À propos de la panne d'Oxalide

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 16 janvier 2015. Dernière mise à jour le 22 janvier 2015

https://www.bortzmeyer.org/oxalide.html

Ce matin, l'hébergeur Oxalide <http://www.oxalide.com/> a été en panne pendant environ une heure et demie, entraînant l'indisponibilité d'un grand nombre de sites Web, notamment de la presse française.

C'est ainsi que 20 Minutes, l'Express, le Parisien, Slate, Mediapart, Marianne, FranceInfo (mais pas Charlie Hebdo) ont été injoignables. Comme tous les zexperts, je ne sais pas ce qui s'est passé donc je vais me contenter de dire ce que j'ai observé.

Plusieurs de ces sites Web renvoyaient un message « "*504 Gateway Time-out - nginx*" » qui est le message typique de CloudFlare lorsque leurs relais n'arrivent pas à joindre le site réel (CloudFlare n'est pas un CDN, ils n'ont pas une copie du site Web, ils servent juste d'écran, notamment en cas de dDoS).

Oxalide avait arrêté d'envoyer des annonces BGP, le protocole qui sert à annoncer au reste de l'Internet qu'on est joignable. (Pourquoi ? Ne me posez pas la question, j'ai dit que je n'en savais rien.) Voici le "*looking glass*" de Hurricane Electric, <http://lg.he.net>, pendant la panne, le préfixe IP 91.208.181.0 est inconnu :

Voyons les annonces BGP pendant la période de la panne. On utilise pour cela les données de Route-Views <http://www.routeviews.org/>. Elles sont en binaire, au format MRT (RFC 6396 [1]), il faut les transformer en texte avec bgpdump <https://bitbucket.org/ripencc/bgpdump/>. On sait d'après Twitter l'heure approximative de la panne, on va donc récupérer le fichier, le transformer en texte et le fouiller :

```
% wget ftp://archive.routeviews.org/route-views.linx/bgpdata/2015.01/UPDATES/updates.20150116.0845.bz2
% bgpdump  updates.20150116.0845 > updates.20150116.0845.txt
```

1. Pour voir le RFC de numéro NNN, https://www.ietf.org/rfc/rfcNNN.txt, par exemple https://www.ietf.org/rfc/rfc6396.txt

Et explorons ce fichier, avec un éditeur ordinaire. On voit bien la panne. L'annonce du préfixe `91.208.181.0/24` a commencé à être perturbée vers 08 :51 :01 UTC. À noter qu'il existe deux types de mise à jour BGP dans un message, l'annonce de nouvelles routes (`ANNOUNCE`) et le retrait de routes qui ne sont pus bonnes (`WITHDRAW`). Paradoxalement, la disparition d'une route (ici celle vers `91.208.181.0/24`) se traduit d'abord par des `ANNOUNCE` avant d'avoir le premier `WITHDRAW`. En effet, les routeurs BGP tentent de passer par un autre chemin et relaient d'abord les autres informations qu'ils ont, avant de renoncer et de retirer la route. Une panne se signale donc d'abord par une floppée d'`ANNOUNCE`. La première était :

```
TIME: 01/16/15 08:51:01
TYPE: BGP4MP/MESSAGE/Update
FROM: 195.66.224.21 AS6939
TO: 195.66.225.222 AS6447
ORIGIN: IGP
ASPATH: 6939 8218 47841
NEXT_HOP: 195.66.224.21
ANNOUNCE
  91.208.181.0/24
```

À 08 :51 :01 (UTC), le routeur `195.66.224.21` transmet à son pair `195.66.225.222` une nouvelle route vers `91.208.181.0/24`, car il vient de perdre celle qu'il connaissait avant. Dans les secondes qui suivent, des tas d'autres routeurs font pareil avant de se résigner, et de retirer la route :

```
TIME: 01/16/15 08:51:10
TYPE: BGP4MP/MESSAGE/Update
FROM: 195.66.224.175 AS13030
TO: 195.66.225.222 AS6447
WITHDRAW
  ...
  91.208.181.0/24
  ...
```

Attention au passage lorsque vous lisez l'attribut `ASPATH` (chemin d'AS), il se lit de droite à gauche, l'AS d'origine est 47841 (Oxalide).

Une heure et demie après, la route vers `91.208.181.0/24` réapparait (avec les deux autres préfixes IPv4 habituels d'Oxalide <`https://stat.ripe.net/widget/routing-status#w.resource=AS47841`>):

```
TIME: 01/16/15 10:20:13
TYPE: BGP4MP/MESSAGE/Update
FROM: 195.66.224.51 AS6453
TO: 195.66.225.222 AS6447
ORIGIN: IGP
ASPATH: 6453 1299 47841
NEXT_HOP: 195.66.224.51
ANNOUNCE
  95.131.136.0/21
  146.185.40.0/21
  91.208.181.0/24
```

En regardant le "*looking glass*", on voit que tout est revenu :

Enfin, presque, Emile Aben me fait remarquer qu'IPv6 a mis plus de temps, le préfixe `2a02:c70::/32` n'est revenu que vers 11 :15 UTC.

Des articles sur cette panne :

`https://www.bortzmeyer.org/oxalide.html`

— Dans Libération <http://ecrans.liberation.fr/ecrans/2015/01/16/plusieurs-sites-de-la-pres
1181944>
— Dans Rue89 <http://rue89.nouvelobs.com/2015/01/16/nombreux-sites-dinfo-francais-inacces
— Dans le journal du Net <http://www.journaldunet.com/solutions/dsi/20-minutes-l-express-zdne
shtml>
— Oxalide a produit un communiqué, donnant certaines informations techniques <http://www.
oxalide.com/2015/01/retour-sur-lincident-du-16-janvier/> sur la panne.
— Un interview d'un dirigeant d'Oxalide <http://www.silicon.fr/apres-panne-oxalide-explique-1067
html> donne encore des détails.