Google Cloud Platform

From Zero to Hero – The Complete Guide

Architecture Summary

When designing cloud architectures for Google Cloud Platform, this summary will help you select the right resources for the right task.

Area	Resources / Notes
Compute	Virtual Machines (VMs) – When a full control is needed, or dev platform is not supported on any other cloud service (e.g. C++). Can be auto scaled using Managed Instance Group. App Engine – PaaS for web apps. Use when system is a web app running on modern platform. Not requiring any setup or configuration. If running a container-based solution, prefer Cloud Run or GKE. Cloud Run – Fully managed container runtime. Upload and manage your container images with autoscaling capabilities. Can be deployed directly from code or using Artifact Registry.

<table>
<tr><td></td><td>Google Kubernetes Engine (GKE) – Use for microservices-based systems that use Docker containers. Fully managed Kubernetes engine. Go for the Autopilot mode when possible.
Cloud Functions – Use for focused, lightweight actions (calculations, conversions, validation etc.). Extremely efficient, beware of cold starts.</td></tr>
<tr><td>Networking</td><td>VPC – Virtual Network. Global. By default a single VPC is created per project. Design your app around VPCs using the Hob-and-Spoke model.
Subnet – Logical, regional segment inside a VPC. By default accessible from other subnets in the VPC.
Firewall rules – Filters traffic based on 5 tuples. ALWAYS make use of firewall rules to allow the minimum traffic into the VPC.
Load Balancers:
<table>
<tr><th>Type</th><th>Deployment Mode</th><th>Use For…</th></tr>
<tr><td>Application Load Balancer (HTTP/S)</td><td>Global external</td><td>Public global websites distributed in multiple regions</td></tr>
<tr><td></td><td>Regional external</td><td>Public global websites distributed in a single region</td></tr>
<tr><td></td><td>Regional internal</td><td>Intra-backend communication distributed in a single region</td></tr>
<tr><td></td><td>Cross-region internal</td><td>Intra-backend communication distributed in multiple regions</td></tr>
</table></td></tr>
</table>

	Proxy Network Load Balancer (TCP)	Global external	Public TCP listener distributed in multiple regions
		Regional external	Public TCP listener distributed in a single region
		Internal	Internal TCP listener
	Passthrough Network Load Balancer (TCP, UDP, ICMP…)	External	Public network listener
		Internal	Internal network listener

Data

Service	Data type	Use for…	Cost
Cloud SQL	Relational (SQL)	Relational, transactional data	$
Spanner	Relational (SQL)	Relational, transactional data, requires distribution	$$$
AlloyDB	Relational (SQL)	Relational, transactional data, high performance, PostgreSQL compatibility	$$
BigTable	NoSQL, columnar	NoSQL data with schema, high volume	$$$
BigQuery	NoSQL	Analytics	$$
Firestore	NoSQL, document	Backend for mobile and web apps, offline and sync support required	$
Memorystore	NoSQL	Fast, distributed cache	$$
Cloud Storage	NoSQL, unstructured	Unstructured data such as files, docs etc.	$

Messaging	**Pub/Sub** • Use when you need full control on events and publish or receive using code **Eventarc** • Use when utilizing built-in events and can use a built-in integration (ie. trigger a Cloud Function)
Authentication	Cloud IAM – Identity and Access Manager (IAM) for cloud resources. Identity Platform – Client IAM, add identity management to your apps, wherever they're hosted.
Monitoring	Set up Alerts to get notifications when something goes wrong Use Metrics to see system's status Read Logs to find out what the system did Put important information on Dashboards to get wholistic view Use Tags and Labels to categorize the resources
Security	- Close unnecessary open ports of a VM - Use Firewall rules - Use authentication - Encrypt data at rest and at transit - Use Secret Management to securely store secrets

DR	- Decide between hot and cold DR - Remember – hot DR is much more difficult to design and expensive to implement - Decide on target RPO and RTO - Use Global External Load Balancer for automatic routing

I Hope you enjoyed the course, and that it made you a Google Cloud expert. Stay tuned to more courses on Google Cloud, which will make you an even better Google Cloud Architect!

For any question or comment contact me at:

memi@memilavi.com

Thanks,

Memi