

Le résolveur DNS public de Freifunk München

Stéphane Bortzmeyer

<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 16 octobre 2025

<https://www.bortzmeyer.org/ffmuc-resolveur-dns.html>

Allez, encore un résolveur DNS <<https://www.bortzmeyer.org/resolveur-dns.html>> public européen, celui de Freifunk München <<https://ffmuc.net/>>. Rien d'extraordinaire mais rappelez-vous que, dans ce domaine, pluralisme et diversité sont cruciaux.

Des résolveurs DNS <<https://www.bortzmeyer.org/resolveur-dns.html>> publics, il y en a beaucoup (j'en gère même un <<https://doh.bortzmeyer.fr/policy>>). Les utilisatrices et administratrices système s'en servent pour des raisons variées, par exemple échapper à la censure <https://labs.ripe.net/author/stephane_bortzmeyer/dns-censorship-dns-lies-as-seen-by-ripe>. Mais ils ne sont pas tous équivalents <<https://www.bortzmeyer.org/dns-resolveurs-publics.html>>, en terme de caractéristiques techniques, de fonctions (certains sont menteurs <<https://www.bortzmeyer.org/censure-francaise.html>>), de politique de gestion des données personnelles, etc. Le service de Freifunk München :

- A DoH, DoH, DNSSEC et IPv6 (comme tous les résolveurs publics sérieux),
- Promet <https://ffmuc.net/wiki/knb:dohdot_en> d'être strict sur la vie privée et notamment de ne pas garder de trace des requêtes faites,
- Est européen (certains résolveurs publics qui se présentent comme européens sont en fait des services étatsuniens un peu repeints, par exemple en s'appuyant sur la nationalité d'origine du fondateur), plus précisément allemand (par contre, le nom de domaine est dans un TLD étatsunien, ce qui est curieux, mais n'a pas trop d'importance car le nom ne sert pas beaucoup pour accéder à un résolveur DNS, sauf pour l'authentification TLS).

Faisons quelques essais techniques. Les adresses et noms à utiliser <https://ffmuc.net/wiki/knb:dohdot_en> sont 185.150.99.255, 5.1.66.255, 2001:678:e68:f000::, 2001:678:ed0:f000::, dot.ffmuc.net, <https://doh.ffmuc.net/dns-query> et [doq.ffmuc.net](https://doh.ffmuc.net/doq) (je n'ai pas testé ce dernier). D'abord, avec dig :

```
% dig @2001:678:ed0:f000:: sci-hub.se
...
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 24707
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1
...
;; ANSWER SECTION:
sci-hub.se. 60 IN A 186.2.163.219

;; Query time: 34 msec
;; SERVER: 2001:678:ed0:f000::#53(2001:678:ed0:f000::) (UDP)
;; WHEN: Thu Oct 16 14:38:17 CEST 2025
;; MSG SIZE rcvd: 55
```

OK, c'est bon, tout marche, et en un temps raisonnable depuis ma connexion Free à Paris. (Évidemment, un résolveur public ne sera jamais aussi rapide qu'un résolveur local <<https://www.bortzmeyer.org/son-propre-resolveur-dns.html>> et il n'est donc pas raisonnable d'utiliser un résolveur public « pour les performances ».)

Et avec DoT?

```
% dig +tls @2001:678:ed0:f000:: liberation.fr
...
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 31755
;; flags: qr rd ra; QUERY: 1, ANSWER: 4, AUTHORITY: 0, ADDITIONAL: 1
...
;; ANSWER SECTION:
liberation.fr. 300 IN A 3.165.113.53
liberation.fr. 300 IN A 3.165.113.101
liberation.fr. 300 IN A 3.165.113.127
liberation.fr. 300 IN A 3.165.113.118

;; Query time: 62 msec
;; SERVER: 2001:678:ed0:f000::#853(2001:678:ed0:f000::) (TLS)
;; WHEN: Thu Oct 16 14:40:02 CEST 2025
;; MSG SIZE rcvd: 106
```

Et du DoH?

```
% kdig +https=https://doh.ffmuc.net/dns-query @185.150.99.255 bortzmeyer.fr NS

;; TLS session (TLS1.3)-(ECDHE-SECP256R1)-(RSA-PSS-RSAE-SHA256)-(AES-128-GCM)
;; HTTP session (HTTP/2-POST)-(doh.ffmuc.net/dns-query)-(status: 200)
;; ->>HEADER<<- opcode: QUERY; status: NOERROR; id: 0
;; Flags: qr rd ra ad; QUERY: 1; ANSWER: 7; AUTHORITY: 0; ADDITIONAL: 1

;; EDNS PSEUDOSECTION:
;; Version: 0; flags: ; UDP size: 512 B; ext-rcode: NOERROR
;; PADDING: 238 B
...
;; ANSWER SECTION:
bortzmeyer.fr. 85495 IN NS ns2.1984hosting.com.
bortzmeyer.fr. 85495 IN NS ns0.1984.is.
bortzmeyer.fr. 85495 IN NS ns4.bortzmeyer.org.
bortzmeyer.fr. 85495 IN NS ns-global.kjsl.com.
bortzmeyer.fr. 85495 IN NS puck.nether.net.
bortzmeyer.fr. 85495 IN NS ns2.bortzmeyer.org.
bortzmeyer.fr. 85495 IN NS ns2.1984.is.

;; Received 468 B
;; Time 2025-10-16 14:42:39 CEST
;; From 185.150.99.255@443(HTTPS) in 91.2 ms
```

C'est parfait, tout marche. Pour la dernière requête, celle faite avec DoH, notez que le résolveur valide bien les domaines signés.

Configurons maintenant un résolveur local pour faire suivre à ffmuc, pour profiter de la mémorisation des réponses par celui-ci. On va utiliser Unbound et faire suivre en TLS :

<https://www.bortzmeyer.org/ffmuc-resolveur-dns.html>

```
forward-zone:
  name: "."
  # Freifunk München
  forward-addr: 2001:678:ed0:f000::@853#dot.ffmuc.net
  forward-tls-upstream: yes
```

Et tout marche, notre résolveur local fera suivre ce qu'il ne sait pas déjà à ffmuc.

ffmuc a-t-il plusieurs machines, réparties par *"anycast"*? On peut regarder les identités de ces serveurs avec NSID (RFC 5001¹):

```
% dig +nsid @5.1.66.255 www.phy.cam.ac.uk
...
;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags: do; udp: 512
; NSID: 64 6f 74 2e 66 66 6d 75 63 2e 6e 65 74 ("dot.ffmuc.net")
;; QUESTION SECTION:
;www.phy.cam.ac.uk. IN A

;; ANSWER SECTION:
www.phy.cam.ac.uk. 3591 IN CNAME tm-128-232-132-117.tm.uis.cam.ac.uk.
tm-128-232-132-117.tm.uis.cam.ac.uk. 3600 IN A 128.232.132.117
...
```

Le NSID est juste le nom du service. Un test avec les sondes RIPE Atlas <<https://atlas.ripe.net/>> montre qu'il n'y a en effet qu'un seul serveur.

Notez enfin que la configuration technique de ce service est publique <<https://github.com/freifunkMUC/ffmuc-salt-public/blob/main/dnsdist/dnsdist.conf.j2>> ainsi que celle des autres services <<https://github.com/freifunkMUC/ffmuc-salt-public/tree/main>>.

Est-ce que je vais utiliser ce service? Non, il en existe plusieurs autres qui me conviennent (dont le mien <<https://doh.bortzmeyer.fr/policy>>, bien sûr, mais aussi celui de FDN <<https://www.bortzmeyer.org/fdn-dot-doh.html>>) mais avoir le choix est une bonne chose.

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