Cloud privé Nextcloud 35 (Hub 26 Summer) sous Debian 13 avec Active Directory

Nov 27, 2026 · @Serge Martins

Objectif

Installer **Nextcloud 35** (« Hub 26 Summer ») sur **CLOUD01** (Debian 13) pour offrir aux utilisateurs de **martinscie.lan** un espace de fichiers, d'agenda et de partage hébergé en interne, avec connexion par leur compte Active Directory.

Élément	Valeur
Nom	cloud01.martinscie.lan
Adresse IP	192.168.10.43/24 (VLAN 10 Serveurs)
Passerelle / DNS	192.168.10.254 (RFW01) / 192.168.10.10 (DC01)
Pile logicielle	Apache 2.4, PHP 8.4 (PHP-FPM), MariaDB 11.8, Redis
Version	Nextcloud 35.0.x (PHP 8.3 minimum, MariaDB 10.11 minimum)
Données	/srv/nextcloud-data (disque dédié conseillé)
Ressources	2 vCPU, 4 Go RAM, 20 Go système + disque de données

Un cloud interne, avec les comptes du domaine



CLOUD01 · Nextcloud dans martinscie.lan

Les utilisateurs accèdent à CLOUD01 en HTTPS ; Nextcloud vérifie leurs identifiants sur l'AD de DC01 et range métadonnées et fichiers dans MariaDB et sur le disque de données.

Étape 1 – Paquets

```
hostnamectl set-hostname cloud01
apt update && apt full-upgrade -y
apt install -y apache2 mariadb-server redis-server php8.4-fpm \
  php8.4-
{mysql,gd,curl,mbstring,intl,xml,zip,bz2,bcmath,gmp,ldap,redis,apcu,imagick,o
pcache} \
  libmagickcore-7.q16-10-extra unzip wget
```

Sur DC01 : `Add-DnsServerResourceRecordA -ZoneName "martinscie.lan" -Name "cloud01" -IPv4Address 192.168.10.43 -CreatePtr`.

Étape 2 – Base de données

```
mariadb-secure-installation
mariadb -u root -p -e "CREATE DATABASE nextcloud CHARACTER SET utf8mb4
COLLATE utf8mb4_general_ci; CREATE USER 'nextcloud'@'localhost' IDENTIFIED BY
'MotDePasseNc!'; GRANT ALL ON nextcloud.* TO 'nextcloud'@'localhost'; FLUSH
PRIVILEGES;"
```

Étape 3 – Télécharger et vérifier Nextcloud

```
cd /tmp
wget https://download.nextcloud.com/server/releases/latest.zip
wget https://download.nextcloud.com/server/releases/latest.zip.sha256
sha256sum -c latest.zip.sha256 < latest.zip
unzip -q latest.zip -d /var/www/
mkdir -p /srv/nextcloud-data
chown -R www-data:www-data /var/www/nextcloud /srv/nextcloud-data
```

Étape 4 – Apache et PHP

```
cat > /etc/apache2/sites-available/nextcloud.conf <<'EOF'
<VirtualHost *:80>
    ServerName cloud01.martinscie.lan
    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>
</VirtualHost>
EOF
a2enmod rewrite headers env dir mime proxy_fcgi setenvif ssl
a2ensite nextcloud && a2dissite 000-default
```

Dans `/etc/php/8.4/fpm/php.ini` : `memory_limit = 512M`, `upload_max_filesize = 2G`, `post_max_size = 2G`, `opcache.interned_strings_buffer = 32`, `date.timezone = Europe/Paris`. Dans `/etc/php/8.4/fpm/pool.d/www.conf` : décommenter `env[PATH]`. Puis `systemctl restart php8.4-fpm apache2`.

Étape 5 – Installation en ligne de commande

```
cd /var/www/nextcloud
sudo -u www-data php occ maintenance:install --database mysql --database-name
nextcloud \
  --database-user nextcloud --database-pass 'MotDePasseNc!' \
  --admin-user ncadmin --admin-pass 'AdminNc!2026' --data-dir /srv/nextcloud-
data
sudo -u www-data php occ config:system:set trusted_domains 1 --
value=cloud01.martinscie.lan
sudo -u www-data php occ config:system:set default_phone_region --value=FR
sudo -u www-data php occ config:system:set memcache.local --
value='\OC\Memcache\APCu'
sudo -u www-data php occ config:system:set memcache.locking --
value='\OC\Memcache\Redis'
sudo -u www-data php occ config:system:set redis host --value=localhost
sudo -u www-data php occ background:cron
echo '*/5 * * * * www-data php -f /var/www/nextcloud/cron.php' >
/etc/cron.d/nextcloud
```

Étape 6 – Connexion à Active Directory

```
sudo -u www-data php occ app:enable user_ldap
```

Puis **Paramètres d'administration → Intégration LDAP/AD** :

Onglet	Réglage
Serveur	dc01.martinscie.lan, port 389 (636 en LDAPS), DN `CN=svc-nextcloud,OU=Services,DC=martinscie,DC=lan`, base `DC=martinscie,DC=lan`
Utilisateurs	Classes `person` et `user`, membres du groupe `GG-Nextcloud`
Attributs de connexion	Nom d'utilisateur LDAP/AD (`sAMAccountName`) et adresse e-mail
Groupes	Groupes de l'OU Groupes
Expert	Attribut de nom d'utilisateur interne : `sAMAccountName`

Tester avec un compte du domaine depuis un poste du VLAN 20.

Étape 7 – HTTPS et contrôles

- Certificat de l'autorité interne (ou Let's Encrypt en production), redirection HTTP → HTTPS et en-tête HSTS.
- **Paramètres d'administration → Vue d'ensemble** : corriger les avertissements de sécurité et de configuration.
- `sudo -u www-data php occ status` et `occ app:update --all`.
- Client de synchronisation Nextcloud sur Windows 11 ; applications Agenda, Contacts et Office (Collabora ou Euro-Office) selon les besoins.

Sécurité et bonnes pratiques

- Rester sur une version maintenue : Nextcloud 32 n'a plus de correctifs depuis septembre 2026.
- Activer la double authentification (application TOTP) pour les administrateurs.

- Sauvegarder la base, `config/config.php` et le dossier de données (mode maintenance pendant la sauvegarde).
- Ne publier sur Internet qu'au travers d'un reverse-proxy et de RFW01, avec l'application de protection contre la force brute active.

Dépannage

Symptôme	Piste
« Accès par un domaine non approuvé »	Ajouter le nom dans `trusted_domains`
Avertissements PHP/OPcache	Réglages `php.ini` FPM, redémarrer PHP-FPM
Utilisateurs AD invisibles	Filtre LDAP, compte de service, groupe GG-Nextcloud
Envois de gros fichiers en échec	`upload_max_filesize`, `post_max_size`, délais Apache