



CHECKLIST DE CHOIX ET DE DÉPLOIEMENT

Votre DNS local anti-publicité : la checklist pour choisir sans vous compliquer le réseau

Utilisez cette fiche pour sélectionner une solution libre adaptée à votre foyer et préparer une installation fiable. L'objectif n'est pas de bloquer le plus possible, mais de filtrer efficacement tout en gardant un réseau facile à dépanner.

Au sommaire

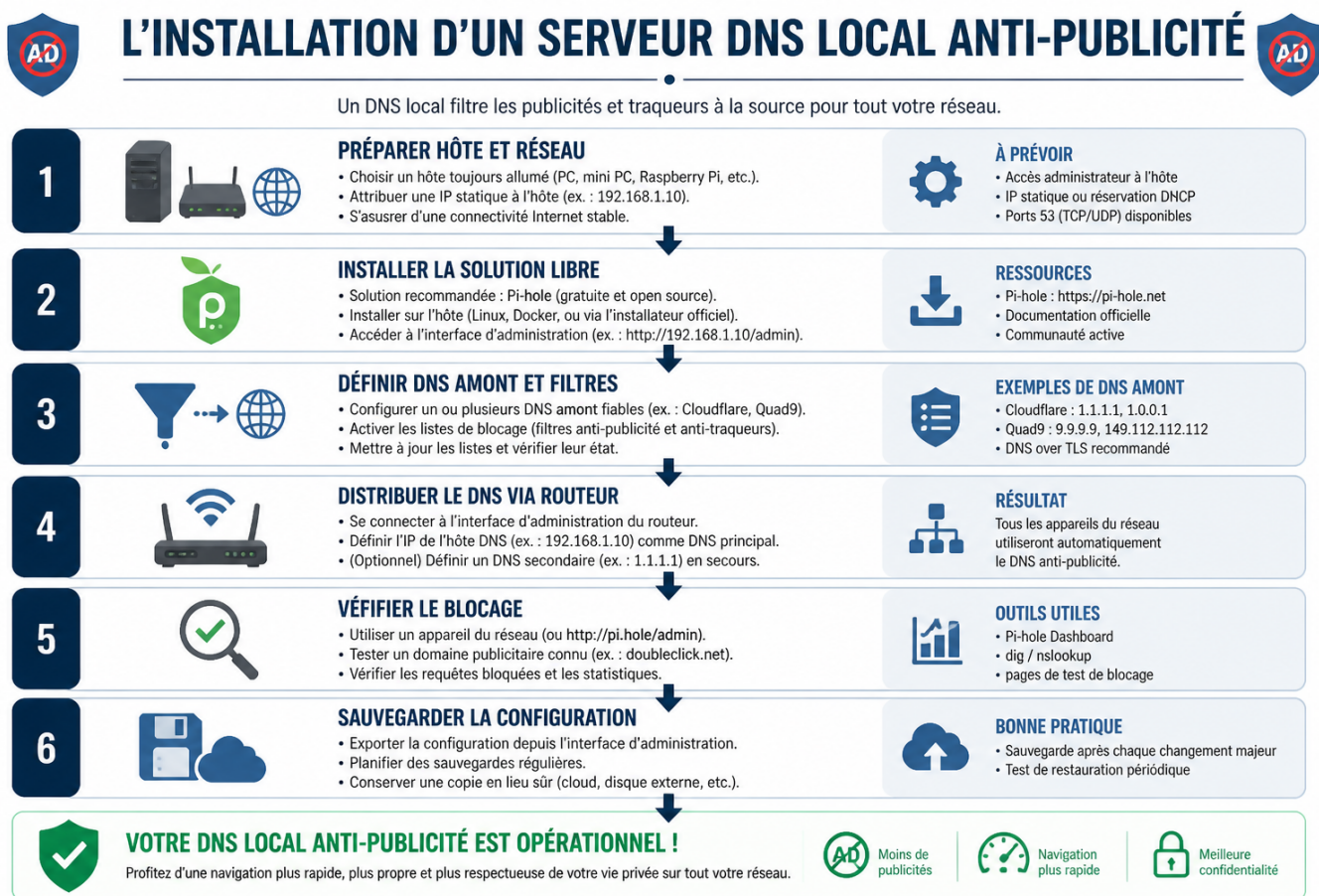
- 1 Le bon repère avant de choisir
- 2 1. Évaluer votre réseau et votre matériel
- 3 2. Comparer les approches avant de vous décider
- 4 3. Valider les fonctions essentielles
- 5 4. Démarrer le filtrage sans provoquer de faux positifs

Le bon repère avant de choisir

Un DNS local filtre les domaines publicitaires et de suivi avant leur chargement, pour les appareils configurés sur le même réseau.

Il complète utilement une extension de navigateur, mais ne peut pas identifier toutes les publicités, notamment lorsqu'elles utilisent le même domaine que le contenu légitime.

Une solution stable, documentée et réversible vaut mieux qu'un filtrage agressif difficile à diagnostiquer.



INFOGRAPHIE Étapes pour installer un serveur DNS local libre anti-publicité sur un réseau domestique.

1. Évaluer votre réseau et votre matériel

Lister les appareils à couvrir

Ordinateurs, mobiles, téléviseurs connectés, consoles et objets connectés peuvent bénéficier du filtrage réseau.

- Choisir une machine qui restera allumée**
Le DNS doit être disponible lorsque les appareils cherchent à accéder à des services par nom de domaine.
- Prévoir une adresse IP locale stable**
Une réservation DHCP dans le routeur aide à éviter les conflits et centralise la gestion.
- Vérifier que le routeur ou le DHCP peut distribuer le DNS local**
C'est ce qui permet de couvrir le réseau sans installer une extension sur chaque appareil.

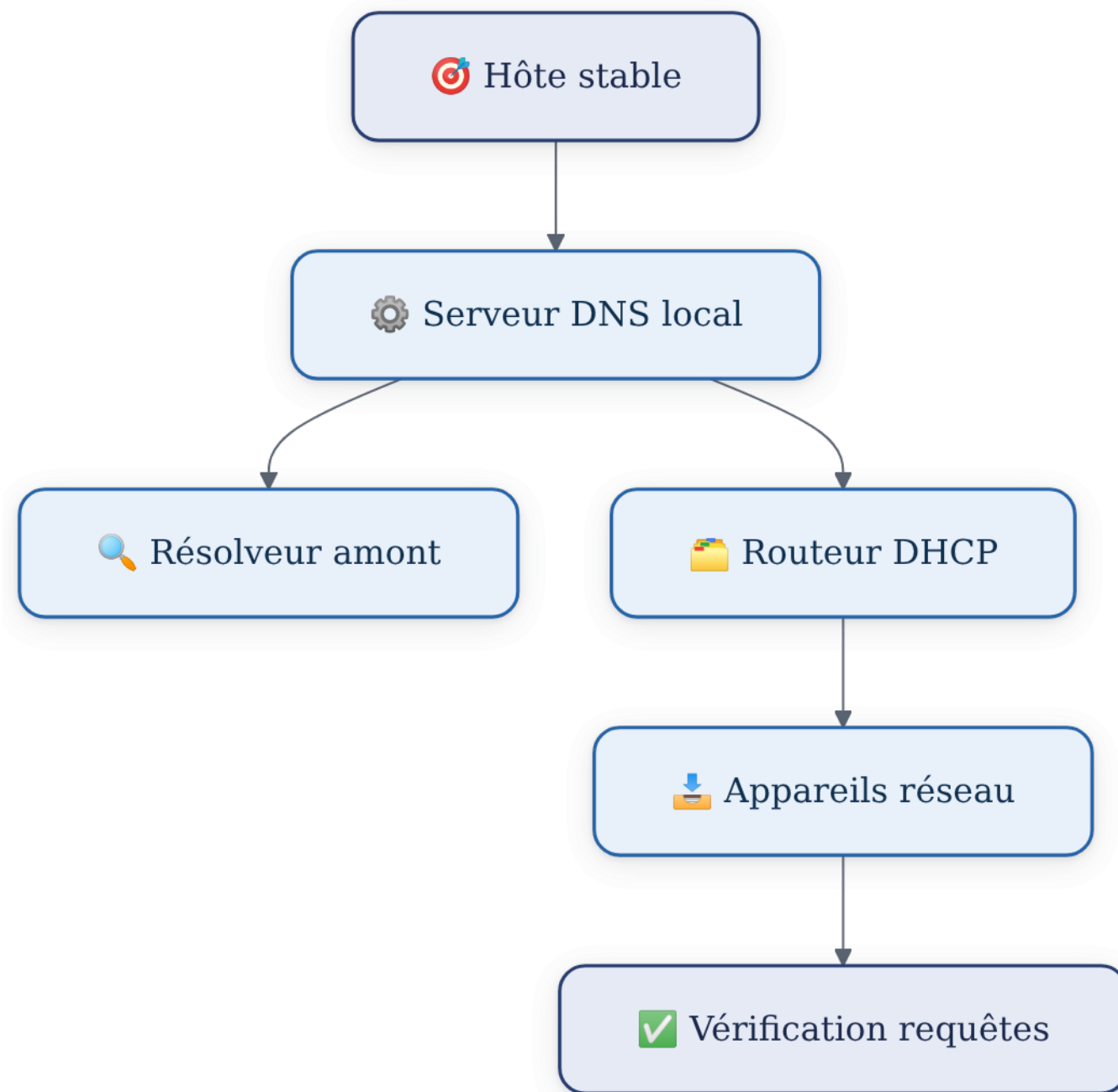


SCHÉMA Vue d'ensemble des étapes d'installation d'un DNS local anti-publicité sur un réseau domestique.

2. Comparer les approches avant de vous décider

Solution	À privilégier si...	Point de vigilance
Pi-hole	Vous recherchez une première installation orientée filtrage réseau direct.	Évaluez l'ergonomie de l'administration et votre capacité à dépanner les blocages.
AdGuard Home	Vous souhaitez réunir filtrage et fonctions de résolution dans une interface accessible.	Vérifiez les fonctions dont vous avez réellement besoin avant de complexifier la configuration.
Technitium DNS Server	Vous voulez administrer plus finement le service DNS.	Le niveau de personnalisation demande une administration plus attentive.
DNS filtrant hébergé	Vous cherchez un démarrage simplifié sans installer de serveur chez vous.	Vous conservez moins de contrôle qu'avec une installation locale.

3. Valider les fonctions essentielles

- ☐ **Contrôler que le projet est maintenu et documenté**
La disponibilité d'une documentation claire facilite l'installation et le dépannage.
- ☐ **Vérifier la présence d'un journal de requêtes**
Il permet d'identifier un domaine bloqué lorsqu'un service ne fonctionne plus.
- ☐ **Tester la simplicité de la liste d'autorisation**
Vous devez pouvoir réautoriser rapidement un domaine légitime.
- ☐ **Prévoir l'export ou la sauvegarde de la configuration**
Conservez un moyen de restaurer votre installation après un changement ou une panne.
- ☐ **Vérifier les protocoles DNS chiffrés auprès du fournisseur choisi**
Les possibilités de DNSCrypt, DoH, DoT ou DoQ doivent être confirmées dans sa documentation officielle.

4. Démarrer le filtrage sans provoquer de faux positifs

- ☐ **Commencer avec une configuration de blocage limitée**
N'ajoutez pas plusieurs listes inconnues avant d'avoir validé le fonctionnement de base.
- ☐ **Tester les services importants du foyer**
Vérifiez notamment les connexions, lecteurs vidéo, applications et services utilisés régulièrement.
- ☐ **Consulter le journal en cas de dysfonctionnement**
Recherchez le domaine bloqué avant de modifier largement les règles.
- ☐ **Ajouter uniquement le domaine nécessaire à la liste d'autorisation**
Évitez de désactiver tout le filtrage pour résoudre un seul problème.
- ☐ **Sauvegarder la configuration après chaque réglage validé**
Vous pourrez revenir à un état fonctionnel si une liste ou une règle devient trop restrictive.

- ! Prévoir une solution de secours**
Si le serveur DNS local devient indisponible sans résolveur secondaire configuré, le réseau peut sembler en panne. Préparez une procédure de retour arrière et un DNS de secours avant de basculer tous les appareils.

Le filtrage DNS réduit l'exposition à la publicité et au suivi au niveau du réseau ; il ne remplace ni les mises à jour de sécurité, ni un antivirus, ni les autres bonnes pratiques de protection.