Mode Opératoire

Gérer le filtrage DNS (Pi-hole)

Code :	MO-PLT-019
Version :	1.0
Date :	13 avril 2026
Auteur :	Cédric LEGRAND
Classification :	USAGE INTERNE — Équipe BTS SIO

Historique des révisions

Version	Date	Modifications
1.0	13/04/2026	Création initiale — Pi-hole v6.4.1, 3 blocklists, 593 337 domaines

1 Objet

Ce mode opératoire décrit l'utilisation courante de **Pi-hole**, le serveur DNS filtrant déployé sur la plateforme BTS SIO. Pi-hole intercepte les requêtes DNS du réseau pédagogique et bloque celles qui correspondent à des domaines publicitaires, malveillants ou indésirables — sans intervention sur les postes clients.

Le document couvre la connexion au tableau de bord, la consultation des statistiques et du journal de requêtes, la gestion des domaines autorisés/bloqués, et l'administration des listes de blocage (adlists). La configuration DNS avancée (serveurs upstream, DNSSEC, enregistrements locaux) n'entre pas dans le périmètre de cette procédure.

2 Champ d'application

Application	Pi-hole v6.4.1 (web v6.5, FTL v6.6)
Hébergement	CT 200 `docker-srv` (`10.0.112.20`), conteneur Docker
Accès	`https://pihole.docker.bts.sio/admin/` (reverse proxy Traefik)
Authentification	Mot de passe local (identifiants dans Vaultwarden, collection *DNS / Filtrage*)
Domaines bloqués	593 337 (3 blocklists actives au 13/04/2026)
Durée estimée	2–10 minutes selon l'opération

3 Prérequis

Prérequis

— Être connecté au réseau du lycée (filaire ou Wi-Fi) ou via VPN WireGuard
— Un navigateur web récent (Firefox, Chrome, Edge)
— Disposer du mot de passe Pi-hole (Vaultwarden, collection « DNS / Filtrage »)

4 Procédure

4.1 Se connecter au tableau de bord Pi-hole

Étape 1 — Ouvrir l'interface et s'authentifier

Ouvrir un navigateur et saisir l'adresse :

`https://pihole.docker.bts.sio/admin/`

La page de connexion Pi-hole s'affiche avec le logo et le champ de mot de passe.

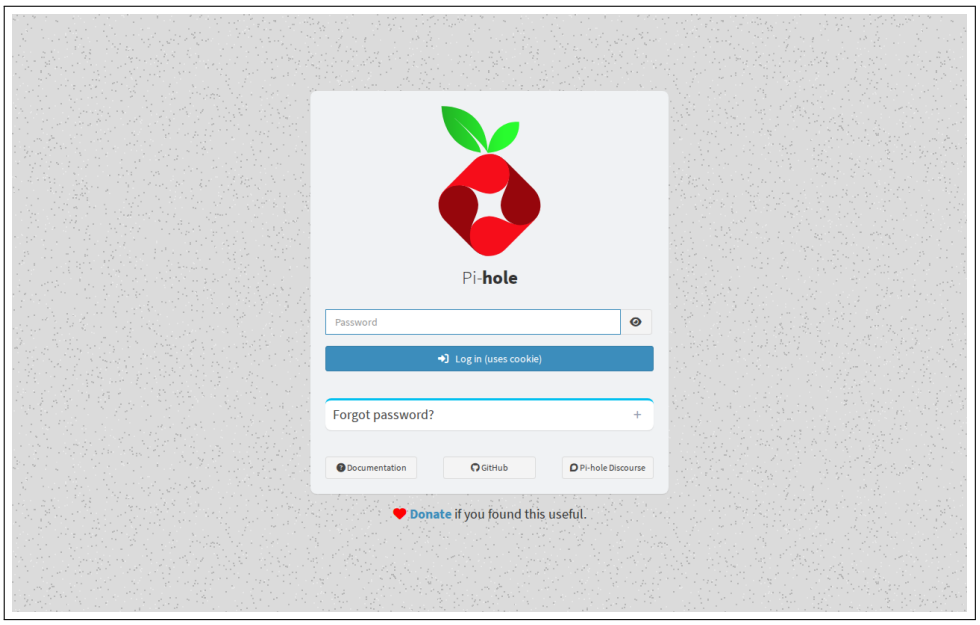

Figure 1 – Page de connexion Pi-hole v6 — saisie du mot de passe

Renseigner le champ *Password* avec le mot de passe stocké dans Vaultwarden, puis cliquer sur **Log in (uses cookie)**. Le tableau de bord s'affiche avec les statistiques globales de filtrage.

Note

Le certificat TLS est auto-signé (TRAEFIK DEFAULT CERT). Le navigateur affichera un avertissement de sécurité : accepter l'exception pour accéder à l'interface. Cela n'affecte pas la sécurité du filtrage DNS.

4.2 Consulter les statistiques et requêtes bloquées

Étape 1 — Lire le tableau de bord

Le dashboard présente quatre indicateurs principaux en haut de page :

— **Total Queries** : nombre total de requêtes DNS traitées

— **Queries Blocked** : requêtes bloquées par les listes de filtrage

— **Percentage Blocked** : taux de blocage (typiquement 1–5 % sur le réseau pédagogique)

— **Domains on Blocklists** : nombre de domaines dans les listes actives (593 337 actuellement)

En dessous, les graphiques montrent l'activité DNS dans le temps, la répartition par client et par type de requête, ainsi que les serveurs upstream utilisés.

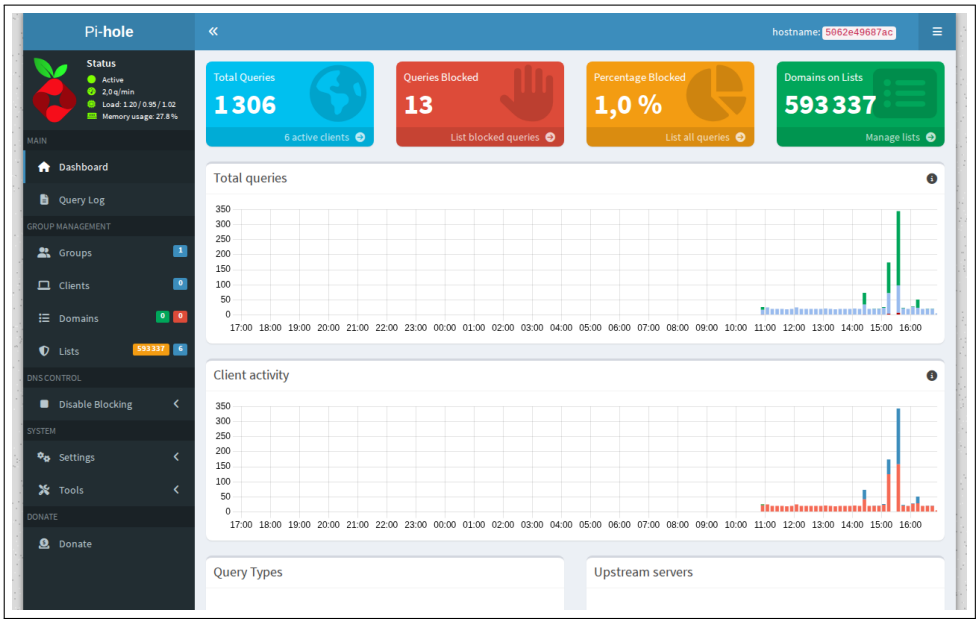

Figure 2 – Tableau de bord Pi-hole : 1 306 requêtes, 13 bloquées, 593 337 domaines filtrés, 6 clients actifs

Astuce

En cliquant sur l'un des quatre indicateurs, Pi-hole filtre automatiquement le journal de requêtes pour afficher la catégorie correspondante. Par exemple, un clic sur « Queries Blocked » n'affichera que les requêtes bloquées.

Étape 2 — Consulter le journal de requêtes (Query Log)

Dans le menu latéral gauche, cliquer sur **Query Log**. La page affiche les requêtes DNS récentes sous forme de tableau :

— **Time** : horodatage de la requête
— **Type** : type d'enregistrement DNS (A, AAAA, PTR, SRV…)
— **Domain** : domaine interrogé
— **Client** : adresse IP du poste ayant émis la requête
— **Status** : résultat (forwarded, cached, blocked by gravity…)

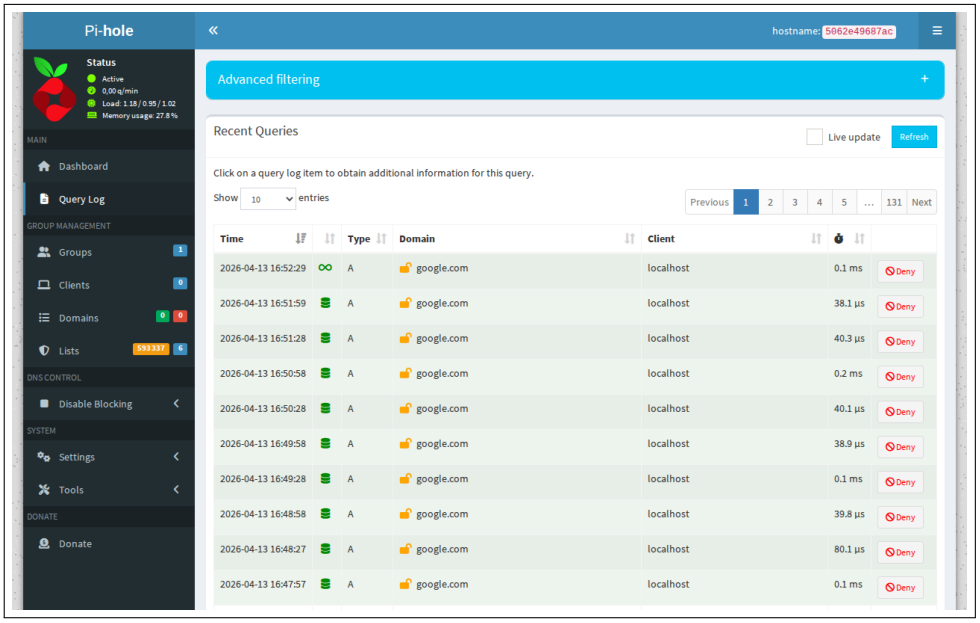

Figure 3 – Journal de requêtes DNS : domaines interrogés, types, clients et statuts de résolution

Note

Le champ *Advanced Filtering* en haut de la page permet de filtrer par domaine, client, type de requête ou statut. Utiliser cette fonction pour diagnostiquer rapidement pourquoi un site est bloqué ou identifier un poste qui génère un trafic DNS anormal.

4.3 Whitelister un domaine bloqué par erreur

Étape 1 — Identifier le domaine bloqué

Depuis le **Query Log**, repérer la requête bloquée (statut *Blocked (gravity)* ou *Blocked (regex)*). Noter le nom de domaine exact.

On peut aussi cliquer directement sur une entrée bloquée dans le journal : Pi-hole propose alors un bouton pour whitelister le domaine concerné.

Étape 2 — Ajouter le domaine à la liste d'autorisation

Dans le menu latéral, naviguer vers **Domains** (sous **Group Management**). La page *Domain management* s'affiche.

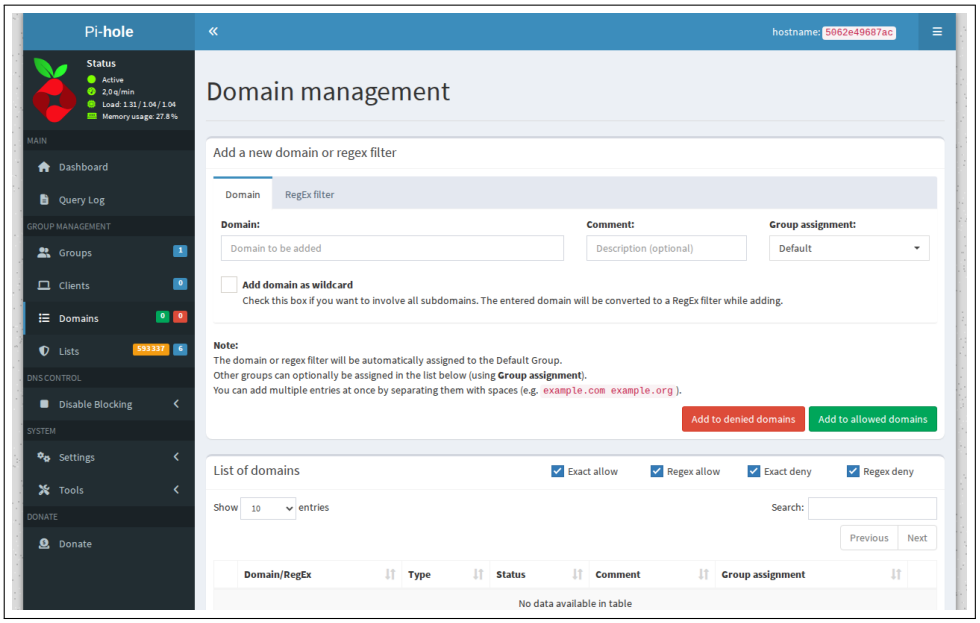

Figure 4 – Gestion des domaines : onglets Allow/Deny, ajout par domaine exact ou expression régulière

Étape 3 — Configurer l'autorisation

1. Sélectionner l'onglet **Allow** (liste blanche)
2. Dans le type, choisir **Exact whitelist** (ou **Regex whitelist** si plusieurs sous-domaines sont concernés)
3. Saisir le domaine dans le champ *Domain*
4. Cocher *Add domain as wildcard* si l'on souhaite inclure tous les sous-domaines
5. Cliquer sur **Add to Allow list** pour valider

La modification prend effet immédiatement : Pi-hole applique les changements sans redémarrage.

⚠ Whitelister avec discernement

Avant d'ajouter un domaine à la liste blanche, vérifier sa légitimité. Certains domaines de tracking ou de télémétrie sont délibérément bloqués. En cas de doute, consulter les listes de référence (HaGeZi, StevenBlack) pour comprendre pourquoi le domaine est filtré.

4.4 Gérer les listes de blocage (adlists)

Étape 1 — Consulter les listes actives

Dans le menu latéral, naviguer vers **Adlists** (sous **Group Management**). Les listes de blocage souscrites s'affichent avec leur adresse, commentaire, statut et nombre de domaines.

Listes actives au 13/04/2026 :

Liste	Domaines	Statut
StevenBlack — Unified hosts	87 771	Active
HaGeZi Pro	408 244	Active
StevenBlack — Ads+Fakenews+Gambling+Porn	97 322+	Active

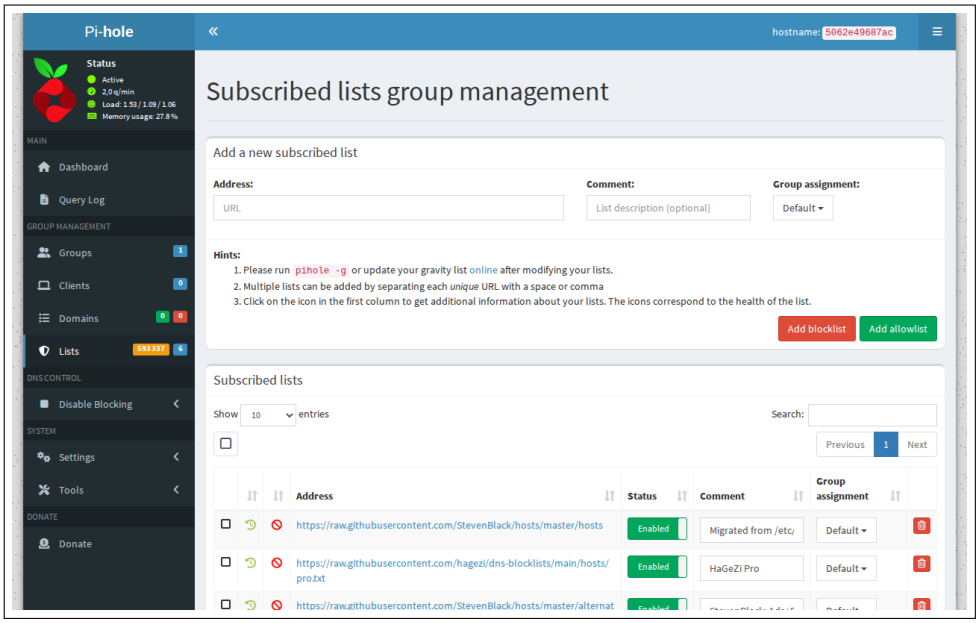

Figure 5 – Listes de blocage souscrites : StevenBlack (unifiée et étendue) et HaGeZi Pro

Étape 2 — Ajouter une nouvelle liste

1. Saisir l'URL de la liste dans le champ *Address*
2. Ajouter un commentaire descriptif dans *Comment*
3. Cliquer sur **Add Subscribed list**

Après l'ajout, naviguer vers **Gravity** dans le menu et lancer **Update Gravity** pour télécharger et intégrer la nouvelle liste. L'opération prend généralement 30 secondes à 2 minutes selon la taille de la liste.

Mise à jour des listes

Pi-hole met automatiquement à jour les listes de blocage via la tâche *Gravity*. Pour forcer une mise à jour manuelle, accéder à **Gravity** dans le menu et cliquer sur **Update Gravity**. Cette opération re-télécharge toutes les listes actives et recalcule la base de filtrage.

Désactiver temporairement le filtrage

Pour désactiver Pi-hole temporairement (débogage, test), utiliser le bouton **Disable Blocking** dans le menu latéral sous **Enable Blocking**. On peut définir une durée (30 secondes, 1 minute, 5 minutes) après laquelle le filtrage se réactive automatiquement.

5 Vérification et dépannage

Vérification

Après toute modification, vérifier les points suivants :

- ☐ Le dashboard est accessible à `https://pihole.docker.bts.sio/admin/`
- ☐ L'authentification fonctionne avec le mot de passe Vaultwarden
- ☐ Les compteurs du dashboard se mettent à jour en temps réel
- ☐ Le journal de requêtes affiche les dernières requêtes DNS
- ☐ Un domaine whiteisté n'apparaît plus comme bloqué dans le Query Log
- ☐ Les listes de blocage sont actives et à jour (colonne *Status*)
- ☐ Gravity est à jour (date de dernière mise à jour visible sur le dashboard)

Dépannage

Problème	Solution
Interface inaccessible	Vérifier la connectivité : `ping 10.0.112.20`. Contrôler le conteneur Docker : `docker ps | grep pihole`.
Mot de passe refusé	Vérifier dans Vaultwarden. Sensible à la casse. Délai de 2 min après 5 échecs.
Site légitime bloqué	Repérer le domaine dans le Query Log. Whitelister via **Domains**.
Aucune requête bloquée	Vérifier le DNS DHCP : OPNsense doit distribuer `10.0.112.20`. Test : `nslookup ads.google.com 10.0.112.20` → `0.0.0.0`.
Gravity en échec	Tester l'accès Internet du conteneur : `docker exec pihole curl -sI https://raw.githubusercontent.com`.