Engineer

Google Cloud

molnplattformen från Google

Vad det är

Google Cloud är den del av Google som hyr ut datorkraft från sina egna datacenter: virtuella maskiner i Compute Engine, objektlagring i Cloud Storage, hanterade databaser i Cloud SQL, Kubernetes-kluster i GKE, analysdatalagret BigQuery och många fler tjänster, som alla betalas efter användning. Det äldre namnet, Google Cloud Platform eller GCP, används fortfarande flitigt, även i delar av Googles egen dokumentation.

Allt som Google Cloud kör åt en kund finns inuti ett projekt. Ett projekt är behållaren för resurser, för de API:er som är påslagna för dem, för de kvoter de tar av och för kopplingen till det faktureringskonto som betalar. Projektet har ett visningsnamn som går att ändra och ett projekt-ID som är unikt i hela Google Cloud och permanent när projektet väl finns. Projekt kan grupperas i mappar, mappar kan innehålla andra mappar, och hela trädet hänger från en organisationsresurs som hör till ett företags konto i Google Workspace eller Cloud Identity. Roller och organisationspolicyer som sätts på organisationen eller på en mapp ärvs av varje projekt därunder, vilket gör ett väl ritat träd lätt att styra och ett dåligt ritat träd svårt att reda ut.

Nätverket är uppritat på ett annat sätt än i de andra stora molnen. Ett VPC-nätverk i Google Cloud är, tillsammans med sina rutter och brandväggsregler, en global resurs som inte hör till någon region, och det är bara dess subnät som är regionala. En virtuell maskin i Belgien och en annan i Iowa kan därför dela ett privat nätverk och nå varandra på interna adresser, helt utan VPN eller peering mellan de två regionerna. I AWS hör däremot varje VPC till en enda region.

Identiteter finns i två slag. Människor loggar in med Google-konton och får IAM-roller på ett projekt, en mapp eller hela organisationen. Program använder tjänstekonton: identiteter som hör till ett enda projekt och som en virtuell

maskin, en container eller en pipeline kan agera som. Koppla ett tjänstekonto till en instans i Compute Engine, så kan koden som körs där anropa Googles API:er med kontots roller, helt utan lösenord eller nyckelfil på disken.

Använd begreppet i ett beslut

Använd ”Vad är Google Cloud?” i ett konkret beslut. Vi kan knyta begreppet till systemet ni bygger eller köper. Servrar dimensionerade efter vad du faktiskt använder, flyttade till molnet eller tillbaka ut ur det, med månadskostnaden uträknad först.

Se våra tjänster Hör av er →

Granska antagandena bakom ordet

Använd förklaringen och det länkade arbetet för att formulera frågor till projektet. Vi kan undersöka antagandena tillsammans innan ett verktyg väljs. Drev 20 Docker-appar på Google Cloud och AWS — 20 containerbaserade applikationer, driftsatta och övervakade

Drev 20 Docker-appar på Google Cloud och AWS Hör av er →

Varför det spelar roll

För många team är data skälet att välja Google Cloud. BigQuery är ett analysdatalager där det inte finns några servrar att dimensionera: tabeller ligger i dataset inuti ett projekt, databasfrågor skrivs i standard-SQL, och med on-demand-modellen debiteras varje fråga efter antalet byte den läser, medan kapacitetsprissättning i stället betalar för en reserverad mängd bearbetning, mätt i slots. Lagringen är kolumnorienterad, så en fråga betalar för de kolumner den rör och inte för hela rader. Cloud Storage står bredvid som landningszon, och att läsa in filer från en bucket är en vanlig väg in. Ett team som på andra ställen skulle provisionera och trimma ett kluster för sitt analysdatalager kan börja med en bucket, ett dataset och en fråga.

Projektgränsen är det andra skälet, eftersom så mycket fäster vid den. Fakturering, kvoter, påslagna API:er och IAM möts alla i projektet, så ett projekt per applikation och miljö drar en ren gräns: produktion och test får separata behörigheter och separata rader på fakturan. Att stänga ned ett projekt stoppar på en gång faktureringen och varje resurs i det. Ägarna kan återställa det i 30 dagar, men vissa tjänster, bland dem Cloud Storage, kan radera sina data tidigare. Ovanför projekten kan en organisationspolicy som sätts en gång på en mapp förbjuda hela klasser av riskabla inställningar, t.ex. standardnätverk eller nedladdningsbara nycklar för tjänstekonton, i varje projekt under den. Så håller ett litet team ett dussin projekt konsekventa utan att kontrollera vart och ett för hand.

Så ser det ut i praktiken

Tre poster i portfolion visar Google Cloud som landningszon för ett analysdatalager, som lagring på annan plats för säkerhetskopior och som ena änden av ett privat nätverk.

I dataarbetet matade sex ETL/ELT-pipelines BigQuery från ett datalager bakom ett IPsec-VPN. Kurerade dataset och tabeller exporterades, komprimerades med gzip och fördes över till en bucket i Google Cloud Storage, och uppladdningen och schemamappningen till BigQuery automatiserades med bq CLI och skript i Python för datainläsning. Arbete som hade tagit över 3 timmar för hand kördes på under 20 minuter från början till slut, datafärskheten gick från veckovis till daglig synkronisering, och de API:er i Python som använde dessa data fick 30 % bättre prestanda.

På säkerhetskopieringssidan var det Google Cloud som förvarade kopiorna på annan plats när hundra kritiska säkerhetskopior av data automatiserades, medan Barman svarade för PostgreSQL-delen. Skript i Bash och Python styrde och validerade flödet. Regler för lagringstid höll säkerhetskopiorna aktuella, och för var och en bekräftade en integritetskontroll att den var bra och inte bara låg där. Säkerhetskopieringen kördes sedan automatiskt och gick att verifiera för varje databas.

På nätverkssidan förvaltades och felsöktes åtta tunnlar med WireGuard och IPsec mellan Google Cloud och lokalt driftade Linux-system som en helhet. Konfigurationen standardiserades, tunnlarnas tillstånd övervakades, och de återkommande problemen med routning och nyckelutbyte åtgärdades vid roten i stället för med en omstart, varefter alla åtta tunnlarna gick säkert och tillförlitligt.

Var det går fel

Google Cloud har sina vassaste kanter i bekvämligheterna: inställningar som gör den första eftermiddagen enkel och som fortfarande finns kvar ett år senare, långt efter att alla har glömt att de valde dem.

Standardnätverket förblir öppet. Om inte en organisationspolicy förhindrar det börjar varje nytt projekt med ett standardnätverk som har ett subnät i varje region och fyra förifyllda brandväggsregler. Tre av dem tar emot trafik från 0.0.0.0/0, alltså hela internet: SSH på tcp:22, Remote Desktop på tcp:3389 och

ICMP. Den fjärde tillåter all TCP-, UDP- och ICMP-trafik från 10.128.0.0/9 inne i nätverket. Varje virtuell maskin som får en extern adress i det nätverket är därför öppen för SSH-försök från var som helst. Villkoret `compute.skipDefaultNetworkCreation` hindrar nya projekt från att få ett sådant nätverk, och ett eget nätverk med regler som namnger sina källor ersätter det.

En nyckel för ett tjänstekonto hamnar i ett repo. En användarhanterad nyckel är en JSON-fil som låter den som har den agera som tjänstekontot, och som standard förblir den giltig tills någon raderar den. Sådana filer sprids lätt: till hemligheterna i CI, till containeravbildningar och, av misstag, till repon. Googles vägledning är att välja ett säkrare alternativ varhelst ett sådant finns. Arbetslaster i Google Cloud använder det tjänstekonto som är kopplat till resursen de körs på, och arbetslaster på andra ställen, t.ex. ett CI-system eller ett annat moln, använder Workload Identity Federation, som byter det externa systemets egna inloggningsuppgifter mot kortlivade token från Google. Organisationer som har skapats den 3 maj 2024 eller senare har skapande och uppladdning av nycklar avstängda som standard genom villkor i organisationspolicyn, och äldre organisationer kan sätta samma villkor.

En liten fråga läser en stor tabell. Med on-demand-modellen debiterar BigQuery för de byte som en fråga läser, och på en tabell som inte är klustrad lämnar en sats med `LIMIT` den siffran oförändrad: `SELECT * ... LIMIT 10` returnerar tio rader och debiterar varje byte i varje kolumn. Välj bara de kolumner som behövs, partitionera stora tabeller efter datum så att frågor som filtrerar på datumet hoppar över gamla partitioner, kontrollera uppskattningen från en torrkörning innan något nytt körs, och sätt ett tak för maximalt antal debiterade byte. En fråga vars uppskattning överstiger taket misslyckas innan den körs, och det kostar ingenting.

Kall lagring håller varma data. Cloud Storage erbjuder klasserna Nearline, Coldline och Archive, som kostar mindre per lagrad gigabyte än Standard i utbyte mot avgifter för hämtning och minsta lagringstider på 30, 90 och 365 dagar. Ett objekt som raderas, ersätts eller flyttas före sin minsta lagringstid debiteras som om det hade lagrats under hela perioden. Säkerhetskopior som roteras dagligen, eller tillfälliga filer som en pipeline skriver och tar bort inom en timme, kan därför kosta mer i Archive än de skulle göra i Standard. De kallare klasserna passar data som skrivs en gång och läses sällan, och en livscykelregel kan flytta objekt dit när de blir äldre.

Läs mer

- Google Cloud Documentation — Googles register över guider, referenser och handledningar för varje produkt i Google Cloud.
- About resource hierarchy — hur organisationer, mappar och projekt ligger i varandra, och hur roller och policyer flödar nedåt genom dem.
- VPC firewall rules — hur brandväggsregler utvärderas, inklusive de regler som standardnätverket börjar med.
- Best practices for managing service account keys — hur nycklar läcker, hur de kan begränsas och vad som ska användas i stället.
- Estimate and control costs — BigQuerys vägledning om torrkörningar, maximalt antal debiterade byte och varför `LIMIT` sparar lite.
- Storage classes — klasserna sida vid sida, med minsta lagringstider, avgifter för hämtning och tillgänglighet.

Ordlista

Välj utifrån era faktiska förutsättningar

Ta med driftsättningsvägen, driftsriskerna och dem som har jour. Vi kan avgränsa en förändring med kontroller, en väg tillbaka och tydligt ansvar.

Se vad det kostar Hör av er →

Gör begreppen praktiska

Fråga hur ”Vad är Google Cloud?” gäller i er organisation. Ett konkret exempel från ert nuvarande system räcker för att börja samtalet.

Se våra tjänster

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

Ta med dig den här sidan

Visitkort

Omsorgsfullt skapad med kärlek av D.

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

Upphovsrätt © 2025 – nu · Engineer ApS · Alla rättigheter förbehållna.

Utskrivet från https://engineer.company/sv/glossary/google-cloud/