OVHcloud coupé du monde (en IPv4) : retour sur une panne à l'échelle mondiale

PRA/PCA FTW !

21 • 11

INTERNET 6 MIN

Par Sébastien Gavois
Le mercredi 13 octobre 2021 à 21:00

Signaler une erreur Offrir

Ce matin, certains découvraient que de nombreux sites et services étaient hors-ligne. Démonstration de la forte présence d'OVHcloud sur le web dans de nombreux pays. Une erreur humaine qui a mené à une panne du routage IPv4 qui intervient à quelques jours de l'entrée en bourse du roubaisien.

Ce matin, à 9h12 (heure de Paris), les réseaux sociaux s'agitent car un nombre important de sites sont inaccessibles : Assemblée nationale, Arte, Arrêt sur Images, le site open data du gouvernement… Ils seraient trop nombreux pour les citer tous. Leur point commun est vite trouvé : « *l'ensemble du réseau OVH est indisponible* », reconnait l'hébergeur sur **son site dédié** au support… qui était lui aussi inaccessible durant la panne.

Une erreur aux États-Unis fait tomber tout le réseau

Aux alentours de 10h, Octave Klaba est **intervenu sur Twitter** pour donner quelques précisions : « *Suite à une erreur humaine durant la reconfiguration du network sur notre DC à VH (US-EST), nous avons un souci sur tout le backbone. Nous allons isoler le DC VH puis fixer la conf* ». Il explique que « *ces derniers jours, l'intensité des attaques DDoS a beaucoup augmenté* ». Pour y faire face, l'hébergeur a décidé d'augmenter sa capacité de traitement « *en ajoutant de nouvelles infrastructures dans* [son] *DC VH (US-EST)* ».

On connait la suite : « *une mauvaise configuration du routeur a provoqué la panne* ». Un communiqué officiel reprenant ces éléments à par la suite été **mis en ligne**. Le post mortem **vient d'être publié**. Analyse.

Contrairement à l'incendie de Strasbourg, aucun serveur n'a été touché physiquement : ils continuaient de tourner comme si de rien n'était, comme le confirme Stéphane Bortzmeyer (spécialiste des réseaux) **sur son blog**.

Il donne une précision importante : « *La panne affectait en fait le routage à l'intérieur même de l'AS 16276, celui d'OVH. (Contrairement à la panne de Facebook, 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* [10h25 heure française, ndlr]*)* ». De son côté, OVHcloud parle d'un retour à la normale à 10h22.

Dans son post mortem, l'entreprise détaille la chronologie des évènements : à 09h05 la mise à jour est effectuée comme prévu, 13 minutes plus tard elle est entrée en action, puis à 09h20 « *pendant la modification de la route-map, une erreur est rencontrée : le routeur ne prend pas le dernier caractère de la commande* ». Sur Twitter, Octave Klaba **a évoqué une erreur de copier-coller** dans la matinée avant de retirer le tweet.

L'équipe détecte rapidement le problème et le remonte afin que le processus de gestion de crise se mette en place. Un retour en arrière est tenté à 09h30 mais ne fonctionne pas, un second plan de mitigation intervient à 09h45, à 10h10 est pris la décision de débrancher le routeur posant problème, le retour des services est constaté vers 10h20.

« *Tout se passait bien en IPv6, tout échouait en IPv4. Ce n'était pas spécifique au DNS, tous les services avaient le même comportement, ce qui est logique puisqu'ils dépendent tous d'IP* », résume Bortzmeyer qui en profite pour lancer une petite pique à l'hébergeur : « *Il est d'ailleurs très dommage que le site web d'information d'OVH sur les travaux en cours n'ait pas d'adresse IPv6… (Idem pour les sites d'information corporate et technique)* ».

Car une partie du problème était là : en cas de souci, les clients OVHcloud savent qu'il faut se rendre sur le site de statut pour savoir ce qu'il se passe… mais il était également indisponible. « *OVHcloud opère un backbone global intervenant sur l'ensemble des continents. Pour s'assurer que les clients ont le meilleur accès possible, il est entièrement maillé. Par nature, ce maillage implique que tous les routeurs prenant part au backbone sont directement et indirectement connectés les uns aux autres et échangent des informations* », déclare l'hébergeur.

Il ajoute que pendant la panne, toute la table de routage d'Internet était annoncée via l'IGP (Interior Gateway Protocol) OVHcloud, ce qui a surchargé la RAM et le CPU de certains routeurs et donc la panne sur IPv4. C'est avec l'accès physique à l'appareil défaillant qui a permis de rapidement résoudre le problème. Pour rappel, dans la panne récente de Facebook, c'est notamment l'impossibilité d'accès aux salles qui avant fait durer la situation.

OVHcloud indique désormais évaluer ses procédures de validation sur ces appareils, notamment pour ce qui concerne l'envoi et la validation des commandes exécutées, afin de les renforcer. Espérons que la généralisation d'IPv6 sur les services critiques fera aussi partie des actions prévues.

Un problème, ça peut arriver, quoi qu'en disent les yakafokons

Stéphane Bortzmeyer tient de son côté à remettre les pendules à l'heure : oui OVHcloud a planté, mais cela peut arriver : « *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)* ». Il reprend ensuite le **tweet de Shnoulle** : « *Même planifiés, testés et vérifiés : l'erreur est toujours possible. En effet : les tests ne pourront jamais tous couvrir* ».

Autre précision importante, 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* ». Pour rappel, dans le premier cas la coupure peut être de 8,76h par an et de 87,6h dans le second.

Il faut donc choisir son hébergeur en fonction de ses besoins. Pour un site personnel ou même professionnel, on peut souvent s'accommoder d'une petite panne comme celle de ce matin tant qu'elle ne revient pas trop souvent. Par contre la situation est différente pour des sites critiques (services d'urgence par exemple).

d'éliminer l'humain et donc les erreurs humaines) ». Or, comme nous venons de le dire, tous les tests de la Terre ne peuvent pas anticiper à 100 % ce qui se passera lors d'un déploiement en production. Google en a récemment **fait les frais**.

Cet incident devrait aussi aller dans le sens de ceux qui vantent une approche multi-cloud : n'importe quel hébergeur peut rencontrer un problème grave, il faut donc assurer une redondance à travers l'un de ses concurrents pour réduire les problèmes potentiels. Mais là aussi, cela dépendra du budget prévu et de votre capacité à tolérer une panne. Des éléments à prendre en compte dans vos plans de continuité d'activité (PCA) et de reprise d'activité (PRA). Vous n'en avez pas ? C'est peut-être l'occasion de vous y mettre.

Pour OVHcloud, le problème c'est l'image de marque

Pour OVHcloud, l'essentiel était de régler rapidement le problème et de passer à autre chose, d'où cette publication le jour même. Car le timing est malheureux : l'entreprise **doit entrer en bourse à la fin de la semaine** et nul doute que la société se serait bien passé de faire les gros titres avec cet incident, qui renvoie certains aux souvenirs de l'incendie du mois de mars. Un accident bien plus grave, qui avait provoqué de gros dégâts avec des données définitivement perdues pour ceux qui n'avaient pas mis en place de procédure de sauvegarde.

- **Une donnée informatique, ça brûle**
- **Qu'est-ce que la stratégie de sauvegarde 3-2-1 ?**

21 commentaires

bohwaz - 13/10/21 à 21:13:19 **#1**

Une heure de black-out c'est relativement peu au final, et la communication d'Oles est toujours très rapide, et riche en détails techniques, en toute transparence. Je préfère ça à du bla bla marketing du genre "nos équipes travaillent à rétablir le service". Par contre cette communication devrait être faite par une équipe, sur un compte Twitter dédié, pas juste par le CEO sur son compte perso...

olt01 - 13/10/21 à 21:25:29 **#2**

J'ai bien lu dans l'article que la panne était différente de celle de Facebook (interne à l'AS v.s. externe). Cependant, sa nature est est identique. La loi des séries ?

cyp - 13/10/21 à 21:30:30 **#3**

> **olt01 a écrit :**
>
> La loi des séries ?

Peut être pas, l'argument donnée par OVH sur l'intensification des DDOS semble crédible (Microsoft vient également d'en subir un très gros) et pousse peut être les opérateur dans des mises à jour un peu précipité.

olt01

Tout à fait, c'est même une série OVeHrkill. 

game1337 - 13/10/21 à 21:56:18 **#5**

Enfin que le site de suivi des incidents sois lui aussi tomber ne fait quand même pas très sérieux

Slaelrod - 13/10/21 à 22:08:18 **#6**

"Quand on vous dit de passer à IPv6"

Dit un site qui ne le supporte pas

SebGF - 13/10/21 à 22:22:35 **#7**

> Cet incident devrait aussi aller dans le sens de ceux qui vantent une approche multi-cloud : n'importe quel hébergeur peut rencontrer un problème grave, il faut donc assurer une redondance à travers l'un de ses concurrents pour réduire les problèmes potentiels. Mais là aussi, cela dépendra du budget prévu et de votre capacité à tolérer une panne.

Tout est dit ici. Ne jamais mettre ses oeufs dans le même panier est une bonne pratique, tout comme il est essentiel de savoir quelle tolérance apporter à la panne versus les moyens qu'on se donne pour réduire le plus possible les risques.

Dans la pratique, hélas, le client va dire qu'il peut se permettre d'avoir X heures d'indisponibilité parce que sinon c'est trop cher, mais en cas de crash il faut remonter dans la seconde sinon c'est un scandale. Confère un meme qui tourne régulièrement dans les réseaux spécialisés avec le pot d'argent quasi vide puis quasi plein et comme légende : "security budget before a data breach / security budget after a data breach" (et sa variante avec un troisième pot largement plus gros : "data breach cost").

Et vous avez bien fait de rappeler que plusieurs des gros acteurs ont eu des problèmes ces derniers temps. L'effet de loupe arrive vite à la moindre défaillance d'un hébergeur et on oublie à côté que la fiabilité est globalement très bonne et que personne n'est à l'abri d'un problème. Pour faire une métaphore, c'est comme le crash d'un avion. C'est extrêmement rare, mais sur-médiatisé lorsque ça arrive, ce qui a tendance à biaiser l'opinion alors que c'est un moyen de transport pourtant très sûr.

Shit happens comme on dit.

Slaelrod
```
ping nextinpact.com
PING nextinpact.com(2606:4700:20::681a:e07 (2606:4700:20::681a:e07)) 56 octets de données
```

Ca ressemble pas à une IPV4 ce que je vois en résultat.

Édité par SebGF le 13/10/2021 à 22:24

traknar - 13/10/21 à 22:43:47 **#8**

> Cet incident devrait aussi aller dans le sens de ceux qui vantent une approche multi-cloud : n'importe quel hébergeur peut rencontrer un problème grave, il faut donc assurer une redondance à travers l'un de ses concurrents pour réduire les problèmes potentiels. Mais là aussi, cela dépendra du budget prévu et de votre capacité à tolérer une panne.

Passer au multi-cloud n'est pas qu'un problème de budget. Le faire revient à se restreindre au plus petit dénominateur commun entre les fournisseurs. On se prive alors du bénéfice des milliard de dollars/euros investis annuellement dans la R&D par les hyperscalers.

Slaelrod - 13/10/21 à 23:50:41 **#9**

SebGF My bad j'aurais du vérifié il y a encore quelque mois il le supportait pas.

TroudhuK - 14/10/21 à 00:02:42 **#10**

> **Slaelrod a écrit :**
>
> "Quand on vous dit de passer à IPv6"
>
> Dit un site qui ne le supporte pas

D'ailleurs concrètement, que veut dire "passer à l'IPv6", au-delà de ne plus la bloquer de partout ? Pourquoi est-ce qu'on peut la bloquer d'ailleurs ?

Page 1 / 3

Votre commentaire

Connecté en tant que TheBigBug

Commentaire...

Envoyer