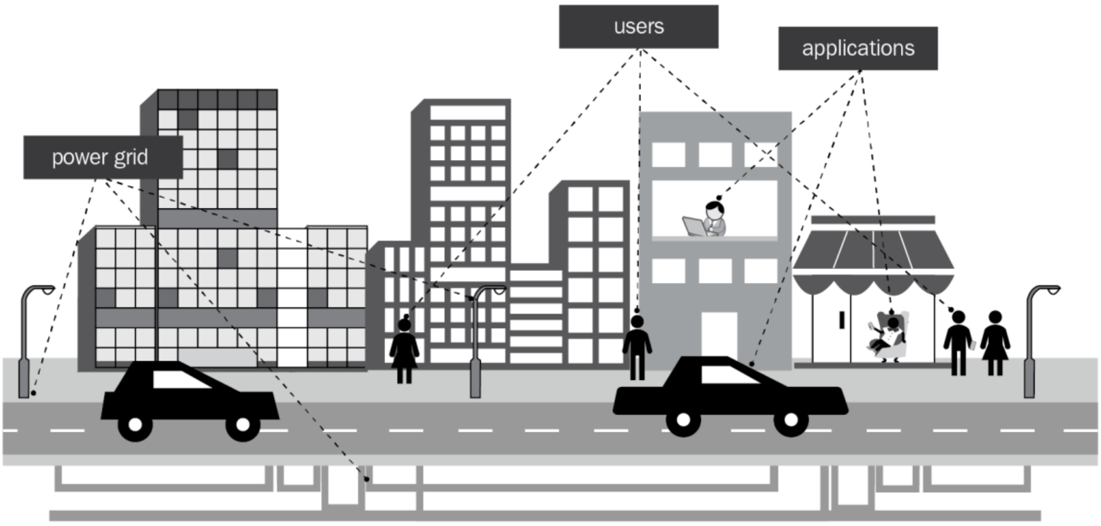
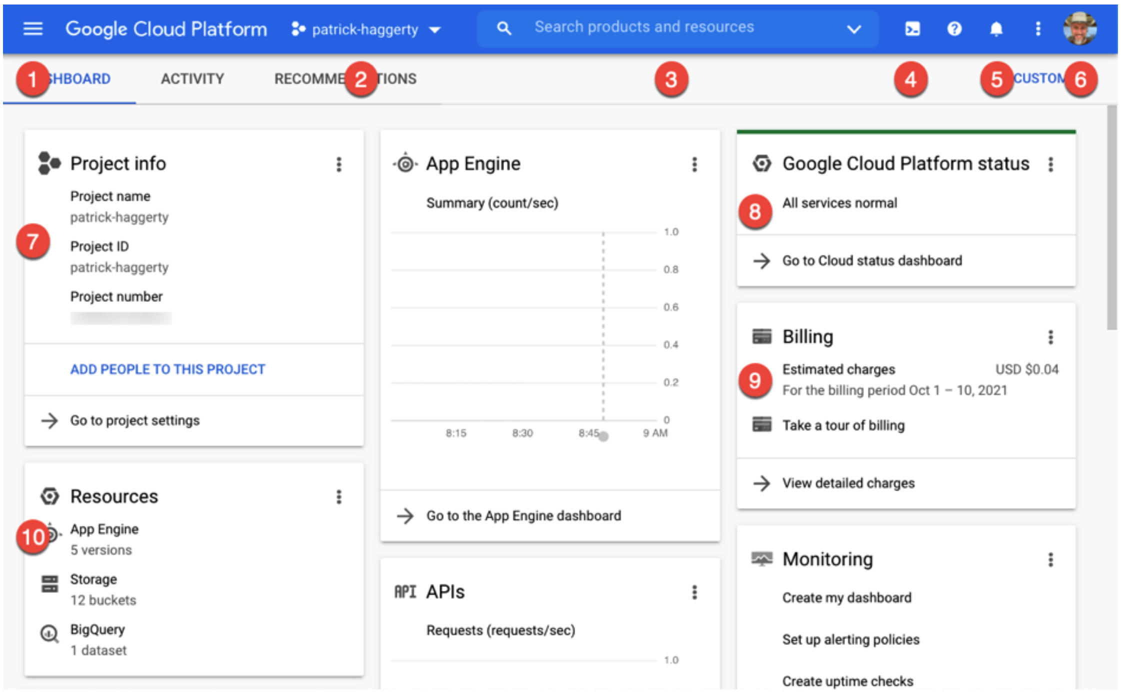
Chapter 1: Getting to Know Google's Cloud





Project info

Project name
patrick-haggerty

Project ID
patrick-haggerty

Project number

ADD PEOPLE TO THIS PROJECT

Go to project settings

Resources

App Engine
5 versions

Storage
12 buckets

BigQuery
1 dataset

App Engine

Summary (count/sec)

1.0 0.8 0.6 0.4 0.2 0

8:15 8:30 8:45 9 AM

Go to the App Engine dashboard

APIs

Requests (requests/sec)

1.0

Google Cloud Platform status

All services normal

Go to Cloud status dashboard

Billing

Estimated charges USD $0.04
For the billing period Oct 1 – 10, 2021

Take a tour of billing

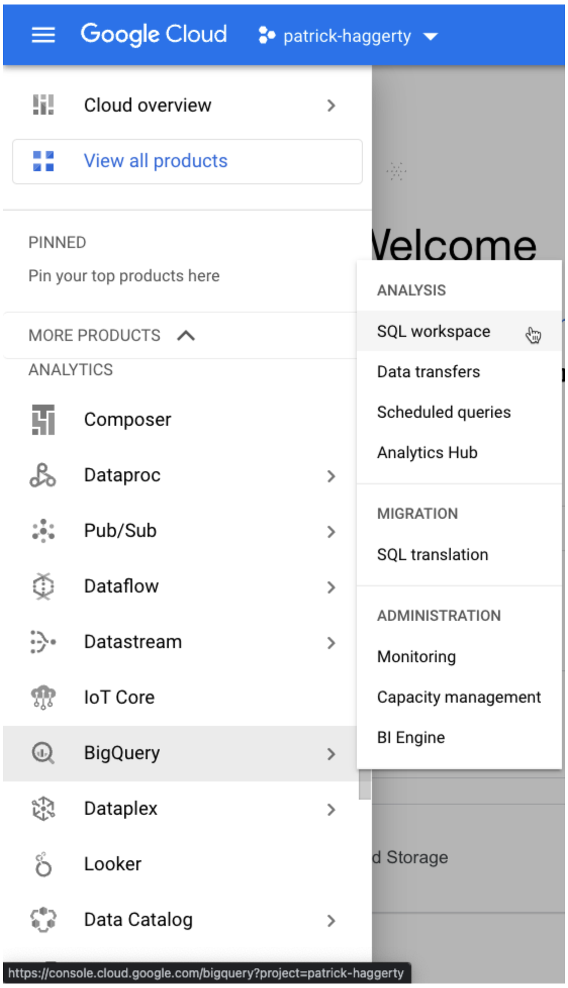
View detailed charges

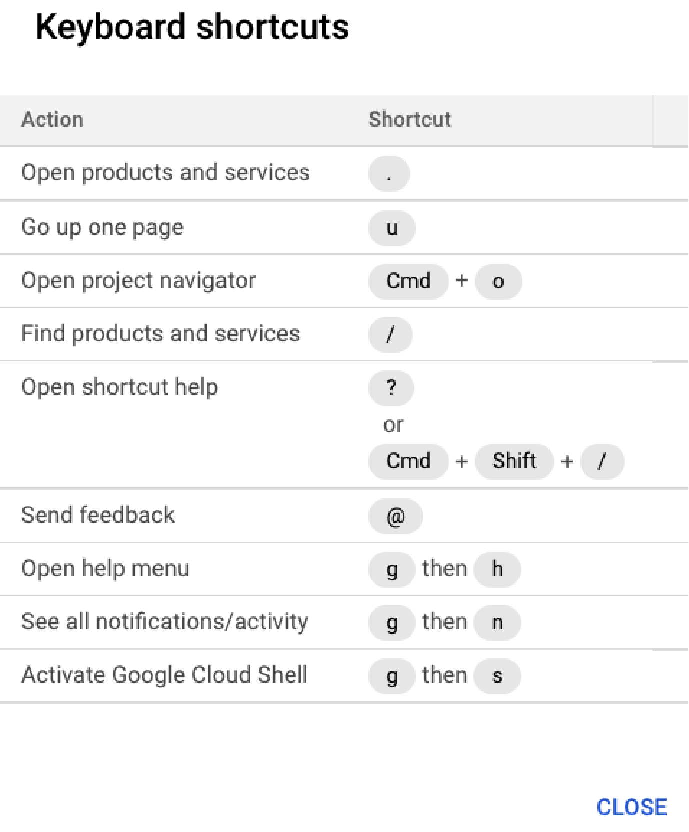
Monitoring

Create my dashboard

Set up alerting policies

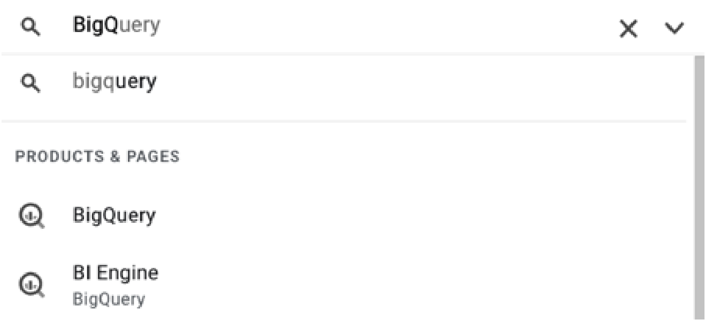
Create uptime checks

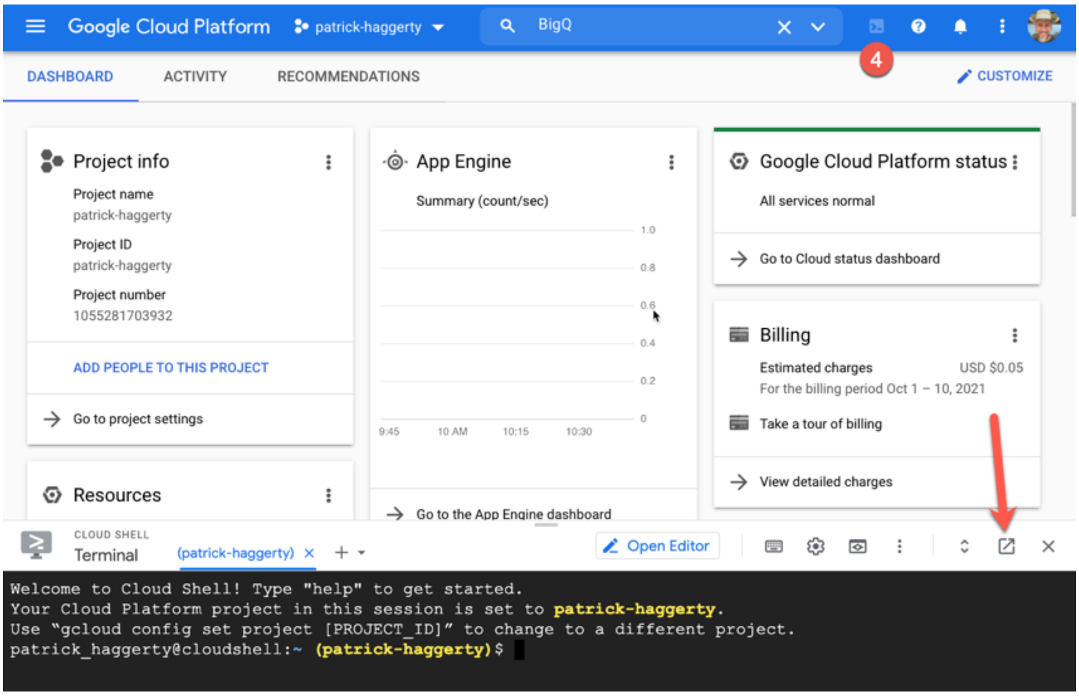




Keyboard shortcuts

Action	Shortcut
Open products and services	.
Go up one page	u
Open project navigator	Cmd + o
Find products and services	/
Open shortcut help	? or Cmd + Shift + /
Send feedback	@
Open help menu	g then h
See all notifications/activity	g then n
Activate Google Cloud Shell	g then s





Project info

Project name
patrick-haggerty

Project ID
patrick-haggerty

Project number
1055281703932

ADD PEOPLE TO THIS PROJECT

Go to project settings

Google Cloud Platform status

All services normal

Go to Cloud status dashboard

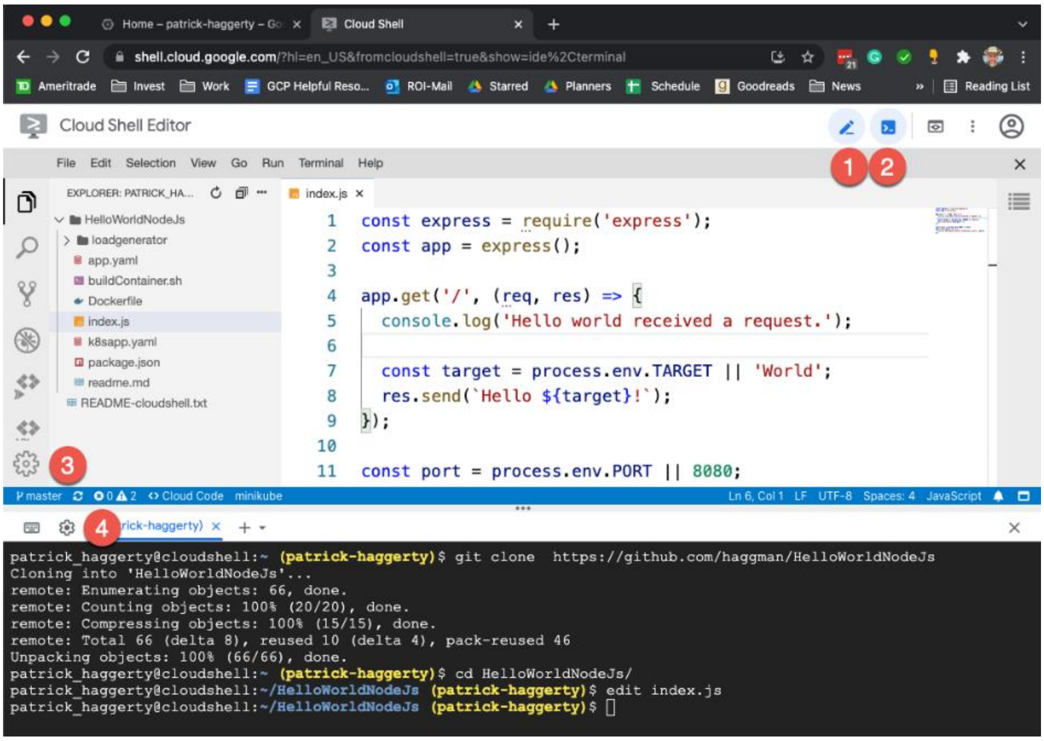
Billing

Estimated charges USD $0.05
For the billing period Oct 1 – 10, 2021

Take a tour of billing

View detailed charges

```
Welcome to Cloud Shell! Type "help" to get started.
Your Cloud Platform project in this session is set to patrick-haggerty.
Use "gcloud config set project [PROJECT_ID]" to change to a different project.
patrick_haggerty@cloudshell:~ (patrick-haggerty)$
```



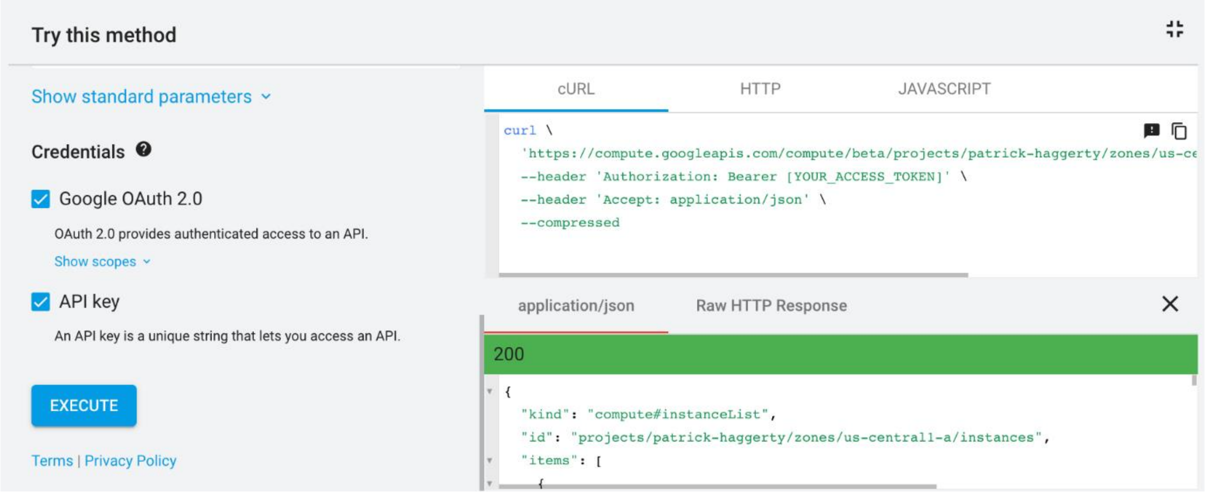
```
const express = require('express');
const app = express();

app.get('/', (req, res) => {
  console.log('Hello world received a request.');

  const target = process.env.TARGET || 'World';
  res.send(`Hello ${target}!`);
});

const port = process.env.PORT || 8080;
```

```
patrick_haggerty@cloudshell:~ (patrick-haggerty)$ git clone  https://github.com/haggman/HelloWorldNodeJs
Cloning into 'HelloWorldNodeJs'...
remote: Enumerating objects: 66, done.
remote: Counting objects: 100% (20/20), done.
remote: Compressing objects: 100% (15/15), done.
remote: Total 66 (delta 8), reused 10 (delta 4), pack-reused 46
Unpacking objects: 100% (66/66), done.
patrick_haggerty@cloudshell:~ (patrick-haggerty)$ cd HelloWorldNodeJs/
patrick_haggerty@cloudshell:~/HelloWorldNodeJs (patrick-haggerty)$ edit index.js
patrick_haggerty@cloudshell:~/HelloWorldNodeJs (patrick-haggerty)$
```



Try this method

Show standard parameters

Credentials

☑ Google OAuth 2.0

OAuth 2.0 provides authenticated access to an API.

Show scopes

☑ API key

An API key is a unique string that lets you access an API.

EXECUTE

Terms | Privacy Policy

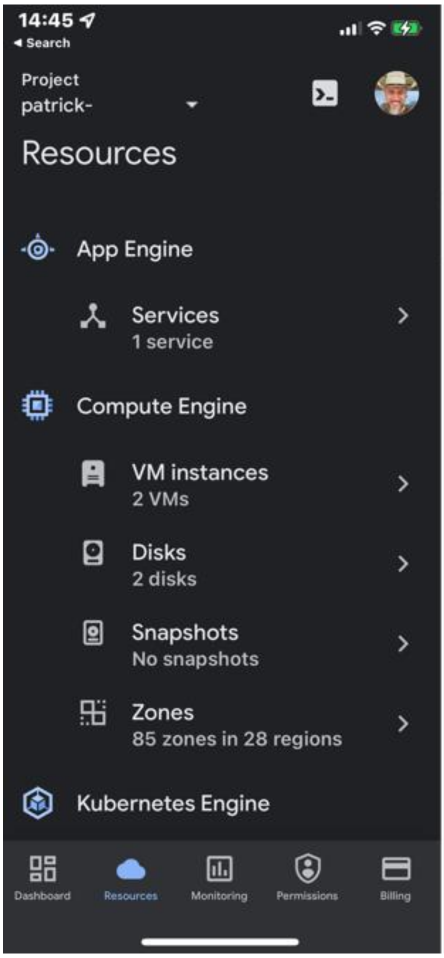
cURL | HTTP | JAVASCRIPT

```
curl \
  'https://compute.googleapis.com/compute/beta/projects/patrick-haggerty/zones/us-ce
  --header 'Authorization: Bearer [YOUR_ACCESS_TOKEN]' \
  --header 'Accept: application/json' \
  --compressed
```

application/json | Raw HTTP Response

200

```
{
  "kind": "compute#instanceList",
  "id": "projects/patrick-haggerty/zones/us-central1-a/instances",
  "items": [
    {
```



14:45
◂ Search

Project
patrick-

Resources

App Engine

Services
1 service

Compute Engine

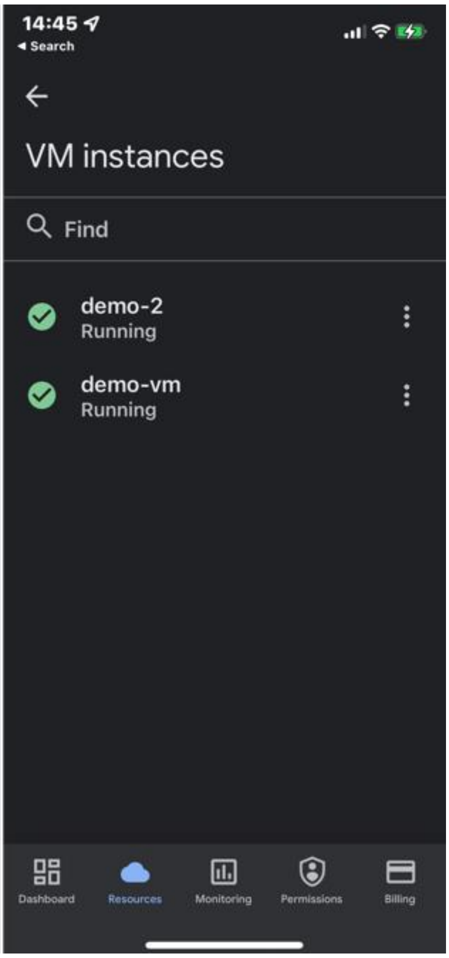
VM instances
2 VMs

Disks
2 disks

Snapshots
No snapshots

Zones
85 zones in 28 regions

Kubernetes Engine



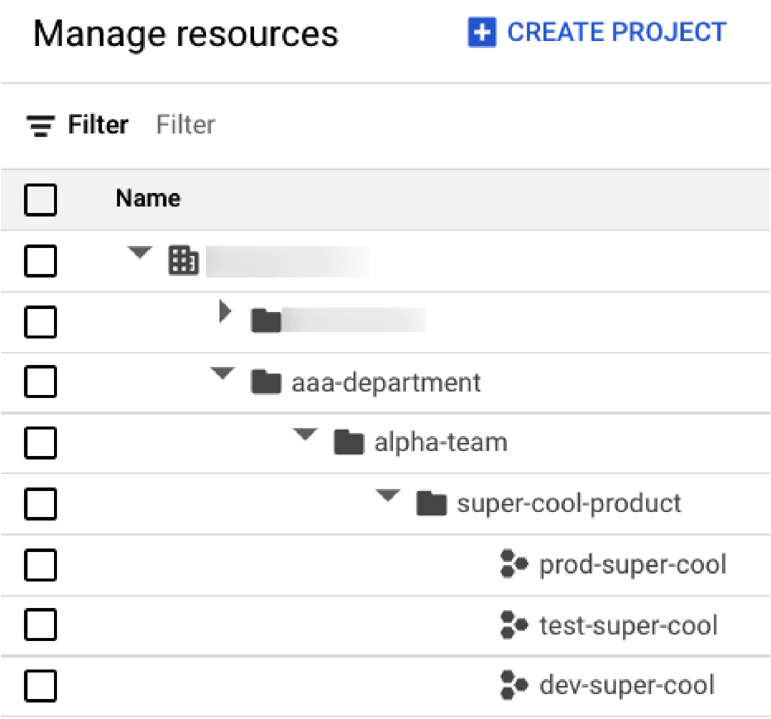
14:45
◂ Search

VM instances

Find

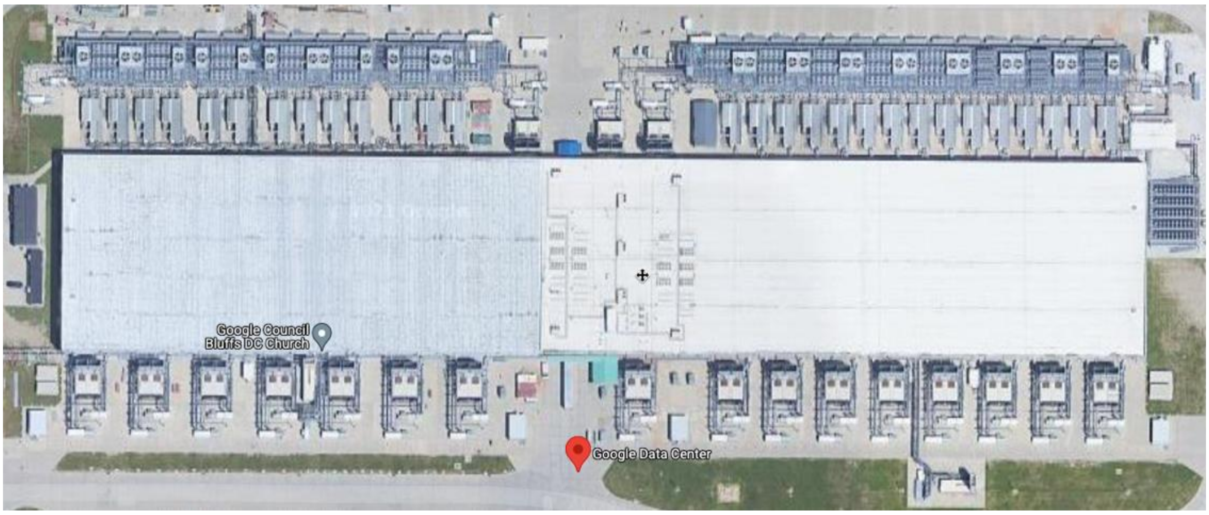
demo-2
Running

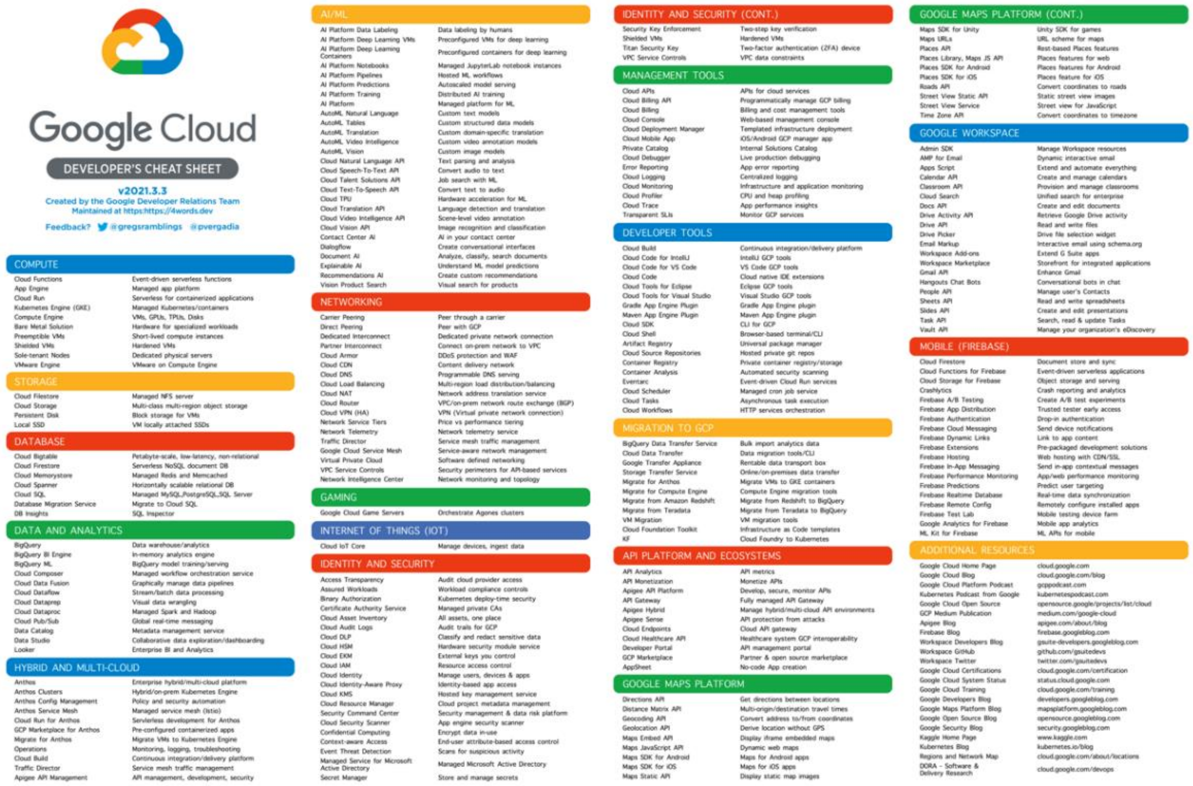
demo-vm
Running



Manage resources

□	Name
□	▾ [redacted]
□	▸ [redacted]
□	▾ aaa-department
□	▾ alpha-team
□	▾ super-cool-product
□	prod-super-cool
□	test-super-cool
□	dev-super-cool





Google Cloud

DEVELOPER'S CHEAT SHEET

v2021.3.3
Created by the Google Developer Relations Team
Maintained at https:https://4words.dev

Feedback? @gregsramblings @pvergadia

COMPUTE

Cloud Functions	Event-driven serverless functions
App Engine	Managed app platform
Cloud Run	Serverless for containerized applications
Kubernetes Engine (GKE)	Managed Kubernetes/containers
Compute Engine	VMs, GPUs, TPUs, Disks
Bare Metal Solution	Hardware for specialized workloads
Preemptible VMs	Short-lived compute instances
Shielded VMs	Hardened VMs
Sole-tenant Nodes	Dedicated physical servers
VMware Engine	VMware on Compute Engine

STORAGE

Cloud Filestore	Managed NFS server
Cloud Storage	Multi-class multi-region object storage
Persistent Disk	Block storage for VMs
Local SSD	VM locally attached SSDs

DATABASE

Cloud Bigtable	Petabyte-scale, low-latency, non-relational
Cloud Firestore	Serverless NoSQL document DB
Cloud Memorystore	Managed Redis and Memcached
Cloud Spanner	Horizontally scalable relational DB
Cloud SQL	Managed MySQL,PostgreSQL,SQL Server
Database Migration Service	Migrate to Cloud SQL
DB Insights	SQL Inspector

DATA AND ANALYTICS

BigQuery	Data warehouse/analytics
BigQuery BI Engine	In-memory analytics engine
BigQuery ML	BigQuery model training/serving
Cloud Composer	Managed workflow orchestration service
Cloud Data Fusion	Graphically manage data pipelines
Cloud Dataflow	Stream/batch data processing
Cloud Dataprep	Visual data wrangling
Cloud Dataproc	Managed Spark and Hadoop
Cloud Pub/Sub	Global real-time messaging
Data Catalog	Metadata management service
Data Studio	Collaborative data exploration/dashboarding
Looker	Enterprise BI and Analytics

HYBRID AND MULTI-CLOUD

Anthos	Enterprise hybrid/multi-cloud platform
Anthos Clusters	Hybrid/on-prem Kubernetes Engine
Anthos Config Management	Policy and security automation
Anthos Service Mesh	Managed service mesh (Istio)
Cloud Run for Anthos	Serverless development for Anthos
GCP Marketplace for Anthos	Pre-configured containerized apps
Migrate for Anthos	Migrate VMs to Kubernetes Engine
Operations	Monitoring, logging, troubleshooting
Cloud Build	Continuous integration/delivery platform
Traffic Director	Service mesh traffic management
Apigee API Management	API management, development, security

AI/ML

AI Platform Data Labeling	Data labeling by humans
AI Platform Deep Learning VMs	Preconfigured VMs for deep learning
AI Platform Deep Learning Containers	Preconfigured containers for deep learning
AI Platform Notebooks	Managed JupyterLab notebook instances
AI Platform Pipelines	Hosted ML workflows
AI Platform Predictions	Autoscaled model serving
AI Platform Training	Distributed AI training
AI Platform	Managed platform for ML
AutoML Natural Language	Custom text models
AutoML Tables	Custom structured data models
AutoML Translation	Custom domain-specific translation
AutoML Video Intelligence	Custom video annotation models
AutoML Vision	Custom image models
Cloud Natural Language API	Text parsing and analysis
Cloud Speech-To-Text API	Convert audio to text
Cloud Talent Solutions API	Job search with ML
Cloud Text-To-Speech API	Convert text to audio
Cloud TPU	Hardware acceleration for ML
Cloud Translation API	Language detection and translation
Cloud Video Intelligence API	Scene-level video annotation
Cloud Vision API	Image recognition and classification
Contact Center AI	AI in your contact center
Dialogflow	Create conversational interfaces
Document AI	Analyze, classify, search documents
Explainable AI	Understand ML model predictions
Recommendations AI	Create custom recommendations
Vision Product Search	Visual search for products

NETWORKING

Carrier Peering	Peer through a carrier
Direct Peering	Peer with GCP
Dedicated Interconnect	Dedicated private network connection
Partner Interconnect	Connect on-prem network to VPC
Cloud Armor	DDoS protection and WAF
Cloud CDN	Content delivery network
Cloud DNS	Programmable DNS serving
Cloud Load Balancing	Multi-region load distribution/balancing
Cloud NAT	Network address translation service
Cloud Router	VPC/on-prem network route exchange (BGP)
Cloud VPN (HA)	VPN (Virtual private network connection)
Network Service Tiers	Price vs performance tiering
Network Telemetry	Network telemetry service
Traffic Director	Service mesh traffic management
Google Cloud Service Mesh	Service-aware network management
Virtual Private Cloud	Software defined networking
VPC Service Controls	Security perimeters for API-based services
Network Intelligence Center	Network monitoring and topology

GAMING

Google Cloud Game Servers	Orchestrate Agones clusters

INTERNET OF THINGS (IOT)

Cloud IoT Core	Manage devices, ingest data

IDENTITY AND SECURITY

Access Transparency	Audit cloud provider access
Assured Workloads	Workload compliance controls
Binary Authorization	Kubernetes deploy-time security
Certificate Authority Service	Managed private CAs
Cloud Asset Inventory	All assets, one place
Cloud Audit Logs	Audit trails for GCP
Cloud DLP	Classify and redact sensitive data
Cloud HSM	Hardware security module service
Cloud EKM	External keys you control
Cloud IAM	Resource access control
Cloud Identity	Manage users, devices & apps
Cloud Identity-Aware Proxy	Identity-based app access
Cloud KMS	Hosted key management service
Cloud Resource Manager	Cloud project metadata management
Security Command Center	Security management & data risk platform
Cloud Security Scanner	App engine security scanner
Confidential Computing	Encrypt data in-use
Context-aware Access	End-user attribute-based access control
Event Threat Detection	Scans for suspicious activity
Managed Service for Microsoft Active Directory	Managed Microsoft Active Directory
Secret Manager	Store and manage secrets

IDENTITY AND SECURITY (CONT.)

Security Key Enforcement	Two-step key verification
Shielded VMs	Hardened VMs
Titan Security Key	Two-factor authentication (2FA) device
VPC Service Controls	VPC data constraints

MANAGEMENT TOOLS

Cloud APIs	APIs for cloud services
Cloud Billing API	Programmatically manage GCP billing
Cloud Billing	Billing and cost management tools
Cloud Console	Web-based management console
Cloud Deployment Manager	Templated infrastructure deployment
Cloud Mobile App	iOS/Android GCP manager app
Private Catalog	Internal Solutions Catalog
Cloud Debugger	Live production debugging
Error Reporting	App error reporting
Cloud Logging	Centralized logging
Cloud Monitoring	Infrastructure and application monitoring
Cloud Profiler	CPU and heap profiling
Cloud Trace	App performance insights
Transparent SLIs	Monitor GCP services

DEVELOPER TOOLS

Cloud Build	Continuous integration/delivery platform
Cloud Code for IntelliJ	IntelliJ GCP tools
Cloud Code for VS Code	VS Code GCP tools
Cloud Code	Cloud native IDE extensions
Cloud Tools for Eclipse	Eclipse GCP tools
Cloud Tools for Visual Studio	Visual Studio GCP tools
Gradle App Engine Plugin	Gradle App Engine plugin
Maven App Engine Plugin	Maven App Engine plugin
Cloud SDK	CLI for GCP
Cloud Shell	Browser-based terminal/CLI
Artifact Registry	Universal package manager
Cloud Source Repositories	Hosted private git repos
Container Registry	Private container registry/storage
Container Analysis	Automated security scanning
Eventarc	Event-driven Cloud Run services
Cloud Scheduler	Managed cron job service
Cloud Tasks	Asynchronous task execution
Cloud Workflows	HTTP services orchestration

MIGRATION TO GCP

BigQuery Data Transfer Service	Bulk import analytics data
Cloud Data Transfer	Data migration tools/CLI
Google Transfer Appliance	Rentable data transport box
Storage Transfer Service	Online/on-premises data transfer
Migrate for Anthos	Migrate VMs to GKE containers
Migrate for Compute Engine	Compute Engine migration tools
Migrate from Amazon Redshift	Migrate from Redshift to BigQuery
Migrate from Teradata	Migrate from Teradata to BigQuery
VM Migration	VM migration tools
Cloud Foundation Toolkit	Infrastructure as Code templates
KF	Cloud Foundry to Kubernetes

API PLATFORM AND ECOSYSTEMS

API Analytics	API metrics
API Monetization	Monetize APIs
Apigee API Platform	Develop, secure, monitor APIs
API Gateway	Fully managed API Gateway
Apigee Hybrid	Manage hybrid/multi-cloud API environments
Apigee Sense	API protection from attacks
Cloud Endpoints	Cloud API gateway
Cloud Healthcare API	Healthcare system GCP interoperability
Developer Portal	API management portal
GCP Marketplace	Partner & open source marketplace
AppSheet	No-code App creation

GOOGLE MAPS PLATFORM

Directions API	Get directions between locations
Distance Matrix API	Multi-origin/destination travel times
Geocoding API	Convert address to/from coordinates
Geolocation API	Derive location without GPS
Maps Embed API	Display iframe embedded maps
Maps JavaScript API	Dynamic web maps
Maps SDK for Android	Maps for Android apps
Maps SDK for iOS	Maps for iOS apps
Maps Static API	Display static map images

GOOGLE MAPS PLATFORM (CONT.)

Maps SDK for Unity	Unity SDK for games
Maps URLs	URL scheme for maps
Places API	Rest-based Places features
Places Library, Maps JS API	Places features for web
Places SDK for Android	Places features for Android
Places SDK for iOS	Places feature for iOS
Roads API	Convert coordinates to roads
Street View Static API	Static street view images
Street View Service	Street view for JavaScript
Time Zone API	Convert coordinates to timezone

GOOGLE WORKSPACE

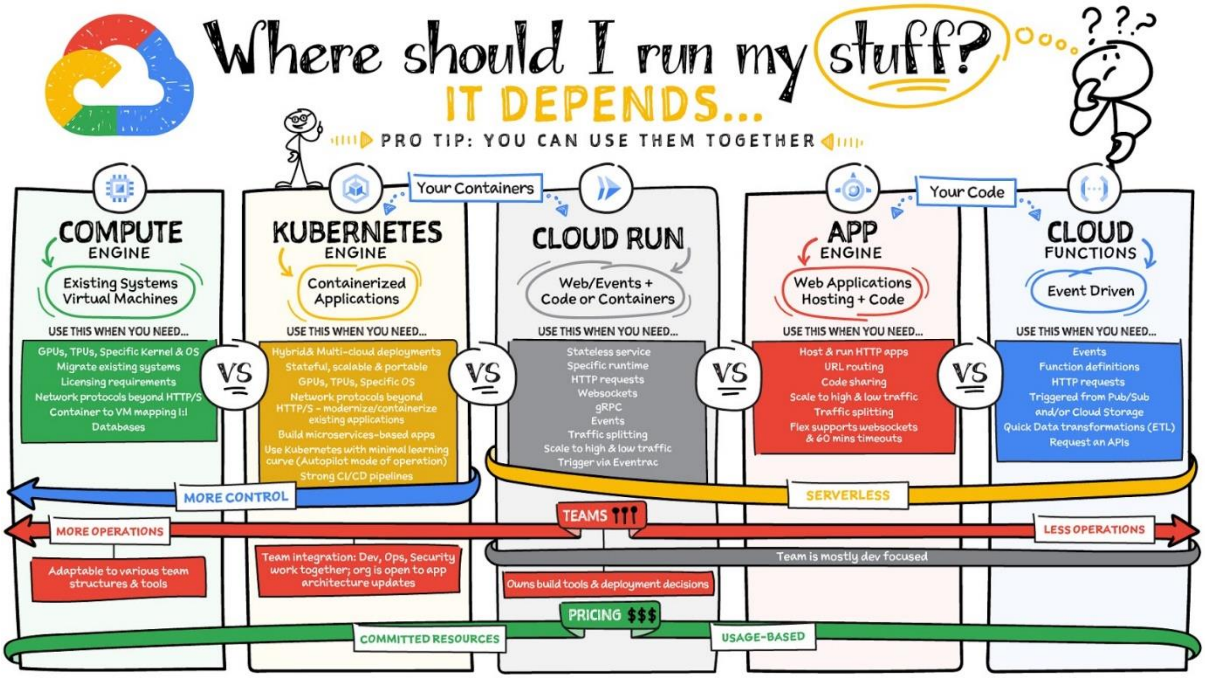
Admin SDK	Manage Workspace resources
AMP for Email	Dynamic interactive email
Apps Script	Extend and automate everything
Calendar API	Create and manage calendars
Classroom API	Provision and manage classrooms
Cloud Search	Unified search for enterprise
Docs API	Create and edit documents
Drive Activity API	Retrieve Google Drive activity
Drive API	Read and write files
Drive Picker	Drive file selection widget
Email Markup	Interactive email using schema.org
Workspace Add-ons	Extend G Suite apps
Workspace Marketplace	Storefront for integrated applications
Gmail API	Enhance Gmail
Hangouts Chat Bots	Conversational bots in chat
People API	Manage user's Contacts
Sheets API	Read and write spreadsheets
Slides API	Create and edit presentations
Task API	Search, read & update Tasks
Vault API	Manage your organization's eDiscovery

MOBILE (FIREBASE)

Cloud Firestore	Document store and sync
Cloud Functions for Firebase	Event-driven serverless applications
Cloud Storage for Firebase	Object storage and serving
Crashlytics	Crash reporting and analytics
Firebase A/B Testing	Create A/B test experiments
Firebase App Distribution	Trusted tester early access
Firebase Authentication	Drop-in authentication
Firebase Cloud Messaging	Send device notifications
Firebase Dynamic Links	Link to app content
Firebase Extensions	Pre-packaged development solutions
Firebase Hosting	Web hosting with CDN/SSL
Firebase In-App Messaging	Send in-app contextual messages
Firebase Performance Monitoring	App/web performance monitoring
Firebase Predictions	Predict user targeting
Firebase Realtime Database	Real-time data synchronization
Firebase Remote Config	Remotely configure installed apps
Firebase Test Lab	Mobile testing device farm
Google Analytics for Firebase	Mobile app analytics
ML Kit for Firebase	ML APIs for mobile

ADDITIONAL RESOURCES

Google Cloud Home Page	cloud.google.com
Google Cloud Blog	cloud.google.com/blog
Google Cloud Platform Podcast	gcppodcast.com
Kubernetes Podcast from Google	kubernetespodcast.com
Google Cloud Open Source	opensource.google/projects/list/cloud
GCP Medium Publication	medium.com/google-cloud
Apigee Blog	apigee.com/about/blog
Firebase Blog	firebase.googleblog.com
Workspace Developers Blog	gsuite-developers.googleblog.com
Workspace GitHub	github.com/gsuitedevs
Workspace Twitter	twitter.com/gsuitedevs
Google Cloud Certifications	cloud.google.com/certification
Google Cloud System Status	status.cloud.google.com
Google Cloud Training	cloud.google.com/training
Google Developers Blog	developers.googleblog.com
Google Maps Platform Blog	mapsplatform.googleblog.com
Google Open Source Blog	opensource.googleblog.com
Google Security Blog	security.googleblog.com
Kaggle Home Page	www.kaggle.com
Kubernetes Blog	kubernetes.io/blog
Regions and Network Map	cloud.google.com/about/locations
DORA – Software & Delivery Research	cloud.google.com/devops



Where should I run my stuff?

IT DEPENDS...

PRO TIP: YOU CAN USE THEM TOGETHER

Your Containers

Your Code

COMPUTE ENGINE

Existing Systems Virtual Machines

USE THIS WHEN YOU NEED...

GPUs, TPUs, Specific Kernel & OS
Migrate existing systems
Licensing requirements
Network protocols beyond HTTP/S
Container to VM mapping 1:1
Databases

VS

KUBERNETES ENGINE

Containerized Applications

USE THIS WHEN YOU NEED...

Hybrid& Multi-cloud deployments
Stateful, scalable & portable
GPUs, TPUs, Specific OS
Network protocols beyond HTTP/S – modernize/containerize existing applications
Build microservices-based apps
Use Kubernetes with minimal learning curve (Autopilot mode of operation)
Strong CI/CD pipelines

VS

CLOUD RUN

Web/Events + Code or Containers

USE THIS WHEN YOU NEED...

Stateless service
Specific runtime
HTTP requests
Websockets
gRPC
Events
Traffic splitting
Scale to high & low traffic
Trigger via Eventrac

VS

APP ENGINE

Web Applications Hosting + Code

USE THIS WHEN YOU NEED...

Host & run HTTP apps
URL routing
Code sharing
Scale to high & low traffic
Traffic splitting
Flex supports websockets & 60 mins timeouts

VS

CLOUD FUNCTIONS

Event Driven

USE THIS WHEN YOU NEED...

Events
Function definitions
HTTP requests
Triggered from Pub/Sub and/or Cloud Storage
Quick Data transformations (ETL)
Request an APIs

MORE CONTROL

SERVERLESS

TEAMS

MORE OPERATIONS

LESS OPERATIONS

Adaptable to various team structures & tools

Team integration: Dev, Ops, Security work together; org is open to app architecture updates

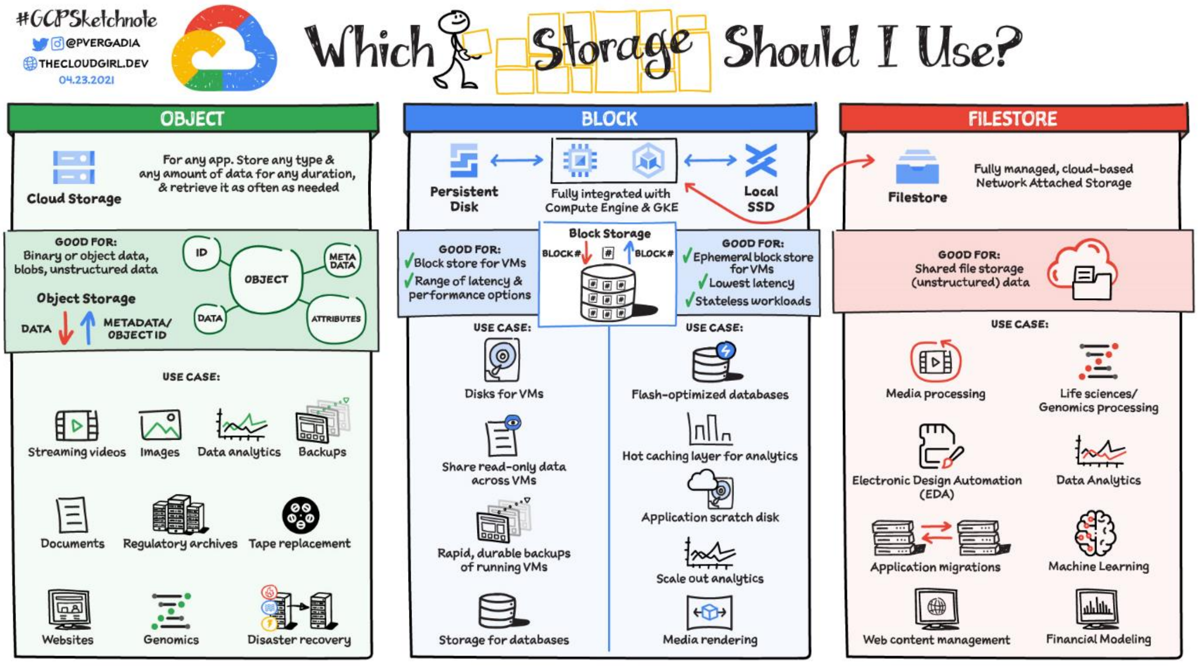
Owns build tools & deployment decisions

Team is mostly dev focused

PRICING $$$

COMMITTED RESOURCES

USAGE-BASED



#GCPSketchnote

@PVERGADIA

THECLOUDGIRL.DEV

04.23.2021

Which Storage Should I Use?

OBJECT

Cloud Storage

For any app. Store any type & any amount of data for any duration, & retrieve it as often as needed

GOOD FOR:
Binary or object data, blobs, unstructured data

Object Storage

DATA ↓ ↑ METADATA/ OBJECT ID

OBJECT — ID, META DATA, DATA, ATTRIBUTES

USE CASE:

- Streaming videos
- Images
- Data analytics
- Backups
- Documents
- Regulatory archives
- Tape replacement
- Websites
- Genomics
- Disaster recovery

BLOCK

Persistent Disk ⟷ Fully integrated with Compute Engine & GKE ⟷ **Local SSD**

Block Storage

BLOCK# ↓ # ↑ BLOCK#

GOOD FOR:
✓Block store for VMs
✓Range of latency & performance options

GOOD FOR:
✓Ephemeral block store for VMs
✓Lowest latency
✓Stateless workloads

USE CASE:

- Disks for VMs
- Share read-only data across VMs
- Rapid, durable backups of running VMs
- Storage for databases

USE CASE:

- Flash-optimized databases
- Hot caching layer for analytics
- Application scratch disk
- Scale out analytics
- Media rendering

FILESTORE

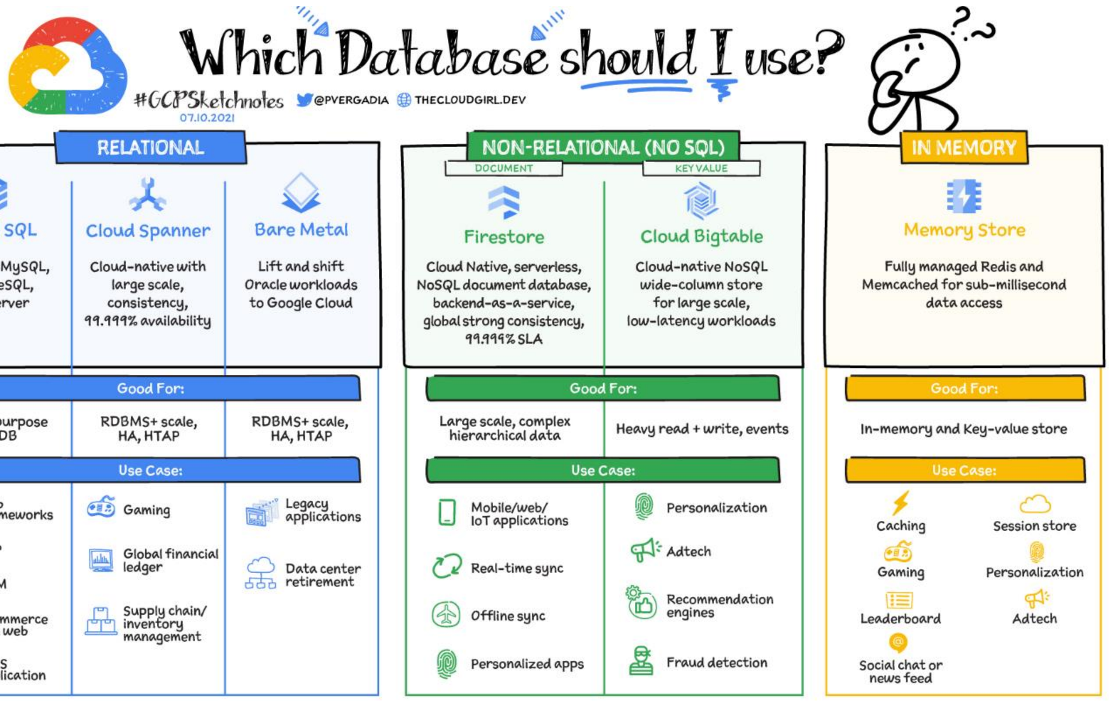
Filestore

Fully managed, cloud-based Network Attached Storage

GOOD FOR:
Shared file storage (unstructured) data

USE CASE:

- Media processing
- Life sciences/ Genomics processing
- Electronic Design Automation (EDA)
- Data Analytics
- Application migrations
- Machine Learning
- Web content management
- Financial Modeling



Which Database should I use?

#GCPSketchnotes @PVERGADIA THECLOUDGIRL.DEV

07.10.2021

RELATIONAL

Cloud SQL	Cloud Spanner	Bare Metal
Managed MySQL, PostgreSQL, SQL Server	Cloud-native with large scale, consistency, 99.999% availability	Lift and shift Oracle workloads to Google Cloud
Good For:		
General purpose SQL DB	RDBMS+ scale, HA, HTAP	RDBMS+ scale, HA, HTAP
Use Case:		
Web frameworks ERP CRM Ecommerce and web SaaS application	Gaming Global financial ledger Supply chain/ inventory management	Legacy applications Data center retirement

NON-RELATIONAL (NO SQL)

DOCUMENT Firestore	KEY VALUE Cloud Bigtable
Cloud Native, serverless, NoSQL document database, backend-as-a-service, global strong consistency, 99.999% SLA	Cloud-native NoSQL wide-column store for large scale, low-latency workloads
Good For:	
Large scale, complex hierarchical data	Heavy read + write, events
Use Case:	
Mobile/web/ IoT applications Real-time sync Offline sync Personalized apps	Personalization Adtech Recommendation engines Fraud detection

IN MEMORY

Memory Store

Fully managed Redis and Memcached for sub-millisecond data access

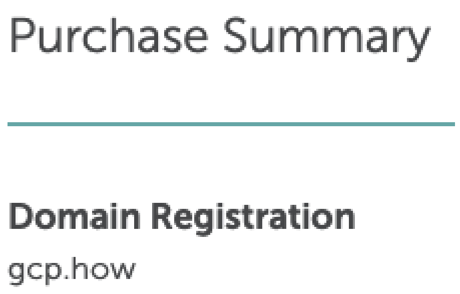
Good For:

In-memory and Key-value store

Use Case:

- Caching
- Session store
- Gaming
- Personalization
- Leaderboard
- Adtech
- Social chat or news feed

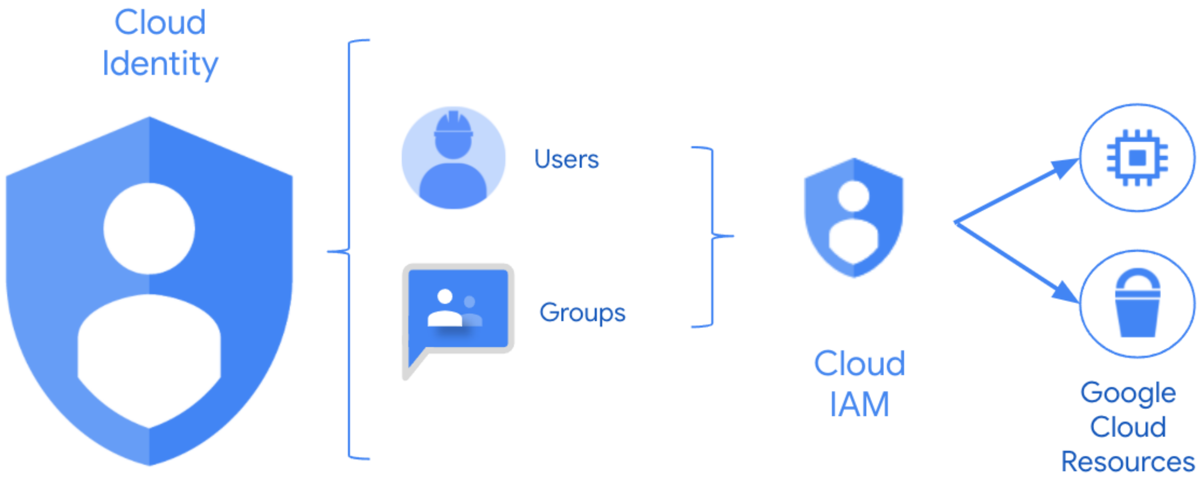
Chapter 2: IAM, Users, Groups, and Admin Access



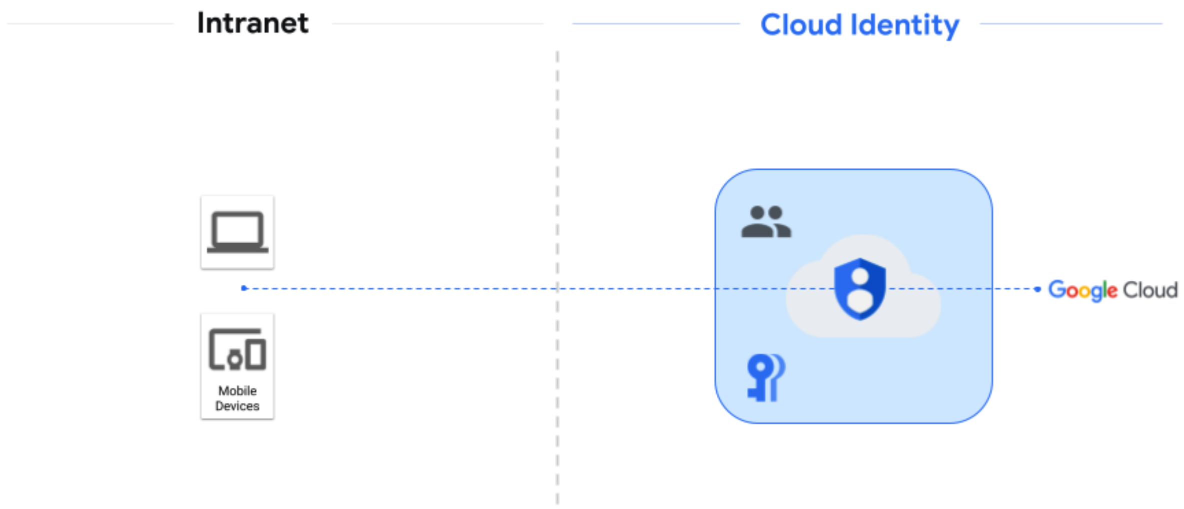
Purchase Summary

Domain Registration

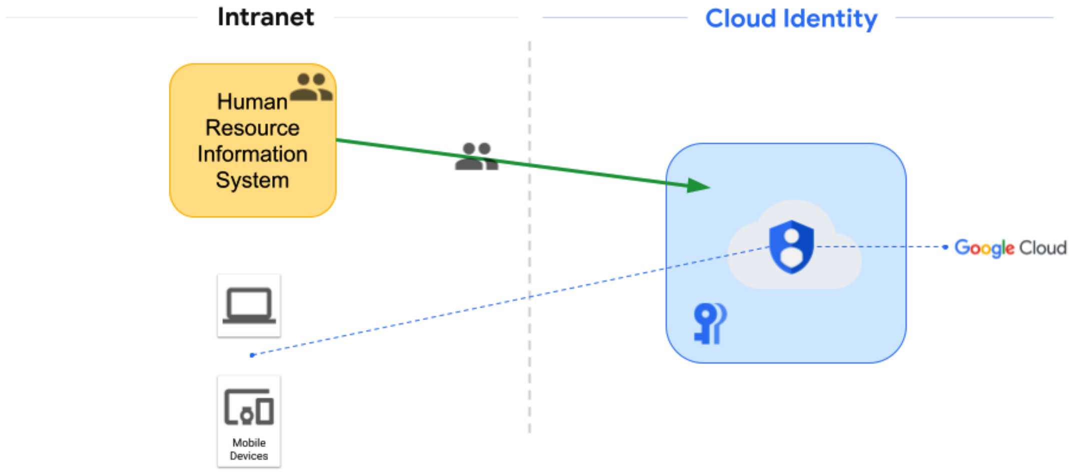
gcp.how



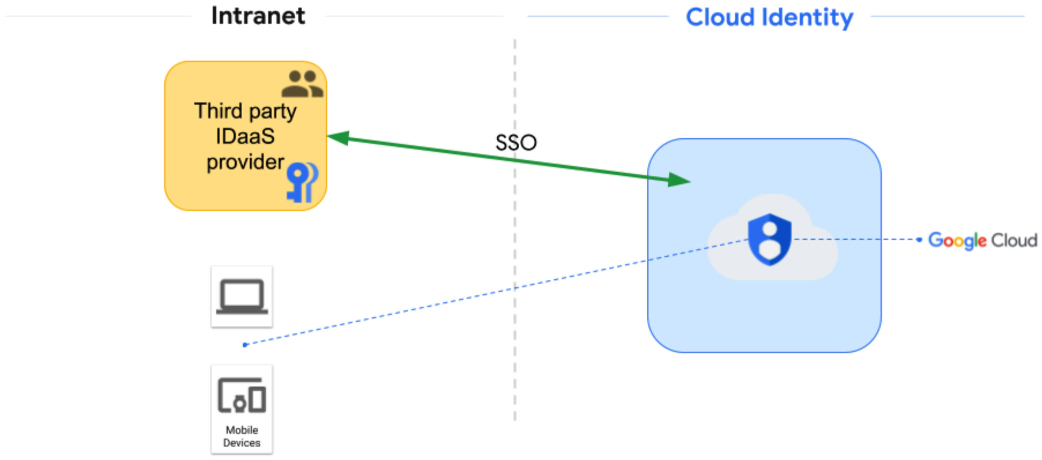
Cloud Identity managing both users and acting as IdP

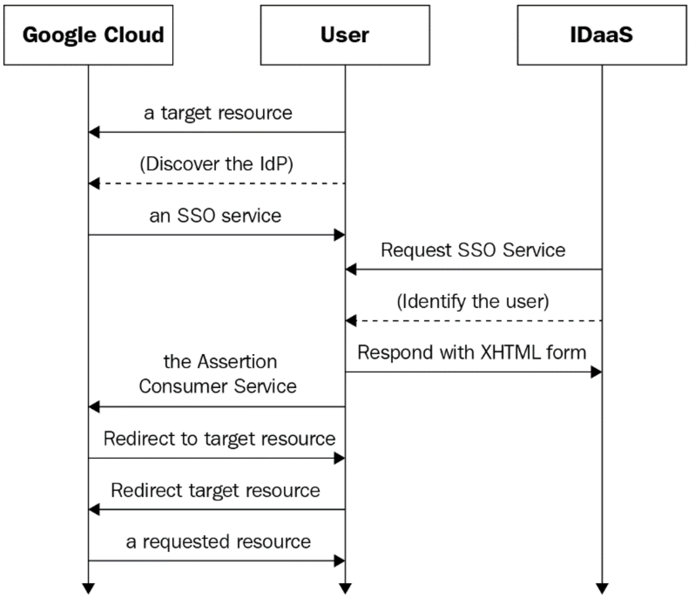


Cloud Identity managing IdP and an HR system managing users

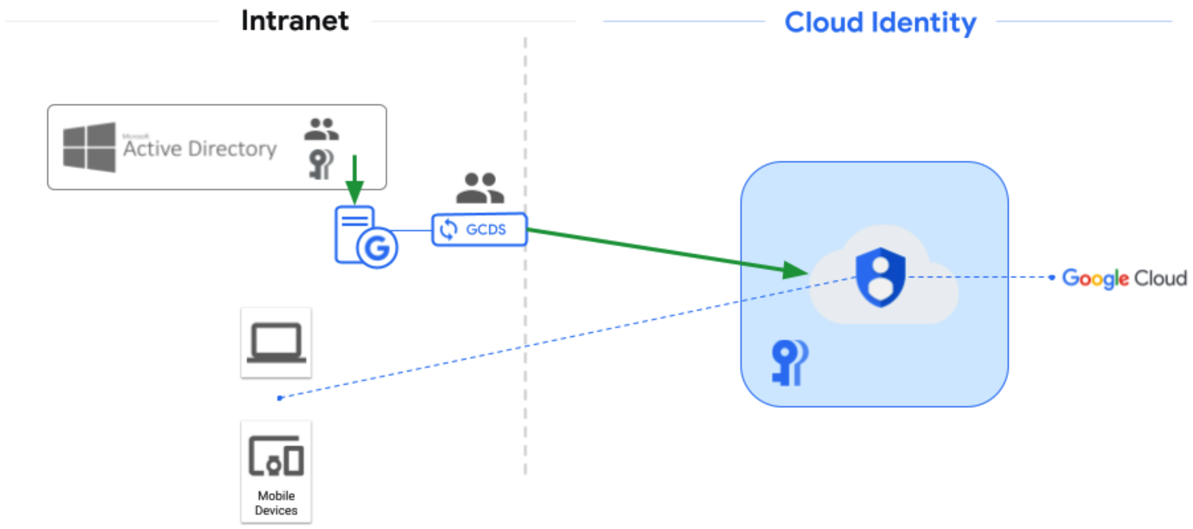


A third-party IDaaS provider acting as an IdP and managing users

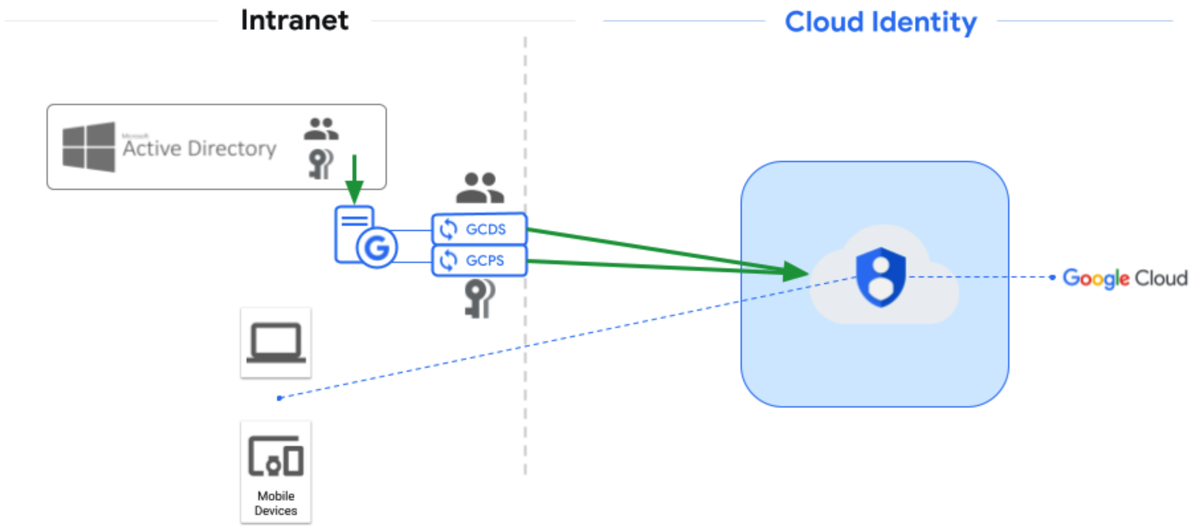




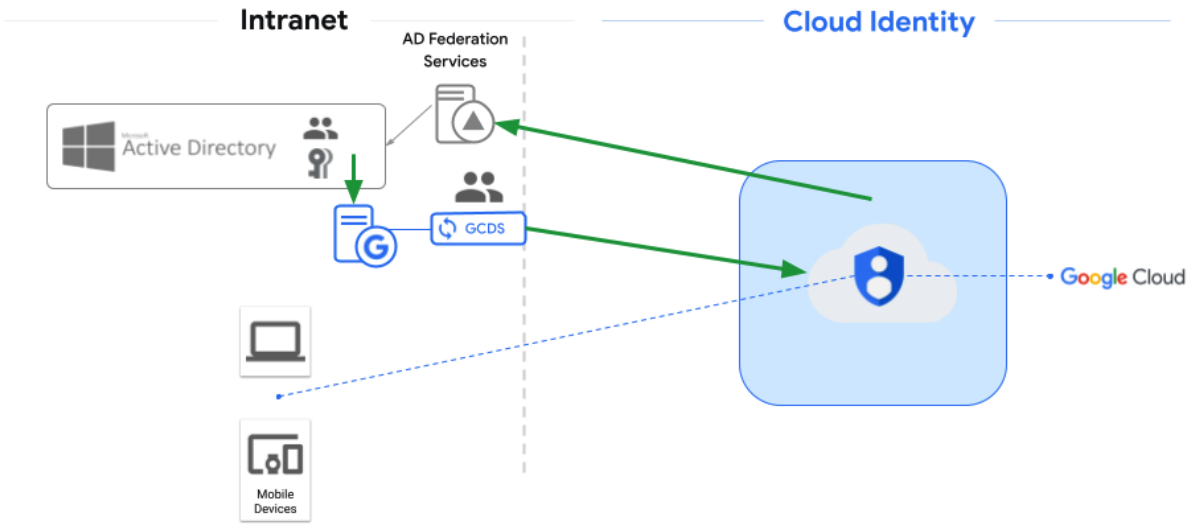
AD manages users and Cloud Identity handles authentication



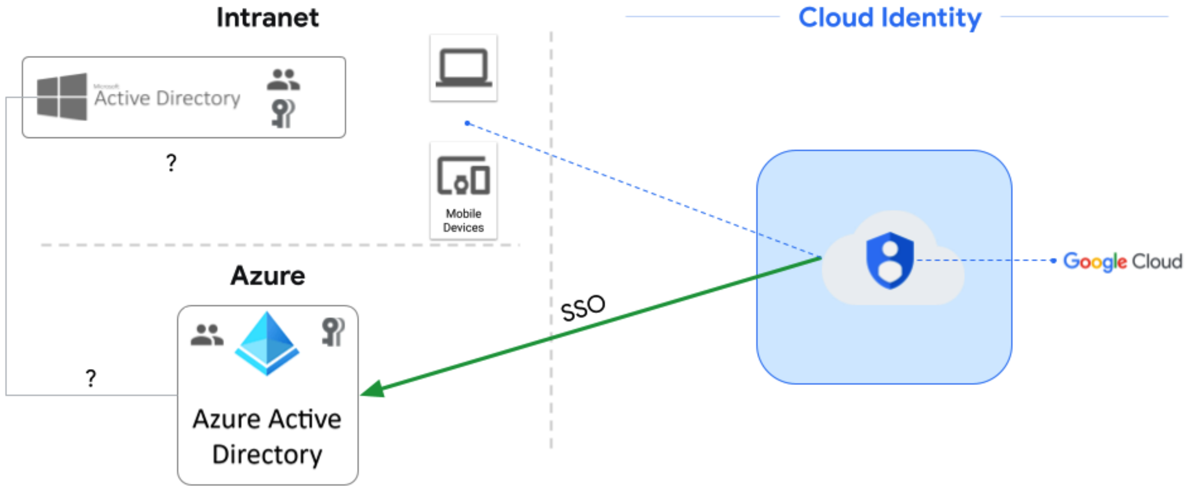
AD manages users and Cloud Identity handles authentication - part two

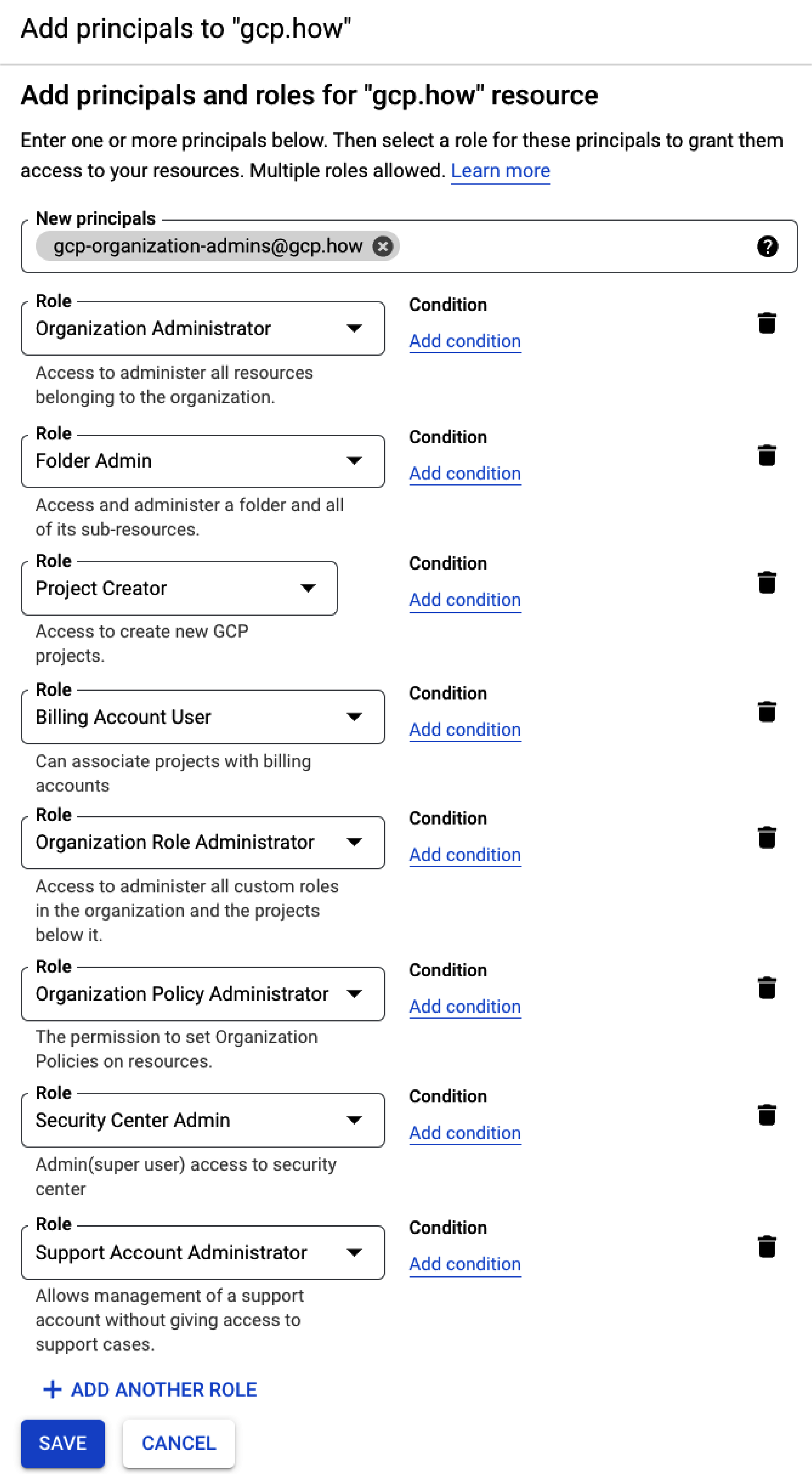


AD manages users and AD FS works as the IdP



Azure AD managing users and acting as IdP





Add principals to "gcp.how"

Add principals and roles for "gcp.how" resource

Enter one or more principals below. Then select a role for these principals to grant them access to your resources. Multiple roles allowed. Learn more

New principals: gcp-organization-admins@gcp.how

Role: Organization Administrator
Access to administer all resources belonging to the organization.
Condition: Add condition

Role: Folder Admin
Access and administer a folder and all of its sub-resources.
Condition: Add condition

Role: Project Creator
Access to create new GCP projects.
Condition: Add condition

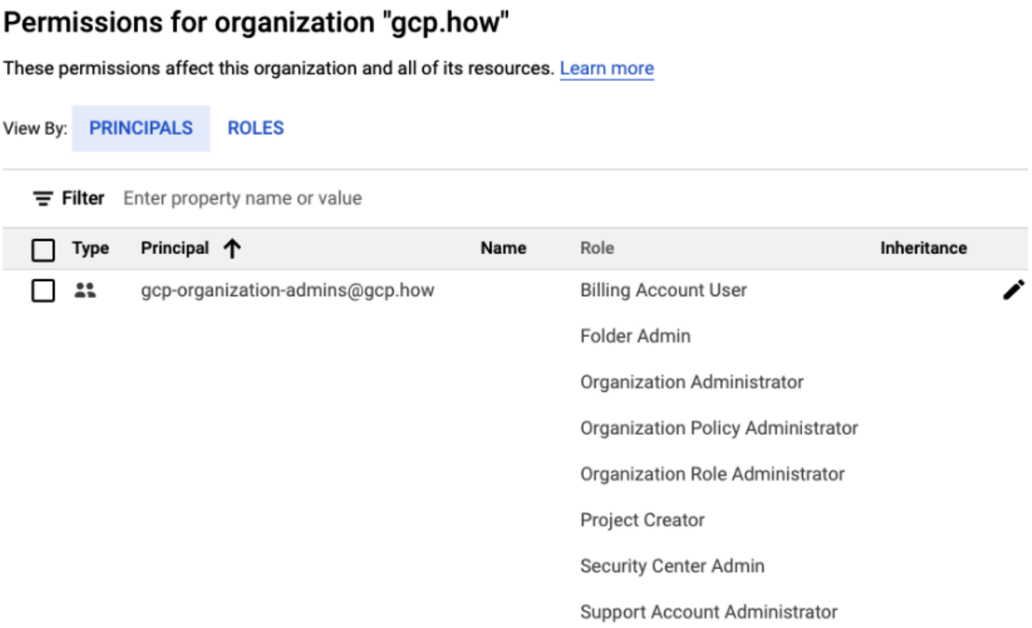
Role: Billing Account User
Can associate projects with billing accounts
Condition: Add condition

Role: Organization Role Administrator
Access to administer all custom roles in the organization and the projects below it.
Condition: Add condition

Role: Organization Policy Administrator
The permission to set Organization Policies on resources.
Condition: Add condition

Role: Security Center Admin
Admin(super user) access to security center
Condition: Add condition

Role: Support Account Administrator
Allows management of a support account without giving access to support cases.
Condition: Add condition



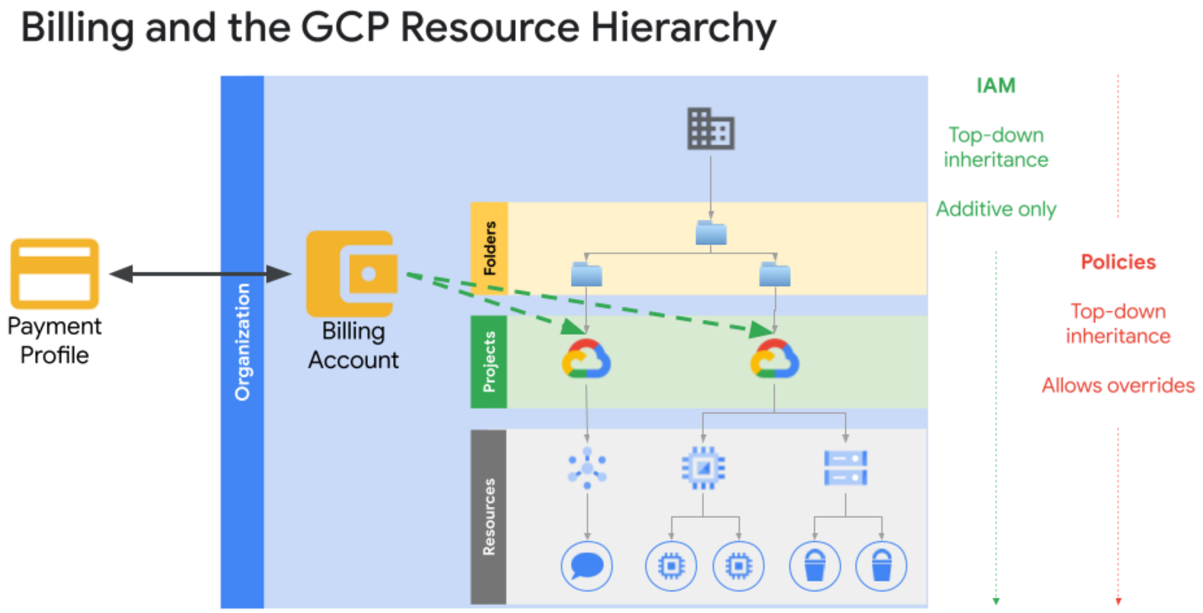
Permissions for organization "gcp.how"

These permissions affect this organization and all of its resources. Learn more

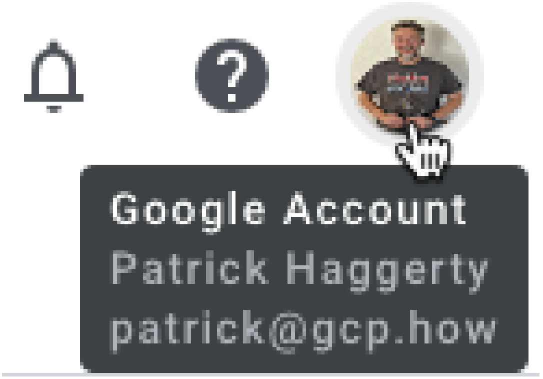
View By: PRINCIPALS ROLES
Filter Enter property name or value

□	Type	Principal ↑	Name	Role	Inheritance
□	👥	gcp-organization-admins@gcp.how		Billing Account User Folder Admin Organization Administrator Organization Policy Administrator Organization Role Administrator Project Creator Security Center Admin Support Account Administrator	

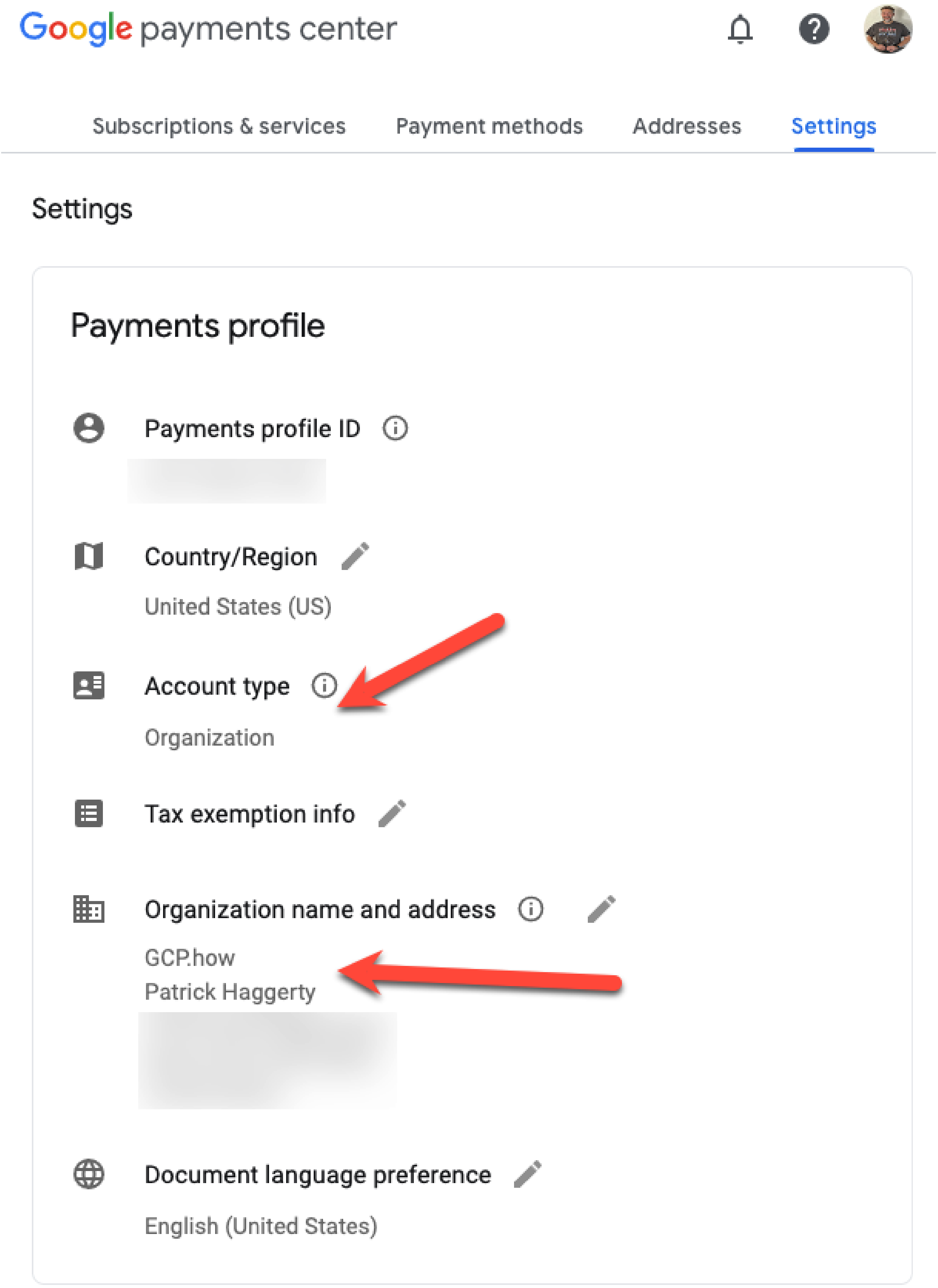
Chapter 3: Setting Up Billing and Cost Controls



Billing and the GCP Resource Hierarchy



Google Account
Patrick Haggerty
patrick@gcp.how



Settings

Payments profile

Payments profile ID

[redacted]

Country/Region

United States (US)

Account type

Organization

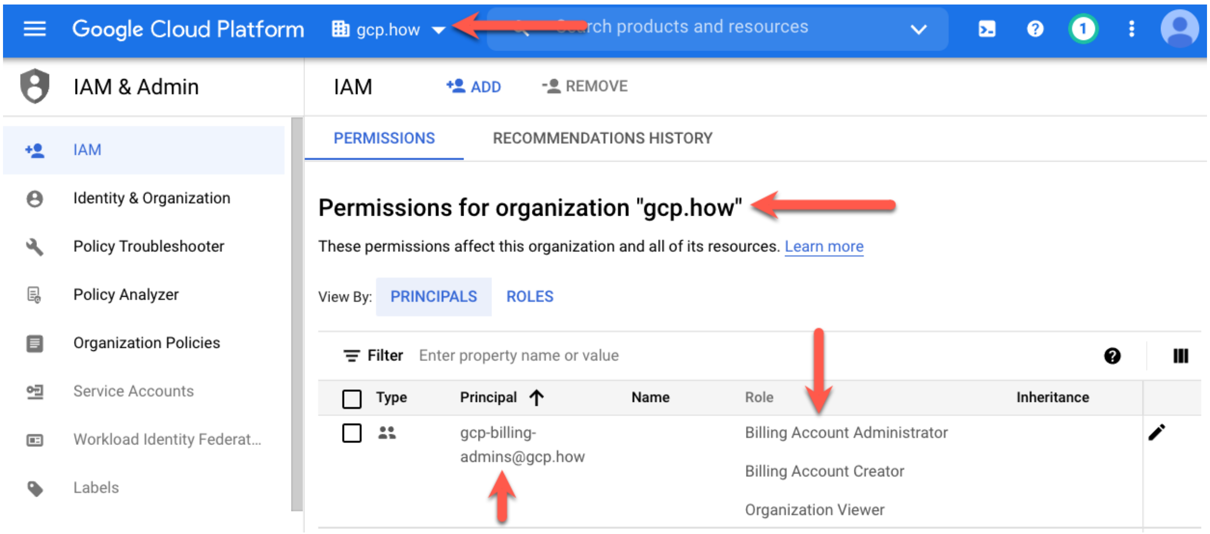
Tax exemption info

Organization name and address

GCP.how
Patrick Haggerty
[redacted]

Document language preference

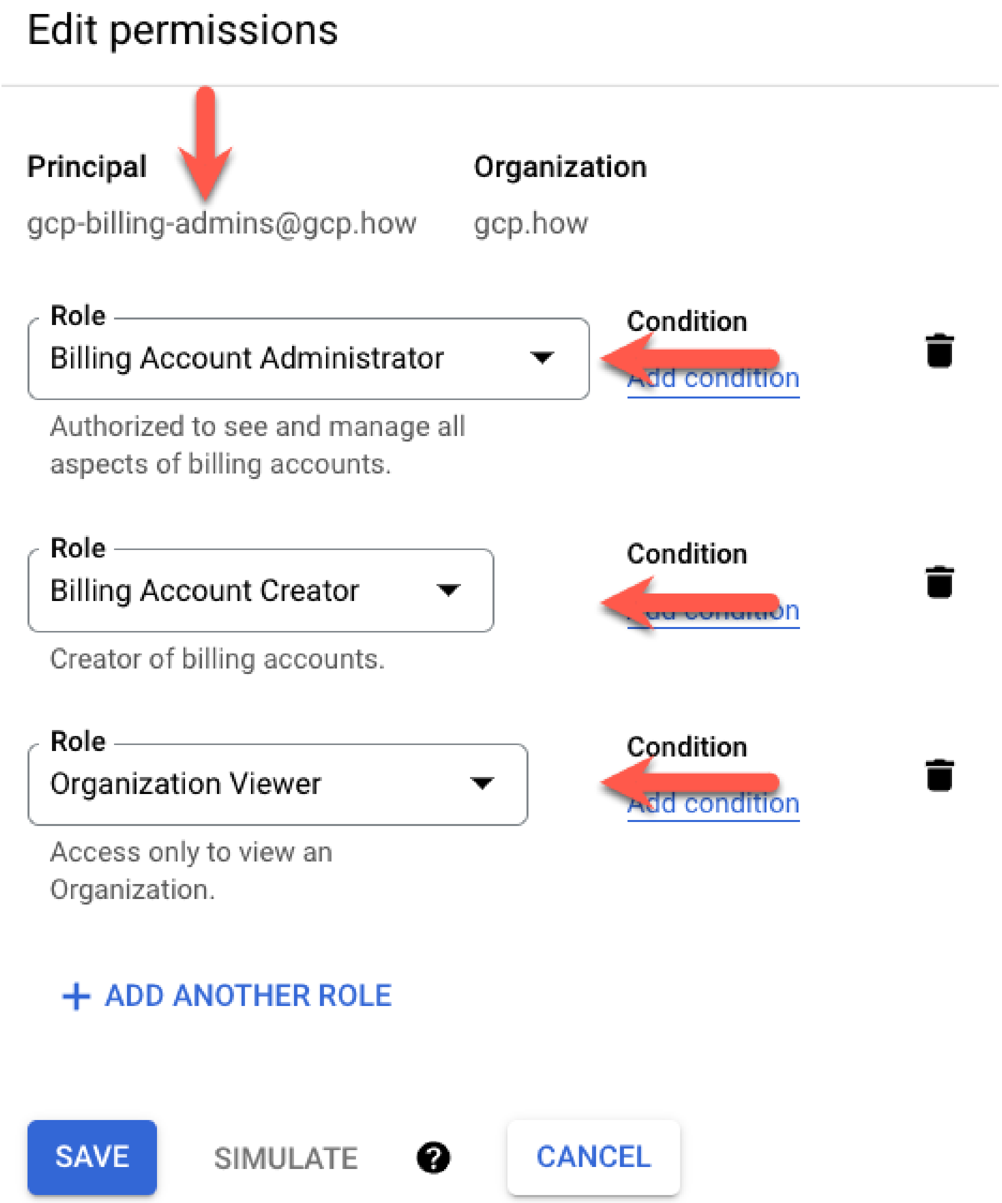
English (United States)



Permissions for organization "gcp.how"

These permissions affect this organization and all of its resources. Learn more

□ Type	Principal	Name	Role	Inheritance
□	gcp-billing-admins@gcp.how		Billing Account Administrator Billing Account Creator Organization Viewer	



Edit permissions

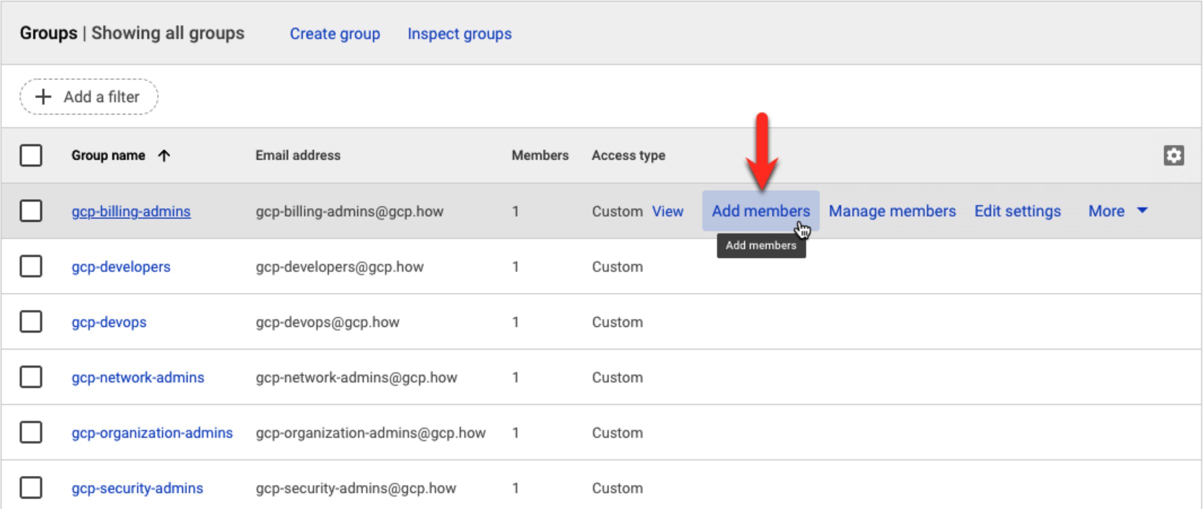
Principal: gcp-billing-admins@gcp.how

Organization: gcp.how

Role: Billing Account Administrator
Authorized to see and manage all aspects of billing accounts.

Role: Billing Account Creator
Creator of billing accounts.

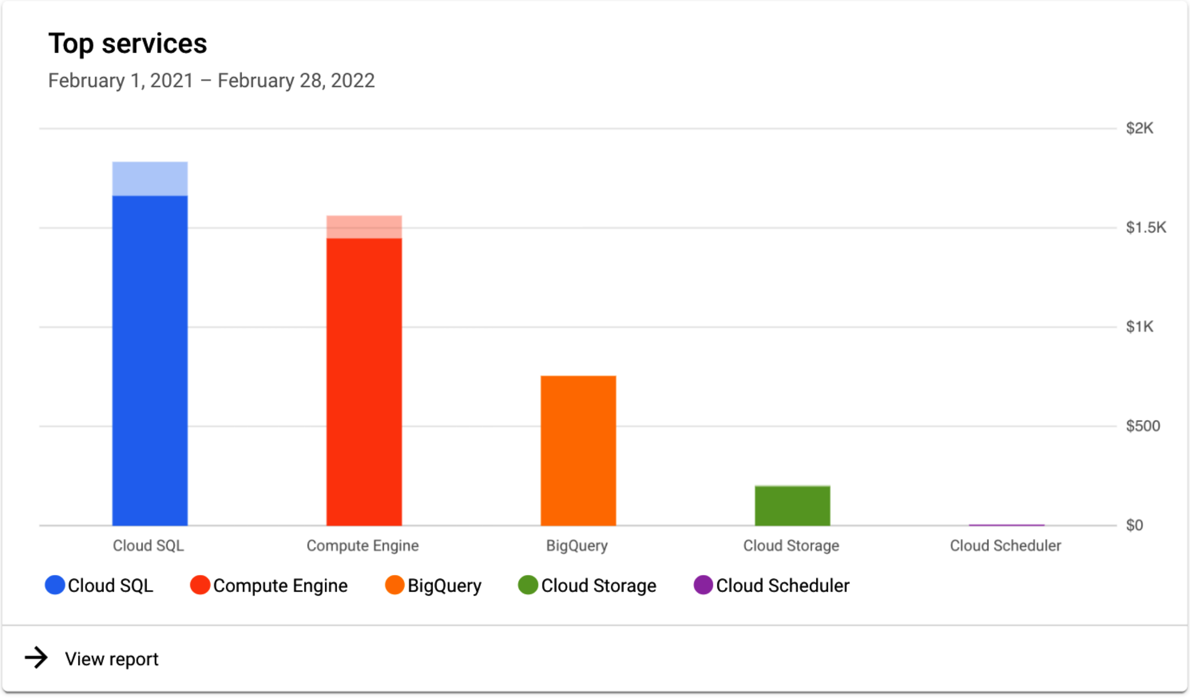
Role: Organization Viewer
Access only to view an Organization.



Groups | Showing all groups   Create group   Inspect groups

+ Add a filter

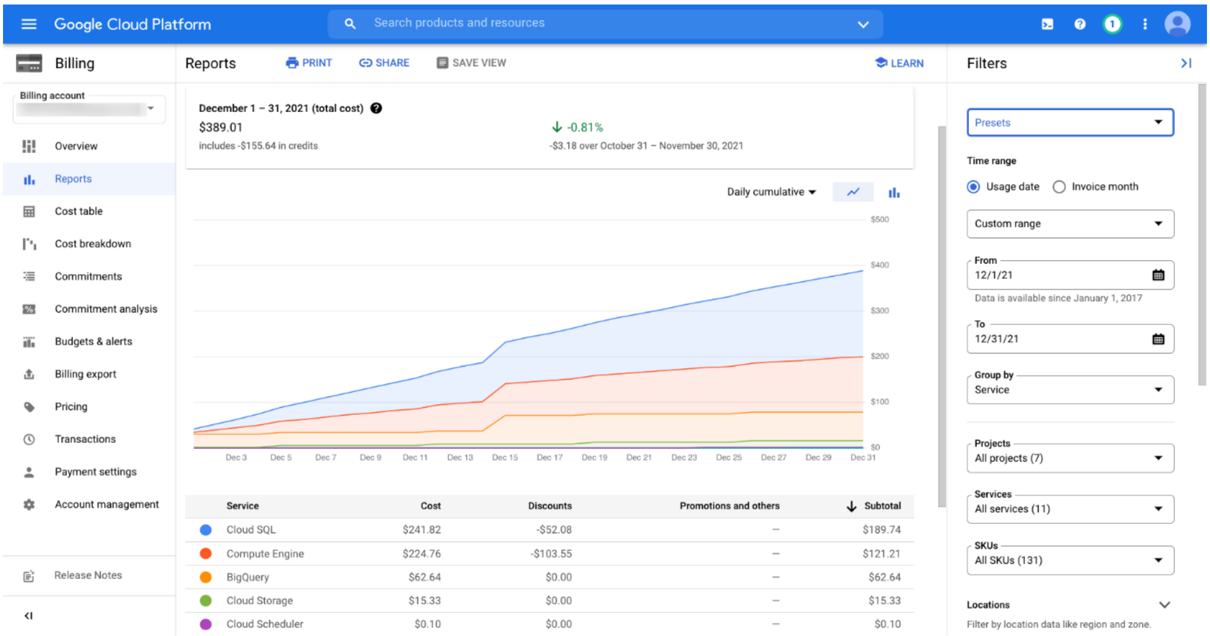
□	Group name ↑	Email address	Members	Access type	
□	gcp-billing-admins	gcp-billing-admins@gcp.how	1	Custom View	Add members Manage members Edit settings More ▾
□	gcp-developers	gcp-developers@gcp.how	1	Custom	
□	gcp-devops	gcp-devops@gcp.how	1	Custom	
□	gcp-network-admins	gcp-network-admins@gcp.how	1	Custom	
□	gcp-organization-admins	gcp-organization-admins@gcp.how	1	Custom	
□	gcp-security-admins	gcp-security-admins@gcp.how	1	Custom	



Top services

February 1, 2021 – February 28, 2022

→ View report



December 1 – 31, 2021 (total cost)

$389.01

includes -$155.64 in credits

-0.81%

-$3.18 over October 31 – November 30, 2021

	Service	Cost	Discounts	Promotions and others	Subtotal
●	Cloud SQL	$241.82	-$52.08	–	$189.74
●	Compute Engine	$224.76	-$103.55	–	$121.21
●	BigQuery	$62.64	$0.00	–	$62.64
●	Cloud Storage	$15.33	$0.00	–	$15.33
●	Cloud Scheduler	$0.10	$0.00	–	$0.10

Time range

● Usage date ○ Invoice month

Custom range

From: 12/1/21

Data is available since January 1, 2017

To: 12/31/21

Group by: Service

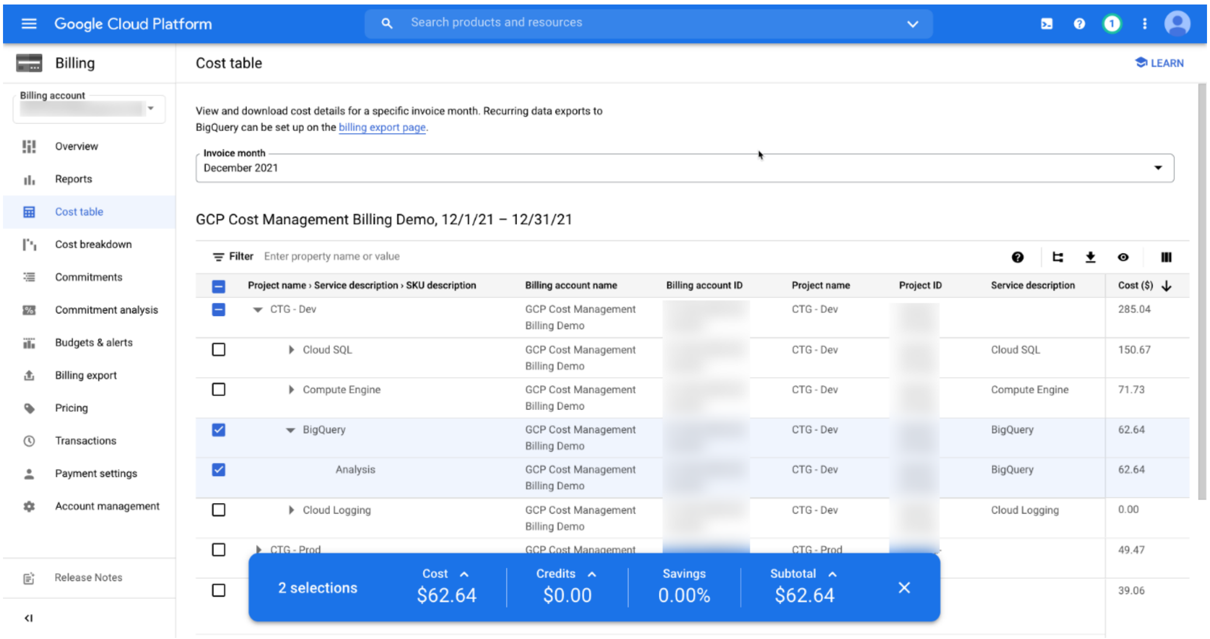
Projects: All projects (7)

Services: All services (11)

SKUs: All SKUs (131)

Locations

Filter by location data like region and zone.



Cost table

View and download cost details for a specific invoice month. Recurring data exports to BigQuery can be set up on the billing export page.

Invoice month: December 2021

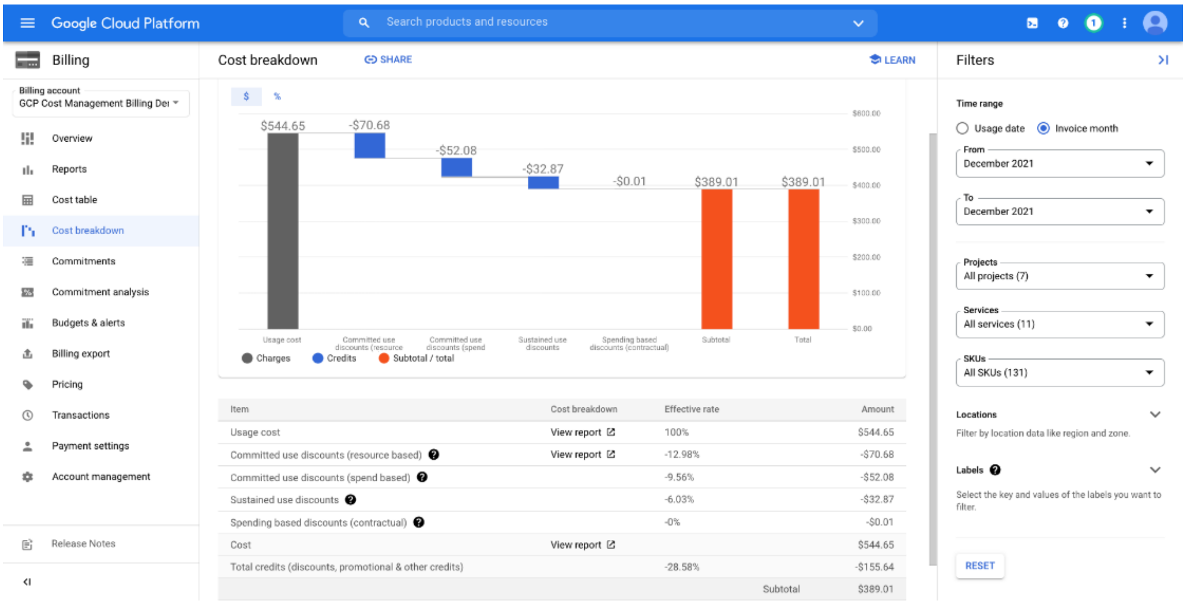
GCP Cost Management Billing Demo, 12/1/21 – 12/31/21

Filter: Enter property name or value

	Project name › Service description › SKU description	Billing account name	Billing account ID	Project name	Project ID	Service description	Cost ($)
▬	CTG - Dev	GCP Cost Management Billing Demo	[redacted]	CTG - Dev	[redacted]		285.04
□	Cloud SQL	GCP Cost Management Billing Demo	[redacted]	CTG - Dev	[redacted]	Cloud SQL	150.67
□	Compute Engine	GCP Cost Management Billing Demo	[redacted]	CTG - Dev	[redacted]	Compute Engine	71.73
☑	BigQuery	GCP Cost Management Billing Demo	[redacted]	CTG - Dev	[redacted]	BigQuery	62.64
☑	Analysis	GCP Cost Management Billing Demo	[redacted]	CTG - Dev	[redacted]	BigQuery	62.64
□	Cloud Logging	GCP Cost Management Billing Demo	[redacted]	CTG - Dev	[redacted]	Cloud Logging	0.00
□	CTG - Prod	GCP Cost Management	[redacted]	CTG - Prod	[redacted]		49.47
□							39.06

2 selections

Cost	Credits	Savings	Subtotal
$62.64	$0.00	0.00%	$62.64



Cost breakdown

Item	Cost breakdown	Effective rate	Amount
Usage cost	View report	100%	$544.65
Committed use discounts (resource based)	View report	-12.98%	-$70.68
Committed use discounts (spend based)		-9.56%	-$52.08
Sustained use discounts		-6.03%	-$32.87
Spending based discounts (contractual)		-0%	-$0.01
Cost	View report		$544.65
Total credits (discounts, promotional & other credits)		-28.58%	-$155.64
		Subtotal	$389.01

Time range

○ Usage date ● Invoice month

From: December 2021

To: December 2021

Projects: All projects (7)

Services: All services (11)

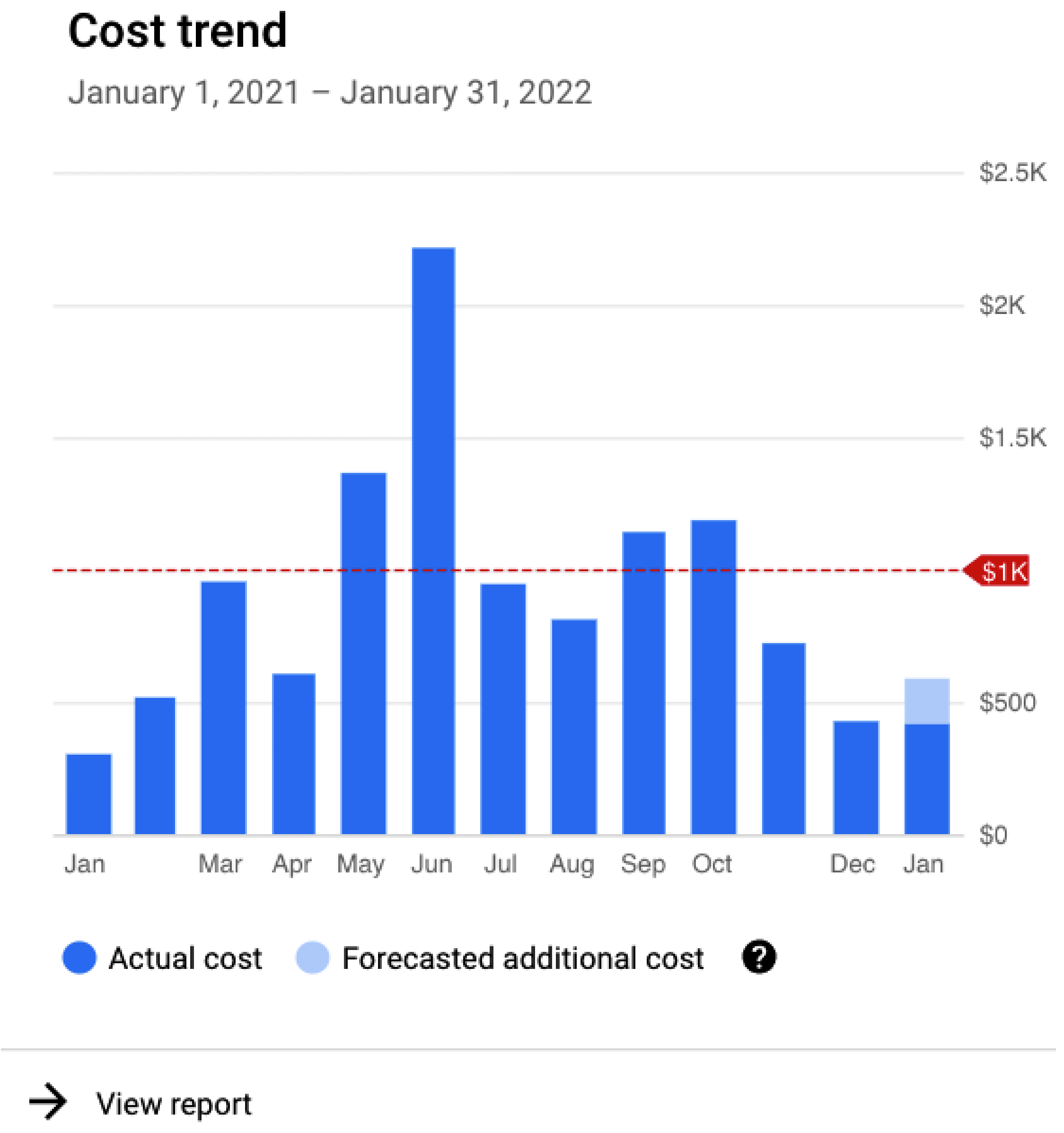
SKUs: All SKUs (131)

Locations

Filter by location data like region and zone.

Labels

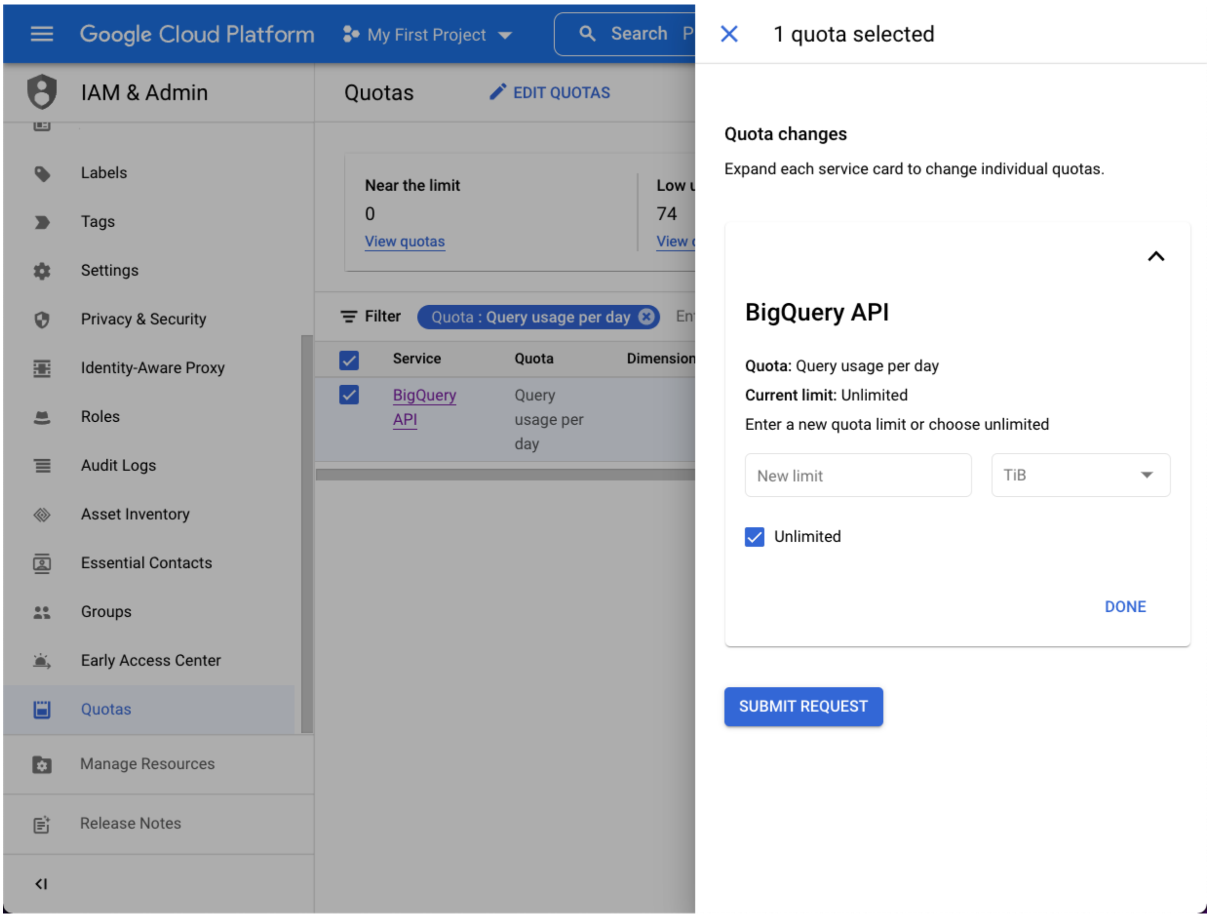
Select the key and values of the labels you want to filter.



Cost trend

January 1, 2021 – January 31, 2022

View report



☑	Service	Quota	Dimension
☑	BigQuery API	Query usage per day	

1 quota selected

Quota changes

Expand each service card to change individual quotas.

BigQuery API

Quota: Query usage per day

Current limit: Unlimited

Enter a new quota limit or choose unlimited

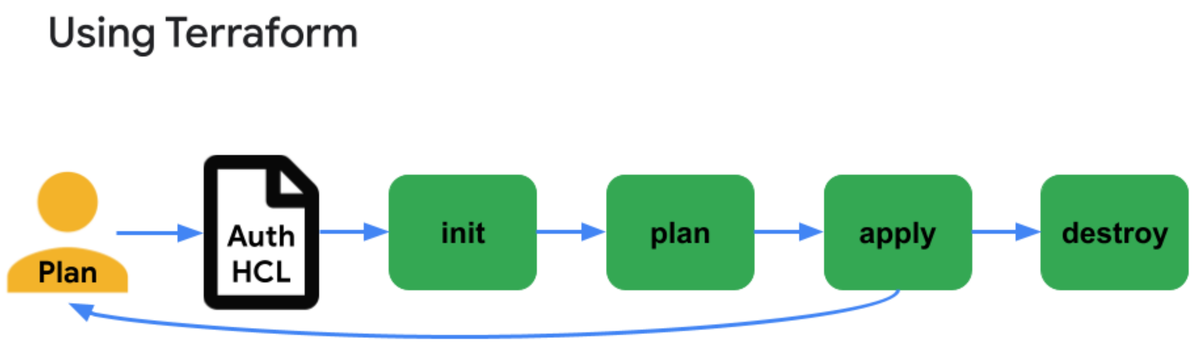
New limit

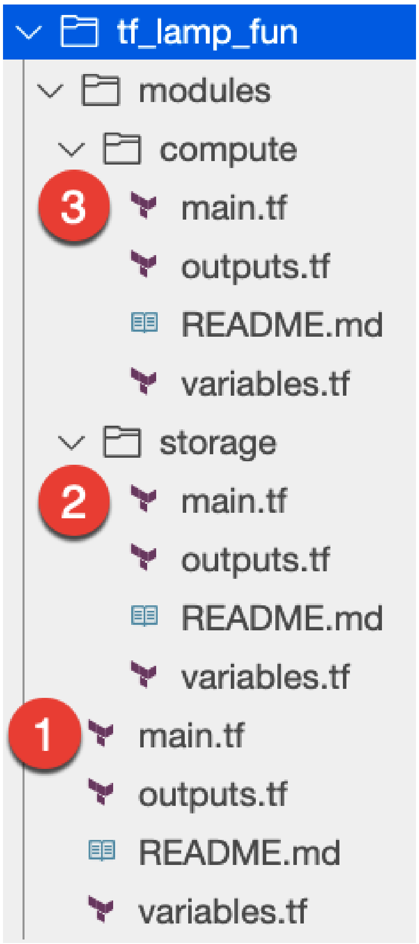
TiB

☑ Unlimited

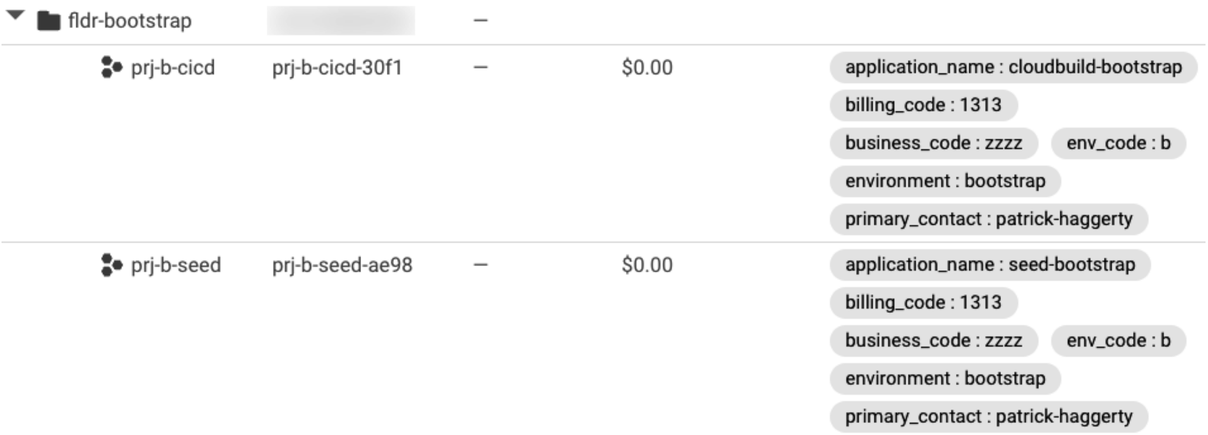
Chapter 4: Terraforming a Resource Hierarchy

HashiCorp Terraform



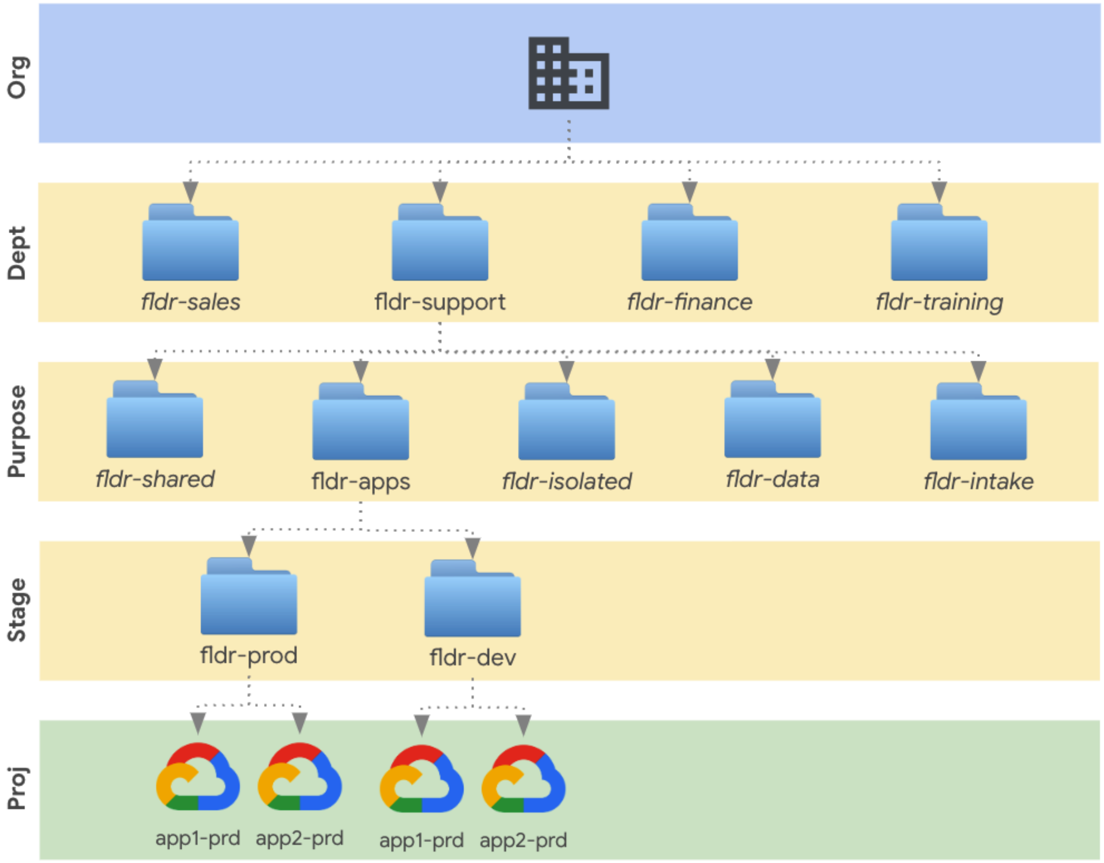


```
tf_lamp_fun
  modules
    compute
      main.tf
      outputs.tf
      README.md
      variables.tf
    storage
      main.tf
      outputs.tf
      README.md
      variables.tf
  main.tf
  outputs.tf
  README.md
  variables.tf
```

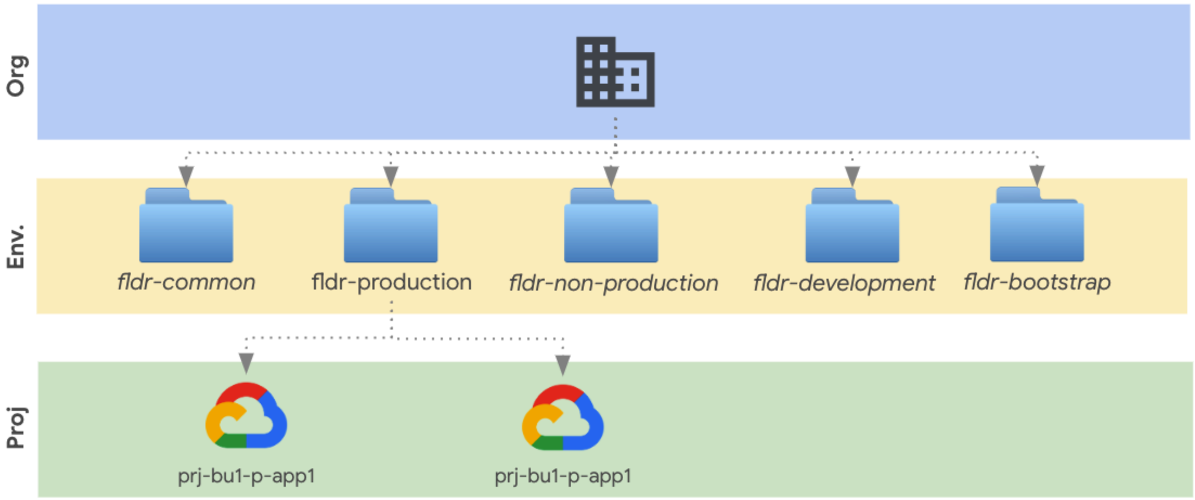


fldr-bootstrap	[redacted]	—		
prj-b-cicd	prj-b-cicd-30f1	—	$0.00	application_name : cloudbuild-bootstrap billing_code : 1313 business_code : zzzz env_code : b environment : bootstrap primary_contact : patrick-haggerty
prj-b-seed	prj-b-seed-ae98	—	$0.00	application_name : seed-bootstrap billing_code : 1313 business_code : zzzz env_code : b environment : bootstrap primary_contact : patrick-haggerty

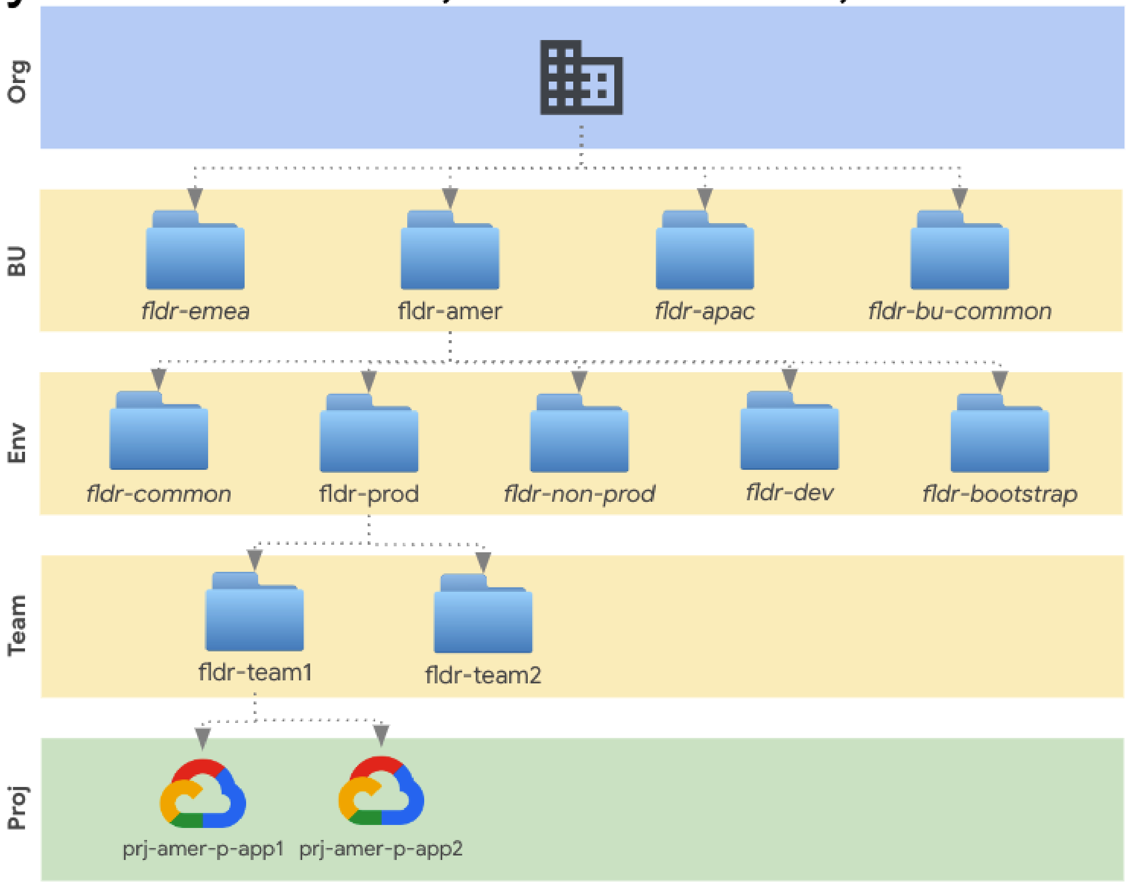
Don't do this



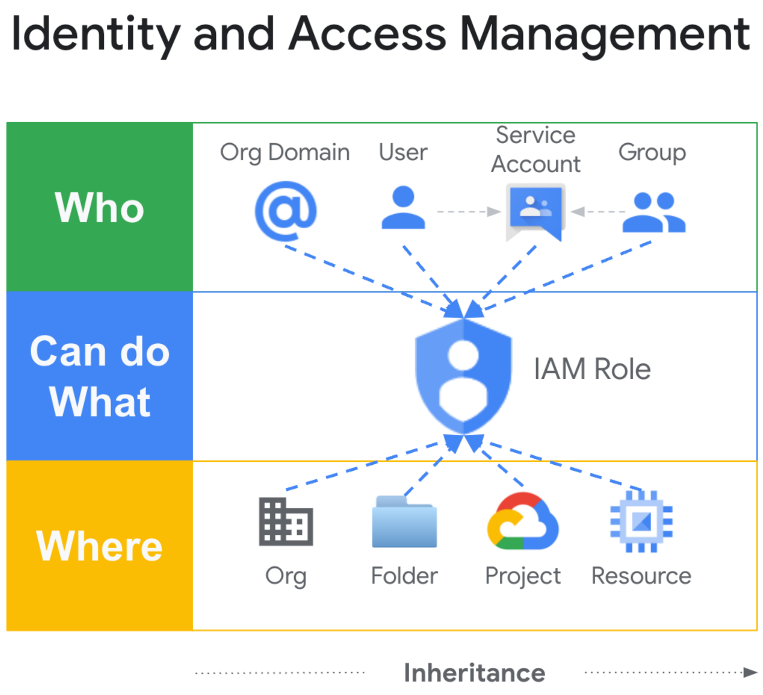
By environment design



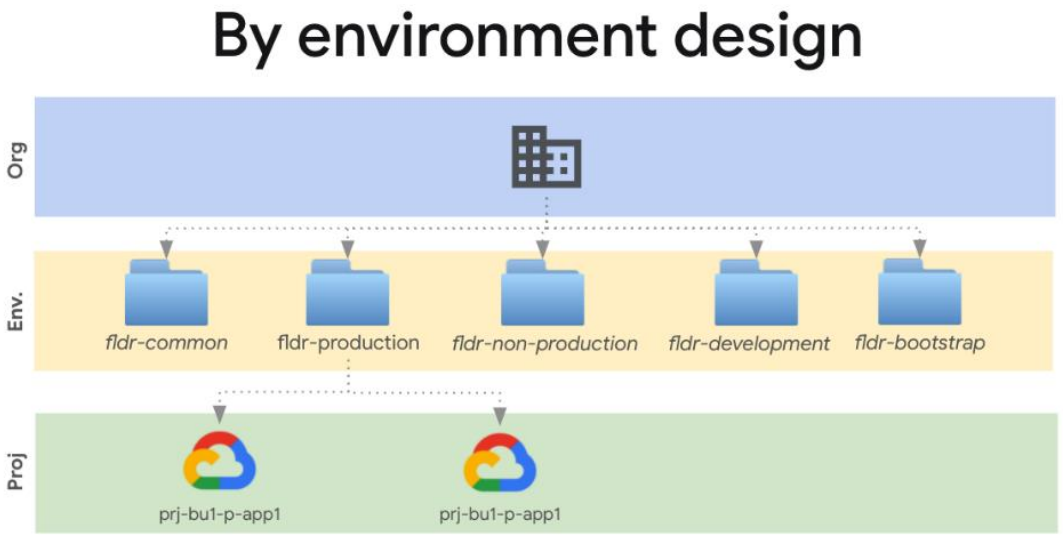
By business unit, environment, and team



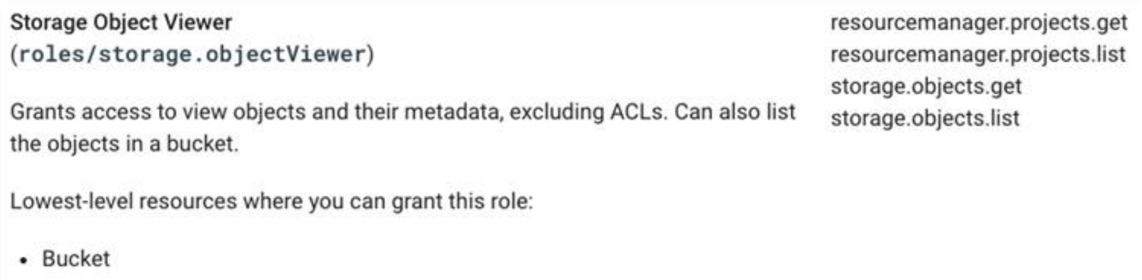
Chapter 5: Controlling Access with IAM Roles



Identity and Access Management



By environment design



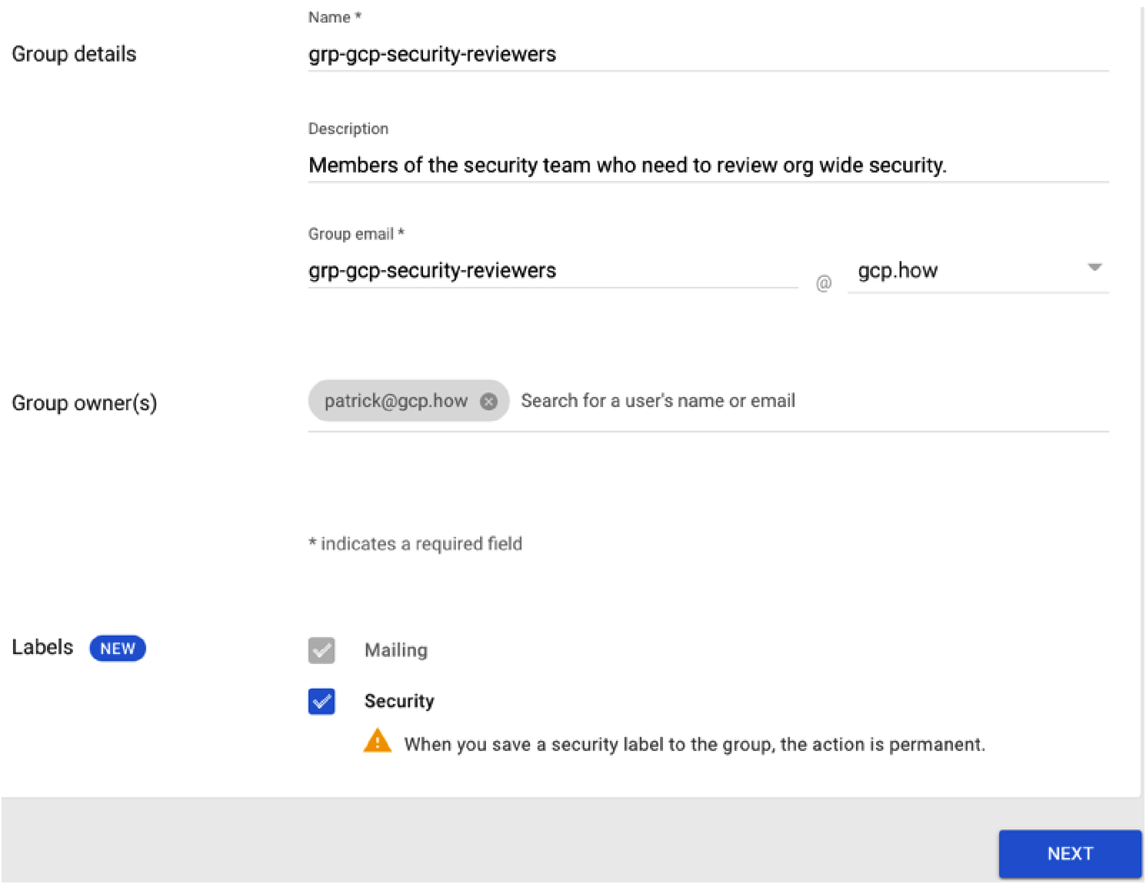
Storage Object Viewer
(`roles/storage.objectViewer`)

Grants access to view objects and their metadata, excluding ACLs. Can also list the objects in a bucket.

Lowest-level resources where you can grant this role:

- Bucket

resourcemanager.projects.get
resourcemanager.projects.list
storage.objects.get
storage.objects.list



Group details

Name *

grp-gcp-security-reviewers

Description

Members of the security team who need to review org wide security.

Group email *

grp-gcp-security-reviewers @ gcp.how

Group owner(s)

patrick@gcp.how

Search for a user's name or email

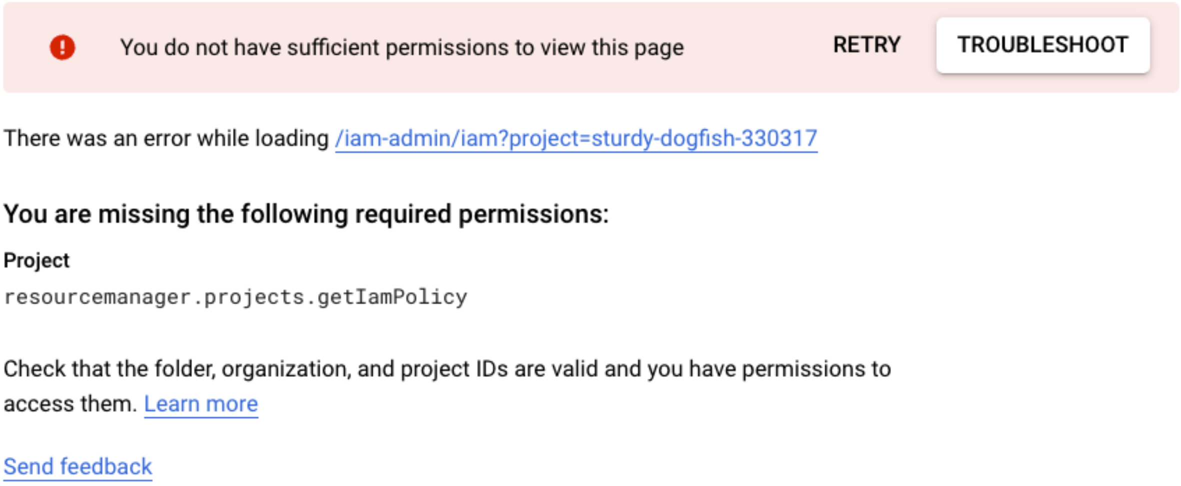
* indicates a required field

Labels NEW

☑ Mailing

☑ Security

When you save a security label to the group, the action is permanent.



You do not have sufficient permissions to view this page

There was an error while loading /iam-admin/iam?project=sturdy-dogfish-330317

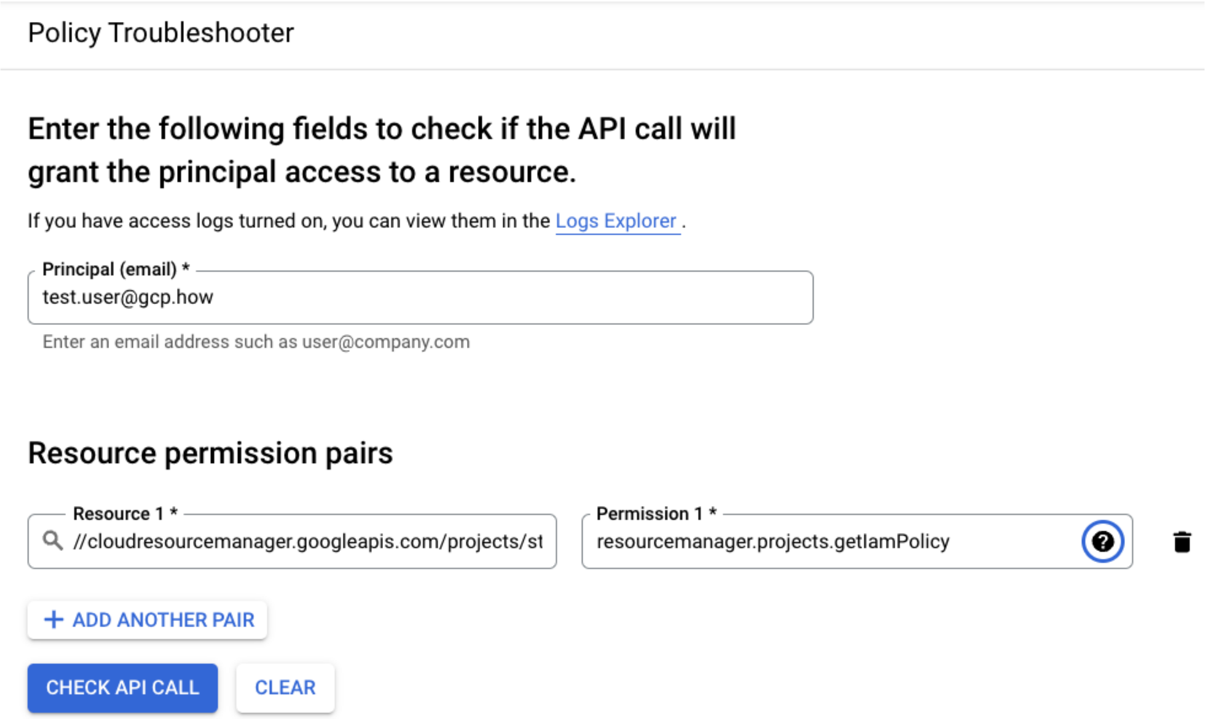
You are missing the following required permissions:

Project

```
resourcemanager.projects.getIamPolicy
```

Check that the folder, organization, and project IDs are valid and you have permissions to access them. Learn more

Send feedback



Policy Troubleshooter

Enter the following fields to check if the API call will grant the principal access to a resource.

If you have access logs turned on, you can view them in the Logs Explorer .

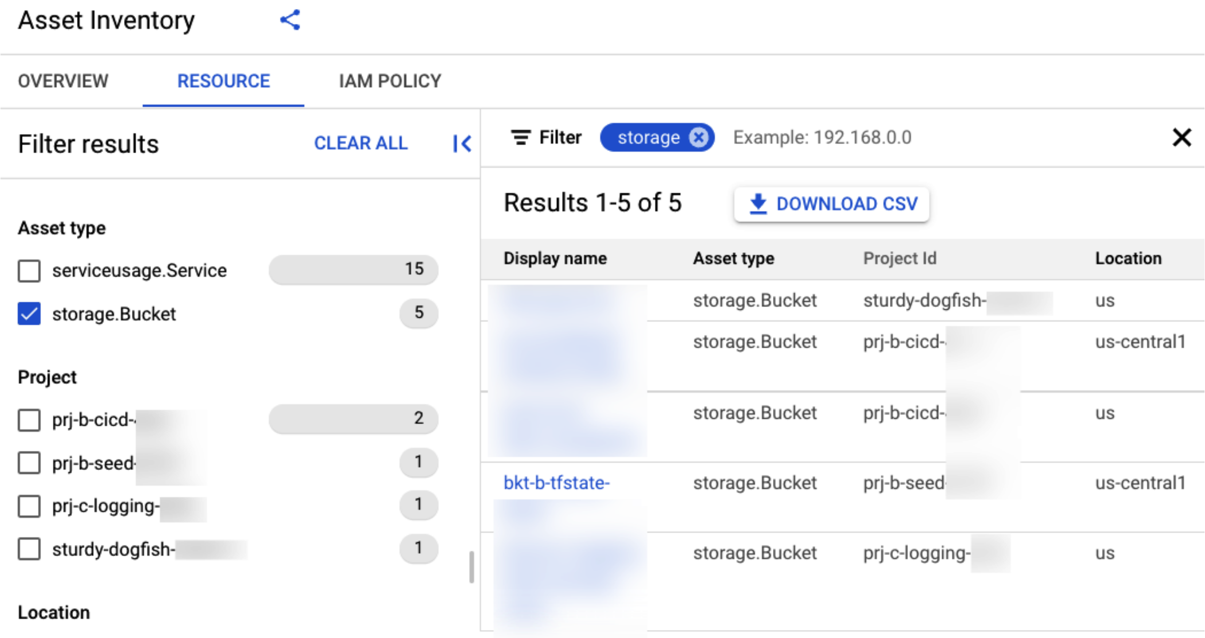
Principal (email) *: test.user@gcp.how

Enter an email address such as user@company.com

Resource permission pairs

Resource 1 *: //cloudresourcemanager.googleapis.com/projects/st

Permission 1 *: resourcemanager.projects.getIamPolicy



Asset Inventory

Filter results

Asset type

- ☐ serviceusage.Service 15
- ☑ storage.Bucket 5

Project

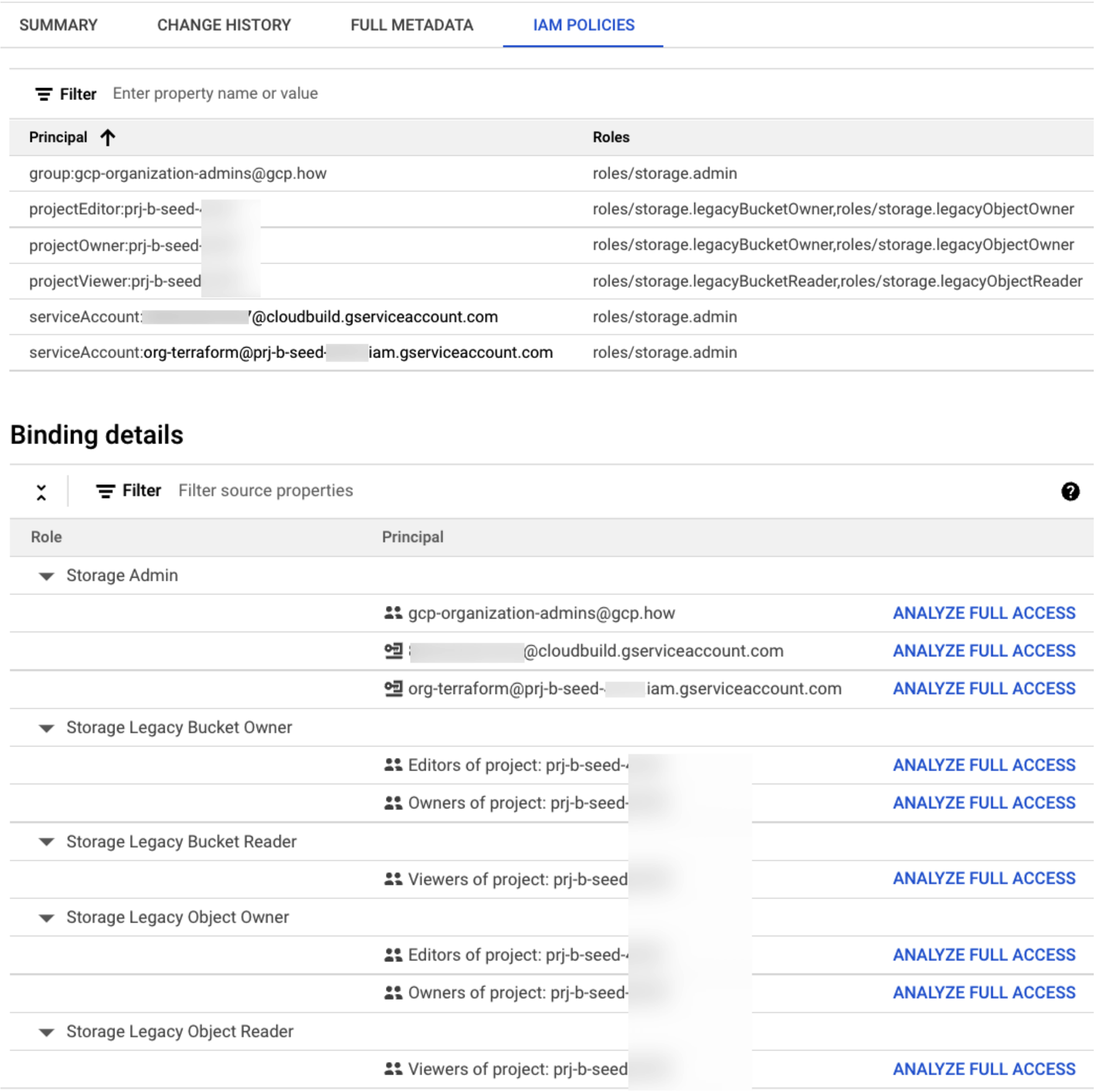
- ☐ prj-b-cicd-[redacted] 2
- ☐ prj-b-seed-[redacted] 1
- ☐ prj-c-logging-[redacted] 1
- ☐ sturdy-dogfish-[redacted] 1

Location

Filter: storage ⊗ Example: 192.168.0.0

Results 1-5 of 5

Display name	Asset type	Project Id	Location
[redacted]	storage.Bucket	sturdy-dogfish-[redacted]	us
[redacted]	storage.Bucket	prj-b-cicd-[redacted]	us-central1
[redacted]	storage.Bucket	prj-b-cicd-[redacted]	us
bkt-b-tfstate-[redacted]	storage.Bucket	prj-b-seed-[redacted]	us-central1
[redacted]	storage.Bucket	prj-c-logging-[redacted]	us



SUMMARY CHANGE HISTORY FULL METADATA **IAM POLICIES**

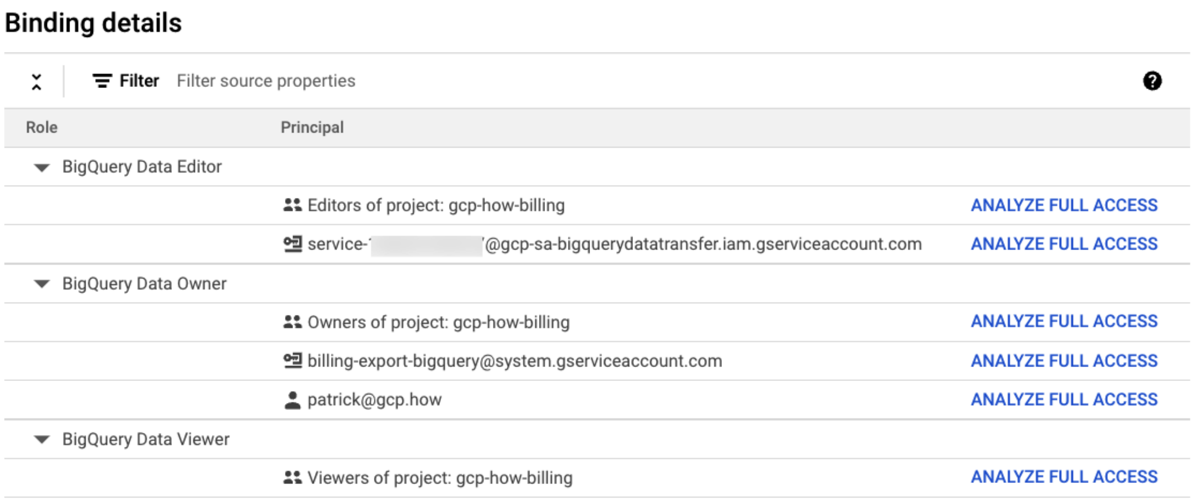
Filter Enter property name or value

Principal ↑	Roles
group:gcp-organization-admins@gcp.how	roles/storage.admin
projectEditor:prj-b-seed-[redacted]	roles/storage.legacyBucketOwner,roles/storage.legacyObjectOwner
projectOwner:prj-b-seed-[redacted]	roles/storage.legacyBucketOwner,roles/storage.legacyObjectOwner
projectViewer:prj-b-seed[redacted]	roles/storage.legacyBucketReader,roles/storage.legacyObjectReader
serviceAccount:[redacted]'@cloudbuild.gserviceaccount.com	roles/storage.admin
serviceAccount:org-terraform@prj-b-seed-[redacted]iam.gserviceaccount.com	roles/storage.admin

Binding details

Filter Filter source properties

Role	Principal	
Storage Admin		
	gcp-organization-admins@gcp.how	ANALYZE FULL ACCESS
	[redacted]@cloudbuild.gserviceaccount.com	ANALYZE FULL ACCESS
	org-terraform@prj-b-seed-[redacted]iam.gserviceaccount.com	ANALYZE FULL ACCESS
Storage Legacy Bucket Owner		
	Editors of project: prj-b-seed-[redacted]	ANALYZE FULL ACCESS
	Owners of project: prj-b-seed-[redacted]	ANALYZE FULL ACCESS
Storage Legacy Bucket Reader		
	Viewers of project: prj-b-seed[redacted]	ANALYZE FULL ACCESS
Storage Legacy Object Owner		
	Editors of project: prj-b-seed-[redacted]	ANALYZE FULL ACCESS
	Owners of project: prj-b-seed-[redacted]	ANALYZE FULL ACCESS
Storage Legacy Object Reader		
	Viewers of project: prj-b-seed[redacted]	ANALYZE FULL ACCESS

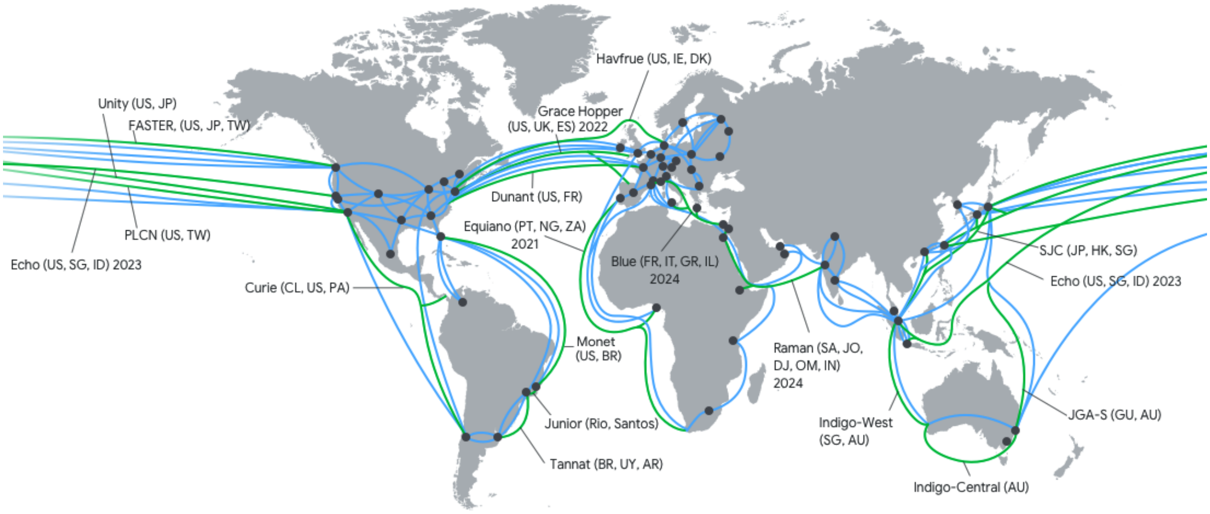


Binding details

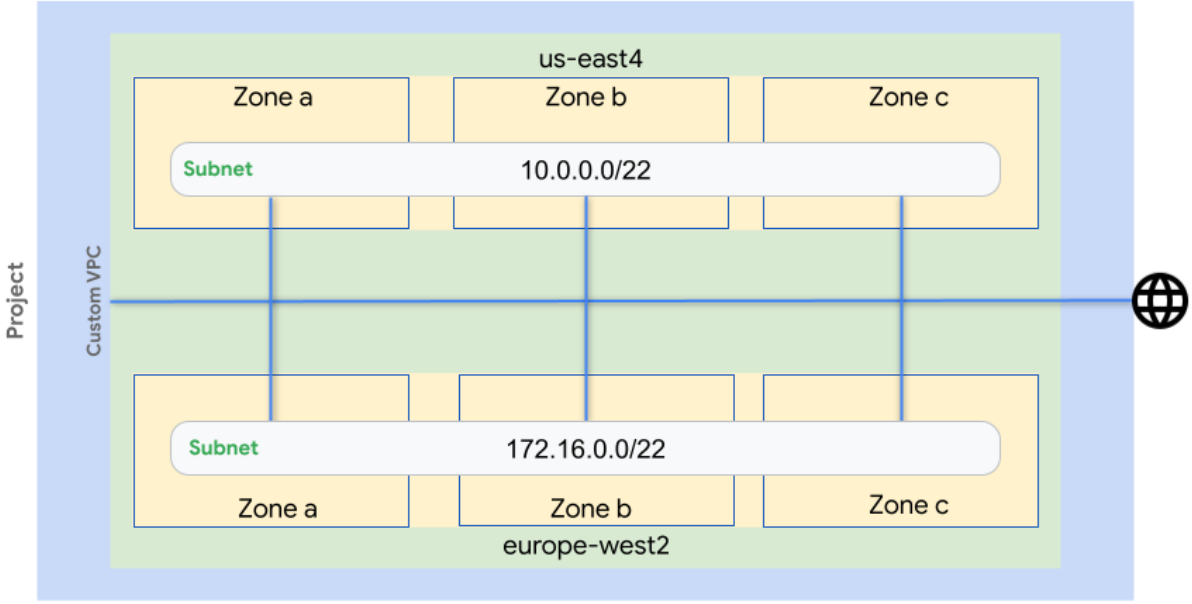
Filter Filter source properties

Role	Principal	
BigQuery Data Editor		
	Editors of project: gcp-how-billing	ANALYZE FULL ACCESS
	service-[redacted]@gcp-sa-bigquerydatatransfer.iam.gserviceaccount.com	ANALYZE FULL ACCESS
BigQuery Data Owner		
	Owners of project: gcp-how-billing	ANALYZE FULL ACCESS
	billing-export-bigquery@system.gserviceaccount.com	ANALYZE FULL ACCESS
	patrick@gcp.how	ANALYZE FULL ACCESS
BigQuery Data Viewer		
	Viewers of project: gcp-how-billing	ANALYZE FULL ACCESS

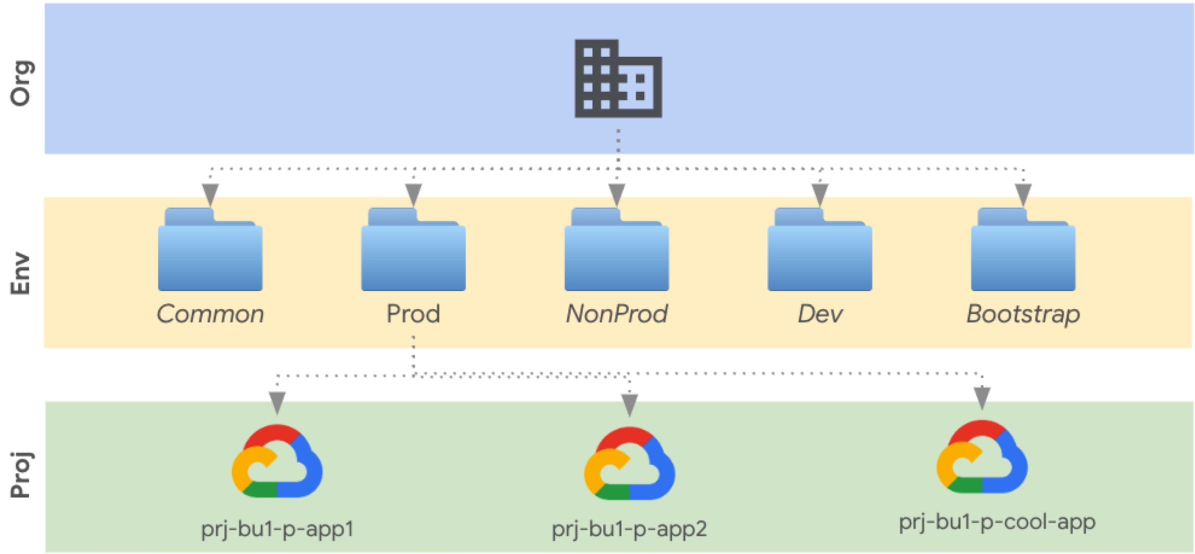
Chapter 6: Laying the Network

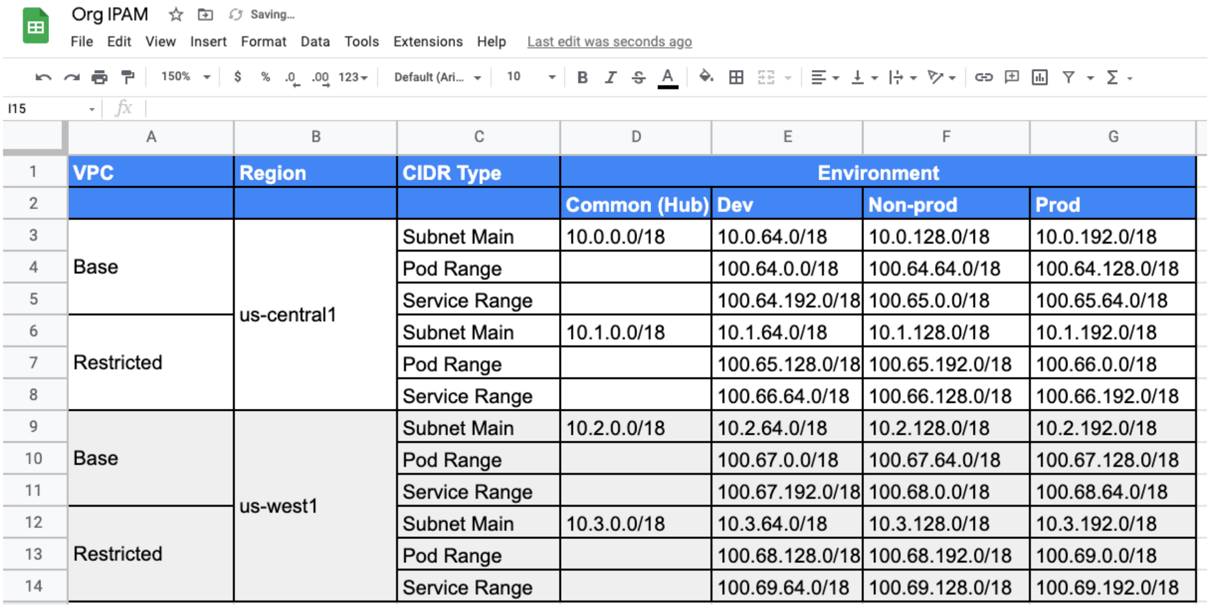


Simple VPC, 1 Project, 2 Regions



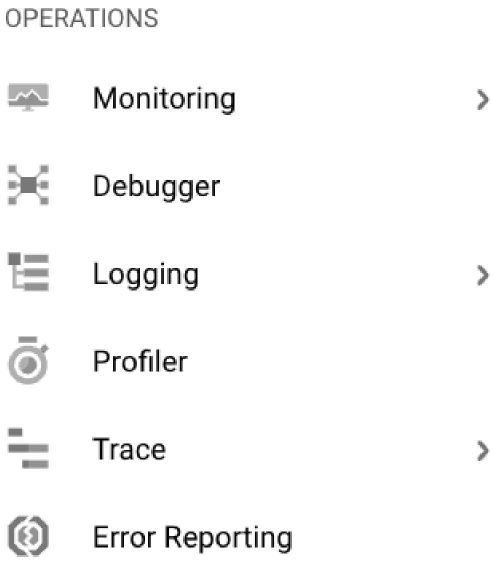
Cool App

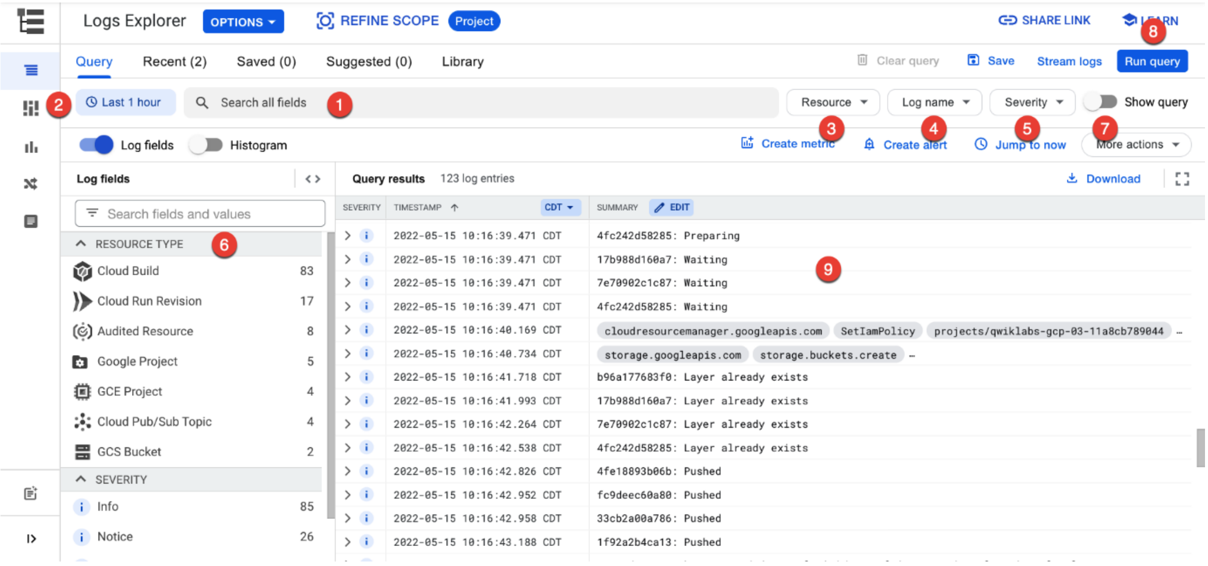




VPC	Region	CIDR Type	Environment			
			Common (Hub)	Dev	Non-prod	Prod
Base	us-central1	Subnet Main	10.0.0.0/18	10.0.64.0/18	10.0.128.0/18	10.0.192.0/18
		Pod Range		100.64.0.0/18	100.64.64.0/18	100.64.128.0/18
		Service Range		100.64.192.0/18	100.65.0.0/18	100.65.64.0/18
Restricted		Subnet Main	10.1.0.0/18	10.1.64.0/18	10.1.128.0/18	10.1.192.0/18
		Pod Range		100.65.128.0/18	100.65.192.0/18	100.66.0.0/18
		Service Range		100.66.64.0/18	100.66.128.0/18	100.66.192.0/18
Base	us-west1	Subnet Main	10.2.0.0/18	10.2.64.0/18	10.2.128.0/18	10.2.192.0/18
		Pod Range		100.67.0.0/18	100.67.64.0/18	100.67.128.0/18
		Service Range		100.67.192.0/18	100.68.0.0/18	100.68.64.0/18
Restricted		Subnet Main	10.3.0.0/18	10.3.64.0/18	10.3.128.0/18	10.3.192.0/18
		Pod Range		100.68.128.0/18	100.68.192.0/18	100.69.0.0/18
		Service Range		100.69.64.0/18	100.69.128.0/18	100.69.192.0/18

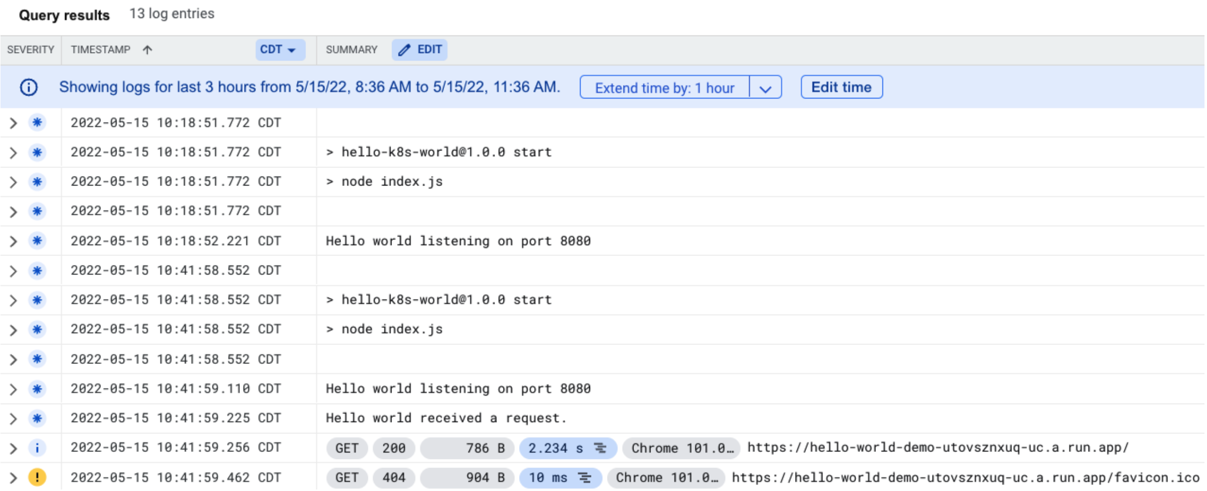
Chapter 7: Foundational Monitoring and Logging





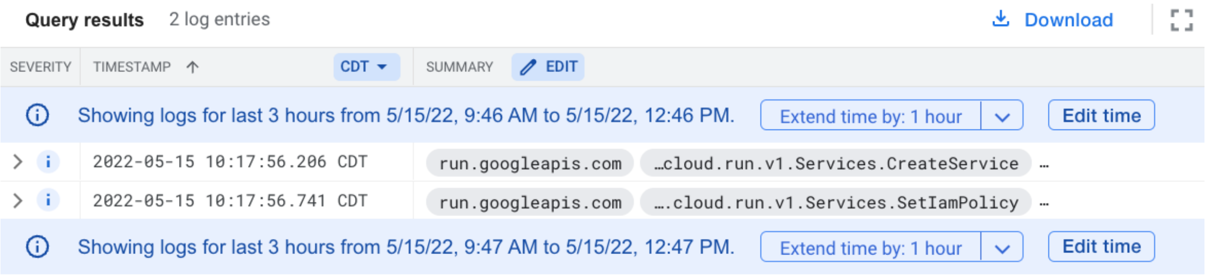
RESOURCE TYPE	
Cloud Build	83
Cloud Run Revision	17
Audited Resource	8
Google Project	5
GCE Project	4
Cloud Pub/Sub Topic	4
GCS Bucket	2
SEVERITY	
Info	85
Notice	26

```
2022-05-15 10:16:39.471 CDT   4fc242d58285: Preparing
2022-05-15 10:16:39.471 CDT   17b988d160a7: Waiting
2022-05-15 10:16:39.471 CDT   7e70902c1c87: Waiting
2022-05-15 10:16:39.471 CDT   4fc242d58285: Waiting
2022-05-15 10:16:40.169 CDT   cloudresourcemanager.googleapis.com  SetIamPolicy  projects/qwiklabs-gcp-03-11a8cb789044 …
2022-05-15 10:16:40.734 CDT   storage.googleapis.com  storage.buckets.create …
2022-05-15 10:16:41.718 CDT   b96a177683f0: Layer already exists
2022-05-15 10:16:41.993 CDT   17b988d160a7: Layer already exists
2022-05-15 10:16:42.264 CDT   7e70902c1c87: Layer already exists
2022-05-15 10:16:42.538 CDT   4fc242d58285: Layer already exists
2022-05-15 10:16:42.826 CDT   4fe18893b06b: Pushed
2022-05-15 10:16:42.952 CDT   fc9deec60a80: Pushed
2022-05-15 10:16:42.958 CDT   33cb2a00a786: Pushed
2022-05-15 10:16:43.188 CDT   1f92a2b4ca13: Pushed
```



Showing logs for last 3 hours from 5/15/22, 8:36 AM to 5/15/22, 11:36 AM.

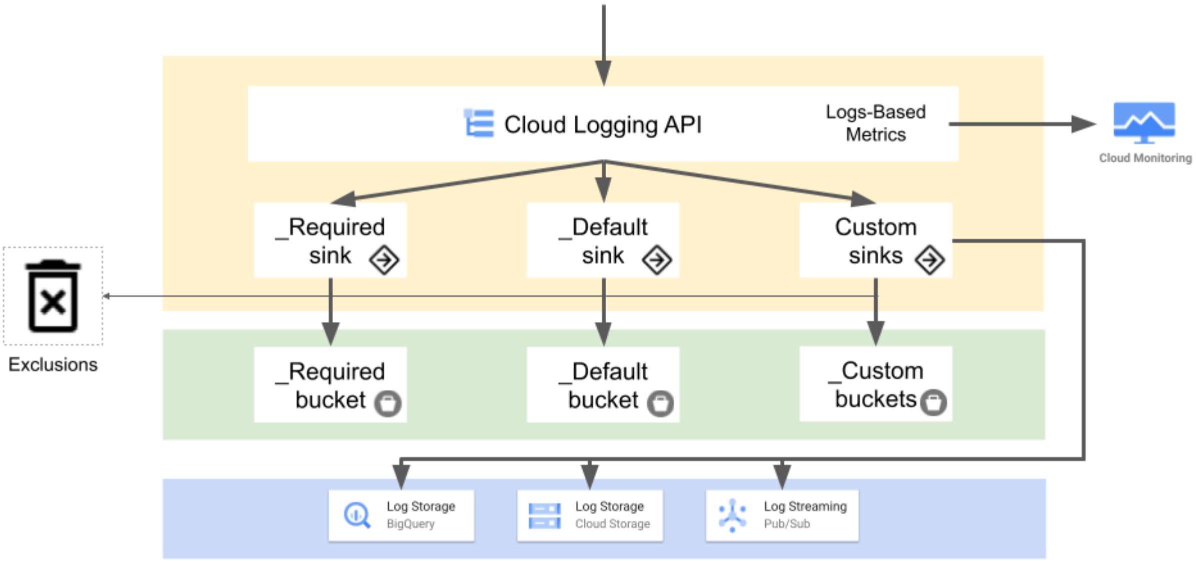
```
2022-05-15 10:18:51.772 CDT
2022-05-15 10:18:51.772 CDT   > hello-k8s-world@1.0.0 start
2022-05-15 10:18:51.772 CDT   > node index.js
2022-05-15 10:18:51.772 CDT
2022-05-15 10:18:52.221 CDT   Hello world listening on port 8080
2022-05-15 10:41:58.552 CDT
2022-05-15 10:41:58.552 CDT   > hello-k8s-world@1.0.0 start
2022-05-15 10:41:58.552 CDT   > node index.js
2022-05-15 10:41:58.552 CDT
2022-05-15 10:41:59.110 CDT   Hello world listening on port 8080
2022-05-15 10:41:59.225 CDT   Hello world received a request.
2022-05-15 10:41:59.256 CDT   GET  200   786 B  2.234 s  Chrome 101.0…  https://hello-world-demo-utovsznxuq-uc.a.run.app/
2022-05-15 10:41:59.462 CDT   GET  404   904 B  10 ms  Chrome 101.0…  https://hello-world-demo-utovsznxuq-uc.a.run.app/favicon.ico
```

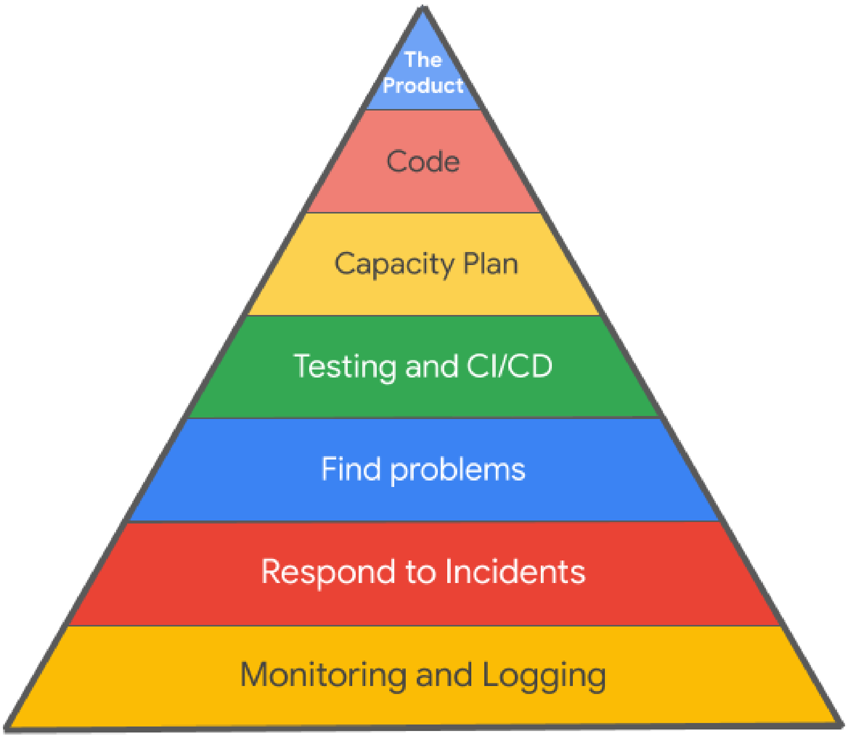


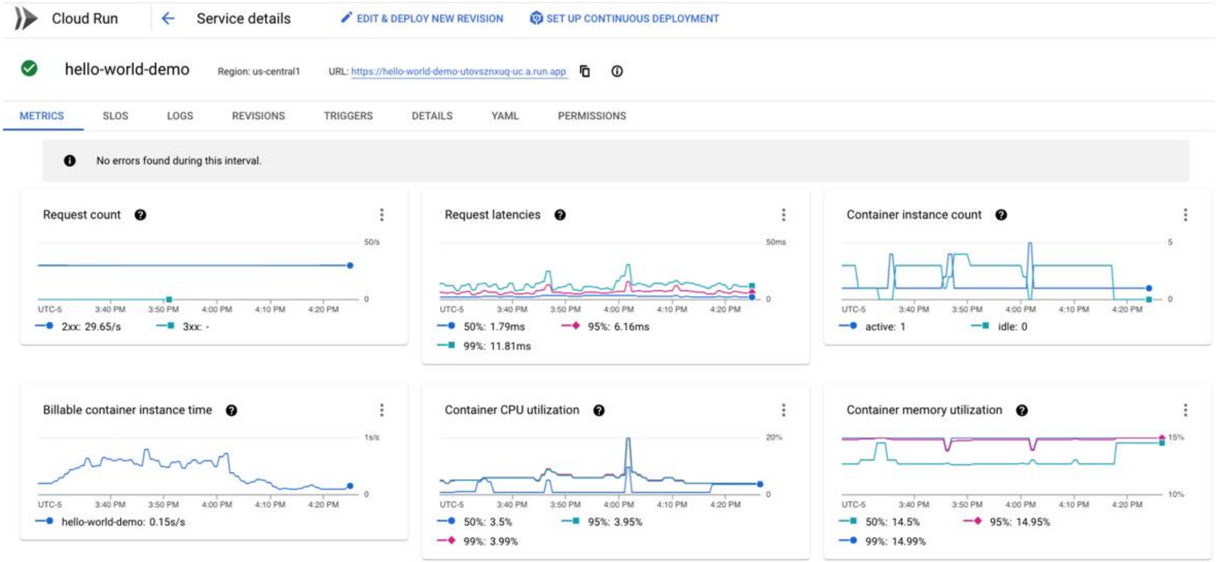
Showing logs for last 3 hours from 5/15/22, 9:46 AM to 5/15/22, 12:46 PM.

```
2022-05-15 10:17:56.206 CDT   run.googleapis.com   …cloud.run.v1.Services.CreateService …
2022-05-15 10:17:56.741 CDT   run.googleapis.com   ….cloud.run.v1.Services.SetIamPolicy …
```

Showing logs for last 3 hours from 5/15/22, 9:47 AM to 5/15/22, 12:47 PM.







hello-world-demo Region: us-central1 URL: https://hello-world-demo-utovsznxuq-uc.a.run.app

No errors found during this interval.

Request count: 2xx: 29.65/s 3xx: -

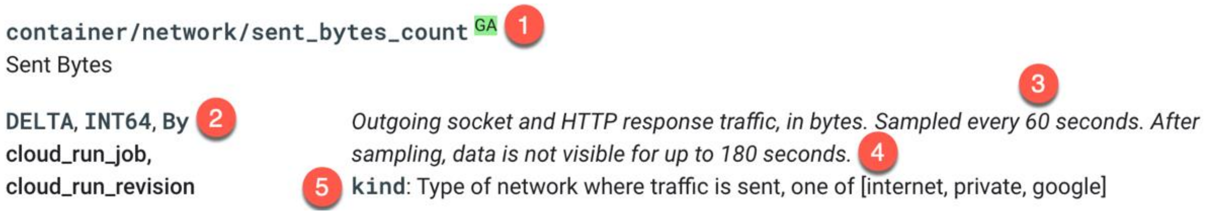
Request latencies: 50%: 1.79ms 95%: 6.16ms 99%: 11.81ms

Container instance count: active: 1 idle: 0

Billable container instance time: hello-world-demo: 0.15s/s

Container CPU utilization: 50%: 3.5% 95%: 3.95% 99%: 3.99%

Container memory utilization: 50%: 14.5% 95%: 14.95% 99%: 14.99%



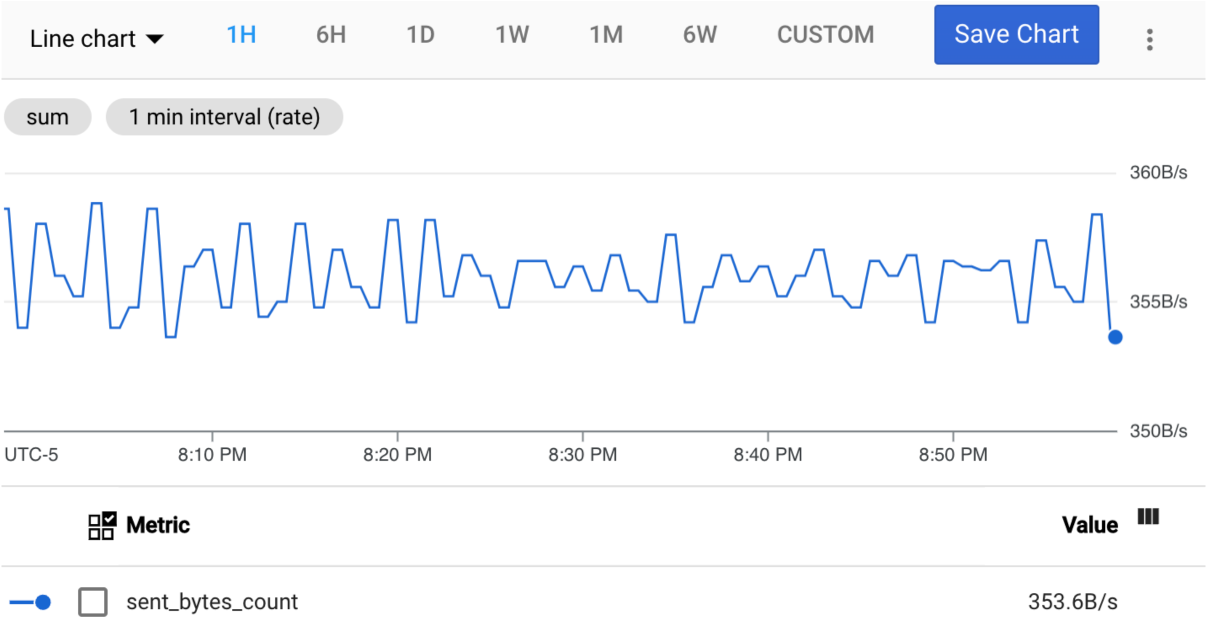
`container/network/sent_bytes_count` GA

Sent Bytes

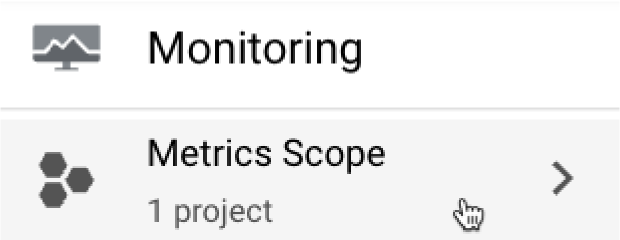
DELTA, INT64, By
cloud_run_job,
cloud_run_revision

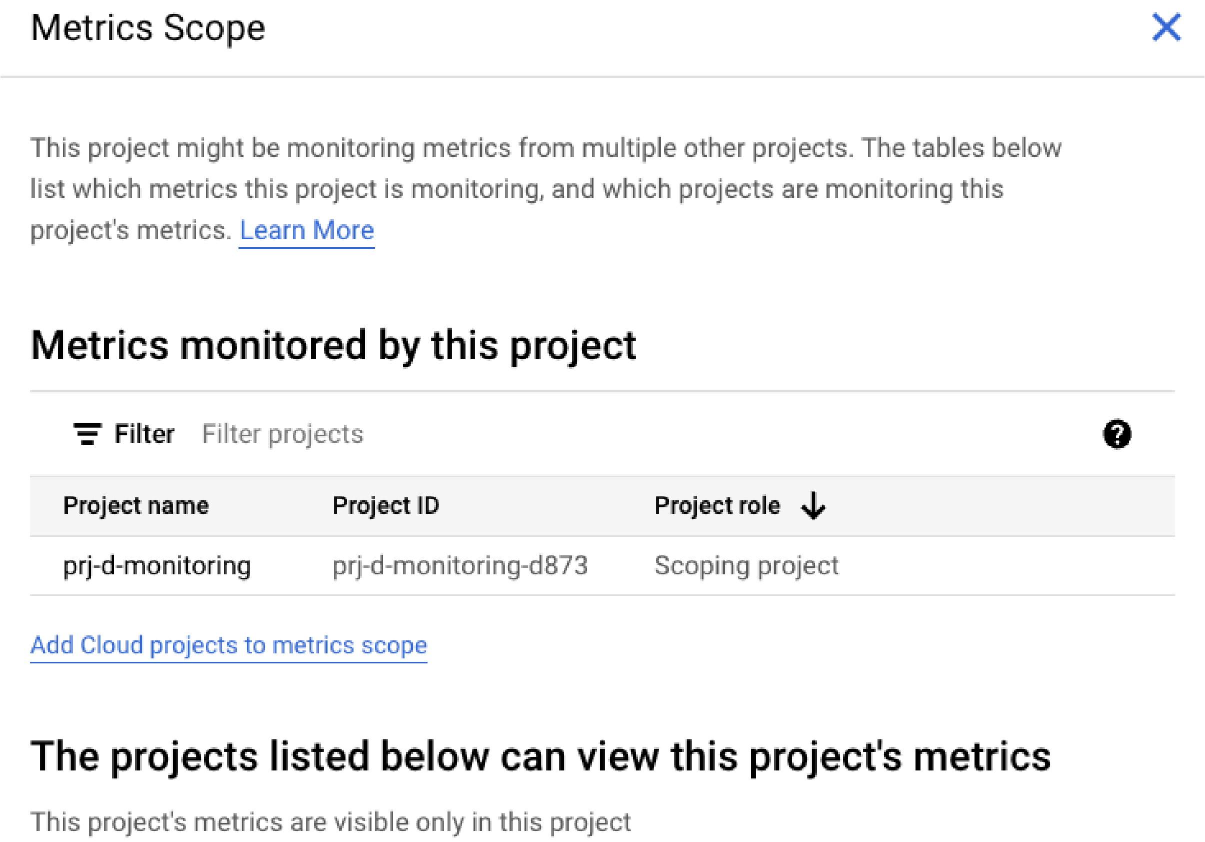
Outgoing socket and HTTP response traffic, in bytes. Sampled every 60 seconds. After sampling, data is not visible for up to 180 seconds.

`kind`: Type of network where traffic is sent, one of [internet, private, google]



Metric	Value
sent_bytes_count	353.6B/s





Metrics Scope

This project might be monitoring metrics from multiple other projects. The tables below list which metrics this project is monitoring, and which projects are monitoring this project's metrics. Learn More

Metrics monitored by this project

Filter Filter projects

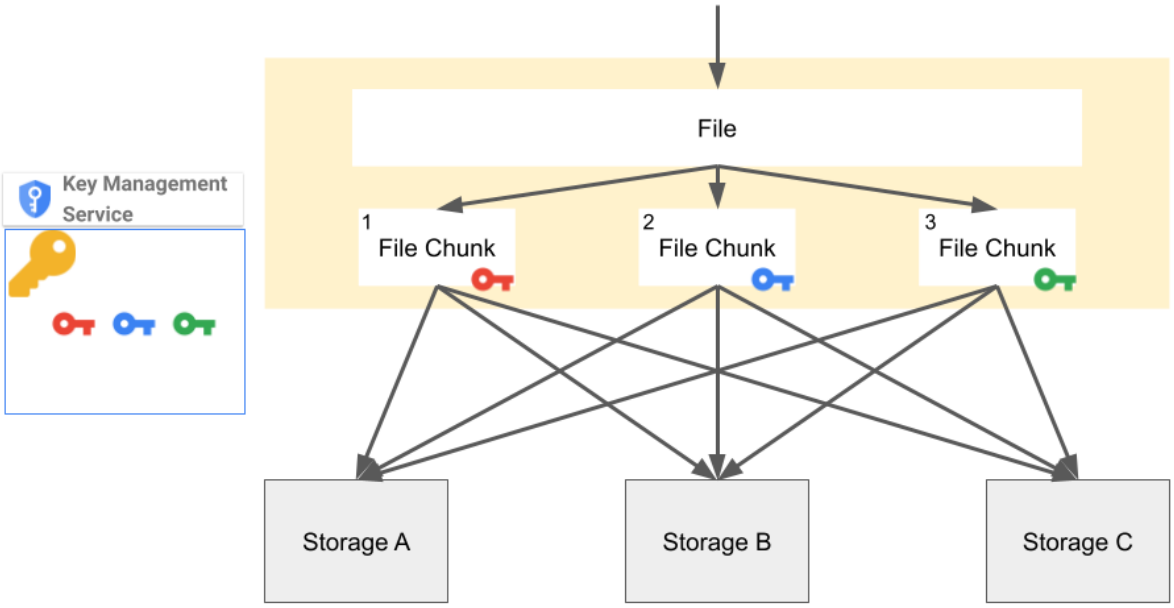
Project name	Project ID	Project role ↓
prj-d-monitoring	prj-d-monitoring-d873	Scoping project

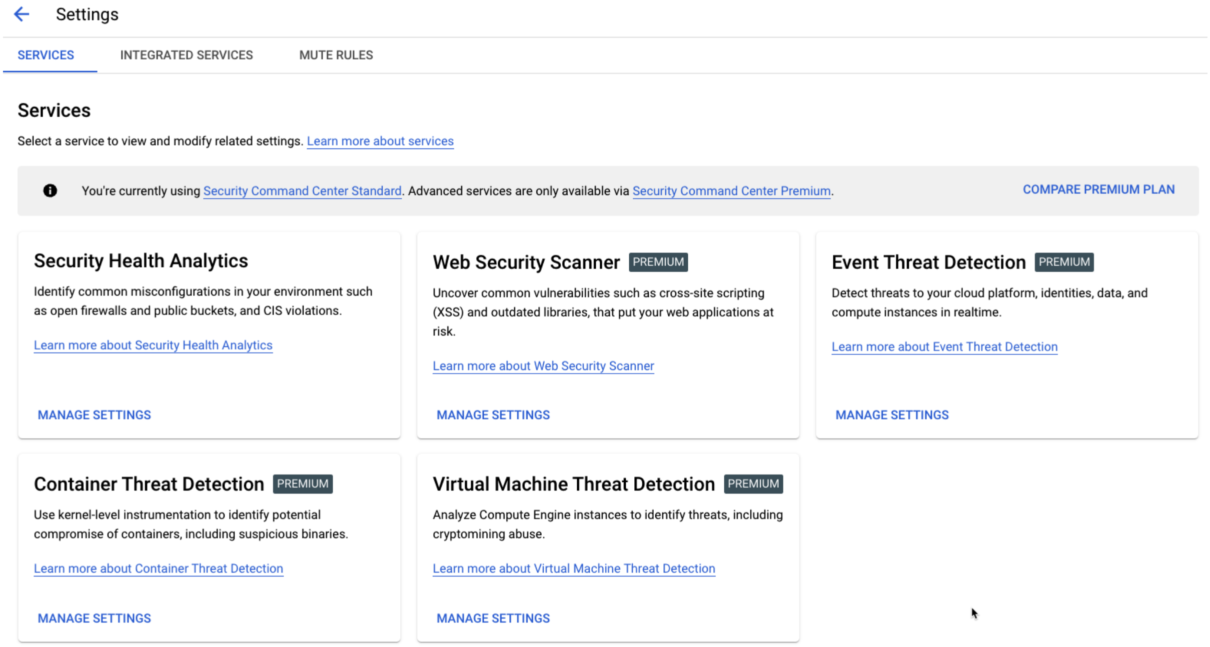
Add Cloud projects to metrics scope

The projects listed below can view this project's metrics

This project's metrics are visible only in this project

Chapter 8: Augmenting Security and Registering for Support





Services

Select a service to view and modify related settings. Learn more about services

You're currently using Security Command Center Standard. Advanced services are only available via Security Command Center Premium.

COMPARE PREMIUM PLAN

Security Health Analytics

Identify common misconfigurations in your environment such as open firewalls and public buckets, and CIS violations.

Learn more about Security Health Analytics

MANAGE SETTINGS

Web Security Scanner PREMIUM

Uncover common vulnerabilities such as cross-site scripting (XSS) and outdated libraries, that put your web applications at risk.

Learn more about Web Security Scanner

MANAGE SETTINGS

Event Threat Detection PREMIUM

Detect threats to your cloud platform, identities, data, and compute instances in realtime.

Learn more about Event Threat Detection

MANAGE SETTINGS

Container Threat Detection PREMIUM

Use kernel-level instrumentation to identify potential compromise of containers, including suspicious binaries.

Learn more about Container Threat Detection

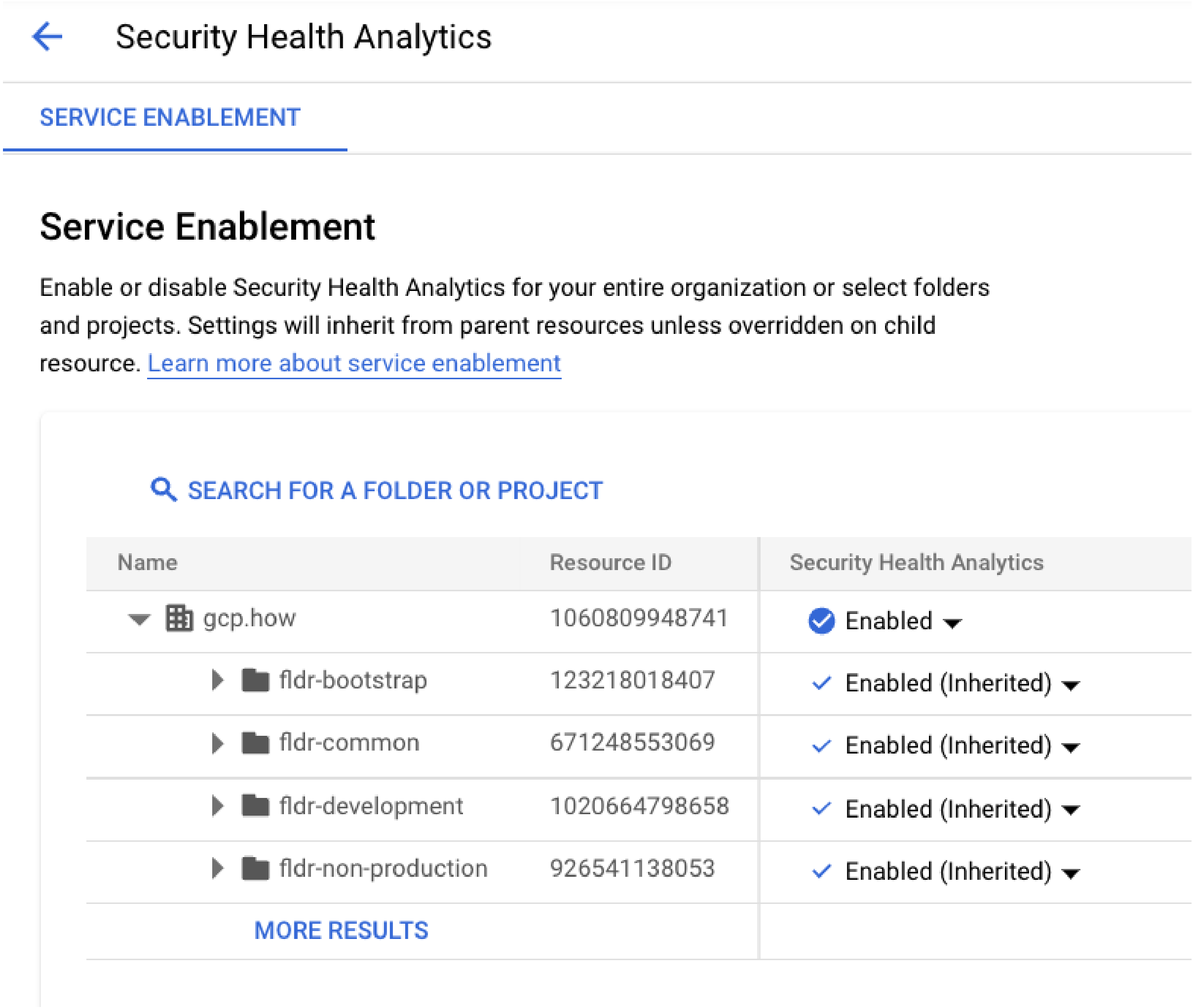
MANAGE SETTINGS

Virtual Machine Threat Detection PREMIUM

Analyze Compute Engine instances to identify threats, including cryptomining abuse.

Learn more about Virtual Machine Threat Detection

MANAGE SETTINGS



Security Health Analytics

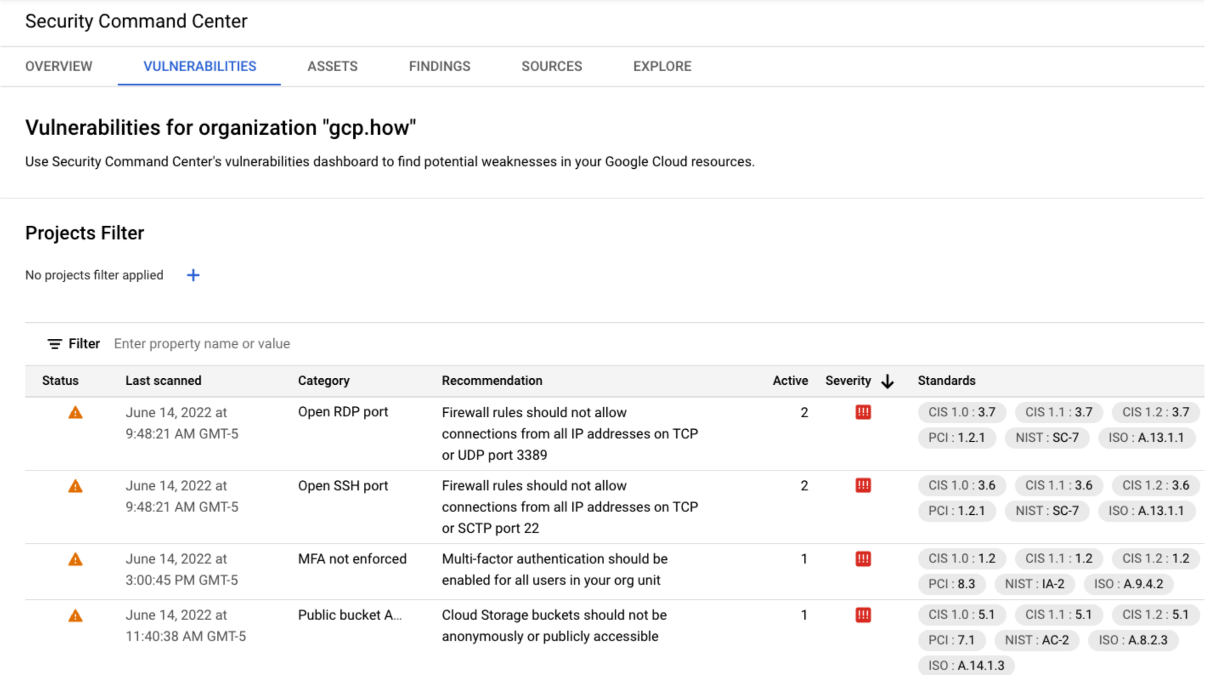
SERVICE ENABLEMENT

Service Enablement

Enable or disable Security Health Analytics for your entire organization or select folders and projects. Settings will inherit from parent resources unless overridden on child resource. Learn more about service enablement

SEARCH FOR A FOLDER OR PROJECT

Name	Resource ID	Security Health Analytics
▼ gcp.how	1060809948741	✓ Enabled ▼
▶ fldr-bootstrap	123218018407	✓ Enabled (Inherited) ▼
▶ fldr-common	671248553069	✓ Enabled (Inherited) ▼
▶ fldr-development	1020664798658	✓ Enabled (Inherited) ▼
▶ fldr-non-production	926541138053	✓ Enabled (Inherited) ▼
MORE RESULTS		



Security Command Center

Vulnerabilities for organization "gcp.how"

Use Security Command Center's vulnerabilities dashboard to find potential weaknesses in your Google Cloud resources.

Projects Filter

No projects filter applied +

Filter Enter property name or value

Status	Last scanned	Category	Recommendation	Active	Severity ↓	Standards
⚠	June 14, 2022 at 9:48:21 AM GMT-5	Open RDP port	Firewall rules should not allow connections from all IP addresses on TCP or UDP port 3389	2	!!!	CIS 1.0 : 3.7 CIS 1.1 : 3.7 CIS 1.2 : 3.7 PCI : 1.2.1 NIST : SC-7 ISO : A.13.1.1
⚠	June 14, 2022 at 9:48:21 AM GMT-5	Open SSH port	Firewall rules should not allow connections from all IP addresses on TCP or SCTP port 22	2	!!!	CIS 1.0 : 3.6 CIS 1.1 : 3.6 CIS 1.2 : 3.6 PCI : 1.2.1 NIST : SC-7 ISO : A.13.1.1
⚠	June 14, 2022 at 3:00:45 PM GMT-5	MFA not enforced	Multi-factor authentication should be enabled for all users in your org unit	1	!!!	CIS 1.0 : 1.2 CIS 1.1 : 1.2 CIS 1.2 : 1.2 PCI : 8.3 NIST : IA-2 ISO : A.9.4.2
⚠	June 14, 2022 at 11:40:38 AM GMT-5	Public bucket A...	Cloud Storage buckets should not be anonymously or publicly accessible	1	!!!	CIS 1.0 : 5.1 CIS 1.1 : 5.1 CIS 1.2 : 5.1 PCI : 7.1 NIST : AC-2 ISO : A.8.2.3 ISO : A.14.1.3