PortailSIO

NOUVELLE FORMULE

TUTORIEL

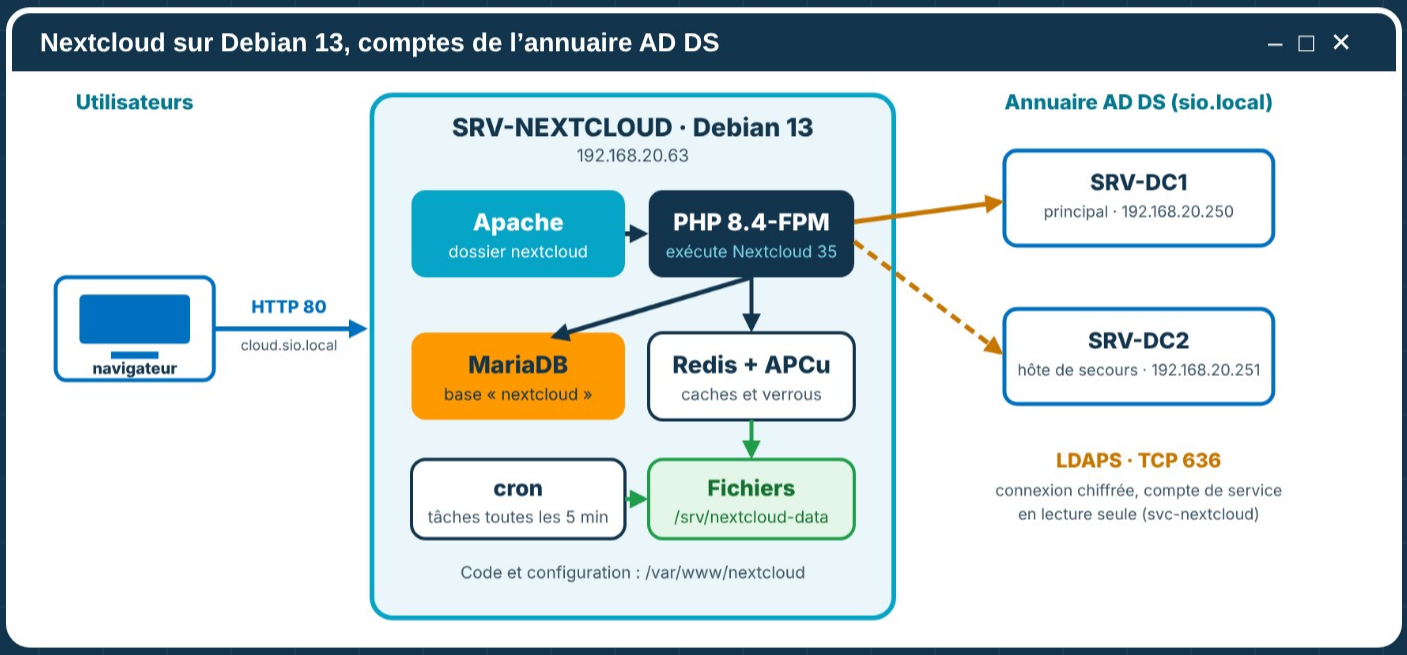
DEBIAN 13 · NEXTCLOUD 35.0.2

Installer et lier à AD/DS

NEXTCLOUD



NIVEAU
Intermédiaire



1 Préparer le serveur Debian 13 et le DNS

2 Installer Apache, PHP 8.4 et MariaDB

3 Installer Nextcloud 35.0.2 en ligne de commande

4 Optimiser et contrôler l'installation

5 Préparer AD DS : compte de service et LDAPS

6 Lier Nextcloud à l'annuaire et se connecter

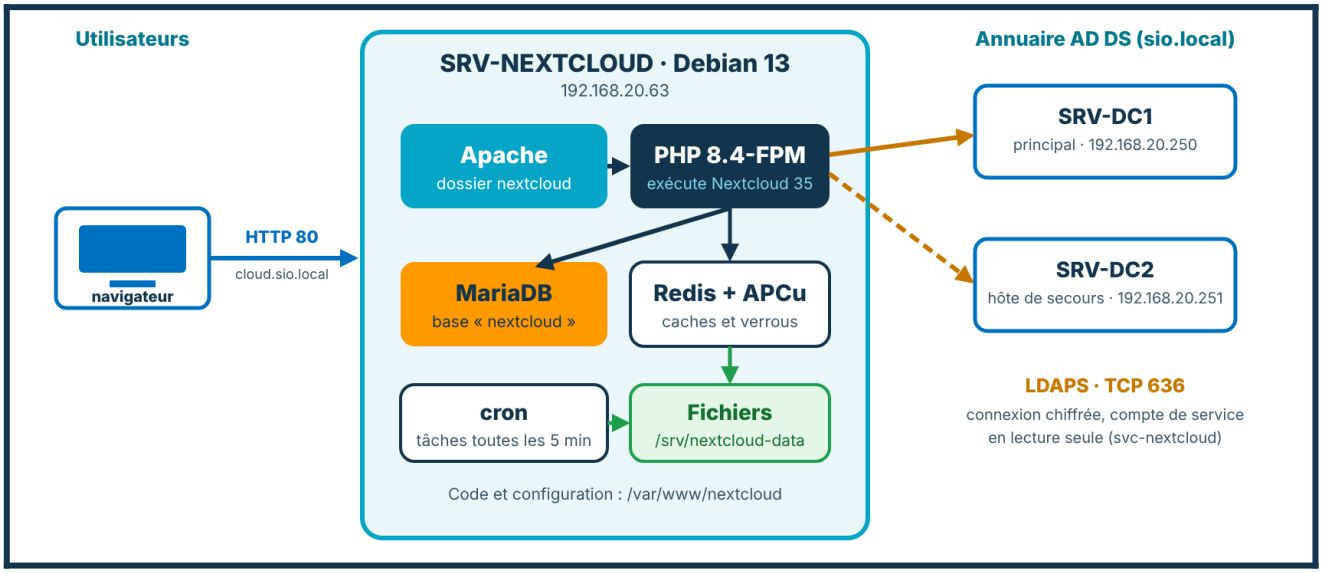
CC BY-NC
Utilisation commerciale interdite
© PortailSIO – 11/2026

Ce tutoriel en ligne
Scannez le QR code. Tous les tutoriels :
portail.sio-ndlp.fr/tutoriels.php

Ce tutoriel a été réalisé avec l'hyperviseur © Proxmox VE. Il peut être réalisé dans un environnement de virtualisation personnel à l'aide des logiciels © VirtualBox ou © VMware Player. Il **suppose que vous disposez d'une machine virtuelle Debian 13** (installation minimale avec serveur SSH) et du domaine **sio.local** construit dans les tutoriels précédents (contrôleurs **SRV-DC1** et **SRV-DC2** sous Windows Server 2025).

Nextcloud est une plateforme libre de **stockage et de partage de fichiers en ligne** : un « cloud » que l'on héberge soi-même, avec ses comptes, ses dossiers partagés, son agenda et ses contacts, accessible depuis un navigateur, un poste Windows ou un téléphone. La version **35.0.2** fonctionne avec **PHP 8.3 à 8.5** et **MariaDB 10.11 ou plus récent** : Debian 13, qui fournit PHP 8.4 et MariaDB 11.8, convient parfaitement.

Dans ce tutoriel, nous installons Nextcloud **« en natif »** (Apache, PHP-FPM, MariaDB et Redis directement sur Debian 13, sans conteneur), nous l'optimisons, puis nous le **lions à l'annuaire AD DS** pour que les utilisateurs se connectent avec leur compte Windows. Voici les composants et leurs échanges :



Les composants

- **Apache** reçoit les requêtes des navigateurs et publie le dossier de Nextcloud
- **PHP-FPM** exécute le code de Nextcloud (une application web écrite en PHP)
- **MariaDB** stocke les comptes, les partages et l'index des fichiers ; les fichiers eux-mêmes sont rangés dans un dossier de données
- **APCu** et **Redis** sont deux caches : ils accélèrent Nextcloud et évitent que deux personnes modifient le même fichier en même temps
- **cron** déclenche toutes les 5 minutes les tâches de fond (nettoyages, notifications, indexation…)
- **AD DS** (SRV-DC1 et son réplicat SRV-DC2) authentifie les utilisateurs par une connexion **chiffrée LDAPS**, à l'aide d'un compte de service en lecture seule

Dans le cadre de ce tutoriel, nous utilisons les machines suivantes (VLAN SERVEURS, réseau 192.168.20.0 /24) :

Machine	Rôle	Système	Adresse IP
SRV-NEXTCLOUD	Serveur Nextcloud (nom `srv-nextcloud`, alias DNS `cloud.sio.local`)	Debian 13	192.168.20.63
SRV-DC1	Contrôleur de domaine, DNS, annuaire principal	Windows Server 2025	192.168.20.250
SRV-DC2	Contrôleur de domaine, DNS, annuaire de secours	Windows Server 2025	192.168.20.251
Poste admin	Navigateur web pour utiliser Nextcloud (DNS = les deux contrôleurs)	Windows 11	DHCP

Pour **SRV-NEXTCLOUD**, prévoyez au minimum **2 vCPU, 4 Go de mémoire et 30 Go de disque** (davantage si les utilisateurs doivent y déposer beaucoup de fichiers : le dossier de données grandit avec eux). Ces valeurs, comme les adresses et les mots de passe d'exemple, sont à adapter à votre environnement. Les commandes Debian sont exécutées avec un compte autorisé à utiliser `sudo` (ou directement en `root`, sans le préfixe `sudo`) ; les commandes Windows, dans **PowerShell** ouvert **en tant qu'administrateur** sur **SRV-DC1**.

01 ÉTAPE 1 SUR 6 — Préparer le serveur Debian 13 et le DNS

Avant d'installer Nextcloud, on prépare le système (mises à jour, nom, adresse fixe, heure) et on déclare le nom **cloud.sio.local** dans le DNS du domaine. Sur **SRV-NEXTCLOUD** :

1. Mettez le système à jour : `sudo apt update && sudo apt full-upgrade -y`
2. Donnez son nom au serveur et déclarez-le dans le fichier `hosts` (nom complet et nom court) :

TERMINAL
```
sudo hostnamectl set-hostname srv-nextcloud
echo "192.168.20.63  cloud.sio.local  srv-nextcloud" | sudo tee -a /etc/hosts
```

3. Réglez le fuseau horaire : `sudo timedatectl set-timezone Europe/Paris`
4. Donnez au serveur une **adresse IP fixe** (adaptez le nom de la carte, ici `ens18`, avec `ip -br address`) : éditez `/etc/network/interfaces` puis redémarrez le réseau avec `sudo systemctl restart networking` :

/etc/network/interfaces
```
auto ens18
iface ens18 inet static
    address 192.168.20.63/24
    gateway 192.168.20.254
```

5. Indiquez les **DNS du domaine** dans `/etc/resolv.conf` (`sudo nano /etc/resolv.conf`) : le serveur doit retrouver `srv-dc1.sio.local` et `srv-dc2.sio.local` :

/etc/resolv.conf
```
search sio.local
nameserver 192.168.20.250
nameserver 192.168.20.251
```

6 Sur **SRV-DC1**, déclarez l'alias DNS de Nextcloud (l'enregistrement est répliqué sur SRV-DC2 avec la zone) :

POWERSHELL

```
Add-DnsServerResourceRecordA -Name "cloud" -ZoneName "sio.local" `
    -IPv4Address "192.168.20.63"
```

7 Vérifiez le résultat : nom, adresse IP, résolution DNS des contrôleurs et de Nextcloud, heure :

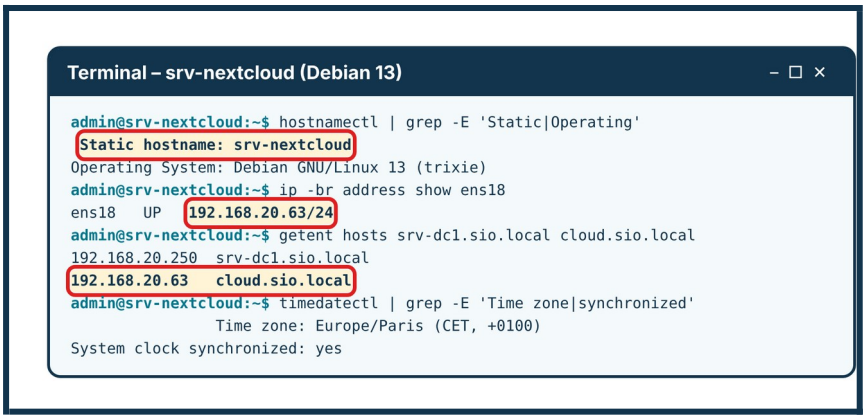


Figure 1 – Contrôle de la préparation du serveur

À SAVOIR

Si « System clock synchronized » indique « no », installez un service de temps (`sudo apt install -y chrony`). L'heure doit être juste : le certificat LDAPS de l'étape 5 a des dates de validité.

✔ **POINT DE CONTRÔLE**

- `hostnamectl` affiche le nom **srv-nextcloud** et Debian GNU/Linux **13**
- L'adresse IP **192.168.20.63** est fixe
- `getent hosts srv-dc1.sio.local cloud.sio.local` renvoie les deux adresses
- Le fuseau horaire est **Europe/Paris** et l'horloge est **synchronisée**

02 ÉTAPE 2 SUR 6 — Installer Apache, PHP 8.4 et MariaDB

A – Installer Apache, PHP-FPM, MariaDB et Redis

Nextcloud s'appuie sur plusieurs **extensions PHP** (base de données, images, LDAP, caches…). Tout s'installe en une seule commande ; Apache est ici associé à **PHP-FPM**, un service PHP séparé plus rapide et mieux isolé que le module classique :

TERMINAL

```
sudo apt install -y apache2 php8.4-fpm php8.4-cli php8.4-mysql php8.4-curl \
    php8.4-gd php8.4-intl php8.4-mbstring php8.4-xml php8.4-zip php8.4-bz2 \
    php8.4-gmp php8.4-bcmath php8.4-ldap php8.4-opcache php8.4-apcu \
    php8.4-redis mariadb-server redis-server
```

Extension / paquet	Utilité pour Nextcloud
php8.4-mysql	Connexion à MariaDB (extension `pdo_mysql`)
php8.4-curl, php8.4-xml, php8.4-zip	Appels web, lecture de fichiers XML, archives
php8.4-gd, php8.4-intl, php8.4-mbstring	Miniatures d'images, langues, caractères accentués
php8.4-gmp, php8.4-bcmath, php8.4-bz2	Calculs, chiffrement, archives (recommandés)
php8.4-ldap	Connexion à l'annuaire AD DS (étape 6)
php8.4-opcache, php8.4-apcu, php8.4-redis	Accélération du code PHP et caches (APCu local, Redis partagé)

1. Vérifiez la version de PHP, puis que **toutes** les extensions utiles sont chargées. Si une extension manque, la commande l'affiche (aucun message = tout est présent) :

TERMINAL
```
php -v | head -1
EXT="ctype curl dom fileinfo gd intl mbstring SimpleXML xmlreader xmlwriter"
EXT="$EXT zip zlib openssl posix pdo_mysql bz2 exif ldap gmp bcmath"
EXT="$EXT apcu redis opcache"
for e in $EXT; do php -m | grep -qiw "$e" || echo "MANQUE : $e"; done
```

B – Régler PHP pour Nextcloud

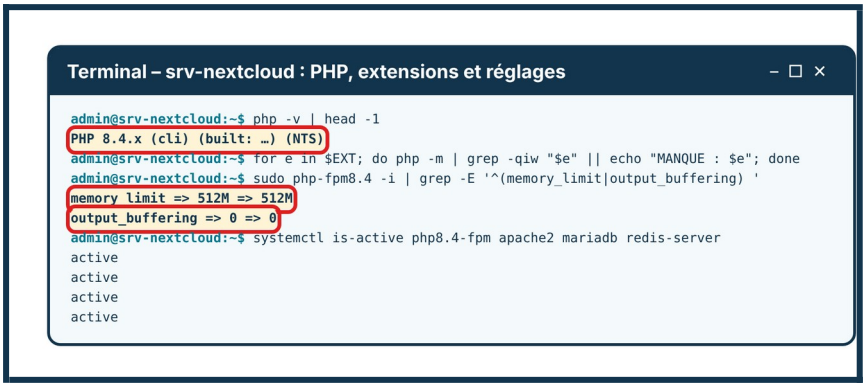
Nextcloud demande plus de mémoire que la configuration par défaut de PHP, et un réglage précis du cache de code (OPcache). On crée un petit fichier de réglages, qui fixe aussi la taille maximale des fichiers envoyés (1 Go ici) :

1. Créez le fichier avec `sudo nano /etc/php/8.4/fpm/conf.d/90-nextcloud.ini` et saisissez :

/etc/php/8.4/fpm/conf.d/90-nextcloud.ini
```
memory_limit = 512M
upload_max_filesize = 1G
post_max_size = 1G
max_execution_time = 360
output_buffering = 0
opcache.interned_strings_buffer = 32
opcache.max_accelerated_files = 10000
opcache.memory_consumption = 128
opcache.save_comments = 1
opcache.revalidate_freq = 60
```

2. Autorisez aussi PHP-FPM à transmettre à Nextcloud les variables d'environnement du système (`clear_env = no` dans le pool par défaut), puis redémarrez le service et contrôlez la prise en compte :

TERMINAL
```
sudo sed -i 's/^;clear_env = no/clear_env = no/' /etc/php/8.4/fpm/pool.d/www.conf
sudo systemctl restart php8.4-fpm
sudo php-fpm8.4 -i | grep -E '^(memory_limit|output_buffering) '
systemctl is-active php8.4-fpm apache2 mariadb redis-server
```



À SAVOIR

Si `php-fpm8.4 -i` affiche encore `128M`, le fichier n'est pas pris en compte : vérifiez son nom (il doit finir par `.ini`) et son dossier `conf.d` de **fpm**, pas celui de `cli`.

Figure 2 – PHP 8.4, extensions et réglages

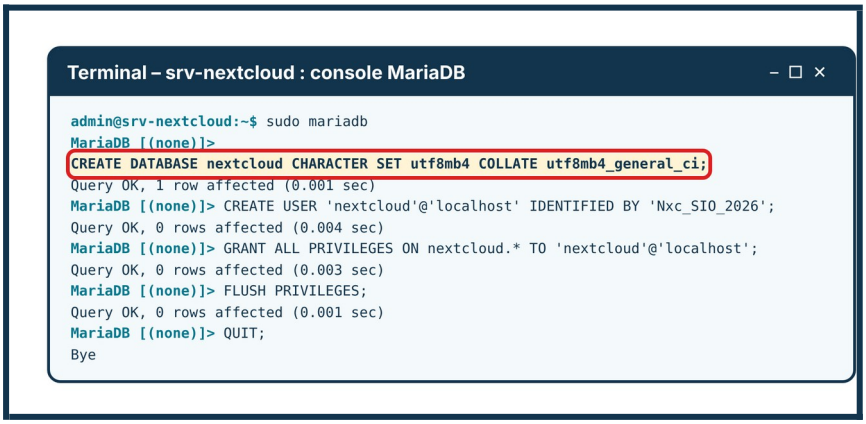
C – Sécuriser MariaDB et créer la base

Debian 13 fournit **MariaDB 11.8**, que Nextcloud 35 prend en charge. Le service est déjà démarré : sécurisez-le, puis créez la base **nextcloud** et son utilisateur :

1. Lancez `sudo mariadb-secure-installation` et répondez : **Entrée** (pas de mot de passe root actuel), `n` (authentification par socket déjà active), `n` (pas de mot de passe root), puis `Y` aux quatre dernières questions (comptes anonymes, root à distance, base de test, rechargement des privilèges)
2. Ouvrez la console avec `sudo mariadb` puis créez la base, l'utilisateur et ses droits :

CONSOLE MARIADB

```
CREATE DATABASE nextcloud CHARACTER SET utf8mb4 COLLATE utf8mb4_general_ci;
CREATE USER 'nextcloud'@'localhost' IDENTIFIED BY 'Nxc_SIO_2026';
GRANT ALL PRIVILEGES ON nextcloud.* TO 'nextcloud'@'localhost';
FLUSH PRIVILEGES;
QUIT;
```



À SAVOIR

Le jeu de caractères utf8mb4 gère tous les caractères (accents, symboles, emoji). L'utilisateur n'a de droits que sur sa propre base et ne peut se connecter que depuis le serveur lui-même (`localhost`).

Figure 3 – Console MariaDB : création de la base et de l'utilisateur

REMARQUE IMPORTANTE

`Nxc_SIO_2026` n'est qu'un exemple : **choisissez un mot de passe solide** pour l'utilisateur **nextcloud** de la base. Vous le saisirez une seule fois, à l'étape 3 ; Nextcloud le range ensuite dans son fichier `config/config.php`, lisible uniquement par `www-data`.

✔ POINT DE CONTRÔLE

- `sudo mariadb -e "SHOW DATABASES;"` liste la base **nextcloud**
- `php -v` indique **PHP 8.4** et le contrôle des extensions n'affiche aucun « MANQUE »
- `php-fpm8.4 -i` indique `memory_limit => 512M` et `output_buffering => 0`
- `systemctl is-active php8.4-fpm apache2 mariadb redis-server` répond **active** quatre fois

03 ÉTAPE 3 SUR 6 Installer Nextcloud 35.0.2 en ligne de commande

A – Télécharger, vérifier et décompresser Nextcloud

1 Installez les outils de téléchargement et de décompression (absents d'une installation minimale), puis récupérez l'archive officielle de la version **35.0.2 et son fichier d'empreinte** :

TERMINAL

```
sudo apt install -y wget bzip2
cd /tmp
URL=https://download.nextcloud.com/server/releases
wget -q $URL/nextcloud-35.0.2.tar.bz2 $URL/nextcloud-35.0.2.tar.bz2.sha256
```

2 Contrôlez que l'archive n'est ni corrompue ni modifiée : la commande doit répondre **OK**. Décompressez ensuite l'archive dans `/var/www` :

TERMINAL

```
sha256sum -c --ignore-missing nextcloud-35.0.2.tar.bz2.sha256
sudo tar -xjf nextcloud-35.0.2.tar.bz2 -C /var/www/
ls /var/www/nextcloud
```

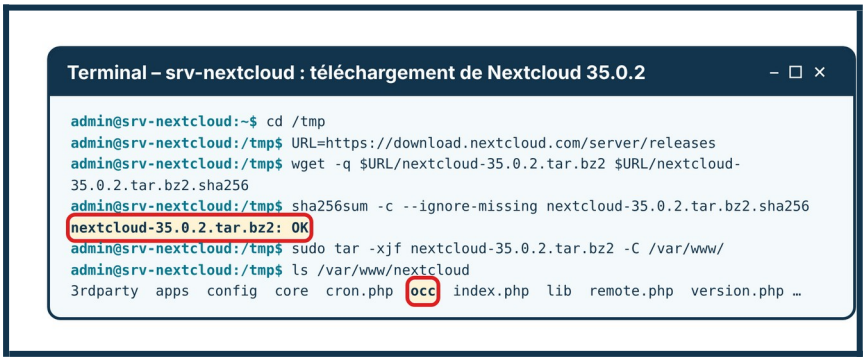


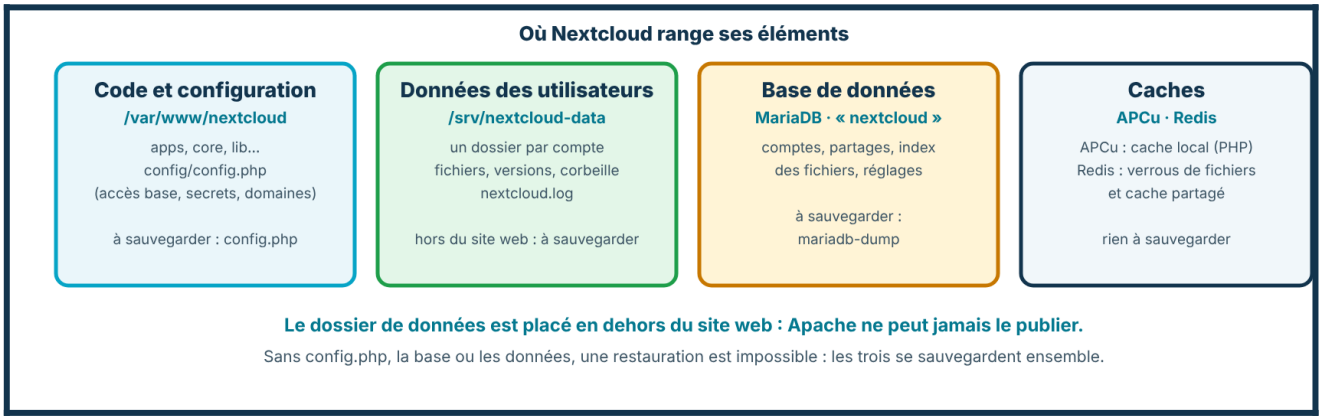
Figure 4 – Téléchargement et contrôle de l'archive

À SAVOIR

Si le contrôle échoue, supprimez l'archive et téléchargez-la de nouveau : n'installez jamais une archive dont l'empreinte ne correspond pas. Le fichier `occ` est l'outil en ligne de commande de Nextcloud.

B – Préparer les dossiers, les droits et la commande occ

Contrairement à d'autres applications, Nextcloud doit pouvoir **écrire dans son propre dossier** (configuration, applications, mises à jour) : il appartient donc à **www-data**, l'utilisateur d'Apache et de PHP-FPM. Les fichiers des utilisateurs sont rangés **hors du site web**, dans `/srv/nextcloud-data` : Apache ne pourra jamais les publier.



1 Créez le dossier de données et appliquez les droits :

TERMINAL
```
sudo mkdir /srv/nextcloud-data
sudo chown -R www-data:www-data /var/www/nextcloud /srv/nextcloud-data
sudo chmod 750 /srv/nextcloud-data
```

2 La commande `occ` doit toujours être lancée **en tant que www-data**, sinon elle crée des fichiers que le site ne peut plus lire. On crée donc un petit script qui s'en charge : `sudo nano /usr/local/bin/occ` :

/usr/local/bin/occ
```
#!/bin/sh
exec runuser -u www-data -- php /var/www/nextcloud/occ "$@"
```

3 Rendez-le exécutable ; à partir de maintenant, toutes les commandes Nextcloud s'écrivent `sudo occ …` :

TERMINAL
```
sudo chmod +x /usr/local/bin/occ
```

C – Installer Nextcloud avec occ

Plutôt que de passer par l'assistant web, on installe Nextcloud **en une commande** : c'est reproductible, et il n'y a aucune page à remplir. Indiquez la base créée à l'étape 2, le compte administrateur de Nextcloud et le dossier de données :

TERMINAL
```
sudo occ maintenance:install --database mysql --database-name nextcloud \
    --database-user nextcloud --database-pass 'Nxc_SIO_2026' \
    --admin-user admin --admin-pass 'Admin_SIO_2026!' \
    --data-dir /srv/nextcloud-data
sudo occ status
```



Figure 5 – Installation en ligne de commande

À SAVOIR

L'installation prend une à deux minutes. Les mots de passe saisis ici restent dans l'historique du shell : en production, saisissez-les depuis un fichier ou effacez l'historique (`history -c`). Le premier chiffre de la version est la version majeure, 35.

REMARQUE IMPORTANTE

`Admin_SIO_2026!` n'est qu'un exemple : **choisissez un mot de passe solide** pour le compte **admin** de Nextcloud, qui peut tout faire. Ce compte est local à Nextcloud, il n'existe pas dans l'annuaire AD DS.

D – Publier Nextcloud avec Apache et programmer les tâches de fond

1 Déclarez le nom du site comme **domaine de confiance** (Nextcloud refuse sinon d'être appelé par un autre nom que `localhost`) et indiquez son adresse :

TERMINAL

```
sudo occ config:system:set trusted_domains 1 --value=cloud.sio.local
sudo occ config:system:set overwrite.cli.url --value=http://cloud.sio.local
```

2 Créez le site Apache avec `sudo nano /etc/apache2/sites-available/nextcloud.conf` :

/etc/apache2/sites-available/nextcloud.conf

```
<VirtualHost *:80>
    ServerName cloud.sio.local
    DocumentRoot /var/www/nextcloud
    <Directory /var/www/nextcloud>
        Require all granted
        AllowOverride All
        Options FollowSymLinks MultiViews
    </Directory>
    <FilesMatch \.php$>
        SetHandler "proxy:unix:/run/php/php8.4-fpm.sock|fcgi://localhost/"
    </FilesMatch>
    ErrorLog ${APACHE_LOG_DIR}/nextcloud-error.log
</VirtualHost>
```

3 Activez les modules nécessaires, remplacez le site par défaut par celui de Nextcloud, vérifiez la syntaxe et rechargez Apache :

TERMINAL

```
sudo a2enmod rewrite headers proxy_fcgi setenvif
sudo a2dissite 000-default
sudo a2ensite nextcloud
sudo apachectl configtest
sudo systemctl reload apache2
```

4 Obtenez des adresses propres, sans `index.php` dans les liens, en demandant à Nextcloud de réécrire son fichier `.htaccess` :

TERMINAL

```
sudo occ config:system:set htaccess.RewriteBase --value=/
sudo occ maintenance:update:htaccess
```

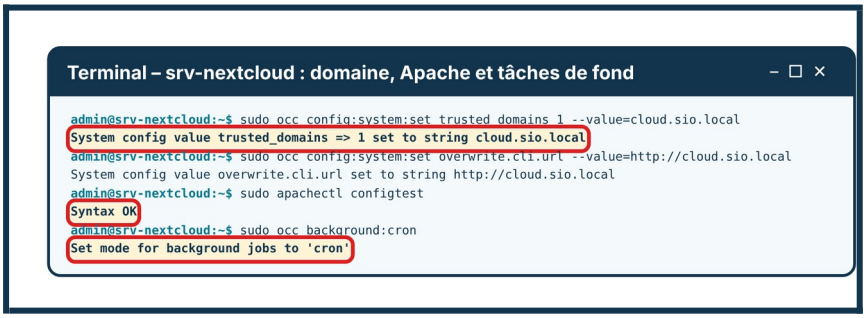
Enfin, Nextcloud doit exécuter régulièrement des tâches (nettoyages, notifications, indexation…). On les confie au planificateur du système, toutes les 5 minutes, plutôt qu'aux visites des utilisateurs. Créez `sudo nano /etc/cron.d/nextcloud` puis déclarez ce mode à Nextcloud :

/etc/cron.d/nextcloud

```
*/5 * * * * www-data /usr/bin/php -f /var/www/nextcloud/cron.php
```

TERMINAL

```
sudo occ background:cron
```



À SAVOIR

Le fichier `/etc/cron.d/nextcloud` doit se terminer par un saut de ligne et appartenir à root. La première exécution a lieu dans les 5 minutes : le contrôle s'en occupe à l'étape 4.

Figure 6 – Domaine de confiance, syntaxe d'Apache et mode cron

✔ POINT DE CONTRÔLE

- `sudo occ status` indique **installed: true** et la version **35.0.2**
- `sudo apachectl configtest` affiche **Syntax OK**
- Le site par défaut d'Apache est désactivé et **nextcloud** est activé (`ls /etc/apache2/sites-enabled`)
- Les fichiers `/etc/cron.d/nextcloud` et `/srv/nextcloud-data` existent

04 ÉTAPE 4 SUR 6
Optimiser et contrôler l'installation

A – Première connexion

Depuis le **poste d'administration**, ouvrez un navigateur et saisissez `http://cloud.sio.local`. La page de connexion de Nextcloud s'affiche : saisissez **admin** et le mot de passe choisi à l'étape 3-C.

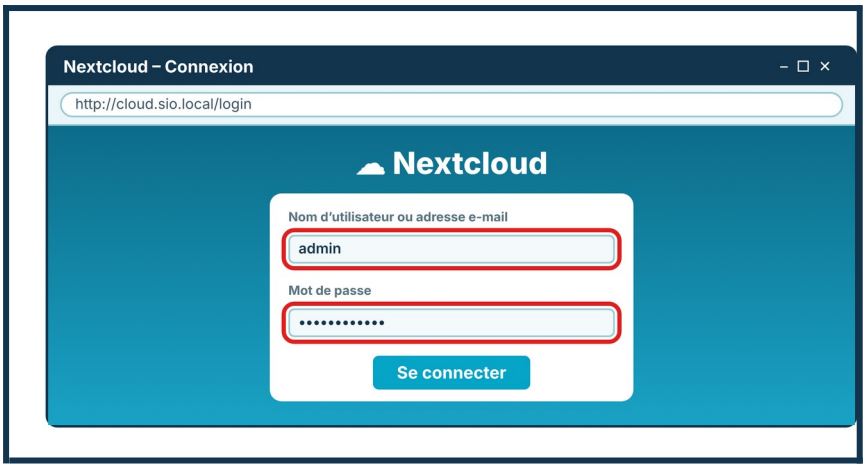


Figure 7 – Page de connexion de Nextcloud

À SAVOIR

Si le message « Accès via un domaine non approuvé » s'affiche, le nom saisi n'est pas dans `trusted_domains` : relisez l'étape 3-D. Si la page « Apache2 Debian Default Page » s'affiche, le site par défaut est resté actif.

À la première connexion, Nextcloud peut proposer une fenêtre de bienvenue et d'**applications recommandées** : cette étape est facultative, vous pouvez la fermer.

B – Appliquer les réglages de maintenance

Un petit ensemble de commandes complète l'installation : création des index manquants dans la base (pour des recherches rapides), réparations « coûteuses » qui ne sont pas lancées d'office, région téléphonique par défaut (France) et fenêtre de maintenance à 1 h du matin, heure UTC (les tâches lourdes s'exécutent la nuit) :

TERMINAL

```
sudo occ db:add-missing-indices
sudo occ maintenance:repair --include-expensive
sudo occ config:system:set default_phone_region --value=FR
sudo occ config:system:set maintenance_window_start --type=integer --value=1
```

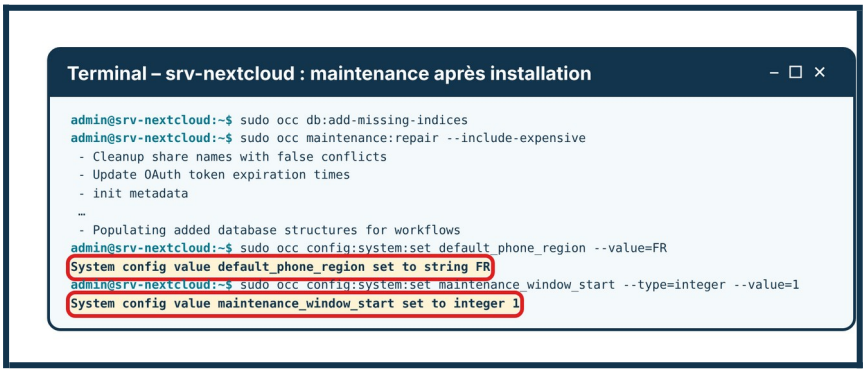


Figure 8 – Réglages de maintenance appliqués

À SAVOIR

La réparation affiche une liste d'opérations qui varie selon la version : l'important est qu'elle se termine sans message d'erreur.

C – Activer les caches APCu et Redis

Sans cache, Nextcloud relit sans cesse sa configuration et sa base. On déclare donc **APCu** comme cache local, et **Redis** pour le cache partagé et le **verrouillage des fichiers** (deux personnes ne peuvent pas écraser en même temps le même fichier) :

TERMINAL

```
sudo occ config:system:set memcache.local --value='\OC\Memcache\APCu'
sudo occ config:system:set memcache.distributed --value='\OC\Memcache\Redis'
sudo occ config:system:set memcache.locking --value='\OC\Memcache\Redis'
sudo occ config:system:set redis host --value=localhost
sudo occ config:system:set redis port --value=6379 --type=integer
```

1 Contrôlez que Redis répond (**PONG**) et que les valeurs sont bien enregistrées :

TERMINAL

```
redis-cli ping
sudo occ config:system:get memcache.local
sudo occ config:system:get memcache.distributed
sudo occ config:system:get memcache.locking
sudo occ config:system:get redis host
```

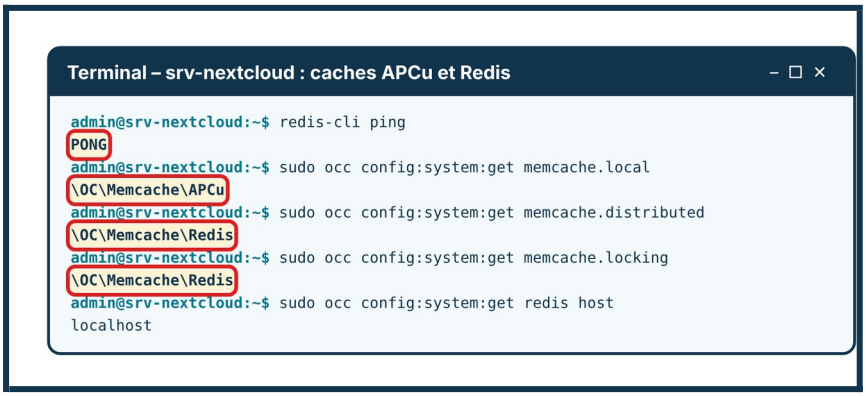


Figure 9 – Redis et les trois caches

À SAVOIR

Redis n'écoute que sur le serveur lui-même (`127.0.0.1`) et n'a pas de mot de passe : c'est suffisant ici. S'il devait un jour être joint par le réseau, protégez-le par un mot de passe et un pare-feu.

D – Lire la page « Vue d'ensemble »

Nextcloud contrôle lui-même sa configuration. Avec l'avatar en haut à droite, ouvrez « **Paramètres d'administration** » puis « **Vue d'ensemble** ». Attendez 5 minutes après la mise en route du cron, puis rechargez la page : la liste doit être presque entièrement verte.

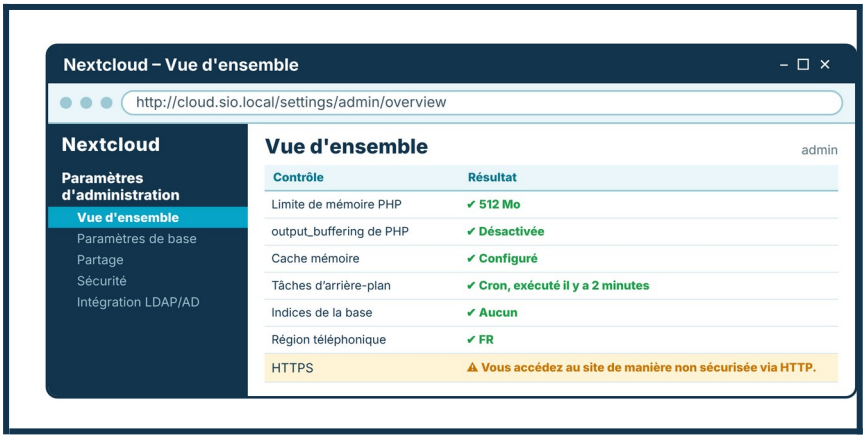


Figure 10 – Paramètres d'administration > Vue d'ensemble

À SAVOIR

Le seul avertissement attendu concerne **HTTPS** : le site est volontairement servi en HTTP dans ce tutoriel. Chaque ligne en erreur ou en avertissement indique sa cause et un lien vers la documentation ; relancez la page après chaque correction.

À SAVOIR

En production, publiez Nextcloud en **HTTPS** (certificat délivré par l'autorité de certification de l'entreprise) : les identifiants et les fichiers des utilisateurs ne doivent pas circuler en clair sur le réseau. Une fois le certificat en place, passez l'adresse `overwrite.cli.url` en `https://`. Dans ce tutoriel, le site reste en HTTP pour se concentrer sur l'installation et sur l'annuaire.

✔ **POINT DE CONTRÔLE**

- La connexion en **admin** fonctionne
- `redis-cli ping` répond **PONG** et les trois caches sont enregistrés
- La « Vue d'ensemble » ne signale plus que l'avertissement **HTTPS**
- La tâche d'arrière-plan indique un **cron** exécuté il y a quelques minutes

05 ÉTAPE 5 SUR 6 Préparer AD DS : compte de service et LDAPS

Pour authentifier les utilisateurs, Nextcloud interroge l'annuaire avec un **compte de service** (lecture seule), puis vérifie le mot de passe de chaque utilisateur. Cette étape se déroule sur les **contrôleurs de domaine** et sur **SRV-NEXTCLOUD**.

REMARQUE IMPORTANTE

Windows Server 2025 impose la signature LDAP : les connexions LDAP simples (port 389, sans chiffrement) avec identifiant et mot de passe sont **refusées par défaut** sur un domaine neuf. Nextcloud doit donc utiliser **LDAPS** (LDAP chiffré, port **636**). Il faut pour cela un **certificat** sur chaque contrôleur et la **confiance** de Debian envers ce certificat.

À SAVOIR

Si vous avez déjà réalisé le tutoriel « Installer GLPI et le lier à AD DS », les unités d'organisation, les utilisateurs **amartin** et **bdurand** et les **certificats des contrôleurs** existent déjà : les commandes de création répondent alors « existe déjà » (ignorez-le) et, à l'étape B, il suffit de copier les certificats vers ce serveur (étape C).

A – Créer le compte de service, les utilisateurs de test et les groupes

Sur **SRV-DC1**, dans PowerShell (**administrateur**), créez les unités d'organisation (OU), le compte **svc-nextcloud** et deux utilisateurs pour les tests. Si votre domaine possède déjà une OU pour vos utilisateurs, utilisez-la à la place de « Utilisateurs » (ce sera le **DN de base** de Nextcloud) :

POWERSHELL

```
$base = "DC=sio,DC=local"
New-ADOrganizationalUnit -Name "Comptes de service" -Path $base
New-ADOrganizationalUnit -Name "Utilisateurs" -Path $base
New-ADOrganizationalUnit -Name "Groupes" -Path $base
$mdp = Read-Host -AsSecureString "Mot de passe de svc-nextcloud"
New-ADUser -Name "svc-nextcloud" -SamAccountName "svc-nextcloud" `
    -UserPrincipalName "svc-nextcloud@sio.local" `
    -Path "OU=Comptes de service,$base" -AccountPassword $mdp `
    -Enabled $true -PasswordNeverExpires $true -CannotChangePassword $true
```

```powershell
$mdp = Read-Host -AsSecureString "Mot de passe des utilisateurs de test"
New-ADUser -Name "Alice Martin" -GivenName Alice -Surname Martin `
    -SamAccountName amartin -UserPrincipalName amartin@sio.local `
    -EmailAddress amartin@sio.local -Path "OU=Utilisateurs,$base" `
    -AccountPassword $mdp -Enabled $true
New-ADUser -Name "Bruno Durand" -GivenName Bruno -Surname Durand `
    -SamAccountName bdurand -UserPrincipalName bdurand@sio.local `
    -EmailAddress bdurand@sio.local -Path "OU=Utilisateurs,$base" `
    -AccountPassword $mdp -Enabled $true
```

1 Nextcloud sait aussi lire les **groupes** de l'annuaire (pour partager un dossier avec tout un service, par exemple). Créez deux groupes et placez-y les utilisateurs :

```powershell
New-ADGroup -Name "GRP-Direction" -GroupScope Global -Path "OU=Groupes,$base"
New-ADGroup -Name "GRP-Technique" -GroupScope Global -Path "OU=Groupes,$base"
Add-ADGroupMember -Identity "GRP-Direction" -Members amartin
Add-ADGroupMember -Identity "GRP-Technique" -Members bdurand
```

2 Contrôlez la création :

```powershell
Get-ADUser svc-nextcloud | Select Name, Enabled, DistinguishedName
Get-ADGroupMember "GRP-Technique" | Select Name, SamAccountName
```

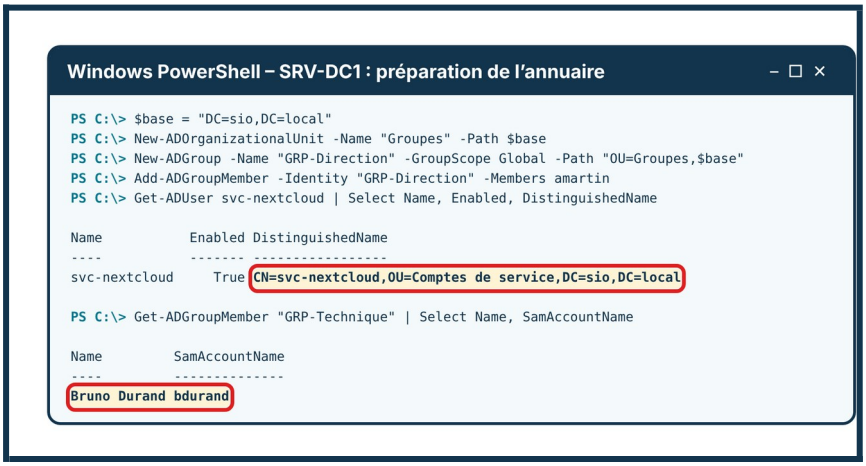


Figure 11 – PowerShell : groupes, compte de service et membres

À SAVOIR

Le compte **svc-nextcloud** est un compte de domaine ordinaire : il peut lire l'annuaire, rien d'autre. Ne l'ajoutez à aucun groupe d'administration. Son mot de passe n'expire pas, sinon Nextcloud cesserait de fonctionner le jour de l'expiration.

B – Créer un certificat LDAPS sur chaque contrôleur

Un contrôleur de domaine active LDAPS dès qu'il trouve, dans le magasin « Ordinateur local > Personnel », un certificat pour son **nom complet** et utilisable pour l'authentification de serveur. En **production**, on le fait délivrer par l'autorité de certification de l'entreprise (AD CS). Pour le **laboratoire**, un certificat auto-signé suffit. Sur **SRV-DC1**, puis sur **SRV-DC2** (en changeant le nom) :

POWERSHELL

```
# SRV-DC2 : remplacer par srv-dc2.sio.local
$fqdn = "srv-dc1.sio.local"
$cert = New-SelfSignedCertificate -Subject "CN=$fqdn" -DnsName $fqdn `
    -CertStoreLocation Cert:\LocalMachine\My -KeyAlgorithm RSA `
    -KeyLength 2048 -HashAlgorithm SHA256 -NotAfter (Get-Date).AddYears(2)
New-Item -ItemType Directory -Path C:\Temp -Force | Out-Null
# SRV-DC2 : srv-dc2.cer
Export-Certificate -Cert $cert -FilePath C:\Temp\srv-dc1.cer
```

1. Patientez quelques minutes (le contrôleur détecte le certificat tout seul ; au besoin, redémarrez-le), puis contrôlez que le port **636** répond :

POWERSHELL

```
Test-NetConnection srv-dc1.sio.local -Port 636
Test-NetConnection srv-dc2.sio.local -Port 636
```

« TcpTestSucceeded : True » prouve seulement que le port est ouvert. La vérification du certificat lui-même se fait depuis Debian (étape suivante).

REMARQUE IMPORTANTE

Un certificat auto-signé de **deux ans** expire un jour : notez la date et renouvelez-le avant, sinon Nextcloud ne pourra plus joindre l'annuaire (message « Can't contact LDAP server »). Avec AD CS, le renouvellement est automatique.

C – Faire confiance au certificat sur SRV-NEXTCLOUD

Debian ne connaît pas votre certificat auto-signé et refuserait la connexion. On l'ajoute à ses **autorités de confiance**. Depuis PowerShell, copiez les deux fichiers vers **SRV-NEXTCLOUD** (ou utilisez WinSCP, ou un partage) :

POWERSHELL (SRV-DC1 ET SRV-DC2)

```
scp C:\Temp\srv-dc1.cer admin@192.168.20.63:/tmp/
scp C:\Temp\srv-dc2.cer admin@192.168.20.63:/tmp/
```

Sur **SRV-NEXTCLOUD**, convertissez les certificats au format attendu (PEM), déclarez-les comme autorités de confiance et redémarrez PHP-FPM pour qu'il en tienne compte :

TERMINAL

```
cd /tmp
openssl x509 -inform der -in srv-dc1.cer -out srv-dc1.crt
openssl x509 -inform der -in srv-dc2.cer -out srv-dc2.crt
sudo cp srv-dc1.crt srv-dc2.crt /usr/local/share/ca-certificates/
sudo update-ca-certificates
sudo systemctl restart php8.4-fpm
```

1 Installez l'outil de test LDAP et vérifiez la chaîne complète : certificat accepté, puis recherche de l'utilisateur **amartin** avec le compte de service (le mot de passe de **svc-nextcloud** est demandé) :

TERMINAL

```
sudo apt install -y ldap-utils
openssl s_client -connect srv-dc1.sio.local:636 -verify_return_error \
    </dev/null 2>&1 | grep -E 'subject=|Verify return code'
ldapsearch -H ldaps://srv-dc1.sio.local \
    -D "CN=svc-nextcloud,OU=Comptes de service,DC=sio,DC=local" -W \
    -b "OU=Utilisateurs,DC=sio,DC=local" "(sAMAccountName=amartin)" dn mail
```

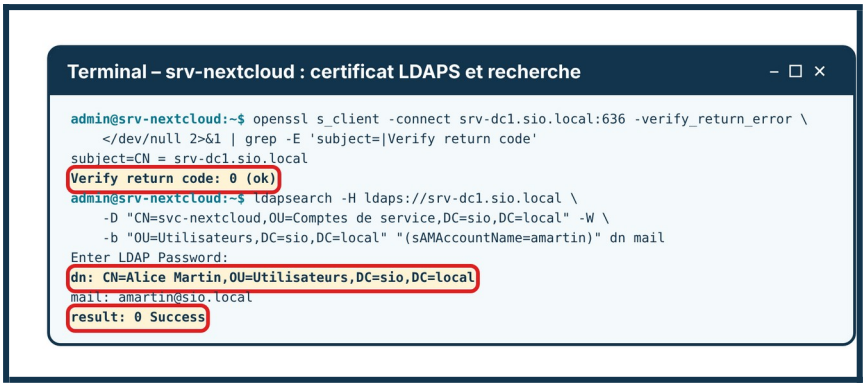


Figure 12 – Debian : confiance dans le certificat et recherche LDAPS

À SAVOIR

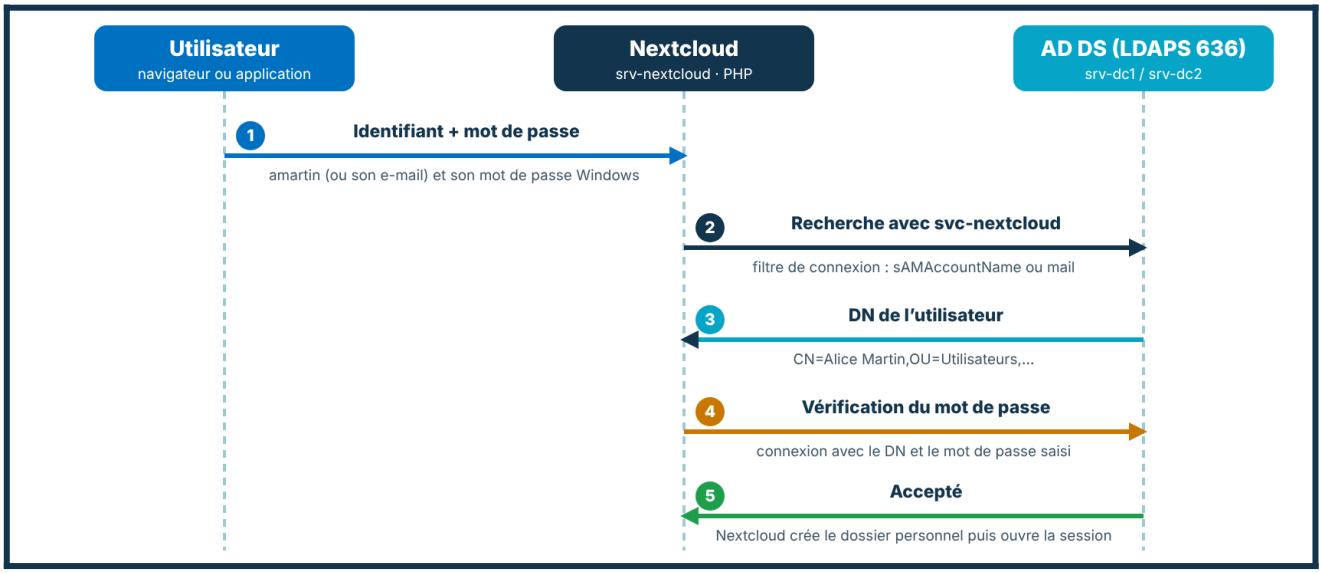
« Verify return code: 0 (ok) » prouve que Debian fait confiance au certificat. « result: 0 Success » et la ligne `dn:` prouvent que le compte de service, le DN de base et LDAPS fonctionnent. Répétez les deux premières commandes avec `srv-dc2.sio.local`.

✔ **POINT DE CONTRÔLE**

- Les OU **Utilisateurs**, **Groupes** et **Comptes de service**, le compte **svc-nextcloud**, les utilisateurs **amartin** et **bdurand** et les deux groupes existent
- Chaque contrôleur présente un certificat à son nom : « Verify return code: **0 (ok)** » pour `srv-dc1` et `srv-dc2`
- `ldapsearch` en **ldaps://** renvoie l'entrée de **Alice Martin** (« result: 0 Success »)

06 ÉTAPE 6 SUR 6
Lier Nextcloud à l'annuaire et se connecter

Tout est prêt : on active l'application LDAP de Nextcloud, on déclare l'annuaire dans son assistant, on teste, puis on se connecte avec un compte Windows. Voici ce qui se passe quand un utilisateur de l'annuaire se connecte :



A – Activer l'application « Intégration LDAP/AD »

L'application est livrée avec Nextcloud mais **désactivée**. Activez-la en une commande (ou dans le menu de l'avatar > « Applications » > « Applications désactivées ») :

```
TERMINAL
sudo occ app:enable user_ldap
sudo occ app:list | grep user_ldap
```

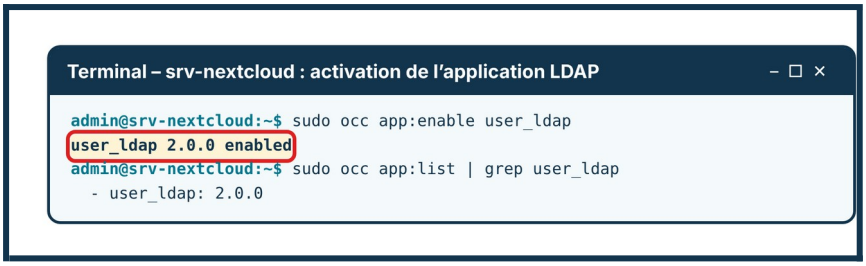


Figure 13 – Activation de l'application LDAP

À SAVOIR

Un nouveau menu « Intégration LDAP/AD » apparaît dans les paramètres d'administration. Déconnectez-vous puis reconnectez-vous en **admin** s'il n'est pas visible.

B – Déclarer l'annuaire AD DS dans l'assistant

Ouvrez « **Paramètres d'administration** » puis « **Intégration LDAP/AD** ». L'assistant se déroule en quatre onglets (**Serveur**, **Utilisateurs**, **Attributs de connexion**, **Groupes**) ; chaque champ est enregistré dès que vous le quittez, et le message en bas de page indique si la configuration est correcte (« Configuration OK »). Cliquez « **Continuer** » pour passer à l'onglet suivant.

Onglet Serveur — saisissez l'hôte en **ldaps://**, le port, le compte de service et le DN de base :

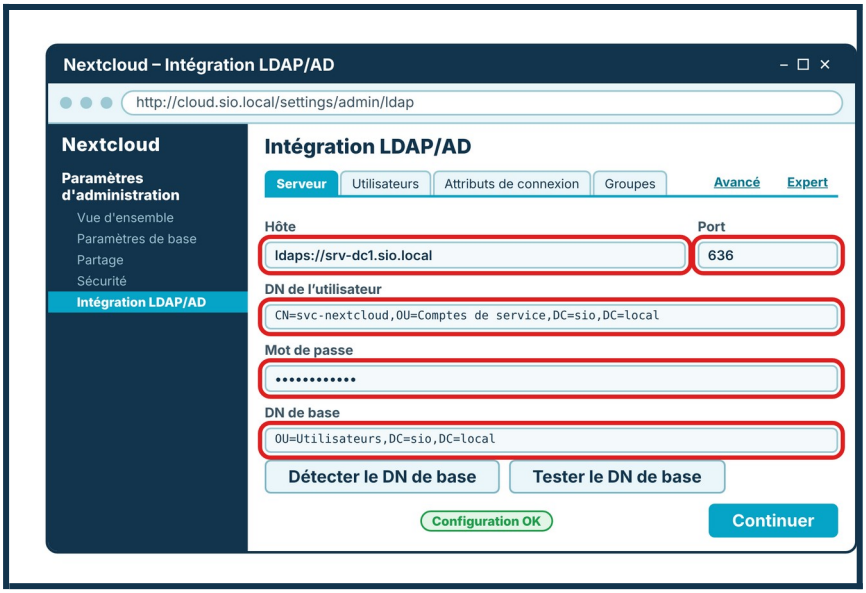


Figure 14 – Intégration LDAP/AD : onglet Serveur

À SAVOIR

Le DN de l'utilisateur est le DN **complet** du compte de service. Le bouton « Détecter le DN de base » propose la racine du domaine ; remplacez-la par l'OU des utilisateurs pour ne présenter à Nextcloud que les comptes voulus. « Tester le DN de base » doit répondre sans erreur.

Champ	Valeur à saisir	Remarque
Hôte	`ldaps://srv-dc1.sio.local`	Le préfixe **ldaps://** active le chiffrement ; utilisez le **nom complet** du contrôleur
Port	`636`	Port LDAPS (389 = LDAP non chiffré)
DN de l'utilisateur	`CN=svc-nextcloud,OU=Comptes de service,DC=sio,DC=local`	DN complet du compte de service
Mot de passe	mot de passe de **svc-nextcloud**	Stocké dans la configuration de Nextcloud
DN de base	`OU=Utilisateurs,DC=sio,DC=local`	Où chercher : seuls les comptes de cette OU sont visibles

Onglet Utilisateurs — Nextcloud propose les classes d'objets de l'annuaire (choisissez **user**). Cochez « **Modifier la requête LDAP** » et remplacez le filtre par celui-ci, qui ne retient que les **vrais comptes utilisateurs actifs** :

```
(&(objectClass=user)(objectCategory=person)(!
(userAccountControl:1.2.840.113556.1.4.803:=2)))
```

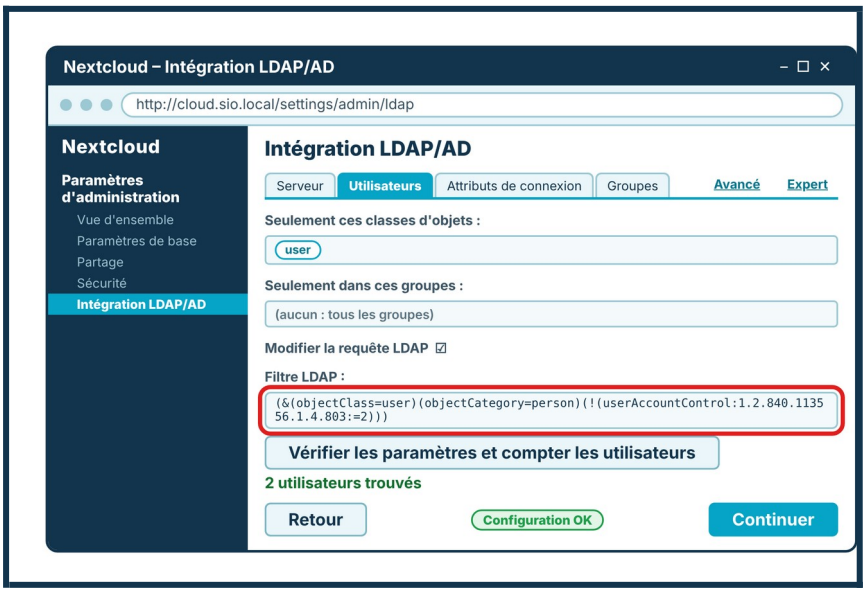


Figure 15 – Intégration LDAP/AD : onglet Utilisateurs

À SAVOIR

Le bit **2** de `userAccountControl` signifie « compte désactivé » : Nextcloud ne filtre pas lui-même les comptes désactivés d'Active Directory, ce filtre s'en charge. Cliquez « Vérifier les paramètres et compter les utilisateurs » : le nombre doit correspondre à votre annuaire (**2** ici).

Onglet Attributs de connexion — indiquez comment les utilisateurs saisissent leur identifiant : cochez « **Nom d'utilisateur LDAP** » (sAMAccountName, détecté automatiquement) et « **Adresse e-mail LDAP** » : ils pourront se connecter avec **amartin** ou avec **amartin@sio.local**. Pour tester, saisissez un identifiant dans « Nom de connexion à tester » :

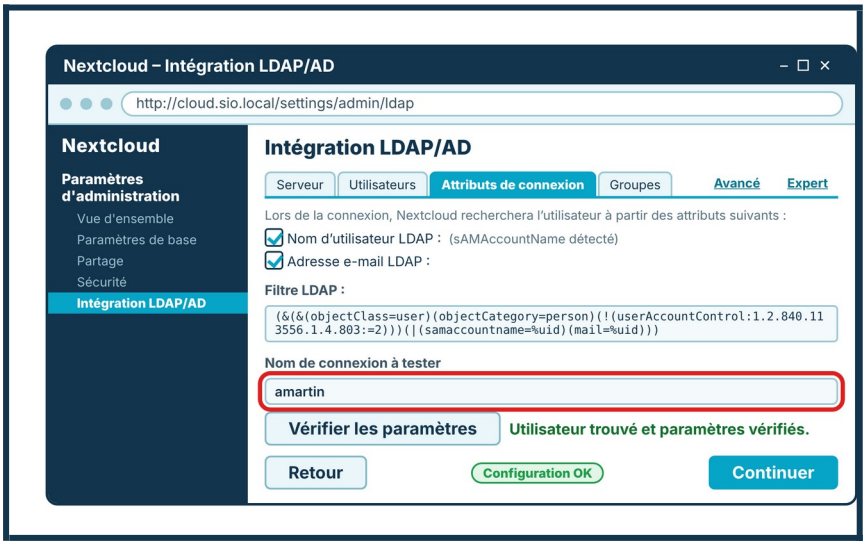


Figure 16 – Intégration LDAP/AD : onglet Attributs de connexion

À SAVOIR

Le filtre de connexion est construit à partir du filtre des utilisateurs : un compte désactivé ne peut donc pas ouvrir de session. Le message « Utilisateur trouvé et paramètres vérifiés » valide le tout.

Onglet Groupes — choisissez la classe **group**, puis sélectionnez dans « Seulement dans ces groupes » les deux groupes **GRP-Direction** et **GRP-Technique** (limiter les groupes évite d'importer tous les groupes de Windows, ce qui alourdirait Nextcloud) :

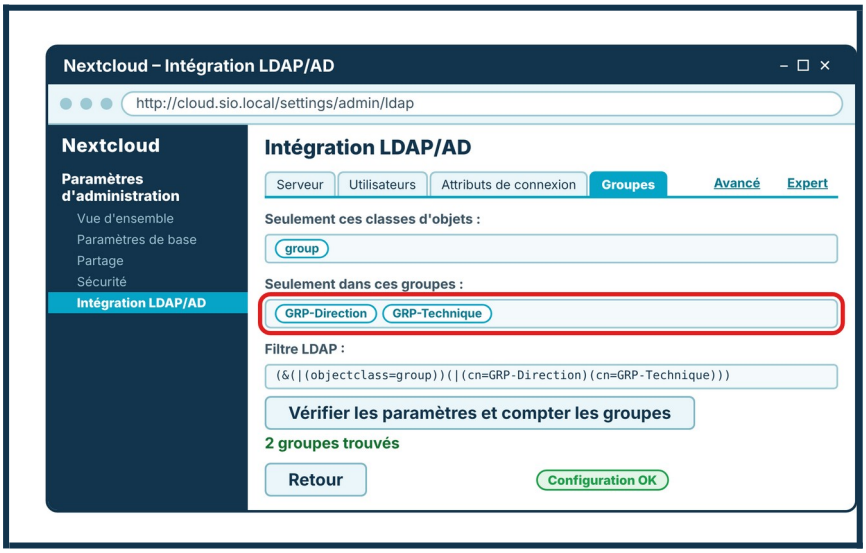


Figure 17 – Intégration LDAP/AD : onglet Groupes

À SAVOIR

Cliquez « Vérifier les paramètres et compter les groupes » : le message « 2 groupes trouvés » confirme la sélection. Les groupes de l'annuaire servent ensuite à partager un dossier ou à fixer des quotas.

C – Choisir le nom d'utilisateur interne et ajouter le second contrôleur

Avant la première connexion d'un utilisateur, ouvrez le lien « **Expert** » en haut de l'assistant. Par défaut, Nextcloud nomme chaque utilisateur d'après son identifiant unique (**objectGUID**) : un long nom illisible qui apparaîtrait dans les fichiers, les journaux et les liens de partage. Choisissez plutôt **samaccountname** :

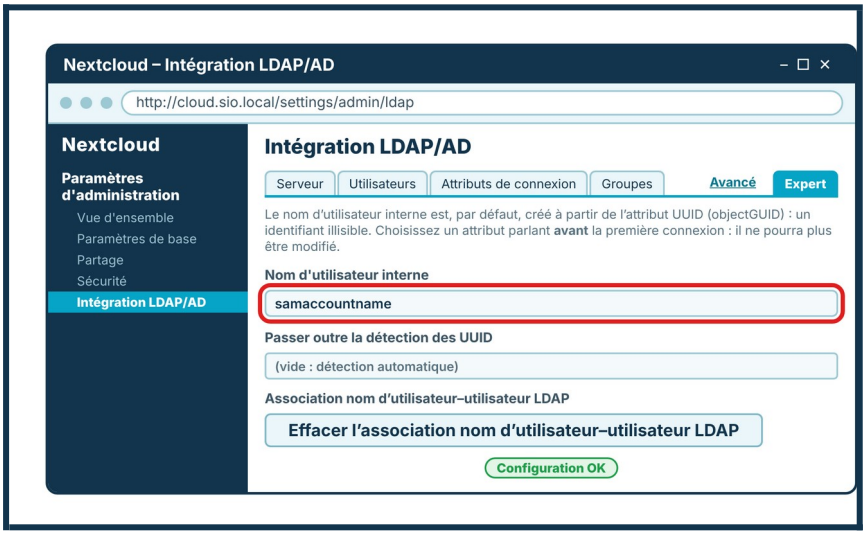


Figure 18 – Intégration LDAP/AD : onglet Expert

À SAVOIR

Ce réglage **ne doit plus changer** une fois des utilisateurs connectés : le bouton « Effacer l'association nom d'utilisateur–utilisateur LDAP » casse le lien avec les comptes et leurs données, ne l'utilisez que sur une installation vierge.

1. Pour la **tolérance de panne**, ajoutez SRV-DC2 comme **hôte de secours** : si SRV-DC1 ne répond plus, Nextcloud interroge SRV-DC2. L'assistant le propose dans l'onglet « **Avancé** » (rubrique « Paramètres de connexion », champs « Hôte de sauvegarde (réplique) » et « Port du serveur de sauvegarde ») ; la ligne de commande est équivalente et plus sûre :

TERMINAL

```
sudo occ ldap:set-config s01 ldapBackupHost ldaps://srv-dc2.sio.local
sudo occ ldap:set-config s01 ldapBackupPort 636
sudo occ ldap:set-config s01 ldapExpertUsernameAttr samaccountname
```

`s01` est le nom de la première configuration créée par l'assistant. La commande `sudo occ ldap:show-config s01` affiche toutes ses valeurs.

D – Tester l'annuaire en ligne de commande

Avant de se connecter, quatre commandes vérifient la configuration sans passer par le navigateur : le test global, la recherche d'un utilisateur, la recherche de groupes et l'état d'un compte :

```
TERMINAL
sudo occ ldap:test-config s01
sudo occ ldap:search "martin"
sudo occ ldap:search --group "GRP"
sudo occ ldap:check-user amartin
```

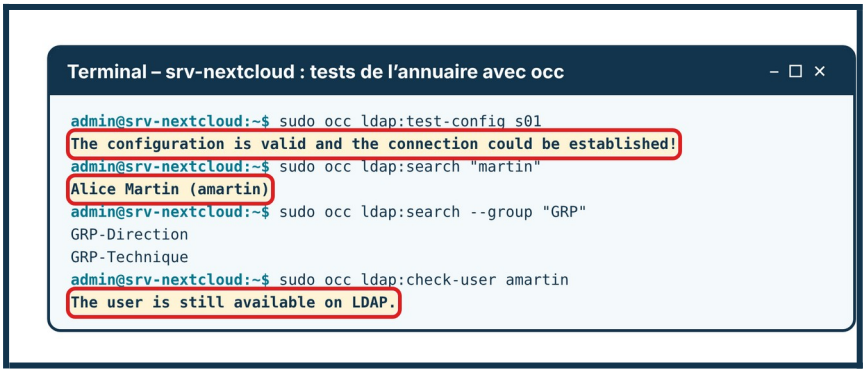


Figure 19 – Tests de l'annuaire avec occ

À SAVOIR

Si le test échoue, le message donne la cause : serveur injoignable (certificat, nom, port) ou identifiants refusés. Reportez-vous au tableau de dépannage en fin de tutoriel.

E – Se connecter avec un compte Windows

1. Connecté en **admin**, ouvrez le menu de l'avatar puis « **Comptes** » : les utilisateurs de l'annuaire y figurent, avec leurs groupes et la mention « jamais » en dernière connexion :



Figure 20 – Comptes : utilisateurs et groupes de l'annuaire

À SAVOIR

Ces comptes sont créés par l'annuaire : leur mot de passe se change dans Active Directory, pas dans Nextcloud. Le quota « Illimité » se règle par compte ou par groupe.

2 Déconnectez-vous de Nextcloud, puis ouvrez la page de connexion dans une **fenêtre de navigation privée** : saisissez **amartin** (ou son adresse e-mail) et son mot de passe de domaine. Le dossier personnel est créé à la première connexion :

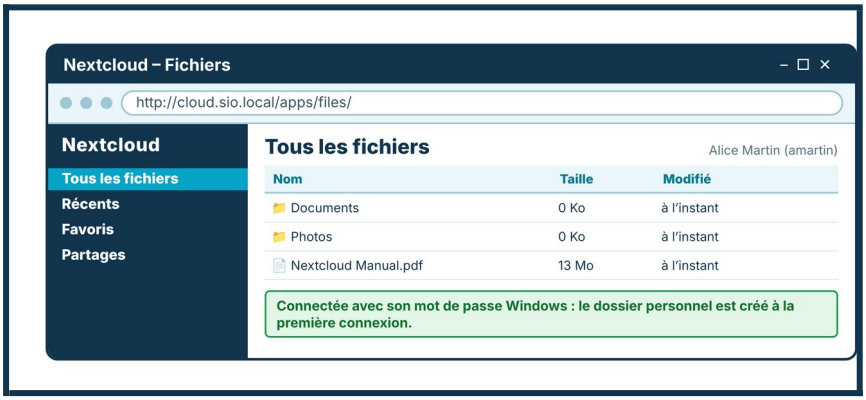


Figure 21 – Fichiers de l'utilisateur Alice Martin

À SAVOIR

Le mot de passe n'est jamais copié dans Nextcloud : à chaque connexion, Nextcloud le fait vérifier par l'annuaire. Désactiver le compte dans Active Directory suffit donc à lui retirer l'accès (ses fichiers restent sur le serveur).

3 **Pour aller plus loin** : `sudo occ ldap:show-remnants` liste les utilisateurs supprimés de l'annuaire dont les données sont encore présentes sur le serveur, et `sudo occ ldap:test-user-settings amartin` détaille ce que Nextcloud voit pour un utilisateur

✔ POINT DE CONTRÔLE

- La **Vue d'ensemble** est verte et l'application **Intégration LDAP/AD** est active
- `sudo occ ldap:test-config s01` répond que la configuration est **valide**
- **amartin** ouvre une session Nextcloud avec son **mot de passe Windows**, sous le nom `amartin`
- Si SRV-DC1 est arrêté, la connexion fonctionne encore grâce à **SRV-DC2**

Notre Nextcloud est **opérationnel** : installé en natif sur Debian 13, accéléré par des caches, tâches de fond planifiées, et relié à AD DS en LDAPS avec un second contrôleur en secours. Il reste à le publier en HTTPS, à organiser les dossiers partagés par groupe et à prévoir les sauvegardes.

Dépannage : les symptômes les plus fréquents

Symptôme	Cause probable	Solution
« Accès via un domaine non approuvé »	Le nom saisi n'est pas dans `trusted_domains`	`sudo occ config:system:set trusted_domains 1 --value=cloud.sio.local`
Page « Apache2 Debian Default Page »	Le site par défaut est resté actif	`sudo a2dissite 000-default && sudo a2ensite nextcloud && sudo systemctl reload apache2`
Erreur 500 ou page blanche	Erreur PHP, de droits ou de configuration	`sudo tail -n 30 /srv/nextcloud-data/nextcloud.log` et `/var/log/apache2/nextcloud-error.log`
Le navigateur télécharge ou affiche le code PHP	PHP-FPM n'est pas relié à Apache	Vérifier `proxy_fcgi` activé et le `SetHandler` du site ; `systemctl status php8.4-fpm`
`occ` **: « Console has to be executed with the user that owns the file config/config.php »**	Commande lancée avec un autre utilisateur que www-data	Toujours passer par le script : `sudo occ …`
Vue d'ensemble : tâches d'arrière-plan jamais exécutées	Cron absent ou mal formé	Fichier `/etc/cron.d/nextcloud` en 644, propriétaire root, saut de ligne final ; tester `sudo -u www-data php -f /var/www/nextcloud/cron.php`
Test LDAP : « Can't contact LDAP server »	Certificat non reconnu, nom différent du certificat ou port 636 bloqué	Refaire l'étape 5-C ; utiliser le **nom complet** du contrôleur, pas son adresse IP ; `sudo systemctl restart php8.4-fpm` ; au besoin, ajouter `TLS_CACERT /etc/ssl/certs/ca-certificates.crt` dans `/etc/ldap/ldap.conf`
`ldapsearch` **: « Strong(er) authentication required »**	Connexion LDAP non chiffrée refusée par Windows Server 2025	Utiliser `ldaps://` et le port **636**, jamais `ldap://` avec mot de passe
« Invalid credentials » (code 49)	DN du compte ou mot de passe incorrect, compte désactivé	Saisir le **DN complet** du compte ; tester `ldapsearch -W` ; vérifier `Get-ADUser svc-nextcloud`
« 0 utilisateur trouvé »	DN de base incorrect ou filtre trop restrictif	Comparer avec `Get-ADUser -SearchBase` ; contrôler la casse et les virgules du DN de base
Un utilisateur de l'annuaire ne peut pas se connecter	Compte hors du DN de base, désactivé, ou filtre de connexion incorrect	Contrôler son OU et son état ; relancer « Vérifier les paramètres » (onglet Attributs de connexion)
Les utilisateurs ont un nom illisible (suite de chiffres et de lettres)	Nom d'utilisateur interne laissé sur l'UUID avant la première connexion	Installation vierge : régler **samaccountname** (étape 6-C) puis effacer l'association ; sinon, conserver l'existant

Pense-bête : où regarder

Où / commande	Utilité
Paramètres d'administration > Vue d'ensemble	Contrôles de santé de Nextcloud, avec la cause et le correctif de chaque alerte
Paramètres d'administration > Intégration LDAP/AD	Assistant de l'annuaire : serveur, utilisateurs, connexion, groupes, avancé, expert
Avatar > Comptes	Liste des comptes et des groupes, quotas, dernière connexion
`/srv/nextcloud-data/nextcloud.log`	Journal de Nextcloud (aussi dans Paramètres d'administration > Journalisation)
`/var/log/apache2/nextcloud-error.log`	Erreurs du serveur web pour le site Nextcloud
`/var/www/nextcloud/config/config.php`	Configuration, accès à la base et secrets : à sauvegarder
`/srv/nextcloud-data/`	Fichiers des utilisateurs : à sauvegarder avec la base (`mariadb-dump nextcloud`)
`sudo occ maintenance:mode --on` / `--off`	Passer en maintenance avant une sauvegarde ou une mise à jour
`sudo occ ldap:show-config s01`	Afficher la configuration de l'annuaire (sans le mot de passe)
`openssl s_client -connect <contrôleur>:636`	Vérifier le certificat LDAPS présenté par un contrôleur
`ldapsearch -H ldaps://… -D … -W`	Tester l'annuaire sans passer par Nextcloud