RFC 6195 : Domain Name System (DNS) IANA Considerations

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 29 mars 2011

Date de publication du RFC : Mars 2011

https://www.bortzmeyer.org/6195.html

Un RFC un peu bureaucratique, pour détailler les mécanismes utilisés pour l'enregistrement dans les registres de l'IANA des paramètres liés au DNS. Il met très légèrement à jour son prédécesseur, le RFC 5395 [1], qui avait libéralisé l'enregistrement de nouveaux paramètres. Et il a lui-même été remplacé par la suite par le RFC 6895.

Un certain nombre de paramètres, dans le DNS, sont enregistrés à l'IANA, afin de s'assurer d'une interprétation identique partout. C'est ainsi que l'IANA gère un registre des paramètres DNS <https://www.iana.org/assignments/dns-parameters> où on trouve, entre autres, les types d'enregistrement (A, codé 1, pour une adresse IPv4, AAAA, codé 28, pour une adresse IPv6, LOC, codé 29, pour les positions géographiques du RFC 1876, etc). Cet espace n'étant pas de taille infinie, il faut y enregistrer de nouveaux paramètres avec prudence, selon les règles qui étaient expliquées dans le RFC 2929, qui a été sérieusement réformé par le RFC 5395 avant de l'être, beaucoup plus légèrement, par notre RFC 6195.

En effet, les règles du RFC 2929 étaient bien trop strictes à l'usage. Notamment, le processus d'enregistrement d'un nouveau type d'enregistrement était tellement pénible que beaucoup de protocoles (comme SPF à ses débuts) préféraient utiliser le fourre-tout TXT pour y mettre leurs enregistrements. Ce goulet d'étranglement était souvent cité comme un exemple typique des blocages liés à l'IETF.

Le RFC 5395 avait donc assoupli les règles d'enregistrement des types de ressources DNS (les autres règles sont peu changées). Avant, il y avait deux solutions (voir le RFC 5226 pour plus d'explications), "*IETF Review*" (ex-"*IETF Consensus*"), un processus long et incertain imposant un RFC sur le chemin

1. Pour voir le RFC de numéro NNN, https://www.ietf.org/rfc/rfcNNN.txt, par exemple https://www.ietf.org/rfc/rfc5395.txt

des normes, approuvé par l'IESG, ou "*Specification required*", qui impose l'écriture d'une norme (pas forcément un RFC) « stable et permanente ».

Le nouveau système est plus léger (section 3.1.1) : il suffit désormais de remplir un formulaire décrivant le nouveau type d'enregistrement (un gabarit figure en annexe A), de le soumettre sur la liste "*dnsext@ietf.org*" et d'attendre le jugement d'un expert, désigné parmi les noms fournis par l'IESG, qui décidera, sur la base du formulaire soumis, d'allouer ou pas la requête. Un tel processus est utilisé pour d'autres enregistrements à l'IANA, par exemple pour les nouvelles étiquettes de langue <http://www.langtag.net/register-new-subtag.html>.

Le nouveau processus a été testé pour la première fois pour le type d'enregistrement ZS <http://www.ietf.org/mail-archive/web/dnsext/current/msg03223.html> ("*Zone Status*") qui a été accepté <http://www.ietf.org/mail-archive/web/dns-rrtype-applications/current/msg00002.html>, sous un autre nom, NINFO, et figure désormais sous le numéro 56 dans le registre IANA <https://www.iana.org/assignments/dns-parameters>. Autre exemple, plus récent, le type URI, permettant de stocker des URI dans le DNS, enregistré en février 2011 <http://www.ietf.org/mail-archive/web/dnsext/current/msg10722.html>, sous le numéro 256. Mais tous les types ne réussissent pas forcément leur entrée dans le registre. CAA, qui sert à indiquer l'autorité de certification du domaine, est toujours en discussion <http://www.ietf.org/mail-archive/web/dnsext/current/msg10632.html>.

Quels sont les changements entre le RFC 5395, qui avait marqué l'entrée dans la nouvelle ère, et notre RFC 6195 ? Ils sont minimes (voir annexe B). Le principal est le changement de nom de la liste de diffusion où se discutent les demandes. Autrement, ce sont surtout des petites corrections éditoriales. À son tour, le successeur de notre RFC, le RFC 6895 n'a apporté que de petits changements.

Outre l'enregistrement de nouveaux types de ressources DNS, notre RFC mentionne également d'autres champs des messages DNS. Un changement ou une extension de leur sémantique continue à nécessiter une action plus lourde à l'IETF. Ainsi, le bit RD ("*Recursion Desired*") n'a de signification que dans une question DNS. Dans une réponse, il est indéfini et son éventuelle utilisation future nécessitera un RFC sur le chemin des normes. Même chose pour le dernier bit qui reste libre dans les options, le bit Z. Quant aux "*opcodes*" qui indiquent le type du message (requête / notification / mise à jour dynamique / etc), un ajout à leur liste nécessitera le même chemin.

Les codes de réponse ("*rcodes*"), comme NXDOMAIN (nom inexistant) ou BADTIME (signature trop ancienne ou trop récente, cf. RFC 8945) sont tirés d'un espace plus vaste et la procédure est donc un peu plus libérale (section 2.3).