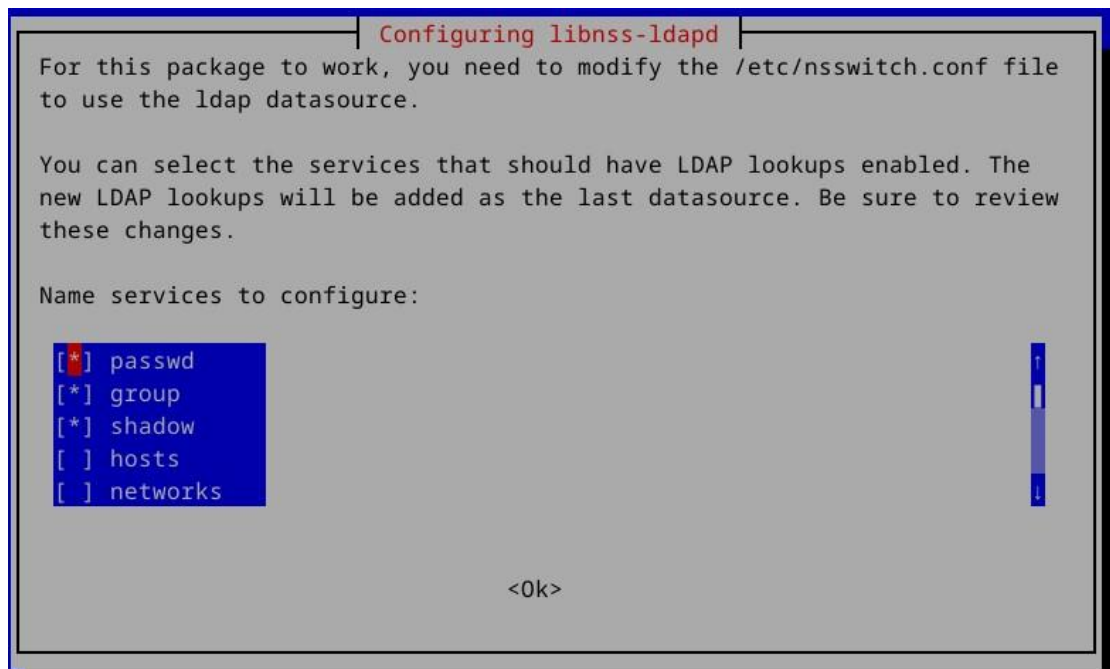
On entre le serveur URI LDAP



Puis le nom du serveur de base de recherche LDAP.



Puis on selectionne le services password.



On utilise la commande **ldapadd** pour ajouter le schéma Samba à l'annuaire LDAP, ce qui permet de gérer les objets et attributs spécifiques à Samba. L'ajout se fait en se connectant à l'annuaire LDAP avec un compte administrateur et en fournissant le fichier **samba.ldif**.

```
root@phone: /usr/share/doc/samba/examples/LDAP# ls
get_next_oid      samba-nds.schema  samba-schema.IBMSecureWay
ol-schema-migrate.pl  samba.schema      samba-schema-netscaped5.x.README
README            samba.schema.at.IBM-DS  samba.schema.oc.IBM-DS
samba.ldif         samba-schema-FDS.ldif
root@phone: /usr/share/doc/samba/examples/LDAP# ldapadd -x -D "cn=admin,cn=config" -W -H ldap://ldap.tp.local -f samba.ldif
Enter LDAP Password:
adding new entry "cn=samba,cn=schema,cn=config"
```

On utilise **slappasswd** pour générer un mot de passe chiffré au format SSHA, sécurisé pour LDAP.

```
phone1@kdc:~$ sudo slappasswd
New password:
Re-enter new password:
{SSHA}6AA5TYlW8t+901lUv9PUtYmWJicJXV3m
```

On crée un fichier LDIF pour ajouter un utilisateur **sambaadmin** dans LDAP, qui **servira d'administrateur Samba**. Cet utilisateur est défini avec plusieurs classes d'objet standard et un mot de passe chiffré en SSHA pour garantir la sécurité. Cela permet à Samba d'utiliser ce compte pour effectuer des opérations nécessitant des droits élevés dans l'annuaire LDAP.

```
GNU nano 7.2          create_samba_admin.ldif
dn: uid=sambaadmin,ou=people,dc=tp,dc=local
objectClass: inetOrgPerson
objectClass: organizationalPerson
objectClass: person
objectClass: top
cn: Samba Admin
sn: Admin
uid: sambaadmin
userPassword: SSHA}6AA5TYlW8t+901lUv9PUtYmWJicJXV3m
```

On ajoute l'utilisateur **sambaadmin** à l'annuaire LDAP en important le fichier LDIF avec la commande **ldapadd**.

```
phone1@kdc:~$ ldapadd -x -D "cn=admin,dc=tp,dc=local" -W -f create_samba_admin.ldif
Enter LDAP Password:
adding new entry "uid=sambaadmin,ou=people,dc=tp,dc=local"
```

On utilise **openssl s\_client** avec l'option **-starttls ldap** pour télécharger le certificat du serveur LDAP sur le port 389.

La commande extrait le **certificat SSL** présenté par le serveur pour vérification, ce qui permet de s'assurer que la communication LDAP est bien chiffrée.

```
root@phone:~# openssl s_client -connect ldap.tp.local:389 -starttls ldap </dev/null | sed -
ne '/-BEGIN CERTIFICATE-/,/-END CERTIFICATE-/p' > ldap_server_cert.pem
depth=0 C = SN, ST = Dakar, L = Dakar, O = SMARTTECH, OU = SN, CN = ldap.tp.local, emailAddre
ss = SMARTTECH@gmail.com
verify error:num=18:self-signed certificate
verify return:1
depth=0 C = SN, ST = Dakar, L = Dakar, O = SMARTTECH, OU = SN, CN = ldap.tp.local, emailAddre
ss = SMARTTECH@gmail.com
verify return:1
DONE
```

Le résultat montre le certificat et indique que la vérification TLS est terminée avec succès.

On copie le certificat LDAP extrait précédemment dans le répertoire système des certificats SSL.

```
root@phone:~# cp ldap_server_cert.pem /etc/ssl/certs/ldap_server_cert.pem
```

On utilise la commande **net getlocalsid** pour récupérer l'identifiant de sécurité (SID) local du domaine Samba.

```
root@phone:~# sudo net getlocalsid
SID for domain KDC is: S-1-5-21-191449322-3505439127-575286341
```

On crée le fichier **add\_samba\_domain.ldif** pour ajouter une unité organisationnelle **Domains** et un domaine Samba nommé **TP** dans l'annuaire LDAP.

L'entrée contient le **SID** Samba récupéré précédemment, nécessaire pour l'intégration des comptes au domaine Samba.

Ce fichier LDIF permet à Samba de **gérer les utilisateurs, groupes et machines à travers LDAP comme un contrôleur de domaine.**

```
GNU nano 7.2                                add_samba_domain.ldif *
dn: ou=Domains,dc=tp,dc=local
objectClass: top
objectClass: organizationalUnit
ou: Domains

# Crée l'entrée de domaine Samba
dn: sambaDomainName=KDC,ou=Domains,dc=tp,dc=local
objectClass: top
objectClass: sambaDomain
sambaDomainName: TP
sambaSID: S-1-5-21-191449322-3505439127-575286341
```

On ajoute la structure du domaine Samba dans l'annuaire LDAP en important le fichier LDIF via **ldapadd**.

La commande s'exécute avec le compte administrateur LDAP et pointe vers le serveur **ldap.tp.local**.

```
phone1@kdc:/etc/ldap/schema$ sudo ldapadd -x \
-D "cn=admin,dc=tp,dc=local" \
-W \
-H ldap://ldap.tp.local \
-ZZ \
-f add_samba_domain.ldif
Enter LDAP Password:
adding new entry "ou=Domains,dc=tp,dc=local"
```

L'unité organisationnelle **ou=Domains** est maintenant créée, ce qui prépare LDAP à accueillir les informations de domaine Samba.

On ajoute l'entrée du domaine Samba **TP** sous l'unité **ou=Domains** dans LDAP.

```
adding new entry "sambaDomainName=TP,ou=Domains,dc=tp,dc=local"
```

On crée le fichier **ajout\_membres\_projects** pour ajouter un groupe LDAP nommé **partageprojet** avec le GID 21000.



Ce groupe est de type **posixGroup** et contiendra les utilisateurs autorisés à accéder au partage Samba.

L'utilisateur **aziz** est ajouté comme membre du groupe via l'attribut **memberUid**.

```
GNU nano 7.2          ajout_membres_projets.ldif
dn: cn=partageprojet,ou=groups,dc=tp,dc=local
objectClass: top
objectClass: posixGroup
cn: projets
gidNumber: 21000
memberUid: aziz
```

On ajoute le groupe partageprojet dans l'annuaire LDAP à l'aide du fichier **ajout\_membres\_projects**.

```
phone1@kdc:~$ ldapadd -x -D "cn=admin,dc=tp,dc=local" -W -f ajout_membres_projects.ldif
Enter LDAP Password:
adding new entry "cn=partageprojet,ou=groups,dc=tp,dc=local"
```

On crée le fichier **perm\_samba** pour modifier les règles d'accès LDAP (ACL) afin de permettre à l'utilisateur **sambaadmin** de **gérer les mots de passe Samba**.

Les droits sont définis pour qu'il puisse écrire sur les attributs sensibles (**userPassword, sambaNTPassword, etc.**) et lire le reste de l'annuaire.

```
GNU nano 7.2          perm_samba
dn: olcDatabase={1}mdb,cn=config
changetype: modify
replace: olcAccess
olcAccess: to attrs=userPassword,sambaNTPassword,sambaLMPassword,sambaPwdLastSe>
  by dn="uid=sambaadmin,ou=people,dc=tp,dc=local" write
  by self write
  by anonymous auth
  by * none
olcAccess: to *
  by dn="uid=sambaadmin,ou=people,dc=tp,dc=local" write
  by * read
```

On applique les nouvelles permissions d'accès LDAP définies dans le fichier **samba\_perm.ldif** avec la commande **ldapmodify**.

```
phone1@kdc:~$ ldapmodify -x -D "cn=admin,cn=config" -W -f samba_perm.ldif
Enter LDAP Password:
modifying entry "olcDatabase={1}mdb,cn=config"
```

On redémarre les services **smbd nmbd**.

```
root@phone:~# sudo systemctl restart smbd nmbd
```

Puis on installe **smbclient** un outil en ligne de commande permettant d'accéder aux partages Samba depuis un client .

```
phone1@phone:~$ sudo apt install smbclient
```

On effectue une recherche LDAP pour vérifier que le groupe partageprojet contient bien les membres **aziz** et **sambaadmin**.

```
phone1@kdc:/etc/ldap/schema$ ldapsearch -x -LLL -b "ou=groups,dc=tp,dc=local" "(cn=partageprojet)" memberUid
dn: cn=partageprojet,ou=groups,dc=tp,dc=local
memberUid: aziz
memberUid: sambaadmin
```

Cette commande confirme que les utilisateurs ont été ajoutés correctement au groupe dans l'annuaire LDAP. Seule ces deux utilisateurs doivent pouvoir accéder fichier de Partage. Nous allons le tester.

On ajoute l'utilisateur **aziz** à la base de mots de passe Samba avec la commande **smbpasswd -a**.

```
root@phone:~# sudo smbpasswd -a aziz
New SMB password:
Retype new SMB password:
```

Puis l'utilisateur **sambaadmin** à la base de mots de passe Samba avec la commande **smbpasswd -a**.

```
phone1@phone:~$ sudo smbpasswd -a sambaadmin
New SMB password:
Retype new SMB password:
Added user sambaadmin.
```

On créer et edite un fichier message .

```
phone1@phone:~$ echo "Bienvenue dans le projet Samba LDAP !" > message.txt
```

On se connecte au partage Samba projets sur le serveur local avec smbclient en utilisant le compte **sambaadmin**.

On transfère ensuite un fichier message.txt vers le partage pour tester l'écriture et la connexion.

```
phone1@phone:~$ smbclient //localhost/projets -U sambaadmin
Password for [TP\sambaadmin]:
Try "help" to get a list of possible commands.
smb: \> put message.txt
putting file message.txt as \message.txt (0.5 kb/s) (average 0.5 kb/s)
smb: \> exit
```

On part dans une autre machine puis on y installe smbclient pour pouvoir faire les tests

```
[practice@parrot]~$ sudo apt install smbclient
```



On se connecte sur le **serveur Samba** avec **smbclient** en utilisant le compte **aziz** et on fait un **Get** pour télécharger le fichier.

```
[practice@parrot]~  
$ smbclient //192.168.10.10/projets -U aziz  
Password for [WORKGROUP\aziz]:  
Try "help" to get a list of possible commands.  
smb: \> get message.txt  
getting file \message.txt of size 38 as message.txt (0,2 KiloBytes/sec) (average  
0,2 KiloBytes/sec)  
smb: \> exit
```

On liste les fichiers présents et on y voit le fichier **message.txt** dont on avait transféré. Cela montre que l'utilisateur peut accéder aux fichiers transférés via le partage Samba depuis sa session.

```
[practice@parrot]~  
$ ls  
crackmes Documents freeradius-2.sh message.txt outils Public Videos  
Desktop Downloads freeradius.sh Music Pictures Templates  
[practice@parrot]~  
$ sudo cat message.txt  
Bienvenue dans le projet Samba LDAP !
```

On crée un nouveau utilisateur **maguette**.

```
phone1@phone:~$ sudo smbpasswd -a maguette  
New SMB password:  
Retype new SMB password:  
Added user maguette.
```

On tente de connecter l'utilisateur **maguette** au partage Samba projets, mais la connexion échoue avec l'erreur **tree connect failed**.

```
phone1@phone:~$ smbclient //localhost/projets -U maguette  
Password for [TP\maguette]:  
tree connect failed: NT_STATUS_ACCESS_DENIED
```

Cela signifie que l'utilisateur ne possède pas les droits nécessaires pour accéder au dossier partagé car elle n'est pas membre du groupe **partageprojet** dans LDAP.

## 2. Nexcloud :

Cette partie consiste à déployer un serveur Nextcloud dans le LAN afin de permettre aux utilisateurs internes de stocker, partager et accéder à leurs fichiers de manière sécurisée. Le service sera intégré à l'annuaire LDAP pour une gestion centralisée des comptes.

On installe **Apache et MariaDB** pour héberger l'application Nextcloud et stocker ses données. On installe aussi **PHP** avec toutes les extensions nécessaires pour faire fonctionner Nextcloud correctement (gestion des fichiers, image, base de données, JSON, etc.).

```
phone1@phone:/var/www$ sudo apt install apache2 mariadb-server libapache2-mod-php php php-gd php-json php-mysql php-curl php-mbstring php-intl php-imagick php-xml php-zip php-bcmath php-gmp unzip curl -y
```

On télécharge la dernière version de Nextcloud depuis le site officiel à l'aide de curl

```
phone1@phone:/var/www$ sudo curl -LO https://download.nextcloud.com/server/releases/latest.zip
```

On dézippe le dossier latest.zip

```
phone1@phone:/var/www$ sudo unzip latest.zip
```

On donne les droits à Apache (www-data) sur le dossier Nextcloud pour qu'il puisse lire et écrire les fichiers. Puis on applique des permissions sécurisées (lecture/exécution pour tous, écriture uniquement pour le propriétaire).

```
phone1@phone:/var/www$ sudo chown -R www-data:www-data nextcloud
phone1@phone:/var/www$ sudo chmod -R 755 nextcloud
phone1@phone:/var/www$ sudo nano /etc/apache2/sites-available/nextcloud.conf
```

On crée un fichier de configuration Apache pour déclarer le site Nextcloud et le rendre accessible via le navigateur.

```
GNU nano 7.2 /etc/apache2/sites-available/nextcloud.conf
<VirtualHost *:80>
    ServerAdmin admin@localhost
    DocumentRoot /var/www/nextcloud
    ServerName nextcloud.local

    <Directory /var/www/nextcloud/>
        Require all granted
        AllowOverride All
        Options FollowSymLinks MultiViews
    </Directory>

    ErrorLog ${APACHE_LOG_DIR}/nextcloud_error.log
    CustomLog ${APACHE_LOG_DIR}/nextcloud_access.log combined
</VirtualHost>
```

Ce fichier déclare le site **nextcloud.local**, accessible via Apache. Il pointe vers le répertoire **/var/www/nextcloud** et autorise l'accès à tous les utilisateurs. Les logs d'erreur et d'accès sont également définis pour le suivi du service.

On active le site Nextcloud dans Apache avec **a2ensite**, puis on recharge le service pour appliquer la nouvelle configuration.

```
phone1@phone:/var/www$ sudo a2ensite nextcloud.conf
Enabling site nextcloud.
To activate the new configuration, you need to run:
    systemctl reload apache2
```

On active les modules Apache nécessaires au bon fonctionnement de Nextcloud (rewrite, headers, etc.), puis on recharge le service pour appliquer les changements.

```
phone1@phone:/var/www$ sudo a2enmod rewrite headers env dir mime
Enabling module rewrite.
Enabling module headers.
Module env already enabled
Module dir already enabled
Module mime already enabled
To activate the new configuration, you need to run:
    systemctl restart apache2
phone1@phone:/var/www$ sudo systemctl reload apache2
```

On crée la base de données nextcloud et un utilisateur **nextclouduser** avec un mot de passe pour qu'il puisse y accéder. On lui accorde tous les droits sur cette base, puis on applique les changements avec **FLUSH PRIVILEGES**.

```
MariaDB [(none)]> CREATE DATABASE nextcloud;
Query OK, 1 row affected (0.008 sec)

MariaDB [(none)]> CREATE USER 'nextclouduser'@'localhost' IDENTIFIED BY 'motdepassefort';
Query OK, 0 rows affected (0.018 sec)

MariaDB [(none)]> GRANT ALL PRIVILEGES ON nextcloud.* TO 'nextclouduser'@'localhost';
Query OK, 0 rows affected (0.004 sec)

MariaDB [(none)]> FLUSH PRIVILEGES;
Query OK, 0 rows affected (0.003 sec)

MariaDB [(none)]> EXIT;
Bye
```

On installe l'extension **php-ldap** pour permettre à Nextcloud de se connecter et s'authentifier via un annuaire LDAP.


```
phone1@phone:/var/www$ sudo apt install php-ldap
Reading package lists... Done
```

On accède à l'interface web de Nextcloud pour créer le compte administrateur, définir le dossier de stockage (/var/www/nextcloud/data) .

### Create an admin account

New admin account name

New admin password

### Storage & database ▾

Data folder

Configure the database

Only MySQL/MariaDB is available. Install and activate additional PHP modules to choose other database types.

**For more details check out the documentation.** ↗

Database account


on configurer la base de données (MariaDB) précédemment créée.

Only MySQL/MariaDB is available. Install and activate additional PHP modules to choose other database types.

**For more details check out the documentation.** ↗

Database account


Database password

Database name

Database host

Please specify the port number along with the host name (e.g., localhost:5432).

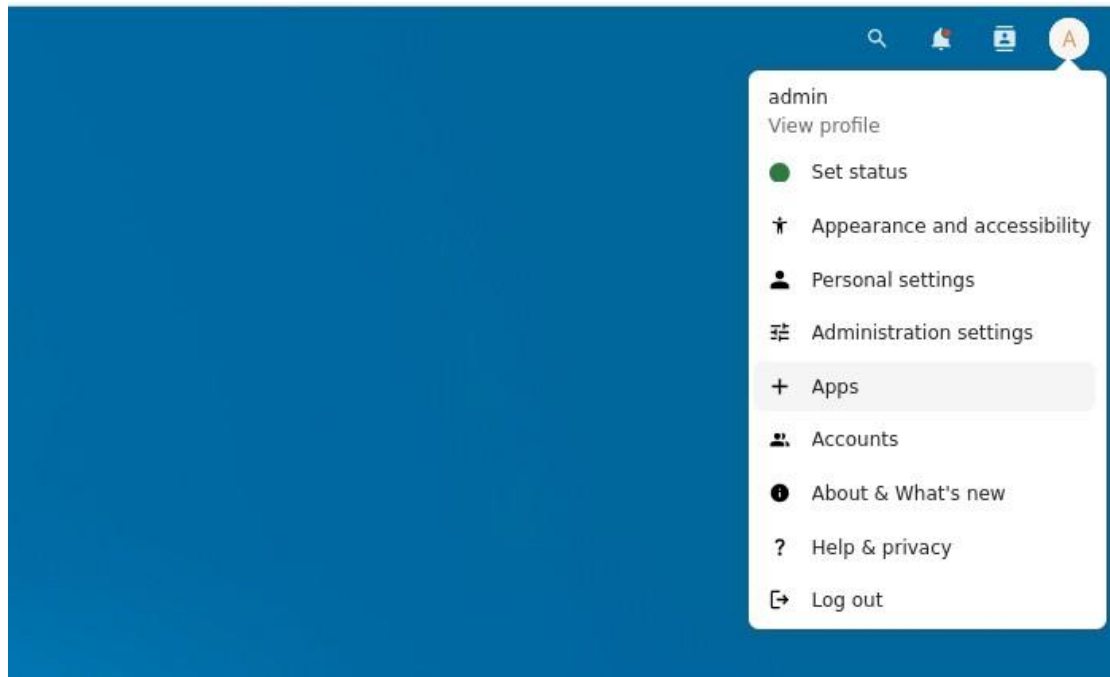


**Installing ...**

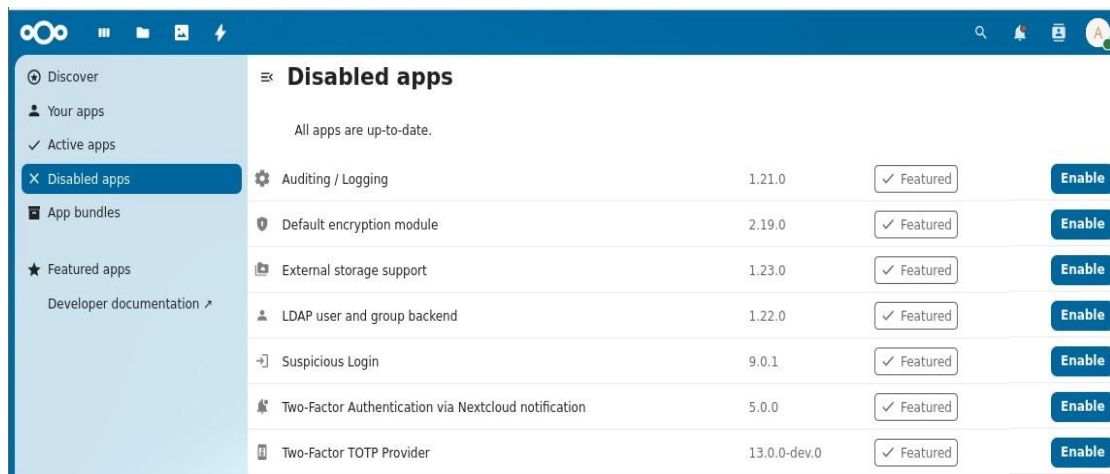
Need help? **See the documentation** ↗

**Nextcloud** – a safe home for all your data

On voit ici le profil de admin qui montre que le compte a été créé avec succès



Dans l'interface Nextcloud, plusieurs applications importantes sont disponibles mais désactivées. Parmi elles : LDAP backend, chiffrement, stockage externe, TOTP, et journalisation. Elles peuvent être activées pour renforcer la sécurité, l'intégration avec LDAP et les fonctionnalités avancées.



On configure la connexion **LDAP** en indiquant l'adresse du **serveur (192.168.200.50)**, le **compte administrateur (cn=admin,dc=tp,dc=local)** et le **port (389)**. Le test de connexion est réussi, ce qui confirme que Nextcloud peut interagir avec l'annuaire LDAP.



1. Server: +

192.168.200.50

389

Detect Port

cn=admin,dc=tp,dc=local

.....

Save Credentials

dc=tp,dc=local

Detect Base DN

Test Base DN

☐ Manually enter LDAP filters (recommended for large directories)

Configuration OK

Continue

Help

Nextcloud filtre les utilisateurs LDAP en se basant sur l'objet *organizationalPerson*. Le filtre (objectclass=organizationalPerson) permet d'identifier les comptes utilisateurs, et la vérification confirme que 3 utilisateurs sont détectés dans l'annuaire.

Personal

Personal info

Security

Notifications

Mobile & desktop

Sharing

Appearance and accessibility

Availability

Flow

Privacy

Administration

Overview

Support

Basic settings

Sharing

Security

LDAP/AD integration

Theming

Artificial Intelligence

AppAPI

Administration privileges

Activity

Notifications

Flow

LDAP/AD integration

Server

Users

Login Attributes

Groups

Advance

Listing and searching for users is constrained by these criteria:

Only these object classes:

organizationalPerson

The most common object classes for users are organizationalPerson, person, user, and inetOrgPerson. If you are not sure which object class to select, please consult your directory admin.

Only from these groups:

Select groups

Edit LDAP Query

LDAP Filter: ((objectclass=organizationalPerson))

Verify settings and count users

3 users found

Nextcloud est configuré pour authentifier les utilisateurs LDAP en utilisant l'attribut *uid* (nom d'utilisateur). Le filtre (&(objectclass=organizationalPerson)(uid=%uid)) permet de cibler uniquement les comptes valides correspondant à l'utilisateur qui tente de se connecter.

## LDAP/AD integration

Server Users **Login Attributes** Groups

When logging in, Nextcloud will find the user based on the following attributes:

LDAP/AD Username: ☒

LDAP/AD Email Address: ☐

Other Attributes:

[Edit LDAP Query](#)

LDAP Filter: (&(|(objectclass=organizationalPerson))(uid=%uid))

**Verify settings**

Nextcloud récupère les groupes LDAP dont l'objet est organizationalUnit. Le filtre (&(objectclass=organizationalUnit)) permet d'importer uniquement les unités organisationnelles, et 3 groupes sont bien détectés dans l'annuaire.

Personal Administration LDAP/AD integration

LDAP/AD integration

Server Users Login Attributes **Groups** Advanced Expert

Groups meeting these criteria are available in Nextcloud:

Only these object classes:

Only from these groups:

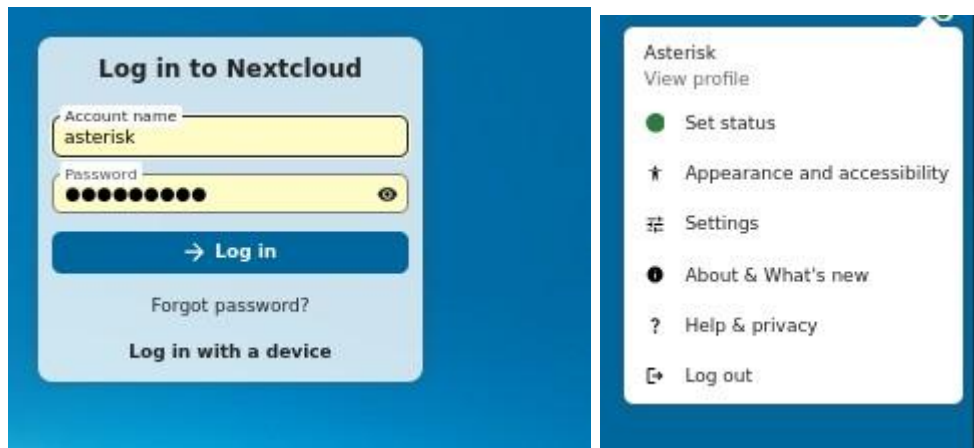
[Edit LDAP Query](#)

LDAP Filter: (&(|(objectclass=organizationalUnit))

**Verify settings and count the groups** 3 groups found

Configuration OK **Back** Help

Une fois la configuration LDAP terminée, l'utilisateur peut se connecter à Nextcloud avec ses identifiants LDAP. Cela valide l'intégration réussie entre Nextcloud et l'annuaire LDAP.



Voici le fichier **Log** ou un **enregistrement** qui garde une **trace des événements, actions, erreurs ou activités** qui se passe dans Nextcloud.

Log reader				Log reader settings	
Level	Application	Message	Time		
Warning	no app in context	Login failed: admin (Remote IP: 127.0.0.1)	Jun 22, 2025, 1:20:36 PM	...	
Warning	PHP	Uninitialized string offset 0 at /var/www/nextcloud/apps/user_ldap/lib/Wizard.php#777	Jun 22, 2025, 1:03:32 PM	...	
Warning	PHP	Uninitialized string offset 0 at /var/www/nextcloud/apps/user_ldap/lib/Wizard.php#777	Jun 22, 2025, 1:03:32 PM	...	
Warning	appstoreFetcher	Response from appstore is invalid, apps could not be retrieved. Try again later.	Jun 22, 2025, 12:59:12 PM	...	
Warning	appstoreFetcher	Response from appstore is invalid, apps could not be retrieved. Try again later.	Jun 22, 2025, 12:59:12 PM	...	
Warning	appstoreFetcher	Response from appstore is invalid, apps could not be retrieved. Try again later.	Jun 22, 2025, 12:59:12 PM	...	
Warning	appstoreFetcher	Response from appstore is invalid, apps could not be retrieved. Try again later.	Jun 22, 2025, 12:59:12 PM	...	
Warning	appstoreFetcher	Response from appstore is invalid, apps could not be retrieved. Try again later.	Jun 22, 2025, 12:59:11 PM	...	
Warning	appstoreFetcher	Response from appstore is invalid, apps could not be retrieved. Try again later.	Jun 22, 2025, 12:59:11 PM	...	
Warning	appstoreFetcher	Response from appstore is invalid, apps could not be retrieved. Try again later.	Jun 22, 2025, 12:59:11 PM	...	
Warning	appstoreFetcher	Response from appstore is invalid, apps could not be retrieved. Try again later.	Jun 22, 2025, 12:59:11 PM	...	
Warning	appstoreFetcher	Response from appstore is invalid, apps could not be retrieved. Try again later.	Jun 22, 2025, 12:59:07 PM	...	
Error	no app in context	ConnectException cURL error 28: Operation timed out after 60000 milliseconds with 7973578 out of 8307173 bytes recei...	Jun 22, 2025, 12:59:07 PM	...	
Warning	appstoreFetcher	Response from appstore is invalid, apps could not be retrieved. Try again later.	Jun 22, 2025, 12:59:07 PM	...	
Error	no app in context	ConnectException cURL error 28: Operation timed out after 60000 milliseconds with 7973578 out of 8307173 bytes recei...	Jun 22, 2025, 12:59:07 PM	...	
Warning	appstoreFetcher	Response from appstore is invalid, apps could not be retrieved. Try again later.	Jun 22, 2025, 12:52:14 PM	...	
Warning	appstoreFetcher	Response from appstore is invalid, apps could not be retrieved. Try again later.	Jun 22, 2025, 12:52:14 PM	...	
Warning	appstoreFetcher	Response from appstore is invalid, apps could not be retrieved. Try again later.	Jun 22, 2025, 12:52:14 PM	...	
Warning	appstoreFetcher	Response from appstore is invalid, apps could not be retrieved. Try again later.	Jun 22, 2025, 12:52:14 PM	...	
Warning	appstoreFetcher	Response from appstore is invalid, apps could not be retrieved. Try again later.	Jun 22, 2025, 12:52:14 PM	...	
Warning	appstoreFetcher	Response from appstore is invalid, apps could not be retrieved. Try again later.	Jun 22, 2025, 12:52:14 PM	...	

Voici tout les comptes qu'on a créer dans le nextcloud , on visualise les utilisateurs LDAP synchronisés, avec leurs noms (ex. : Maguette, Aziz) .

Display name	Account name	Password	Email	Groups	Group admin for	Quota
M Maguette	06161bb8-e3c4-103f...					Unlim / ...
FA FreeRADIUS Admin	0b150cec-e3b4-103f...					Unlim / ...
A Aziz	60df4cd4-e3da-103f...					Unlim / ...
A Asterisk	73120566-e337-103f...					Unlim / ...
A admin	admin			admin		Unlim / ...

Cela confirme que la récupération des comptes et groupes depuis LDAP fonctionne correctement.

**CONCLUSION :**

La configuration du LAN a permis d'assurer un environnement interne sécurisé et fonctionnel pour les employés.

Les services sont isolés du réseau public et accessibles uniquement via authentification centralisée, ce qui réduit fortement les risques de compromission.

Le déploiement des outils internes facilite la collaboration tout en respectant les principes de confidentialité et de contrôle d'accès.