PortailSIO

NOUVELLE FORMULE

TUTORIEL

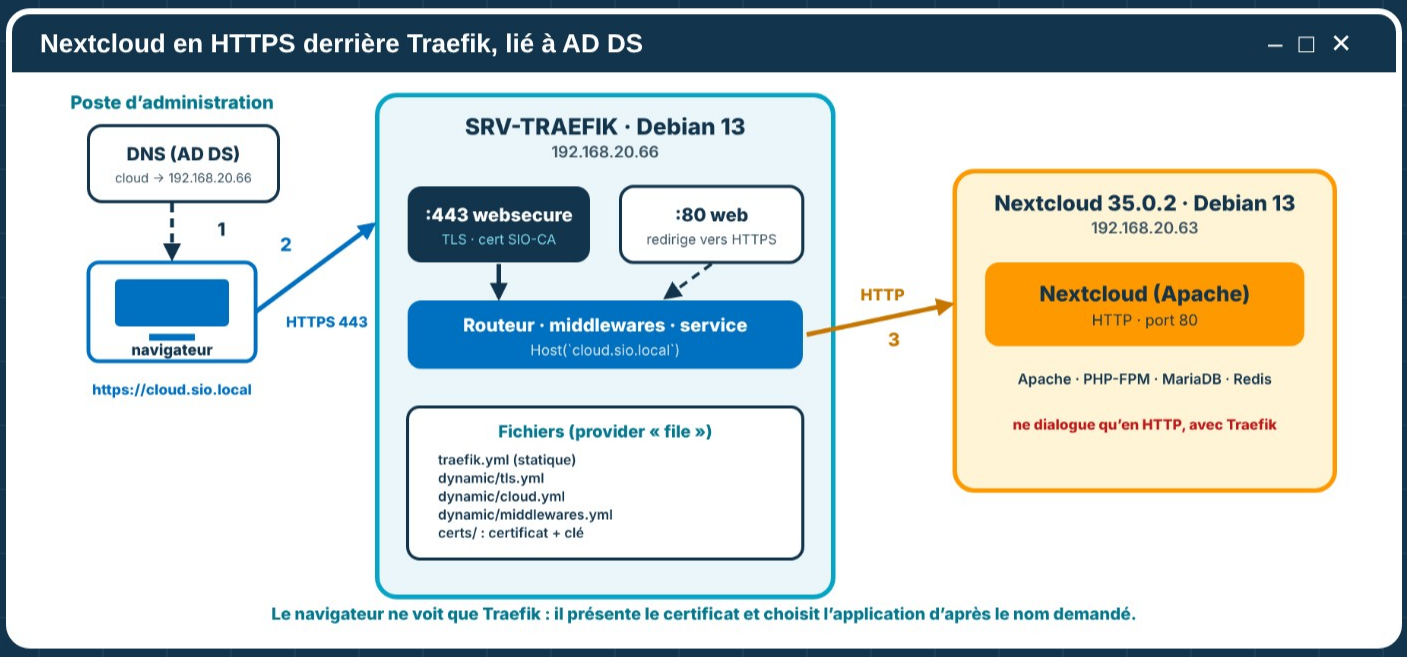
DEBIAN 13 · TRAEFIK 3.7 · HTTPS

Installer derrière Traefik

NEXTCLOUD



NIVEAU
Expert



1 Préparer les deux serveurs et le DNS

2 Installer Nextcloud en natif sur Debian 13

3 Installer Traefik et obtenir le certificat

4 Publier Nextcloud avec les fichiers dynamiques de Traefik

5 Adapter Nextcloud au proxy et l'optimiser

6 Lier Nextcloud à l'annuaire AD DS

CC BY-NC

Utilisation commerciale interdite

© PortailSIO – 11/2026

Ce tutoriel en ligne

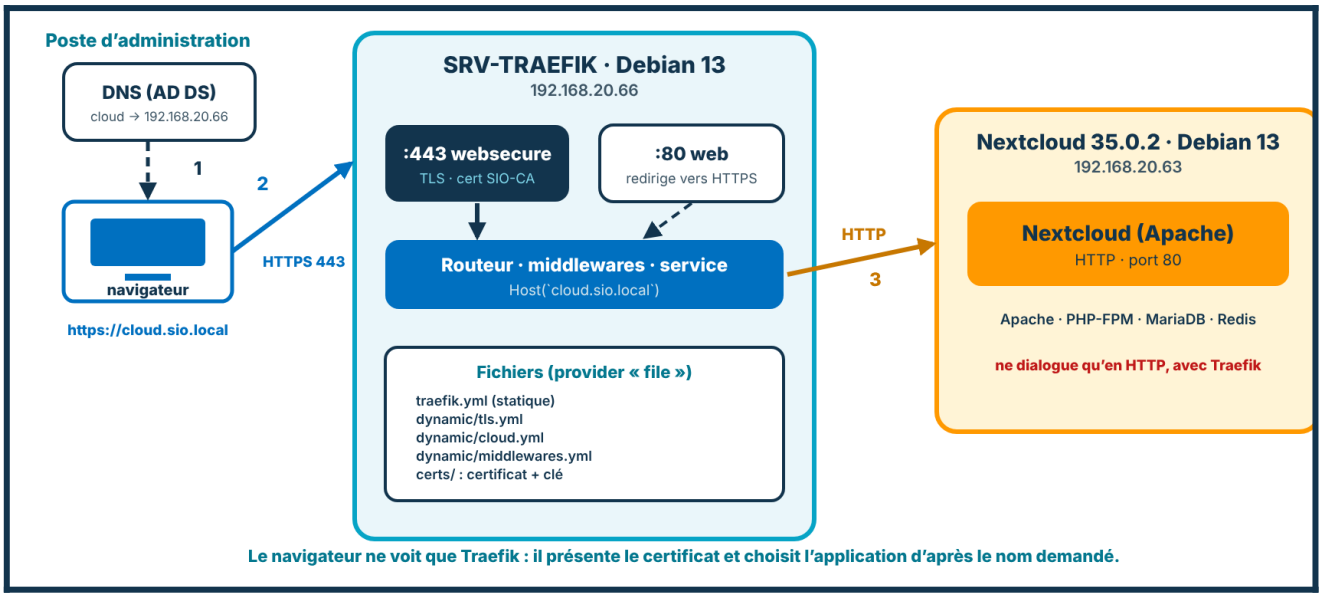
Scannez le QR code. Tous les tutoriels :

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 de deux machines virtuelles 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, avec l'autorité de certification **SIO-CA** et **LDAPS** activé : voir le tutoriel « Activer LDAPS sur AD DS »). Le tutoriel est de niveau **expert** : il demande d'être à l'aise avec Linux, le DNS et les certificats.

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. Ses utilisateurs y saisissent leurs identifiants et y déposent leurs documents : le site doit donc être servi en **HTTPS**, et non en HTTP simple.

Traefik est un **proxy inverse** (en anglais *reverse proxy*) : un serveur placé **devant** les applications, qui reçoit toutes les connexions des utilisateurs et les transmet à la bonne application. Il apporte trois choses. Il **chiffre** les échanges (c'est lui qui présente le certificat HTTPS), il **aiguille** chaque requête d'après le nom demandé (`cloud.sio.local`, `glpi.sio.local`…) et il ajoute des **protections** (en-têtes de sécurité, filtrage par adresse). Nextcloud n'a plus à gérer le HTTPS ni à être exposé aux utilisateurs.

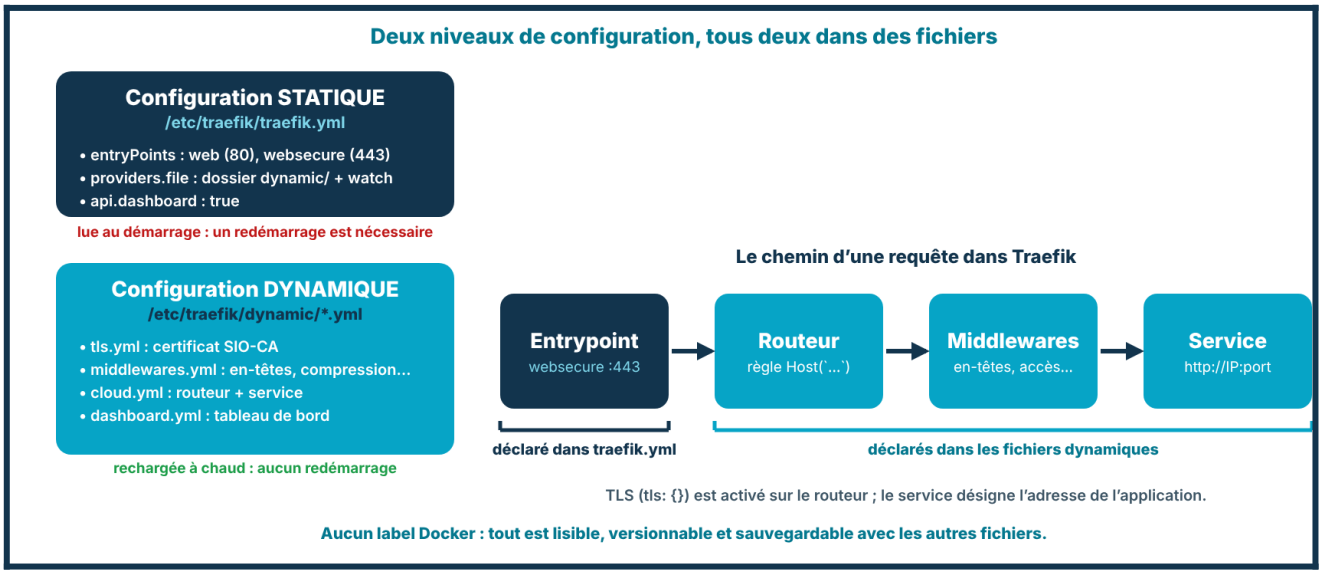


Le trajet d'une requête

- **1 – Le DNS** : le nom `cloud.sio.local` est déclaré dans l'annuaire AD DS et pointe vers l'adresse de **Traefik**, pas vers celle de Nextcloud
- **2 – HTTPS** : le navigateur se connecte à Traefik sur le port **443**. Traefik présente un certificat délivré par **SIO-CA**, auquel les postes du domaine font déjà confiance. Le port 80 existe aussi, mais il ne fait que renvoyer vers HTTPS
- **3 – HTTP** : Traefik transmet la requête à Apache sur SRV-NEXTCLOUD, en clair, sur le réseau des serveurs. Seul Traefik peut joindre Apache : nous fermerons l'accès direct à l'étape 5

La liaison avec l'annuaire (étape 6) est **indépendante** de Traefik : c'est SRV-NEXTCLOUD qui interroge directement les contrôleurs de domaine, par une connexion chiffrée **LDAPS**, pour vérifier le mot de passe de chaque utilisateur.

Traefik se configure avec **deux niveaux de fichiers**. La configuration **statique** (ports d'écoute, emplacement des autres fichiers) n'est lue qu'au démarrage. La configuration **dynamique** (certificats, routes, middlewares) est répartie en un **fichier par sujet** et rechargée à chaud. **Dans ce tutoriel, toute la configuration passe par ces fichiers : aucun label Docker n'est utilisé**, et Docker n'est d'ailleurs pas installé :



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-TRAEFIK	Proxy inverse Traefik (nom `srv-traefik`) : seul point d'entrée des utilisateurs	Debian 13	192.168.20.66
SRV-NEXTCLOUD	Serveur Nextcloud : Apache, PHP-FPM, MariaDB et Redis (nom `srv-nextcloud`)	Debian 13	192.168.20.63
SRV-DC1	Contrôleur de domaine, DNS, annuaire principal, autorité de certification SIO-CA	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 (DNS = les deux contrôleurs, poste membre du domaine, réseau 192.168.10.0 /24)	Windows 11	DHCP

Prévoyez **2 vCPU, 4 Go de mémoire et 30 Go de disque** pour SRV-NEXTCLOUD (davantage si les utilisateurs doivent y déposer beaucoup de fichiers : le dossier de données grandit avec eux), et **1 vCPU, 1 Go de mémoire et 10 Go de disque** pour SRV-TRAEFIK. 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**.

ÉTAPE 1 SUR 6

01 Préparer les deux serveurs et le DNS

Les utilisateurs ne connaîtront que **SRV-TRAEFIK** : les deux noms `cloud.sio.local` et `traefik.sio.local` désigneront son adresse. Chaque serveur reçoit un nom, une adresse fixe, le bon fuseau horaire et les DNS du domaine.

A – Préparer 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 (SRV-NEXTCLOUD)

```
sudo hostnamectl set-hostname srv-nextcloud
echo "192.168.20.63  srv-nextcloud.sio.local  srv-nextcloud" | sudo tee -a /etc/hosts
sudo timedatectl set-timezone Europe/Paris
```

3. Donnez au serveur une **adresse IP fixe** (adaptez le nom de la carte, ici `ens18`, avec `ip -br address`) : éditez `/etc/network/interfaces`, indiquez les DNS du domaine dans `/etc/resolv.conf`, puis redémarrez le réseau avec `sudo systemctl restart networking` :

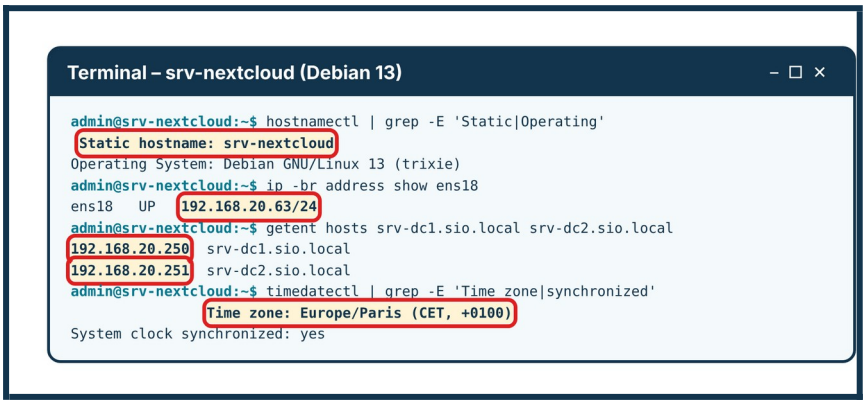
/etc/network/interfaces

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

/etc/resolv.conf

```
search sio.local
nameserver 192.168.20.250
nameserver 192.168.20.251
```

4. Vérifiez le résultat : nom, adresse IP, résolution DNS des contrôleurs, heure :



À SAVOIR

Si « System clock synchronized » indique « no », installez un service de temps (`sudo apt install -y chrony`). L'heure doit être juste : les certificats ont des dates de validité.

Figure 1 – Contrôle de la préparation de SRV-NEXTCLOUD

B – Déclarer les noms dans le DNS

Sur **SRV-DC1**, dans PowerShell (**administrateur**), créez les deux enregistrements. Ils pointent tous deux vers l'adresse de **Traefik** (192.168.20.66) ; l'enregistrement est répliqué sur SRV-DC2 avec la zone :

POWERSHELL (SRV-DC1)

```
Add-DnsServerResourceRecordA -ZoneName sio.local -Name cloud `
    -IPv4Address 192.168.20.66
Add-DnsServerResourceRecordA -ZoneName sio.local -Name traefik `
    -IPv4Address 192.168.20.66
Resolve-DnsName cloud.sio.local, traefik.sio.local -Type A | Select Name, Type, TTL,
IPAddress
```

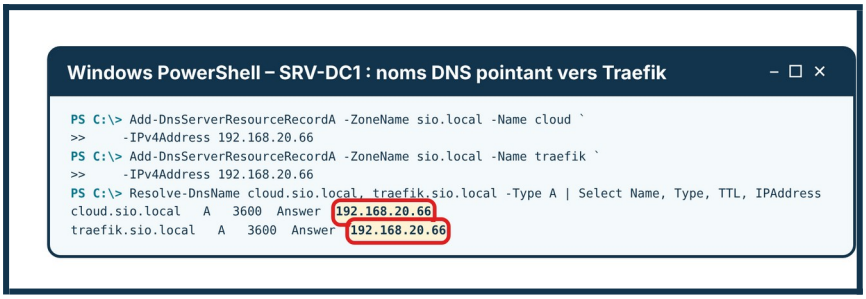


Figure 2 – PowerShell : noms DNS pointant vers Traefik

À SAVOIR

Le nom `cloud` désigne le **service** rendu aux utilisateurs, pas la machine qui l'héberge : si Nextcloud change de serveur un jour, seule la configuration de Traefik change, pas l'adresse que connaissent les utilisateurs.

À SAVOIR

Si un enregistrement `cloud` pointant vers **192.168.20.63** existe déjà (tutoriel « Installer Nextcloud et le lier à AD DS »), la commande `Add-` échoue ou crée un doublon. Supprimez d'abord l'ancien : `Remove-DnsServerResourceRecord -ZoneName sio.local -RRType A -Name cloud -Force`, puis recréez-le vers 192.168.20.66.

C – Préparer SRV-TRAEFIK

1 Sur **SRV-TRAEFIK**, mettez le système à jour (`sudo apt update && sudo apt full-upgrade -y`), nommez le serveur, réglez le fuseau et installez `curl` et `tree`, utiles pour les contrôles :

TERMINAL (SRV-TRAEFIK)

```
sudo hostnamectl set-hostname srv-traefik
echo "192.168.20.66  srv-traefik.sio.local  srv-traefik" | sudo tee -a /etc/hosts
sudo timedatectl set-timezone Europe/Paris
sudo apt install -y curl tree wget ca-certificates
```

2 Donnez-lui l'adresse **192.168.20.66** et les mêmes DNS que SRV-NEXTCLOUD, dans `/etc/network/interfaces` et `/etc/resolv.conf` (même méthode qu'au point A), puis redémarrez le réseau. Contrôlez le résultat, en particulier la résolution des deux noms :

/etc/network/interfaces

```
auto ens18
iface ens18 inet static
    address 192.168.20.66/24
    gateway 192.168.20.254
```



Figure 3 – Contrôle de la préparation de SRV-TRAEFIK

À SAVOIR

`getent hosts` interroge le DNS du domaine comme le ferait une application. Si les noms ne sont pas résolus, vérifiez `/etc/resolv.conf` et que les enregistrements existent sur SRV-DC1 (`Get-DnsServerResourceRecord -ZoneName sio.local -Name cloud`).

✔ POINT DE CONTRÔLE

- SRV-NEXTCLOUD répond au nom **srv-nextcloud** et à l'adresse **192.168.20.63**, SRV-TRAEFIK au nom **srv-traefik** et à **192.168.20.66**
- `cloud.sio.local` et `traefik.sio.local` sont résolus en **192.168.20.66** depuis SRV-TRAEFIK
- Le fuseau horaire est **Europe/Paris** et l'horloge est **synchronisée** sur les deux serveurs

02

ÉTAPE 2 SUR 6

Installer Nextcloud en natif sur Debian 13

Cette étape installe Nextcloud **35.0.2** sur **SRV-NEXTCLOUD**, comme dans le tutoriel « Installer Nextcloud et le lier à AD DS » ; seul l'essentiel est repris ici. À la fin, Nextcloud est installé mais ne répond qu'en HTTP : son adaptation au proxy est faite à l'étape 5. Toutes les commandes de cette étape s'exécutent sur **SRV-NEXTCLOUD**.

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 associé à **PHP-FPM**, un service PHP séparé plus rapide et mieux isolé que le module classique. Le serveur ne publiera que du HTTP : le HTTPS est l'affaire de Traefik.

TERMINAL (SRV-NEXTCLOUD)

```
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 (SRV-NEXTCLOUD)

```
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

1 Nextcloud demande plus de mémoire que la configuration par défaut de PHP, et un réglage précis du cache de code (OPcache). Créez `sudo nano /etc/php/8.4/fpm/conf.d/90-nextcloud.ini` : il fixe aussi la taille maximale des fichiers envoyés (1 Go ici) :

```
/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 (SRV-NEXTCLOUD)

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
```

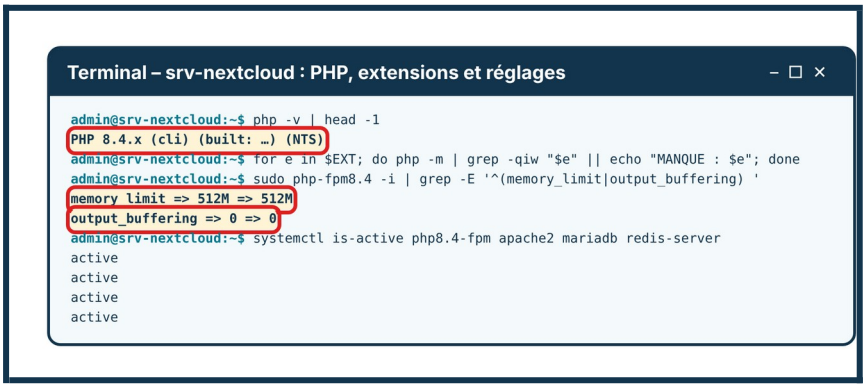


Figure 4 – PHP 8.4, extensions et réglages

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`.

C – Sécuriser MariaDB et créer la base

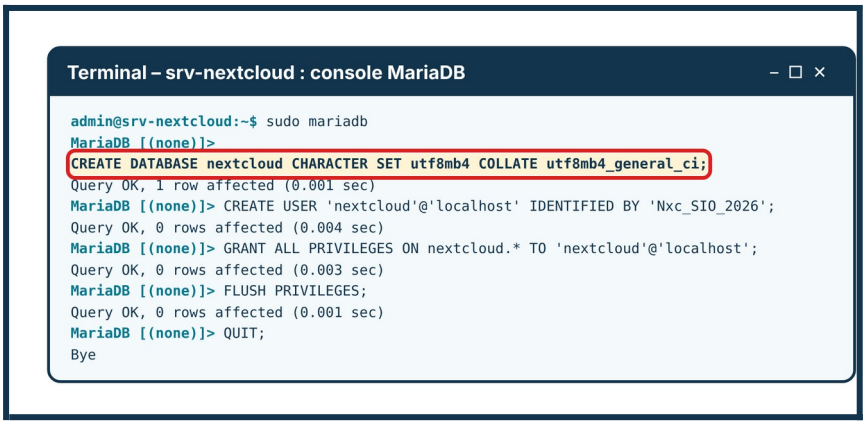
Debian 13 fournit **MariaDB 11.8**, que Nextcloud 35 prend en charge. Le service est déjà démarré : sécurisez-le, puis créez la base **nextcloud** et son utilisateur :

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 5 – 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, au point E ; Nextcloud le range ensuite dans son fichier `config/config.php`, lisible uniquement par `www-data`.

D – 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** :

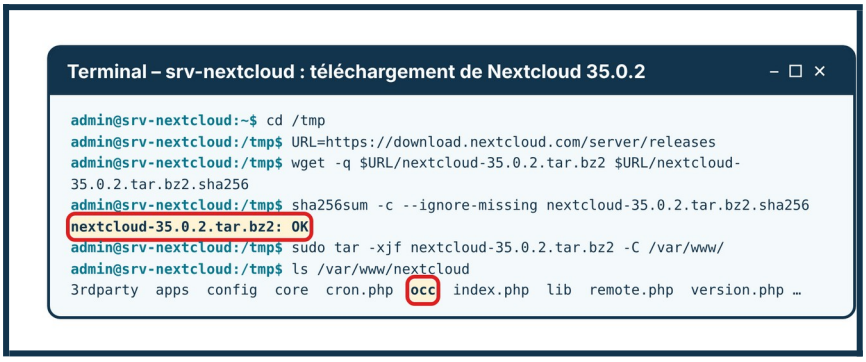
TERMINAL (SRV-NEXTCLOUD)

```
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 (SRV-NEXTCLOUD)

```
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
```



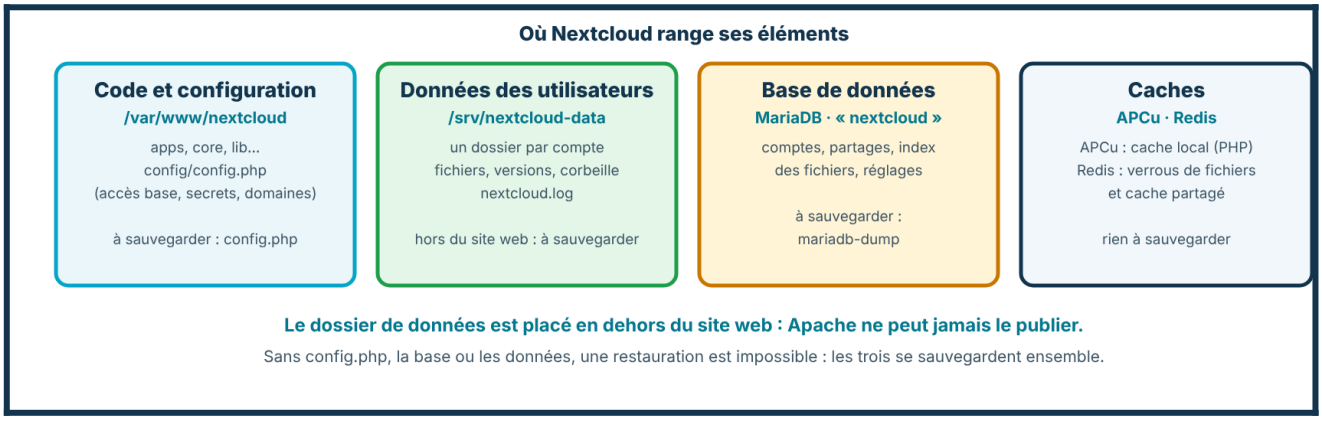
À SAVOIR

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.

Figure 6 – Téléchargement et contrôle de l'archive

E – Préparer les dossiers, les droits et installer avec 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 (SRV-NEXTCLOUD)

```
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. Créez 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 …`), puis installez Nextcloud **en une commande**, sans passer par l'assistant web : indiquez la base créée au point C, le compte administrateur et le dossier de données :

TERMINAL (SRV-NEXTCLOUD)

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



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.

Figure 7 – Installation en ligne de commande

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.

F – 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`). Traefik transmet à Apache le nom demandé par l'utilisateur : c'est donc bien `cloud.sio.local` :

TERMINAL (SRV-NEXTCLOUD)

```
sudo occ config:system:set trusted_domains 1 --value=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 (SRV-NEXTCLOUD)

```
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 (SRV-NEXTCLOUD)

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

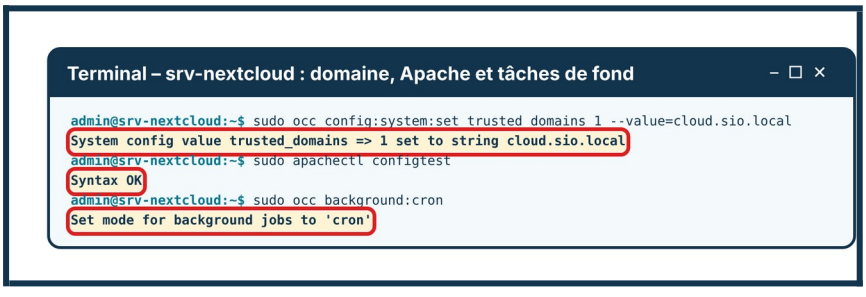
Enfin, Nextcloud doit exécuter régulièrement des tâches (nettoyages, notifications, indexation…). On les confie au planificateur du système, toutes les 5 minutes, plutôt qu'aux visites des utilisateurs. Créez `sudo nano /etc/cron.d/nextcloud` puis déclarez ce mode à Nextcloud :

/etc/cron.d/nextcloud

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

TERMINAL (SRV-NEXTCLOUD)

```
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.

Figure 8 – 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

03 ÉTAPE 3 SUR 6 Installer Traefik et obtenir le certificat

Traefik s'installe sur **SRV-TRAEFIK** : tout ce qui suit, jusqu'à l'étape 4 incluse, est exécuté sur cette machine (sauf indication contraire). L'installation se fait **en natif**, sans conteneur : un exécutable, un compte système et un service.

A – Télécharger et installer l'exécutable

Traefik est distribué sous la forme d'**un seul exécutable**, sans dépendance. On le télécharge depuis la page des versions du projet (GitHub), on vérifie son **empreinte** (somme de contrôle) puis on l'installe dans `/usr/local/bin`. Sur **SRV-TRAEFIK** :

TERMINAL

```
cd /tmp
V=3.7.16
URL=https://github.com/traefik/traefik/releases/download/v$V
wget -q $URL/traefik_v${V}_linux_amd64.tar.gz $URL/traefik_v${V}_checksums.txt
sha256sum -c --ignore-missing traefik_v${V}_checksums.txt
tar -xzf traefik_v${V}_linux_amd64.tar.gz traefik
sudo install -m 0755 traefik /usr/local/bin/traefik
traefik version | head -1
```



Figure 9 – Téléchargement, vérification et installation de Traefik 3.7.16

À SAVOIR

La ligne « OK » prouve que le fichier téléchargé n'a pas été altéré. Si la commande répond « No such file » ou « FAILED », vérifiez le numéro de version dans la page des versions du projet : les noms de fichiers en dépendent.

B – Créer l'utilisateur et les dossiers

1. Traefik ne doit pas tourner en `root` : on crée un compte système dédié, sans mot de passe ni interpréteur de commandes, et les trois dossiers de configuration (statique, dynamique, certificats) :

TERMINAL

```
sudo useradd --system --no-create-home --shell /usr/sbin/nologin traefik
sudo install -d -o traefik -g traefik /etc/traefik /etc/traefik/dynamic
sudo install -d -o traefik -g traefik /etc/traefik/certs /var/log/traefik
```

C – Écrire la configuration statique

La configuration de Traefik se compose de **deux parties**. La **statique** décrit les bases (ports d'écoute, d'où viennent les routes) et n'est lue qu'au démarrage. La **dynamique** décrit les routes, les certificats et les middlewares ; elle est lue dans des **fichiers** et rechargée **à chaud**. Créez `sudo nano /etc/traefik/traefik.yml` :

/etc/traefik/traefik.yml

```
entryPoints:
  web:
    address: ":80"
    http:
      redirections:
        entryPoint:
          to: websecure
          scheme: https
          permanent: true
  websecure:
    address: ":443"

providers:
  file:
    directory: /etc/traefik/dynamic
    watch: true

api:
  dashboard: true

log:
  level: INFO

accessLog:
  filePath: /var/log/traefik/access.log
```

Bloc	Rôle
`entryPoints`	Les ports d'écoute : **web** (80) redirige tout vers **websecure** (443, HTTPS)
`providers.file`	La source des routes : les fichiers du dossier `dynamic`, surveillés (`watch`) pour un rechargement à chaud
`api.dashboard`	Active le tableau de bord ; il sera publié par un routeur protégé (étape 5), pas sur un port ouvert
`accessLog`	Journal des requêtes, utile pour diagnostiquer une route

REMARQUE IMPORTANTE

Traefik offre aussi d'autres sources de configuration (notamment les **labels Docker**). Ici, **toute la configuration passe par des fichiers** : un fichier par application, lisible, comparable et sauvegardable comme n'importe quel autre fichier du serveur. Aucun accès au moteur Docker n'est donc nécessaire.

D – Créer le service systemd et le démarrer

1 Créez `sudo nano /etc/systemd/system/traefik.service` :

```
/etc/systemd/system/traefik.service
[Unit]
Description=Traefik (proxy inverse)
After=network-online.target
Wants=network-online.target

[Service]
User=traefik
Group=traefik
ExecStart=/usr/local/bin/traefik --configFile=/etc/traefik/traefik.yml
AmbientCapabilities=CAP_NET_BIND_SERVICE
NoNewPrivileges=true
Restart=on-failure
LimitNOFILE=65536

[Install]
WantedBy=multi-user.target
```

La ligne `AmbientCapabilities` autorise le compte `traefik` à ouvrir les ports **80 et 443** (ports réservés) sans être `root`. Activez et démarrez le service, puis contrôlez-le :

```
TERMINAL
sudo systemctl daemon-reload
sudo systemctl enable --now traefik
systemctl is-active traefik
sudo ss -tlnp | grep traefik
```

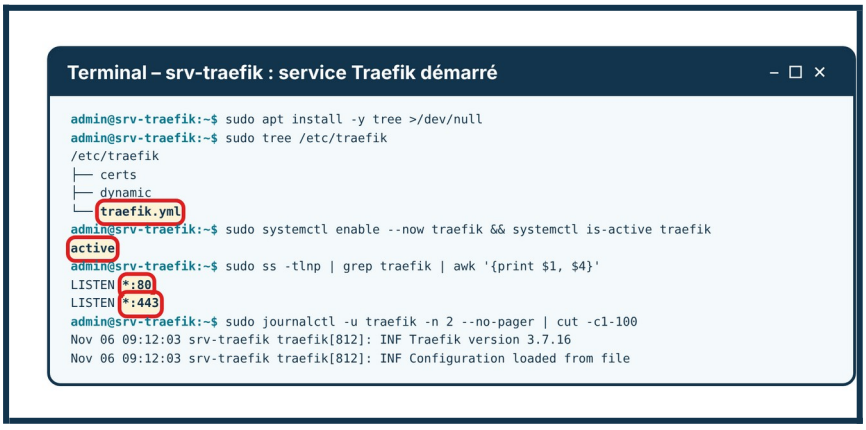


Figure 10 – Traefik démarré : arborescence et ports en écoute

À SAVOIR

À ce stade, le dossier `dynamic` est vide : Traefik répond « 404 page not found » à toute requête, ce qui est normal. En cas d'échec, `sudo journalctl -u traefik -n 20` indique la ligne du fichier YAML en cause (indentation, guillemets).

✔ POINT DE CONTRÔLE

- `sha256sum` affiche **OK** et `traefik version` indique **3.7.16**
- Le service **traefik** est « active » et écoute sur les ports **80** et **443**
- Les dossiers `/etc/traefik/dynamic` et `/etc/traefik/certs` existent et appartiennent à `traefik`

Les navigateurs n'acceptent un site HTTPS que si son certificat est délivré par une autorité **qu'ils connaissent**. Dans le domaine **sio.local**, c'est l'autorité interne **SIO-CA** (construite dans le tutoriel « Activer LDAPS sur AD DS ») : les postes Windows du domaine lui font déjà confiance. Nous allons lui demander un certificat pour **cloud.sio.local et traefik.sio.local**. La clé privée est créée sur **SRV-TRAEFIK** et ne le quitte jamais : seule la demande (CSR) voyage.

E – Créer la clé privée et la demande de certificat

1 Créez le fichier de description `sudo nano /tmp/cloud.cnf` : le certificat doit porter **tous les noms** utilisés (champ « Subject Alternative Name »), les navigateurs ignorant le nom principal seul :

/tmp/cloud.cnf

```
[req]
distinguished_name = dn
req_extensions = ext
prompt = no

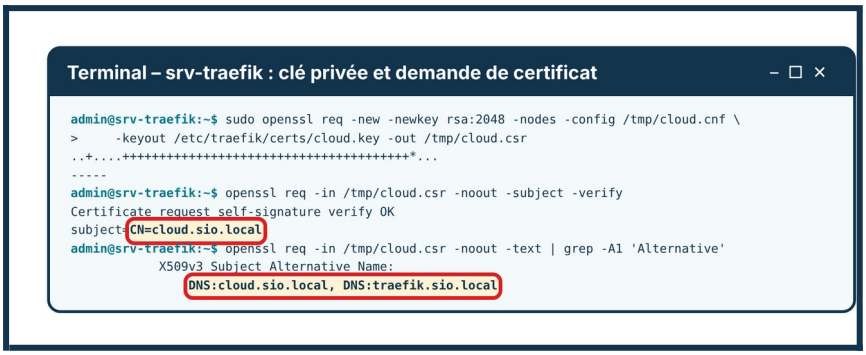
[dn]
CN = cloud.sio.local

[ext]
subjectAltName = DNS:cloud.sio.local, DNS:traefik.sio.local
```

2 Générez la clé privée (RSA 2048) et la demande de certificat, puis contrôlez le contenu de la demande :

TERMINAL

```
sudo openssl req -new -newkey rsa:2048 -nodes -config /tmp/cloud.cnf \
    -keyout /etc/traefik/certs/cloud.key -out /tmp/cloud.csr
openssl req -in /tmp/cloud.csr -noout -subject -verify
openssl req -in /tmp/cloud.csr -noout -text | grep -A1 Alternative
```



À SAVOIR

Le fichier `.key` est la clé privée : elle reste sur SRV-TRAEFIK, avec des droits restreints (voir plus bas). Le fichier `.csr` ne contient que la clé **publique** et les noms : il peut circuler librement.

Figure 11 – Clé privée et demande de certificat avec ses deux noms

F – Faire signer la demande par SIO-CA

Sur **SRV-DC1** (qui héberge l'autorité de certification), dans PowerShell ouvert **en tant qu'administrateur**, récupérez la demande, soumettez-la avec le modèle « **Serveur Web** » (nom interne `WebServer`) puis renvoyez le certificat obtenu vers SRV-TRAEFIK :

POWERSHELL

```
scp admin@192.168.20.66:/tmp/cloud.csr C:\Temp\
certreq -submit -config "SRV-DC1.sio.local\SIO-CA" `
    -attrib "CertificateTemplate:WebServer" `
    C:\Temp\cloud.csr C:\Temp\cloud.cer
scp C:\Temp\cloud.cer admin@192.168.20.66:/tmp/
```



Figure 12 – Signature de la demande par l'autorité SIO-CA

À SAVOIR

Si `certreq` répond « Refusé » ou « En attente », le modèle « Serveur Web » n'est pas activé sur l'autorité (console certsrv > Modèles de certificats > Nouveau > Modèle de certificat à délivrer) ou le compte n'a pas le droit « Inscrire » dessus.

G – Installer le certificat sur SRV-TRAEFIK

1 Convertissez le certificat reçu au format PEM, donnez la clé au compte `traefik` seul, puis vérifiez que le certificat correspond bien à la clé :

TERMINAL

```
sudo openssl x509 -in /tmp/cloud.cer -out /etc/traefik/certs/cloud.crt
sudo chown -R traefik:traefik /etc/traefik/certs
sudo chmod 600 /etc/traefik/certs/cloud.key
sudo openssl x509 -in /etc/traefik/certs/cloud.crt -noout -subject -issuer -enddate
sudo openssl x509 -in /etc/traefik/certs/cloud.crt -noout -ext subjectAltName
cmp <(sudo openssl x509 -in /etc/traefik/certs/cloud.crt -noout -pubkey) \
    <(sudo openssl pkey -in /etc/traefik/certs/cloud.key -pubout) \
    && echo "Clé et certificat correspondent"
```

À SAVOIR

Si OpenSSL répond « Could not read certificate » (ou « unable to load »), le fichier reçu est au format binaire : ajoutez l'option `-inform der` à la première commande.



Figure 13 – Certificat installé : émetteur, noms et correspondance avec la clé

À SAVOIR

Le certificat vaut deux ans environ (durée du modèle). Notez sa date de fin : **un certificat expiré rend le site inaccessible** (alerte du navigateur). Pour un renouvellement, répétez ces trois points puis remplacez les deux fichiers : Traefik les relit à chaud.

✔ POINT DE CONTRÔLE

- La demande `cloud.csr` contient les noms **cloud.sio.local** et **traefik.sio.local**
- SIO-CA a émis le certificat (« **Émis** ») et il est copié dans `/etc/traefik/certs`
- L'émetteur affiché est **SIO-CA** et la clé privée est lisible uniquement par `traefik`

ÉTAPE 4 SUR 6

04 Publier Nextcloud avec les fichiers dynamiques de Traefik

Nous créons maintenant les fichiers du dossier `/etc/traefik/dynamic`. Traefik les **surveille** : il charge chaque fichier dès qu'il est enregistré, sans redémarrage. Un fichier invalide est ignoré (et signalé dans le journal) : le reste de la configuration continue de fonctionner. Les trois premiers fichiers sont **communs** à toutes les applications que Traefik publiera un jour ; le dernier est propre à Nextcloud.

A – Déclarer le certificat et les options TLS

1 Créez `sudo nano /etc/traefik/dynamic/tls.yml` : il indique à Traefik le certificat à présenter (il choisit le bon d'après le nom demandé par le navigateur) et impose TLS 1.2 au minimum :

/etc/traefik/dynamic/tls.yml

```
tls:
  certificates:
    - certFile: /etc/traefik/certs/cloud.crt
      keyFile: /etc/traefik/certs/cloud.key
  options:
    default:
      minVersion: VersionTLS12
```

B – Créer les middlewares réutilisables

Un **middleware** modifie la requête ou la réponse au passage dans Traefik. On en déclare trois dans un fichier, que tous les routeurs pourront réutiliser. Créez `sudo nano /etc/traefik/dynamic/middlewares.yml` :

/etc/traefik/dynamic/middlewares.yml

```
http:
  middlewares:
    secure-headers:
      headers:
        stsSeconds: 31536000
        contentTypeNosniff: true
        referrerPolicy: same-origin
        customFrameOptionsValue: SAMEORIGIN
    compression:
      compress: {}
    admin-seulement:
      ipAllowList:
        sourceRange:
          - 192.168.20.0/24
          - 192.168.10.0/24
```

Middleware	Effet
`secure-headers`	Ajoute des en-têtes de sécurité : HSTS (le navigateur n'utilisera plus que HTTPS pendant un an), interdiction de deviner le type des fichiers, cadres limités au même site
`compression`	Compresse les réponses (pages plus légères sur le réseau)
`admin-seulement`	Autorise uniquement les adresses listées (`ipAllowList`) : à utiliser pour les interfaces d'administration

REMARQUE IMPORTANTE

Adaptez les réseaux de `sourceRange` : ils doivent contenir l'adresse du **poste d'administration** (ici 192.168.10.0/24, à remplacer par votre réseau), sinon vous ne pourrez plus ouvrir le tableau de bord. **Le HSTS est mémorisé un an par le navigateur** : ne l'activez pas sur un nom de domaine que vous pourriez devoir exposer un jour en HTTP.

C – Publier le tableau de bord de Traefik

1. Créez `sudo nano /etc/traefik/dynamic/dashboard.yml` : un routeur, réservé aux administrateurs, vers le service interne `api@internal` :

/etc/traefik/dynamic/dashboard.yml

```
http:
  routers:
    dashboard:
      rule: "Host(`traefik.sio.local`)"
      entryPoints:
        - websecure
      middlewares:
        - admin-seulement
        - secure-headers
      service: api@internal
      tls: {}
```

Un routeur associe trois éléments : une **règle** (`rule` : ici, le nom de site demandé), des **middlewares** (appliqués dans l'ordre) et un **service** (la destination). `tls: {}` active HTTPS sur ce routeur avec le certificat déclaré à l'étape A.

D – Publier Nextcloud

Un fichier par application : routeur, service (où se trouve Nextcloud) et un middleware qui renvoie `/.well-known/caldav` et `/.well-known/carddav`, adresses cherchées par les clients d'agenda et de contacts, vers `/remote.php/dav/`. Créez `sudo nano /etc/traefik/dynamic/cloud.yml` :

/etc/traefik/dynamic/cloud.yml

```
http:
  routers:
    cloud:
      rule: "Host(`cloud.sio.local`)"
      entryPoints: [websecure]
      middlewares: [secure-headers, cloud-dav]
      service: cloud
      tls: {}

  middlewares:
    cloud-dav:
      redirectRegex:
        regex: '^https://cloud\.sio\.local/\.well-known/(?:card|cal)dav$'
        replacement: "https://cloud.sio.local/remote.php/dav/"
        permanent: true

  services:
    cloud:
      loadBalancer:
        servers:
          - url: "http://192.168.20.63"
```

Élément	Signification
`rule`	Condition d'aiguillage : la requête est destinée à ce routeur si le nom de site demandé est `cloud.sio.local`
`entryPoints: websecure`	Le routeur n'écoute que sur le port 443 ; le port 80 ne fait que rediriger (configuration statique)
`middlewares`	Appliqués dans l'ordre : en-têtes de sécurité (défini dans `middlewares.yml`), puis redirection des adresses `.well-known` (défini plus bas dans le même fichier)
`redirectRegex`	Compare l'adresse complète demandée à l'expression régulière ; si elle correspond (`caldav` ou `carddav` exactement), renvoie vers `/remote.php/dav/`. Les autres adresses ne sont pas touchées
`loadBalancer.servers`	L'adresse d'Apache sur SRV-NEXTCLOUD. Une seule adresse ici ; en ajouter une deuxième répartirait la charge entre deux serveurs
`tls: {}`	Active HTTPS sur ce routeur avec le certificat déclaré dans `tls.yml`

REMARQUE IMPORTANTE

Nous n'appliquons pas le middleware `compression` à Nextcloud : la plupart des fichiers qu'il sert (images, archives, documents Office) sont **déjà compressés**, et Apache compresse lui-même les pages. Dans un fichier YAML, une **erreur d'indentation** change le sens du fichier ou l'invalide ; l'expression régulière est écrite entre **apostrophes**, ce qui conserve les barres obliques inverses (`\.`) telles quelles.

E – Contrôler les fichiers et le démarrage

1. Sur **SRV-TRAEFIK**, affichez l'arborescence de la configuration, les ports en écoute et le nombre d'erreurs du journal des cinq dernières minutes :

TERMINAL (SRV-TRAEFIK)

```
sudo tree /etc/traefik
sudo ss -tlnp | grep traefik | awk '{print $1, $4}'
sudo journalctl -u traefik --since "5 min ago" --no-pager | grep -ci error
```

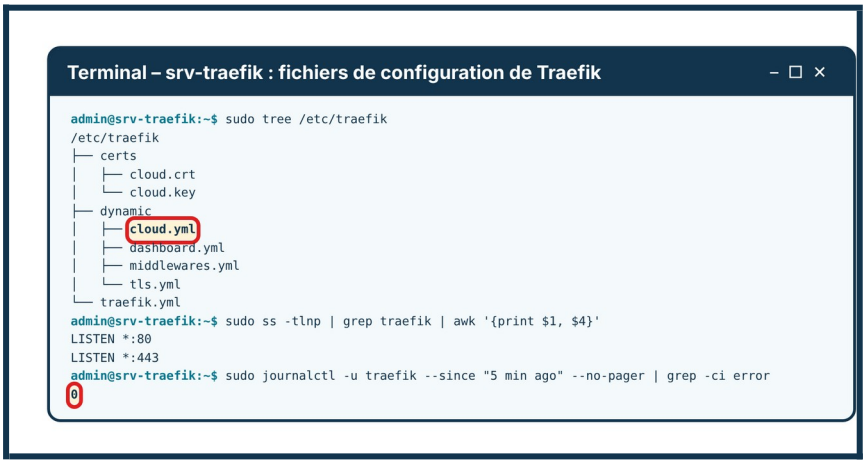


Figure 14 – Fichiers de configuration de Traefik

À SAVOIR

Un compteur différent de 0 indique un fichier mal formé : `sudo journalctl -u traefik -n 20` donne le nom du fichier et la ligne. Traefik n'a pas besoin d'être redémarré : les fichiers dynamiques sont rechargés à chaud.

F – Tester la chaîne en ligne de commande

Pour tester depuis SRV-TRAEFIK lui-même, ce serveur doit faire confiance à **SIO-CA** (les postes Windows du domaine lui font déjà confiance, pas Debian). Sur **SRV-DC1**, exportez le certificat de l'autorité et copiez-le :

POWERSHELL (SRV-DC1)

```
New-Item -ItemType Directory -Path C:\Temp -Force | Out-Null
certutil -ca.cert C:\Temp\sio-ca.cer
scp C:\Temp\sio-ca.cer admin@192.168.20.66:/tmp/
```

Sur **SRV-TRAEFIK**, convertissez-le au format PEM, ajoutez-le aux autorités de confiance du système et vérifiez le certificat de Traefik par rapport à ce magasin :

TERMINAL (SRV-TRAEFIK)

```
sudo openssl x509 -inform der -in /tmp/sio-ca.cer \
    -out /usr/local/share/ca-certificates/sio-ca.crt
sudo update-ca-certificates
openssl verify /etc/traefik/certs/cloud.crt
```



À SAVOIR

« OK » prouve que le certificat de Traefik est signé par SIO-CA. Si OpenSSL répond « Could not read certificate », le fichier exporté est déjà au format PEM : copiez-le simplement dans `/usr/local/share/ca-certificates/sio-ca.crt`.

Figure 15 – Confiance dans SIO-CA et vérification du certificat

1 Testez la redirection HTTP vers HTTPS, la redirection `.well-known` et le certificat présenté :

TERMINAL (SRV-TRAEFIK)

```
curl -sI http://cloud.sio.local | grep -iE '^(HTTP|location)'
curl -sI https://cloud.sio.local/.well-known/carddav | grep -iE '^(HTTP|location)'
curl -sv https://cloud.sio.local/ -o /dev/null 2>&1 \
    | grep -E 'subject:|issuer:|verify'
```



À SAVOIR

Le premier test montre le port 80 qui renvoie vers HTTPS ; le deuxième, l'adresse `.well-known` qui renvoie vers `/remote.php/dav/` (middleware `cloud-dav`) ; le troisième, l'émetteur du certificat. « 404 page not found » signale qu'aucun routeur ne correspond au nom demandé ; « 502 Bad Gateway », que Traefik n'atteint pas Apache.

Figure 16 – Redirections et certificat vus par curl

G – Ouvrir le tableau de bord de Traefik

Depuis le **poste d'administration** (membre du domaine), ouvrez `https://traefik.sio.local`. Le navigateur affiche le cadenas **sans avertissement** : il fait confiance à SIO-CA. Le tableau de bord liste les routeurs lus dans les fichiers :

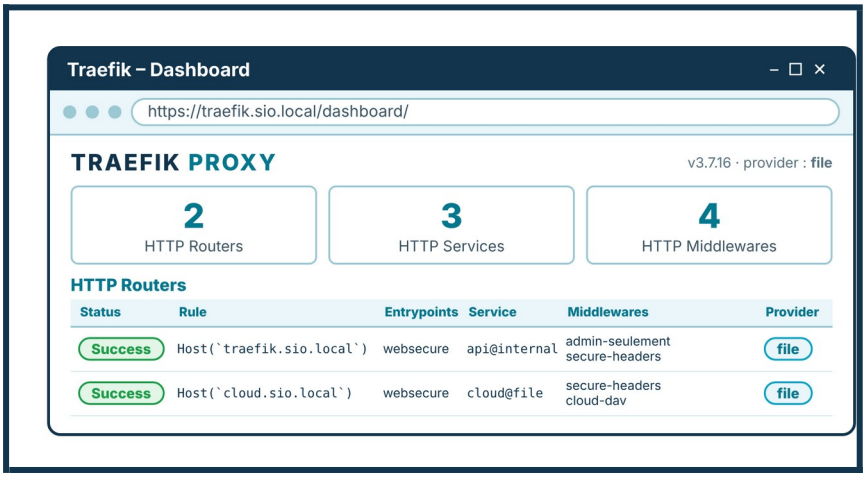


Figure 17 – Tableau de bord de Traefik : routeurs, services et middlewares

À SAVOIR

Un routeur « Success » est actif ; une erreur s'affiche en rouge avec sa cause. Le provider « file » rappelle que la configuration vient des fichiers. Un message « 403 Forbidden » signale que l'adresse du poste n'est pas dans `sourceRange` (middleware `admin-seulement`).

À SAVOIR

Un poste **hors domaine** n'a pas SIO-CA dans ses autorités de confiance : le navigateur affiche un avertissement. Importez le fichier `sio-ca.cer` dans les « Autorités de certification racines de confiance » du poste, ou déployez-le par GPO pour tous les postes du domaine.

✔ POINT DE CONTRÔLE

- Le dossier `/etc/traefik/dynamic` contient **tls.yml**, **middlewares.yml**, **dashboard.yml** et **cloud.yml**
- `openssl verify` répond **OK**, `curl` affiche **308** vers `https://cloud.sio.local/` et la redirection `.well-known` fonctionne
- Les réseaux de `sourceRange` incluent l'adresse du **poste d'administration**
- Le tableau de bord de Traefik affiche les routeurs **dashboard** et **cloud** en « Success »

05 ÉTAPE 5 SUR 6 — Adapter Nextcloud au proxy et l'optimiser

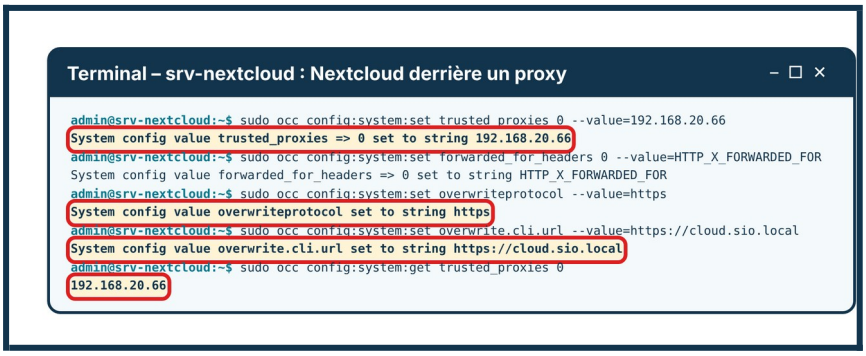
Traefik est en place : il reste à dire à Nextcloud qu'il est **derrière un proxy** (sans quoi il se croit en HTTP et ne reconnaît pas ses visiteurs), à lever une limite de Traefik qui gênerait les gros fichiers, à optimiser Nextcloud puis à fermer l'accès direct à Apache. Sauf indication contraire, les commandes s'exécutent sur **SRV-NEXTCLOUD**.

A – Déclarer Traefik comme proxy de confiance

Nextcloud reçoit désormais toutes ses requêtes **de Traefik**, en HTTP : sans réglage, il croit que ses visiteurs ont tous l'adresse 192.168.20.66, qu'ils utilisent HTTP, et il construit des liens `http://`. On lui indique donc quatre choses : l'adresse du proxy **de confiance**, l'en-tête dans lequel Traefik range l'adresse d'origine, le protocole réellement utilisé par les visiteurs et l'adresse publique du site :

TERMINAL (SRV-NEXTCLOUD)

```
sudo occ config:system:set trusted_proxies 0 --value=192.168.20.66
sudo occ config:system:set forwarded_for_headers 0 --value=HTTP_X_FORWARDED_FOR
sudo occ config:system:set overwriteprotocol --value=https
sudo occ config:system:set overwrite.cli.url --value=https://cloud.sio.local
sudo occ config:system:get trusted_proxies 0
```



À SAVOIR

Les valeurs sont enregistrées dans `config/config.php`. Le « 0 » désigne le premier élément d'une liste : on pourrait ajouter un second proxy avec l'indice 1. La dernière commande relit la valeur.

Figure 18 – Nextcloud derrière un proxy : réglages enregistrés

Réglage	Rôle
`trusted_proxies`	Liste des proxys **de confiance**. Nextcloud ne lit l'en-tête `X-Forwarded-For` que si la connexion vient de l'un d'eux : sans cette liste, n'importe quel client pourrait falsifier son adresse
`forwarded_for_headers`	En-tête transmis par Traefik contenant l'adresse du visiteur ; Nextcloud s'en sert pour ses journaux et pour la limitation des tentatives de connexion
`overwriteprotocol`	Force le protocole des liens et des redirections à `https`, même si la connexion reçue de Traefik est en HTTP
`overwrite.cli.url`	Adresse publique de Nextcloud, utilisée pour les liens créés hors navigateur (tâches de fond, notifications par e-mail)

B – Première connexion en HTTPS

Depuis le **poste d'administration**, ouvrez un navigateur et saisissez `https://cloud.sio.local`. La page de connexion de Nextcloud s'affiche, avec le cadenas : saisissez **admin** et le mot de passe choisi à l'étape 2-E.

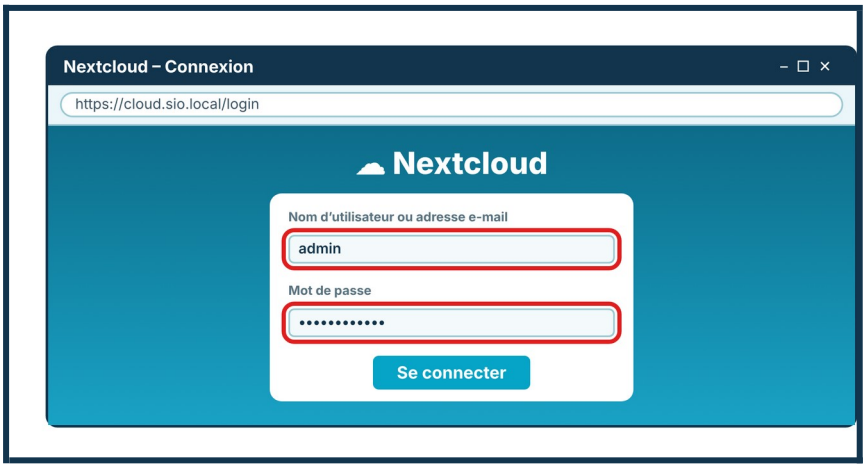


Figure 19 – Page de connexion de Nextcloud

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 2-F. 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 : vous pouvez la fermer.

C – Autoriser l'envoi de gros fichiers à travers Traefik

Par défaut, Traefik **interrompt** une requête dont la lecture dépasse **60 secondes** (réglage `readTimeout`) : l'envoi d'un gros fichier sur une liaison lente serait coupé avant la fin, alors que PHP accepte ici jusqu'à 1 Go. On supprime cette limite (valeur `0`) pour le port 443. C'est un réglage de la configuration **statique** : contrairement aux fichiers dynamiques, il n'est lu qu'au démarrage et demande un **redémarrage** de Traefik. Sur **SRV-TRAEFIK**, éditez `sudo nano /etc/traefik/traefik.yml` et complétez le point d'entrée **websecure** :

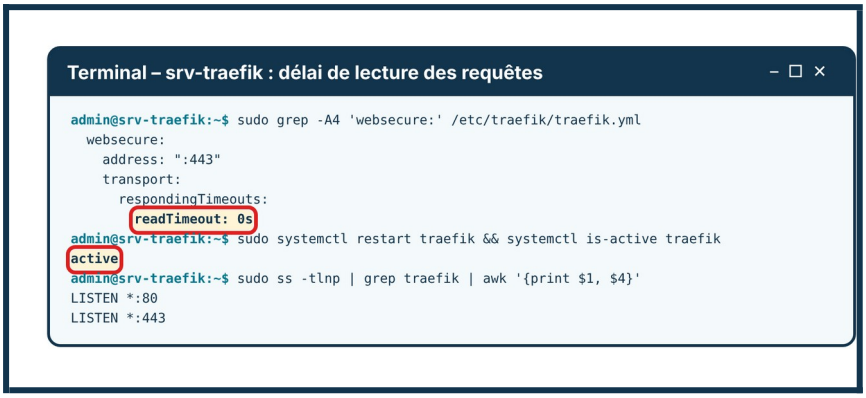
/etc/traefik/traefik.yml (extrait)

```
  websecure:
    address: ":443"
    transport:
      respondingTimeouts:
        readTimeout: 0s
```

1. Redémarrez Traefik (les fichiers dynamiques, eux, n'ont jamais besoin de cette opération) puis contrôlez le résultat :

TERMINAL (SRV-TRAEFIK)

```
sudo grep -A4 'websecure:' /etc/traefik/traefik.yml
sudo systemctl restart traefik && systemctl is-active traefik
sudo ss -tlnp | grep traefik | awk '{print $1, $4}'
```



À SAVOIR

Si Traefik ne redémarre pas, `sudo journalctl -u traefik -n 20` indique la ligne en cause : l'indentation du bloc `transport` doit être exactement celle de `address`. D'autres limites existent côté PHP (`upload_max_filesize`, `post_max_size`, étape 2-B) : elles doivent rester cohérentes avec la taille maximale voulue.

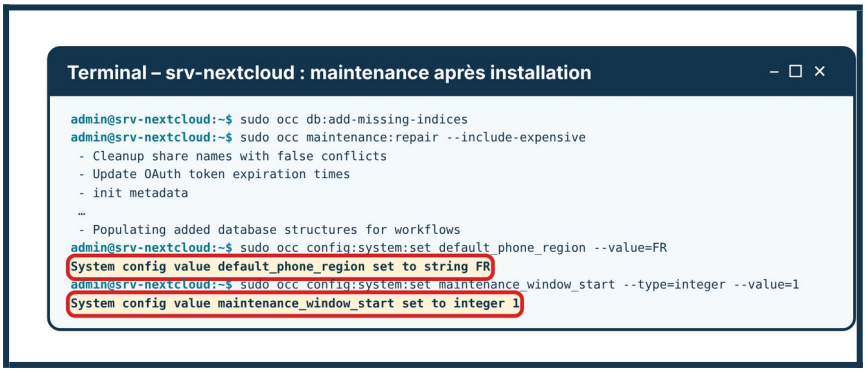
Figure 20 – Délai de lecture des requêtes supprimé

D – 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 (SRV-NEXTCLOUD)

```
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
```



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.

Figure 21 – Réglages de maintenance appliqués

E – 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 (SRV-NEXTCLOUD)

```
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 (SRV-NEXTCLOUD)

```
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
```

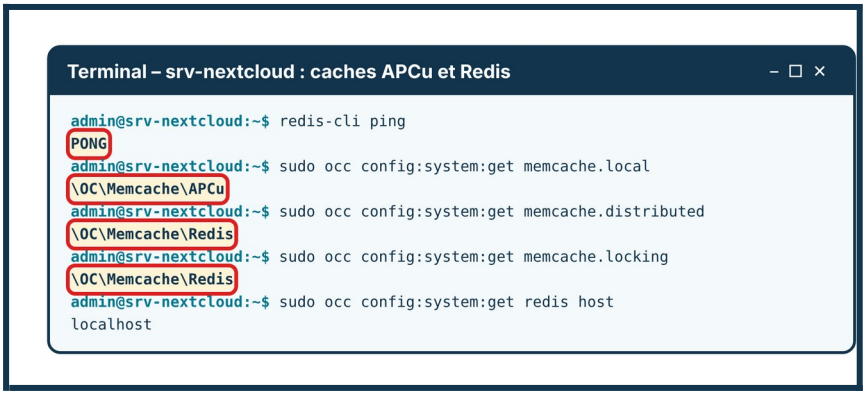


Figure 22 – Redis et les trois caches

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.

F – 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 **entièrement verte**, y compris l'accès **HTTPS** et les en-têtes du **reverse proxy**.

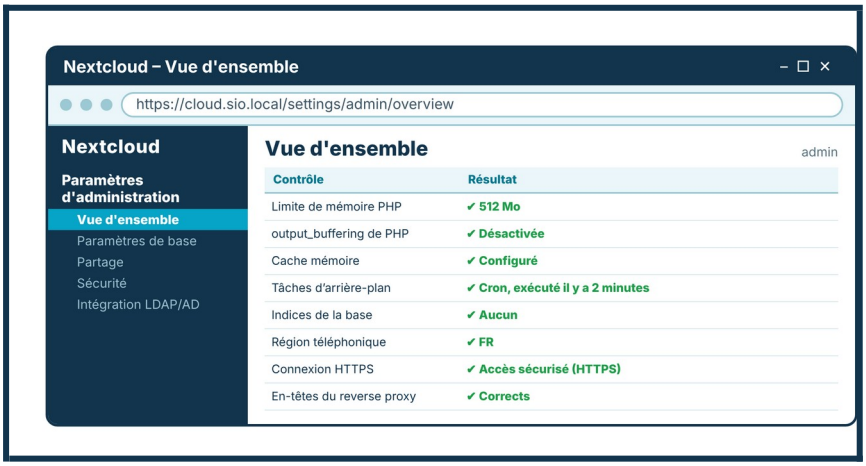


Figure 23 – Paramètres d'administration > Vue d'ensemble

À SAVOIR

Chaque ligne en erreur ou en avertissement indique sa cause et un lien vers la documentation ; relancez la page après chaque correction. Un avertissement sur les **en-têtes du reverse proxy** signale que `trusted_proxies` ne contient pas l'adresse de Traefik (point A). Un avertissement sur `/.well-known/caldav` ou `carddav` signale un problème du middleware `cloud-dav`.

G – Fermer l'accès direct à Nextcloud

Tant qu'Apache répond à tout le monde, un utilisateur peut contourner Traefik (et donc le HTTPS) en saisissant `http://192.168.20.63`. On installe un pare-feu sur SRV-NEXTCLOUD qui n'autorise que l'indispensable : le **SSH** depuis le réseau d'administration et le **port 80 depuis Traefik seulement**.

TERMINAL (SRV-NEXTCLOUD)

```
sudo apt install -y ufw
sudo ufw allow from 192.168.10.0/24 to any port 22 proto tcp
sudo ufw allow from 192.168.20.66 to any port 80 proto tcp
sudo ufw --force enable
sudo ufw status numbered
```

REMARQUE IMPORTANTE

Autorisez le SSH avant d'activer le pare-feu : une règle d'accès SSH erronée vous enferme dehors (adaptez le réseau d'administration 192.168.10.0/24 au vôtre). En cas de blocage, reprenez la main depuis la **console Proxmox** et saisissez `sudo ufw disable`. Gardez cette console ouverte pendant l'opération.

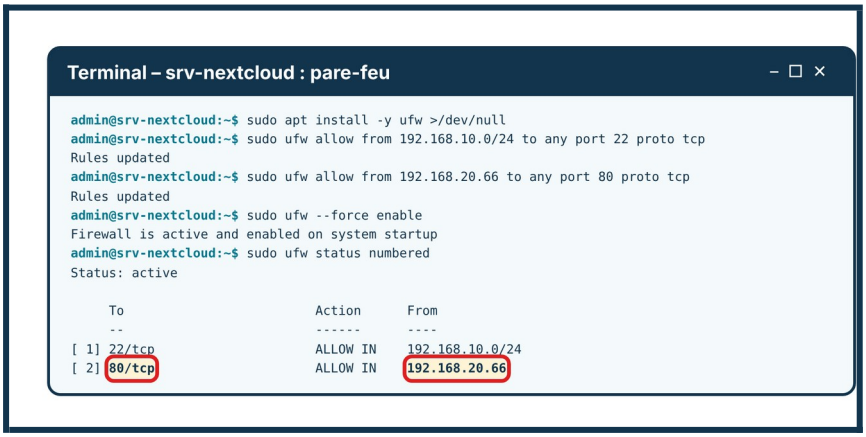


Figure 24 – Pare-feu de SRV-NEXTCLOUD : seul Traefik joint le port 80

À SAVOIR

Le pare-feu refuse tout ce qui n'est pas listé (politique par défaut d'ufw : entrant refusé, sortant autorisé). Les connexions de Nextcloud vers l'annuaire (LDAPS, port 636) sont des connexions **sortantes** : elles ne sont pas concernées.

Contrôlez depuis le **poste d'administration** : `http://192.168.20.63` ne répond plus (le navigateur attend puis abandonne), alors que `https://cloud.sio.local` fonctionne toujours.

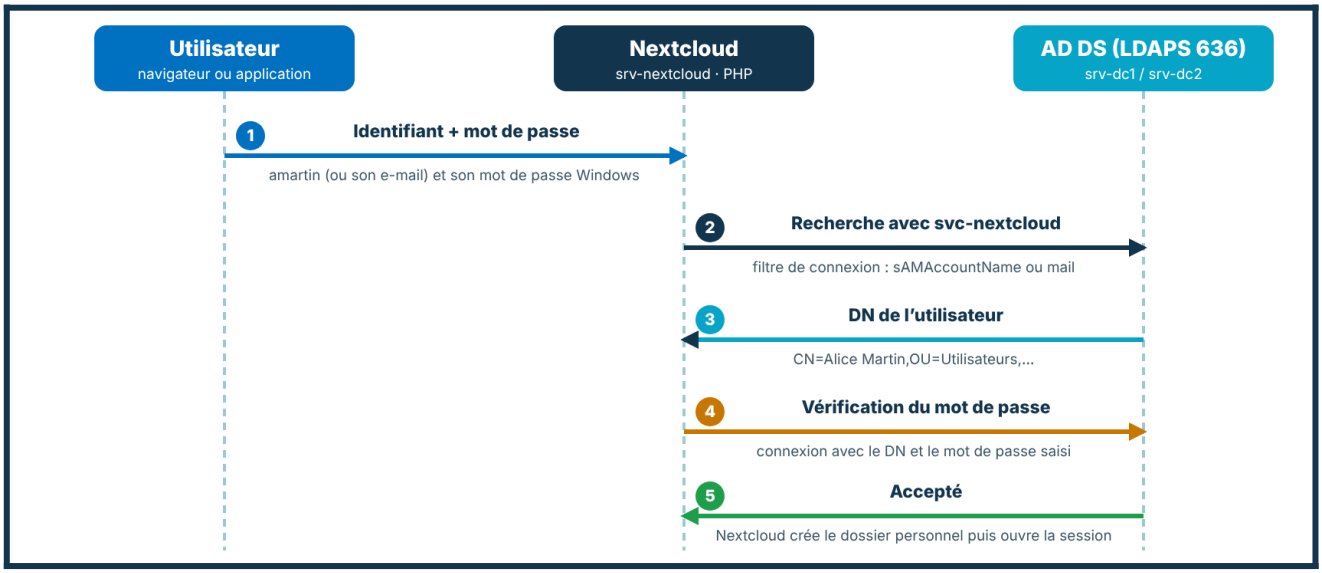
✔ POINT DE CONTRÔLE

- La connexion en **admin** fonctionne à l'adresse `https://cloud.sio.local`
- La **Vue d'ensemble** est verte, **HTTPS** et **reverse proxy** compris
- `redis-cli ping` répond **PONG** et les trois caches sont enregistrés
- Le point d'entrée **websecure** a `readTimeout: 0s` et Traefik a été redémarré
- `http://192.168.20.63` est **inaccessible** depuis le poste d'administration

ÉTAPE 6 SUR 6

06 Lier Nextcloud à l'annuaire AD DS

Pour authentifier les utilisateurs, Nextcloud interroge l'annuaire avec un **compte de service** (lecture seule), puis vérifie le mot de passe de chaque utilisateur. Voici ce qui se passe quand un utilisateur de l'annuaire se connecte :



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**). Chaque contrôleur présente un certificat délivré par **SIO-CA** ; il suffit que **SRV-NEXTCLOUD fasse confiance à cette autorité**.

À SAVOIR

Si vous avez déjà réalisé un autre tutoriel de cette série (GLPI, Nextcloud natif), les unités d'organisation et les utilisateurs **amartin** et **bdurand** existent déjà : les commandes de création répondent alors « existe déjà » (ignorez-le).

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 (SRV-DC1)

```
$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 (SRV-DC1)

```
$mdp = Read-Host -AsSecureString "Mot de passe des utilisateurs de test"
New-ADUser -Name "Alice Martin" -GivenName Alice -Surname Martin `
    -SamAccountName amartin -UserPrincipalName amartin@sio.local `
    -EmailAddress amartin@sio.local -Path "OU=Utilisateurs,$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 :

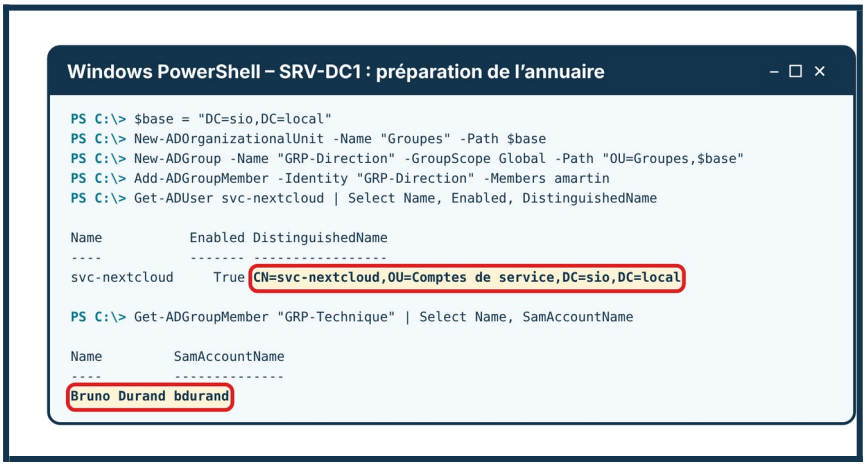
POWERSHELL (SRV-DC1)

```
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 (SRV-DC1)

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



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.

Figure 25 – PowerShell : groupes, compte de service et membres

B – Faire confiance à SIO-CA sur SRV-NEXTCLOUD et tester LDAPS

Pour vérifier le certificat d'un contrôleur, un client n'a besoin que du **certificat de l'autorité**, pas de ceux des contrôleurs : un seul fichier couvre SRV-DC1, SRV-DC2 et tout futur contrôleur. C'est le fichier `sio-ca.cer` exporté à l'étape 4-F (refaites l'export si besoin). Depuis **SRV-DC1**, copiez-le vers **SRV-NEXTCLOUD** :

POWERSHELL (SRV-DC1)

```
scp C:\Temp\sio-ca.cer admin@192.168.20.63:/tmp/
```

Sur **SRV-NEXTCLOUD**, convertissez-le au format PEM, déclarez-le comme autorité de confiance et redémarrez PHP-FPM pour qu'il en tienne compte (PHP utilise le magasin de confiance du système). Installez ensuite l'outil de test LDAP :

TERMINAL (SRV-NEXTCLOUD)

```
sudo openssl x509 -inform der -in /tmp/sio-ca.cer \
    -out /usr/local/share/ca-certificates/sio-ca.crt
sudo update-ca-certificates && sudo systemctl restart php8.4-fpm
sudo apt install -y ldap-utils
```

1 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 (SRV-NEXTCLOUD)

```
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
```

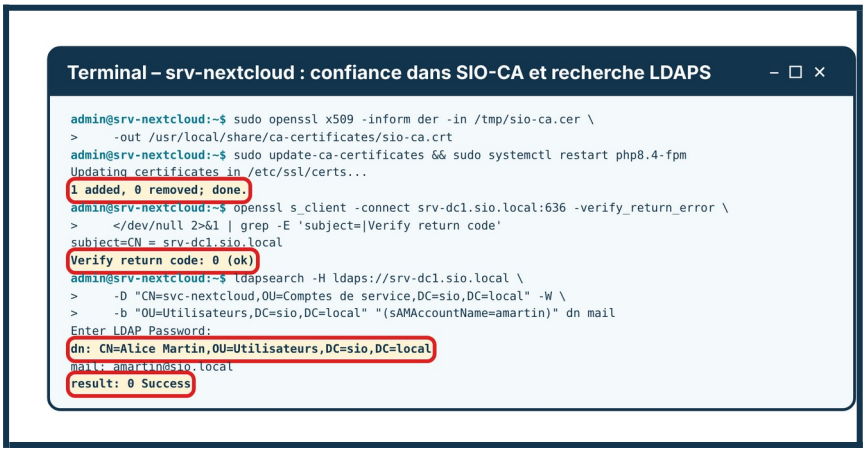


Figure 26 – Debian : confiance dans SIO-CA et recherche LDAPS

À SAVOIR

« Verify return code: 0 (ok) » prouve que SRV-NEXTCLOUD 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 avec `srv-dc2.sio.local` : le même fichier suffit. Si `-inform der` échoue, le fichier est déjà au format PEM : copiez-le simplement.

À SAVOIR

Si vos contrôleurs utilisent des certificats **auto-signés** (tutoriel « natif » sans autorité), il n'y a pas de SIO-CA : exportez les certificats de SRV-DC1 et de SRV-DC2, convertissez-les en PEM et copiez-les tous deux dans `/usr/local/share/ca-certificates/`. Le reste du tutoriel est identique.

C – 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 (SRV-NEXTCLOUD)

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

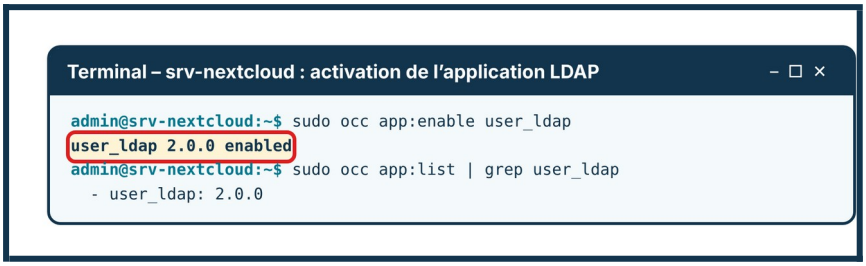


Figure 27 – Activation de l'application LDAP

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.

D – 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 :

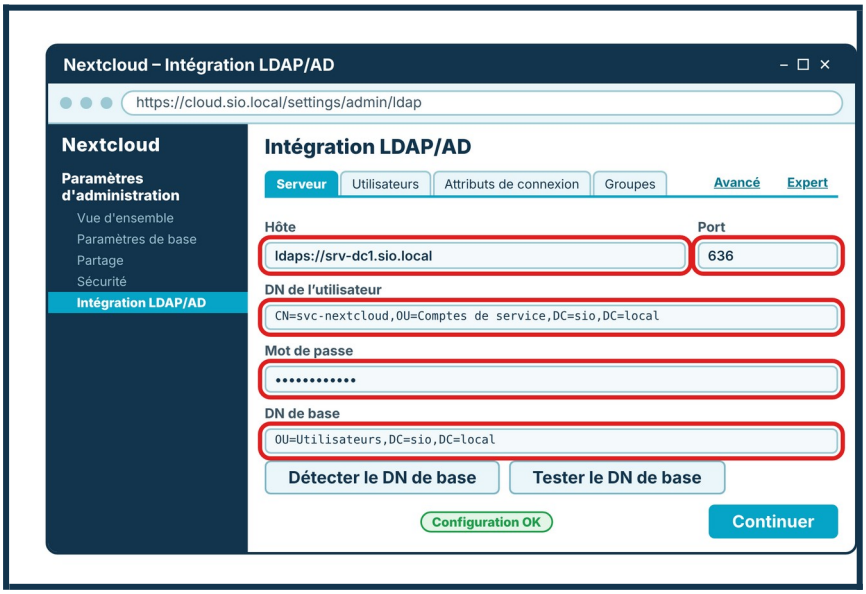


Figure 28 – Intégration LDAP/AD : onglet Serveur

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)))
```

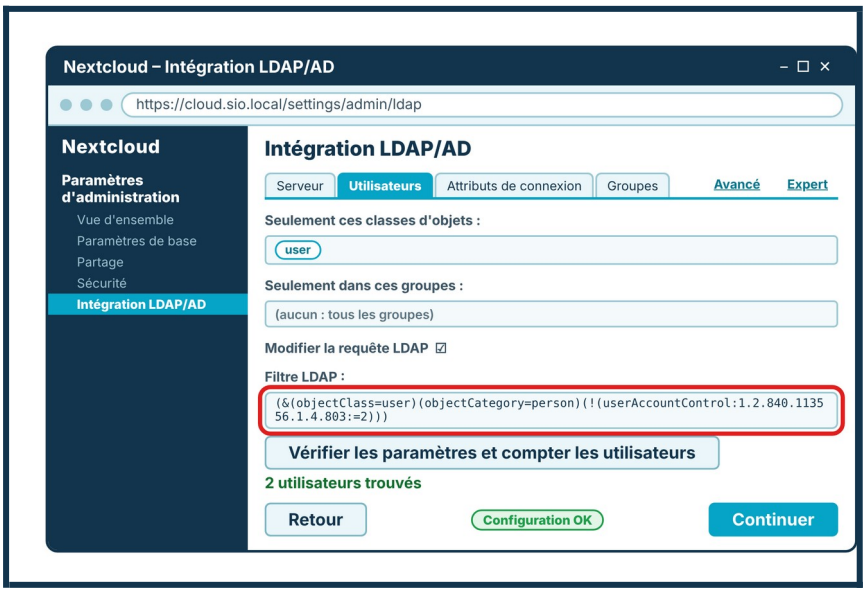


Figure 29 – Intégration LDAP/AD : onglet Utilisateurs

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 » :

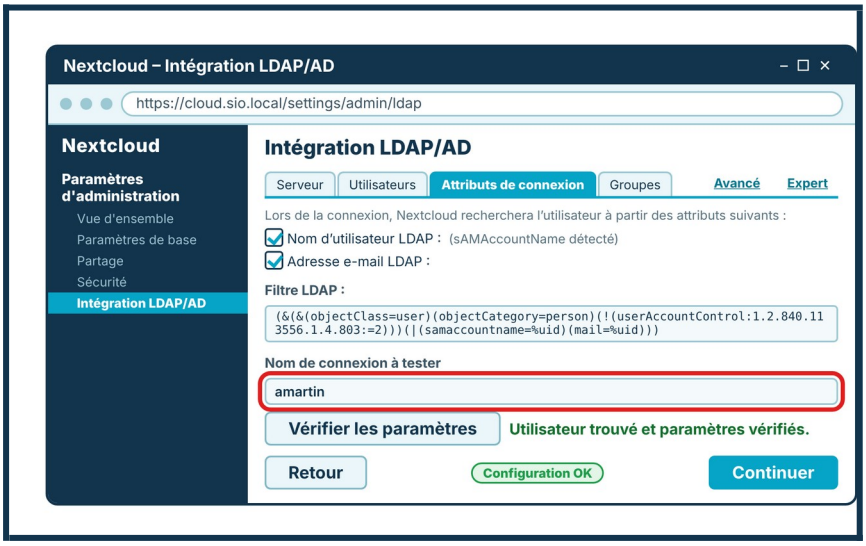


Figure 30 – Intégration LDAP/AD : onglet Attributs de connexion

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) :

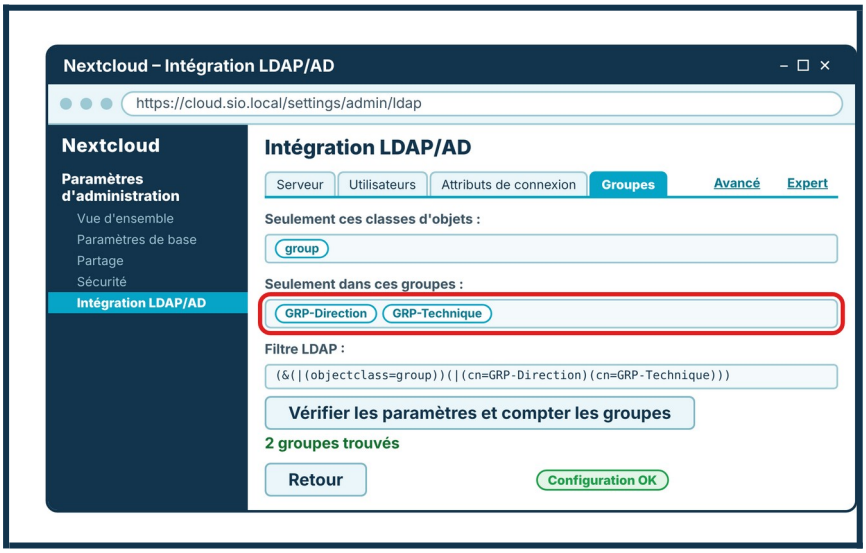


Figure 31 – Intégration LDAP/AD : onglet Groupes

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.

E – 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** :

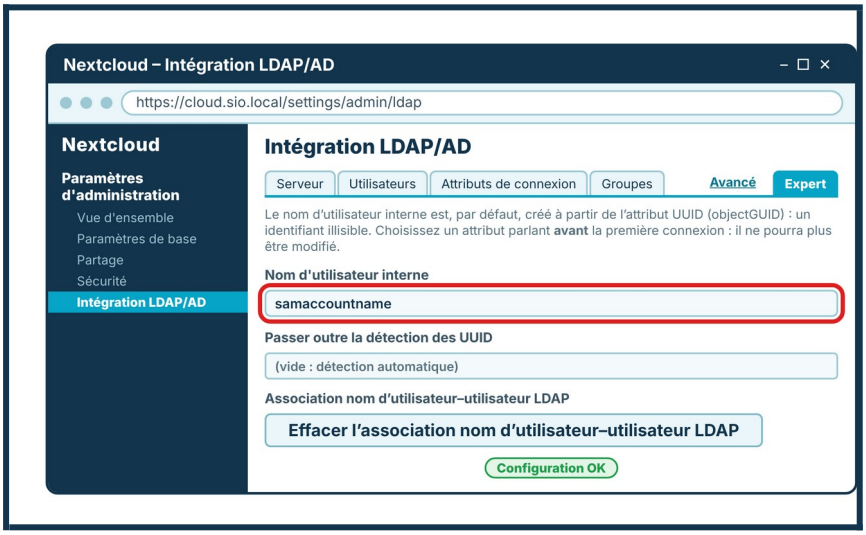


Figure 32 – Intégration LDAP/AD : onglet Expert

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 (SRV-NEXTCLOUD)

```
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.

F – 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 (SRV-NEXTCLOUD)
sudo occ ldap:test-config s01
sudo occ ldap:search "martin"
sudo occ ldap:search --group "GRP"
sudo occ ldap:check-user amartin
```

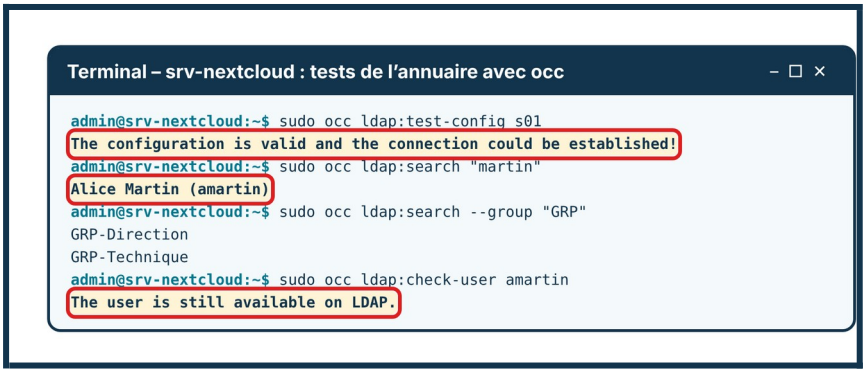


Figure 33 – Tests de l'annuaire avec occ

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.

G – 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 34 – 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 `https://cloud.sio.local` 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 :

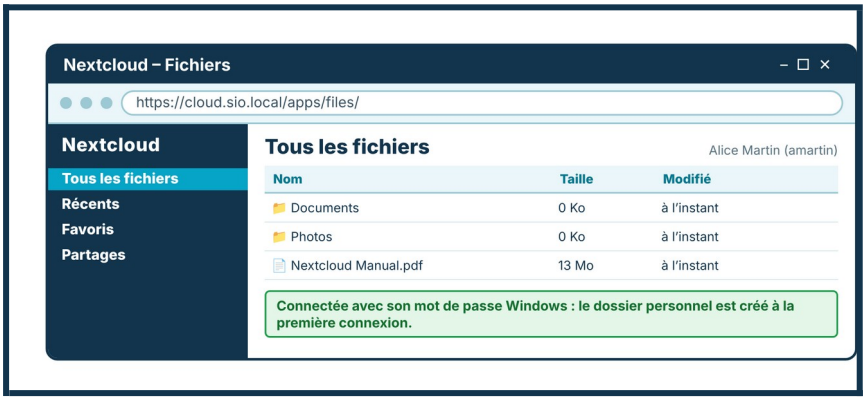


Figure 35 – Fichiers de l'utilisateur Alice Martin

À SAVOIR

Le mot de passe n'est jamais copié dans Nextcloud : à chaque connexion, Nextcloud le fait vérifier par l'annuaire. Il circule chiffré de bout en bout : HTTPS entre le navigateur et Traefik, puis LDAPS entre Nextcloud et le contrôleur. Désactiver le compte dans Active Directory suffit 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 sur le serveur ; `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**, à l'adresse `https://cloud.sio.local`, sous le nom `amartin`
- Si SRV-DC1 est arrêté, la connexion fonctionne encore grâce à **SRV-DC2**

Notre Nextcloud est **opérationnel et publié en HTTPS** : les utilisateurs ne connaissent que `https://cloud.sio.local`, Traefik présente le certificat de l'autorité interne, Apache n'est joignable que par Traefik, et les comptes Windows servent de comptes Nextcloud. Il reste à organiser les dossiers partagés par groupe et à prévoir les sauvegardes.

Dépannage : les symptômes les plus fréquents

Symptôme	Cause probable	Solution
Le service traefik ne démarre pas	Erreur dans `traefik.yml`, ou droits insuffisants sur `/etc/traefik` ou `/var/log/traefik`	`sudo journalctl -u traefik -n 20` ; contrôler l'indentation ; `sudo chown -R traefik:traefik /etc/traefik /var/log/traefik`
`certreq` : « Refusé » ou « En attente »	Le modèle « Serveur Web » n'est pas publié sur SIO-CA ou le compte n'a pas le droit « Inscrire »	Console `certsrv` > Modèles de certificats > Nouveau > Modèle à délivrer ; vérifier les droits du modèle
Avertissement de certificat dans le navigateur	Poste hors domaine (SIO-CA inconnue), nom absent des noms alternatifs ou certificat expiré	Importer SIO-CA ; vérifier `openssl x509 -noout -ext subjectAltName` ; contrôler `-enddate`
« 404 page not found » (réponse de Traefik)	Aucun routeur ne correspond : nom absent du DNS ou de la règle `Host`, fichier invalide ou non chargé	`getent hosts cloud.sio.local` ; relire `cloud.yml` ; consulter le journal et le tableau de bord
« 502 Bad Gateway »	Traefik ne joint pas Apache : service arrêté, mauvaise adresse, pare-feu	Depuis SRV-TRAEFIK : `curl -sI http://192.168.20.63` ; vérifier `systemctl status apache2` et `sudo ufw status`
« 403 Forbidden » sur `traefik.sio.local`	L'adresse du poste n'est pas dans `sourceRange`	Ajouter le réseau du poste dans `middlewares.yml` (rechargement automatique)
« 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`
Liens en `http://`, boucle de redirection ou page de connexion qui se recharge	`overwriteprotocol` ou `trusted_proxies` absent, ou adresse de Traefik incorrecte	Reprendre l'étape 5-A ; `sudo occ config:system:get trusted_proxies 0` doit répondre 192.168.20.66
Vue d'ensemble : « en-têtes du reverse proxy incorrects »	L'adresse de Traefik n'est pas dans `trusted_proxies`	Reprendre l'étape 5-A, puis recharger la page
Envoi d'un gros fichier interrompu au bout d'une minute	Délai de lecture de Traefik (60 s) ou limites de PHP	`readTimeout: 0s` dans `traefik.yml` + `systemctl restart traefik` (5-C) ; vérifier `upload_max_filesize` et `post_max_size`
Vue d'ensemble : alerte sur `/.well-known/caldav`	Middleware `cloud-dav` absent du routeur ou expression régulière erronée	`curl -sI https://cloud.sio.local/.well-known/carddav` doit renvoyer vers `/remote.php/dav/` ; relire `cloud.yml`
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`
Accès SSH perdu après activation du pare-feu	Règle du port 22 absente ou réseau d'administration incorrect	Console Proxmox : `sudo ufw disable`, corriger la règle, réactiver
Test LDAP : « Can't contact LDAP server »	SIO-CA non reconnue par SRV-NEXTCLOUD, nom différent du certificat ou port 636 bloqué	Refaire l'étape 6-B ; utiliser le **nom complet** du contrôleur, pas son adresse IP ; `sudo systemctl restart php8.4-fpm`
« Invalid credentials » (code 49) ou « Strong(er) authentication required »	DN ou mot de passe du compte incorrect ; connexion non chiffrée refusée par Windows Server 2025	Saisir le **DN complet** ; utiliser `ldaps://` et le port **636** ; vérifier `Get-ADUser svc-nextcloud`

Pense-bête : commandes et emplacements

Commande / emplacement	Utilité
`sudo systemctl status traefik`	État de Traefik (`restart` après une modification de `traefik.yml`)
`sudo journalctl -u traefik -f`	Journal de Traefik en direct (erreurs de fichiers, de certificat)
`/etc/traefik/dynamic/*.yml`	Configuration dynamique : rechargée à chaud, un fichier par sujet (dont `cloud.yml`)
`/etc/traefik/certs/`	Certificat et clé privée (clé lisible uniquement par `traefik`)
`openssl x509 -in /etc/traefik/certs/cloud.crt -noout -enddate`	Date d'expiration du certificat : à surveiller, renouvellement en suivant l'étape 3 (E à G)
`https://traefik.sio.local`	Tableau de bord de Traefik : routeurs, services, middlewares, erreurs
`sudo ufw status numbered`	Règles du pare-feu de SRV-NEXTCLOUD
`/srv/nextcloud-data/nextcloud.log`	Journal de Nextcloud (aussi dans Paramètres d'administration > Journalisation)
`/var/www/nextcloud/config/config.php`	Configuration, accès à la base et secrets : à sauvegarder avec `/srv/nextcloud-data/` et 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