Fiche Pratique N°20c : Installer et configurer AdGuard Home sur un sous-domaine local avec YunoHost V1.1

7 nov, 2026 · @Gabriel

Objectif : *Installer le serveur DNS filtrant AdGuard Home sur votre serveur YunoHost, administrer son interface en HTTPS depuis votre réseau local et depuis l'extérieur via le tunnel WireGuard, pour filtrer publicités et traqueurs sur tous vos appareils.*

- ***Public visé :*** *Intermédiaire (quelques bases en ligne de commande sont utiles)*
- ***Temps estimé :*** *30 à 45 minutes*
- ***Difficulté :*** *★★★☆☆ (Moyen)*
- ***Prérequis :*** *un serveur YunoHost 12 à jour avec une IP locale fixe, un accès SSH administrateur, le tunnel WireGuard de la fiche N°20a pour l'accès distant*
- ***Fiches associées :*** *N°20 (YunoHost), N°20a (WireGuard), N°20b (SearXNG)*

1. Pourquoi installer AdGuard Home ?

Une fois le tunnel WireGuard opérationnel (fiche N°20a) et SearXNG installé (fiche N°20b), vous pouvez ajouter un filtrage DNS pour tout votre réseau. **AdGuard Home** est un serveur DNS qui bloque publicités, traqueurs et sites malveillants avant même qu'ils ne soient contactés.

Les bénéfices concrets :

- **Blocage à la source :** tous les appareils qui l'utilisent comme DNS (ordinateurs, smartphones, TV, tablettes) sont filtrés, sans rien installer dessus.
- **Navigation plus légère :** les publicités et traqueurs bloqués ne sont pas téléchargés.
- **Protection de la vie privée :** les domaines de pistage (Google Analytics, pixel Meta…) ne sont plus résolus.
- **Contrôle parental :** blocage de catégories de sites et recherche sécurisée.
- **Réécritures DNS :** vos sous-domaines privés (search, adguard…) pointent vers votre serveur, à la maison comme dans le tunnel.

Cas d'usage typiques :

- Vous voulez protéger tous les appareils du foyer sans configurer chaque navigateur.
- Vous voulez un filtrage centralisé pour toute la famille.
- Vous voulez que vos appareils en déplacement profitent du même filtrage via WireGuard.

⚠️ **Règle de sécurité :** l'interface d'administration d'AdGuard Home et son port DNS 53 ne doivent **jamais** être exposés sur Internet. Utilisez-les uniquement en local et via le VPN.

2. Prérequis

- Un serveur YunoHost 12 avec une IP locale fixe (exemple : 192.168.1.200).
- Un sous-domaine dédié (exemple : adguard.votre-domaine.org).
- Un ordinateur client (exemple : Linux Mint) sur le même réseau local.
- **Pour l'accès depuis Internet :**
    - un serveur WireGuard configuré (fiche N°20a) ;
    - un client WireGuard sur votre appareil distant ;

gabriel.ananda@mailo.com
CC BY SA

Fiche Pratique N°20c : Installer et configurer AdGuard Home sur un sous-domaine local avec YunoHost V1.1

- une box avec IPv4 full-stack (fiche N°20, section 5).

3. Ajouter le sous-domaine dans YunoHost

Ajoutez d'abord le sous-domaine, en SSH sur le serveur :

```
sudo yunohost domain add adguard.votre-domaine.org
```

YunoHost crée automatiquement un **certificat auto-signé** pour ce domaine, suffisant pour un usage local et via le VPN.

4. Installer AdGuard Home

4.1. Les réglages de l'application

L'application AdGuard Home du catalogue YunoHost demande, à l'installation :

Réglage	Rôle	Valeur conseillée
`domain`	Domaine de l'interface web	adguard.votre-domaine.org
`path`	Chemin de l'interface (par défaut `/adguard`)	`/`
`init_main_permission`	Qui peut ouvrir l'interface (par défaut tous les utilisateurs)	`admins`
`admin`	Utilisateur YunoHost administrateur d'AdGuard Home	votre identifiant
`password`	Mot de passe de l'interface AdGuard Home, **choisi par vous**	un mot de passe fort
`expose_port_53`	Ouvre le port DNS 53 dans le pare-feu de YunoHost (désactivé par défaut)	voir ci-dessous
`dns_over_https`	Active le DNS chiffré (DoH)	selon vos besoins

À propos du port 53 : l'application avertit qu'un port 53 ouvert sur Internet peut servir à des attaques par amplification DNS.

- Sur un **VPS**, laissez `expose_port_53=false`.
- À la **maison**, derrière une box, vos appareils locaux doivent pouvoir joindre le port 53 du serveur. Ne redirigez **jamais** le port 53 sur votre box.

4.2. Lancer l'installation

Le plus simple est la webadmin : **Applications** › **Installer** › AdGuard Home, puis remplissez le formulaire. En ligne de commande :

```
sudo yunohost app install adguardhome -a "domain=adguard.votre-
domaine.org&path=/&init_main_permission=admins&admin=votre_identifiant&pass
word=VotreMotDePasseFort&expose_port_53=true&dns_over_https=false"
```


gabriel.ananda@mailo.com
CC BY SA

Fiche Pratique N°20c : Installer et configurer AdGuard Home sur un sous-domaine local avec YunoHost V1.1

Lors de l'installation, l'application ajuste la configuration de dnsmasq (le DNS interne de YunoHost) pour qu'AdGuard Home puisse écouter sur le port 53 des adresses réseau du serveur.

4.3. Vérifications

```
# L'application est installée
sudo yunohost app list | grep -i adguard

# Informations (version, domaine, dossier d'installation)
sudo yunohost app info adguardhome

# Le serveur DNS répond et filtre (doit renvoyer 0.0.0.0 ou aucune adresse)
dig @192.168.1.200 doubleclick.net +short
```

Vous devez voir :

- AdGuard Home dans la liste des applications ;
- une réponse 0.0.0.0 (ou vide) pour un domaine publicitaire.

⚠️ **Ne modifiez pas à la main les fichiers Nginx générés par YunoHost** dans `/etc/nginx/conf.d/` : ils sont régénérés lors des mises à jour. Les accès se règlent dans **Groupes et permissions**.

5. Configurer le fichier hosts sur le client local

5.1. Ouvrir le fichier hosts

```
sudo nano /etc/hosts
```

5.2. Ajouter la ligne

```
192.168.1.200 adguard.votre-domaine.org
```

5.3. Vérifier la résolution

```
ping -c 3 adguard.votre-domaine.org
# Doit répondre avec l'IP locale du serveur
```

Une fois AdGuard Home utilisé comme DNS (section 7), une réécriture DNS remplace avantageusement le fichier hosts.

6. Ouvrir l'interface d'administration

1. Ouvrez https://adguard.votre-domaine.org dans le navigateur du client.
2. Acceptez l'avertissement de sécurité (certificat auto-signé).
3. Identifiez-vous sur le portail YunoHost si demandé, puis dans AdGuard Home avec l'identifiant et le mot de passe choisis à l'installation.

Vous devez voir :

- le tableau de bord d'AdGuard Home (requêtes DNS, requêtes bloquées).

gabriel.ananda@mailo.com
CC BY SA

Fiche Pratique N°20c : Installer et configurer AdGuard Home sur un sous-domaine local avec YunoHost V1.1

Mot de passe oublié ? AdGuard Home stocke un hachage bcrypt du mot de passe dans son fichier `AdGuardHome.yaml` (dans le dossier d'installation indiqué par `yunohost app info adguardhome`). La documentation d'AdGuard Home explique comment le remplacer : générez un nouveau hachage avec `htpasswd -B -C 10 -n -b identifiant MotDePasse`, collez-le dans le fichier, puis redémarrez le service.

7. Utiliser AdGuard Home comme DNS

7.1. Sur le réseau local

- **Pour tout le foyer :** dans votre box, réglez le serveur DNS distribué par le DHCP sur 192.168.1.200 (si votre box le permet).
- **Appareil par appareil :** dans les paramètres réseau, indiquez 192.168.1.200 comme serveur DNS.

7.2. Choisir les serveurs DNS en amont

Dans **Paramètres** › **Paramètres DNS** › **Serveurs DNS upstream**, choisissez des résolveurs respectueux de la vie privée, par exemple Quad9 en DNS chiffré :

```
https://dns.quad9.net/dns-query
tls://dns.quad9.net
```

Cliquez sur **Tester les upstreams**, puis **Appliquer**.

Rappel : Mullvad a fermé son service DNS public le 2 novembre 2026. Si vous l'utilisiez en amont, remplacez-le (par exemple par Quad9).

7.3. Activer des listes de blocage

Dans **Filtres** › **Listes de blocage DNS**, gardez la liste par défaut (AdGuard DNS filter) et ajoutez au besoin une liste française.

8. Accéder à AdGuard Home via WireGuard

8.1. Prérequis pour l'accès distant

- Un serveur WireGuard configuré sur votre serveur (fiche N°20a).
- Le port UDP de WireGuard (51820 par défaut) redirigé sur votre box vers le serveur, ce qui nécessite une IPv4 full-stack.
- Un client WireGuard configuré sur votre appareil distant.

8.2. Connexion via le VPN

1. Activez le tunnel WireGuard sur votre appareil distant (fiche N°20a).
2. Vérifiez la connectivité (adapter les adresses à votre tunnel) :

```
ping -c 3 10.10.10.1
ping -c 3 192.168.1.200
```

8.3. Filtrer aussi en déplacement

Dans la configuration du client WireGuard, indiquez l'IP du serveur dans le tunnel comme DNS :

gabriel.ananda@mailo.com
CC BY SA

```
[Interface]
DNS = 10.10.10.1
```

Vos appareils distants profitent alors du filtrage d'AdGuard Home.

8.4. Réécritures DNS pour vos services

Dans AdGuard Home, ouvrez **Filtres** › **Réécritures DNS** et ajoutez :

- **Domaine :** search.votre-domaine.org › **Réponse :** 10.10.10.1
- **Domaine :** adguard.votre-domaine.org › **Réponse :** 10.10.10.1

Tous les appareils qui utilisent AdGuard Home résolvent alors ces noms vers votre serveur. Utilisez toujours les noms de domaine (https://adguard.votre-domaine.org) : YunoHost choisit l'application selon le nom demandé.

Si vos appareils locaux (hors VPN) utilisent aussi AdGuard Home, choisissez une réponse joignable des deux côtés (l'IP locale 192.168.1.200 si le tunnel donne accès au réseau local).

9. Dépannage

Problème	Cause probable	Solution
Redirection vers le portail `/yunohost/sso`	Vous n'êtes pas connecté au portail, ou pas dans le groupe autorisé	Connectez-vous au portail YunoHost ; vérifiez **Groupes et permissions**
Le navigateur affiche le portail ou une autre application	Accès par adresse IP au lieu du nom de domaine	Utilisez https://adguard.votre-domaine.org et vérifiez la résolution
Les appareils locaux ne sont pas filtrés	Ils n'utilisent pas AdGuard Home comme DNS, ou le port 53 n'est pas joignable	Vérifiez le DNS de l'appareil ; testez `dig @192.168.1.200 example.com` ; vérifiez le réglage `expose_port_53`
Le navigateur contourne le filtrage	« DNS sécurisé » (DoH) activé dans le navigateur	Désactivez-le, ou pointez-le vers votre propre AdGuard Home
Service arrêté	Erreur au démarrage	Webadmin › **Outils** › **Services** › adguardhome ; consultez les journaux

gabriel.ananda@mailo.com
CC BY SA

Fiche Pratique N°20c : Installer et configurer AdGuard Home sur un sous-domaine local avec YunoHost V1.1

10. Vérification finale

```
# L'application est installée
sudo yunohost app list | grep -i adguard

# Le DNS filtre
dig @192.168.1.200 doubleclick.net +short

# L'interface répond
curl -k -I https://adguard.votre-domaine.org
```

Vous devez voir :

- AdGuard Home dans la liste, une réponse bloquée pour le domaine publicitaire, et une réponse HTTP (200 ou redirection vers la page de connexion).

C'est terminé ! AdGuard Home filtre votre réseau local et vos appareils connectés via WireGuard, et vous l'administrez en HTTPS sans jamais l'exposer sur Internet.

Références

- Catalogue YunoHost – AdGuard Home
- Paquet adguardhome_ynh (manifeste : admin, password, expose_port_53, dns_over_https)
- AdGuard Home – Wiki officiel
- AdGuard Home – FAQ (réinitialiser le mot de passe)
- YunoHost – Documentation (domaines, groupes et permissions, regen-conf)
- Quad9 – Résolveur DNS
- Mullvad – Fermeture du DNS public, parrainage de Quad9

gabriel.ananda@mailo.com
CC BY SA