

# 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

The screenshot shows the Proxmox VM configuration for 'Virtual Machine 104 (WinUse2) on node 'parker''. The 'Network Device (net0)' is configured with 'tag=50'. To the right, the Windows network configuration window shows the IP address '192.168.50.4' and the gateway '192.168.50.1', both highlighted in red, indicating successful assignment to the VLAN 50.

The screenshot shows the Proxmox VM configuration for 'Virtual Machine 104 (WinUse2) on node 'parker''. The 'Network Device (net0)' is configured with 'tag=10'. To the right, the Windows network configuration window shows the IP address '192.168.10.3' and the gateway '192.168.10.1', both highlighted in red, indicating successful assignment to the VLAN 10.

Tunnel VPN fonctionnel depuis un autre réseau :

L'accès à l'infra fonctionne aussi :

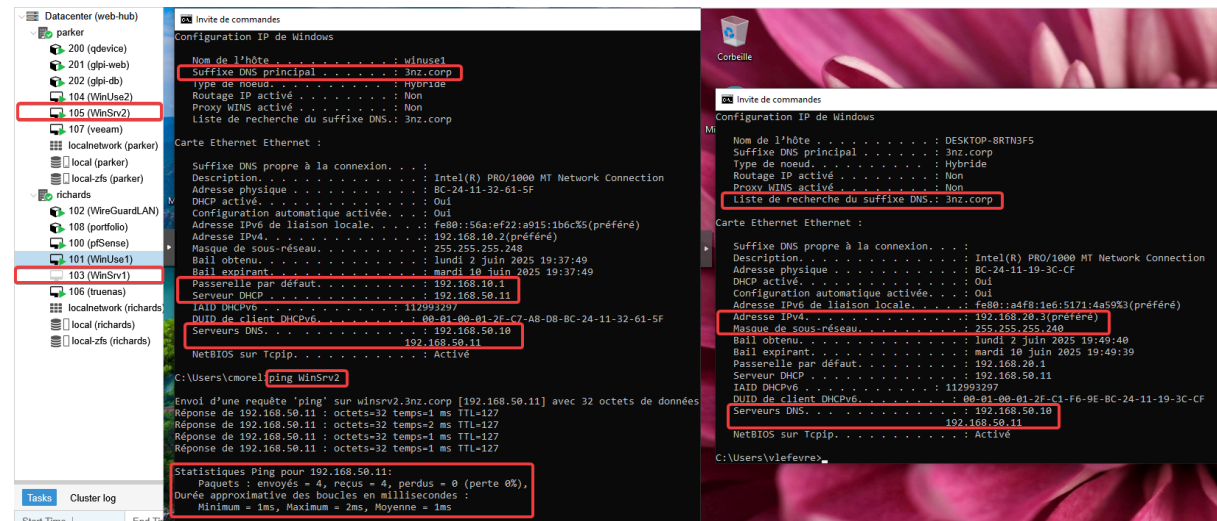
The screenshot shows the Proxmox network configuration table and a terminal window. The table lists network devices and their configurations. The terminal window shows the output of the 'ifconfig' command for the 'lo' interface, displaying the IP address '10.0.0.2/24' and the gateway '10.0.0.1', indicating successful access to the infrastructure.

Type	Description	Disk usage...	Memory us...
lxc	200 (qdevice)	18.1 %	8.6 %
lxc	201 (gpi-web)	17.4 %	14.2 %
lxc	202 (gpi-db)	15.7 %	42.1 %
lxc	102 (WireGuard_LAN)	7.5 %	3.5 %
lxc	108 (portfolio)	5.0 %	2.2 %
node	parker	0.4 %	95.3 %
node	richards	0.1 %	81.1 %
qemu	104 (WinUse2)	0.0 %	70.8 %
qemu	105 (WinSrv2)	0.0 %	72.9 %
qemu	107 (veeam)	0.0 %	67.3 %
qemu	100 (pfSense)	0.0 %	70.9 %
qemu	101 (WinUse1)	0.0 %	70.8 %
qemu	103 (WinSrv1)	0.0 %	76.4 %
qemu	106 (Truenas)	0.0 %	94.3 %
sdn	localnetwork (parker)		

```
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
inet 127.0.0.1/8 scope host lo
    valid_lft forever preferred_lft forever
inet6 ::1/128 scope host noprefixroute
    valid_lft forever preferred_lft forever
2: enp3s0f0: <NO-CARRIER,BROADCAST,MULTICAST,UP> mtu 1500 qdisc fq_codel state DOWN group default qlen 1
000
link/ether f4:a8:0d:99:a0:65 brd ff:ff:ff:ff:ff:ff
inet 169.254.11.78/16 brd 169.254.255.255 scope link enp3s0f0:avahi
    valid_lft forever preferred_lft forever
3: wlp6s0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
link/ether cc:5e:f8:4b:1e:c8 brd ff:ff:ff:ff:ff:ff
inet 172.30.71.86/24 brd 172.30.71.255 scope global dynamic noprefixroute wlp6s0
    valid_lft 3554sec preferred_lft 3554sec
inet6 fe80::519b:94d3:882a:18a4/64 scope link noprefixroute
    valid_lft forever preferred_lft forever
5: wq0: <POINTOPOINT,NOARP,UP,LOWER_UP> mtu 1380 qdisc noqueue state UNKNOWN group default qlen 1000
link/none
inet 10.0.0.2/24 scope global wq0
    valid_lft forever preferred_lft forever
en2TPGOAT:~$
```

## 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 :

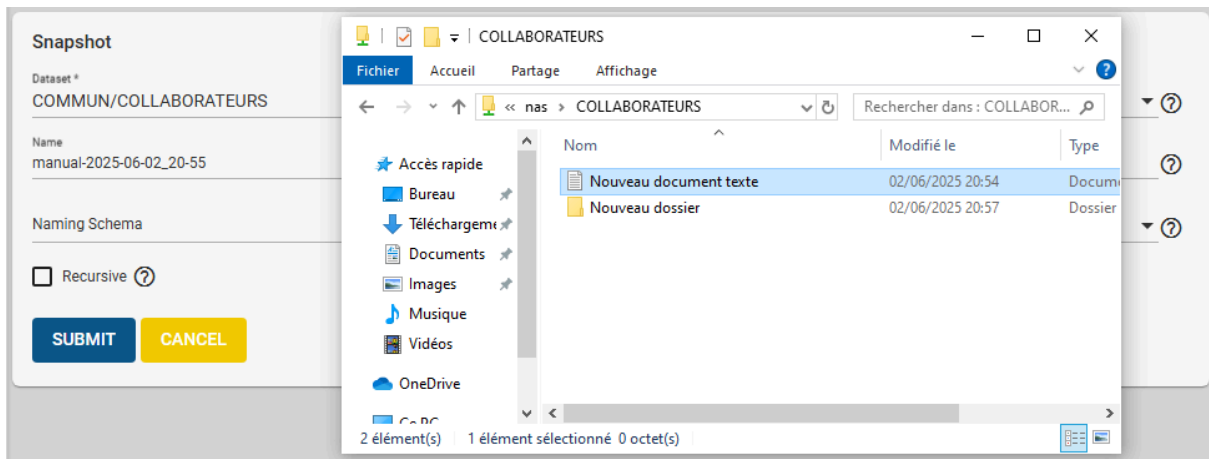


## Test et restauration des snapshots sur TrueNAS :

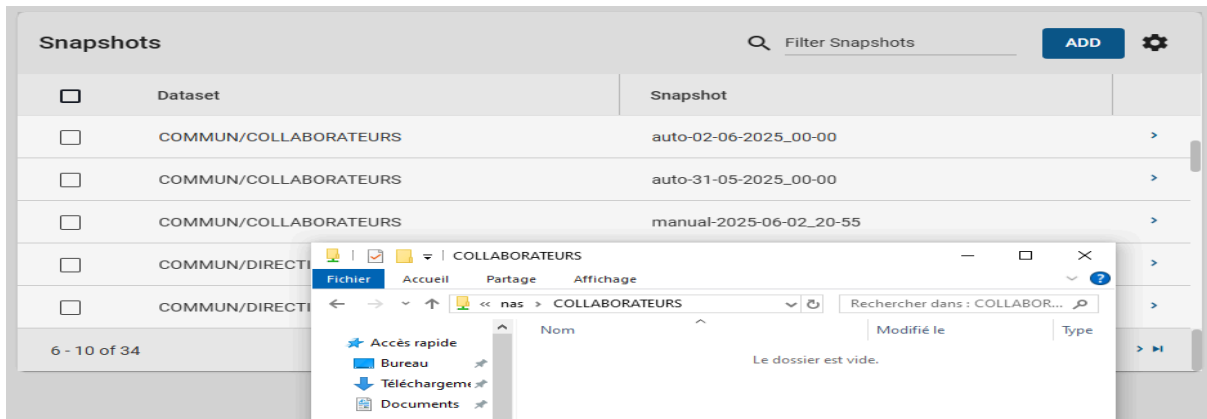
Les snapshots sont bien créés tous les jours :

<input type="checkbox"/>	COMMUN	auto-01-06-2025_0	>
<input type="checkbox"/>	COMMUN	auto-02-06-2025_0	>
<input type="checkbox"/>	COMMUN	auto-31-05-2025_0	>
<input type="checkbox"/>	COMMUN/COLLABORATEURS	auto-01-06-2025_0	>
<input type="checkbox"/>	COMMUN/COLLABORATEURS	auto-02-06-2025_0	>

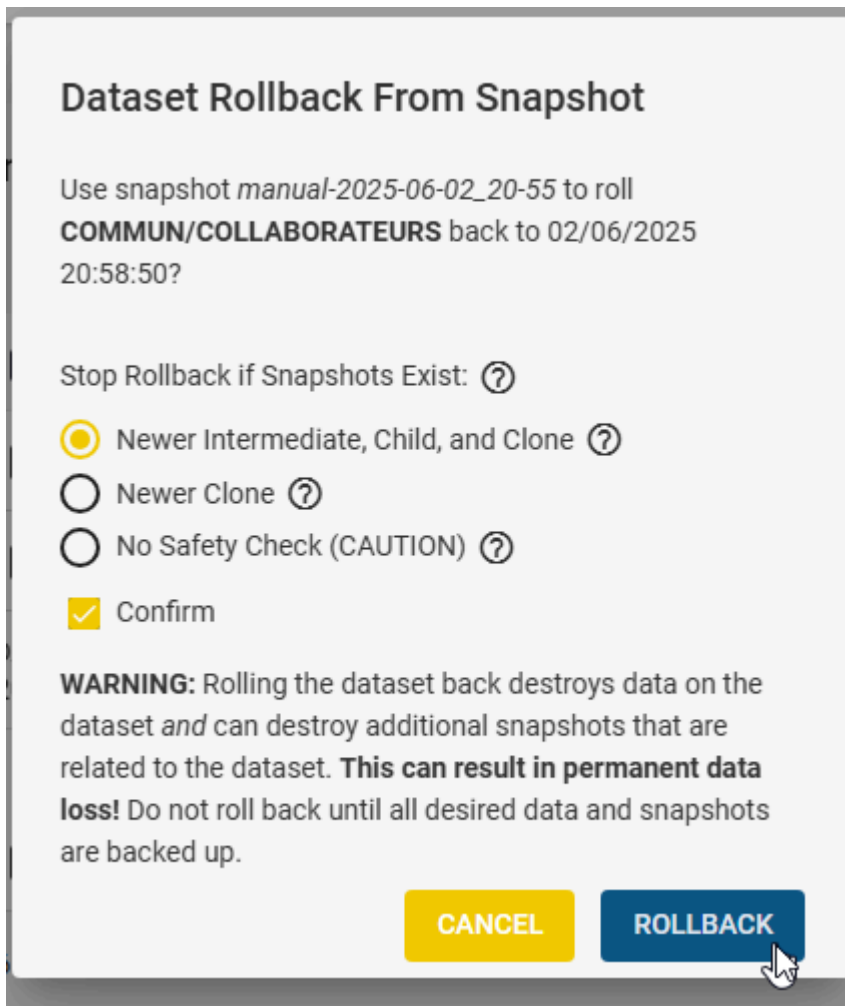
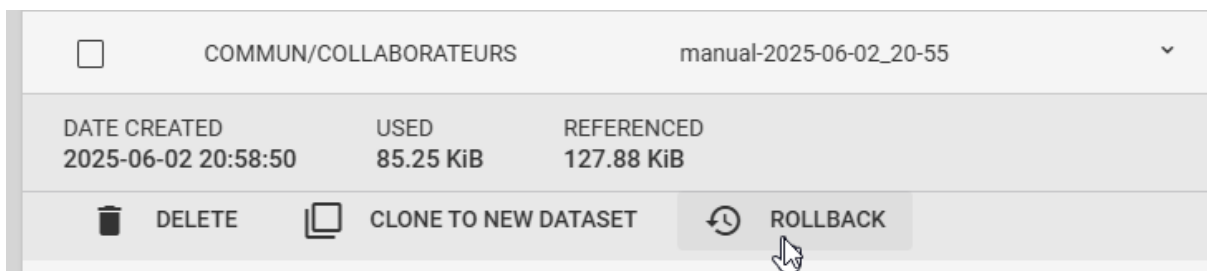
## Création d'une snapshot pour le test :



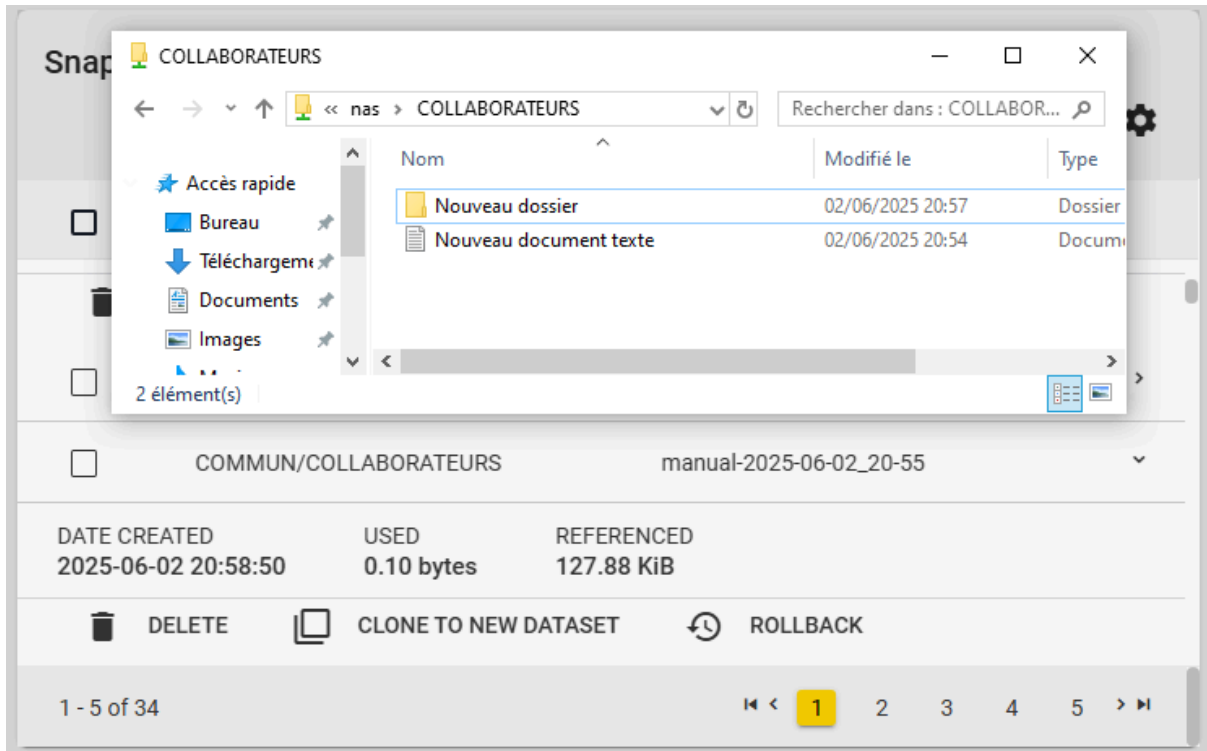
Suppression des dossiers/fichiers :



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

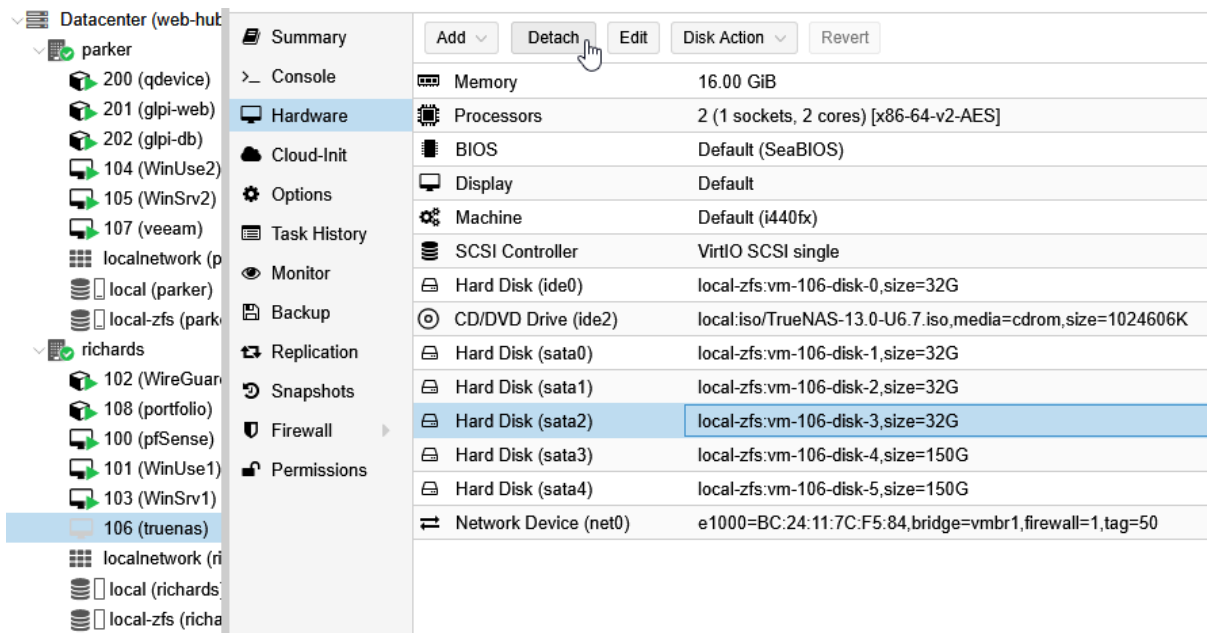


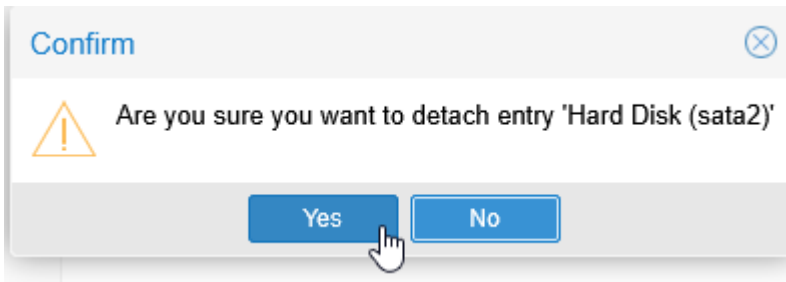
Les fichiers/dossiers sont récupérés :



Simulation d'une panne disque dur et remplacement du disque défectueux :

J'éteins la VM truenas et détache un disque :

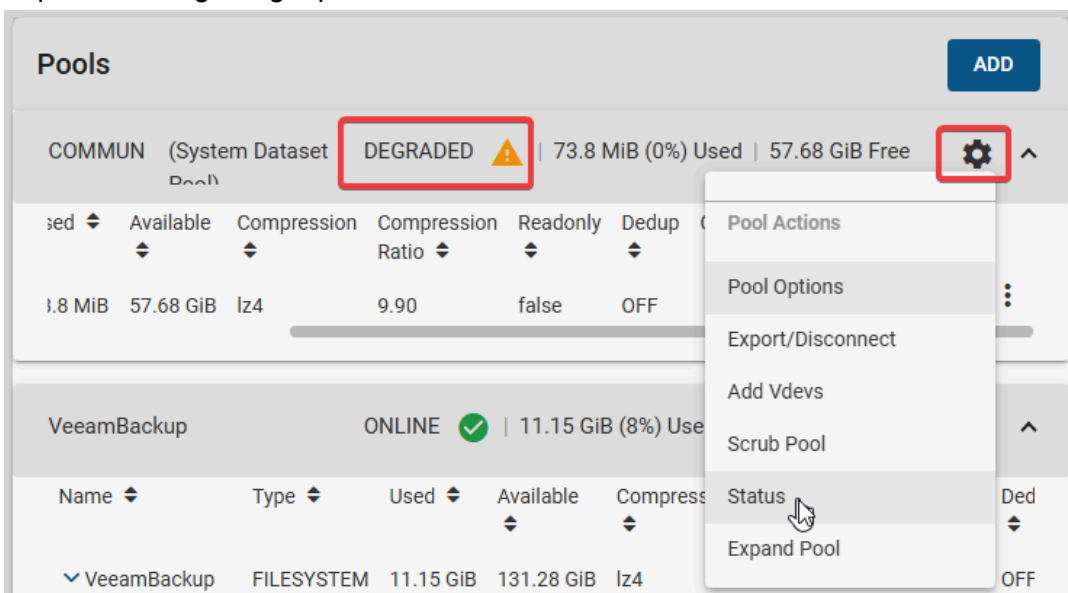




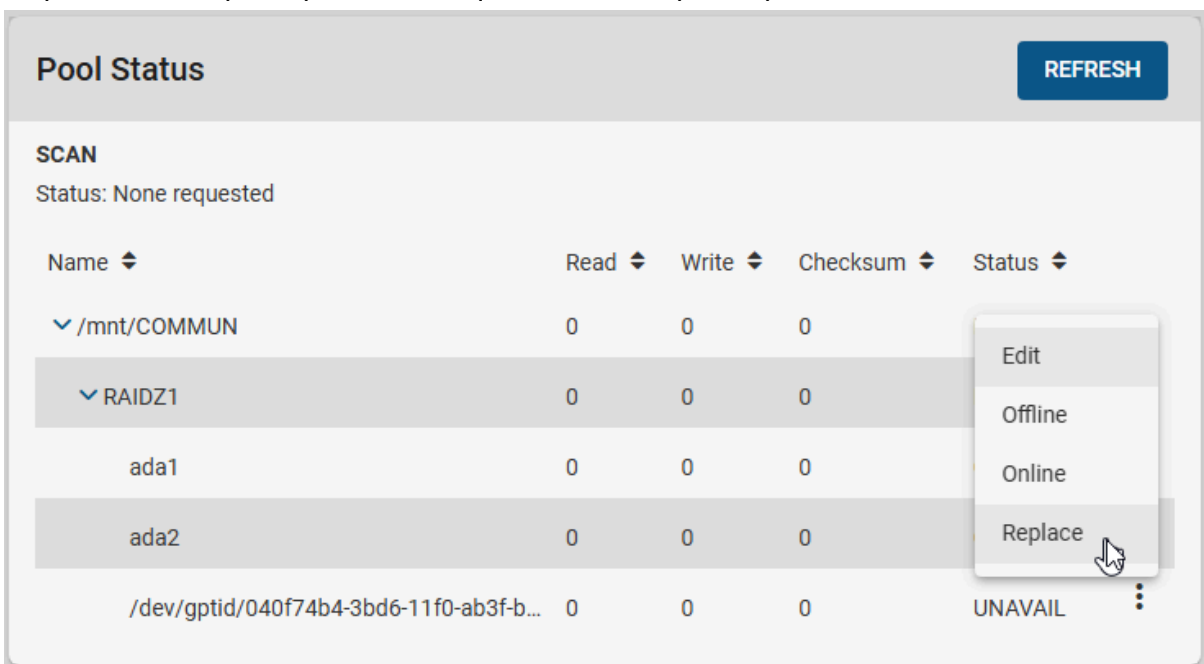
Ajouter un disque de même taille que ceux dans votre raid :

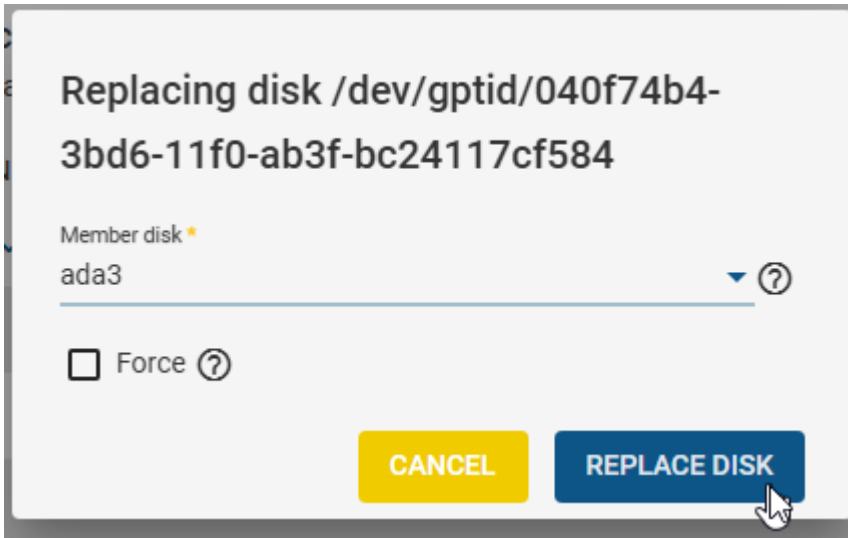
Hard Disk (sata2) local-zfs:vm-106-disk-6,size=32G

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 :





**Pool Status** REFRESH

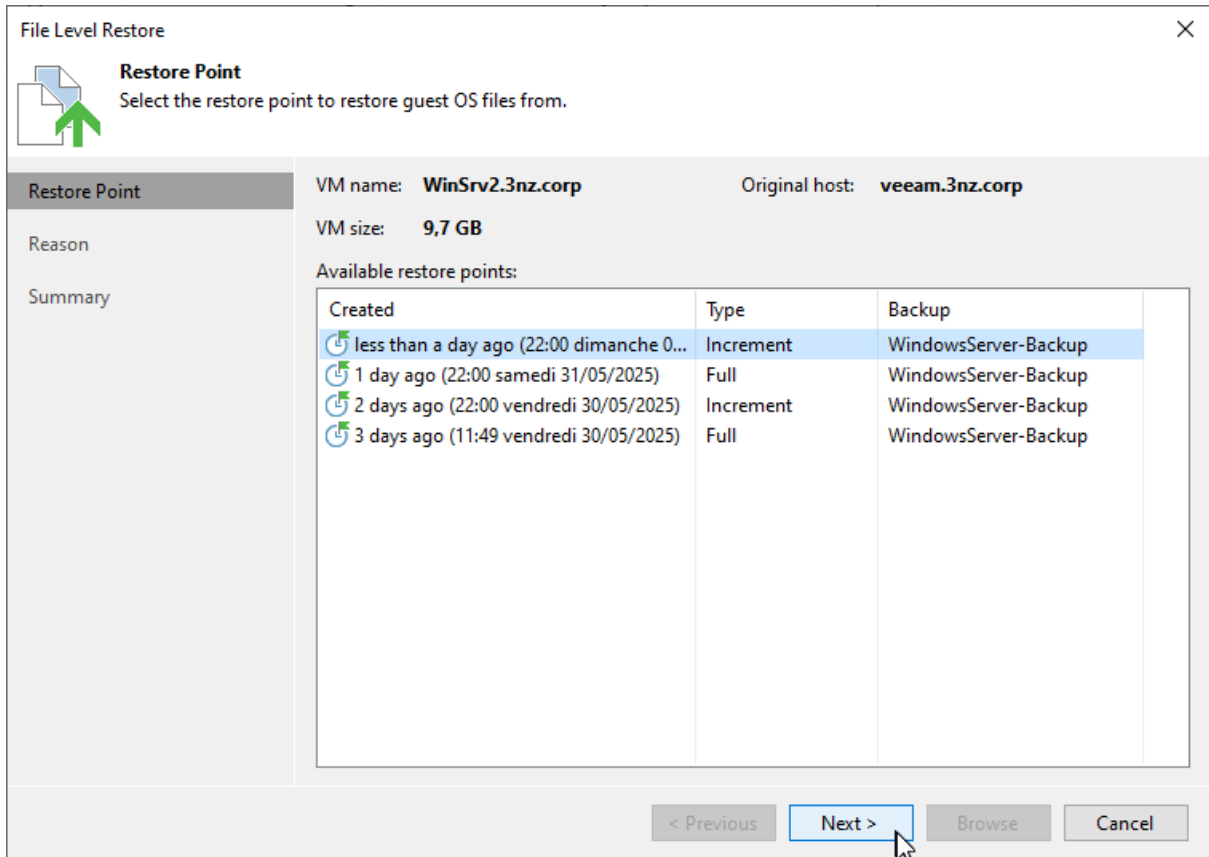
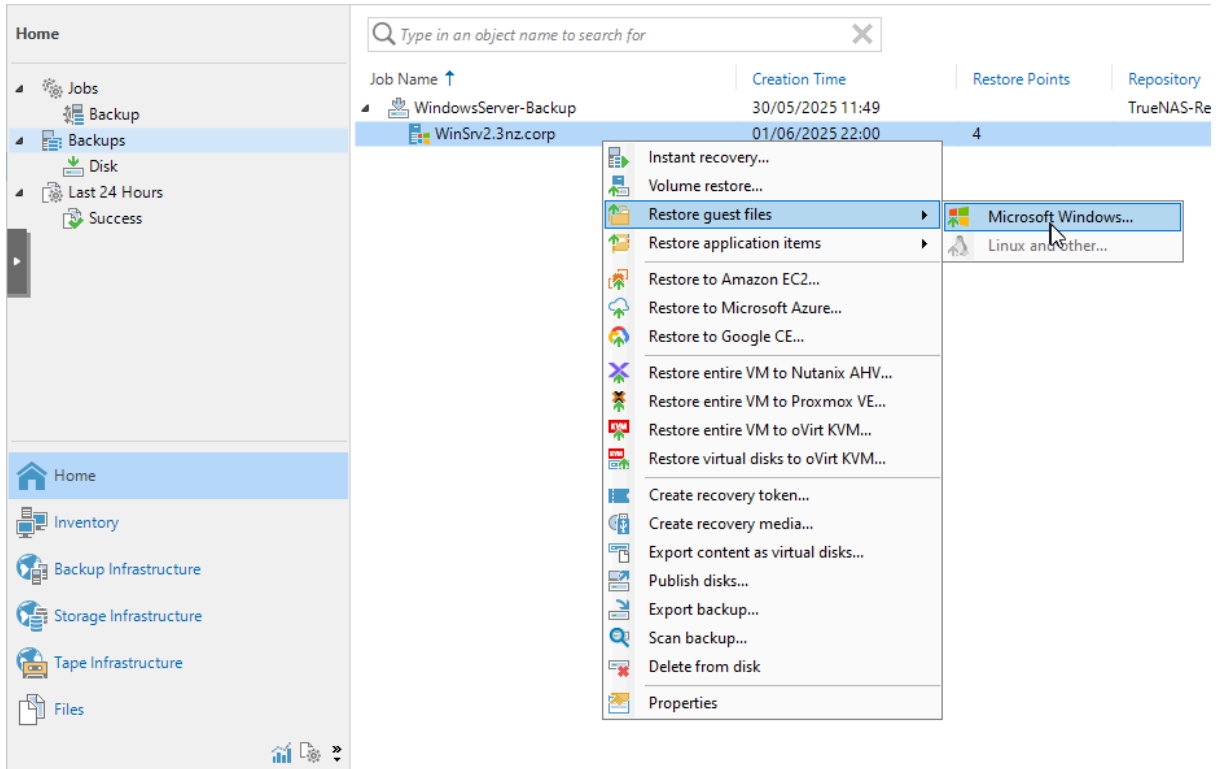
**RESILVER**  
Status: FINISHED  
Errors: 0  
Date: 2025-06-02 21:36:49

Name	Read	Write	Checksum	Status
▼ /mnt/COMMUN	0	0	0	ONLINE
▼ RAIDZ1	0	0	0	ONLINE
ada1	0	0	0	ONLINE
ada2	0	0	0	ONLINE
ada3	0	0	0	ONLINE


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

Nom	Modifié le	Type	Taille
WindowsServer-Backup - 192.168.50.11D2025-05-30T114936_6414	30/05/2025 11:55	Veeam full backup file	5 379 880 Ko
WindowsServer-Backup - 192.168.50.11D2025-05-30T220016_05D4	30/05/2025 22:01	Veeam incremental backup file	447 588 Ko
WindowsServer-Backup - 192.168.50.11D2025-05-31T220250_5839	31/05/2025 22:10	Veeam full backup file	5 762 392 Ko
WindowsServer-Backup - 192.168.50.11D2025-06-01T220017_8C04	01/06/2025 22:01	Veeam incremental backup file	191 724 Ko
WindowsServer-Backup - 192.168.50.11	01/06/2025 22:02	Veeam backup chain metadata file	116 Ko

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



**File Level Restore** [Close]


 **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	Restore reason: Pour le fun
<b>Reason</b>	
Summary	

Do not show me this page again

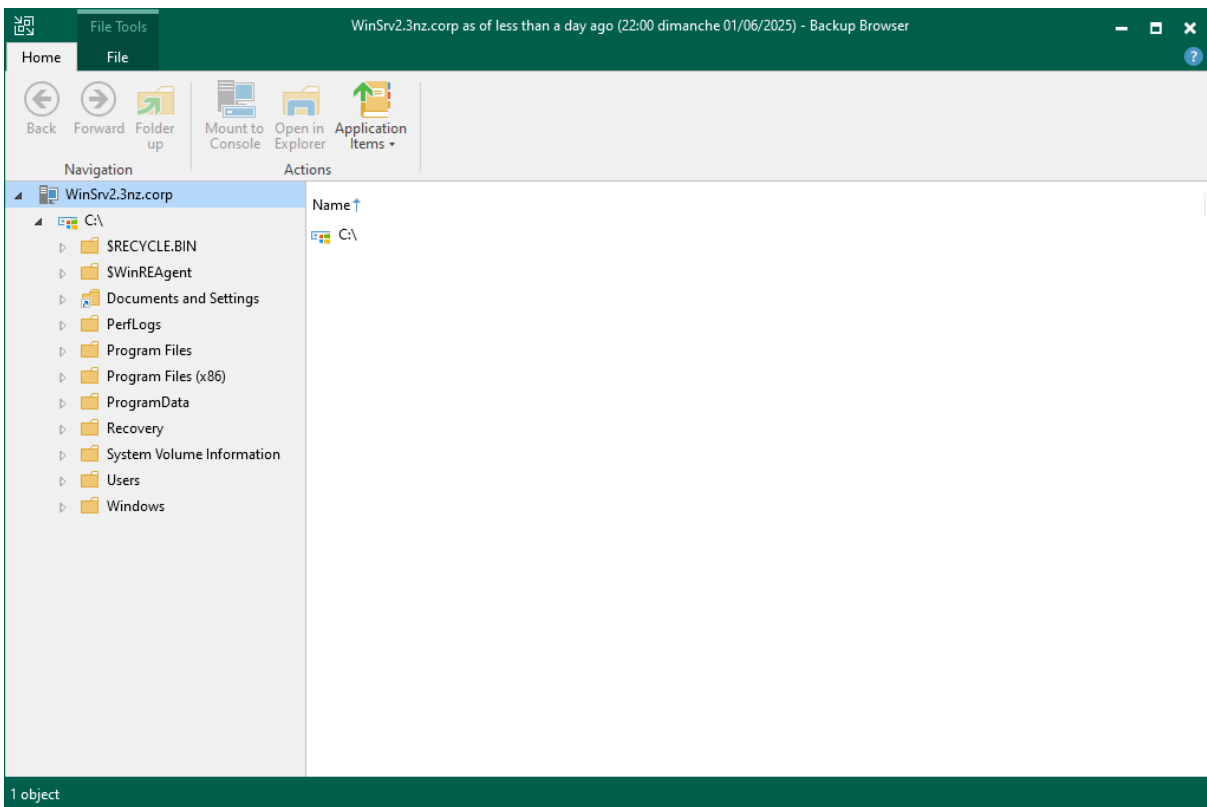
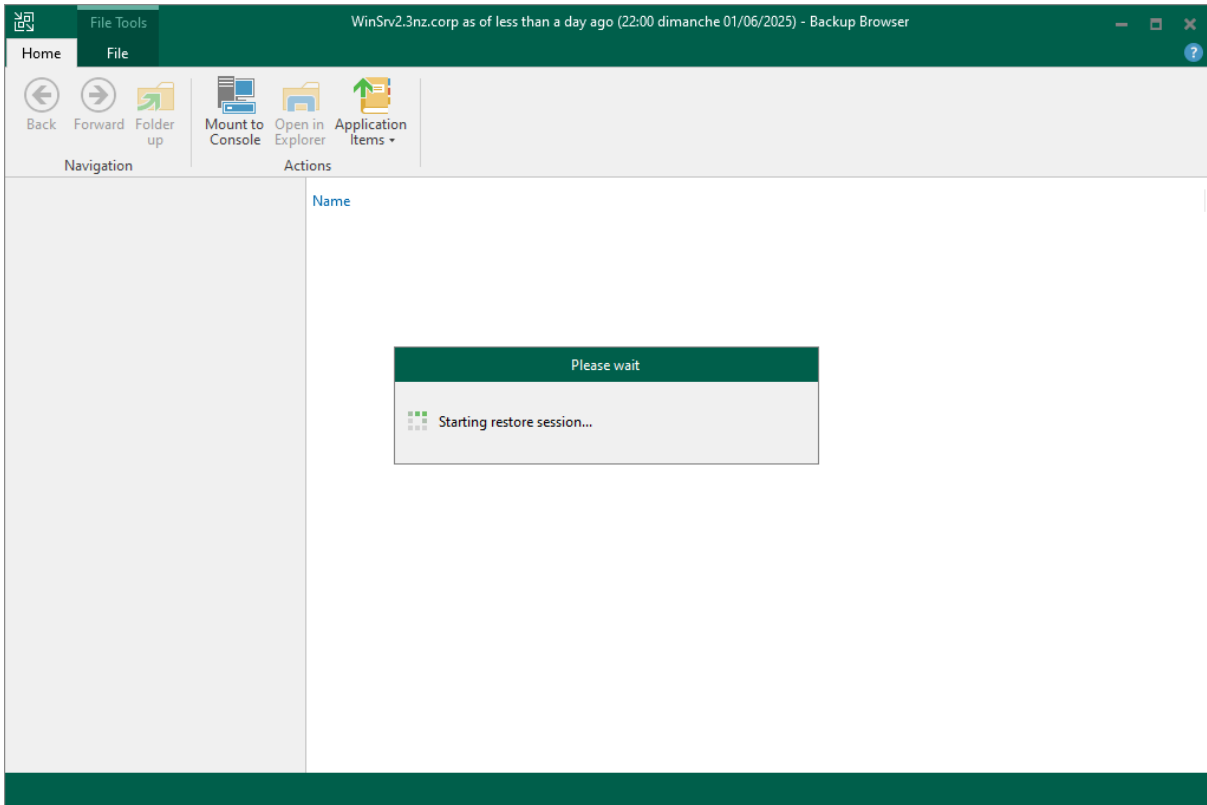
< Previous   **Next >**   Browse   Cancel

**File Level Restore** [Close]

 **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	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)
Reason	
<b>Summary</b>	

< Previous   Next >   **Browse**   Cancel



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 :

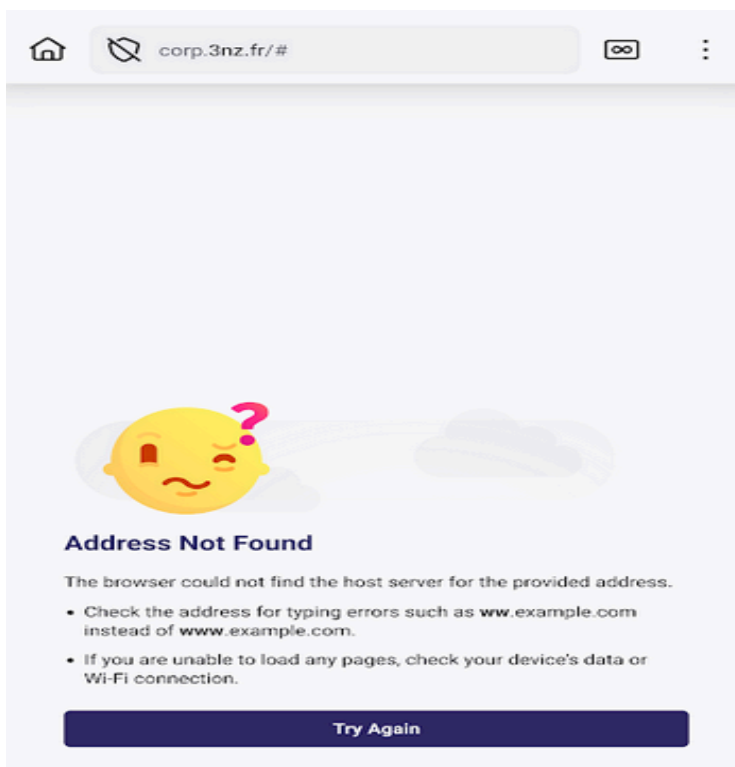
```
tail -f /var/log/nginx/access.log
```

```
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 :

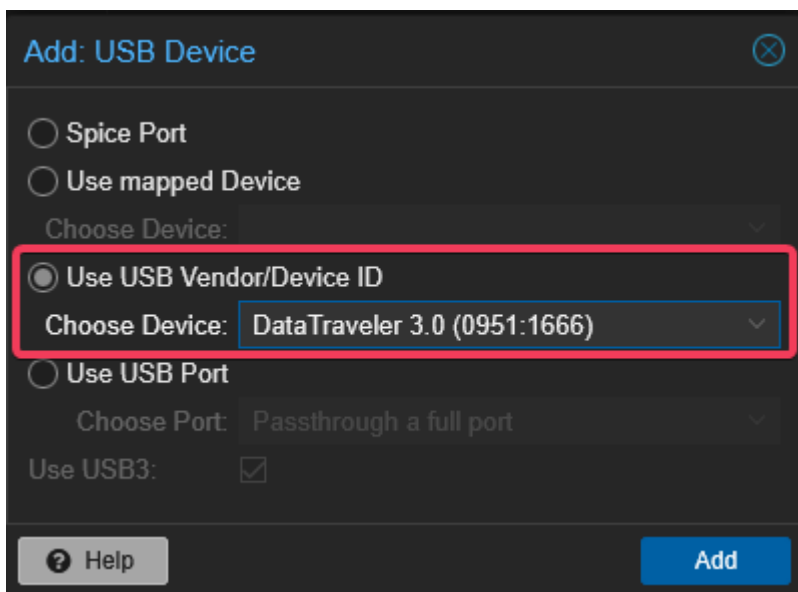
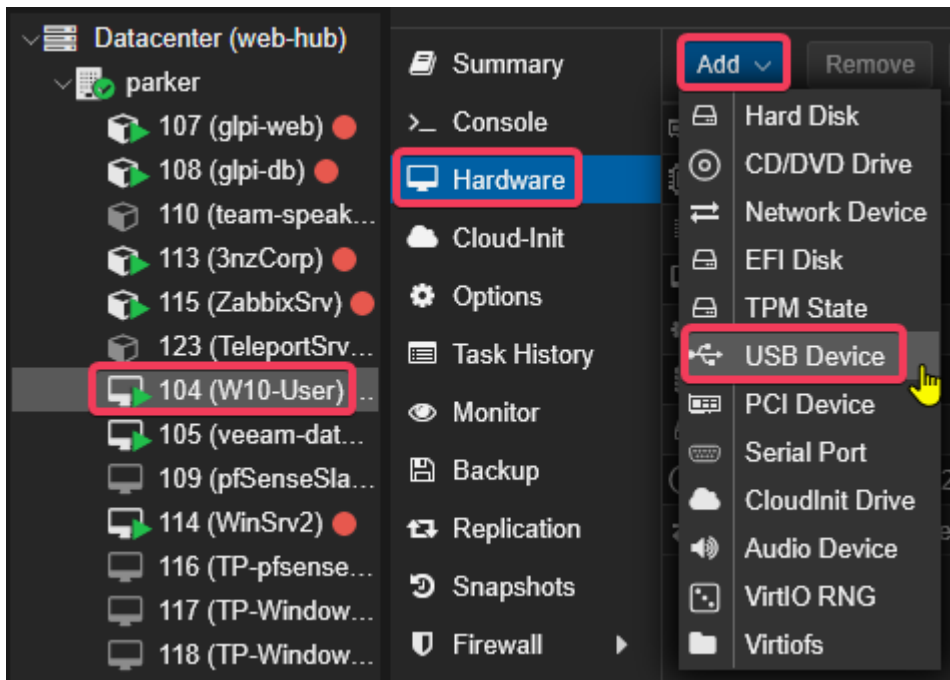
```
root@ReverseProxy:~# fail2ban-client status nginx-botsearch
Status for the jail: nginx-botsearch
|- Filter
| |- Currently failed: 0
| |- Total failed:    0
| `-- File list:      /var/log/nginx/access.log
`-- Actions
   |- Currently banned: 1
   |- Total banned:    1
   `-- Banned IP list: 37.170.247.176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

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 :

