RFC 7314 : Extension Mechanisms for DNS (EDNS) EXPIRE Option

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 18 juillet 2014

Date de publication du RFC : Juillet 2014

https://www.bortzmeyer.org/7314.html

L'enregistrement DNS SOA ("*Start Of Authority*") a un champ `expire` qui indique au bout de combien de temps un serveur esclave qui ne réussit pas à contacter le maître peut arrêter de servir la zone. Si l'esclave a eu les données, non pas directement du maître, mais d'un autre esclave, la durée d'expiration peut ne pas être correcte. C'est ce (rare) problème que règle l'option EDNS `EXPIRE`.

En effet, il faut se rappeler que la distribution d'une zone DNS depuis un serveur maître (le RFC utilise l'ancien terme de « serveur primaire ») n'est pas forcément directe. On peut avoir un maître qui envoie des données à un esclave, qui à son tour les envoie à un autre esclave. Cela permet notamment davantage de robustesse (si le maître n'est temporairement pas joignable depuis certains esclaves). Notez que l'esclave ne sait même pas si la machine qui lui a envoyé les données était un maître ou pas.

Si la période de validité donnée par le champ `expire` du SOA (RFC 1035 [1], section 3.3.13) vaut V et que le transfert de l'esclave à un autre esclave prend place S secondes après le transfert depuis le maître (les transferts ne sont pas forcément instantanés, par exemple en cas de coupure réseau), la zone sera servie pendant V + S secondes et pas seulement pendant V secondes. Pire, s'il existe une boucle dans le graphe de distribution, la zone risque de ne jamais expirer, les esclaves se rafraichissant mutuellement.

Personnellement, le problème me semble rare et de peu d'importance. Il y a des tas d'autres choses plus urgentes à régler dans le DNS. Mais, bon, c'est juste une expérience.

La nouvelle option de ce RFC dépend de EDNS (RFC 6891). Elle a le numéro 9. Mise dans une requête (a priori une requête de type SOA, AXFR ou IXFR), elle indique que le client DNS connait cette option

1. Pour voir le RFC de numéro NNN, `https://www.ietf.org/rfc/rfcNNN.txt`, par exemple `https://www.ietf.org/rfc/rfc1035.txt`

et voudrait sa valeur. Un serveur qui ne connait pas l'option `EXPIRE` ne mettra pas l'option dans sa réponse.

Par contre, un serveur qui connait cette option répondra avec une option `EXPIRE` dans sa réponse. Elle comporte quatre octets de données (comme pour le champ `expire` du SOA), indiquant le nombre de secondes de la période de validité. Si le serveur est un maître, il met toujours dans cette option la valeur du champ `expire` du SOA. S'il est un esclave, il met la valeur actuelle de son compteur d'expiration. Ainsi, si le champ `expire` du SOA vaut 7 200 secondes (2 heures) et que le serveur secondaire reçoit une demande 30 minutes après le transfert depuis le maître, il mettra 5 400 dans l'option EDNS `EXPIRE` (120 minutes de validité moins les 30 minutes écoulées). C'est ainsi qu'on évite l'accumulation des périodes de validité en cas de transfert indirect.

Un serveur esclave (le RFC utilise l'ancien terme de « serveur secondaire ») qui utilise l'option, et qui reçoit une réponse lors d'un transfert initial de la zone, devrait utiliser comme durée de validité la valeur de l'option `EXPIRE` (et pas le champ `expire` du SOA, sauf si ce champ a une valeur inférieure à celle de l'option `EXPIRE`). Cette durée de validité est ensuite mise dans un compteur d'expiration qui décroît avec le temps. Pour les rafraichissements ultérieurs, le serveur esclave doit également utiliser comme durée de validité la valeur de l'option, sauf si le compteur actuel a une valeur plus élevée. Par exemple, si le compteur du secondaire dit que la zone est encore valable pour 4 500 secondes, et qu'une réponse IXFR (RFC 1995) contient une option `EXPIRE` de valeur 9 300 secondes, alors le compteur est mis à 9 300 secondes. Si l'option `EXPIRE` avait valu 2 400 secondes, le compteur n'aurait pas été modifié.

Une conséquence amusante de cette option est qu'elle permet de savoir quand a eu lieu le dernier transfert de zone réussi, juste en interrogeant un esclave. Cela peut être vu comme indiscret, mais cela peut aussi être un outil de supervision très pratique.

Cette option est utilisable depuis dig, à partir de la version 9.10 <http://www.isc.org/blogs/bind-9-10-statistics-troubleshooting-and-zone-configuration/>. Wireshark a récemment été modifié pour <https://code.wireshark.org/review/#/c/3101/> reconnaître cette option.