



# Les 5 fondamentaux de la sauvegarde et de la restauration dans Google Cloud

Le stockage des données de votre entreprise dans Google Cloud est une décision importante. Vous en tirerez de nombreux avantages, notamment la réduction des coûts d'investissement, l'évolutivité et l'agilité. Mais cette initiative comporte aussi des risques, le plus important étant de préserver la sécurité de vos données.

Gardez ces cinq fondamentaux en tête et vous n'aurez aucun mal à prendre des décisions judicieuses sur la manière de protéger vos données dans le cloud.

## Sachez qui est responsable de vos données

Il est tout à fait normal de supposer que les données de votre entreprise stockées sur Google Cloud sont automatiquement protégées grâce aux sauvegardes, aux snapshots et à la redondance des données. Mais ce n'est pas forcément le cas.

Google Cloud fonctionne selon un modèle de partage des responsabilités, ce qui signifie que Google est responsable de ses datacenters, de ses systèmes d'exploitation, de ses serveurs et de la couche de virtualisation de l'OS qui héberge votre machine virtuelle et d'autres ressources cloud. Vous êtes responsable de tout ce que vous déployez dans le cloud, notamment les applications, les comptes, les paramètres et vos données.

## Comprenez les risques liés au cloud

Il existe des risques supplémentaires répartis en quatre catégories : 1) un risque plutôt faible lié à l'infrastructure Google Cloud, estimé par Google à seulement 0,000000001 % de chances de perdre définitivement des données en raison d'un problème lié à son infrastructure ; 2) un risque lié à la configuration du cloud (avec des ressources cloud correctement paramétrées et configurées) ; 3) un risque lié à l'infrastructure locale (votre réseau, vos clés de chiffrement et vos collaborateurs) ; et 4) un risque lié aux accidents (erreur de l'utilisateur, erreur de script ou processus Google Cloud mal configurés).

## Planifiez la haute disponibilité

La haute disponibilité se caractérise par la capacité d'une ressource cloud à rester fonctionnelle et réactive, même en cas de défaillance d'un ou plusieurs de ses éléments ou composants associés. Google Cloud assure la haute disponibilité en stockant les données dans des buckets situés dans deux régions au minimum, ce qui rend les données géoredondantes : elles sont répliquées dans deux zones géographiques (ou plus) distantes d'au moins 160 kilomètres. Google Cloud propose également la conservation de buckets, la préservation d'objets et les versions d'objets pour minimiser les pertes de données.

## Élaborez un plan de sauvegarde

Les catastrophes arrivent, mais vous pouvez reprendre vos activités plus rapidement grâce à un plan de sauvegarde et restauration. Définissez un objectif de temps de restauration (RTO) et un délai optimal de reprise d'activité (RPO) pour déterminer respectivement la durée pendant lequel il est acceptable d'être hors ligne et la durée pendant laquelle les données peuvent être temporairement perdues. Plus vous souhaitez une restauration rapide de vos données, c'est-à-dire plus les RTO et RPO sont restreints, plus le coût du stockage des données augmente.

## Assurez la pérennité de vos données

Si vous voulez vraiment assurer la sécurité de vos données dans le cloud, voici quelques meilleures pratiques supplémentaires à envisager : automatisez vos sauvegardes, chiffrez vos données, créez plusieurs sauvegardes dans différents emplacements, utilisez un pare-feu, révoquez l'accès lorsqu'il n'est pas nécessaire, appliquez tous les correctifs possibles et surveillez vos coûts de sauvegarde.



Pour en savoir plus sur la sauvegarde et la restauration de vos données dans Google Cloud, consultez l'ouvrage *Sauvegarde Google Cloud pour les Nuls, Édition spéciale Veeam*.

LIRE L'E-BOOK

VEEAM

pour les nuls®