Google Cloud for Newbies

Greg Horie

github.com/netserf

… for Newbies

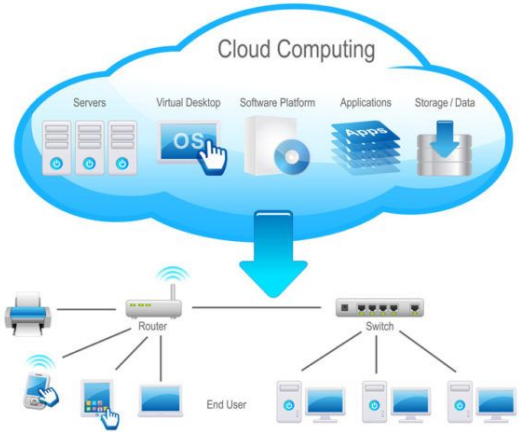
Because I'm new too !

Overview

- What is Cloud Computing?
- Google Cloud
- GCP Admin Tools
- GCP Projects
- VPCs - Virtual Private Clouds
- GCE - Google Compute Engine
- Cloud Ops Suite (Stackdriver)

What is Cloud Computing?

- Someone else's computer.
- A virtually limitless pool of compute, storage and higher-order resources / APIs.
- Accessible from remote.
- Resources geographically dispersed.
- "Pay-as-you-go".
- Some benefits
  - Cost savings.
  - Improved availability, latency, scaling, and disaster recovery.
  - Unlocks new levels of compute automation and efficiency.
  - Easy access to solutions that previously required IT staff.



Google Cloud

- 29 regions, 88 zones.
  - Toronto region opened in 2021.
- 146 network edges, 200+ countries.
- 100+ cloud products.
- Specialties:
  - Integrating with Google Workspace.
  - Fast (low latency) networking.
  - Global over regional.
  - Big data analytics.
  - Kubernetes.
  - AI / machine learning.

Regions and Zones

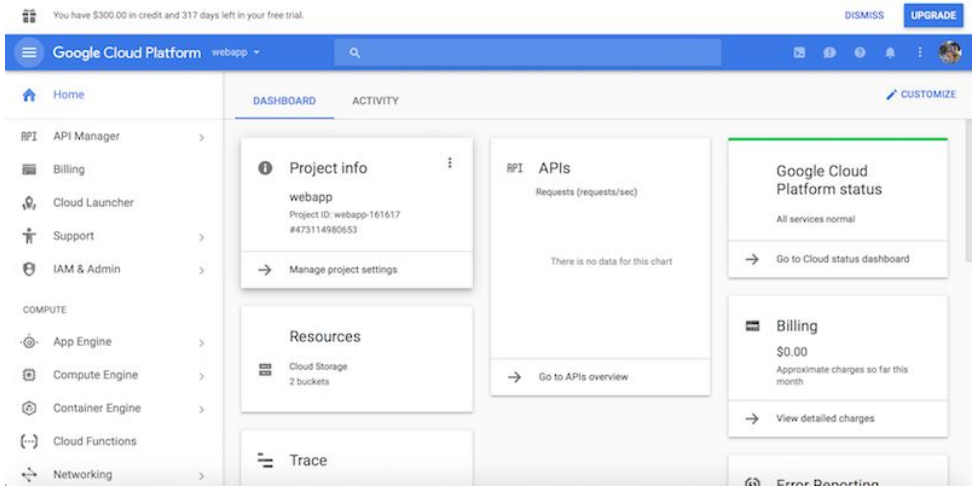
Locations	Description
Zone	A distinct GCP data centre.
Region	A collection of zones. At least 3 zones per region. Fast connections between zone members.
Multi-Region	Some services are aware of multiple regions. Useful in high availability and low latency use cases.
Network Edge	Not a full service region. Hosts a subset of services. e.g. CDN

GCP Admin Tools

- https://console.cloud.google.com/
- GCP Cloud Console.
- GCP SDK.
- GCP Cloud Shell.

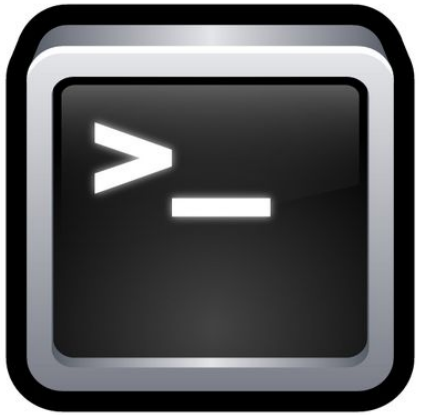
GCP Cloud Console

- Web browser interface for GCP admin interactions.
- Allows provisioning for all GCP services in one location.
- Provides centralized logging, monitoring, and debugging capabilities.



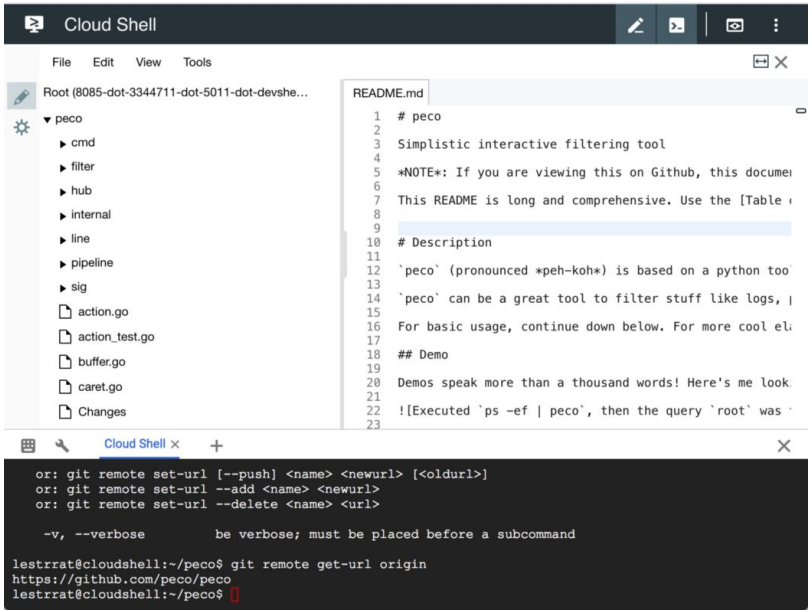
GCP SDK

- Includes CLI tools for managing GCP - gcloud, gsutil, bq
- Also, language specific cloud client libraries.
- Easy access through Cloud Shell.
- Can be installed locally.
  - https://cloud.google.com/sdk/docs/install
- Also has a Docker image available.



GCP Cloud Shell

- Admin VM for your personal use.
- CLI access to your cloud resources inside a browser.
- Manage GCP resources without having to install the Cloud SDK.
  - Always up to date and authenticated.
- Like a DMZ bastion host (jump box) without the overhead of managing a DMZ.



Cloud Shell Demo

Networking Packages

```
$ sudo apt install -y iputils-ping nmap ncat \
  traceroute arping
```

Cloud Shell Editor

```
$ echo "testing cloud shell editor" > foo
$ edit foo
```

Cloud Shell Networking

Basic Networking

```
$ ifconfig -a
$ route -vn
$ curl api.ipify.org
$ ping vicpimakers.ca
$ ping -6 vicpimakers.ca   # ?
```

From the Internet to Cloud Shell VM

```
$ ping <cloud shell public IP>
$ nmap <cloud shell public IP>
```

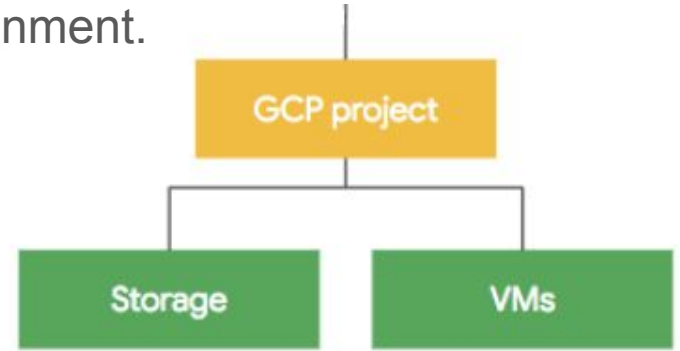
Cloud Shell - gcloud

GCP SDK - gcloud

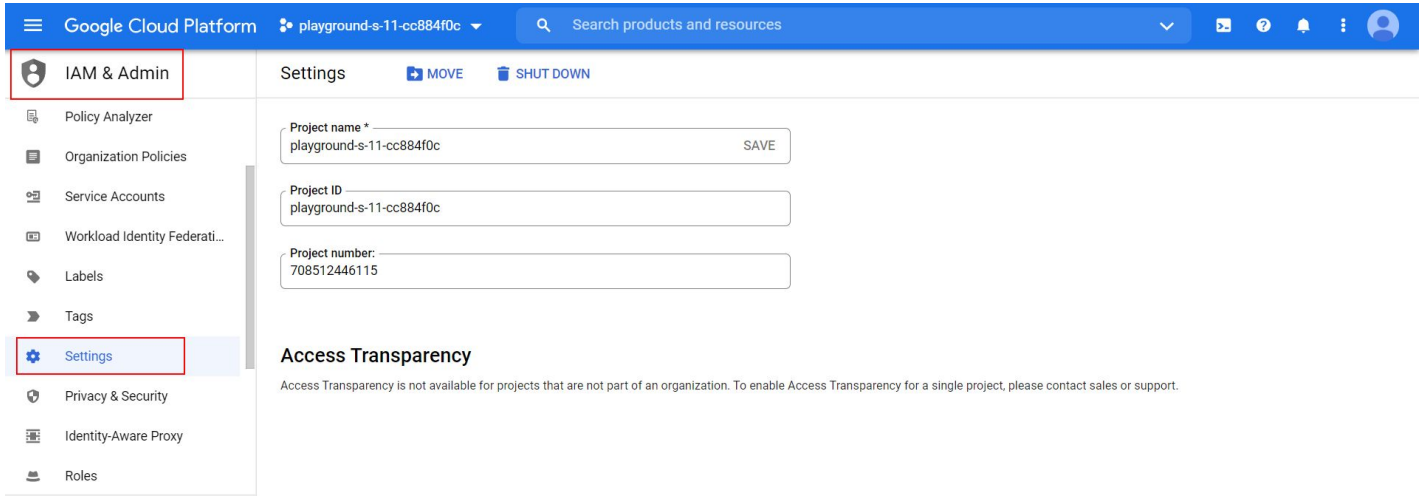
```
$ gcloud help
$ gcloud config list
$ gcloud config get-value project
$ gcloud config set compute/region us-west1
$ gcloud config set compute/zone us-west1-b
$ gcloud config list
```

GCP Project

- Logical boundary for a set of cloud resources (services).
- Project owner may add other users to their Project.
- Project demarcs the "trust boundary".
- A Project typically provides access to only a subset of services.
  - i.e. Principle of least privilege.
- Each Project is associated to a billing account.
- Best practice - One Project per app per environment.
  - e.g. Project architecture
    - my-web-portal-dev
    - my-web-portal-prod
    - my-finance-app-dev
    - my-finance-app-prod

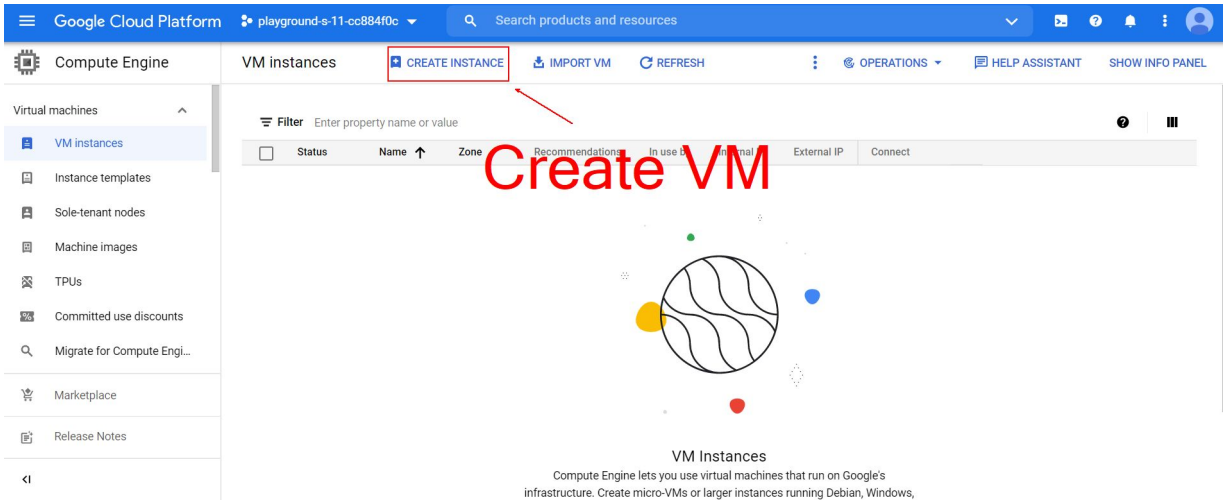


GCP Project


Google Cloud Platform
playground-s-11-cc884f0c
Search products and resources
IAM & Admin
Policy Analyzer
Organization Policies
Service Accounts
Workload Identity Federati...
Labels
Tags
Settings
Privacy & Security
Identity-Aware Proxy
Roles
Settings
MOVE
SHUT DOWN
Project name *
playground-s-11-cc884f0c
SAVE
Project ID
playground-s-11-cc884f0c
Project number:
708512446115
Access Transparency
Access Transparency is not available for projects that are not part of an organization. To enable Access Transparency for a single project, please contact sales or support.

GCE - Google Compute Engine

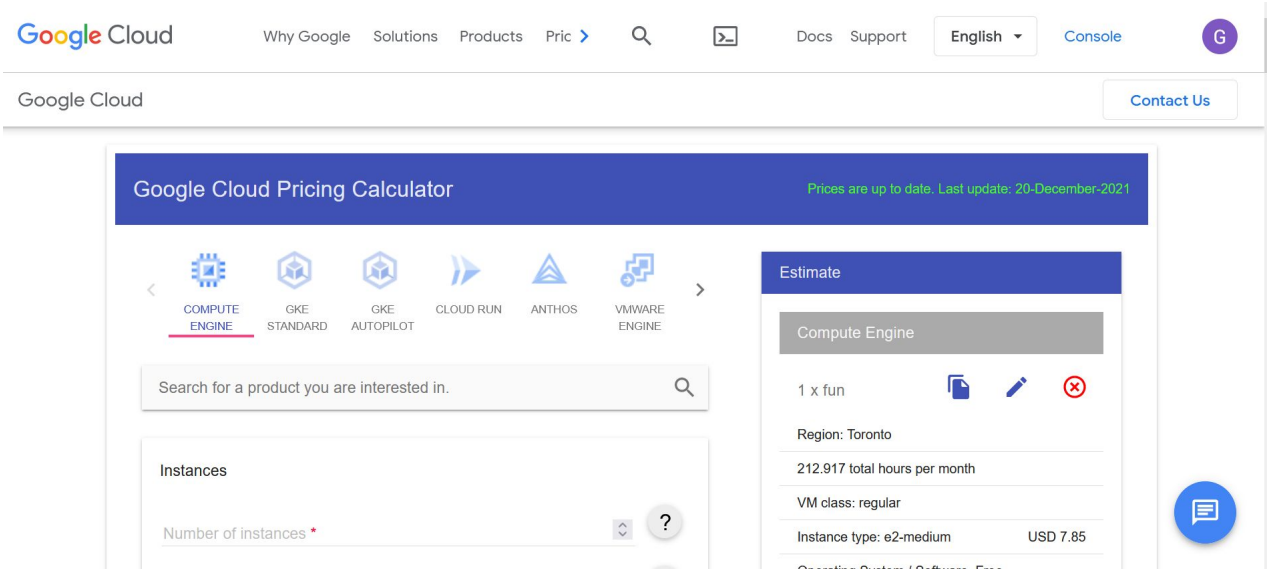
Service that allows you to create and run VMs in Google Cloud.



Try preemptibility ON for cost savings.

GCP Cost Estimates

https://cloud.google.com/products/calculator



GCE - Google Compute Engine

GCE through Cloud Shell

```
# Clean up old VM
$ gcloud compute instances list
$ gcloud compute instances delete instance-1
$ gcloud compute instances list
# New VM instance
$ gcloud compute instances create myvm
$ gcloud compute instances describe myvm
$ gcloud compute ssh myvm
```

GCE - Metadata Server

- Each GCE VM has access to its own metadata server for management and automation.

```
$ grep metadata /etc/hosts
169.254.169.254 metadata.google.internal  # Added by Google
```

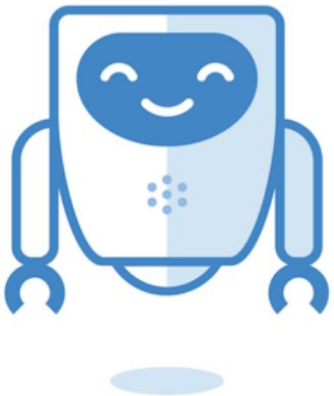
  - IPv4 link local address - https://en.wikipedia.org/wiki/Link-local_address
    - i.e. only valid for communications inside the local network (broadcast domain).
    - Routers will not forward outside the local network.
- Metadata endpoint provides useful information for the local compute node.

```
$ curl -H "Metadata-Flavor:Google" \
  metadata.google.internal/computeMetadata/

$ curl -H "Metadata-Flavor:Google" \
  metadata.google.internal/computeMetadata/v1/project/attributes/ssh-keys
```

GCP Service Accounts

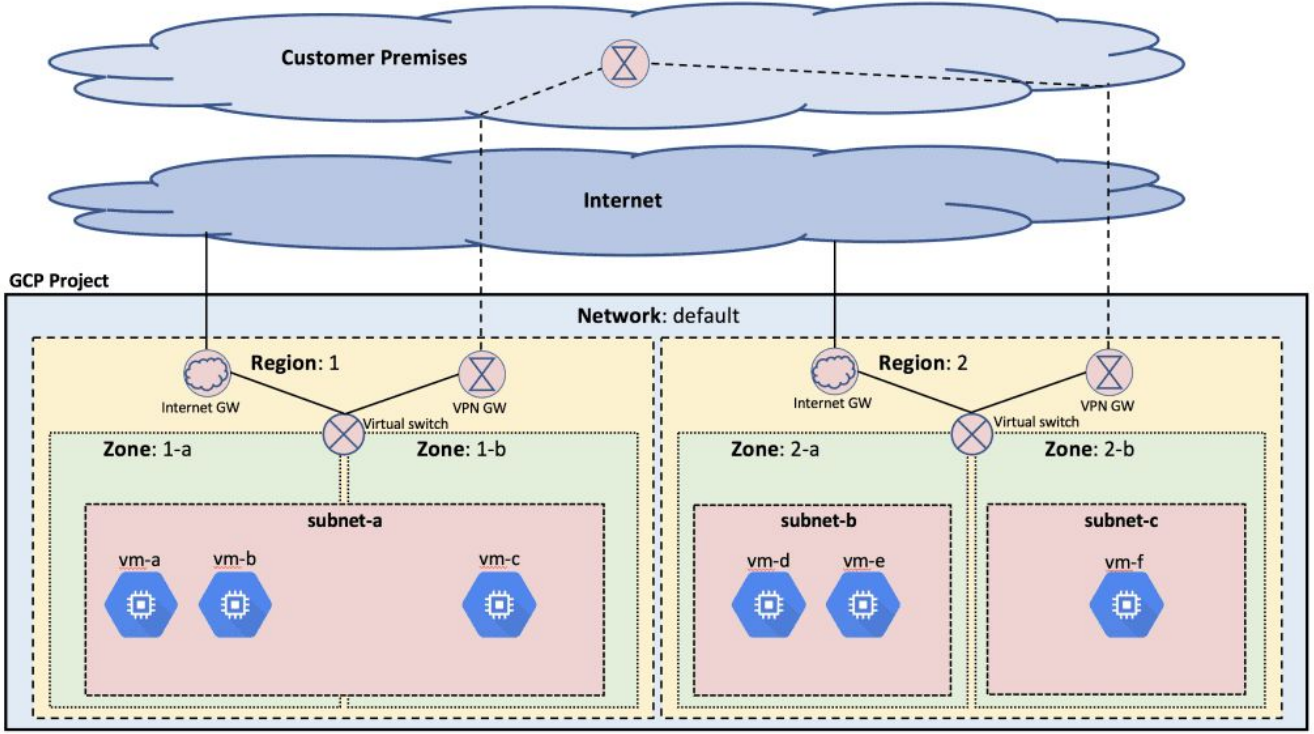
- Special account used by an app or compute workload rather than a person.
- Applications use service accounts to make authorized API calls.
- Can be given permissions to access various cloud resources.
- In essence, it is the identity of the given resource.
- Think of it as a service bot for enabling automation.
  - e.g. VM service account accessing a file from GCS.
  - e.g. VM integrates with a Cloud SQL database.



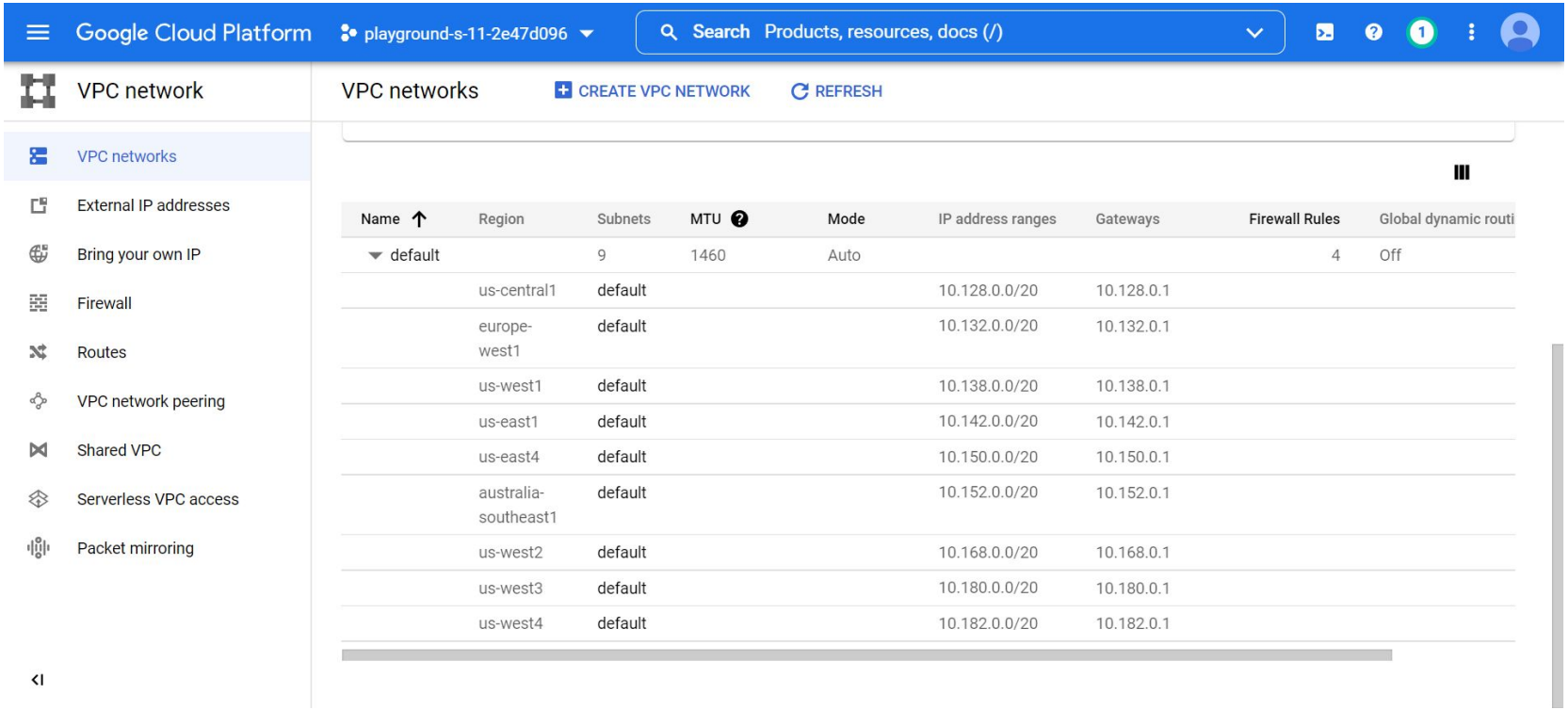
GCP Virtual Private Cloud

- A virtual version of the traditional on-prem physical network.
- Unlike other cloud providers, VPCs are global in GCP.
  - i.e. VPC subnets can be located in regions all across the world.
- Each region is assigned one or more subnets.
  - Private IPv4 addresses by default.
  - IPv6 supported, if dual stack is enabled.
- Your resources can communicate privately inside the VPC.
  - i.e. not over the Internet.
  - This privacy extends globally if you're using VMs in different regions.

Virtual Private Cloud



VPCs in Cloud Console



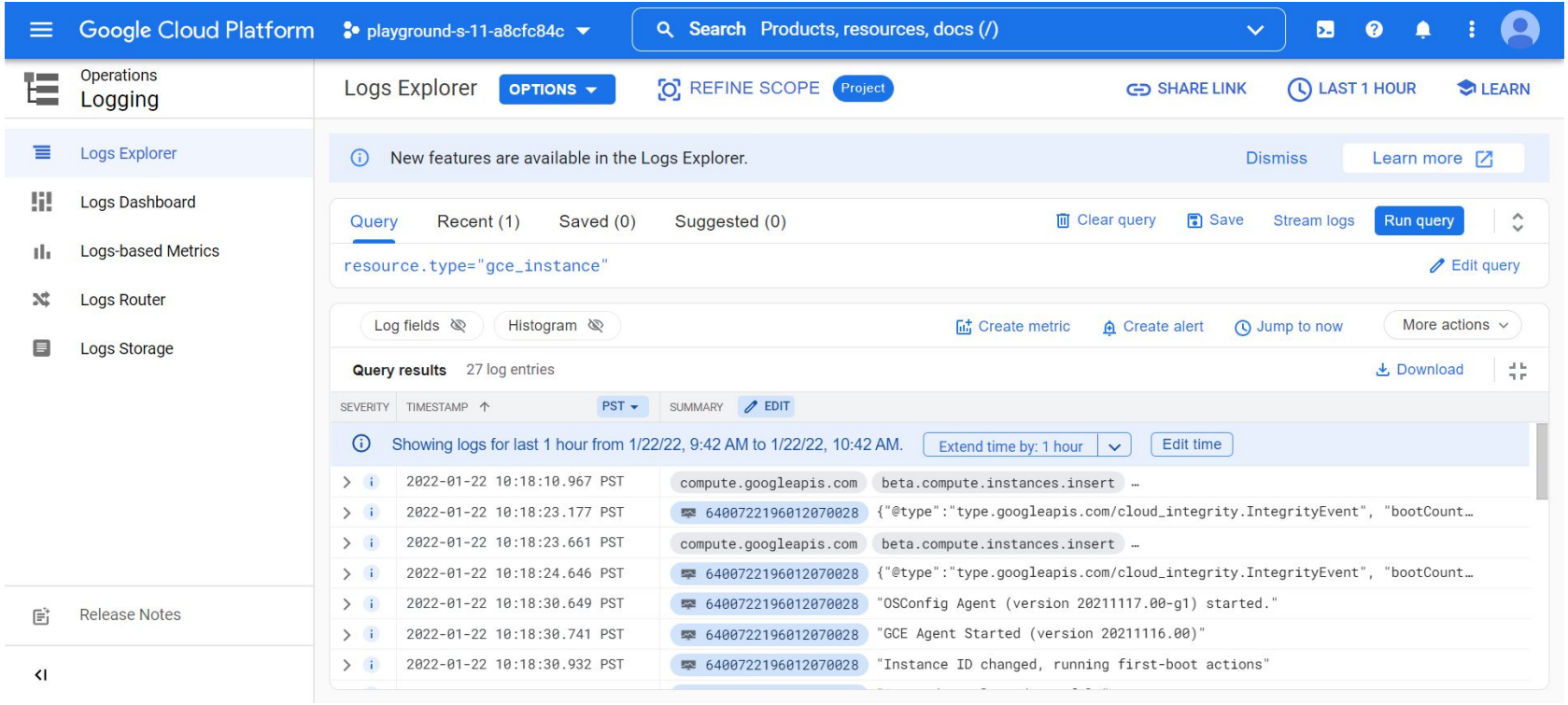
GCE IPv6 Support

- Yes, GCE can support IPv6.
- Unfortunately, no time to demo.
- Homework:
  - https://github.com/netserf/netsig-presentation-gcp-for-newbies/blob/main/gcp-cheat-sheet.txt

GCP Cloud Operations Suite

- Formerly called Stackdriver.
- Metrics, logs, and traces collected from your infrastructure.
- Metrics dashboards available (and customizable) in Cloud Console.
- Logs Explorer available for queries and log analytics.
- Customize-able alerts on metrics and logs.
- Error Reports, Debugging, and Profiling services also available.

GCP Cloud Logging



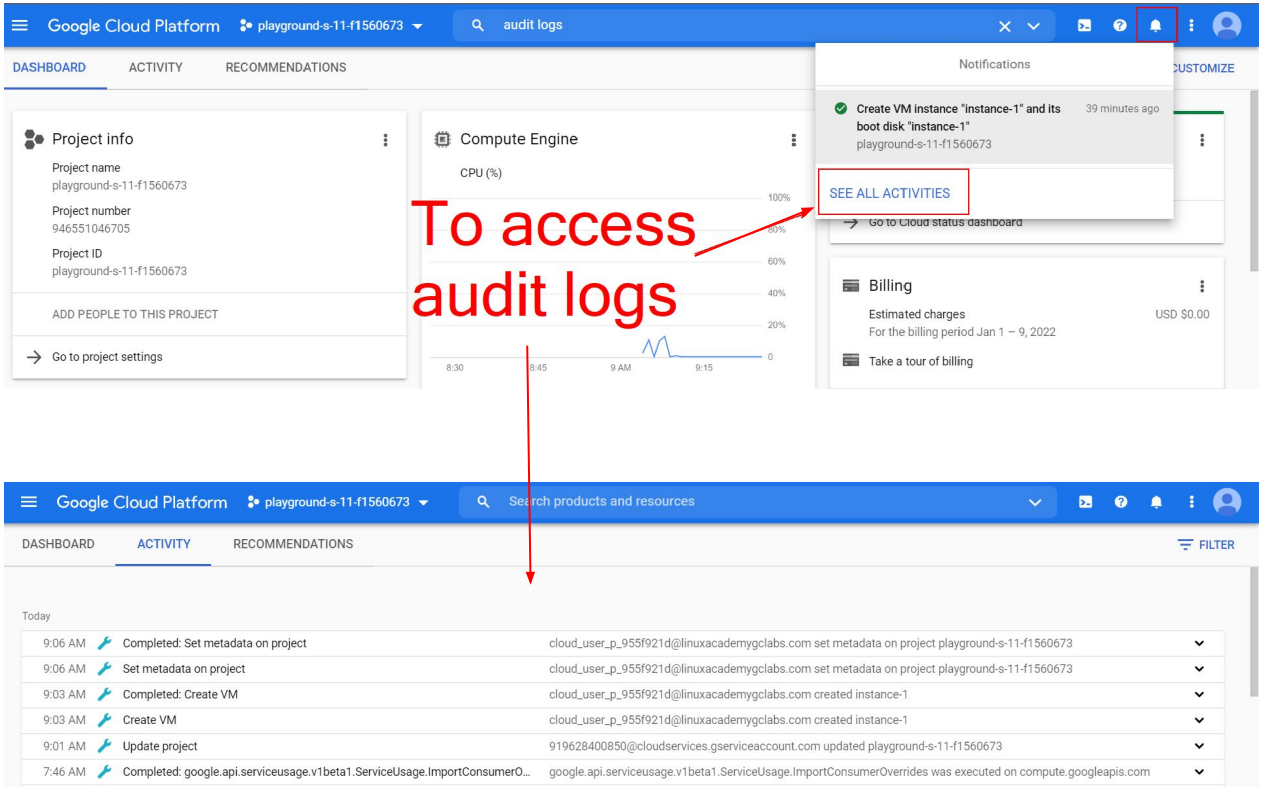
GCP Cloud Logging

- Aggregates log data from all your GCP platform resources and applications.
- Platform logs are collected automatically.
- Custom apps may integrate through the fluentd logging agent or the cloud logging API.
- Logs are available for one month with longer-term storage options via:
  - Google Cloud Storage
  - BigQuery
  - Cloud Pub/Sub to a 3rd party

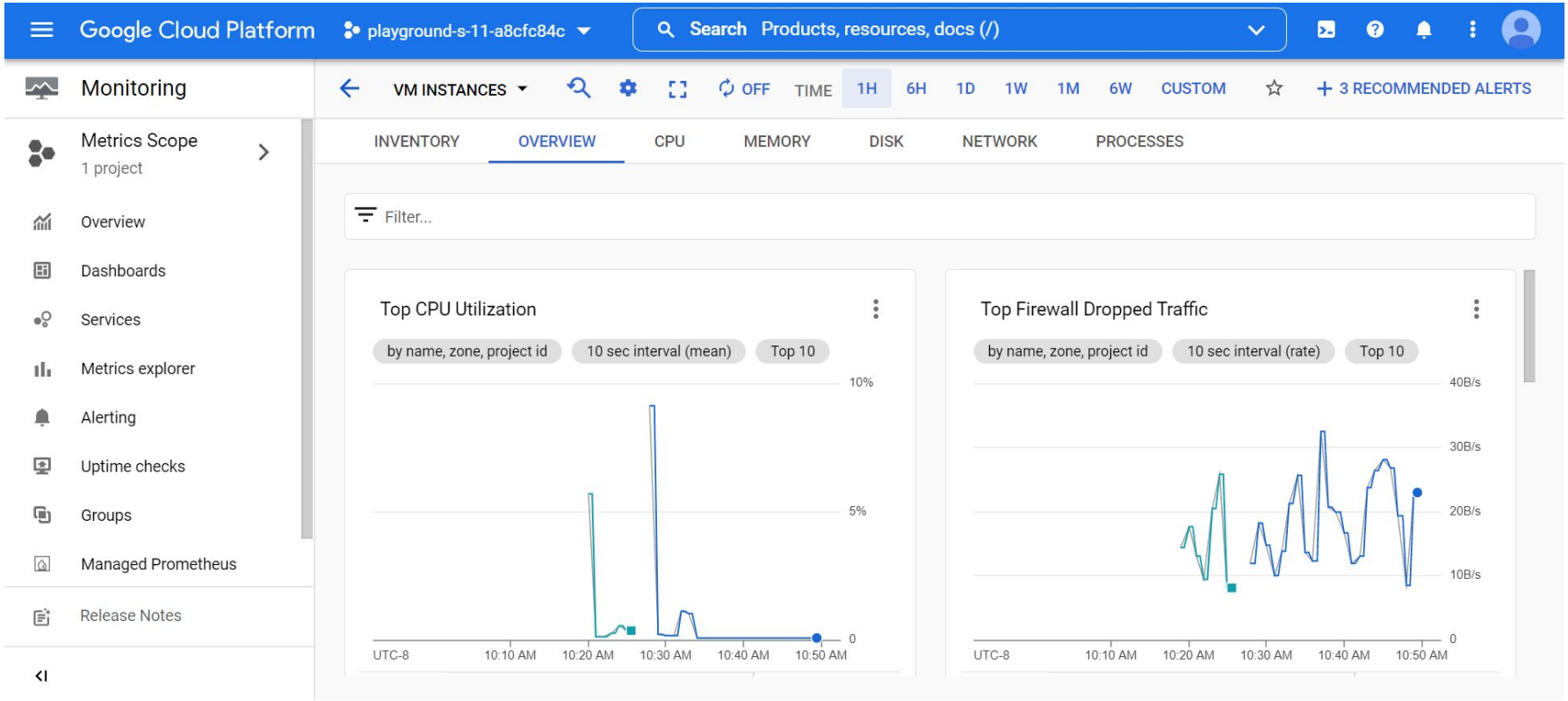
GCP Audit Logs

- A subset of the GCP Cloud Logging logs.
- Who did what and when.
- 3 types of audit logs:
  1. System events
  2. Admin activity
  3. Data access
- Audit logs are immutable and written automatically.
  - No ability to tamper or turn off the audit logs.
  - Not charged for these logs.
- You can enable additional data access audit logs.
  - These will be charged and can be quite verbose.

GCP Audit Logs

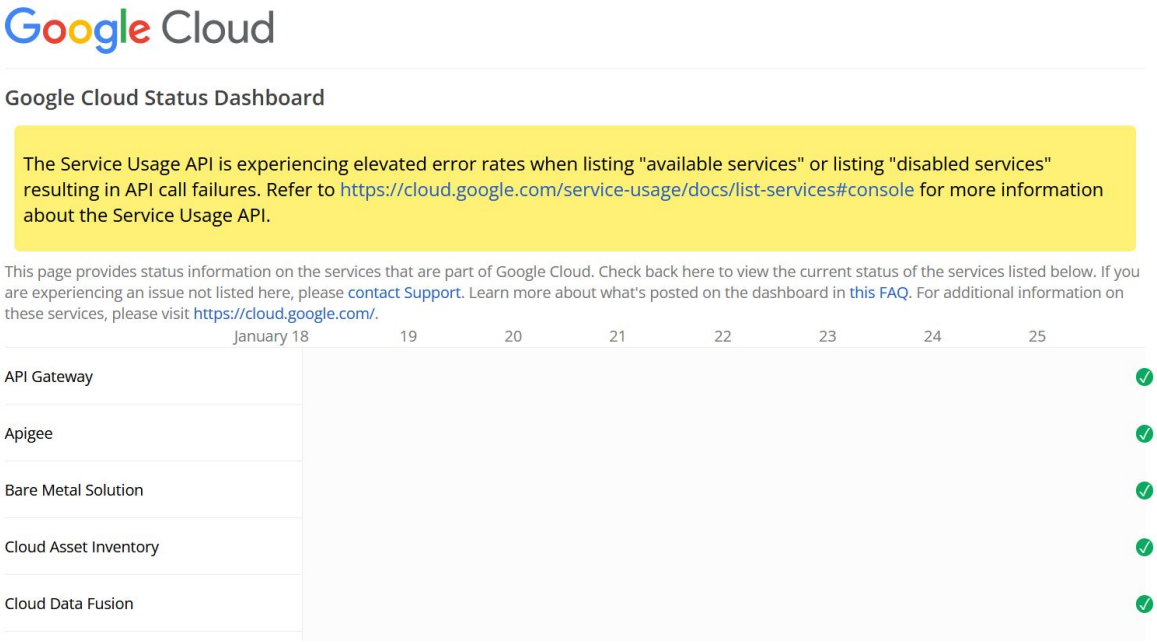


GCP Cloud Monitoring



GCP Status Page

- https://status.cloud.google.com/



GCP For Free

Trial Account

- https://cloud.google.com/free
- $300 in free credits for 90 days.
- **Note** - Will need your credit card to sign-up.

Free Tiers

- https://cloud.google.com/free/docs/gcp-free-tier/#free-tier-usage-limits
- Some GCP service tiers are offered for free (outside any trial).
- **Note** - Set up billing alerts.

Free Training

- https://www.cloudskillsboost.google/
- A 30-day trial to their online video and lab training.

Summary

- If you're looking for cloud solutions, Google Cloud is a compelling choice.
- If you're just starting, use the $300 free credit to trial GCP services.
- Certainly worth a test drive.

- GCP for Newbies Slides & Cheat Sheet
    - https://github.com/netserf/netsig-presentation-gcp-for-newbies

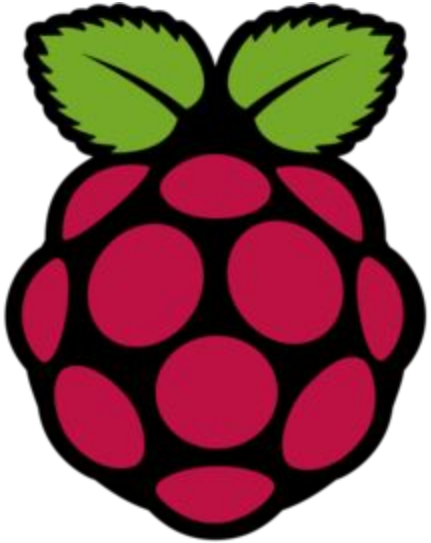
NetSIG Email Forum

- Send a message with "**subscribe**" in the subject to:

netsig-join@vicpimakers.ca

VicPiMakers Slack

- Please let us know if you want an invite to this Slack group



Possible Future Discussions

- Terraform for Newbies
- Kubernetes Engine / Anthos
- Cloud DNS / Cloud Load Balancer
- App Engine
- Cloud Pub/Sub
- Cloud Functions
- Prometheus / Grafana

Backup Slides

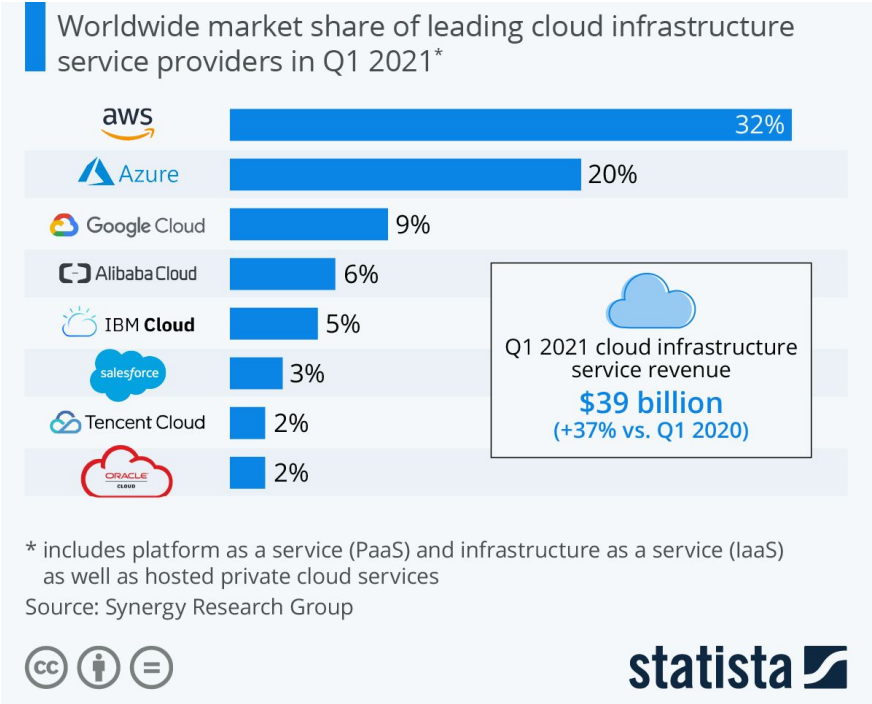
Milestones in Cloud Computing

Year	Milestone
2006	AWS launched IaaS solutions - Introduces S3 (object store) and EC2 (VMs).
2008	Google releases GAE (PaaS).
2010	Microsoft's Azure launched. Amazon store moved to AWS. Google releases GCS (object store). Rackspace and NASA launch OpenStack.
2012	Google introduces GCE (virtual machines). Netflix migrates all infrastructure to AWS.
2013	Docker debuts at PyCon.

Milestones in Cloud Computing

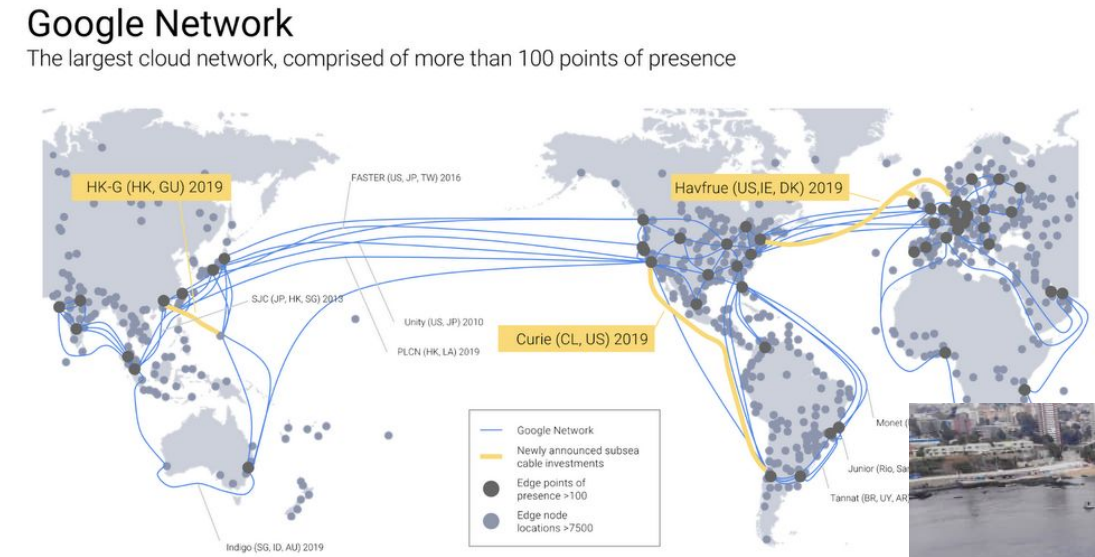
Year	Milestone
2014	AWS introduces Lambda (FaaS).
2015	Kubernetes 1.0 released.
2016	Google Container Engine GA. - Eventually rebranded to Kubernetes Engine.
2017	GCP introduces Functions (FaaS).
2018	AWS EKS released.
2021	Google begins the YouTube migration to GCP.

Cloud Market Share

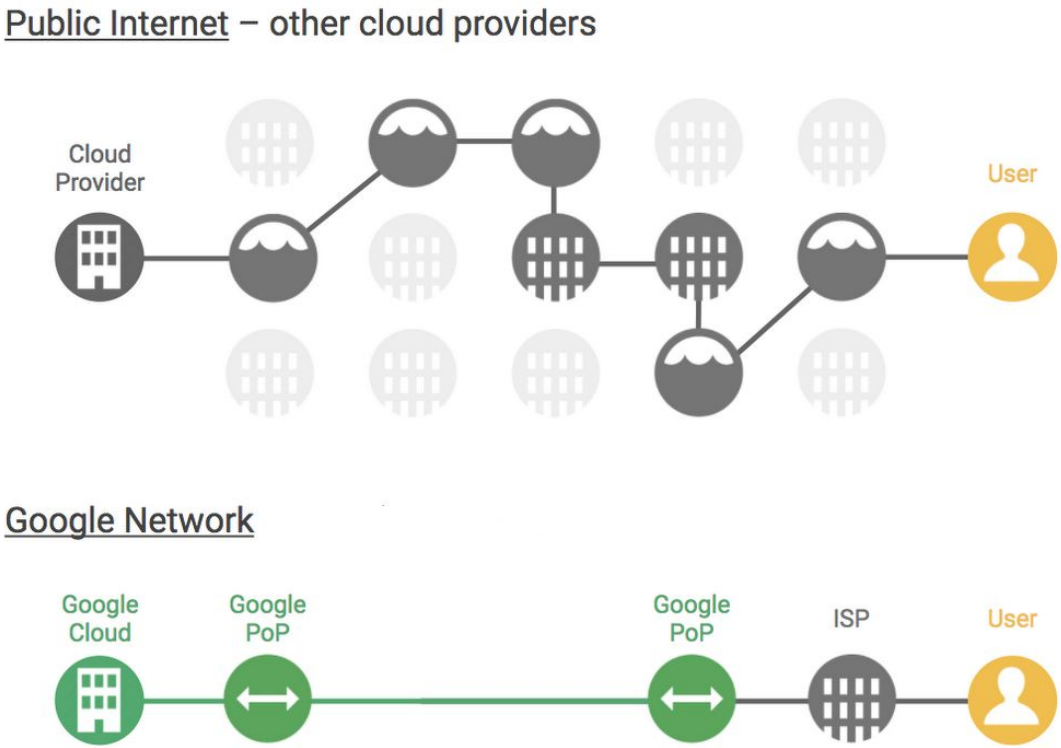


https://www.statista.com/chart/18819/worldwide-market-share-of-leading-cloud-infrastructure-service-providers/

Google's Network

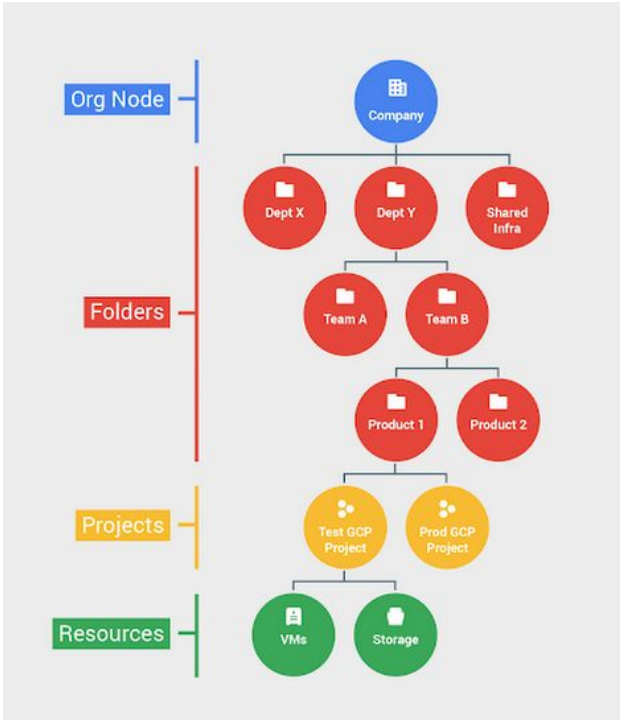


Google's Network



GCP Resource Hierarchy

- The resource hierarchy allows an organization to group access control policies and configs.
- 3 levels - Organization, Folders, and Projects.
  - Orgs and Folders are only relevant to organizations.
  - Most users will only interact at the Project level.
- Top level is the Organization.
  - High-level policies and permissions are set here.
- Folders provide further grouping of resources.
  - Often aligned with an org-chart.
  - More policies and permissions.
- Projects are where the cloud resources reside.
  - Further permissions / restrictions may be set at this level.



GCP Services (APIs)

GCP Services

```
$ gcloud services list --enabled | grep NAME
$ gcloud services list --available | grep NAME | wc -l
$ gcloud services enable container.googleapis.com  # k8s
$ gcloud services list --enabled | grep NAME
```