

# Installation

Parfait, on plonge dans **Seafile** en détail ! Voici tout ce qu'il faut savoir pour **maîtriser Seafile** : installation avancée, optimisation, gestion des utilisateurs, sauvegardes, et astuces pour une utilisation fluide en équipe. Je vais te donner des éléments concrets, des exemples de commandes, et des retours d'expérience pour éviter les pièges.

---

## 1. Architecture et Concepts Clés de Seafile

### a. Comment Seafile organise les données ?

Seafile utilise un système de **blocs de fichiers** (comme Git) :

- Chaque fichier est découpé en **blocs de 1 Mo** (par défaut).
- Les blocs sont **hashés** (SHA-1) et stockés dans `/shared/seafile-data`.
- Les métadonnées (noms, permissions) sont stockées dans la **base de données MariaDB**.

#### Avantages :

- **Économie d'espace** : Les blocs identiques (ex : fichiers dupliqués) ne sont stockés qu'une fois.
- **Synchro rapide** : Seuls les blocs modifiés sont transférés.
- **Intégrité des données** : Les hashes permettent de détecter les corruptions.

#### Exemple de structure de dossiers :

```
/srv/seafile/data/  
├─ seafile-data/      # Blocs de fichiers  
├─ seafile-conf/     # Configurations  
└─ logs/             # Logs du serveur
```

### b. Ports utilisés par Seafile

Port	Usage	À exposer ?
8000	Interface web	Oui (via Nginx)

Port	Usage	À exposer ?
8082	API pour le client desktop	Oui (si synchro hors réseau local)
10001	Service de notification	Non (interne)
12001	Service de recherche	Non (interne)

**Conseil** : Dans ton Nginx, expose **uniquement le port 8000** (le reste est géré en interne par Docker).

## 2. Optimisation des Performances

### a. Configuration de Seafile pour Docker

Pour optimiser les performances, ajoute ces variables d'environnement dans ton `docker-compose.yml` :

```
environment:  
  - SEAFILE_SERVER_HOSTNAME=seafile.tacampagne.fr  
  - SEAFILE_ADMIN_EMAIL=admin@tacampagne.fr  
  - SEAFILE_ADMIN_PASSWORD=tonmotdepasse  
  - SEAFILE_MYSQL_HOST=seafile-db  
  - SEAFILE_MYSQL_ROOT_PASSWORD=motdepassebdd  
  - SEAFILE_TIMEZONE=Europe/Paris # Pour les horodatages  
  - SEAFILE_FILE_SERVER_ROOT=https://seafile.tacampagne.fr # URL publique  
  - SEAFILE_ENABLE_FILE_LOCKING=true # Évite les conflits d'édition
```

### b. Tuning de la base de données (MariaDB)

Ajoute ces lignes dans la section `seafile-db` de ton `docker-compose.yml` pour améliorer les performances :

```
command: [  
  '--character-set-server=utf8mb4',  
  '--collation-server=utf8mb4_unicode_ci',  
  '--innodb-buffer-pool-size=512M', # Augmente si tu as beaucoup de fichiers  
  '--max-connections=200'  
]
```

### c. Configuration Nginx pour les gros fichiers

Si tu partages des fichiers > 100 Mo, ajoute ces directives dans ton bloc `server` Nginx :

```
proxy_connect_timeout 300;  
proxy_send_timeout 300;
```

```
proxy_read_timeout    300;
send_timeout          300;
client_max_body_size  10G; # Autorise les uploads jusqu'à 10 Go
```

---

## 3. Gestion des Utilisateurs et Permissions

### a. Créer des utilisateurs en masse

Seafile permet d'importer des utilisateurs via un **fichier CSV**. Exemple de format :

```
Email,Password,Name,Quota (in MB)
user1@tacampagne.fr,motdepasse1,Jean Dupont,1024
user2@tacampagne.fr,motdepasse2,Marie Martin,1024
```

**Commande pour importer** (à exécuter dans le conteneur Seafile) :

```
docker exec -it seafile bash
cd /opt/seafile/seafile-server-latest
./seafile-admin.sh import-users user_list.csv
```

### b. Gérer les groupes

- **Crée un groupe** pour ton équipe :

```
docker exec -it seafile bash
cd /opt/seafile/seafile-server-latest
./seafile-admin.sh create-group "Equipe Campagne"
```

- **Ajoute des utilisateurs au groupe** :

```
./seafile-admin.sh add-group-member "Equipe Campagne" user1@tacampagne.fr
```

### c. Partager un dossier avec un groupe

1. Connecte-toi à l'interface web (`https://seafile.tacampagne.fr`).
  2. Crée un dossier (ex: `Documents Campagne`).
  3. Clique sur **Partager** → Sélectionne le groupe **"Equipe Campagne"** → Choisis les permissions (**Lecture/Ecriture**).
- 

## 4. Sauvegardes et Restauration

# a. Sauvegarde complète (données + DB)

Script de sauvegarde (`/srv/seafiler/backup.sh`) :

```
#!/bin/bash
BACKUP_DIR="/srv/backups/seafiler-$(date +%Y-%m-%d)"
mkdir -p "$BACKUP_DIR"

# Sauvegarde des données
docker-compose -f /srv/seafiler/docker-compose.yml exec seafiler tar -czvf /tmp/seafiler-data.tar.gz
/shared
docker cp seafiler:/tmp/seafiler-data.tar.gz "$BACKUP_DIR"

# Sauvegarde de la base de données
docker-compose -f /srv/seafiler/docker-compose.yml exec seafiler-db mysqldump -uroot -pomotdepassebdd
--all-databases > "$BACKUP_DIR/seafiler-db.sql"

# Nettoyage
docker-compose -f /srv/seafiler/docker-compose.yml exec seafiler rm /tmp/seafiler-data.tar.gz
```

Automatise avec cron :

```
0 2 * * * /bin/bash /srv/seafiler/backup.sh # Sauvegarde tous les jours à 2h
```

# b. Restauration

## 1. Restaure les données :

```
docker cp "$BACKUP_DIR/seafiler-data.tar.gz" seafiler:/tmp
docker-compose -f /srv/seafiler/docker-compose.yml exec seafiler tar -xzvf /tmp/seafiler-
data.tar.gz -C /
```

## 2. Restaure la DB :

```
cat "$BACKUP_DIR/seafiler-db.sql" | docker-compose -f /srv/seafiler/docker-compose.yml exec
-T seafiler-db mysql -uroot -pomotdepassebdd
```

## 3. Redémarre les conteneurs :

```
docker-compose -f /srv/seafiler/docker-compose.yml restart
```

# 5. Sécurité Avancée

## a. Activer le chiffrement côté serveur

Seafiler propose un **chiffrement des fichiers au repos** (server-side encryption) :

### 1. Active-le dans `docker-compose.yml` :

```
environment:
  - SEAFILER_ENABLE_ENCRYPTION=true
```

### 2. Chiffre un dossier existant :

- Va dans l'interface web → Sélectionne un dossier → **Propriétés** → **Activer le chiffrement**.

**Attention** : Si tu perds la clé de chiffrement, les données sont **perdues à jamais**.

## b. Restreindre l'accès par IP

Dans ton Nginx, ajoute une **liste blanche d'IPs** pour limiter l'accès :

```
location / {  
    allow 192.168.1.0/24; # Remplace par ton réseau local ou les IPs de ton équipe  
    allow 82.123.45.67; # IP fixe d'un membre  
    deny all;  
    proxy_pass http://<IP_SERVEUR_A>:8000;  
    ...  
}
```

## c. Activer la double authentification (2FA)

1. Dans l'interface admin ( <https://seafile.tacampagne.fr/sysadmin/> ), va dans **Paramètres** → **2FA**.
2. Active **Google Authenticator** ou **Email OTP**.
3. Demande à tes utilisateurs de configurer le 2FA via leur profil.

---

# 6. Intégration avec d'Outils Externes

## a. Synchronisation avec le client desktop

- **Télécharge le client** : [Seafile Desktop](#) (Windows/macOS/Linux).
- **Configuration** :
  - URL du serveur : <https://seafile.tacampagne.fr>
  - Email/mot de passe de l'utilisateur.
- **Options utiles** :
  - **Synchro sélective** : Pour ne pas tout télécharger.
  - **Verrouillage de fichiers** : Évite les conflits si 2 personnes éditent le même fichier.

## b. Montage en WebDAV (pour les power users)

Seafile supporte le **WebDAV** pour monter le stockage comme un disque réseau :

- **URL WebDAV :** `https://seafiler.tacampagne.fr/seafdav`

- **Exemple de montage sous Linux :**

```
sudo apt install davfs2
```

```
echo "https://seafiler.tacampagne.fr/seafdav /mnt/seafiler davfs user,noauto 0 0" >>  
/etc/fstab
```

```
mount /mnt/seafiler
```

(L'utilisateur devra entrer son email/mot de passe.)

---

## 7. Monitoring et Logs

### a. Vérifier les logs

- **Logs Seafiler :**

```
docker-compose -f /srv/seafiler/docker-compose.yml logs -f seafiler
```

- **Logs Nginx :**

```
tail -f /var/log/nginx/seafiler.tacampagne.fr-access.log
```

### b. Surveiller l'espace disque

```
docker exec seafiler du -sh /shared/seafiler-data
```

### c. Alertes par email

Configure Seafiler pour envoyer des alertes (ex : espace disque faible) :

1. Dans l'interface admin, va dans **Paramètres** → **Email**.
  2. Configure un serveur SMTP (ex : ton serveur mail ou Gmail).
  3. Active les notifications pour les **quotas** et les **erreurs système**.
- 

## 8. Astuces pour les Utilisateurs

### a. Partager un fichier avec un externe

1. **Crée un lien public :**
  - Clique droit sur un fichier/dossier → **Partager** → **Créer un lien**.
  - Définis une **date d'expiration** et un **mot de passe** si besoin.
2. **Envoie le lien** par email ou messagerie.

## b. Récupérer un fichier supprimé

- Seafile garde une **corbeille** (30 jours par défaut).
- Pour restaurer : **Corbeille** → Sélectionne le fichier → **Restaurer**.

## c. Utiliser l'API

Seafile propose une [API REST](#) pour automatiser des tâches (ex : uploads depuis un script Python).  
Exemple pour lister les dossiers :

```
curl -u admin@tacampagne.fr:tonmotdepasse https://seafile.tacampagne.fr/api2/repos/
```

# 9. Résolution des Problèmes Courants

Problème	Solution
<b>Erreur 502 Bad Gateway (Nginx)</b>	Vérifie que le conteneur Seafile est démarré ( <code>docker ps</code> ).
<b>Synchro bloquée</b>	Redémarre le client desktop ou vérifie les logs ( <code>docker logs seafile</code> ).
<b>Quota dépassé</b>	Augmente le quota via l'interface admin ou supprime des fichiers.
<b>Lien public inaccessible</b>	Vérifie que le port <code>8000</code> est bien exposé et que Nginx proxy correctement.

# 10. Pour Aller Plus Loin

## a. High Availability (HA)

Si tu veux une **redondance** (ex : 2 serveurs Seafile) :

- Utilise **Seafile Pro** (version payante) avec support HA.
- Ou configure un **réplica de la base de données** + un partage NFS pour `/shared/seafile-data`.

## b. Intégration avec OnlyOffice

Si tu veux éditer des docs en ligne (comme Nextcloud) :

1. Déploie **OnlyOffice** en conteneur Docker.
  2. Configure l'intégration dans Seafile :
    - Dans l'admin, va dans **Paramètres** → **OnlyOffice**.
    - Renseigne l'URL de ton instance OnlyOffice.
- 

# 11. Ressources Utiles

- **Documentation officielle** : [Seafile Manual](#)
  - **Forum communautaire** : [Seafile Forum](#)
  - **Dépôt Docker** : [Seafile sur Docker Hub](#)
- 

# 12. Prochaines Étapes

1. **Veux-tu que je te génère un script complet pour les sauvegardes incrémentielles (avec rotation) ?**
2. **As-tu besoin d'aide pour configurer OnlyOffice ou un autre outil intégré ?**
3. **Veux-tu un exemple de politique de sécurité (mots de passe, 2FA, etc.) pour ton équipe ?**

Dis-moi ce qui t'intéresse en priorité, et on creuse ! ☐☐

---

Revision #1

Created 2026-03-03 17:23:44 UTC by Nicolas Farrie

Updated 2026-03-03 17:23:59 UTC by Nicolas Farrie