TP DNS



- Sous Windows, le fichier interrogé pour la résolution des noms de domaine est : C:\WINDOWS\system32\drivers\etc\host s
- Lorsque l'on ajoute un nom de domaine à l'adresse IP d'un site dans ce fichier, celle-ci sera accessible en tapant le nom de domaine dans le navigateur : exemple avec le site 192.168.100.43 du TP Wordpress que j'ai associé au nom de domaine clinique-lpfs.fr

	clinique.lpfs.fr				
٢	clinique.lpfs.fr				
Q	clinique.lpfs.fr - Re	cherche : Bing			
Filt	rez votre recherche :	🕑 Historique	☆ Favoris	Onglets	£\$3

Modification du fichier e résolution des noms de domaine

	hosts - Bloc-notes	-		×
	Fichier Edition Format Affichage Aide			
	# Copyright (c) 1993-2009 Microsoft Corp. #			
	‴ # This is a √ample HOSTS file used by Microsoft TCP/IP for Windows.			
	#			
	# This file contains the mappings of IP addresses to host names. Each # entry should be kent on an individual line. The IP address should			
	# be placed in the first column followed by the corresponding host name.			
	# The IP address and the host name should be separated by at least one # space			
	# space.			
	# Additionally, comments (such as these) may be inserted on individual			
	# lines or following the machine name denoted by a # symbol. #			
	# For example:			
	# 102 54 94 97 rhino acme com # source server			
	# 38.25.63.10 x.acme.com # x client host			
	# localhost name resolution is handled within DNS itself			
	# 127.0.0.1 localhost			
	# ::1 localhost			
	192.168.100.43 clinique-lpfs.fr			
	<			>
	Ln 23, Col 37 100% Windows (CRLF)	UTF-	8	
÷	ර් 🔺 Non sécurisé 192.168.100.43 වි වි 🖓 🖓 🖓			
	CLINIQUE LPFS 👧			
	🔓 🛇 Cambrai, 59400 💊 06 38 56 70 42 🖻 contact-clinique@lpfs.com			
	Bienvenue sur le site de la Clinique LPFS, votre partenaire de			
	confiance pour des soins de qualité depuis 1981. Découvrez nos			
-	services, rencontrez notre équipe médicale et trouvez des			
	informations prátiques pour planifier votre visite. Nous sommes là			
	pour vous, a chaque etape de voire parcours medical.			

Modification du fichier

• Lorsque l'on ajoute 127.0.0.1 (le localhost) devant un nom de domaine le site n'est plus accessible, exemple avec google.fr

(i) https://www.google.fr
Désolé, impossible d'accéder à cette page.
www.google.fr a refusé la connexion.
Essayez :
Vérification de la connexion
Vérification du proxy et du pare-feu
ERR_CONNECTION_REFUSED
Actualiser
✓ Détails
is a sample HOSTS file used by Microsoft TCP/IP for Wind
file contains the mappings of IP addresses to host names

This file contains the mappings of IP addresses to host names # entry should be kept on an individual line. The IP address sh # be placed in the first column followed by the corresponding h # The IP address and the host name should be separated by at le # space.

Additionally, comments (such as these) may be inserted on ind: # lines or following the machine name denoted by a '#' symbol.

For example:

This

ŧ	102.54.94.97	rhino.acme.com	<pre># source server</pre>
ŧ	38.25.63.10	x.acme.com	<pre># x client host</pre>

localhost name resolution is handled within DNS itself.

	127.0.0.1	localhost
÷	::1	localhost

192.168.100.43 clinique-lpfs.fr 127.0.0.1 www.google.fr

Bloquer ChatGPT

• Pour bloquer ChatGPT, la démarche a suivre est la meme que pour google et le site sera inaccessible.

		q chatgpt -	Recherche	×	openai.com		×	+						-	Ð	×
\leftarrow	С	① http	s://openai.com/ble	og/chatg	pt/				Aø	☆	Ф	£≡	Ē	-86		0
																Q
			\sim													
			\bigcirc													
			••													X *
																0
			Désolé, i	mpo	ssible d'ao	ccéder à	ce	tte page	ə.							0
			openai.com a i	efusé la i	connexion.											*
			Essayez :													
			Vérification	de la con	nexion											+
			Vérification	du proxy	et du pare-feu											
			ERR_CONNECTION_F	EFUSED												
			Actualiser				1	÷								
			✓ Détails													
			20000													
																ŵ

```
*hosts - Bloc-notes
                                                                             – 🗆 🗙
Fichier Edition Format Affichage Aide
#
# This file contains the mappings of IP addresses to host names. Each
# entry should be kept on an individual line. The IP address should
# be placed in the first column followed by the corresponding host name.
# The IP address and the host name should be separated by at least one
# space.
# Additionally, comments (such as these) may be inserted on individual
# lines or following the machine name denoted by a '#' symbol.
# For example:
      102.54.94.97
                    rhino.acme.com
                                               # source server
       38.25.63.10
                       x.acme.com
                                               # x client host
# localhost name resolution is handled within DNS itself.
       127.0.0.1
                       localhost
#
       ::1
                       localhost
       192.168.100.43 clinique-lpfs.fr
       127.0.0.1
                      www.google.fr
        87.98.154.146 www.btssio.fr
        127.0.0.1
                       openai.com
                                        Ln 26, Col 22
                                                        100% Windows (CRLF) UTF-8
```

Cache DNS

- La commande ipconfig /displaydns sert à afficher le contenu du cache de la resolution DNS
- La commande ipconfig /flushdns sert a vider le cache de resolution DNS. Cela peut permettre de faciliter le dépannage des erreurs DNS.

```
fe3cr.delivery.mp.microsoft.com
Nom d'enregistrement. : fe3cr.delivery.mp.microsoft.com
Type d'enregistrement : 5
Durée de vie . . . : 78
Longueur de données . : 8
Section . . . . . . : Réponse
Enregistrement CNAME : fe3.delivery.mp.microsoft.com
Nom d'enregistrement. : fe3.delivery.mp.microsoft.com
Type d'enregistrement : 5
Durée de vie . . . : 78
Longueur de données . : 8
Section . . . . . . . Réponse
Enregistrement CNAME : glb.cws.prod.dcat.dsp.trafficmanager.net
Nom d'enregistrement. : glb.cws.prod.dcat.dsp.trafficmanager.net
Type d'enregistrement : 1
Durée de vie . . . : 78
Longueur de données . : 4
Section . . . . . . : Réponse
Enregistrement (hôte) : 20.166.126.56
clinique-lpfs.fr
Aucun enregistrement de type AAAA
clinique-lpfs.fr
```

```
Nom d'enregistrement. : clinique-lpfs.fr
Type d'enregistrement : 1
Durée de vie . . . : 604205
Longueur de données . : 4
Section . . . . . . : Réponse
Enregistrement (ñôte) : 102.168.100.43
```

nregistrement (hôte) : 13.107.213.42



Microsoft Windows [version 10.0.19043.928] (c) Microsoft Corporation. Tous droits réservés. C:\Users\Windows>ipconfig /flushdns Configuration IP de Windows Cache de résolution DNS vidé. C:\Users\Windows>_

Nslookup

- Le poste client peut interroger un servuer DNS pour obtenir des informations de resolutions de noms. C'est-à-dire qu'il envoie une requête DNS au serveur pour obtenir l'IP associée au nom de domaine.
- Pour se faire il faut utiliser la commande nslookup, puis le nom de domaine, exemple avec google.fr

```
user@debian:~$ nslookup
> www.google.fr
Server: 8.8.8.8
Address: 8.8.8.8#53
```

Non-authoritative answer: Name: www.google.fr Address: 142.250.74.227 Name: www.google.fr Address: 2a00:1450:4007:80b::2003 > ■

Nslookup

- La commande Nslookup permet d'interroger le serveur DNS pour avoir d'autres informations sur le domaine comme par exemple le serveur de messageries, de nom, le mode d'interrogation etc...
- Sur linux la commande est : **dig domaine aaa**

```
user@debian:~$ nslookup
> www.google.fr
Server: 8.8.8.8
Address: 8.8.8.8#53
Non-authoritative answer:
Name: www.google.fr
Address: 142.250.74.227
Name: www.google.fr
Address: 2a00:1450:4007:80b::2003
>
```

Par exemple pour obtenir le service de messagerie d'un domaine sur Windows on utilise la commande **set type=mx** ce qui donne :

> set type=mx > btssio.fr Serveur : UnK Address: 192.1	nown 68.1.254
Réponse ne fais	ant pas autorité :
btssio.fr	MX preference = 1, mail exchanger = mx1.mail.ovh.net
btssio.fr	MX preference = 100, mail exchanger = mx3.mail.ovh.net
btssio.fr	MX preference = 5, mail exchanger = mx2.mail.ovh.net

user@debian:~\$ dig www.google.fr aaaa

```
<>>> DiG 9.16.44-Debian <<>> www.google.fr aaaa
  global options: +cmd
  Got answer:
  ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 51069
  flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1
  OPT PSEUDOSECTION:
 EDNS: version: 0, flags:; udp: 512
 : OUESTION SECTION:
 www.google.fr.
                                IN
                                       AAAA
  ANSWER SECTION:
                                               2a00:1450:4007:80b::2003
www.google.fr.
                        300
                               IN
                                       AAAA
  Query time: 24 msec
  SERVER: 8.8.8.8#53(8.8.8.8)
  WHEN: Wed Apr 17 15:03:41 CEST 2024
;; MSG SIZE rcvd: 70
```

Capture de Trame DNS

 Lorsque nous lançons une résolution du FQDN, avec la commande Nslookup après avoir vidé le cache local DNS avec la commande ipconfig /flushdns, nous pouvons constater que nous trouvons des trames DNS sur wireshark, l'adresse IP à laquelle est associée le FQDN pour www.btssio.fr est 185.156.80.7

227 20.707256	192.168.60.101	185.156.80.7	DNS	79 Standard query 0x0002 A btssio.fr.sio.local
252 22.714821	192.168.60.101	185.156.80.7	DNS	79 Standard query 0x0003 AAAA btssio.fr.sio.local