Serveur DNS faisant autorité : définition

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 11 mai 2020

https://www.bortzmeyer.org/serveur-dns-faisant-autorite.html

Ce court article explique ce qu'est un serveur DNS **faisant autorité**. 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 **serveur faisant autorité** est le serveur qui stocke les données, qui seront récupérées via le protocole DNS. C'est pour cela qu'on dit qu'il « fait autorité » : par définition, ce qu'il dit est la vérité. Il n'est jamais interrogé par les machines des utilisateurs, mais il est questionné indirectement, par les serveurs de l'autre catégorie, les résolveurs <https://www.bortzmeyer.org/resolveur-dns.html>.

Les serveurs faisant autorité, et leur rôle dans la résolution DNS :

Un serveur faisant autorité ne fait pas autorité pour tous les noms de domaine, puisque le DNS est décentralisé. Il fait autorité pour une partie de l'arbre des noms de domaine. Par exemple :

- Les serveurs de l'AFNIC, l'organisation qui gère le TLD `.fr` font autorité pour `.fr`.
- Les serveurs faisant autorité pour les domaines du CNAM sont gérés par le service informatique du CNAM.
- Je gère moi-même la plupart des serveurs qui font autorité pour le domaine de ce blog, `bortzmeyer.org`.
- Les serveurs faisant autorité pour le Ministère des Armées français sont sous-traités à la société Orange (via la marque Oleane).

À noter qu'un serveur faisant autorité se dit en anglais "*authoritative server*", ce qu'on voit parfois bêtement traduit par « serveur autoritaire ». Non. Un adjudant est autoritaire, un serveur DNS fait autorité.

Si un serveur DNS faisant autorité est en panne, les autres serveurs faisant autorité pour la même zone (sous-arbre de l'arbre des noms de domaine) restent disponibles. Pour qu'une zone ne marche plus, il faut une panne de tous les serveurs faisant autorité (cf. la fameuse attaque contre Dyn, ou bien cette panne chez Microsoft <https://www.bortzmeyer.org/microsoft-dns-panne.html>). Mais cela n'affectera que les domaines hébergés sur ces serveurs, pas le reste du DNS.

Si vous êtes informaticien ou simplement intéressé par l'informatique, et que vous voulez monter des serveurs faisant autorité, il existe de nombreux logiciels libres pour cela, comme NSD ou Knot.

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>.

Où les serveurs faisant autorité trouvent-ils leurs données, celles qu'ils vont servir à tout les résolveurs <https://www.bortzmeyer.org/resolveur-dns.html> de la planète ? Cela dépend du serveur, c'est une décision locale. Il est courant de stocker les données dans un fichier de zone, dont la syntaxe absconse et pleine de pièges a souvent créé des problèmes :

```
$TTL 86400
@ IN  SOA ns4.bortzmeyer.org. hostmaster.bortzmeyer.org. (
        2020043001
        7200
        3600
        604800
        43200 )

  IN  NS  ns4.bortzmeyer.org.
  IN  NS  ns1.bortzmeyer.org.
  ...

  IN MX 0 mail.bortzmeyer.org.
  IN TXT  "v=spf1 mx ?all"

  IN TXT "My personal domain - Domaine personnel"

 IN CAA 0 issue "cacert.org"
 IN CAA 0 issuewild ";"
 IN CAA 0 issue "letsencrypt.org"

www   IN AAAA 2001:4b98:dc0:41:216:3eff:fe27:3d3f
www   IN AAAA 2605:4500:2:245b::42

mercredifiction  IN CNAME ayla
_443._tcp.mercredifiction IN TLSA 1 1 1 928dde55df4cd94cdcf998c55085fbb5228b561cc237a122d950260029c5b8c9
...
```

Mais d'autres méthodes existent, par exemple l'utilisation d'un SGBD.

Et si on veut continuer dans la technique et regarder les données d'un serveur faisant autorité ? Normalement, ils ne sont pas interrogés directement mais via les résolveurs. Ceci dit, les serveurs faisant autorité sont publics, et on peut, sur Unix, utiliser dig pour les interroger, en mettant le nom ou l'adresse IP du serveur après le signe @. Ici, on interroge un serveur de l'AFNIC sur le domaine `sante.gouv.fr` :

```
% dig @d.nic.fr A sante.gouv.fr
...
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 38097
;; flags: qr rd; QUERY: 1, ANSWER: 0, AUTHORITY: 6, ADDITIONAL: 6
;; WARNING: recursion requested but not available
...
;; AUTHORITY SECTION:
sante.gouv.fr. 172800 IN NS ns3.nameshield.net.
sante.gouv.fr. 172800 IN NS ns2.observatoiredesmarques.fr.
sante.gouv.fr. 172800 IN NS ns1.travail.gouv.fr.
```

```
sante.gouv.fr. 172800 IN NS ns1.sante.gouv.fr.
sante.gouv.fr. 172800 IN NS ns2.sante.gouv.fr.
sante.gouv.fr. 172800 IN NS a.ns.developpement-durable.gouv.fr.
...
;; Query time: 3 msec
;; SERVER: 2001:678:c::1#53(2001:678:c::1)
;; WHEN: Fri May 08 17:25:44 CEST 2020
;; MSG SIZE  rcvd: 326
```

La question posée au serveur `d.nic.fr`, qui fait autorité pour `.fr` était « quelle est l'adresse IPv4 de `sante.gouv.fr`? » Nous n'avons pas eu de réponse directe, car `d.nic.fr` fait autorité pour `.fr` mais pas pour `sante.gouv.fr` (rappelez-vous que le DNS est décentralisé). On a donc une délégation, `d.nic.fr` nous renvoie à six serveurs qui font autorité pour `sante.gouv.fr`. L'avertissement « "*recursion requested but not available*" » est normal, s'agissant d'un serveur faisant autorité, pas d'un résolveur (les résolveurs sont également appelés serveurs récursifs).

Au passage, cela me permet d'expliquer comment on trouve les serveurs faisant autorité pour une zone donnée : le DNS utilise le DNS pour son propre fonctionnement. Une requête de type NS ("*Name Servers*") permet de trouver les serveurs, ici, ceux faisant autorité pour `.fi` (j'ai pensé à ce TLD car je venais de lire des récits de randonnée en Finlande <`https://sgurrthuilm.wordpress.com/2020/05/04/randonnee-laponie-4/`>):

```
% dig NS fi
...
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 7282
;; flags: qr rd ra ad; QUERY: 1, ANSWER: 9, AUTHORITY: 0, ADDITIONAL: 1
...
;; ANSWER SECTION:
fi. 86400 IN NS e.fi.
fi. 86400 IN NS b.fi.
fi. 86400 IN NS a.fi.
fi. 86400 IN NS h.fi.
fi. 86400 IN NS i.fi.
fi. 86400 IN NS f.fi.
fi. 86400 IN NS d.fi.
fi. 86400 IN NS g.fi.
fi. 86400 IN NS c.fi.

;; Query time: 176 msec
;; SERVER: ::1#53(::1)
;; WHEN: Fri May 08 18:42:25 CEST 2020
;; MSG SIZE  rcvd: 175
```

On a vu plus haut que demander des informations sur `sante.gouv.fr` à un serveur qui fait autorité pour `.fr` renvoie une délégation. Si on suit cette délégation et qu'on pose la même question à un serveur qui fait autorité pour `sante.gouv.fr`, on a notre réponse :

```
% dig @a.ns.developpement-durable.gouv.fr. A sante.gouv.fr
...
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 15886
;; flags: qr aa rd; QUERY: 1, ANSWER: 1, AUTHORITY: 6, ADDITIONAL: 5
;; WARNING: recursion requested but not available
```

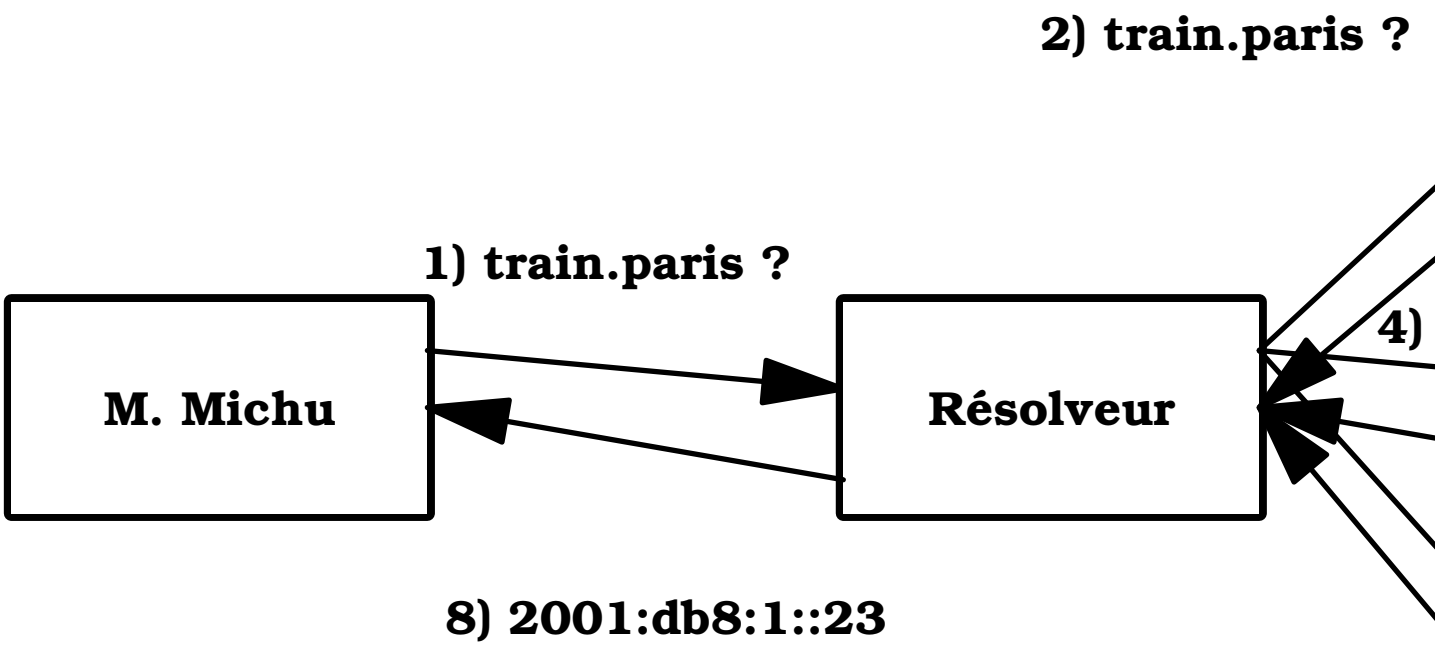
```
;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;sante.gouv.fr. IN A

;; ANSWER SECTION:
sante.gouv.fr. 600 IN A 213.162.60.164
...
;; Query time: 25 msec
;; SERVER: 194.5.172.19#53(194.5.172.19)
;; WHEN: Fri May 08 17:26:21 CEST 2020
;; MSG SIZE  rcvd: 298
```

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

— Dans les "*flags*", il y a le bit AA ("*Authoritative Answer*"), qui serait absent sur un résolveur, qui aurait plutôt le bit RA.
— Le TTL est un chiffre rond.

Notez que la motivation originelle pour cet article était le désir de pouvoir parler de « serveur faisant autorité » 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.



https://www.bortzmeyer.org/serveur-dns-faisant-autorite.html