Google cloud platform fundamentals-core platform

# Introduction

## Welcome to gcp fundamentals

Gcp offers four main kind of services

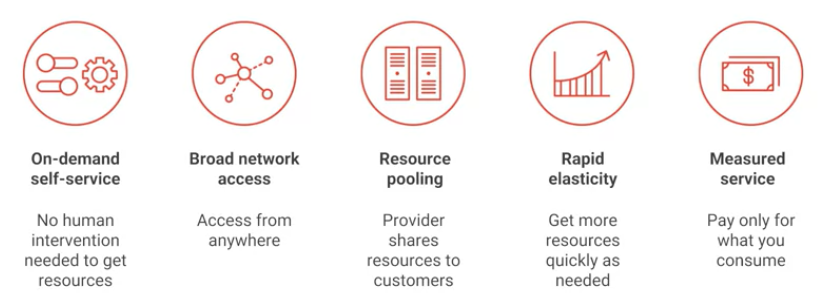
1. Compute
2. Storage
3. Big data
4. Machine learning

The cloud is a great home for your applications and data

We also learn about the cloud networking to use the resources of the cloud

## What is cloud computing

Cloud computing is a way of using IT

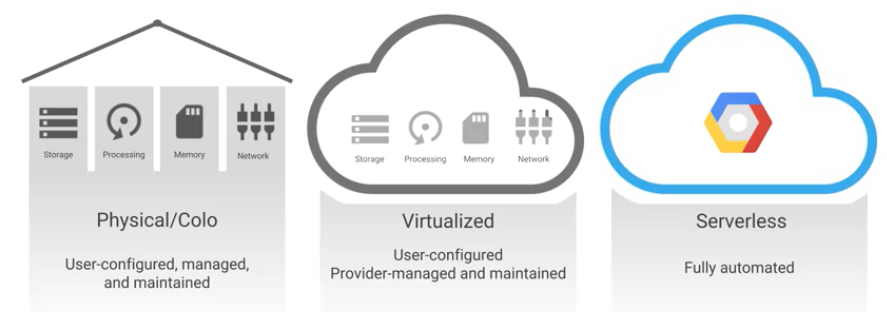


## How did we get there ?

The first trend that brought us towards cloud computing was colocation i.e instead of building costly data centers they just rent up the space whenever they needed.

In order to get an efficient use of it, departments drove towards virtualization , it also let us be more flexible.

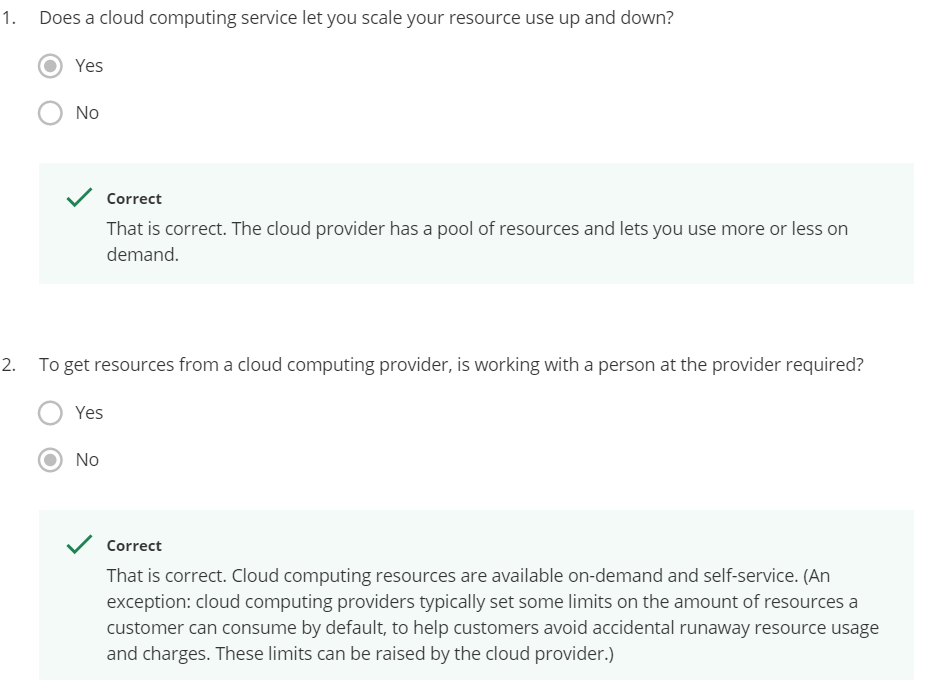
Google later thought that virtualization was not of much use and then it shifted towards the container based architecture which was built for the automated services



Google cloud provides a wide variety of services for managing and computing data and also getting value from the data.

Google predicts that every company will become a **data company** very soon.

## Quiz-1



## Gcp computing architecture

* Infrastructure as a service (Iaas) is a form of cloud computing that provides virtualized computing resources over the internet

These provide the raw compute, storage and network organization in a way familier to that of data centers

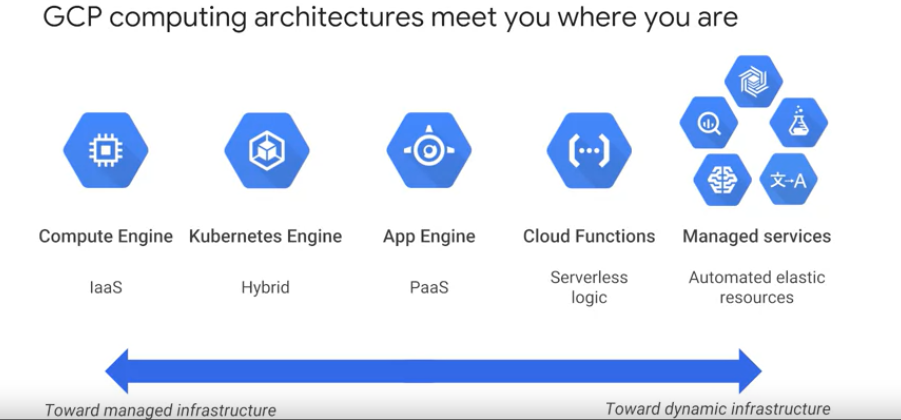
You pay for what you allocate

* Software as service(Saas)

Google's popular applications like searches,Gmail,docs,drive,Gsuits are Saas driven that directly connect to the end users

* Platform as service(Paas) bind application code to the libraries which gives access to the infrastructure that your application needs

You pay for what you use



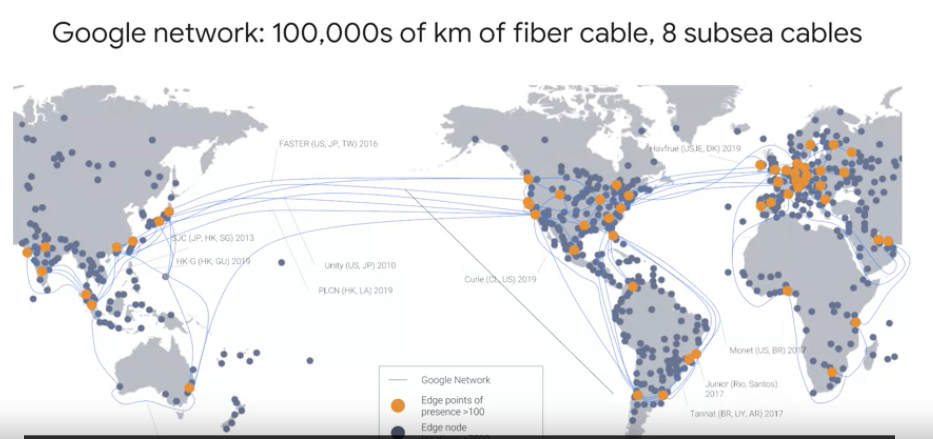
## Google's network

This network carries over 40% of the network traffic

It provides the highest possible throughput(the amount of data transferred from one location to another in a given time) and lowest latencies (the amount of time the message takes to traverse a system)

The network interconnects more than 90 internet changes and 100 points of presence(Pop) worldwide

Google’s edge caching network sites content close to end users for smaller latency



## Gcp regions and zones

A zone is a deployed area for the google cloud computing resources

Zones are grouped into regions

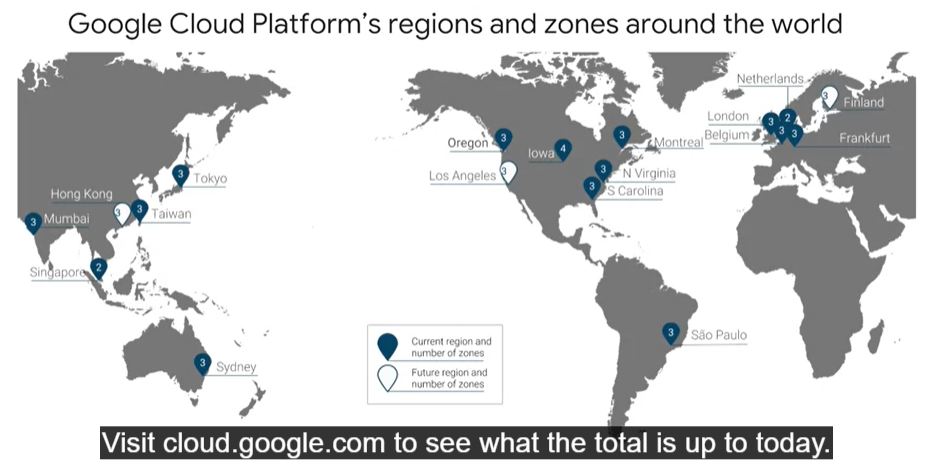
All zones within a region have a faster connectivity

Locations within a region have a round trip network latencies

Google cloud platform prefer storing their resources in a multi region i.e the data is stored redundantly over at least 2 regions separated by 160km apart

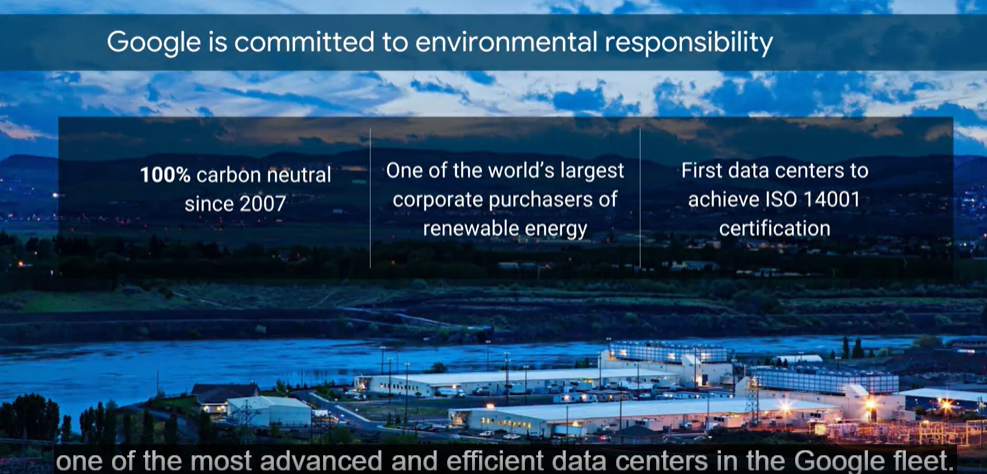


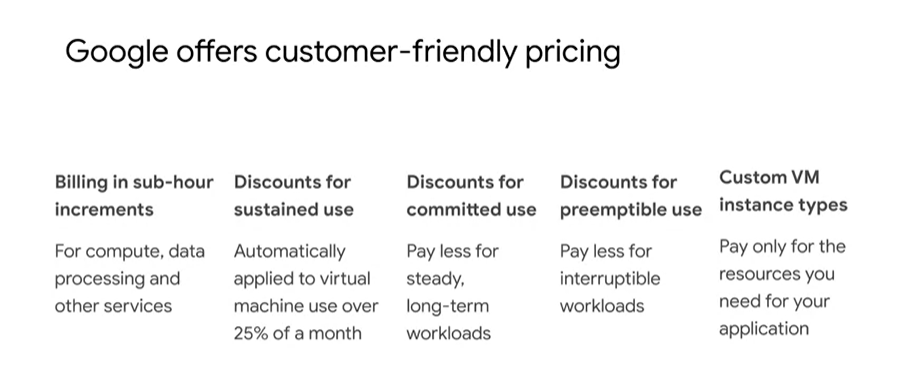
Gcp has over 15 regions over this course



## Environmental responsibility

As all the virtual world is built on physical platform the data centers use about a 2% of the world electricity





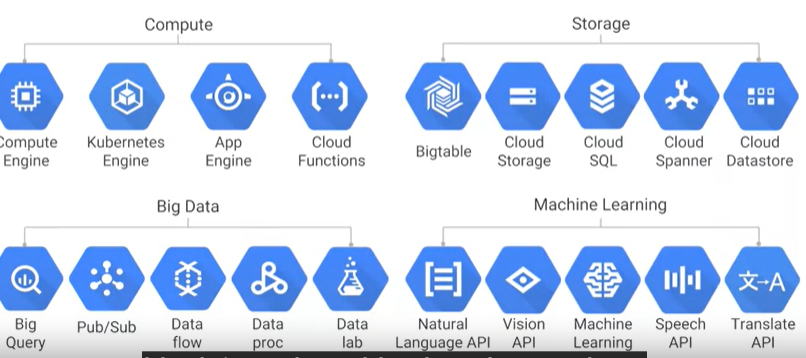
## Google API

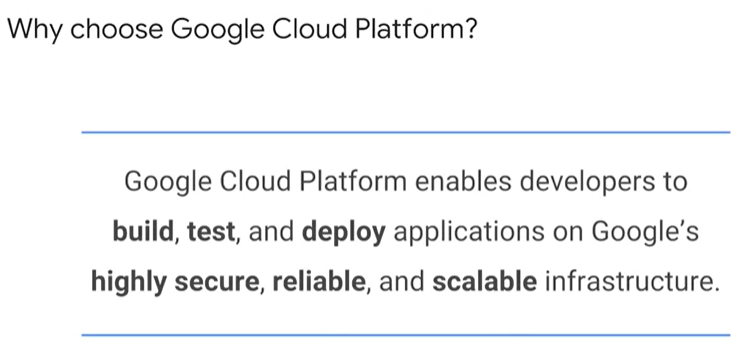
* Google gives customers the ability to run their applications elsewhere
* Bigtable uses the interface of the open source database Apache HBase, which gives customers the benefit of code portability.
* Cloud Dataproc offers the open source big data environment Hadoop, as a managed service.
* Google publishes key elements of technology using open source licenses to create ecosystems that provide customers with options other than Google.
* TensorFlow, an open source software library for machine learning developed inside Google, is at the heart of a strong open source ecosystem.
* Kubernetes gives customers the ability to mix and match microservices running across different clouds, and Google Stackdriver lets customers monitor workload across multiple cloud providers.

## Quiz-2

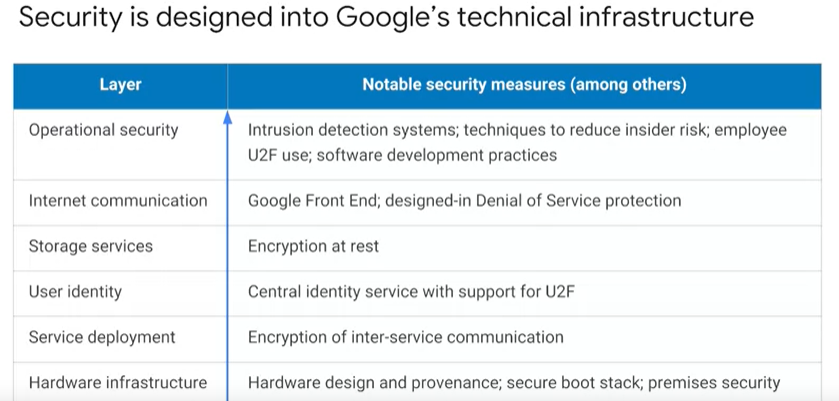


## Why choose google cloud platform





## Multi layer security approach for security



## Budgets and billing

Gcp provides 4 tool to help

1. Budgets and export
2. Billing , export
3. Reports
4. Quotes

Because Google has seven services with more than a billion users, you can bet security is always on the minds of Google's employees. Design for security is pervasive, throughout the infrastructure, the GCP and Google services run-on. Let's talk about a few ways Google works to keep customers' data safe, starting at the bottom and working up. Both the server boards and the networking equipment in Google data centers are custom designed by Google. Google also designs custom chips, including a hardware security chip called Titan that's currently being deployed on both servers and peripherals. Google server machines use cryptographic signatures to make sure they are booting the correct software. Google designs and builds its own data centers which incorporate multiple layers of physical security protections. Access to these data centers is limited to only a very small fraction of Google employees, not including me. Google's infrastructure provides cryptographic privacy and integrity for remote procedure called data-on-the-network, which is how Google services communicate with each other. The infrastructure automatically encrypts our PC traffic in transit between data centers. Google Central Identity Service, which usually manifests to end users as the Google log-in page, goes beyond asking for a simple username and password. It also intelligently challenges users for additional information based on risk factors such as whether they have logged in from the same device or a similar location in the past. Users can also use second factors when signing in, including devices based on the universal second factor U2F open standard. Here's mine. Most applications at Google access physical storage indirectly via storage services and encryption is built into those services. Google also enables hardware encryption support in hard drives and SSDs. That's how Google achieves encryption at rest of customer data. Google services that want to make themselves available on the Internet register themselves with an infrastructure service called the Google Front End, which checks incoming network connections for correct certificates and best practices. The GFE also additionally, applies protections against denial of service attacks. The sheer scale of its infrastructure, enables Google to simply absorb many denial of service attacks, even behind the GFEs. Google also has multi-tier, multi-layer denial of service protections that further reduce the risk of any denial of service impact. Inside Google's infrastructure, machine intelligence and rules warn of possible incidents. Google conducts Red Team exercises, simulated attacks to improve the effectiveness of its responses. Google aggressively limits and actively monitors the activities of employees who have been granted administrative access to the infrastructure. To guard against phishing attacks against Google employees, employee accounts including mine require use of U2F compatible security keys. I don't forget my keys as much as I used to. To help ensure that code is as secure as possible Google stores its source code centrally and requires two-party review of new code. Google also gives its developers libraries that keep them from introducing certain classes of security bugs. Externally, Google also runs a vulnerability rewards program, where we pay anyone who is able to discover and inform us of bugs in our infrastructure or applications.

## Billing and budgets

You're probably thinking, how can I make sure I don't accidentally run up a big GCP bill? GCP provides four tools to help: budgets and alerts, billing, export, reports and quotas. Let's look at budgets and alerts first. You can define budgets either per billing account or per GCP project. A budget can be a fixed limit or you can tie it to another metric. For example, a percentage of the previous month spend. To be notified when costs approach your budget limit, create an alert. For example, with a budget limit of $20,000 and an alert set at 90 percent, you'll receive a notification alert when your expenses reach $18,000. Alerts are generally set at 50 percent, 90 percent, and 100 percent. But you can customize that. Billing export lets you store detailed billing information in places where it's easy to retrieve for more detailed analysis, such as a BigQuery dataset or a Cloud storage bucket. Reports is a visual tool in the GCP console that allows you to monitor your expenditure. GCP also implements quotas, which protect both account owners and the GCP community as a whole. Quotas are designed to prevent the over-consumption of resources, whether because of error or malicious attack. There are two types of quotas: rate quotas and allocation quotas. Both get applied at the level of the GCP project. Rate quotas reset after a specific time. For example, by default, the Kubernetes Engine service sets a quota of a 1000 calls to its API from each GCP project every 100 seconds. After that 100 seconds, the limit is reset. Allocation quotas, on the other hand, govern the number of resources you can have in your projects. For example, by default, each GCP project has a quota allowing it no more than five Virtual Private Cloud networks. Although projects all start with the same quotas, you can change some of them by requesting an increase from Google Cloud support.

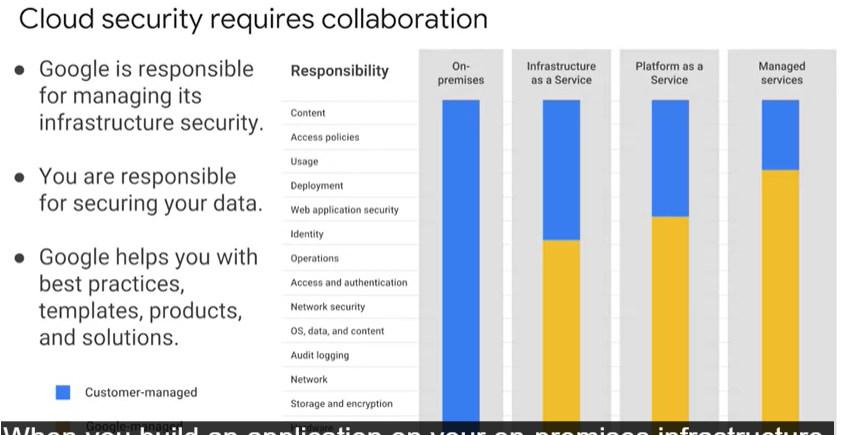
## Quiz-3

<https://quizlet.com/au/311391485/introducing-google-cloud-platform-flash-cards/#>

# Model introduction

1. When you run workloads in GCP you use projects to organise them , use projects to group together the related resources because they have common business objective
2. Google cloud identity and access management IAM or IM for this
3. The principle of least privilege is used to manage any kind of computer infrastructure if its cloud or on premises
4. In least privilege design people are protected from the entire set of errors
5. 4 ways to interact with GCP’s management layer

* Web based console
* Through API’s
* Sdk and its command line tools
* Mobile app



1. From the physical security of the hardware, and the premises in which they're housed, through the encryption of the data on disk, the integrity of your network, all the way up to securing the content stored in those applications.
2. When you move an application to Google Cloud Platform, Google handles many of the lower layers of security. Because of its scale, Google can deliver a higher level of security at these layers than most of its customers could afford to do on their own. The upper layers of the security stack remain the customers' responsibility.
3. Google provides tools such as IAM to help customers implement the policies they choose at these layers.

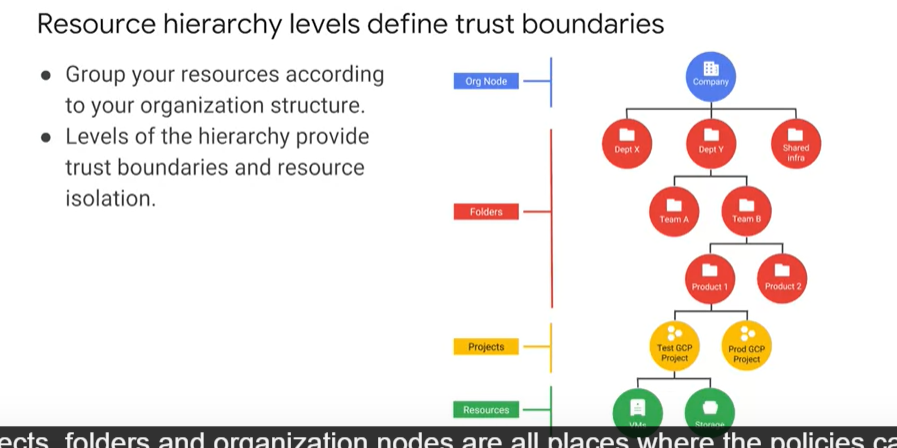
## The google cloud platform resource hierarchy

1. All the resources that we use like

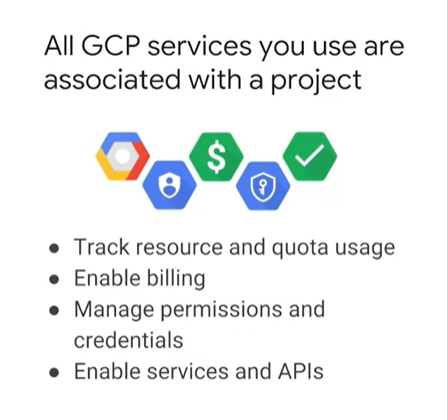
* Virtual machines
* Cloud storage buckets
* Tables and big query

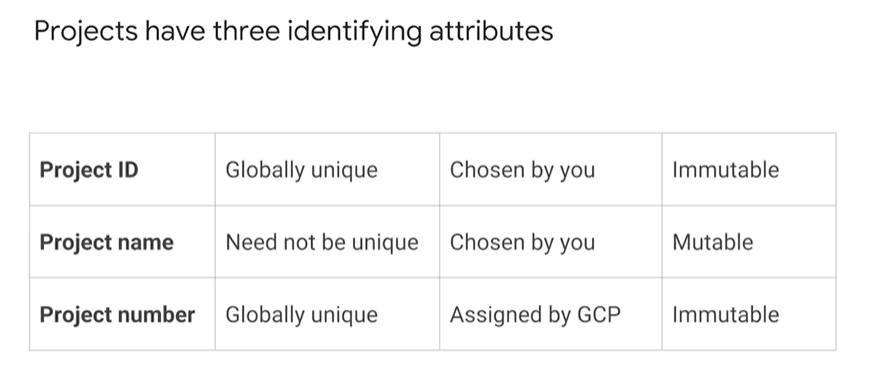
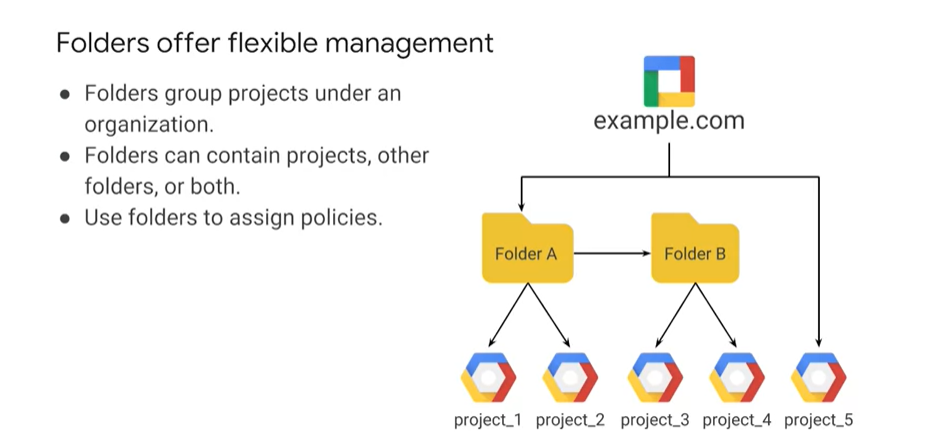
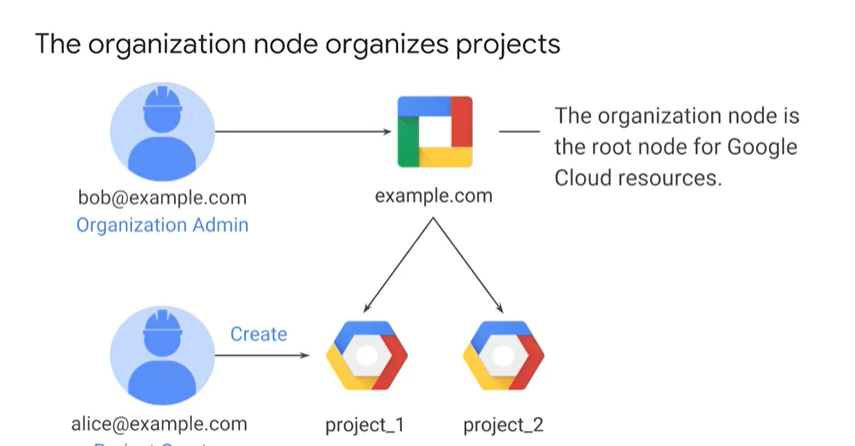
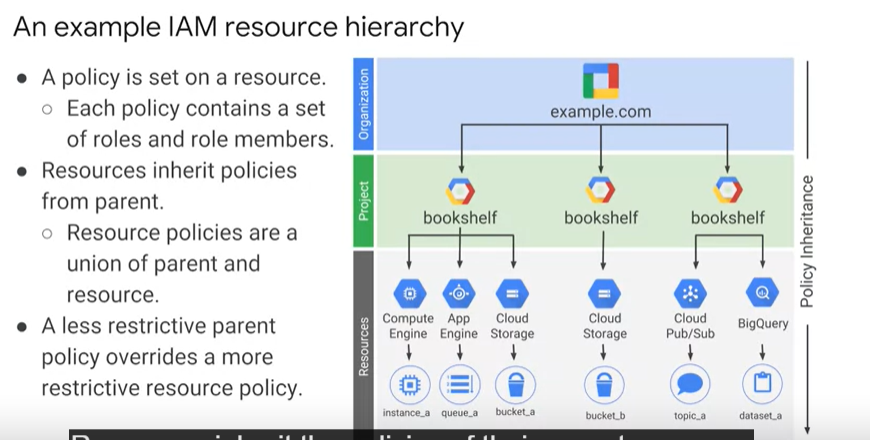
Are organised into projects

1. And these projects might be organised into folders



1. These are the nodes where policies are defined
2. Policies are inherited downwards



1. 
2. 
3. 
4. Organisation node is top of the priority
5. I.e only people with priority can change the the domain
6. And under organization node we can add folders and projects
7. 
8. Resourses inherit the properties of the parent
9. There's one important rule to keep in mind. The policies implemented at a higher level in this hierarchy can't take away access that's granted at a lower level.

# IAM

