Deux exemples d'un problème DNS sur des domaines importants

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 5 août 2023

https://www.bortzmeyer.org/probleme-dns-nc.html

Vous le savez, l'Internet n'est pas un long fleuve tranquille. Il y a des pannes, des attaques, des erreurs…La vie des administrateurs système et réseau est donc rarement ennuyeuse. Ainsi, aujourd'hui, deux domaines importants ont eu des problèmes. Plongeons-nous un peu dans le DNS et ses particularités.

Premier domaine touché, `gouv.nc`, le domaine du gouvernement néo-calédonien. Des utilisateurs se plaignent qu'ils n'arrivent pas à accéder aux services sous ce nom, ni à ceux sous des noms hébergés sur les mêmes serveurs, comme `prix.nc`. Voyons (avec check-soa <https://framagit.org/bortzmeyer/check-soa>) les serveurs faisant autorité <https://www.bortzmeyer.org/serveur-dns-faisant-autorite.html> pour ce domaine :

```
% check-soa -i gouv.nc
ns4.gouv.nc.
61.5.212.4: OK: 2020111850 (293 ms)
ns5.gouv.nc.
61.5.212.5: OK: 2020111850 (293 ms)
```

Ici, tout marche. Mais ce n'est pas le cas tout le temps, on observe de nombreux "*timeouts*" :

```
%    check-soa -i gouv.nc
ns4.gouv.nc.
61.5.212.4: ERROR: read udp 192.168.2.4:33577->61.5.212.4:53: i/o timeout
ns5.gouv.nc.
61.5.212.5: ERROR: read udp 192.168.2.4:41598->61.5.212.5:53: i/o timeout
```

On le voit aussi en utilisant les sondes RIPE Atlas <https://atlas.ripe.net/> (via le programme Blaeu <https://labs.ripe.net/author/stephane_bortzmeyer/creating-ripe-atlas-one-off-m>) :

```
% blaeu-resolve --type A --requested 100 gouv.nc
[ERROR: SERVFAIL] : 40 occurrences
[61.5.212.17] : 22 occurrences
Test #58257507 done at 2023-08-05T18:32:26Z
```

Pourquoi ce problème ? De l'extérieur, je ne peux évidemment pas donner de réponse définitive mais j'observe déjà que ce domaine n'a que deux serveurs de noms, ce qui est souvent insuffisant, et que la proximité de leurs adresses IP fait fortement soupçonner qu'ils sont dans la même pièce, formant un SPOF. Y a-t-il eu une panne complète, par exemple une coupure de courant dans cette pièce ? Comme on observe que ces serveurs répondent parfois, on peut écarter cette hypothèse et penser plutôt, soit à une dégradation importante du réseau (réseau surchargé, ou bien physiquement abimé), soit à une attaque par déni de service. Ces attaques, sous leur forme la plus simple, volumétrique (l'attaquant envoie simplement le plus possible de requêtes), saturent le réseau ou les serveurs. Dans ce cas, les serveurs répondent encore parfois, mais pas toujours. Comme le problème a été souvent observé ces derniers mois <https://www.bortzmeyer.org/service-public-impots-dns.html>, et que le domaine `gouv.nc` a les mêmes caractéristiques (domaine d'un service public français, et hébergement DNS très faible), il n'est pas impossible qu'il soit victime de la même campagne d'attaques.

Et le deuxième domaine ? C'est `impots.gouv.fr`, qui a lui aussi les mêmes caractéristiques, quoique moins marquées, et qui faisait déjà partie des victimes précédentes.

```
% check-soa impots.gouv.fr
dns1.impots.gouv.fr.
145.242.11.22: ERROR: read udp 192.168.2.4:35263->145.242.11.22:53: i/o timeout
dns2.impots.gouv.fr.
145.242.31.9: OK: 2023080400
```

Et, avec les sondes Atlas :

```
% blaeu-resolve --type A --requested 100 --country FR impots.gouv.fr
[145.242.11.100] : 55 occurrences
[ERROR: SERVFAIL] : 14 occurrences
Test #58257393 done at 2023-08-05T18:25:42Z
```

On notera que `gouv.nc` a une autre caractéristique, que n'a pas le domaine des impôts : les TTL sont très bas. On le voit avec dig :

```
%  dig @61.5.212.4 gouv.nc A
;; communications error to 61.5.212.4#53: timed out
;; communications error to 61.5.212.4#53: timed out
...
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 2499
;; flags: qr aa rd; QUERY: 1, ANSWER: 1, AUTHORITY: 2, ADDITIONAL: 3
...
;; ANSWER SECTION:
gouv.nc. 30 IN A 61.5.212.17

;; AUTHORITY SECTION:
gouv.nc. 300 IN NS ns4.gouv.nc.
gouv.nc. 300 IN NS ns5.gouv.nc.
...
;; Query time: 292 msec
;; SERVER: 61.5.212.4#53(61.5.212.4) (UDP)
```

Le TTL pour l'adresse IP associée à gouv.nc est de seulement 30 secondes. Cela veut dire que, même si un client DNS, comme un résolveur <https://www.bortzmeyer.org/resolveur-dns.html> a de la chance et réussit à obtenir une réponse d'un des serveurs faisant autorité, elle ne lui servira que pendant trente secondes, suite auxquelles il devra retenter sa chance, avec une forte probabilité que ça rate. C'est en effet un des plus gros inconvénients des TTL extrêmement bas, comme ceux-ci : ils aggravent considérablement les effets des dénis de service. Les variations d'une mesure à l'autre sont donc bien plus marquées pour gouv.nc que pour impots.gouv.fr.

Le TTL des enregistrements NS (serveurs de noms) est plus long (cinq minutes). Notez que celui affiché ci-dessus est le TTL indiqué par les serveurs faisant autorité, celui de la zone gouv.nc elle-même. Il y a un autre TTL (une heure) dans la délégation depuis .nc, dans la zone parente :

```
%  dig @ns1.nc gouv.nc A
...
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 30267
;; flags: qr rd; QUERY: 1, ANSWER: 0, AUTHORITY: 6, ADDITIONAL: 3
...
;; AUTHORITY SECTION:
gouv.nc. 3600 IN NS ns4.gouv.nc.
gouv.nc. 3600 IN NS ns5.gouv.nc.
```

La plupart des résolveurs enregistreront le TTL de la zone (ici, cinq minutes), qui, lui, fait autorité (regardez le "*flag*" aa - "*Authoritative Answer*" - dans la réponse).

Pour mieux évaluer l'état d'un serveur de noms (résolveur ou serveur faisant autorité) lors d'un problème comme une attaque par déni de service, j'ai fait un petit script (en ligne sur https://www.bortzmeyer.org/files/assess-dos.py) en Python simple qui interroge le serveur plusieurs fois et affiche le taux de réussite :

```
% python assess-dos.py  --server 145.242.31.9   impots.gouv.fr
Expect an answer in more or less 300.0 seconds
2 requests among 10 (20.0 %) succeeded. Average time 0.010 s. Measurement done on 2023-08-05T18:46:30Z.
```

Le script dispose de plusieurs options utiles (pour l'instant, sa seule documentation est le code source (en ligne sur https://www.bortzmeyer.org/files/assess-dos.py)) : le nombre de requêtes à faire, l'écart entre deux requêtes, la gigue à ajouter, le délai d'attente maximum, le serveur à utiliser (par défaut, c'est le résolveur habituel de votre machine), le type d'enregistrement DNS à demander, etc. Voici un exemple pendant le problème, utilisant de nombreuses options :

```
% python assess-dos.py  --number 118 --delay 30.1  --server 145.242.31.9  --jitter 6  --type a impots.gouv.fr
Expect an answer in more or less 3551.8 seconds
0 requests among 118 (0.0 %) succeeded. Average time N/A. Measurement done on 2023-08-05T18:00:16Z.
```

Ici, le serveur de impots.gouv.fr ne répondait pas du tout pendant la mesure.

```
% python assess-dos.py  --number 118 --delay 30.1  --server 61.5.212.4  --jitter 6  --type a gouv.nc
Expect an answer in more or less 3551.8 seconds
19 requests among 118 (16.1 %) succeeded. Average time 0.3 s. Measurement done on 2023-08-05T17:56:51Z.
```

Ici, le serveur de `gouv.nc` répondait encore dans 16 % des cas. C'est très insuffisant, la plupart des résolveurs ne réessaient que trois, quatre ou cinq fois.

Dans le tout premier exemple, on n'avait pas indiqué de serveur, dans ce cas, c'est le résolveur par défaut qui est utilisé. Comme il mémorise les réponses, il vaut mieux indiquer un délai qui soit supérieur au TTL :

```
% python assess-dos.py  --number 113 --delay 30.1    --type a gouv.nc
Expect an answer in more or less 3401.3 seconds
62 requests among 113 (54.9 %) succeeded. Average time 0.350 s. Measurement done on 2023-08-05T18:57:25Z.
```

Traditionnellement, les résolveurs DNS ne renvoyaient guère d'information à leur client en cas d'échec, on était loin de la richesse des codes de retour HTTP. Mais cela a changé avec EDE, les "*Extended DNS Errors*" du RFC 8914 [1]. Demandons au résolveur de Google, on obtient bien le code EDE 22 et une explication :

```
% dig @8.8.8.8 gouv.nc A
...;; ->>HEADER<<- opcode: QUERY, status: SERVFAIL, id: 26442
;; flags: qr rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 0, ADDITIONAL: 1
...
; EDE: 22 (No Reachable Authority): (At delegation gouv.nc for gouv.nc/a)
...
```

1. Pour voir le RFC de numéro NNN, `https://www.ietf.org/rfc/rfcNNN.txt`, par exemple `https://www.ietf.org/rfc/rfc8914.txt`