Le cas du serveur DNS qui ne se mettait plus à jour

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 11 novembre 2024

https://www.bortzmeyer.org/dns-afrinic-stale.html

La semaine dernière, 26 TLD africains avaient des problèmes DNS. Pourquoi ? Parce qu'une machine quelque part ne se mettait plus à jour et servait des données erronées.

Le problème semble s'être déclenché autour du 29 octobre. Des signalements ont été faits sur les réseaux sociaux comme quoi certain·es utilisateurices n'arrivaient pas à résoudre des noms en .mg. On voit ici un test fait avec les sondes RIPE Atlas <https://atlas.ripe.net/> et le logiciel Blaeu <https://framagit.org/bortzmeyer/blaeu> :

```
% blaeu-resolve --requested 100 --displayvalidation --type NS mg
[dns-tld.ird.fr. ns-mg.afrinic.net. ns-mg.malagasy.com. ns.dts.mg. ns.nic.mg. pch.nic.mg.] : 39 occurrences
[ (Authentic Data flag)  dns-tld.ird.fr. ns-mg.afrinic.net. ns-mg.malagasy.com. ns.dts.mg. ns.nic.mg. pch.nic.mg
[ERROR: SERVFAIL] : 5 occurrences
[ERROR: NXDOMAIN] : 2 occurrences
Test #81689686 done at 2024-11-08T15:45:06Z
```

Cinq sondes ont un résolveur <https://www.bortzmeyer.org/resolveur-dns.html> qui répond SERVFAIL ("*Server Failure*"). On peut soupçonner un problème DNSSEC et on voit en effet avec DNSviz <https://dnsviz.net/d/mg/Zy4zHQ/dnssec/> que des signatures expirées sont reçues par certains clients DNS. Le fait que la plupart des utilisateurices ne voient pas de problème laisse entendre que tous les serveurs faisant autorité <https://www.bortzmeyer.org/serveur-dns-faisant-autorite.html> pour .mg ne sont pas également affectés. Examinons-les tous :

```
% for ns in ns.dts.mg. ns-mg.malagasy.com. dns-tld.ird.fr. pch.nic.mg. ns.nic.mg. ns-mg.afrinic.net.; do
for> echo $ns
for> dig @$ns mg. NS
for> done

ns.dts.mg.
...
;; ANSWER SECTION:
mg. 7200 IN NS ns.nic.mg.
```

```
mg. 7200 IN NS ns-mg.afrinic.net.
mg. 7200 IN NS ns.dts.mg.
mg. 7200 IN NS ns-mg.malagasy.com.
mg. 7200 IN NS pch.nic.mg.
mg. 7200 IN NS dns-tld.ird.fr.
mg. 7200 IN RRSIG NS 8 1 7200 (
20241113113756 20241030045734 18 mg.
ExrGRrWttb4umpOtW2d8gbW2J1p68LENdw3X409lP1hm
...
;; Query time: 193 msec
;; SERVER: 196.192.32.2#53(ns.dts.mg.) (UDP)
;; WHEN: Fri Nov 08 16:46:03 CET 2024
;; MSG SIZE  rcvd: 548

ns-mg.afrinic.net.
...
;; ANSWER SECTION:
mg. 7200 IN NS ns.dts.mg.
mg. 7200 IN NS ns.nic.mg.
mg. 7200 IN NS dns-tld.ird.fr.
mg. 7200 IN NS ns-mg.malagasy.com.
mg. 7200 IN NS pch.nic.mg.
mg. 7200 IN NS ns-mg.afrinic.net.
mg. 7200 IN RRSIG NS 8 1 7200 (
20241101171148 20241018111647 18 mg.
UIIoFCD8kaXyqTIVsrgBdiwQZxwHOXsnZjpPky5p5dRa
...
; Query time: 156 msec
;; SERVER: 2001:43f8:120::35#53(ns-mg.afrinic.net.) (UDP)
;; WHEN: Fri Nov 08 16:46:04 CET 2024
;; MSG SIZE  rcvd: 504
```

Je n'ai gardé que la réponse de deux des serveurs. Celle de `ns.dts.mg` ne montre aucun problème particulier mais celle de `ns-mg.afrinic.net` montre une signature expirée (20241101171148 = 1 novembre alors que le test a été fait le 8). Pas étonnant que les résolveurs qui valident avec DNSSEC soient mécontents. Mais pourquoi ce serveur fait-il cela ? En testant avec le logiciel check-soa <`https://framagit.org/bortzmeyer/check-soa`>, on voit :

```
% check-soa mg
dns-tld.ird.fr.
13.39.116.127: OK: 2024110815
ns-mg.afrinic.net.
2001:43f8:120::35: OK: 2024102913
196.216.168.35: OK: 2024102913
ns-mg.malagasy.com.
51.178.182.212: OK: 2024110815
ns.dts.mg.
196.192.32.2: OK: 2024110815
ns.nic.mg.
196.192.42.153: OK: 2024110815
pch.nic.mg.
2001:500:14:6121:ad::1: OK: 2024110815
204.61.216.121: OK: 2024110815
```

Aïe, le numéro de série est en retard (2024102913 alors que les autres serveurs sont à 2024110815). Donc, ce serveur ne se met plus à jour avec son serveur maitre, il continue à distribuer de vieilles données.

Mais attention, ce serveur `ns-mg.afrinic.net` est "*anycasté*". Ce ne sont peut-être pas toutes les instances "*anycast*" qui ont le problème. D'ailleurs, check-soa depuis d'autres machines ne montre pas de

problème. Utilisons encore les sondes RIPE Atlas pour interroger uniquement ce serveur, en demandant son NSID (RFC 5001 [1]) :

```
% blaeu-resolve --requested 100 --nameserver  ns-mg.afrinic.net. --nsid  --type SOA mg
Nameserver ns-mg.afrinic.net.
[NSID: s03-ns2.iso; ns.nic.mg. ramboa.nic.mg. 2024110815 14400 3600 604800 3600] : 41 occurrences
[NSID: s01-ns2.pkl; ns.nic.mg. ramboa.nic.mg. 2024102913 14400 3600 604800 3600] : 28 occurrences
[NSID: s01-ns2.pkl; ns.nic.mg. ramboa.nic.mg. 2024110815 14400 3600 604800 3600] : 24 occurrences
[NSID: s04-ns2.jnb; ns.nic.mg. ramboa.nic.mg. 2024110815 14400 3600 604800 3600] : 4 occurrences
[NSID: None; ns.nic.mg. ramboa.nic.mg. 2024110815 14400 3600 604800 3600] : 1 occurrences
[TIMEOUT] : 2 occurrences
Test #81689801 done at 2024-11-08T15:54:11Z
```

On voit ici que l'instance `s01-ns2.pkl` est celle qui a le problème : le numéro de série est vieux. (Pour compliquer les choses, notons qu'il y a deux instances ayant le même NSID, ce qui ne facilite pas le déboguage.)

Une partie des clients DNS (ceux qui ont la malchance de tomber sur cette instance) reçoivent donc de la vieille information. Les domaines créés récemment, par exemple, ne sont pas connus de cette instance. Et, comme vu plus haut, elle sert des signatures expirées, ce qui peut planter DNSSEC. (Normalement, le résolveur validant, en recevant ces signatures expirées, devrait réessayer auprès d'un autre serveur du domaine mais, apparemment, certains ne le font pas.)

Et le problème n'affectait pas que `.mg`. Ce serveur secondaire, géré par Afrinic, sert 26 TLD en tout. (Les gérants de ces TLD ont été notifiés. Si vous voulez en parler à Afrinic, c'est leur ticket [DNS #924626]. Si vous connaissez l'Internet, vous ne serez pas surpris d'apprendre que, dans deux cas, l'adresse de contact était invalide et générait un message d'erreur.) Voici par exemple ce que cela donnait pour `.td` :

```
% blaeu-resolve --requested 100 --nameserver  ns-td.afrinic.net. --nsid  --type SOA td
Nameserver ns-td.afrinic.net.
[NSID: s01-ns2.pkl; pch.nic.td. hostmaster.nic.td. 2024110815 21600 3600 604800 7200] : 20 occurrences
[NSID: s01-ns2.pkl; pch.nic.td. hostmaster.nic.td. 2024102914 21600 3600 604800 7200] : 25 occurrences
[NSID: s03-ns2.iso; pch.nic.td. hostmaster.nic.td. 2024110815 21600 3600 604800 7200] : 47 occurrences
[NSID: None; pch.nic.td. hostmaster.nic.td. 2024110815 21600 3600 604800 7200] : 1 occurrences
[NSID: s04-ns2.jnb; pch.nic.td. hostmaster.nic.td. 2024110815 21600 3600 604800 7200] : 5 occurrences
Test #81691145 done at 2024-11-08T16:55:58Z
```

Le problème a finalement été réparé le 10 novembre. Afrinic a retiré du service l'instance invalide. Ici, on voit qu'elle n'est plus présente (test avec le `.mz`) :

```
% blaeu-resolve --requested 100 --displayvalidation --nsid --nameserver ns-mz.afrinic.net --type SOA mz
Nameserver ns-mz.afrinic.net
[NSID: s03-ns2.iso; anyns.uem.mz. hostmaster.nic.mz. 2024111106 480 300 259200 21600] : 48 occurrences
[NSID: s01-ns2.jinx; anyns.uem.mz. hostmaster.nic.mz. 2024111106 480 300 259200 21600] : 13 occurrences
[TIMEOUT] : 33 occurrences
[NSID: s04-ns2.jnb; anyns.uem.mz. hostmaster.nic.mz. 2024111106 480 300 259200 21600] : 4 occurrences
[NSID: None; anyns.uem.mz. hostmaster.nic.mz. 2024111106 480 300 259200 21600] : 1 occurrences
Test #81847650 done at 2024-11-11T06:14:08Z
```

1. Pour voir le RFC de numéro NNN, `https://www.ietf.org/rfc/rfcNNN.txt`, par exemple `https://www.ietf.org/rfc/rfc5001.txt`