

Fiche Pratique N°20c : Installer et configurer AdGuard Home sur un sous-domaine local avec Yunohost V1.0

Objectif : Installer le serveur DNS de blocage AdGuard Home sur votre serveur Yunohost, le rendre accessible en HTTPS sur votre réseau local, et depuis l'extérieur via le tunnel sécurisé 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

Niveau de difficulté : ★★☆☆☆ (Moyen)

1. Pourquoi installer AdGuard Home ?

Maintenant que le tunnel WireGuard est opérationnel (Fiche N°20a) et que SearXNG est accessible (Fiche N°20b), vous pouvez ajouter une couche de filtrage DNS pour toute votre infrastructure. **AdGuard Home** est un serveur DNS de blocage qui filtre les publicités, les traqueurs et les sites malveillants au niveau du réseau.

Les bénéfices concrets :

- **Blocage à la source** : Tous les appareils de votre réseau (ordinateurs, smartphones, TV, tablettes) bénéficient du filtrage, sans rien installer.
- **Performance accrue** : Les publicités et traqueurs sont bloqués avant d'être chargés, ce qui réduit le temps de chargement des pages.
- **Protection de la vie privée** : En bloquant les traqueurs (Google Analytics, Facebook Pixel, etc.), vous empêchez les régies publicitaires de vous suivre.
- **Contrôle parental** : Vous pouvez bloquer des catégories entières de contenus (adultes, jeux d'argent, réseaux sociaux).

Fiche Pratique N°20c : Installer et configurer AdGuard Home sur un sous-domaine local avec YunoHost V1.0

- **Accès distant** : Grâce à WireGuard, vous pouvez administrer AdGuard Home depuis l'extérieur.
- **Gestion DNS centralisée** : Vous pouvez créer des réécritures DNS pour simplifier l'accès à vos services via le VPN.

Cas d'usage typique :

- Vous voulez protéger tous les appareils de votre foyer sans configurer chaque navigateur.
 - Vous êtes une famille nombreuse et vous souhaitez un filtrage centralisé.
 - Vous cherchez à améliorer la vitesse de navigation en bloquant les contenus superflus.
 - Vous voulez administrer votre serveur DNS à distance depuis l'extérieur, en toute sécurité.
-

2. Prérequis

- Un serveur avec YunoHost installé et une IP fixe (ex: 192.168.1.200).
 - Un sous-domaine dédié pour AdGuard Home (ex: adguard.votre-domaine.org).
 - Un client (ex: Linux Mint) sur le même réseau local pour la configuration.
 - **Pour un accès depuis Internet :**
 - Avoir configuré un serveur WireGuard sur votre serveur local (Fiche N°20a).
 - Avoir un client WireGuard sur votre appareil distant.
 - **Votre box Internet doit avoir une IPv4 Full Stack** (voir Fiche N°20, section 4.5).
-

3. Installation d'AdGuard Home via YunoHost

3.1. Installer l'application

bash

Fiche Pratique N°20c : Installer et configurer AdGuard Home sur un sous-domaine local avec Yunohost V1.0

```
sudo yunohost app install adguardhome -a "domain=adguard.votre-domaine.org&path=/&is_public=Yes"
```

3.2. Vérifications

```
bash
```

```
# Vérifier que l'application est installée
```

```
yunohost app list | grep adguardhome
```

```
# Vérifier que le service tourne
```

```
sudo systemctl status adguardhome
```

```
# Vérifier le port d'écoute (3000 pour l'interface web)
```

```
sudo ss -tulpn | grep adguardhome
```

4. Certificat SSL auto-signé

```
bash
```

```
sudo yunohost domain cert install adguard.votre-domaine.org --self-signed --force
```

Vérifier la présence du certificat :

```
bash
```

```
ls -la /etc/yunohost/certs/adguard.votre-domaine.org/
```

5. Configuration du fichier hosts sur le client local

5.1. Ouvrir le fichier hosts

```
bash
```

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

5.2. Ajouter la ligne

Fiche Pratique N°20c : Installer et configurer AdGuard Home sur un sous-domaine local avec YunoHost V1.0

text

192.168.1.200 adguard.votre-domaine.org

5.3. Vérifier la résolution

bash

`ping` adguard.votre-domaine.org

Doit répondre avec l'IP locale du serveur

6. Configuration de Nginx

6.1. Vérifier le port d'écoute d'AdGuard Home

bash

`sudo ss -tulpn | grep` adguardhome

AdGuard Home écoute normalement sur le port **3000** pour l'interface web.

6.2. Créer la configuration Nginx

bash

`sudo nano` /etc/nginx/conf.d/adguard.votre-domaine.org.conf

6.3. Copier le contenu suivant

nginx

```
server {  
    listen 443 ssl http2;  
    listen [::]:443 ssl http2;  
    server_name adguard.votre-domaine.org;  
  
    ssl_certificate /etc/yunohost/certs/adguard.votre-domaine.org/crt.pem;  
    ssl_certificate_key /etc/yunohost/certs/adguard.votre-domaine.org/key.pem;
```

Fiche Pratique N°20c : Installer et configurer AdGuard Home sur un sous-domaine local avec YunoHost V1.0

```
include /etc/nginx/conf.d/security.conf.inc;

location / {
    proxy_pass http://127.0.0.1:3000;
    proxy_set_header Host $host;
    proxy_set_header X-Real-IP $remote_addr;
    proxy_set_header X-Forwarded-For $proxy_add_x_forwarded_for;
    proxy_set_header X-Forwarded-Proto $scheme;
}

access_log /var/log/nginx/adguard.votre-domaine.org-access.log;
error_log /var/log/nginx/adguard.votre-domaine.org-error.log;
}

server {
    listen 80;
    listen [::]:80;
    server_name adguard.votre-domaine.org;
    return 301 https://$server_name$request_uri;
}
```

6.4. Supprimer les fichiers du répertoire `.d` (pour éviter les conflits)

```
bash

sudo rm -f /etc/nginx/conf.d/adguard.votre-domaine.org.d/*.conf
```

6.5. Tester et recharger Nginx

```
bash

sudo nginx -t
sudo systemctl reload nginx
```

Fiche Pratique N°20c : Installer et configurer AdGuard Home sur un sous-domaine local avec YunoHost V1.0

7. Vérification du fonctionnement

7.1. Test avec curl (depuis le serveur)

```
bash

# Test direct du port 3000
curl -v http://127.0.0.1:3000
# Doit renvoyer une redirection vers /login.html

# Test via le domaine
curl -k https://adguard.votre-domaine.org
# Doit renvoyer <a href="/login.html">Found</a>.
```

7.2. Test depuis le navigateur (client local)

Ouvrez un navigateur et allez sur <https://adguard.votre-domaine.org>.

- Acceptez l'avertissement de sécurité (certificat auto-signé).
-

8. Récupérer le mot de passe administrateur

YunoHost génère un mot de passe aléatoire lors de l'installation. Pour le récupérer :

```
bash

sudo yunohost app setting adguardhome admin_password
```

Exemple de sortie : [J8kLm9pQr2sTuvWxYz](#)

Pour changer le mot de passe :

```
bash

sudo yunohost app setting adguardhome admin_password --new
```

Fiche Pratique N°20c : Installer et configurer AdGuard Home sur un sous-domaine local avec YunoHost V1.0

9. Accès à AdGuard Home depuis Internet via WireGuard

9.1. Prérequis pour l'accès distant

Pour qu'AdGuard Home soit accessible depuis l'extérieur de manière sécurisée, vous devez :

- Avoir configuré un serveur WireGuard sur votre serveur local (Fiche N°20a).
- Avoir redirigé le port UDP 51820 de votre box vers votre serveur local (192.168.1.200). Cette étape nécessite une IPv4 Full Stack.
- Avoir configuré un client WireGuard sur votre appareil distant.

9.2. Connexion via le VPN

1.Établissez le tunnel WireGuard sur votre appareil distant (Fiche N°20a).

2.Vérifiez la connectivité :

```
bash
```

```
ping 10.10.10.1
```

```
ping 192.168.1.200
```

9.3. Accéder à l'interface d'AdGuard Home

Une fois le VPN actif, ouvrez votre navigateur et utilisez l'une de ces adresses :

- <https://adguard.votre-domaine.org> (via le fichier `hosts` configuré sur votre client distant).
- <http://192.168.1.200:3000> (adresse IP locale du serveur et port de l'interface web).
- <http://10.10.10.1:3000> (adresse IP du serveur sur le réseau VPN).

Note : L'interface d'AdGuard Home utilise le port 3000. L'accès via le sous-domaine HTTPS n'est possible que si la résolution DNS est configurée.

9.4. Configuration DNS pour un accès simplifié

- Depuis l'interface d'AdGuard Home (accessible localement), allez dans "**Paramètres**" → "**Réécritures DNS**".

Fiche Pratique N°20c : Installer et configurer AdGuard Home sur un sous-domaine local avec YunoHost V1.0

•Ajoutez des règles pour vos services :

•**Domaine** : search.votre-domaine.org → **Réponse** : 10.10.10.1

•**Domaine** : adguard.votre-domaine.org → **Réponse** : 10.10.10.1

•Tous les appareils utilisant AdGuard Home comme DNS pourront résoudre ces domaines.

10. Dépannage

Problème : Accès impossible à AdGuard Home.

Solution : Vérifiez que la configuration Nginx contient bien proxy_pass
http://127.0.0.1:3000; :

```
bash
```

```
sudo grep -r "proxy_pass" /etc/nginx/conf.d/adguard.votre-domaine.org.conf
```

Problème : Redirection vers le SSO de YunoHost.

Solution : Supprimez ou commentez les inclusions SSO :

```
bash
```

```
sudo grep -r "yunohost_sso" /etc/nginx/conf.d/adguard.votre-domaine.org.conf
```

11. Arborescence des fichiers importants

```
text
```

```
/etc/
```

```
|— nginx/
```

```
|   └─ conf.d/
```

```
|       └─ adguard.votre-domaine.org.conf # Configuration principale
```

Fiche Pratique N°20c : Installer et configurer AdGuard Home sur un sous-domaine local avec Yunohost V1.0

```
|— hosts                # Résolution locale du domaine
|— yunohost/
|   |— certs/
|       |— adguard.votre-domaine.org/    # Certificat auto-signé

/var/log/nginx/
|— adguard.votre-domaine.org-*.log      # Logs Nginx

/var/www/adguardhome/
|— AdGuardHome                # Binaire principal
|— AdGuardHome.yaml           # Configuration d'AdGuard Home
```

12. Vérification finale

```
bash

# Vérifier que les services tournent
sudo systemctl status adguardhome
sudo systemctl status nginx

# Vérifier le port d'écoute
sudo ss -tulpn | grep adguardhome # Doit afficher le port 3000

# Vérifier la résolution
ping adguard.votre-domaine.org    # Doit répondre avec l'IP locale

# Vérifier l'accès web
curl -k https://adguard.votre-domaine.org # Doit renvoyer /login.html
```

C'est terminé ! AdGuard Home est installé et accessible en HTTPS sur votre réseau local, et depuis Internet via le tunnel WireGuard sécurisé. Vous pouvez désormais utiliser AdGuard Home comme serveur DNS pour simplifier l'accès à tous vos services locaux.