

8 - Stratégie de sauvegarde

Protéger la base, les médias, la configuration et les copies distantes avec des tests de restauration.

- [8.1 - Périmètre et stratégie 3-2-1](#)
- [8.2 - Sauvegarder PostgreSQL](#)
- [8.3 - Snapshots ZFS et réplication TrueNAS](#)
- [8.4 - Copie distante vers Proxmox et validation](#)

8.1 - Périmètre et stratégie

3-2-1

Immich recommande une stratégie 3-2-1 :

- 3 copies des données ;
- 2 types de supports ou systèmes ;
- 1 copie hors du serveur principal.

Éléments à protéger

Élément	Pourquoi
PostgreSQL	utilisateurs, albums, chemins, visages, partages et paramètres
<code>upload</code>	originaux internes
<code>library</code>	originaux organisés si le modèle est actif
<code>profile</code>	profils utilisateurs
<code>backups</code>	dumps automatiques de la base
<code>thumbs</code>	régénérable mais coûteux en temps
<code>encoded-video</code>	régénérable mais coûteux en ressources
bibliothèques externes	originaux hors du stockage interne
configuration	Compose, <code>.env</code> , paramètres de proxy et montages

Exemple adapté

1. copie de production sur TrueNAS ;
2. snapshots ZFS locaux ;
3. réplication ou rsync vers DreamProxmox ;
4. copie supplémentaire déconnectée ou hors site.

Un snapshot sur le même pool protège contre certaines suppressions mais pas contre la panne du pool, le vol ou la destruction du serveur.

Cohérence

Le dump PostgreSQL et les médias doivent correspondre à une période proche. Pour un point de restauration parfaitement cohérent :

1. mettre Immich en maintenance ou arrêter les écritures ;
2. créer le dump ;
3. copier ou snapshotter les médias ;
4. reprendre le service.

Les dumps automatiques quotidiens offrent une bonne protection, mais il faut aussi sauvegarder le dossier qui les contient.

Objectifs de reprise

Définir :

- RPO - quantité maximale de données récentes pouvant être perdue ;
- RTO - durée maximale de remise en service ;
- rétention quotidienne, hebdomadaire et mensuelle ;
- responsable du contrôle ;
- emplacement des secrets de restauration.

Vérification

Chaque sauvegarde doit être contrôlée :

```
gzip -t dump.sql.gz  
sha256sum dump.sql.gz  
find /chemin/sauvegarde -type f | wc -l  
du -sh /chemin/sauvegarde
```

Le test réel consiste à restaurer dans un environnement isolé, ouvrir des photos, vérifier albums, comptes, recherche et bibliothèques externes.

Référence : <https://docs.immich.app/administration/backup-and-restore/>

8.2 - Sauvegarder PostgreSQL

Immich crée automatiquement des dumps PostgreSQL dans :

```
UPLOAD_LOCATION/backups
```

La rétention et l'horaire se règlent dans :

```
Administration > Settings > Backup
```

Le réglage par défaut documenté est un dump quotidien à 02:00 avec conservation des 14 derniers dumps.

Déclencher un dump depuis Immich

```
Administration > Job Queues > Create job > Create Database Dump
```

Dump manuel Docker

Identifier le conteneur :

```
docker ps --format '{{.Names}} {{.Image}}' | grep -Ei 'immich.*postgres|postgres.*immich'
```

Créer un dump :

```
mkdir -p /srv/backups/immich

docker exec -t immich_postgres \
  pg_dump --clean --if-exists --dbname=immich --username=postgres \
```

```
| gzip > /srv/backups/immich/immich-$(date +%F-%H%M).sql.gz
```

Vérifier :

```
gzip -t /srv/backups/immich/immich-AAAA-MM-JJ-HHMM.sql.gz  
ls -lh /srv/backups/immich
```

TrueNAS

Découvrir le conteneur exact :

```
sudo docker ps --format '{{.Names}} {{.Image}}' | grep -Ei 'immich|postgres|vector'
```

Puis adapter :

```
sudo docker exec -t NOM_CONTENEUR_POSTGRES \  
pg_dump --clean --if-exists --dbname=immich --username=postgres \  
| gzip > /mnt/HDD_DATA_TRUENAS/IMMICH/data/backups/manuel-$(date +%F-%H%M).sql.gz
```

Ce que le dump ne contient pas

- photos ;
- vidéos ;
- miniatures ;
- fichiers externes ;
- configuration `.env` ;
- paramètres du reverse proxy.

Règles

- ne pas utiliser une copie brute du dossier PostgreSQL comme seule sauvegarde ;
- protéger le dump avec les mêmes exigences de confidentialité que les photos ;
- copier le dump hors du serveur ;
- tester `gzip -t` ;
- tester une restauration ;
- utiliser une version compatible.

Le processus de restauration a changé avec Immich v2.5.0. Pour un ancien dump, consulter la documentation correspondant à la version de création.

Référence : <https://docs.immich.app/administration/backup-and-restore/>

8.3 - Snapshots ZFS et réplication TrueNAS

Les snapshots ZFS protègent rapidement l'état d'un dataset. Ils ne remplacent pas un dump PostgreSQL logique ni une copie hors du pool.

Snapshot manuel

Après un dump de base :

```
sudo zfs snapshot HDD_DATA_TRUENAS/IMMICH/data@manuel-$(date +%F-%H%M)
sudo zfs snapshot HDD_DATA_TRUENAS/IMMICH/pgData@manuel-$(date +%F-%H%M)
```

Adapter les noms ZFS réels obtenus avec :

```
sudo zfs list
```

Tâche périodique TrueNAS

Dans `Data Protection > Periodic Snapshot Tasks` :

1. choisir le dataset parent ou les datasets enfants ;
2. activer la récursivité si nécessaire ;
3. définir l'horaire ;
4. définir la durée de conservation ;
5. éviter une rétention qui remplit le pool ;
6. vérifier les snapshots créés.

Cohérence PostgreSQL

Un snapshot de `pgData` pendant que PostgreSQL écrit est généralement comparable à un arrêt brutal. PostgreSQL sait souvent récupérer, mais ce snapshot ne doit pas remplacer un dump

logique.

Pour un snapshot applicatif cohérent :

1. activer la maintenance ;
2. créer un dump ;
3. arrêter Immich si un point strict est requis ;
4. prendre les snapshots ;
5. redémarrer ;
6. vérifier les services.

Réplication

Dans `Data Protection > Replication Tasks` :

- source : datasets Immich ;
- destination : autre pool, autre TrueNAS ou serveur compatible ;
- transport : local ou SSH ;
- snapshots : tâche périodique correspondante ;
- rétention : cohérente avec la source et la capacité.

Vérifier

```
sudo zfs list -t snapshot | grep -i immich  
sudo zpool status  
sudo zpool list
```

Restauration d'un fichier

Préférer cloner ou parcourir un snapshot puis copier le fichier voulu. Éviter un rollback complet sans analyse, car il supprime les modifications plus récentes du dataset.

Après réplication

Vérifier que la destination contient :

- les médias ;
- les dumps ;
- les profils ;
- les datasets séparés ;
- les bibliothèques externes si elles font partie du plan.

8.4 - Copie distante vers Proxmox et validation

Ton environnement utilise déjà une liaison SSH de TrueNAS vers Proxmox. Elle peut transporter une copie supplémentaire des données Immich.

Préparer la destination

Sur Proxmox :

```
sudo mkdir -p /srv/backups/immich
sudo chown UTILISATEUR_BACKUP:UTILISATEUR_BACKUP /srv/backups/immich
```

Restreindre la clé SSH au compte et à l'usage de sauvegarde si possible.

Simulation rsync

Depuis TrueNAS :

```
rsync -aHn --numeric-ids --info=progress2 \  
/mnt/HDD_DATA_TRUENAS/IMMICH/data/ \  
UTILISATEUR_BACKUP@ADRESSE_PROXMOX:/srv/backups/immich/data/
```

Après vérification :

```
rsync -aH --numeric-ids --info=progress2 \  
/mnt/HDD_DATA_TRUENAS/IMMICH/data/ \  
UTILISATEUR_BACKUP@ADRESSE_PROXMOX:/srv/backups/immich/data/
```

Ne pas ajouter `--delete` tant qu'une politique de miroir et de rétention séparée n'est pas en place.

Base PostgreSQL

Créer le dump avant rsync afin que le dossier `backups` contienne une version récente et cohérente.

Borg

Immich fournit un modèle Borg qui sauvegarde la base et les médias avec déduplication et rétention. Borg peut réduire l'espace par rapport à des copies complètes répétées. Il demande cependant une configuration, une clé et des tests de restauration.

Contrôles de destination

```
ssh UTILISATEUR_BACKUP@ADRESSE_PROXMOX \  
'du -sh /srv/backups/immich/data; find /srv/backups/immich/data -type f | wc -l'
```

Comparer quelques sommes :

```
sha256sum /mnt/HDD_DATA_TRUENAS/IMMICH/data/backups/FICHER.sql.gz  
ssh UTILISATEUR_BACKUP@ADRESSE_PROXMOX \  
'sha256sum /srv/backups/immich/data/backups/FICHER.sql.gz'
```

Script fourni

Le pack contient :

```
./scripts/sauvegarde_immich_docker.sh
```

Il crée un dump logique puis copie les médias sans suppression vers un dossier de sauvegarde. Lire et configurer ses variables avant exécution.

Test trimestriel conseillé

1. choisir une sauvegarde ;
2. la restaurer sur un réseau isolé ;

3. vérifier plusieurs originaux ;
4. ouvrir des albums ;
5. tester un compte ;
6. vérifier les bibliothèques externes ;
7. documenter la durée et les problèmes.

Référence Borg : <https://docs.immich.app/guides/template-backup-script/>