

# Stockage Cloud : Amazon Web Services sécurise son offre S3

Amazon Web Services (AWS) veut mettre un terme à la mauvaise publicité rencontrée par son service de stockage cloud AWS S3 (Simple Storage Service) suite à plusieurs incidents qui ont vu des données non sécurisées exposées sur Internet. Dans cette optique, la firme de Jeff Bezos vient d'annoncer, dans un [billet de blog](#), la mise en service de 5 nouvelles fonctions visant à consolider la sécurité d'AWS S3.

Cette annonce intervient après que plusieurs grands comptes, tels qu'Accenture, Verizon et TigerSwan, aient accidentellement laissé des buckets (compartiments) contenant des données confidentielles exposés sur le Web. Il s'agit systématiquement d'erreurs humaines résultant d'une mauvaise configuration de leurs compartiments S3.

AWS a pris la mesure des difficultés qu'il pouvait y avoir à sécuriser les données sur S3. Et y répond en proposant l'option de chiffrement par défaut. Cela signifie que tous les objets transférés dans des compartiments S3 seront chiffrés par défaut. Une initiative qui confère aux administrateurs un bon moyen de s'assurer que les données sont toujours chiffrées d'une manière beaucoup plus fluide que précédemment.

## **Partage de propriété**

Autre mesure, désormais la console d'administration de S3 avertit les administrateurs avec un indicateur (Permission Checks) situé à côté de chaque compartiment S3 laissé ouvert au public.

Rappelons que les listes de contrôle d'accès (ACL pour Access Control Lists) permettent aux administrateurs de définir et de gérer qui a accès aux compartiments et aux objets dans S3. Cela permet notamment de s'assurer que les autorisations d'accès « voyagent » avec les données lorsque celles-ci sont déplacées. Maintenant, il est possible de partager la propriété d'un compartiment en transit. Cela peut être pertinent pour transférer le contrôle d'un compartiment à un autre administrateur, lorsque le transfert se fait par exemple entre différentes régions.

Cela permet également de partager la propriété, tout en conservant une propriété distincte suivant qu'il s'agisse des objets d'origine ou de leurs répliques.

De plus, les administrateurs peuvent maintenant aussi répliquer des objets chiffrés avec des clés gérées par AWS Key Management Service (KMS). Le rapport inclut désormais le statut de chiffrement de chaque objet stocké dans S3. Il peut aussi être lui-même chiffré.

*Crédit Photo : AWS*