Résolveur DNS : définition

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 11 mai 2020

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

Ce court article explique ce qu'est un **résolveur** DNS. Il existe plein de ressources en ligne sur le DNS mais très peu expliquent la différence cruciale entre un résolveur et un serveur faisant autorité.

Il y a en effet deux catégories de serveurs DNS. Ils sont tellement différents que c'est en général une mauvaise idée de dire « serveur DNS » tout court. Le **résolveur** est le serveur qu'interrogent directement les machines terminales (comme celle que vous touchez en ce moment, lorsque vous consultez cet article). Ces machines terminales ne parlent jamais directement aux serveurs faisant autorité <https://www.bortzmeyer.org/serveur-dns-faisant-autorite.html>, l'autre catégorie de serveurs DNS.

Comme c'est le serveur contacté pour toute résolution DNS, il est absolument critique : s'il tombe en panne <https://www.bortzmeyer.org/resolveur-dns-en-panne.html>, ce sera, pour la très grande majorité des activités, comme si on n'avait plus d'Internet du tout. S'il ment <https://www.bortzmeyer.org/censure-francaise.html>, il pourra emmener l'utilisateur où il veut. Et s'il capture des données, il peut avoir accès à énormément d'informations sur votre activité (cf. RFC 7626 [1]).

Notez que le résolveur est parfois appelé « serveur récursif » ou « serveur cache ».

Des exemples de résolveurs :

— Le cas le plus courant est celui où vous utilisez le résolveur fourni par votre FAI ou par le service informatique qui gère votre réseau d'accès à l'Internet.
— Mais il existe aussi des résolveurs DNS publics, dont les plus célèbres sont ceux des GAFA Google <https://www.bortzmeyer.org/google-dns.html> et Cloudflare. Les utiliser n'est pas forcément une bonne idée <https://www.bortzmeyer.org/dns-resolveurs-publics.html>.

1. Pour voir le RFC de numéro NNN, https://www.ietf.org/rfc/rfcNNN.txt, par exemple https://www.ietf.org/rfc/rfc7626.txt

— Vous pouvez parfaitement avoir votre propre résolveur DNS, pour un maximum de contrôle ; c'est ce qui arrive avec le Pi-hole mais cela peut se faire avec beaucoup d'autres logiciels libres comme Unbound ou Knot <https://www.knot-resolver.cz/>. Notez toutefois qu'aucune solution n'est parfaite <https://www.bortzmeyer.org/choix-resolveur-dns.html>.

Comment la machine terminale connait le résolveur à utiliser ? L'adresse IP du résolveur est apprise via des protocoles comme DHCP, mais peut aussi avoir été configurée statiquement, dans une base comme le fichier de configuration `/etc/resolv.conf` sur Unix. En pratique, ce n'est pas toujours trivial <https://www.bortzmeyer.org/changer-dns.html>.

Le résolveur ne connait quasiment aucune donnée au démarrage, il apprend petit à petit en contactant les serveurs faisant autorité <https://www.bortzmeyer.org/serveur-dns-faisant-autorite.html>.

Le résolveur, au milieu de la résolution DNS :

Notez que certains logiciels DNS permettent d'assurer les fonctions de résolveur et de serveur faisant autorité dans le même serveur. C'est en général une mauvaise idée <https://www.bortzmeyer.org/separer-resolveur-autorite.html>.

Et si vous êtes branché[Caractère Unicode non montré [2]]e technique, et que vous voulez interroger un résolveur directement, pour voir ce qu'il raconte ? Sur Unix, le logiciel dig permet de le faire. Si on n'indique pas explicitement un serveur, il interroge le résolveur par défaut de la machine, ici il a l'adresse IP `::1` (la ligne `SERVER`) :

```
% dig AAAA cyberstructure.fr
...
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 50365
;; flags: qr rd ra ad; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 1
...
;; ANSWER SECTION:
cyberstructure.fr. 82347 IN AAAA 2001:4b98:dc0:41:216:3eff:fe27:3d3f
...
;; Query time: 137 msec
;; SERVER: ::1#53(::1)
;; WHEN: Fri May 08 17:23:54 CEST 2020
;; MSG SIZE  rcvd: 251
```

On voit qu'on parle à un résolveur, et non pas à un serveur faisant autorité à deux détails :

— Dans les "*flags*", il y a le bit RA ("*Recursion Available*"), qui serait absent sur un serveur faisant autorité, qui aurait plutôt le bit AA.
— Le TTL n'est pas un chiffre rond, ce qui arrive lorsque la donnée était déjà dans la mémoire du résolveur.

Notez que la motivation originelle pour cet article était le désir de pouvoir parler de « résolveur » dans les articles de ce blog sans devoir l'expliquer à chaque fois, uniquement en mettant un lien. D'habitude, je résous le problème en mettant un lien vers Wikipédia <https://www.bortzmeyer.org/politique-liens-wikipedia.html> mais, ici, il n'existe pas de bon article Wikipédia sur la question. Je n'ai pas le courage de l'écrire, et surtout de le gérer par la suite, surtout face aux « corrections » erronnées. Mais, ce blog étant sous une licence libre, et compatible avec celle de Wikipédia, si vous souhaitez le faire, n'hésitez pas à copier/coller du texte.

2. Car trop difficile à faire afficher par LaTeX

”

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