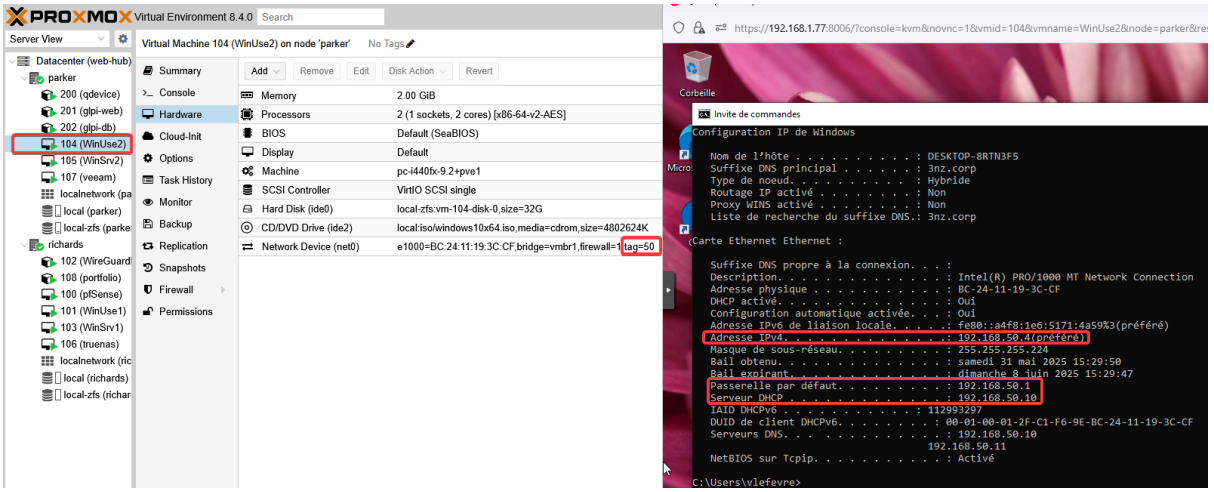
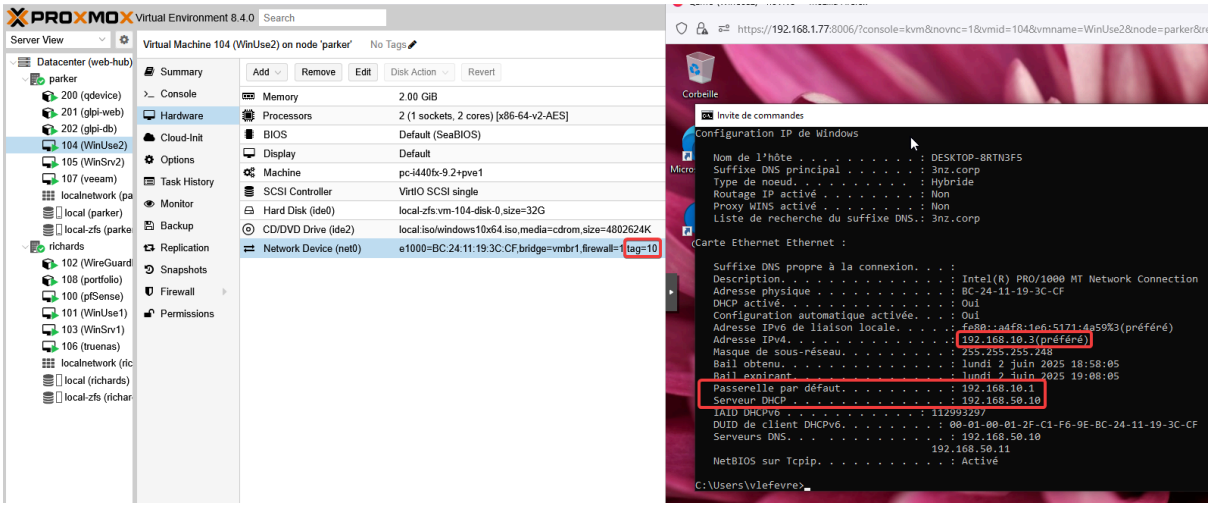
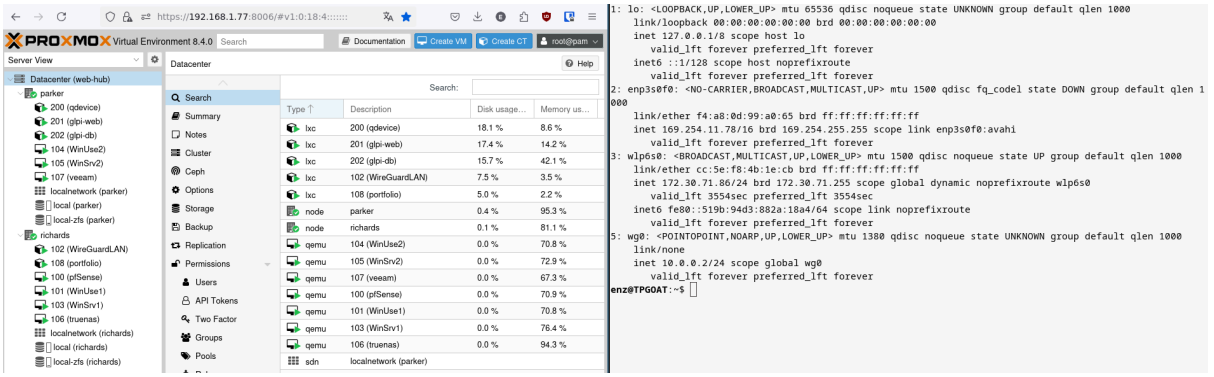
Rapport de tests

Configuration des vlans et du dhcp :
Lorsque l'on assigne le tag vlan 50 au network device de la machine sur proxmox alors celle-ci prend bien une ip du vlan 50



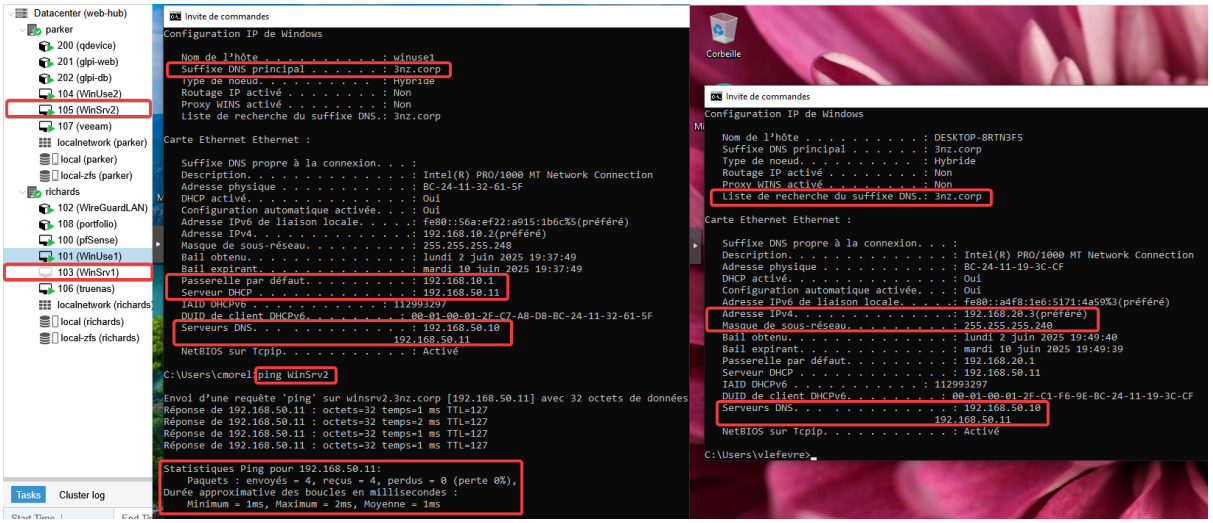


Tunnel VPN fonctionnel depuis un autre réseau :
L'accès à l'infra fonctionne aussi :



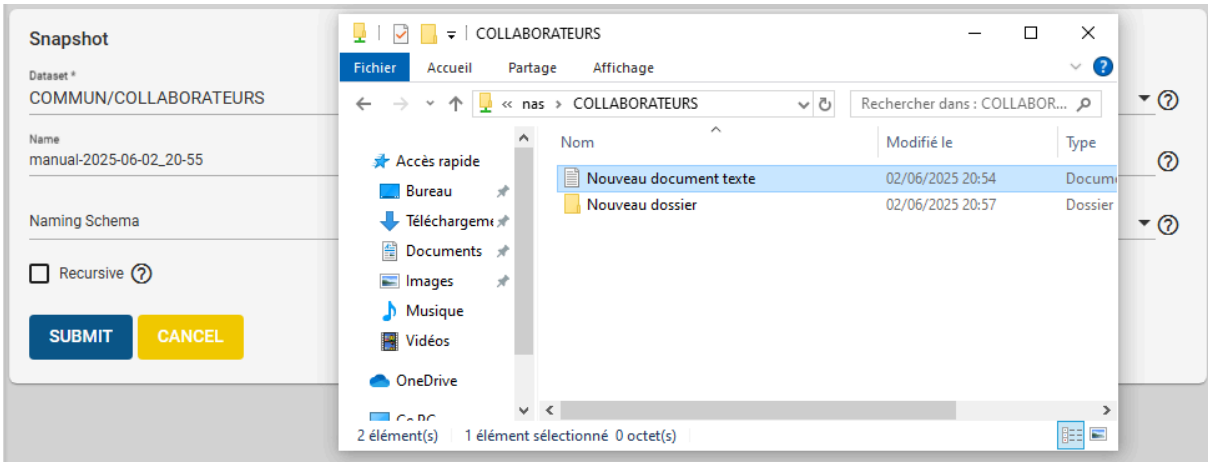
Redondance AD, DNS + DHCP Failover :
Si WinSrv1 tombe en panne, les machines clientes récupèrent une adresse ip, peuvent se

connecter au domaine et résolvent des noms DNS grâce au WinSrv2 :

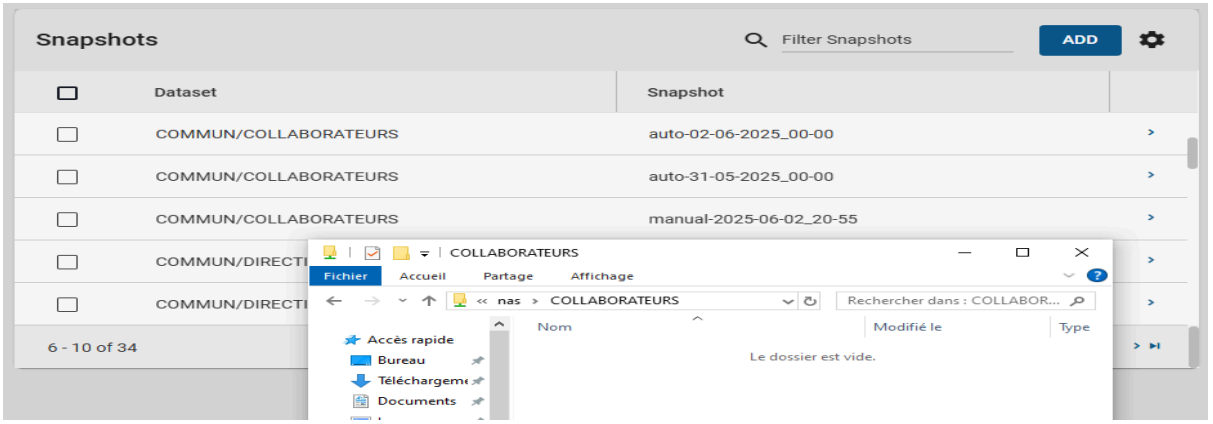


Test et restauration des snapshots sur TrueNAS :
Les snapshots sont bien créée tous les jours :

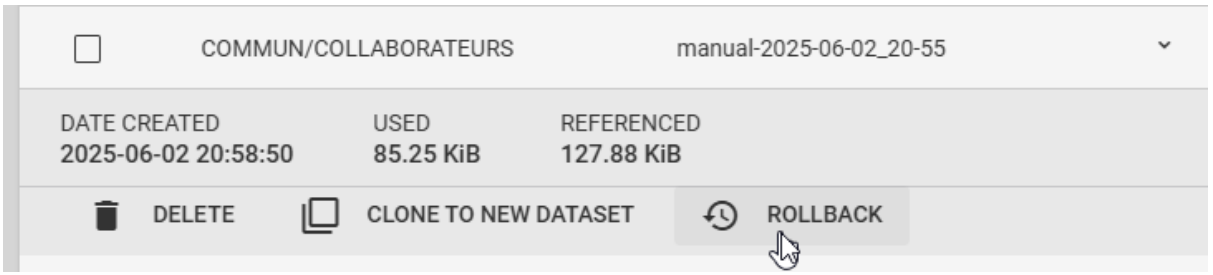
Création d'une snapshot pour le test :

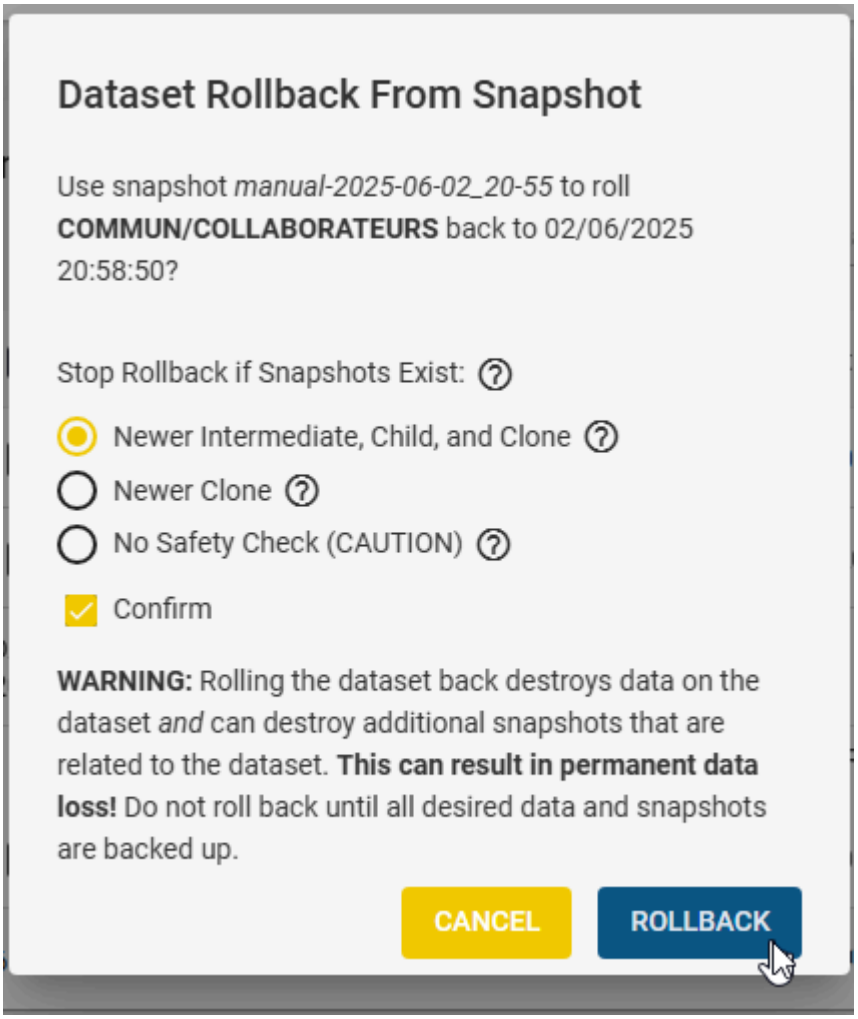


Suppression des dossiers/fichiers :

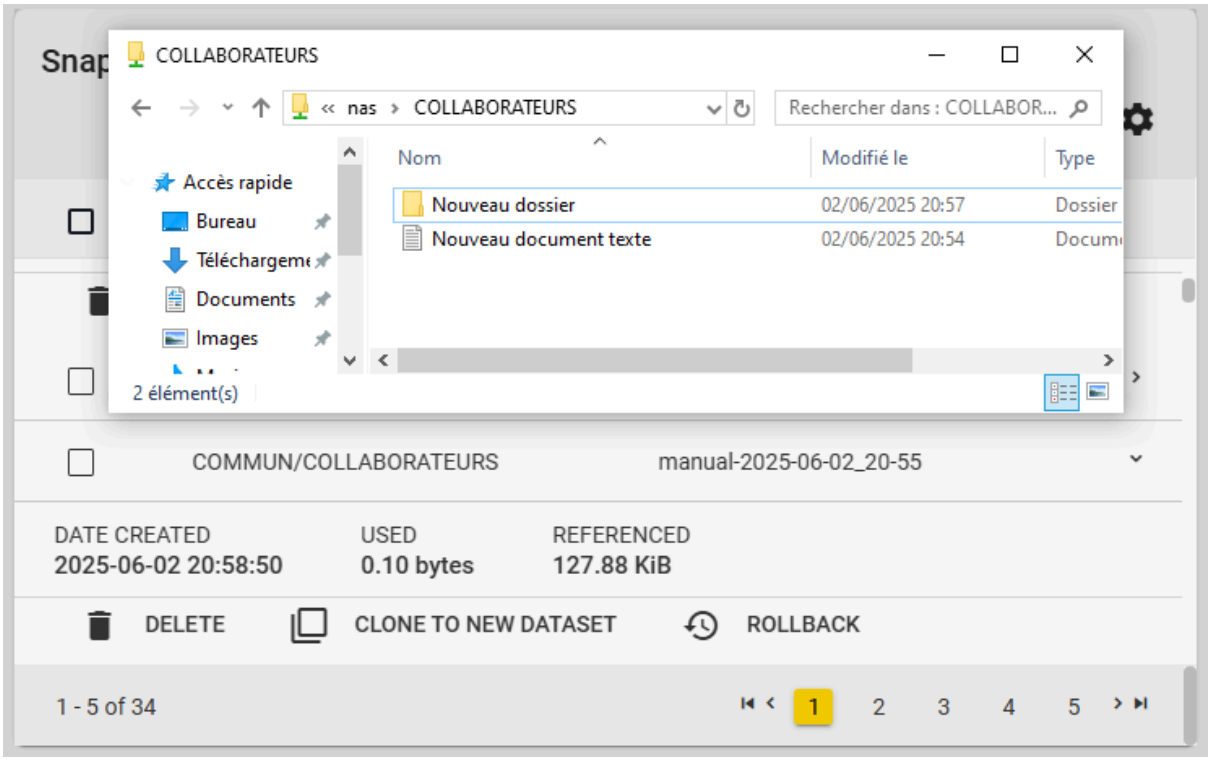


Je cherche la snapshot dans Storage > Snapshots, la déplie avec la flèche bleu > et clique sur rollback :

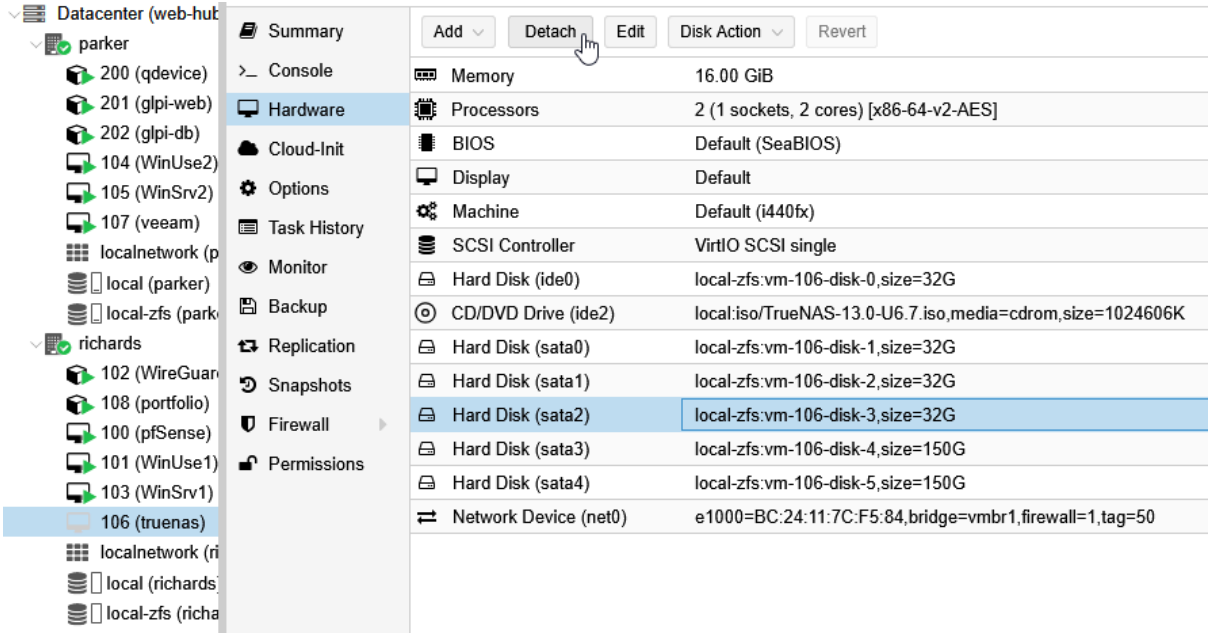


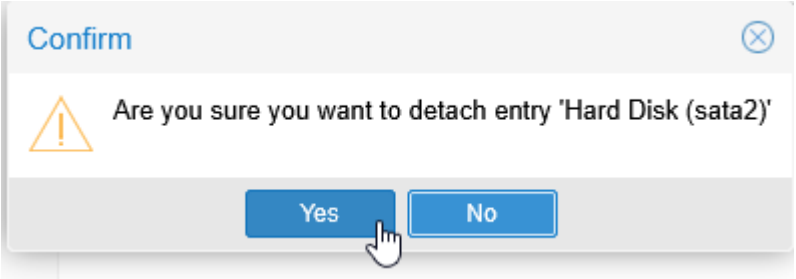


Les fichiers/dossiers sont récupérés :

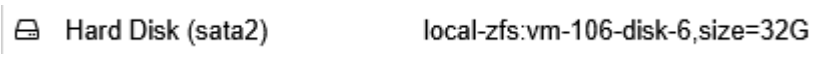


Simulation d'une panne disque dur et remplacement du disque défectueux :
J'éteins la VM truenas et détache un disque :

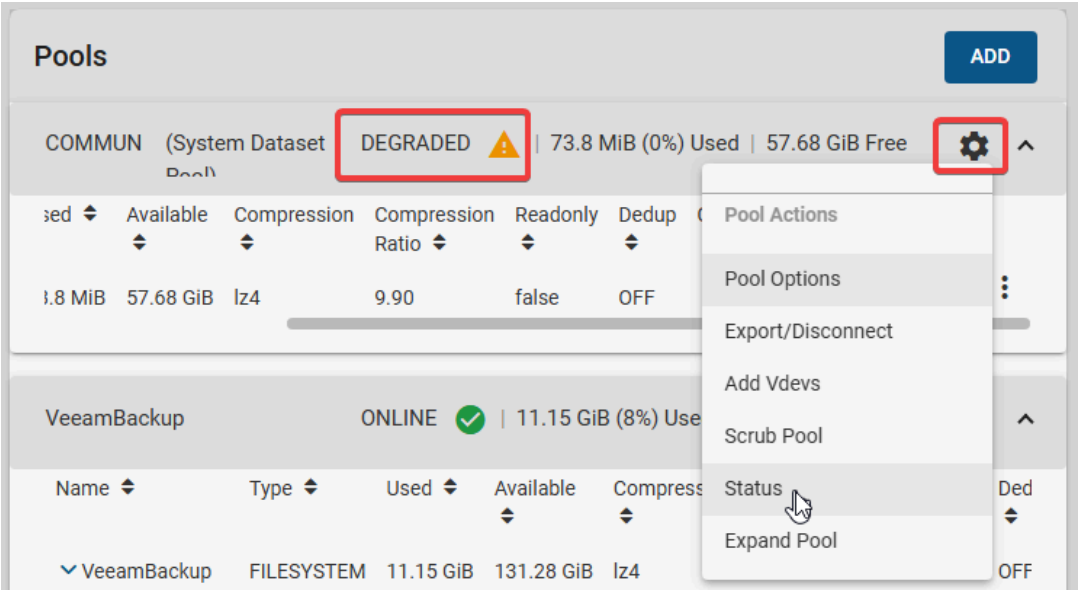




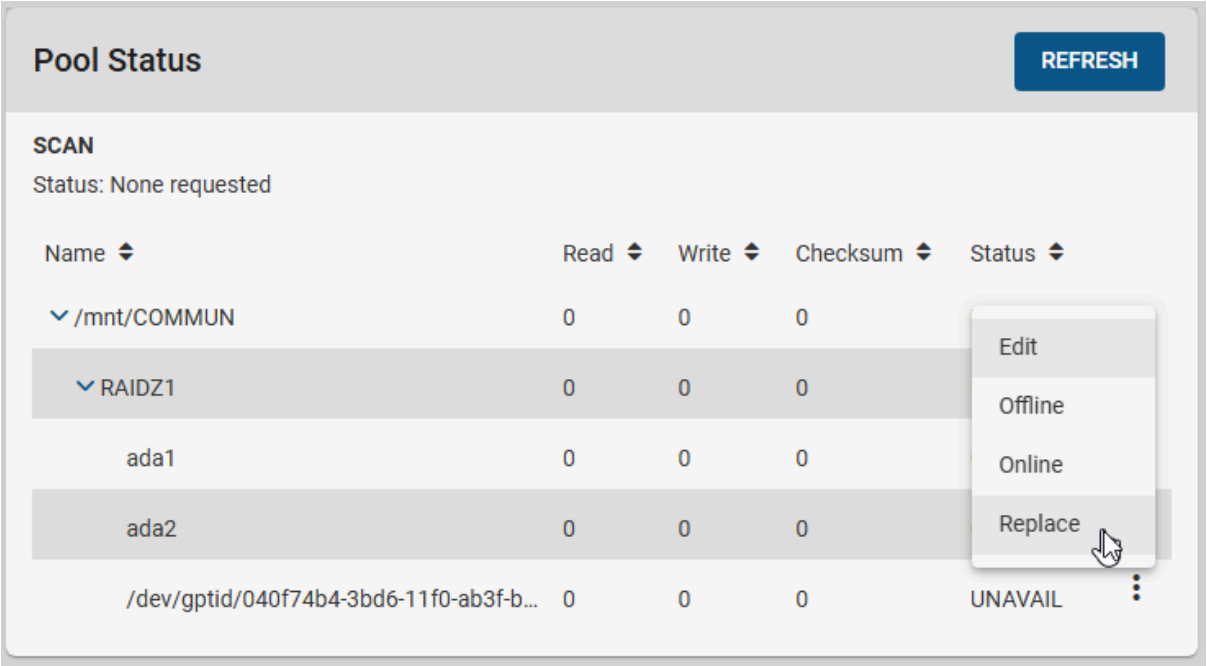
Ajouter un disque de même taille que ceux dans votre raid :

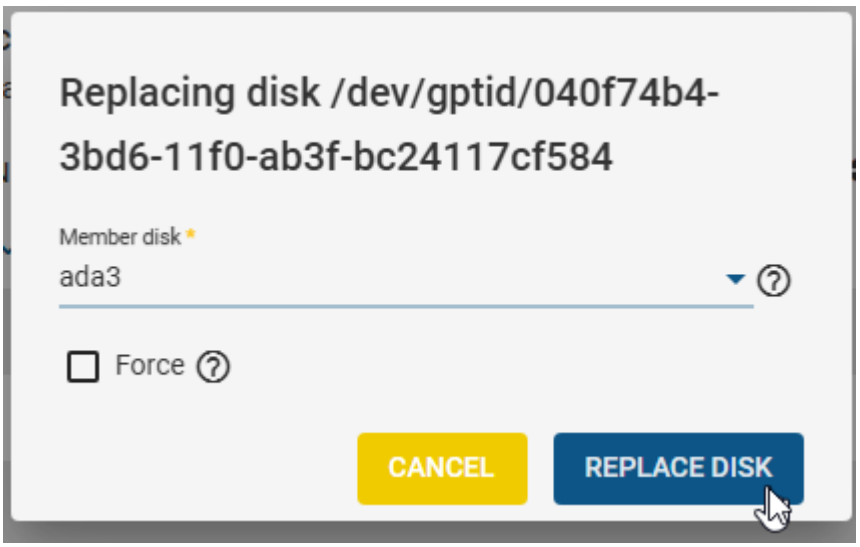


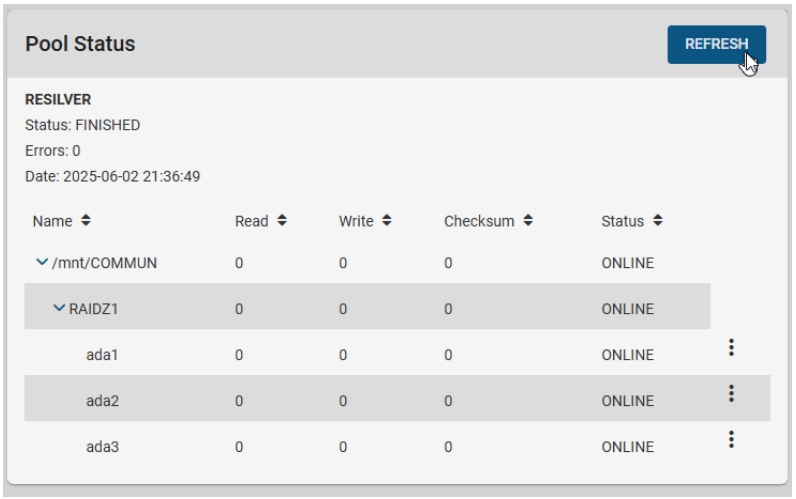
Redémarrer la VM, allez dans Storage > Pools, allez sur la pool qui est en état degraded et cliquez sur l'engrenage, puis status :



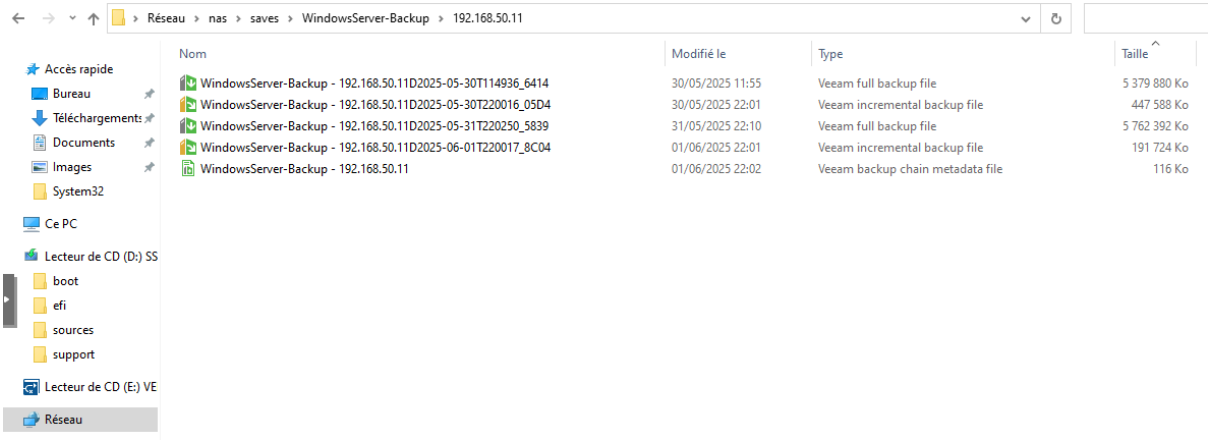
Cliquez sur les 3 petits points du disque défectueux puis replace :



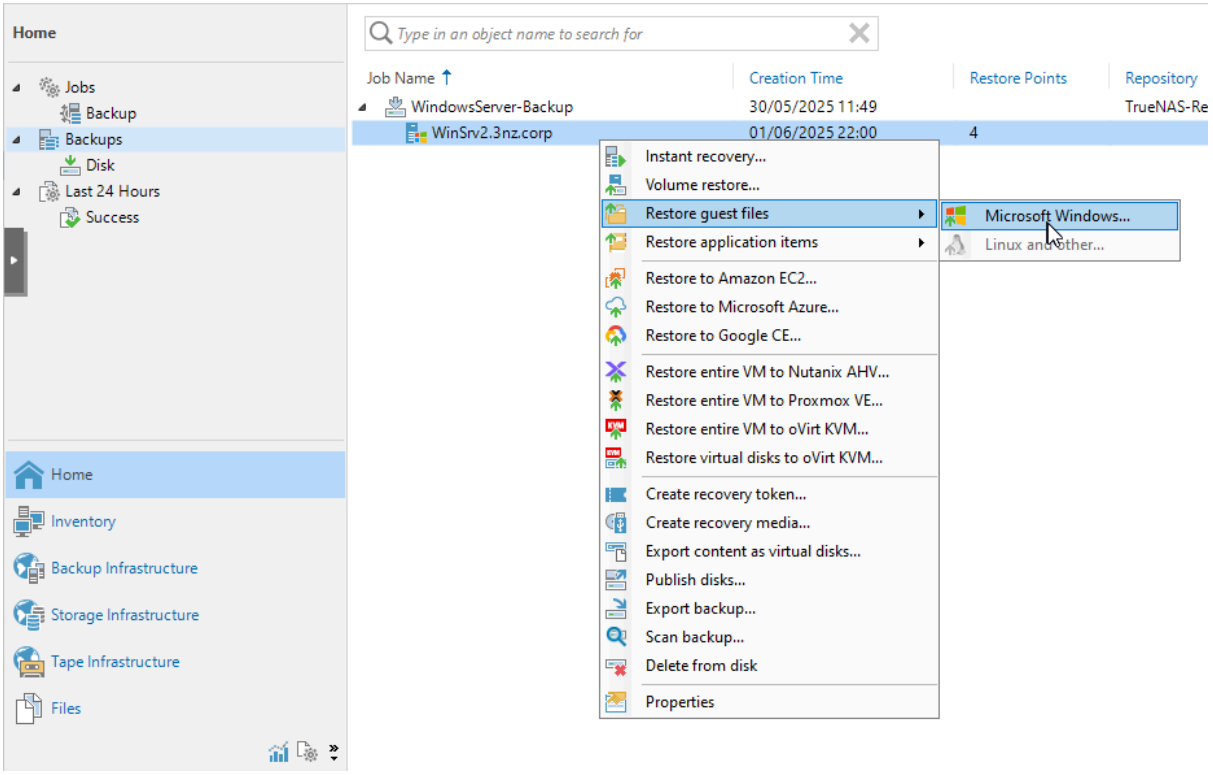


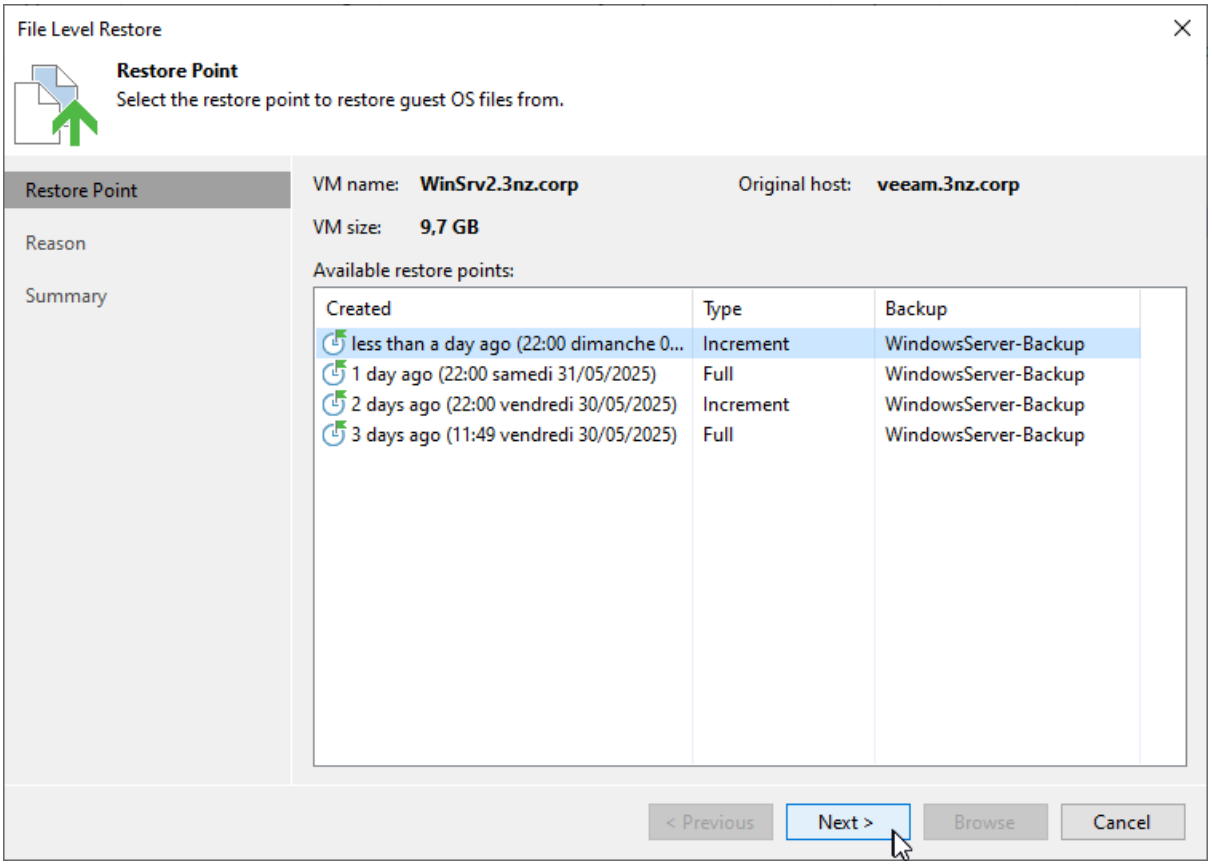


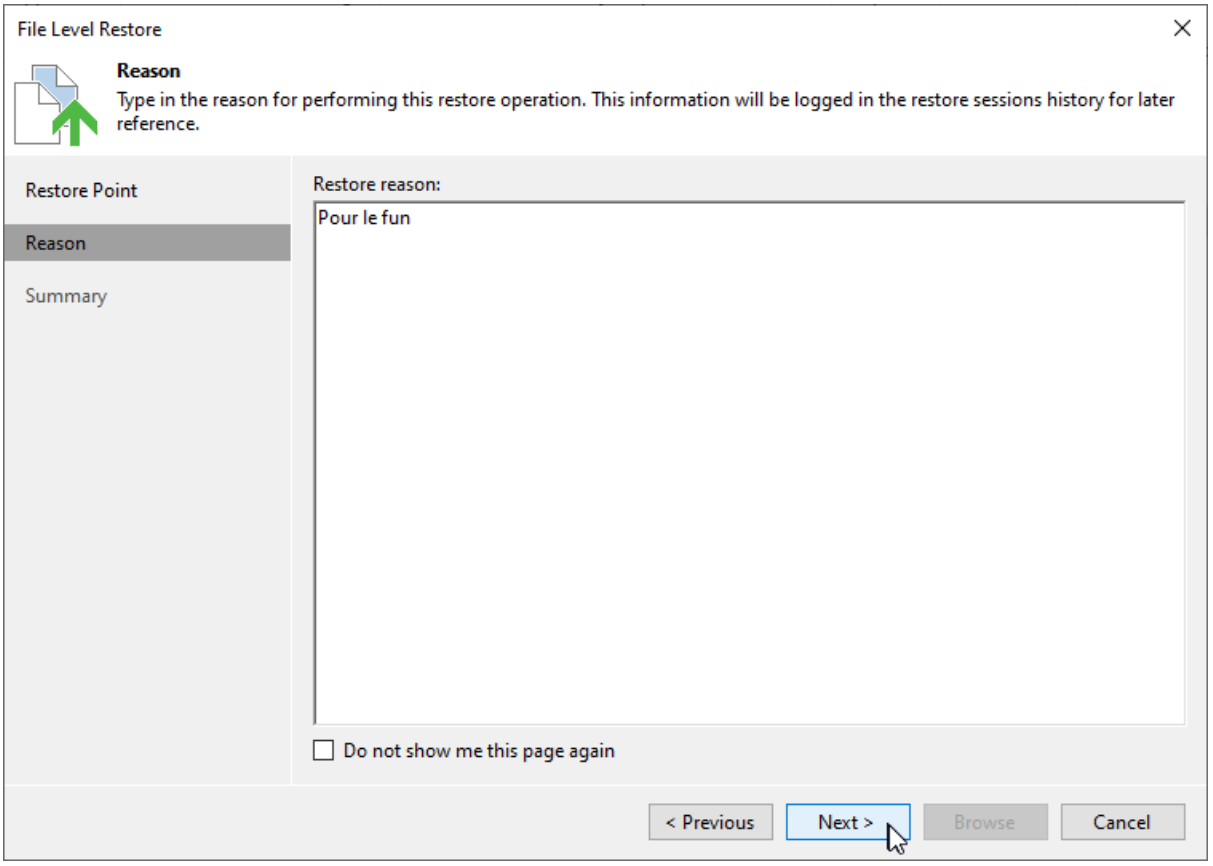
Vérifications et restauration pour Veeam Backup :
On peut déjà voir que les backup on été réalisé avec succès :

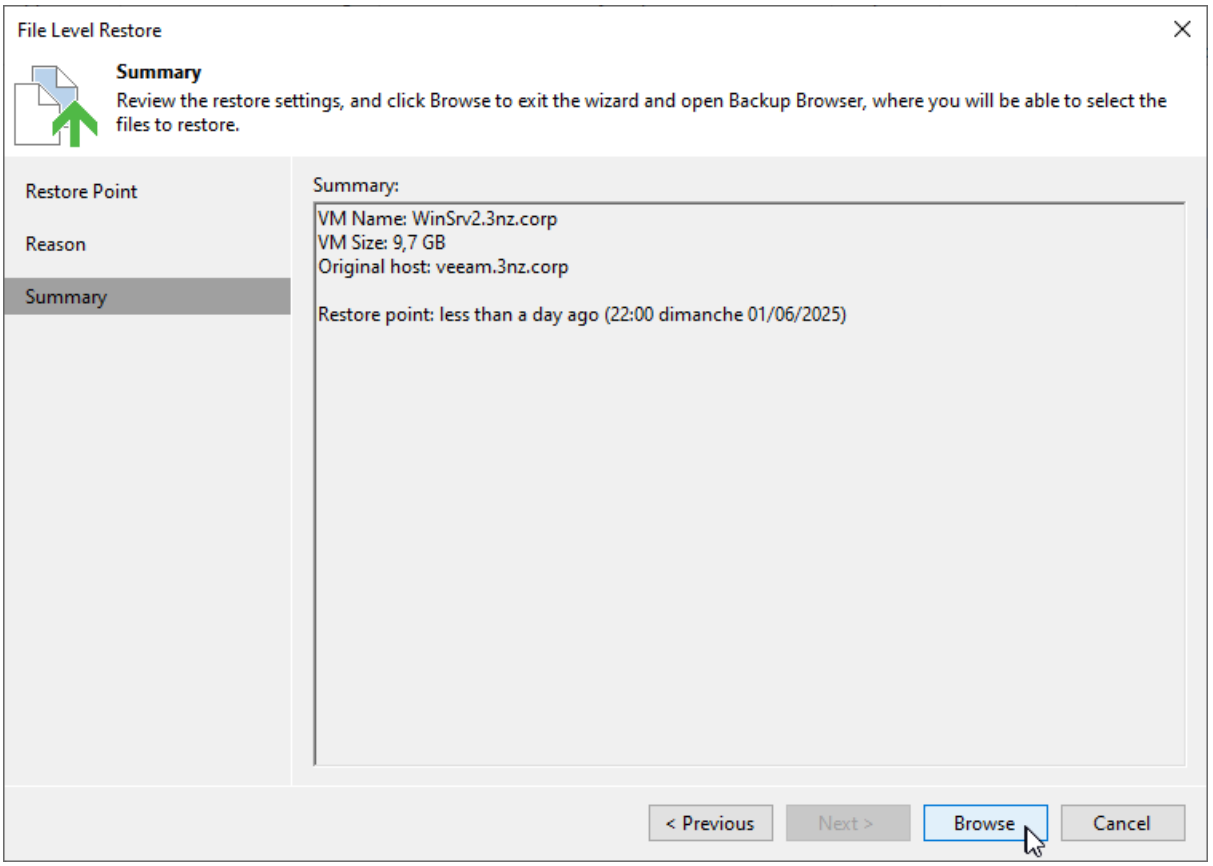


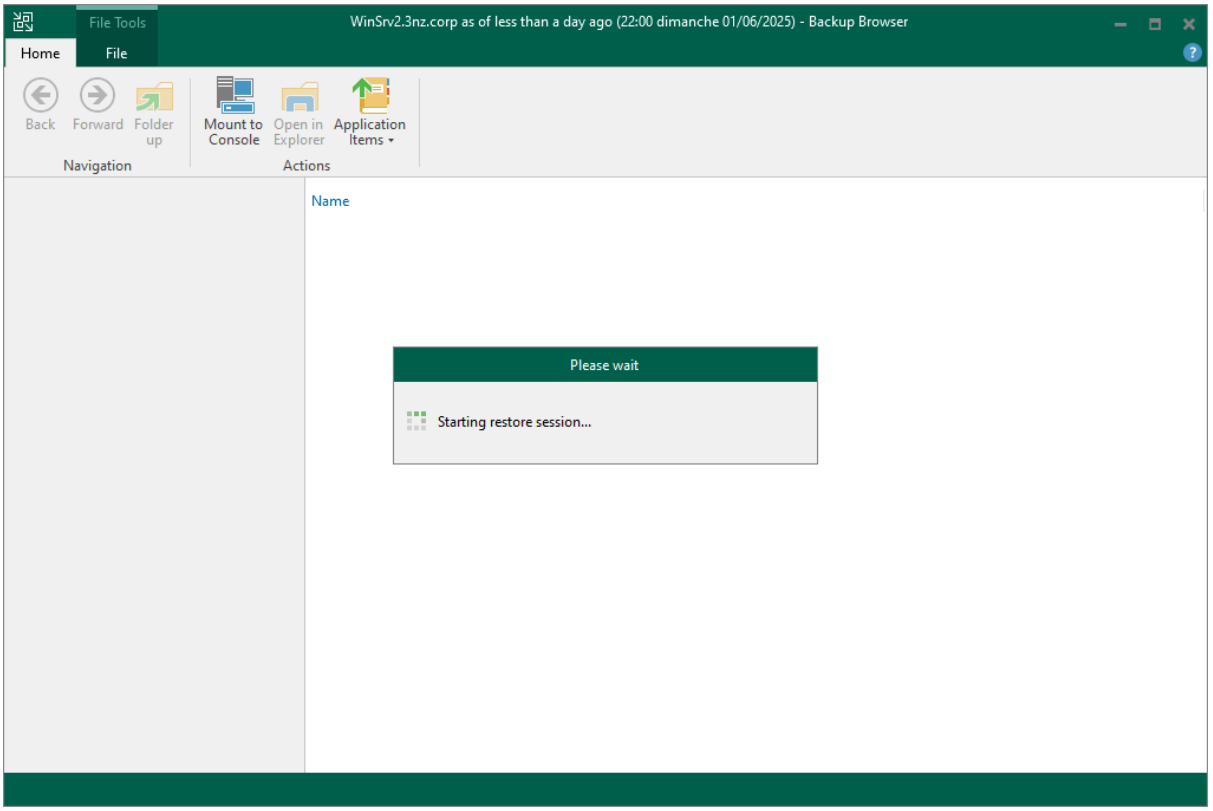
Allez dans la console Veeam, Backups, clic droit sur votre serveur

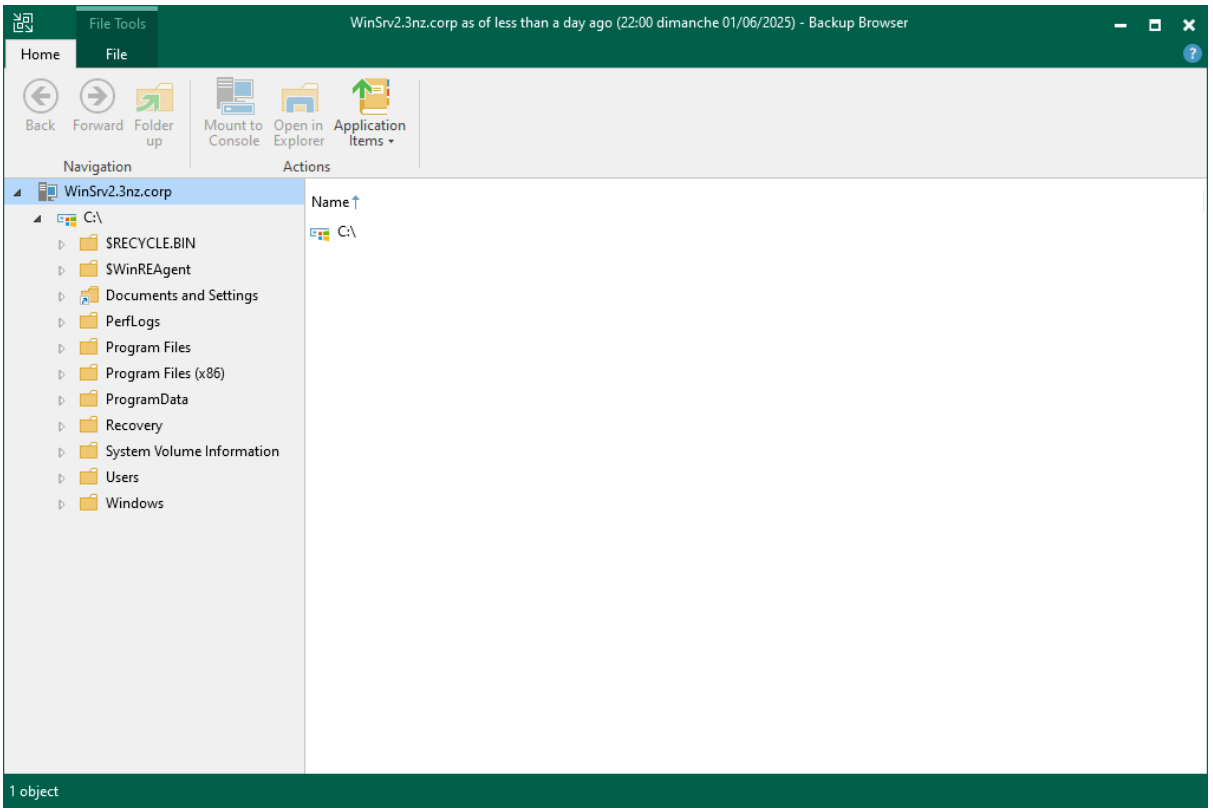





File Level Restore
Reason
Type in the reason for performing this restore operation. This information will be logged in the restore sessions history for later reference.
Restore Point
Reason
Summary
Restore reason:
Pour le fun
Do not show me this page again
< Previous
Next >
Browse
Cancel


File Level Restore
Summary
Review the restore settings, and click Browse to exit the wizard and open Backup Browser, where you will be able to select the files to restore.
Restore Point
Reason
Summary
Summary:
VM Name: WinSrv2.3nz.corp
VM Size: 9,7 GB
Original host: veeam.3nz.corp
Restore point: less than a day ago (22:00 dimanche 01/06/2025)
< Previous
Next >
Browse
Cancel


File Tools
WinSrv2.3nz.corp as of less than a day ago (22:00 dimanche 01/06/2025) - Backup Browser
Home
File
Back
Forward
Folder up
Navigation
Mount to Console
Open in Explorer
Application Items
Actions
Name
Please wait
Starting restore session...


File Tools
WinSrv2.3nz.corp as of less than a day ago (22:00 dimanche 01/06/2025) - Backup Browser
Home
File
Back
Forward
Folder up
Navigation
Mount to Console
Open in Explorer
Application Items
Actions
WinSrv2.3nz.corp
C:\
$RECYCLE.BIN
$WinREAgent
Documents and Settings
PerfLogs
Program Files
Program Files (x86)
ProgramData
Recovery
System Volume Information
Users
Windows
Name
C:\
1 object

COMPLETE !

Test du Fail2Ban & Intrusion

Pour ce test, je vais avec un réseau différent du mien faire des requêtes douteuses, je me rends sur l'url https://corp.3nz.fr/wp-admin et j'actualise pleins de fois.

On ouvre le terminal pour voir le ban en direct

```
tail -f /var/log/fail2ban.log
```

Avec cette commande on peut voir l'attaque en direct :

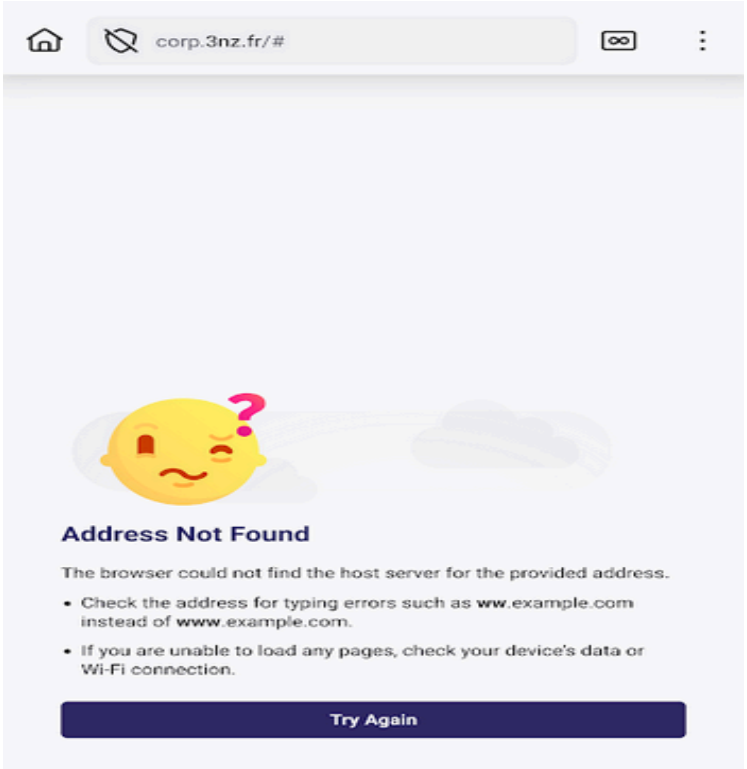
```
tail -f /var/log/nginx/access.log
```

```
37.170.247.176 - - [29/Nov/2025:22:25:03 +0000] "GET /wp-admin HTTP/1.1" 404 125 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:145.0) Gecko/20100101 Firefox/145.0"
```

L'ip a bien été banni :

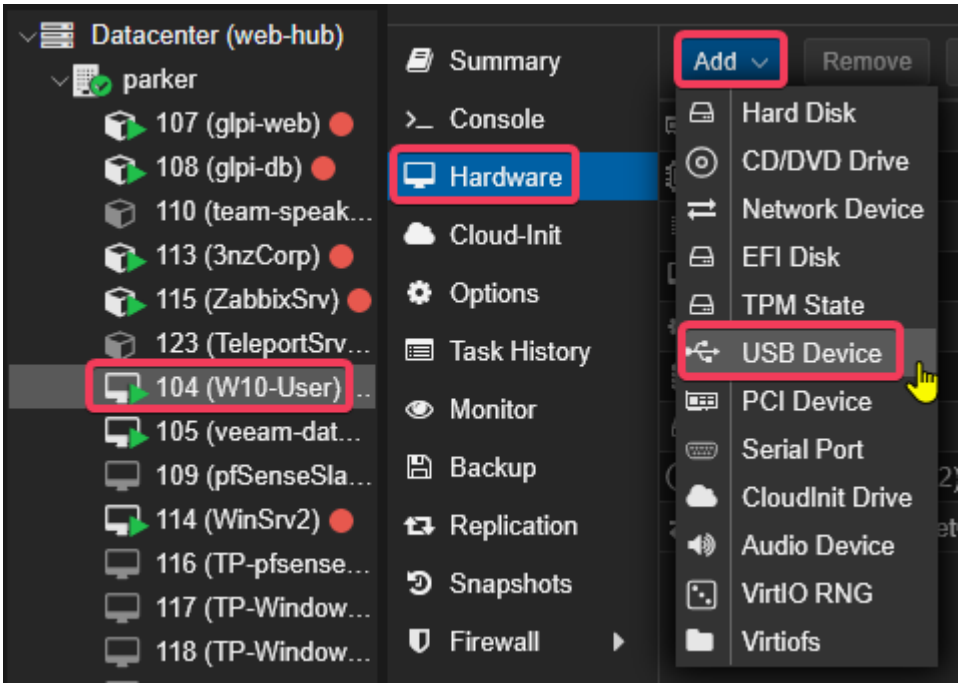
```
root@ReverseProxy:~# fail2ban-client status nginx-botsearch
Status for the jail: nginx-botsearch
|- Filter
|  |- Currently failed: 0
|  |- Total failed:     0
|  `- File list:        /var/log/nginx/access.log
`- Actions
   |- Currently banned: 1
   |- Total banned:     1
   `- Banned IP list:   37.170.247.176
```

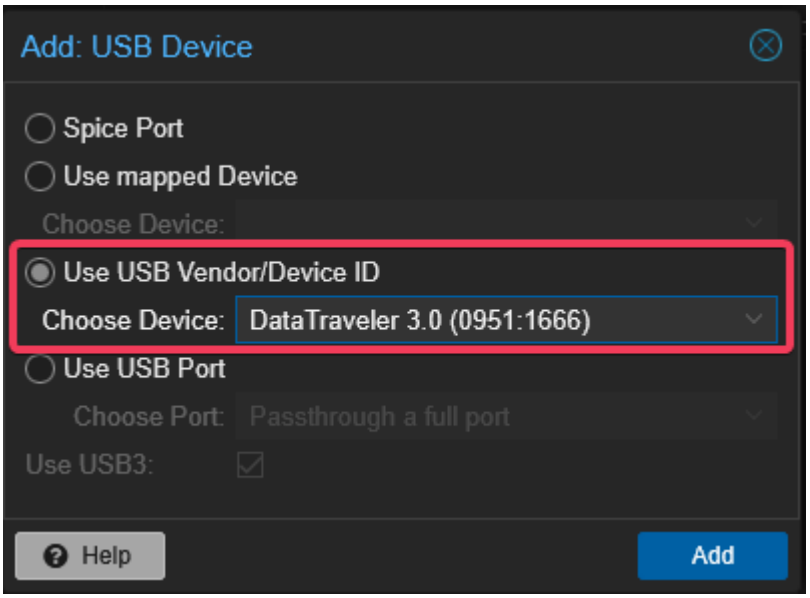
Et je n'ai plus accès au site sur mon smartphone :



Test de la GPO de sécurité des disques amovibles sur les postes utilisateurs :

Je branche une clé usb physique sur mon serveur, puis j'ajoute depuis l'interface Proxmox un USB Device :





L'accès est refusé à l'utilisateur en l'occurrence Luc Durand :