Engineer

Google Cloud

Googles skyplattform

Hva det er

Google Cloud er den delen av Google som leier ut datakraft fra selskapets egne datasentre: virtuelle maskiner i Compute Engine, objektlagring i Cloud Storage, administrerte databaser i Cloud SQL, Kubernetes-klynger i GKE, datavarehuset BigQuery og mange flere tjenester, alt betalt etter bruk. Det eldre navnet, Google Cloud Platform eller GCP, er fortsatt mye brukt, også i deler av Googles egen dokumentasjon.

Alt Google Cloud kjører for en kunde, bor i et prosjekt. Et prosjekt er beholderen for ressursene, for API-ene som er slått på for dem, for kvotene de trekker på, og for koblingen til faktureringskontoen som betaler. Det har et visningsnavn som kan endres, og en prosjekt-ID som er unik i hele Google Cloud og ligger fast så snart prosjektet finnes. Prosjekter kan samles i mapper, mapper kan holde andre mapper, og hele treet henger under en organisasjonsressurs som hører til selskapets konto i Google Workspace eller Cloud Identity. Roller og organisasjonspolicyer som settes på organisasjonen eller på en mappe, arves av hvert prosjekt under, og det gjør et godt tegnet tre lett å styre og et dårlig tegnet tre tungt å nøste opp i.

Nettverket er tegnet annerledes enn hos de andre store skyene. Et VPC-nettverk i Google Cloud er, sammen med rutene og brannmurreglene sine, en global ressurs som ikke hører til noen region; bare subnettene er regionale. En virtuell maskin i Belgia og en annen i Iowa kan derfor dele ett privat nettverk og nå hverandre på interne adresser, uten VPN eller peering mellom de to regionene. På AWS lever derimot hver VPC i én enkelt region.

Identitet finnes i to slag. Mennesker logger inn med Google-kontoer og får IAM-roller på et prosjekt, en mappe eller hele organisasjonen. Programmer bruker tjenestekontoer: identiteter som hører til ett prosjekt, og som en virtuell maskin,

en container eller en pipeline kan opptre som. Knytter du en tjenestekonto til en Compute Engine-instans, kan koden som kjører der, kalle Googles API-er med rollene til den kontoen, uten passord eller nøkkelfil på disken.

Bruk begrepet i en beslutning

Bruk «Hva er Google Cloud?» i en konkret beslutning. Vi kan knytte begrepet til systemet dere bygger eller kjøper. Servere dimensjonert etter det du faktisk bruker, flyttet inn i skyen eller ut av den igjen, med månedsregningen regnet ut på forhånd.

Se tjenestene våre Ta kontakt →

Undersøk antakelsene bak ordet

Bruk forklaringen og det tilknyttede arbeidet til å formulere spørsmål for prosjektet. Vi kan undersøke antakelsene sammen før et verktøy velges. Driftet 20 Docker-apper på Google Cloud og AWS — 20 containeriserte applikasjoner produksjonssatt og overvåket

Driftet 20 Docker-apper på Google Cloud og AWS Ta kontakt →

Hvorfor det er viktig

For mange team er data grunnen til å velge Google Cloud. BigQuery er et datavarehus uten servere å dimensjonere: tabellene ligger i datasett inne i et prosjekt, spørringene skrives i standard SQL, og med prismodellen on-demand faktureres hver spørring etter antall byte den leser, mens kapasitetsprising i stedet betaler for en reservert mengde prosessering, målt i slots. Lagringen er kolonnebasert, så en spørring betaler for kolonnene den rører, og ikke for hele rader. Cloud Storage står ved siden av som mottaksområde, og å laste inn filer fra en bucket er en vanlig vei inn. Et team som andre steder ville satt opp og finjustert en klynge for datavarehuset, kan begynne med en bucket, et datasett og en spørring.

Prosjektgrensen er den andre grunnen, fordi så mye fester seg til den. Fakturering, kvoter, aktiverte API-er og IAM møtes alle i prosjektet, så ett prosjekt per applikasjon og miljø trekker en ren linje: produksjon og test får hver sine rettigheter og hver sine linjer på regningen. Stenges et prosjekt ned, stopper faktureringen og hver ressurs i det på én gang. Eierne kan gjenopprette det i 30 dager, men noen tjenester, blant dem Cloud Storage, kan slette dataene sine tidligere. Over prosjektene kan en organisasjonspolicy som settes én gang på en mappe, forby hele klasser av risikable innstillinger, som standardnettverk eller nøkler til tjenestekontoer som kan lastes ned, i hvert prosjekt under. Slik holder et lite team et dusin prosjekter konsistente uten å sjekke hvert av dem for hånd.

Slik ser det ut i praksis

Tre sider i porteføljen viser Google Cloud som mottaksområdet for et datavarehus, lageret utenfor huset for sikkerhetskopier og den ene enden av et privat nettverk.

I dataarbeidet matet seks ETL/ELT-pipelines BigQuery fra et datavarehus bak et IPsec-VPN. Kuraterte datasett og tabeller ble eksportert, komprimert med gzip og overført til en bucket i Google Cloud Storage, og opplastingen og skjemamappingen inn i BigQuery ble automatisert med bq CLI og Python-skript for innlasting. Med bucketen og BigQuery som de to siste leddene tok hele løpet under 20 minutter mot 3+ timer for hånd, synkroniseringen ble daglig i stedet for ukentlig, og Python-API-ene som brukte dataene, fikk 30 % bedre ytelse.

For sikkerhetskopiene ble hundre kritiske sikkerhetskopier av data automatisert, med Barman på PostgreSQL-siden og Google Cloud til kopiene utenfor huset. Bash og Python orkestrerte og validerte hele ordningen, med oppbevaringsregler som holdt kopiene oppdatert, og integritetskontroller som bekreftet at hver enkelt var god og ikke bare til stede. Etter det kjørte sikkerhetskopiene automatisk og kunne verifiseres for hver eneste database.

På nettverkssiden ble åtte WireGuard- og IPsec-tunneler mellom Google Cloud og lokale Linux-systemer forvaltet og feilsøkt som ett sett. Konfigurasjonen deres ble standardisert, helsen deres ble overvåket, og de gjentakende problemene med ruting og nøkkelutveksling ble rettet ved roten i stedet for med en omstart. Etter det kjørte alle åtte tunnelene sikkert og pålitelig.

Hvor det går galt

De skarpeste kantene i Google Cloud er bekvemmelighetene: innstillinger som gjør den første ettermiddagen enkel, og som fortsatt står der et år senere, lenge etter at alle har glemt at de ble valgt.

Standardnettverket blir stående åpent. Med mindre en organisasjonspolicy hindrer det, starter hvert nytt prosjekt med et standardnettverk som har et subnett i hver region og fire forhåndsutfylte brannmurregler. Tre av dem tar imot trafikk fra 0.0.0.0/0, altså hele internett: SSH på tcp:22, Remote Desktop på tcp:3389 og ICMP. Den fjerde tillater all TCP-, UDP- og ICMP-trafikk fra 10.128.0.0/9 inne i nettverket. Enhver virtuell maskin som får en ekstern adresse

i det nettverket, er derfor åpen for SSH-forsøk fra hvor som helst. Begrensningen `compute.skipDefaultNetworkCreation` hindrer at nye prosjekter får et slikt nettverk, og et egendefinert nettverk med regler som navngir kildene sine, tar plassen.

En nøkkel til en tjenestekonto havner i et repo. En brukeradministrert nøkkel er en JSON-fil som lar den som har den, opptre som tjenestekontoen, og som standard er den gyldig helt til noen sletter den. Slike filer sprer seg lett: inn i CI-hemmeligheter, inn i containerimages og, ved en feil, inn i repoer. Googles veiledning er å velge et tryggere alternativ der det finnes et. Arbeidslaster i Google Cloud bruker tjenestekontoen som er knyttet til ressursen de kjører på, og arbeidslaster andre steder, som et CI-system eller en annen sky, bruker Workload Identity Federation, som bytter det eksterne systemets egen legitimasjon mot kortlivede tokener fra Google. Organisasjoner som er opprettet 3. mai 2024 eller senere, har oppretting og opplasting av nøkler slått av som standard gjennom begrensninger i organisasjonspolicyen, og eldre organisasjoner kan sette de samme begrensningene selv.

En liten spørring leser en stor tabell. Med prismodellen on-demand fakturerer BigQuery for antall byte en spørring leser, og på en tabell som ikke er klynget, lar en `LIMIT`-klausul det tallet stå uendret: `SELECT * ... LIMIT 10` returnerer ti rader og fakturerer hver byte i hver kolonne. Velg bare kolonnene du trenger, partisjoner store tabeller etter dato slik at spørringer som filtrerer på den, hopper over gamle partisjoner, sjekk anslaget fra en tørrkjøring før du kjører noe nytt, og sett en grense for maksimalt antall fakturerte byte. En spørring der anslaget overstiger den grensen, feiler før den kjører, uten at det påløper noen kostnad.

Kald lagring holder varme data. Cloud Storage tilbyr klassene Nearline, Coldline og Archive, som koster mindre per lagret gigabyte enn Standard, mot gebyrer for uthenting og minste lagringstider på 30, 90 og 365 dager. Et objekt som slettes, erstattes eller flyttes før minstetiden er ute, faktureres som om det hadde vært lagret i hele perioden. Sikkerhetskopier som roteres daglig, eller midlertidige filer en pipeline skriver og fjerner innen en time, kan derfor koste mer i Archive enn de ville gjort i Standard. De kaldere klassene passer for data som skrives én gang og leses sjelden, og en livssyklusregel kan flytte objekter over i dem etter hvert som de blir eldre.

Les mer

- Google Cloud Documentation — Googles oversikt over veiledninger, referanser og opplæring for hvert Google Cloud-produkt.
- About resource hierarchy — hvordan organisasjoner, mapper og prosjekter ligger inni hverandre, og hvordan roller og policyer arves nedover.
- VPC firewall rules — hvordan brannmurreglene blir evaluert, også reglene standardnettverket starter med.
- Best practices for managing service account keys — hvordan nøkler lekker, hvordan du begrenser dem, og hva du bør bruke i stedet.
- Estimate and control costs — BigQuerys råd om tørrkjøringer, maksimalt antall fakturerte byte og hvorfor `LIMIT` sparer lite.
- Storage classes — klassene side om side, med minste lagringstid, gebyrer for uthenting og tilgjengelighet.

Ordliste

Velg ut fra deres faktiske rammer

Ta med utrullingsløpet, driftsrisikoene og dem som har vakt. Vi kan avgrense en endring med kontroller, en vei tilbake og tydelig ansvar.

Se hva det koster Ta kontakt →

Gjør begrepene praktiske

Spør hvordan «Hva er Google Cloud?» gjelder i organisasjonen deres. Et konkret eksempel fra dagens system er nok til å starte samtalen.

Se tjenestene våre

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

Ta med deg denne siden

Visittkort

Laget med kjærlighet av D.

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

Opphavsrett © 2025 – nå · Engineer ApS · Alle rettigheter forbeholdt.

Skrevet ut fra https://engineer.company/nb/glossary/google-cloud/