OpenLDAP & Nextcloud

1. Présentation du scénario

Cette documentation présente la mise en place d'un annuaire LDAP (OpenLDAP) sur Ubuntu, puis son intégration avec un serveur Nextcloud installé via Snap. L'objectif est de centraliser la gestion des comptes utilisateurs : un utilisateur créé dans LDAP devient automatiquement exploitable comme identité de connexion pour Nextcloud, sans création de compte local supplémentaire.

2. Installation et configuration d'OpenLDAP

2.1 Installation des paquets

Installation du serveur LDAP (slapd) et des outils clients en ligne de commande :

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

2.2 Reconfiguration du domaine LDAP

L'assistant de reconfiguration permet de définir le domaine et l'organisation qui structureront la base LDAP :

```
sudo dpkg-reconfigure slapd
```

Valeurs renseignées lors de l'assistant :

- Domaine DNS : lucasubuntu.local
- Organisation : lucasubuntu
- Base LDAP : dc=lucasubuntu,dc=local
- Compte admin LDAP : cn=admin,dc=lucasubuntu,dc=local

2.3 Vérification du fonctionnement

Une requête ldapsearch sur la base DN permet de confirmer que le service répond correctement :

```
ldapsearch -x \
  -H ldap://localhost \
  -D "cn=admin,dc=lucasubuntu,dc=local" \
  -W \
  -b "dc=lucasubuntu,dc=local"
```

Une réponse contenant result: 0 Success confirme que l'annuaire LDAP répond correctement aux requêtes.

2.4 Création de l'arborescence (people / groups)

Avant de créer des comptes, deux unités organisationnelles sont ajoutées à la base : people pour les utilisateurs, groups pour les groupes.

```
nano /root/base.ldif
```

```
dn: ou=people,dc=lucasubuntu,dc=local
objectClass: organizationalUnit
ou: people

dn: ou=groups,dc=lucasubuntu,dc=local
objectClass: organizationalUnit
ou: groups
```

```
ldapadd -x \
  -D "cn=admin,dc=lucasubuntu,dc=local" \
  -W \
  -f /root/base.ldif
```

2.5 Réinitialisation du mot de passe administrateur

Le mot de passe du compte admin LDAP est régénéré via un hash SSHA, puis appliqué directement dans la configuration cn=config :

```
HASH=$(slappasswd -s 'root')

cat > /root/reset-ldap-password.ldif <<EOF
dn: olcDatabase={1}mdb,cn=config
changetype: modify
replace: olcRootPW
olcRootPW: $HASH
EOF

ldapmodify -Y EXTERNAL -H ldapi:/// \
  -f /root/reset-ldap-password.ldif
```

Test d'authentification du compte admin avec le nouveau mot de passe :

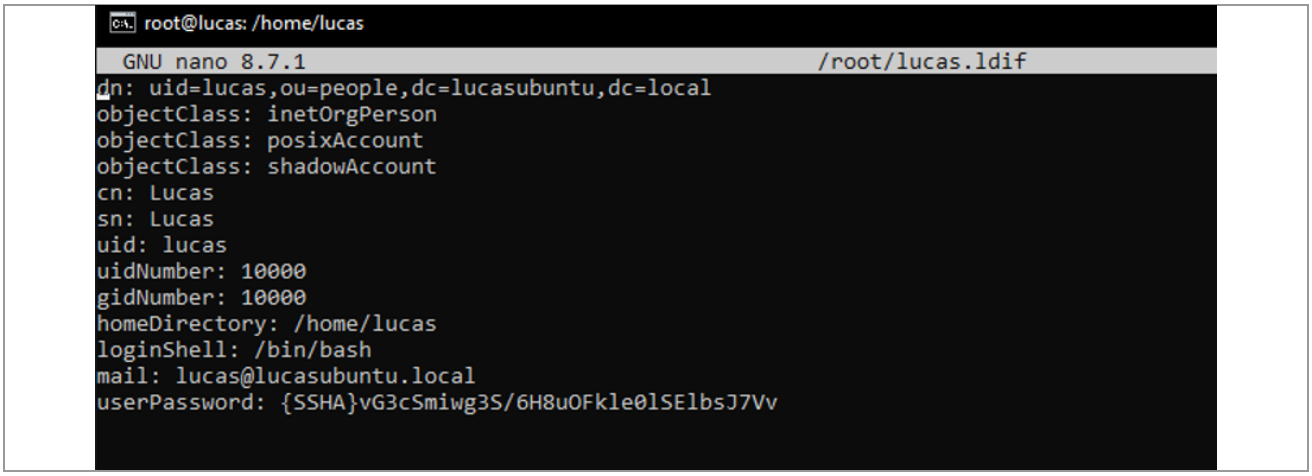
```
ldapwhoami -x \
  -H ldap://127.0.0.1 \
  -D "cn=admin,dc=lucasubuntu,dc=local" \
  -w 'root'

# Résultat attendu :
dn:cn=admin,dc=lucasubuntu,dc=local
```

3. Création de l'utilisateur LDAP lucas

Un hash de mot de passe est généré avec slappasswd, puis utilisé dans un fichier LDIF décrivant l'entrée de l'utilisateur lucas (classes inetOrgPerson, posixAccount, shadowAccount) :

```
slappasswd
nano /root/lucas.ldif
```



Ajout de l'entrée dans l'annuaire :

```
ldapadd -x \
  -H ldap://127.0.0.1 \
  -D "cn=admin,dc=lucasubuntu,dc=local" \
  -w 'root' \
  -f /root/lucas.ldif
```

3.1 Vérification et test de connexion

Recherche de l'entrée lucas dans l'unité people :

```
ldapsearch -x -LLL \
  -H ldap://127.0.0.1 \
  -D "cn=admin,dc=lucasubuntu,dc=local" \
  -w 'root' \
  -b "ou=people,dc=lucasubuntu,dc=local" \
  "(uid=lucas)"
```

Changement du mot de passe LDAP de lucas, puis test d'authentification avec son propre DN :

```
ldappasswd -x \
  -D "cn=admin,dc=lucasubuntu,dc=local" \
  -w 'root' \
  -S "uid=lucas,ou=people,dc=lucasubuntu,dc=local"

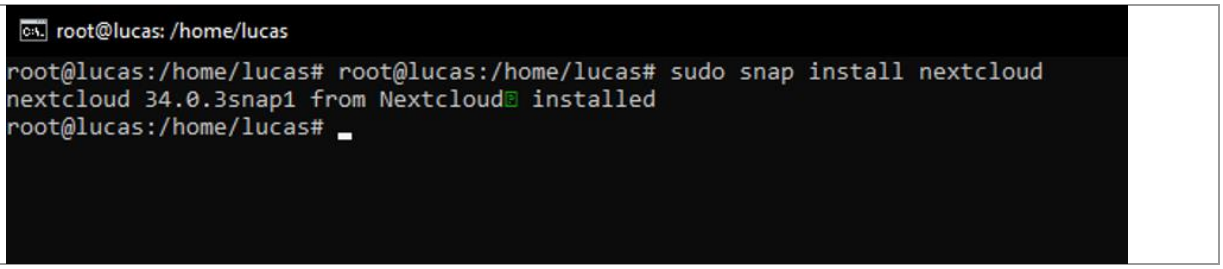
ldapwhoami -x \
  -H ldap://127.0.0.1 \
  -D "uid=lucas,ou=people,dc=lucasubuntu,dc=local" \
  -W

# Résultat attendu :
dn:uid=lucas,ou=people,dc=lucasubuntu,dc=local
```

4. Installation de Nextcloud (Snap)

Nextcloud est installé sous forme de paquet Snap, ce qui embarque automatiquement Apache, PHP et une base de données SQLite préconfigurée :

```
sudo snap install nextcloud
sudo snap services nextcloud
```

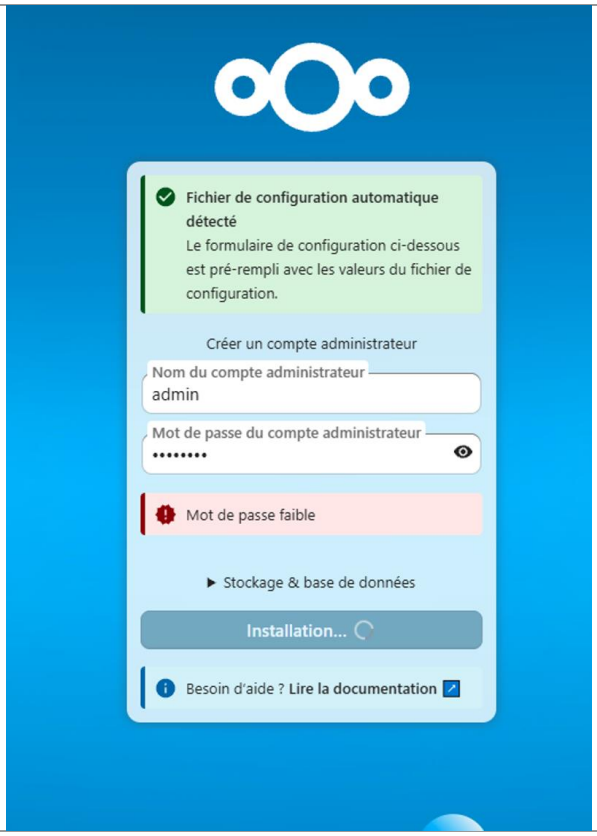


L'adresse IP du serveur est récupérée pour accéder à l'interface web depuis un navigateur :

```
hostname -I
# puis ouvrir : http://IP_DU_SERVEUR
```

4.1 Création du compte administrateur

Au premier accès, Nextcloud propose la création du compte administrateur local ainsi qu'un rappel du fichier de configuration détecté :

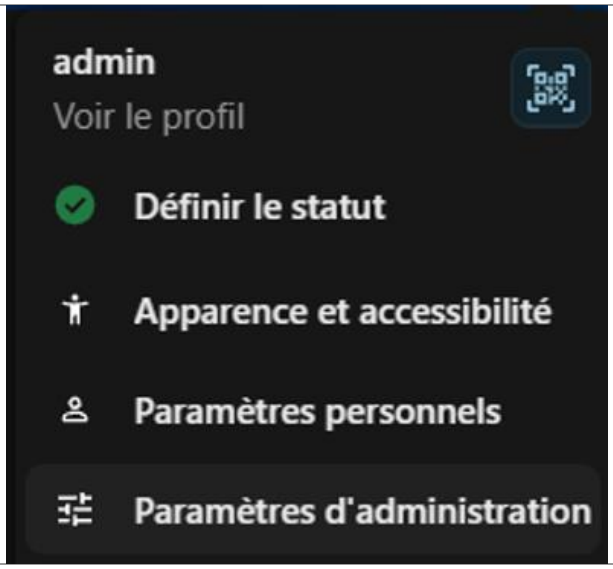


5. Intégration LDAP dans Nextcloud

Le module d'authentification LDAP/AD est activé en ligne de commande via l'utilitaire occ :

```
sudo nextcloud.occ app:enable user_ldap
sudo nextcloud.occ app:list | grep ldap
```

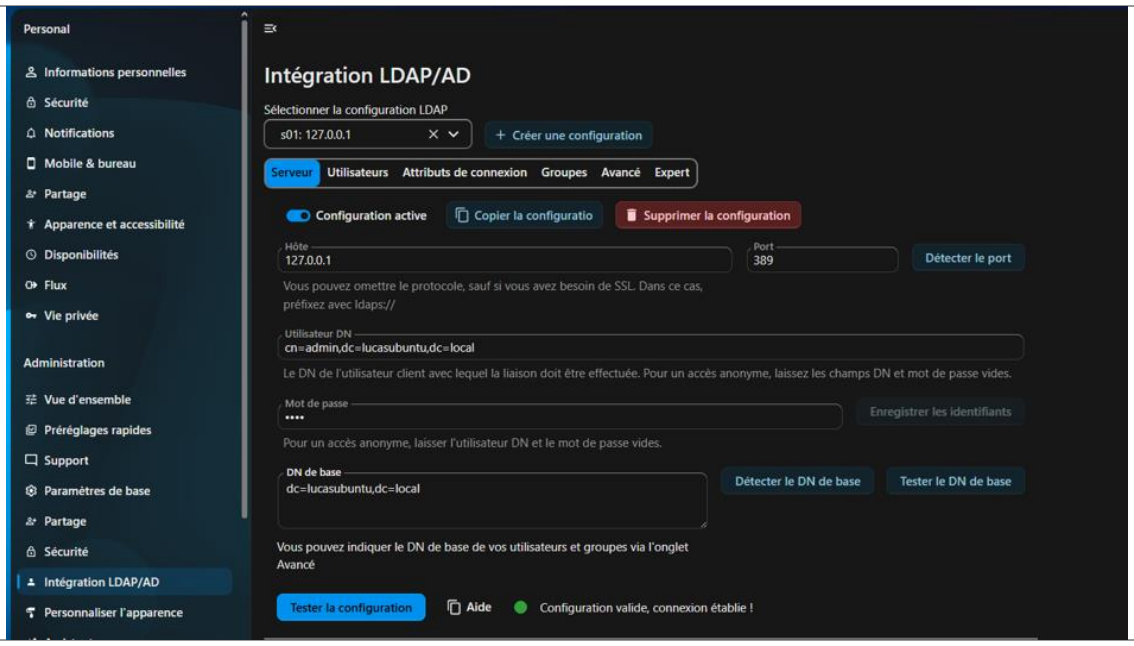
L'intégration se poursuit ensuite depuis l'interface graphique, dans les Paramètres d'administration :



5.1 Onglet Serveur

Les paramètres de connexion à l'annuaire sont renseignés dans l'onglet Serveur de la section Intégration LDAP/AD :

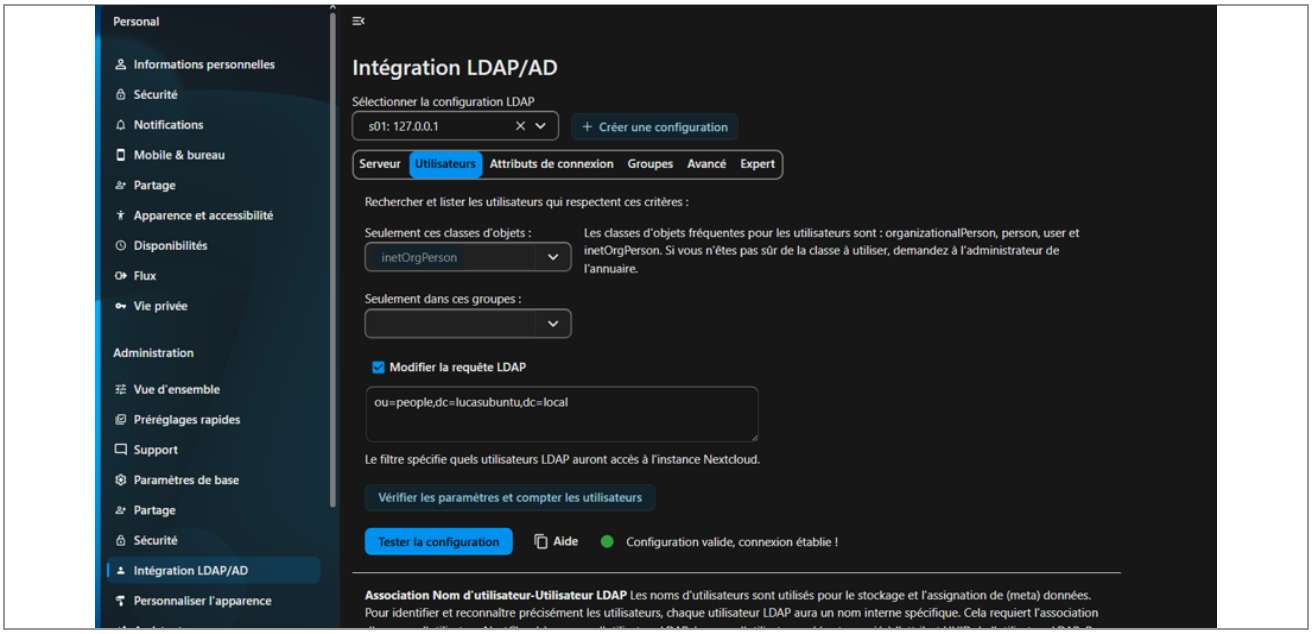
- Hôte : 127.0.0.1
- Port : 389
- Utilisateur DN : cn=admin,dc=lucasubuntu,dc=local
- Mot de passe : root
- DN de base : dc=lucasubuntu,dc=local



5.2 Onglet Utilisateurs

Le filtre utilisateurs est restreint à l'unité organisationnelle people avec la classe d'objet inetOrgPerson :

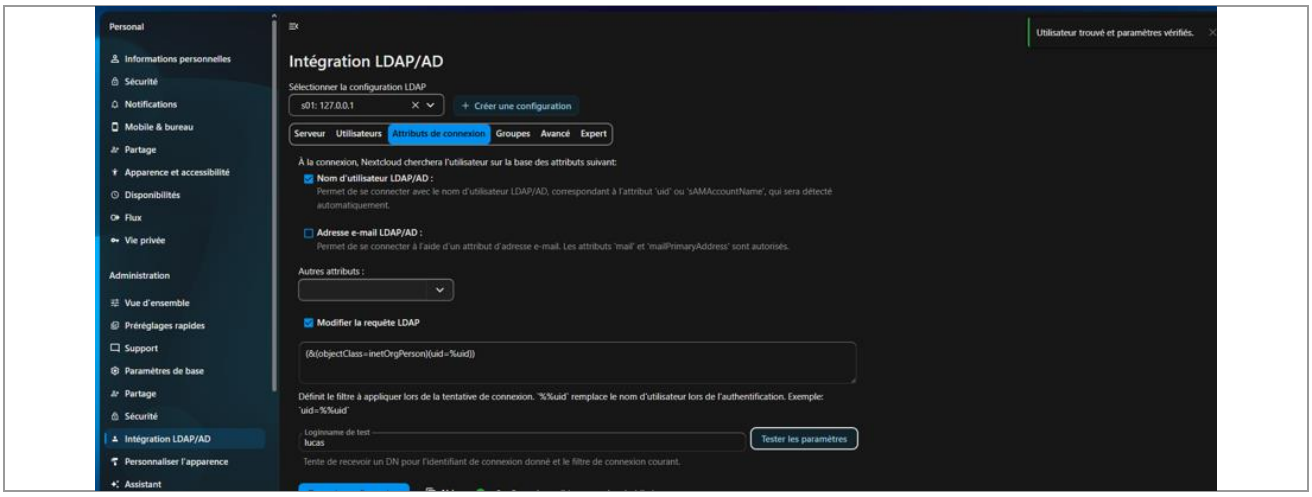
- DN de base utilisateurs : ou=people,dc=lucasubuntu,dc=local
- Filtre : (objectClass=inetOrgPerson)



5.3 Onglet Attributs de connexion

L'attribut uid est sélectionné comme identifiant de connexion, avec un filtre LDAP explicite associant le login saisi à l'attribut uid. Le test avec le login lucas confirme que l'utilisateur est trouvé et les paramètres vérifiés :

- Attribut de connexion : uid
- Filtre LDAP : (&(objectClass=inetOrgPerson)(uid=%uid))
- Login de test : lucas → "Utilisateur trouvé et paramètres vérifiés"



5.4 Activation de la configuration

La case Configuration active est cochée pour finaliser l'intégration. Le schéma d'authentification obtenu est le suivant :

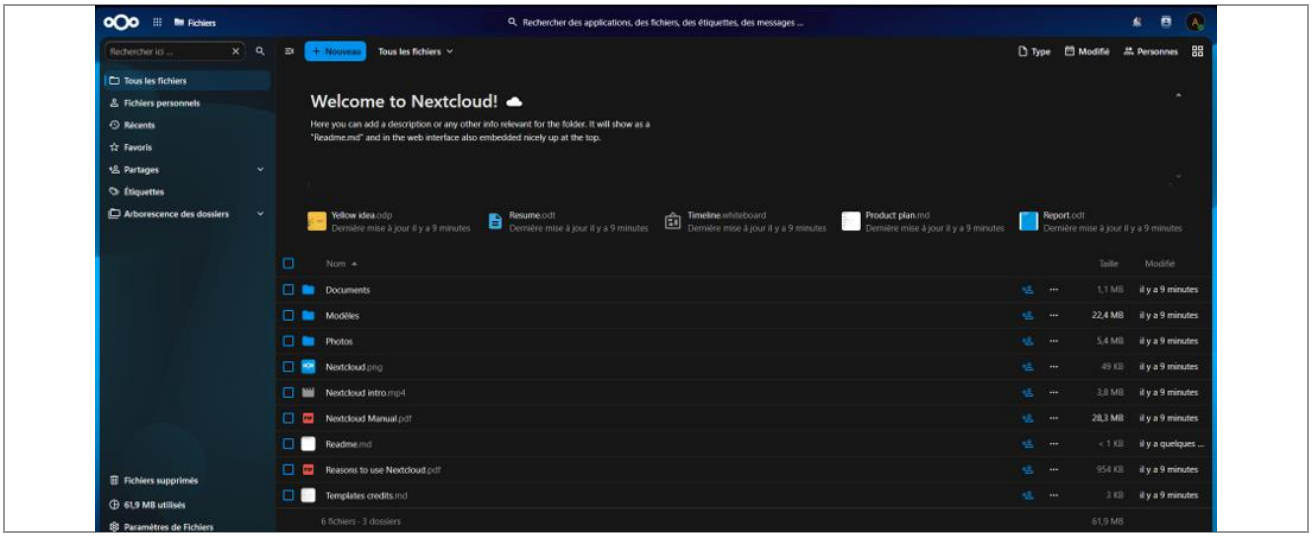
- OpenLDAP → compte lucas → Nextcloud

Le compte lucas est stocké dans LDAP ; Nextcloud délègue son authentification à l'annuaire au lieu de gérer un compte local.

6. Vérification finale

Connexion à Nextcloud avec les identifiants LDAP de lucas. L'interface de fichiers confirme l'accès effectif au compte, authentifié via l'annuaire OpenLDAP :

- Utilisateur : lucas
- Mot de passe : mot de passe LDAP de lucas



.