



Migrer le LDAP d'un Nextcloud

Armando FEMAT
PyConFR2025

Worteks

Société d'expertise, d'édition et d'hébergement Open Source
Centre de formation certifié Qualiopi

Contribue activement à de nombreux logiciels libres comme LSC, LemonLDAP::NG, LDAP Tool Box, FusionIAM et OpenStack

Partenaires



Sommaire

Introduction

Pourquoi migrer d'un LDAP à un autre ?

LDAP 101

De LDAP vers NextCloud

Difficultés du chemin

Pourquoi migrer d'annuaire ?

- Changement d'identité de la structure
 - changement du nom de la structure
 - changement dans les outils informatiques
 - adresse mail
 - nom de domaine
 - l'annuaire



Lightweight Directory Access Protocol

- Protocole / norme pour les systèmes d'annuaire.
- Il inclut:
 - Modèle des données
 - Modèle de nommage
- Structure arborescente avec à chaque nœud des attributs associés à leurs valeurs.



uid=bsamson

dn: uid=bsamson,ou=people,dc=osi,dc=com

cn: brock samson

sn: brock

uid: bsamson

carLicense: 09262-87265-001

mail: brock@osi.com

telephoneNumber: +33651489734

pager: +33651489733



Nextcloud a LDAP

- Comment Nextcloud crée un compte dans depuis LDAP ?
-

LDAP/AD integration

Server Users Login Attributes Groups

3. Server +

Import Export

Host Port Detect Port

Save Credentials

One Base DN per line Detect Base DN Test Base DN

Manually enter LDAP filters (recommended for large directories)

Configuration incomplete Continue Help

Nextcloud a LDAP

- Comment Nextcloud crée un compte dans depuis LDAP ?
- entryUUID
 - Universally Unique Identifier
- 16 caractères en hexadécimal
- 597ae2f6-16a6-1027-98f4-d28b5365dc14
- La table utilisateur contient aussi le DN et le hash du DN.

LDAP/AD integration

Server Users Login Attributes Groups

3. Server

Host

One Base DN per line

Manually enter LDAP filters (recommended for large directories)

Configuration incomplete

uid=bsamson opérationnel

dn: uid=bsamson,ou=people,dc=osi,dc=com
structuralObjectClass: inetOrgPerson
entryUUID: eeb417d6-589b-103e-9dfb-63a92ccfce7d
creatorsName: cn=Manager,dc=osi,dc=com
createTimestamp: 20240205175837Z
pwdChangedTime: 20250211172012Z
pwdLastSuccess: 20250211173225Z
entryCSN:
20250211173225.999347Z#000000#000#000000
modifyTimestamp: 20250211173225Z
[...]



Nextcloud

- Par défaut, Nextcloud utilise l'entryUUID pour nommer
 - les utilisateurs
 - les dossiers des utilisateurs
 - dossiers partagés
 - ...



Difficultés supplémentaires

- Nextcloud ne synchronise pas les comptes inexistantes
- Un environnement de test pas similaire à la prod...
- Des annuaires pas identiques...
- Rebolotte pour les groupes...

Solution : python-ldap

- Dump de la base de données
- Script python :
 - retrouver les comptes dans le dump,
 - trouver leur entryUUID dans le nouveau annuaire,
 - modifier le dump.



WorTeKS

make IT work, make IT free

www.wortek.com

-  info@wortek.com
-  +33 1 84 20 86 47
-  [wortek_com](https://twitter.com/wortek_com)
-  [wortek](https://www.linkedin.com/company/wortek/)