

Des services de DNS secondaires gratuits

Stéphane Bortzmeyer

<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 30 août 2024. Dernière mise à jour le 3 septembre 2024

<https://www.bortzmeyer.org/dns-secondaire.html>

Pour des raisons de robustesse, il est fortement recommandé d'avoir plusieurs serveurs faisant autorité <<https://www.bortzmeyer.org/serveur-dns-faisant-autorite.html>> pour une zone DNS. Mais ce n'est pas tout : il faut aussi de la diversité, pour éviter que la même cause ne rende plusieurs serveurs injoignables. Il est donc très souhaitable d'avoir des serveurs secondaires en dehors de son réseau habituel. Si on est une grosse organisation, il existe des offres commerciales pour cela. Et si on est une petite organisation, avec peu de moyens ? Des solutions existent quand même.

Un nombre important de serveurs faisant autorité <<https://www.bortzmeyer.org/serveur-dns-faisant-autorite.html>> est certes souhaitable (la résolution doit toujours fonctionner même si un serveur est en panne) mais il vaut encore mieux qu'ils soient divers. Si on a quatre serveurs (un bon nombre) mais qu'ils sont dans la même armoire, ou alimentés par le même système électrique, ou routés ensemble par le même AS, ces quatre serveurs vivent sous la menace d'un SPOF : une panne peut les planter tous les quatre.

La solution est donc d'avoir des serveurs secondaires, qui iront récupérer les données sur le serveur primaire (d'où le terme de serveurs esclaves, que l'on trouve par exemple dans les fichiers de configuration de certains logiciels). Mais pour avoir le maximum de diversité, il vaut mieux qu'ils soient routés via des AS différents, et même qu'ils soient gérés par des organisations différentes. On peut toujours demander à des copains ou copines d'héberger de tels secondaires (le DNS fonctionnait souvent comme cela au début). Mais si on n'a pas de copines ou copains qui fournissent ce service ? Alors, il y a plusieurs solutions gratuites :

- [puck.nether.net](https://puck.nether.net/dns) <<https://puck.nether.net/dns>>.
- NS-Global <<https://www.ns-global.zone/signup/>>. L'utilisation est originale : vous n'avez pas de compte, vous configurez votre primaire et demandez ensuite le service.
- 1984 Hosting <<https://1984.hosting/product/freedns/>>.
- Hurricane Electric <<https://dns.he.net/>>.
- FreeDNS 42 <<https://freedns.42.pl/>>.
- FreeDNS <<https://freedns.afraid.org/>> (sans lien avec le précédent) : je trouve l'utilisation très peu claire (heureusement que Jean-Philippe Pick m'a aidé). Il faut aller dans la section "Backup DNS" et suivre les instructions <<https://freedns.afraid.org/secondary/instructions.php>>.

- Certains bureaux d'enregistrement fournissent un service de secondaire mais uniquement si le domaine est enregistré chez eux.

Pour tous ces services, quelques points à garder en tête :

- Cela va de soi mais je le répète quand même : il faut avoir un serveur primaire que vous gérez vous-même. Cet article ne parle que de trouver des secondaires.
- Il s'agit à chaque fois de services gratuits, qui font au mieux, mais qui ne peuvent pas fournir une fiabilité de 100 % (mais, comme souvent avec les services créés par des passionné-es, cela marche souvent mieux que les services commerciaux et le support répond plus vite et plus sérieusement). Soyez gentil-les avec leurs administrateurices.
- Si vous vous inquiétez pour l'intégrité de vos données DNS (qui nous dit que ces administrateurices ne vont pas subrepticement modifier les enregistrements?), signez avec DNSSEC. De toute façon, signez avec DNSSEC.
- Tous ces services fournissent ce qu'il faut pour DNSSEC mais vérifiez quand même. Et, bien sûr, c'est vous qui êtes responsable de la supervision.
- Si vous vous inquiétez pour la confidentialité des requêtes (pas des données, qui sont publiques, mais des requêtes), vous avez raison de vous inquiéter. Si vous ne vous inquiétez pas, lisez le RFC 7626¹. DNSSEC ne traite pas ce problème.

Outre les copains et copines, outre les services gratuits comme ceux cités ici, on peut aussi recourir aux services de gens de son écosystème professionnel ou associatif. Ainsi, les services publics ne devraient pas hésiter à échanger des services de DNS secondaire (ils ne sont pas concurrents, après tout), mais on constate que ce n'est pas le cas, les rendant vulnérables aux pannes et aux attaques par déni de service <<https://www.bortzmeyer.org/service-public-impots-dns.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>