RFC 4892 : Requirements for a Mechanism Identifying a Name Server Instance

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 22 juin 2007

Date de publication du RFC : Juin 2007

https://www.bortzmeyer.org/4892.html

Autrefois, tout était plus simple, les serveurs de noms DNS étaient simplement identifiables par leur adresse IP et on savait donc toujours à quel serveur on s'adressait. Mais un certain nombre d'innovations techniques assez récentes comme l'anycast ont rendu le déboguage plus difficile. D'où l'importance d'un nouveau mécanisme pour trouver à quel serveur on parle.

A priori, si je pose une question à 192.93.0.4, une et une seule machine peut répondre à la question posée, non ? Eh bien non, en raison de l'anycast (voir le RFC 4786 [1]) et des répartiteurs de charge. Plusieurs machines peuvent désormais se « cacher » derrière une même adresse. Normalement, on ne s'en aperçoit même pas mais, s'il y a un problème, par exemple si elles se désynchronisent, il est nécessaire de pouvoir déterminer à quelle machine physique on parle.

La méthode traditionnelle, popularisée par le logiciel BIND était d'utiliser une requête de la classe CH (pour CHAOS), classe inutilisée et donc disponible. Essayons sur f.root-servers.net, qui est anycasté :

```
% dig @f.root-servers.net CH TXT hostname.bind
...
;; ANSWER SECTION:
hostname.bind.          0       CH      TXT     "cdg1b.f.root-servers.org"
```

1. Pour voir le RFC de numéro NNN, https://www.ietf.org/rfc/rfcNNN.txt, par exemple https://www.ietf.org/rfc/rfc4786.txt

On voit qu'on est tombé sur l'instance parisienne de cette machine (l'ISC identifiant ses machines par le code à trois lettres de l'aéroport international le plus proche, ici Roissy / CDG).

Mais cette méthode, qui n'avait jamais été normalisée ou documentée a ses limites, que décrit notre RFC :

— Elle est spécifique, y compris dans son nom, à BIND (mais son concurrent NSD la met également en œuvre, vous pouvez tester avec `k.root-servers.net`, également anycasté et utilisant NSD).
— Et, surtout, elle nécessite une requête séparée, qui n'arrivera pas forcément au même serveur de noms que la requête originale (le routage ayant pu changer pendant ce temps).

Notre RFC pose donc le cahier des charges pour un remplaçant. Celui-ci devra :

— Garder une excellente propriété de la solution actuelle, le fait qu'elle fonctionne sur le DNS et ne nécessite donc pas d'ouvrir un nouveau port dans le coupe-feu ou d'installer un logiciel supplémentaire,
— Mais faire en sorte que l'identification du serveur passe désormais dans la même session.

Un projet existe déjà pour ce nouveau système, utilisant EDNS (RFC 6891). Adopté par l'IESG, il n'est pas encore publié en RFC.