# Comment activer DNS over HTTPS (DoH) dans Windows 10

Microsoft a annoncé que la prise en charge initiale de DNS sur HTTPS (DoH) est désormais disponible dans *Windows 10 Insider Preview Build 19628* pour Windows Insiders dans l'anneau rapide.

DoH permet la résolution DNS sur les connexions HTTPS chiffrées, tandis que DoT est conçu pour chiffrer les requêtes DNS via le protocole Transport Layer Security (TLS), au lieu d'utiliser des recherches DNS en texte clair.

Cela permet donc de **sécuriser vos résolutions DNS** et éviter les attaques Man In the Middle. Par défaut cette option n'est pas activée. L'utilisateur doit donc l'activer s'il veut en bénéficier.

Voici comment **activer DNS over HTTPS (DoH) dans Windows 10**.


**a) Activer DNS over HTTPS (DoH) dans Windows 10**

- Ouvrir l'éditeur du registre Windows à l'aide des touches claviers Windows + R
- Ensuite, saisir **regedit** et cliquer sur OK.
- Dérouler à gauche, l'arborescence suivante
  **KEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Dnscache\Parameters**
- A droite, faites un clic droit puis Nouveau
- Cliquer sur D-Word (32-bits)
- Nommer la **EnableAutoDoh**
- Double-cliquer sur la valeur **EnableAutoDoh** et attribuer la valeur **2**

### b) Modifier les DNS de Windows vers DoH

Enfin vous devez utiliser des serveurs DNS proposant DNS Over HTTPS (DoH). Reportez-vous au tableau ci-dessous. L'article suivant explique modifier les DNS de Windows : Comment changer les DNS de Windows.

Voici une liste de serveurs DNS proposant le DoH.

| Fournisseurs | IP des serveurs |
|---|---|
| Cloudflare | 1.1.1.1<br>1.0.0.1<br>2606:4700:4700::1111<br>2606:4700:4700::1001 |
| Google | 8.8.8.8<br>8.8.4.4<br>2001:4860:4860::8888<br>2001:4860:4860::8844 |
| Quad9 | 9.9.9.9<br>149.112.112.112<br>2620:fe::fe<br>2620:fe::fe:9 |

Fournisseurs DNS avec DoH

Bravo ! vous avez réussi à activer DNS Over HTTPs (DoH) sur Windows 10.

### c) Comment vérifier si DoH est bien actif dans Windows 10

Vous pouvez ensuite vérifier que DNS Over HTTPs est bien actif dans Windows.

Pour ce faire, ouvrez une invite de commandes ou une fenêtre PowerShell et exécutez les commandes suivantes pour réinitialiser les filtres de trafic réseau PacketMon.
Ajoutez un filtre de trafic pour le port 53 (le port utilisé pour les requêtes DNS non chiffrées) et pour démarrer la journalisation du trafic en temps réel:

- Ouvrez une invite de commandes en administrateur
- Puis copier/coller les commandes suivantes.

**pktmon filter remove**
**pktmon filter add -p 53**
**pktmon start --etw -m real-time**

Windows 10 va écouter les requêtes DNS et les afficher. Lorsque DoH n'est pas actic, pktmon peut récupérer et afficher les résolutions DNS en cours.

Alors que lorsque DoH est actif, il n'est pas capable de les afficher car les requêtes DNS sont chiffrées.
Bravo ! vous avez réussi à activer DNS Over HTTPs (DoH) sur Windows 10 afin de sécuriser vos DNS.

**d) DoH dans les navigateurs WEB**

Les navigateurs WEB sont aussi concernés par le DNS Over HTTPS.

Ainsi, Mozilla Firefox propose déjà DoH en natif que vous pouvez activer facilement. Google exécute également actuellement un essai DoH limité sur toutes les plates-formes (à l'exception de Linux et iOS) à partir de la sortie de Chrome 79.

Pour aller plus loin dans la sécurisation des requêtes DNS, suivez aussi cet article : Sécuriser les connexions DNS avec Firefox ou Chrome.

**e) Liens**

- DNS et serveurs de noms : Comment cela fonctionne ?
- Firefox : Activer et changer adresse du DNS Over HTTPs (DoH)
- Sécuriser les connexions DNS avec Firefox ou Chrome
- YogaDNS : un client DNS avancé

source : https://techcommunity.microsoft.com/t5/networking-blog/windows-insiders-can-now-test-dns-over-https/ba-p/1381282