

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

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

- ☐ 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	<code>refsutil salvage</code> , 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]