KAZAKH KBTU BRITISH
TECHNICAL
UNIVERSITY

Application Security Best Practices and Scaling Applications on Google Cloud

Student: Islam Aip

Course: Cloud application development

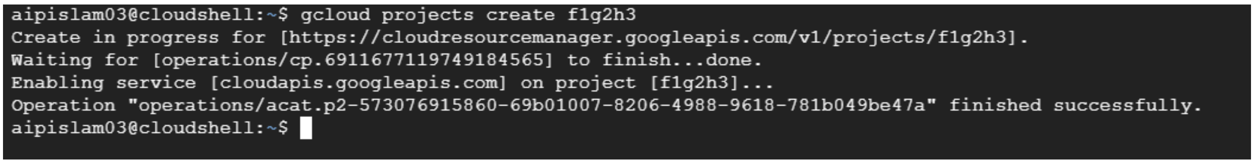
Date: 24.11.2024

Almaty, 2024

Introduction

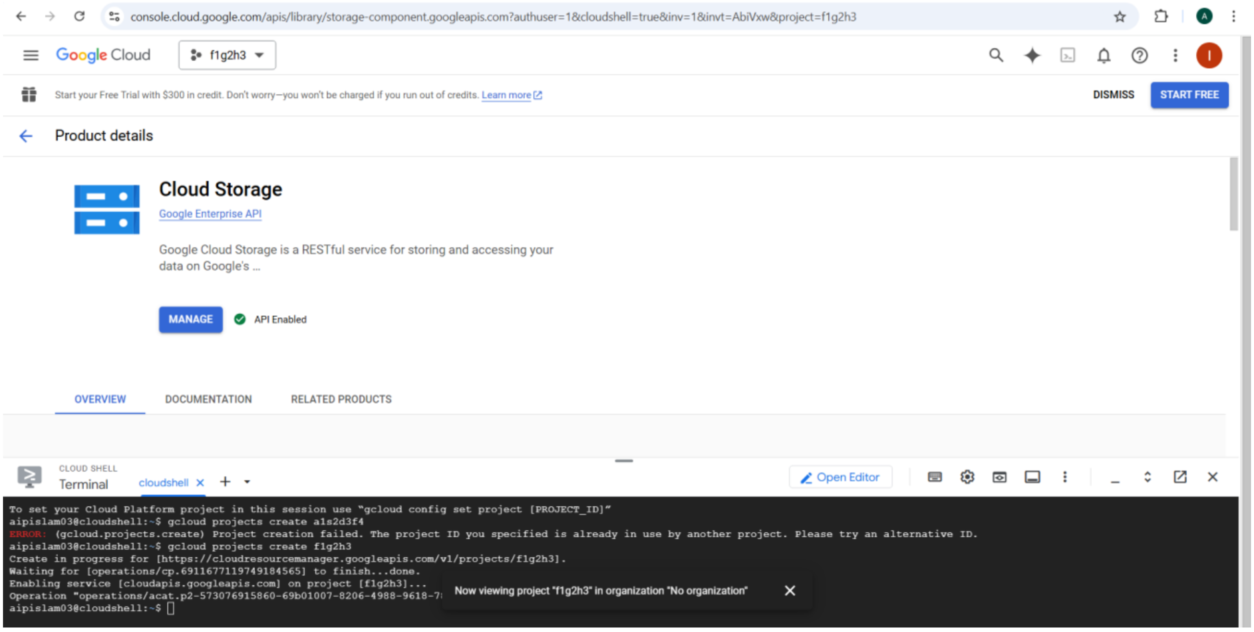
Application Security Best Practices

1. Google Cloud Project



```
aipislam03@cloudshell:~$ gcloud projects create f1g2h3
Create in progress for [https://cloudresourcemanager.googleapis.com/v1/projects/f1g2h3].
Waiting for [operations/cp.6911677119749184565] to finish...done.
Enabling service [cloudapis.googleapis.com] on project [f1g2h3]...
Operation "operations/acat.p2-573076915860-69b01007-8206-4988-9618-781b049be47a" finished successfully.
aipislam03@cloudshell:~$ █
```

Let’s create a new GCP project and enable all necessary APIs.



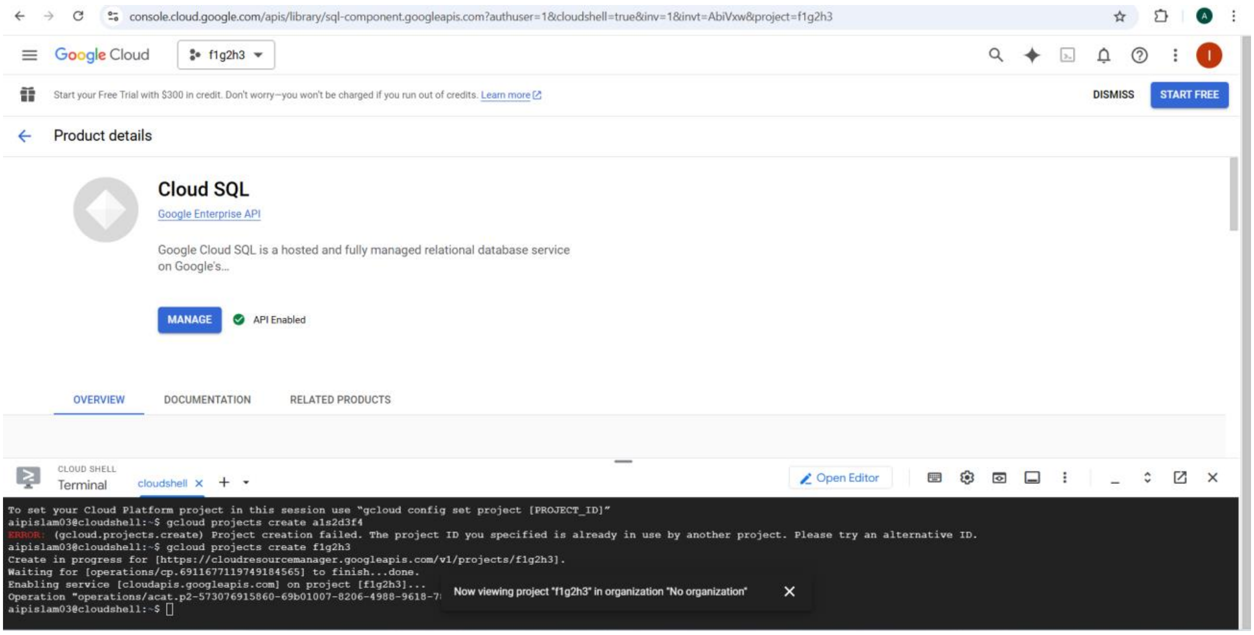
console.cloud.google.com/apis/library/storage-component.googleapis.com?authuser=1&cloudshell=true&inv=1&invt=AbiVxw&project=f1g2h3
Google Cloud
f1g2h3
Start your Free Trial with $300 in credit. Don't worry—you won't be charged if you run out of credits. Learn more
DISMISS
START FREE
Product details
Cloud Storage
Google Enterprise API

Google Cloud Storage is a RESTful service for storing and accessing your data on Google's ...

MANAGE
API Enabled
OVERVIEW
DOCUMENTATION
RELATED PRODUCTS
CLOUD SHELL
Terminal
cloudshell
Open Editor

```
To set your Cloud Platform project in this session use "gcloud config set project [PROJECT_ID]"
aipislam03@cloudshell:~$ gcloud projects create a1s2d3f4
ERROR: (gcloud.projects.create) Project creation failed. The project ID you specified is already in use by another project. Please try an alternative ID.
aipislam03@cloudshell:~$ gcloud projects create f1g2h3
Create in progress for [https://cloudresourcemanager.googleapis.com/v1/projects/f1g2h3].
Waiting for [operations/cp.6911677119749184565] to finish...done.
Enabling service [cloudapis.googleapis.com] on project [f1g2h3]...
Operation "operations/acat.p2-573076915860-69b01007-8206-4988-9618-7
aipislam03@cloudshell:~$ 
```

Now viewing project "f1g2h3" in organization "No organization"



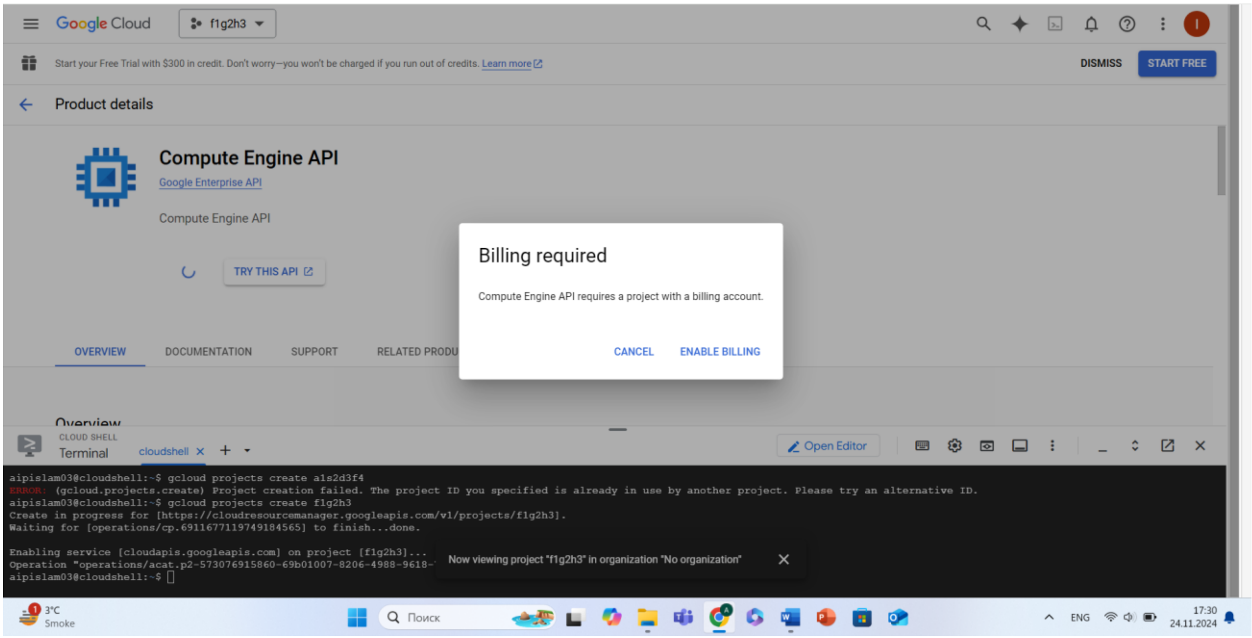
console.cloud.google.com/apis/library/sql-component.googleapis.com?authuser=1&cloudshell=true&inv=1&invt=AbiVxw&project=f1g2h3
Google Cloud
f1g2h3
Start your Free Trial with $300 in credit. Don't worry—you won't be charged if you run out of credits. Learn more
DISMISS
START FREE
Product details
Cloud SQL
Google Enterprise API

Google Cloud SQL is a hosted and fully managed relational database service on Google's...

MANAGE
API Enabled
OVERVIEW
DOCUMENTATION
RELATED PRODUCTS
CLOUD SHELL
Terminal
cloudshell
Open Editor

```
To set your Cloud Platform project in this session use "gcloud config set project [PROJECT_ID]"
aipislam03@cloudshell:~$ gcloud projects create a1s2d3f4
ERROR: (gcloud.projects.create) Project creation failed. The project ID you specified is already in use by another project. Please try an alternative ID.
aipislam03@cloudshell:~$ gcloud projects create f1g2h3
Create in progress for [https://cloudresourcemanager.googleapis.com/v1/projects/f1g2h3].
Waiting for [operations/cp.6911677119749184565] to finish...done.
Enabling service [cloudapis.googleapis.com] on project [f1g2h3]...
Operation "operations/acat.p2-573076915860-69b01007-8206-4988-9618-7
aipislam03@cloudshell:~$ 
```

Now viewing project "f1g2h3" in organization "No organization"



Billing required

Compute Engine API requires a project with a billing account.

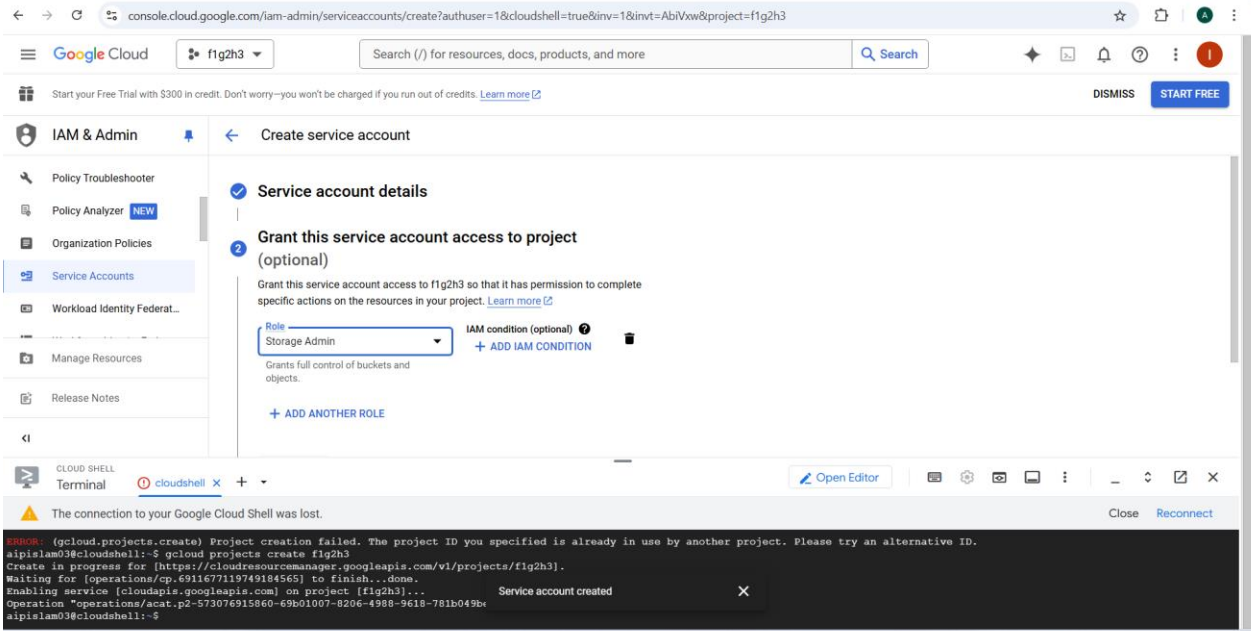
```
aipislam03@cloudshell:~$ gcloud projects create a1s2d3f4
ERROR: (gcloud.projects.create) Project creation failed. The project ID you specified is already in use by another project. Please try an alternative ID.
aipislam03@cloudshell:~$ gcloud projects create f1g2h3
Create in progress for [https://cloudresourcemanager.googleapis.com/v1/projects/f1g2h3].
Waiting for [operations/cp.6911677119749184565] to finish...done.

Enabling service [cloudapis.googleapis.com] on project [f1g2h3]...
Operation "operations/acat.p2-573076915860-69b01007-8206-4988-9618-
aipislam03@cloudshell:~$ 
```

Now viewing project "f1g2h3" in organization "No organization"

For some APIs billing should be enabled.

2. Identity and Access Management

Now let’s create a service account and grant access to project.



console.cloud.google.com/iam-admin/serviceaccounts/create?authuser=1&cloudshell=true&inv=1&invt=AbiVxw&project=f1g2h3

Create service account

Service account details

Grant this service account access to project (optional)

Grant this service account access to f1g2h3 so that it has permission to complete specific actions on the resources in your project. Learn more

Role: Storage Admin

Grants full control of buckets and objects.

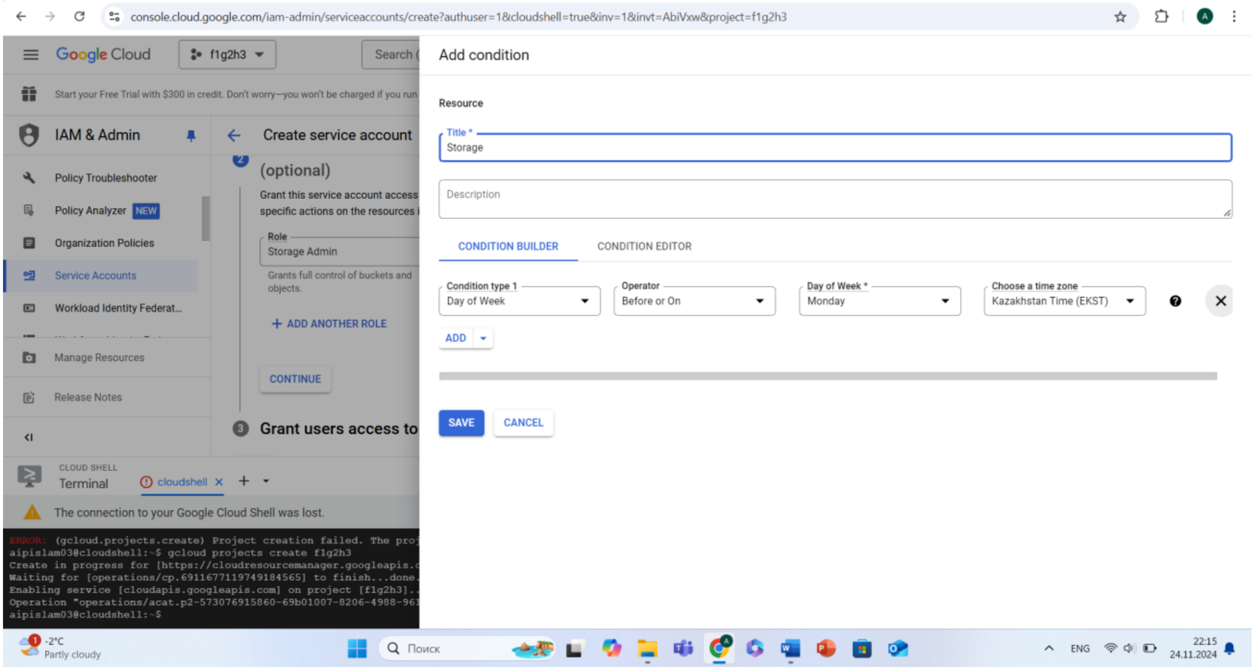
IAM condition (optional)

The connection to your Google Cloud Shell was lost.

```
ERROR: (gcloud.projects.create) Project creation failed. The project ID you specified is already in use by another project. Please try an alternative ID.
aipislam03@cloudshell:~$ gcloud projects create f1g2h3
Create in progress for [https://cloudresourcemanager.googleapis.com/v1/projects/f1g2h3].
Waiting for [operations/cp.6911677119749184565] to finish...done.
Enabling service [cloudapis.googleapis.com] on project [f1g2h3]...
Operation "operations/acat.p2-573076915860-69b01007-8206-4988-9618-781b049b
aipislam03@cloudshell:~$
```

Service account created

Now we can assign conditions based on attributes such as time, day of week and so on.



Start your Free Trial with $300 in credit. Don't worry—you won't be charged if you run

2 (optional)

Grant this service account access ... specific actions on the resources ...

Role: Storage Admin

Grants full control of buckets and objects.

3 Grant users access to

Add condition

Resource

Title *: Storage

Description

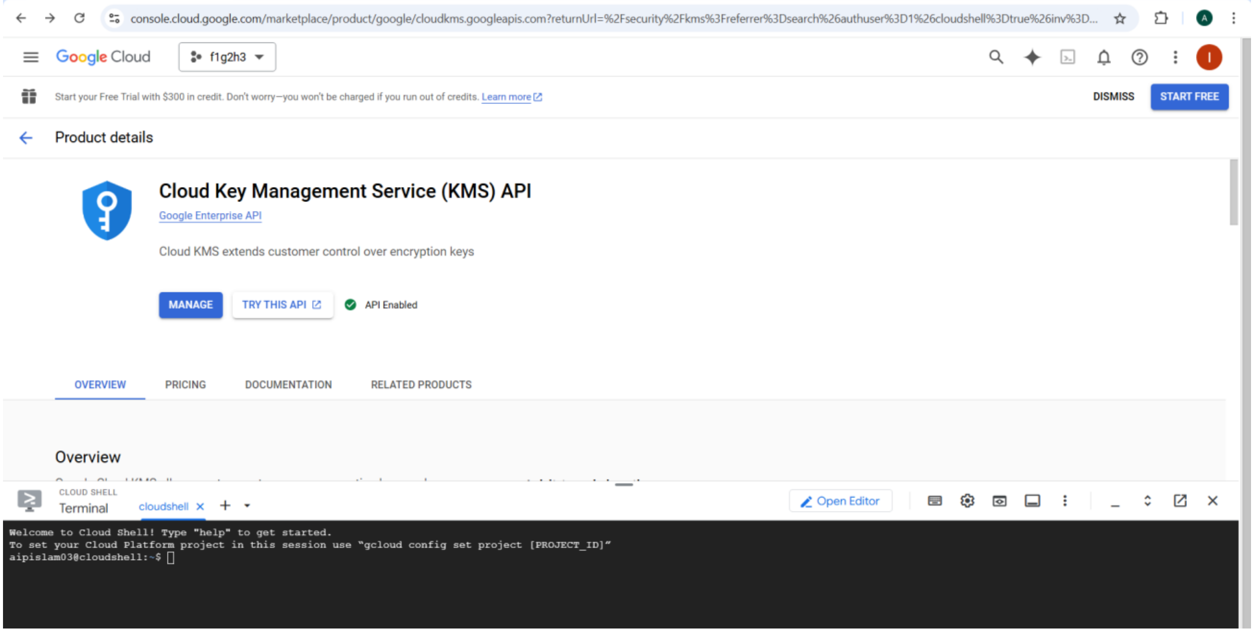
Condition type 1: Day of Week
Operator: Before or On
Day of Week *: Monday
Choose a time zone: Kazakhstan Time (EKST)

The connection to your Google Cloud Shell was lost.

```
ERROR: (gcloud.projects.create) Project creation failed. The proj
aipislam03@cloudshell:~$ gcloud projects create f1g2h3
Create in progress for [https://cloudresourcemanager.googleapis.c
Waiting for [operations/cp.6911677119749184565] to finish...done.
Enabling service [cloudapis.googleapis.com] on project [f1g2h3]..
Operation "operations/acat.p2-573076915860-69b01007-8206-4988-961
aipislam03@cloudshell:~$
```

3. Data Protection

In order set up encryption for data at rest we can use Google Cloud KMS.


console.cloud.google.com/marketplace/product/google/cloudkms.googleapis.com?returnUrl=%2Fsecurity%2Fkms%3Freferrer%3Dsearch%26authuser%3D1%26cloudshell%3Dtrue%26inv%3D...
Google Cloud
f1g2h3
DISMISS
START FREE
MANAGE
TRY THIS API
API Enabled
OVERVIEW
PRICING
DOCUMENTATION
RELATED PRODUCTS
CLOUD SHELL
Terminal
cloudshell
Open Editor

Start your Free Trial with $300 in credit. Don't worry—you won't be charged if you run out of credits. Learn more

Product details

Cloud Key Management Service (KMS) API

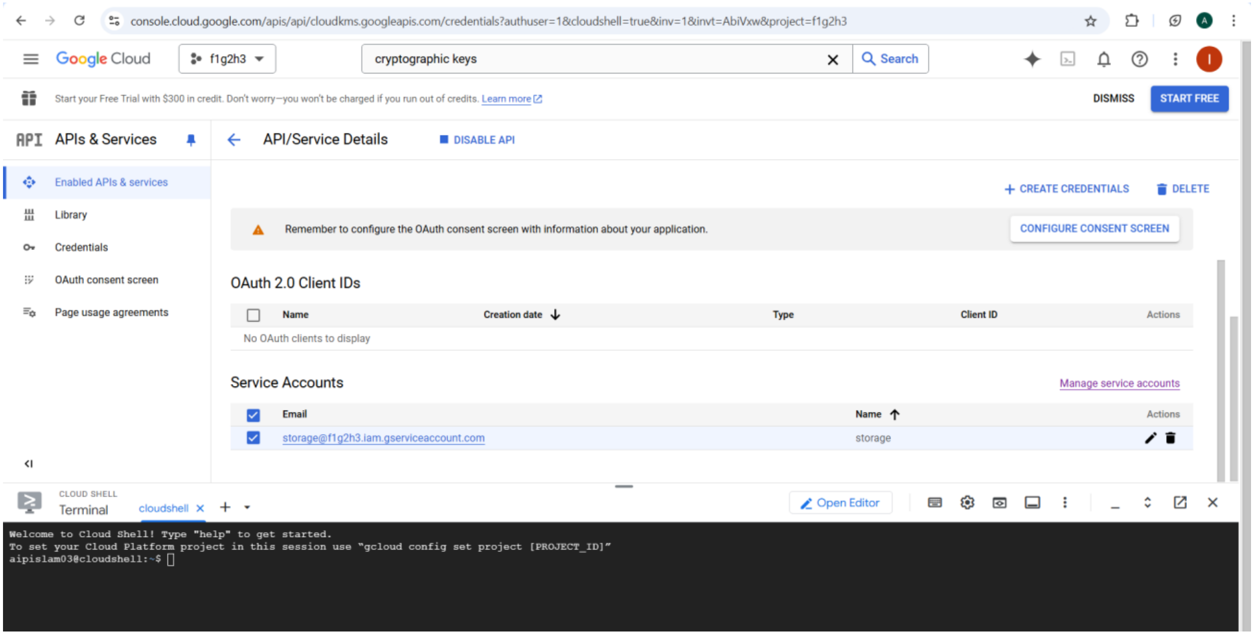
Google Enterprise API

Cloud KMS extends customer control over encryption keys

Overview

```
Welcome to Cloud Shell! Type "help" to get started.
To set your Cloud Platform project in this session use "gcloud config set project [PROJECT_ID]"
aipislam03@cloudshell:~$ 
```

After enabling Google Cloud KMS API, we can create credentials and choose our service account that we created before.



Start your Free Trial with $300 in credit. Don't worry—you won't be charged if you run out of credits. Learn more

Remember to configure the OAuth consent screen with information about your application.

OAuth 2.0 Client IDs

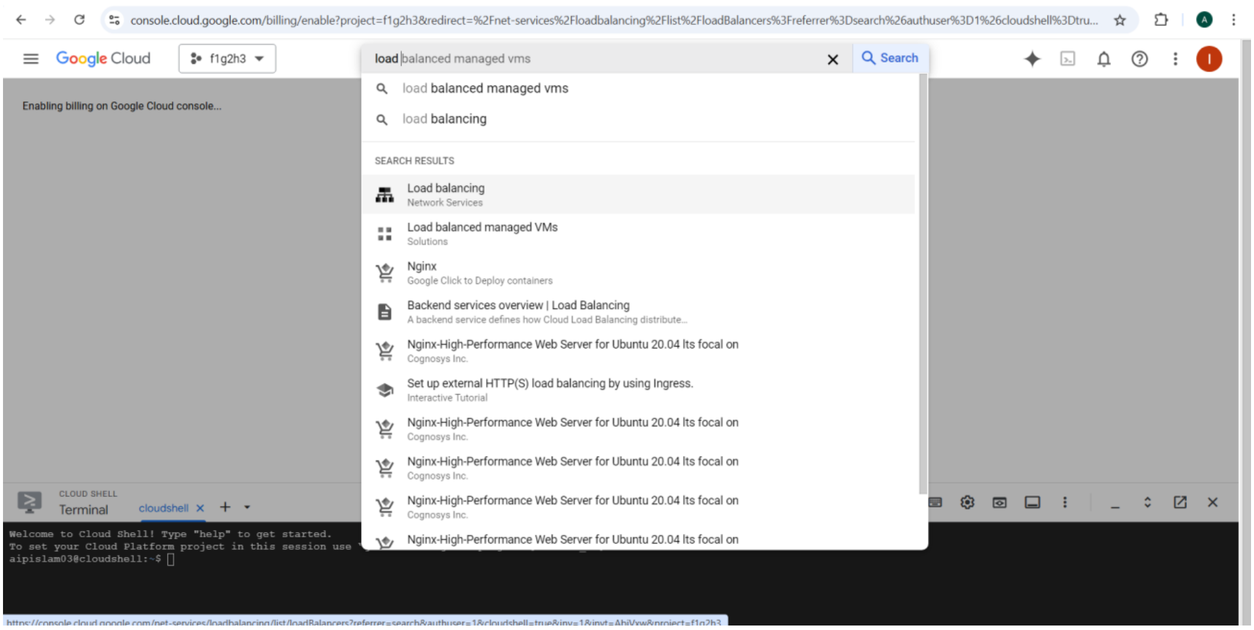
□	Name	Creation date ↓	Type	Client ID	Actions
	No OAuth clients to display				

Service Accounts

☑	Email	Name ↑	Actions
☑	storage@f1g2h3.iam.gserviceaccount.com	storage	

```
Welcome to Cloud Shell! Type "help" to get started.
To set your Cloud Platform project in this session use "gcloud config set project [PROJECT_ID]"
aipislam03@cloudshell:~$
```

Now, in order to set up a load balancer, we need billing account.



console.cloud.google.com/billing/enable?project=f1g2h3&redirect=%2Fnet-services%2Floadbalancing%2Flist%2FloadBalancers%3Freferrer%3Dsearch%26authuser%3D1%26cloudshell%3Dtru...
Google Cloud
f1g2h3
load balanced managed vms
Search
load balanced managed vms
load balancing
SEARCH RESULTS
Load balancing
Network Services
Load balanced managed VMs
Solutions
Nginx
Google Click to Deploy containers
Backend services overview | Load Balancing
A backend service defines how Cloud Load Balancing distribute...
Nginx-High-Performance Web Server for Ubuntu 20.04 lts focal on
Cognosys Inc.
Set up external HTTP(S) load balancing by using Ingress.
Interactive Tutorial
Nginx-High-Performance Web Server for Ubuntu 20.04 lts focal on
Cognosys Inc.
Nginx-High-Performance Web Server for Ubuntu 20.04 lts focal on
Cognosys Inc.
Nginx-High-Performance Web Server for Ubuntu 20.04 lts focal on
Cognosys Inc.
Nginx-High-Performance Web Server for Ubuntu 20.04 lts focal on
CLOUD SHELL
Terminal
cloudshell
https://console.cloud.google.com/net-services/loadbalancing/list/loadBalancers?referrer=search&authuser=1&cloudshell=true&inv=1&invt=AbiVxw&project=f1g2h3

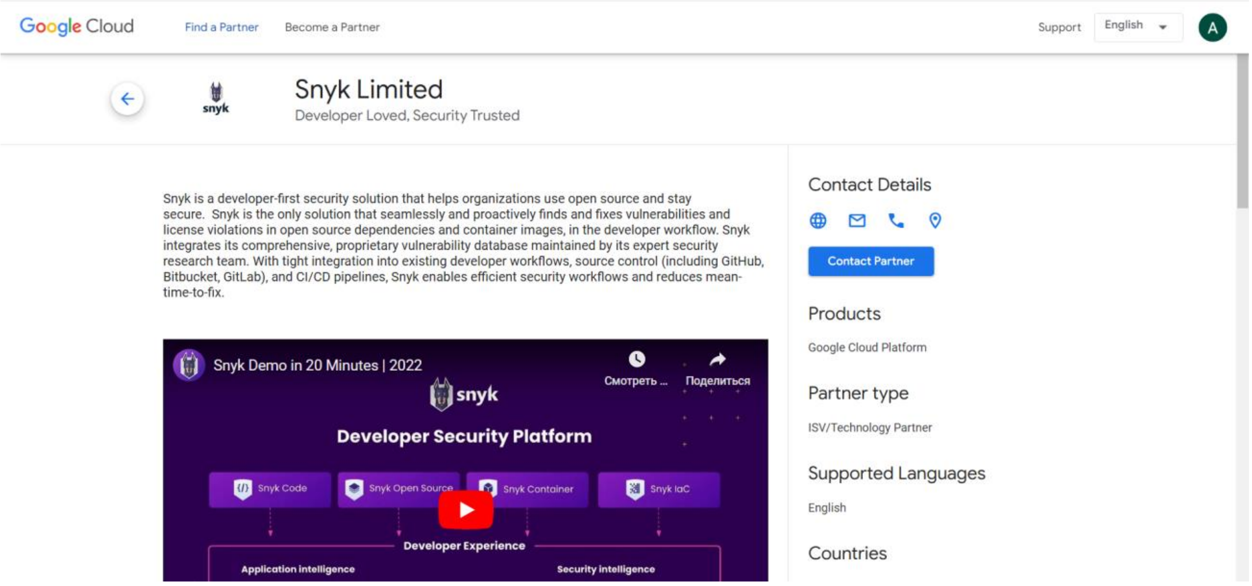
Enabling billing on Google Cloud console...

```
Welcome to Cloud Shell! Type "help" to get started.
To set your Cloud Platform project in this session use
aipislam03@cloudshell:~$
```

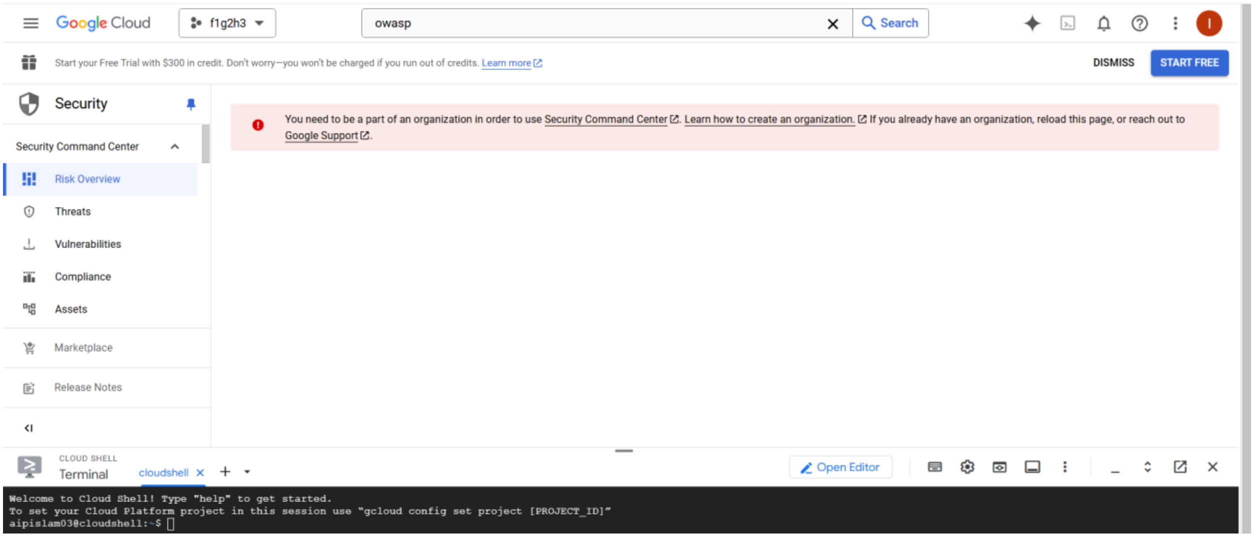
After enabling billing we should be able to configure load balance and upload an SSL certificate or use Google managed SSL.

4. Application Security Testing

Security testing is crucial part of the application development. In Google Cloud we can integrate a security scanning tools such as Snyk, or we can use security command center to check threats, vulnerabilities and risks.



Snyk is a developer-first security solution that helps organizations use open source and stay secure. Snyk is the only solution that seamlessly and proactively finds and fixes vulnerabilities and license violations in open source dependencies and container images, in the developer workflow. Snyk integrates its comprehensive, proprietary vulnerability database maintained by its expert security research team. With tight integration into existing developer workflows, source control (including GitHub, Bitbucket, GitLab), and CI/CD pipelines, Snyk enables efficient security workflows and reduces mean-time-to-fix.



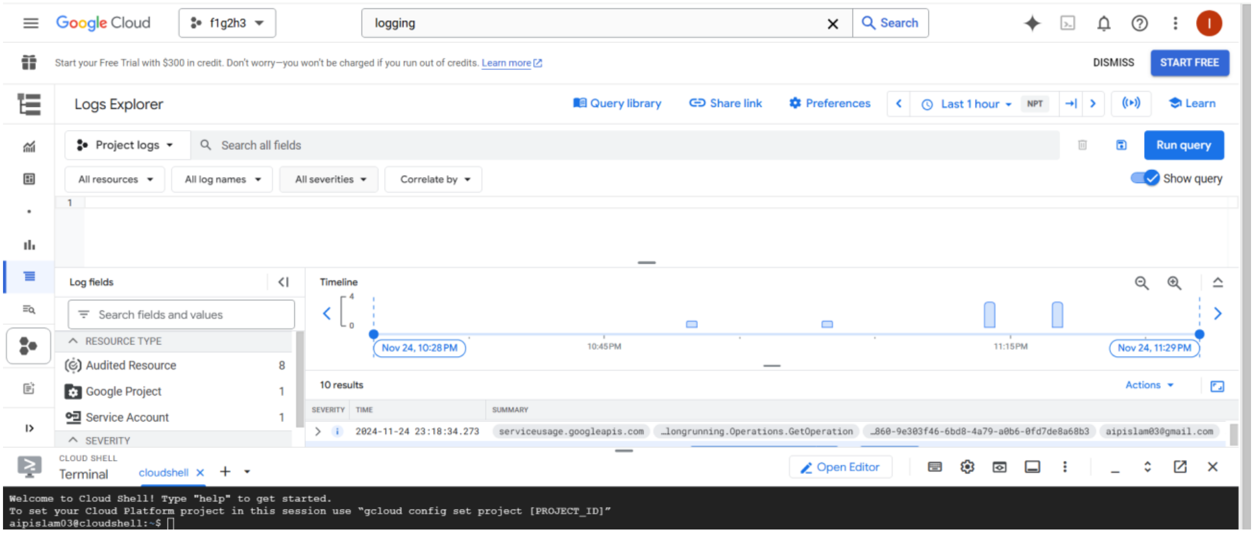
Start your Free Trial with $300 in credit. Don't worry—you won't be charged if you run out of credits. Learn more

You need to be a part of an organization in order to use Security Command Center. Learn how to create an organization. If you already have an organization, reload this page, or reach out to Google Support.

```
Welcome to Cloud Shell! Type "help" to get started.
To set your Cloud Platform project in this session use "gcloud config set project [PROJECT_ID]"
aipislam03@cloudshell:~$ 
```

5. Monitoring and Logging

In Google Cloud we can use Logs Explorer for logging.



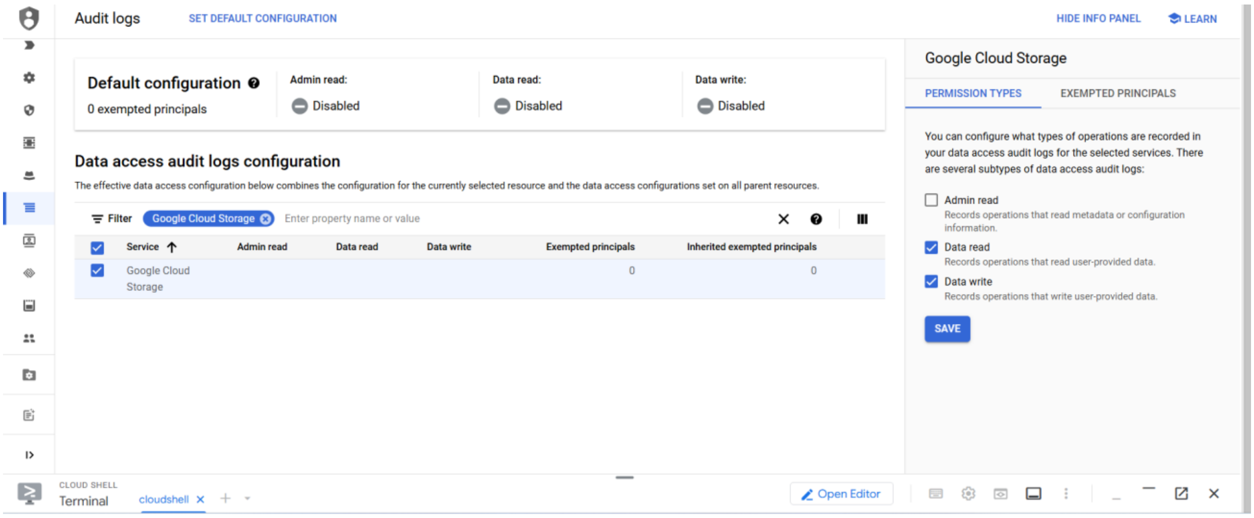
Start your Free Trial with $300 in credit. Don't worry—you won't be charged if you run out of credits. Learn more

10 results

```
SEVERITY  TIME                     SUMMARY
>  i      2024-11-24 23:18:34.273  serviceusage.googleapis.com  …longrunning.Operations.GetOperation  …860-9e303f46-6bd8-4a79-a0b6-0fd7de8a68b3  aipislam03@gmail.com
```

```
Welcome to Cloud Shell! Type "help" to get started.
To set your Cloud Platform project in this session use "gcloud config set project [PROJECT_ID]"
aipislam03@cloudshell:~$ 
```

Now let’s enable audit logs. Admin Activity logs are typically enabled by default, for data access logs let’s enable read and write for Cloud Storage.



Default configuration

0 exempted principals

Admin read: Disabled

Data read: Disabled

Data write: Disabled

Data access audit logs configuration

The effective data access configuration below combines the configuration for the currently selected resource and the data access configurations set on all parent resources.

☑	Service ↑	Admin read	Data read	Data write	Exempted principals	Inherited exempted principals
☑	Google Cloud Storage				0	0

Google Cloud Storage

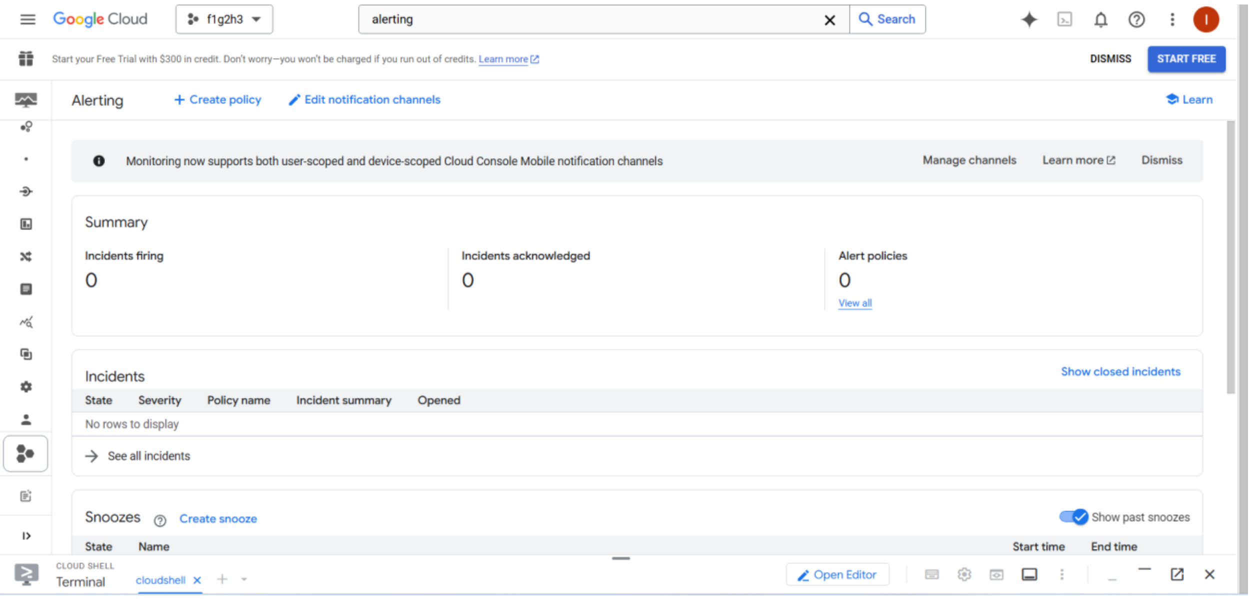
You can configure what types of operations are recorded in your data access audit logs for the selected services. There are several subtypes of data access audit logs:

☐ Admin read
Records operations that read metadata or configuration information.

☑ Data read
Records operations that read user-provided data.

☑ Data write
Records operations that write user-provided data.

Now, to monitor suspicious activities or errors we can create a new alert policy in Monitoring > Alerting.



Start your Free Trial with $300 in credit. Don't worry—you won't be charged if you run out of credits. Learn more

Monitoring now supports both user-scoped and device-scoped Cloud Console Mobile notification channels

Summary

Incidents firing	Incidents acknowledged	Alert policies
0	0	0

Incidents

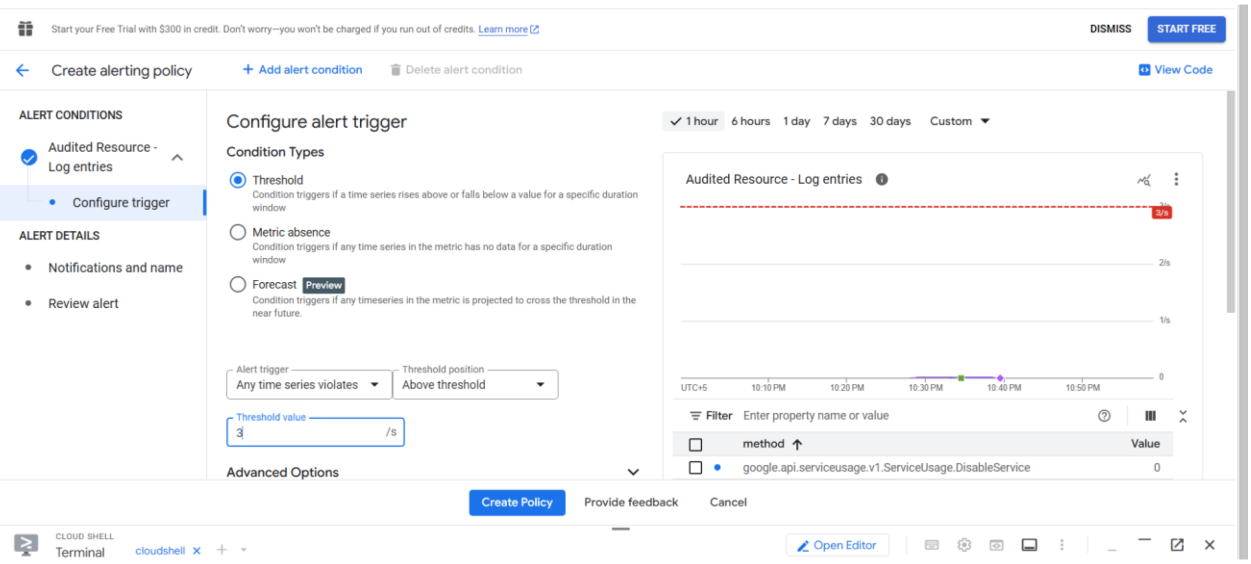
State	Severity	Policy name	Incident summary	Opened

No rows to display

Snoozes

State	Name	Start time	End time

Here we can configure alert trigger for number of log entries.



Start your Free Trial with $300 in credit. Don't worry—you won't be charged if you run out of credits. Learn more

Create alerting policy

Configure alert trigger

Condition Types

● Threshold
Condition triggers if a time series rises above or falls below a value for a specific duration window

○ Metric absence
Condition triggers if any time series in the metric has no data for a specific duration window

○ Forecast Preview
Condition triggers if any timeseries in the metric is projected to cross the threshold in the near future.

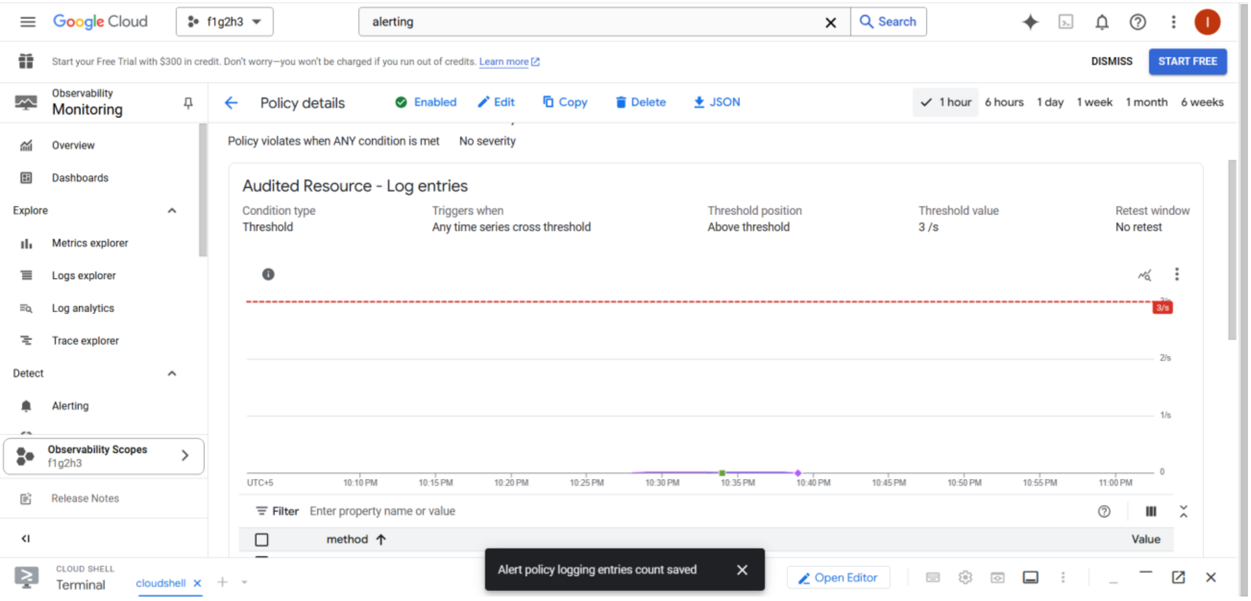
Alert trigger: Any time series violates

Threshold position: Above threshold

Threshold value: 3 /s

Audited Resource - Log entries

method: google.api.serviceusage.v1.ServiceUsage.DisableService — Value: 0



Start your Free Trial with $300 in credit. Don't worry—you won't be charged if you run out of credits. Learn more

Policy details

Policy violates when ANY condition is met — No severity

Audited Resource - Log entries

Condition type	Triggers when	Threshold position	Threshold value	Retest window
Threshold	Any time series cross threshold	Above threshold	3 /s	No retest

Alert policy logging entries count saved

6. Incident Response

An Incident Response Plan ensures that team of developers can effectively handle security breaches. IRPs steps include:

1. Identify – we define how to detect and classify an incident. We can use tools like Cloud monitoring, Cloud Security Command Center, or logs from Cloud Audit Logs.

2. Contain – we define steps to isolate the system to prevent further damage. We can use tool like IAM permissions.

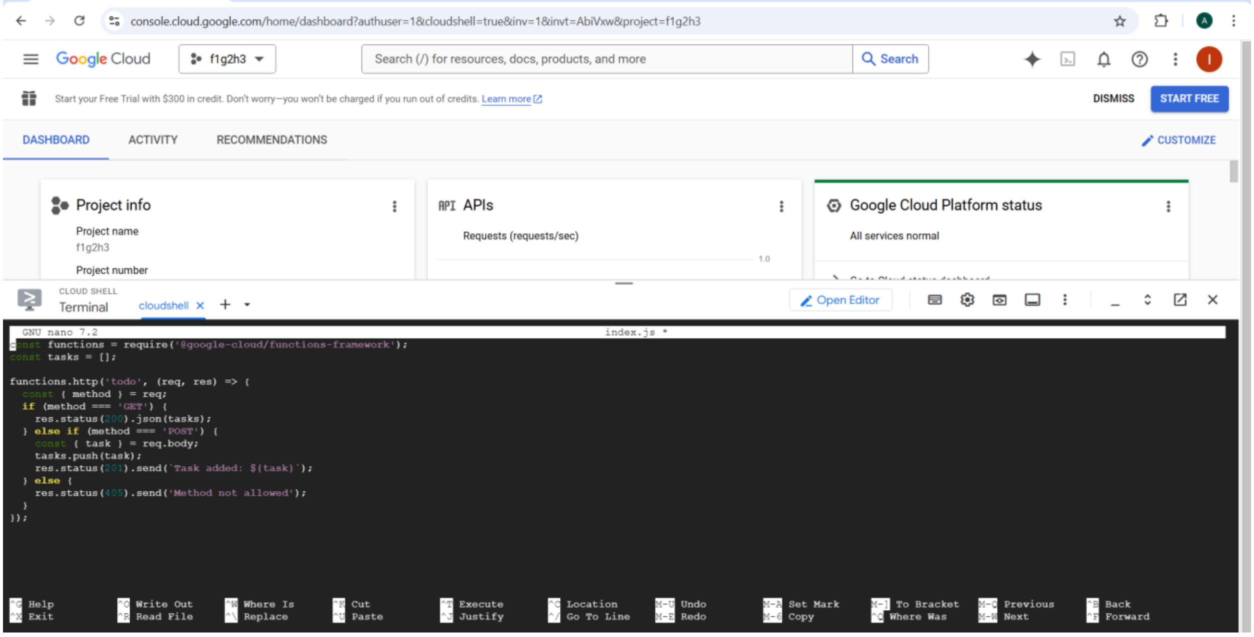
3. Eradicate – we remove the root cause of the incident, such as deleting malicious code or fixing vulnerability. We can patch software, update IAM roles etc.

4. Recover – we restore system to normal operation and ensure that vulnerability is fixed.

Scaling Applications on Google Cloud

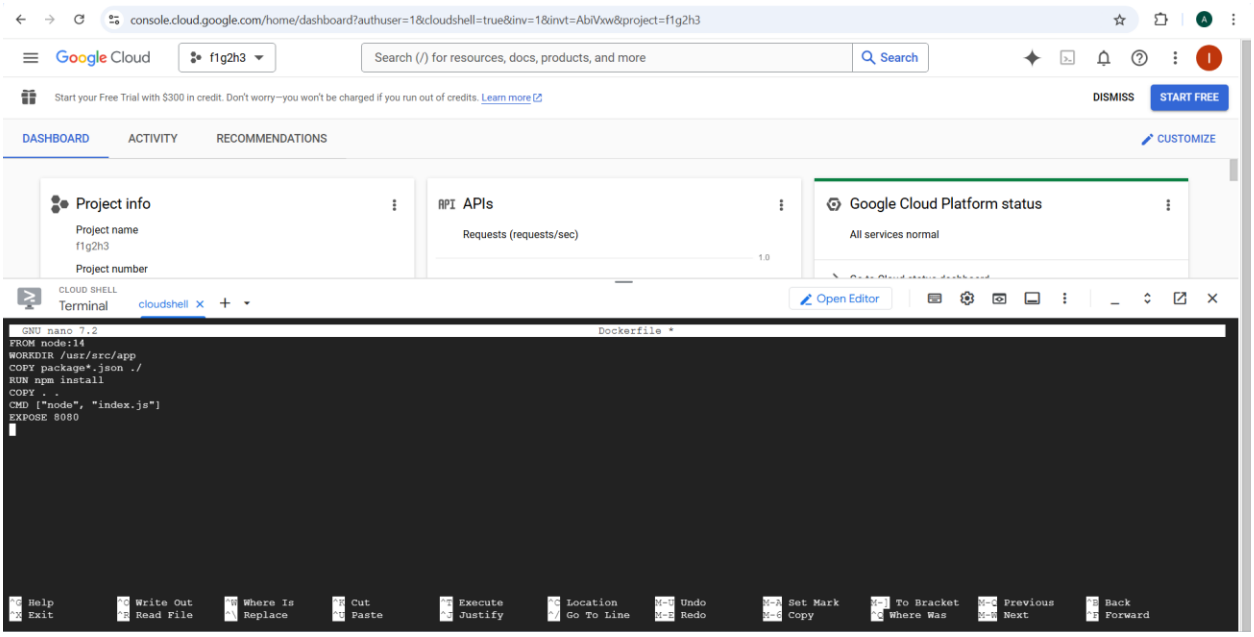
1. Application Design

Let’s create a simple to-do app.

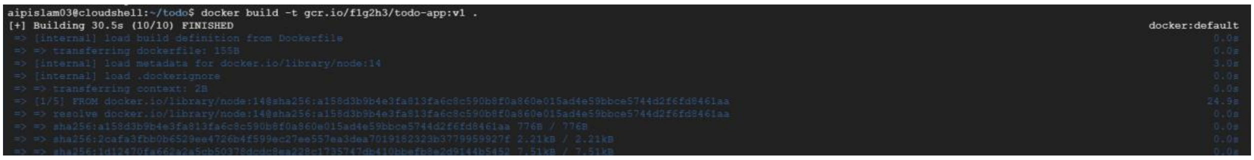

console.cloud.google.com/home/dashboard?authuser=1&cloudshell=true&inv=1&invt=AbiVxw&project=f1g2h3
Google Cloud
f1g2h3
Search (/) for resources, docs, products, and more
Search
Start your Free Trial with $300 in credit. Don't worry—you won't be charged if you run out of credits. Learn more
DISMISS
START FREE
DASHBOARD
ACTIVITY
RECOMMENDATIONS
CUSTOMIZE
Project info
Project name
f1g2h3
Project number
APIs
Requests (requests/sec)
Google Cloud Platform status
All services normal
CLOUD SHELL
Terminal
cloudshell
Open Editor

```
  GNU nano 7.2                                  index.js *
const functions = require('@google-cloud/functions-framework');
const tasks = [];

functions.http('todo', (req, res) => {
  const { method } = req;
  if (method === 'GET') {
    res.status(200).json(tasks);
  } else if (method === 'POST') {
    const { task } = req.body;
    tasks.push(task);
    res.status(201).send(`Task added: ${task}`);
  } else {
    res.status(405).send('Method not allowed');
  }
});

^G Help      ^O Write Out  ^W Where Is  ^K Cut      ^T Execute  ^C Location    M-U Undo  M-A Set Mark  M-] To Bracket  M-Q Previous  ^B Back
^X Exit      ^R Read File  ^\ Replace   ^U Paste    ^J Justify  ^/ Go To Line  M-E Redo  M-6 Copy      ^Q Where Was    M-W Next      ^F Forward
```

We can use serverless computing or GKE for containerized applications. Let’s add Dockerfile for our app and build the Docker image:

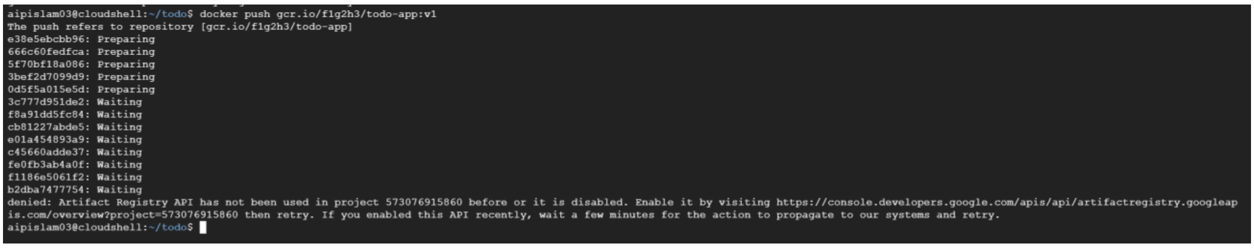

console.cloud.google.com/home/dashboard?authuser=1&cloudshell=true&inv=1&invt=AbiVxw&project=f1g2h3
Google Cloud
f1g2h3
Search (/) for resources, docs, products, and more
Search
Start your Free Trial with $300 in credit. Don't worry—you won't be charged if you run out of credits. Learn more
DISMISS
START FREE
DASHBOARD
ACTIVITY
RECOMMENDATIONS
CUSTOMIZE
Project info
Project name
f1g2h3
Project number
APIs
Requests (requests/sec)
Google Cloud Platform status
All services normal
CLOUD SHELL
Terminal
cloudshell
Open Editor

```
  GNU nano 7.2                                  Dockerfile *
FROM node:14
WORKDIR /usr/src/app
COPY package*.json ./
RUN npm install
COPY . .
CMD ["node", "index.js"]
EXPOSE 8080

^G Help      ^O Write Out  ^W Where Is  ^K Cut      ^T Execute  ^C Location    M-U Undo  M-A Set Mark  M-] To Bracket  M-Q Previous  ^B Back
^X Exit      ^R Read File  ^\ Replace   ^U Paste    ^J Justify  ^/ Go To Line  M-E Redo  M-6 Copy      ^Q Where Was    M-W Next      ^F Forward
```

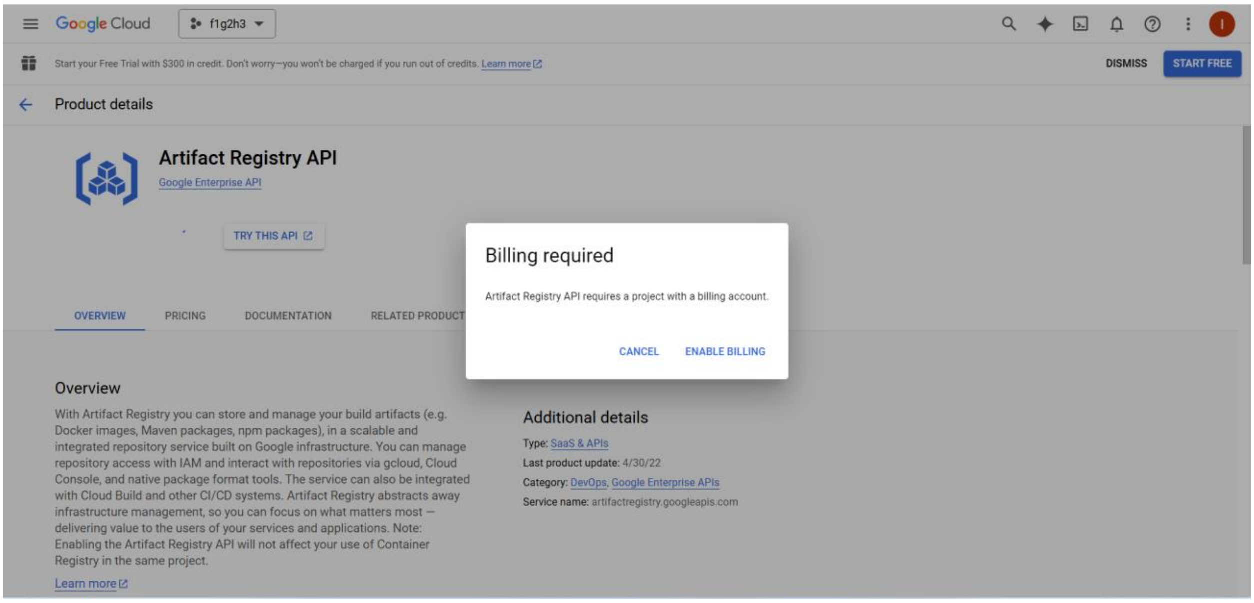


```
aipislam03@cloudshell:~/todo$ docker build -t gcr.io/f1g2h3/todo-app:v1 .
[+] Building 30.5s (10/10) FINISHED                                                                   docker:default
 => [internal] load build definition from Dockerfile                                                            0.0s
 => => transferring dockerfile: 155B                                                                            0.0s
 => [internal] load metadata for docker.io/library/node:14                                                      3.0s
 => [internal] load .dockerignore                                                                               0.0s
 => => transferring context: 2B                                                                                 0.0s
 => [1/5] FROM docker.io/library/node:14@sha256:a158d3b9b4e3fa813fa6c8c590b8f0a860e015ad4e59bbce5744d2f6fd8461aa  24.9s
 => => resolve docker.io/library/node:14@sha256:a158d3b9b4e3fa813fa6c8c590b8f0a860e015ad4e59bbce5744d2f6fd8461aa  0.0s
 => => sha256:a158d3b9b4e3fa813fa6c8c590b8f0a860e015ad4e59bbce5744d2f6fd8461aa 776B / 776B                      0.0s
 => => sha256:2cafa3fbb0b6529ee4726b4f599ec27ee557ea3dea7019162323b3779959927f 2.21kB / 2.21kB                  0.0s
 => => sha256:1d12470fa662a2a5cb50378dcdc8ea228c1735747db410bbefb8e2d9144b5452 7.51kB / 7.51kB                  0.0s
```

Now we can push the image to the Google Container Registry, but we need billing account to be enabled:



```
aipislam03@cloudshell:~/todo$ docker push gcr.io/f1g2h3/todo-app:v1
The push refers to repository [gcr.io/f1g2h3/todo-app]
e38e5ebcbb96: Preparing
666c60fedfca: Preparing
5f70bf18a086: Preparing
3bef2d7099d9: Preparing
0d5f5a015e5d: Preparing
3c777d951de2: Waiting
f8a91dd5fc84: Waiting
cb81227abde5: Waiting
e01a454893a9: Waiting
c45660adde37: Waiting
fe0fb3ab4a0f: Waiting
f1186e5061f2: Waiting
b2dba7477754: Waiting
denied: Artifact Registry API has not been used in project 573076915860 before or it is disabled. Enable it by visiting https://console.developers.google.com/apis/api/artifactregistry.googleap
is.com/overview?project=573076915860 then retry. If you enabled this API recently, wait a few minutes for the action to propagate to our systems and retry.
aipislam03@cloudshell:~/todo$ 
```



Start your Free Trial with $300 in credit. Don't worry—you won't be charged if you run out of credits. Learn more

Product details

Artifact Registry API

Google Enterprise API

Billing required

Artifact Registry API requires a project with a billing account.

Overview

With Artifact Registry you can store and manage your build artifacts (e.g. Docker images, Maven packages, npm packages), in a scalable and integrated repository service built on Google infrastructure. You can manage repository access with IAM and interact with repositories via gcloud, Cloud Console, and native package format tools. The service can also be integrated with Cloud Build and other CI/CD systems. Artifact Registry abstracts away infrastructure management, so you can focus on what matters most — delivering value to the users of your services and applications. Note: Enabling the Artifact Registry API will not affect your use of Container Registry in the same project.

Additional details

Type: SaaS & APIs

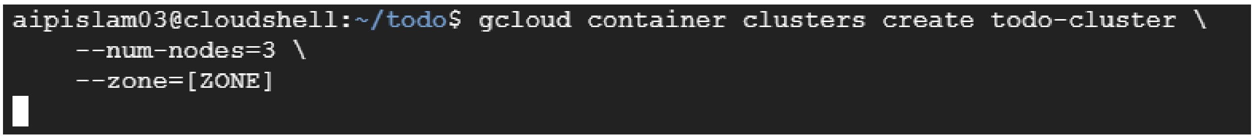
Last product update: 4/30/22

Category: DevOps, Google Enterprise APIs

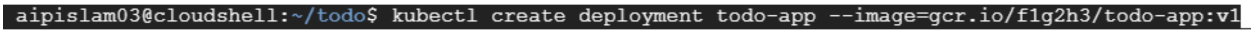
Service name: artifactregistry.googleapis.com

After pushing the image we can deploy our application on GKE.

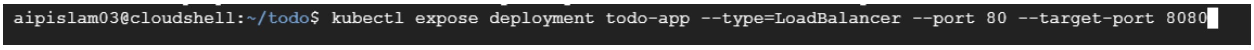
We create a GKE cluster, deploy container to the cluster and expose our app.



```
aipislam03@cloudshell:~/todo$ gcloud container clusters create todo-cluster \
    --num-nodes=3 \
    --zone=[ZONE]
```



```
aipislam03@cloudshell:~/todo$ kubectl create deployment todo-app --image=gcr.io/f1g2h3/todo-app:v1
```



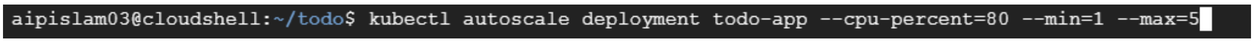
```
aipislam03@cloudshell:~/todo$ kubectl expose deployment todo-app --type=LoadBalancer --port 80 --target-port 8080
```

2. Horizontal vs. Vertical Scaling

Horizontal scaling involves adding more instances or nodes to distribute the workload. This approach is preferable over vertical scaling in some scenarios:

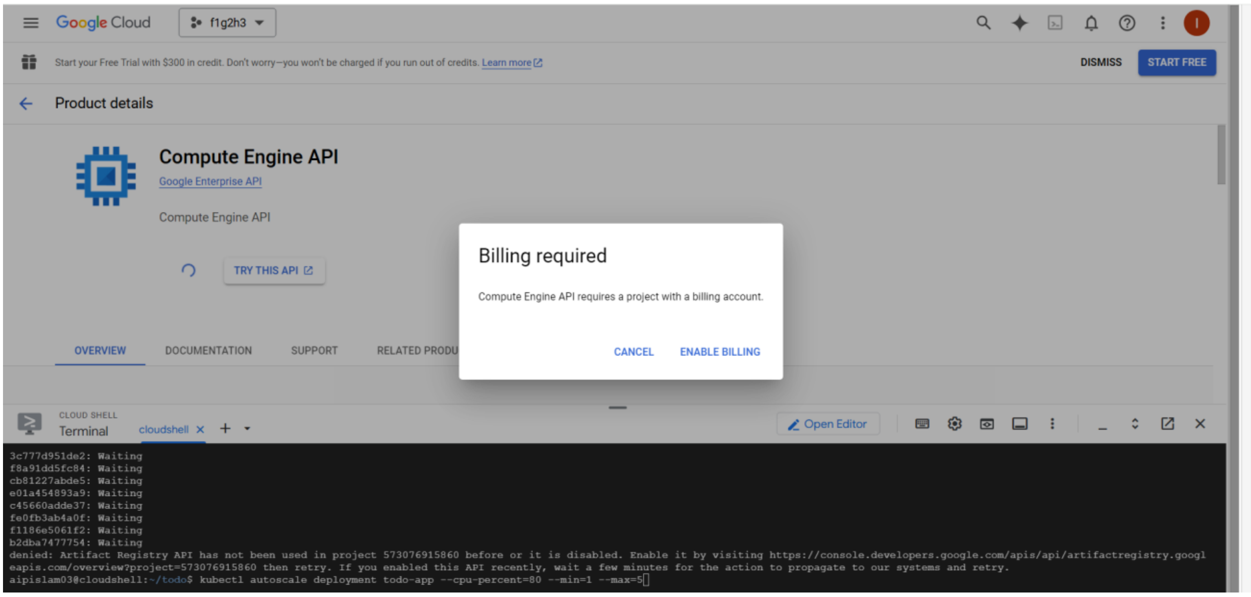
1) A web application or API must remain available even if one server fails.
2) Application experiences spikes in traffic.
3) Application designed to use multiple smaller nodes instead of a single powerful one.

In GKE we can enable horizontal auto pod scaling:



```
aipislam03@cloudshell:~/todo$ kubectl autoscale deployment todo-app --cpu-percent=80 --min=1 --max=5
```

For Vertical Scaling in Compute Engine we can navigate to our VM instances and upgrade the machine type(billing account is required):



Billing required

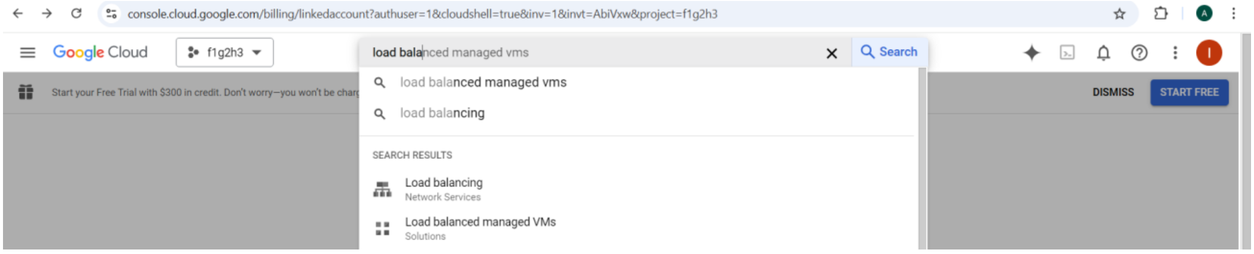
Compute Engine API requires a project with a billing account.

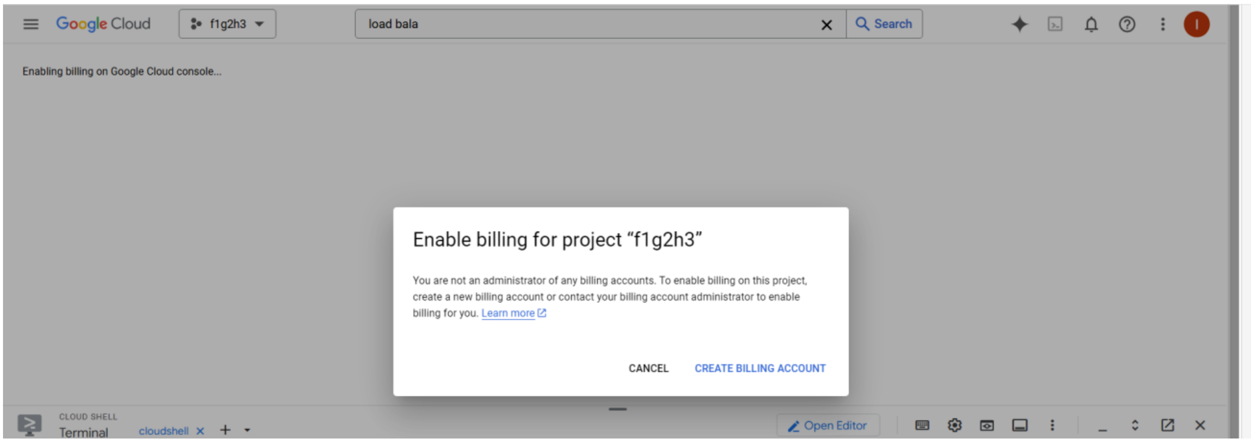
CANCEL ENABLE BILLING

```
3c777d951de2: Waiting
f8a91dd5fc84: Waiting
cb81227abde5: Waiting
e01a454893a9: Waiting
c45660adde37: Waiting
fe0fb3ab4a0f: Waiting
f1186e5061f2: Waiting
b2dba7477754: Waiting
denied: Artifact Registry API has not been used in project 573076915860 before or it is disabled. Enable it by visiting https://console.developers.google.com/apis/api/artifactregistry.googl
eapis.com/overview?project=573076915860 then retry. If you enabled this API recently, wait a few minutes for the action to propagate to our systems and retry.
aipislam03@cloudshell:~/todo$ kubectl autoscale deployment todo-app --cpu-percent=80 --min=1 --max=5
```

3. Load Balancing

In order to set up a Load Balancer for our project we can navigate to Network Services > Load balancing


console.cloud.google.com/billing/linkedaccount?authuser=1&cloudshell=true&inv=1&invt=AbiVxw&project=f1g2h3
Google Cloud
f1g2h3
load balanced managed vms
Search
load balanced managed vms
load balancing
SEARCH RESULTS
Load balancing
Network Services
Load balanced managed VMs
Solutions
Start your Free Trial with $300 in credit. Don't worry—you won't be charg
DISMISS
START FREE



Enabling billing on Google Cloud console...

Enable billing for project “f1g2h3”

You are not an administrator of any billing accounts. To enable billing on this project, create a new billing account or contact your billing account administrator to enable billing for you. Learn more

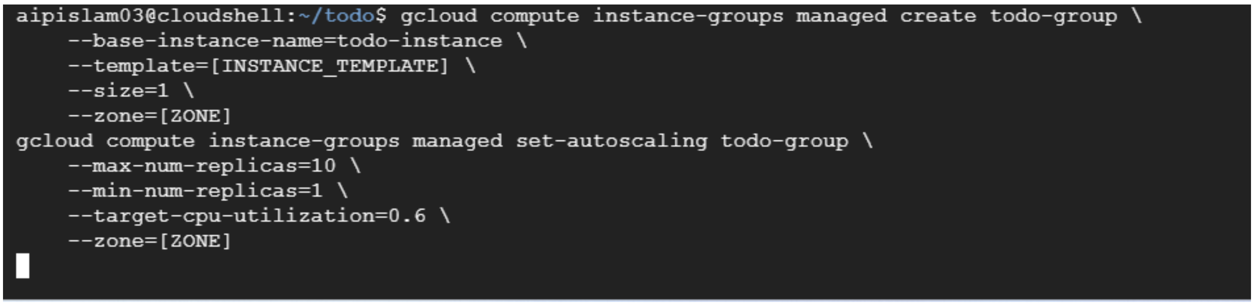
CANCEL CREATE BILLING ACCOUNT

Billing is required

Here we create Load Balancer and we can choose HTTPS Load balancer. After creating, we can attach backend services(GKE pods, Compute Engine instances).

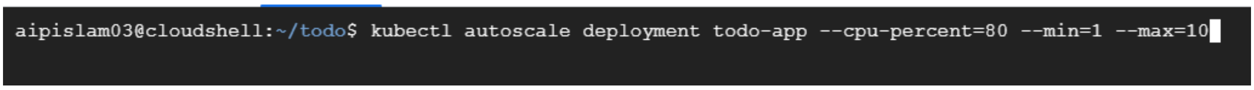
4. Auto-Scaling

For Compute Engine we can create an instance group with auto-scaling ebnabled:



```
aipislam03@cloudshell:~/todo$ gcloud compute instance-groups managed create todo-group \
    --base-instance-name=todo-instance \
    --template=[INSTANCE_TEMPLATE] \
    --size=1 \
    --zone=[ZONE]
gcloud compute instance-groups managed set-autoscaling todo-group \
    --max-num-replicas=10 \
    --min-num-replicas=1 \
    --target-cpu-utilization=0.6 \
    --zone=[ZONE]
```

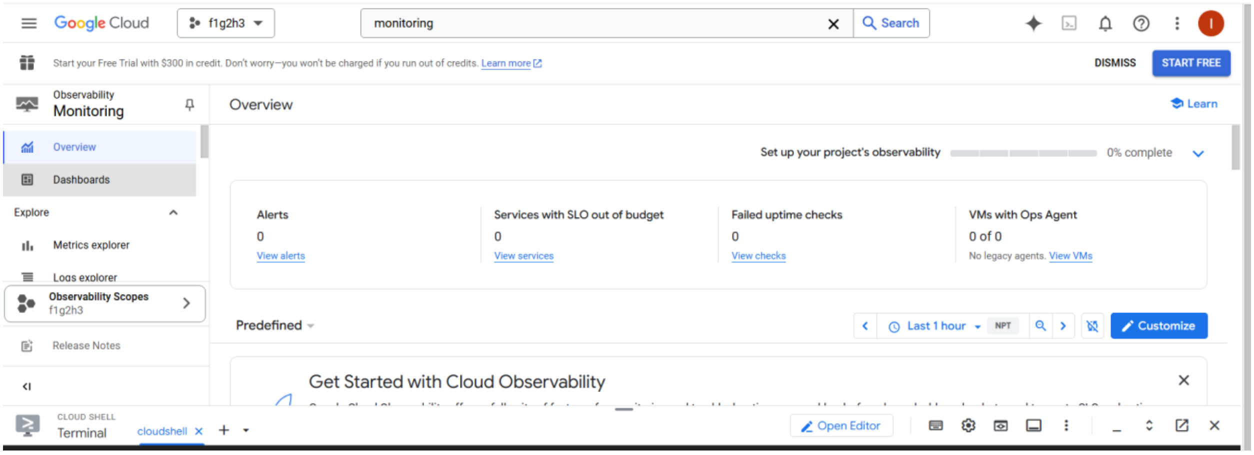
For GKE:



```
aipislam03@cloudshell:~/todo$ kubectl autoscale deployment todo-app --cpu-percent=80 --min=1 --max=10
```

5. Monitoring Performance

1) Track Metrics



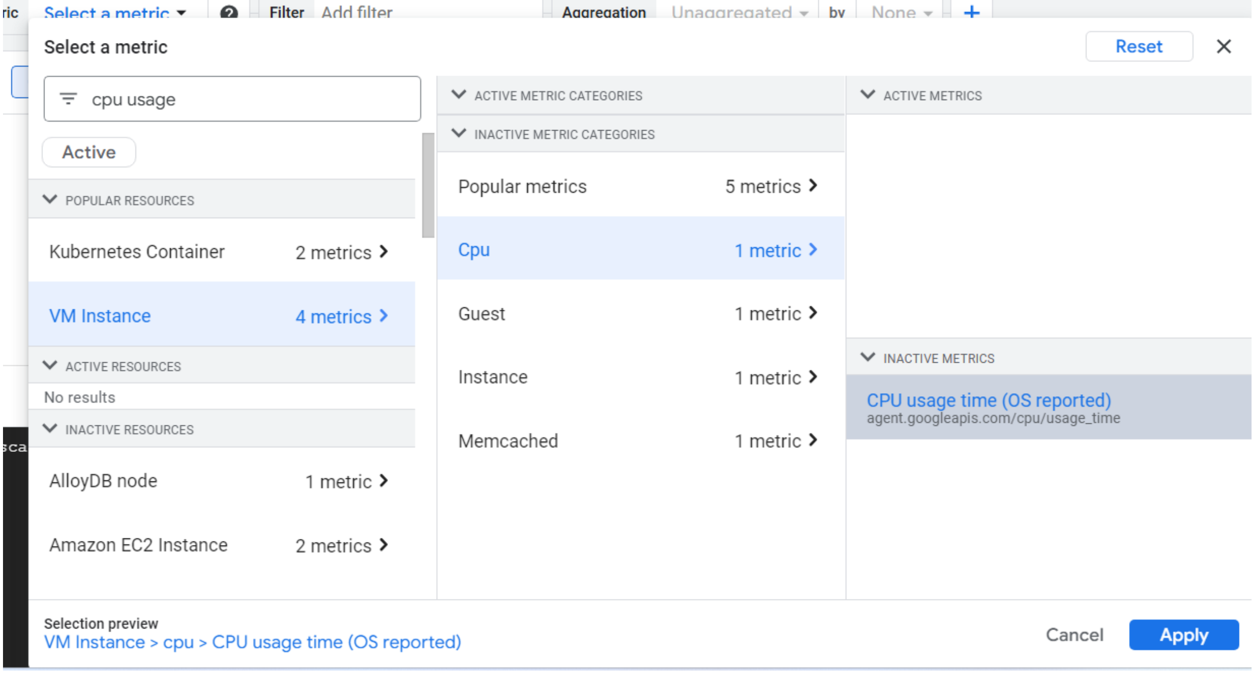
Alerts 0 View alerts

Services with SLO out of budget 0 View services

Failed uptime checks 0 View checks

VMs with Ops Agent 0 of 0 No legacy agents. View VMs

Get Started with Cloud Observability



Select a metric

cpu usage

Kubernetes Container	2 metrics
VM Instance	4 metrics

No results

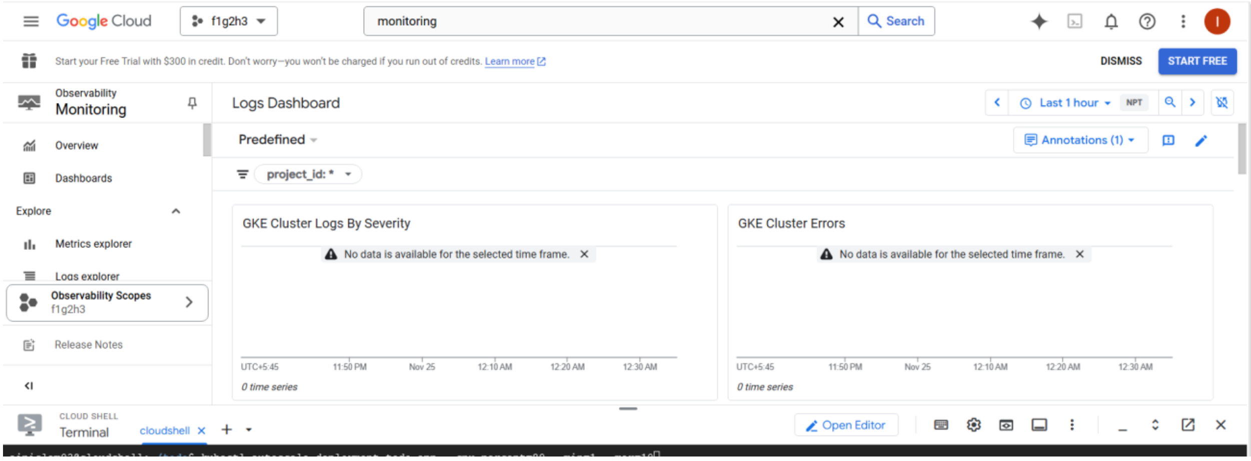
AlloyDB node	1 metric
Amazon EC2 Instance	2 metrics

Popular metrics	5 metrics
Cpu	1 metric
Guest	1 metric
Instance	1 metric
Memcached	1 metric

CPU usage time (OS reported)
agent.googleapis.com/cpu/usage_time

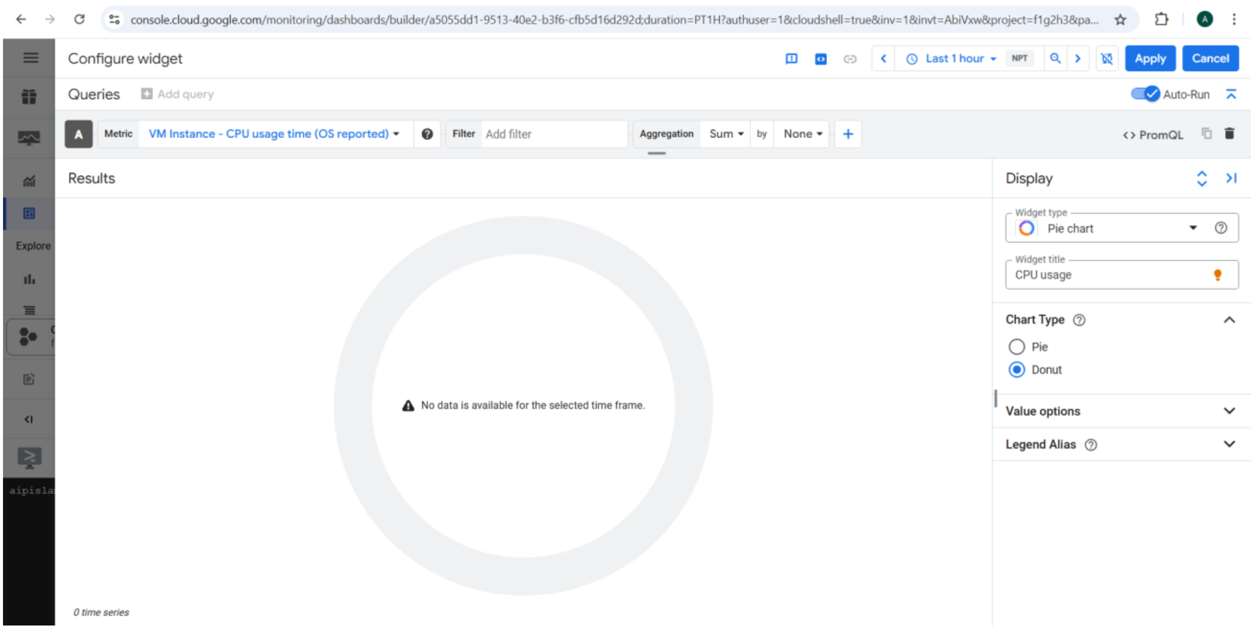
Selection preview
VM Instance > cpu > CPU usage time (OS reported)

2) Dashboards



No data is available for the selected time frame.

No data is available for the selected time frame.



```
console.cloud.google.com/monitoring/dashboards/builder/a5055dd1-9513-40e2-b3f6-cfb5d16d292d;duration=PT1H?authuser=1&cloudshell=true&inv=1&invt=AbiVxw&project=f1g2h3&pa...
```

Metric: VM Instance - CPU usage time (OS reported)
Filter: Add filter
Aggregation: Sum by None

No data is available for the selected time frame.

Widget type: Pie chart
Widget title: CPU usage
Chart Type
○ Pie
● Donut
Value options
Legend Alias

6. Cost Optimization

We can use Cloud Billing Reports to identify high-cost resources or underutilized resources. We can also use preemptive VMs and track before/after costs in Cloud Biling Reports

Conclusion

In this exercise, we explored essential practices for securing and scaling applications on Google Cloud, focusing on robust design, automation, and incident preparedness. For security, we implemented measures like IAM policies, encryption, and audit logs, complemented by a detailed Incident Response Plan. For scalability, we designed applications leveraging serverless and containerized approaches, implemented load balancing, auto-scaling, and monitored performance to optimize cost-effectiveness.

Recommendations

We can implement regular security testing and optimize our auto-scaling policies