Plusieurs domaines de premier niveau en panne

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 7 octobre 2021

https://www.bortzmeyer.org/panne-godaddy.html

Le monde des noms de domaine a vu aujourd'hui un incident rare : la panne complète d'un TLD, .club, et même de plusieurs autres.

Commençons par les faits : ce jeudi 7 octobre, vers 1035 UTC, plus moyen de résoudre aucun nom de domaine en .club. Tous les résolveurs <https://www.bortzmeyer.org/resolveur-dns.html> renvoyaient le code de retour SERVFAIL ("*SERver FAILure*"). Une telle panne complète d'un TLD est rare (la dernière de .com a eu lieu en 1997 <https://www.bortzmeyer.org/panne-com.html>).

Pour le débogage, on peut regarder les jolies images de DNSviz <https://dnsviz.net/d/powerdns.club/YV7Mpg/dnssec/>, ou bien utiliser dig :

```
%  dig NS club

; <<>> DiG 9.16.21 <<>> NS club
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: SERVFAIL, id: 30784
;; flags: qr rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags: do; udp: 1232
;; QUESTION SECTION:
;club. IN NS

;; Query time: 2606 msec
;; SERVER: 127.0.0.1#53(127.0.0.1)
;; WHEN: Thu Oct 07 13:55:28 CEST 2021
;; MSG SIZE  rcvd: 33
```

Un test avec les sondes RIPE Atlas <https://atlas.ripe.net/> montrait que le problème n'était pas juste avec mon résolveur :

```
% blaeu-resolve --type SOA -r 100 club
[ERROR: SERVFAIL] : 81 occurrences
[ns1.dns.nic.club. admin.tldns.godaddy. 1633603168 1800 300 604800 1800] : 1 occurrences
Test #32444898 done at 2021-10-07T11:55:21Z
```

La raison ? Les serveurs faisant autorité <https://www.bortzmeyer.org/serveur-dns-faisant-autorit
html> pour .club répondaient tous SERVFAIL :

```
 dig @2610:a1:1076::d7 SOA club

; <<>> DiG 9.16.21 <<>> @2610:a1:1076::d7 SOA club
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: SERVFAIL, id: 58363
;; flags: qr rd; QUERY: 1, ANSWER: 0, AUTHORITY: 0, ADDITIONAL: 1
;; WARNING: recursion requested but not available

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags: do; udp: 4096
;; QUESTION SECTION:
;club. IN SOA

;; Query time: 66 msec
;; SERVER: 2610:a1:1076::d7#53(2610:a1:1076::d7)
;; WHEN: Thu Oct 07 13:57:39 CEST 2021
;; MSG SIZE  rcvd: 33
```

Contrairement à la récente panne de Facebook <https://www.bortzmeyer.org/facebook-octobre-2021
html>, il ne s'agissait donc pas d'un problème de routage ; les serveurs répondaient bien, mais mal. (Typiquement, quand un serveur faisant autorité répond SERVFAIL, c'est qu'il n'a pas pu charger les données de la zone, par exemple suite à une erreur de syntaxe dans le fichier de zone.)

Le TLD .hsbc (même opérateur technique de registre et même hébergeur DNS) a été frappé de la même façon :

```
% blaeu-resolve --type SOA -r 100 hsbc
[ERROR: SERVFAIL] : 90 occurrences
[ns1.dns.nic.hsbc. admin.tldns.godaddy. 1633405738 1800 300 604800 1800] : 1 occurrences
Test #32445325 done at 2021-10-07T12:23:28Z
```

La panne semble avoir été complètement résolue vers 1410 UTC :

```
% blaeu-resolve --type SOA -r 100 club
[ns1.dns.nic.club. admin.tldns.godaddy. 1633615537 1800 300 604800 1800] : 90 occurrences
[ns1.dns.nic.club. admin.tldns.godaddy. 1633613754 1800 300 604800 1800] : 1 occurrences
[ns1.dns.nic.club. admin.tldns.godaddy. 1633615179 1800 300 604800 1800] : 4 occurrences
Test #32446901 done at 2021-10-07T14:14:47Z
```

Quelques informations publiques :

— Le fil de l'incident <https://status.ultradns.neustar/pages/incident/5f80d63ea1c48e04c1dfa100615ee7dd272a3a053aefce50>, par l'hébergeur DNS UltraDNS/Neustar. Si la chronologie est correcte, on notera par contre que cette communication officielle parle de "*timeouts*" et de retards, ce qui n'est pas exact (comme on l'a vu plus haut, les serveurs répondaient, et vite). Autre fausseté : la panne affectait le monde entier, contrairement à ce que dit cette communication.
— Le tweet du registre <https://twitter.com/getDotClub/status/1446118781856595969> et celui de son opérateur technique <https://twitter.com/GoDaddyRegistry/status/1446124321324220417> (très sommaires !).
— La panne vue par un des bureaux d'enregistrement de .club <https://www.namecheap.com/status-updates/archives/63707>.
— Et vue par un utilisateur <https://community.cloudflare.com/t/domain-down-cloudflare-response313008>.
— Les opérateurs de gros résolveurs ont aussi vu le problème <https://twitter.com/CloudflareHelp/status/1446091625323708423>.
— Un article du site d'information sur les noms de domaine DomainIncite <http://domainincite.com/27084-breaking-club-the-whole-tld-just-went-down>.