Engineer

Google Cloud

Googles Cloudplattform

Was es ist

Google Cloud ist der Teil von Google, der Rechenleistung aus den eigenen Rechenzentren vermietet: virtuelle Maschinen auf Compute Engine, Objektspeicher in Cloud Storage, verwaltete Datenbanken in Cloud SQL, Kubernetes-Cluster in GKE, das Data Warehouse BigQuery und viele weitere Dienste, jeweils nach Nutzung bezahlt. Der ältere Name Google Cloud Platform oder GCP ist weiterhin verbreitet, selbst in Teilen von Googles eigener Dokumentation.

Alles, was Google Cloud für einen Kunden betreibt, liegt in einem Projekt. Ein Projekt fasst Ressourcen, die dafür aktivierten APIs, die genutzten Kontingente und die Verbindung zum zahlenden Abrechnungskonto zusammen. Es hat einen veränderbaren Anzeigenamen und eine Projekt-ID, die in ganz Google Cloud eindeutig ist und nach dem Anlegen nicht mehr geändert werden kann. Projekte lassen sich in Ordnern gruppieren, Ordner können weitere Ordner enthalten. Der ganze Baum hängt an einer Organisationsressource, die zum Google-Workspace- oder Cloud-Identity-Konto eines Unternehmens gehört. Rollen und Organisationsrichtlinien auf Organisations- oder Ordnerebene werden an alle darunterliegenden Projekte vererbt. Ein gut angelegter Baum lässt sich dadurch leicht verwalten, ein schlecht angelegter nur schwer entwirren.

Das Netzwerk ist anders zugeschnitten als bei den anderen großen Clouds. Ein VPC-Netzwerk in Google Cloud ist zusammen mit seinen Routen und Firewallregeln eine globale Ressource ohne Regionsbindung; nur seine Subnetze sind regional. Eine virtuelle Maschine in Belgien und eine andere in Iowa können deshalb dasselbe private Netz nutzen und einander über interne Adressen erreichen, ohne VPN oder Peering zwischen den beiden Regionen. Bei AWS liegt dagegen jede VPC in genau einer Region.

Es gibt zwei Arten von Identitäten. Menschen melden sich mit Google-Konten an und erhalten IAM-Rollen für ein Projekt, einen Ordner oder die ganze Organisation. Programme verwenden Dienstkonten: Identitäten, die zu einem Projekt gehören und unter denen eine virtuelle Maschine, ein Container oder ein Build-Job handeln kann. Wird einer Compute-Engine-Instanz ein Dienstkonto zugewiesen, kann der dort ausgeführte Code Google-APIs mit dessen Rollen aufrufen, ohne Passwort oder Schlüsseldatei auf der Festplatte.

Das Konzept für eine Entscheidung nutzen

Nutzen Sie „Was ist Google Cloud?" für eine konkrete Entscheidung. Wir können helfen, das Konzept mit dem System in Verbindung zu bringen, das Sie entwickeln oder einkaufen. Server werden nach dem tatsächlichen Bedarf dimensioniert und in die Cloud oder aus ihr heraus verlagert — die monatlichen Kosten stehen vorher fest.

Unsere Leistungen entdecken Kontakt aufnehmen →

Die Annahmen hinter dem Begriff prüfen

Nutzen Sie die Erklärung und die verlinkten Arbeiten, um Fragen für Ihr Projekt zu formulieren. Wir können die Annahmen gemeinsam mit Ihnen prüfen, bevor ein Werkzeug ausgewählt wird. 20 Docker-Apps auf Google Cloud und AWS betrieben — 20 bereitgestellte und überwachte Containeranwendungen

20 Docker-Apps auf Google Cloud und AWS betrieben Kontakt aufnehmen →

Warum es wichtig ist

Für viele Teams sind Daten der Grund, Google Cloud zu wählen. BigQuery ist ein Warehouse, für das keine Server dimensioniert werden müssen. Tabellen liegen in Datasets innerhalb eines Projekts, Abfragen werden in Standard-SQL geschrieben. Beim On-Demand-Modell wird jede Abfrage nach den gelesenen Bytes berechnet; bei der kapazitätsbasierten Preisgestaltung bezahlt man stattdessen reservierte Verarbeitungskapazität, gemessen in Slots. Der Speicher ist spaltenorientiert. Eine Abfrage bezahlt daher für die berührten Spalten und nicht für ganze Zeilen. Cloud Storage dient daneben als Ablage für eingehende Daten; Dateien aus einem Bucket zu laden ist ein üblicher Einstieg. Ein Team, das anderswo einen Warehouse-Cluster bereitstellen und abstimmen müsste, kann hier mit einem Bucket, einem Dataset und einer Abfrage beginnen.

Die Projektgrenze ist der zweite Grund, weil so viel daran hängt. Abrechnung, Kontingente, aktivierte APIs und IAM treffen sich im Projekt. Ein Projekt pro Anwendung und Umgebung zieht daher eine klare Grenze: Produktion und Test erhalten getrennte Rechte und eigene Positionen auf der Rechnung. Wird ein Projekt stillgelegt, endet seine Abrechnung und alle Ressourcen darin werden zugleich gestoppt. Die Eigentümer können es 30 Tage lang wiederherstellen, einige Dienste, darunter Cloud Storage, löschen ihre Daten jedoch möglicherweise früher. Oberhalb der Projekte kann eine einmal auf einem

Ordner gesetzte Organisationsrichtlinie ganze Klassen riskanter Einstellungen in allen darunterliegenden Projekten verbieten, etwa Standardnetzwerke oder herunterladbare Dienstkontoschlüssel. So hält ein kleines Team ein Dutzend Projekte konsistent, ohne jedes einzeln von Hand zu prüfen.

Wie es in der Praxis aussieht

Drei Portfolioeinträge zeigen Google Cloud als Ablage für Daten, die in ein Data Warehouse geladen werden, als externen Speicher für Sicherungen und als ein Ende eines privaten Netzes.

Bei der Datenarbeit versorgten sechs ETL/ELT-Pipelines BigQuery aus einem Warehouse hinter einem IPsec-VPN. Aufbereitete Datasets und Tabellen wurden exportiert, mit gzip komprimiert und in einen Google-Cloud-Storage-Bucket übertragen. Upload und Schemazuordnung nach BigQuery wurden mit der bq CLI und Python-Ingestionsskripten automatisiert. Nachdem der Zwischenschritt über Cloud Storage und das Laden in BigQuery selbstständig liefen, dauerte der gesamte Vorgang weniger als 20 Minuten statt mindestens 3 Stunden von Hand. BigQuery wurde täglich statt wöchentlich aktualisiert, und die daraus lesenden Python-APIs gewannen 30 % an Leistung.

Für Sicherungen wurden hundert kritische Datensicherungen automatisiert. Barman übernahm die PostgreSQL-Seite, Google Cloud hielt die externen Kopien. Bash und Python orchestrierten und validierten das gesamte Verfahren. Aufbewahrungsrichtlinien hielten die Kopien aktuell, Integritätsprüfungen bestätigten, dass jede verwendbar und nicht bloß vorhanden war. Die Sicherungen liefen danach automatisch und ließen sich über alle Datenbanken hinweg verifizieren.

Auf der Netzwerkseite wurden acht WireGuard- und IPsec-Tunnel zwischen Google Cloud und Linux-Systemen vor Ort gemeinsam verwaltet und Fehler darin untersucht. Ihre Konfiguration wurde vereinheitlicht, ihr Zustand überwacht. Wiederkehrende Routing- und Schlüsselaustauschprobleme wurden an der Ursache behoben statt mit einem Neustart übergangen. Danach liefen alle acht Tunnel sicher und zuverlässig.

Wo es schiefgeht

Was Google Cloud bequem macht, birgt seine größten Fallstricke: Einstellungen, die den ersten Nachmittag erleichtern und ein Jahr später noch bestehen, wenn sich längst niemand mehr an die ursprüngliche Entscheidung erinnert.

Das Standardnetzwerk bleibt offen. Sofern keine Organisationsrichtlinie es verhindert, beginnt jedes neue Projekt mit einem Standardnetzwerk, das in jeder Region ein Subnetz und vier vorab angelegte Firewallregeln besitzt. Drei akzeptieren Verkehr aus 0.0.0.0/0, also aus dem gesamten Internet: SSH auf tcp:22, Remote Desktop auf tcp:3389 und ICMP. Die vierte erlaubt sämtlichen TCP-, UDP- und ICMP-Verkehr aus 10.128.0.0/9 innerhalb des Netzes. Jede virtuelle Maschine mit einer externen Adresse in diesem Netz ist deshalb SSH-Versuchen von überall aus ausgesetzt. Die Einschränkung `compute.skipDefaultNetworkCreation` verhindert, dass neue Projekte ein solches Netz erhalten. An seine Stelle tritt ein eigenes Netz mit Regeln, die ihre Quellen ausdrücklich benennen.

Ein Dienstkontoschlüssel landet in einem Repository. Ein vom Nutzer verwalteter Schlüssel ist eine JSON-Datei, mit der jeder Besitzer als das Dienstkonto handeln kann. Standardmäßig bleibt der Schlüssel gültig, bis jemand ihn löscht. Solche Dateien verbreiten sich leicht: in CI-Secrets, in Container-Images und versehentlich in Repositories. Google empfiehlt, überall eine sicherere Alternative zu wählen, wo sie verfügbar ist. Workloads auf Google Cloud verwenden das an ihre Ressource gebundene Dienstkonto. Workloads außerhalb, etwa ein CI-System oder eine andere Cloud, verwenden Workload Identity Federation: Die eigenen Zugangsdaten des externen Systems werden gegen kurzlebige Google-Tokens getauscht. Bei Organisationen, die am oder nach dem 3. Mai 2024 angelegt wurden, sind Schlüsselerstellung und Schlüsselupload durch Organisationsrichtlinien standardmäßig deaktiviert. Ältere Organisationen können dieselben Einschränkungen setzen.

Eine kleine Abfrage liest eine große Tabelle. Beim On-Demand-Modell berechnet BigQuery die Bytes, die eine Abfrage liest. Auf einer nicht geclusterten Tabelle ändert eine `LIMIT`-Klausel diese Zahl nicht: `SELECT * ... LIMIT 10` liefert zehn Zeilen und berechnet jedes Byte jeder Spalte. Wählen Sie nur die benötigten Spalten aus. Partitionieren Sie große Tabellen nach Datum, damit darauf filternde Abfragen alte Partitionen überspringen. Prüfen Sie vor einer neuen Abfrage die Schätzung eines Probelaufs und setzen Sie ein Maximum für die abrechenbaren Bytes. Überschreitet die Schätzung dieses Limit, scheitert die Abfrage vor ihrer Ausführung, ohne Kosten zu verursachen.

Kalter Speicher hält warme Daten. Cloud Storage bietet Nearline, Coldline und Archive an. Pro gespeichertem Gigabyte kosten sie weniger als Standard, verlangen dafür aber Abrufgebühren und Mindestspeicherzeiten von 30, 90 beziehungsweise 365 Tagen. Wird ein Objekt vor Ablauf dieser Zeit gelöscht, ersetzt oder verschoben, wird es berechnet, als wäre es den ganzen Zeitraum gespeichert worden. Täglich rotierende Sicherungen oder temporäre Dateien, die eine Pipeline innerhalb einer Stunde schreibt und wieder entfernt, können in Archive deshalb mehr kosten als in Standard. Die kälteren Klassen eignen sich für Daten, die einmal geschrieben und selten gelesen werden. Eine Lebenszyklusregel kann Objekte mit zunehmendem Alter dorthin verschieben.

Weiterführende Lektüre

- Google-Cloud-Dokumentation — Googles Verzeichnis der Anleitungen, Referenzen und Tutorials für alle Google-Cloud-Produkte.
- Über die Ressourcenhierarchie — Wie Organisationen, Ordner und Projekte ineinanderliegen und wie Rollen und Richtlinien nach unten weitergegeben werden.
- VPC-Firewallregeln — Die Auswertung von Firewallregeln, einschließlich der Regeln eines neuen Standardnetzwerks.
- Dienstkontoschlüssel sicher verwalten — Wie Schlüssel nach außen gelangen, wie sie eingeschränkt werden und was sie ersetzen kann.
- Kosten schätzen und begrenzen — BigQuery-Hinweise zu Probeläufen, maximal abgerechneten Bytes und warum `LIMIT` wenig spart.
- Speicherklassen — Die Klassen im Vergleich, mit Mindestdauer, Abrufgebühren und Verfügbarkeit.

Glossar

Für Ihre tatsächlichen Rahmenbedingungen auswählen

Beschreiben Sie den Bereitstellungsweg, die Betriebsrisiken und die Bereitschaftsverantwortlichen. Wir können eine Änderung mit Prüfungen, einem Wiederherstellungsweg und klaren Zuständigkeiten abgrenzen.

Preise ansehen Kontakt aufnehmen →

Die Begriffe praktisch nutzbar machen

Fragen Sie, wie „Was ist Google Cloud?“ auf Ihre Organisation zutrifft. Ein konkretes Beispiel aus Ihrem bestehenden System reicht aus, um das Gespräch zu beginnen.

Unsere Leistungen entdecken

welcome@engineer.company +45 50 10 61 84 Kopenhagen, Dänemark

Nehmen Sie diese Seite mit

Kontaktkarte

Mit Sorgfalt und Liebe gestaltet von D.

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

Copyright © 2025 – heute · Engineer ApS · Alle Rechte vorbehalten.

Gedruckt von https://engineer.company/de/glossary/google-cloud/