Associate Cloud Engineer

Favorite	☐
Archived	☐
Fleeting	☐
Area/Resource	
Project	
Type	
Review Date	
Image	
URL	
Created	@January 30, 2023 10:48 AM
Updated	@February 1, 2023 6:15 PM
Root Area	
Project Area	
Updated (short)	02/01/2023
Pulls	
Resource Pulls	
Project Archived	
URL Base	
Recipe Divider	🥗🥗🥗 RECIPE BOOK PROPERTIES 🥗🥗🥗
Recipe Tags	
Book Divider	📚📚📚 BOOK TRACKER PROPERTIES 📚📚📚
Author	
Date Started	
Date Finished	
Book Status	

📚 Rating	

> 💡 Cloud engineers are proficient in four things. Setting up cloud environments and deploying applications, configuring security access, and creating and maintaining enterprise solutions.

- You can get to this point by getting hands-on experience in these areas

Exam guide

Section 1. Setting up a cloud solution environment

- Setting up cloud projects and accounts. Activities include:
  - Creating a resource hierarchy
  - Applying organizational policies to the resource hierarchy
  - Granting members IAM roles within the project

    - Managing users and groups in Cloud Identity
    - Enabling APIs within projects
    - Provision and setting up products in Google Cloud’s operations suite
- Managing billing configuration. Activities include:
    - Creating one or more billing accounts
    - Linking projects to a billing account
    - Establishing billing budgets and alerts
    - Setting up billing exports
- Installing and configuring the command line interface, and the cloud SDK

Section 2. Planning and configuring a cloud solution

- Planning and estimating google cloud product use using the Pricing calculator
- Planning and configuring networking resources

Section 3. Deploying and implementing a cloud solution

Section 4. Ensuring successful operation of a cloud solution

- Managing compute engine resources
- Managing google k8s engine resources
- Manage cloud run
- Managing networking resources

Section 5. Configure access and security

Key takeaways

1. Set up a cloud solution environment
2. Must know how to plan, configure, deploy and implement a cloud solution
3. Understand how to ensure a successful operation of a cloud solution
4. Understand how to configure access and security

Introduction to Google Cloud

Understanding google cloud

> 💡 Provides Iaas, Saas, and Faas environments for users of the platform. Designed for services built around building and maintaining applications.

- Infrastructure as a service
- Software as a service
- Functions as a service

Google Cloud Design and Structure

3 Pillar GCP Design

1. Trust and Security
2. Open Cloud
3. Analytics and Artificial Intelligence

> 💡 Powered everything here are data centers that are located across the globe. They also connect with eachother in the same zones for low latency. Google Cloud is a global fiber network. Data centers are built and upgraded for high availability.

Networking Basics of Google Cloud

3 Layers of Networking

- VPC: Virtual Private Cloud. A virtual version of a physical network that houses your resources.
    - PC that houses the network card, and computing power
- Subnets: Allows you to group those resources in your networking using private IP addresses
- Routers: Allows traffic to be routed to your resources within your network and subnets.

Networking explained

💡 Networking is a relatively complex topic in computer science however in the context of Google Cloud it can be explained through a series of analogies.

✏️ Networking is the practice of connecting and exchanging information between devices and computers, typically over the internet.
It refers to the infrastructure and systems that enable communication and data exchange between different devices, both within a single organization and across the internet. It can be thought of as a post office which allows you to send and receive mail (information) between different locations (devices). Just how a post office has rules and processes for sorting and delivering mail, a network has protocols and technologies for transmitting data and ensuring it reaches it's destination. Networking can involve complex infrastructure that are designed to manage traffic, ensure security and support various applications and services.

VPC

✏️ A virtual private cloud can be thought of as a private neighborhood for your resources in the cloud. It is a secure area within the cloud where you can put your resources. Within a VPC you can decide which resources to talk to each other and which ones can talk to the outside world. You can choose the resource IP addresses and control access to them with firewalls. You would create a VPC to have a secure, isolated network environment for your resources in the cloud where you can control access to them, and customize your network configuration to meet your needs.

Subnets

✏️ A subnet is a smaller part of a large networking. It can be thought of, as a house within this neighborhood. Where services are logically grouped together in a smaller part of the larger network. This allows you to further organize and segment your networking into smaller, more manageable parts. The advantages of subnets is primarily regarding granular access to resources, through IP address management, network traffic control and resource organization. A subnet can have it's own firewall rules.

💡 In the example of a stock market app, you might choose to divide the resources into different subnets based on the function of each resource and the security requirements of the application. A web server subnet will contain resources relating to the front end users of the application to users. It would allow incoming traffic from HTTP and HTTPS ports. A database subnet, would contain database resources which store information and stock market data. Firewall rules in this subnet would allow access from the backend application server subnet. **The idea is logically grouping resources based on their networking needs and security.**

Firewall

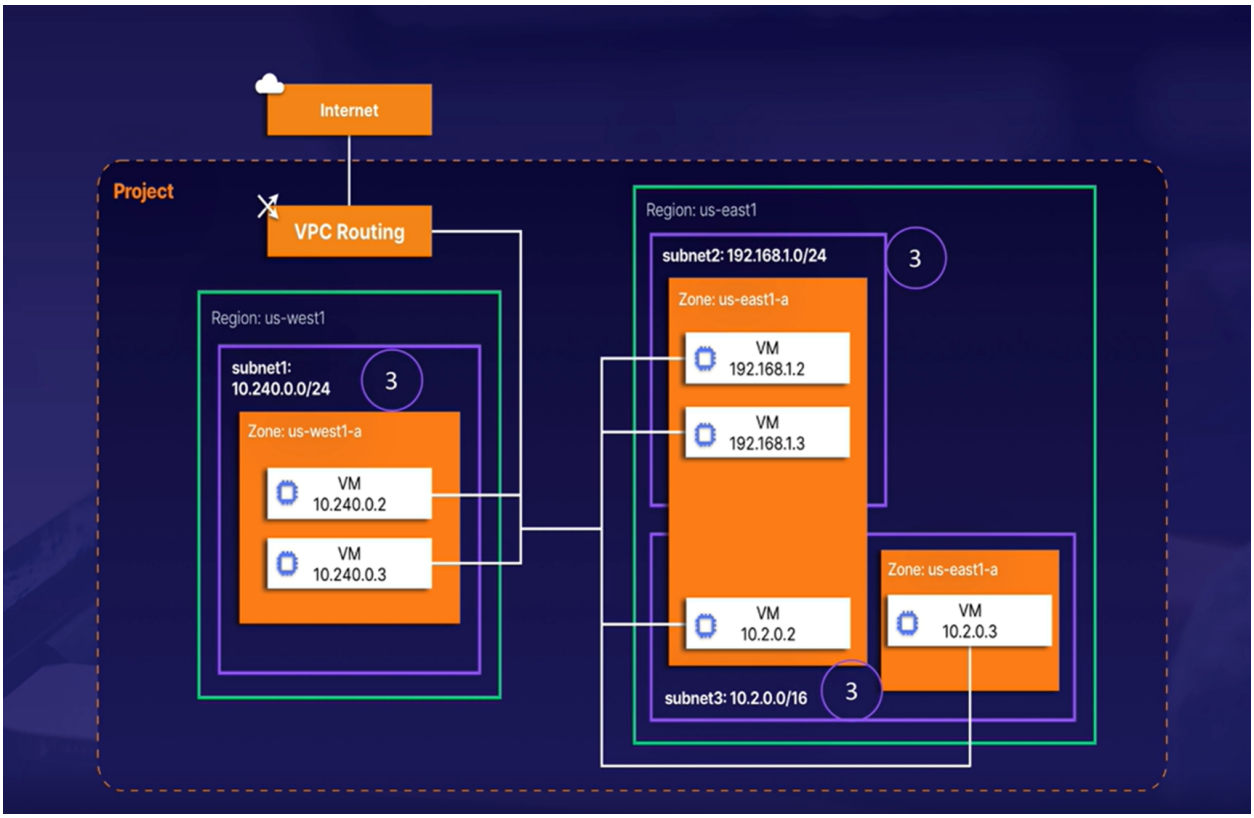
✏️ The firewall can be thought of as a bouncer. There can be many bouncers. The one at the gate of the neighborhood. One at the step of the house, and one right in front of the resources. Which ensures granular access to resources, however the modularity of the network architecture allows us to have bouncers which can ensure access to similar types of resources.

Routers

✏️ Routers serve as a traffic director, forwarding networking traffic from one part of the network to another.

IAM and Firewall rules

💡 IAM and firewall rules allow traffic to flow in and out the VPC. IAM allows you to set granular policies to practice the principle of least privilege. Allows complete control over your network architecture.



Review

Projects, network and subnets build the 3-layer networks of Google Cloud. IAM permissions and firewall rules allow ingress and egress traffic inside of your network. Controlling for ingress and egress ensures the security and performance of your network.

Egress refers to the flow of data leaving a network. It is the process of transmitting data from one network to another networking or the internet

Ingress refers to the flow of data entering a network. It is the process of receiving data from another network or the internet.

Security in google cloud

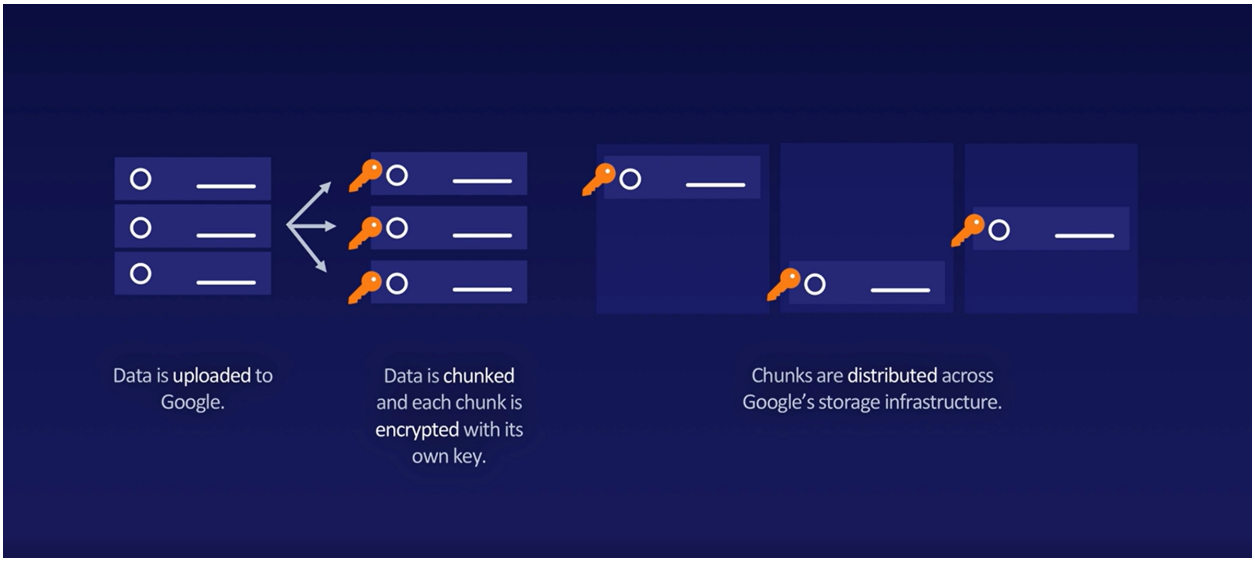
Google cloud focuses on two things with trust and security. Trusted cloud infrastructure and security at rest.

Trusted cloud infrastructure

Google cloud provides security at every layer across the infrastructure. Device, internet, identity, storage, deployment and hardware

Encryption at rest

Data is chunked and each chunk is encrypted with it’s own key using the SHA 256 algorithm.



Google Cloud APIs

APIs are interfaces that allow you to interact with Google Cloud services programmatically. Allows you to automate your workflow using google cloud SDK. The API management console allows you to monitor the requests, traffic, error and latency on any enable API. Create API credentials, meaning you can help GCP to identify users of an API.

Database overview of google cloud

> 💡 Google cloud offers two types of databases. There is relational and non-relational databases. In NoSQL databases it provides data in a non tabular form.

Relational databases

- Cloud SQL
- Cloud Spanner

NoSQL databases

- Cloud Bigtable
- Firestore
- Firebase
- Memorystore

Google cloud shell

> 💡 Container for operations and development that can access from anywhere that has 5gb of storage. It is powered by linux, and provides access to the GCP CLI.

Set up your GCP organization Lab 🔬

Set up compute engine servers

Cost calculation

Preemptible machine type: It is cost effective but has limitations, can be shut off at any time by GCP

Machine family: General purpose, will provide relatively good performance in all areas

✏️ **Machine family**: A curated set of processor and hardware configurations optimized for specific workloads. When you create a VM instance, you choose a predefined or custom machine type from your preferred machine family.

Machine family series: https://cloud.google.com/compute/docs/machine-resource Choose E2 for cost purposes

✏️ **Series**: Machine families are further classified by series and generation. For example, the N1 series within the general-purpose machine family is the older version of the N2 series. Generally, generations of a machine series use a higher number to describe the newer generation. For example, the N2 series is the newer generation of the N1 series.

Machine Type: e2-micro for cost effectiveness

✏️ **Machine type**: Every machine series has predefined machine types that provide a set of resources for your VM. If a predefined machine type does not meet your needs, you can also create a custom machine type.

Deploy

We can deploy these instances through the google cloud CLI

```
gcloud compute instances create t1 t2 t3 --project=name --zone=est-east1-b --machine-type=e2-micro
--preemptible
```

Cloud storage

💡 We have three types of storage on GCP. Object storage that manages data as objects, file storage that is used to organize and store data on a computer hard drive or on network attached storage and block storage which is used to store data files on storage area network usually in a sequence of bytes or bits.

Cloud storage

💡 Cloud storage provides object storage. The objects are stored in containers called Buckets, allows you to choose a geographical location of where your data lives.

Cloud filestore

💡 Cloud filestore is a managed filesystem interface and a shared filesystem for data.

Persistent disk

💡 A durable network storage device, that your compute instance can access like physical disks. There are two types of Persistent Disks (SSD and HDD). With HDD GCP offers low cost storage when bulk throughput (bytes read or written per second) is of primary importance. With SSD GCP offers consistently high performance for both random access workloads and bulk throughput.

Types of persistent disk

- Zonal persistent disk
  - Default
- Regional persistent disk
  - Replicated between two zones in a region
- Local SSD
  - Very high IO

Using storage buckets

💡 A bucket is a container that houses your objects in cloud storage that you can access at any time. This allows for the organization of objects.

Reasons for buckets:

- Security
  - Allow granular access for bucket usage
- Storage class and location
  - Being able to choose between storage classes can allow you to choose how available your objects are, how durable and how redundant.
- Globally unique name
  - This helps with having your buckets stand out to you
  - No overlap

Permissions

> 💡 Public access to buckets can be limited. Uniform policies means that any of the principles, will limit them to bucket-level permissions (IAM). Fine-grained policies allow for object level permissions using ACLs (Access control lists).

Bucket features

> 💡 **Bucket locking:** Allows you to configure data retention policies. This means you get too choose what data should be stored, where it should store and how long

> 💡 **Object lifecycle management**: This is where you can set a Time To Live TTL for your objects — keeping certain versions of your objects or even changing storage class of the object to meet compliance or cost efficiency

- Delete stage: After a certain time delete the object
- SetStorageClass: This changes the storage class of the object to meet the lifecycle conditions you set

Compute engine

Introduction

💡 A compute engine instance is a hosting and computing service that allows you to host and run VMs on GCP. Thishelps you run VMs you can easily scale and deliver high quality apps to users. You pay for what you use.

Types of way to use compute engine

- Pre-defined machine type
  - Default configurations
- Custom Machine types
  - Cost optimized VMs
- Spot machines
  - VMs you can use if the state of the instances are not important to you

Different Machine types

General Purpose

- These are cost optimized, balanced and scaled out optimized machine types which are great for web app service, small to medium databases, media, and virtual desktops.
- E2, N2

Memory optimized

- These are high memory optimized machine types for medium to large in memory databases, analytics and microsfot SQL database
- M2, and M1

Compute optimized

- Typically for AI/ML, high performing web computing and web serving.
- C2

Accelerator optimized

- High performance computing workloads
- Parallel computing platform
- API interfaces that allow software to use certain types of GPU
- A2 machine types

Managed instance groups

💡 An instance group is a collection of VMs instances that you can manage as a single entity.
You can scale out to add more instances to handle the load. Scaling in means reducing instances.

- Horizontal scaling refers to adding more servers
- Vertical scaling refers to adding more power to individual servers

💡 An instance group helps you create a base of instances that can continue running to help you deploy your app to the end users. You can scale in and out to meet your business needs. They also help you with auto healing and auto updating.

✏️ **Auto healing:** If your instance fails to launch, the instance group can quickly add a new instance to take it's place.

✏️ **Auto updating:** GCP rolls out the updated configurations for your VM to the instance template.

Instance template

💡 Without an instance template there would not be an instance group. The instance group pulls the configuration information you set on a template to launch the instances the exact way you state. You can use that template to provision the instance group to launch the minimum needed instances to handle user demand.

Instance groups 🔬

Creating templates:

- Access scopes gives your instances access to other GCP services
- You can also change firewall rules, as well as the service account the instance uses

Create instance group:

- You can create an instance group from the template
- You can choose the zones for high availability and disaster recovery
- Autoscaling: Autoscale, Don’t autoscale and autoscale only out
- Autoscaling policy: Determines the percentage of CPU utilization that needs to be passed to automatically scale out. i.e. 60%
- Health checks: we can create new health checks.
  - ☐ Look into health checks

Managing compute engine resources

- Security
  - Using SSH keys to control access to VMs
- Snapshots
  - How to capture a point in time snapshot of your instance to use for duplication or disaster recovery
- Monitoring and logging
  - How to install monitoring and logging on your instances to get key insights on heath.

Security

> 💡 With GCP you can create custom SSH keys and upload them to the instances details to allow you to access to the instance outside of the GCP environment.

- You can control access to it, and manage your own environment
- Or allow GCP manage SSH keys for you which would then be controlled and applied by google for any future instances

> ✏️ SSH: Secure Shell provides a encrypted and secured way to communicate and interact with servers and virtual machines. It has also ensures encrypted communication.

Snapshots

> 💡 Snapshots allow you to take a point in time recovery of your instance to store In case you need a faster rollback to a previous point in time recovery. You can also create a VM Image that is the exact same duplicate of the instance.

What is the difference between a snapshot and a image

> 💡 A snapchat is a capture of the data on the storage, they are smaller in size and can be created and restored more quickly than duplicate images. They do not include information about the OS, or configuration, and so assume the VM has the exact same OS and configuration. A image however, includes app data, OS information and configuration and usually takes longer.

Monitoring

> 💡 Cloud monitoring agents allow you to assess the health of your VMS and ensure responsiveness. Or learn more about the instance activity. You can do this by installing monitoring and logging agents

- You can install googles cloud monitoring suite.
- It streams logs from instances and third party packages to cloud logging for your viewing
- You can also create sinks which use the logs for monitoring purposes.

Launch a compute instance VM 🔬

Objectives

1. Launch a VM
2. Look at creating SSH keys
3. Take a snapshot and create a new instance
4. install a monitoring and logging agent

Work

- [x] ~~Learn about Boot disks and operating systems~~
  - [ ] Why are some operating systems better suited than others

Bootdisk

Reasons to configure boot disk:

1. Operating system: You may want to change the operating system depending on the software you are using or what you are comfortable with
2. Boot disk: You may want to change the size of the disk that will store your operating system and data files. Or you can change to a boot disk that offers increased performance for your work load.
3. Disk encryption: You can configure disk encryption to secure your data at rest, which helps against unauthorized access.
4. Image and pre-installed software: you can choose an image with a pre-installed language or database.

Security

> ⚙️ You can create a SSH key on your local computer. Go into your console, and enter the SSH key into the VM. This will allow you to have access to the console using your Public private key combination.

- [ ] What makes an SSH key work

Logging and monitoring

- [ ] What is fluentd
- [ ] What does stackdriver do?

The logging agent is just going to collect logs and data, and create a serverless response to whatever our logs say.

> ⚙️ You can run stackdriver scripts to install logging and monitoring agents on the VM.

Snapshots

⚙️ We can create snapshots of the state from the compute engine UI. The snapshot will be a point in time recovery. If you are concerned with replication and duplication, you will have a snapshot ready to go. Quickest way to replicate an instance in another zone is to take a snapshot of it. You can then create a new instance using the snapshot.

Virtual Private Cloud Networking

💡 GCP offers VPC that can help host an entire organization. Provides the network for your resources to use and scale with your business. You can scale your network and resources with no downtime. You are allowed to bring your own IPs to minimize downtime if you are migrating. With flow logs, you can capture traffic in and out of your network.

Major VPC components and Services

Routes: Controls where traffic is directed

✏️ VPC route: Is a set of directions within a network that determines the path a network traffic takes within a VPC. They determine how traffic is networked across different subnets and between the VPC and other networks

Firewall Rules: Controls who and what is accessed

VPN: Securely connects you to another network

VPC Peering: Connects two VPC networks together

Cloud Load Balancing: Distributes network traffic evenly within compute VPC

✏️ Cloud Load Balancing: Ensure high availability, reliability and performance by distributing traffic across different resources. There are different techniques to use for balancing load.

Subnets: Network neighborhoods. Who has what access.

VPC demo 🔬

Objectives

1. Create a custom VPC
2. Create a custom subnet

Work

> ⚙️ You have to choose the IP range for the subnets

VPN Connection Know How

> 💡 A VPN is a virtual private network to connect to another network securely. The VPN will create a secure connection which protects your IP address using the IP security protocol. For this to happen you must have gateways than conneect networks privately between eachother.

- [ ] What is a gateway

Types of VPNs

- High availability Cloud VPN (HA VPN)
  - IP address will not be preserved, GCP will created two new addresses and 2 new interfaces for high availability
- Classic VPN
  - Only uses single IP address and single interface

Shared VPC networks

A Shared Virtual Private Cloud (VPC) network in Google Cloud Platform (GCP) is a network infrastructure that can be shared by multiple projects within an organization. With a shared VPC network, multiple projects can use the same network resources, such as subnets and firewall rules, to connect their resources, enabling communication between the resources.

A shared VPC network provides a centralized and flexible way to manage network resources for multiple projects, making it easier to implement network-related policies and security

controls, as well as to optimize network performance.

In a shared VPC network, there are two types of projects: host projects and service projects. The host project is responsible for creating and managing the shared VPC network, while the service projects use the network resources provided by the host project. Service projects can be granted different levels of access to the network resources, allowing the host project to control network access and enforce network-related policies.

Shared VPC networks are useful in scenarios where multiple projects need to communicate with each other and share network resources, such as in a multi-tier application architecture or in a multi-department organization. By using a shared VPC network, administrators can simplify network management and reduce operational costs while still maintaining network security and performance.

> 💡 A shared VPC network is a network infrastructure that can be shared by multiple projects within an organization. This allows multiple projects to use the same network resources, such as subnets and firewall rules to connect their resources, enabling communication. This simplifies netwrok management and reduces operational costs will still maintaining network security and performance. There are two types of projects in a VPC shared network. Host projects and service projects. Resources from other VPCs can connect to shared VPC.

Host project

Responsible for creating and managing the shared VPC network.

Service project

Can be granted different levels of access to the VPC network, and has rules enforced on it by host project.

Create a load balancer to distribute application network traffic to an application 🔬

> 🎯 Your team needs you to create an environment that will serve their test pages that will installed on two instances at all times. They want to ensure that any user that tries to access this will have their app traffic distributed to both instances. Take the IP address of the load balancer that you will create to distribute the traffic and see if they can access both instances.