Un service d'hébergement de zones DNS accessible au[Caractère Unicode non montré *]à la non-geek ?

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 3 novembre 2018. Dernière mise à jour le 17 mai 2021

https://www.bortzmeyer.org/hebergement-dns-chaton.html

Dans cet article, je ne vais pas décrire un logiciel ou service existant, ni résumer un RFC. Je voudrais au contraire pointer du doigt un manque dans l'offre existante, à la fois l'offre de services non-commerciaux accessibles au[Caractère Unicode non montré]à la non-geek, et l'offre de logiciel libre. Pourquoi n'y a-t-il pas de système simple pour héberger une zone DNS ? Et, si un[Caractère Unicode non montré]e militant[Caractère Unicode non montré]e de la liberté sur Internet passe par là, ne serait-ce pas une bonne idée d'en créer un ? J'espère que cet article donnera des idées.

Un peu de contexte d'abord. Le DNS est à la base de quasiment toutes les transactions sur l'Internet. Si on se soucie de la liberté et de l'indépendance de l'utilisateur qui veut publier quelque chose, et pas être un[Caractère Unicode non montré]e simple consommat[Caractère Unicode non montré]eur[Caractère Unicode non montré]rice, avoir un nom de domaine à soi est crucial. Acheter/louer un tel nom est simple et peu coûteux (encore qu'il semble qu'il n'existe que très peu, voire pas du tout, de bureaux d'enregistrement non-commerciaux). L'héberger est une autre histoire. L'hébergeur DNS (qui n'est **pas** forcément le bureau d'enregistrement) joue un rôle crucial. S'il est en panne, plus rien ne marche. S'il enregistre les données, la vie privée est menacée (sur ce risque, voir le RFC 7626 [1]). Il faut donc le choisir avec soin.

Or, beaucoup de titulaires de nom de domaine choisissent une entreprise (par exemple Cloudflare) un peu au hasard, sans avoir étudié ses pratiques. Il serait évidemment préférable de faire héberger ses serveurs de noms dans un endroit plus sûr.

Un solution geek existe pour cela, l'auto-hébergement des serveurs de noms. Ce n'est pas très compliqué (un logiciel libre comme nsd fait cela très bien) et cela ne demande que peu de ressources (un

*Car trop difficile à faire afficher par LaTeX

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

serveur DNS ne représente que peu de trafic, un Raspberry Pi connecté en ADSL suffit largement pour la plupart des zones, d'autant plus que le vrai serveur primaire n'a pas forcément besoin d'être accessible de tout l'Internet, il peut être caché, visible uniquement des secondaires). Si on veut améliorer les choses, on peut demander à des cop[Caractère Unicode non montré]ain[Caractère Unicode non montré]ine[Caractère Unicode non montré]s d'héberger un serveur secondaire de sa zone. C'est ainsi qu'est hébergée la zone DNS de ce blog, `bortzmeyer.org`.

Mais, évidemment, c'est uniquement une solution pour geek. On ne peut pas demander à toute personne qui publie sur Internet de configurer nsd ou Knot même si, je le répète, c'est relativement simple. Et il faudrait en plus éditer son fichier de zone DNS avec un éditeur de texte, ce qui n'enchante pas le non-geek. Or, la liberté d'expression ne doit pas être réservée aux informaticiens !

Il faudrait donc une solution pour ces utilisateurices. Il y a deux moyens de fournir cette solution, via un **service** ou via un **logiciel**. Concentrons-nous d'abord sur les services car, même s'il existait un logiciel tout fait, libre et tout, il resterait à gérer l'administration quotidienne du serveur, et un serveur DNS fait parfois face à des problèmes (voir plus loin dans cet article le problème des dDoS). Des services pour M. ou Mme Toutlemonde, libres, éthiques, non-commerciaux et le reste, existent, ce sont par exemple les CHATONS <`https://chatons.org/`>, dont le plus connu est Framasoft. Mais, à l'heure actuelle, à ma connaissance, aucun CHATON ne propose d'hébergement DNS.

Esquissons brièvement le cahier des charges d'un tel service :

— Utilisable indépendamment d'autres services (comme l'hébergement Web),
— Permet aux internautes de s'inscrire, puis de donner une liste de domaines qu'ils souhaitent voir gérés par le service,
— Permet de gérer le contenu de la zone DNS, en indiquant différents enregistrements, de tous les types possibles, avec leurs valeurs. L'interface proposée doit être simple d'usage, sans limiter les possibilités. Tous les hébergeurs DNS ont aujourd'hui une telle interface, typiquement via le Web et parfois via une API en prime.
— Raisonnablement sécurisé, car il ne faut pas qu'un utilisateur puisse modifier le domaine d'un autre !
— Ne réinventant pas la roue, donc reposant sur un logiciel de serveur DNS faisant autorité qui soit stable et sérieux comme nsd ou Knot.
— D'un point de vue de l'utilisateur, il serait bon d'avoir un mode simple, où on donne juste l'adresse IP du serveur Web, avec des modes plus avancés pour les utilisateurs qui ne se contentent pas d'un site Web.
— D'un point de vue politique, certains peuvent aussi souhaiter pouvoir maîtriser où sont situés les serveurs faisant autorité (on peut vouloir éviter tel ou tel pays, et migrer facilement),
— D'un point de vue plus technique, il faudrait DNSSEC (passage des enregistrements DS mais, surtout, gestion des clés et signatures par l'hébergeur), les mises à jour dynamiques du RFC 2136 (mais une bonne API peut les remplacer).

Un tel service, à ma connaissance, n'existe pas aujourd'hui dans le monde associatif. Il faut dire qu'il existe quelques risques :

— Le service pourrait être confronté à des menaces juridiques (la liberté d'expression ne plait pas à tout le monde), venant par exemple d'ayant-trop-de-droits si on héberge une zone DNS comme celle de Sci-Hub, ou bien venant d'adversaires politiques (cf. le cas d'IndyMedia <`https://nantes.indymedia.org/articles/38602`>),
— Tout le monde ne croit pas à l'état de droit et donc les menaces pourraient être suivies, voire précédées d'attaques par déni de service. L'exemple de Dyn ou bien celui du domaine national turc <`https://www.dailydot.com/layer8/turkey-ddos-attack-tk-universities/`> invitent à être prudent. Un hébergement DNS sympa fait par deux-trois potes pourrait ne pas résister à une dDoS un peu sérieuse.

— L'attaque par déni de service n'est pas la seule menace. Il existe aussi le risque de détournement du nom, comme c'était arrivé à Wikileaks <https://www.bortzmeyer.org/observations-wikileaks.html> et à beaucoup d'autres. Bien sûr, si le détournement avait exploité une faute de l'utilisateur, le logiciel n'y peut pas grand'chose. Mais certains détournements étaient dus à une faille de sécurité du logiciel.

On peut citer quelques services possibles qui se rapprochent de ce but :

— Le plus connu est Xname <http://xname.org/>, dont la documentation est très complète, mais il est apparement abandonné (aucune nouvelle depuis 2013). Je teste et "*Error : bad zone name example.com*". Donc, cela ne semble pas marcher. Le service semble vraiment mort, d'autant plus que leur propre zone est pleine d'erreurs <https://gist.github.com/bortzmeyer/a9d905d1e899af3e5c3c0e3665788c7d>.
— J'ai essayé de tester NetLibre <http://netlib.re/>. Il ne fournit pas d'hébergement sec, il faut utiliser NetLibre pour acquérir son nom (pour lequel on n'a donc pas un choix complet, on est limité aux domaines de NetLibre). C'est donc plutôt l'équivalent de `eu.org`, avec hébergement en plus. De toute façon, le service semble peu maintenu : "*Oh ! Une erreur est survenue. scp failed : unable to fork ssh master : Cannot allocate memory at /home/ppittoli/dnsmanager/bin/../lib/copycat.pm line 35*" (et la seule adresse de contact est sur IRC).
— Le service Free DNS <http://freedns.afraid.org/> est franchement trop compliqué pour moi. Je n'ai tout simplement pas compris ce qu'on pouvait faire avec, et comment s'en servir (mon domaine est marqué comme "*BROKEN*" et la FAQ est incompréhensible <http://freedns.afraid.org/faq/#11>, et fausse quand elle prétend " *The central authority for all domains on the Internet is ICANN*").
— On m'a cité `nohost.me`, mais, si j'ai bien compris, c'est utilisable uniquement depuis YunoHost.

Cela, c'était pour un service en ligne. Et un logiciel ? Je vois deux cas d'usage :

— Pour ce[Caractère Unicode non montré]ux[Caractère Unicode non montré]elles qui ne font confiance à personne, et/ou ne veulent dépendre de personne. Le logiciel n'a alors pas besoin d'avoir la notion de comptes ou d'utilisateur, puisqu'il n'existe qu'un[Caractère Unicode non montré]e utilisat[Caractère Unicode non montré]eur[Caractère Unicode non montré]rice.
— Pour ce[Caractère Unicode non montré]ux[Caractère Unicode non montré]elles qui veulent faire essaimer le service. (Dans ce cas, le logiciel pourrait être utilisé par l'éventuel service public, puis par ses "*spin-offs*".)

Ce doit être bien sûr un logiciel libre, qui doit pouvoir être installé relativement facilement, et fournir le service décrit ci-dessus. Pour le premier cas d'usage, le cas individuel, il serait peut-être encore mieux qu'il soit intégré à une plate-forme comme Cozy. Là encore, à ma connaissance, un tel logiciel n'existe pas (il existe plusieurs trucs plus ou moins bricolés, pas évidents à installer sur sa machine, et encore moins à maintenir).

Les logiciels existants qui pourraient servir d'inspiration :

— DNS zones manager <https://github.com/KaneRoot/dnsmanager>, le logiciel derrière NetLib.re. Je n'ai pas réussi à l'installer <https://github.com/KaneRoot/dnsmanager/issues/16> (`perlbrew install perl-5.18.0` donne « "*ERROR : Failed to download http ://www.cpan.org/authors/id/R/RJ/RJBS/perl-5.18.0.tar.bz2*" », il faut manifestement des compétences Perl plus pointues que les miennes.)
— Il existe des logiciels bien plus génériques que des seuls gestionnaires de zones DNS, qui pourraient servir de point de départ. C'est le cas de ISPConfig ou Webmin, par exemple.

Mais notez bien que le logiciel ne résout qu'une partie du problème : il faut encore les serveurs. C'est pour cela que je pense que la solution « service hébergé » est plus adaptée aux non-geeks.

Notons enfin qu'un service limité, qui ne fournisse que le serveur secondaire, charge à l'utilisateur d'avoir son propre primaire, serait déjà très utile. Là encore, il me semble qu'il n'existe rien de tel. Peut-être :

— Puck <https://puck.nether.net/dns/>. L'interface est vraiment rude (elle n'indique même pas quelle est l'adresse IP à autoriser, il faut regarder son journal !) mais ça marche bien. (Pensez à mettre ensuite `puck.nether.net` dans l'ensemble des enregistrements NS.)
— Au Danemark, il y a GratisDNS <https://web.gratisdns.dk/>, depuis 1999 (documentation uniquement en danois.)

— EntryDNS <https://entrydns.net> faisait un service gratuit, mais il est désormais arrêté et remplacé par un service payant (mais très bon marché).

Je serai ravi d'apprendre que j'ai mal cherché et qu'un tel service ou un tel logiciel existent. N'hésitez pas à me le faire savoir. Et, si je ne me suis pas trompé, si un[Caractère Unicode non montré]e courageu[Caractère Unicode non montré]x[Caractère Unicode non montré]se pouvait le réaliser…

La partie « interface de gestion du contenu » est traitée par le très prometteur projet happyDNS <https://www.bortzmeyer.org/happydns.html> (mais pas encore la partie « hébergement »). Il existe aussi le service d'hébergement deSEC <https://desec.io/>, qui semble très bien, il fait l'hébergement et l'avitaillement (avec interface de gestion du contenu), mais pas la gestion d'un serveur secondaire, il faut complètement leur déléguer sa zone. (La question est discutée <https://talk.desec.io/t/dns-slave-support/41>.)