GCP Associate Cloud Engineer Deep Dive notes. Preparing for the exam

Joseph Holbrook
Sep 27 · 13 min read ★

GCP Associate Cloud Engineer Deep Dive notes. Preparing for the exam

The entry way to Google Cloud Certification.

The Cloud Engineer exam from Google is one of the more interesting certifications for technically focused engineers. If you like command lines such as gcloud and bq you will do great.

This exam is very different than the cloud architect exam. No case studies just Command Line such as gcloud and kubernetes, services understanding and cloud best

practices.

For the GCP Cloud Engineer Exam its very important to distinguish what type of compute options should be deployed . A good focus of the exam is to be able to specify: Compute Engine, App Engine, Cloud Functions or Kubernetes Engine as well. Data services are tested as well such how to migrate to Bigtable or import to Cloud Storage.

gcloud commands are part of the objectives and of course were on the exam in several areas such as projects, kubernetes engine and gsutil

GCLOUD COMMANDS

-List Projects

gcloud projects list

-Set Your Default Project In GCP

gcloud config set project myProject

-Set Your Default Region

gcloud config set compute/region "europe-west1"

-List Compute Regions

gcloud compute zones list

-Set Cloud Functions Default region

to use when working with Cloud Functions resources.

gcloud alpha functions regions list

-Describe List Compute Zones

gcloud compute zones list

-Print List All the URI in a zone

gcloud compute zones list -uri

-List DNS info in Project

gcloud dns project-info describe

Describe a Project

gcloud compute project-info describe -project

Hierarchy

Knowing the GCP hierarchy is important. Organization may be a focus but also where Folders fit in. Know the use cases for each and how they solve customer issues.

*Understand the gcloud command line for changing the following * *Regions/zones *Default project *Create project

To set the project property in the core section, run:

$ gcloud config set project myProject *
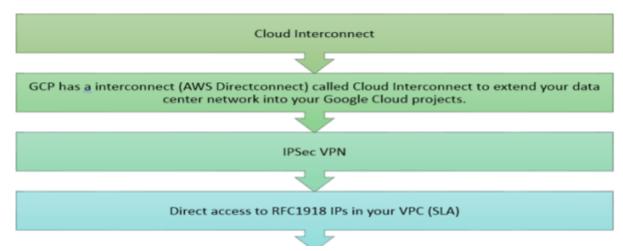
To set the zone property in the compute section, run:

$ gcloud config set compute/zone asia-east1-b

Hybrid Connectivity

Hybrid connectivity knowledge around when to use Cloud Interconnect, Peering or Cloud VPN. Straight forward.

Cloud VPN is a managed service. -Its is a gateway to gateway service. -Use case is for secure connection over the internet.

Cloud Interconnect is a private provisioned low latency connection to a Google Edge. Partner Interconnect is similar and may provide better costing if Cloud Interconnect not available in your region.

Partner Interconnect

VM Protocols VM Networking Protocols

Supported Protocols *TCP *UDP *ICMP

Every VM Instances belongs to a network.

Default network is used if none selected…

You can optionally assign a secondary IP range to the subnet for use with Alias IP. The secondary IP range also cannot overlap the IP ranges of existing connected subnets

VM Discounts

Inferred instances- for billing purposes, the same type of machine used in the same zone will be combined into a single charge (Increase your discounts) *Google does discounts their resources

Billed for minimum of **1 minute** and thereafter **every second**, Lower price for a PREMPTIVE instances.. Custom-type is discounted on a percent of total use

Below is a chart that compares AWS to GCP discounts.

	AWS	GCP
Per Second	Yes	Yes
Discounts (Instances)	Spot (Regular/Block)	Preemptable (24 hrs)
Discounts	Reserved	Committed Use
Savings	Prepay and discount	Up to 80% and no Prepaid contract

VM Features

Auto restart refers to what behavior the VM should take after a hardware failure or a system event. *If marked auto restart, the system will try to launch a replacement VM. *Auto restart does not restart the VM if it was terminated due to a user event, such as shutting down and terminating the VM.

NOTE: If the VM availability policy is set to the default, live migrate, during regular system maintenance your VM will be migrated to different hardware so there is no downtime

Bastion Hosts and NAT

Bastion Hosts *Know the use case for a bastion host. *Generally think of using a "bastion"host for "ingress "traffic and NAT for traffic "egress"

You may also want to know the commonly used ports for RDP and SSH *3389 and 22 *

Command line for connecting to a Compute Engine Instance is

gcloud compute ssh (instance name) **Instance Groups**

A managed instance group use for the following

*Autoscaling

*Load balancing

*Updates

There are two Types of Managed Instance Groups.

*Zonal Managed Instance Group

*Regional Managed Instance Group *(Recommended)*

Networking

Subnets are ways to group similar or related resources *If you have a VPN this allows you to target the VPN tunnels To a specific region for better control and performance.

*Benefit where you don't need to know much networking nor layout a network right away. *Define IP ranges in two ways.

- -Auto — -Custom

FREE GCP Practice Exams…

https://myblockchainexperts.org/gcpfreepracticequestions/

Firewalls

Firewalls (TAGS)

*Tags are needed to know for exam *Used to identify routes and firewall rules for VMS.

*Tags are user defined

*Not limited to topology like an IP address.

*64 tags to an instance

A list of instance tags indicating the set of instances on the network which may accept inbound connections that match the firewall rule.

If both target tags and target service account are omitted, all instances on the network can receive inbound connections that match the rule.

gcloud compute instances add-tags Instance1 -tag1 tag2

https://cloud.google.com/vpc/docs/add-remove-network-tags

Firewalls as a VPC Resource

VPC networks has two implied firewall rules. Note that these "implied" rules CAN NOT be removed..

* **implied allow egress rule (65535 Priority)**

* **implied deny ingress rule (65535 Priority)**

https://cloud.google.com/vpc/docs/firewalls

Firewall rules **cannot** be used to un-block traffic that is always blocked.

Rules are evaluated for priority. 0–65535 Default is 1000

DevOps Services

There was a good amount of Kubernetes questions for sure and perhaps the algo popped with a bunch of special questions right off the bat just for me.

- Taking the exam you must have a concise background for Kubenetes Engine (kubectl/gcloud cli commands)

- You must know what the Error Codes 400/403 are in several contexts.

- Know the complementary services around containers and Kube but also how to monitor containers. The easiest way to install Stackdriver monitoring is let it happen at deployment..

Complementary services for Kubernetes/DevOps are…….

Service	Why Use
Google Container Registry	Easy to store and access your private Docker images in GCP. Push and Pull images.
Google Cloud Build	Deploy your containers on Kubernetes Engine without needing to setup authentication.
Google Source Repositories	A single place for your team to store, manage, and track code. Private Github

Kubernetes Engine Container Services Complimentary Services

Compute Services

Know your use cases for data services. Connecting to Services(Cloud Storage, App Engine, Kubernetes Engine, Cloud Pub/Sub, Cloud Dataflow and Cloud Endpoints).

gcloud app deploy app.yaml -v a

What Compute service do you choose. But also containers can be deployed on App Engine in the Flex environment.

	Kubenetes Engine	App Engine Std	App Engine Flex
Language	Any	Java, Python, Go, PHP, Node.js	Any
Service Model	Hybrid	PaaS	PaaS
Use Case	Containers	Web & Mobile	Web and Mobile container based.

So What do I choose. App Engine or Kubenetes Engine?

Kubernetes

If your running a single-node database on GKE you Need = Persistent Volumes and Persistent Volume Claims.

You want to understand how to scale Kubernetes engine *You want to scale you Kubenetes cluster and what gcloud command do you use?

gcloud container clusters resize "Number of nodes"

More Kubernetes commands to learn

gcloud config set container/cluster [CLUSTER_NAME]
gcloud container clusters get-credentials [CLUSTER_NAME]

Learn more about containers here on Linux Foundation

http://shrsl.com/1uc6c

Heres a question…..What will happen if a running GKE pod encounters a fatal error? Answer.. GKE tries to ensure that the number of pods you've specified in your deployment are always running, so it will restart one if it fails.

Stackdriver is the default logging solution for clusters deployed on Google Kubernetes Engine. Stackdriver Logging is deployed to a new cluster by default unless you explicitly opt-out

Ensure you can create a Kubernetes Cluster and configure it to host an application. Lastly, understand how to make the cluster auto repairable and upgradable with Node auto-upgrades and auto-repairing feature

DataProc or Dataflow?

*Know that you can use DataProc for batch data? *Apache Spark and Hadoop on exam,,, This is likely the answer* * Don't confuse DataProc and DataFlow. *Cloud Dataflow is for newly-built processing that can take advantage of Apache Beam

Structured or Unstructured Data services choices?

We need to services such as Cloud Storage, BigTable, BigQuery, etc. heres a thought..

Choosing Storage *_____is made for large analytical workloads. * *With Cloud Storage is for _____ storage. * * *Bigtable / Object

Structured Data Services	Unstructured Data Services
Cloud SQL	Cloud Storage (Blob)
Cloud BigTable	Cloud Filestore (NAS)
Cloud BigQuery (Warehouse)	
Cloud Datastore	
Cloud Spanner	

Cloud Storage

Data cannot be moved from Multi-Regional to Regional through Lifecycle Management

Data can be moved from Nearline to Coldline for example

*30days or less- keep on Multi-regional or regional.

*30 -90 days = Nearline

*90 or more days = Coldline

What? Signed URL to give temporary access and the users do not need to be GCP users
. Note that changes are in accordance to object creation date for life cycle management.
* Review IAM vs ACLs on buckets

Cloud Storage Transfer Service

* **GCP to GCP Bucket**

* **AWS S3 bucket to GCP Bucket**

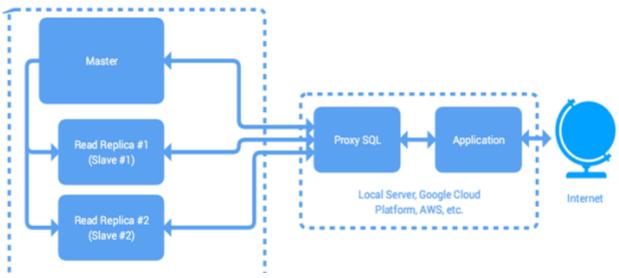* **On Prem Url List to GCP Bucket**

Cloud SQL

Understand that Cloud SQL scales **Regionally not Globally.**

Note to self…….Specify Cloud Spanner over Cloud SQL if there is a Cross Regional
requirement. Horizontal vs Vertical Scaling

Cloud SQL Proxy provides secure access to your Cloud SQL Second Generation
instances without having to: 1.Whitelisting 2.Configure SSL

Cloud SQL Proxy works by having a local client, called the proxy, running in the local
environment.

Google
Cloud SQL

Cloud SQL VS Cloud Spanner

Globally distributed and can scale and handle more than 10TB. *Not a direct replacement and would need migration

Regional(Vertical) vs Global (Horizontal) *CloudSQL is fully relational database for supporting customized table views, stored procedures, tons of indexes and ACID compliance. It supports MySQL and PostGreSQL (Vertical)

*Cloud Spanner is the first and only Global Scale relational database service that is both strongly consistent and horizontally scalable. *Cloud Spanner is a tool really for scaling globally (Horizontally). *Cloud SQL is your standard SQL databases and scales like. You can select machine type, hard disk type and size, region and zone.

Data Service Summary

*Cloud Storage as the medium to store data as data lake

*Cloud Pub/Sub as the messaging service to capture real time data esp.IoT *Cloud Pub/Sub is designed to provide reliable, many-to-many, asynchronous messaging between applications esp. real time IoT data capture

*Cloud Dataflow to process, transform, transfer data and the key service to integrate store and analytics.

*Cloud BigQuery for storage and analytics. Remember BigQuery provides the same cost-effective option for storage as Cloud Storage

*Cloud Dataprep to clean and prepare data. It can be used anomaly detection.

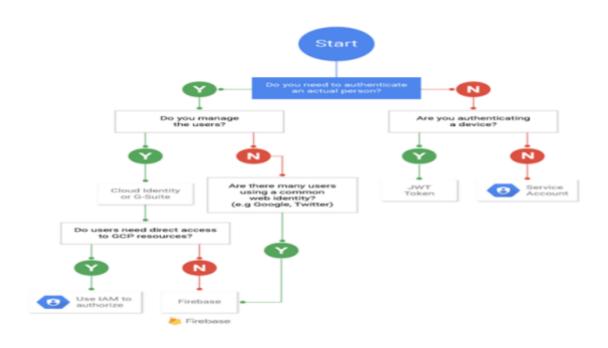*Cloud Dataproc to handle existing Hadoop/Spark jobs. Use it to replace existing Hadoop infra.

*Cloud Datalab is an interactive tool for exploration, transformation, analysis and visualization of your data on Google Cloud Platform

Cloud IAM

- IAM Permissions basics. Know what service accounts are, know how to setup up audit logs for auditors and logging best practices. Customize Permissions for Hybrid cloud applications. Use service for secure authentication and not API keys

- Org Nodes, Projects, folders and the hierarchy in GCP. GCDS is nice to know around use cases with orgs.

Identity and Access Management (IAM)

Cloud IAM, you grant access to members. Members can be of following types:

Google account

Service account

Google group

G Suite domain

Cloud Identity domain

Understand the options for authentication This IAM Decision tree is worth its weight in gold.

What about the auditors?

We need to understand how auditors can access compliance required data and how we as a cloud engineer can provide access. Remember Google uses the least privalege approach.

If you just want to give a user the ability to connect to a virtual machine instance using SSH, but don't want to grant them the ability to manage Compute Engine resources, add the user's public key to the project, or add a user's public key to a specific instance. You can avoid adding a user as a project member, while still granting them access to specific instances.

https://cloud.google.com/compute/docs/access/

Command to copy roles to different projects or organization.

OS Login simplifies SSH access management by linking your Linux user account to your Google identity. Use OS Login to manage SSH access to your instances using IAM without having to create and manage individual SSH keys. OS Login maintains a consistent Linux user identity across VM instances and is the recommended way to manage many users across multiple instances or projects.

gcloud iam roles copy

Roles and Permissions

Roles to understand for exam

*Cloud Storage — Admin vs Creator vs Viewer

*Compute Engine — Admin vs Instance Admin

*Spanner — Viewer vs Database User

*BigQuery — User vs JobUser

*App Engine — Viewer vs Deployer

Develop a Service account key-management strategy for migrating user profiles. (Key Management)

Auditors — Export audit logs to GCS bucket and set IAM policy

*Cloud Identity- IDaaS

Understand the difference between Primitive, Pre-defined and Custom roles and their use cases

Project Roles to give to Auditors such as Org viewer, project viewer

Auditors are referenced on almost all GCP exams. *Googles best practice is to create a group and then a role.*
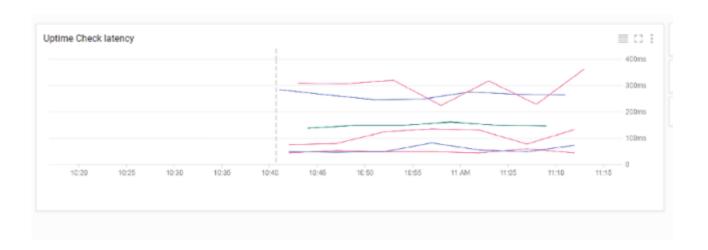
"We recommend collecting users with the same responsibilities into groups and assigning Cloud IAM roles to the groups rather than to individual users." Create a ROLE for Auditors after you create a group and they will inherit the defined permissions. You can create and manage groups through the Admin Console.

Stackdriver

Do not even take the exam if your not confident in Stackdriver logging setup, setup alerts and you can spell out the difference between Stackdriver modules, workflows and to note that Debug and Trace were on the objectives.

How do you install Stackdriver agents?

Command Line for any GCP Exam

- Command Line questions around installing agents were on the exam outline.
- Command for installing the monitoring agent
- curl -sSO https://dl.google.com/cloudagents/install-monitoring-agent.sh
- Command for installing the logging agent
- curl -sSO https://dl.google.com/cloudagents/install-logging-agent.sh

Know how to setup an Uptime Check in Stackdriver Monitoring *Feature to enable filters of aggregated logs down (Logging)

Debug one piece of the application across many hosts(Debug) *Understand API requests to microservices-based applications (Trace)

Know Stackdriver Monitoring default retention policy and how to export/analyze for legal purposes. (7/30/BigQuery)

Use Stackdriver Logging and setup triggers to alert for events

PCI Compliance — Enable Logging export to Google BigQuery,ACLs, views to scope the data shared with the auditor

Deployment Manager

The Deployment Manager service previews the configuration by expanding the full configuration, including any templates and the creating a deployment and "shell" resources.

- Deployment Manager Objectives are lightly covered.

Automation of Provisioning

Read YAML

Preview Feature

Know how to dry run the deployments. "preview feature" gcloud command

gcloud deployment-manager deployments create example-deployment -config configuration-file.yaml \ — preview
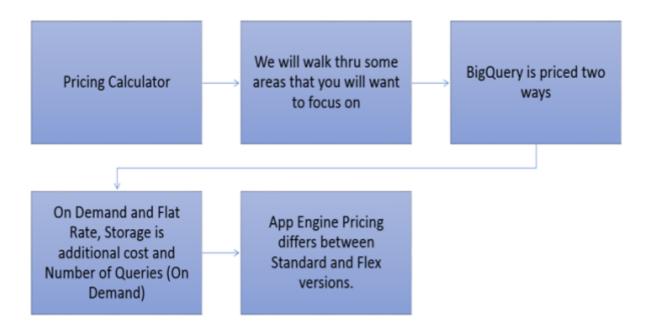
Cloud Marketplace

It can help minimize deployment time and can be used without any knowledge about the product *Provides a way to launch common software packages in a pre packaged stack.

Billing *Monthly vs Threshold and which has priority?*

Change a billing account for a project and what roles you need. Project Owner and Billing Administrator for the billing account. Billing is an area that could be on your exam so review these focus areas.

Pricing/Cost Estimating

Estimating the cost of certain services is part of the exam. You should go to the pricing calculator and understand how to estimate BigQuery, Cloud Storage and other services.

Pricing Calculator is here. https://cloud.google.com/products/calculator/

Google Cloud Best Practices

A reccuring them on any GCP exam seems to be about best practices. Another way on the exams they are phrased are "Recommended best practices, Enterprise Best Practices are linked below.

Trust me there will be exam content indirectly from this page around best practices.

Best practices for enterprise organizations | Documentation | Google Cloud

This guide introduces best practices to help enterprise customers like you on your journey to...

cloud.google.com

Resources to help Study. Resources to use for studying for GCP Cloud Engineer Updated 09/15/2019

https://cloud.google.com/certification/practice- exam/cloud-engineer

https://cloud.google.com/certification/cloud-engineer

https://landing.google.com/sre/book/index.html (Ebook)

https://www.safaribooksonline.com/library/view/the-site-reliability/9781492029496/

(Ebook)

https://amzn.to/2JDDJ6p (Amazon)

https://cloud.google.com/icons/ https://cloud.google.com/free/docs/map-aws-google-cloud-platform

Classes on Pearson Safari

Google Cloud Certified Associate Cloud Engineer Crash Course

This training is focused on preparing IT professionals in GCP who want to achieve their...

learning.oreilly.com

Getting Started with Google Cloud Platform LiveLessons
https://www.safaribooksonline.com/videos/getting-started-with/9780135181522

Classes on Pearson Safari

https://www.safaribooksonline.com/live-training/courses/google-cloud-platform-gcp-for-aws-professionals/0636920223047/ **New.**

Google Cloud Certified Associate Cloud Engineer Video
https://learning.oreilly.com/videos/google-cloud-certified/9780135768082

My Youtube has GCP Videos for Certification

https://www.youtube.com/channel/UCLcRBsiL_BIgDdn7P6uZbnQ

Medium Post Summing up the GCP Associate Cloud Engineer Exam (updated 02/2019) https://medium.com/faun/summing-up-the-gcp-associate-cloud-engineer-exam-updated-09-2018-96fc719a5855

Exam Objective links **Compute Engine App Engine Container Engine Storage Decisions Cloud Storage Spanner Cloud SQL Bigtable Datastore Storage Transfer Service Networking Stackdriver Logging Stackdriver Monitoring Stackdriver Error Reporting Stackdriver Trace Stackdriver Debugger Endpoints Security Scanner Identity and Security Identity-Aware Proxy KMS Resource Management Infrastructure as Code Cloud Pub/Sub Cloud Development Tools** https://cloud.google.com/tools/docs/ **DataProc DataFlow** AWS Cloud SecurityCloud Computing

AWS Security Best Practices and Resources to utilize.

CryptocurrencyFacebook LibraGoogle Cloud Platform

Facebook Libra Basics for Techies

Google Cloud Architect Exam Review.