Panne du service DNS chez Microsoft

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 22 novembre 2013

https://www.bortzmeyer.org/microsoft-dns-panne.html

Une grande panne DNS a planté hier soir tous les services de Microsoft, comme Hotmail. Comme d'habitude, l'information diffusée dans les médias et les forums ne vaut pas grand'chose, donc, revenons aux faits.

Les cris ont commencé le 21 novembre vers 2250 UTC sur Twitter. Plein de services ne répondaient plus. Une rapide analyse montrait un problème DNS. Ainsi, en demandant à DNSyo <http://samarudge.github.io/dnsyo/> vers 2301 UTC, on avait « *"I asked 500 servers for NS records related to microsoft.com, 199 responded with records and 301 gave errors"* » (les résolveurs <https://www.bortzmeyer.org/resolveur-dns.html> ouverts interrogés par DNSyo et qui avaient réussi ont en fait utilisé leur cache). Vers 2330 UTC, le problème a disparu.

Le DNS est un service crucial pour toute présence en ligne, puisque quasiment toute opération sur l'Internet commence par des requêtes DNS. Celui-ci doit donc être proprement configuré et géré. Malgré cela, il est régulièrement oublié lors des investissements.

Mais plus précisement, pourquoi est-ce que les résolveurs interrogés par DNSyo n'ont pas pu résoudre `microsoft.com` (ou `xbox.com` ou `outlook.com`, tous hébergés sur les mêmes serveurs et victimes du même problème) ? Regardons vers 2300 UTC :

```
% check-soa -i microsoft.com
ns1.msft.net.
2a01:111:2005::1:1: OK: 2013112102 (146 ms)
65.55.37.62: ERROR: Timeout
ns2.msft.net.
2a01:111:2006:6::1:1: OK: 2013112102 (97 ms)
64.4.59.173: ERROR: Timeout
ns3.msft.net.
2a01:111:2020::1:1: OK: 2013112102 (15 ms)
213.199.180.53: ERROR: Timeout
ns4.msft.net.
2404:f800:2003::1:1: OK: 2013112102 (287 ms)
207.46.75.254: ERROR: Timeout
ns5.msft.net.
2a01:111:200f:1::1:1: OK: 2013112102 (100 ms)
65.55.226.140: ERROR: Timeout
```

C'est le point le plus amusant de la panne, et aucun média ou forum ne l'a noté : le problème ne frappait qu'IPv4. Tous les serveurs répondaient normalement en IPv6. Un résolveur <https://www.bortzmeyer.org/resolveur-dns.html> qui pouvait utiliser IPv6 n'avait donc aucun problème et les services de Microsoft marchaient comme avant. (Vous pouvez tester avec la requête `dig SOA droneaud.org`. Si vous récupérez un `SERVFAIL`, c'est que votre résolveur n'a pas été mis à jour depuis le siècle dernier et ne parle toujours qu'IPv4.)

Bien, cela montre qu'il faut avoir des résolveurs modernes, connectés en IPv6. Mais pourquoi cette curieuse panne ? Qu'est-ce qui a pu rendre tous ces serveurs, situés dans des réseaux très différents, inaccessibles en IPv4 tout en étant joignables en IPv6 ?

J'avoue que je ne sais pas. La liste des serveurs de noms est stable (vu avec DNSDB <https://www.bortzmeyer.org/dnsdb.html>) depuis longtemps. RIPEstat <https://www.bortzmeyer.org/stat-ripe.html>, pas assez réactif, n'a pas encore de données sur cette panne. Une attaque par déni de service sur les machines n'épargnerait pas IPv6 (quoi que, attention, les services IPv4 et IPv6 correspondant à un même nom ne sont pas forcément sur la même machine). C'est encore plus vrai pour une attaque sur le réseau. Une panne d'une machine ou d'un réseau n'allait pas affecter **tous** les serveurs de Microsoft. Donc, pas d'explication simple, on peut se laisser aller à la spéculation. (Microsoft n'a évidemment rien communiqué et ne communiquera rien.)