

Cloud Computing : QUAND LA MAGIE PART EN FUMÉE

QUELLES LEÇONS TIRER DE L'INCENDIE D'OVH ?



L'incendie qui aura donné un coup de chaud à la planète Cloud

La nuit du 09 mars 2021 fût le théâtre d'un **spectaculaire incendie** sur le site strasbourgeois d'OVHcloud. Un des quatre Datacenter du campus s'est vu réduire à l'état de cendres tandis qu'un autre a perdu plusieurs salles serveurs, ravagées elles aussi par les flammes. Un incendie qui n'arrive pas du tout au bon moment (si tant est qu'il y en ait un) pour le fleuron français et leader européen du cloud qui était sur le point d'entrer en bourse. Conséquence directe à cela : **entre dix et vingt mille clients se retrouvent dépourvus de leurs données ou encore dans l'impossibilité de profiter des services que proposent habituellement la firme roubaisienne** (OVH ayant coupé l'électricité sur les deux autres centres du campus). De quoi impacter fortement l'entreprise française mais également et plus généralement le monde du cloud computing.

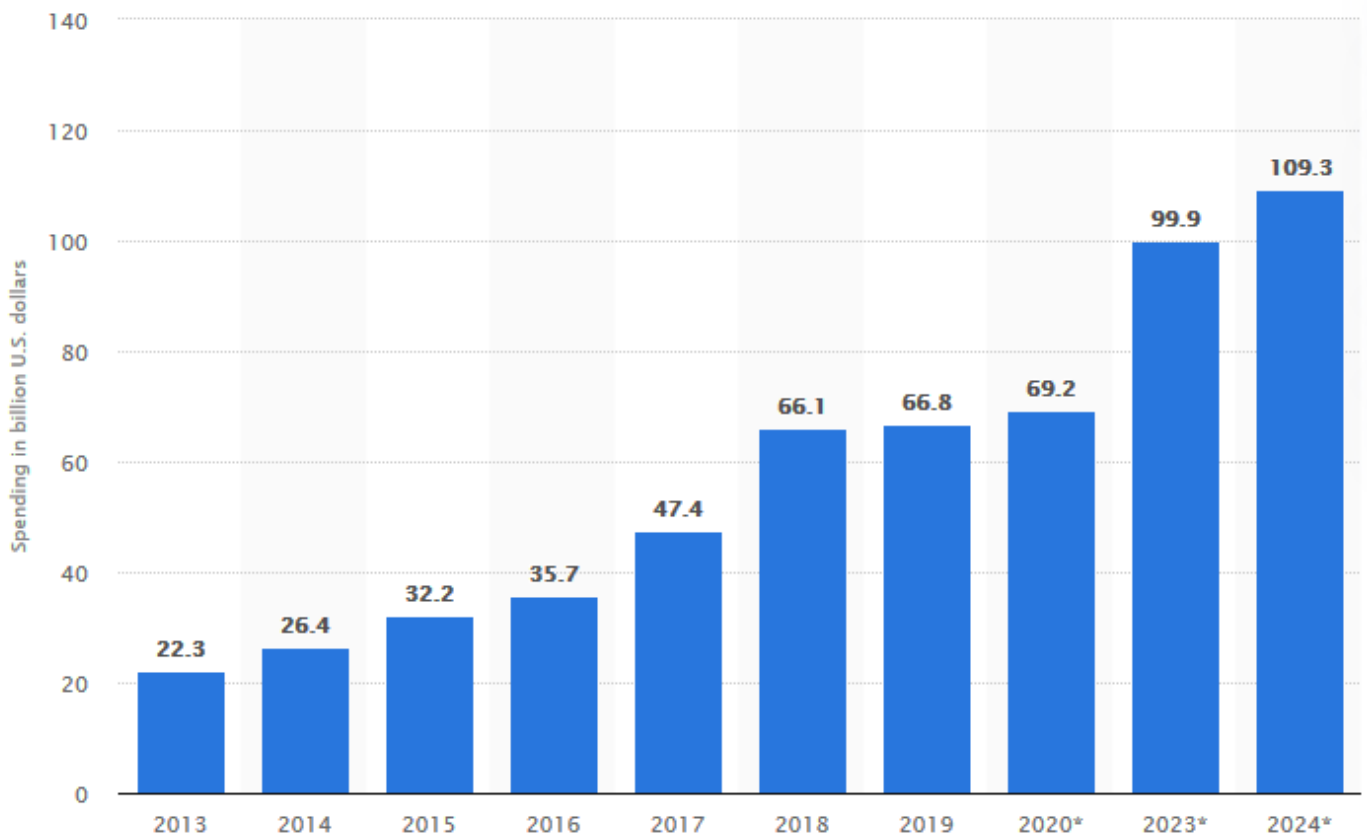


Logo du fournisseur cloud français OVHcloud

Un évènement malheureux pour OVH et le cloud computing...

Ce triste accident vient couper brutalement **OVHcloud** dans son élan qui était jusque-là très encourageant pour le cloud français et européen : certifié **SecNumCloud** depuis peu, au cœur du projet de cloud souverain européen **GAIA-X**, à l'aube d'une entrée en bourse et, plus récemment d'après les rumeurs, proche de la société **Blade** pour racheter **Shadow** (l'offre concurrente de **Stadia** de cloud gaming). Le géant français devra donc probablement revoir ses ambitions à la baisse sur le court et moyen termes afin de compenser les pertes (financières mais aussi d'image et de réputation) engendrées par cette mésaventure. Au-delà de ces aspects, **c'est le cloud dans sa globalité** (du moins pour le marché français) **qui devrait en pâtir**, ce qui est d'autant plus regrettable

étant donné que le secteur était jusque-là en pleine expansion et que les sceptiques se faisaient de moins en moins nombreux. Le risque découlant de cet incendie est de voir **ralentir un certain nombre de projets de migration vers le nuage**, la confiance vis-à-vis des cloud providers étant forcément ébranlée. S'ajoute à cela **l'émergence probable d'inquiétudes vis-à-vis des infrastructures/données déjà externalisées**. Mais au final, n'est-ce pas un mal pour un bien ?



« Dépenses mondiales annuelles dans les infrastructures cloud de 2013 à 2024 (en milliard de dollars). ». Source : Statista. *prévisions.

... nous ramenant à nos fondamentaux

En effet, il existait jusqu'à présent une sorte d'aura et de **magie** autour du cloud. Peut-être qu'après la défiance envers les géants étrangers, un certain **excès de confiance** était en train de s'installer petit à petit, nous faisant oublier nos fondamentaux. Le marketing de ces entreprises et la qualité de leurs services n'y sont probablement pas pour rien. Néanmoins, ce triste événement vient nous rappeler **qu'externaliser ses ressources chez un tiers ne les protège pas pour autant de tout**. Cet incendie va remettre les pendules à l'heure et appuyer le **développement des bonnes pratiques** qui étaient jusque-là **encouragées par les fournisseurs cloud eux-mêmes** mais pas pour autant toujours appliquées (en témoignent les nombreuses pertes de données issues de l'incendie).

Comment se prémunir de ce genre de situation ?

Un travail dès la conception

Il faut réfléchir au besoin de disponibilité des ressources dès la phase de conception des infrastructures sous-jacentes (et même avant cette phase dans l'idéal). Dès lors, il est important de définir un niveau de disponibilité cible qui ne risque pas **d'impacter négativement l'entreprise**, directement ou indirectement. Il faut cependant rester réaliste et avoir conscience que **plus le niveau de disponibilité attendu est élevé, plus cela coûte cher**. Il est donc nécessaire de **mettre en perspective le coût de la mise en place de ces mesures et l'impact qu'aurait un arrêt de l'infrastructure en question**.

Plan de reprise d'activité

Le **plan de reprise d'activité (PRA)** a pour objectif de **décrire les solutions de secours** (procédures informatiques et solutions techniques) à **dérouler en cas d'incident majeur et pour relancer au plus vite l'activité**. Le cloud ne doit pas remettre en question cet exercice qui pourrait naïvement être mis de côté sous prétexte que le niveau de disponibilité et le SLA promis par le fournisseur cloud sont conséquents. Ils le sont très probablement, mais que fait-on le jour où tout s'arrête ? A **Pramana**, nous conseillons à nos partenaires de **réaliser des simulations de PRA** sur leurs environnements hors production et étant sur le cloud. Cela permet de voir si les **mesures en place permettent de relancer l'activité dans les temps impartis** et surtout de **s'exercer pour être le plus efficace possible** le moment venu !

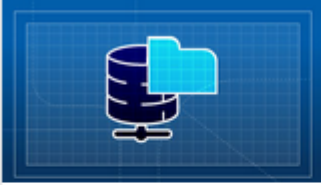






Politique de sauvegarde

La sauvegarde consiste à recopier les données d'un système d'information (données système et de production) de manière à pouvoir s'en resservir en cas de **défaillance** ou, pire, en cas de **PRA**. Quelques **principes de base** sont à respecter concernant la disponibilité des sauvegardes, même lorsque l'on est sur le cloud :

- La fréquence de sauvegarde doit être définie pour chaque type de données/outils.
- Les sauvegardes doivent être stockées sur un site géographique différent mais rester accessibles en 24/7.
- Les copies doivent être testées régulièrement pour s'assurer de leur bon fonctionnement.
- Leur cycle de vie doit être clairement défini (évolution dans le temps de la méthode de stockage / du lieu en fonction du besoin en accessibilité).

Les fournisseurs mettent à disposition tout un panel d'outils permettant de faciliter la réplication des sauvegardes et leur gestion (comme Backup Storage, Veeam Backup, NAS HA ou encore Object Storage chez OVHCloud). Il serait dommage de s'en priver.

Stockage en réseau - administration par OVH.com

 NAS HA À partir de 59,00 € HT/mois	 Backup Storage À partir de 12,00 € HT/mois	 Veeam Backup À partir de 10,00 € HT/mois/VM backupée
<p>Stockage Hardware</p>  Serveurs stockage À partir de 84,99 € HT/mois		
<p>Stockage Cloud</p>		
 Object Storage À partir de 0,01 € HT/mois/Go	 Additional Disks À partir de 0,04 € HT/mois/Go	 Veeam Cloud Connect À partir de 14,99 € HT

Solutions de stockage et sauvegardes proposées par OVHCloud (mars 2021)

Que retenir de cette mésaventure ?

La morale de tout cela est que **personne n'est à l'abri d'un accident**. Derrière leurs belles promesses (et qui sont bien souvent tenues, soulignons-le), les cloud providers restent des entreprises comme les autres, à savoir **faillibles**. Et d'ailleurs, ils ne s'en cachent pas puisqu'ils insistent bien sur le fait que **chaque client doit concevoir et mettre en place ses infrastructures en considérant de potentiels arrêts de services et pertes de données**. Le problème est que derrière cet aspect boîte noire qui rassure, où tout fonctionne en quelques clics et très simplement, **on en oublie nos fondamentaux**. Par conséquent, la mise en place de PRA et d'une politique de sauvegarde adaptée reste **indispensable** pour se protéger de ce genre de mésaventure. Les outils natifs proposés par les cloud providers permettent de faciliter grandement les choses. Autant en profiter !

Composé de spécialistes cloud certifiés connaissant parfaitement les rouages du nuage, le cabinet de conseil **Pramana accompagne depuis plusieurs années déjà ses partenaires des secteurs public et privé dans leurs projets cloud**. Afin d'éviter les désagréments potentiels liés à cette problématique, n'hésitez pas à contacter nos spécialistes pour construire ou faire évoluer ensemble votre projet. Pour plus d'informations sur nos offres, n'hésitez pas à nous solliciter via le formulaire de contact présent sur notre site web : www.pramana.fr