Engineer

Google Cloud

plateforme cloud de Google

Ce que c’est

Google Cloud est la partie de Google qui loue des capacités de calcul depuis ses propres centres de données : machines virtuelles Compute Engine, stockage objet Cloud Storage, bases gérées Cloud SQL, clusters Kubernetes GKE, entrepôt de données BigQuery et beaucoup d’autres services, tous facturés à l’usage. Son ancien nom, Google Cloud Platform ou GCP, reste courant, même dans une partie de la documentation de Google.

Tout ce que Google Cloud exploite pour un client réside dans un projet. Celui-ci regroupe les ressources, leurs API activées, les quotas consommés et le lien vers le compte de facturation qui paie. Il possède un nom affiché modifiable et un ID de projet unique dans tout Google Cloud, définitif une fois le projet créé. Les projets peuvent être regroupés dans des dossiers, eux-mêmes imbriqués ; tout l’arbre dépend d’une ressource d’organisation appartenant au compte Google Workspace ou Cloud Identity d’une entreprise. Les rôles et règles d’organisation définis sur l’organisation ou un dossier sont hérités par tous les projets en dessous. Un arbre bien conçu se gouverne facilement ; un arbre mal conçu est difficile à démêler.

Le réseau est organisé différemment des autres grands clouds. Dans Google Cloud, un réseau VPC, ses routes et ses règles de pare-feu forment une ressource de portée globale qui n’appartient à aucune région ; seuls les sous-réseaux sont régionaux. Une machine virtuelle en Belgique et une autre dans l’Iowa peuvent donc partager un réseau privé et se joindre par leurs adresses internes, sans VPN ni peering entre les deux régions. Sur AWS, en revanche, chaque VPC réside dans une seule région.

Il existe deux sortes d'identités. Les personnes se connectent avec des comptes Google et reçoivent des rôles IAM sur un projet, un dossier ou toute l'organisation. Les programmes utilisent des comptes de service : des identités qui appartiennent à un projet et qu'une machine virtuelle, un conteneur ou une tâche de compilation peut endosser. Associez un compte de service à une instance Compute Engine : le code qui s'y exécute peut appeler les API Google avec ses rôles, sans mot de passe ni fichier de clé sur disque.

Utilisez le concept pour prendre une décision

Utilisez « Qu'est-ce que Google Cloud ? » pour éclairer une décision réelle. Nous pouvons vous aider à relier ce concept au système que vous construisez ou achetez. Des serveurs dimensionnés selon vos usages réels, migrés vers le cloud ou hors du cloud, avec une estimation préalable de la facture mensuelle.

Découvrir nos prestations Contactez-nous →

Vérifiez les hypothèses derrière le terme

Appuyez-vous sur l'explication et les réalisations liées pour formuler les questions de votre projet. Nous pouvons examiner les hypothèses avec vous avant le choix d'un outil. 20 applications Docker sur Google Cloud et AWS — 20 applications conteneurisées déployées et surveillées

20 applications Docker sur Google Cloud et AWS Contactez-nous →

Pourquoi c'est important

Pour beaucoup d'équipes, les données motivent le choix de Google Cloud. BigQuery est un entrepôt sans serveurs à dimensionner : les tables résident dans des jeux de données d'un projet, les requêtes s'écrivent en SQL standard. Dans le modèle à la demande, chaque requête est facturée selon les octets lus ; avec la tarification à la capacité, on paie plutôt une capacité de traitement réservée, mesurée en slots. Le stockage est en colonnes : une requête paie les colonnes touchées plutôt que des lignes entières. À ses côtés, Cloud Storage sert de zone d'arrivée des données, et le chargement de fichiers depuis un bucket est une entrée classique. Une équipe qui devrait ailleurs provisionner et régler un cluster d'entrepôt peut commencer par un bucket, un jeu de données et une requête.

La frontière du projet est le deuxième motif : beaucoup de choses y sont rattachées. Facturation, quotas, API activées et IAM s'y rejoignent. Un projet par application et environnement trace une séparation nette : production et test ont des droits et des lignes de facture distincts. Fermer un projet arrête sa facturation et toutes ses ressources d'un coup. Ses propriétaires peuvent le restaurer pendant 30 jours, mais certains services, dont Cloud Storage, peuvent supprimer leurs données plus tôt. Au-dessus, une règle d'organisation définie une fois sur un dossier peut interdire des catégories entières de paramètres risqués, comme les réseaux créés automatiquement avec les projets ou les clés

de comptes de service téléchargeables, dans chaque projet inférieur. Une petite équipe garde ainsi une douzaine de projets cohérents sans vérifier chacun à la main.

À quoi cela ressemble en pratique

Trois réalisations du portfolio montrent Google Cloud comme zone d'arrivée pour un entrepôt de données, stockage distant des sauvegardes et extrémité d'un réseau privé.

Dans le travail sur les données, six pipelines ETL/ELT alimentaient BigQuery depuis un entrepôt derrière un VPN IPsec. Les jeux de données et tables sélectionnés et préparés étaient exportés, compressés avec gzip et transférés dans un bucket Google Cloud Storage. Le chargement et le mappage des schémas vers BigQuery étaient automatisés avec la CLI bq et des scripts d'ingestion Python. Une fois l'étape Cloud Storage et le chargement BigQuery automatisés, le travail entier prenait moins de 20 minutes contre au moins 3 heures à la main. BigQuery était actualisé chaque jour au lieu de chaque semaine, et les API Python qui le lisaient gagnaient 30 % de performances.

Pour les sauvegardes, cent sauvegardes de données critiques ont été automatisées, avec Barman pour PostgreSQL et Google Cloud pour les copies distantes. Bash et Python orchestraient et validaient tout le dispositif. Des règles de conservation maintenaient les copies à jour et des contrôles d'intégrité confirmaient que chacune était valide, et pas seulement présente. Les sauvegardes fonctionnaient ensuite automatiquement et pouvaient être vérifiées pour toutes les bases.

Côté réseau, huit tunnels WireGuard et IPsec entre Google Cloud et des systèmes Linux sur site ont été gérés et dépannés comme un ensemble. Leur configuration a été standardisée et leur état supervisé. Les problèmes récurrents de routage et d'échange de clés ont été résolus à la racine plutôt que par un redémarrage. Les huit tunnels fonctionnaient ensuite de manière sûre et fiable.

Où les problèmes surviennent

Les plus grands pièges de Google Cloud sont ses commodités : des réglages qui facilitent le premier après-midi et restent en place un an plus tard, bien après que tout le monde a oublié les avoir choisis.

Le réseau créé automatiquement reste ouvert. Sauf règle d'organisation l'empêchant, chaque nouveau projet commence avec un réseau créé automatiquement contenant un sous-réseau par région et quatre règles de pare-feu préconfigurées. Trois acceptent le trafic de 0.0.0.0/0, soit tout Internet : SSH sur tcp:22, bureau à distance sur tcp:3389 et ICMP. La quatrième autorise tout trafic TCP, UDP et ICMP provenant de 10.128.0.0/9 dans le réseau. Toute machine virtuelle dotée d'une adresse externe y est donc exposée aux tentatives SSH du monde entier. La contrainte `compute.skipDefaultNetworkCreation` évite ce réseau aux nouveaux projets ; un réseau personnalisé avec des règles désignant leurs sources le remplace.

Une clé de compte de service finit dans un dépôt. Une clé gérée par l'utilisateur est un fichier JSON permettant à son détenteur d'agir comme le compte de service. Sans restriction de durée configurée, la clé reste valable jusqu'à sa suppression. Ces fichiers se répandent facilement : dans les secrets CI, les images de conteneurs et, par erreur, les dépôts. Google recommande de choisir une alternative plus sûre partout où elle existe. Les charges de travail sur Google Cloud utilisent le compte de service associé à leur ressource. Ailleurs, par exemple dans un système CI ou un autre cloud, elles utilisent Workload Identity Federation, qui échange les propres identifiants du système externe contre des jetons Google de courte durée. Dans les organisations créées le 3 mai 2024 ou après, des contraintes de règles d'organisation désactivent initialement la création et le téléversement de clés ; les plus anciennes peuvent appliquer ces mêmes contraintes.

Une petite requête lit une grande table. Dans le modèle à la demande, BigQuery facture les octets lus par la requête. Sur une table non clusterisée, une clause `LIMIT` ne change pas cette quantité : `SELECT * ... LIMIT 10` renvoie dix lignes et facture chaque octet de chaque colonne. Sélectionnez uniquement les colonnes nécessaires, partitionnez les grandes tables par date pour que les requêtes filtrant sur celle-ci ignorent les anciennes partitions, vérifiez l'estimation d'une simulation avant toute nouvelle exécution et fixez un maximum d'octets facturés. Une requête dont l'estimation dépasse cette limite échoue avant de s'exécuter, sans frais.

Le stockage froid contient des données chaudes. Cloud Storage propose Nearline, Coldline et Archive, moins chers par gigaoctet stocké que Standard, en échange de frais de récupération et de durées minimales de 30, 90 et 365 jours. Un objet supprimé, remplacé ou déplacé avant ce minimum est facturé comme s'il était resté pendant toute la période. Des sauvegardes soumises à une rotation quotidienne ou des fichiers temporaires écrits puis supprimés par un

pipeline en moins d'une heure peuvent donc coûter plus cher dans Archive que dans Standard. Les classes plus froides conviennent aux données écrites une fois et rarement lues ; une règle de cycle de vie peut y déplacer les objets à mesure qu'ils vieillissent.

Pour aller plus loin

- Documentation Google Cloud — L'index Google des guides, références et tutoriels de chaque produit Google Cloud.
- Hiérarchie des ressources — L'imbrication des organisations, dossiers et projets et l'héritage de leurs rôles et règles.
- Règles de pare-feu VPC — Leur évaluation, y compris les règles initiales du réseau créé automatiquement.
- Bonnes pratiques de gestion des clés de comptes de service — Les fuites de clés, leur restriction et les solutions de remplacement.
- Estimer et maîtriser les coûts — Les conseils BigQuery sur les simulations, le maximum d'octets facturés et le faible gain de `LIMIT` .
- Classes de stockage — Les classes comparées, avec leurs durées minimales, frais de récupération et disponibilité.

Glossaire

Choisissez selon vos contraintes réelles

Présentez le parcours de déploiement, les risques opérationnels et les personnes d'astreinte. Nous pouvons définir un changement avec des vérifications, une procédure de reprise et une responsabilité claire.

Consulter les tarifs Contactez-nous →

Rendez la terminologie concrète

Demandez comment « Qu'est-ce que Google Cloud ? » s'applique à votre organisation. Un exemple concret tiré de votre système actuel suffit pour engager la discussion.

Découvrir nos prestations

welcome@engineer.company +45 50 10 61 84 Copenhague, Danemark

Emportez cette page avec vous

Fiche de contact

Créé avec soin et amour par D.

CVR 45969703 · Tagensvej 105C, 3. th, 2200 København N

Droit d'auteur © 2025 – aujourd'hui · Engineer ApS · Tous droits réservés.

Imprimé depuis https://engineer.company/fr/glossary/google-cloud/