RFC 9859 : Generalized DNS Notifications

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 5 octobre 2025

Date de publication du RFC : Septembre 2025

https://www.bortzmeyer.org/9859.html

Vous le savez, le protocole DNS permet plusieurs sortes de messages <https://www.iana.org/assignments/dns-parameters/dns-parameters.xml#dns-parameters-5>, identifiés par un code d'opération <https://www.iana.org/assignments/dns-parameters/dns-parameters.xml#dns-parameters-5>. Si le classique QUERY, pour demander à résoudre un nom en informations pratiques, est le plus connu, il y a aussi le UPDATE (modifier les données), le DSO ("*DNS Stateful Operations*") et quelques autres. Et puis il y a le NOTIFY, qui sert à indiquer à un serveur DNS qu'il y a quelque chose de nouveau et d'intéressant. NOTIFY est surtout connu pour son utilisation afin de...notifier un serveur secondaire que le primaire a une nouvelle version de la zone (c'est dans le RFC 1996 [1]). Ce nouveau RFC généralise le concept et permet d'utiliser NOTIFY pour d'autres choses comme un changement dans la liste des serveurs faisant autorité <https://www.bortzmeyer.org/serveur-dns-faisant-autorite.html> ou un changement de clé DNSSEC.

Si vous avez oublié à quoi servait initialement NOTIFY, relisez le RFC 1996. Il permettait de donner une indication (uniquement une indication, le NOTIFY ne fait pas autorité) comme quoi il faudrait envisager un nouveau transfert de zone (RFC 5936) pour mettre à jour un serveur. Cela permettait des mises à jour plus rapides qu'avec le système traditionnel où chaque serveur esclave devait de temps en temps demander à son maître s'il y avait du nouveau. Mais il y a d'autres cas où un serveur DNS voudrait dire à un autre qu'il y a quelque chose à regarder, par exemple si une nouvelle clé doit être utilisée. D'où l'extension d'utilisation que permet notre RFC 9859. Elle ne change pas le protocole, elle se contente d'utiliser plus largement une fonction existante.

Bon, mais c'est bien joli de dire qu'on peut notifier pour bien des choses mais on notifie qui ? Dans le cas traditionnel d'une nouvelle version de la zone, le primaire savait qu'il devait notifier ses secondaires, qu'il connait (après tout, il doit leur autoriser le transfert de zone et, dans le pire des cas, il peut toujours regarder l'ensemble d'enregistrements NS de sa zone). Mais si on généralise le NOTIFY, on peut ne pas savoir qui notifier (les autres mécanisms de notification, ; comme une API ou comme la mise à jour dynamique du RFC 2136, ont d'ailleurs le même problème). La section 3 du RFC couvre ce problème. La méthode recommandée est de publier un enregistrement de type DSYNC, normalisé dans notre RFC, section 2. Il se place sous le nom `_dsync` de la zone :

1. Pour voir le RFC de numéro NNN, https://www.ietf.org/rfc/rfcNNN.txt, par exemple https://www.ietf.org/rfc/rfc1996.txt

```
sousdomaine._dsync  IN DSYNC  CDS   NOTIFY 5359 cds-scanner.example.net.
```

Notez qu'un joker est possible, par exemple :

```
*._dsync  IN DSYNC  CDS   NOTIFY 5359 cds-scanner.example.net.
*._dsync  IN DSYNC  CSYNC NOTIFY 5359 cds-scanner.example.net.
```

Ce nom `_dsync` a été ajouté dans le registre des noms précédés d'un trait bas <https://www.iana.org/assignments/dns-parameters/dns-parameters.xml#underscored-globally-scoped-dns (RFC 8552). Voici un autre exemple d'enregistrement DSYNC :

```
_dsync.example.net.   IN DSYNC  CDS   NOTIFY 5359 cds-scanner.example.net.
```

Que dit-il ? Qu'`example.net`, a priori un hébergeur DNS, voudrait que ses clients, lorsqu'ils ont un nouvel enregistrement CDS (indiquant l'activation d'une nouvelle clé DNSSEC, cf. RFC 8078), notifient `cds-scanner.example.net` sur le port 5359. Ce nouveau type DSYNC a été ajouté au registre des types <https://www.iana.org/assignments/dns-parameters/dns-parameters.xml#dns-parameters-4>, avec la valeur 66.

La section 4.1 détaille comment on trouve le serveur à qui envoyer la notification en utilisant `_dsync`. Imaginons qu'on gère `extra.sub.exodus-privacy.eu.org` et qu'on veuille notifier la zone parente. On insère le composant `_dsync` après le premier composant (cela donne `extra._dsync.sub.exodus-privacy.eu.org`) et on fait une requête pour ce nom et le type DSYNC. Si ça marche, c'est bon, sinon, on utilise le SOA dans la réponse pour trouver la zone parente, et on met le `_dsync` devant. Si ça ne donne toujours rien, on retire les composants avant la zone parente et on recommence. Donc, on interrogera successivement (jusqu'au premier succès), `extra._dsync.sub.exodus-privacy.eu` `extra.sub._dsync.exodus-privacy.eu.org` et `_dsync.exodus-privacy.eu.org`.

Et le NOTIFY dans l'enregistrement DSYNC d'exemple plus haut ? C'est le plan ("*scheme*", à ne pas confondre avec le code d'opération - "*opcode*" - NOTIFY) car DSYNC, dans le futur, pourra servir à autre chose que les notifications. Pour l'instant, dans le nouveau registre des plans <https://www.iana.org/assignments/dns-parameters/dns-parameters.xml#dsync-location-of-synchronization-en il n'y a que NOTIFY mais dans le futur, d'autres pourront être ajoutés (suivant la politique « Examen par un expert » du RFC 8126).

Comment utiliser ce mécanisme de notification généralisé pour traiter les enregistremebts CDS et CDNSKEY des RFC 7344, RFC 8078 et RFC 9615 ? Ces enregistrements servent à signaler à la zone parente la disponibilité de nouvelles clés DNSSEC. La section 4 de notre RFC détaille comment le mécanisme de notification permet d'indiquer qu'un CDS ou un CDNSKEY a changé. Cela évite au gestionnaire de la zone parente de balayer toute la zone ce qui, pour un TLD de plusieurs millions de noms comme `.fr` serait long et pénible. La solution de ce RFC 9859 est donc de chercher les DSYNC puis d'envoyer les NOTIFY, au moins deux, un pour le type CDS et un pour le type CDNSKEY (on ne sait pas forcément à l'avance lesquels utilisent la zone parente). La zone parente doit effectuer les mêmes vérifications que lorsqu'elle a détectée un nouveau CDS (ou CDNSKEY) : RFC 9615 si on active une zone signée pour la premièr fois et RFC 7344 et RFC 8078 autremùent.

Les messages utilisant le code d'opération NOTIFY sont censés produire une réponse (RFC 1996, section 4.7). Si aucune réponse n'arrive avant l'expiration du délai de garde, on réessaie. Si on a trop réessayé, on peut signaler le problème avec la technique du RFC 9567.

Il est important de se souvenir qu'une notification n'est pas sérieusement authentifiée, et que le récepteur doit donc, s'il choisit d'agir sur une notification, être prudent. Dans le RFC 1996, rien de grave ne pouvait arriver, le récepteur du NOTIFY demandait juste le SOA de la zone puis, si nécessaire, un transfert de zone. Mais avec les CDS et CDNSKEY, des attaques plus sérieuses sont possibles et le destinataire de la notification doit donc effectuer davantage de vérifications (par exemple, si la zone est déjà signée, faire une requête pour le CDS ou le CDNSKEY et vérifier que la réponse est valide et sécurisée, si elle ne l'est pas, faire tous les contrôles du RFC 9615). La notification elle-même n'est pas un problème de sécurité (elle dit juste « tu devrais regarder cela »), c'est l'action qui en résulte qui doit être bien réfléchie. Voilà pourquoi les notifications, même généralisées, ne sont pas plus sécurisées que cela. (Voir aussi la section 5 du RFC, qui insiste sur ce point ; la notification peut accélérer les choses mais ne doit pas à elle-même changer quelque chose.) Il est quand même préférable de limiter le nombre de notifications qu'on traite, au cas où un client malveillant vous bombarde de notifications.

Ces notifications généralisées pourront aussi s'utiliser pour les CSYNC du RFC 7477.

Qui met en œuvre ce RFC à l'heure actuelle ? Des opérateurs comme deSEC <https://desec.io/> ont annoncé que c'était en cours, côté client. Côté serveur, les registres de `.ch` et `.se` ont annoncé que c'était en cours, ou bien prévu.

Voici un exemple d'un client en Python (utilisant dnspython <https://www.dnspython.org/>) qui notifie pour un nouveau CDS :

```
import dns.message
import dns.query
import dns.opcode

notify = dns.message.make_query("bortzmeyer.fr", "CDS")
notify.set_opcode(dns.opcode.NOTIFY)
response = dns.query.udp(notify, "192.0.2.211")
print(response)
```

Et en C ? Vous pouvez utiliser le programme d'exemple , qui utilise l'excellente bibliothèque ldns <https://www.nlnetlabs.nl/projects/ldns/>. Compiler et exécuter :

```
% gcc -o generalized-notify -Wall generalized-notify.c -lldns

% ./generalized-notify bortzmeyer.fr 192.0.2.211
Reply code: NOERROR
```

Je note à ce sujet que certains serveurs faisant autorité <https://www.bortzmeyer.org/serveur-dns-faisant-html>, lorsqu'ils ne font pas autorité pour le domaine signalé, répondent REFUSED, ce qui est logique, mais on voit aussi des FORMERR ou NXDIOMAIN (!), sans doute parce que le type CDS ne leur plait pas.

L'annexe A du RFC prend de la hauteur et décrit plus en détail le problème du balayage DNS. Comment savoir qu'il y a du nouveau, sans tout examiner (dans le cas du SOA, au rythme indiqué par le

champ Refresh ; mais il n'y a pas de telle solution pour les CDS et CDNSKEY). Le DNS traditionnel ne marchait que sur un modèle "*pull*" (et c'est pour cela qu'il est faux de parler de propagation DNS <https://www.bortzmeyer.org/dns-propagation.html>) mais les NOTIFY du RFC 1996 introduisaient un peu de "*push*". Heureusement car balayer .com à la recherche de nouveaux enregistrements serait lent (et attirerait probablement l'attention des IDS). Pour les CDS et CDNSKEY, cela serait d'autant plus agaçant qu'ils seront a priori peu nombreux et que la plupart des requêtes ne donneront donc rien.