Projet personnel — Auto-hébergement

Pi-hole

Bloqueur de publicités à l'échelle du réseau domestique

Docker — docker-compose

Auteur	Cyrille COUR
Type de projet	Personnel — infrastructure réseau domestique
Stack technique	Docker / docker-compose / Pi-hole
Objectif	Bloquer les publicités pour tous les appareils du réseau, sans logiciel par poste
Environnement	Box Orange, résolution DNS locale

1. Contexte et objectif

Les publicités sont quelque chose d'extrêmement ennuyant : elles coupent dans l'élan, consomment de la mémoire et sont parfois très intrusives.

J'ai toujours utilisé uBlock Origin pour les bloquer, mais après un procès perdu par Google le service a cessé de fonctionner correctement. J'ai alors découvert Pi-hole, un programme à l'origine prévu pour Raspberry Pi qui permet de détourner les publicités au niveau du réseau plutôt que poste par poste.

Différence clé : contrairement à uBlock Origin qui s'installe sur chaque navigateur, Pi-hole agit comme serveur DNS pour tout le réseau domestique — un seul point de blocage protège tous les appareils connectés (ordinateurs, téléphones, TV, consoles...), sans rien installer sur chacun d'eux.

Installation choisie ici : dans un conteneur Docker (plutôt que sur un Raspberry Pi physique), via docker-compose.

2. Prérequis

- Docker Desktop installé et fonctionnel sur la machine hôte.
- Un accès PowerShell (ou terminal équivalent).
- Les ports 53 (DNS) et 80 (interface web) disponibles sur la machine hôte.

3. Installation

3.1 Préparer le dossier de travail

- Créer un dossier nommé PiHole (par exemple dans Mes documents).
- À l'intérieur de ce dossier : clic droit → Nouveau → Document texte.
- Renommer exactement en `docker-compose.yml` (bien supprimer l'extension .txt).

3.2 Fichier docker-compose.yml

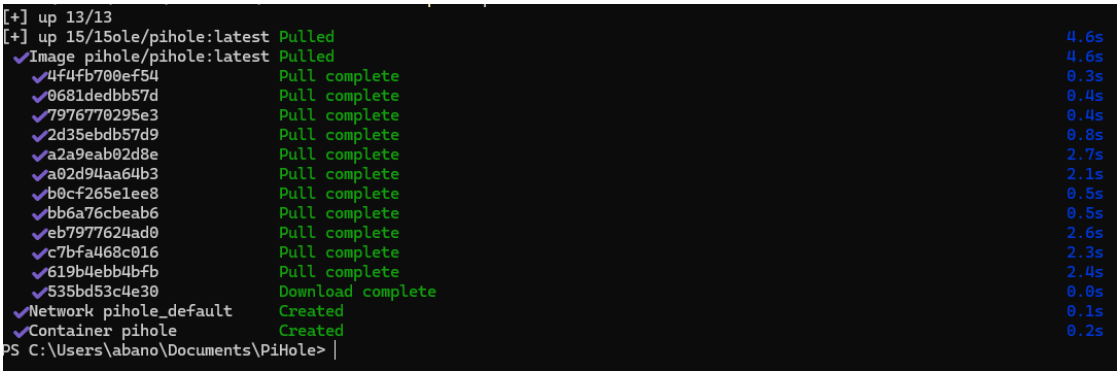
Ouvrir ce fichier avec le Bloc-notes et y coller le contenu suivant :

```
services:
  pihole:
    container_name: pihole
    image: pihole/pihole:latest
    ports:
      - "53:53/tcp"
      - "53:53/udp"
      - "80:80/tcp"
    environment:
      TZ: 'Europe/Paris'
      WEBPASSWORD: 'ton_mot_de_passe_ici'   # à remplacer par son propre mot de passe
    volumes:
      - './etc-pihole:/etc/pihole'
      - './etc-dnsmasq.d:/etc/dnsmasq.d'
    restart: unless-stopped
```

Penser à remplacer WEBPASSWORD par un mot de passe personnel avant de lancer le conteneur — c'est celui qui protège l'interface d'administration.

3.3 Lancer le conteneur

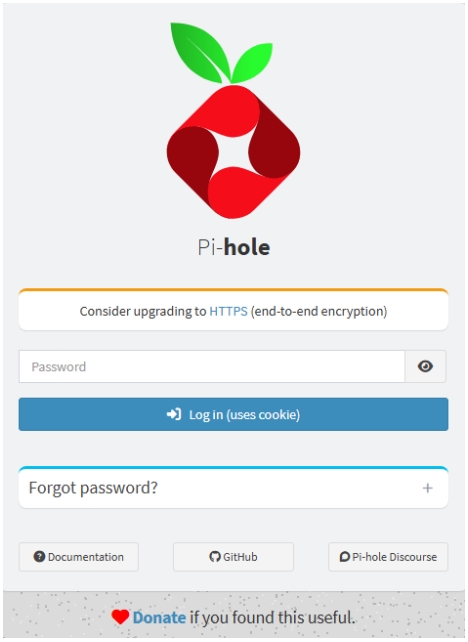
- Dans le dossier PiHole, faire Maj + Clic droit dans le vide puis choisir « Ouvrir avec PowerShell ».
- Taper la commande suivante et appuyer sur Entrée : `docker-compose up -d`
- Docker télécharge alors l'image et démarre le conteneur.



Récupération de l'image et démarrage du conteneur Pi-hole via docker-compose

4. Accéder à l'interface web

Ouvrir le navigateur et saisir dans l'URL : http://localhost/admin



Écran de connexion à l'interface Pi-hole

Après avoir saisi le mot de passe défini dans docker-compose.yml, on arrive sur le tableau de bord. À ce stade, aucune requête n'a encore transité par Pi-hole (0 requête, 0 % bloqué) : le serveur DNS est en ligne mais pas encore utilisé par le réseau.

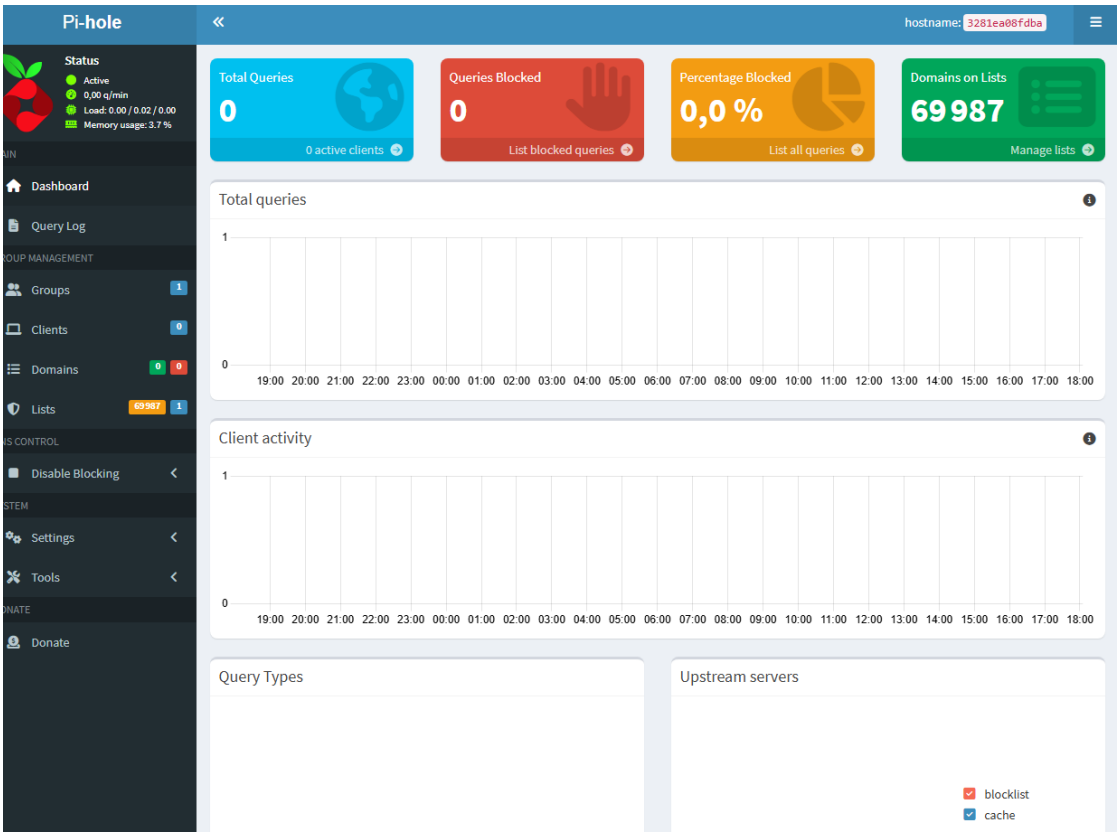


Tableau de bord Pi-hole juste après l'installation — aucune requête traitée

5. Configuration réseau

Pi-hole est installé, mais pour qu'il filtre réellement le trafic il faut l'utiliser comme serveur DNS du réseau. De nombreux tutoriels existent ; un suivi précis a été nécessaire ici car l'installation est chez Orange et Pi-hole tourne en local (pas sur un serveur dédié exposé).

Ajouter des listes de blocage

- Chercher des listes de blocage (blocklists) sur internet.
- Dans Pi-hole → Lists → coller l'URL de la liste → Add to blocklist.

Rediriger le DNS du poste vers Pi-hole

- Aller dans Propriétés réseau.
- Désactiver IPv6 (Disable IPv6).
- Double-cliquer sur IPv4.
- Renseigner `127.0.0.1` en DNS 1, et laisser le DNS 2 vide.

Résultat : une fois cette redirection DNS en place, Pi-hole devient actif et commence à filtrer toutes les requêtes du poste (ou du réseau, selon la configuration du routeur).

6. Résultat — Pi-hole actif

Une fois la configuration DNS appliquée, le tableau de bord se remplit : les requêtes du réseau transitent désormais par Pi-hole, qui bloque celles correspondant aux listes configurées.

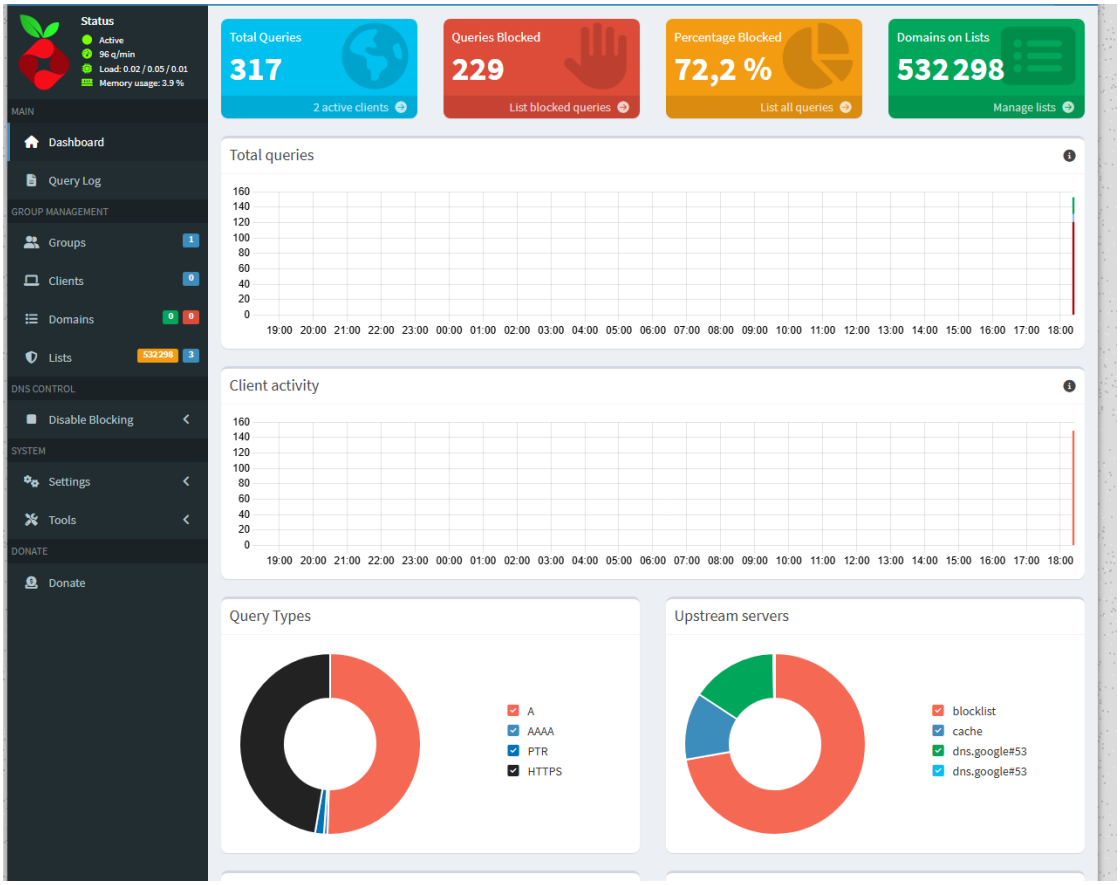


Tableau de bord Pi-hole actif — 317 requêtes, 72,2 % bloquées, 532 298 domaines en liste

7. Bilan

Pi-hole tourne désormais dans un conteneur Docker et filtre les publicités pour l'ensemble des appareils du réseau, sans dépendre d'une extension de navigateur par poste. Ce projet a permis de se familiariser avec docker-compose pour un service exposant à la fois un port DNS (53) et un port web (80), ainsi qu'avec la configuration DNS locale d'un réseau domestique chez un fournisseur d'accès grand public.