RFC 9567 : DNS Error Reporting

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 27 avril 2024

Date de publication du RFC : Avril 2024

https://www.bortzmeyer.org/9567.html

Lorsqu'un résolveur DNS <https://www.bortzmeyer.org/resolveur-dns.html> détecte un problème avec une zone, l'empêchant de résoudre les noms dans cette zone, il n'avait pas de moyen simple et automatique de prévenir les gérants des serveurs faisant autorité <https://www.bortzmeyer.org/serveur-dns-faisant-autorite.html> pour cette zone. Leur envoyer un message en utilisant l'information dans l'enregistrement SOA ou les adresses classiques du RFC 2142 [1] ? Mais, justement, si la zone ne marche pas, le courrier ne partira pas forcément. Ce nouveau RFC propose un nouveau système. Les serveurs faisant autorité annoncent un domaine (qui marche, espérons-le), qui acceptera des requêtes DNS spéciales signalant le problème.

Cela dépend évidemment du problème pratique qui se pose. Si la zone n'a **aucun** serveur faisant autorité <https://www.bortzmeyer.org/serveur-dns-faisant-autorite.html> qui marche, il n'y a évidemment rien à faire. Mais s'ils marchent, tout en servant des données problématiques (par exemple des signatures DNSSEC expirées), alors, le résolveur <https://www.bortzmeyer.org/resolveur-dns.html> pourra agir. Les serveurs faisant autorité mettent dans leurs réponses une option EDNS qui indique le domaine qui recevra les rapports (cela doit être un autre domaine, qui n'a pas de problème), le résolveur fera alors une requête DNS se terminant par le nom du domaine de signalement, et encodant le problème. L'agent, le domaine de signalement, pourra alors récolter ces requêtes et savoir qu'il y a un problème. Cela ne traite pas tous les cas (il faudra toujours utiliser RDAP ou whois pour récolter des informations sur les contacts du domaine erroné, puis leur écrire depuis un autre réseau) mais c'est simple, léger et automatisable. Les gérants de domaine sérieux, qui prennent au sérieux les signalements de problèmes techniques (soit 0,00001 % des domaines) pourront alors agir. (Note si vous gérez un résolveur et que vous constatez un problème avec un domaine et que les contacts ne répondent pas : un message méchant sur Twitter est souvent plus efficace.)

1. Pour voir le RFC de numéro NNN, https://www.ietf.org/rfc/rfcNNN.txt, par exemple https://www.ietf.org/rfc/rfc2142.txt

Donc, les détails techniques : le domaine qui veut recevoir les éventuels signalements va devoir configurer ses serveurs faisant autorité pour renvoyer une option EDNS, de numéro 18 <https://www.iana.org/assignments/dns-parameters/dns-parameters.xml#dns-parameters-11> (section 5 du RFC), indiquant l'**agent**, c'est-à-dire le domaine qui va recevoir les signalements (il faut évidemment veiller à ce qu'il n'ait pas de point de défaillance commun avec le domaine surveillé). Notez que cette option est systématiquement envoyée, le client (le résolveur) n'a pas à dire quoi que ce soit (la question avait fait l'objet d'un sérieux débat à l'IETF).

En cas de problème, notamment DNSSEC, le résolveur qui a noté le problème va alors construire un nom de domaine formé, successivement (section 6.1.1) par :

— Le composant `_er`,
— Le type de données qui posait problème (adresse IP, enregistrement de service, etc),
— Le nom de domaine qui était initialement demandé par le résolveur,
— L'erreur étendue (EDE, RFC 8914),
— Le composant `_er` (oui, encore),
— Le nom de domaine de l'agent.

Par exemple, si le domaine `dyn.bortzmeyer.fr` annonce comme agent `report.dyn.sources.org`, et qu'un résolveur découvre des signatures DNSSEC expirées (EDE 7) en cherchant à résoudre `hello.dyn.bortzmey / TXT` (TXT a la valeur 16 <https://www.iana.org/assignments/dns-parameters/dns-parameters.xhtml#dns-parameters-4>), la requête de signalement du résolveur sera `_er.16.hello.dyn.bortzmeyer.fr er.report.dyn.sources.org` (ouf). Le type demandé est TXT. Lorsque cette requête arrivera au serveur faisant autorité pour `report.dyn.sources.org`, il pourra enregistrer qu'il y a eu un problème, et mettre cette information à la disposition de son administrateur système.

Ce serveur faisant autorité est censé répondre au signalement avec une réponse de type TXT comme ici :

```
% dig _er.16.hello.dyn.bortzmeyer.fr.7._er.report.dyn.sources.org TXT
...
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 12032
;; flags: qr rd ra ad; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 1
...
;; ANSWER SECTION:
_er.16.hello.dyn.bortzmeyer.fr.7._er.report.dyn.sources.org. 30 IN TXT "Thanks for the report of error 7 on
...
```

L'agent peut ensuite être interrogé, par des méthodes propres à la mise en œuvre utilisée :

```
% echo report | socat - UNIX-CONNECT:/home/drink/drink.sock
REPORT state:
hello.dyn.bortzmeyer.fr, 7
ip.dyn.bortzmeyer.fr, 7
```

Ici, on voit que deux domaines ont été signalés comme ayant des signatures expirées (rassurez-vous, c'était juste des tests). Le nombre de signalements n'est pas indiqué, ni la source des signalements (travail futur <https://framagit.org/bortzmeyer/drink/-/issues/75>).

Quelques petits points de sécurité à garder en tête (section 9 du RFC) :

— Le fait de signaler va, par définition, donner au serveur faisant autorité des informations sur le résolveur (par exemple, un résolveur menteur qui signalerait les blocages informerait sur sa politique, ce que les censeurs ne font en général pas).
— Il en donnera aussi aux serveurs des zones parentes du domaine agent, et il est donc très recommandé de minimiser le nom (RFC 9156).
— Il n'y a pas spécialement d'authentification donc tous ces rapports doivent être traités avec prudence. Un méchant peut facilement fabriquer de faux rapports, de toute façon. Ils doivent donc toujours être vérifiés.

Cette technique a été mise en œuvre dans Drink <https://framagit.org/bortzmeyer/drink> lors d'un hackathon IETF <https://www.bortzmeyer.org/hackathon-ietf-115.html>. Drink peut à la fois signaler un domaine agent, et être serveur pour un domaine agent.

Un exemple de signalisation EDNS de cette option, vu la version de développement de Wireshark (merci à Alexis La Goutte) :