Encore un résolveur DNS public européen, DNS4ALL

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 7 juin 2024

https://www.bortzmeyer.org/resolveur-dns-sidn.html

Utiliser un résolveur DNS <https://www.bortzmeyer.org/resolveur-dns.html> public est souvent nécessaire pour contourner la censure faite, notamment, au profit des ayant-tous-les-droits. Mais il ne faut pas que tout le monde se concentre sur deux ou trois gros résolveurs, surtout s'ils sont gérés depuis un pays qui se moque de la protection des données personnelles. Il faut au contraire une multiplicité de résolveurs DNS publics, et gérés depuis des pays divers. D'où l'intérêt de ce nouveau résolveur public géré aux Pays-Bas, DNS4ALL <https://dns4all.eu/>.

Merci donc à SIDN, registre de .nl, pour cette contribution au pluralisme et à la diversité. (Il y a peu de résolveurs DNS publics européens mais on peut citer celui de FDN <https://www.bortzmeyer.org/fdn-dot-doh.html> ou celui de DNS.sb <https://www.bortzmeyer.org/dns-sb.html>.) Peut-être que cela fera enfin taire la propagande qui essaie de s'opposer à ces résolveurs publics en faisant semblant de croire qu'il n'y a que ceux de Google et Cloudflare ?

Commençons par le commencement, est-ce qu'il marche ? Regardons avec dig :

```
% dig @2001:678:8::3 www.bortzmeyer.org

; <<>> DiG 9.18.24-1-Debian <<>> @2001:678:8::3 www.bortzmeyer.org
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 20893
;; flags: qr rd ra ad; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
;; QUESTION SECTION:
;www.bortzmeyer.org. IN A

;; ANSWER SECTION:
www.bortzmeyer.org. 86397 IN A 80.77.95.49

;; Query time: 4 msec
;; SERVER: 2001:678:8::3#53(2001:678:8::3) (UDP)
;; WHEN: Fri Jun 07 11:05:20 CEST 2024
;; MSG SIZE  rcvd: 63
```

OK, il fonctionne (« *"status : NOERROR"* »), il donne bien la bonne réponse, et il valide avec DNSSEC (« *"flags : ad"* », ce qui veut dire *"Authentic Data"*). Ici, on a utilisé du DNS classique sur UDP, en clair, testons avec du DNS chiffré via TLS (kdig nous donne un peu plus de détails que dig, mais ce dernier marche aussi pour DNS sur TLS) :

```
% kdig +tls @2001:678:8::3 www.bortzmeyer.org
;; TLS session (TLS1.3)-(ECDHE-SECP256R1)-(RSA-PSS-RSAE-SHA256)-(AES-256-GCM)
;; ->>HEADER<<- opcode: QUERY; status: NOERROR; id: 57888
;; Flags: qr rd ra ad; QUERY: 1; ANSWER: 1; AUTHORITY: 0; ADDITIONAL: 1

;; EDNS PSEUDOSECTION:
;; Version: 0; flags: ; UDP size: 1232 B; ext-rcode: NOERROR

;; QUESTION SECTION:
;; www.bortzmeyer.org.  IN A

;; ANSWER SECTION:
www.bortzmeyer.org.  86259 IN A 80.77.95.49

;; Received 63 B
;; Time 2024-06-07 11:07:37 CEST
;; From 2001:678:8::3@853(TCP) in 94.9 ms
```

Parfait, là aussi, on s'est connecté en TLS (authentifié par RSA, clés échangées par ECDHE, chiffré par AES). On peut donc utiliser ce résolveur de manière sécurisée. (Il a également DoH mais pas encore DoQ.)

Que se passe-t-il avec les domaines qui ont un problème technique, nous donne-t-il des détails ?

```
% dig +tls @2001:678:8::3 servfail.nl
...
;; ->>HEADER<<- opcode: QUERY, status: SERVFAIL, id: 40616
...
; EDE: 9 (DNSKEY Missing): (validation failure <servfail.nl. A IN>: signatures from unknown keys from 96.126
...
```

C'est à juste titre qu'il échoue (« *"status : SERVFAIL"* donc *"Server Failure"*) et il nous explique pourquoi en utilisant les EDE (*"Extended DNS Errors"*) du RFC 8914 [1] : « *"signatures from unknown keys"* » (ce domaine sert à des tests et ses signatures DNSSEC sont délibérement cassées).

Bon, on utilise souvent les résolveurs publics pour contourner la censure mais certains peuvent aussi censurer. Je dois dire que j'ai été trop paresseux pour lire leur politique de censure et je me suis contenté de tester Sci-Hub (il n'est pas possible de tout vérifier, mais, si vous connaissez un nom censuré, vous pouvez le tester) :

1. Pour voir le RFC de numéro NNN, `https://www.ietf.org/rfc/rfcNNN.txt`, par exemple `https://www.ietf.org/rfc/rfc8914.txt`

```
% dig +tls @2001:678:8::3 sci-hub.se
...
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 20416
...
;; ANSWER SECTION:
sci-hub.se. 60 IN A 186.2.163.219
```

Au moins Sci-Hub fonctionne (c'est l'adresse IP légitime).

Les gérants de ce service disent qu'il est "*anycasté*", ce qui est une bonne chose mais vérifions avec les sondes Atlas <https://atlas.ripe.net/> :

```
% blaeu-resolve --requested 200 --nsid --tls --nameserver 2001:678:8::3  www.gouda.nl
Nameserver 2001:678:8::3
[2001:9a8:a6:0:87:233:198:3 NSID: america-mex1;] : 24 occurrences
[2001:9a8:a6:0:87:233:198:3 NSID: asia-sin1;] : 60 occurrences
[2001:9a8:a6:0:87:233:198:3 NSID: eur-fra1;] : 106 occurrences
[TIMEOUT] : 5 occurrences
[NO RESPONSE FOR UNKNOWN REASON at probe 1006022] : 1 occurrences
[TUCONNECT (may be a TLS negotiation error or a TCP connection issue)] : 1 occurrences
[NO RESPONSE FOR UNKNOWN REASON at probe 62742] : 1 occurrences
Test #73149926 done at 2024-06-07T09:18:33Z
```

On notera :

— Quelques problèmes techniques (combiner IPv6 et TLS, je cherchais la difficulté, mais on voit à peu près la même chose en IPv4, et ce n'est pas forcément la faute de l'opérateur du résolveur, le port 853 peut être bloqué sur le réseau local),

— Apparemment trois serveurs, si on se fie aux NSID (RFC 5001), un sur chaque continent. Un article des opérateurs du projet <https://www.sidnlabs.nl/en/news-and-blogs/dns4all-sidn-labs-experi dit qu'il y a 30 nœuds "*anycast*", qui envoient vers 3 résolveurs, ce que nous avons pu vérifier.

L'article cité <https://www.sidnlabs.nl/en/news-and-blogs/dns4all-sidn-labs-experimental-public mentionne que les nœuds utilisent dnsdist <https://dnsdist.org/> (qui a sa propre mémoire, donc n'envoie pas forcément aux résolveurs) et les résolveurs utilisent Unbound <https://unbound.net/>. (C'est amusant, c'est pareil <https://www.bortzmeyer.org/doh-mon-resolveur.html> pour mon propre résolveur public <https://doh.bortzmeyer.fr/policy>.)

Terminons avec un exemple de configuration où on utilise sur son réseau local ou sur sa machine un résolveur Unbound qui fait suivre les requêtes dont les réponses ne lui sont pas connues à DNS4ALL. On notera qu'on indique le nom du serveur, ce qui permet à Unbound de vérifier le certificat (dont le titulaire est « CN=*.dns4all.eu,O=Stichting Internet Domeinregistratie Nederland,ST=Gelderland,C=NL ») :

```
forward-zone:
  name: "."
  # DNS4ALL
  forward-addr: 2001:678:8::3#dot.dns4all.eu
  forward-tls-upstream: yes
```

En tout cas, voici un nouveau résolveur public (alors que le projet officiel de la Commission, DNS4EU, est toujours inexistant, des années après son annonce), ce qui contribue à accroitre la diversité des offres.

---

https://www.bortzmeyer.org/resolveur-dns-sidn.html