Il n'existe pas de TLD interne standard

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 25 octobre 2019

https://www.bortzmeyer.org/pas-de-tld-interne.html

Dans beaucoup d'organisations, les noms de domaine locaux sont attribués dans un TLD, un domaine de tête, non normalisé, comme `.loc` ou `.lan`. Pourquoi n'y a t-il pas de domaine de premier niveau normalisé pour ces usages « internes » ?

Un certain nombre de personnes, sans avoir vérifié, croient savoir qu'il y a un domaine de premier niveau prévu pour cela. On cite parfois à tort `.local` (qui est en fait affecté à autre chose par le RFC 6762 [1]). Parfois, le `.loc`, plus court, est utilisé. La plupart du temps, on ne se pose pas la question, et on utilise un TLD non affecté, sans réfléchir.

Alors, peut-on répondre aux administrateurs réseaux de ces organisations « vous auriez dû utiliser le TLD standard prévu pour cela » ? Après tout, il y a des TLD standards pour des usages spécifiques, comme `.test` pour les essais et le développement ou comme `.example` pour les exemples dans la documentation. Ils sont normalisés dans le RFC 2606 et, depuis, a été créé un registre IANA <https://www.iana.org/assignments/special-use-domain-names/special-use-domain-names.xml#special-use-domain>, peuplé selon des règles définies dans le RFC 6761, pour stocker tous ces noms « spéciaux ». (Le RFC 8244 peut être aussi une bonne lecture, mais à lire avec son sens critique allumé.)

Mais, parmi eux, il n'y a pas de TLD réservé comme « usage interne des organisations ». Ce n'est pas faute d'avoir essayé, plusieurs tentatives ont été faites pour normaliser un tel nom, mais sans résultat. Pour comprendre, il faut d'abord revenir sur la question « pourquoi ne pas prendre un nom un peu au hasard et l'utiliser ? » Imaginons une organisation nommée « Foobar » et qui nommerait ses ressources internes sous le TLD non-existant `.foobar`. (Il y a de nombreux exemples réels. Par exemple, la société Belkin livrait des produits pré-configurés avec le TLD `.belkin`.) Quel(s) problème(s) cela poserait ? Ils sont au nombre de trois :

1. Pour voir le RFC de numéro NNN, `https://www.ietf.org/rfc/rfcNNN.txt`, par exemple `https://www.ietf.org/rfc/rfc6762.txt`

— Pendant longtemps, il semblait que la liste des TLD ne changeait pas et qu'un nom libre le resterait longtemps. Les indépendances suite à la fin de la guerre froide, et la création par l'ICANN de centaines de nouveaux TLD à partir de 2013 ont mis fin à cette légende. Si demain, l'ICANN ouvre un nouveau cycle d'enregistrement de TLD, et que quelqu'un demande et obtient `.foobar`, notre entreprise sera bien embêtée, il y aura de nombreuses collisions entre ses noms internes et les noms externes. Le résultat de la résolution DNS dépendra de beaucoup de choses. Cela avait par exemple posé des problèmes pour .dev <https://ma.ttias.be/chrome-force-dev-domains-https->.
— Quand on utilise un nom assez répandu comme, aujourd'hui, `.loc`, `.home` ou `.corp`, un autre danger se présente, celui lié aux fusions/acquisitions. Si une organisation fusionne avec une autre, par exemple une entreprise se fait acheter, et que les deux organisations utilisaient le même TLD interne, on retombe dans le même problème de collisions. La DSI aura bien du mal à gérer ce choc entre les deux utilisations du même nom. Utiliser un nom aléatoire tel que `.fa43h7hiowxa3lk9aio` comme TLD interne rendrait ce risque peu vraisemblable, mais ça ne serait pas très pratique.
— Et enfin il y a le problème des fuites. Lorsqu'on crée un TLD interne, c'est pour qu'il reste interne, d'autant plus qu'il recense des ressources privées, mais, en pratique, il est très difficile de s'assurer qu'il n'y aura pas de fuites. Un employé oublie qu'il n'a pas lancé le VPN de l'entreprise, et cherche à accéder à des ressources internes. Ou bien il rapporte le portable chez lui et ses logiciels tentent automatiquement de résoudre ces noms internes. Dans tous ces cas, les noms internes vont fuiter vers les serveurs faisant autorité, et la racine du DNS voit une part significative de requêtes pour des TLD n'existant pas. (Vous pouvez regarder vous-même ces requêtes pour des TLD non existants, par exemple sur la page de statistiques du serveur C-root <https://c.root-servers.org/dsc/dsc-grapher.pl?window=86400&plot=qtype_vs_all_tld&server=C-Root>.) Les fuites ne se produisent d'ailleurs pas que vers la racine du DNS. Le ministère de l'intérieur utilise `.mi` en interne et a déjà publié des appels d'offres, des offres d'emploi ou des communiqués de presse <https://twitter.com/nicoladiaz/status/941313829778214912> en indiquant un URL en `.mi`.

Pour ces trois raisons, utiliser un TLD imaginaire n'est pas une bonne idée. Notez qu'un certain nombre d'administrateurs réseau s'en moquent : ils se disent que le problème n'arrivera que dans plusieurs années, qu'ils auront changé d'entreprise à ce moment et que ce sera leur successeur ou successeuse qui devra gérer les conséquences de leurs décisions erronnées.

Mais alors, puisque ce n'est pas une bonne idée de prendre un TLD au pifomètre, pourquoi est-ce que l'IETF, qui a déjà enregistré plusieurs TLD spéciaux <https://www.iana.org/assignments/special-use-domain-names/special-use-domain-names.xml#special-use-domain>, n'enregistre pas un `.internal` (ou un autre nom) en le marquant comme « Usage interne seulement » ? Ce serait en gros l'analogue pour le DNS de ce que sont les adresses IP privées du RFC 1918. L'opération a été tentée, et pas qu'une seule fois. Le dernier essai était l'"*Internet-Draft*" `draft-wkumari-dnsop-internal`, qui réservait `.internal`.

Le brouillon `draft-wkumari-dnsop-internal` examinait également les autres possibilités, alternatives au `.internal` :

— Le TLD `.alt` a finalement été adopté longtemps après (RFC 9476) mais, de toute façon, il est réservé aux cas où la résolution de noms ne se faisait **pas** via le DNS mais, par exemple, via GNUnet.
— L'IETF a déjà un TLD quasiment à sa disposition, `.arpa`. On aurait pu envisager un `quelquechose.arpa`. Mais le sigle "*ARPA*" n'est pas parlant à M. Toutlemonde, et un suffixe de nom de domaine à deux composants est jugé moins pratique qu'un suffixe à un seul composant, le TLD.
— Les noms déjà réservés comme spéciaux <https://www.iana.org/assignments/special-use-domain-names.xml#special-use-domain> comme `.local` ou `.invalid` ont tous une sémantique bien précise, et restrictive. Bref, ils servent déjà à autre chose.

D'où le choix du `.internal` par l'auteur du document.

À noter qu'une question intéressante, lorsqu'on décide de réserver un pseudo-TLD pour les sites locaux, est celle de DNSSEC. Si le TLD n'est pas délégué par la racine, les résolveurs validants rejetteront ce nom, puisque la racine est signée. Ce n'est peut-être pas trop grave puisqu'ils auront de toute façon besoin d'une configuration spécifique pour l'utiliser. Un exemple ? Ici, avec Unbound, on délègue `.internal` à deux serveurs internes :

```
server:
     domain-insecure: "internal" # Only necessary if there is no
     # insecure delegation from the root.

forward-zone:
     name:   "internal"
     forward-addr: 10.42.1.68
     forward-addr: fd9d:ebf3:dd41:6094::1:53
```

Et si on délègue le nom (par exemple au nouvel AS112 du RFC 7535) ? Pas moyen de signer cette délégation (puisqu'il faudrait distribuer publiquement la clé privée, pour que chacun signe sa zone locale). La seule solution est donc une délégation non signée (des enregistrements NS mais pas de DS). Notez que `.alt`, s'il avait été accepté, n'aurait pas eu ce problème, puisqu'il était réservé aux usages non-DNS.

Mais le brouillon `draft-wkumari-dnsop-internal` note que c'est bien joli de choisir un joli nom, encore faut-il, si on a décidé qu'il était mieux de le déléguer, convaincre l'ICANN de le faire. Et, là, on est partis pour dix ans de "*multistakeholder bottom-up decision process*" et d'innombrables réunions. C'est en partie ce qui explique le manque d'intérêt qui a finalement coulé le projet `<https://mailarchive.ietf.org/arch/msg/dnsop/9oDqDo7BBzFSLU_Su_UgaUvRp_U>` `.internal`. Le marécage de la gouvernance Internet est difficile à traverser.

De toute façon, `.internal` n'aurait résolu que le premier problème (risque de délégation d'un vrai TLD du même nom). Il aurait un peu aggravé le second (collision lors d'une fusion/acquisition) puisque tout le monde utiliserait le même nom. Et il aurait un peu aidé pour le troisième (les fuites) puisqu'il aurait été plus facile de prendre des mesures standard pour gérer les fuites d'un TLD standard. Bref, l'idée n'est pas forcément excellente, la motivation principale pour le `.internal` était « c'est une mauvaise idée mais il y a une demande donc on donne ce TLD aux administrateurs réseau pour qu'ils arrêtent de râler ». On a vu que cette motivation n'avait pas été suffisante et que, finalement, on n'a pas de TLD (ou de suffixe) standard pour les noms internes.

Que doit faire l'administrateur réseau, alors ? Le plus simple, étant donné que toute organisation a (ou devrait avoir) un nom de domaine à soi, est de prendre un sous-domaine de ce domaine. Si l'organisation Foobar citée plus haut a `foobar.com`, qu'elle nomme ses ressources internes en `internal.foobar.com`. Du fait de la nature arborescente des noms de domaine, aucun risque que ce nom soit attribué à un autre, aucun risque de collision en cas de fusion/acquisition, et aucun risque de fuites.
