Le résolveur DNS public dns.sb

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 27 septembre 2023

https://www.bortzmeyer.org/dns-sb.html

Je ne sais pas exactement quand il a été lancé mais je viens de voir passer un résolveur DNS <https://www.bortzmeyer.org/resolveur-dns.html> public que je ne connaissais pas, DNS.sb. Il a quelques caractéristiques intéressantes.

Bon, des résolveur 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 utilisateurices et administrateurices 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> ou bien contourner un problème technique <https://twitter.com/abyssproject_ns/status/1706552932227772718>. 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 DNS.sb :

— A DoT, DNSSEC et IPv6 (comme tous les résolveurs publics sérieux),
— Promet 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 aux îles Salomon, 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),
— Ne modifie pas les réponses DNS (ce n'est pas un résolveur menteur <https://www.bortzmeyer.org/blocage-telegram-france.html>, c'est l'information reçue de leur équipe, ce n'est pas clairement documenté et ce n'est pas facile à tester ; j'ai essayé quelques noms susceptibles d'être censurés, et j'obtiens en effet la bonne réponse).

Faisons quelques essais techniques. Comme DNS.sb a des adresses IPv6 dont la forme texte <https://www.bortzmeyer.org/representation-texte.html> est très courte, on va les utiliser. D'abord, avec dig :

```
% dig  @2a09:: sci-hub.se
...
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 30101
;; 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: 32 msec
;; SERVER: 2a09::#53(2a09::) (UDP)
;; WHEN: Wed Sep 27 11:47:18 CEST 2023
;; 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 ? Passons à kdig :

```
% kdig +tls @2a09::   disclose.ngo
;; TLS session (TLS1.3)-(ECDHE-SECP256R1)-(ECDSA-SECP256R1-SHA256)-(AES-256-GCM)
;; ->>HEADER<<- opcode: QUERY; status: NOERROR; id: 46687
;; Flags: qr rd ra; QUERY: 1; ANSWER: 1; AUTHORITY: 0; ADDITIONAL: 1
...
;; QUESTION SECTION:
;; disclose.ngo.        IN A

;; ANSWER SECTION:
disclose.ngo.        300 IN A 84.16.72.183

;; Received 57 B
;; Time 2023-09-27 11:50:43 CEST
;; From 2a09::@853(TCP) in 326.4 ms
```

C'est parfait, tout marche (la première ligne nous montre les algorithmes cryptographiques utilisés).

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

```
forward-zone:
        name: "."
        # DNS.sb
        forward-addr: 2a11::@853#dot.sb
        forward-tls-upstream: yes
```

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

`DNS.sb` dit qu'ils ont plusieurs machines, réparties par "*anycast*". On peut regarder les identités de ces serveurs avec NSID (RFC 5001 [1]) :

```
% dig +nsid @2a09:: www.lycee-militaire-autun.terre.defense.gouv.fr
...
;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags: do; udp: 512
; NSID: 64 6e 73 2d 6c 6f 6e 32 ("dns-lon2")
...
;; Query time: 80 msec
;; SERVER: 2a09::#53(2a09::) (UDP)
;; WHEN: Wed Sep 27 12:00:55 CEST 2023
;; MSG SIZE  rcvd: 137
```

On tombe apparemment sur une machine située à Londres ("`dns-lon2`"). Ça pourrait être mieux, mais l'"*anycast*" est un sport difficile.

Avec les sondes RIPE Atlas <`https://atlas.ripe.net/`>, on peut avoir une idée du nombre de serveurs :

```
% blaeu-resolve --requested 100 --nameserver 2a09::  --nsid --type TXT ee
Nameserver 2a09::
["the zone content is (c) ... NSID: fra1;] : 4 occurrences
["the zone content is (c) ... NSID: debian;] : 6 occurrences
["the zone content is (c) ... NSID: us-sjc;] : 2 occurrences
["the zone content is (c) ... NSID: s210;] : 3 occurrences
["the zone content is (c) ... NSID: fra2;] : 5 occurrences
["the zone content is (c) ... NSID: dns-fra4;] : 3 occurrences
["the zone content is (c) ... NSID: dns-lon2;] : 2 occurrences
["the zone content is (c) ... NSID: dns-a;] : 3 occurrences
["the zone content is (c) ... NSID: lon-dns;] : 2 occurrences
["the zone content is (c) ... NSID: dns-ams3;] : 1 occurrences
[TIMEOUT] : 2 occurrences
Test #60486061 done at 2023-09-27T10:03:17Z
```

On voit dix instances différentes. Le schéma de nommage ne semble pas cohérent ("debian"???) donc il est difficile d'en dire plus. Mais des traceroute nous montrent que ces machines sont en effet bien réparties, en tout cas pour l'Europe.

Je suis en tout cas satisfait de découvrir un résolveur DNS public européen (et qui marche, contrairement au projet coûteux et bureaucratique de la Commission Européenne <`https://www.whalebone.io/dns4eu`>, qui n'est toujours pas en service). 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 cela semble un service bien fait et qui pourrait me convenir.

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