Backup as a Service : les 6 défis à relever

Le Backup as a Service entend répondre à l'explosion du volume de données. Mais toutes les entreprises ne l'adopteront pas de la même façon. Cloud public ou privé ? Sauvegardes figées ou pont entre données centrales et archivées ? Tour d'horizon des problématiques d'un projet BaaS.

1 – Backup as a Service : dans quel contexte ?

Le Backup as a Service (BaaS) profite de tous les bénéfices du Cloud. À savoir, une mise en œuvre simplifiée et sans maintenance, l'absence de coûts d'acquisition, un paiement à l'usage et une capacité à monter aisément en charge.

C'est une solution pour ceux qui :
– ne disposent pas des équipes IT nécessaires pour organiser leur plan de sauvegarde ;
– veulent basculer ce poste du CAPEX (investissement) vers de l'OPEX (dépense d'exploitation)
– voient leur volume de données à sauvegarder croitre très rapidement ;
– utilisent massivement d'autres offres Cloud en mode as a Service.

2- BaaS sur infrastructure publique ou privée ?

L'augmentation des débits Internet, en particulier avec le déploiement de la fibre et de la 4G, favorise l'utilisation de solutions publiques de BaaS, telles que proposées sur les Cloud d'Amazon, Microsoft ou Google.

Mais, comme nous le rappelle Olivier Tant, chez HPE, le BaaS n'est pas uniquement accessible sur le Cloud public : « Beaucoup de clients font du Backup as a Service en interne. Chez les grands comptes, nous recensons 80 % d'infrastructures de backup « on premise » pour 20 % sur le Cloud public. » Il est en effet envisageable d'adopter le BaaS sur des infrastructures de Cloud privé, tout en conservant la flexibilité, la capacité à monter en charge, voire le paiement à l'usage propre aux solutions de Cloud public.
Et de rappeler ainsi qu'il est possible de proposer des solutions physiques sur site, mais avec un paiement à l'usage.

Philippe de Trogoff, chez Veeam, évalue les choix des entreprises suivant leur taille :
– Les grands comptes préfèrent construire leur propre solution de backup. Certains vont dans le Cloud (souvent privé ou privé hébergé), mais pas tous ;
– Les ETI adoptent pour la plupart le backup « on premise », mais sont nombreuses à réfléchir à une bascule en mode Cloud ;
– Les PME disposant d'infrastructures IT continuent à préférer des solutions sur site, tout en réfléchissant à la séparation entre les données sensibles et les autres ;
– Les TPE et PME ne disposant pas d'infrastructures IT sont en général grosses consommatrices d'offres SaaS et seront donc les plus friandes de BaaS public.

Pour des raisons réglementaires et de contrôle, les grands comptes et les entreprises où la data est stratégique adopteront des solutions de BaaS sur des infrastructures de Cloud privé (« on

premise » ou hébergées chez un prestataire). Le Cloud public peut servir de relais en cas de pics de charge, mais essentiellement pour des données non critiques.
Philippe de Trogoff note que la tendance est d'opter pour de l'IaaS public, qui servira de renfort à une solution de backup existante.

À l'opposé, pour les TPE et PME ne disposant pas de solution de sauvegarde, les offres BaaS des grands opérateurs de Cloud public sont souvent la seule possibilité accessible (en moyens humains comme financiers) pour disposer enfin de sauvegardes efficaces. Avec une simplicité proche de celle des offres SaaS que ces petites entreprises connaissent déjà.

3 – Une intégration au plus près des applications

« Le backup est de moins un moins un sujet à part, affirme Olivier Tant, HPE. Il devient un service de données parmi d'autres. Les solutions de backup doivent être fluides, flexibles et indolores. » C'est pourquoi elles sont dorénavant intégrées à tous les niveaux de l'infrastructure IT. Que ce soit dans les serveurs, au pied des bases de données ou encore adossées aux machines virtuelles.

Les mécanismes de backup sont partout et adressent les couches hautes du SI. Et il ne faut pas oublier les services Cloud. « Les applications hébergées, comme Office 365, doivent aussi être sauvegardées », rappelle Florian Malecki de StorageCraft.

Cette approche holistique du backup fait que les solutions sont souvent intégrées en standard dans les offres matérielles des constructeurs. « 60 % des ventes de logiciels de sauvegarde se font avec les ventes de la solution de stockage », confirme Veeam Software. Une affirmation appuyée par HPE, qui a signé des accords de partenariat avec de nombreux éditeurs du secteur. Les sociétés de service et les hébergeurs proposent, eux aussi, ces offres directement dans leur catalogue.

Pour piloter l'ensemble de ces solutions, il faut une gestion globale, avec un pilotage par le logiciel (software-defined) et en tant que service (as a service). Le tout avec des connecteurs et API qui assureront le lien entre les différents composants. Une approche moderne qui évitera que la sauvegarde ne se transforme en casse-tête.

4 – Pensez à la consolidation des backups… et à la restauration

Reste que la multiplication des offres intégrées peut aller à l'encontre de l'objectif de « gestion globale ». Un nouveau marché se met donc en place ; celui de la consolidation des backups. Tout le monde y va de ses intégrations avec des solutions tierces.
Un acteur toutefois s'est fait une spécialité de la consolidation des sauvegardes : Cohesity, avec une plate-forme scale-out proposant une compression et déduplication globale des données.

L'autre partie de la sauvegarde, c'est la restauration. Opération difficile à mener lorsque plusieurs solutions de backup sont utilisées en parallèle. Consolider les sauvegardes est une chose, assurer la restauration est en une autre. La reprise d'activité devient parfois complexe et peut justifier l'adoption d'une solution de Disaster Recovery as a Service en complément du Backup as a Service.

Ceci sera encore plus vrai lors de la sauvegarde de VM (machines virtuelles). Il faut parfois – fort

heureusement rarement – restaurer l'ensemble d'une VM pour retrouver un fichier. C'est pourquoi certains acteurs proposent aujourd'hui de faire démarrer une VM sauvegardée directement sur le Cloud où elle est stockée.

5 – BaaS public : gare à la qualité des infrastructures réseau

La mise en place en France de la fibre permet de faciliter l'adoption de solutions de BaaS public. Attention toutefois à la qualité de l'infrastructure réseau des autres pays. L'Allemagne est souvent choisie pour son haut niveau réglementaire, « mais son infrastructure Internet reste en retrait, constate Florian Malecki, StorageCraft. Elle est nettement moins bonne que celle des pays nordiques ou du Royaume-Uni ».

Avec son offre de déduplication et compression globale, effectuée avant le transfert des données vers un Cloud public, Cohesity entend aider à solutionner ce problème. « Le plus bloquant c'est le réseau et c'est donc le point à traiter, analyse Christophe Lambert de Cohesity. Le backup n'a pas évolué dans le même sens que le volume de données généré. Il faut donc des plates-formes scale-out capables d'avaler tous ces gisements de données. »

La qualité et la vitesse de la connexion sont importantes lors de la sauvegarde, mais deviennent primordiales lors de la restauration. « L'infrastructure de communication doit alors être très bonne », explique StorageCraft, sans quoi le temps d'indisponibilité sera allongé d'autant. Sans compter le coût de téléchargement des données depuis un fournisseur de BaaS public.
« La restauration est le point noir des offres en Cloud public », confirme Cohesity, qui suggère une solution : un premier niveau de sauvegarde local, seuls les backups les plus anciens étant poussés vers le Cloud.

6 – Des données qui ne dorment que d'un œil

Jusqu'alors les données sauvegardées étaient figées. « La fonction régalienne du backup, qui est de sauvegarder le primaire, existe toujours, explique notre expert HPE. Mais on sauvegarde également de plus en plus de données non structurées, susceptibles d'être réutilisées. » Le backup se transforme alors en pont entre des données primaires et secondaires.

« Les approches historiques sont de plus en challengées par de nouveaux modèles, plus intégrés, plus fluides, plus flexibles. » Des offres où le backup n'est plus seulement un sas de sortie pour la donnée, mais aussi un sas d'entrée. La sauvegarde se transforme en un ensemble de données dormantes, mais réutilisables à tout instant.

Ce concept devient de plus en plus capital avec le RGPD (règlement général sur les données privées). En cas d'audit sur les données, chaque sauvegarde doit être restaurée afin d'en étudier le contenu. Lorsque le backup est vu comme une plate-forme de données secondaires, il est possible d'indexer les informations des sauvegardes, puis de les requêter. C'est non sans raison que Cohesity présente les données sous la forme d'un système de fichiers, où les éléments sont tous indexés, afin d'être plus facilement réutilisés ou audités.

Concernant le RGPD, la conformité des fournisseurs de Cloud doit être vérifiée. Les grands noms du Cloud public sont bien évidemment dans les clous… à condition d'opter pour des datacenters

situés en Europe, voire en France. « In fine, le RGPD a permis de mieux encadrer les différentes offres de Backup as a Service », constate StorageCraft. Et ainsi de faire le tri entre le bon grain et l'ivraie.