Panne de routage OVH d'octobre 2021

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 13 octobre 2021

https://www.bortzmeyer.org/routage-ovh-octobre-2021.html

La panne a été vite détectée <https://twitter.com/bortzmeyer/status/1448188569831546880>, vu la taille d'OVH et le nombre d'utilisateurs. Personnellement, c'est Icinga qui m'a notifié vers 0722 UTC : une de mes machines ne répondait plus. Notons tout de suite qu'il n'y a pas eu de problème matériel (contrairement à l'incendie de mars 2021). Les machines dans les centres de données n'ont pas vu de problème et elles continuaient à tourner :

```
% uptime
 10:06:49 up 27 days, 16:20,  1 user,  load average: 0.12, 0.08, 0.07
```

La panne affectait en fait le routage à l'intérieur même de l'AS 16276, celui d'OVH. (Contrairement à la panne de Facebook <https://www.bortzmeyer.org/facebook-octobre-2021.html>, qui, elle, était externe.) Si IPv6 a eu une courte coupure (il est reparti au bout de sept minutes), IPv4 est resté en panne environ une heure (la reprise était vers 0825 UTC).

On peut voir ici (vers 0800 UTC) cette différence IPv4/IPv6 en testant les serveurs DNS faisant autorité <https://www.bortzmeyer.org/serveur-dns-faisant-autorite.html> pour le domaine ovh.net, avec l'outil check-soa <https://www.bortzmeyer.org/check-soa-go.html> : seul le routage IPv4 est resté en panne (IPv6 n'a eu qu'une courte coupure). Exemple vers 0800 UTC :

```
% check-soa -i ovh.net
dns10.ovh.net.
        2001:41d0:1:4a81::1: OK: 2021101333 (4 ms)
        213.251.188.129: ERROR: read udp 92.243.4.211:56767->213.251.188.129:53: i/o timeout
dns11.ovh.net.
        2001:41d0:1:4a82::1: OK: 2021101333 (5 ms)
        213.251.188.130: ERROR: read udp 92.243.4.211:45421->213.251.188.130:53: i/o timeout
dns12.ovh.net.
        2001:41d0:1:4a83::1: OK: 2021101333 (5 ms)
        213.251.188.131: ERROR: read udp 92.243.4.211:58442->213.251.188.131:53: i/o timeout
dns13.ovh.net.
        2001:41d0:1:4a84::1: OK: 2021101333 (5 ms)
        213.251.188.132: ERROR: read udp 92.243.4.211:50141->213.251.188.132:53: i/o timeout
```

```
dns15.ovh.net.
        2001:41d0:1:4a86::1: OK: 2021101333 (5 ms)
        213.251.188.134: ERROR: read udp 92.243.4.211:47705->213.251.188.134:53: i/o timeout
ns10.ovh.net.
        2001:41d0:1:1981::1: OK: 2021101333 (4 ms)
        213.251.128.129: ERROR: read udp 92.243.4.211:38867->213.251.128.129:53: i/o timeout
ns11.ovh.net.
        2001:41d0:1:1982::1: OK: 2021101333 (4 ms)
        213.251.128.130: ERROR: read udp 92.243.4.211:36897->213.251.128.130:53: i/o timeout
ns12.ovh.net.
        2001:41d0:1:1983::1: OK: 2021101333 (4 ms)
        213.251.128.131: ERROR: read udp 92.243.4.211:35883->213.251.128.131:53: i/o timeout
ns13.ovh.net.
        2001:41d0:1:1984::1: OK: 2021101333 (4 ms)
        213.251.128.132: ERROR: read udp 92.243.4.211:51549->213.251.128.132:53: i/o timeout
ns15.ovh.net.
        2001:41d0:1:1986::1: OK: 2021101333 (4 ms)
        213.251.128.134: ERROR: read udp 92.243.4.211:37332->213.251.128.134:53: i/o timeout
```

Tout se passait bien en IPv6, tout échouait en IPv4. Ce n'était pas spécifique au DNS, tous les services avaient le même comportement <https://twitter.com/MatthieuPieres/status/1448198839291240451> ce qui est logique puisqu'ils dépendent tous d'IP. Ici, la visualisation par le logiciel de supervision Icinga (citée dans la phrase précédente) : .

Il est d'ailleurs très dommage que le site Web d'information d'OVH sur les travaux en cours <https://travaux.ovh.net/> n'ait pas d'adresse IPv6...(Idem pour les sites d'information "*corporate*" et technique.)

Et, au passage, cela rappelle pourquoi il ne faut **pas** mettre tous les serveurs DNS faisant autorité pour une zone dans le même AS.

Bien sûr, cette différence entre les deux versions d'IP n'est pas le résultat d'une propriété particulière d'IPv6. Les erreurs dans la configuration, les bogues dans le logiciel du routeur et les imprévus d'un grand réseau arrivent aussi en IPv6. Mais cela explique pourquoi certains services (ceux qui avaient activé IPv6) continuaient à fonctionner, pendant que les autres (qui, en 2021, n'ont toujours pas IPv6 !) étaient injoignables.

La reprise s'est ensuite fait progressivement. Par exemple vers 0823 UTC, on voyait qu'une partie des serveurs DNS faisant autorité étaient à nouveau joignables en IPv4 :

```
% check-soa -i ovh.net
dns10.ovh.net.
2001:41d0:1:4a81::1: OK: 2021101333 (7 ms)
213.251.188.129: ERROR: read udp 92.243.4.211:46201->213.251.188.129:53: i/o timeout
dns11.ovh.net.
2001:41d0:1:4a82::1: OK: 2021101333 (10 ms)
213.251.188.130: ERROR: read udp 92.243.4.211:48037->213.251.188.130:53: i/o timeout
dns12.ovh.net.
2001:41d0:1:4a83::1: OK: 2021101333 (10 ms)
213.251.188.131: ERROR: read udp 92.243.4.211:50868->213.251.188.131:53: i/o timeout
dns13.ovh.net.
2001:41d0:1:4a84::1: OK: 2021101333 (6 ms)
213.251.188.132: ERROR: read udp 92.243.4.211:55136->213.251.188.132:53: i/o timeout
dns15.ovh.net.
2001:41d0:1:4a86::1: OK: 2021101333 (9 ms)
213.251.188.134: ERROR: read udp 92.243.4.211:38200->213.251.188.134:53: i/o timeout
ns10.ovh.net.
2001:41d0:1:1981::1: OK: 2021101333 (13 ms)
```

```
213.251.128.129: OK: 2021101333 (4 ms)
ns11.ovh.net.
2001:41d0:1:1982::1: OK: 2021101333 (11 ms)
213.251.128.130: OK: 2021101333 (12 ms)
ns12.ovh.net.
2001:41d0:1:1983::1: OK: 2021101334 (4 ms)
213.251.128.131: OK: 2021101334 (4 ms)
ns13.ovh.net.
213.251.128.132: OK: 2021101333 (4 ms)
2001:41d0:1:1984::1: OK: 2021101333 (4 ms)
ns15.ovh.net.
213.251.128.134: OK: 2021101333 (4 ms)
2001:41d0:1:1986::1: OK: 2021101333 (4 ms)
```

Une fois tout réparé (ici vers 0830 UTC), tout le monde marchait bien :

```
% check-soa -i ovh.net
dns10.ovh.net.
2001:41d0:1:4a81::1: OK: 2021101333 (11 ms)
213.251.188.129: OK: 2021101333 (11 ms)
dns11.ovh.net.
2001:41d0:1:4a82::1: OK: 2021101333 (9 ms)
213.251.188.130: OK: 2021101333 (9 ms)
dns12.ovh.net.
2001:41d0:1:4a83::1: OK: 2021101333 (8 ms)
213.251.188.131: OK: 2021101333 (8 ms)
dns13.ovh.net.
2001:41d0:1:4a84::1: OK: 2021101333 (9 ms)
213.251.188.132: OK: 2021101333 (10 ms)
dns15.ovh.net.
2001:41d0:1:4a86::1: OK: 2021101333 (12 ms)
213.251.188.134: OK: 2021101333 (4 ms)
ns10.ovh.net.
213.251.128.129: OK: 2021101333 (4 ms)
2001:41d0:1:1981::1: OK: 2021101333 (4 ms)
ns11.ovh.net.
213.251.128.130: OK: 2021101333 (4 ms)
2001:41d0:1:1982::1: OK: 2021101333 (4 ms)
ns12.ovh.net.
213.251.128.131: OK: 2021101334 (4 ms)
2001:41d0:1:1983::1: OK: 2021101334 (4 ms)
ns13.ovh.net.
213.251.128.132: OK: 2021101333 (5 ms)
2001:41d0:1:1984::1: OK: 2021101333 (5 ms)
ns15.ovh.net.
2001:41d0:1:1986::1: OK: 2021101333 (6 ms)
213.251.128.134: OK: 2021101333 (7 ms)
```

La panne était apparemment le résultat d'une maintenance qui était prévue <https://twitter.com/ovh_status/status/1448185498812485633> mais qui a eu des conséquences intattendues. Comme d'habitude, OVH a communiqué sur la panne <http://travaux.ovh.net/?do=details&id=53798> (contrairement à tant d'autres acteurs de l'Internet qui croient qu'en ne parlant pas d'un problème, on ne le verra pas) : « *"Details Start time : 13/10/2021 07 :20 UTC Impact : Since 07 :20 UTC this morning the entire OVH network is unavailable. We are experiencing a network incident located in the United States. All the technical teams are working to resolve the incident Comment : Since 08 :22 UTC all services are gradually returning following the isolation of network equipment in the US."* [Caractère Unicode non montré [1]][Caractère Unicode non montré][Caractère Unicode non montré][Caractère Unicode non montré

1. Car trop difficile à faire afficher par LaTeX

][Caractère Unicode non montré][Caractère Unicode non montré][Caractère Unicode non montré][Caractère Unicode non montré][Caractère Unicode non montré][Caractère Unicode non montré][Caractère Unicode non montré][Caractère Unicode non montré][Caractère Unicode non montré][Caractère Unicode non montré][Caractère Unicode non montré][Caractère Unicode non montré][Caractère Unicode non montré] Heure de début : 13/10/2021 07 :20 UTC Impact : Depuis 07h20 UTC ce matin, l'ensemble du réseau OVH est indisponible. Nous sommes confrontés à un incident réseau situé aux Etats-Unis. Toutes les équipes techniques travaillent à la résolution de cet incident. Comment : Depuis 08 :22 UTC L[Caractère Unicode non montré]ensemble des services reviennent progressivement suite à l[Caractère Unicode non montré]isolation d[Caractère Unicode non montré]un équipement réseau sur aux Etats Unis. » Ce fut également le cas sur Twitter <https://twitter.com/olesovhcom/status/1448196879020433409> et dans le communiqué de presse <https://twitter.com/OVHcloud_FR/status/1448220880396500995>. (VH = Vint Hill)

La cause immédiate de la panne semble être une erreur humaine. Selon un message publié puis supprimé, un technicien a fait une faute de frappe lors d'une commande : . L'erreur portait sur IPv4 (ce qui explique qu'IPv6 n'ait pas eu trop de problèmes) et s'est propagée à tous les routeurs de l'AS. (Séparer complètement le réseau d'OVH en plusieurs AS aurait limité les conséquences de l'erreur ; mais cela aurait rendu la gestion du réseau plus compliquée et donc plus coûteuse.)

Maintenant, les leçons à en tirer. Comme d'habitude en cas de problème, on a vu plein de donneurs de leçons et de rois du yakafokon expliquer doctement tout ce qu'OVH aurait dû faire. Certes, OVH aurait pu mieux faire (on peut toujours s'améliorer). Mais ces consultants à qui on n'avait rien demandé oublient plusieurs choses importantes. La première est qu'un réseau de la taille de celui d'OVH est un objet socio-technique très complexe et qu'il est très difficile de prévoir les conséquences d'une action (ici, la maintenance). Exiger que tous les changements du réseau soit auparavant testés au laboratoire est une bonne idée mais il faut en comprendre les limites : le laboratoire ne sera jamais une reproduction exacte du vrai réseau. Un réseau physique de test est forcément plus petit que le réseau réel, et un réseau virtuel, simulé, ne sera pas identique au réseau réel. Tester, oui, mais ne pas croire que cela attrapera tous les problèmes à l'avance. Comme le dit Shnoulle <https://twitter.com/Shnoulle/status/1448209146961072129>, « Même planifiés, testés et vérifiés : l'erreur est toujours possible. En effet : les tests ne pourront jamais tous couvrir. »

Deuxième chose, le coût. J'utilise OVH, comme beaucoup, parce que ce n'est pas cher. Exiger une fiabilité de centrale nucléaire est irréaliste pour ce prix. S'assurer qu'un réseau fonctionne pendant 99,999 % du temps n'est pas un peu plus cher que de s'assurer qu'il fonctionne pendant 99,99 % du temps, c'est **beaucoup plus cher**. Et cette fiabilité n'est pas indispensable à tous les usages. Que mon blog personnel ou mon résolveur DNS public (plus embêtant, celui-là) soient en panne pendant une heure de temps en temps, ce n'est pas dramatique. Le site de données ouvertes de l'État <https://data.gouv.fr/> a été inaccessible pendant une heure. Et alors ? Ce n'est pas un hôpital ou la police ou l'ANSSI. En tant que contribuable et citoyen, je pense que les responsables de ce site ont bien fait de choisir un hébergement bon marché, quitte à avoir une panne de temps en temps.

Dans son pamphlet « L'enfer numérique <https://www.bortzmeyer.org/enfer-numerique.html> », Guillaume Pitron s'indigne de l'exigence de fiabilité, coûteuse également en termes écologiques. Il a tort, bien sûr, car, contrairement à ce qu'il croit, l'Internet ne sert pas qu'à regarder des vidéos de chats. Mais il a raison sur un point : la fiabilité coûte cher et il peut être parfaitement raisonnable de ne pas chercher 99,999 % de fonctionnement.

(Attention toutefois avec l'argument du coût ; s'il n'y a aucun doute que la qualité - ici, la fiabilité - coûte cher, l'inverse n'est pas vrai. On trouve facilement des hébergeurs plus chers qu'OVH mais pas meilleurs. Il faut entre autres se rappeler qu'on parle des pannes d'OVH car, vu la taille de cet acteur,

les pannes sont très spectaculaires et affectent beaucoup de monde. Un acteur moins connu et qui se prétend plus fiable peut avoir des pannes, aussi, mais qui ne feront pas la une des médias.)

Troisième point, les solutions. Les yakafokons ne proposent en général pas de solutions concrètes, ils se contentent la plupart du temps de proposer des "*process*" (règles bureaucratiques à suivre aveuglément, dans l'espoir d'éliminer l'humain et donc les erreurs humaines). Du genre « aucun changement dans la configuration des routeurs sans la signature de N "*managers*" ». Dans la réalité, ce sont souvent au contraire ces règles qui créent les problèmes, par leur rigidité. Il faut se rappeler que le changement de configuration chez OVH qui a créé le problème était en réponse à un accroissement des attaques par déni de service. Faut-il patienter alors que les attaques sont en cours, au nom du "*process*" ?

Sinon, Numérama a fait un bon article de synthèse <https://www.numerama.com/tech/747034-de-nombreux-
html>.