

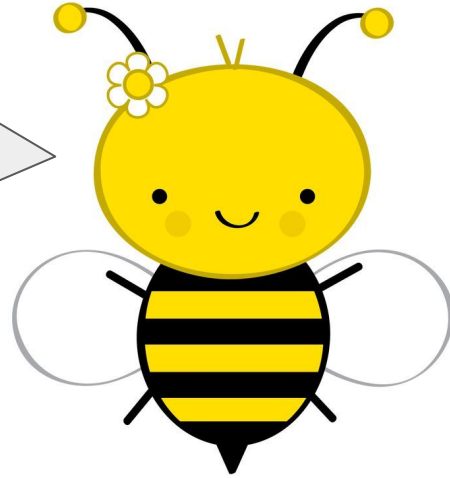
# Google Cloud for Newbies



Greg Horie

... for Newbies

Because I'm  
new too !



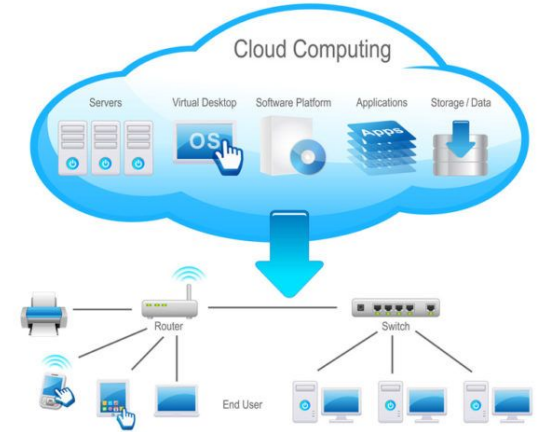
# Overview

- What is Cloud Computing?
- A Brief History
- Google Cloud
- GCP Resource Hierarchy
- GCP Projects
- VPCs - Virtual Private Clouds
- GCE - Google Compute Engine



# What is Cloud Computing?

- Someone else's computers.
- Limitless pool of compute & storage resources.
- Accessible from remote.
  - Physical infrastructure completely abstracted by provider.
  - Virtual access via web portal, API, CLI.
- Resources geographically dispersed.
  - Supports high availability, low latency, data sovereignty, etc.
  - Easy to scale up or down - "Elastic".
- "Pay-as-you-go".
  - Customers rent resources.
- Benefits
  - Unlocks new levels of compute automation and efficiency.
  - Easy access to solutions that previously required IT staff .



# 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.



Google Cloud



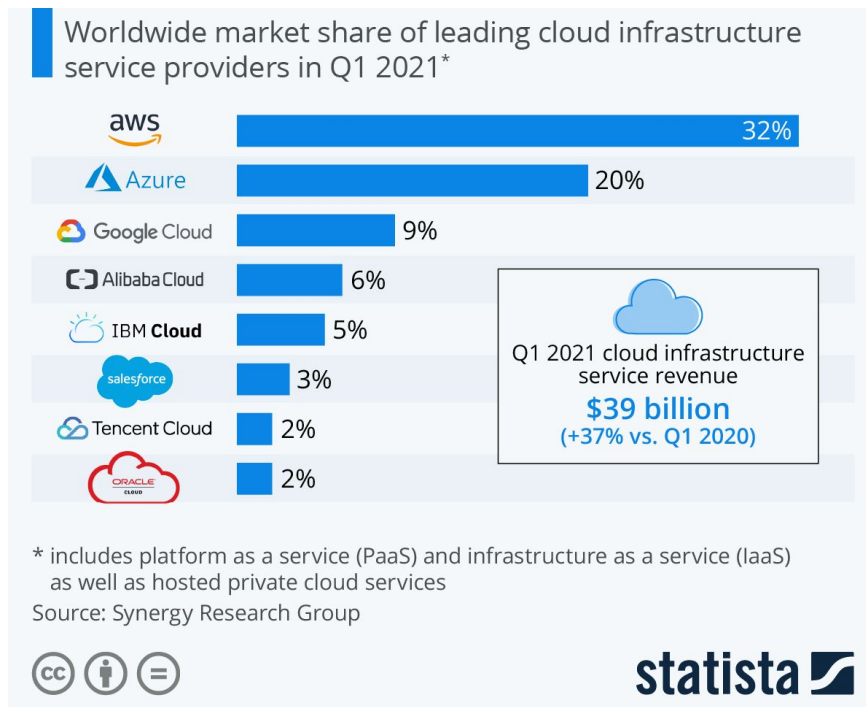
Azure

# 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 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.
  - Enabling devops / SRE practices.





# Regions and Zones

Locations	Description
Zone	A distinct GCP data centre. Fast connections to other zones in the same region.
Region	A collection of zones. At least 3 zones per region.
Multi-Region	Some services are aware of multiple regions. Useful in high availability and low latency use cases.
Network Edge	Also called PoPs. Provides subset of services that are in a GCP Region.

## GCP Regions and Zones

Google Cloud Platform is organized into regions and zones



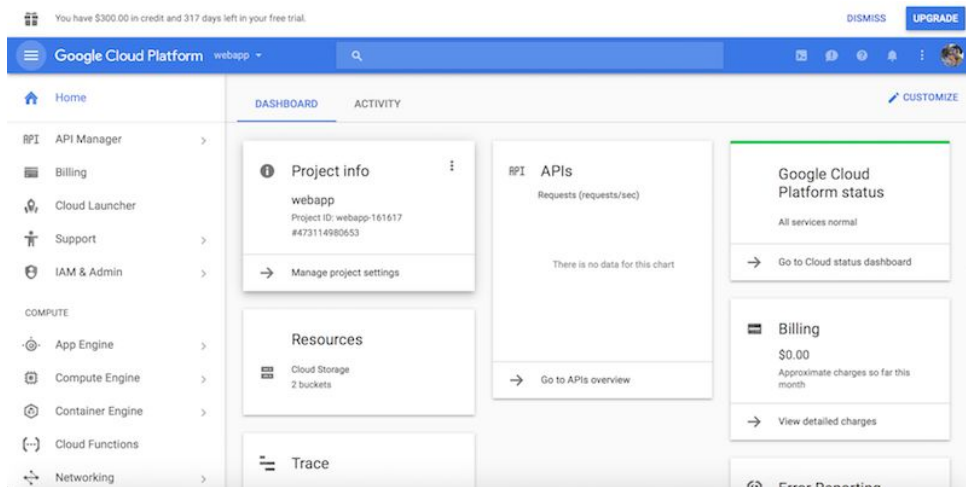
# GCP Admin Tools

- GCP Cloud Console.
- GCP SDK.
- GCP Cloud Shell.



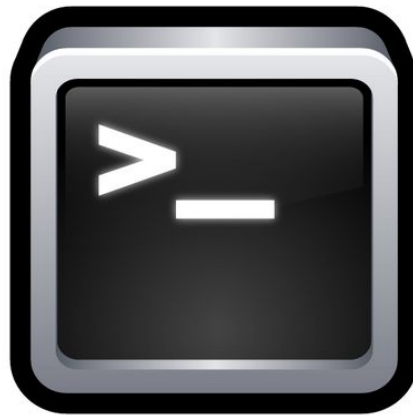
# GCP Cloud Console

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



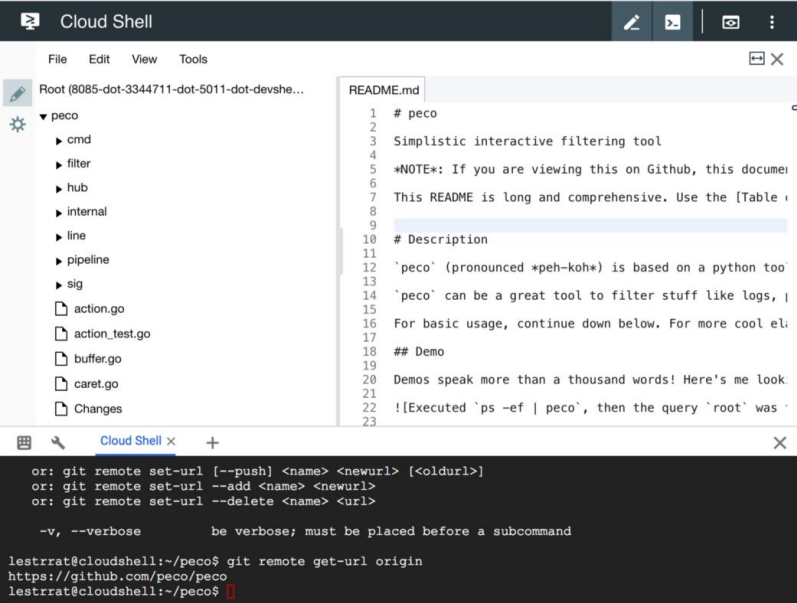
# GCP SDK

- 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.



The screenshot displays the GCP Cloud Shell environment. At the top, the title bar reads 'Cloud Shell'. Below it, a menu bar includes 'File', 'Edit', 'View', and 'Tools'. The main workspace is divided into three sections. On the left is a file explorer showing a directory structure for 'peco' with subdirectories like 'cmd', 'filter', 'hub', 'internal', 'line', 'pipeline', and 'sig', along with files like 'action.go', 'action\_test.go', 'buffer.go', 'caret.go', and 'Changes'. The center section shows a 'README.md' file with the following content:

```
1 # peco
2
3 Simplistic interactive filtering tool
4
5 *NOTE*: If you are viewing this on Github, this document
6
7 This README is long and comprehensive. Use the [Table of Contents]
8
9
10 # Description
11
12 `peco` (pronounced *peh-koh*) is based on a python tool
13
14 `peco` can be a great tool to filter stuff like logs,
15
16 For basic usage, continue down below. For more cool el
17
18 ## Demo
19
20 Demos speak more than a thousand words! Here's me look
21
22 ![Executed `ps -ef | peco`, then the query `root` was
23
```

At the bottom is a terminal window with the following text:

```
or: git remote set-url [--push] <name> <newurl> [<oldurl>]
or: git remote set-url --add <name> <newurl>
or: git remote set-url --delete <name> <url>

-v, --verbose          be verbose; must be placed before a subcommand

lestrrat@cloudshell:~/peco$ git remote get-url origin
https://github.com/peco/peco
lestrrat@cloudshell:~/peco$
```

# Cloud Shell Demo

## Cloud Shell Editor

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

```
$ edit foo
```

## Networking Packages

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

# 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 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
```

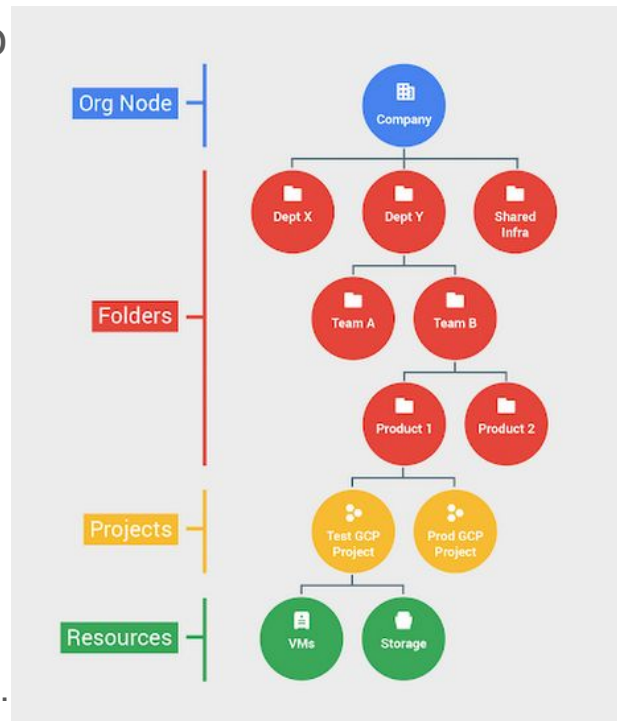
## # Better

```
$ gcloud compute project-info add-metadata --metadata \
google-compute-default-region=us-west1,google-compute-default-zone=us-west-1-b
```



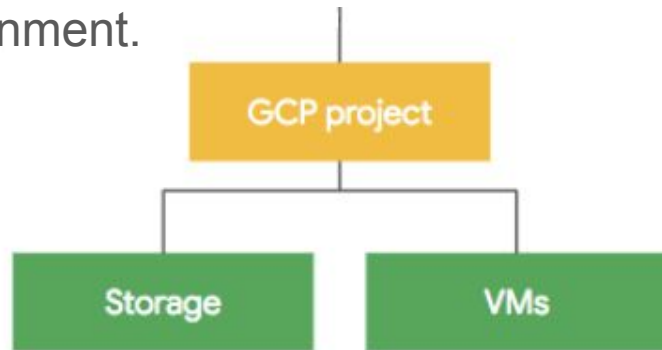
# GCP Resource Hierarchy

- 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 Project

- Project contains all your cloud resources (services).
- Project owner may add other users to their Project.
- Project demarcates the "trust boundary".
- Any given Project typically provides access to 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.
    - my-web-portal-prod
    - my-web-portal-dev
    - my-finance-app-prod
    - my-finance-app-dev



# GCP Services (APIs)

## **GCP Services**

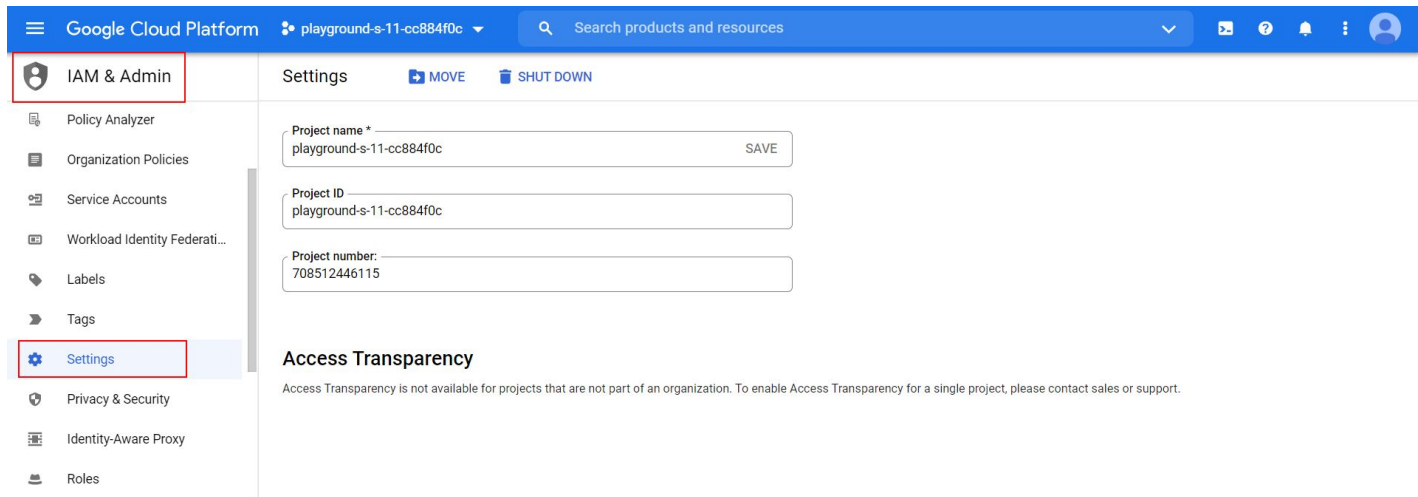
```
$ gcloud services list --enabled | grep NAME
```

```
$ gcloud services list --available | grep NAME | wc -l
```

```
$ gcloud services enable container.googleapis.com # k8s
```

```
$ gcloud services list --enabled | grep NAME
```

# GCP Project



The screenshot displays the Google Cloud Platform (GCP) console interface. At the top, a blue header bar contains the 'Google Cloud Platform' logo, the current project name 'playground-s-11-cc884f0c', a search bar, and various utility icons. On the left side, a navigation menu lists several categories: 'IAM & Admin' (highlighted with a red box), 'Policy Analyzer', 'Organization Policies', 'Service Accounts', 'Workload Identity Federati...', 'Labels', 'Tags', 'Settings' (highlighted with a red box), 'Privacy & Security', 'Identity-Aware Proxy', and 'Roles'. The main content area is titled 'Settings' and includes two buttons: 'MOVE' and 'SHUT DOWN'. Below these, there are three input fields: 'Project name \*' with the value 'playground-s-11-cc884f0c' and a 'SAVE' button, 'Project ID' with the value 'playground-s-11-cc884f0c', and 'Project number' with the value '708512446115'. Further down, the 'Access Transparency' section is visible, with a note stating: '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.'

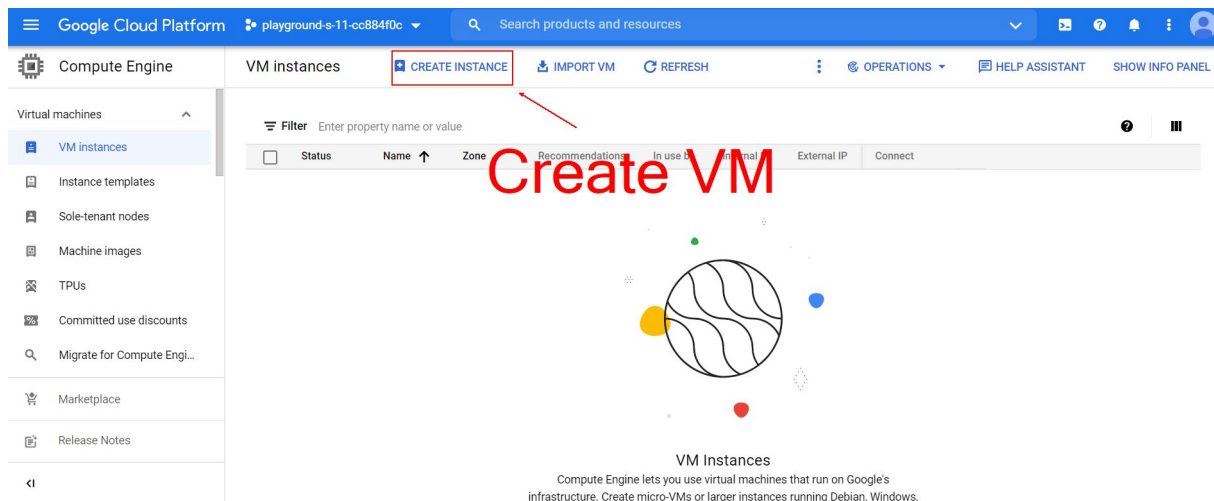
```
$ gcloud projects list
```

```
$ gcloud projects describe [project-name]
```



# 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>

The screenshot shows the Google Cloud Pricing Calculator interface. At the top, the Google Cloud logo is on the left, and navigation links for 'Why Google', 'Solutions', 'Products', 'Pricing', 'Docs', 'Support', 'English', and 'Console' are on the right. Below this is a 'Google Cloud' header with a 'Contact Us' button. The main section is titled 'Google Cloud Pricing Calculator' with a note that prices are up to date as of 20-December-2021. A horizontal menu shows various services: COMPUTE ENGINE (selected), GKE STANDARD, GKE AUTOPILOT, CLOUD RUN, ANTHOS, and VMWARE ENGINE. Below the menu is a search bar. On the left, under the 'Instances' section, there is a field for 'Number of instances' with a dropdown arrow and a help icon. On the right, the 'Estimate' section for 'Compute Engine' shows the following details: 1 x fun (with a document icon, edit icon, and delete icon), Region: Toronto, 212.917 total hours per month, VM class: regular, and Instance type: e2-medium with a price of USD 7.85. A chat bubble icon is visible on the right side of the interface.

Google Cloud Pricing Calculator Prices are up to date. Last update: 20-December-2021

COMPUTE ENGINE GKE STANDARD GKE AUTOPILOT CLOUD RUN ANTHOS VMWARE ENGINE

Search for a product you are interested in.

Instances

Number of instances \*

Estimate

Compute Engine

1 x fun

Region: Toronto

212.917 total hours per month

VM class: regular

Instance type: e2-medium USD 7.85



# 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](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.

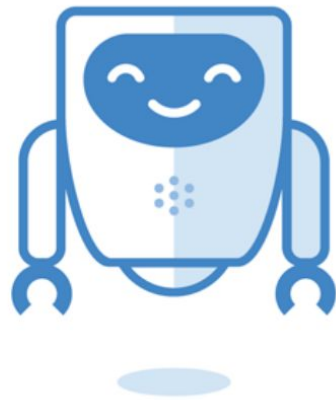
```
$ curl -H "Metadata-Flavor:Google" \  
  metadata.google.internal/computeMetadata/
```

```
$ 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 service.
- Think of it as a service bot for enabling automation.

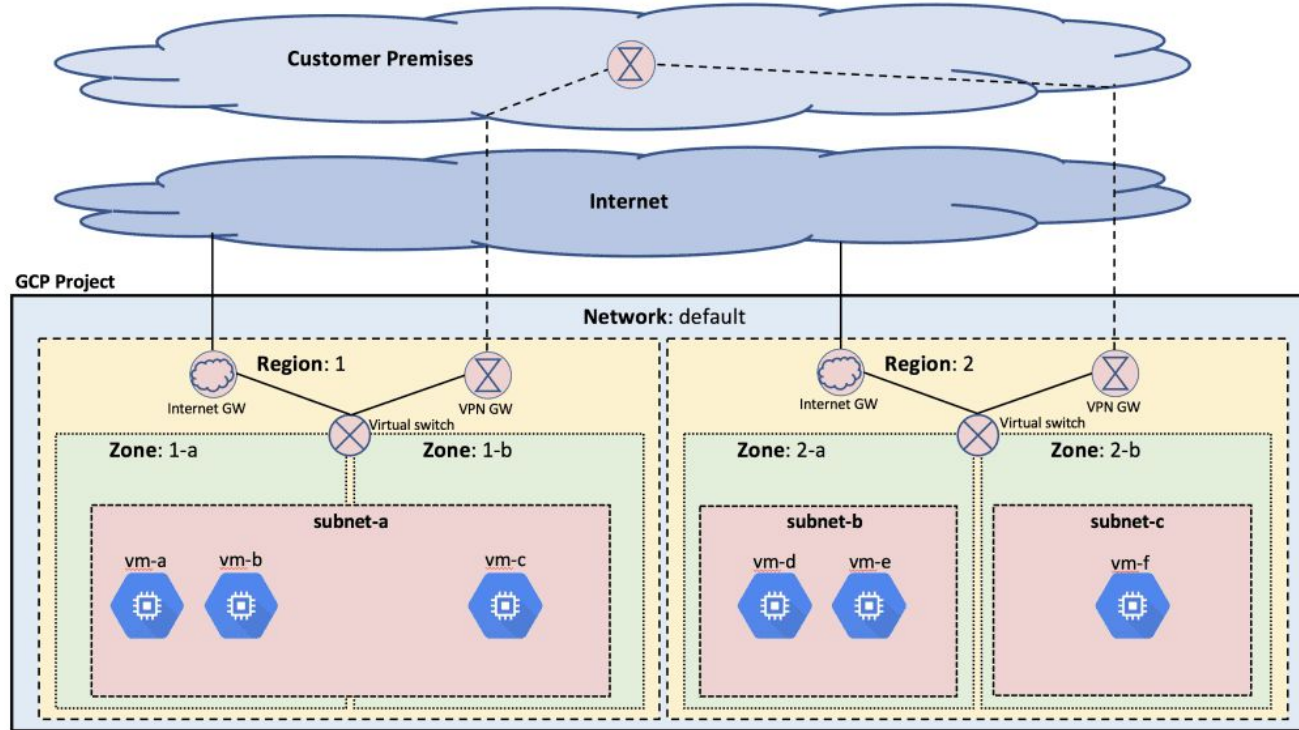




# GCP Virtual Private Cloud

- 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.
  - Public IPv6 /?, if dual stack is enabled.
- You VM can communicate in the VPC privately.
  - This privacy extends across the global if you're using VMs in different regions.
- Global VPC abstracts complexities encountered with on-prem global networks.

# Virtual Private Cloud



# GCE IPv6 Support

- Yes, GCE can support IPv6.
- Check the presentation cheat sheet for more details:
  - <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.
- Alert on metrics and logs.
- Error Reports, Debugging, and Profiling services also available.



# GCP Cloud Logging

Google Cloud Platform

playground-s-11-a8cfc84c

Search Products, resources, docs (/)

Operations Logging

Logs Explorer

Logs Dashboard

Logs-based Metrics

Logs Router

Logs Storage

Release Notes

Logs Explorer

OPTIONS

REFINE SCOPE Project

SHARE LINK

LAST 1 HOUR

LEARN

New features are available in the Logs Explorer.

Dismiss

Learn more

Query

Recent (1)

Saved (0)

Suggested (0)

Clear query

Save

Stream logs

Run query

Edit query

Log fields

Histogram

Create metric

Create alert

Jump to now

More actions

Query results

27 log entries

Download

SEVERITY

TIMESTAMP

PST

SUMMARY

EDIT

Showing logs for last 1 hour from 1/22/22, 9:42 AM to 1/22/22, 10:42 AM.

Extend time by: 1 hour

Edit time

>	i	2022-01-22 10:18:10.967 PST	compute.googleapis.com	beta.compute.instances.insert	...
>	i	2022-01-22 10:18:23.177 PST	6400722196012070028	{"@type": "type.googleapis.com/cloud.integrity.IntegrityEvent", "bootCount...	
>	i	2022-01-22 10:18:23.661 PST	compute.googleapis.com	beta.compute.instances.insert	...
>	i	2022-01-22 10:18:24.646 PST	6400722196012070028	{"@type": "type.googleapis.com/cloud.integrity.IntegrityEvent", "bootCount...	
>	i	2022-01-22 10:18:30.649 PST	6400722196012070028	"OSConfig Agent (version 20211117.00-g1) started."	
>	i	2022-01-22 10:18:30.741 PST	6400722196012070028	"GCE Agent Started (version 20211116.00)"	
>	i	2022-01-22 10:18:30.932 PST	6400722196012070028	"Instance ID changed, running first-boot actions"	



# 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
- Log Viewer available to visualize, monitor, analyze, and alert.

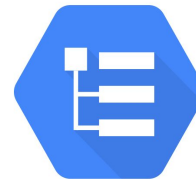


# GCP Audit Logs

- 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
- System events and admin activity are immutable and written automatically.
  - No control over these 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



Google Cloud Platform playground-s-11-f1560673 audit logs

DASHBOARD ACTIVITY RECOMMENDATIONS

Project info

- Project name: playground-s-11-f1560673
- Project number: 946551046705
- Project ID: playground-s-11-f1560673

ADD PEOPLE TO THIS PROJECT

Go to project settings

Compute Engine

CPU (%)

100% 80% 60% 40% 20% 0%

8:30 8:45 9 AM 9:15

Notifications

- Create VM instance "instance-1" and its boot disk "instance-1" 39 minutes ago playground-s-11-f1560673

SEE ALL ACTIVITIES

Go to Cloud status dashboard

Billing

Estimated charges For the billing period Jan 1 – 9, 2022 USD \$0.00

Take a tour of billing

To access audit logs

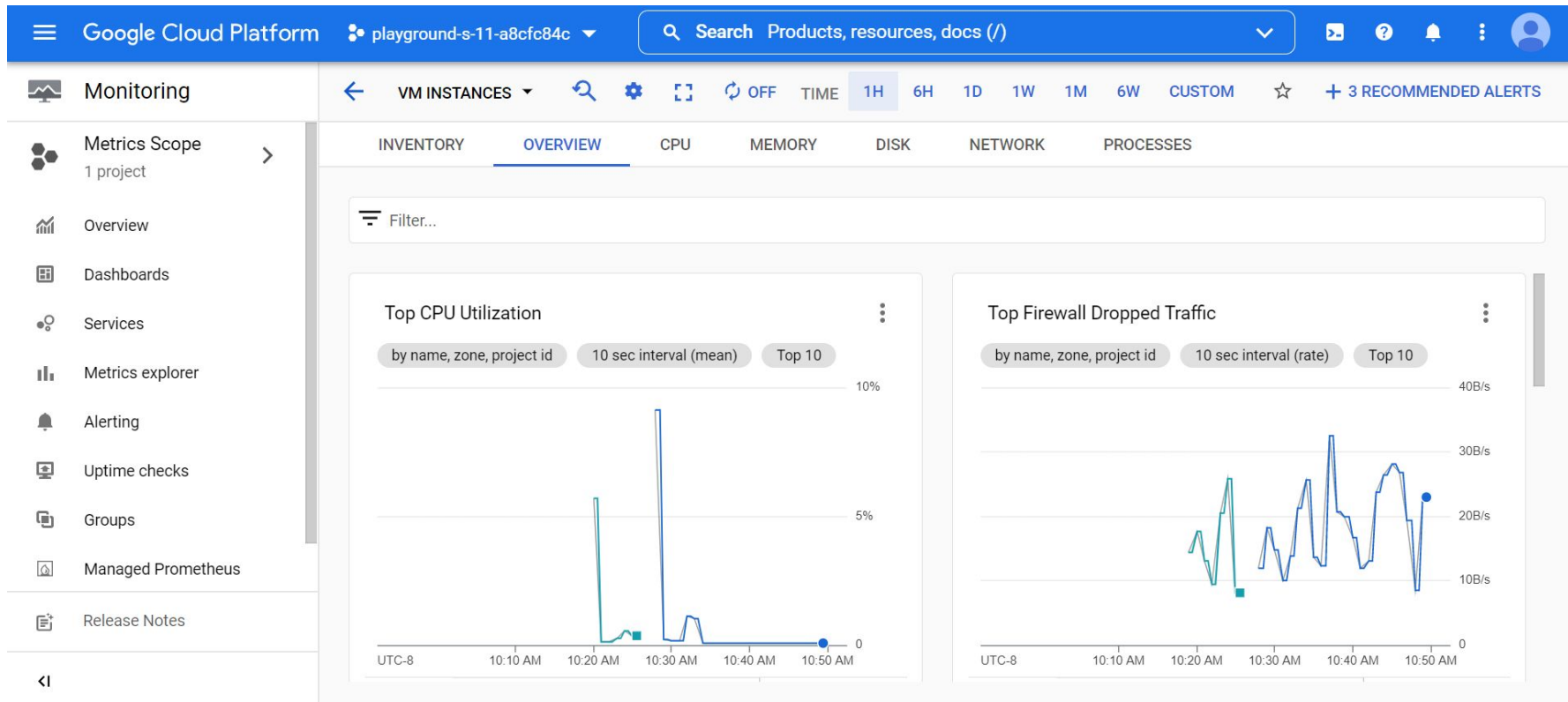
Google Cloud Platform playground-s-11-f1560673 Search products and resources

DASHBOARD ACTIVITY RECOMMENDATIONS

Today

9:06 AM	Completed: Set metadata on project	cloud_user_p_955f921d@linuxacademygclabs.com set metadata on project playground-s-11-f1560673	▼
9:06 AM	Set metadata on project	cloud_user_p_955f921d@linuxacademygclabs.com set metadata on project playground-s-11-f1560673	▼
9:03 AM	Completed: Create VM	cloud_user_p_955f921d@linuxacademygclabs.com created instance-1	▼
9:03 AM	Create VM	cloud_user_p_955f921d@linuxacademygclabs.com created instance-1	▼
9:01 AM	Update project	919628400850@cloudservices.gserviceaccount.com updated playground-s-11-f1560673	▼
7:46 AM	Completed: google.api.serviceusage.v1beta1.ServiceUsage.ImportConsumerO...	google.api.serviceusage.v1beta1.ServiceUsage.ImportConsumerOverrides was executed on compute.googleapis.com	▼

# GCP Cloud Monitoring



# GCP Trial Account & Free Tier

## Trial Account

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

## Free Tier

- Offered for various GCP services.
- Usage limits applied before the charging begins.
- <https://cloud.google.com/free/docs/gcp-free-tier/#free-tier-usage-limits>
- **Note** - Set up billing alerts and MFA for peace of mind.

# Summary

- If you're looking for cloud solutions, Google Cloud is a compelling choice.
  - A test account gives you a \$300 credit trial their services.
  - It's worth a test drive.
- 
- Github Repo
    - <https://github.com/netserf/netsig-presentation-gcp-for-newbies>

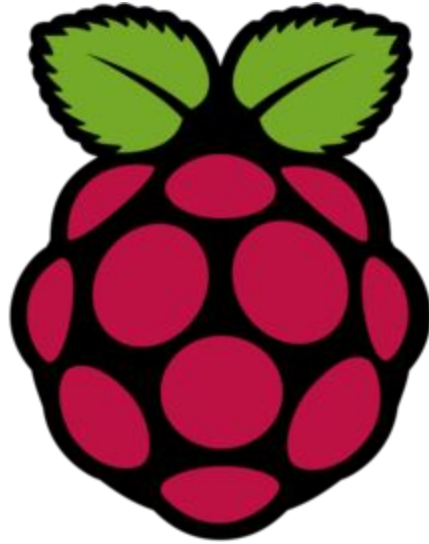
# Possible Future Discussions

- Kubernetes Engine
- Cloud DNS
- App Engine
- Cloud Load Balancer
- Cloud Pub/Sub
- Cloud Functions
- Cloud Operations Suite
- Database services
- Machine Learning services



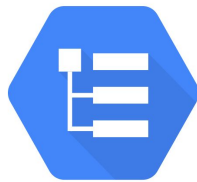
# VicPiMakers and Others Slack

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



# Backup Slides





# GCP Cloud Logging

On a provisioned VM:

```
$ ps -ef | grep agent
```

Retrofit the cloud ops agents via the console:

```
$ ps -ef | grep agent
```

Show logs in Log Viewer ... do I need to install agent as well?

Try:

```
logger -p "local1.err" "JUST A TEST"
```

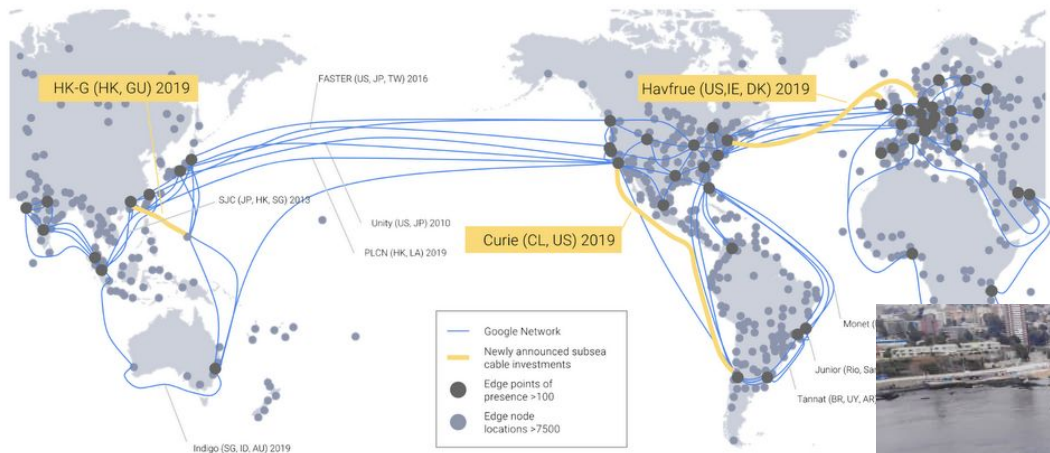
Check in Log Viewer for message.



# Google's Network

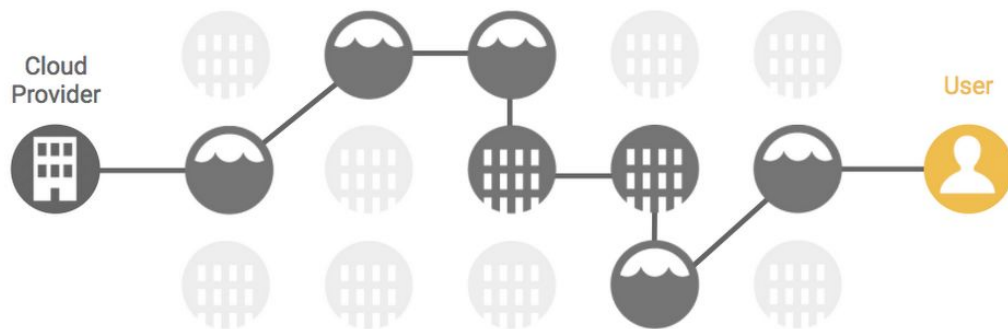
## Google Network

The largest cloud network, comprised of more than 100 points of presence



# Google's Network

Public Internet – other cloud providers



Google Network



# Cloud Shell - gsutil

## GCP SDK - gsutil

```
$ gsutil ls
```

```
$ gsutil mb gs://my-gsutil-demo-23711
```

```
$ gsutil ls
```

```
$ gsutil cp foo gs://my-gsutil-demo-23711
```

```
$ gsutil ls gs://my-gsutil-demo-23711
```

```
$ gsutil cp gs://my-gsutil-demo-23711/foo bar
```

```
$ cat bar
```