Documentation d'Installation

ownCloud

Installation Linux & Intégration LDAP / Active Directory & SNMP

Version 10.16 — Mars 2025

Sommaire

1. Présentation de la solution

ownCloud est une plateforme open-source de partage de fichiers et de collaboration. Cette documentation décrit l'installation complète d'une instance ownCloud v10.16 sur un serveur Linux (Debian/Ubuntu), sa configuration avec authentification Active Directory via LDAP, ainsi que la supervision du serveur via le protocole SNMP.

Environnement de déploiement :

- Serveur ownCloud : 192.168.147.77 / 192.168.3.31 (port 8082)
- Serveur LDAP/AD : 192.168.1.12 (port 389)
- DN de base : DC=gourmet,DC=fr
- Compte de liaison : CN=Administrateur,CN=Users,DC=gourmet,DC=fr
- Base de données : MariaDB / MySQL — owncloud_db
- Supervision SNMP : communauté « gourmet » — accès depuis 192.168.1.11

---

2. Installation de ownCloud sur un serveur Linux

2.1 Prérequis système

Système d'exploitation recommandé : Debian 11/12 ou Ubuntu 22.04 LTS.

Ressources minimales recommandées pour une installation de production :

- CPU : 2 vCPU | RAM : 4 Go | Disque : 40 Go minimum

Mise à jour du système avant toute installation :

```
sudo apt update && sudo apt upgrade -y
```

2.2 Installation des dépendances (Apache, PHP, MariaDB)

ownCloud nécessite un serveur web Apache, PHP 8.0 (ou 7.4 selon la version) et une base de données MariaDB ou MySQL.

Installation d'Apache, MariaDB et des extensions PHP requises :

```
sudo apt install -y apache2 mariadb-server \
  php php-mysql php-xml php-curl php-gd php-mbstring \
  php-zip php-intl php-ldap php-apcu php-imagick \
  libapache2-mod-php
```

Activation des modules Apache nécessaires :

```
sudo a2enmod rewrite headers env dir mime setenvif ssl
sudo systemctl restart apache2
```

Sécurisation de MariaDB (définir le mot de passe root, supprimer les accès anonymes) :

```
sudo mysql_secure_installation
```

2.3 Création de la base de données

Connexion à MariaDB puis création de la base et de l'utilisateur ownCloud :

```
sudo mysql -u root -p

CREATE DATABASE owncloud_db CHARACTER SET utf8mb4 COLLATE utf8mb4_general_ci;
CREATE USER 'admin_oc'@'localhost' IDENTIFIED BY 'Btssio64!';
GRANT ALL PRIVILEGES ON owncloud_db.* TO 'admin_oc'@'localhost';
FLUSH PRIVILEGES;
EXIT;
```

2.4 Téléchargement et déploiement de ownCloud

Téléchargement de l'archive ownCloud 10.16 et d

ploiement dans le répertoire web :

```
cd /tmp
wget
https://download.owncloud.com/server/stable/owncloud-complete-20240724.tar.bz2
tar -xjf owncloud-complete-20240724.tar.bz2
sudo mv owncloud /var/www/html/
```

Attribution des permissions correctes à Apache :

```
sudo chown -R www-data:www-data /var/www/html/owncloud
sudo find /var/www/html/owncloud/ -type d -exec chmod 750 {} \;
sudo find /var/www/html/owncloud/ -type f -exec chmod 640 {} \;
```

2.5 Configuration Apache (Virtual Host)

Création du fichier de configuration Apache pour ownCloud :

```
sudo nano /etc/apache2/sites-available/owncloud.conf
```

Contenu du fichier owncloud.conf :

```
<VirtualHost *:8082>
    ServerName 192.168.147.77
    DocumentRoot /var/www/html/owncloud

    <Directory /var/www/html/owncloud>
        Options +FollowSymlinks
```

```
        AllowOverride All
        Require all granted
        <IfModule mod_dav.c>
            Dav off
        </IfModule>
        SetEnv HOME /var/www/html/owncloud
        SetEnv HTTP_HOME /var/www/html/owncloud
    </Directory>

    ErrorLog ${APACHE_LOG_DIR}/owncloud_error.log
    CustomLog ${APACHE_LOG_DIR}/owncloud_access.log combined
</VirtualHost>
```

Activation du Virtual Host et redémarrage d'Apache :

```
# Ajouter le port 8082 si nécessaire dans /etc/apache2/ports.conf :
echo "Listen 8082" | sudo tee -a /etc/apache2/ports.conf

sudo a2ensite owncloud.conf
sudo systemctl restart apache2
```

2.6 Finalisation de l'installation via l'interface web

Ouvrez un navigateur et accédez à l'URL de votre instance :

```
http://192.168.147.77:8082/owncloud
```

L'assistant d'installation ownCloud vous demande de :

1. Définir un compte administrateur (login / mot de passe).
2. Renseigner le chemin du répertoire de données (/var/www/html/owncloud/data).
3. Saisir les paramètres de connexion à la base de données (admin_oc / Btssio64! / owncloud_db).
4. Cliquer sur « Terminer l'installation ».

> **Note :** Une fois l'installation terminée, le fichier config/config.php est automatiquement généré. Vérifiez qu'il contient bien votre adresse IP dans trusted_domains.

---

3. Vérification du fichier de configuration (config.php)

Après installation, vérifiez le fichier /var/www/html/owncloud/config/config.php via SSH :

```
sudo nano /var/www/html/owncloud/config/config.php
```

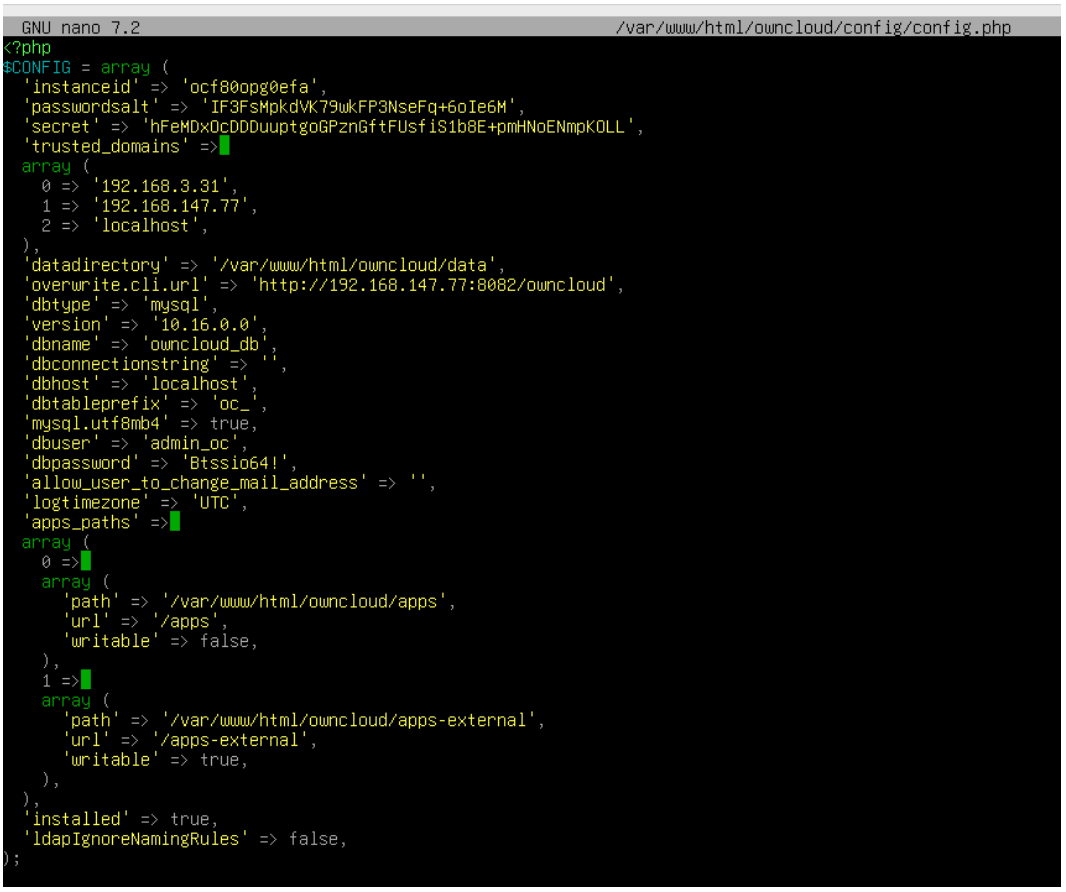

Figure 1 — Contenu du fichier config/config.php édité via nano

Paramètres importants à contrôler :

- trusted_domains : vérifiez que l'IP du serveur est bien listée
- overwrite.cli.url : URL publique de l'instance ownCloud
- dbtype / dbname : moteur (mysql) et nom de la base de données
- datadirectory : chemin vers le répertoire de données

> **Note :** Après toute modification de config.php, rechargez Apache (sudo systemctl reload apache2).

---

4. Installation du plugin LDAP Integration

L'intégration LDAP nécessite l'installation du plugin officiel « LDAP Integration » disponible dans le Market ownCloud.

Procédure :

1. Connectez-vous à ownCloud en tant qu'administrateur.

2. Accédez au menu principal → Market.
3. Recherchez « LDAP Integration » dans la catégorie Integration.
4. Cliquez sur le bouton INSTALLER et attendez la fin du téléchargement.

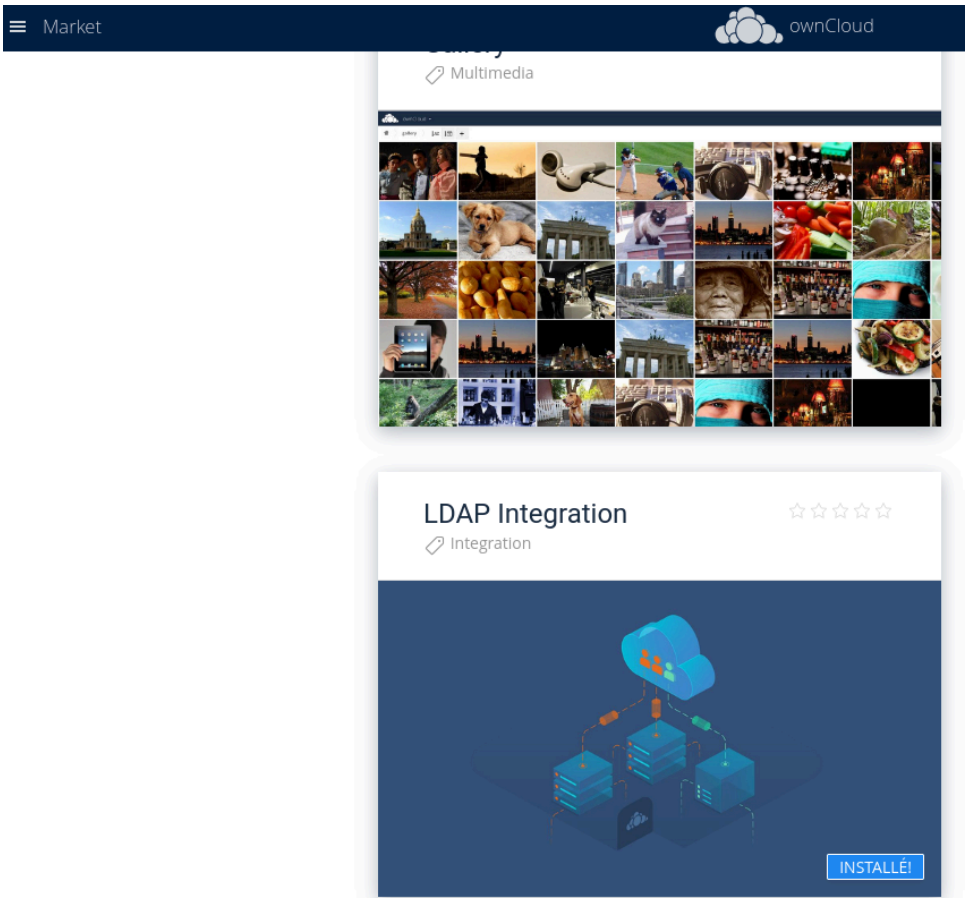

Figure 2 — Plugin LDAP Integration dans le Market (statut : INSTALLÉ)

> **Note :** Une fois le plugin activé, la section « Authentification de l'utilisateur » apparaît dans Administration → Paramètres.

Alternative : installation du plugin en ligne de commande (occ) :

```
sudo -u www-data php /var/www/html/owncloud/occ app:enable user_ldap
```

---

5. Configuration LDAP — Onglet Serveur

Accédez à Administration → Paramètres → Authentification de l'utilisateur → LDAP. Renseignez les informations de connexion au contrôleur de domaine dans l'onglet Serveur :

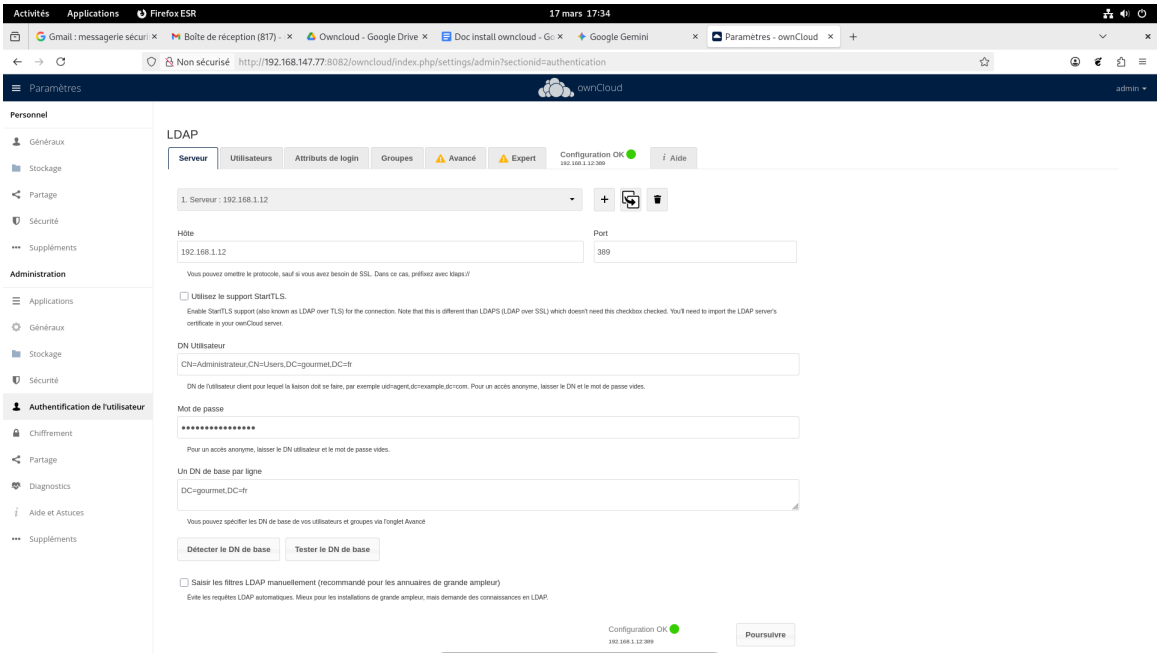

Figure 3 — Onglet Serveur : paramètres de connexion au contrôleur de domaine

Champs à renseigner :

- Hôte : 192.168.1.12
- Port : 389 (LDAP standard — utiliser 636 pour LDAPS)
- DN Utilisateur : CN=Administrateur,CN=Users,DC=gourmet,DC=fr
- Mot de passe : mot de passe du compte de liaison AD
- DN de base : DC=gourmet,DC=fr

Cliquez sur « Détecter le DN de base » puis « Tester le DN de base » pour valider la connexion. Le voyant « Configuration OK » doit passer au vert avant de cliquer sur Poursuivre.

> **Note :** Ne cochez pas « StartTLS » si l'AD n'est pas configuré pour le chiffrement TLS. Pour LDAPS (port 636), préfixez l'hôte avec ldaps://.

---

6. Configuration LDAP — Onglet Utilisateurs

L'onglet Utilisateurs définit le filtre LDAP déterminant quels comptes AD sont autorisés à se connecter à ownCloud.

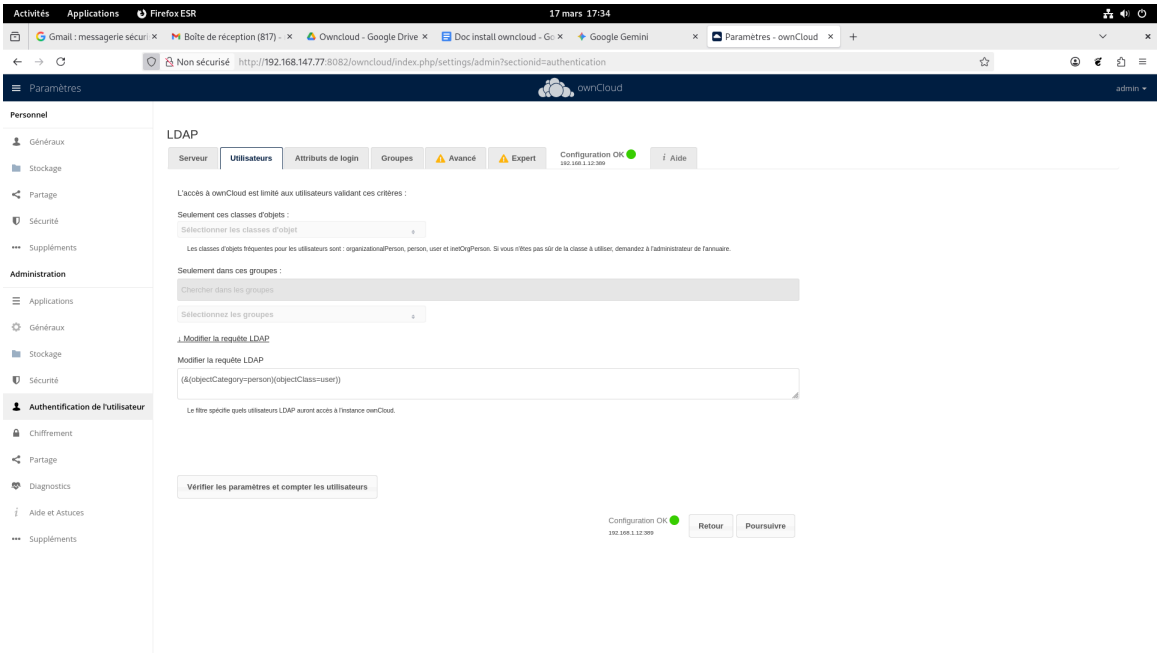

Figure 4 — Onglet Utilisateurs : filtre LDAP des comptes autorisés

Filtre LDAP appliqué :

(&(objectCategory=person)(objectClass=user))

Ce filtre inclut l'ensemble des comptes utilisateurs de l'AD. Pour restreindre l'accès à certains groupes, ajoutez une condition memberOf dans le filtre.

Cliquez sur « Vérifier les paramètres et compter les utilisateurs » : le nombre de comptes détectés s'affiche en bas de l'écran.

---

7. Configuration LDAP — Onglet Groupes

L'onglet Groupes synchronise les groupes Active Directory dans ownCloud pour faciliter la gestion des partages et des droits.

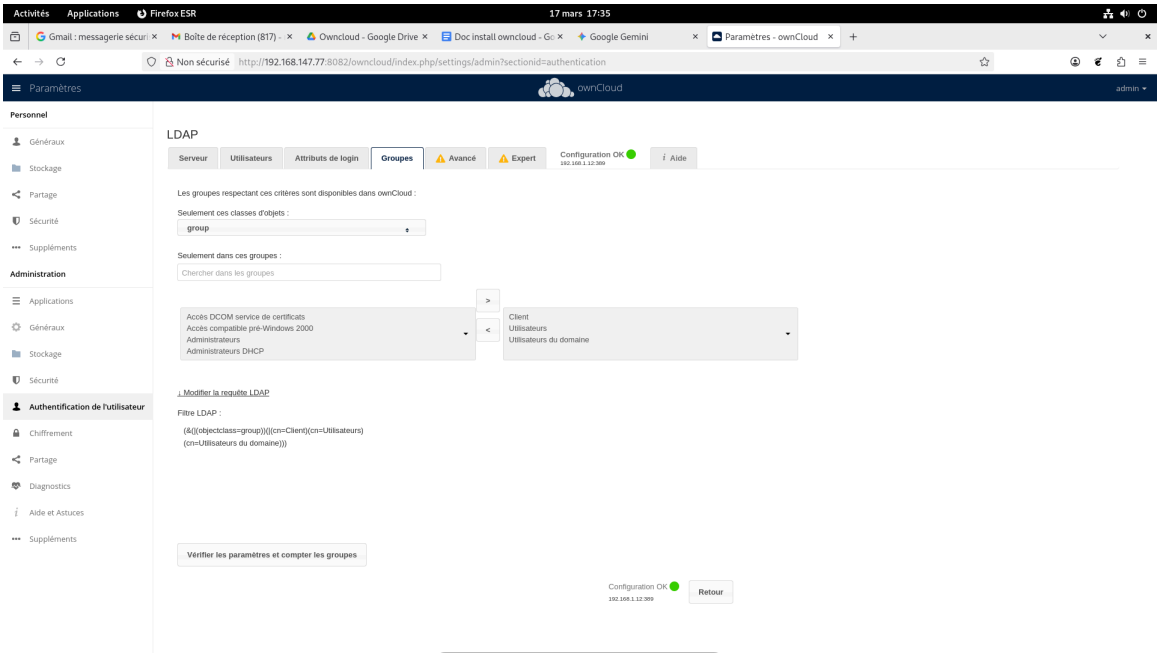

Figure 5 — Onglet Groupes : sélection des groupes AD synchronisés dans ownCloud

Paramètres configurés :

- Classe d'objets : group
- Groupes sélectionnés : Client, Utilisateurs, Utilisateurs du domaine
- Filtre LDAP généré : (&((objectclass=group))((cn=Client)(cn=Utilisateurs)(cn=Utilisateurs du domaine)))

Les groupes disponibles côté gauche correspondent aux groupes présents dans l'AD. Déplacez-les vers la droite avec « > » pour les activer dans ownCloud.

> **Note :** Seuls les groupes sélectionnés seront disponibles dans ownCloud pour la gestion des partages et des droits d'accès.

---

8. Configuration LDAP — Onglet Avancé (Paramètres du répertoire)

L'onglet Avancé permet de configurer les attributs LDAP utilisés pour l'affichage des noms d'utilisateurs et de groupes dans ownCloud.

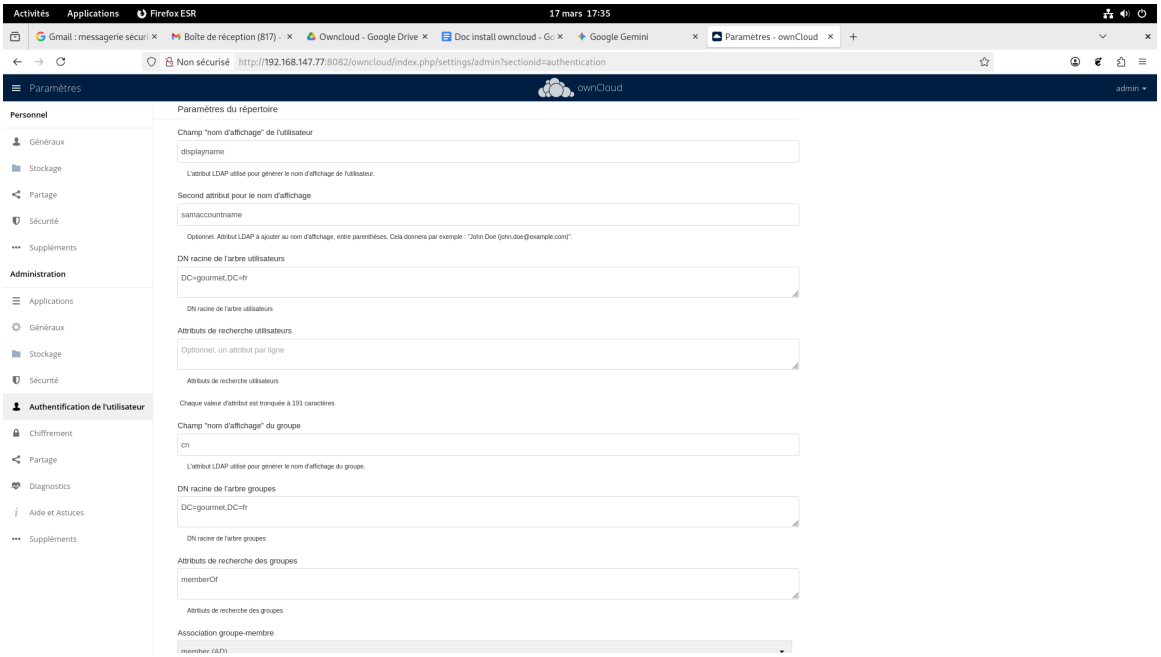

Figure 6 — Onglet Avancé : paramètres du répertoire LDAP

Paramètres utilisateurs :

- Champ "nom d'affichage" : displayname
- Second attribut d'affichage : samaccountname
- DN racine arbre utilisateurs : DC=gourmet,DC=fr
- Attributs de recherche : (optionnel, un attribut par ligne)

Paramètres groupes :

- Champ "nom d'affichage" groupe : cn
- DN racine arbre groupes : DC=gourmet,DC=fr
- Attributs de recherche groupes : memberOf
- Association groupe-membre : member (AD)

> **Note :** L'attribut samaccountname est recommandé comme second attribut d'affichage pour garantir l'unicité des noms dans ownCloud.

---

9. Vérification — Accès au dossier partagé Espace_Direction

Une fois la configuration LDAP terminée et validée, connectez-vous avec un compte utilisateur Active Directory pour vérifier que l'intégration fonctionne correctement et que les partages sont bien accessibles.

9.1 Connexion avec un compte utilisateur AD

Ouvrez un navigateur et accédez à l'URL ownCloud. Saisissez les identifiants d'un compte présent dans l'annuaire LDAP (ici : Nicolas). Après connexion, l'interface affiche les fichiers et dossiers partagés avec cet utilisateur.

9.2 Vérification des dossiers partagés (vue « Partagés avec vous »)

Dans le menu latéral, cliquez sur « Partagés avec vous ». Le dossier « Espace_Direction » doit apparaître dans la liste — il a été partagé par l'administrateur avec les membres du groupe correspondant dans l'Active Directory.

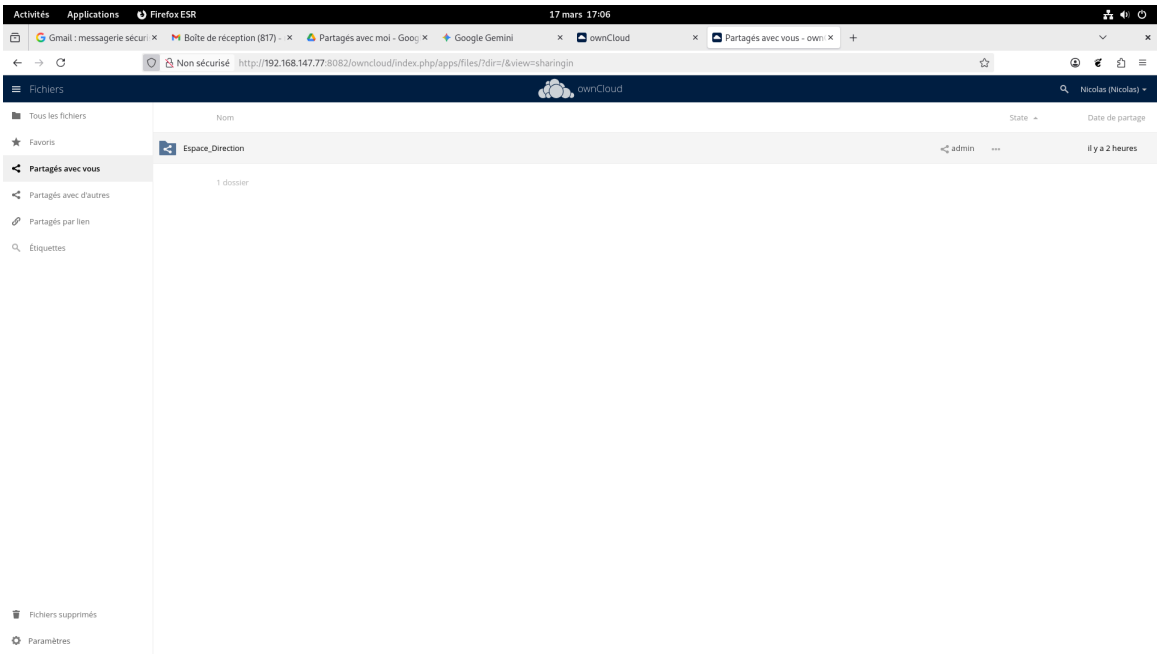

Figure 7 — Vue « Partagés avec vous » : le dossier Espace_Direction est bien visible pour l'utilisateur Nicolas

9.3 Vérification de l'arborescence complète (vue « Tous les fichiers »)

La vue « Tous les fichiers » confirme l'ensemble des dossiers accessibles pour l'utilisateur connecté. Le dossier Espace_Direction apparaît avec l'icône de partage et le nom du propriétaire (admin).

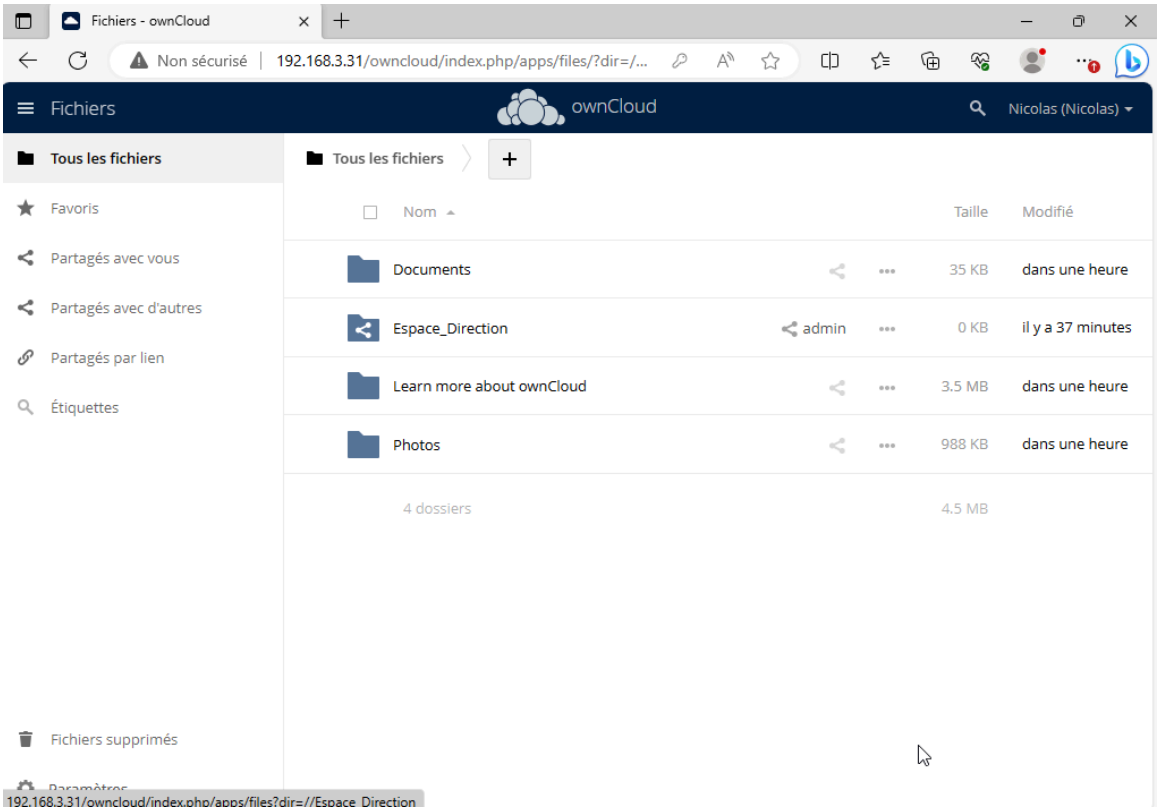

Figure 8 — Vue « Tous les fichiers » : arborescence complète accessible à l'utilisateur Nicolas

> **Note :** Si le dossier Espace_Direction n'apparaît pas, vérifiez que l'utilisateur AD appartient bien au groupe partagé dans ownCloud, et que la synchronisation LDAP a bien été effectuée (onglet Utilisateurs → Vérifier les paramètres).

9.4 Dépannage rapide

En cas de problème de connexion ou de dossier manquant :

Vérification de la connectivité réseau vers le serveur LDAP :

```
ping 192.168.1.12
telnet 192.168.1.12 389
```

Consultation des journaux ownCloud en temps réel :

```
sudo tail -f /var/www/html/owncloud/data/owncloud.log
```

Forcer la synchronisation LDAP via la commande occ :

```
sudo -u www-data php /var/www/html/owncloud/occ ldap:show-remnants
sudo -u www-data php /var/www/html/owncloud/occ user:sync
'OCA\User_LDAP\User_Proxy' -m disable
```

10. Configuration SNMP sur le serveur ownCloud

Le protocole SNMP (Simple Network Management Protocol) permet la supervision du serveur ownCloud depuis un outil de monitoring réseau (Zabbix, Nagios, PRTG, etc.). Cette section décrit l'installation de l'agent SNMP et la configuration des accès depuis le serveur de supervision.

10.1 Installation du service SNMP

Installation du démon snmpd et des outils SNMP :

```
sudo apt update
sudo apt install -y snmpd snmp libsnmp-dev
```

Activation et démarrage automatique du service au boot :

```
sudo systemctl enable snmpd
sudo systemctl start snmpd
```

Vérification que le service est bien actif :

```
sudo systemctl status snmpd
```

10.2 Modification du fichier de configuration snmpd.conf

Le fichier de configuration principal est /etc/snmp/snmpd.conf. Il définit l'adresse d'écoute de l'agent, les vues OID autorisées et les communautés d'accès.

Édition du fichier de configuration SNMP :

```
sudo nano /etc/snmp/snmpd.conf
```

Appliquez les modifications suivantes dans le fichier :

1. Définir l'adresse IP d'écoute de l'agent SNMP (remplacer agentaddress par l'IP du serveur) :

```
agentaddress 192.168.3.31
```

2. Déclarer les vues OID autorisées (system + hrSystem uniquement) :

```
# system + hrSystem groups only
```

```
view   systemonly  included   .1.3.6.1.2.1.1
view   systemonly  included   .1.3.6.1.2.1.25.1
```

3. Définir la communauté SNMP v1/v2c en lecture seule (rocommunity) :

```
# Accès en lecture seule pour le serveur de supervision (192.168.1.11)
# sur la vue systemonly avec la communauté "gourmet"
rocommunity  gourmet  192.168.1.11
rocommunity6 gourmet  default  -V systemonly
```

```
agentaddress 192.168.3.31


###############################################################################
# SECTION: Access Control Setup
#
#   This section defines who is allowed to talk to your running
#   snmp agent.

# Views
#   arguments viewname included [oid]

#  system + hrSystem groups only
view   systemonly  included   .1.3.6.1.2.1.1
view   systemonly  included   .1.3.6.1.2.1.25.1


# rocommunity: a SNMPv1/SNMPv2c read-only access community name
#   arguments:  community [default|hostname|network/bits] [oid | -V view]

# Read-only access to everyone to the systemonly view
rocommunity gourmet 192.168.1.11
rocommunity6 gourmet default -V systemonly
```

Figure 9 — Extrait du fichier /etc/snmp/snmpd.conf après modification

Explication des directives :

- agentaddress 192.168.3.31 : l'agent SNMP écoute uniquement sur cette IP (sécurité)
- view systemonly included ... : restreint l'accès aux OIDs système et hrSystem
- rocommunity gourmet 192.168.1.11 : accès lecture seule depuis le serveur de supervision uniquement
- rocommunity6 gourmet default : accès IPv6 avec la même communauté sur la vue systemonly

> **Note :** La communauté SNMP (ici : « gourmet ») joue le rôle de mot de passe. Ne pas utiliser la valeur par défaut « public » en production. Restreindre toujours l'accès à l'IP du serveur de supervision.

10.3 Redémarrage et vérification du service

Redémarrage de snmpd pour prendre en compte les modifications :

```
sudo systemctl restart snmpd
```

Vérification locale que l'agent répond correctement (depuis le serveur lui-même) :

```
# Test en SNMPv2c — doit retourner le nom du système
snmpwalk -v2c -c gourmet 192.168.3.31 system
```

Test depuis le serveur de supervision (192.168.1.11) :

```
snmpwalk -v2c -c gourmet 192.168.3.31 .1.3.6.1.2.1.1
```

Vérification que le port UDP 161 est bien ouvert :

```
sudo ss -ulnp | grep snmpd
# Résultat attendu : udp  UNCONN  0  0  192.168.3.31:161  ...
```

Note : Si le pare-feu (ufw/iptables) est actif sur le serveur, autorisez le port UDP 161 uniquement depuis l'IP du serveur de supervision : sudo ufw allow from 192.168.1.11 to any port 161 proto udp

---

— Fin de la documentation —