Google Cloud Architect Cheatsheet

Compiled by Aleksandra T. Sekalska

Last Updated December 18, 2019

GCP Cloud Architect

What is GCP Professional Cloud Architect Certificate

- Design and plan a cloud solution architecture
- Manage and provision the cloud solution infrastructure
- Design for secure and compliance
- Analyze and optimize technical and business processes
- Manage implementations of cloud architecture
- Ensure solution and operations reliability

Virtual Machines

Google Cloud VPC provides networking functionality to Compute Engine virtual machine instances, Google Kubernetes Engine containers, and the App Engine flexible environment.

Private Cloud Networks:

A Private Cloud Network is a virtual version of a physical network, such as a data center network. Projects can contain multiple VPC networks.

VPC networks, including their associated routes and firewall rules, are global resources. They are not associated with any particular region or zone.

Subnets are regional resources. Each subnet defines a range of IP addresses.

Virtual Machines (VM) running in Google's global data center. Ideal for when you need complete control over your infrastructure and direct access to high-performance hardward or need OS-level changes.

Google Cloud VPC networks are global; subnets are regional (coursera)

You control the topology of your VPC network:

- Use its route table to forward traffic within the network, even across subnets.
- Use its firewall to control what network traffic is allowed.
- You can use VPC Peering to interconnect different VPC across GCP.
-

Compute Engine:

It offers managed virtual machines. Pick memory and CPU: use predefined types, or make a custom VM; (coursera)

You can choose 2 of persistant storage: SD or standard. (coursera)

You can choose preemtible instances: high throughput to storage at no extra cost; no longer than 24 hours

Storage

Overview

Cloud Storage:

It is a binary large-object storage (coursera)

Always encrypt the data on the server side (coursera)

The files are organized into buckets: the buckets have globally unique name (coursera)

Choose among Cloud Storage classes:

- **Multi-regional**: Most frequenlty accessed
- **Regional**: Accessed frequently within a region
- **Nearline**: Accessed less than once a month
- **Coldline**: Accessed less than once a year

There are several ways to bring data to Cloud Storage:

- **Storage Transfer Service**: move data from other cloud providers or from an on-premise storage

;

- **Transfer Appliance**: securely migrate large data (¿ 10TB) using hardware appliance

Cloud BigTable:

Fully managed, scalable NoSQL DB for analytical workload. ms latency. Perfect for event data (OLAP): fintech, digital media, IoT.

Cloud SQL:

Fully managed relational database services for MySQL, PostgreSQL and SQL Server. Perfect for transactional workload (OLTP)

Cloud Spanner:

Fully managed relational database with strong consistency and horizontal scalability. Perfect for multi-regional transactions.

Cloud DataStore:

Highly scalable NoSQL database. Provides ACID transactions and SQL-like queries.

Cloud Memorystore:

Scalable, secure and highly available in-memory service for Redis and Memcached.

Containers

Overview

Containers:

Choosing an option to run containers

Kubernetes:

a service that manages containerized workloads and services.

Kubernetes Compute Engine:

Owner (full access to resources, manage roles), Editor (edit access to resources, change or add), Viewer (read access to resources)

Applications

GCP's monitoring, logging, and diagnostics solution. Provides insights to health, performance, and availability of applications.

Main Functions

App Engine:

fully managed serverless platform for highly scalable applications.

Cloud Endpoints:

Develop, deploy, protect, and monitor your APIs with Cloud Endpoints. An NGINX-based proxy and distributed architecture give unparalleled performance and scalability.

Apigee Sense:

Apigee Sense works with the Apigee Edge API management platform to protect APIs from attacks. It identifies and alerts administrators to suspicious API behaviors.

Developing, Deploying and Monitoring????

Overview

Cloud Source Repositories:

Design, develop, and securely manage your code. Collaborate easily on a fully featured, scalable, and private Git repository. Extend your Git workflow by connecting to other Google Cloud tools, including Cloud Build, App Engine, Pub/Sub, and operations products such as Cloud Monitoring and Cloud Logging.

Cloud Functions:

allows you to trigger your code from Google Cloud, Firebase, and Google Assistant, or call it directly from any web, mobile, or backend application via HTTP. It supports Node.js, Python, Go, Java and .NET. You are only billed for your function's execution time, metered to the nearest 100 milliseconds.

Compute Choices

Overview

Cloud Dataflow:

BigQuery:

Cloud Pub/Sub:

Cloud Datalab:

GCP Machine Learning Services:

GCP IAM Part I

Cloud Identity and Access Management (IAM) lets administrators authorize who can take action on specific resources, giving you full control and visibility to manage cloud resources centrally. For established enterprises with complex organizational structures, hundreds of workgroups, and potentially many more projects, Cloud IAM provides a unified view into security policy across your entire organization, with built-in auditing to ease compliance processes.

It is the process of determining who can do what on which resource.

With Cloud IAM you manage access control by defining who (identity) has what access (role) for which resource. In Cloud IAM, permission to access a resource isn't granted directly to the end user. Permissions are grouped into roles, and roles are granted to authenticated members. A Cloud IAM policy defines and enforces what roles are granted to which members and this policy is attached to a resource.

All the components are resources:

organizations, projects, folders, services. Those resources are organized hierarchically:

The organization is the root node in the hierarchy. Folders are children of the organization. Projects are children of the organization, or of a folder. Resources for each service are descendants of projects.

GCP IAM Part II

Roles:

A collection of permissions.

Permissions determine what specific operations are allowed on resource. When you grant a role to a member, you grant all the permissions that the role contains.

Permissions are not directly assigned to a Member. Permissions are assigned to a Role and that role is assigned to Members.

- **Primitive Roles:** These roles are **Owner**, **Editor** and **Viewer**. Avoid using these roles if possible, because they include a wide range of permissions accross all Google Cloud services.
- **Predefined Roles:** Roles that give finer-grained access control than the primitive roles. ???
- **Custom Roles:** Roles that you create to tailor permissions to the needs of your organization when predefined roles don't meet your needs.

Members:

A member can be a person, a service account, a Google Group, or a G Suite or Cloud Identity domain. It is represented by an email address.

Service Accounts:

It is represented by an email address and it is associated with an application or a server, not a person. Applications use service accounts to make authorized API calls.

Policy:

The Cloud IAM policy binds one or more members to a role. When you want to define who has what type of access on a resource, you create a policy and attach it to the resource.

More info here.

Cloud Stackdriver

Aggregates metrics, logs and events for monitoring, logging and tracking diagnostics.

Stackdriver Logging:

Allows you to store, search, analyze, monitor, and alert on log data and events from GCP and AWS.

Stackdriver Monitoring:

Provides visibility into the performance, uptime and overall health of cloud-powered applications. It collects metrics, events, and metadata from different services.

Stackdriver ingests data and generates dashboards, charts, and alerts.

Stackdriver Error Reporting:

Counts, analyzes, and aggregates the crashed running cloud services.

Stackdriver Trace:

A distributed tracing system for GCP that collects latency data from App Engine applications and displays it in near real time.

Stackdriver Debugger:

Lets you inspect the state of an application, at any code location, without stopping or slowing down the running app.

Stackdriver Profiler:

A statistical profiler. It does not require pervasive changes to the program code to collect data. Instead, a piece of code, called profiling agent, is essentially attached to the code, where it can periodically look at the call stack of the program to collect information about, for example, CPU or memory usage.

Interconnecting Networking

Overview

Cloud VPN:

Some text to be introduced

Cloud Interconnect:

Some text to be introduced

Cloud Peering:

Some text to be introduced

Shared VPC and VPC Peering:

Some text to be introduced

Load Balancing and Autoscaling

Choosing a Load Balancer

HTTP(S) Load Balancing:
Some text to be introduced

SSL Proxy Load Balancing:
Some text to be introduced

TCP Proxy Load Balancing:
Some text to be introduced

Network Load Balancing:
Some text to be introduced

Internal Load Balancing:
Some text to be introduced

Intro

- **TCP/UDP Load Balancing:** Tables partitioned based on the data's ingestion (load) date or arrival date. Each partitioned table will have pseudocolumn _PARTITIONTIME, or time data was loaded into table. Pseudocolumns are reserved for the table and cannot be used by the user.
- **Internal HTTP(s) Load Balancing:** Tables that are partitioned based on a TIMESTAMP or DATE column.

Infrastructure Automation

Deployment Manager:
Some text to be introduced

Explore best practices:

GCP Marketplace: Some text to be introduced

Managed Services

BigQuery:
Some text to be introduced

Cloud Dataflow:
Some text to be introduced

Cloud Dataprep:
Some text to be introduced

Cloud Dataproc:
Some text to be introduced

Case Studies

Overview **Mountkirk Games:**

Dress4Win:

TerramEarth: