Le TLD du Gabon en panne depuis quatre mois

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 12 janvier 2012

https://www.bortzmeyer.org/tld-gabon.html

Depuis septembre 2011, le TLD du Gabon, .ga est en panne quasi-complète. Quelle est la panne exacte ? Pourquoi cette panne ? Que fait le gouvernement ? Quelles sont les conséquences pour le reste du DNS ?

La panne a commencé le 13 septembre mais ses conséquences n'ont pas été visibles tout de suite. Le serveur maître à Libreville a commencé par refuser à ses esclaves les transferts de zone (RFC 5936 [1]). Le champ « expiration » dans l'enregistrement SOA de .ga étant de 42 jours, les esclaves ont fini par renoncer le 27 octobre, répondant SERVFAIL (Server Failure) :

```
% dig @b.hosting.nic.fr. SOA ga.
...
;; ->>HEADER<<- opcode: QUERY, status: SERVFAIL, id: 48352
...
```

Cela concerne les deux esclaves extérieurs, un à l'AFNIC et un au RIPE-NCC. Et les deux serveurs situés dans le pays ? Leur comportement est plus bizarre. Souvent, ils ne répondent pas (et ce n'est pas un problème réseau, puisqu'un ping fonctionne) :

```
% ping -c 3 nyali.inet.ga
PING nyali.inet.ga (217.77.71.33) 56(84) bytes of data.
64 bytes from nyali.inet.ga (217.77.71.33): icmp_req=1 ttl=241 time=366 ms
64 bytes from nyali.inet.ga (217.77.71.33): icmp_req=2 ttl=241 time=365 ms
64 bytes from nyali.inet.ga (217.77.71.33): icmp_req=3 ttl=241 time=377 ms

--- nyali.inet.ga ping statistics ---
```

1. Pour voir le RFC de numéro NNN, https://www.ietf.org/rfc/rfcNNN.txt, par exemple https://www.ietf.org/rfc/rfc5936.txt

```
3 packets transmitted, 3 received, 0% packet loss, time 1999ms
rtt min/avg/max/mdev = 365.277/369.877/377.792/5.664 ms

% dig @nyali.inet.ga. SOA ga.

; <<>> DiG 9.7.3 <<>> @nyali.inet.ga. SOA ga.
; (1 server found)
;; global options: +cmd
;; connection timed out; no servers could be reached
```

Plus rigolo, la réponse peut dépendre du type de données demandé :

```
% dig @nyali.inet.ga. ga. SOA

; <<>> DiG 9.7.3 <<>> @nyali.inet.ga. ga. SOA
; (1 server found)
;; global options: +cmd
;; connection timed out; no servers could be reached

% dig @nyali.inet.ga. ga. NS

; <<>> DiG 9.7.3 <<>> @nyali.inet.ga. ga. NS
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 16007
;; flags: qr rd ra; QUERY: 1, ANSWER: 4, AUTHORITY: 0, ADDITIONAL: 6

;; QUESTION SECTION:
;ga.                            IN      NS

;; ANSWER SECTION:
ga.                     15900   IN      NS      ns-ga.ripe.net.
ga.                     15900   IN      NS      nyali.inet.ga.
ga.                     15900   IN      NS      b.hosting.nic.fr.
ga.                     15900   IN      NS      ogooue.inet.ga.
...
```

Lorsqu'ils répondent, le code de retour renvoyé par les serveurs est `FORMERR` si on a essayé avec EDNS0 (RFC 2671), ce qui est pourtant le comportement normal d'un résolveur DNS (rappelez-vous que dig, par défaut, n'avait pas le même comportement qu'un vrai résolveur, il n'activait pas EDNS0 ; ce comportement par défaut a changé récemment) :

```
 % dig +bufsize=1400 @nyali.inet.ga. ga. ANY

; <<>> DiG 9.7.3 <<>> +bufsize=1400 @nyali.inet.ga. ga. ANY
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: FORMERR, id: 4032
;; flags: qr rd ra; QUERY: 0, ANSWER: 0, AUTHORITY: 0, ADDITIONAL: 0

;; Query time: 370 msec
;; SERVER: 217.77.71.33#53(217.77.71.33)
;; WHEN: Thu Jan 12 11:13:11 2012
;; MSG SIZE  rcvd: 12
```

```
% dig @nyali.inet.ga. ga. ANY

; <<>> DiG 9.7.3 <<>> @nyali.inet.ga. ga. ANY
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 32644
;; flags: qr rd ra; QUERY: 1, ANSWER: 4, AUTHORITY: 4, ADDITIONAL: 6

;; QUESTION SECTION:
;ga.                            IN      ANY

;; ANSWER SECTION:
ga.                     7189    IN      NS      ogooue.inet.ga.
ga.                     7189    IN      NS      ns-ga.ripe.net.
ga.                     7189    IN      NS      nyali.inet.ga.
ga.                     7189    IN      NS      b.hosting.nic.fr.
...
```

Comme il n'y a plus guère de logiciels serveurs qui ne gèrent pas EDNS0, douze ans après sa normalisation, le plus probable est qu'il y a **devant** le serveur DNS une "*middlebox*" boguée (pléonasme, vu le niveau de qualité du logiciel de la plupart de ces équipements). C'est sans doute elle qui répond aux ping, et massacre les questions et/ou les réponses DNS.

Si on ne met pas EDNS0, le serveur répond, mais sans le bit AA ("*Authoritative Answer*"), ce qui est anormal pour un serveur faisant autorité <https://www.bortzmeyer.org/serveur-dns-faisant-autorite.html> (vues les données renvoyées en réponse à une requête `ANY`, il est probable que ce serveur ne contienne plus les données de la zone `.ga`). Donc, on peut dans certains cas, certains jours, avoir une réponse des serveurs de `.ga` mais uniquement si on les interroge sans EDNS0. Certains résolveurs se rabattent automatiquement sur le vieux DNS, sans EDNS0, lorsqu'ils ne reçoivent pas de réponse. Pour le cas où ils reçoivent `FORMERR`, le RFC 2671, section 5.3 dit qu'ils doivent en effet réessayer, ce que Christophe Deleuze a testé rapidement : il semble que BIND9 répète la requête sans EDNS0, et cache l'info (n'utilise plus EDNS0 avec ce serveur dans les requêtes suivantes). Unbound répète la requête sans EDNS0 mais semble ne pas cacher l'info, car il retente avec EDNS0 à la prochaine requête.

Donc, dans beaucoup de cas, `.ga` est quasiment inutilisable.

Que s'est-il passé ? Sans être sur place, et sans nouvelles des gérants du TLD, on ne peut que faire des hypothèses. Le plus probable est que le vrai serveur est en panne et que la "*middlebox*", placée devant (une mauvaise architecture, mais passons), n'assure plus qu'une partie des fonctions (je sais, cela n'explique pas tout). Le fait d'avoir plusieurs serveurs DNS faisant autorité <https://www.bortzmeyer.org/serveur-dns-faisant-autorite.html> n'aide pas lorsque le maître est panne trop longtemps (les 42 jours de grâce étant écoulés).

Pourquoi personne ne répare-t-il ? Le problème aurait dû être détecté par les administrateurs de `.ga`, Gabon Télécom. Sinon, il a été signalé par courrier électronique en décembre 2011 (et pas seulement à des adresses en `.ga`, évidemment), et par fax, pour augmenter les chances de réussite. Aucune réaction. Il faut bien se rappeler deux choses : les bases de données des administrateurs de TLD (ici, la base IANA sur .GA <https://www.iana.org/domains/root/db/ga.html>) sont maintenues par les administrateurs eux-mêmes. S'ils sont empêchés, ou bien irresponsables, la base va dériver petit à petit et les informations (noms, numéros, etc) devenir dépassées. Et, d'autre part, la réparation nécessite que quelqu'un agisse (les pannes ne se réparent pas seules). Le Gabon n'est pas un état de droit et une des conséquences de ce système politique est que personne ne prend d'initiatives (c'est trop risqué). Donc, tous les officiels restent les bras ballants. Le problème n'est pas d'argent (le Gabon est un pays

relativement riche, grâce au pétrole), ni la compétence (des tas de gens compétents sur l'Internet sont prêts à aider leurs collègues gabonais, si ceux-ci répondaient) mais de responsabiité.

Et pour le reste de l'arbre du DNS, quelles conséquences ? À peu près aucune. La structure non-centralisée du DNS fait que la panne d'un TLD n'affecte pas les autres. Contrairement à ce que prétend l'ICANN (qui justifie ainsi les tarifs colossaux de ses nouveaux TLD <http://newgtlds.icann.org/>), un TLD n'a rien de particulier. C'est un domaine comme un autre ; s'il est en panne, cela ne gène que ses utilisateurs.

À noter qu'un problème du même genre était survenu au Tchad <https://www.bortzmeyer.org/tld-tchad.html>.

Merci à Ed Lewis pour son premier signalement du problème, grâce à son script magique de suivi des TLD, et à Jean-Philippe Pick pour des informations supplémentaires.