Un domaine de tête entier, le suédois, disparait temporairement

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 14 octobre 2009

https://www.bortzmeyer.org/panne-de-point-se.html

Lundi 12 octobre, vers 20h00 UTC, le domaine de tête .se a chargé la zone DNS de numéro de série 2009101210 qui comprenait une énorme erreur. Pendant une heure, plus **aucun** nom de domaine se terminant par .se ne fonctionnait.

Très vite, Twitter a vu des tweets sur le sujet <http://twitter.com/jkemikal/statuses/4817556299>, puis des rapports et des discussions ont commencé sur les listes de diffusion d'opérateurs comme Nanog <http://mailman.nanog.org/pipermail/nanog/2009-October/014021.html>.

La cause immédiate était le manque d'un point dans le fichier de zone, les enregistrement NS de la zone avaient tous un .se en trop à la fin, par exemple h.ns.se.se. En effet, dans le format standard des fichiers de zone DNS, tel qu'il est défini en section 5 du RFC 1035 [1], un nom qui ne se termine pas par un point est complété par la nom de la zone, ici .se. Pendant la panne, on a donc pu voir :

```
% dig +cd NS se.
...
;; ANSWER SECTION:
se.                     172540  IN      NS      h.ns.se.se.
se.                     172540  IN      NS      g.ns.se.se.
...
```

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

Vous avez remarqué ? (Moi, je ne l'avais pas vu.) Un `.se` de trop à la fin, les noms des serveurs de noms étaient donc tous considérés comme inexistants. `.se` avait donc disparu de l'Internet, plus de Web, plus de courrier, plus de XMPP, etc. Comme quasiment toutes les interactions sur l'Internet commencent par une requête DNS, plus rien ne marchait.

Selon la façon dont les résolveurs remplaçaient la délégation venue de la racine (qui était correcte) par celle faisant autorité (car publiée par le domaine `.se` lui-même), ils arrivaient encore à résoudre les noms en `.se` ou pas (BIND se débrouillait mieux qu'Unbound, l'inverse aurait été vrai si l'erreur avait été à la racine).

Le problème ne concernait pas que les enregistrement NS du TLD mais aussi ceux de toutes les zones déléguées :

```
ballou.se.              42617   NS      ns1.ballou.se.se.
                        42617   NS      ns2.ballou.se.se.
                        45098   NS      ns3.aname.se.se.
```

Vers 21h00 UTC, `.se` a chargé la zone 2009101211 qui corrigeait l'erreur... et en introduisait d'autres, notamment des signatures DNSSEC invalides pour le SOA <http://unbound.nlnetlabs.nl/pipermail/unbound-users/2009-October/000887.html>. (Ce problème a été reconnu par le registre <http://www.iis.se/en/2009/10/13/felaktig-dns-information/>.)

Tout a finalement été réparé **mais** la mauvaise information pouvait encore se trouver dans des caches. Pendant un certain temps, les sites en `.se` restaient injoignables, sauf à obtenir de votre FAI qu'il redémarre son résolveur (comme conseillé par le registre <http://www.iis.se/en/2009/10/13/felaktig-dns-information/>, command `rndc flush` pour BIND). Pendant quelle durée exactement ? Le TTL est de deux jours, donc j'avais pensé que ce serait la durée de la panne (et c'est aussi ce qu'annonce le registre <http://www.iis.se/en/2009/10/13/felaktig-dns-information/>) mais Jay Daley me fait remarquer à juste titre que, les noms n'existant pas, c'est le cache négatif (RFC 2308) qui compte et que celui-ci est de seulement deux heures pour `.se`.

Cette panne est une des plus graves qui aient jamais affecté un domaine de tête sérieux. Aurait-elle pu être évitée ? Il est évident qu'il faut faire tourner des tests de validité <https://lists.dns-oarc.net/pipermail/dns-operations/2009-October/004562.html> avant de publier la zone. Mais aucun test ne détecte tous les problèmes possibles. Par exemple, un outil de vérification livré avec BIND aurait pu détecter le problème :

```
% named-checkzone example example.zone
zone example/IN: NS 'ns1.nic.example.example' has no address records (A or AAAA)
```

Mais `named-checkzone` a aussi des limites. Il ne positionne pas le code de retour dans le cas ci-dessus, par exemple (et, non, `-n fail` ne change rien). Et il ne marche pas si la zone est mise à jour par "*dynamic update*" (RFC 2136).

Quelques leçons à en tirer :
— Les problèmes surviennent, donc une détection et correction rapide est primordiale,
— DNSSEC, pour lequel le registre suédois était pionnier, n'a pas aidé. Si les données sont fausses, DNSSEC ne va pas les corriger. "*Garbage In, Garbage Out*".

Quelques articles sur le sujet :

---

https://www.bortzmeyer.org/panne-de-point-se.html

— "*Sweden's Internet broken by DNS mistake*" <http://royal.pingdom.com/2009/10/13/sweden%25E2%2580%2599s-internet-broken-by-dns-mistake/>, analyse détaillée par Pingdom,
— "*I Don't Want to Say "I Told You So"...*" <http://www.cricketondns.com/post.cfm/i-don-t-want-to-say> l'avis d'un expert,
— "*Crisis information in the modern society...*" <http://www.kurtis.pp.se/blog/2009/10/crisis_information_in_the_mode.html>, et d'un autre expert,
— Tech glitch darkens Swedish websites <http://www.thelocal.se/22618/20091013/>, des nouvelles par un journal suédois anglophone,
— "*Stora internetproblem fl*Caractère Unicode non montré [2] *]r Sverige*" <http://www.svd.se/nyheter/inrikes/artikel_3642747.svd> et des nouvelles pour ceux qui parlent la langue de Henning Mankell et Stieg Larsson.
— Le registre de .se a publié quelques mois après une étude très détaillée en anglais <http://www.iis.se/docs/26875-Svar-till-PTSv2-eng.pdf>.

Je dois aussi des remerciements à Jay Daley, David Blacka, Gilles Massen, Jakob Schlyter, Jelte Jansen et Olaf Kolkman pour leurs analyses et le partage d'information.

2. Car trop difficile à faire afficher par LaTeX