Proxmox

Il s'agit d'une plateforme de virtualisation gratuite (sous licence AGPLv3) qui s'appuie sur l'hyperviseur Linux KVM. Elle offre également des conteneurs avec LXC. Cette plateforme propose également un service d'assistance payant.

- Sauvegarde Proxmox Virtual Environment
- Proxmox VE Helper-Scripts
- Applications
    - qBittorrent avec VPN dans un conteneur LXC
- Instructions d'installation des nouveaux drivers NVIDIA Tesla P4
- Optimiser les performances des machines virtuelles

Sauvegarde Proxmox Virtual Environment

Méthode de sauvegarde des configurations et données critiques Proxmox. Avoir des sauvegardes fiables et facilement restaurables est primordial, que ce soit pour se prémunir contre une panne matérielle, une erreur de manipulation ou une attaque.

Méthode de sauvegarde en local

Prérequis

- Un disque dur USB ou un stockage en réseau monté pour les sauvegardes s'il ne l'est pas déjà fait pour vos sauvegardes.
- Sauvegarder l'intégralité des machines virtuelles et des conteneurs dans un stockage externe (voir Backup and Restore).
- La sauvegarde : 3-2-1-1-0 et bonnes pratiques

Point de montage

Pour monter la clé USB qui est formatée en `ext4` automatiquement au démarrage, vous pouvez ajouter la ligne suivante dans le fichier `/etc/fstab` :

```
sudo -i
```

```
nano /etc/fstab
```

```
/dev/sdb1 /mnt/pve/backup-proxmox ext4 defaults,nofail 0 0
```

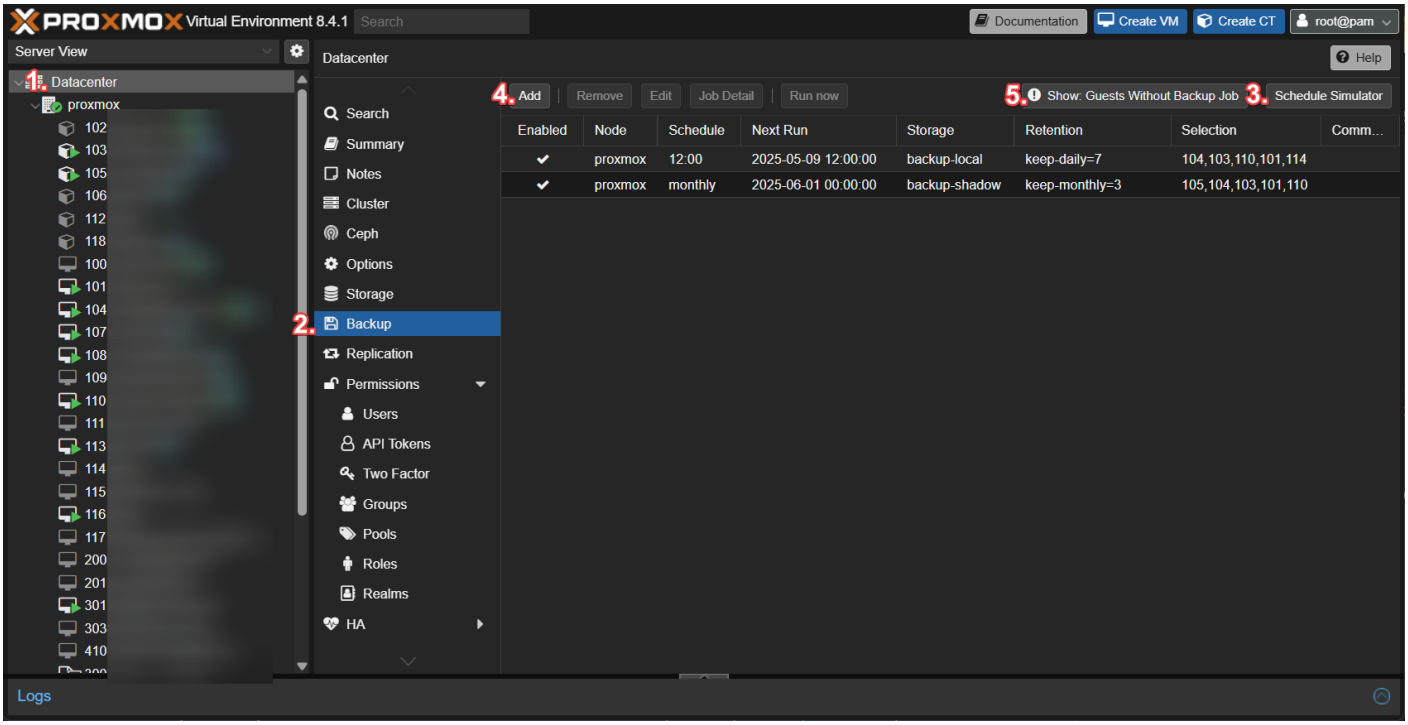
Si vous avez un partage de fichiers réseau NFS grâce à un NAS TrueNAS ou Synology, vous pouvez prendre l'exemple ci-dessous en installant au préalable le paquet `nfs-common` :

```
192.168.1.666:/mnt/stockage/backup-proxmox /mnt/pve/backup-proxmox nfs defaults,nofail 0 0
```

```
systemctl daemon-reload && mount -a
```

L'option `nofail` permet de ne pas bloquer le démarrage si la clé USB ou le partage NFS n'est pas connectée. Assurez-vous de remplacer `/dev/sdb1` par le bon nom de périphérique de votre clé USB en effectuant la commande `lsblk` et `/mnt/pve/backup-proxmox` par le point de montage de votre choix.

Sauvegarde LXC, machine virtuelle



Sauvegarde configuration

```
sudo -i
```

```
nano ~/proxmox_configuration_backup.sh
```

Il vous suffit de changer la destination pour les sauvegardes par la vôtre :

```
#!/bin/bash

# Description
# Ce script effectue une sauvegarde des dossiers spécifiés.
# Les sauvegardes sont conservées pendant 7 jours
# Le script est exécuté via une tâche cron tous les jours à 2h du matin.

# Dossiers à sauvegarder
BACKUP_DIRS=("/etc/pve" "/etc/passwd" "/etc/network/interfaces" "/var/log")

# Destination des sauvegardes
```

```
BACKUP_DEST="/mnt/pve/backup-proxmox/proxmox_configuration_backup"

# Nombre de jours de conservation
RETENTION_DAYS=7

# Exécution de la sauvegarde
for dir in "${BACKUP_DIRS[@]}"; do
    filename="$(basename "$dir")_$(date +%Y-%m-%d).tar.gz"
    tar -czf "$BACKUP_DEST/$filename" "$dir"

    # Création du fichier de checksum SHA-256
    sha256sum "$BACKUP_DEST/$filename" > "$BACKUP_DEST/$filename.sha256"
done

# Suppression des sauvegardes obsolètes
find "$BACKUP_DEST" -type f -mtime +$RETENTION_DAYS -delete

# Fin du script
echo "Sauvegarde terminée."

# Pour vérifier le checksum d'un fichier de sauvegarde, utilisez la commande suivante :
# sha256sum -c nom_du_fichier.tar.sha256"
# Remplacez "nom_du_fichier" par le nom de votre fichier de sauvegarde.
```

Rendre exécutable le script :

```
chmod +x ~/proxmox_configuration_backup.sh
```

La tâche cron pour effectuer la sauvegarde chaque matin à 2h :

```
crontab -e
```

```
0 2 * * * ./proxmox_configuration_backup.sh
```

Testez les archives pour vérifier qu'elles ont bien été archivées :

```
root@proxmox:/mnt/pve/backup-shadow/proxmox_configuration_backup# ls
interfaces_2025-05-05.tar.gz         passwd_2025-05-05.tar.gz         pve_2025-05-05.tar.gz
interfaces_2025-05-05.tar.gz.sha256  passwd_2025-05-05.tar.gz.sha256  pve_2025-05-05.tar.gz.sha256
root@proxmox:/mnt/pve/backup-shadow/proxmox_configuration_backup# tar -tzf interfaces_2025-05-05.tar.gz
etc/network/interfaces
root@proxmox:/mnt/pve/backup-shadow/proxmox_configuration_backup# tar -tzf passwd_2025-05-05.tar.gz
etc/passwd
root@proxmox:/mnt/pve/backup-shadow/proxmox_configuration_backup# tar -tzf pve_2025-05-05.tar.gz
etc/pve/
etc/pve/.debug
etc/pve/.vmlist
etc/pve/.members
etc/pve/lxc
etc/pve/local
etc/pve/.rrd
etc/pve/.version
etc/pve/.clusterlog
etc/pve/openvz
etc/pve/qemu-server
etc/pve/storage.cfg
```

Sauvegarde hebdomadaire vers site distant

Sauvegarder de manière hebdomadaire et incrémentielle les données Proxmox sur un stockage chiffré chez SwissBackup.

Prérequis

- Rclone d'installé
- Configurer Rclone avec un service de stockage comme SwissBackup ou autres

La tâche cron :

```
crontab -e
```

```
0 2 * * * rclone sync /mnt/pve/backup-proxmox crypt_SwissBackup_backup-proxmox:/backup-proxmox
--verbose --log-file=/mnt/backupHDD/rclone_SwissBackup_backup-proxmox.txt
```

Fonctionnement :

- Exécution tous les jours à 2h du matin
- Synchronisation du répertoire local `/mnt/pve/backup-proxmox` vers le répertoire distant `crypt_SwissBackup_backup-proxmox:/backup-proxmox`
- Utilisation du chiffrement pour le stockage distant sur SwissBackup
- Mode verbeux activé pour plus de détails

- Journalisation des opérations dans le fichier `/mnt/pve/backup-proxmox/rclone_SwissBackup_backup-proxmox.txt`

Restaurer Proxmox Virtual Environment

Voici les étapes à suivre pour restaurer Proxmox :

1. Installez la dernière version de Proxmox VE 8.x à partir de l'ISO (cela supprimera toutes les données sur l'hôte existant) si nécessaire.
2. Videz le cache de votre navigateur et/ou forcez le rechargement de l'interface Web (CTRL + SHIFT + R, ou pour macOS ⌘ + Alt + R).
3. Reconstruisez votre cluster si nécessaire.
4. Restaurez le fichier `/etc/pve/storage.cfg` pour rendre le stockage externe utilisé pour la sauvegarde disponible.
5. Restaurez les configurations du pare-feu dans `/etc/pve/firewall/` et `/etc/pve/nodes/<node>/host.fw` si nécessaire.
6. Restaurez toutes vos machines virtuelles à partir des sauvegardes (voir la documentation sur la sauvegarde et la restauration).

Voici les commandes pour restaurer les fichiers de configuration sauvegardés :

1. Placez-vous dans le répertoire contenant vos sauvegardes :

```
cd /mnt/pve/backup-proxmox
ls
```

2. Restaurez les fichiers de configuration :

Restaurer le fichier `/etc/pve/storage.cfg` :

```
# Restaurer le fichier /etc/pve/storage.cfg
sudo tar -xzf pve_YYYY-MM-DD.tar.gz -C /etc/pve/ etc/pve/storage.cfg
```

Remplacez `YYYY-MM-DD` par la date de la sauvegarde que vous voulez restaurer.

Restaurer les configurations du pare-feu :

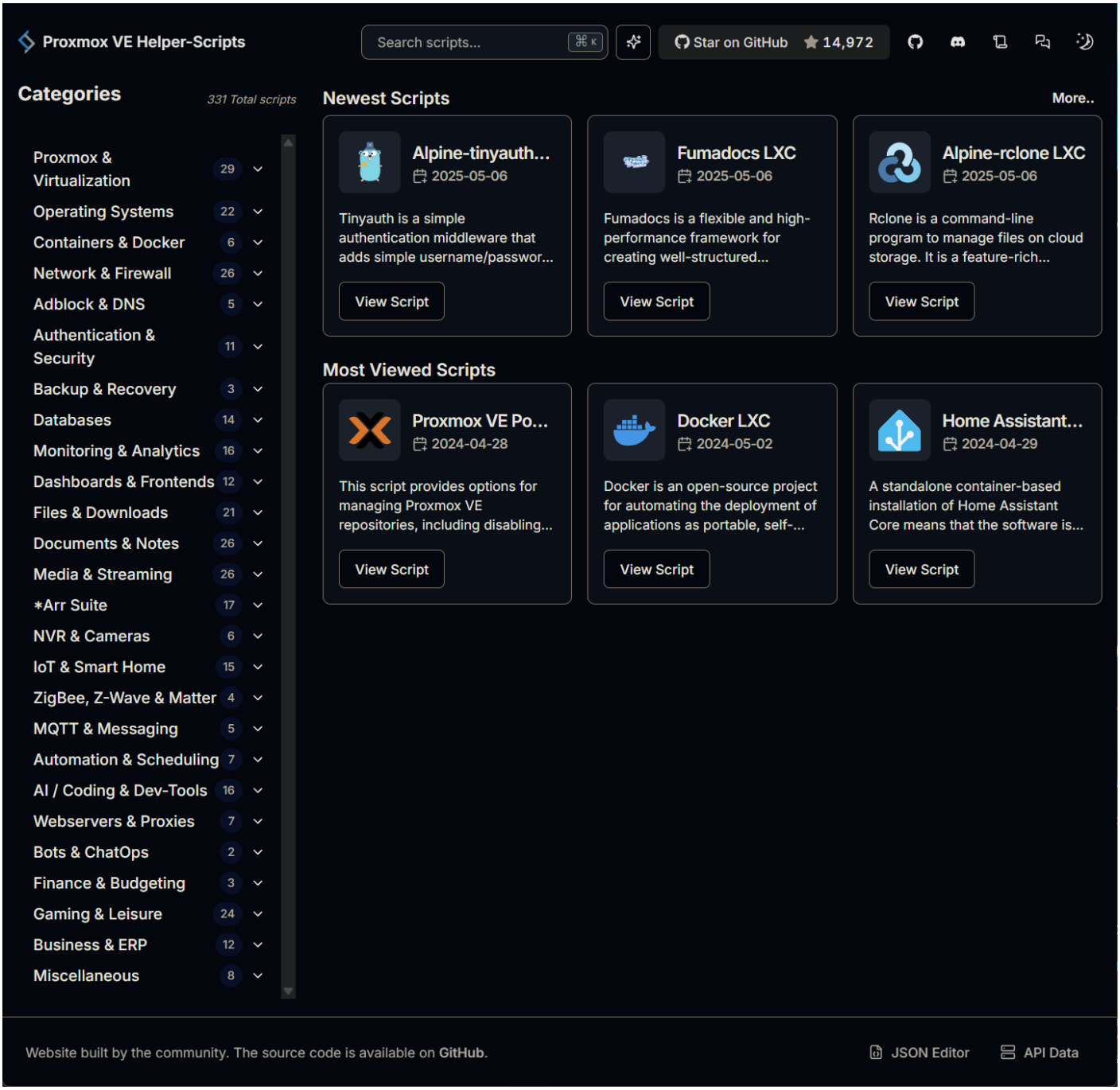
```
# Restaurer le dossier /etc/pve/firewall/
sudo tar -xzf pve_YYYY-MM-DD.tar.gz -C /etc/pve/ etc/pve/firewall/

# Restaurer le fichier /etc/pve/nodes/<node>/host.fw
sudo tar -xzf pve_YYYY-MM-DD.tar.gz -C /etc/pve/nodes/<node>/ etc/pve/nodes/<node>/host.fw
```

Remplacez `YYYY-MM-DD` par la date de la sauvegarde et `<node>` par le nom du nœud Proxmox correspondant.

Proxmox VE Helper-Scripts

Une initiative menée par une communauté qui simplifie la configuration de l'environnement virtuel Proxmox.

Avec plus de 300 scripts pour vous aider à gérer votre environnement Proxmox VE, que vous soyez un utilisateur chevronné ou un nouvel arrivant, ils sont disponibles sur cette page.

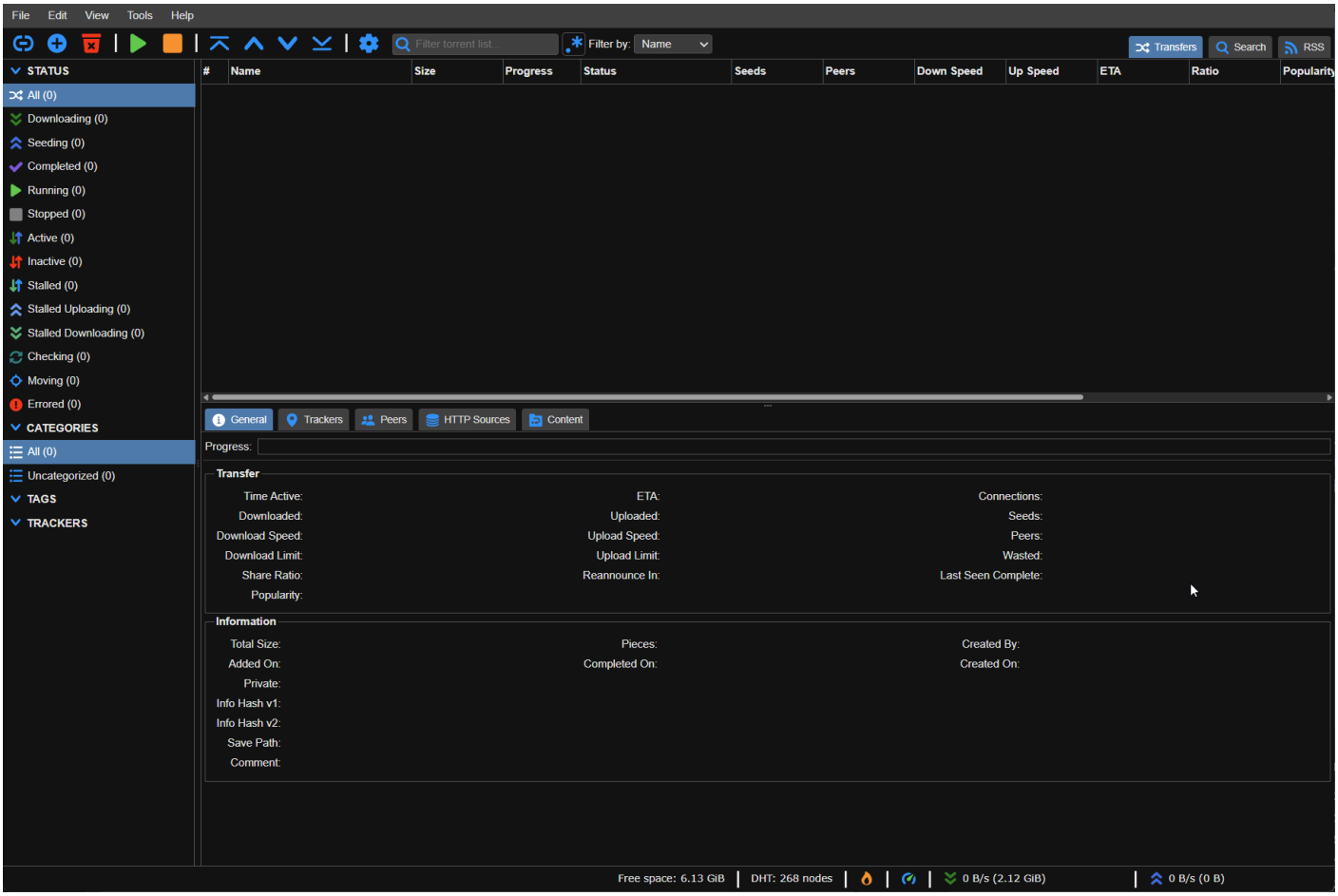


Applications

Applications

qBittorrent avec VPN dans un conteneur LXC

Créer un serveur de téléchargement de torrent avec qBittorrent et une interface conviviale, et installer un VPN.



Prérequis

1. Installer l'application en utilisant le script :

   https://community-scripts.github.io/ProxmoxVE/scripts?id=qbittorrent
2. Récupérer le fichier de configuration WireGuard de votre fournisseur.
   Il devrait ressembler à ceci lorsqu'on l'ouvre avec un éditeur de texte :

```
[Interface]
PrivateKey = VOTRE_CLE_PRIVEE_CLIENT_ICI
Address = 10.0.0.2/24
DNS = 9.9.9.9

[Peer]
PublicKey = CLE_PUBLIQUE_DU_SERVEUR_ICI
Endpoint = 123.45.67.89:51820
AllowedIPs = 0.0.0.0/0, ::/0
PersistentKeepalive = 25
```

3. Ajouter les lignes suivantes **sous** la ligne DNS dans votre configuration WireGuard :

```
PostUp = iptables -I OUTPUT ! -o %i -m mark ! --mark $(wg show %i fwmark) -m addrtype ! --dst-type LOCAL ! -d 192.168.0.0/16 -j REJECT && ip6tables -I OUTPUT ! -o %i -m mark ! --mark $(wg show %i fwmark) -m addrtype ! --dst-type LOCAL -j REJECT
PreDown = iptables -D OUTPUT ! -o %i -m mark ! --mark $(wg show %i fwmark) -m addrtype ! --dst-type LOCAL ! -d 192.168.0.0/16 -j REJECT && ip6tables -D OUTPUT ! -o %i -m mark ! --mark $(wg show %i fwmark) -m addrtype ! --dst-type LOCAL -j REJECT
```

> “ Ces commandes ajoutent (au démarrage) et retirent (à l’arrêt) des règles dans le pare-feu pour empêcher que votre serveur envoie du trafic Internet « en clair » hors du tunnel WireGuard, évitant ainsi les fuites de données non protégées.

Votre configuration devrait ressembler à ceci :

```
[Interface]
PrivateKey = VOTRE_CLE_PRIVEE_CLIENT_ICI
Address = 10.0.0.2/24
DNS = 9.9.9.9

PostUp = iptables -I OUTPUT ! -o %i -m mark ! --mark $(wg show %i fwmark) -m addrtype ! --dst-type LOCAL ! -d 192.168.0.0/16 -j REJECT && ip6tables -I OUTPUT ! -o %i -m mark ! --mark $(wg show %i fwmark) -m addrtype ! --dst-type LOCAL -j REJECT
PreDown = iptables -D OUTPUT ! -o %i -m mark ! --mark $(wg show %i fwmark) -m addrtype ! --dst-type LOCAL ! -d 192.168.0.0/16 -j REJECT && ip6tables -D OUTPUT ! -o %i -m mark ! --mark $(wg show %i fwmark) -m addrtype ! --dst-type LOCAL -j REJECT

[Peer]
```

```
PublicKey = CLE_PUBLIQUE_DU_SERVEUR_ICI
Endpoint = 123.45.67.89:51820
AllowedIPs = 0.0.0.0/0, ::/0
PersistentKeepalive = 25
```

4. Installer le VPN et iptables :

```
sudo apt install -y curl wireguard iptables resolvconf
```

Configuration du VPN

1. Configurer le serveur

Créez et éditez le fichier de configuration WireGuard :

```
sudo nano /etc/wireguard/wg0.conf
```

Collez la configuration VPN dans ce fichier.

Pour enregistrer et sortir de nano :

- Appuyez sur `Ctrl + O` (pour écrire/ enregistrer le fichier),
- puis appuyez sur `Entrée` pour confirmer le nom du fichier,
- ensuite appuyez sur `Ctrl + X` pour quitter l'éditeur.

2. Démarrer le serveur WireGuard

Démarrez et activez le service WireGuard :

```
sudo wg-quick up wg0
sudo systemctl enable wg-quick@wg0 --now
```

3. Vérifier la connexion

Vérifiez le statut de WireGuard :

```
sudo wg
```

4. Tester l'adresse IP publique

Vérifiez votre adresse IP publique en utilisant `curl` :

```
curl ifconfig.me
```

5. Outil permettant de télécharger un fichier torrent privé afin de vérifier l'adresse IP de votre client torrent :

Il vous suffit de faire un clic droit sur le bouton pour copier le lien magnet, puis de l’ajouter dans qBittorrent afin de vérifier qu’aucune fuite de votre adresse IP réelle ne se produit.

Vous pouvez accéder à cet outil à l’adresse suivante :

https://torguard.net/checkmytorrentipaddress.php

Accès

- URL d’accès local : `http://IP_DU_SERVEUR:8090`
  Remplacez `IP_DU_SERVEUR` par l'adresse IP indiquée lors de l'installation de qBittorrent.

Instructions d'installation des nouveaux drivers NVIDIA Tesla P4

1. **Téléchargez les nouveaux drivers :**

   NVIDIA Drivers
2. **Transférez-les sur le serveur CDN :**
   `cdn.favrep.ovh`
3. **Téléchargez les drivers sur Proxmox avec `wget` :**

   ```
   wget <URL_DU_DRIVER>
   ```

4. **Téléchargez le patch :**

   Lien vers le patch
5. **Désinstallez les anciens drivers NVIDIA :**

   ```
   nvidia-uninstall
   ```

   Instructions supplémentaires pour Pascal et les anciennes GPU
6. **Appliquez le patch aux drivers :**

   ```
   ./NVIDIA-Linux-x86_64-550.163.02-vgpu-kvm.run --apply-patch 550.163.02.patch
   ```

7. **Téléchargez le fichier `vgpuConfig.xml` depuis le CDN :**

   ```
   wget --content-disposition --no-check-certificate
   https://lien.com/f.php?h=1nTXJqIG&d=1
   ```

8. **Remplacez le fichier `vgpuConfig.xml` :**

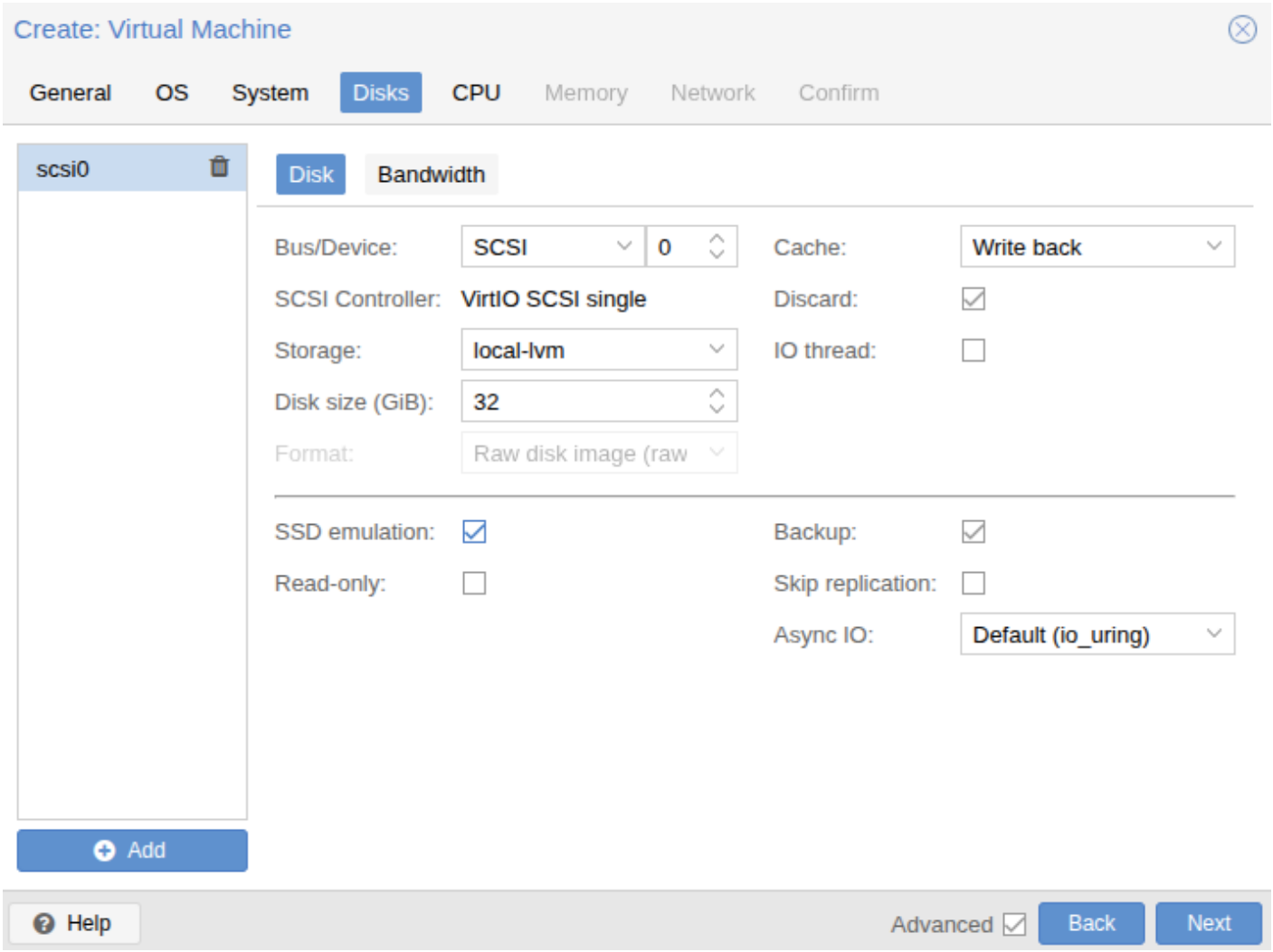
   ```
   mv vgpuConfig.xml /usr/share/nvidia/vgpu/vgpuConfig.xml
   ```

Optimiser les performances des machines virtuelles

Proxmox permet d’optimiser les performances des machines virtuelles (VM) utilisant des disques NVMe ou SSD compatibles en configurant certains paramètres clés. Il est recommandé d’activer le TRIM avec le mode "Write Back" sur les disques virtuels : cette fonctionnalité informe le disque des blocs de données libérés, améliorant les performances et réduisant l’espace utilisé lors des sauvegardes. De plus, cocher l’option "SSD Emulation" indique au système que le disque est un SSD ou NVMe, ce qui optimise la gestion des entrées/sorties par rapport aux disques durs mécaniques.

Il est également conseillé de définir le type de CPU de la VM sur "Host" afin d’exploiter pleinement les capacités du processeur physique.

Concernant l’option "IO Thread" dans la configuration des disques, il vaut mieux **la décocher pour les SSD et NVMe**. Cette option, qui permet de traiter les opérations d’entrée/sortie en parallèle, peut générer une surcharge inutile, le matériel rapide gérant déjà efficacement les accès concurrents. La désactivation des IO threads simplifie ce traitement et évite d’éventuels conflits qui nuiraient aux performances.



Pour optimiser la gestion de l'espace disque et réduire la taille des sauvegardes, on recommande d'exécuter régulièrement la commande `fstrim` via une tâche cron. Cette commande effectue un TRIM sur tous les systèmes de fichiers montés, libérant ainsi de l'espace inutilisé sur les SSD. Ajoutez dans le crontab (`crontab -e`) la ligne suivante :

```
@weekly /sbin/fstrim --all || true
```

Cette tâche s'exécutera chaque dimanche à minuit. Le "|| true" garantit la poursuite du script même en cas d'erreur. Notez que cette opération nécessite des droits administrateur ainsi qu'un système et matériel compatibles TRIM.

En combinant ces réglages, vous améliorez la réactivité des VM, prolongez la durée de vie des disques SSD/NVMe et optimisez les performances d'E/S tout en réduisant la taille des sauvegardes. Pour plus d'informations, la documentation officielle Proxmox reste la meilleure référence :

https://pve.proxmox.com/pve-docs/chapter-qm.html#qm_hard_disk