Le résolveur DNS public de Wikimédia

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 2 août 2024

https://www.bortzmeyer.org/wikidough.html

Encore un résolveur DNS <https://www.bortzmeyer.org/resolveur-dns.html> public ? Oui, mais c'est une bonne chose, il en faut le plus possible, pour éviter de dépendre d'un petit nombre d'acteurs. Et celui-ci est géré par la fondation Wikimédia.

Rien n'est plus agaçant que les gens qui croient s'y connaitre et qui, à chaque panne, censure ou autre problème mettant en jeu (croient-ils) le DNS, répondent tout de suite qu'il faut utiliser 8.8.8.8 (Google) ou parfois un autre résolveur étatsunien comme 1.1.1.1 ou 9.9.9.9. Non seulement il est mauvais, pour la vie privée, d'envoyer toutes ses requêtes DNS aux USA mais il y a aussi un problème plus stratégique. Si tout le monde dépend d'un petit nombre d'acteurs, nous devenons tous vulnérables à des changements de politique, de tarification, ou à une offensive de la censure (qui a d'ailleurs commencé à frapper les résolveurs publics <https://www.bortzmeyer.org/opendns-quitte-france.html>). Il faut au contraire une grande diversité de résolveurs DNS. Saluons donc le travail de la fondation Wikimédia, qui a un résolveur public <https://meta.wikimedia.org/wiki/Wikimedia_DNS>, « Wikimedia DNS ».

Je vous recommande la documentation très claire et très détaillée <https://meta.wikimedia.org/wiki/Wikimedia_DNS> de ce service. Ce résolveur est bien noté comme expérimental et sans garantie, mais, si vous lisez les petites lettres des CGU, c'est pareil pour tous les autres. Au moins, il est géré par une association et pas par une personne unique (comme l'est le mien <https://doh.bortzmeyer.fr/policy>) donc il est moins dépendant d'un individu.

Notez aussi qu'il n'est accessible qu'en DoT et DoH, ce qui est raisonnable techniquement, et normal pour un service surtout destiné à contourner la censure (qui aurait beau jeu de tripoter des réponses envoyés en clair). En traditionnel UDP en clair, on n'aura donc pas de réponse :

```
% dig @185.71.138.138 ratzeburg.de
;; communications error to 185.71.138.138#53: timed out
;; communications error to 185.71.138.138#53: timed out
;; communications error to 185.71.138.138#53: timed out

; <<>> DiG 9.18.28-0ubuntu0.22.04.1-Ubuntu <<>> @185.71.138.138 ratzeburg.de
; (1 server found)
;; global options: +cmd
;; no servers could be reached
```

Mais le serveur marche bien, ici en DoT :

```
% dig +tls @185.71.138.138 ratzeburg.de

; <<>> DiG 9.18.28-0ubuntu0.22.04.1-Ubuntu <<>> +tls @185.71.138.138 ratzeburg.de
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 16221
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags: do; udp: 512
;; QUESTION SECTION:
;ratzeburg.de. IN A

;; ANSWER SECTION:
ratzeburg.de. 3600 IN A 213.178.85.153

;; Query time: 56 msec
;; SERVER: 185.71.138.138#853(185.71.138.138) (TLS)
;; WHEN: Fri Aug 02 13:29:26 CEST 2024
;; MSG SIZE  rcvd: 57
```

On peut donc l'utiliser directement depuis les systèmes qui peuvent utiliser DoT (Android, par exemple) ou indirectement via un résolveur local comme Unbound qui fera suivre à Wikimédia DNS. Voici un exemple de configuration de Unbound pour cela :

```
forward-zone:
  name: "."

# Wikimedia DNS. On authentifie le nom dans le certificat
# (émis par Let's Encrypt) donc, sur Debian/Ubuntu, ne pas
# oublier le "tls-system-cert: yes" dans le bloc "server:".
forward-addr: 185.71.138.138#wikimedia-dns.org

        forward-tls-upstream: yes
```

On notera que, comme tous les résolveurs sérieux, il valide avec DNSSEC :

```
% dig +tls @185.71.138.138 denic.de
...
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 30888
;; flags: qr rd ra ad; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1
                   ^^
                   Authentic Data
...
;; ANSWER SECTION:
denic.de. 3578 IN A 81.91.170.12
...
```

Et la répartition des instances de ce serveur dans le monde ? Regardons avec les sondes RIPE Atlas <https://atlas.ripe.net/> :

```
% blaeu-resolve --nameserver 2001:67c:930::1 --nsid --type A --tls \
     --requested 200 ratzeburg.de
Nameserver 2001:67c:930::1
[213.178.85.153 NSID: doh3004;] : 45 occurrences
[213.178.85.153 NSID: doh1001;] : 10 occurrences
[213.178.85.153 NSID: doh3003;] : 52 occurrences
[213.178.85.153 NSID: doh2001;] : 6 occurrences
[TIMEOUT] : 7 occurrences
[213.178.85.153 NSID: doh6001;] : 14 occurrences
[213.178.85.153 NSID: doh1002;] : 11 occurrences
[213.178.85.153 NSID: doh6002;] : 16 occurrences
[213.178.85.153 NSID: doh5002;] : 12 occurrences
[213.178.85.153 NSID: doh5001;] : 8 occurrences
[213.178.85.153 NSID: doh7002;] : 2 occurrences
[213.178.85.153 NSID: doh4002;] : 5 occurrences
[213.178.85.153 NSID: doh4001;] : 6 occurrences
[213.178.85.153 NSID: doh7001;] : 1 occurrences
[TUCONNECT (may be a TLS negotiation error or a TCP connection issue)] : 1 occurrences
Test #76486532 done at 2024-08-02T11:40:00Z
```

On voit qu'on a plusieurs NSID (RFC 5001 [1]), ce qui indique que le résolveur est "*anycasté*", sur l'infrastructure de la fondation <https://wikitech.wikimedia.org/wiki/Network_design> (qui héberge notamment Wikipédia). Les pros de l'administration système noteront que la configuration Puppet est disponible <https://gerrit.wikimedia.org/r/plugins/gitiles/operations/puppet/+/refs/heads/production/modules/role/manifests/wikidough.pp>. Sinon, une meilleure preuve de la répartition "*anycastée*" est donnée en regardant la latence depuis divers pays <https://atlas.ripe.net/measurements/76486732/results> : qu'on soit en Europe ou en Amérique, on obtient des RTT très courts, ce qui n'arriverait pas s'il existait une seule instance physique du serveur.

1. Pour voir le RFC de numéro NNN, https://www.ietf.org/rfc/rfcNNN.txt, par exemple https://www.ietf.org/rfc/rfc5001.txt