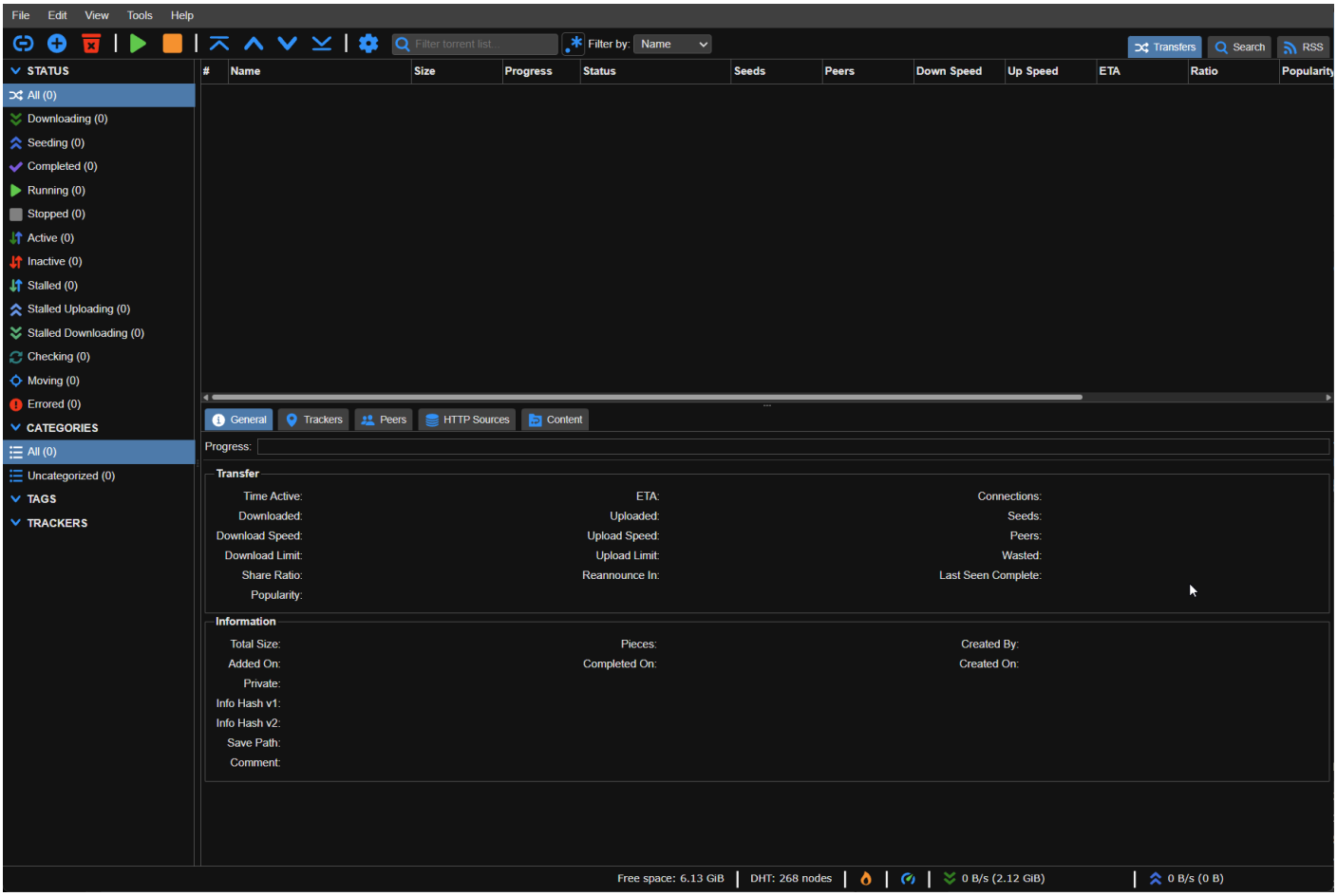
qBittorrent avec VPN dans un conteneur LXC

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.

Révision #3
Créé 2025-06-06 10:59:17 CEST par Philippe Favre
Mis à jour 2025-06-06 12:08:18 CEST par Philippe Favre