

RFC 6761 : Special-Use Domain Names

Stéphane Bortzmeyer

<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 20 février 2013

Date de publication du RFC : Février 2013

<https://www.bortzmeyer.org/6761.html>

Parmi tous les noms de domaines existants, certains sont « spéciaux » au sens où ils ont des propriétés particulières ou ont été réservés pour un certain usage. Jusqu'à présent, il n'y avait pas de liste exhaustive de tels noms, ni de définition stricte, ni surtout de spécification des conséquences (par exemple, est-ce que les mises en œuvre du DNS sont censées traiter différemment ces noms?) C'est désormais fait avec ce RFC, qui fournit une description de ces noms « spéciaux » et crée un registre <<https://www.iana.org/assignments/special-use-domain-names/special-use-domain-names.xml>> où ils seront répertoriés. Écrit chez Apple, il a surtout pour but de permettre l'enregistrement direct (sans passer par l'ICANN) du TLD `.local`, utilisé unilatéralement par le protocole Apple Bonjour. L'utilisation sans vergogne de ce nom avait en effet suscité bien des critiques.

On peut faire une analogie avec les adresses IP : certaines sont « spéciales » (RFC 6890¹) et certaines de ces adresses spéciales sont reconnues par les mises en œuvre d'IP, qui les traitent d'une manière particulière. C'est par exemple le cas des adresses multicast comme `224.0.0.0` à `239.255.255.255` (en IPv4), ou comme l'adresse locale `::1` (en IPv6, cf. RFC 4291). Les noms de domaine ont un concept analogue avec les noms réservés du RFC 2606 comme `example.org`. Mais le RFC 2606 ne précise pas si un client ou un serveur DNS doit appliquer un traitement particulier à ces noms. Et il n'est pas extensible, il ne fournit pas de mécanisme d'enregistrement de noms supplémentaires. Si on voulait, mettons, ajouter un exemple IDN, il faudrait une nouvelle version du RFC 2606.

Pour mieux comprendre ce qu'est un nom de domaine « spécial » et ce que signifie un traitement spécial, reprenons l'exemple des adresses IP. Lorsque le "*multicast*" a été créé par le RFC 1112, les mises en œuvre d'IP ont du être modifiées pour reconnaître une adresse "*multicast*" et savoir en faire quelque chose. Ainsi, une adresse comme `224.0.0.1` (qui désigne toutes les machines à la fois) devenait « spéciale » et du code particulier était nécessaire (essayez de configurer une machine IP avec

1. Pour voir le RFC de numéro NNN, <https://www.ietf.org/rfc/rfcNNN.txt>, par exemple <https://www.ietf.org/rfc/rfc6890.txt>

224.0.0.1 comme adresse et vous verrez tout un tas de choses bizarres se produire, puisque cette adresse est traitée spécialement par la pile IP). Ce traitement spécial s'applique à toute machine IP, quel que soit le réseau auquel elle est connectée, et qu'elle utilise le "multicast" ou pas.

De la même façon, un nom de domaine va être spécial lorsqu'on aura besoin d'un traitement particulier de ce nom, **par le logiciel**. Le RFC donne l'exemple d'une norme qui utilise un nom dont on est certain qu'il n'existe pas (il renvoie toujours NXDOMAIN, le code de retour pour « domaine non existant »). On ne peut pas garantir un tel nom avec les procédures d'enregistrement actuelles. Prenons par exemple "foobar.42", qui n'existe pas aujourd'hui. Même si la racine n'inclut pas un TLD .42, rien ne garantit qu'un résolveur quelque part ne va pas utiliser une autre racine ou, tout simplement, avoir une règle spéciale pour le TLD .42 (directives `stub-zone` ou `local-zone` dans Unbound, par exemple).

Si on veut **garantir** un certain comportement, il ne suffit donc pas de compter sur les règles d'enregistrement, il faut l'indiquer dans le code. (Et cela a l'avantage de couper court à la discussion sur le fait de savoir s'il faut que l'IETF débourse 185 000 \$ à l'ICANN lorsqu'elle a besoin d'un TLD spécial.) À l'inverse, si on n'a pas besoin d'un comportement uniforme sur toutes les machines IP, connectées à l'Internet ou pas, alors on n'a pas besoin de ces noms spéciaux.

Bon, d'accord, les noms spéciaux sont cool, j'en veux un, comment je fais? La section 3 expose les règles d'enregistrement dans la liste des domaines spéciaux <<https://www.iana.org/assignments/special-use-domain-names/special-use-domain-names.xml>>. Il faut une norme ou bien une approbation de l'IESG (cf. RFC 5226). À noter que ce n'est pas juste un nom qui est ainsi réservé mais tout un sous-arbre des noms de domaines, commençant par ce nom. La demande de réservation d'un nom spécial doit préciser (section 5 du RFC) :

- Si les utilisateurs humains doivent reconnaître ce nom comme différent et le traiter d'une manière spéciale.
- Si les applications qui manipulent des noms de domaine (par exemple un navigateur Web) doivent reconnaître le caractère spécial de ce nom et le traiter différemment.
- Si les bibliothèques de manipulation et de résolution des noms (par exemple `getaddrinfo`) doivent traiter ces noms spécialement.
- Si les serveurs DNS récursifs (les résolveurs) doivent gérer ces noms de manière spécifique.
- Si les serveurs DNS faisant autorité doivent appliquer une politique particulière pour ces noms.
- Si les gérants des serveurs DNS doivent connaître ces noms spéciaux. Par exemple, si un serveur faisant autorité, par défaut, répond pour un tel nom, même sans avoir été configuré pour cela, que se passe-t-il si son opérateur tente de le configurer explicitement?
- Si les registres et bureaux d'enregistrement (curieusement, le RFC ne parle que de ces derniers, comme si tous les domaines permettant l'enregistrement imposaient le passage par un tel bureau) doivent traiter spécialement ces noms et, pas exemple, ne pas permettre leur enregistrement. Le RFC note avec humour qu'`example.org` est réservé par les procédures normales d'enregistrement et que le site Web derrière <<http://www.example.org/>> affirme au contraire que ce nom ne peut pas être enregistré.

Si la réponse à toutes ces sept questions est **non** (pas de traitement spécial), le RFC note que, dans ce cas, il vaut mieux abandonner l'enregistrement, qui n'a pas de sens.

Pour mieux comprendre les sept questions, voyons leur application aux domaines spéciaux qui font partie du registre initial. D'abord, les noms correspondant aux adresses IP privées du RFC 1918, par exemple `23.172.in-addr.arpa` :

- Les utilisateurs peuvent s'en servir comme ils veulent, une fois qu'on les a prévenu que ces noms, n'étant pas gérés par un registre, donneront probablement des résultats différents selon le lieu.
- Les applications ne devraient pas considérer ces noms comme spéciaux.
- Même chose pour les bibliothèques.

- Mais les serveurs récursifs, eux, doivent traiter ces noms à part. Ils ne devraient pas chercher les résultats dans le DNS mais, par défaut, générer une réponse locale, afin de limiter la charge sur les serveurs de ces domaines (RFC 7534). (C'était déjà normalisé dans le RFC 6303, que notre RFC Apple ignore complètement.)
 - Même chose pour les serveurs faisant autorité.
 - Les opérateurs de serveurs DNS peuvent déclarer ces zones sur leurs serveurs, s'ils utilisent ces adresses.
 - Et évidemment les registres ne doivent pas permettre l'enregistrement de noms sous ces noms...
- Autre exemple, le TLD `.test` qui avait été réservé par le RFC 2606 :
- Les utilisateurs peuvent s'en servir, sachant que, le TLD n'étant pas enregistré, les résultats vont varier selon le lieu.
 - Applications et bibliothèques ne devraient pas avoir de code spécial pour ces noms.
 - Les serveurs DNS (récursifs ou faisant autorité) devraient par défaut traiter ces noms à part : pas de recherche dans le DNS et émission de réponse synthétisées localement (probablement `NXDOMAIN` par défaut). Le but est de ne pas embêter les serveurs racine avec ces noms bidon.
 - Mais les opérateurs des serveurs DNS sont libres de configurer leurs serveurs pour ces noms.
 - Et les registres ne devraient pas les enregistrer.

Les TLD `.localhost` et `.invalid` sont traités ensuite. Par exemple, pour `.invalid`, le fait de répondre `NXDOMAIN` est demandé (alors que, pour `.test`, ce n'était qu'une possibilité). D'autre part, pour ces deux TLD, il est recommandé que les bibliothèques de manipulation de noms de domaine traitent ces noms à part, n'envoyant pas de requêtes au résolveur DNS.

Quant aux domaines d'exemple du RFC 2606, il est également demandé qu'ils soient considérés comme spéciaux et ne génèrent pas de requêtes DNS (et, si c'est le cas, qu'elles reçoivent immédiatement une réponse négative). Ce n'est pas le cas actuellement et, comme vu plus haut, vous pouvez visiter `<http://www.example.org/>`.

Voilà, le registre géré par l'IANA est désormais en ligne `<https://www.iana.org/assignments/special-use-domain-names/special-use-domain-names.xml>` et `.local` y a déjà été ajouté (RFC 6762). Le second TLD important qui a été mis dans ce registre a été le `.onion` dans le RFC 7686, en octobre 2015. Cet enregistrement a fait des vagues, et mené à des critiques, exprimées dans le RFC 8244.