Avoir son propre résolveur DNS ?

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 4 décembre 2013

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

Faut-il avoir son propre résolveur DNS, sur sa machine (ou, au moins, sur son réseau local à soi) ? Question compliquée à laquelle je réponds désormais **oui**, en raison de l'intensification de la censure utilisant le DNS.

D'abord, un petit rappel : la quasi-totalité des activités sur l'Internet commencent par une requête DNS, une demande faite au **résolveur <https://www.bortzmeyer.org/resolveur-dns.html>** DNS par les applications « quelle est l'adresse IP de www.slate.fr ? » Le résolveur, après interrogation des **serveurs DNS faisant autorité <https://www.bortzmeyer.org/serveur-dns-faisant-autorite.html>** (gérés, dans le cas de ce nom de domaine, par la racine, par l'AFNIC et par Slate), va répondre aux applications et le reste de l'activité Internet pourra continuer. Comme tout commence par le DNS, ce service est particulièrement tentant pour tous ceux qui veulent censurer / dévier / détourner les activités de l'utilisateur. Il y a donc une histoire déjà ancienne de tentatives de filtrage via le DNS <https://www.bortzmeyer.org/dns-filtering.html> et une histoire tout aussi ancienne de textes expliquant pourquoi c'est une très mauvaise idée <http://www.afnic.fr/fr/l-afnic-en-bref/actualites/actualites-generales/6573/show/le-conseil-scientifique-de-l-afnic-partage-sur-html>. Le filtrage via le DNS peut se faire dans le réseau, comme en Chine <https://www.bortzmeyer.org/detournement-racine-pekin.html>. Mais le plus courant est de le faire dans le résolveur. Cette machine est typiquement gérée, pour un accès Internet par un particulier, par son FAI. En raison de la concentration du marché, en contraignant les quatre ou cinq plus gros FAI à effectuer ce filtrage, on pourrait frapper un bon nombre des MM. Michu. Techniquement, c'est simple à faire, avec des systèmes comme RPZ <https://www.bortzmeyer.org/rpz-faire-mentir-resolveur-dns.html>. Et cette voie a déjà été suivie, en France par l'ARJEL <https://www.bortzmeyer.org/arjel.html>.

Une solution évidente à ce filtrage est d'avoir son propre résolveur DNS, de ne plus compter sur celui du FAI. Cette solution a deux défauts, le premier est temporaire : sa mise en œuvre est encore trop complexe, comme déjà expliqué dans un de mes articles <https://www.bortzmeyer.org/changer-dns.html>. La deuxième est moins visible : si chaque utilisateur de l'Internet a son propre résolveur DNS, ils ne partageront plus leur mémoire (leur « cache ») et la charge sur les serveurs faisant autorité s'aggravera. Pour cette raison, je prônais plutôt des systèmes comme dnssec-trigger <https://www.bortzmeyer.org/dnssec-trigger.html> qui installaient un résolveur local mais faisaient

suivre les requêtes non résolues aux résolveurs (et donc aux caches) des FAI. C'est une solution simple et élégante (et qui permettait aussi de faire de la validation DNSSEC <https://www.bortzmeyer.org/ou-valider-dnsssec.html> proprement).

Mais dnssec-trigger a une limite. Certes, avant d'utiliser les résolveurs du réseau local comme relais, il les teste pour s'assurer qu'ils transmettent les données DNSSEC correctement. Mais il ne teste pas s'ils mentent ou pas <https://www.bortzmeyer.org/dns-menteur.html>. Si le résolveur officiel du réseau local applique la censure, dnssec-trigger ne pourra plus accéder aux données (si DNSSEC est utilisé, on aura un code d'erreur, SERVFAIL, plutôt qu'une réponse mensongère comme l'adresse IP 127.0.0.1 dans l'exemple ci-dessous, mais cela ne change pas grand'chose ; DNSSEC protège contre le détournement, pas contre le déni de service qu'est la censure).

Or, l'usage du DNS pour la censure se répand. Ainsi, le 28 novembre 2013, un tribunal français a ordonné la censure par le DNS <http://pro.clubic.com/legislation-loi-internet/telechargement-il actualite-604000-allostreaming-consorts-justice-ordonne-blocage.html> de sites Web de diffusion de films. Et cette censure semble effectivement appliquée. En testant depuis un très gros FAI français, avec dig :

```
% dig +short @192.168.2.254 A alloshare.com
127.0.0.1
```

Or, cette adresse IP bidon (127.0.0.1 désigne la machine locale, donc ce mensonge renvoie votre navigateur Web vers votre machine) n'est pas la vraie. Avec mon résolveur personnel :

```
% dig +short A alloshare.com
204.236.239.5
```

Cela vous semble exagéré de parler de censure, pour une affaire essentiellement commerciale (les intérêts des ayant-trop-de-droits) ? Sauf que cela commence comme ça <https://hackurx.wordpress.com/2013/11/29/ca-commence-comme-ca/> puis, une fois que l'outil est au point, on pourra de la même façon demander la censure de n'importe quel nom qui déplait aux autorités. Il est donc normal que les citoyens se détournent des résolveurs DNS menteurs et veuillent configurer leur propre résolveur.

La situation technique n'est pas aujourd'hui tellement meilleure qu'à l'époque de mon précédent article sur le changement de résolveur <https://www.bortzmeyer.org/changer-dns.html>. Mais le problème devenant plus crucial, il faut quand même se lancer.

Donc, d'abord, pour les systèmes que je connais le mieux, les Unix. Il faut 1) installer le logiciel résolveur 2) configurer la machine pour l'utiliser et surtout 3) faire en sorte que DHCP ne vienne pas écraser ce réglage. Pour le logiciel résolveur, on a plusieurs choix, notamment BIND et Unbound, disponibles sous forme de paquetage dans n'importe quel Unix. Un exemple de configuration BIND pour un résolveur, validant avec DNSSEC pendant qu'on y est :

```
options {
// N'écouter que sur l'interface locale. Autrement, faites
// attention à interdire l'accès aux machines non-locales, pour
// ne pas faire un résolveur ouvert.
        listen-on {127.0.0.1;};
        dnssec-enable yes;
        dnssec-validation yes;
};
trusted-keys {
           "." LA CLÉ DNSSEC DE LA RACINE EST EN GÉNÉRAL DISTRIBUÉE AVEC BIND (fichier bind.keys)
};
```

Et pour Unbound :

```
server:
    interface: 127.0.0.1
    auto-trust-anchor-file: "/var/lib/unbound/root.key"
```

Pour récupérer de manière sûre la clé de la racine avec Unbound, le plus simple est un `unbound-anchor -a "/var/lib/unbound/root.key"`. Une fois le résolveur démarré, testez avec dig qu'il peut résoudre les noms :

```
% dig @127.0.0.1 A www.techn0polis.net
...
;; flags: qr rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 1
...
;; ANSWER SECTION:
www.techn0polis.net. 2917 IN CNAME gpaas6.dc0.gandi.net.
gpaas6.dc0.gandi.net. 1156 IN A 217.70.180.136
...
;; SERVER: 127.0.0.1#53(127.0.0.1)
...
```

Testez aussi depuis des machines extérieures que votre résolveur ne répond **pas** aux machines extérieures. Autrement, c'est un résolveur ouvert <https://www.bortzmeyer.org/fermer-les-recursifs-ouverts.html>, ce qui est très dangereux. Si vous voulez rendre accessible votre joli résolveur depuis tout votre réseau local, vous devez également écouter sur les adresses IP du réseau local (et bien utiiser le contrôle d'accès de votre serveur - `acl` dans BIND et `access-control:` dans Unbound - pour ne pas devenir un résolveur ouvert).

Une fois que c'est fait, configurez votre machine pour interroger le serveur/résolveur en question. Mais attention, le problème est que DHCP vient souvent dans votre dos changer ce réglage. Donc, simplement éditer `/etc/resolv.conf`, comme on le lit parfois sur des forums de neuneus, n'est pas suffisant. Il faut modifier la configuration du client DHCP. Cela dépend du client mais, par exemple, sur une Debian, éditer `/etc/resolvconf/resolv.conf.d/head` pour y mettre :

```
nameserver 127.0.0.1
```

suffit. Une fois que c'est fait, vous pouvez tester avec dig sans indiquer `@127.0.0.1` et la ligne `SERVER` dans la sortie doit vous indiquer quel serveur vous utilisez.

Pour Mac OS X, je n'ai pas d'expérience de ce système mais je suggère l'article de hukl <http://smyck.net/2010/12/30/your-own-dns-server/>. Sinon, Ludovic Hirlimann propose « installer MacPorts puis `sudo port install unbound` et c'est tout ». Experts OS X, si vous avez d'autres idées ?

Et pour Windows ? Apparemment, Unbound tourne sur Windows (si quelqu'un a une expérience d'utilisation à raconter...) Je ne connais pas assez Windows pour le reste mais je vous suggère une solution pour la partie « configurer sa machine pour accéder au résolveur local ». Un certain nombre de services commerciaux vous fournissent des résolveurs alternatifs, pour accéder plus rapidement à certains services bridés comme YouTube <https://www.bortzmeyer.org/debrider-avec-dns.html>. Je ne vous dis pas d'utiliser ces résolveurs, qui sont aussi menteurs (même si c'est pour la bonne cause)

mais tous viennent avec une documentation, conçue pour un large public, indiquant comment changer de résolveur. Par exemple, c'est le cas de la documentation de Unlocator <https://unlocator.com/setup/>.

Enfin n'oubliez pas que, si vous avez plusieurs machines sur votre réseau local, il n'est pas nécessaire qu'elles aient toutes leur propre résolveur, vous pouvez mettre un seul résolveur partagé.

Quelle sera la prochaine étape de la course aux armements entre les censeurs et les utilisateurs de l'Internet ? Peut-être d'essayer de faire filtrer le port 53 <https://www.bortzmeyer.org/port53-filtre.html>. En attendant, voici d'autres documents sur le thème de cet article :

— Installation et configuration de Unbound <https://calomel.org/unbound_dns.html>.
— Configuration d'Unbound sur Slackware <http://www.ellendhel.net/article.php?ref=2011+10+20-0> (en français)
— Unbound, notamment sur Windows <http://korben.info/installer-serveur-dns-unbound.html>