Stockage & Systèmes de Fichiers

- Synology NAS (NFS/ACL)
  - Résoudre les erreurs de permission NFS (EACCES) entre Synology et Docker
- Linux
  - Cheat Sheet - Commandes utiles Linux (Debian & Oracle Linux)
- ReFS
  - Troubleshooting ReFS - Guide de dépannage
  - ReFS - Présentation, Supervision et Dépannage

Synology NAS (NFS/ACL)

Résoudre les erreurs de permission NFS (EACCES) entre Synology et Docker

□□ Problème d'ACL Synology avec NFS + Docker

> **TL;DR** : Ton conteneur Docker ne peut pas écrire sur ton partage NFS Synology malgré des permissions `777` ? C'est l'ACL Windows qui prime sur les bits Unix. Solution : `synoacltool -del` récursif.

□□ Contexte

Tu as configuré un partage NFS sur ton Synology pour stocker les backups de Proxmox Backup Server (PBS) tournant dans Docker. PBS démarre, puis crash avec :

```
Error: unable to create rrdb stat dir - EACCES: Permission denied
```

Pourtant, `ls -la` affiche `drwxrwxrwx` et le propriétaire est bien `backup:backup` (UID 34).

La cause racine : Sur DSM, les dossiers partagés créés sur Btrfs/ext4 ont **l'ACL Windows activée par défaut**. Cette ACL prend le pas sur les permissions Unix classiques, même via NFS. Résultat : les bits `rwx` visibles sont ignorés, et l'écriture est refusée pour l'UID du conteneur.

□□ Symptômes typiques

- Container Docker qui boucle en crash (`restart: always` + erreur `EACCES`).
- `ls -la` affiche `drwxrwxrwx` ou `0777`, mais `mkdir` échoue.
- Les lignes `ls -la` ont un `+` après les permissions : `drwxr-xr-x+`.
- Le squash NFS est déjà sur "Pas de mappage" — donc ce n'est pas ça.

□□ Diagnostic rapide

1. Identifier l'UID attendu dans le conteneur

```
docker run --rm --entrypoint sh IMAGE -c "id backup"
# Exemple : uid=34(backup) gid=34(backup)
```

2. Vérifier les permissions actuelles sur l'hôte

```
ls -la /mnt/ton-partage-nfs
# Cherche le + après les permissions
```

3. Tester l'écriture réelle avec le bon UID

```
docker run --rm -v /mnt/ton-partage-nfs:/data --user 34:34 --entrypoint sh IMAGE \
  -c "mkdir -p /data/test && echo OK || echo FAIL"
```

Si `FAIL` malgré `777` → **ACL Synology en cause**.

4. Confirmer via SSH sur le Synology

```
ssh admin@IP_SYNOLOGY
sudo synoacltool -get /volume1/TonDossier
# Si tu vois des entrées [0], [1], etc. → ACL active
```

🔧 Résolution (étape par étape)

Étape 1 : Supprimer l'ACL du dossier racine

```
sudo synoacltool -del /volume1/TonDossier
```

Étape 2 : Retirer les flags d'archive ACL

```
sudo synoacltool -del-archive /volume1/TonDossier has_ACL
sudo synoacltool -del-archive /volume1/TonDossier is_support_ACL
```

Étape 3 : Nettoyer récursivement toutes les ACL des sous-éléments

```
sudo find /volume1/TonDossier -exec synoacltool -del {} \;
```

Étape 4 : Vérifier qu'il n'y a plus de `+`

```
ls -la /volume1/TonDossier
# Plus de + après les permissions (sauf @eaDir, dossier système)
```

Étape 5 : Remettre des permissions Unix propres

```
chown -R 34:34 /volume1/TonDossier
chmod -R 0755 /volume1/TonDossier
```

Étape 6 : Retester depuis l'hôte Docker

```
docker run --rm -v /mnt/ton-partage-nfs:/data --user 34:34 --entrypoint sh IMAGE \
  -c "mkdir -p /data/test && echo OK || echo FAIL"
```

Si `OK` → □ C'est résolu.

□□ Bonnes pratiques préventives

Pour tes futurs partages NFS Docker :

Réglage	Valeur recommandée
Squash	Pas de mappage (No mapping)
Sécurité	`sys` uniquement (décoche Kerberos si pas utilisé)
Permissions	Appliquer `synoacltool -del` dès la création si tu utilises Docker

---

□□ Référence rapide (copier-coller)

```
# SSH sur Synology
ssh admin@IP_SYNOLOGY

# Supprimer ACL
sudo synoacltool -del /volume1/TonDossier
sudo synoacltool -del-archive /volume1/TonDossier has_ACL
sudo synoacltool -del-archive /volume1/TonDossier is_support_ACL
sudo find /volume1/TonDossier -exec synoacltool -del {} \;

# Vérification
ls -la /volume1/TonDossier
```

```
# Côté hôte Docker
chown -R 34:34 /mnt/ton-partage-nfs
chmod -R 0755 /mnt/ton-partage-nfs

# Test
docker run --rm -v /mnt/ton-partage-nfs:/data --user 34:34 --entrypoint sh IMAGE \
  -c "mkdir -p /data/test && echo OK || echo FAIL"
```

□□ Le saviez-vous ?

> Les ACL (Access Control Lists) sont un héritage du monde Windows (NTFS). Synology les a intégrées pour faciliter la compatibilité SMB, mais elles créent des conflits silencieux avec les workflows Linux/NFS/Docker qui s'attendent à des permissions Unix classiques. C'est un peu comme essayer de conduire une voiture avec un volant à droite sur une autoroute française : techniquement possible, mais tout le système est conçu pour l'autre sens.

Auteur : Jonathan BIODORE
Date : 27 septembre 2026
Tags : #Synology #NFS #Docker #Proxmox #ACL #Troubleshooting

Linux

Linux

Cheat Sheet - Commandes utiles Linux (Debian & Oracle Linux)

Redémarrer une interface réseau
ifdown ens224 && ifup ens224

ReFS

Troubleshooting ReFS - Guide de dépannage

□□ Vue d'ensemble

ReFS (Resilient File System) protège les données via des **checksums** et de l'**auto-réparation**, mais certains scénarios (perte d'alimentation, panne matérielle, corruption de métadonnées) peuvent rendre un volume **RAW** ou inaccessible.

Ce guide couvre les **Event IDs critiques**, les **commandes de diagnostic**, et les **procédures de récupération** basées sur la documentation officielle Microsoft. [46]

1□ Event IDs à surveiller

□□ Journal `Microsoft-Windows-DeviceSetupManager/Admin` [46]

Event ID	Signification	Gravité
131	Structure du système de fichiers ne peut pas être corrigée	□□ Critique
133	Erreur de checksum non corrigée (fichier/dossier concerné indiqué)	□□ Critique
135	Volume formaté ReFS mais impossible à monter — état "recovery failed"	□□ Critique
140	Volume RAW ou périphérique occupé	□□ Élevé

□□ Journal `Système`

Event ID	Signification
55	Erreur générique de système de fichiers
129	Réinitialisation du périphérique de stockage (timeout SAN/iSCSI)

□□ Journal `VSS / Backup`

Event ID	Signification
12289	Échec de création de shadow copy
8193	Erreur VSS Writer

□□ **Astuce terrain** : L'Event ID 133 mentionne souvent le nom de l'objet corrompu (ex: "*Object ID Table*", "*Container Table*", "*Duplicate Container Table*"). Ces tables sont des métadonnées internes ReFS — leur corruption est un signe direct de problème disque ou de coupure brutale. [48][59]

2□ Causes courantes de corruption [46]

- ⚡ **Perte d'alimentation** (coupure brutale sans arrêt propre)
- □□ **Panne matérielle** (disque, contrôleur RAID, câble SAS/SATA)
- □□ **Version ReFS non supportée** (mismatch entre OS et version du volume)
- □ **Processus en arrière-plan non terminés** (dédup, scrubbing interrompu)

3□ Diagnostic initial

Étape 1 — Vérifier l'état du volume

```
Get-Volume | Select-Object DriveLetter, FileSystemType, HealthStatus, OperationalStatus
```

Étape 2 — Vérifier la version ReFS

```
fsutil fsinfo refsinfo <Drive>
```

Étape 3 — Identifier le matériel en cause

1. Consulter les journaux d'événements pour des erreurs matérielles récurrentes.
2. Lancer des diagnostics **SMART** sur tous les disques physiques.
3. Remplacer immédiatement tout disque défaillant.
4. Vérifier que firmware, BIOS et pilotes sont à jour et compatibles (surtout en S2D). [46]

4□ Procédure de récupération — Volume RAW (Event 133/135)

⚠ **Important** : Microsoft ne fournit **aucun utilitaire de réparation en ligne** pour ReFS comme `chkdsk` sur NTFS. La méthode officielle est le **salvage** vers un disque sain. [46][57]

Étape 1 — Préparer un disque de destination

Un second disque, de taille égale ou supérieure au volume corrompu.

Étape 2 — Lancer le salvage

```
refsutil salvage -s <SourceVolume> -d <DestinationFolder>
```

- `<SourceVolume>` : lettre du volume corrompu (ex: `D:`)
- `<DestinationFolder>` : chemin sur le disque sain (ex: `E:\Recovery`)

Étape 3 — Si le salvage échoue

- □□ Examiner les logs générés par le processus de salvage.
- □□ Vérifier le matériel de stockage (SMART, contrôleur).
- □□ Envisager un utilitaire tiers de récupération de données.
- □□ **Si un backup récent existe** : reformater le volume et restaurer plutôt que de s'acharner sur le salvage.

- □□ Contacter le **support Microsoft** en joignant les logs de salvage + les journaux d'événements. [46]

5□ Désactiver temporairement la validation d'intégrité

Si le volume ne monte toujours pas après un salvage échoué, une option avancée (à utiliser avec **précaution**, idéalement en coordination avec le support Microsoft) :

1. Ouvrir `regedit` sur le système où le volume est monté.
2. Naviguer vers :

   ```
   HKLM\SYSTEM\CurrentControlSet\Control\FileSystem\
   ```

3. Définir `RefsDisableVolumeIntegrityValidation` à **0**.
4. Retenter le montage du volume.
5. Si l'échec persiste, retenter le salvage, ou escalader vers un correctif kernel/registre via le support Microsoft. [46]

⚠ Cette manipulation ne **corrige pas** la corruption — elle contourne temporairement une vérification pour permettre l'accès aux données.

6□ Cas particulier : ReFS + Storage Spaces / S2D

Si le volume ReFS a l'**Integrity Streams** activé et repose sur **Storage Spaces**, le système peut **auto-réparer** certaines corruptions grâce à la redondance (mirror/parity). [50][52]

Actions recommandées :

```
# Lancer un health-check manuel sur le pool
Get-StoragePool | Get-PhysicalDisk | Get-StorageHealthAction


# Réparer un volume Storage Spaces après remplacement disque
```

```
Repair-VirtualDisk -FriendlyName "<NomDuVolume>"
```

- □□ Configurer un **health-check hebdomadaire automatique** pour détecter et corriger la corruption avant qu'elle ne s'aggrave. [50]
- ⚠ Le health-check **détecte** la corruption mais ne la répare pas toujours seul — une action manuelle reste parfois nécessaire.

7□ Collecte des journaux de cluster (environnement S2D/CSV)

Si le volume ReFS problématique est un **CSV** (Cluster Shared Volume) dans un cluster Hyper-V/S2D :

```
Import-Module FailoverClusters


# Log des 15 dernières minutes, tous les nœuds
Get-ClusterLog -TimeSpan 15 -Destination C:\ClusterLogs -UseLocalTime
```

- □□ Les fichiers sont déposés dans `C:\Windows\Cluster\Reports` par défaut (ou dans `-Destination` si spécifié). [47][49][53]
- □□ Rechercher la section `DiagnosticVerbose` dans le `cluster.log` pour les détails bas niveau. [53]
- □ Sans `-TimeSpan`, le fichier généré peut être **très volumineux** — toujours cibler une fenêtre de temps précise autour de l'incident. [60]

8□ Tableau récapitulatif — Action par symptôme

Symptôme	Event ID	Action immédiate
Volume passé en **RAW**	133, 135	`refsutil salvage`, puis restaurer depuis backup
Structure système non corrigible	131	Vérifier matériel, tenter salvage
Montage impossible / périphérique occupé	140	Vérifier verrous, redémarrer service storage

Symptôme	Event ID	Action immédiate
Erreur checksum sur table interne	133	Vérifier SMART disques, envisager salvage
Réinitialisation stockage répétée	129	Vérifier réseau SAN/iSCSI, câblage, contrôleur
Échec shadow copy / backup	12289, 8193	Vérifier VSS Writers, espace disque libre
Volume CSV en échec (cluster)	—	`Get-ClusterLog`, analyser `DiagnosticVerbose`

---

9 Bonnes pratiques préventives

- Activer les **Integrity Streams** sur les données critiques (checksums + auto-réparation via Storage Spaces).
- Toujours coupler ReFS avec de la **redondance** (mirror, parity) — ReFS seul sur disque unique n'offre pas de réparation automatique réelle.
- Mettre en place des **backups réguliers et testés** — c'est la seule garantie de récupération fiable en cas de corruption sévère.
- Surveiller proactivement les Event IDs listés ci-dessus via un outil de monitoring (Centreon, par exemple).
- Maintenir firmware/BIOS/pilotes à jour, en particulier sur les configurations S2D.
- Ne pas utiliser ReFS sur du matériel non certifié ou en configuration à disque unique pour des données critiques.

Sources

- Guidance for troubleshooting ReFS volumes — Microsoft Learn [46]
- Get-ClusterLog — Microsoft Learn [47]
- Cluster Log Enhancements — Tech Community [53]
- Discussions terrain Veeam / Reddit sur Event ID 133 [48][50][52][59]

ReFS - Présentation, Supervision et Dépannage

□□ Qu'est-ce que ReFS ?

ReFS est un système de fichiers moderne conçu par Microsoft pour **Windows Server**, optimisé pour :

- □ **Intégrité des données** (protection contre la corruption avec checksums)
- □ **Virtualisation** (Hyper-V, machines virtuelles)
- □ **Scénarios de haute disponibilité** (Storage Spaces Direct, clusters)
- □ **Gros volumes de données** (jusqu'à 35 PB théoriques)

⚠ **Important** : ReFS n'est **pas un remplacement universel de NTFS**. Il est conçu pour des **workloads spécifiques** (virtualisation, stockage résilient). nakivo

---

□□ Processus liés à ReFS

ReFS s'appuie sur plusieurs composants système :

Processus / Service	Rôle
System (ntoskrnl.exe)	Gestion kernel du système de fichiers □□
Storage Spaces (storsvc.dll)	Si ReFS est utilisé avec Storage Spaces
Filter Manager (fltmgr.sys)	Gestion des filtres de système de fichiers
VSS (Volume Shadow Copy Service)	Snapshots et backups
Cluster Service (clussvc.exe)	Si utilisé en environnement cluster

□□ **Astuce** : Utilisez `Get-Process` et `Get-Service` pour surveiller l'activité liée au stockage :

```
Get-Service -Name "*stor*" | Select-Object Name, Status
```

Event IDs critiques à surveiller

Journal **Microsoft-Windows-DeviceSetupManager/Admin**

learn.microsoft

Event ID	Signification	Action
131	Problème d'initialisation du volume	Vérifier l'état du disque
133	Volume passé en **RAW**	Données inaccessibles - urgence !
134	Échec de montage du volume	Métadonnées corrompues
135	Volume RAW ou inaccessible	Réparation nécessaire
137	Corruption de métadonnées	Checksum errors
140	Périphérique occupé ou erreur de montage	Conflit d'accès

Journal **Système** learn.microsoft

Event ID	Signification
55	Erreur de système de fichiers (NTFS/ReFS)
129	Réinitialisation de l'appareil de stockage

Journal **VSS / Backup** learn.microsoft

Event ID	Signification
12289	Échec de création de shadow copy
8193	Erreur VSS Writer

□□ Commandes de diagnostic essentielles

```
# Vérifier l'état des volumes ReFS
Get-Volume | Where-Object FileSystemType -EQ "ReFS" | Select-Object DriveLetter, HealthStatus,
OperationalStatus

# Vérifier l'intégrité avec ReFS (auto-correction si possible)
Repair-Volume -DriveLetter X -Scan

# Forcer une réparation (si nécessaire)
Repair-Volume -DriveLetter X -OfflineScanAndFix

# Logs de cluster (si environnement clusterisé)
Get-ClusterLog -UseLocalTime -Destination "C:\ClusterLogs"
```

⚡ Bonnes pratiques ReFS

□ À faire :

- □□ Utiliser ReFS pour **Hyper-V** (stockage VM) nakivo
- □□ Activer **integrity streams** pour les données critiques
- □□ Combiner avec **Storage Spaces Direct** pour la résilience
- □□ Monitorer régulièrement les **Event IDs** cités plus haut

□ À éviter :

- □□ ReFS sur le **volume système** (sauf preview Windows Server 2025+) learn.microsoft
- □□ ReFS pour des **workloads transactionnels** (SQL, Exchange)
- □□ Oublier de tester vos **backups** avec ReFS
- □□ Utiliser ReFS sur des **postes clients** (non supporté) nakivo

---

□□ Scénarios de dépannage rapide

Symptôme	Event ID	Action
Volume en **RAW**	133, 135	`Repair-Volume`, vérifier Storage Spaces
Échec de **montage**	134, 137, 140	Checksum errors → restaurer depuis backup
Backup VSS échoue	12289, 8193	Vérifier VSS Writers, espace libre
Performance lente	-	Vérifier fragmentation, privilégier 3-way mirror learn.microsoft

---

□□ Ressources officielles Microsoft

- □□ Dépannage des volumes ReFS - Microsoft Learn learn.microsoft
- □□ ReFS sur Windows Server - Documentation
- □□ ReFS Boot Volume (preview 2025) learn.microsoft

□□ Quiz rapide (pour valider votre compréhension)

1. **Quel Event ID indique un volume ReFS passé en RAW ?**
2. **Peut-on utiliser ReFS pour le volume système en production ?**
3. **Quelle commande PowerShell répare un volume ReFS ?**

(Réponses : 133/135 | Non, sauf preview | `Repair-Volume`)