RFC 8198 : Aggressive Use of DNSSEC-Validated Cache

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 26 juillet 2017

Date de publication du RFC : Juillet 2017

https://www.bortzmeyer.org/8198.html

Lorqu'un client DNS interroge un résolveur, celui-ci peut répondre très vite si l'information demandée est dans sa mémoire (son « "*cache*" ») mais cela peut être beaucoup plus lent s'il faut aller demander aux serveurs faisant autorité. Il est donc essentiel, pour les performances du DNS, d'utiliser le cache le plus possible. Traditionnellement, le résolveur n'utilisait le cache que si la question posée par le client avait une réponse **exacte** dans le cache. Mais l'arrivée de DNSSEC autorise un usage plus **énergique** et plus efficace du cache : ce nouveau RFC permet aux résolveurs de **synthétiser** des réponses à partir des informations DNSSEC.

Comment peut-il faire ? Eh bien prenons par exemple les enregistrements NSEC. Ils indiquent une plage où il n'y a pas de noms enregistrés. Ainsi, si une zone `example.com` contient :

```
albatross IN AAAA 2001:db8:1028::a:1
elephant  IN AAAA 2001:db8:1028::a:2
zebra     IN AAAA 2001:db8:1028::a:3
```

Sa signature DNSSEC va ajouter des enregistrements NSEC, notamment :

```
albatross.example.com. IN NSEC elephant.example.com. AAAA
```

qui veut dire qu'il n'y a pas de nom entre `albatross` et `elephant`. Si le client interroge le résolveur à propos de `cat.example.com`, le résolveur ira voir les serveurs faisant autorité, il aura une réponse négative (NXDOMAIN, ce nom n'existe pas) et l'enregistrement NSEC. Les deux informations seront renvoyées au client, et pourront être mémorisées dans le cache. Maintenant, si le client demande `dog.example.com`, les résolveurs traditionnels retourneront demander aux serveurs faisant autorité. Alors que les résolveurs modernes, conformes à ce nouveau RFC 8198 [1], pourront déduire du NSEC que `dog.example.com` n'existe pas non plus, et immédiatement générer un NXDOMAIN pour le client. Cela fera gagner du temps et des efforts à tout le monde. (Les règles exactes sont dans la section 5.1 de notre RFC.)

La règle (désormais dépassée) comme quoi le résolveur ne peut répondre immédiatement que s'il a l'information correspondant à la question exacte est spécifiée dans le RFC 2308, pour le cache négatif (mémoriser les réponses NXDOMAIN). Désormais, elle n'est plus obligatoire si (**et seulement si**, voir section 9) le résolveur valide avec DNSSEC, **et** si la zone est signée (aucun changement si elle ne l'est pas). Outre le cas simple de NSEC avec des réponses négatives, présenté plus haut, il y a deux cas plus complexes, les enregistrements NSEC3, et les jokers. Si la zone est signée avec NSEC3 au lieu de NSEC, les enregistrements NSEC3 indiqueront des condensats et pas des noms et le résolveur devra donc condenser le nom demandé, pour voir s'il tombe dans un NSEC3 connu, et si on peut synthétiser le NXDOMAIN. Les règles exactes sur les NSEC3 sont dans le RFC 5155 (attention, c'est compliqué), sections 8.4 à 8.7, et dans notre RFC, section 5.2. Évidemment, si la zone est signée avec l'option « *"opt-out"* » (c'est le cas de la plupart des TLD), le résolveur ne peut pas être sûr qu'il n'y a pas un nom non signé dans une plage indiquée par un enregistrement NSEC, et ne peut donc pas synthétiser. Tout aussi évidemment, toute solution qui empêchera réellement l'énumération des noms dans une zone signée (comme le projet, désormais abandonné, NSEC5) sera incompatible avec cette solution.

Si la zone inclut des jokers (RFC 1034, section 4.3.3), par exemple `example.org` :

```
avocado   IN A 192.0.2.1
*         IN A 192.0.2.2
zucchini IN A 192.0.2.3
```

Alors, le résolveur pourra également synthétiser des réponses positives. S'il a déjà récupéré et mémorisé le joker, et que le client lui demande l'adresse IPv4 de `leek.example.org`, le résolveur pourra tout de suite répondre `192.0.2.2`. (J'ai simplifié : le résolveur doit aussi vérifier que le nom `leek.example.org` n'existe pas, ou en tout cas n'a pas d'enregistrement A. Le joker ne masque en effet pas les noms existants. Détails en section 5.3 du RFC.)

Pour cette utilisation plus énergique de la mémoire d'un résolveur validant, il a fallu amender légèrement le RFC 4035, dont la section 4.5 ne permettait pas cette synthèse de réponses (la nouvelle rédaction est en section 7). Notez un inconvénient potentiel de cette synthèse : un nom ajouté ne sera pas visible tout de suite. Mais c'est de toute façon une propriété générale du DNS et de ses caches souvent appelée, par erreur, « durée de propagation `<https://www.bortzmeyer.org/dns-propagation.html>` ».

La durée exacte pendant laquelle le résolveur « énergique » pourra garder les informations qui lui servent à la synthèse des réponses est donnée par le TTL des NSEC.

1. Pour voir le RFC de numéro NNN, `https://www.ietf.org/rfc/rfcNNN.txt`, par exemple `https://www.ietf.org/rfc/rfc8198.txt`

Quel intérêt à cette synthèse énergique de réponses ? Comme indiqué plus haut, cela permet de diminuer le temps de réponse (section 6). Du fait de la diminution de nombre de questions à transmettre, cela se traduira également par une diminution de la charge, et du résolveur, et du serveur faisant autorité. Sur la racine du DNS, comme 65 % des requêtes entrainent un NXDOMAIN (voir par exemple les statistiques de A-root <http://a.root-servers.org/metrics/index.html>), le gain devrait être important. Un autre avantage sera pour la lutte contre les attaques dites « random QNAMEs » lorsque l'attaquant envoie plein de requêtes pour des noms aléatoires (générant donc des NXDOMAIN). Si l'attaquant passe par un résolveur, celui-ci pourra écluser la grande majorité des requêtes sans déranger le serveur faisant autorité.

Mais la synthèse énergique entraine aussi un gain en matière de vie privée (cf. RFC 7626) : les serveurs faisant autorité verront encore moins de questions.

Cette technique de « cache négatif énergique » avait été proposée pour la première fois dans la section 6 du RFC 5074. Elle s'inscrit dans une série de propositions visant à augmenter l'efficacité des caches DNS, comme le « "*NXDOMAIN cut*" » du RFC 8020. La synthèse énergique de réponses prolonge le RFC 8020, en allant plus loin (mais elle nécessite DNSSEC).

Il semble que Google Public DNS <https://www.bortzmeyer.org/google-dns.html> mette déjà en œuvre une partie (les réponses négatives) de ce RFC, mais je n'ai pas encore vérifié personnellement.