Combien y a t-il vraiment de serveurs DNS racine ?

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 27 novembre 2009. Dernière mise à jour le 13 janvier 2010

https://www.bortzmeyer.org/combien-serveurs-racines.html

La question resurgit régulièrement dans les discussions sur la gouvernance de l'Internet : combien le DNS a t-il de serveurs racine ?

Comme souvent avec les chiffres, tout dépend de ce qu'on mesure. La marionette du gouvernement états-unien se contredit même dans sa propre propagande. En 2007, l'ICANN criait bien fort qu'il n'y en avait pas que treize serveurs racine <http://blog.icann.org/2007/11/there-are-not-13-root-servers/>, pour se moquer des critiques de son concurrent, l'UIT. En 2009, dans les publications officielles de la même organisation, ils sont redevenus treize <https://www.icann.org/en/announcements/announcement-26oct09-en.htm>.

En fait, les deux textes ont raison, car ils ne mesurent pas la même chose. Ce qui est drôle est que le texte de 2007 est très agressif, très arrogant, laissant entendre que les gens qui parlent des « treize serveurs » sont des ignorants, alors que la même organisation reprend ce compte deux ans après.

Donc, si on veut les chiffres authentiques, il faut passer un peu de temps et mieux comprendre ce qu'il y a derrière les chiffres. On peut trouver tous les détails sur le site (non officiel) <http://www.root-servers.org/> de certains des opérateurs des serveurs racine. Le résultat :

— Il y a **onze** organisations qui gèrent un serveur racine (VeriSign, ISI, Cogent, université du Maryland, NASA, ISC, armée US, Autonomica, RIPE-NCC, ICANN et WIDE). Seulement deux sont européennes et une japonaise, toutes les autres sont états-uniennes. Changer cette liste est à peu près impossible pour des raisons politiciennes. Il n'y a aucun processus pour recruter un gérant de serveur racine et aucun pour en licencier un, quelles que soient les choses étranges qu'il fasse <https://www.bortzmeyer.org/qui-controle-les-serveurs-racine.html>. En l'absence d'autorité (au sens moral et politique du terme) qui puisse dire qu'on va remplacer telle organisation, qui ne rend pas un service génial, par telle autre (les bons ne manquent pas), la liste n'a jamais connu une seule modification depuis quinze ans, cas unique de stabilité dans l'Internet. Le statu quo semble la seule solution.

— Il y a **treize** noms dans la racine (treize enregistrements NS pour « "*Name Server*" »), de `A.root-servers.net` à `M.root-servers.net`. Avec dig, la commande `dig NS .` vous les affichera. Déduire de ce nombre une insuffisance de la résistance de la racine aux pannes (« Il n'y a que treize pauvres machines (et là on imagine un vieux serveur Dell sur son "*rack*") ») serait donc erroné, ces treize serveurs ne sont pas treize machines. À noter que le nombre de treize vient de vieilles considérations sur l'ancienne taille des paquets DNS, limitée à 512 octets autrefois. La limite a été étendue il y a dix ans et a été effectivement dépassée lors de l'introduction des adresses IPv6 dans la racine en 2008 <https://www.icann.org/en/announcements/announcement-04feb08.htm> mais personne n'ose prendre la responsabilité de remettre en cause ce nombre magique de treize.
— Il y a **vingt et une** adresses IP de serveurs de noms de la racine (certains n'ont pas encore une adresse IPv6).
— Grâce à l'"*anycast*", il y a **cent quatre vingt neuf** sites physiques différents où se trouve un serveur racine, comme celui de Prague, annoncé dans le communiqué de l'ICANN <https://www.icann.org/en/announcements/announcement-26oct09-en.htm> d'octobre 2009. Un bon nombre de ces sites sont purement locaux, leurs annonces BGP ne sont pas propagées en dehors d'un cercle limité et ces sites ne sont donc pas accessibles de l'extérieur (par exemple, ils sont souvent limités aux opérateurs connectés à un même point d'échange). Ce nombre varie souvent et dépend uniquement des décisions de chaque organisation gérant un serveur. Certaines, les plus dynamiques comme l'ISC, ouvrent des sites à un rythme soutenu.
— Il y a un nombre inconnu de **machines** qui assurent ce service, certainement nettement plus de deux cents, la plupart des sites hébergeant plus qu'une machine, derrière un répartiteur de charge.

Si on va analyser la résistance de la racine aux pannes, le chiffre à prendre en considération dépend de la panne envisagée. Si c'est la panne d'un composant électronique dans un ordinateur, c'est bien le nombre de machines physiques qui est le paramètre important. Si la panne est un incendie ou un tremblement de terre <http://earthquake.usgs.gov/>, c'est plutôt le nombre de sites qui compte car la panne affectera tous les serveurs situés sur le site. Enfin, si la panne est de nature organisationnelle (cas de certains serveurs racines où l'organisation qui les héberge ne fait guère d'efforts et ne déploie guère de moyens, voire connait des conflits internes), c'est bien le chiffre de onze, le nombre d'organisations, qu'il faut prendre en compte pour évaluer la fiabilité de la racine.

Autres lectures sur ce sujet : un article technique très détaillé <http://www.miek.nl/blog/archives/2013/11/10/why_13_dns_root_servers/index.html> sur « pourquoi 13 et pas 14 » et une discussion sur certains points historiques <https://supine.com/posts/2013/11/historical-dns-qui>.