Panne des résolveurs DNS d'Orange, observations et remarques

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 17 novembre 2016

https://www.bortzmeyer.org/resolveur-dns-en-panne.html

Le 16 novembre, deux pannes successives ont affecté les résolveurs <https://www.bortzmeyer.org/resolveur-dns.html> DNS d'Orange. Que s'est-il passé exactement, et quelles conséquences peut-on en tirer ?

Commençons par les observations. Au moins, il s'agira de faits. Les deux pannes sont survenues approximativement entre 0840 UTC (soit quasiment en même temps que la plénière de l'IETF dont le thème était... « "*Attacks Against the Architecture*" <https://www.ietf.org/blog/2016/10/attack-against-the-archit> » !) et 1030 pour la première, et entre 1315 et 1410 (toujours UTC) pour la seconde. N'ayant pas de compte chez Orange, j'ai utilisé deux sources d'informations, les rézosocios, où d'innombrables messages ont signalé la panne, et les sondes RIPE Atlas <https://labs.ripe.net/Members/stephane_bortzmeyer/using-ripe-atlas-to-debug-network-connectivity-problems>. Pour ces dernières, j'ai demandé des sondes se trouvant dans l'AS 3215, celui d'Orange (notez qu'il abrite des services très différents, ne dépendant pas forcément des mêmes résolveurs <https://www.bortzmeyer.org/resolveur-dns.html> DNS). À ma connaissance, Orange n'a rigoureusement rien communiqué, ni pendant la panne (malgré les innombrables cris lancés par ses clients sur les rézosocios), ni après, donc je ne peux me fier qu'à ces observations. Les messages des utilisateurs d'Orange étaient pour la plupart trop vagues (« rien ne marche »), ne citant même pas un nom de domaine qu'on puisse ensuite tester. Personne hélas pour procéder à une récolte sérieuse de données, par exemple avec dig. Ces messages des utilisateurs ne peuvent donc servir qu'à signaler et confirmer qu'il y avait un gros problème. Mais les sondes Atlas nous en disent davantage.

Que nous montrent-elles ? Je prends par exemple le domaine de l'Université Stanford. Si je veux vérifier qu'il est bien visible, je demande à cent sondes RIPE Atlas de résoudre ce nom en adresse IP :

```
% atlas-resolve --requested 100 online.stanford.edu
[] : 1 occurrences
[171.67.216.22] : 33 occurrences
[171.67.216.23] : 28 occurrences
[171.67.216.21] : 37 occurrences
Test #6935163 done at 2016-11-17T04:56:58Z
```

C'était le lendemain de la panne, et tout marche bien (une seule sonde n'a pas eu de réponse, et cela peut être de la faute de son réseau d'accès). Mais pendant la panne ? On voyait, en se limitant à l'AS 3215, des choses comme :

```
% atlas-resolve --requested 100 --as 3215 online.stanford.edu
[TIMEOUT(S)] : 13 occurrences
[ERROR: SERVFAIL] : 65 occurrences
[171.67.216.22] : 8 occurrences
[171.67.216.23] : 7 occurrences
[171.67.216.21] : 7 occurrences
Test #6934676 done at 2016-11-16T08:53:51Z
```

Regardons de plus près. La majorité des sondes RIPE Atlas situées dans l'AS d'Orange n'a pu résoudre le nom, et a au contraire obtenu un code `SERVFAIL` ("*SERVer FAILure*"), indiquant que le résolveur (je reviens sur ce terme plus loin) utilisé n'a pu joindre aucun des serveurs faisant autorité pour le domaine `stanford.edu`. Pas mal de sondes n'ont simplement pas eu de réponses de leur résolveur à temps.

Mais cette unique observation ne nous permet pas de dire que le problème venait d'Orange. Il est parfaitement possible que ce soit Stanford qui ait des ennuis, panne ou dDoS. Il faut donc, comme toujours lorsqu'on fait des observations scientifiques, comparer avec des mesures faites dans d'autres circonstances. Ici, on va simplement demander aux sondes situées dans un pays voisin, l'Allemagne :

```
% atlas-resolve --requested 100 --country DE online.stanford.edu
[] : 1 occurrences
[171.67.216.22] : 33 occurrences
[171.67.216.23] : 31 occurrences
[171.67.216.21] : 35 occurrences
Test #6934677 done at 2016-11-16T08:54:06Z
```

Au pays de Konrad Zuse, toutes les sondes ou presque ont une réponse. Cela laisse entendre que tout va bien à Stanford et que le problème ne vient pas de l'université californienne. (J'aurais aussi pu tester avec un autre AS français, celui de SFR ou de Free.)

Autre façon de voir que le problème était bien chez Orange et pas du côté des domaines testés, essayer avec d'autres domaines :

```
%  atlas-resolve --requested 100 --as 3215 kotaku.com
[ERROR: SERVFAIL] : 47 occurrences
[151.101.1.34 151.101.129.34 151.101.193.34 151.101.65.34] : 50 occurrences
Test #6934730 done at 2016-11-16T10:10:01Z

% atlas-resolve --requested 100 --as 3215 spotify.com
[194.132.197.147 194.132.198.165 194.132.198.228] : 76 occurrences
[ERROR: SERVFAIL] : 19 occurrences
[TIMEOUT(S)] : 4 occurrences
Test #6934675 done at 2016-11-16T08:52:10Z
```

Tous ces domaines marchaient parfaitement depuis d'autres AS ou d'autres pays.

Donc, problème de résolution DNS chez Orange. Comme l'ont vite découvert bien des utilisateurs, changer de résolveur DNS suffisait à résoudre le problème (ce qu'on pouvait également tester avec ce programme `atlas-resolve` et l'option `--nameserver`).

Notons bien, qu'il s'agissait des **résolveurs** DNS, pas des **serveurs faisant autorité**, comme cela avait été le cas récemment lors de l'attaque contre Dyn <http://www.nextinpact.com/news/101857-dyn-attaque-ddo
htm>. La distinction est cruciale car ces deux types de serveurs DNS n'ont pas grand'chose en commun. Si vous lisez un article qui parle de « serveur DNS » tout court, sans préciser s'il s'agit d'un résolveur ou bien d'un serveur faissant autorité, méfiez-vous, c'est souvent un signe d'ignorance, ou de négligence, de la part de l'auteur de l'article.

Maintenant, les remarques. D'abord, beaucoup de gens (par exemple dans cet article de Numerama <http://www.numerama.com/tech/208908-comment-changer-ses-dns-ubuntu-macos-windows.html>, mais aussi dans d'innombrables tweets) ont suggéré de passer des résolveurs DNS d'Orange (ceux utilisés par défaut par les abonnés à ce FAI) à ceux de Google Public DNS <https://www.bortzmeyer.org/google-dns.html> ou bien à ceux de Cisco OpenDNS <https://www.bortzmeyer.org/opendns-non-merci.html>. La plupart des sociétés à but lucratif doivent payer des commerciaux et des chargés de relation publique pour faire leur publicité, mais Google n'en a pas besoin, ayant des millions de vendeurs bénévoles et enthousiastes parmi ses utilisateurs. Mais ceux qui écoutent ces conseils et passent à Google Public DNS lui donneront les données personelles qui permettent leur propre surveillance <https://www.bortzmeyer.org/surveillance.html> (cf. le RFC 7626 [1] sur le caractère sensible des requêtes DNS). Je ne développe pas davantage ce point ici, Shaft l'a fait mieux que moi <https://www.shaftinc.fr/arretez-google-dns.html>. J'observe que, si ce genre de pannes continue, les utilisateurs français dépendront presque tous, pour une activité critique, d'un résolveur états-unien d'une entreprise privée. Cela devrait logiquement agiter ceux qui nous parlent tout le temps de souveraineté numérique, mais, en général, ces gens ne sont pas intéressés par les problèmes concrets et opérationnels.

Mais alors quelle serait la bonne solution ? Le mieux évidemment est d'utiliser des résolveurs proches, donc a priori dans le cas idéal, ceux de son FAI. Ceux-ci ne devraient pas tomber en panne, le DNS étant absolument indispensable à tout usage de l'Internet. Mais lorsque des pannes aussi longues surviennent, il est normal d'envisager d'autres solutions, et la bonne est certainement d'avoir un résolveur sur son réseau local <https://www.bortzmeyer.org/son-propre-resolveur-dns.html> (pas forcément sur chaque machine), ce qui est facile avec des équipements comme le Turris Omnia <https://www.bortzmeyer.org/turris.html>.

Notez qu'une minorité des sondes RIPE Atlas sont déjà sur un réseau local qui utilise un tel résolveur. Cela explique en partie pourquoi, dans les tests ci-dessus, un certain nombre de sondes arrivaient à résoudre les noms de domaine, même au plus fort de la panne. (Cela n'explique qu'une partie du phénomène. Il semble que certains noms avaient un taux de réussites plus fort que d'autres, ce qui ne peut pas s'expliquer par le choix du résolveur.) Notez qu'on peut avoir l'adresse IP du résolveur utilisé par la sonde (avec l'option `--displayresolvers`) mais que cela ne renseigne pas tellement. D'abord, c'est souvent une adresse IP privée (RFC 1918), ensuite, le premier résolveur vu par la sonde fait fréquemment suivre à un résolveur plus gros, qu'on ne voit pas, et qui peut être ou ne pas être un résolveur « officiel » du FAI. Je vous montre quand même le résultat pour l'une des mesures faites ci-dessus (notez la bogue pour le cas du "*timeout*", où le résolveur n'est pas connu) :

1. Pour voir le RFC de numéro NNN, `https://www.ietf.org/rfc/rfcNNN.txt`, par exemple `https://www.ietf.org/rfc/rfc7626.txt`

```
% atlas-resolve -r 100 --as 3215 --displayresolvers --measurement 6934670  kotaku.com
[ERROR: SERVFAIL] : 27 occurrences (resolvers ['172.31.255.254', '192.168.1.1', '80.10.246.2', '192.168.2.1'
[151.101.1.34 151.101.129.34 151.101.193.34 151.101.65.34] : 69 occurrences (resolvers ['2a01:cb08:898c:fc00
[TIMEOUT(S)] : 4 occurrences (resolvers <__main__.Set instance at 0x7fedc8194f80>)
Test #6934670 done at 2016-11-16T08:44:41Z
```

Deuxième sujet de réflexions sur cette panne, que s'est-il passé ? En l'absence de toute communication de la part d'Orange, on ne peut guère que spéculer. Notons tout de suite qu'il ne s'agissait pas cette fois d'un détournement (comme lorsque Orange avait redirigé Google et Wikipédia vers le Ministère de l'Intérieur <https://www.bortzmeyer.org/google-detourne-par-orange.html>) mais d'une absence de réponse. Cette absence dépendait des domaines. Je n'ai pas eu immédiatement de signalement d'un problème pour un domaine hébergé en France, seulement pour des domaines états-uniens (c'est après, donc trop tard pour les mesures, que j'ai appris que des domaines hébergés en France étaient également touchés). Comme le code de retour `SERVFAIL` indique que le résolveur n'a pas réussi à parler aux serveurs faisant autorité, on peut donc supposer que les liens menant à ces réseaux outre-Atlantique étaient inutilisables. Suite à une erreur de configuration, par exemple dans des ACL ? À un problème de routage vers certaines destinations ? À une attaque par déni de service ? Je ne le sais pas. Mais je me demande bien quelle était la panne ou l'attaque qui pouvait bloquer les résolveurs, tout en laissant passer toutes les autres machines (puisque, une fois qu'on avait un résolveur normal, le trafic n'était pas affecté).