LoLi GrUB

Logiciels Libres Groupe Utilisateurs Borains

A.S.B.L.

LoLi GrUB

Logiciels Libres Groupe Utilisateurs Borains

A.S.B.L.

Cet atelier fait suite à celui de décembre qui était consacré à une présentation de Pi-Hole.

Le point après plusieurs mois d’utilisation

Petites rappels - Pi-Hole c’est quoi ?

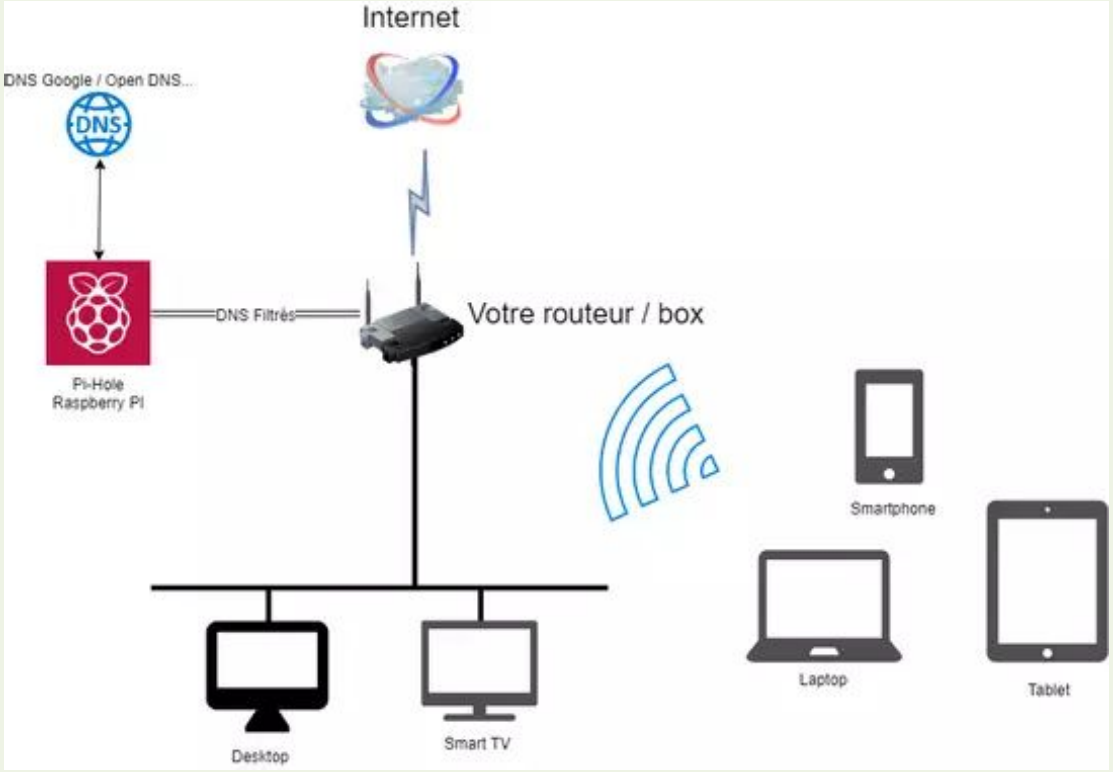
https://www.malekal.com/pi-hole-bloquer-publicite-trackers/
https://mediacenterz.com/tutoriel-complete-pi-hole-bloqueur-dannonces-pour-toute-la-maison/

- Bloqueur de pub et de trackers
- Un projet libre qui permet de créer un serveur pour bloquer la publicité et le pistage sur internet (trackers).
- Vous protège des publicités et trackers grâce à un blocage efficace pour une meilleur vie privée.
- Fonctionne sous Linux et peut se voir donc comme un serveur anti-publicité et anti-trackers.
- Peut être installé sur raspberry pi dans un réseau LAN ou sur un serveur dédié sur internet.
- Pi-Hole est une application de blocage de publicités à l’échelle du réseau.
- Il configure un serveur DNS et gère toutes les demandes DNS générées à partir de votre réseau domestique.
- En termes simples, un serveur DNS est un registre d’adresses Internet qui permet de localiser le serveur à l’aide du nom de domaine. Lorsque vous visitez un site, le serveur DNS est interrogé afin de localiser l’adresse IP (emplacement) du serveur auquel se connecter.

Pi-Hole c’est quoi ?

https://www.malekal.com/pi-hole-bloquer-publicite-trackers/

Pi-Hole se place entre votre appareil et le serveur DNS, il bloque toutes les demandes adressées à des serveurs de publicité connus.



Pi-Hole - Comment ça fonctionne ?

https://www.malekal.com/pi-hole-bloquer-publicite-trackers/

- **Pi-hole est un DNS sinkhole qui protège vos appareils contre le contenu indésirable, sans installer de logiciel côté client.**
- **Cela est assez pratique pour les petites configurations car vous évitez de surcharger le navigateur internet.**
- **Voici les caractéristiques et avantages qu'offrent pi-hole :**

  - Facile à installer : notre installateur polyvalent vous guide tout au long du processus et prend moins de dix minutes.
  - Filtrage complet contre les trackers : le contenu est bloqué dans des emplacements autres que des navigateurs, tels que les applications mobiles chargées de publicités et les téléviseurs intelligents.
  - Réactif : accélère de manière transparente la sensation de la navigation quotidienne en mettant en cache les requêtes DNS.
  - Léger : fonctionne sans problème avec des exigences matérielles et logicielles minimales. Une machine avec 512Mo RAM suffit.
  - Robuste : une interface de ligne de commande dont la qualité est garantie pour l'interopérabilité.
  - Perspicace : un magnifique tableau de bord d'interface Web réactif pour afficher et contrôler votre trou Pi.
  - Polyvalent : peut éventuellement fonctionner comme un serveur DHCP, garantissant que tous vos appareils sont automatiquement protégés.
  - Évolutif : capable de gérer des centaines de millions de requêtes lorsqu'il est installé sur du matériel de qualité serveur.
  - Moderne : bloque les publicités sur IPv4 et IPv6.
  - Gratuit : logiciel open source qui vous aide à être le seul à contrôler votre vie privée.

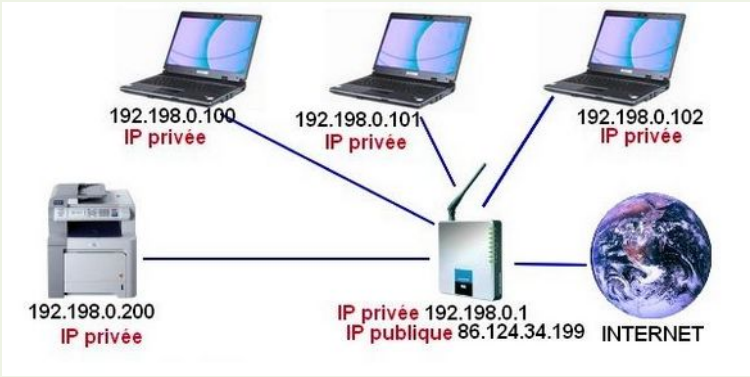
DNS ? Adresse IP ? Adresse MAC ?

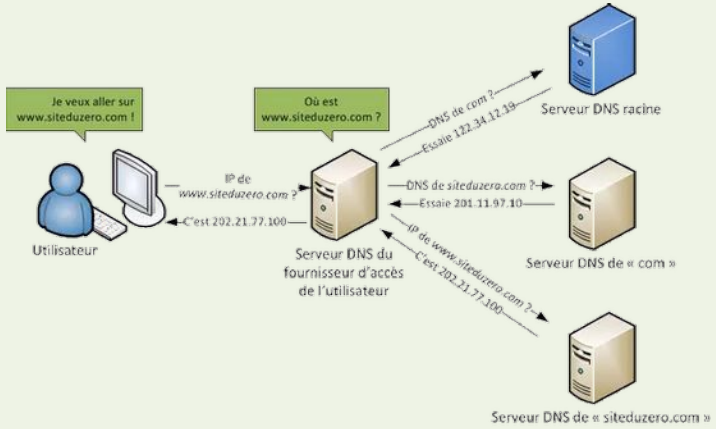
https://www.cloudflare.com/fr-fr/learning/dns/what-is-dns/

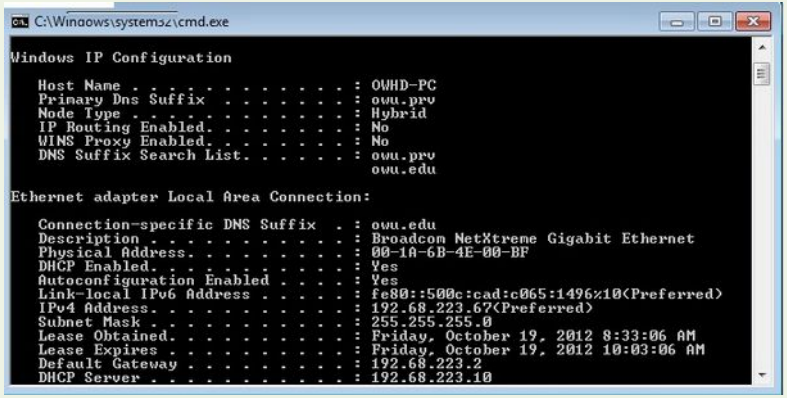
- Le DNS (Domain Name System, système de nom de domaine) est en quelque sorte le répertoire téléphonique d'Internet.
- Les internautes accèdent aux informations en ligne via des noms de domaine (par exemple, loligrub.be ou espn.com), tandis que les navigateurs interagissent par le biais d'adresses IP (Internet Protocol, protocole Internet).
- Le DNS traduit les noms de domaine en adresses IP afin que les navigateurs puissent charger les ressources web.
- Chaque appareil connecté à Internet dispose d'une adresse IP unique que les autres appareils utilisent afin de le trouver.
- Grâce aux serveurs DNS, les internautes n'ont pas à mémoriser les adresses IP (par exemple, 192.168.1.1 en IPv4) ni les adresses IP alphanumériques plus récentes et plus complexes (par exemple, 2400:cb00:2048:1::c629:d7a2 en IPv6).

DNS ? Adresse IP ? Adresse MAC ?

https://www.cloudflare.com/fr-fr/learning/dns/what-is-dns/



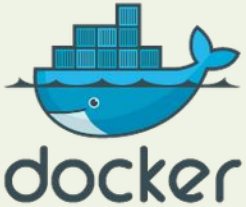




Voici quelques-unes des fonctionnalités / avantages de Pi Hole:?

https://mediacenterz.com/tutoriel-complete-pi-hole-bloqueur-dannonces-pour-toute-la-maison/

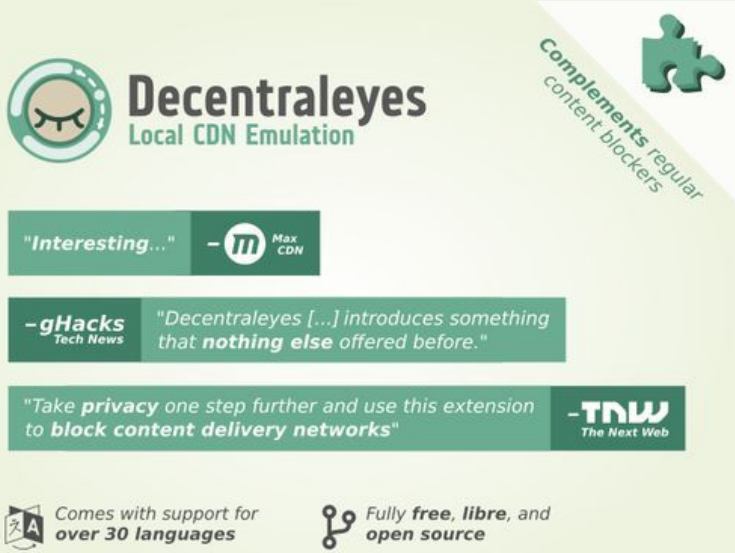
- Libre!!! Tout ce dont vous avez besoin est un appareil sur lequel exécuter Pi-Hole: Raspberry Pi, Linux Machine ou Docker.



Voici quelques-unes des fonctionnalités / avantages de Pi Hole:?

https://mediacenterz.com/tutoriel-complete-pi-hole-bloqueur-dannonces-pour-toute-la-maison/

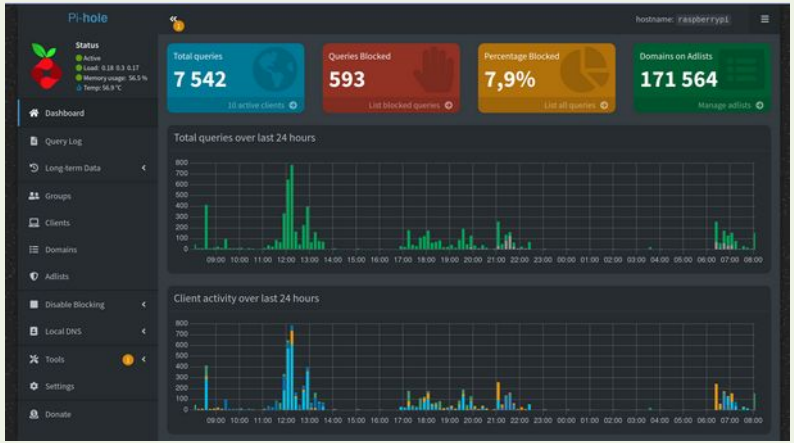
- Aucun logiciel de bloc d'annonces côté client requis.



Voici quelques-unes des fonctionnalités / avantages de Pi Hole:?

https://mediacenterz.com/tutoriel-complete-pi-hole-bloqueur-dannonces-pour-toute-la-maison/

- Plus de 100 000 domaines de diffusion d'annonces bloqués. Vous pouvez développer cela en utilisant des listes de serveurs librement disponibles.
- Bloque les publicités sur tous les appareils, y compris les téléviseurs intelligents et autres appareils qui ne vous permettent aucune modification.
- Réduit la bande passante et améliore les performances globales du réseau.
- Fournit un tableau de bord génial pour surveiller diverses statistiques sur le blocage des publicités. Pi-Hole a un serveur Web intégré qui fournit une interface utilisateur Web facile à utiliser pour l'administration.



Procédure pour installer Pi-Hole

https://mediacenterz.com/tutoriel-complete-pi-hole-bloqueur-dannonces-pour-toute-la-maison/

Sans oublier un point important : Pi Hole a besoin d'une adresse IP Statique (c-à-d fixe) au niveau de votre Box

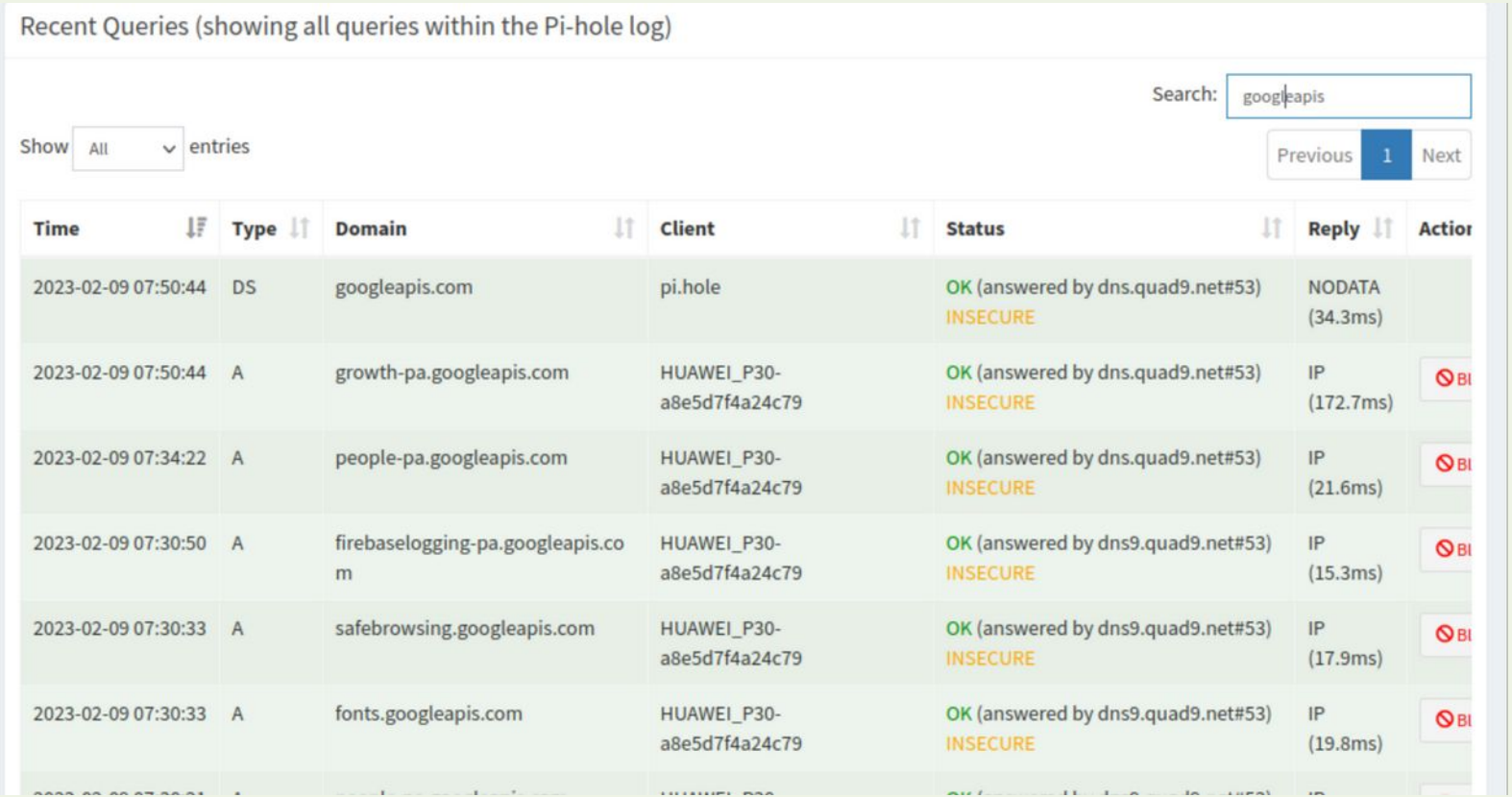
- DNS primaire = adresse IP du Raspberry
- Ne pas oublier de renseigner un DNS Secondaire en cas d'indisponibilité du Raspberry

https://raspberrytips.fr/installer-pihole-raspberry-pi/

Vérification du réseau

Les paramètres de configuration sont bien enregistrés
DNS Primaire
DNS Secondaire

Pour bloquer un domaine … (ex. : googleapis.com)



Recent Queries (showing all queries within the Pi-hole log)

Search: googleapis

Show All entries

Previous 1 Next

Time	Type	Domain	Client	Status	Reply	Actior
2023-02-09 07:50:44	DS	googleapis.com	pi.hole	OK (answered by dns.quad9.net#53) INSECURE	NODATA (34.3ms)	
2023-02-09 07:50:44	A	growth-pa.googleapis.com	HUAWEI_P30-a8e5d7f4a24c79	OK (answered by dns.quad9.net#53) INSECURE	IP (172.7ms)	Bl
2023-02-09 07:34:22	A	people-pa.googleapis.com	HUAWEI_P30-a8e5d7f4a24c79	OK (answered by dns.quad9.net#53) INSECURE	IP (21.6ms)	Bl
2023-02-09 07:30:50	A	firebaselogging-pa.googleapis.com	HUAWEI_P30-a8e5d7f4a24c79	OK (answered by dns9.quad9.net#53) INSECURE	IP (15.3ms)	Bl
2023-02-09 07:30:33	A	safebrowsing.googleapis.com	HUAWEI_P30-a8e5d7f4a24c79	OK (answered by dns9.quad9.net#53) INSECURE	IP (17.9ms)	Bl
2023-02-09 07:30:33	A	fonts.googleapis.com	HUAWEI_P30-a8e5d7f4a24c79	OK (answered by dns9.quad9.net#53) INSECURE	IP (19.8ms)	Bl

Pour bloquer un domaine … (ex. : googleapis.com)

COMMENTSUPPRIMER ?

Virus | Services en ligne | Applications | Télécharger

Supprimer storage.googleapis.com

12 janvier 2017 Jean Sugoi Adware Pas de commentaires

Google propose de nombreux outils qui permettent aux développeurs de créer des applications et des services Web, **storage.googleapis.com** en fait partie.

storage.googleapis.com est le service qui héberge Google Cloud Storage. Vous pouvez lire les informations sur ce servuice à l'adresse cloud.google.com/storage . Ce service permet aux développeurs de stocker les fichiers que vous souhaitez télécharger. Google Cloud Storage n'est pas destiné à être un service de service d'hébergement de site Web, c'est un service de téléchargement. Malheureusement, lorsque votre navigateur tente de « télécharger » le code d'une page Web, il est chargé en tant que site Web. Les développeurs malveillants ont abusé de ce service en s'en servant pour développer des sites malicieux et des adwares. C'est pour cela que **storage.googleapis.com** est souvent assimilé à un site malveillant alors qu'il s'agit plutôt de l'utilisation qu'en ont fait certaines personnes malveillantes.

Pour supprimer les accès malveillant ou suspect à storage.googleapis.com vous devez nettoyer votre ordinateur. Le faire sans outils spécifique est quasiement mission impossible, à part utiliser la restauration du système à une date antérieur ou résinstaller complètement vos navigateurs ou Windows, il n'y a pas vraiment d'autres choix. Les outils que nous avons selectionnés pour vous sont gratuits et reconnus par la communauté anti-malware comme étant les plus performant.

Comment supprimer storage.googleapis.com ?

Vous trouverez ci-dessous des explications précises pour éradiquer définitivement **storage.googleapis.com** de votre ordinateur. Il est très important d'effectuer toutes les indications ci-dessous. Les utilitaires que vous serez amenés à télécharger sont **gratuits** et controlés par notre équipe. Si jamais vous avez un problème pendant l'élimination de storage.googleapis.com n'hésitez pas à poser votre question sur la page **Demander de l'aide** accessible dans la barre de menu du site.

- Étape 1 - Supprimer storage.googleapis.com avec Malwarebytes Anti-Malware
- Étape 2 - Supprimer storage.googleapis.com avec l'aide d'Adwcleaner
- Étape 3 - Supprimer storage.googleapis.com avec ZHPCleaner
- Étape 4 - Supprimer storage.googleapis.com avec HitmanPro
- Étape 5 - Réinitialiser votre navigateur (si nécessaire)

…. ou alors utiliser Pi-Hole

Quelques sites intéressants

- https://nicolasforcet.com/2019/11/02/meilleures-listes-de-filtrage-dns-pour-pihole-et-autres/
- https://lecrabeinfo.net/les-meilleurs-serveurs-dns-rapides-et-gratuits.html#comment-changer-ses-serveurs-dns
- https://www.lucaswillems.com/fr/articles/25/tutoriel-pour-maitriser-les-expressions-regulieres
- https://www.cloudflare.com/fr-fr/learning/dns/dns-server-types/
- https://www.malekal.com/les-meilleures-listes-de-blocage-adlists-pour-pi-hole/

Problèmes rencontrés durant ce test

1. Carte Micro SD hs
2. Blocage de Pi-Hole (1x)
3. Requêtes en boucles - Queries PTR

Problèmes rencontrés avec la **carte SD** durant ce test (p1)

https://raspberrytips.fr/installer-pihole-raspberry-pi/

Lors de la phase d'installation ...

…. Ensuite, vous verrez une option pour activer ou désactiver **la journalisation des requêtes**.

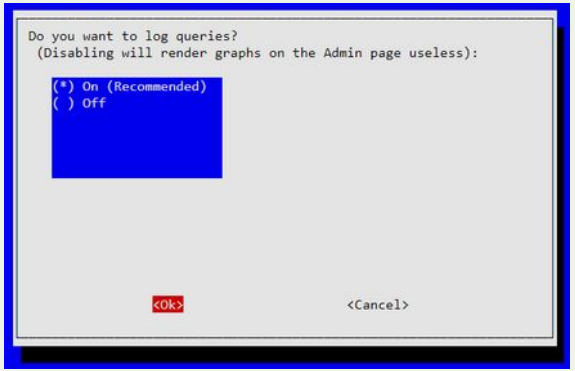
La journalisation Querry vous fournit toutes les statistiques intéressantes sur le nombre de demandes bloquées, etc.

Il est également important de dépanner un site Web légitime que vous visitez ne fonctionne pas correctement.

Laisser l'enregistrement des requêtes augmenterait les écritures sur votre carte SD et en réduirait la durée de vie.

Ainsi, après avoir utilisé PiHole pendant quelques semaines et vérifié que tout fonctionne correctement, vous pouvez envisager de désactiver la journalisation des requêtes via l'interface Web d'administration.

Vous pouvez également envisager de déplacer vos journaux vers la RAM ou booter le Raspberry sur une disque USB externe.



Booter sur un disque SSD externe (1)

https://raspberry-pi.fr/boot-raspberry-pi-usb/

Autoriser la Raspberry Pi à booter sur une clé USB

À noter, pour la Raspberry Pi 3B+, vous n'avez pas besoin d'effectuer les opérations ci-dessous, simplement d'installer Raspbian sur votre périphérique USB, l'inséré dans la Pi sans la carte MicroSD, il sera détecté automatiquement.

Maintenant que vous avez l'ensemble du matériel nécessaire, vous allez devoir commencer par installer Raspbian sur votre carte SD. Pour cela, nous vous renvoyons à notre article pour installer Raspbian depuis Windows, ou depuis Linux.

Raspbian installé sur votre carte microSD, répétez l'opération en installant cette fois-ci Raspbian sur votre clef USB/disque dur. Une fois fini, débranchez la clef USB/disque dur.

Une fois les deux installations terminées, connectez la carte SD à votre PC et rendez vous dans la partition `boot` de la carte (la seule accessible depuis Windows, normalement) pour éditer le fichier `config.txt` et rajouter à la fin du fichier la ligne suivante :

```
program_usb_boot_mode=1
```

Booter sur un disque SSD externe (2)

https://raspberry-pi.fr/boot-raspberry-pi-usb/

Sauvegardez le fichier, puis insérez la carte micro SD dans votre Raspberry Pi et démarrez la (insérez seulement la carte SD, pas la clef USB/disque dur). Normalement une fois démarrée, la Raspberry Pi va automatiquement se configurer pour à l'avenir démarrer sur la clé USB.

Pour vérifier que tout est bon, on peut regarder le registre 17 de l'OPT (One-Time programmable qui désigne la mémoire morte qui ne peut être programmée qu'une seule fois). Pour cela on utilise la commande suivante :

```
vcgencmd otp_dump | grep 17
```

La Raspberry Pi doit nous retourner : **17:3020000a**. Si ce n'est pas le cas, c'est que vous avez mal effectué une étape précédente et que vous devez recommencer la création de la carte.

Vous pouvez maintenant éteindre votre Raspberry Pi, sortir votre carte micro SD et insérer votre clef USB/disque dur avec Raspbian installé.

Il ne vous reste plus qu'à brancher votre Raspberry Pi, le démarrage va prendre quelques secondes, et ça y est, votre Raspberry Pi boot depuis votre clef USB !

Service DNS

https://www.it-connect.fr/chapitres/les-types-denregistrements-dns/

Les types d'enregistrements DNS

https://www.it-connect.fr/chapitres/les-types-denregistrements-dns/

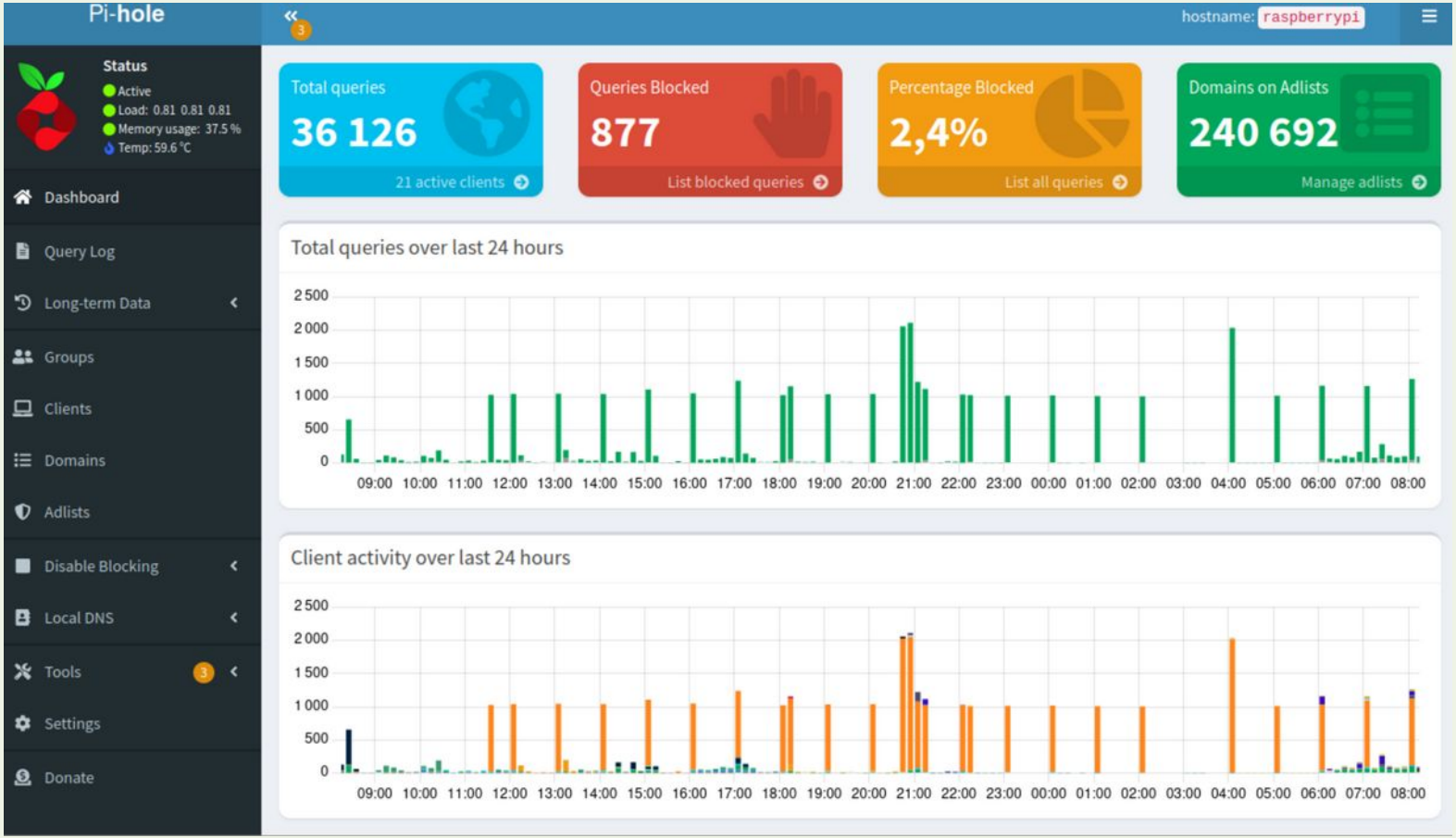
Le DNS n'était rien d'autre qu'un annuaire (au même titre qu'un simple bottin téléphonique), mettant en relation les adresses IP des équipements du réseau avec un nom (plus exploitable), lié à la machine.

Donc, un DNS peut être vu comme une base de données répartie, contenant des enregistrements de ressources, appelés Resource Records (ou RR), codés sur 16bits, concernant les noms de domaine et codifiant les types d'enregistrements suivants :

- **A** : il s'agit des enregistrements d'adresses faisant correspondre un nom d'hôte à une adresse IPv4 de 32bits.
- En IPv6, on utilise des enregistrements **AAAA** codés sur 128bits.
- **CNAME** : il s'agit d'enregistrements canoniques créant un alias d'un domaine vers un autre. L'alias hérite de tous les sous-domaines de l'original.
- **MX** : définit les serveurs de messagerie pour le domaine.
- **PTR** : associe une adresse IP à un enregistrement de nom de domaine (on parle de reverse puisqu'il s'agit du contraire de l'enregistrement A).
- **NS** : définit les serveurs DNS du domaine (primaire et secondaire).
- **SOA** : fournit les informations générales de la zone : serveur principal, contact, délai d'expiration, n° de série de la zone.
- **SRV** : généralise la notion d'enregistrement MX en proposant des fonctions avancées : taux de répartition de charge (décrit dans la RFC2782).
- **NAPTR** : donne accès aux règles de réécriture de l'information permettant de lier le nom de domaine et une ressource (RFC3403).
- **TXT** : permet à l'administrateur d'insérer un texte quelconque pour un enregistrement DNS.

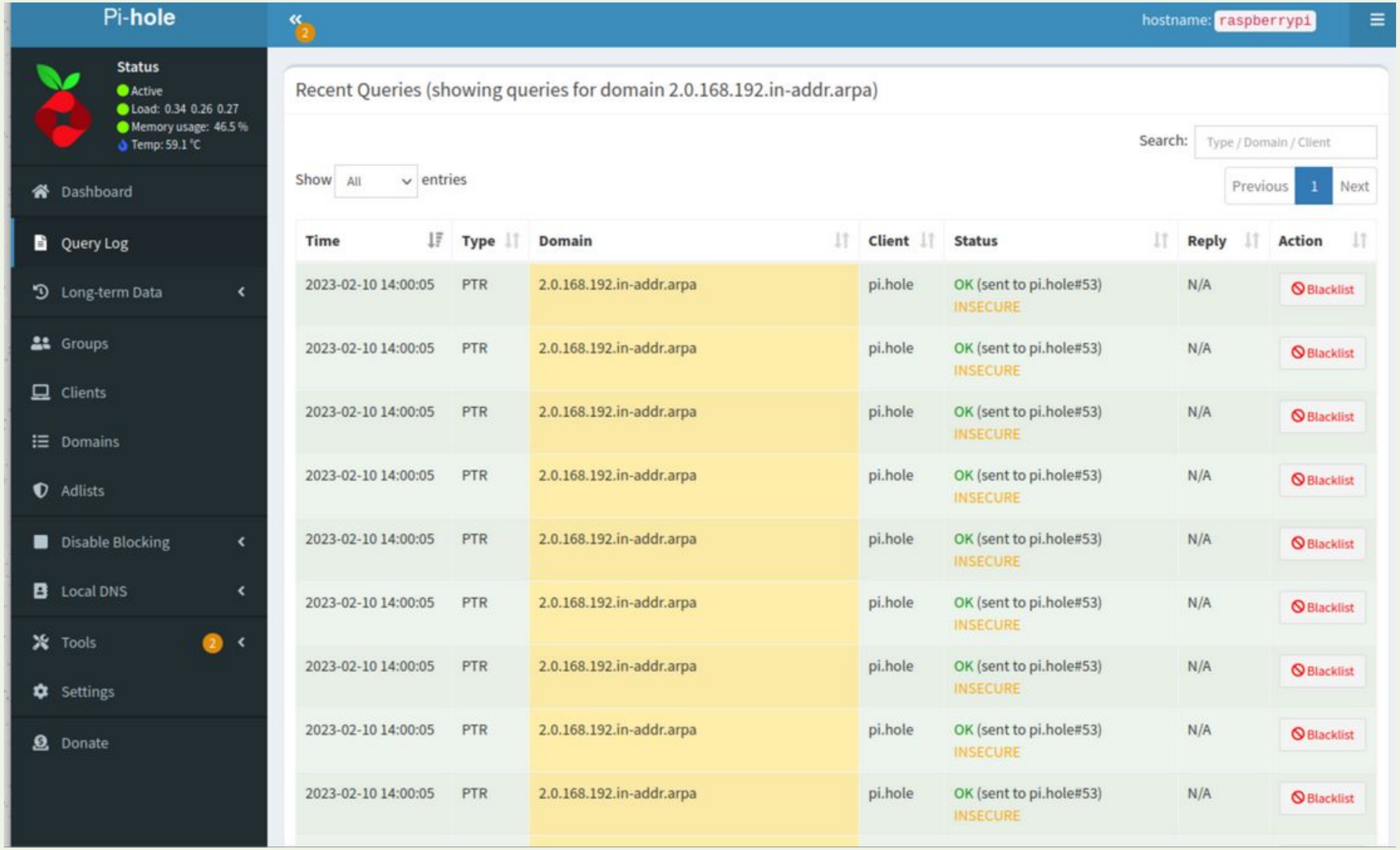
REMARQUE : pour les amateurs de géolocalisation, il existe également des enregistrements LOC permettant de fournir longitude et latitude précises d'un serveur.

Requêtes PTR - Résolutions Inverses



Pq ces requêtes ?

Requêtes PTR - Résolutions Inverses - in-addr.arpa



C'est quoi ces requêtes ?

Les types d’enregistrements DNS

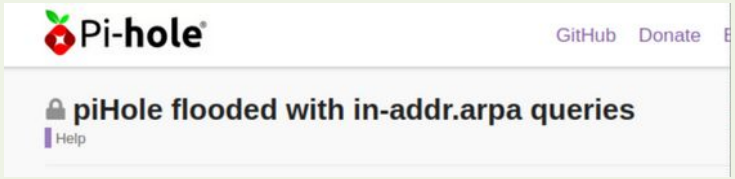
https://discourse.pi-hole.net/t/lot-of-ptr-queries/8380/3

DanSchaper Developer Apr '18

PTR queries are attempts to find the name associated with the IP address.

`85.0.168.192.in-addr.arpa from 127.0.0.1`

That means the localhost is trying to find out the name for 192.168.0.85. Are you running anything like Avahi/mDNS/Bonjour on any of the clients or on the Pi-hole?



Résolution inverse [modifier | modifier le code]

Pour trouver le nom de domaine associé à une adresse IP, on utilise un principe semblable. Dans un nom de domaine, la partie la plus générale est à droite : org dans fr.wikipedia.org, le mécanisme de résolution parcourt donc le nom de domaine de droite à gauche. Dans une adresse IP V4, c'est le contraire : 213 est la partie la plus générale de 213.228.0.42. Pour conserver une logique cohérente, on inverse l'ordre des quatre termes de l'adresse et on la concatène au pseudo domaine *in-addr.arpa*. Ainsi, par exemple, pour trouver le nom de domaine de l'adresse IP 91.198.174.2, on résout 2.174.198.91.in-addr.arpa.

La déclaration inverse est importante sur les adresses IP publiques Internet puisque l'absence d'une résolution inverse est considérée comme une erreur opérationnelle (RFC 1912[17]) qui peut entraîner le refus d'accès à un service. Par exemple, un serveur de messagerie électronique se présentant en envoi avec une adresse IP n'ayant pas de résolution inverse (PTR) a de grandes chances de se voir refuser, par l'hôte distant, la transmission du courrier (message de refus de type : *IP lookup failed*).

De plus, cette résolution inverse est importante dans le cadre de la réalisation de diagnostics réseaux car c'est elle qui permet de rendre les résultats de la commande traceroute humainement exploitables. Les dénominations des noms d'hôtes inverses sont souvent des composites de sous-domaines de localisation (ville, région, pays) et de domaines explicites indiquant le fournisseur d'accès Internet traversé comme francetelecom.net (- - - -.nctou202.Toulouse.francetelecom.net) et opentransit.net (- - - -.Aubervilliers.opentransit.net) pour France Télécom, ou encore proxad.net (- - - -.intf.routers.proxad.net) pour Free.

Une adresse IP peut être associée à différents noms de domaine via l'enregistrement de plusieurs entrées PTR dans le sous-domaine *.arpa* consacré à cette adresse (in-addr.arpa. pour IPv4 et ip6.arpa. pour IPv6). L'utilisation d'enregistrements PTR multiples pour une même adresse IP est éventuellement présente dans le cadre de l'hébergement virtuel de multiples domaines web derrière la même adresse IP mais n'est pas recommandée dans la mesure où le nombre des champs PTR à renvoyer peut faire dépasser à la réponse la taille des paquets UDP de réponse et entraîner l'utilisation du protocole TCP (plus coûteux en ressources) pour envoyer la réponse à la requête DNS[18].

Requêtes PTR - Résolutions Inverses

PTR record [modifier | modifier le code]

À l'inverse d'une entrée de type A ou AAAA, une entrée PTR indique à quel nom d'hôte correspond une adresse IPv4 ou IPv6. Si elle est spécifiée, elle doit contenir l'enregistrement inverse d'une entrée DNS A ou AAAA.

Par exemple (pour une adresse IPv4) cet enregistrement PTR est :

```
232.174.198.91.in-addr.arpa. IN PTR text.esams.wikimedia.org.
```

correspond à cette entrée A :

```
text.esams.wikimedia.org. IN A 91.198.174.232
```

Dans le cas d'une adresse IPv6, les entrées de type PTR sont enregistrées dans la zone ip6.arpa. (pendant de la zone in-addr.arpa. des adresses IPv4).

La règle permettant de retrouver l'entrée correspondant à une adresse IPv6 est similaire à celle pour les adresses IPv4 (renversement de l'adresse et recherche dans un sous-domaine dédié de la zone arpa.), mais diffère au niveau du nombre de bits de l'adresse utilisés pour rédiger le nom du domaine où rechercher le champ PTR : là où pour IPv4 le découpage de l'adresse se fait par octet, pour IPv6 c'est un découpage par quartet qui est utilisé.

Par exemple à l'adresse IPv6 :

```
2001:610:240:22::c100:68b
```

correspond le nom de domaine :

```
b.8.6.0.0.0.1.c.0.0.0.0.0.0.0.0.2.2.0.0.0.4.2.0.0.1.6.0.1.0.0.2.ip6.arpa. PTR   www.ipv6.ripe.net.
```

Là, j’avoue je n’ai pas tout compris …

Liste des meilleurs serveurs DNS en 2023 (Serveurs DNS rapides)

https://lecrabeinfo.net/les-meilleurs-serveurs-dns-rapides-et-gratuits.html#comment-changer-ses-serveurs-dns

DNS les plus rapides en 2023			
#	DNS	Adresses IPv4	Adresses IPv6
1	**Cloudflare 1.1.1.1**	1.1.1.1 1.0.0.1	2606:4700:4700::1111 2606:4700:4700::1001
2	Cisco OpenDNS Home	208.67.222.222 208.67.220.220	2620:119:35::35 2620:119:53::53
3	Neustar UltraDNS Public	64.6.64.6 64.6.65.6	2620:74:1b::1:1 2620:74:1c::2:2
4	NextDNS	45.90.28.0 45.90.30.0	2a07:a8c0:: 2a07:a8c1::
5	Google Public DNS	8.8.8.8 8.8.4.4	2001:4860:4860::8888 2001:4860:4860::8844
6	**Quad9**	9.9.9.9 149.112.112.112	2620:fe::fe 2620:fe::9
7	Comodo Secure DNS	8.26.56.26 8.20.247.20	–
8	Yandex.DNS	77.88.8.8 77.88.8.1	2a02:6b8::feed:0ff 2a02:6b8:0:1::feed:0ff
9	SafeDNS	195.46.39.39 195.46.39.40	2001:67c:2778::3939 2001:67c:2778::3940

Le DNS de **Cloudflare** (1.1.1.1) est celui à privilégier : il est rapide, sécurisé et respectueux de la vie privée.

Quad9 est également un excellent choix, il est respectueux de la vie privée et offre en plus une protection contre les menaces (exploits, logiciels malveillants, rançongiciels, logiciels espions et autres sites potentiellement dangereux).

Liste des meilleurs serveurs DNS en 2023 (Serveurs DNS sécurisés)

https://lecrabeinfo.net/les-meilleurs-serveurs-dns-rapides-et-gratuits.html#comment-changer-ses-serveurs-dns

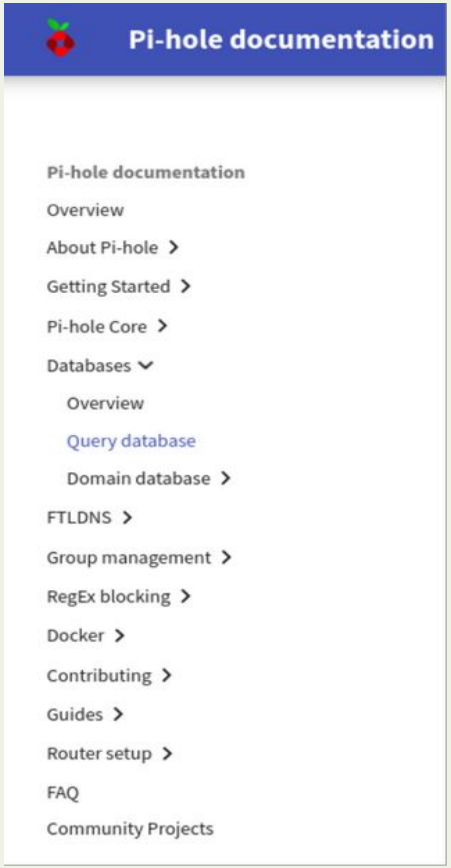
DNS les plus sécurisés en 2023		
DNS	**Adresses IPv4**	**Adresses IPv6**
CleanBrowsing Security Filter – Bloque les sites malveillants	185.228.168.9 185.228.169.9	2a0d:2a00:1::2 2a0d:2a00:2::2
CleanBrowsing Adult Filter – Bloque les sites malveillants – Bloque le contenu pour adultes	185.228.168.10 185.228.169.11	2a0d:2a00:1::1 2a0d:2a00:2::1
CleanBrowsing Family Filter – Bloque les sites malveillants – Bloque les sites pour adultes – Bloque les proxy et les VPN – Bloque les sites à contenu mixte (comme Reddit) – Google, Bing et Youtube sont configurés avec le filtre adulte activé	185.228.168.168 185.228.169.168	2a0d:2a00:1:: 2a0d:2a00:2::
Yandex Safe – Bloque les sites frauduleux	77.88.8.88 77.88.8.2	–
Yandex Family – Bloque les sites frauduleux – Bloque le contenu pour adultes	77.88.8.7 77.88.8.3	–
Neustar UltraDNS Threat Protection – Bloque les sites malveillants	156.154.70.2 156.154.71.2	2610:a1:1018::2 2610:a1:1019::2
Neustar UltraDNS Family Secure – Bloque les sites malveillants – Bloque les jeux d'argent, la pornographie, la violence et la haine/discrimination	156.154.70.3 156.154.71.3	2610:a1:1018::3 2610:a1:1019::3
Cisco OpenDNS Family Shield – Bloque le contenu pour adultes	208.67.222.123 208.67.220.123	–
Quad9 – Bloque les malwares, ransomwares et le phishing	9.9.9.9 149.112.112.112	2620:fe::fe 2620:fe::9
Comodo Secure Internet Gateway – Bloque les sites web malveillants	8.26.56.10 8.20.247.10	–

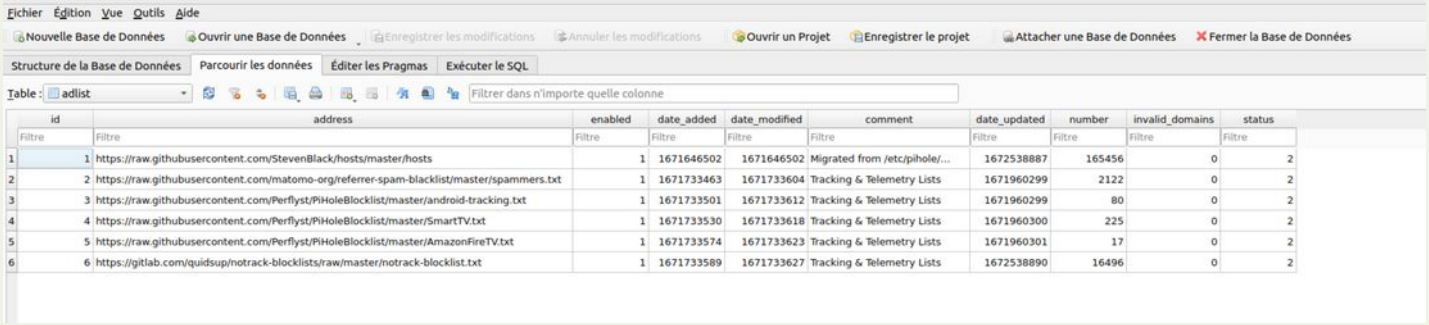
Choisissez le DNS qui offre la protection adaptée à vos besoins.

Les DNS de **CleanBrowsing** et **Quad9** sont à privilégier.

Mes prochaines étapes

https://docs.pi-hole.net/database/ftl/





	id	address	enabled	date_added	date_modified	comment	date_updated	number	invalid_domains	status
1	1	https://raw.githubusercontent.com/StevenBlack/hosts/master/hosts	1	1671646502	1671646502	Migrated from /etc/pihole/...	1672538887	165456	0	2
2	2	https://raw.githubusercontent.com/matomo-org/referrer-spam-blacklist/master/spammers.txt	1	1671733463	1671733604	Tracking & Telemetry Lists	1671960299	2122	0	2
3	3	https://raw.githubusercontent.com/Perflyst/PiHoleBlocklist/master/android-tracking.txt	1	1671733501	1671733612	Tracking & Telemetry Lists	1671960299	80	0	2
4	4	https://raw.githubusercontent.com/Perflyst/PiHoleBlocklist/master/SmartTV.txt	1	1671733530	1671733618	Tracking & Telemetry Lists	1671960300	225	0	2
5	5	https://raw.githubusercontent.com/Perflyst/PiHoleBlocklist/master/AmazonFireTV.txt	1	1671733574	1671733623	Tracking & Telemetry Lists	1671960301	17	0	2
6	6	https://gitlab.com/quidsup/notrack-blocklists/raw/master/notrack-blocklist.txt	1	1671733589	1671733627	Tracking & Telemetry Lists	1672538890	16496	0	2

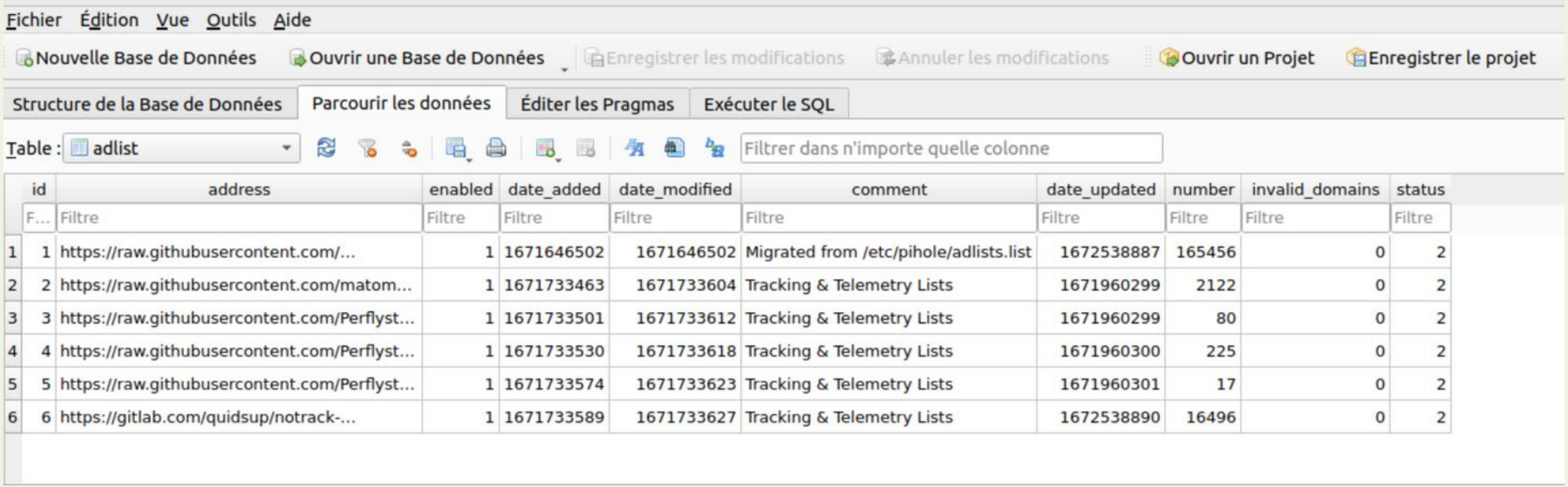
- Exploitation des bases de données
- Utilisation des expressions régulières pour simplifier la gestion des domaines, …

```
^ad([sxv]?[0-9]*|system)[_.-]([^.[:space:]]+\.){1,}|[_.-]ad([sxv]?[0-9]*|system)[_.-]
```

```
^analytics?[_.-]
```

Exploitation des bases de données de Pi-Hole

https://docs.pi-hole.net/database/ftl/



Fichier Édition Vue Outils Aide

Nouvelle Base de Données | Ouvrir une Base de Données | Enregistrer les modifications | Annuler les modifications | Ouvrir un Projet | Enregistrer le projet

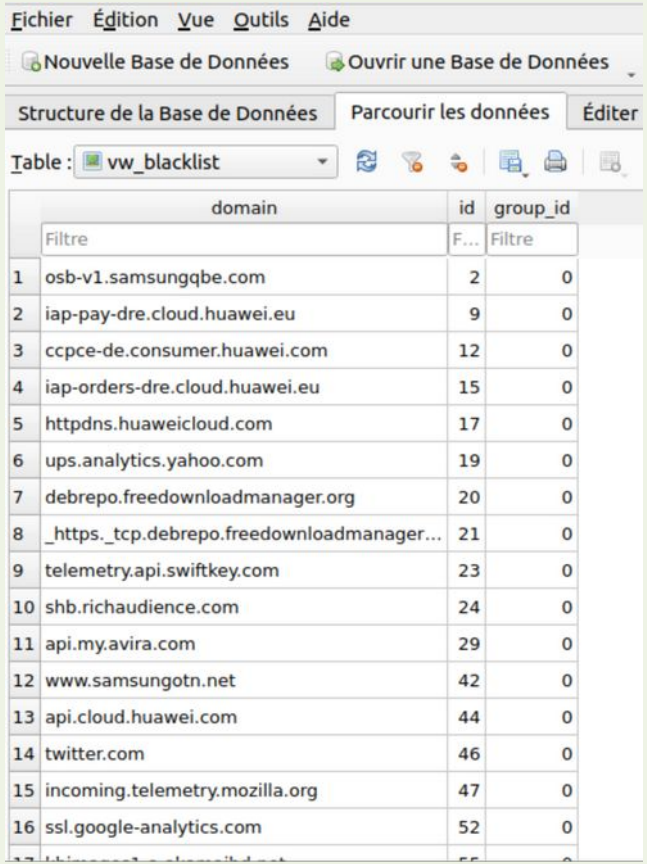
Structure de la Base de Données | Parcourir les données | Éditer les Pragmas | Exécuter le SQL

Table : adlist — Filtrer dans n'importe quelle colonne

	id	address	enabled	date_added	date_modified	comment	date_updated	number	invalid_domains	status
1	1	https://raw.githubusercontent.com/...	1	1671646502	1671646502	Migrated from /etc/pihole/adlists.list	1672538887	165456	0	2
2	2	https://raw.githubusercontent.com/matom...	1	1671733463	1671733604	Tracking & Telemetry Lists	1671960299	2122	0	2
3	3	https://raw.githubusercontent.com/Perflyst...	1	1671733501	1671733612	Tracking & Telemetry Lists	1671960299	80	0	2
4	4	https://raw.githubusercontent.com/Perflyst...	1	1671733530	1671733618	Tracking & Telemetry Lists	1671960300	225	0	2
5	5	https://raw.githubusercontent.com/Perflyst...	1	1671733574	1671733623	Tracking & Telemetry Lists	1671960301	17	0	2
6	6	https://gitlab.com/quidsup/notrack-...	1	1671733589	1671733627	Tracking & Telemetry Lists	1672538890	16496	0	2

Exploitation des bases de données de Pi-Hole

https://docs.pi-hole.net/database/ftl/



	domain	id	group_id
	Filtre	F...	Filtre
1	osb-v1.samsungqbe.com	2	0
2	iap-pay-dre.cloud.huawei.eu	9	0
3	ccpce-de.consumer.huawei.com	12	0
4	iap-orders-dre.cloud.huawei.eu	15	0
5	httpdns.huaweicloud.com	17	0
6	ups.analytics.yahoo.com	19	0
7	debrepo.freedownloadmanager.org	20	0
8	_https._tcp.debrepo.freedownloadmanager...	21	0
9	telemetry.api.swiftkey.com	23	0
10	shb.richaudience.com	24	0
11	api.my.avira.com	29	0
12	www.samsungotn.net	42	0
13	api.cloud.huawei.com	44	0
14	twitter.com	46	0
15	incoming.telemetry.mozilla.org	47	0
16	ssl.google-analytics.com	52	0

Les expressions régulières (RegEx)

```
^ad([sxv]?[0-9]*|system)[_.-]([^.[:space:]]+\.){1,}|[_.-]ad([sxv]?[0-9]*|system)[_.-]
```

```
^analytics?[_.-]
```

How to Use Regular Expressions (regexes) on Linux

By Dave McKay · How-To Geek · 14 min

March 25, 2020

View Original

linux regex

Fatmawati Achmad Zaenuri/Shutterstock

Tutoriel pour maîtriser les expressions régulières (regex)

lucaswillems.com · 10 min

View Original

linux regex

Les expressions régulières, ou plus communément regex (contraction de *regular expression*) permettent de représenter des modèles de chaînes de caractère. Ce sont des outils très puissants et très utilisés : on peut les retrouver dans de nombreux langages comme le PHP, MySQL, Javascript... ou encore dans des logiciels d'édition de code ! Cependant, si cet outil est très puissant, il est relativement difficile à appréhender au début car les expressions régulières peuvent prendre des formes de ce genre :

```
#^[a-zA-Z-]+@[a-zA-Z-]+\.[a-zA-Z]{2,6}$#
```

Et pourquoi pas … pour prochain atelier


LoLiGrUB


LoLiGrUB

Et vous comment faites vous ?