Les retards du serveur racine C

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 22 mai 2024. Dernière mise à jour le 23 mai 2024

https://www.bortzmeyer.org/c-root-retard.html

On fait souvent remarquer que c'est pendant les pannes qu'on peut le mieux observer comment un système marche. Les perturbations qui affectent le serveur racine du DNS identifié par la lettre C sont donc l'occasion d'apprendre comment fonctionne ce système des serveurs racine.

À la racine du DNS, se trouvent treize serveurs (≪ serveur ≫ au sens virtuel car cela fait évidemment bien plus que treize machines), chacun identifié par une lettre de A à M, et nommés dans le domaine `root-servers.net`. Un programme comme check-soa <https://framagit.org/bortzmeyer/check-soa/> permet de les voir en action (l'option `-i` permet d'avoir le temps de réponse), ici le 22 mai à 08 :47 :24 UTC :

```
% check-soa -i .
a.root-servers.net.
2001:503:ba3e::2:30: OK: 2024052200 (14 ms)
198.41.0.4: OK: 2024052200 (15 ms)
b.root-servers.net.
2801:1b8:10::b: OK: 2024052200 (14 ms)
170.247.170.2: OK: 2024052200 (14 ms)
c.root-servers.net.
2001:500:2::c: OK: 2024052101 (25 ms)
192.33.4.12: OK: 2024052101 (25 ms)
d.root-servers.net.
2001:500:2d::d: OK: 2024052200 (4 ms)
199.7.91.13: OK: 2024052200 (5 ms)
e.root-servers.net.
192.203.230.10: OK: 2024052200 (6 ms)
2001:500:a8::e: OK: 2024052200 (6 ms)
f.root-servers.net.
2001:500:2f::f: OK: 2024052200 (6 ms)
192.5.5.241: OK: 2024052200 (6 ms)
g.root-servers.net.
2001:500:12::d0d: OK: 2024052200 (52 ms)
192.112.36.4: OK: 2024052200 (65 ms)
h.root-servers.net.
2001:500:1::53: OK: 2024052200 (11 ms)
198.97.190.53: OK: 2024052200 (14 ms)
i.root-servers.net.
192.36.148.17: OK: 2024052200 (10 ms)
```

```
2001:7fe::53: OK: 2024052200 (10 ms)
j.root-servers.net.
2001:503:c27::2:30: OK: 2024052200 (15 ms)
192.58.128.30: OK: 2024052200 (14 ms)
k.root-servers.net.
2001:7fd::1: OK: 2024052200 (8 ms)
193.0.14.129: OK: 2024052200 (14 ms)
l.root-servers.net.
199.7.83.42: OK: 2024052200 (15 ms)
2001:500:9f::42: OK: 2024052200 (14 ms)
m.root-servers.net.
2001:dc3::35: OK: 2024052200 (4 ms)
202.12.27.33: OK: 2024052200 (5 ms)
```

(Le point désigne la racine.)

Avez-vous remarqué le problème ? L'un des serveurs, `C.root-servers.net`, est en retard. Le numéro de série dans l'enregistrement SOA est 2024052101 alors que tous les autres sont à 2024052200. Dans le cas de la racine (c'est une convention courante mais pas du tout obligatoire), le numéro de série indique la date de modification, on voit donc qu'il est resté à hier, 21 mai.

C'était pire avant : du 18 au 21 mai, ce serveur est resté en 2024051801, ignorant donc tout changement qui aurait pu avoir lieu dans le contenu de la racine (heureusement, il n'y en a eu aucun pendant cette période) :

```
% date -u
Tue 21 May 20:03:11 UTC 2024

% check-soa -i .
a.root-servers.net.
198.41.0.4: OK: 2024052101 (23 ms)
2001:503:ba3e::2:30: OK: 2024052101 (96 ms)
b.root-servers.net.
170.247.170.2: OK: 2024052101 (23 ms)
2801:1b8:10::b: OK: 2024052101 (84 ms)
c.root-servers.net.
192.33.4.12: OK: 2024051801 (22 ms)
2001:500:2::c: OK: 2024051801 (22 ms)
d.root-servers.net.
199.7.91.13: OK: 2024052101 (16 ms)
2001:500:2d::d: OK: 2024052101 (16 ms)
e.root-servers.net.
192.203.230.10: OK: 2024052101 (16 ms)
2001:500:a8::e: OK: 2024052101 (16 ms)
f.root-servers.net.
192.5.5.241: OK: 2024052101 (22 ms)
2001:500:2f::f: OK: 2024052101 (96 ms)
g.root-servers.net.
2001:500:12::d0d: OK: 2024052101 (54 ms)
192.112.36.4: OK: 2024052101 (66 ms)
h.root-servers.net.
198.97.190.53: OK: 2024052101 (23 ms)
2001:500:1::53: OK: 2024052101 (96 ms)
i.root-servers.net.
192.36.148.17: OK: 2024052101 (23 ms)
2001:7fe::53: OK: 2024052101 (23 ms)
j.root-servers.net.
192.58.128.30: OK: 2024052101 (23 ms)
2001:503:c27::2:30: OK: 2024052101 (96 ms)
k.root-servers.net.
2001:7fd::1: OK: 2024052101 (23 ms)
```

```
193.0.14.129: OK: 2024052101 (22 ms)
l.root-servers.net.
199.7.83.42: OK: 2024052101 (16 ms)
2001:500:9f::42: OK: 2024052101 (22 ms)
m.root-servers.net.
2001:dc3::35: OK: 2024052101 (16 ms)
202.12.27.33: OK: 2024052101 (16 ms)
```

Le serveur C est "*anycasté*" donc le test ci-dessus laisse ouverte la possibilité d'un problème spécifique à l'instance à laquelle je parle. Mais une mesure faite avec les sondes RIPE Atlas <https://atlas.ripe.net/> montre que non, le problème touche presque toutes les instances :

```
% blaeu-resolve --requested 200 --nsid --type SOA --nameserver c.root-servers.net .
Nameserver c.root-servers.net
[NSID: lax1a.c.root-servers.org; ... 2024051801 1800 900 604800 86400] : 10 occurrences
[NSID: fra1b.c.root-servers.org; ... 2024051801 1800 900 604800 86400] : 37 occurrences
[NSID: mad1a.c.root-servers.org; ... 2024051801 1800 900 604800 86400] : 5 occurrences
[NSID: rio1a.c.root-servers.org; ... 2024051801 1800 900 604800 86400] : 2 occurrences
[NSID: fra1a.c.root-servers.org; ... 2024051801 1800 900 604800 86400] : 37 occurrences
[NSID: iad1b.c.root-servers.org; ... 2024051801 1800 900 604800 86400] : 10 occurrences
[NSID: lax1b.c.root-servers.org; ... 2024052101 1800 900 604800 86400] : 8 occurrences
[NSID: sin1b.c.root-servers.org; ... 2024051801 1800 900 604800 86400] : 3 occurrences
[NSID: par1b.c.root-servers.org; ... 2024051801 1800 900 604800 86400] : 20 occurrences
[NSID: par1a.c.root-servers.org; ... 2024051801 1800 900 604800 86400] : 20 occurrences
[TIMEOUT] : 9 occurrences
[NSID: mad1b.c.root-servers.org; ... 2024051801 1800 900 604800 86400] : 1 occurrences
[NSID: iad1a.c.root-servers.org; ... 2024051801 1800 900 604800 86400] : 7 occurrences
[NSID: sin1a.c.root-servers.org; ... 2024051801 1800 900 604800 86400] : 1 occurrences
[NSID: bts1a.c.root-servers.org; ... 2024051801 1800 900 604800 86400] : 4 occurrences
[NSID: ord1a.c.root-servers.org; ... 2024051801 1800 900 604800 86400] : 9 occurrences
[NSID: jfk1b.c.root-servers.org; ... 2024051801 1800 900 604800 86400] : 1 occurrences
[NSID: bts1b.c.root-servers.org; ... 2024051801 1800 900 604800 86400] : 6 occurrences
[NSID: ord1b.c.root-servers.org; ... 2024051801 1800 900 604800 86400] : 3 occurrences
[NSID: jfk1a.c.root-servers.org; ... 2024051801 1800 900 604800 86400] : 2 occurrences
[... 2024052100 1800 900 604800 86400] : 1 occurrences
Test #72103734 done at 2024-05-21T20:15:03Z
```

Quelles sont les conséquences pratiques pour les utilisateurices ? Si leur résolveur <https://www.bortzmeyer.org/resolveur-dns.html> interroge C (ce qui dépend d'un certain nombre de facteurs, dont le temps de réponse des différents serveurs faisant autorité <https://www.bortzmeyer.org/serveur-dns-faisant-autorite.html>), ledit résolveur aura des informations peut-être dépassées. Ainsi, ce matin du 22 mai, on voit que le TLD .int a publié hier un nouvel enregistrement DS (dans le cadre de sa migration vers la cryptographie en courbes elliptiques) mais le serveur C ne le voit toujours pas :

```
% dig +short  @a.root-servers.net int DS
59895 13 2 10C789F286599316D3A74C2C513434C3F8A33B9238976D5DE2A178E5 4DA353F3
27433 7 2 5864812D4DF2A4A455D905AF311389F479AFCD96FD369060941C7E17 0B40CA4F

% dig +short  @c.root-servers.net int DS
27433 7 2 5864812D4DF2A4A455D905AF311389F479AFCD96FD369060941C7E17 0B40CA4F
```

Un problème identique se pose pour .gov qui planifiait la même transition vers ECDSA et a dû la retarder <https://lists.dns-oarc.net/pipermail/dns-operations/2024-May/022566.html>.

Cela sera encore pire si un TLD était redélégué ou si les signatures DNSSEC servies par C finissaient par expirer.

Que peut-on faire ? Pas grand'chose. Le gestionnaire du serveur C, Cogent va peut-être réparer mais on ne sait pas quand et on n'a pas d'informations. Techniquement, il serait possible de retirer C de la liste des serveurs racine <https://dns.bortzmeyer.org/root/NS> ou bien de confier C à un autre opérateur, mais personne n'a le droit et/ou l'autorité de supprimer ou de réaffecter un serveur racine. Contrairement à ce qu'écrivent les journalistes, l'ICANN n'est pas régulateur du DNS, encore moins de l'Internet et ne peut donc pas agir. (La liste des serveurs et de leurs opérateurs est disponible en ligne <https://root-servers.org/>.)

Le problème a finalement été réparé vers le 23 mai, d'abord sans explications et sans communication de la part de Cogent, puis finalement par un court texte sur leur site Web <https://c.root-servers.org/> : « *"2024[Caractère Unicode non montré [1]]05[Caractère Unicode non montré]23 - On May 21 at 15 :30 UTC the c-root team at Cogent Communications was informed that the root zone as served by c-root had ceased to track changes from the root zone publication server after May 18. Analysis showed this to have been caused by an unrelated routing policy change whose side effect was to silence the relevant monitoring systems. No production DNS queries went unanswered by c-root as a result of this outage, and the only impact was on root zone freshness. Root zone freshness as served by c-root was fully restored on May 22 at 16 :00 UTC."* ».

À noter qu'à peu près au même moment (mais nous ne savons pas s'il s'agit d'une coïncidence ou bien si les deux problèmes sont liés), le site Web d'information sur le serveur C, (notez le .org alors que le serveur DNS est en .net) avait cessé de fonctionner vers le 17 mai. Il utilisait l'adresse IP 38.230.3.4, allouée à Orange Côte d'Ivoire et, depuis le 17 mai, annoncée par eux <https://stat.ripe.net/ui2013/38.230.3.4#tabId=routing> dans BGP.

```
% whois 38.230.3.4
...
Found a referral to rwhois.cogentco.com:4321.

%rwhois V-1.5:0010b0:00 rwhois.cogentco.com (CGNT rwhoisd 1.2.0)
network:ID:NET4-26E6000011
network:Network-Name:NET4-26E6000011
network:IP-Network:38.230.0.0/17
network:Org-Name:Orange Cote d'Ivoire
network:Street-Address:CABLE SAT3 CLS, RUA AMÉLIA FRADE
  network:City:SESIMBRA
network:Country:PT
network:Postal-Code:2970 { 712
network:Tech-Contact:ZC108-ARIN
network:Updated:2024-05-10 16:33:20
```

Orange Côte d'Ivoire est un client de Cogent et, manifestement, Cogent avait délégué ce préfixe à son client sans remarquer qu'ils l'utilisaient pour C.root-servers.org. Ou bien ils ne s'étaient pas aperçus du problème car, en interne, cela marchait, en raison d'une route plus spécifique <https://lists.dns-oarc.net/pipermail/dns-operations/2024-May/022562.html>. (Quand j'ai signalé le problème à Cogent, l'employé avait répondu que ça marchait pour lui. De manière très peu professionnelle, il testait le service depuis sa machine, sur le réseau interne de son employeur.)

Il n'y avait donc aucun détournement BGP, contrairement à ce qui a parfois été écrit, l'annonce d'Orange Côte d'Ivoire est parfaitement légitime. Le service Web a désormais une autre adresse IP

1. Car trop difficile à faire afficher par LaTeX

<https://dns.bortzmeyer.org/c.root-servers.org> et qui fonctionne, ce qui permet de voir le site et de constater qu'il n'y avait aucune information publiée avant le 23 mai :

(Merci à Bert Hubert pour avoir détecté le problème de synchronisation du serveur DNS racine C, à Jan-Piet Mens pour avoir détecté le problème avec le serveur Web C.root-servers.org et à Alarig Le Lay pour ses explications sur le routage dans Cogent.)

---

https://www.bortzmeyer.org/c-root-retard.html