RFC 8914 : Extended DNS Errors

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 24 octobre 2020

Date de publication du RFC : Octobre 2020

https://www.bortzmeyer.org/8914.html

Un problème classique du DNS est qu'il n'y a pas assez de choix pour le code de retour renvoyé par un serveur DNS. Contrairement à la richesse des codes de retour HTTP <https://www.bortzmeyer.org/http-code-emoji.html>, le DNS est très limité. Ainsi, le code de retour `SERVFAIL` ("*SERver FAILure*") sert à peu près à tout, et indique des erreurs très différentes entre elles. D'où ce nouveau RFC qui normalise un mécanisme permettant des codes d'erreur étendus, les EDE, ce qui facilitera le diagnostic des problèmes DNS.

Ces codes de retour DNS (RCODE, pour "*Response CODE*") sont décrits dans le RFC 1035[1], section 4.1.1. Voici un exemple de requête faite avec dig. Le code de retour est indiqué par l'étiquette "*status :*". Ici, c'est `REFUSED`, indiquant que le serveur faisant autorité <https://www.bortzmeyer.org/serveur-dns-faisant-autorite.html> pour `google.com` ne veut pas répondre aux requêtes pour mon `.org` :

```
% dig @ns1.google.com AAAA www.bortzmeyer.org

; <<>> DiG 9.11.3-1ubuntu1.12-Ubuntu <<>> @ns1.google.com AAAA www.bortzmeyer.org
; (2 servers found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: REFUSED, id: 4181
;; flags: qr rd; QUERY: 1, ANSWER: 0, AUTHORITY: 0, ADDITIONAL: 1
;; WARNING: recursion requested but not available

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags: do; udp: 512
;; QUESTION SECTION:
;www.bortzmeyer.org. IN AAAA

;; Query time: 7 msec
;; SERVER: 2001:4860:4802:32::a#53(2001:4860:4802:32::a)
;; WHEN: Sat Jun 20 11:07:13 CEST 2020
;; MSG SIZE  rcvd: 47
```

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

Codés sur seulement quatre bits, ces codes de retour ne peuvent pas être très nombreux. Le RFC 1035 en normalisait six, et quelques autres ont été ajoutés par la suite <https://www.iana.org/assignments/dns-parameters/dns-parameters.xml#dns-parameters-6>, mais sont rarement vus sur le terrain. En pratique, les plus fréquents sont NOERROR (pas de problème), NXDOMAIN (ce nom de domaine n'existe pas) et SERVFAIL (la plupart des autres erreurs). Notez que le RFC 1034 n'utilisait pas ces sigles à l'origine ils ont été introduits après.

On l'a dit, ces codes de retour sont insuffisants. Lorsqu'un client DNS reçoit SERVFAIL, il doit essayer de deviner ce que cela voulait dire. Lorsqu'on parle à un résolveur <https://www.bortzmeyer.org/resolveur-dns.html>, le SERVFAIL indique-t-il un problème de validation DNSSEC ? Ou bien que les serveurs faisant autorité <https://www.bortzmeyer.org/serveur-dns-faisant-autorite.html> sont injoignables ? Lorsqu'on parle à un serveur faisant autorité <https://www.bortzmeyer.org/serveur-dns-faisant-autorite.html>, le SERVFAIL indiquait-il que ce serveur n'avait pas pu charger sa zone (peut-être parce que le serveur maître était injoignable) ? Ou bien un autre problème ?

L'un des scénarios de débogage les plus communs est celui de DNSSEC. Au moins, il existe un truc simple : refaire la requête avec le bit CD ("*Checking Disabled*"). Si ça marche (NOERROR), alors on est raisonnablement sûr que le problème était un problème DNSSEC. Mais cela ne nous dit pas lequel (signatures expirées ? clés ne correspondant pas à la délégation ?). DNSSEC est donc un des principaux demandeurs d'erreurs plus détaillées.

Alors, après cette introduction (section 1 du RFC), la solution (section 2). Les erreurs étendues (EDE, pour "*Extended DNS Errors*") sont transportées via une option EDNS (RFC 6891) dans la réponse. Cette option comporte un type (numéro 15 <https://www.iana.org/assignments/dns-parameters/dns-parameters.xml#dns-parameters-11>) et une longueur (comme toutes les options EDNS) suivis d'un code d'information (sur deux octets) et de texte libre, non structuré (en UTF-8, cf. RFC 5198, et attention à ne pas le faire trop long, pour éviter la troncation DNS). Les codes d'information possibles sont dans un registre à l'IANA <https://www.iana.org/assignments/dns-parameters/dns-parameters.xml#extended-dns-error-codes>. En ajouter est simple, par la procédure « Premier Arrivé, Premier Servi » du RFC 8126. Cette option EDNS peut être envoyée par le serveur DNS, quel que soit le code de retour (y compris donc NOERROR). Il peut y avoir plusieurs de ces options. La seule condition est que la requête indiquait qu'EDNS est accepté par le client. Le client n'a pas à demander explicitement des erreurs étendues et ne peut pas forcer l'envoi d'une erreur étendue, cela dépend uniquement du serveur.

Les codes d'information initiaux figurent en section 4 du RFC. Le RFC ne précise pas avec quels codes de retour les utiliser (ce fut une grosse discussion à l'IETF…) mais, évidemment, certains codes d'erreur étendus n'ont de sens qu'avec certains codes de retour, je les indiquerai ici. Voici quelques codes d'erreur étendus :

— 0 indique un cas non prévu, le texte qui l'accompagne donnera des explications.
— 1 signale que le domaine était signé, mais avec uniquement des algorithmes inconnus du résolveur <https://www.bortzmeyer.org/resolveur-dns.html>. Il est typiquement en accompagnement d'un NOERROR pour expliquer pourquoi on n'a pas validé (en DNSSEC, un domaine signé avec des algorithmes inconnus est considéré comme non signé).
— 3 (ou 19, pour le NXDOMAIN) indique une réponse rassise (RFC 8767). Voir aussi le 22, plus loin.
— 4 est une réponse fabriquée de toutes pièces par un résolveur menteur <https://www.bortzmeyer.org/dns-menteur.html>. Notez qu'il existe d'autres codes, plus loin, de 15 à 17, permettant de détailler les cas de filtrage. 4 est typiquement en accompagnement d'un NOERROR puisqu'il y a une réponse.
— 6 vient avec les SERVFAIL pour indiquer que la validation DNSSEC a déterminé un problème (signature invalide ou absente). Plusieurs autres codes traitent des problèmes DNSSEC plus spécifiques.

— 7 vient également avec SERVFAIL pour le cas des signatures expirées (sans doute un des problèmes DNSSEC les plus fréquents).
— Trois codes viennent pour les cas où le résolveur refuse de répondre pour ce domaine, et le dit (au lieu, ou en plus, de fabriquer une réponse mensongère). Ce sont 15 (réponse bloquée par une décision de l'administrateur du résolveur), 16 (réponse bloquée par une décision extérieure, typiquement l'État, et il ne sert donc à rien de se plaindre à l'administrateur du résolveur, c'est de la censure) et 17 (réponse bloquée car le client a demandé qu'on filtre pour lui, par exemple parce qu'il a choisi de bloquer les domaines liés à la publicité, cf. l'exemple plus loin). 16 est donc à peu près l'équivalent du 451 de HTTP, normalisé dans le RFC 7725. Gageons que les résolveurs menteurs en France <https://www.bortzmeyer.org/censure-francaise.html> se garderont bien de l'utiliser…
— 18 accompagne en général REFUSED et indique au client qu'il n'est pas le bienvenu (par exemple une requête à un résolveur venue de l'extérieur du réseau local).
— 22 indique qu'un résolveur n'a pu joindre aucun des serveurs faisant autorité. Ce code peut accompagner une réponse rassise ou bien un SERVFAIL. J'en profite pour vous rappeler que, si vous gérez une zone DNS, attention à sa robustesse : évitez les SPOF. Ayez plusieurs serveurs faisant autorité, et dans des lieux séparés (et de préférence dans des AS distincts).

Voici un exemple où un résolveur se présentant comme « pour les familles » ment sur la réponse à une requête pour pornhub.com et ajoute l'EDE 17, puisque c'est l'utilisateur qui, en choisissant ce résolveur public, a demandé ce filtrage :

```
% dig @1.1.1.3 pornhub.com

; <<>> DiG 9.18.28-0ubuntu0.24.04.1-Ubuntu <<>> @1.1.1.3 pornhub.com
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 34585
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags: do; udp: 1232
; EDE: 17 (Filtered)
;; QUESTION SECTION:
;pornhub.com. IN A

;; ANSWER SECTION:
pornhub.com. 60 IN A 0.0.0.0

;; Query time: 9 msec
;; SERVER: 1.1.1.3#53(1.1.1.3) (UDP)
;; WHEN: Wed Sep 25 14:48:50 CEST 2024
;; MSG SIZE  rcvd: 62
```

Le client DNS qui reçoit un code d'erreur étendu est libre de l'utiliser comme il le souhaite (les précédentes versions de ce mécanisme prévoyaient des suggestions faites au client mais ce n'est plus le cas). Le but principal de cette technique est de fournir des informations utiles pour le diagnostic. (Une discussion à l'IETF <https://mailarchive.ietf.org/arch/msg/dnsop/b3wtVj_aWm24PXyHr1M9NMj3LJ0/> avait porté sur des codes indiquant précisément si le problème était local - et devait donc être soumis à son administrateur système - ou distant, auquel cas il n'y avait plus qu'à pleurer, mais cela n'a pas été retenu. Notez que la différence entre les codes 15 et 16 vient de là, du souci d'indiquer à qui se plaindre.)

Attention à la section 6 du RFC, sur la sécurité. Elle note d'abord que certains clients, quand ils reçoivent un SERVFAIL, essaient un autre résolveur <http://www.potaroo.net/presentations/2016-06-27-dnssec.pdf> (ce qui n'est pas une bonne idée si le SERVFAIL était dû à un problème

DNSSEC). Ensuite, les codes d'erreur étendus ne sont **pas** authentifiés (comme, d'ailleurs, les codes de retour DNS habituels), sauf si on utilise, pour parler au serveur, un canal sécurisé comme DoT (RFC 7858) ou DoH (RFC 8484). Il ne faut donc pas s'y fier trop aveuglément. Enfin, ces codes étendus vont fuiter de l'information à un éventuel observateur (sauf si on utilise un canal chiffré, comme avec DoT ou DoH) ; par exemple, 18 permet de savoir que vous n'êtes pas le bienvenu sur le serveur.

Et, désolé, je ne connais pas de mise en œuvre de cette option à l'heure actuelle. J'avais développé le code nécessaire pour Knot <https://www.knot-resolver.cz/> lors du hackathon de l'IETF à Prague en mars 2019 <https://www.bortzmeyer.org/hackathon-ietf-104.html> (le format a changé depuis donc ce code ne peut pas être utilisé tel quel). La principale difficulté n'était pas dans le formatage de la réponse, qui est trivial, mais dans le transport de l'information, depuis les entrailles du résolveur où le problème était détecté, jusqu'au code qui fabriquait la réponse. Il fallait de nouvelles structures de données, plus riches.

Sinon, le RFC mentionne le groupe "*Infected Mushroom*". Si vous voulez voir leurs clips <https://www.youtube.com/user/InfectedMushroomVids>...