Trouver l'adresse IP de son serveur de noms

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 24 janvier 2010. Dernière mise à jour le 24 janvier 2011

https://www.bortzmeyer.org/trouver-adresse-ns.html

Je cherche un moyen de trouver l'adresse IP avec laquelle mon serveur de noms interroge le monde extérieur. C'est bien plus compliqué que cela n'en a l'air.

Lorsque j'appelle `www.example.org`, l'application que j'utilise (que ce soit Firefox ou curl) fait appel (en général via le sous-programme `getaddrinfo()`) à un **résolveur** DNS ; sur Unix, son adresse est trouvé dans `/etc/resolv.conf`. Il y a des fois où j'aimerai bien savoir quelle adresse utilise ce résolveur pour interroger les serveurs **faisant autorité**. On ne peut pas simplement prendre l'adresse qui se trouve dans `/etc/resolv.conf` pour au moins trois raisons :

— Le résolveur peut faire appel à un autre résolveur (appelé un "*forwarder*" ; avec BIND, c'est le nom de la directive qui sert à configurer un tel « résolveur supérieur »).
— Le résolveur peut être derrière un routeur NAT, qui va changer son adresse.
— Le résolveur n'utilise pas forcément la même adresse pour les requêtes sortantes et les requêtes entrantes.

Je vois trois façons possibles de trouver l'adresse utilisée par la résolution de noms :

— Regarder sa configuration en détail, notamment des directives comme `forwarder` et `query-source` sur BIND. Cela ne marche que si on accès à cette configuration, ce qui n'est pas le cas de tout le monde.
— Sur une zone qu'on contrôle, écouter le trafic (par exemple avec tcpdump) sur tous les serveurs de noms faisant autorité et faire une requête pour `nexistepas.MAZONE` (il vaut mieux utiliser un nom non existant pour ne pas risquer qu'il soit dans le cache d'un résolveur). Cela oblige à avoir une zone dont on contrôle tous les serveurs de noms et ce n'est pas très pratique.
— Avoir quelque part une zone spécialement configurée pour servir de réflecteur qui, aux requêtes DNS, renvoie l'adresse IP du client qui l'a interrogé. C'est de loin la meilleure méthode.

Mais un tel service existe t-il ? Aucun serveur de noms standard ne sait faire cela, il faut donc écrire un serveur adapté. Par manque de temps, je cherche un service déjà existant.

Le premier testé est celui créé par l'OARC <http://www.dns-oarc.net/> pour un tout autre but, replysizetest <https://www.dns-oarc.net/oarc/services/replysizetest> et disponible en `rs.dns-oarc.net` et `rs.ripe.net`. Ignorons le but principal de ce service, ce qui m'intéresse ici est qu'il donne l'adresse IP de son client DNS. Ainsi, depuis Free, j'obtiens :

```
% dig +short TXT rs.dns-oarc.net
...
"213.228.63.32 sent EDNS buffer size 4096"
```

donc le résolveur de Free sort avec l'adresse IP `213.228.63.32`. Et Google DNS <https://www.bortzmeyer.org/google-dns.html> :

```
% dig +short TXT rs.dns-oarc.net
...
"209.85.228.94 lacks EDNS, defaults to 512"
```

On voit qu'il n'utilise pas en sortie les fameuses `8.8.8.8` et `8.8.4.4`.

À noter qu'il fonctionne également avec IPv6 (contrairement à ce que j'avais écrit dans une précédente version de l'article).

À noter également que l'OARC a un outil équivalent <https://www.dns-oarc.net/oarc/services/porttest> qui avait également été fait dans un autre but (détecter les résolveurs vulnérables à la faille Kaminsky <https://www.bortzmeyer.org/comment-fonctionne-la-faille-kaminsky.html>) et qui peut également être « détourné » pour nos recherches :

```
% dig +short porttest.dns-oarc.net TXT

porttest.y.x.w.v.u.t.s.r.q.p.o.n.m.l.k.j.i.h.g.f.e.d.c.b.a.pt.dns-oarc.net.
"192.134.4.162 is GREAT: 26 queries in 3.9 seconds from 8 ports with std dev 21270"
```

Même chose pour le service de test <http://dns.measurement-factory.com/surveys/openresolvers.html> des résolveurs ouverts <https://www.bortzmeyer.org/fermer-les-recursifs-ouverts.html> (merci à Nicolas Aupetit) :

```
% dig +short amiopen.openresolvers.org TXT
"Your resolver at 192.134.7.248 is CLOSED"
```

Ce service est-il une solution parfaite ? Outre qu'il est un peu lent car il fait bien autre chose que renvoyer l'adresse IP, je regrette qu'il ne puisse pas renvoyer une adresse binaire (en réponse à une question de type A ou AAAA).

Les entreprises qui font du "*load-balancing*" ont souvent des noms qu'on peut résoudre dans le DNS pour obtenir l'adresse IP du résolveur, à des fins de déboguage. C'est le cas de `whoami.ultradns.net` et de `whoami.akamai.net`. Ces deux services ont l'avantage de renvoyer l'adresse IPv4 en binaire (il faut donc faire une requête de type `A` et pas `TXT`), ce qui est pratique. Celui d'UltraDNS a l'inconvénient de planter complètement avec des adresses IPv6 (renvoyant `NXDOMAIN` au lieu du normal `NODATA`, ce qui est une bogue énorme

```
% dig AAAA whoami.ultradns.net
...
;; ->>HEADER<<- opcode: QUERY, status: NXDOMAIN, id: 51301
...
```

mais celui d'Akamai semble bien marcher.

D'un modèle analogue est celui de Cloudfront, `resolver-identity.cloudfront.net` (types A et TXT).

Encore mieux, le service de Cedexis (merci à Stéphane Enten), `1-01-2743-000d.cdx.cedexis.net`. Si le nom est un peu bizarre (le service ne semble pas encore stabilisé et plante parfois), le réflecteur marche très bien, renvoyant un CNAME vers un nom qui code le client, indiquant même le numéro d'AS :

```
% dig +short A 1-01-2743-000d.cdx.cedexis.net
client-ip-208.75.84.80--client-asn-23372.
```

Enfin, le meilleur service (notamment parce qu'il marche correctement avec IPv6) : `myresolver.info` (merci à Nicolas Aupetit). On peut l'utiliser en visitant simplement la page Web, grâce à d'astucieuses redirections, ou bien via dig :

```
% dig +short ANY self.myresolver.info
2001:db8:1f10:3aa::2
```

Je continue à chercher. Si vous avez des idées...