Architecture Diagram

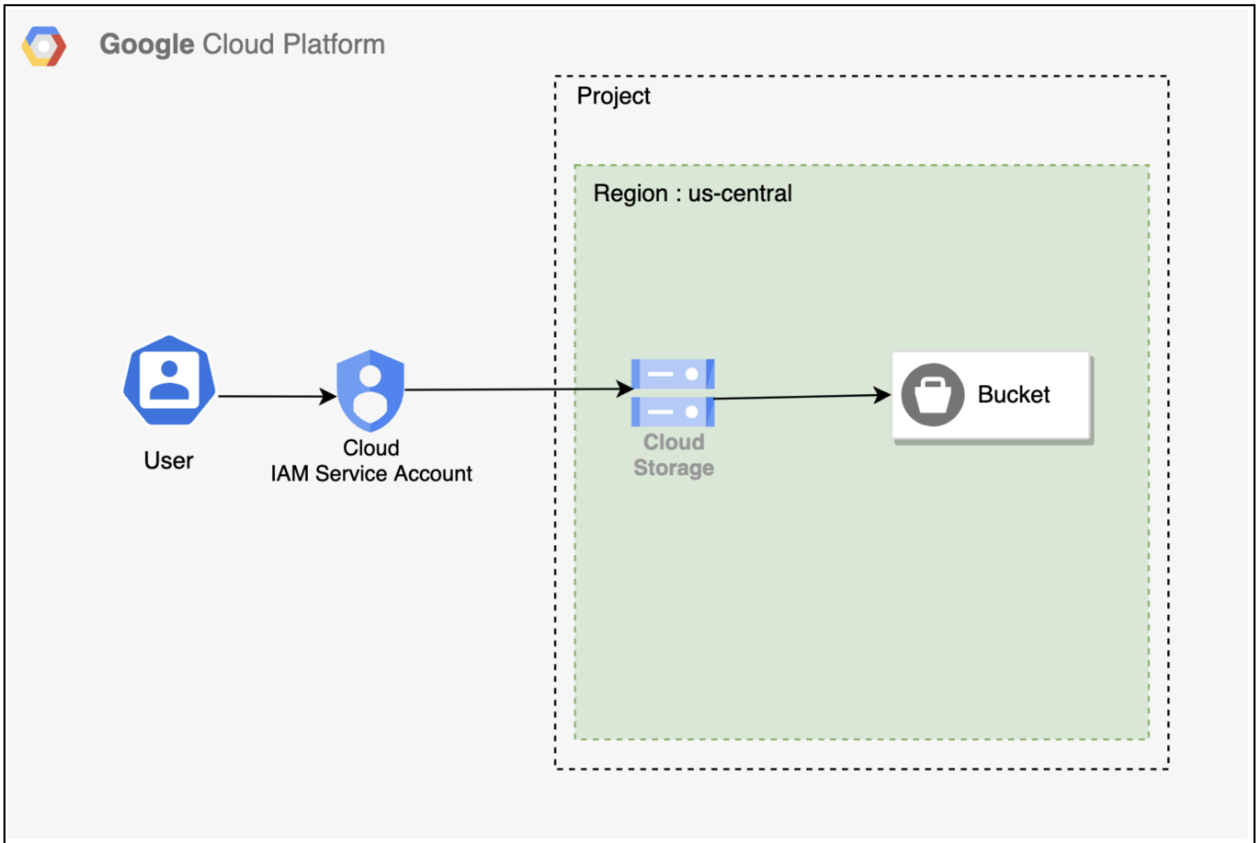


Figure: Lab_2 - Google Cloud Storage

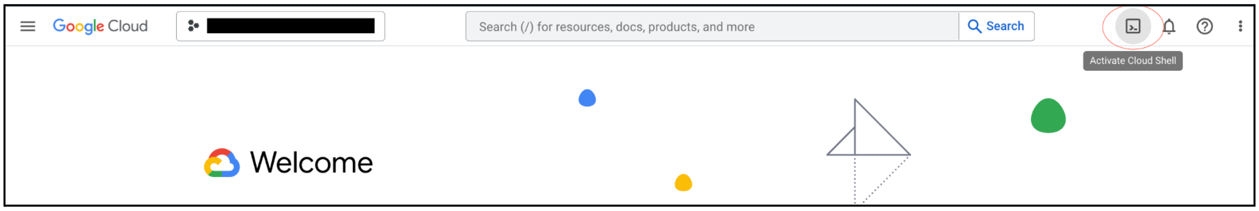
Creating a Google Cloud Storage(GCS) Bucket

Overview

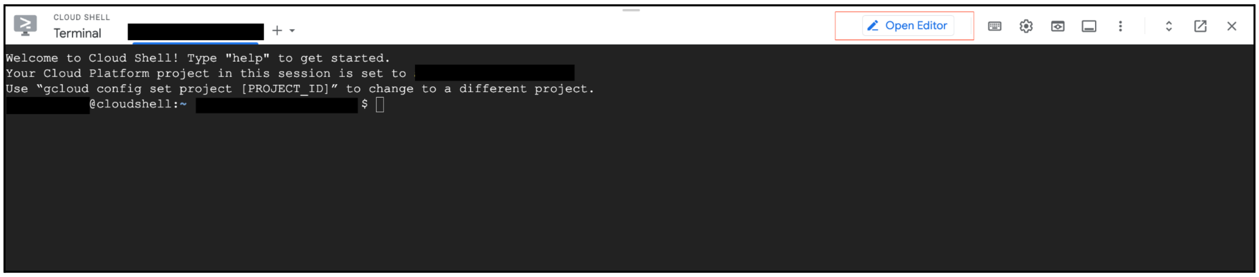
Google Cloud Storage is an object storage service provided by Google Cloud. Google Cloud Storage serves as the foundation for many services.
Perhaps some of the most underrated features of Google Cloud Storage are its use of different storage classes and lifecycle management rules for data buckets.
The usual approach is to choose Standard. In this case, you can choose to store your buckets in a specific Google Cloud region or multiple regions.

Prerequisites

NOTE : In this lab we are going to use some commands. Run that command on the Cloud shell editor.
You can use Cloud Shell Editor to run lab's commands. On the GCP Console, on top right click on **Activate Cloud Shell**.

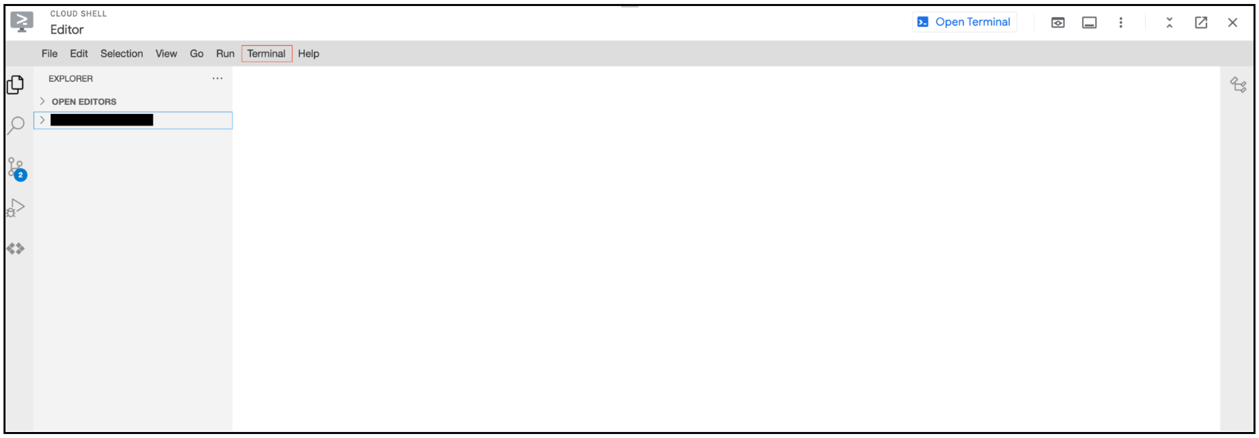


Cloud Shell terminal will open at the bottom of the screen. Click on the **Open Editor** button to access the Cloud Shell Editor.

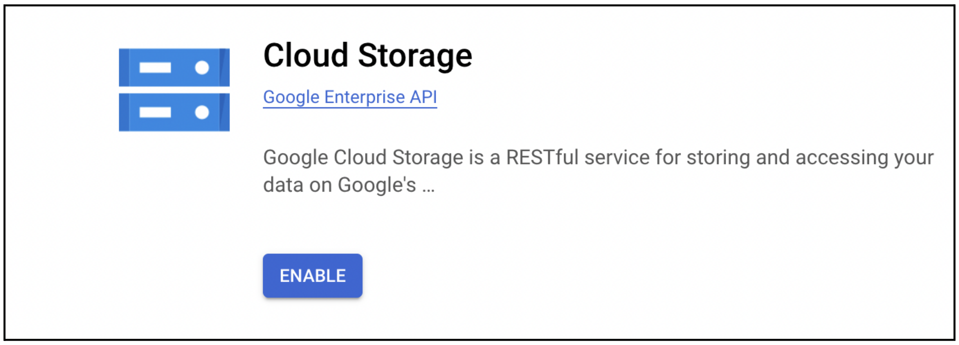


```
Welcome to Cloud Shell! Type "help" to get started.
Your Cloud Platform project in this session is set to [redacted]
Use “gcloud config set project [PROJECT_ID]” to change to a different project.
[redacted]@cloudshell:~ [redacted] $
```

Cloud Shell Editor will be opened refer to below screenshot. Click on **Terminal** to open terminal to run various operations.



- Enable the IAM API - IAM API
- Make sure that **IAM User or Principal** have the right permission : **(Storage admin, Service Account Token Creator, Service Account User)**. Refer to this link to provide permission.
- If you are using a new project, Cloud Storage API service should be Enabled. Follow the link to Enable the Cloud Storage API



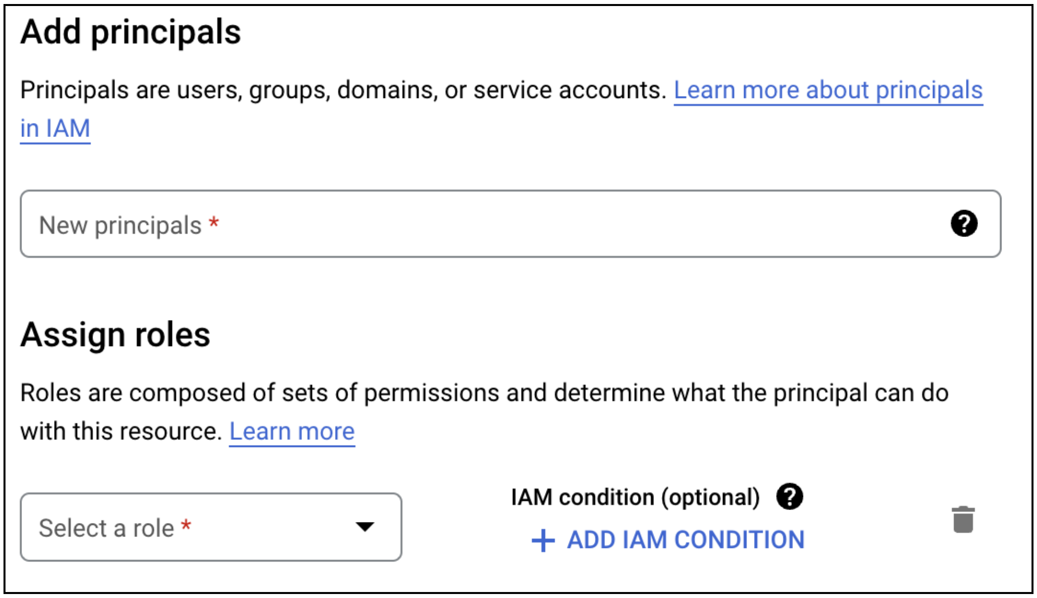
Cloud Storage

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

- To access the Google cloud APIs via command line you need to install the Gcloud CLI Tool.
- To view, create service accounts and impersonate service account user require following permission :
  Create Service Accounts (roles/iam.serviceAccountCreator)
  Service Account Token Creator (roles/iam.serviceAccountTokenCreator)

- Use Service Account to access the Google Cloud bucket.
  Follow the below to set up a service account.
  - Click IAM & Admin in the left navigation panel.
  - Click on Service Account.
  - On Service Account dashboard click on the Create service account
  - Enter service account name in service account name column.
  - Click on create and continue and click on Done.

- We can use the above created service account to access Google cloud Storage. So It requires Impersonating the Active users. Also add storage admin permission to this service account.
- To Impersonate the user follow the below steps:
  - Click on IAM & Admin > IAM.
  - Click on Grant Access
  - Enter principal name (Email ID of the user who requires access) and select the roles **Service Account User, Service Account Token Creator** and **Storage Admin**.

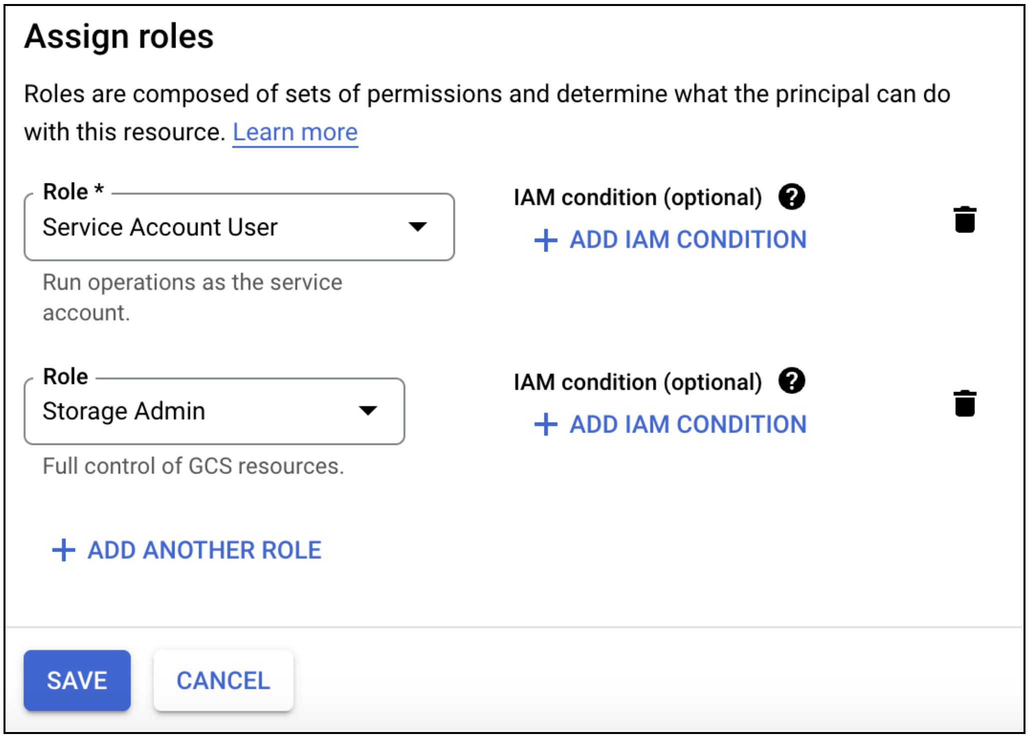


Add principals

Principals are users, groups, domains, or service accounts. Learn more about principals in IAM

Assign roles

Roles are composed of sets of permissions and determine what the principal can do with this resource. Learn more



Assign roles

Roles are composed of sets of permissions and determine what the principal can do with this resource. Learn more

Role *: Service Account User

Run operations as the service account.

IAM condition (optional)

Role: Storage Admin

Full control of GCS resources.

IAM condition (optional)

- Enter following command to impersonate in command line :
  Command :

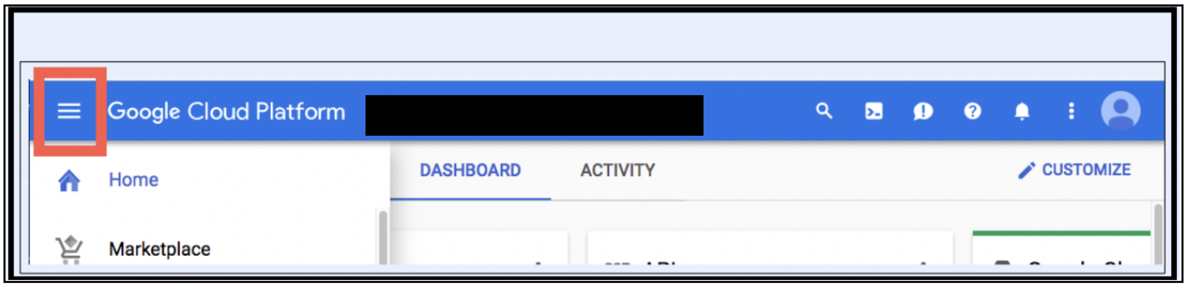
```
gcloud config set auth/impersonate_service_account
<service-aacount-name>@<project-id>.iam.gserviceaccount.com

export GOOGLE_OAUTH_ACCESS_TOKEN=$(gcloud auth
print-access-token)
```

Gsutil

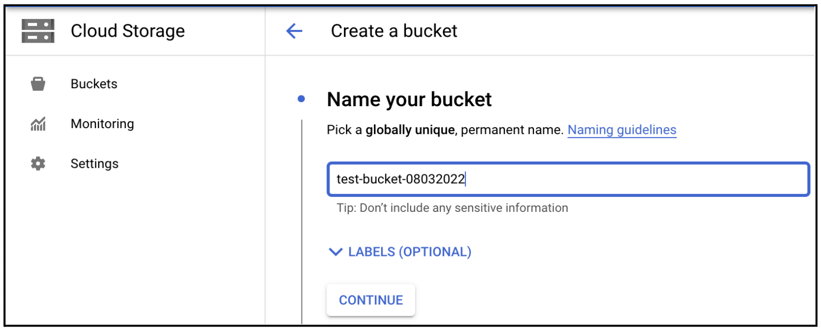
gsutil is a command line tool for buckets in Google Cloud Storage. It come with the installation of Google Cloud SDK.

Setup for Cloud Storage



Note: You can view the menu with a list of Google Cloud Products and Services by clicking the Navigation menu at the top-left.

1. Configure the Google cloud Storage (GCS) Bucket
    - Click Cloud Storage in the left navigation panel.
    - your bucket information and click Continue to complete each step:
        - Name your bucket: Enter a unique name for your bucket.



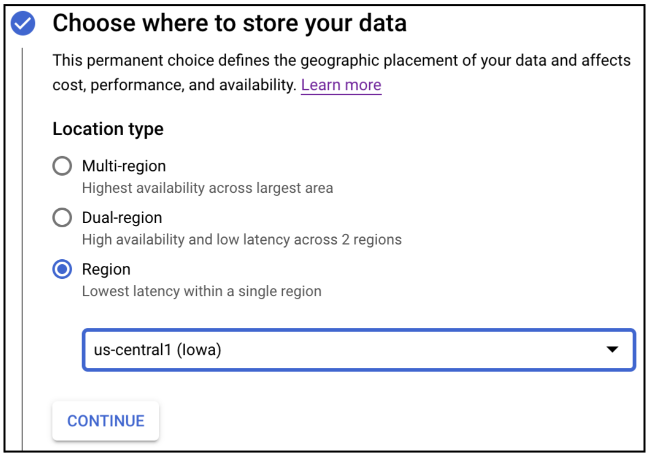
Name your bucket

Pick a **globally unique**, permanent name. Naming guidelines

test-bucket-08032022

Tip: Don't include any sensitive information

- Choose Region for Location type and us-east1 (South Carolina) for Location. You can choose from the following location types:



Choose where to store your data

This permanent choice defines the geographic placement of your data and affects cost, performance, and availability. Learn more

Location type

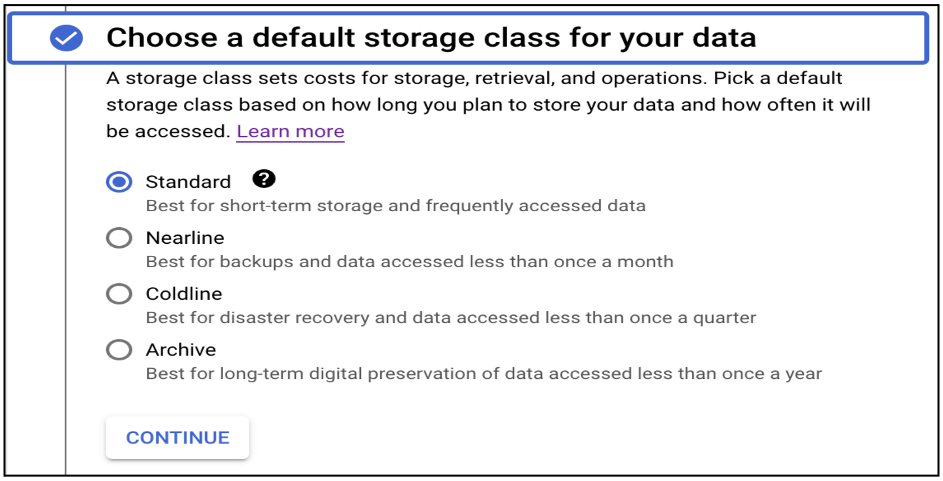
○ Multi-region
Highest availability across largest area

○ Dual-region
High availability and low latency across 2 regions

● Region
Lowest latency within a single region

us-central1 (Iowa)

- Choose Standard for default storage class. In this step you have four Storage class.



Choose a default storage class for your data

A storage class sets costs for storage, retrieval, and operations. Pick a default storage class based on how long you plan to store your data and how often it will be accessed. Learn more

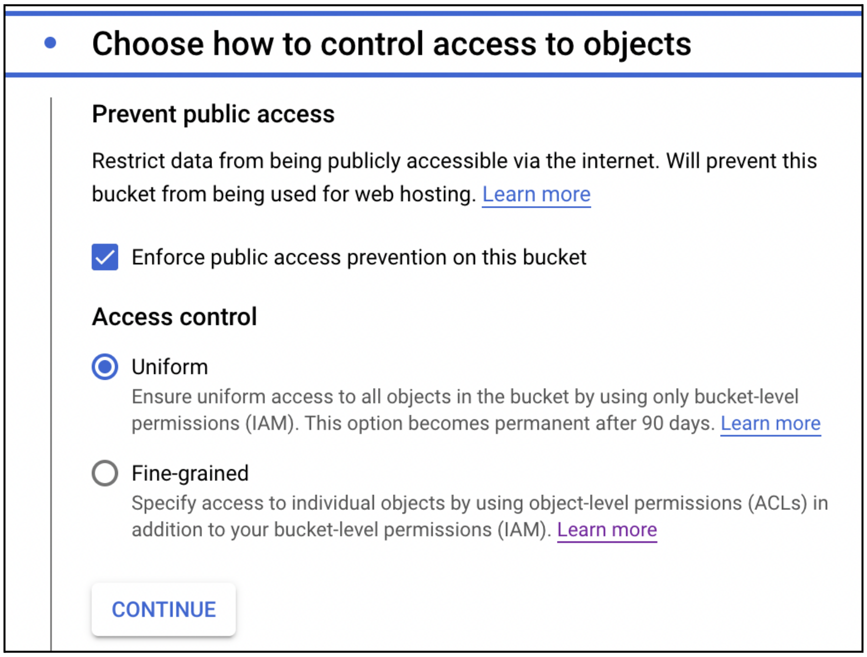
● Standard
Best for short-term storage and frequently accessed data

○ Nearline
Best for backups and data accessed less than once a month

○ Coldline
Best for disaster recovery and data accessed less than once a quarter

○ Archive
Best for long-term digital preservation of data accessed less than once a year

- Choose Uniform for Access control and check Enforce public access prevention on this bucket to turn it on. Note : Please make sure Enforce public access should be checked. Cloud Storage provides two systems for granting permissions to users to access buckets and objects: IAM and Access Control Lists (ACLs).



Choose how to control access to objects

Prevent public access

Restrict data from being publicly accessible via the internet. Will prevent this bucket from being used for web hosting. Learn more

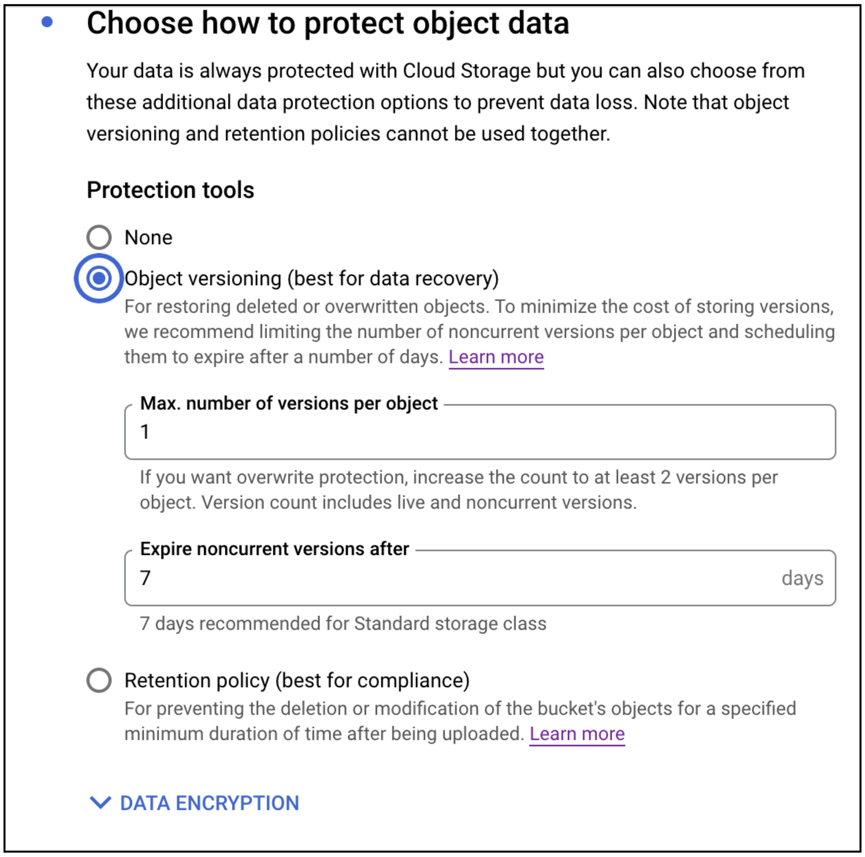
☑ Enforce public access prevention on this bucket

Access control

● Uniform
Ensure uniform access to all objects in the bucket by using only bucket-level permissions (IAM). This option becomes permanent after 90 days. Learn more

○ Fine-grained
Specify access to individual objects by using object-level permissions (ACLs) in addition to your bucket-level permissions (IAM). Learn more

- Select Object versioning that of the fields as their default values and click Create.



Choose how to protect object data

Your data is always protected with Cloud Storage but you can also choose from these additional data protection options to prevent data loss. Note that object versioning and retention policies cannot be used together.

Protection tools

○ None

● Object versioning (best for data recovery)
For restoring deleted or overwritten objects. To minimize the cost of storing versions, we recommend limiting the number of noncurrent versions per object and scheduling them to expire after a number of days. Learn more

Max. number of versions per object: 1
If you want overwrite protection, increase the count to at least 2 versions per object. Version count includes live and noncurrent versions.

Expire noncurrent versions after: 7 days
7 days recommended for Standard storage class

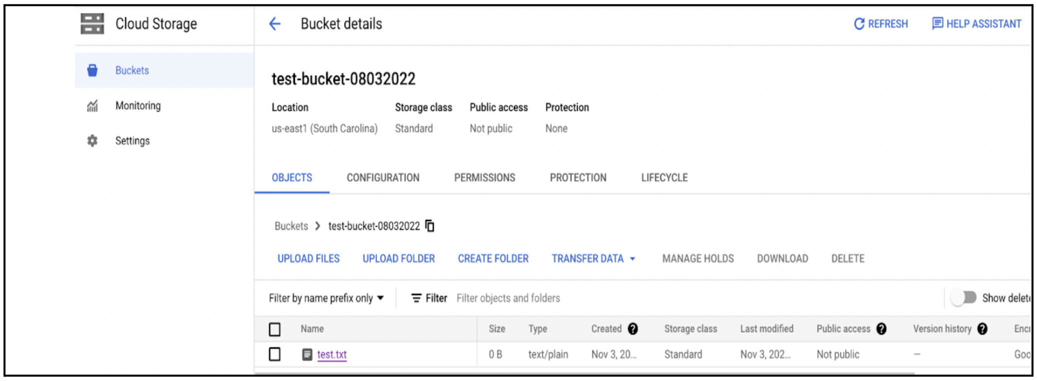
○ Retention policy (best for compliance)
For preventing the deletion or modification of the bucket's objects for a specified minimum duration of time after being uploaded. Learn more

It also has a command line option to create bucket, Follow the command below :

```
gcloud storage buckets create gs://BUCKET_NAME or
gsutil mb gs://BUCKET_NAME
```

Upload and Delete the file in Bucket

- The following step to upload and delete the file Via a Console and Command line:
    - Click Cloud Storage in the left navigation panel.
    - Click on the bucket name which is created in the previous step.
    - Click on **UPLOAD FILES** and select your file to upload.



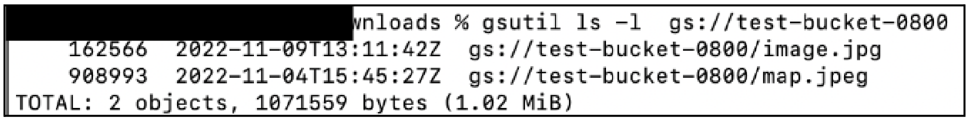
test-bucket-08032022

Location	Storage class	Public access	Protection
us-east1 (South Carolina)	Standard	Not public	None

☐ Name	Size	Type	Created	Storage class	Last modified	Public access	Version history	Encr
☐ test.txt	0 B	text/plain	Nov 3, 20...	Standard	Nov 3, 202...	Not public	–	Goo

- To list the bucket object via a command line :

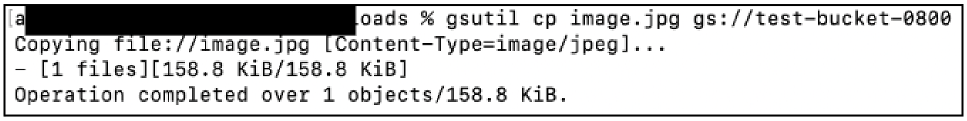
```
gsutil ls -l  gs://bucket_name/
```



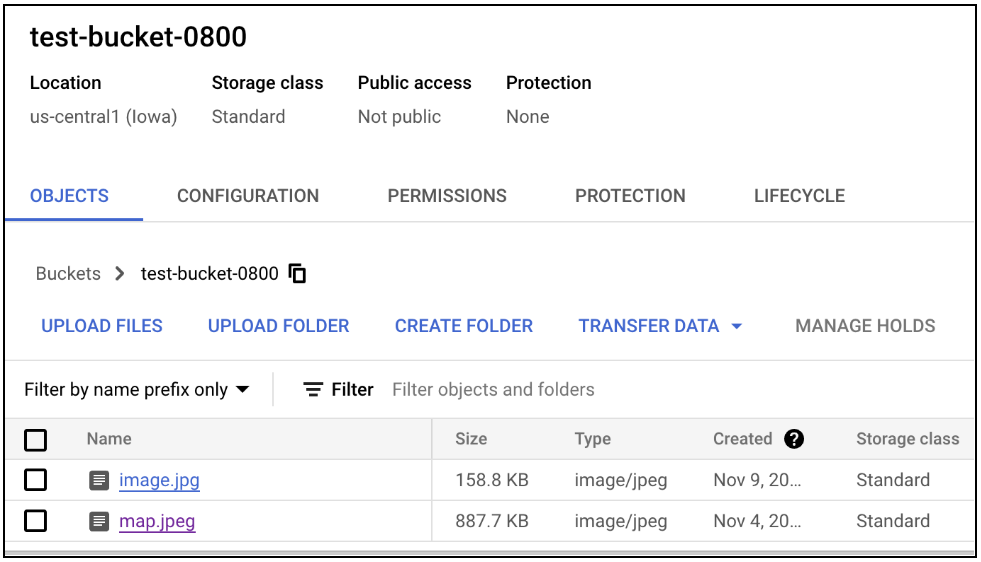
```
[redacted]wnloads % gsutil ls -l  gs://test-bucket-0800
    162566  2022-11-09T13:11:42Z  gs://test-bucket-0800/image.jpg
    908993  2022-11-04T15:45:27Z  gs://test-bucket-0800/map.jpeg
TOTAL: 2 objects, 1071559 bytes (1.02 MiB)
```

- If you want to upload a file using command prompt use gsutil cli tool.

```
gsutil cp file_name   gs://bucket_name
EX : gsutil cp  image.jpg  gs://test-bucket-080
```



```
[a[redacted]oads % gsutil cp image.jpg gs://test-bucket-0800
Copying file://image.jpg [Content-Type=image/jpeg]...
- [1 files][158.8 KiB/158.8 KiB]
Operation completed over 1 objects/158.8 KiB.
```

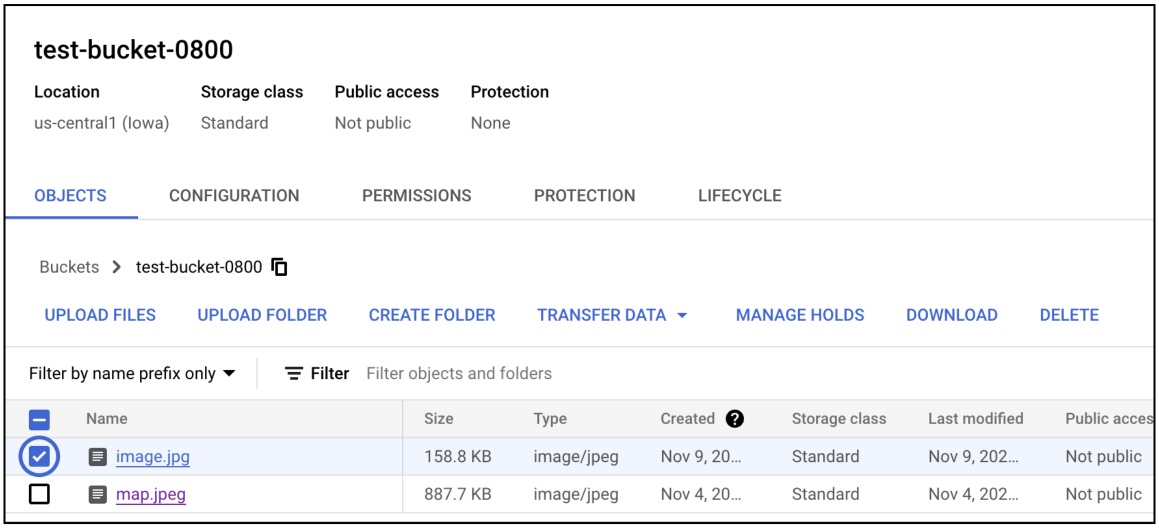


test-bucket-0800

Location	Storage class	Public access	Protection
us-central1 (Iowa)	Standard	Not public	None

□	Name	Size	Type	Created	Storage class
□	image.jpg	158.8 KB	image/jpeg	Nov 9, 20...	Standard
□	map.jpeg	887.7 KB	image/jpeg	Nov 4, 20...	Standard

- To Delete the file click on the checkbox of the respective file and then click on **DELETE** Button.



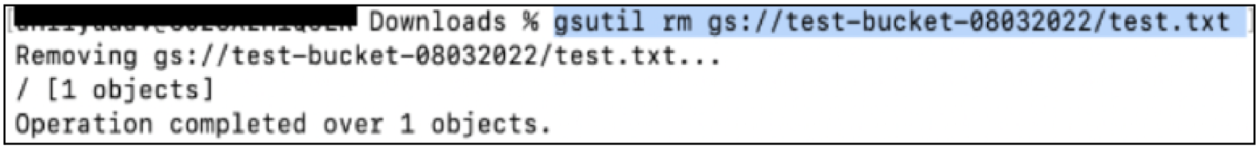
test-bucket-0800

Location	Storage class	Public access	Protection
us-central1 (Iowa)	Standard	Not public	None

▬	Name	Size	Type	Created	Storage class	Last modified	Public acces
☑	image.jpg	158.8 KB	image/jpeg	Nov 9, 20...	Standard	Nov 9, 202...	Not public
□	map.jpeg	887.7 KB	image/jpeg	Nov 4, 20...	Standard	Nov 4, 202...	Not public

If you want to delete the file via Command use gsutil command as follow:

Gsutil command : gsutil rm
Ex: gsutil rm gs://test-bucket-08032022/test.txt



```
[redacted] Downloads % gsutil rm gs://test-bucket-08032022/test.txt
Removing gs://test-bucket-08032022/test.txt...
/ [1 objects]
Operation completed over 1 objects.
```

Manage the Permission

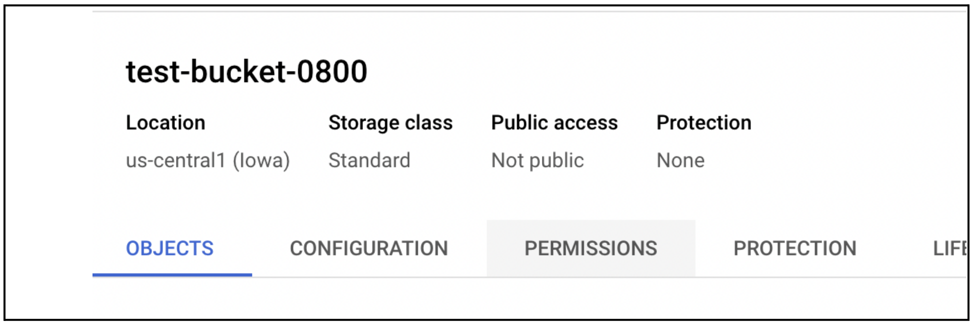
There are two types of permission that you can provide.

- Uniform : This permission you can provide on Bucket-level access.
- Fine-grained : This permission you can provide on object (file) level access.

Bucket-level Permission

Bucket level permission only implements Uniform access control.

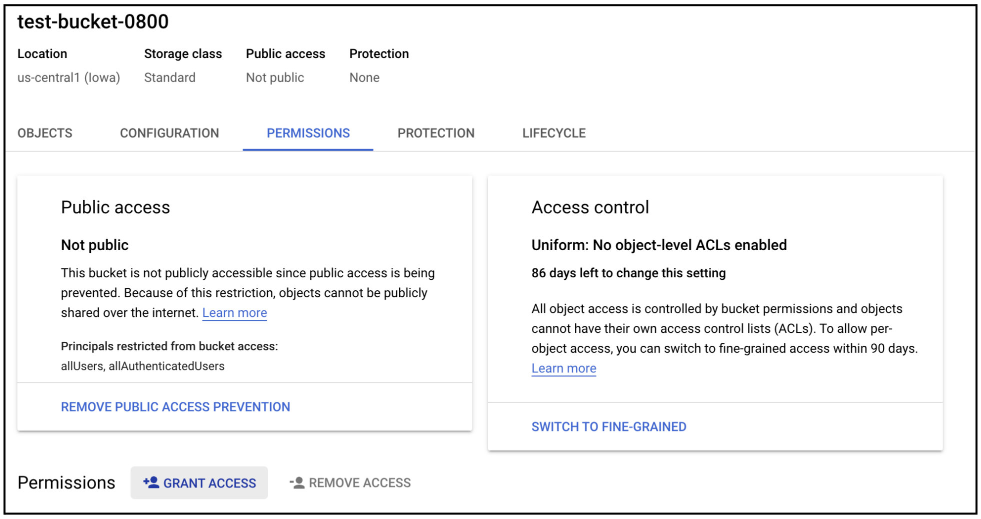
- Follow the given step to perform Uniform access control permission:
    - Click Cloud Storage in the left navigation panel.
    - Select the bucket.
    - Click on Permission



test-bucket-0800

Location	Storage class	Public access	Protection
us-central1 (Iowa)	Standard	Not public	None

    - Click on the Grant Access button.



test-bucket-0800

Location	Storage class	Public access	Protection
us-central1 (Iowa)	Standard	Not public	None

Public access

Not public

This bucket is not publicly accessible since public access is being prevented. Because of this restriction, objects cannot be publicly shared over the internet. Learn more

Principals restricted from bucket access:
allUsers, allAuthenticatedUsers

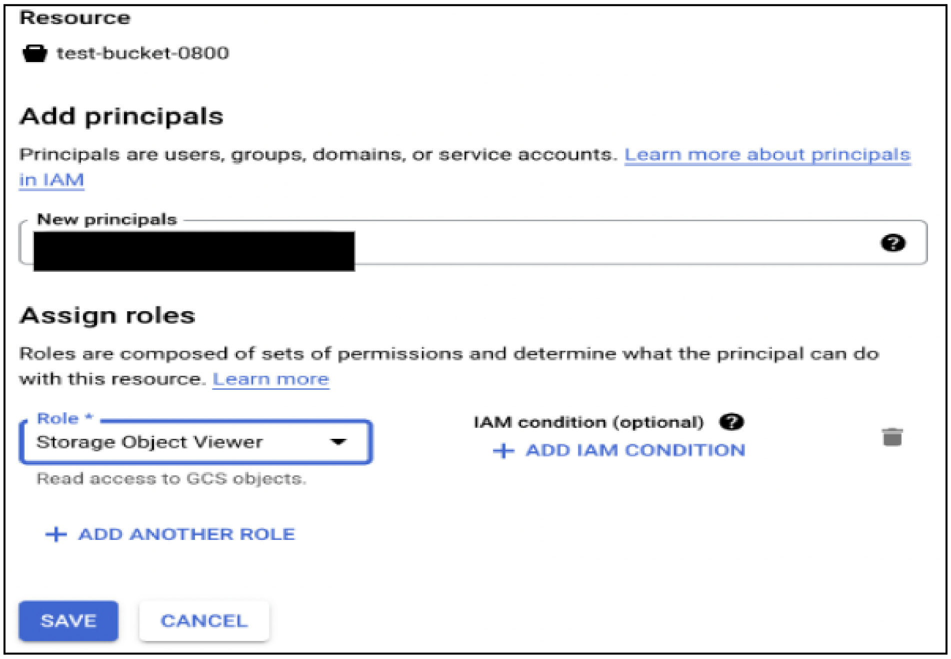
Access control

Uniform: No object-level ACLs enabled

86 days left to change this setting

All object access is controlled by bucket permissions and objects cannot have their own access control lists (ACLs). To allow per-object access, you can switch to fine-grained access within 90 days. Learn more

- ○ Add principal in the New principal box **allusers** and select Storage Object Viewer and save it.



Resource

test-bucket-0800

Add principals

Principals are users, groups, domains, or service accounts. Learn more about principals in IAM

New principals: [redacted]

Assign roles

Roles are composed of sets of permissions and determine what the principal can do with this resource. Learn more

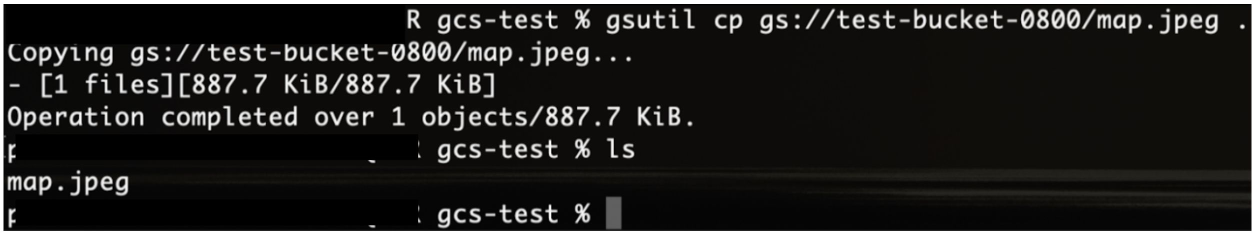
Role *: Storage Object Viewer

Read access to GCS objects.

IAM condition (optional)

Command for changing the bucket permission :

Gsutil command : gsutil iam ch user:john.doe@example.com:objectViewer gs://example-bucket
#To check the above setup enter the following command :
command : gsutil cp gs://<bucket_name>/<file_name> path/
Example : gsutil cp gs://test-bucket-0800/map.jpeg path

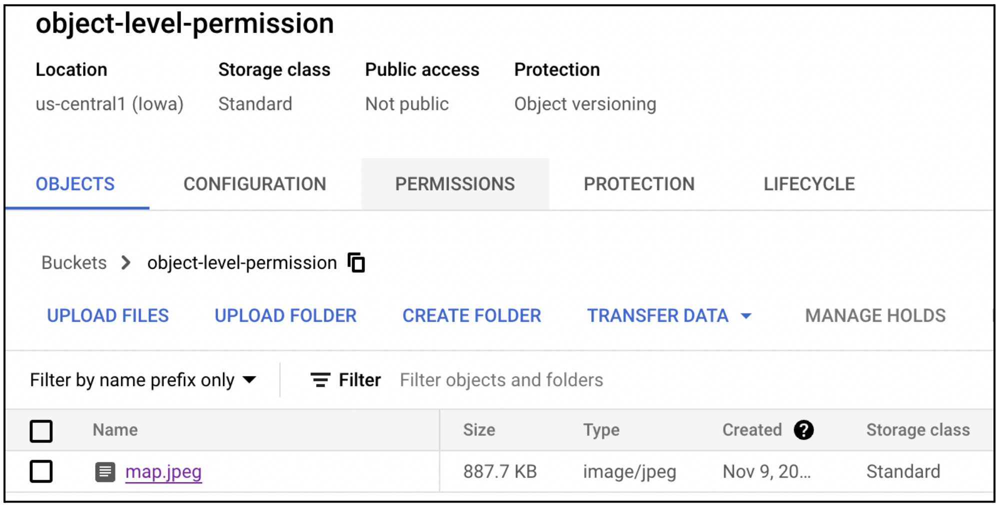


```
[redacted] R gcs-test % gsutil cp gs://test-bucket-0800/map.jpeg .
Copying gs://test-bucket-0800/map.jpeg...
- [1 files][887.7 KiB/887.7 KiB]
Operation completed over 1 objects/887.7 KiB.
[redacted] gcs-test % ls
map.jpeg
[redacted] gcs-test %
```

Object-level Permission

Object level permission only implements Fine-grained access control.

- Follow the given step :
    - Click Cloud Storage in the left navigation panel.
    - Select the bucket.
    - Click on Permission

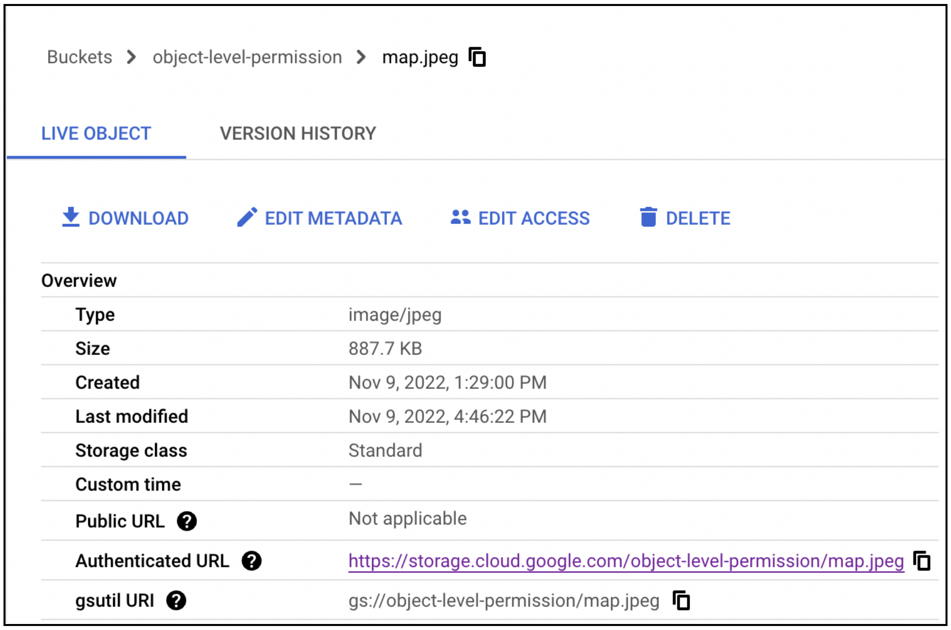


object-level-permission

Location	Storage class	Public access	Protection
us-central1 (Iowa)	Standard	Not public	Object versioning

☐	Name	Size	Type	Created	Storage class
☐	map.jpeg	887.7 KB	image/jpeg	Nov 9, 20…	Standard

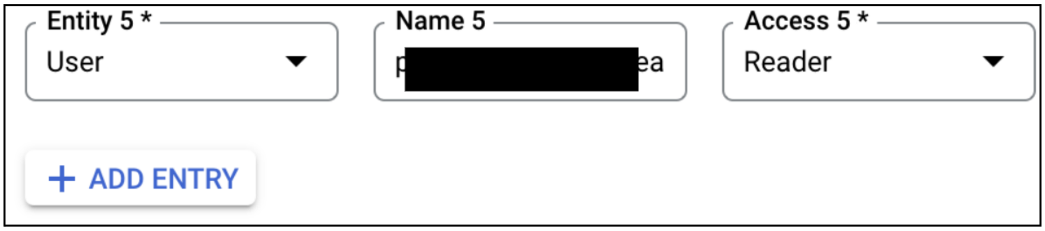
    - click on the file (Object).



Overview	
Type	image/jpeg
Size	887.7 KB
Created	Nov 9, 2022, 1:29:00 PM
Last modified	Nov 9, 2022, 4:46:22 PM
Storage class	Standard
Custom time	—
Public URL	Not applicable
Authenticated URL	https://storage.cloud.google.com/object-level-permission/map.jpeg
gsutil URI	gs://object-level-permission/map.jpeg

    - Click on the Edit Access button.

- ○ Click on the Add Entry button and select User in Entity, Enter Principal in Name and select Reader in Access.



Entity 5 * User

Name 5 [redacted]

Access 5 * Reader

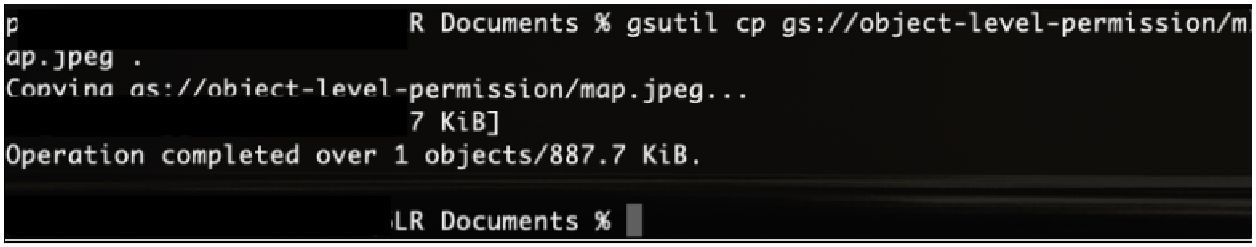
- ○ click on **Save**.

Command for changing the bucket permission :

Gsutil command : gsutil acl ch -u john.doe@example.com:R gs://example-bucket

To check the above setup enter the following command :

Gsutil command : gsutil cp gs://<bucket_name>/<file_name> path/
Example : gsutil cp gs://object-level-permission/map.jpeg path/



```
[redacted] R Documents % gsutil cp gs://object-level-permission/m
ap.jpeg .
Copying gs://object-level-permission/map.jpeg...
[redacted] 7 KiB]
Operation completed over 1 objects/887.7 KiB.

[redacted] LR Documents % 
```

Best Practices

- IAM provides an audit trail, so use IAM over ACL when possible.
- Cloud Storage's autoscaling works well for gradual increases in requests rather than sudden spikes.
    - No boot is required if the request rate is less than 1000 write requests per second or 5000 read requests per second.
    - If you expect your request rate to exceed these thresholds, start with a request rate below or near the threshold and double your request rate every 20 minutes.
- Cloud Storage uploads data to different shards based on file name/path, avoiding the sequential naming bottleneck, as using the same pattern would overload the shards and degrade performance.
- Use Truncated exponential backoff as a standard error handling strategy
- For multiple smaller files, use gsutil with -m option that performs a batched, parallel, multi-threaded/multi-processing to upload which can significantly increase the performance of an upload
- For large objects downloads, use gsutil with HTTP Range GET requests to perform “sliced” downloads in parallel
- To upload large files efficiently, use parallel composite upload with object composition to perform uploads in parallel for large, local files. It splits a large file into component pieces, uploads them in parallel, and then recomposes them once they’re in the cloud (and deletes the temporary components it created locally).

Reference link

- https://cloud.google.com/storage/docs/introduction
- https://cloud.google.com/storage/docs/gsutil/commands/iam
- https://cloud.google.com/storage/docs/access-control
- https://cloud.google.com/storage/docs/access-control/create-manage-lists
- https://cloud.google.com/storage/docs/using-uniform-bucket-level-access