Météo-France et les nuages sur le DNS

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 12 avril 2023. Dernière mise à jour le 17 avril 2023

https://www.bortzmeyer.org/meteofrance-dns.html

Ce matin, le site Web de Météo-France est en panne. Pourquoi ? Déjà, le nom de domaine `meteofrance.com` ne fonctionne pas. Il faut dire qu'il est mal configuré.

Voyons d'abord ce que voit l'utilisateurice moyen·ne :

Bref, ça ne marche pas. « Problème technique », comme annoncé sur Twitter <https://twitter.com/meteofrance/status/1646051181981061120> :

Creusons maintenant. Presque toutes les transactions sur l'Internet commencent par une requête DNS. Sans le DNS, c'est un peu comme de ne pas avoir d'Internet du tout. Testons le domaine `meteofrance.com` avec dig :

```
% dig A meteofrance.com

; <<>> DiG 9.16.37-Debian <<>> A meteofrance.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: SERVFAIL, id: 19940
;; flags: qr rd; QUERY: 1, ANSWER: 0, AUTHORITY: 0, ADDITIONAL: 0
;; WARNING: recursion requested but not available

;; QUESTION SECTION:
;meteofrance.com. IN A

;; Query time: 5008 msec
;; SERVER: 127.0.0.1#53(127.0.0.1)
;; WHEN: Wed Apr 12 10:18:13 CEST 2023
;; MSG SIZE  rcvd: 33
```

Bon, c'est cassé (SERVFAIL = "*Server Failure*"). Que se passe-t-il ? En demandant aux serveurs de `.com`, on voit que le domaine a deux serveurs de noms (ce qui est insuffisant : la robustesse exige davantage, pour faire face aux pannes) :

```
% dig @f.gtld-servers.net. NS meteofrance.com
...
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 41215
...
;; AUTHORITY SECTION:
meteofrance.com. 172800 IN NS cadillac.meteo.fr.
meteofrance.com. 172800 IN NS vivaldi.meteo.fr.
```

Interrogeons-les directement :

```
%   dig @vivaldi.meteo.fr. NS meteofrance.com
dig: couldn't get address for 'vivaldi.meteo.fr.': failure
```

Ah oui, c'est amusant. `meteo.fr` est également en panne. Pour avoir les adresses IP des serveurs de noms, on ne peut plus compter sur le DNS ? Si, il y a la colle, envoyée par les serveurs de `.fr` :

```
% dig @d.nic.fr NS meteo.fr
...
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 40768
...
;; AUTHORITY SECTION:
meteo.fr. 3600 IN NS cadillac.meteo.fr.
meteo.fr. 3600 IN NS vivaldi.meteo.fr.
...
;; ADDITIONAL SECTION:
cadillac.meteo.fr. 3600 IN A 137.129.1.4
vivaldi.meteo.fr. 3600 IN A 137.129.1.2
```

Seulement deux serveurs, on l'a dit, aucune adresse IPv6 (en 2023 !) et, surtout, on voit de la proximité des deux adresses IP que les deux machines sont au même endroit, et donc forment un SPOF. C'est la plus grave erreur dans la configuration de `meteofrance.com` et `meteo.fr`.

Bon, interrogeons ces adresses IP :

```
% dig @137.129.1.4 NS meteofrance.com

; <<>> DiG 9.16.37-Debian <<>> @137.129.1.4 NS meteofrance.com
; (1 server found)
;; global options: +cmd
;; connection timed out; no servers could be reached
```

Idem pour l'autre (logique, puisqu'ils sont au même endroit). Les deux serveurs ne répondent pas. Un traceroute montre qu'on n'arrive nulle part :

```
% sudo tcptraceroute  137.129.1.4  53
Running:
traceroute -T -O info -p 53 137.129.1.4
traceroute to 137.129.1.4 (137.129.1.4), 30 hops max, 60 byte packets
...
 3  vl387-te2-6-paris1-rtr-021.noc.renater.fr (193.51.184.214)  2.581 ms  2.571 ms  2.561 ms
 4  et-2-0-0-ren-nr-paris1-rtr-131.noc.renater.fr (193.51.180.134)  4.719 ms  4.703 ms  4.692 ms
 5  et-2-0-0-ren-nr-paris2-rtr-131.noc.renater.fr (193.55.204.193)  3.112 ms  3.102 ms  3.088 ms
 6  * * *
 7  83.142.144.35 (83.142.144.35)  2.258 ms  2.482 ms  2.425 ms
 8  83.142.144.34 (83.142.144.34)  2.970 ms  2.951 ms  2.992 ms
 9  206.96.106.212.in-addr.arpa.celeste.fr (212.106.96.206)  14.541 ms  13.816 ms  13.855 ms
10  95.96.106.212.in-addr.arpa.celeste.fr (212.106.96.95)  13.102 ms 7.96.106.212.in-addr.arpa.celeste.fr (212.1
11  149.96.106.212.in-addr.arpa.celeste.fr (212.106.96.149)  15.013 ms  14.821 ms *
12  137.129.20.1 (137.129.20.1)  14.069 ms 35.229.180.159.in-addr.arpa.celeste.fr (159.180.229.35)  15.118 ms 13
13  * * *
14  * * *
15  * * *
16  * * *
...
```

Le réseau qui mène aux serveurs DNS faisant autorité <https://www.bortzmeyer.org/serveur-dns-faisant-html> semble en panne.

Le problème n'est pas spécifique à mon réseau de départ. Les sondes RIPE Atlas <https://atlas.ripe.net/> le voient partout :

```
% blaeu-resolve --requested 100 --type A meteofrance.com
[ERROR: SERVFAIL] : 56 occurrences
[185.86.168.137 185.86.168.138 185.86.168.139 185.86.168.140] : 10 occurrences
Test #52152926 done at 2023-04-12T08:01:45Z
```

Le fait que dix des sondes puissent résoudre le nom en adresse IP est probablement dû à la mémorisation par les résolveurs <https://www.bortzmeyer.org/resolveur-dns.html>,meteofrance.com étant un nom souvent sollicité.

On peut aussi tester avec l'excellent DNSviz <https://dnsviz.net/> (archivage du test <https://dnsviz.net/d/meteofrance.com/ZDZirA/dnssec/>) :

Notez que le site Web est hébergé sur un tout autre réseau et marche bien (si on a la chance d'avoir l'adresse IP dans la mémoire de son résolveur **ou bien** si on colle l'adresse IP 185.86.168.137 en dur dans sa configuration locale, par exemple le /etc/hosts) pendant ce temps…Ça permet de voir le communiqué officiel envoyé pendant le problème :

Vers 14 h UTC, après d'autres changements bizarres (ajouter un troisième serveur de noms qui ne marchait pas davantage), Météo-France est passé chez Cloudflare, et tant pis pour la souveraineté numérique :

```
% check-soa meteofrance.com
cadillac.segui.eu.
2400:cb00:2049:1::a29f:1a33: OK: 2023041200
162.159.26.51: OK: 2023041200
vivaldi.segui.eu.
2400:cb00:2049:1::a29f:1b6c: OK: 2023041200
162.159.27.108: OK: 2023041200
```

(Ne vous fiez pas aux noms, dans le domaine « familial » <http://www.segui.eu/> segui.eu, les adresses IP sont bien celles des serveurs de Cloudflare.) Le problème disparait donc petit à petit au fur et à mesure de la réjuvénation <https://www.bortzmeyer.org/dns-propagation.html> :

```
% blaeu-resolve -r 100 - -type NS meteofrance.com
[cadillac.meteo.fr. vivaldi.meteo.fr.] : 19 occurrences
[cadillac.segui.eu. vivaldi.segui.eu.] : 37 occurrences
[ERROR: SERVFAIL] : 24 occurrences
Test #52160057 done at 2023-04-12T14:23:11Z
```

Depuis la première parution de cet article, plusieurs choses sont à noter :

— Météo-France a mis à jour sa communication <https://meteofrance.com/actualites-et-dossiers/actualites/meteo-france-victime-d1-attaque-informatique> pour expliqur que la cause du problème est une attaque par déni de service (ce qui est possible, vu ce qui a été observé).
— D'autres problèmes <https://www.bortzmeyer.org/service-public-impots-dns.html> dont certains ressemblent beaucoup à celui de Météo-France ont frapé les domains d'autres services publics.
— Le nom des serveurs de noms <https://dns.bortzmeyer.org/meteofrance.com/NS> a encore changé (mais ce sont toujours des machines de Cloudflare), repassant du domaine personnel segui.eu à meteo.fr.