Google Cloud se dote d'un gestionnaire de secrets

Mots de passe, certificats, clés d'API… Comment gérer ces données sensibles sur Google Cloud ?

Une option consiste à assembler plusieurs briques autour de l'outil *open source* Berglas.

Depuis quelques semaines, Google propose une alternative « tout-en-un » : Secret Manager.

Disponible en bêta, la solution se fonde sur deux concepts :

- Les « secrets », utilisés à l'échelle des projets GCP
- Les « versions » de secrets

Ce sont ces « versions » qui contiennent la « charge utile ». On peut les activer, les désactiver et les supprimer ; pas les modifier.

Les « secrets » renferment quant à eux des métadonnées. Elles définissent entre autres les permissions d'accès et les politiques de réplication entre régions Google Cloud.

On accède aux secrets par le biais de la console Google Cloud ou par des API (REST, RPC).

Le principe du moindre privilège s'applique.
Par défaut, seuls les propriétaires de projets GCP peuvent accéder aux secrets. Les autres autorisations doivent être définies à travers le gestionnaires Cloud IAM. Trois rôles sont disponibles :

- administrateur ;
- « viewer » (autorisé à afficher les métadonnées des secrets) ;
- « secretAccessor » (autorisé à accéder à la charge utile).

La jonction est faite avec plusieurs services Google Cloud :

- la fonction de journaux d'audit ;
- Cloud DLP pour la découverte de secrets ;
- VPC Service Controls pour établir des périmètres de sécurité.

Elle est également effective dans la dernière version (0.5.0) de Berglas.

Tarification annoncée : 0,03 $ pour 10 000 opérations et 0,06 $ par mois pour chaque instance régionale d'une version de secret active. L'API accepte une taille maximale de 64 Ko par secret.

Photo d'illustration via Shutterstock.com