Engineer

Google Cloud

Googles cloud-platform

Hvad det er

Google Cloud er den del af Google, der udlejer computerkraft fra sine egne datacentre: virtuelle maskiner i Compute Engine, objektlager i Cloud Storage, administrerede databaser i Cloud SQL, Kubernetes-klynger i GKE, data warehouset BigQuery og mange flere tjenester, alle betalt efter forbrug. Det ældre navn, Google Cloud Platform, og forkortelsen GCP bruges stadig bredt, også i dele af Googles egen dokumentation.

Alt, hvad Google Cloud kører for en kunde, ligger i et projekt. Et projekt er beholderen for ressourcerne, for de API'er, der er slået til for dem, for de kvoter, de trækker på, og for koblingen til den faktureringskonto, der betaler. Det har et visningsnavn, som kan ændres, og et projekt-id, der er unikt på tværs af hele Google Cloud og ligger fast, så snart projektet findes. Projekter kan samles i mapper (folders), mapper kan rumme andre mapper, og hele træet hænger under en organisationsressource, der hører til virksomhedens Google Workspace- eller Cloud Identity-konto. Roller og organisationspolitikker, der sættes på organisationen eller på en mappe, arves af hvert projekt nedenunder, så et velordnet træ er let at styre, og et rodet træ er svært at rede ud.

Netværket er tegnet anderledes end hos de andre store clouds. Et VPC-netværk i Google Cloud er sammen med sine ruter og firewallregler en global ressource, der står uden for enhver region; kun dets subnets er regionale. En virtuel maskine i Belgien og en anden i Iowa kan derfor dele ét privat netværk og nå hinanden på interne adresser uden VPN eller peering mellem de to regioner. Hos AWS ligger hvert VPC derimod i én enkelt region.

Identitet findes i to slags. Mennesker logger ind med Google-konti, som regel styret gennem organisationens Workspace eller Cloud Identity, og får IAM-roller på et projekt, en mappe eller hele organisationen. Programmer bruger

servicekonti (service accounts): identiteter, der hører til ét projekt, og som en virtuel maskine, en container eller et automatiseret job kan optræde som. Knyttes en servicekonto til en Compute Engine-instans, kan koden dér kalde Googles API'er med kontoens roller uden en adgangskode eller en nøglefil på disken.

Brug begrebet i en beslutning

Brug »Hvad er Google Cloud?« i en konkret beslutning. Vi kan knytte begrebet til det system, I bygger eller køber. Servere dimensioneret efter det, I rent faktisk bruger, flyttet op i skyen eller hjem igen, med den månedlige regning regnet ud først.

Se vores ydelser Kontakt os →

Undersøg antagelserne bag ordet

Brug forklaringen og det tilknyttede arbejde til at formulere spørgsmål til jeres projekt. Vi kan undersøge antagelserne sammen, før et værktøj vælges. Har drevet 20 Docker-apps på Google Cloud og AWS — 20 containeriserede applikationer udrullet og overvåget

Har drevet 20 Docker-apps på Google Cloud og AWS Kontakt os →

Hvorfor det betyder noget

For mange hold er data grunden til at vælge Google Cloud. BigQuery er et data warehouse uden servere at dimensionere: tabeller ligger i datasæt i et projekt, databaseforespørgsler skrives i standard-SQL, og i on demand-modellen faktureres hver forespørgsel efter de bytes, den læser, mens kapacitetsprissætning i stedet betaler for en reserveret mængde behandlingskraft, målt i slots. Lageret er kolonneorienteret, så en forespørgsel betaler for de kolonner, den rører, frem for hele rækker. Cloud Storage står ved siden af som modtagelsesområde, og at indlæse filer fra en bucket er en af standardvejene ind. Et hold, der andre steder skulle provisionere og tune en warehouse-klynge, kan begynde med en bucket, et datasæt og en forespørgsel.

Projektgrænsen er den anden grund, fordi så meget hænger på den. Fakturering, kvoter, aktiverede API'er og IAM mødes alle i projektet, så ét projekt pr. applikation og miljø trækker en klar streg: produktion og test får hver sine rettigheder og hver sin linje på regningen. Lukkes et projekt ned, stopper faktureringen og alle ressourcerne i det på én gang. Ejerne kan gendanne det i 30 dage, men nogle tjenester, heriblandt Cloud Storage, kan slette deres data før. Over projekterne kan en organisationspolitik, der sættes én gang på en mappe, forbyde hele klasser af risikable indstillinger, for eksempel standardnetværk eller servicekontonøgler, der kan downloades, i hvert projekt under den. Sådan holder et lille hold et dusin projekter ensartede uden at tjekke hvert enkelt i hånden.

Sådan ser det ud i praksis

Tre forløb i porteføljen viser Google Cloud som hjemsted for et data warehouse, som offsite-lager for backups og som den ene ende af et privat netværk.

I dataarbejdet forsynede seks ETL/ELT-pipelines BigQuery med data fra et warehouse bag en IPsec VPN. Komprimerede dataarkiver blev hentet over den sikre forbindelse, dataene blev renset og beriget med PL/pgSQL- og T-SQL-procedurer, og upload og skema-mapping til Google BigQuery blev automatiseret via bq CLI og Python-baseret dataindtagelse. Arbejde, der havde taget over 3 timer manuelt, kørte på under 20 minutter fra ende til anden, dataaktualiteten gik fra ugentlig til daglig synkronisering, og Python-API'erne, der forbrugte dataene, opnåede en 30 % ydeevneforbedring.

Til backups blev hundrede kritiske databackups automatiseret, med Barman på PostgreSQL-siden og Google Cloud, der holdt offsite-kopierne. Bash og Python orkestrerede og validerede hele regimet, med retention-politikker til at holde kopierne aktuelle og integritetstjek til at bekræfte, at hver enkelt faktisk var god og ikke bare til stede. Derefter kørte backups automatisk og kunne verificeres på tværs af hver database.

På netværkssiden blev otte WireGuard- og IPsec-tunneler mellem Google Cloud og on-premises-Linux-systemerne administreret og fejlfundet som ét sæt. Konfigurationen blev standardiseret, tilstanden blev overvåget, og de tilbagevendende routing- og key-exchange-problemer blev tacklet ved roden frem for med en genstart, hvorefter alle otte tunneler kørte sikkert og pålideligt.

Hvor det går galt

Google Clouds skarpeste kanter er bekvemmelighederne: indstillinger, der gør den første eftermiddag let og stadig står der et år senere, når ingen længere husker at have valgt dem.

Standardnetværket står åbent. Medmindre en organisationspolitik forhindrer det, starter hvert nyt projekt med et standardnetværk (default network), der har et subnet i hver region og fire forudfyldte firewallregler. Tre af dem tillader trafik fra 0.0.0.0/0, altså hele internettet: SSH på tcp:22, Remote Desktop på tcp:3389 og ICMP. Den fjerde tillader al TCP-, UDP- og ICMP-trafik fra 10.128.0.0/9 inde i netværket. Enhver virtuel maskine med en ekstern adresse på det netværk er derfor åben for SSH-forsøg fra hele verden. Begrænsningen

`compute.skipDefaultNetworkCreation` forhindrer, at nye projekter får et, og et brugerdefineret netværk med regler, der navngiver deres kilder, afløser det gamle.

En servicekontonøgle havner i et repository. En brugeradministreret nøgle er en JSON-fil, der lader enhver, som har den, optræde som servicekontoen, og som standard har den intet udløbstidspunkt: den gælder, indtil nogen sletter den. Den slags filer spreder sig let: til CI-secrets, til container-images og ved en fejl til repositories. Googles vejledning er at vælge et sikrere alternativ, hvor der findes et. Arbejdsbelastninger på Google Cloud bruger den servicekonto, der er knyttet til den ressource, de kører på, og arbejdsbelastninger andre steder, som et CI-system eller en anden cloud, bruger Workload Identity Federation, der bytter det eksterne systems egne legitimationsoplysninger til kortlivede Google-tokens. Organisationer oprettet den 3. maj 2024 eller senere har oprettelse og upload af nøgler slået fra som standard gennem begrænsninger i organisationspolitikken, og ældre organisationer kan sætte de samme begrænsninger.

En lille forespørgsel læser en stor tabel. I on demand-modellen fakturerer BigQuery for de bytes, en forespørgsel læser, og på en tabel, der ikke er klynget (clustered), lader en `LIMIT` -klausul det tal være uændret: `SELECT * ... LIMIT 10` returnerer ti rækker og fakturerer hver byte i hver kolonne. Vælg kun de kolonner, der skal bruges, partitionér store tabeller efter dato, så forespørgsler, der filtrerer på den, springer gamle partitioner over, tjek estimatet fra en dry run, før noget nyt køres, og sæt maximum bytes billed. En forespørgsel, hvis estimat overstiger den grænse, fejler, før den kører, uden at koste noget.

Koldt lager rummer varme data. Cloud Storage tilbyder klasserne Nearline, Coldline og Archive, der koster mindre pr. gigabyte lagret end Standard, til gengæld for gebyrer ved hentning og minimumslagringstider på 30, 90 og 365 dage. Et objekt, der slettes, erstattes eller flyttes før sit minimum, faktureres, som om det havde ligget der hele perioden. Backups, der roterer dagligt, eller midlertidige filer, som en pipeline skriver og fjerner inden for en time, kan derfor koste mere i Archive end i Standard. De koldere klasser passer til data, der skrives én gang og læses sjældent, og en livscyklusregel kan flytte objekter derned, efterhånden som de ældes.

Læs mere

- Google Cloud Documentation — Googles oversigt over vejledninger, referencer og tutorials til hvert Google Cloud-produkt.

- About resource hierarchy — hvordan organisationer, mapper og projekter indlejres, og hvordan roller og politikker arves nedad.
- VPC firewall rules — hvordan firewallregler evalueres, herunder de regler, standardnetværket starter med.
- Best practices for managing service account keys — hvordan nøgler lækker, hvordan de begrænses, og hvad man bruger i stedet.
- Estimate and control costs — BigQuerys vejledning om dry runs, maximum bytes billed og hvorfor `LIMIT` sparer så lidt.
- Storage classes — klasserne side om side med minimumslagringstider, hentningsgebyrer og tilgængelighed.

Ordliste

Vælg ud fra jeres faktiske vilkår

Medbring udrulningsforløbet, driftsrisiciene og dem, der har vagten. Vi kan afgrænse en ændring med kontroller, en vej tilbage og tydeligt ansvar.

Se, hvad det koster Kontakt os →

Gør begreberne praktiske

Spørg, hvordan »Hvad er Google Cloud?« gælder i jeres organisation. Et konkret eksempel fra jeres nuværende system er nok til at begynde samtalen.

Se vores ydelser

welcome@engineer.company +45 50 10 61 84 København, Danmark

Tag denne side med dig

Visitkort

Lavet med kærlighed af D.

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

Copyright © 2025 – nu · Engineer ApS · Alle rettigheder forbeholdes.

Udskrevet fra https://engineer.company/da/glossary/google-cloud/