

Google Cloud for Newbies



Greg Horie

github.com/netserf

... for Newbies

Because I'm
new too !



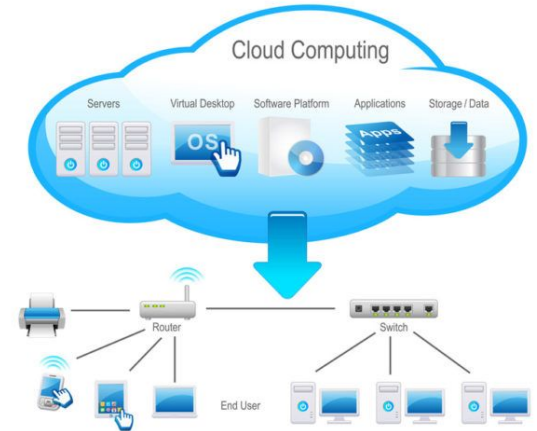
Overview

- 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.

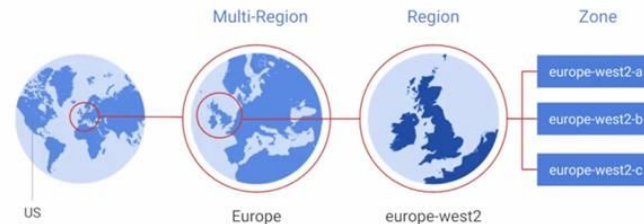


Regions and Zones

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 Regions and Zones

Google Cloud Platform is organized into regions and zones



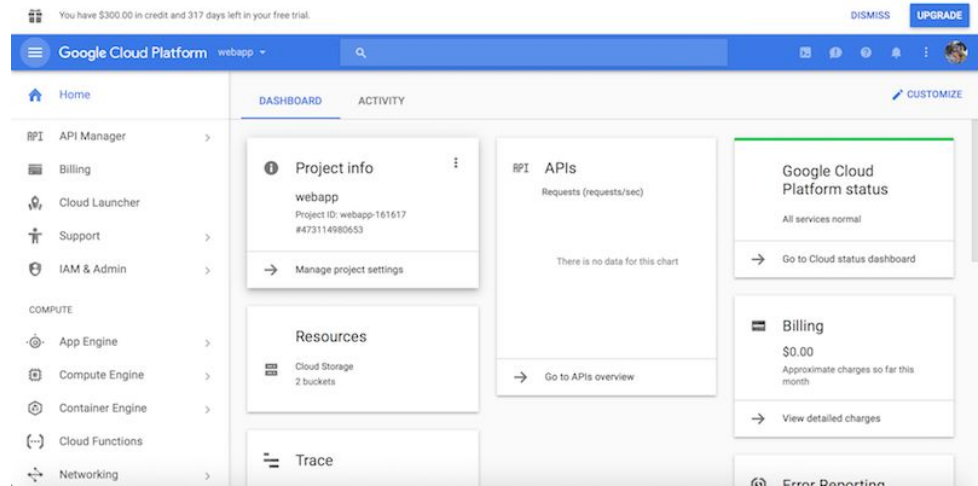
GCP Admin Tools

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



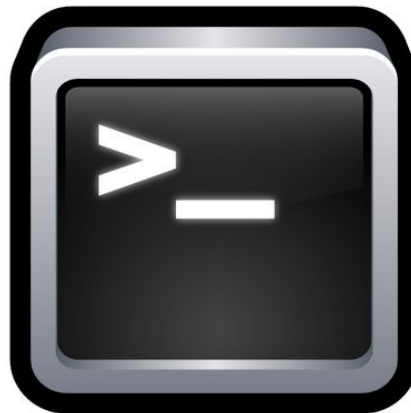
GCP Cloud Console

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



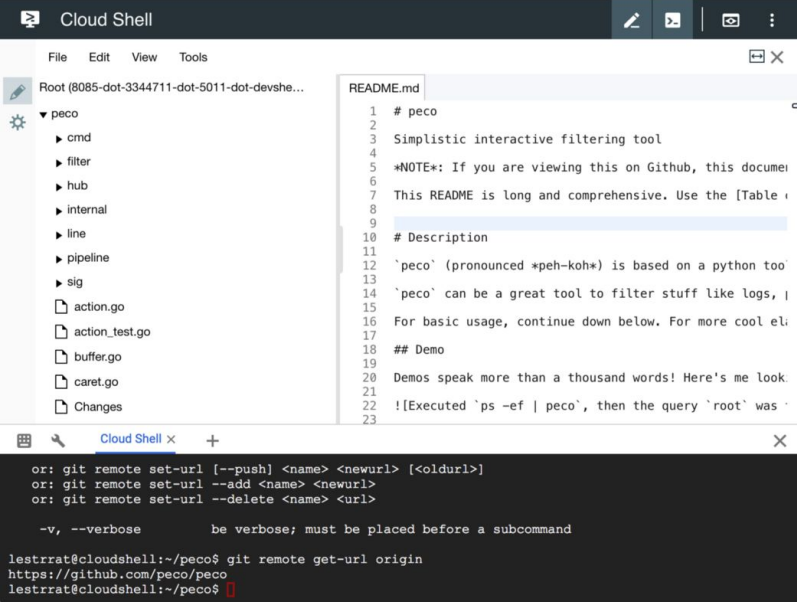
GCP SDK

- 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.



The screenshot displays the GCP Cloud Shell environment. At the top, there's a dark header with the 'Cloud Shell' title and navigation icons. Below it is a menu bar with 'File', 'Edit', 'View', and 'Tools'. A file explorer on the left shows a directory structure for a project named 'peco', including 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 main area 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, a terminal window shows the following commands and output:

```
lestrrat@cloudshell:~/peco$ 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

Networking Packages

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

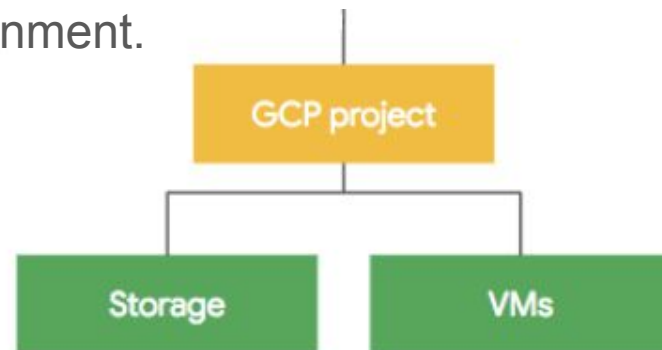
```
$ gcloud config set compute/region us-west1
```

```
$ 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 demarcates 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

The screenshot shows the Google Cloud Platform interface. At the top, the header includes the Google Cloud Platform logo, the project ID 'playground-s-11-cc884f0c', a search bar for products and resources, and user profile icons. The left sidebar contains the 'IAM & Admin' menu, with 'Settings' highlighted. The main content area is titled 'Settings' and includes 'MOVE' and 'SHUT DOWN' buttons. It features three input fields: 'Project name *' (playground-s-11-cc884f0c), 'Project ID' (playground-s-11-cc884f0c), and 'Project number' (708512446115). Below these is the 'Access Transparency' section, which includes a note that the feature is not available for projects not part of an organization.

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.

The screenshot shows the Google Cloud Platform interface for the Compute Engine VM instances page. The top navigation bar includes the Google Cloud Platform logo, the account ID 'playground-s-11-cc884f0c', a search bar, and user profile icons. The main header shows 'Compute Engine' and 'VM instances' with a red box around the 'CREATE INSTANCE' button. A red arrow points to this button. Below the header is a filter bar and a table with columns for Status, Name, Zone, Recommendations, In use, External IP, and Connect. The main content area features a large graphic of a globe with a chip icon and the text 'VM Instances' and 'Compute Engine lets you use virtual machines that run on Google's infrastructure. Create micro-VMs or larger instances running Debian, Windows,'.

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', and 'Pric >' are in the center. On the right, there are links for 'Docs', 'Support', a language dropdown set to 'English', and a 'Console' button. A user profile icon with the letter 'G' is also present.

Below the navigation bar, the text 'Google Cloud' is on the left, and a 'Contact Us' button is on the right.

The main content area is titled 'Google Cloud Pricing Calculator' in a blue header. To the right of the title, it says 'Prices are up to date. Last update: 20-December-2021'. Below the header, there is a row of product icons: COMPUTE ENGINE (highlighted with a red underline), GKE STANDARD, GKE AUTOPILOT, CLOUD RUN, ANTHOS, and VMWARE ENGINE.

Below the product icons is a search bar with the placeholder text 'Search for a product you are interested in.' and a magnifying glass icon.

Under the search bar, there is a section titled 'Instances' with a dropdown menu and a question mark icon. The text 'Number of instances *' is visible next to the dropdown.

On the right side of the interface, there is an 'Estimate' panel. It has a blue header and a grey sub-header 'Compute Engine'. Below this, it shows the following details:

- 1 x fun (with a document icon, a pencil icon, and a red 'x' icon)
- Region: Toronto
- 212.917 total hours per month
- VM class: regular
- Instance type: e2-medium USD 7.85

At the bottom right of the interface, there is a blue circular chat icon with a white speech bubble.



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
```

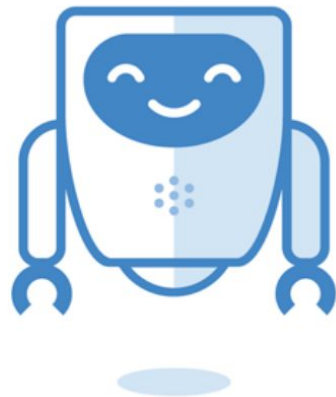
- IPv4 link local address - https://en.wikipedia.org/wiki/Link-local_address
 - i.e. only valid for communications inside the local network (broadcast domain).
 - Routers will not forward outside the local network.
- Metadata endpoint provides useful information for the local compute node.

```
$ 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.

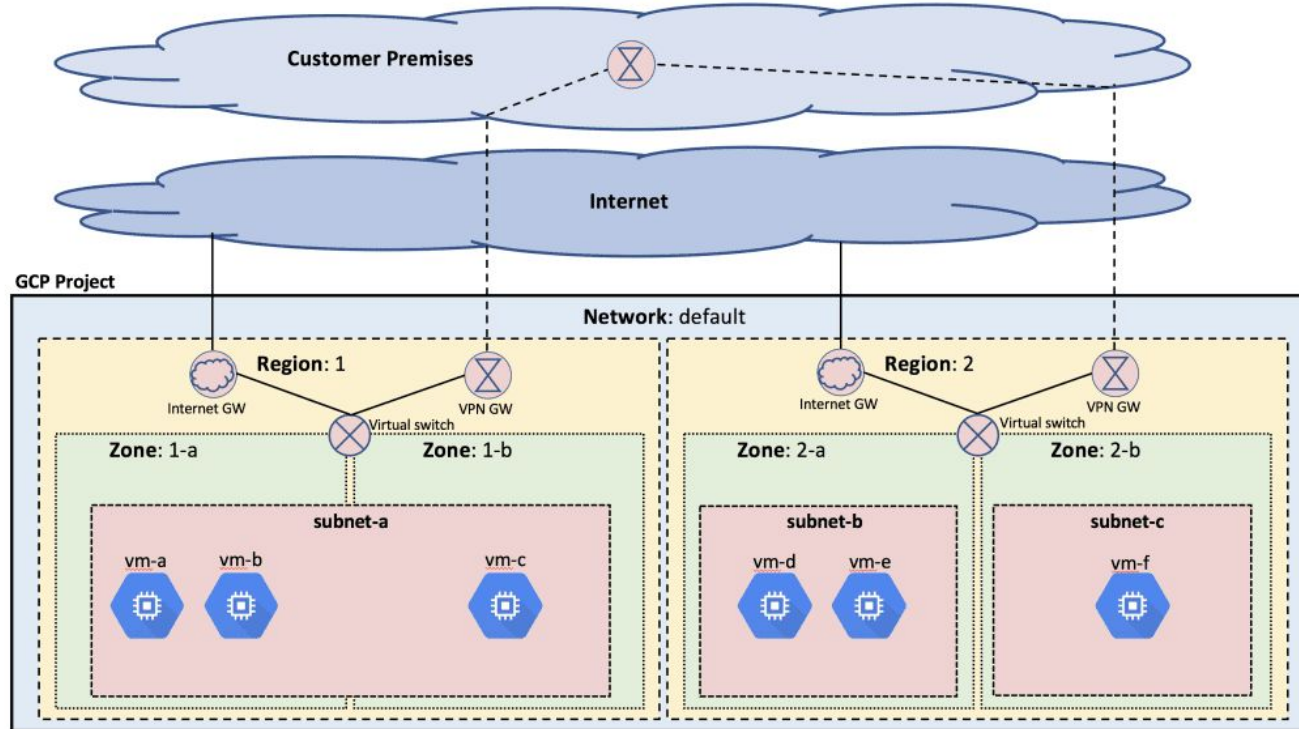




GCP Virtual Private Cloud

- 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

Google Cloud Platform playground-s-11-2e47d096 Search Products, resources, docs (/)

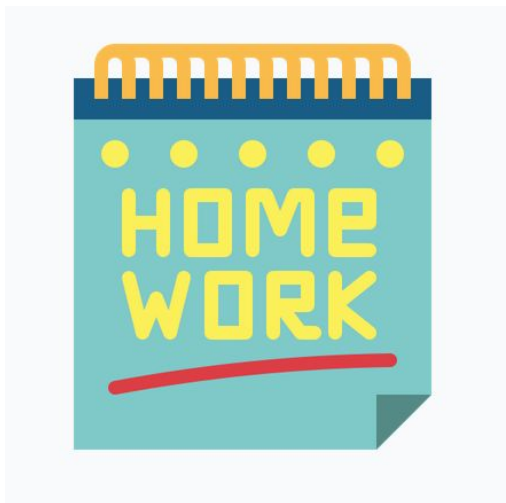
VPC network VPC networks + CREATE VPC NETWORK REFRESH

- VPC networks
- External IP addresses
- Bring your own IP
- Firewall
- Routes
- VPC network peering
- Shared VPC
- Serverless VPC access
- Packet mirroring

Name ↑	Region	Subnets	MTU ?	Mode	IP address ranges	Gateways	Firewall Rules	Global dynamic routing
▼ default		9	1460	Auto			4	Off
	us-central1	default			10.128.0.0/20	10.128.0.1		
	europa-west1	default			10.132.0.0/20	10.132.0.1		
	us-west1	default			10.138.0.0/20	10.138.0.1		
	us-east1	default			10.142.0.0/20	10.142.0.1		
	us-east4	default			10.150.0.0/20	10.150.0.1		
	australia-southeast1	default			10.152.0.0/20	10.152.0.1		
	us-west2	default			10.168.0.0/20	10.168.0.1		
	us-west3	default			10.180.0.0/20	10.180.0.1		
	us-west4	default			10.182.0.0/20	10.182.0.1		

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

The screenshot shows the Google Cloud Platform (GCP) Logs Explorer interface. At the top, there is a navigation bar with the Google Cloud Platform logo, the project name 'playground-s-11-a8cfc84c', a search bar, and user profile icons. The left sidebar contains navigation options: Operations Logging, Logs Explorer (selected), Logs Dashboard, Logs-based Metrics, Logs Router, and Logs Storage. The main content area is titled 'Logs Explorer' and includes an 'OPTIONS' dropdown, 'REFINE SCOPE' button, 'SHARE LINK', 'LAST 1 HOUR' filter, and 'LEARN' link. A notification banner states 'New features are available in the Logs Explorer.' Below this, the query bar shows 'resource.type=gce_instance' with options for 'Query', 'Recent (1)', 'Saved (0)', and 'Suggested (0)'. There are buttons for 'Clear query', 'Save', 'Stream logs', and 'Run query'. Below the query bar, there are options for 'Log fields', 'Histogram', 'Create metric', 'Create alert', 'Jump to now', and 'More actions'. The 'Query results' section shows '27 log entries' with a 'Download' button. The log entries are displayed in a table with columns for SEVERITY, TIMESTAMP, and SUMMARY. The table shows logs from 2022-01-22 10:18:10.967 PST to 10:18:30.932 PST. The log entries include messages from 'compute.googleapis.com' and 'OSConfig Agent'.

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

resource.type=gce_instance 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

SEVERITY	TIMESTAMP	SUMMARY
> 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	"OSConfig Agent (version 20211117.00-g1) started."
> i	2022-01-22 10:18:30.741 PST	"GCE Agent Started (version 20211116.00)"
> i	2022-01-22 10:18:30.932 PST	"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



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



To access audit logs

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

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 (%)

8:30 8:45 9 AM 9:15

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

DASHBOARD ACTIVITY RECOMMENDATIONS FILTER

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

Google Cloud Platform playground-s-11-a8cfc84c Search Products, resources, docs (/)

Monitoring VM INSTANCES 1H 6H 1D 1W 1M 6W CUSTOM + 3 RECOMMENDED ALERTS

INVENTORY OVERVIEW CPU MEMORY DISK NETWORK PROCESSES

Filter...

Top CPU Utilization

by name, zone, project id 10 sec interval (mean) Top 10

Time	CPU Utilization (%)
10:20 AM	~6.5
10:25 AM	~1.5
10:30 AM	~9.5
10:35 AM	~1.5
10:40 AM	~1.5
10:50 AM	~0.5

Top Firewall Dropped Traffic

by name, zone, project id 10 sec interval (rate) Top 10

Time	Firewall Dropped Traffic (B/s)
10:20 AM	~15
10:25 AM	~25
10:30 AM	~15
10:35 AM	~25
10:40 AM	~35
10:45 AM	~25
10:50 AM	~20

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

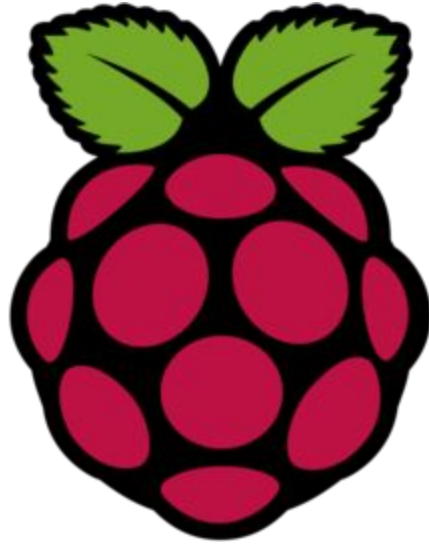
- Send a message with "**subscribe**" in the subject to:

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.



Google Cloud



Azure

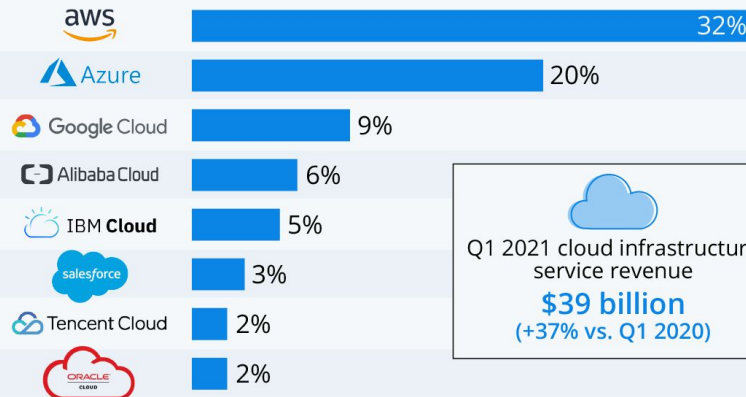
Milestones in Cloud Computing

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

Worldwide market share of leading cloud infrastructure service providers in Q1 2021*



Q1 2021 cloud infrastructure service revenue
\$39 billion
(+37% vs. Q1 2020)

* includes platform as a service (PaaS) and infrastructure as a service (IaaS) as well as hosted private cloud services

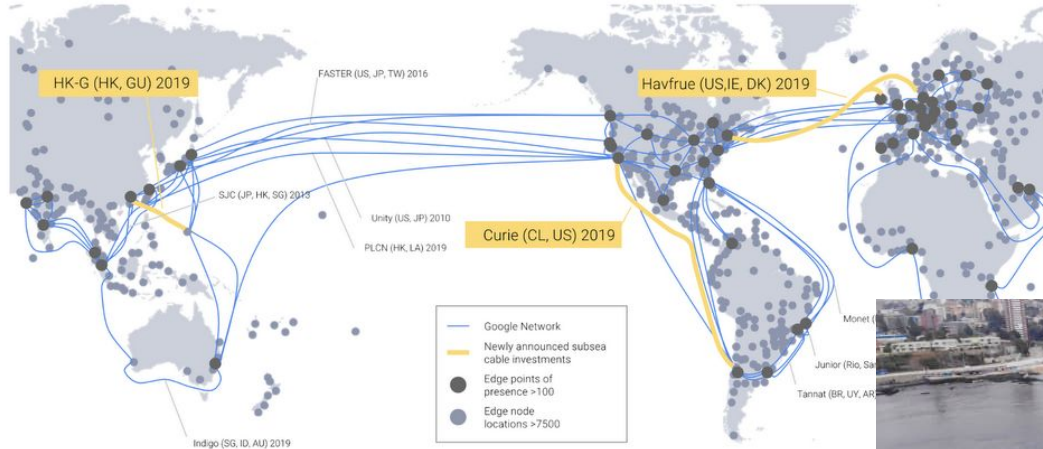
Source: Synergy Research Group



Google's Network

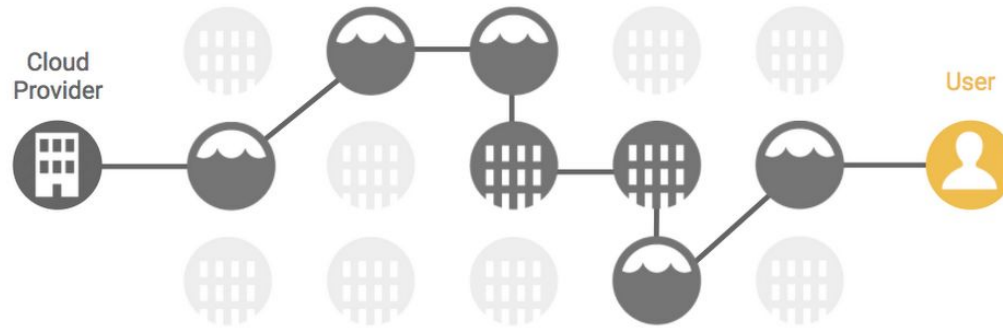
Google Network

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



Google's Network

Public Internet – other cloud providers

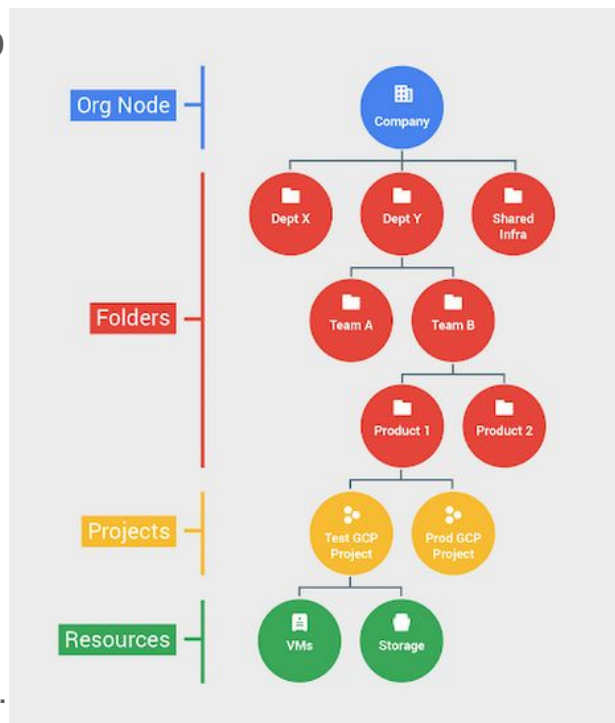


Google Network



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
```