Figure 1: image

Tutorial Google Cloud Platform: Dari Nol Hingga Mahir dengan GCP

Selamat datang di tutorial Google Cloud Platform (GCP) dari nol hingga mahir! Artikel ini akan membimbing Anda dalam memahami konsep dasar dan mahir menggunakan Google Cloud Platform untuk berbagai kebutuhan, mulai dari desain platform analitik permainan mobile hingga pengelolaan sumber daya dan data besar. Mari kita mulai!

Apa itu Google Cloud Platform (GCP)?

Google Cloud Platform (GCP) adalah rangkaian layanan komputasi awan yang ditawarkan oleh Google. GCP memungkinkan Anda untuk membangun, mengelola, dan mengoptimalkan berbagai jenis aplikasi dan layanan melalui infrastruktur Google yang aman dan skalabel.

Mengapa GCP Penting?

GCP memiliki banyak keunggulan, seperti:

- **Biaya Fleksibel**: Anda hanya membayar untuk sumber daya yang digunakan.
- **Skalabilitas**: Mudah untuk menyesuaikan dengan kebutuhan Anda.
- **Layanan Analitik dan Machine Learning**: Mendukung pengembangan aplikasi cerdas dengan dukungan analitik data dan pembelajaran mesin.

- **Manajemen Sumber Daya**: Memungkinkan pengelolaan dan organisasi yang efisien.
- **Kinerja Tinggi**: GCP menawarkan kinerja komputasi dan jaringan yang andal.

Bagian 1: Memulai dengan Google Cloud Platform

Membuat Akun GCP Gratis

Anda dapat memulai perjalanan Anda di GCP dengan mendaftar untuk akun gratis dengan masa percobaan selama 3 bulan dan kredit sebesar $300. Ini memungkinkan Anda untuk mencoba layanan GCP tanpa biaya awal. Setelah masa percobaan selesai, Anda tidak akan dikenakan biaya kecuali Anda memutuskan untuk meningkatkan paket Anda.

Untuk memaksimalkan manfaat dari masa percobaan ini, Anda disarankan untuk:

- **Mencoba Sendiri**: Belajar dengan mencoba langsung, menghadapi masalah, dan memperbaikinya.
- **Praktik**: Menggunakan GCP untuk menjalankan aplikasi dan eksperimen.
- **Eksplorasi**: Mempelajari dokumentasi resmi dan mencoba berbagai layanan.

Mengapa Migrasi ke GCP?

GCP menawarkan berbagai keuntungan bagi bisnis dan pengembang:

- **Biaya Rendah**: Tidak perlu investasi besar untuk perangkat keras.
- **Skalabilitas**: Dapat disesuaikan dengan permintaan, membayar hanya untuk yang Anda gunakan.
- **Proof of Concept**: Cepat membuat konsep baru dengan cepat.
- **Layanan Analitik dan Pembelajaran Mesin**: Mendukung pengembangan aplikasi cerdas.

Bagian 2: Mengoptimalkan Biaya dengan GCP

Menyusun Mesin Virtual (VM) dengan Efisien

Ada beberapa cara untuk mengoptimalkan biaya saat menggunakan mesin virtual di GCP:

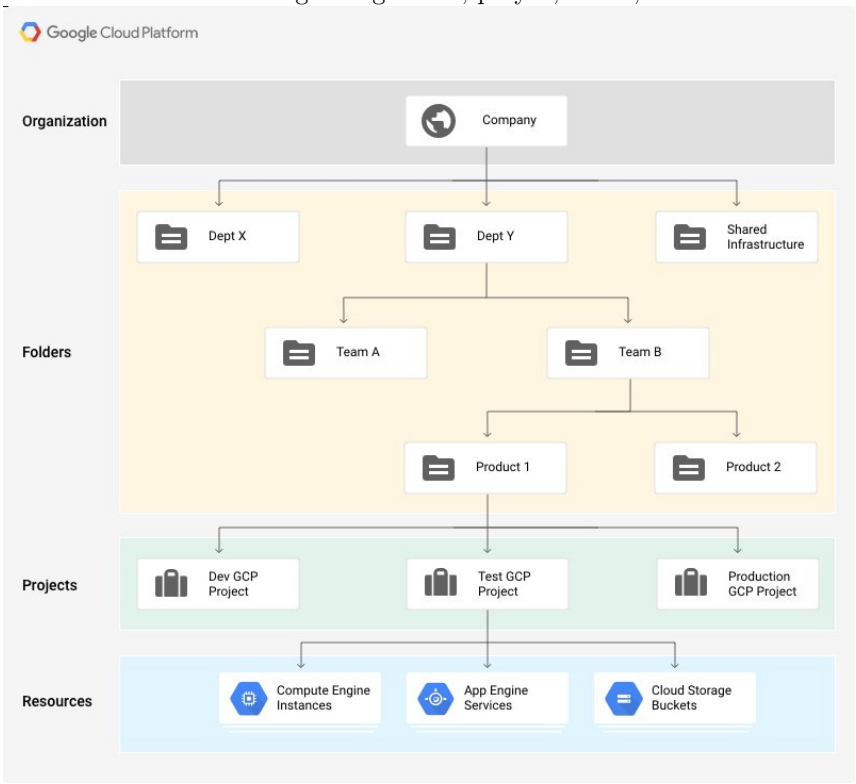
- **Custom Machine Types**: Pilih tipe mesin yang sesuai dengan kebutuhan RAM dan CPU Anda.
- **Preemptible VM's**: Gunakan mesin virtual preemptible untuk menghemat biaya hingga 80%. Ini cocok untuk aplikasi yang tidak kritis.
- **Sustained Use Discounts**: Semakin lama Anda menggunakan VM atau Cloud SQL instances, semakin besar diskonnya.

- **Committed Use Discounts**: Dapatkan diskon hingga 57% dengan berkomitmen untuk CPU dan RAM dalam periode tertentu.

Mengelola Sumber Daya di GCP

Pengelolaan sumber daya di GCP melibatkan hierarki sumber daya yang terdiri dari organisasi, proyek, folder, dan sumber daya itu sendiri. Pengaturan ini membantu dalam mengelola akses, konfigurasi, dan pengaturan sumber daya.

- **Resource Hierarchy**: Terdapat empat jenis sumber daya yang dapat dikelola melalui Resource Manager: organisasi, proyek, folder, dan sumber daya.



- **Labels**: Labels adalah pasangan kunci-nilai yang membantu mengorganisir sumber daya Anda. Gunakan labels untuk mengelompokkan dan memfilter sumber daya.
- **Cloud IAM**: Cloud IAM mengontrol siapa yang dapat melakukan apa pada sumber daya. Pengaturan ini didasarkan pada peran dan izin.

Identities Akun G Suite Domain adalah jenis akun yang dapat Anda gunakan untuk mengidentifikasi organisasi. Jika organisasi Anda sudah menggunakan Active Directory, Anda dapat menyinkronkannya dengan Cloud IAM menggunakan Cloud Identity.

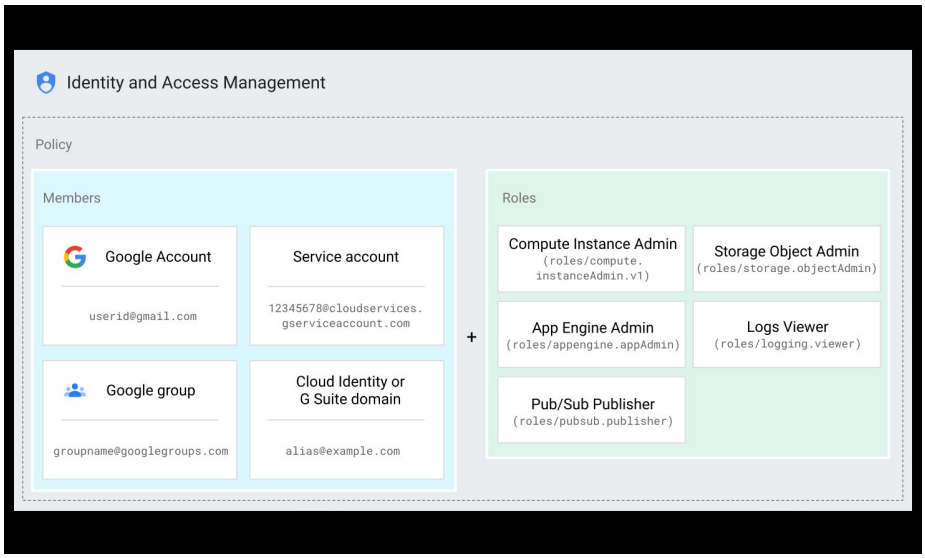


Figure 2: image

`allAuthenticatedUsers` digunakan untuk mewakili pengguna yang diautentikasi dalam GCP.

`allUsers` digunakan untuk mewakili siapa pun, baik yang sudah diautentikasi maupun belum.

Terkait akun layanan, beberapa praktik terbaik dari Google meliputi:

1. **Tidak Menggunakan Akun Layanan Default**
2. **Menerapkan Prinsip Privilege yang Paling Rendah**
   - Memperbolehkan siapa saja yang dapat berperan sebagai akun layanan.
   - Memberikan hanya kumpulan izin minimum yang diperlukan oleh akun tersebut.
   - Membuat akun layanan untuk setiap layanan dengan izin yang diperlukan oleh akun tersebut.

Roles (Peran) Peran adalah kumpulan izin. Ada tiga jenis peran:

1. **Primitive (Primitif)**: Peran GCP asli yang berlaku untuk seluruh proyek. Ada tiga peran dasar: Viewer, Editor, dan Owner. Editor berisi Viewer dan Owner berisi Editor.
2. **Predefined (Tersedia Awal)**: Memberikan akses ke layanan tertentu, misalnya, `storage.admin`.
3. **Custom (Kustom)**: Memungkinkan Anda membuat peran sendiri dengan menggabungkan izin tertentu yang Anda butuhkan.

Ketika memberikan peran, ikuti prinsip privilege yang paling rendah juga. Secara

umum, lebih baik menggunakan peran yang tersedia awal daripada peran primitif.

Cloud Deployment Manager Cloud Deployment Manager mengotomatisasi tugas yang dapat diulang seperti penyediaan, konfigurasi, dan penyebaran untuk banyak mesin.

Ini adalah layanan "Infrastructure as Code" Google, mirip dengan Terraform - meskipun Anda hanya dapat mendeploy sumber daya GCP. Ini digunakan oleh GCP Marketplace untuk membuat penyebaran yang telah dikonfigurasi sebelumnya.

Anda mendefinisikan konfigurasi Anda dalam file YAML, yang mencantumkan sumber daya yang ingin Anda buat (dibuat melalui panggilan API) dan properti mereka. Sumber daya didefinisikan oleh nama (VM-1, disk-1), tipe (compute.v1.disk, compute.v1.instance), dan properti (zone:europe-west4, boot:false).

Untuk meningkatkan kinerja, sumber daya dideploy secara paralel. Oleh karena itu, Anda perlu menentukan ketergantungan apa pun menggunakan referensi. Misalnya, jangan membuat mesin virtual VM-1 sampai persistent disk disk-1 telah dibuat. Sebaliknya, Terraform akan menentukan ketergantungan secara otomatis.

Anda dapat memodularkan file konfigurasi Anda menggunakan template sehingga dapat diperbarui dan dibagikan secara independen. Template dapat didefinisikan dalam Python atau Jinja2. Konten template Anda akan di-inline dalam file konfigurasi yang merujuk pada mereka.

Cloud Deployment Manager akan membuat manifest yang berisi konfigurasi asli Anda, semua template yang telah Anda impor, dan daftar diperluas dari semua sumber daya yang ingin Anda buat.

Cloud Operations (dahulu Stackdriver)

Cloud Operations menyediakan seperangkat alat untuk memantau, mengelola log, debugging, pelaporan kesalahan, profil, dan pelacakan sumber daya di GCP, AWS, dan bahkan on-premise.

Cloud Logging Cloud Logging adalah solusi terpusat GCP untuk manajemen log secara real-time. Untuk setiap proyek Anda, itu memungkinkan Anda untuk

menyimpan, mencari, menganalisis, memantau, dan memberikan peringatan pada data logging:

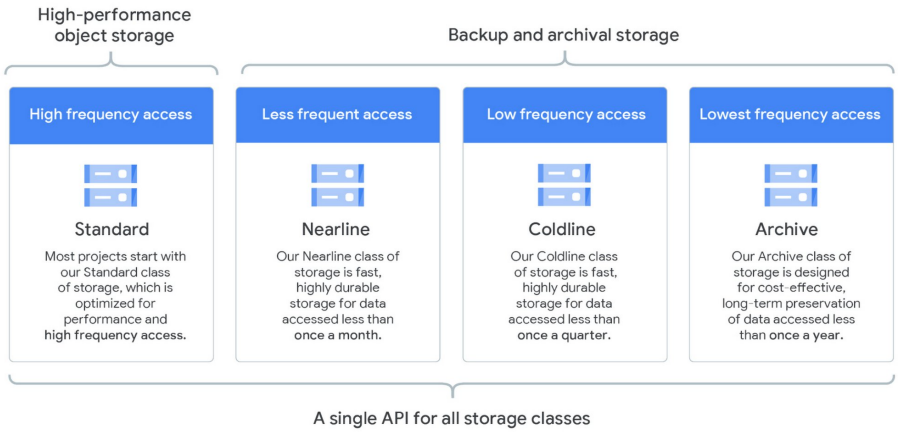
Secara default, data akan disimpan selama periode waktu tertentu. Periode retensi bervariasi tergantung pada jenis log. Anda tidak dapat mengambil log setelah melewati periode retensi ini. Log dapat diekspor untuk tujuan yang berbeda. Untuk melakukannya, Anda membuat sink, yang terdiri dari filter (untuk memilih apa yang ingin Anda log) dan tujuan: Google Cloud Storage (GCS) untuk retensi jangka panjang, BigQuery untuk analisis, atau Pub/Sub untuk streaming ke aplikasi lain. Anda dapat membuat metrik berbasis log di Cloud Monitoring dan bahkan mendapatkan peringatan ketika ada masalah. Log adalah kumpulan entri log. Entri log mencatat status atau acara dan mencakup nama log-nya, misalnya, `compute.googleapis.com/activity`. Ada dua jenis utama log:

- User Logs: Dibuat oleh aplikasi dan layanan Anda. Mereka ditulis ke Cloud Logging menggunakan API Cloud Logging, pustaka klien, atau agen logging yang diinstal pada mesin virtual Anda.
- Security logs: Dibagi menjadi:
  - Audit logs, untuk perubahan administratif****

Bagian 3: Penyimpanan Data di GCP

Menggunakan Google Cloud Storage (GCS)

Google Cloud Storage adalah layanan penyimpanan Google untuk data tak terstruktur seperti gambar, video, berkas, dan lainnya. Data ditempatkan dalam "buckets" dan dapat dikelola dengan perizinan dan kelas penyimpanan tertentu.



- **Objects dan Buckets**: Data disimpan dalam "objects" yang ditempatkan dalam "buckets".

- **Storage Classes**: Penyimpanan kelas memungkinkan Anda memilih SLA penyimpanan yang sesuai dengan kebutuhan Anda.
- **Object Lifecycle Management**: Anda dapat menentukan aturan yang mengatur tindakan pada suatu objek saat kondisi tertentu terpenuhi.

Dalam tutorial ini, Anda akan mempelajari langkah-langkah awal dalam memulai dengan Google Cloud Platform, mengoptimalkan biaya dengan bijak, serta mengelola dan menyimpan data secara efisien.

```
{    "lifecycle":{       "rule":[          {             "action":{
"type":"Delete"             },             "condition":{                "age":30,
"isLive":true             }          },          {             "action":{
"type":"Delete"             },             "condition":{                "numNewerVersions":2
}          },          {             "action":{                "type":"Delete"
},             "condition":{                "age":180,                "isLive":false
}          }       ]    } }
```

Permissions in GCS (Lanjutan) Selain peran IAM, Anda juga dapat menggunakan Access Control Lists (ACLs) untuk mengelola akses ke sumber daya dalam sebuah bucket.

Gunakan peran IAM jika memungkinkan, tetapi ingatlah bahwa ACL memberikan akses ke bucket dan objek individu, sementara peran IAM adalah izin yang berlaku di seluruh proyek atau bucket. Kedua metode ini bekerja bersamaan.

Untuk memberikan akses sementara kepada pengguna di luar GCP, Anda dapat menggunakan Signed URLs.

Bucket Lock (Kunci Bucket) Bucket lock memungkinkan Anda menerapkan periode retensi minimum untuk objek dalam sebuah bucket. Anda mungkin memerlukan ini untuk tujuan audit atau hukum.

Setelah bucket dikunci, itu tidak dapat dibuka kembali. Untuk menghapusnya, Anda harus terlebih dahulu menghapus semua objek dalam bucket, yang hanya dapat Anda lakukan setelah semua objek mencapai periode retensi yang ditentukan oleh kebijakan retensi. Hanya setelah itu, Anda dapat menghapus bucket.

Anda dapat menyertakan kebijakan retensi saat Anda membuat bucket atau menambahkan kebijakan retensi ke bucket yang sudah ada (ini juga berlaku secara retrospektif untuk objek yang sudah ada dalam bucket).

Fakta menarik: periode retensi maksimum adalah 100 tahun.

Relational Managed Databases in GCP Cloud SQL dan Cloud Spanner adalah dua layanan database yang dikelola yang tersedia di GCP. Jika Anda tidak ingin berurusan dengan semua pekerjaan yang diperlukan untuk menjaga database online, mereka adalah pilihan yang bagus. Anda selalu dapat membuat mesin virtual dan mengelola database Anda sendiri.

Cloud SQL Cloud SQL memberikan akses ke instans database MySQL atau PostgreSQL yang dikelola di GCP. Setiap instans terbatas pada satu wilayah (region) dan memiliki kapasitas maksimum 30 TB.

Google akan mengurus instalasi, cadangan, skalabilitas, pemantauan, failover, dan replika baca. Untuk alasan ketersediaan, replika harus didefinisikan di wilayah yang sama tetapi zona yang berbeda dari instans utama.

Data dapat dengan mudah diimpor (dengan mengunggah data ke Google Cloud Storage terlebih dahulu, kemudian ke instans) dan diekspor menggunakan SQL dumps atau format file CSV. Data dapat dikompres untuk mengurangi biaya (Anda dapat mengimpor file .gz secara langsung). Untuk migrasi "lift and shift," ini adalah pilihan yang bagus.

Jika Anda memerlukan ketersediaan global atau lebih banyak kapasitas, pertimbangkan menggunakan Cloud Spanner.

Cloud Spanner Cloud Spanner tersedia secara global dan dapat dengan baik meliputi skala (horizontal).

Dua fitur ini membuatnya mampu mendukung kasus penggunaan yang berbeda dari Cloud SQL dan juga lebih mahal. Cloud Spanner bukanlah pilihan untuk migrasi "lift and shift."

NoSQL Managed Databases in GCP Demikian pula, GCP menyediakan dua database NoSQL yang dikelola, Bigtable dan Datastore, serta layanan database in-memory, Memorystore.

Datastore Datastore adalah database dokumen yang sangat skalabel yang tidak memerlukan operasi yang rumit, ideal untuk aplikasi web dan mobile: status permainan, katalog produk, persediaan real-time, dan sebagainya. Cocok untuk:

Profil pengguna - aplikasi mobile Status simpan permainan Secara default, Datastore memiliki indeks bawaan yang meningkatkan kinerja pada kueri sederhana. Anda dapat membuat indeks Anda sendiri, disebut indeks komposit, yang didefinisikan dalam format YAML.

Jika Anda memerlukan throughput ekstrim (jumlah besar baca/tulis per detik), gunakan Bigtable sebagai gantinya.

Bigtable Bigtable adalah database NoSQL yang ideal untuk beban kerja analitis di mana Anda dapat mengharapkan volume tulis yang sangat tinggi, baca dalam hitungan milidetik, dan kemampuan untuk menyimpan informasi dalam terabyte hingga petabyte. Cocok untuk:

Analisis keuangan Data IoT Data pemasaran Bigtable memerlukan pembuatan dan konfigurasi node Anda sendiri (berbeda dengan Datastore atau BigQuery yang sepenuhnya dikelola). Anda dapat menambahkan atau menghapus node dari kluster Anda tanpa waktu henti. Cara paling sederhana untuk berinteraksi dengan Bigtable adalah dengan perangkat baris perintah cbt.

Kinerja Bigtable akan tergantung pada desain skema database Anda.

Anda hanya dapat mendefinisikan satu kunci per baris dan harus menyimpan semua informasi yang terkait dengan entitas dalam baris yang sama. Pikirkan ini seperti tabel hash. Tabel adalah langka: jika tidak ada informasi yang terkait dengan kolom, tidak ada ruang yang diperlukan. Untuk membuat pembacaan lebih efisien, coba simpan entitas terkait dalam baris yang berdekatan.

Karena topik ini sepadan dengan artikel tersendiri, saya sarankan Anda membaca dokumentasinya.

Memorystore Memorystore menyediakan versi yang dikelola dari Redis dan Memcache (database in-memory), menghasilkan kinerja yang sangat cepat. Instans bersifat regional, seperti Cloud SQL, dan memiliki kapasitas hingga 300 GB.

Bagaimana Memilih Database Anda Google menyukai pohon keputusan. Ini akan membantu Anda memilih database yang tepat untuk proyek Anda. Untuk data yang tidak terstruktur, pertimbangkan GCS atau prosesnya menggunakan Dataflow (akan dibahas nanti).

Jaringan di GCP

Virtual Private Cloud (VPC)

Infrastruktur jaringan GCP dibagi menjadi wilayah (regions), zona (zones), dan titik akses tepi (edge points of presence). Komponen-komponen ini menyediakan jaringan yang tangguh dan efisien untuk menjalankan layanan.

- **Wilayah (Regions):** Ini adalah area geografis independen di mana Google meng-host pusat data. Setiap wilayah terdiri dari tiga atau lebih zona, dan setiap wilayah didesain untuk berjarak setidaknya 100 mil dari wilayah lainnya. Contohnya, “us-central1.”
- **Zona (Zones):** Zona-zona adalah pusat data individu di dalam sebuah wilayah. Mereka dirancang untuk memberikan redundansi dan failover. Sebagai contoh, “us-central1-a.”
- **Titik Akses Tepi (Edge Points of Presence):** Ini adalah titik-titik di mana jaringan Google terhubung dengan internet, memastikan pertukaran data yang efisien.

Virtual Private Cloud (VPC) memungkinkan Anda membangun jaringan Anda di atas infrastruktur Google. VPC adalah jaringan yang didefinisikan oleh perangkat lunak di mana konsep-konsep jaringan tradisional berlaku.

- **Subnet:** Subnet adalah partisi logis dari sebuah jaringan, yang didefinisikan menggunakan notasi CIDR. Mereka hanya berada di satu wilayah, tetapi bisa melintasi beberapa zona. Pastikan rentang CIDR tidak tumpang tindih di antara subnet.
- **Alamat IP:** Alamat IP bisa internal (untuk komunikasi pribadi di dalam GCP) atau eksternal (untuk komunikasi dengan internet). Alamat IP eksternal dapat bersifat sementara (ephemeral) atau tetap (static). Secara

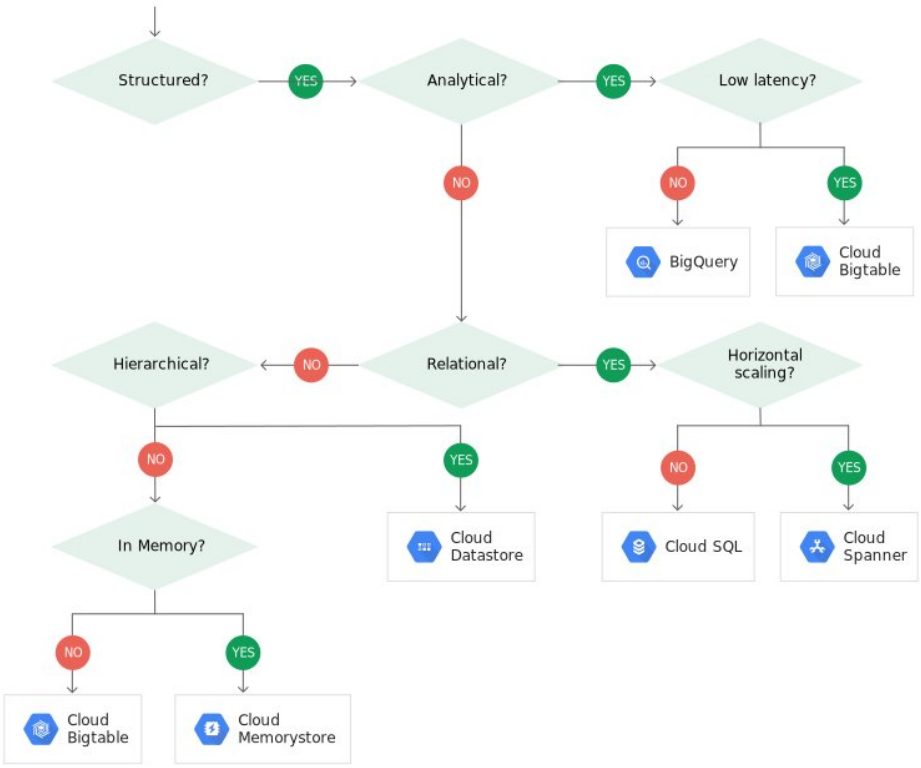


Figure 3: image

umum, Anda memerlukan alamat IP eksternal untuk terhubung ke layanan GCP. Namun, dalam beberapa kasus, Anda dapat mengonfigurasi akses privat untuk instansi yang hanya memiliki alamat IP internal.

Peraturan Firewall: Peraturan firewall digunakan untuk mengizinkan atau melarang lalu lintas ke mesin virtual Anda, baik masuk (ingress) maupun keluar (egress). Secara default, semua lalu lintas masuk diblokir dan semua lalu lintas keluar diizinkan. Peraturan firewall didefinisikan pada tingkat VPC, tetapi berlaku untuk instansi-individu atau kelompok instansi dengan menggunakan label jaringan (network tags) atau rentang IP.

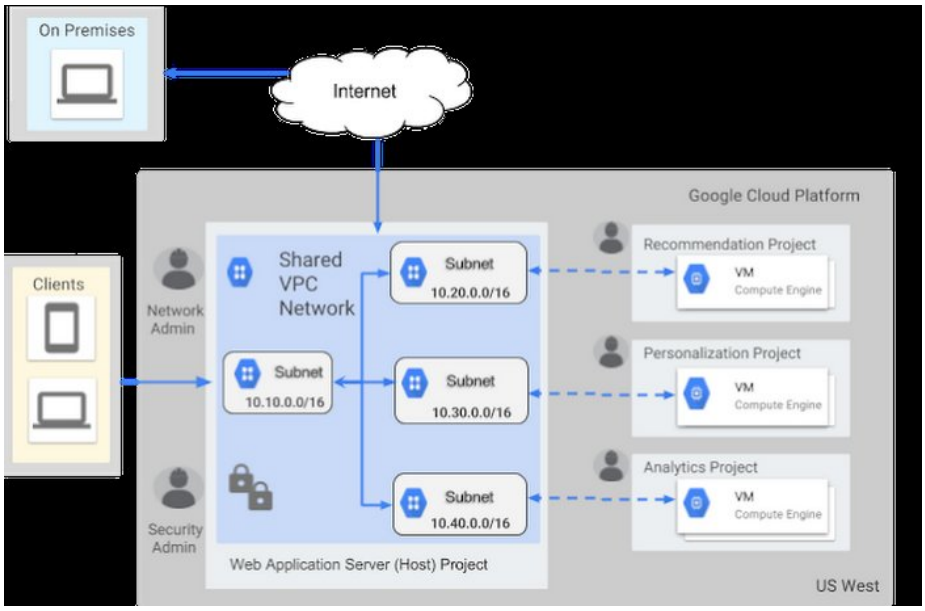


Figure 4: image

Shared VPC dan VPC Network Peering

- **Shared VPC:** Shared VPC adalah cara untuk berbagi sumber daya antara proyek-proyek yang berbeda dalam satu organisasi. Ini memungkinkan Anda mengendalikan faktur dan mengelola akses ke sumber daya di berbagai proyek, mengikuti prinsip kebijakan paling sedikit. Tanpa Shared VPC, Anda harus menempatkan semua sumber daya di satu proyek tunggal. Shared VPC terdiri dari proyek tuan rumah (host project), proyek layanan (service project), dan proyek mandiri (standalone project).
- **VPC Network Peering:** VPC Network Peering bukanlah layanan GCP, tetapi Anda dapat menggunakannya untuk menghubungkan jaringan Anda ke jaringan Google dan mengakses layanan seperti Youtube, Drive, atau layanan GCP lainnya. Ini berguna saat Anda perlu menghubungkan ke

Google tetapi tidak ingin melakukannya melalui internet publik. Dalam VPC Network Peering, Anda perlu memetakan alamat IP antara VPC yang terhubung.

Menghubungkan Infrastruktur On-Premise dan GCP

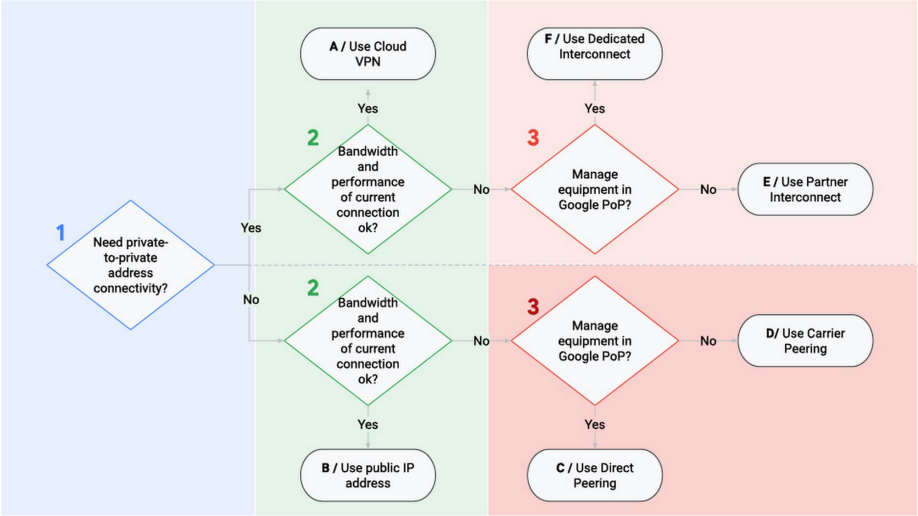


Figure 5: image

Ada tiga opsi untuk menghubungkan infrastruktur on-premise Anda ke GCP:

- **Cloud VPN:** Dengan Cloud VPN, lalu lintas Anda berjalan melalui internet publik melalui sebuah terowongan terenkripsi. Setiap terowongan memiliki kapasitas maksimum 3 Gbps dan Anda dapat menggunakan hingga 8 terowongan untuk kinerja yang lebih baik. Anda dapat mendefinisikan rute statis atau dinamis antara VPC Anda dan jaringan on-premise Anda.
- **Cloud Interconnect:** Dengan Cloud Interconnect, ada koneksi fisik langsung antara jaringan on-premise Anda dan VPC Anda. Ada dua jenis interkoneksi yang tersedia: Dedicated Interconnect dan Partner Interconnect. Dedicated Interconnect adalah koneksi langsung dengan kapasitas 10 hingga 200 Gbps, sedangkan Partner Interconnect melalui penyedia layanan dengan kecepatan 50 Mbps hingga 10 Gbps.
- **Cloud Peering:** Cloud Peering bukan layanan GCP, tetapi Anda dapat menggunakannya untuk menghubungkan jaringan Anda ke jaringan Google dan mengakses layanan seperti Youtube, Drive, atau layanan GCP lainnya. Ini berguna saat Anda perlu menghubungkan ke Google tetapi tidak ingin melakukannya melalui internet publik.

Dalam bagian berikutnya, saya akan membahas layanan database yang tersedia

di Google Cloud Platform (GCP).

Bagian 3 - Layanan Jaringan Lainnya dan Pemrosesan Data Besar di Google Cloud Platform (GCP)

Load Balancers di GCP

Di GCP, load balancer adalah perangkat lunak yang mendistribusikan permintaan pengguna di antara sekelompok instance. Load balancer dapat memiliki beberapa backend yang terkait dengannya, dengan aturan untuk memutuskan backend yang sesuai untuk permintaan tertentu.

Ada berbagai jenis load balancer. Perbedaannya terletak pada jenis lalu lintas (HTTP vs TCP/UDP - Layer 7 atau Layer 4), apakah mereka menangani lalu lintas eksternal atau internal, dan apakah lingkupnya regional atau global:

- **HTTP(s) Load Balancer:** Load balancer global yang menangani permintaan HTTP(s), mendistribusikan lalu lintas ke berbagai wilayah berdasarkan lokasi pengguna (ke wilayah terdekat dengan instance yang tersedia) atau pemetaan URL (load balancer dapat dikonfigurasi untuk meneruskan permintaan ke URL/news ke layanan backend tertentu dan URL/videos ke yang lain). Load balancer ini dapat menerima lalu lintas IPv4 dan IPv6 (IPv6 dihentikan di tingkat load balancer dan diteruskan sebagai IPv4 ke backend) dan memiliki dukungan asli untuk WebSockets.
- **SSL Proxy Load Balancer:** Load balancer global yang menangani lalu lintas TCP yang dienkripsi, mengelola sertifikat SSL untuk Anda.
- **TCP Proxy Load Balancer:** Load balancer global yang menangani lalu lintas TCP yang tidak dienkripsi. Secara default, tidak akan mempertahankan alamat IP klien, tetapi ini bisa diubah.
- **Network Load Balancer:** Load balancer regional yang menangani lalu lintas eksternal TCP/UDP, berdasarkan alamat IP dan port.
- **Internal Load Balancer:** Mirip dengan Network LB, tetapi untuk lalu lintas internal.

Cloud DNS

Cloud DNS adalah layanan Domain Name System (DNS) yang dikelola oleh Google, baik untuk lalu lintas internal maupun eksternal (publik). Ini akan memetakan URL seperti https://www.freecodecamp.org/ ke alamat IP. Ini adalah satu-satunya layanan di GCP dengan SLA 100% - tersedia sepanjang waktu.

Google Cloud CDN

Google Cloud CDN adalah Jaringan Pengiriman Konten Google. Jika Anda memiliki data yang tidak sering berubah (gambar, video, CSS, dll.), Masuk akal untuk menyimpannya dekat dengan pengguna Anda. Cloud CDN menyediakan 90 Edge Point of Presence (POP) untuk menyimpan data dekat dengan pengguna akhir Anda.

Setelah permintaan pertama, data statis dapat disimpan di POP, biasanya jauh lebih dekat dengan pengguna Anda daripada server utama Anda. Dengan demikian, dalam permintaan berikutnya, Anda dapat mengambil data lebih cepat dari POP dan mengurangi beban pada server backend Anda.

Tempat Anda Dapat Menjalankan Aplikasi di GCP

Saya akan menyajikan 4 tempat di mana kode Anda dapat dijalankan di GCP:

Figure 6: image

- **Google Compute Engine (GCE):** Mengizinkan Anda membuat mesin virtual di GCP. Ini adalah tempat di mana GKE dan GAE berjalan.
- **Google Kubernetes Engine (GKE):** Memudahkan Anda untuk menjalankan dan mengelola kluster Kubernetes di GCP.
- **App Engine:** Pilihan yang baik ketika Anda ingin fokus pada kode dan membiarkan Google mengelola infrastruktur Anda.
- **Cloud Functions:** Fungsi serverless yang memungkinkan Anda fokus pada kode tanpa khawatir tentang infrastruktur tempat kode akan dijalankan.

Google Compute Engine (GCE)

Google Compute Engine memungkinkan Anda membuat mesin virtual di GCP. GCE menyediakan infrastruktur tempat GKE dan GAE berjalan.

- **Disks:** Anda dapat menyimpan data VM Anda di Persistent disks, Local SSDs, atau Cloud Storage.
- **Snapshots:** Snapshots adalah cadangan disk Anda.
- **Images:** Images mengacu pada gambar sistem operasi yang diperlukan untuk membuat disk boot untuk instance Anda.
- **Instance Groups:** Instance groups memungkinkan Anda memperlakukan sekelompok instance sebagai satu kesatuan.
- **Security Best Practices:** Meliputi aspek keamanan untuk GCE, seperti Shielded VMs, menghindari akses dari internet publik, menggunakan gambar yang terpercaya, dan lainnya.

App Engine

App Engine merupakan pilihan yang baik ketika Anda ingin fokus pada kode dan membiarkan Google mengelola infrastruktur Anda. Ini cocok untuk berbagai penggunaan seperti website, aplikasi seluler, dan backend game.

- **Standard Environment:** Cepat dalam skalabilitas, namun hanya mendukung beberapa bahasa pemrograman.
- **Flexible Environment:** Lebih fleksibel daripada Standard Environment, cocok untuk lalu lintas yang lebih konsisten.

Google Kubernetes Engine (GKE)

Google Kubernetes Engine adalah layanan yang memudahkan Anda untuk menjalankan dan mengelola kluster Kubernetes di GCP.

Cloud Functions

Cloud Functions adalah fungsi serverless yang memungkinkan Anda fokus pada kode dan tidak perlu khawatir tentang infrastruktur.

Big Data di GCP

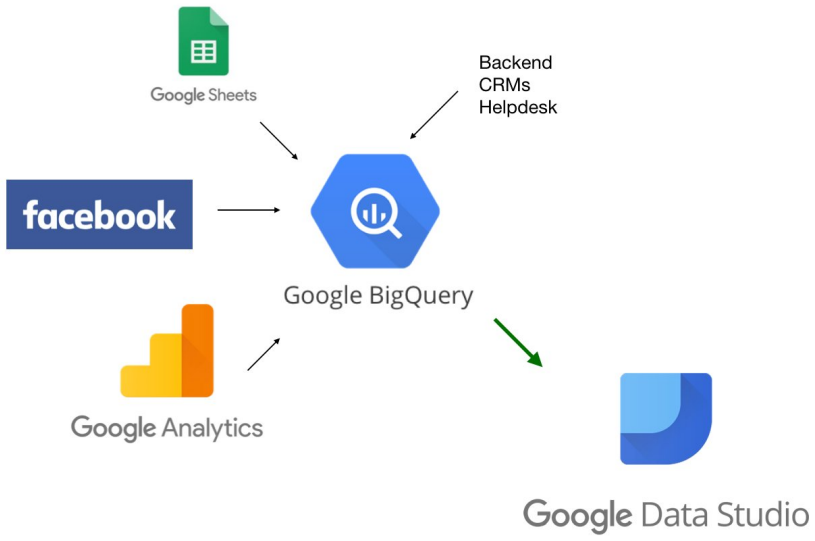


Figure 7: image

BigQuery: BigQuery adalah data warehousing berbasis serverless yang menyediakan kemampuan analitik untuk database skala petabyte.

Pub/Sub: Pub/Sub adalah antrian pesan yang dikelola sepenuhnya, memungkinkan Anda untuk mengontrol akses aplikasi GCP melalui HTTPs tanpa menginstal perangkat lunak VPN.

Cloud Dataflow: Cloud Dataflow adalah layanan dikelola untuk pemrosesan data stream dan batch, berbasis Apache Beam.

Cloud Dataproc: Cloud Dataproc adalah ekosistem Hadoop dan Spark yang dikelola oleh Google.

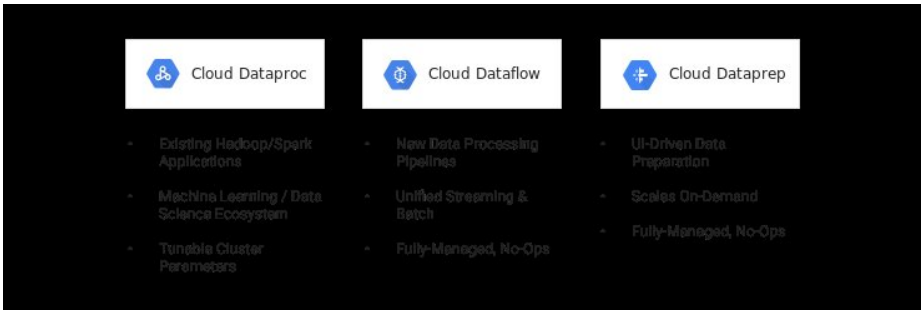


Figure 8: image

Google Cloud Dataproc: Managed Spark and Hadoop

Google Cloud Dataproc adalah layanan yang dikelola untuk menjalankan kerangka kerja pemrosesan data terdistribusi seperti Apache Spark dan Apache Hadoop dengan mudah dan cepat. Layanan ini memberikan kemudahan dalam mengelola klaster, skalabilitas, dan integrasi dengan alat analisis data lainnya di Google Cloud Platform. Berikut adalah penjelasan singkat dan langkah-langkah tutorial mengenai Google Cloud Dataproc:

Apa Itu Google Cloud Dataproc?

Google Cloud Dataproc memungkinkan Anda untuk membuat dan mengelola klaster pemrosesan data terdistribusi berdasarkan kerangka kerja populer seperti Apache Spark, Apache Hadoop, Apache Pig, dan Apache Hive. Dataproc mengotomatiskan tugas-tugas pengelolaan klaster, seperti provisioning, penjadwalan, dan penanganan kesalahan, sehingga Anda dapat fokus pada pemrosesan data.

Langkah-Langkah Tutorial: Menjalankan Klaster Spark di Cloud Dataproc

Berikut adalah contoh langkah-langkah sederhana untuk menjalankan klaster Spark menggunakan Google Cloud Dataproc:

Langkah 1: Persiapan Awal

1. Buka Konsol Google Cloud dan buat proyek baru (jika belum ada).
2. Aktifkan API Google Cloud Dataproc untuk proyek Anda.

Langkah 2: Membuat Klaster Dataproc

1. Di konsol GCP, buka bagian Dataproc dan pilih “Create Cluster.”
2. Tentukan pengaturan klaster seperti nama, zona, jenis mesin virtual, dan versi kerangka kerja (misalnya, Spark atau Hadoop).

3. Tentukan skrip inisialisasi yang akan dijalankan pada setiap node klaster saat pembuatan.

Langkah 3: Menjalankan Tugas Spark

1. Setelah klaster berhasil dibuat, buka tampilan klaster untuk melihat detailnya.
2. Di bagian "Jobs," pilih "Submit Job" dan pilih jenis pekerjaan Spark yang ingin Anda jalankan.
3. Tentukan parameter pekerjaan, seperti file JAR Spark, argumen, dan tujuan penyimpanan hasil.

Langkah 4: Memantau dan Menganalisis Hasil

1. Setelah pekerjaan selesai, Anda dapat melihat keluaran dan log di tampilan pekerjaan.
2. Anda juga dapat menganalisis data hasil pekerjaan menggunakan alat analisis data lainnya di GCP, seperti BigQuery atau Google Sheets.

Catatan Penting: - Google Cloud Dataproc memberikan kemampuan otomatisasi, seperti penjadwalan pekerjaan dan penanganan kesalahan. - Anda dapat mengubah ukuran klaster sesuai kebutuhan, baik untuk meningkatkan performa atau mengurangi biaya. - Dataproc mendukung banyak kerangka kerja pemrosesan data terdistribusi dan menyediakan lingkungan yang terisolasi untuk menjalankan pekerjaan Anda.

Dengan Google Cloud Dataproc, Anda dapat menjalankan dan mengelola klaster pemrosesan data terdistribusi dengan mudah, memungkinkan analisis data dalam skala besar dengan efisien.

Dataprep

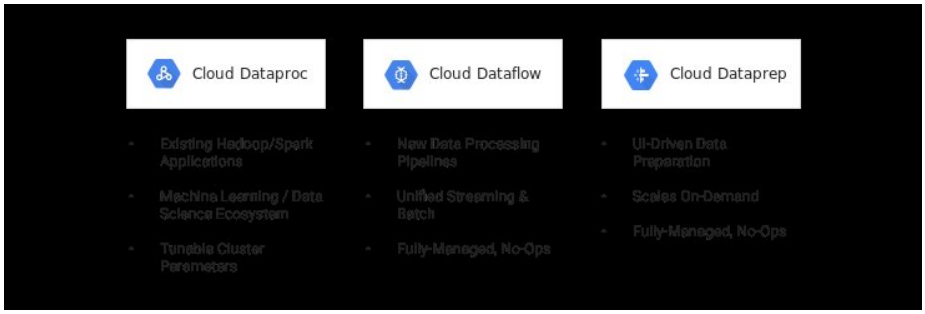


Figure 9: image

Google Cloud Dataprep: Data Cleaning and Preparation

Google Cloud Dataprep adalah layanan yang memungkinkan Anda membersihkan dan mempersiapkan data Anda sebelum diproses. Layanan ini menyediakan

antarmuka berbasis web untuk melakukan transformasi data yang beragam sebelum data dijalankan melalui proses analisis atau penyimpanan. Berikut adalah penjelasan dan langkah-langkah tutorial mengenai Google Cloud Dataprep:

Apa Itu Google Cloud Dataprep?

Google Cloud Dataprep memungkinkan Anda membersihkan, mentransformasi, dan memformat data mentah Anda menjadi bentuk yang lebih terstruktur dan siap untuk diolah lebih lanjut. Dengan antarmuka berbasis web yang intuitif, Anda dapat menjalankan berbagai transformasi pada data tanpa perlu menulis kode atau menggunakan alat pemrosesan data lainnya.

Langkah-Langkah Tutorial: Membersihkan dan Memformat Data Menggunakan Cloud Dataprep

Berikut adalah contoh langkah-langkah sederhana untuk membersihkan dan memformat data menggunakan Google Cloud Dataprep:

Langkah 1: Persiapan Awal

1. Buka Konsol Google Cloud dan buat proyek baru (jika belum ada).
2. Aktifkan API Google Cloud Dataprep untuk proyek Anda.

Langkah 2: Membuat Flow Data

1. Di konsol GCP, buka bagian Dataprep dan pilih "Create Flow."
2. Pilih sumber data Anda, seperti file CSV, JSON, atau database.
3. Tentukan pengaturan sumber data, seperti lokasi file dan format.

Langkah 3: Transformasi Data

1. Setelah flow data dibuat, Anda akan melihat antarmuka Dataprep dengan tampilan visual dari data Anda.
2. Gunakan fitur "Recipe" untuk menerapkan transformasi pada data. Misalnya, Anda dapat menghapus kolom yang tidak diperlukan, menggabungkan kolom, membersihkan data duplikat, dan lainnya.
3. Saat Anda menentukan transformasi, Anda akan melihat hasilnya secara real-time dalam tampilan data.

Langkah 4: Menjalankan Dataflow Job

1. Setelah transformasi selesai diterapkan, pilih "Run Job" untuk menjalankan Dataflow job yang akan memproses data berdasarkan transformasi yang Anda definisikan.
2. Setelah proses selesai, Anda dapat melihat hasilnya dalam tampilan job yang berjalan.

Langkah 5: Menyimpan Data yang Telah Ditransformasi

1. Setelah data telah diolah, Anda dapat menyimpannya ke berbagai tujuan, seperti Google Cloud Storage (GCS), BigQuery, atau bahkan ke file lokal.
2. Pilih "Export" dan tentukan tujuan penyimpanan serta format output yang diinginkan.

Catatan Penting: - Google Cloud Dataprep memberikan antarmuka visual yang memungkinkan Anda melakukan transformasi data tanpa perlu pengetahuan kode yang mendalam. - Anda dapat menjalankan transformasi secara interaktif dan melihat hasilnya secara langsung. - Setelah data telah diformat dan dicuci, Anda dapat menjalankan Dataflow job untuk memproses data dalam skala besar atau menyimpannya ke penyimpanan yang lebih lanjut.

Dengan Google Cloud Dataprep, Anda dapat mempersiapkan dan membersihkan data Anda dengan mudah sebelum melanjutkan ke tahap analisis atau penyimpanan selanjutnya.

Cloud Composer: Cloud Composer adalah layanan manajemen alur kerja berbasis Apache Airflow. **Google Cloud Composer: Penjelasan dan Tutorial**

Google Cloud Composer adalah layanan manajemen alur kerja berbasis cloud yang menggabungkan Apache Airflow untuk otomatisasi tugas dan pengelolaan alur kerja. Dalam komposer ini, Anda dapat membuat, menjadwalkan, dan mengelola alur kerja yang kompleks dengan dukungan penuh dari Google Cloud Platform. Berikut adalah penjelasan dan langkah-langkah tutorial untuk memulai dengan Google Cloud Composer:

Apa Itu Google Cloud Composer?

Google Cloud Composer adalah layanan yang memungkinkan Anda membuat dan menjalankan alur kerja otomatisasi dengan dukungan penuh untuk manajemen alur kerja Apache Airflow. Apache Airflow adalah alat open-source yang membantu mengotomatisasi tugas-tugas terjadwal dengan menyediakan antarmuka yang mudah digunakan untuk membuat dan menjalankan alur kerja kompleks.

Langkah-Langkah Tutorial: Membuat dan Menjalankan Alur Kerja dengan Google Cloud Composer

Langkah 1: Persiapan Awal

1. Buka Konsol Google Cloud dan buat proyek baru (jika belum ada).
2. Aktifkan API Google Cloud Composer untuk proyek Anda.

Langkah 2: Membuat Lingkungan Composer

1. Di konsol GCP, buka bagian Composer dan pilih "Create Environment."
2. Tentukan konfigurasi lingkungan, seperti nama, lokasi, dan versi Airflow yang ingin Anda gunakan.

3. Anda juga dapat menyesuaikan konfigurasi lingkungan, seperti ukuran klaster dan lokasi penyimpanan.

Langkah 3: Membuat dan Menjadwalkan Alur Kerja

1. Setelah lingkungan dibuat, buka komposer dan pilih lingkungan yang baru saja Anda buat.
2. Pilih "DAGs" di sisi kiri dan klik "Create" untuk membuat alur kerja baru.
3. Pilih tugas-tugas yang ingin Anda jalankan dalam alur kerja. Anda dapat menambahkan tugas-tugas seperti eksekusi skrip, mengirim email, menjalankan SQL, dan lain-lain.

Langkah 4: Menjadwalkan Alur Kerja

1. Setelah alur kerja selesai dibuat, Anda dapat menjadwalkannya untuk dijalankan secara berkala.
2. Pilih "Trigger" untuk menjadwalkan alur kerja. Anda dapat memilih frekuensi dan waktu pelaksanaan alur kerja.

Langkah 5: Melihat dan Memantau Alur Kerja

1. Di antarmuka komposer, Anda dapat melihat daftar alur kerja (DAGs) yang telah Anda buat.
2. Anda juga dapat melihat log pelaksanaan alur kerja, mendapatkan informasi tentang kesuksesan atau kegagalan tugas, dan melakukan pemantauan terhadap alur kerja Anda.

Catatan Penting: - Google Cloud Composer mengintegrasikan Apache Airflow dengan fitur-fitur GCP seperti Cloud Storage, BigQuery, dan lainnya. - Alur kerja yang dijalankan melalui Google Cloud Composer dapat membantu mengotomatisasi tugas-tugas rutin dan kompleks dengan mudah. - Anda dapat mengubah, memodifikasi, atau menambahkan tugas-tugas dalam alur kerja sesuai kebutuhan. - Composer memungkinkan Anda untuk mengelola alur kerja di GCP dengan cepat dan efisien.

Dengan Google Cloud Composer, Anda dapat mengelola alur kerja otomatisasi dengan lebih baik, mengotomatisasi tugas-tugas, dan memantau pelaksanaannya dengan mudah.

Bagian 8: AI dan Machine Learning di GCP

- **AI Platform:** AI Platform menyediakan platform yang dikelola sepenuhnya untuk menggunakan perpustakaan pembelajaran mesin seperti TensorFlow. **AI Platform di Google Cloud Platform: Penjelasan**

AI Platform adalah layanan di Google Cloud Platform yang dirancang khusus untuk memungkinkan pengembangan, pelatihan, dan penyebaran model machine

learning dan kecerdasan buatan. Dengan AI Platform, Anda dapat memanfaatkan sumber daya cloud untuk mengembangkan solusi AI yang canggih tanpa harus khawatir tentang kompleksitas infrastruktur.

Fitur Utama AI Platform:

1. **Pengembangan Model:**
   - **Notebooks:** AI Platform menyediakan lingkungan berbasis Jupyter yang dapat digunakan untuk membuat dan menjalankan notebook interaktif, memungkinkan eksplorasi data dan pengembangan model.
   - **AI Hub:** Platform ini memiliki katalog internal yang memungkinkan tim untuk berbagi notebook, pipeline, dan artefak lainnya yang berkaitan dengan machine learning.
2. **Pelatihan Model:**
   - **AutoML:** AI Platform AutoML memungkinkan Anda membuat model machine learning berkualitas tinggi tanpa perlu pengetahuan mendalam tentang machine learning. Ini mengotomatisasi sebagian besar proses, termasuk prapemrosesan data, pemilihan fitur, dan penyetelan model.
   - **Custom Training:** Anda juga dapat melatih model khusus Anda menggunakan sumber daya komputasi skala besar yang ditawarkan oleh Google Cloud. Anda dapat mengelola siklus hidup pelatihan, melihat metrik pelatihan, dan menyesuaikan parameter pelatihan.
3. **Penyebaran Model:**
   - **AI Platform Predictions:** Setelah model dilatih, Anda dapat dengan mudah menerapkannya dengan membuat layanan prediksi yang dapat digunakan oleh aplikasi eksternal melalui API.
   - **Managed Pipelines:** Anda dapat membuat pipeline end-to-end untuk mengotomatisasi alur kerja machine learning, mulai dari pra pemrosesan data hingga penyebaran model.
4. **Monitoring dan Penyempurnaan:**
   - **Monitoring dan Logging:** Anda dapat memantau performa model secara real-time dengan melihat metrik dan log yang dihasilkan oleh model saat dijalankan.
   - **Hyperparameter Tuning:** AI Platform juga mendukung penyetelan hiperparameter otomatis yang membantu Anda menemukan kombinasi parameter terbaik untuk meningkatkan performa model.

Langkah-Langkah Penggunaan AI Platform:

1. **Persiapan Data:**
   - Siapkan data pelatihan yang sesuai untuk model Anda. Bersihkan, transformasi, dan sesuaikan data sesuai kebutuhan.
2. **Pengembangan Model:**
   - Jika Anda ingin menggunakan AutoML, gunakan alat ini untuk membuat model dengan cepat dan mudah.
   - Jika Anda ingin membuat model khusus, gunakan lingkungan notebook AI Platform untuk mengembangkan dan menguji kode Anda.

3. **Pelatihan Model:**
    - Gunakan AI Platform untuk melatih model Anda dengan data pelatihan. Anda dapat menentukan parameter pelatihan dan menyimpan model yang dihasilkan.
4. **Penyebaran Model:**
    - Setelah model dilatih, gunakan AI Platform Predictions untuk menyebarkan model dan membuatnya dapat diakses melalui API.
5. **Pemantauan dan Penyempurnaan:**
    - Pantau performa model secara terus-menerus dan lakukan penyempurnaan jika diperlukan.

Dengan AI Platform, Anda dapat mengambil keuntungan dari infrastruktur cloud yang kuat untuk mengembangkan dan menerapkan solusi machine learning yang cerdas tanpa harus khawatir tentang konfigurasi dan manajemen infrastruktur yang rumit.

- **Cloud AutoML:** Google memungkinkan Anda menggunakan data Anda untuk melatih model mereka. **Cloud AutoML di Google Cloud Platform: Penjelasan**

Cloud AutoML adalah layanan di Google Cloud Platform yang dirancang untuk memungkinkan pengembang dan profesional non-ML untuk membuat dan melatih model machine learning berkualitas tinggi tanpa perlu memiliki pengetahuan mendalam tentang machine learning atau pemrograman yang kompleks. Dengan Cloud AutoML, Anda dapat memanfaatkan kecerdasan buatan untuk menyelesaikan masalah bisnis dengan cara yang lebih sederhana.

Fitur Utama Cloud AutoML:

1. **AutoML Vision:**
    - Layanan ini memungkinkan Anda untuk membuat model visi komputer yang dapat mengenali objek dalam gambar.
    - Anda hanya perlu memberikan kumpulan data gambar yang diberi label, dan Cloud AutoML Vision akan menghasilkan model yang dapat mengenali objek yang serupa dalam gambar baru.
2. **AutoML Natural Language:**
    - Layanan ini memungkinkan Anda untuk membangun model pemrosesan bahasa alami (NLP) yang dapat memahami dan menganalisis teks.
    - Dengan memberikan contoh teks yang diberi label, Cloud AutoML Natural Language dapat membuat model yang dapat mengklasifikasikan teks, mengekstrak informasi, dan lainnya.
3. **AutoML Tables:**
    - Layanan ini digunakan untuk membangun model machine learning untuk analisis tabel atau data terstruktur.
    - Anda hanya perlu memberikan data dalam bentuk tabel, dan Cloud AutoML Tables akan menghasilkan model yang dapat memprediksi nilai dalam kolom tertentu berdasarkan data lainnya.

4. **AutoML Video Intelligence:**
    - Layanan ini memungkinkan Anda untuk membuat model untuk menganalisis konten video.
    - Anda dapat membuat model yang dapat mendeteksi objek dalam video, mengenali aktivitas, dan melakukan analisis lainnya.

Langkah-Langkah Menggunakan Cloud AutoML:

1. **Persiapan Data:**
    - Siapkan data yang relevan dan berkualitas tinggi yang berkaitan dengan masalah yang ingin Anda selesaikan.
2. **Pengembangan Model:**
    - Pilih jenis model yang sesuai dengan masalah Anda (Vision, Natural Language, Tables, atau Video).
    - Unggah dan labelkan data Anda di antarmuka Cloud AutoML yang mudah digunakan.
3. **Pelatihan Model:**
    - Setelah data diunggah, model akan melatih berdasarkan data tersebut.
    - Anda dapat memantau dan menganalisis metrik pelatihan untuk memastikan kualitas model.
4. **Penilaian Model:**
    - Setelah model dilatih, Anda dapat mengevaluasi kinerjanya menggunakan data pengujian yang belum pernah dilihat sebelumnya.
5. **Penerapan Model:**
    - Setelah model dianggap memadai, Anda dapat menggunakannya untuk melakukan prediksi atau analisis pada data baru.

Dengan Cloud AutoML, Anda dapat memanfaatkan kemampuan machine learning tanpa perlu menjadi ahli dalam bidang tersebut. Ini sangat berguna bagi perusahaan dan individu yang ingin memanfaatkan teknologi machine learning untuk tujuan bisnis atau pengembangan tanpa harus menguasai detail teknis yang rumit.

Eksplorasi dan Visualisasi Data di GCP

- **Cloud Data Studio:** Data Studio memungkinkan Anda membuat visualisasi dan dasbor berdasarkan data yang ada di layanan Google dan GCP.

Google Cloud Data Studio: Penjelasan

Google Cloud Data Studio adalah alat visualisasi data gratis yang disediakan oleh Google. Alat ini memungkinkan Anda untuk membuat laporan interaktif dan dasbor visual dari berbagai sumber data, termasuk sumber data Google seperti Google Analytics, Google BigQuery, Google Sheets, dan sumber data lainnya seperti database SQL, file CSV, dan banyak lagi.

Fitur Utama Cloud Data Studio:

1. **Kustomisasi Visualisasi:**

- Cloud Data Studio menyediakan berbagai jenis visualisasi data, termasuk grafik batang, grafik garis, grafik lingkaran, tabel, kartu, dan lainnya.
- Anda dapat menyesuaikan gaya visualisasi, warna, label, dan elemen lainnya sesuai preferensi Anda.

2. **Sumber Data Fleksibel:**
   - Anda dapat menghubungkan Cloud Data Studio ke berbagai sumber data, termasuk Google Sheets, Google Analytics, Google BigQuery, file CSV, database SQL, dan sumber data lainnya.
   - Data dapat dianalisis dan divisualisasikan dalam satu dasbor interaktif.
3. **Interaktivitas dan Filter:**
   - Anda dapat menambahkan filter interaktif ke laporan Anda, yang memungkinkan pengguna untuk memfilter data berdasarkan kriteria tertentu.
   - Interaktivitas ini memungkinkan pengguna untuk menjelajahi data dengan lebih mendalam.
4. **Pengaturan Dasbor dan Halaman:**
   - Anda dapat membuat dasbor dengan beberapa halaman untuk mengatur visualisasi data Anda.
   - Setiap halaman dapat berisi grafik, tabel, dan visualisasi lainnya yang relevan dengan topik tertentu.
5. **Kolaborasi dan Berbagi:**
   - Anda dapat berkolaborasi dengan tim Anda dengan berbagi laporan Cloud Data Studio.
   - Laporan dapat dibagikan sebagai tautan yang dapat diakses atau disematkan di situs web atau platform lainnya.
6. **Ekspor Data:**
   - Anda dapat mengekspor data visualisasi dalam berbagai format, termasuk PDF, gambar, dan format data lainnya.

Langkah-Langkah Menggunakan Cloud Data Studio:

1. **Persiapan Data:**
   - Persiapkan data Anda dengan cara membersihkan dan mengolahnya sehingga siap untuk divisualisasikan.
2. **Buat Laporan:**
   - Buka Cloud Data Studio dan buat laporan baru.
   - Pilih jenis visualisasi yang ingin Anda tambahkan dan pilih sumber data yang sesuai.
3. **Pengaturan Visualisasi:**
   - Sesuaikan gaya visualisasi, tambahkan label, pilih metrik, dan tentukan filter jika diperlukan.
4. **Penambahan Interaktivitas:**
   - Tambahkan filter interaktif dan parameter jika ingin memberikan kemampuan pengguna untuk menyesuaikan tampilan data.
5. **Pengaturan Halaman:**

- Buat halaman tambahan dalam laporan untuk mengorganisasi visualisasi sesuai topik.

6. **Berbagi Laporan:**
   - Berbagi laporan dengan orang lain dengan membagikan tautan atau menanamkan laporan di situs web.

Cloud Data Studio memungkinkan Anda untuk membuat laporan visual yang kaya dan informatif tanpa perlu memiliki keterampilan pemrograman atau desain yang kompleks. Ini sangat berguna untuk mengkomunikasikan informasi bisnis atau data analitis dengan tim atau klien Anda.

- **Cloud Datalab:** Datalab memungkinkan Anda menjelajahi, menganalisis, dan memvisualisasikan data di berbagai layanan GCP.

Google Cloud Datalab: Penjelasan

Google Cloud Datalab adalah lingkungan interaktif yang memungkinkan Anda untuk menjalankan analisis data, eksplorasi, visualisasi, dan pemrosesan data di Google Cloud Platform (GCP). Datalab dirancang khusus untuk bekerja dengan data besar dan berbagai sumber data, termasuk Google BigQuery, Google Cloud Storage, dan banyak lagi.

Fitur Utama Cloud Datalab:

1. **Jupyter Notebooks Berbasis Cloud:**
   - Cloud Datalab dibangun di atas proyek Jupyter, yang memungkinkan Anda untuk menggabungkan kode, teks naratif, dan visualisasi dalam satu dokumen interaktif yang disebut notebook.
   - Anda dapat menjalankan blok kode dalam notebook dan melihat hasilnya secara langsung.
2. **Integrasi dengan GCP:**
   - Cloud Datalab terintegrasi dengan layanan Google Cloud seperti Google BigQuery, Google Cloud Storage, dan Google Compute Engine.
   - Anda dapat mengakses, menganalisis, dan memproses data di lingkungan yang familier.
3. **Pustaka Python dan SQL:**
   - Cloud Datalab mendukung bahasa pemrograman Python dan SQL.
   - Anda dapat menggunakan pustaka dan alat Python untuk analisis data, seperti pandas, numpy, dan scikit-learn.
4. **Eksplorasi Data:**
   - Anda dapat menjalankan kueri SQL di BigQuery untuk mengambil data dan melakukan eksplorasi.
   - Hasil kueri dapat divisualisasikan dalam bentuk grafik dan visualisasi lainnya.
5. **Visualisasi Interaktif:**
   - Cloud Datalab mendukung visualisasi interaktif menggunakan pustaka seperti Matplotlib dan Seaborn.

- Anda dapat membuat grafik, plot, dan visualisasi lainnya untuk mewakili data secara visual.

6. **Kustomisasi Lingkungan:**
   - Anda dapat menginstal pustaka tambahan dan mengonfigurasi lingkungan Datalab sesuai kebutuhan Anda.

Langkah-Langkah Menggunakan Cloud Datalab:

1. **Buat Instance Datalab:**
   - Buka Google Cloud Console dan buat instance Datalab di GCP.
2. **Buka Notebook:**
   - Buka Datalab dalam browser dan buka notebook baru.
3. **Eksplorasi Data:**
   - Gunakan SQL untuk mengambil data dari BigQuery atau GCS.
   - Analisis dan eksplorasi data menggunakan pustaka Python seperti pandas.
4. **Visualisasi Data:**
   - Gunakan pustaka visualisasi Python untuk membuat grafik dan visualisasi lainnya.
   - Lihat hasilnya langsung dalam notebook.
5. **Pemrosesan Data:**
   - Lakukan pemrosesan data menggunakan kode Python.
   - Terapkan transformasi dan manipulasi data sesuai kebutuhan.
6. **Berbagi Hasil:**
   - Anda dapat mengunduh notebook, berbagi tautan notebook, atau menyimpan hasil visualisasi dalam format gambar.

Google Cloud Datalab memungkinkan para ilmuwan data, analis bisnis, dan pengembang untuk bekerja dengan data besar secara interaktif dan efisien. Dengan menggunakan notebook Jupyter yang kuat, Anda dapat menjalankan analisis mendalam, mengeksplorasi data, dan menciptakan visualisasi yang informatif.

Keamanan di GCP

- **Enkripsi di Google Cloud Platform:** Data di GCP dienkripsi baik saat beristirahat (data yang disimpan di disk) maupun saat transit (data yang bergerak di jaringan).

Enkripsi di Google Cloud Platform (GCP)

Enkripsi adalah praktik penting dalam keamanan informasi untuk melindungi data dari akses yang tidak sah dan potensi pelanggaran privasi. Dalam GCP, terdapat dua konsep utama dalam enkripsi: enkripsi pada saat istirahat (encryption at rest) dan enkripsi saat transit (encryption in transit).

1. Encryption at Rest (Enkripsi pada Saat Istirahat): Enkripsi pada saat istirahat adalah praktik mengenkripsi data saat data disimpan di tempat penyimpanan fisik, seperti disk keras atau penyimpanan cloud. GCP menyediakan mekanisme otomatis untuk mengenkripsi data pada saat istirahat:

Figure 10: image

- **Google Cloud Storage (GCS):** Data yang disimpan di GCS secara default dienkripsi pada saat istirahat dengan menggunakan Advanced Encryption Standard (AES) dengan 256-bit key.
- **Google Compute Engine (GCE):** Persistent disks di GCE juga dienkripsi pada saat istirahat dengan menggunakan AES-256.
- **Google BigQuery:** Data yang disimpan di BigQuery dienkripsi pada saat istirahat secara otomatis.
- **Google Cloud SQL:** Data dalam instance Google Cloud SQL juga dienkripsi pada saat istirahat.

Anda tidak perlu melakukan konfigurasi khusus untuk mendapatkan enkripsi pada saat istirahat ini. GCP mengelola enkripsi ini di belakang layar untuk melindungi data Anda.

2. Encryption in Transit (Enkripsi Saat Transit): Enkripsi saat transit merujuk pada praktik mengenkripsi data ketika data sedang dalam perjalanan antara sumber dan tujuan, seperti saat data dikirim melalui jaringan atau internet. GCP juga menyediakan enkripsi saat transit:

- **HTTPS:** Komunikasi antara layanan GCP dan klien Anda (seperti browser web) dienkripsi menggunakan protokol HTTPS yang menggunakan SSL/TLS.
- **VPN:** Ketika Anda menghubungkan jaringan Anda ke GCP menggunakan VPN (Virtual Private Network), data yang dikirim antara jaringan Anda dan GCP dienkripsi.
- **Interconnect:** Jika Anda menggunakan Cloud Interconnect untuk menghubungkan jaringan fisik Anda dengan GCP, data yang dikirim melalui Interconnect juga dienkripsi.
- **VPC Peering:** Ketika data dikirim antara Virtual Private Cloud (VPC) yang berbeda melalui VPC peering, data juga dienkripsi pada saat transit.
- **Google Cloud Pub/Sub:** Data yang dikirim melalui layanan Pub/Sub dienkripsi saat transit.

Penting untuk diingat bahwa sementara GCP menyediakan enkripsi otomatis pada saat istirahat dan enkripsi pada saat transit, Anda juga bertanggung jawab untuk mengatur pengaturan keamanan yang sesuai di sisi klien Anda untuk memastikan keamanan data secara keseluruhan dalam solusi GCP Anda.

Link Encryption at rest : https://cloud.google.com/docs/security/encryption/default-encryption **Link Encryption in transit** : https://cloud.google.com/docs/security/encryption-in-transit

- **Cloud Key Management Service (KMS):** KMS adalah layanan yang memungkinkan Anda mengelola kunci enkripsi Anda.

Cloud Key Management Service (KMS) adalah layanan yang disediakan oleh Google Cloud Platform (GCP) yang memungkinkan Anda untuk mengelola dan mengontrol kunci enkripsi Anda dengan aman. KMS memungkinkan Anda untuk membuat, mengimpor, mengelola, dan menggunakan kunci enkripsi untuk melindungi data dan sumber daya yang ada di GCP.

Fitur Utama Cloud KMS:

1. **Pengelolaan Kunci yang Sentral:** Cloud KMS memungkinkan Anda untuk membuat dan mengelola kunci enkripsi yang sentral untuk digunakan di seluruh solusi GCP Anda. Ini memungkinkan Anda untuk memiliki kontrol penuh atas pengelolaan kunci dan enkripsi data.
2. **Hierarchy of Keys:** Cloud KMS memungkinkan Anda untuk membuat hirarki kunci dengan kunci induk (parent keys) dan kunci anak (child keys). Hal ini membantu dalam pengelolaan skala dan struktur kunci yang kompleks.
3. **Enkripsi Custom:** Anda dapat menggunakan Cloud KMS untuk mengenkripsi data Anda sendiri dengan kunci yang Anda kelola, baik di dalam GCP maupun di luar GCP.
4. **Integrasi dengan Layanan GCP:** Cloud KMS terintegrasi dengan layanan GCP lainnya seperti Google Cloud Storage (GCS), Google Compute Engine (GCE), Google Cloud SQL, dan lainnya. Anda dapat menggunakan kunci yang dikelola oleh Cloud KMS untuk melindungi data di layanan-layanan ini.
5. **Audit dan Logging:** Cloud KMS menyediakan audit trail untuk aktivitas pengelolaan kunci dan penggunaan kunci. Ini membantu dalam pemantauan dan pemahaman aktivitas yang terjadi terkait dengan kunci Anda.

Keuntungan Menggunakan Cloud KMS:

- **Keamanan:** Cloud KMS membantu melindungi kunci enkripsi Anda dari akses yang tidak sah dengan menggunakan praktik keamanan tingkat tinggi.
- **Pengelolaan Sentral:** Anda dapat mengelola semua kunci enkripsi Anda dari satu tempat yang sentral, memudahkan pengelolaan dan pemantauan.
- **Skalabilitas:** Cloud KMS dirancang untuk skalabilitas, memungkinkan Anda untuk mengelola ribuan kunci dengan efisien.
- **Integrasi GCP:** Cloud KMS terintegrasi dengan layanan GCP lainnya, memungkinkan Anda untuk melindungi data di seluruh infrastruktur cloud Anda.

Penggunaan Cloud KMS:

Anda dapat menggunakan Cloud KMS untuk mengenkripsi data pada saat istirahat, mengelola kunci yang digunakan untuk mengenkripsi dan mendekripsi data, serta memenuhi kebutuhan kepatuhan dan regulasi terkait keamanan data.

Tutorial Penggunaan Cloud KMS:

1. **Membuat Keyring dan Key:** Anda dapat membuat keyring untuk mengelompokkan kunci enkripsi Anda. Kemudian, Anda bisa membuat kunci di dalam keyring tersebut.
2. **Enkripsi dan Dekripsi Data:** Setelah memiliki kunci, Anda dapat menggunakan Cloud KMS untuk mengenkripsi dan mendekripsi data yang perlu dilindungi.
3. **Integrasi dengan Layanan GCP:** Anda dapat menggunakan kunci yang dikelola oleh Cloud KMS untuk melindungi data di layanan GCP seperti GCS, GCE, Cloud SQL, dan lainnya.
4. **Penggunaan dalam Aplikasi:** Anda dapat mengintegrasikan Cloud KMS dalam aplikasi Anda untuk melindungi data sensitif saat berada dalam proses penyimpanan dan pengambilan.

Perlu diingat bahwa Cloud KMS membantu dalam pengelolaan kunci enkripsi dan memastikan penggunaan yang aman dan efektif, tetapi juga penting untuk merancang kebijakan keamanan dan praktik keamanan yang tepat di seluruh solusi GCP Anda.

- **Identity-Aware Proxy (IAP):** IAP memungkinkan Anda mengontrol akses aplikasi GCP melalui HTTPs tanpa instalasi perangkat lunak VPN.

Identity-Aware Proxy (IAP) adalah layanan keamanan yang disediakan oleh Google Cloud Platform (GCP) yang memungkinkan Anda untuk mengamankan dan mengontrol akses ke aplikasi web yang di-host di lingkungan GCP. IAP memungkinkan Anda untuk mengamankan aplikasi web Anda dengan mengotentikasi pengguna dan mengotorisasi akses ke aplikasi tersebut berdasarkan identitas pengguna, bukan berdasarkan alamat IP.

Fitur Utama IAP:

1. **Access Control Berbasis Identitas:** IAP memungkinkan Anda untuk mengatur akses ke aplikasi web berdasarkan identitas pengguna yang diautentikasi. Hal ini memberikan tingkat keamanan yang lebih tinggi daripada mengandalkan alamat IP.
2. **Secure Remote Access:** Dengan IAP, Anda dapat memberikan akses aman ke aplikasi web yang di-host di GCP, bahkan jika aplikasi tersebut tidak dapat diakses secara publik melalui Internet.
3. **MFA dan Otorisasi:** IAP mendukung multi-factor authentication (MFA) dan pengaturan otorisasi yang tepat, memastikan hanya pengguna yang sah dan diotorisasi yang dapat mengakses aplikasi.

4. **Integrasi dengan Identity Providers:** IAP dapat diintegrasikan dengan berbagai penyedia identitas (identity providers) seperti Google Workspace (sebelumnya G Suite), Cloud Identity, dan penyedia identitas berbasis standar seperti OpenID Connect.

5. **Audit dan Logging:** IAP menyediakan audit trail untuk aktivitas akses pengguna ke aplikasi web, membantu dalam pemantauan dan pemahaman aktivitas yang terjadi terkait dengan akses.

Keuntungan Menggunakan IAP:

- **Akses Berbasis Identitas:** IAP memungkinkan Anda untuk memberikan akses ke aplikasi web berdasarkan identitas pengguna yang dikenali, meningkatkan tingkat keamanan.
- **Fleksibilitas Akses:** Anda dapat memberikan akses ke aplikasi web dari mana saja, bahkan jika akses langsung ke server dihindari.
- **Akses Aman untuk Remote Work:** IAP memungkinkan akses aman ke aplikasi web dari lokasi jarak jauh tanpa perlu terhubung ke jaringan perusahaan melalui VPN.

Penggunaan IAP:

Anda dapat menggunakan IAP untuk mengamankan akses ke aplikasi web Anda yang di-host di lingkungan GCP. Ini cocok untuk skenario seperti memberikan akses ke anggota tim yang berada di lokasi yang berbeda atau mengamankan akses ke aplikasi web internal yang di-host di GCP.

Tutorial Penggunaan IAP:

1. **Aktifkan IAP untuk Aplikasi Web:** Aktifkan IAP untuk aplikasi web Anda yang di-host di lingkungan GCP.

2. **Konfigurasi Identity Providers:** Pilih dan konfigurasi identity providers yang ingin Anda gunakan untuk mengotentikasi pengguna.

3. **Atur Otorisasi:** Tentukan peran dan izin yang diberikan kepada pengguna yang diotentikasi untuk mengakses aplikasi web.

4. **Lakukan Testing:** Lakukan uji coba untuk memastikan bahwa hanya pengguna yang sah dan diotorisasi yang dapat mengakses aplikasi web.

Perlu diingat bahwa penggunaan IAP tidak hanya melibatkan konfigurasi di GCP tetapi juga mungkin melibatkan konfigurasi di sisi aplikasi web Anda. Pastikan Anda mengikuti panduan resmi GCP dan dokumentasi aplikasi web Anda untuk mengimplementasikan IAP dengan benar.

- **Cloud Armor:** Cloud Armor melindungi infrastruktur Anda dari serangan DDoS.

Cloud Armor adalah layanan keamanan di Google Cloud Platform (GCP) yang menyediakan perlindungan lapisan aplikasi terhadap serangan siber yang

ditujukan ke aplikasi web Anda. Layanan ini dirancang untuk melindungi aplikasi Anda dari serangan DDoS (Distributed Denial of Service), serangan aplikasi, dan ancaman siber lainnya.

Fitur Utama Cloud Armor:

1. **Proteksi Terhadap DDoS:** Cloud Armor membantu melindungi aplikasi Anda dari serangan DDoS dengan menentukan aturan pemfilteran yang memungkinkan Anda mengidentifikasi lalu lintas yang mencurigakan dan memblokirnya sebelum mencapai aplikasi Anda.
2. **Pemfilteran Lalu Lintas:** Anda dapat mengonfigurasi aturan pemfilteran untuk mengizinkan atau memblokir lalu lintas berdasarkan alamat IP, negara, protokol, atau pola serangan tertentu.
3. **Pemeliharaan Akses yang Tepat:** Cloud Armor memungkinkan Anda untuk memastikan bahwa hanya lalu lintas yang sah yang dapat mencapai aplikasi Anda, sementara lalu lintas yang berpotensi berbahaya atau mencurigakan dapat diblokir.
4. **Integrasi dengan Google Cloud Load Balancing:** Cloud Armor terintegrasi dengan layanan Google Cloud Load Balancing, memungkinkan Anda untuk memproteksi aplikasi yang dijalankan di lingkungan global dan memanfaatkan keunggulan skala dan redudansi dari Google Cloud.
5. **Manajemen Aturan Pemfilteran:** Anda dapat mengelola aturan pemfilteran dengan mudah melalui konsol manajemen Google Cloud atau melalui API.

Keuntungan Menggunakan Cloud Armor:

- **Perlindungan DDoS:** Cloud Armor membantu melindungi aplikasi Anda dari serangan DDoS yang dapat mengganggu ketersediaan layanan.
- **Pemfilteran Lalu Lintas:** Anda dapat mengontrol dan memeriksa lalu lintas yang mencapai aplikasi Anda, memastikan bahwa hanya lalu lintas yang diizinkan yang diterima.
- **Adaptif dan Skalabilitas Tinggi:** Layanan ini dapat beradaptasi dengan pola serangan baru dan terus memantau lalu lintas aplikasi Anda.

Penggunaan Cloud Armor:

Anda dapat menggunakan Cloud Armor untuk melindungi aplikasi web Anda yang di-host di lingkungan Google Cloud. Ini cocok untuk skenario di mana Anda ingin melindungi aplikasi Anda dari serangan siber dan memastikan ketersediaan layanan yang tinggi.

Tutorial Menggunakan Cloud Armor:

1. **Aktifkan Cloud Armor:** Aktifkan layanan Cloud Armor melalui konsol manajemen Google Cloud.

2. **Definisikan Aturan Pemfilteran:** Tentukan aturan pemfilteran untuk memblokir atau mengizinkan lalu lintas berdasarkan kriteria seperti alamat IP, negara, atau pola serangan.
3. **Terapkan Aturan ke Load Balancer:** Terapkan aturan pemfilteran ke layanan Google Cloud Load Balancing yang digunakan untuk menjalankan aplikasi Anda.
4. **Uji Coba dan Monitor:** Lakukan uji coba dan monitor lalu lintas yang mencapai aplikasi Anda untuk memastikan bahwa aturan pemfilteran berjalan dengan benar.

Pastikan Anda mengacu pada panduan resmi GCP dan dokumentasi Cloud Armor untuk memastikan implementasi yang tepat dan efektif.

Link Cloud Armor: https://cloud.google.com/armor/docs/cloud-armor-overview

- **Cloud Data Loss Prevention:** Data Loss Prevention adalah layanan yang dirancang untuk membantu Anda menemukan, mengklasifikasikan, dan melindungi data sensitif.

Cloud Data Loss Prevention (DLP) adalah layanan yang sepenuhnya dikelola yang dirancang untuk membantu Anda menemukan, mengklasifikasikan, dan melindungi data sensitif, seperti:

1. **Personal Identifiable Information (PII):** Informasi pribadi yang dapat mengidentifikasi seseorang, seperti nama, nomor KTP, nomor SIM, nomor rekening bank, nomor paspor, alamat email, dan sebagainya.
2. **Secrets:** Informasi rahasia, seperti kata sandi, kunci API, dan kredensial akses.
3. **Credentials:** Informasi otentikasi, seperti token akses, sandi, dan kunci rahasia.

DLP terintegrasi dengan Google Cloud Storage (GCS), BigQuery, dan Datastore. Sumber data yang dianalisis oleh DLP tidak harus berasal dari lingkungan Google Cloud Platform (GCP), namun bisa juga dari sumber data eksternal.

Anda dapat menentukan jenis data yang ingin Anda deteksi, yang disebut sebagai “info type.” Anda bisa menggunakan jenis data bawaan, membuat jenis data sendiri berdasarkan kamus kata atau frasa, atau menggunakan ekspresi regex. DLP akan mengembalikan hasil deteksi bersama dengan tingkat kemungkinan data cocok dengan jenis info tertentu: LIKELIHOOD_UNSPECIFIED, VERY_UNLIKELY, UNLIKELY, POSSIBLE, LIKELY, VERY_LIKELY.

Setelah mendeteksi informasi PII atau data sensitif lainnya, DLP dapat mengubahnya agar tidak dapat dihubungkan kembali dengan pengguna. DLP menggunakan beberapa teknik untuk menghilangkan identifikasi data sensitif, seperti tokenisasi, pengelompokan, dan pergeseran tanggal. DLP juga dapat mendeteksi dan merahasiakan data sensitif dalam gambar.

Langkah-langkah Penggunaan Cloud DLP:

1. **Aktifkan Cloud DLP:** Aktifkan layanan Cloud DLP melalui konsol manajemen Google Cloud.
2. **Konfigurasi Info Types:** Tentukan jenis info yang ingin Anda deteksi, baik menggunakan jenis bawaan, jenis kustom, atau ekspresi regex.
3. **Pilih Sumber Data:** Tentukan sumber data yang akan dianalisis oleh DLP, seperti GCS atau BigQuery.
4. **Menggunakan Transformasi:** Opsional, Anda dapat mengonfigurasi transformasi untuk mengubah data sensitif menjadi data yang tidak dapat diidentifikasi kembali.
5. **Eksekusi Analisis:** Jalankan analisis DLP dan tinjau hasil deteksi serta transformasi (jika diterapkan).
6. **Aplikasikan Hasil:** Terapkan hasil analisis DLP, seperti menghapus atau mengenkripsi data sensitif.

Pastikan Anda mengacu pada panduan resmi GCP dan dokumentasi Cloud DLP untuk implementasi yang tepat dan pemahaman lebih lanjut tentang fitur-fitur yang ditawarkan oleh layanan ini.

Link DLP : https://cloud.google.com/dlp/docs/schedule-inspection-scan

- **VPC Service Control:** VPC Service Control membantu mencegah eksfiltrasi data dengan mendefinisikan batas di sekitar sumber daya yang ingin Anda lindungi.

VPC Service Controls adalah fitur di Google Cloud Platform (GCP) yang memungkinkan Anda untuk mengamankan sumber daya GCP Anda dengan lebih cermat di tingkat jaringan. Ini memberi Anda kontrol yang lebih besar atas bagaimana sumber daya Anda dapat berinteraksi di dalam atau di luar Virtual Private Cloud (VPC) Anda.

Dengan VPC Service Controls, Anda dapat membatasi akses sumber daya GCP Anda berdasarkan kondisi tertentu, seperti:

1. **Access Context Manager:** Anda dapat mengatur kebijakan akses berdasarkan atribut seperti zona jaringan, alamat IP, dan koneksi jaringan. Ini memungkinkan Anda untuk membatasi akses ke sumber daya hanya untuk jaringan atau wilayah tertentu.

2. **Perimeter:** Anda dapat membuat perimeter keamanan yang mengelilingi sumber daya Anda. Misalnya, Anda dapat membuat perimeter untuk proyek tertentu dan mengontrol bagaimana sumber daya dalam perimeter ini dapat berinteraksi dengan sumber daya di luar perimeter.

3. **Batasan Layanan:** Anda dapat menentukan layanan GCP mana yang dapat diakses oleh sumber daya dalam VPC tertentu. Anda dapat memutuskan apakah Anda ingin memungkinkan akses ke layanan tertentu atau melarangnya sepenuhnya.

Manfaat dari VPC Service Controls termasuk:

- **Peningkatan Keamanan:** Anda dapat menerapkan kontrol yang lebih ketat atas akses sumber daya Anda, mengurangi risiko akses yang tidak sah atau tidak diinginkan.
- **Pemisahan:** Anda dapat memisahkan sumber daya yang sensitif atau kritis dalam perimeter keamanan khusus, membatasi potensi serangan dan risiko bocor informasi.
- **Keamanan Berlapis:** Dengan kombinasi VPC Service Controls dan kontrol akses lainnya, Anda dapat membangun keamanan yang berlapis untuk lingkungan GCP Anda.

Penting untuk diingat bahwa konfigurasi VPC Service Controls mungkin mempengaruhi cara sumber daya Anda berinteraksi di lingkungan GCP Anda. Oleh karena itu, sebelum menerapkan VPC Service Controls, Anda harus memahami dampaknya terhadap aplikasi dan layanan Anda.

VPC Service Controls merupakan fitur lanjutan yang digunakan dalam skenario keamanan yang lebih kompleks. Pastikan Anda merujuk pada dokumentasi resmi GCP dan sumber daya lainnya untuk memastikan implementasi yang tepat dan pemahaman yang mendalam tentang fitur ini.

Link VPC Service Control : https://cloud.google.com/vpc-service-controls

- **Cloud Web Security Scanner:** Cloud Web Security Scanner memindai aplikasi yang berjalan di GCP untuk kerentanannya.

Cloud Web Security Scanner adalah layanan keamanan yang disediakan oleh Google Cloud Platform (GCP) yang dirancang untuk mendeteksi kerentanan dan risiko keamanan di situs web dan aplikasi web Anda. Layanan ini membantu mengidentifikasi potensi ancaman dan celah keamanan yang dapat dieksploitasi oleh penyerang.

Beberapa fitur dan kemampuan utama dari Cloud Web Security Scanner adalah:

1. **Automatisasi:** Layanan ini secara otomatis mengidentifikasi dan memindai kerentanan pada aplikasi web Anda. Ini menghemat waktu dan usaha dalam mengidentifikasi potensi risiko keamanan.
2. **Pendeteksian Kerentanan:** Cloud Web Security Scanner dapat mendeteksi berbagai jenis kerentanan umum, seperti kerentanan injeksi SQL, kerentanan lintas situs (XSS), dan kerentanan berbasis kueri yang lain.
3. **Skala Besar:** Layanan ini dapat mengatasi pemindaian di berbagai aplikasi dan situs web secara bersamaan, mengingat skala dan kompleksitas lingkungan yang berbeda.
4. **Laporan Detil:** Setelah pemindaian selesai, Anda akan menerima laporan detil tentang kerentanan yang ditemukan, termasuk informasi tentang jenis kerentanannya, lokasi di situs web, dan rekomendasi tindakan yang dapat diambil.

5. **Integrasi dengan Google Cloud Security Command Center:** Hasil pemindaian dapat diintegrasikan dengan Cloud Security Command Center untuk memberikan pandangan keseluruhan tentang keamanan lingkungan Anda.

6. **Pengaturan Pemindaian:** Anda dapat mengatur pemindaian sesuai dengan kebutuhan Anda, termasuk konfigurasi proxy dan memilih skop pemindaian.

Namun, penting untuk diingat bahwa Cloud Web Security Scanner hanya satu komponen dari strategi keamanan yang komprehensif. Meskipun dapat membantu mengidentifikasi kerentanan umum, tidak semua kerentanan dapat terdeteksi oleh alat otomatis. Oleh karena itu, perlu melengkapi pemindaian dengan pemeriksaan keamanan manual dan pengujian penetrasi secara periodik.

Sebelum menggunakan Cloud Web Security Scanner, disarankan untuk membaca dokumentasi resmi dan memahami cara mengkonfigurasi dan menganalisis hasil pemindaian dengan benar.

Link : https://cloud.google.com/security-command-center/docs/concepts-web-security-scanner-overview

CREDIT : - https://www.freecodecamp.org/news/google-cloud-platform-from-zero-to-hero/?utm_source=pocket_saves - Tambahan yang saya pelajari sendiri

NB Tutorial akan terus update