

Incendie OVHcloud : comment Jamespot a sauvé 130 000 utilisateurs grâce au PRA

•

Touché par l'incendie de Strasbourg, l'éditeur de la plateforme collaborative française Jamespot a pu sortir ses clients du black-out grâce à un plan de reprise d'activité soigné, qui est revenu à une migration en urgence.



par

- **Yann Serra**, LeMagIT

Publié le: **22 mars 2021**

C'est le récit d'un sauvetage extraordinairement huilé. Dans la nuit du 9 au 10 mars 2021, à minuit passé de 47 minutes, un incendie [éclatait](#) sur le site strasbourgeois de l'hébergeur OVHcloud. Au petit matin, le constat est dramatique : le feu a emporté le bâtiment SBG2 et ses 12 000 serveurs physiques qui exécutaient des millions de sites web et services applicatifs en ligne. Parmi les victimes numériques, 130 000 utilisateurs de la [plateforme collaborative française Jamespot](#) n'ont plus accès à leurs documents ni aux

outils essentiels pour travailler. Les machines virtuelles qui portaient leurs activités sont parties en fumée.

Mais alors que tout le monde ignore encore en combien de temps OVHcloud pourra restaurer ce qui a brûlé – ni même s’il y parviendra –, Jamespot a su remettre tous ses clients en opération en quelques heures grâce à un [PRA](#). Un Plan de Reprise d’Activité qui, en la matière, est un exemple du genre.

« Un PRA est un processus qui doit être écrit et mis à jour régulièrement. C’est le cas chez nous ; nos clients les plus importants l’exigent d’ailleurs à la signature du contrat », explique au MagIT Alain Garnier, le président de Jamespot. « Ce PRA décrit l’organisation à suivre en cas d’incident, mais aussi quelle architecture utiliser pour relancer l’activité et quelle politique décider pour sauvegarder les données ».

Alain Garnier rappelle au passage qu’un PRA a deux coûts : celui des ressources matérielles et celui des procédures. « Il faut par exemple prendre en compte qu’un stockage peu cher coûtera plus cher en procédures de restauration et de tests. Mais aussi que les procédures comprennent le coût de maintenance perpétuelle du code, pour prendre en compte les évolutions régulières des packages fonctionnels », souligne-t-il.

En fin de compte, plus le PRA comprend de procédures, plus son coût est exponentiel. Selon Alain Garnier, en tenant compte de toutes les précautions mises en place pour reprendre l’activité dans les plus brefs délais, le coût d’un PRA peut multiplier par huit le coût initial d’un simple hébergement, car « il faut y ajouter des infras supplémentaires pour la [redondance](#), des logiciels de monitoring et aussi du service autour pour assurer le suivi 24H ».

Un outil de communication, des backups ailleurs



JAMESPOT-NATHALIE-OUNDJIAN

Alain Garnier, président et fondateur de Jamespot

Au cours de sa carrière, Alain Garnier a connu d'autres situations qui avaient nécessité de [déclencher un PRA](#). Il en a tiré une certaine expérience. « Concernant l'organisation en elle-même, le parent pauvre d'un tel plan est l'outil de communication. Or, il se trouve qu'il s'agit justement du genre d'outils que nous [commercialisons](#). Nous avons donc très tôt mis en place une plateforme Jamespot dédiée au PRA, pour distribuer les tâches, pour chronométrer chaque action ».

Il en a aussi retiré des réflexes. « Dès qu'OVHcloud nous a informés de l'incident, j'ai eu l'intuition que s'ils ne nous donnaient pas accès aux [snapshots](#), cela signifiait que la situation allait durer. Et nous avons enclenché notre PRA dans les quinze minutes qui ont suivi. »

Les snapshots sont les sauvegardes d'appoint qui permettent de redémarrer dans les plus brefs délais un service en ligne en cas d'incident mineur. Parce qu'ils sont sans cesse sollicités, les serveurs « plantent » ou tombent en panne. Dans ce cas, le snapshot permet de redémarrer la machine virtuelle d'un service sur le serveur d'à côté. Lorsque les snapshots ne sont plus accessibles, cela signifie que l'incident va au-delà d'un simple serveur, qu'il concerne jusqu'au site entier où avait lieu l'exploitation et, donc, que les réparations nécessaires sont potentiellement importantes.



« La réplication à chaud des données depuis un autre serveur dans le même bâtiment [n'était pas possible](#). Donc nous devons repartir depuis des [backups](#) », raconte Alain Garnier. « Les backups que nous effectuons sont stockés sur le site de Roubaix d'OVHcloud. Nous en faisons aussi des copies de secours qui, elles, sont stockées chez un autre hébergeur, en l'occurrence Scaleway ». Alain Garnier précise que le site de Roubaix sert aussi à exécuter des instances des services Jamespot ; celles-ci sont sauvegardées encore ailleurs.

Techniquement parlant, un [backup](#) est une sauvegarde bien plus complète qu'un snapshot. Il permet de récupérer des données plus anciennes et de le faire sur des serveurs très différents de ceux d'origine. Mais il impose aussi des contraintes. « La problématique des backups est qu'ils supposent un délai de restauration, c'est-à-dire qu'il faut extraire leurs contenus et les réinstaller sur des instances en production. Cette étape est d'autant plus longue quand, comme c'est notre cas, les contenus sont cryptés et qu'il faut les déchiffrer », explique Alain Garnier.

Comme une migration, mais en urgence

Concernant l'architecture de récupération, celle définie par Jamespot n'a plus rien à voir avec les [machines virtuelles](#) en production à Strasbourg. « À Roubaix, nous n'exécutons pas nos services sur des machines virtuelles, mais sur des conteneurs [Kubernetes](#). Il se trouve que nous menions depuis plusieurs semaines une politique de modernisation en migrant petit à petit nos applicatifs vers le nouveau format [container](#). Restaurer nos backups de Strasbourg dans des containers à Roubaix revenait finalement à boucler en urgence notre migration. »

Alain Garnier

Migrer des machines virtuelles vers des containers est compliqué. C'est pourquoi Jamespot ne l'a pas fait sous cette forme. « Nos backups ne sont pas des répliques de nos VMs, mais de leurs contenus, essentiellement des bases de données [SQL](#). Nous avons fait ce choix pour des raisons de

pérennité : si vous restaurez du binaire, vous courez le risque qu'il ne soit plus compatible avec les environnements que vous avez entretemps mis à jour » justifie le président de Jamespot. En l'occurrence, les données SQL sont indépendantes du format des serveurs qui les exécutent.

Les backups censés restaurer l'activité des 130 000 utilisateurs en souffrance pèsent dans les 7 To et comprennent plus d'un millier de bases de données SQL. « Nous avons réussi à restaurer les données des premiers clients dès 11 h 00 du matin, le mercredi même. À 20 h 00, nous étions parvenus à remettre en ligne 83 % de nos clients. Les toutes dernières bases à avoir été restaurées étaient en réalité celles qui nous posaient le plus de difficulté : leur taille était colossale, avec des chiffrements imbriqués les uns dans les autres. »

Le jeudi, tous les clients de Jamespot ont retrouvé leurs services. « Nous avons suivi une procédure qui était rodée. Il nous arrive régulièrement de devoir restaurer des backups pour des clients qui ont effacé par erreur des données. »

Le défi de restaurer sur des ressources dédiées à autre chose

À ce stade, Jamespot n'est pourtant pas encore au bout de ses peines. « Le problème est qu'il nous fallait des ressources – des datastores, des hosts – dans lesquelles restaurer ces backups. Et OVHcloud ne nous les promettait que pour le week-end suivant. En attendant, nous avons dû aménager de la place sur nos ressources existantes. »

Alain Garnier

« Nous avons assez de capacités en CPU, en RAM et en disques à Roubaix pour tout restaurer... mais au cordeau ! Or, lorsque votre infrastructure est occupée à 90 %, vous ne dormez plus très bien. Vous surveillez tout plus que d'habitude. Cela explique aussi le temps que nous avons pris pour restaurer nos clients : nous avons déployé leurs données de manière très

minutieuse pour être sûrs que tout allait tenir », se souvient Alain Garnier qui compare cette étape à une partie de Tetris.

Il glisse que, dans cette situation, ses équipes ont néanmoins bénéficié d'une certaine sidération de la part des clients de Jamespot qui, à la suite de l'ampleur de l'événement qui a touché OVHcloud, ont d'eux-mêmes ralenti leurs activités.

Lorsque les nouvelles ressources d'OVHcloud arrivent, comme prévu dès le week-end, l'occupation de l'infrastructure retombe « C'est à ce moment-là que la pression sur les équipes redescend. Il n'aurait pas fallu pas que ça dure. D'autant que dès le lundi, la sidération passée, nos clients reprenaient à plein leurs activités. »

Le défi de conjuguer sécurité et rapidité de réaction

Alain Garnier tire une double conclusion de cette mésaventure. « Nous avons pu nous appuyer sur l'infrastructure du prestataire. Et force est de reconnaître que nous avons bien les capacités industrielles de supporter de telles catastrophes. En interne, il n'y a pas eu de drame, pas de prises de bec, juste de la mobilisation sur des procédures rodées. Je suis fier de nos équipes », lance-t-il.

Alain Garnier

Le président de Jamespot explique aussi que cet événement a renforcé sa conviction de ne pas mettre ses œufs [dans le même panier](#). Nombre de petits clients d'OVHcloud [pensaient](#) en effet que les snapshots d'appoint, réalisés dans le même bâtiment, suffisaient à les protéger contre tous les risques. Mais la véritable utilité de ces snapshots est de pouvoir réagir rapidement aux incidents mineurs. Pas en cas de force majeure.

« En résumé, la rapidité de réaction ne va pas de pair avec la sécurité. Notre problème a été la durée de déchiffrement des backups. Pour la suite, nous allons donc travailler à réduire ces temps d'indisponibilité. Mais comment

trouver le meilleur compromis ? La solution est sans doute de découper les risques en petits risques moins importants pour gagner en agilité », conclut Alain Garnier.