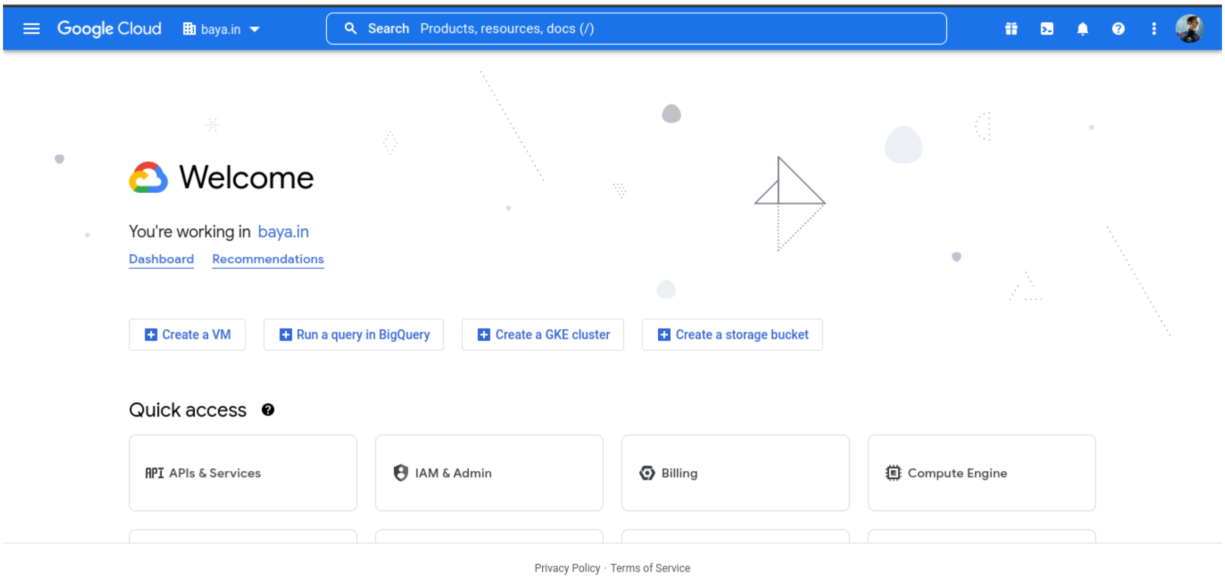
Creating a Service Account to access bucket

Creating a Service Account to access bucket

Create a Service Account:

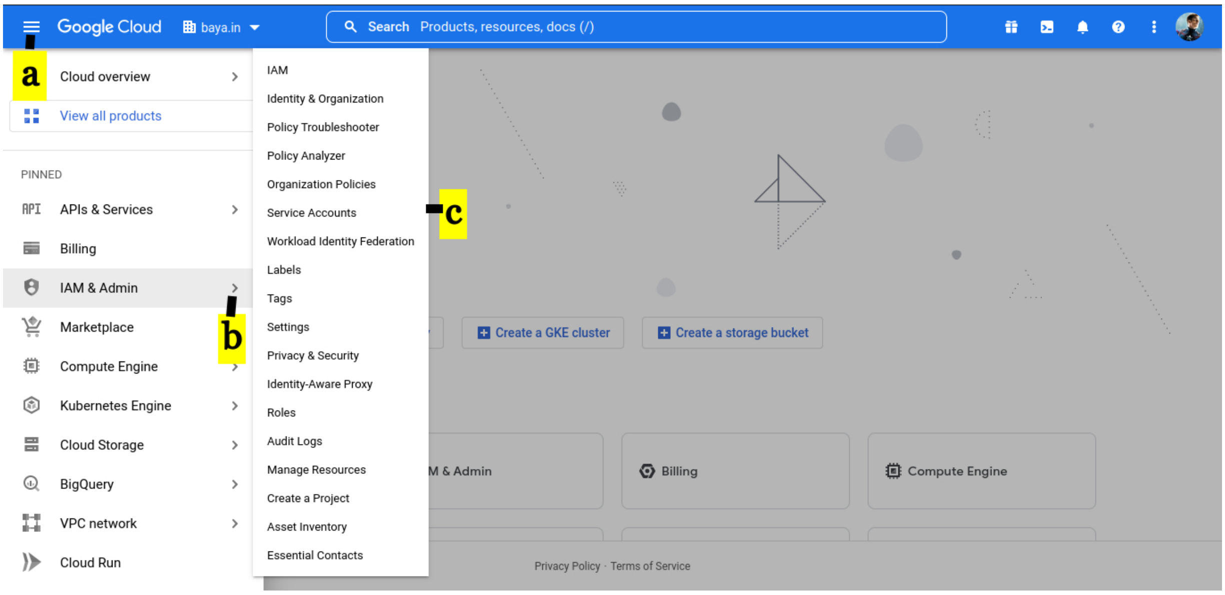
1. Login to G-suite Admin account and navigate to Google Developers Console (https://console.developers.google.com/)(https://console.developers.google.com/)



a. Select hamburger menu in top left corner.

b. Select IAM & Admin.

c. Select Service Accounts.



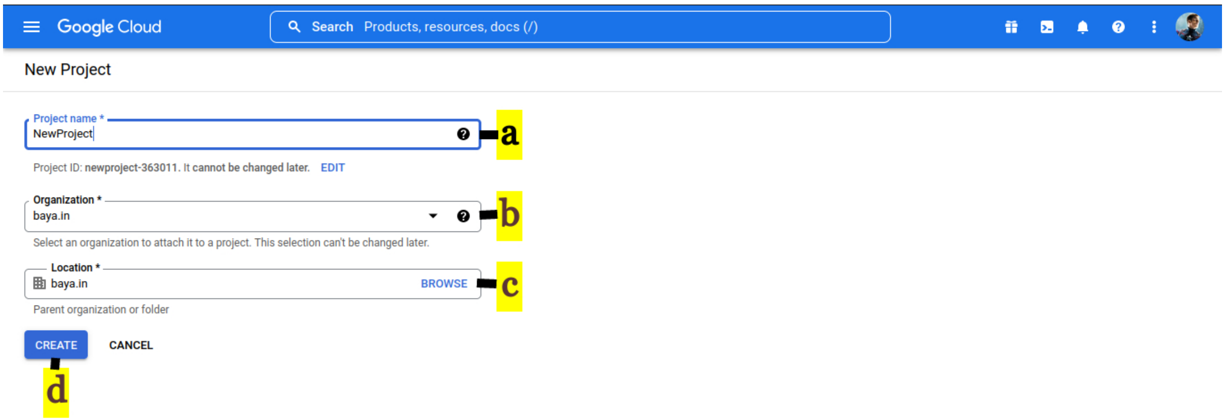
2. CREATE A PROJECT

a. Provide Project name

b. Specify the Organization

c. Select the Location

d. Click CREATE



New Project

Project name * NewProject

Project ID: newproject-363011. It cannot be changed later. EDIT

Organization * baya.in

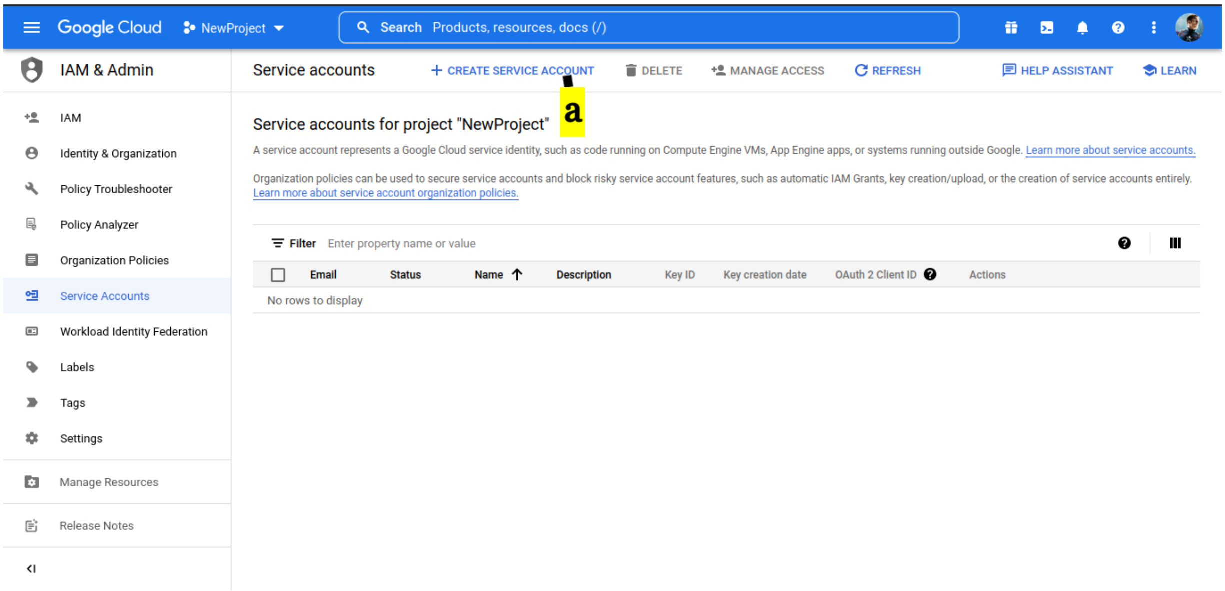
Select an organization to attach it to a project. This selection can't be changed later.

Location * baya.in BROWSE

Parent organization or folder

3. Create a service account

a. Click CREATE SERVICE ACCOUNT.



Service accounts for project "NewProject"

A service account represents a Google Cloud service identity, such as code running on Compute Engine VMs, App Engine apps, or systems running outside Google. Learn more about service accounts.

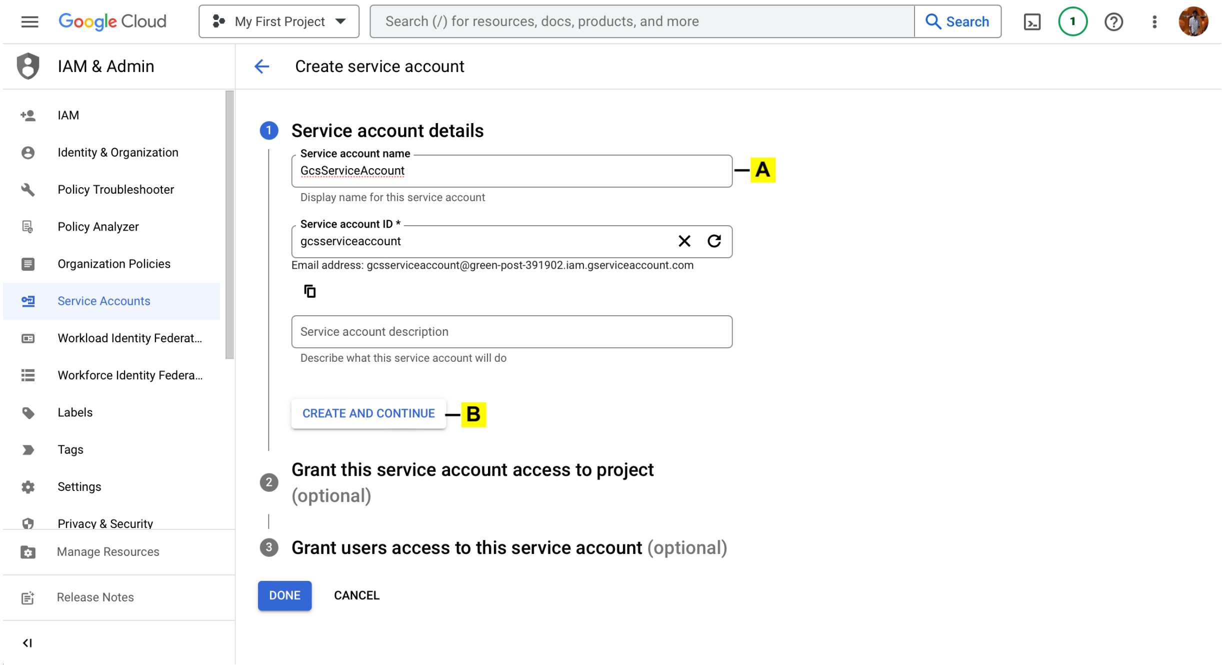
Organization policies can be used to secure service accounts and block risky service account features, such as automatic IAM Grants, key creation/upload, or the creation of service accounts entirely. Learn more about service account organization policies.

□	Email	Status	Name ↑	Description	Key ID	Key creation date	OAuth 2 Client ID	Actions
No rows to display								

4. On the service account details window.

   A. Provide Service account name

   B. Click CREATE AND CONTINUE



1 Service account details

Service account name: GcsServiceAccount

Display name for this service account

Service account ID *: gcsserviceaccount

Email address: gcsserviceaccount@green-post-391902.iam.gserviceaccount.com

Service account description

Describe what this service account will do

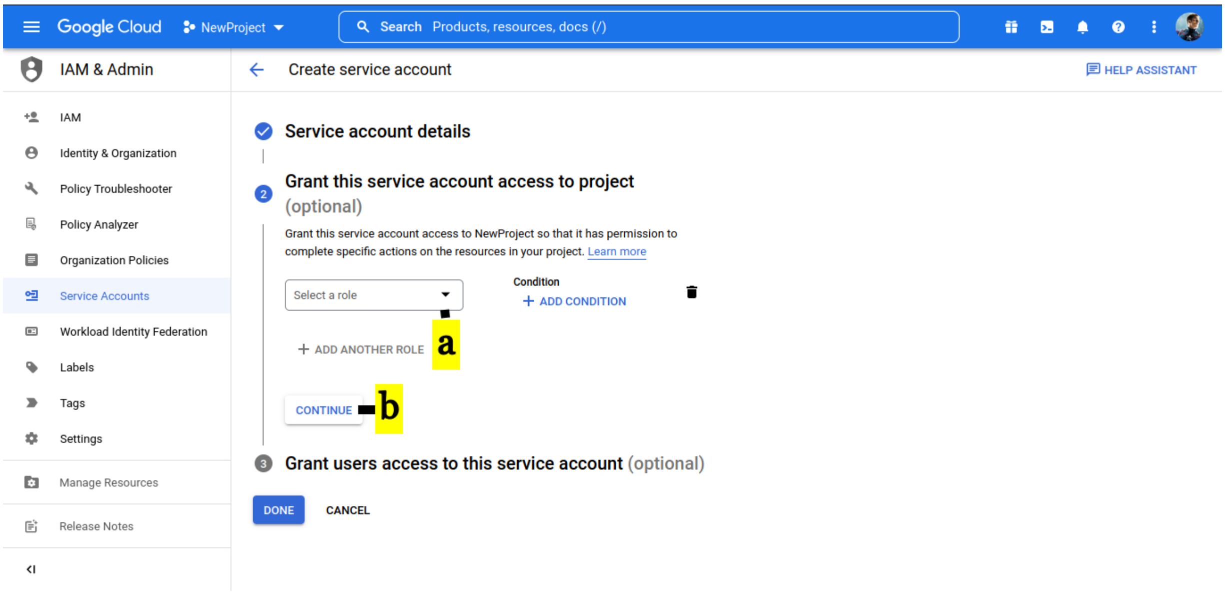
2 Grant this service account access to project (optional)

3 Grant users access to this service account (optional)

5. Grant this service account access to project.

   a. Leave this empty

b. Click CONTINUE



Service account details

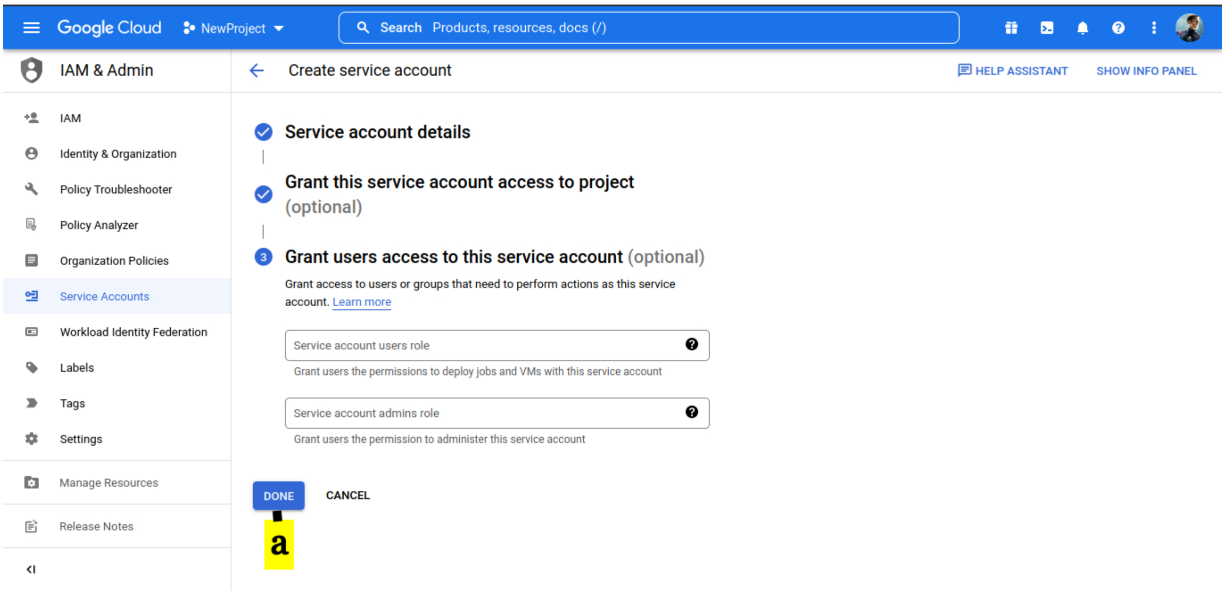
2 Grant this service account access to project (optional)

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

3 Grant users access to this service account (optional)

6. Grant users access to this service account (optional)

a. Click DONE



Service account details

Grant this service account access to project (optional)

3 Grant users access to this service account (optional)

Grant access to users or groups that need to perform actions as this service account. Learn more

Grant users the permissions to deploy jobs and VMs with this service account

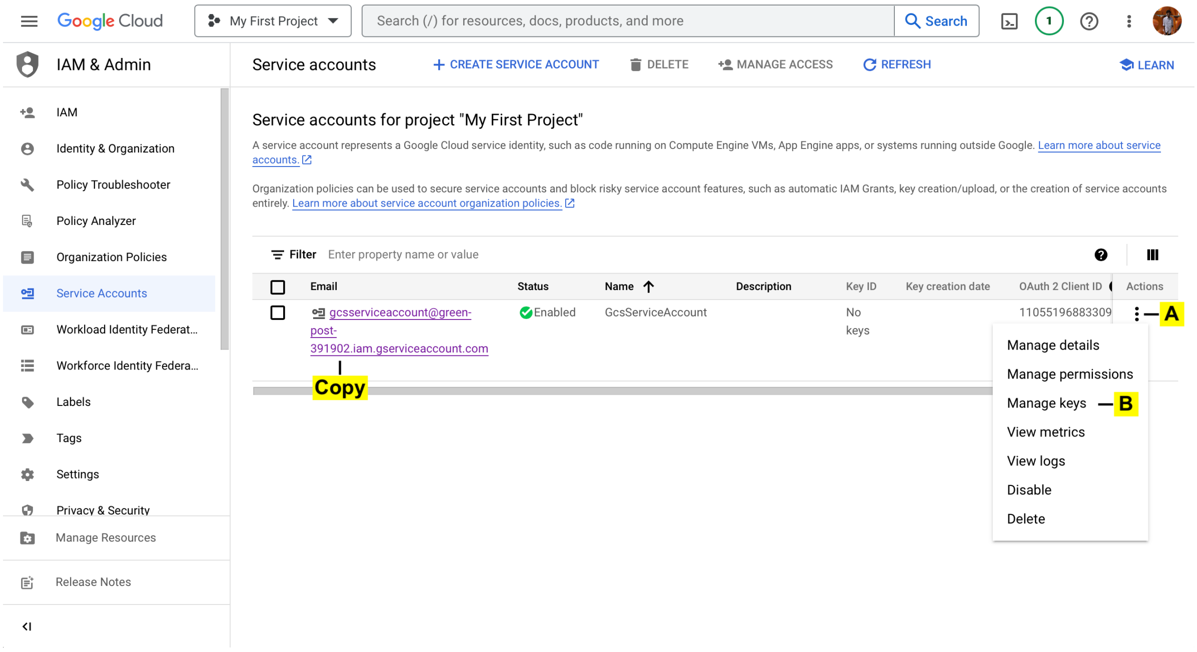
Grant users the permission to administer this service account

7. On service account window.

A. Click on Action button denoted by three dots

B. Select Manage Keys

COPY. Copy the email id (This id should be copied at this stage as it will not be visible later. This id will be used for Assigning Permissions)



Service accounts for project "My First Project"

A service account represents a Google Cloud service identity, such as code running on Compute Engine VMs, App Engine apps, or systems running outside Google. Learn more about service accounts.

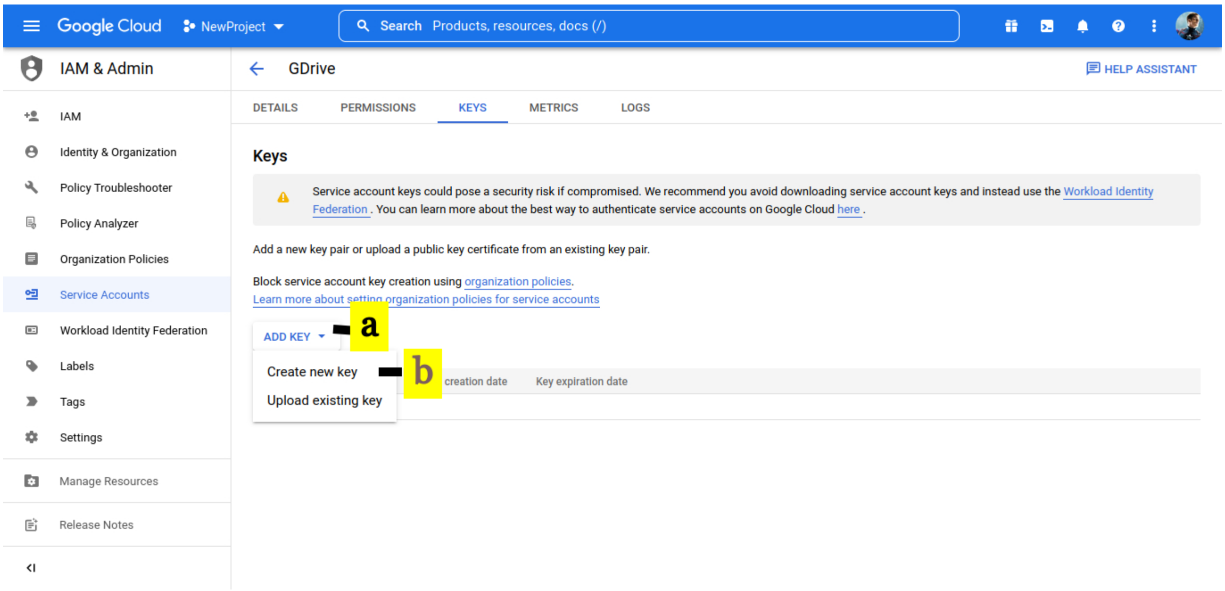
Organization policies can be used to secure service accounts and block risky service account features, such as automatic IAM Grants, key creation/upload, or the creation of service accounts entirely. Learn more about service account organization policies.

□	Email	Status	Name ↑	Description	Key ID	Key creation date	OAuth 2 Client ID	Actions
□	gcsserviceaccount@green-post-391902.iam.gserviceaccount.com	✓ Enabled	GcsServiceAccount		No keys		11055196883309	⋮

8. Create a key

a. ADD KEY

b. Create new key



Keys

Service account keys could pose a security risk if compromised. We recommend you avoid downloading service account keys and instead use the Workload Identity Federation . You can learn more about the best way to authenticate service accounts on Google Cloud here .

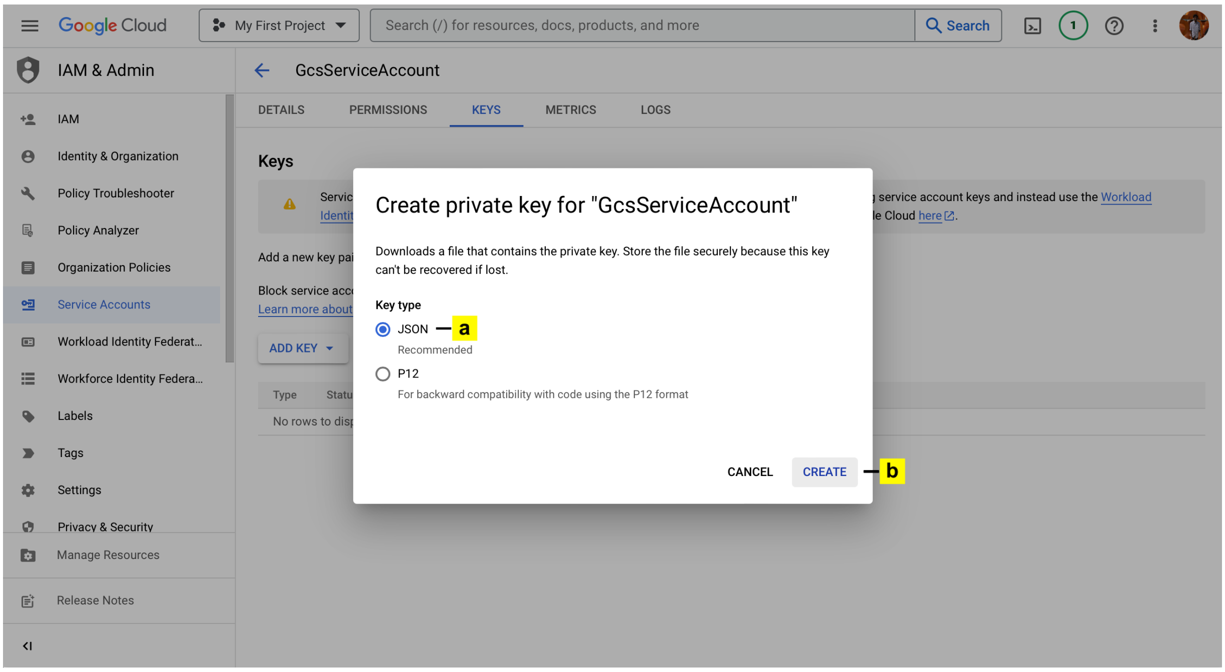
Add a new key pair or upload a public key certificate from an existing key pair.

Block service account key creation using organization policies.
Learn more about setting organization policies for service accounts

9. Create private key.

a. Click on JSON

b. Click on CREATE. On creation, the key will be downloaded to your desktop. **Save this JSON file as you will need it when registering the bucket with LegacyFlo. (https://docs.mithi.com/home/preparing-a-destination-gcs-bucket-for-legacyflo)**



Create private key for "GcsServiceAccount"

Downloads a file that contains the private key. Store the file securely because this key can't be recovered if lost.

Key type

● JSON

Recommended

○ P12

For backward compatibility with code using the P12 format

CANCEL CREATE

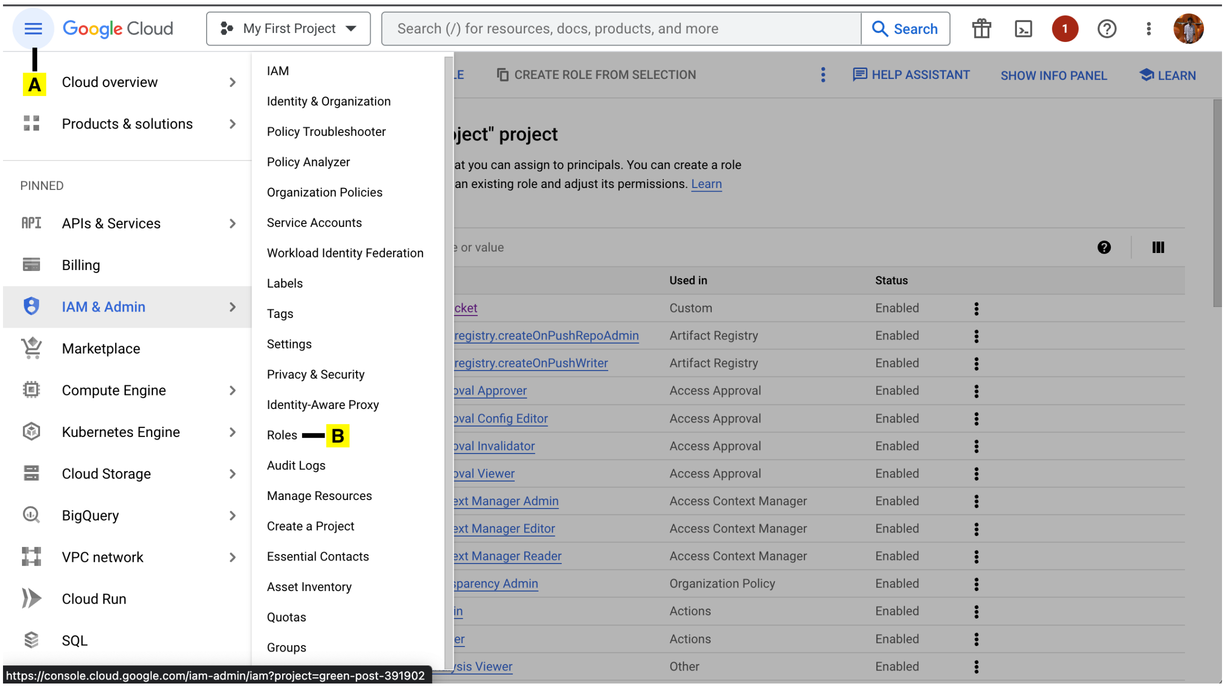
Give access to the bucket via the service account

By default, a newly created service account won't have any permissions. To limit access to a single bucket, you need to grant it the necessary permissions for that bucket only. Here's how:

10. First Create an IAM role with minimal permissions.

A. Go to the Console Menu

B. Choose Roles under IAM & Admin.

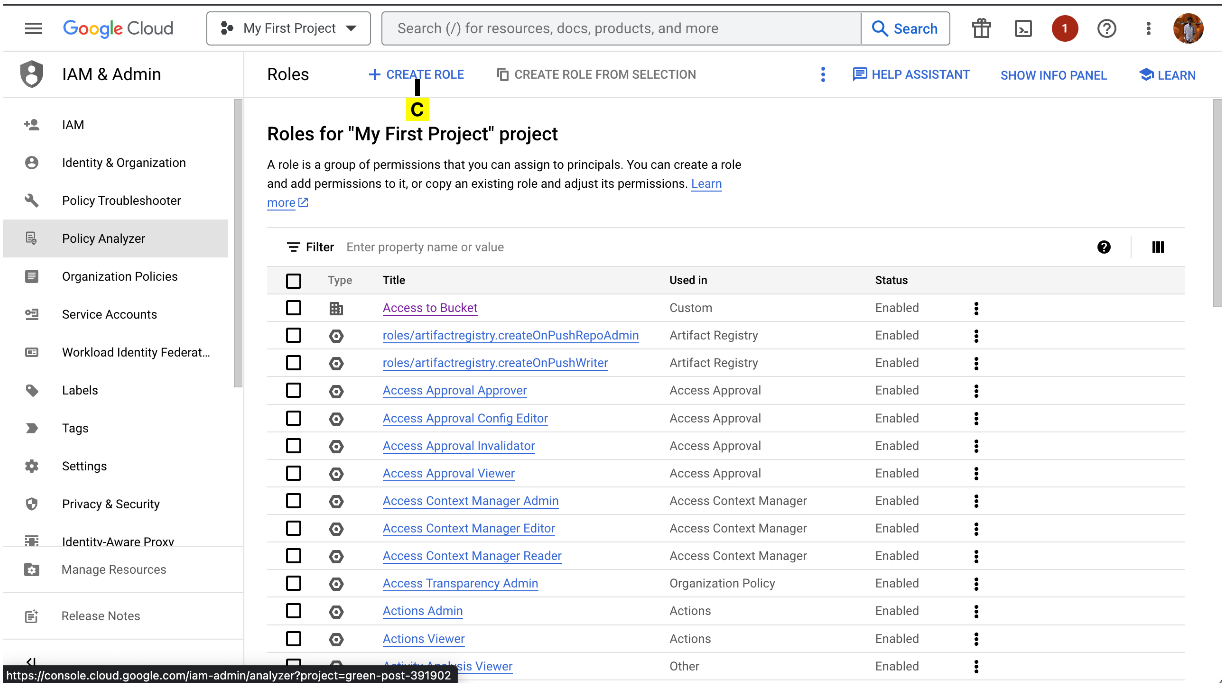


ject" project

at you can assign to principals. You can create a role an existing role and adjust its permissions. Learn

	Used in	Status
cket	Custom	Enabled
registry.createOnPushRepoAdmin	Artifact Registry	Enabled
registry.createOnPushWriter	Artifact Registry	Enabled
oval Approver	Access Approval	Enabled
oval Config Editor	Access Approval	Enabled
oval Invalidator	Access Approval	Enabled
oval Viewer	Access Approval	Enabled
ext Manager Admin	Access Context Manager	Enabled
ext Manager Editor	Access Context Manager	Enabled
ext Manager Reader	Access Context Manager	Enabled
sparency Admin	Organization Policy	Enabled
in	Actions	Enabled
er	Actions	Enabled
ysis Viewer	Other	Enabled

C. Click on Create Role



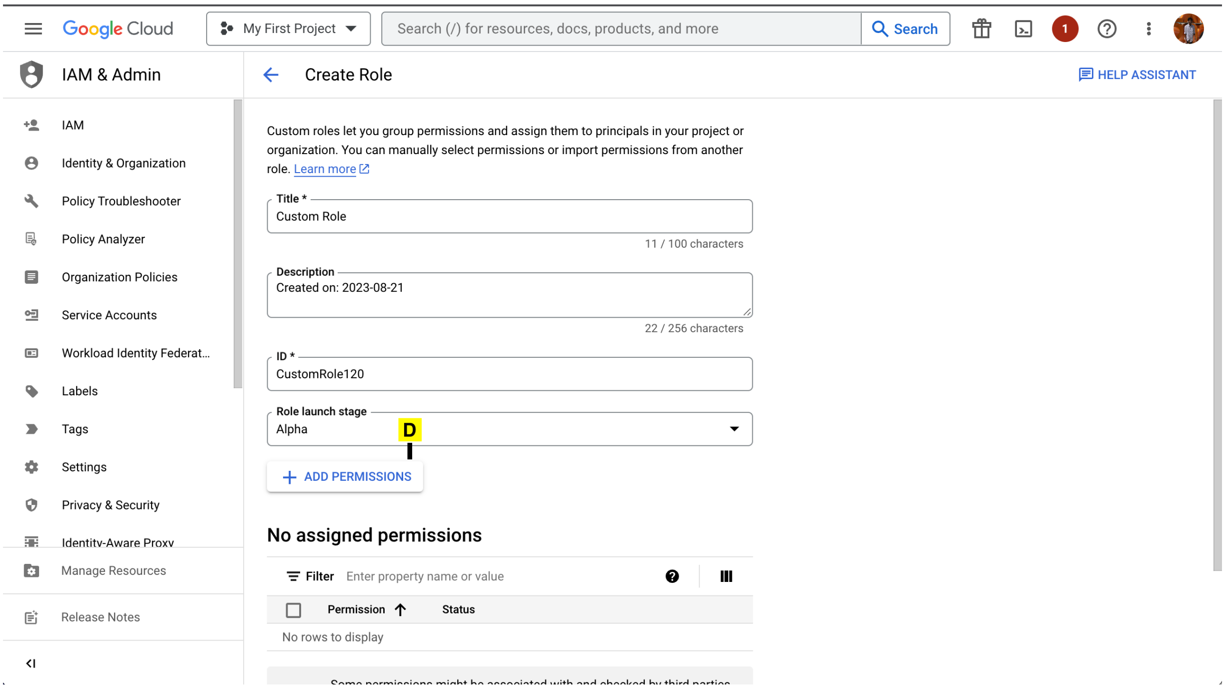
Roles for "My First Project" project

A role is a group of permissions that you can assign to principals. You can create a role and add permissions to it, or copy an existing role and adjust its permissions. Learn more

□	Type	Title	Used in	Status
□		Access to Bucket	Custom	Enabled
□		roles/artifactregistry.createOnPushRepoAdmin	Artifact Registry	Enabled
□		roles/artifactregistry.createOnPushWriter	Artifact Registry	Enabled
□		Access Approval Approver	Access Approval	Enabled
□		Access Approval Config Editor	Access Approval	Enabled
□		Access Approval Invalidator	Access Approval	Enabled
□		Access Approval Viewer	Access Approval	Enabled
□		Access Context Manager Admin	Access Context Manager	Enabled
□		Access Context Manager Editor	Access Context Manager	Enabled
□		Access Context Manager Reader	Access Context Manager	Enabled
□		Access Transparency Admin	Organization Policy	Enabled
□		Actions Admin	Actions	Enabled
□		Actions Viewer	Actions	Enabled
□		Activity Analysis Viewer	Other	Enabled

Fill the Title and Create a Custom ID

D. Click on Add Permissions



Custom roles let you group permissions and assign them to principals in your project or organization. You can manually select permissions or import permissions from another role. Learn more

Title *: Custom Role
11 / 100 characters

Description: Created on: 2023-08-21
22 / 256 characters

ID *: CustomRole120

Role launch stage: Alpha

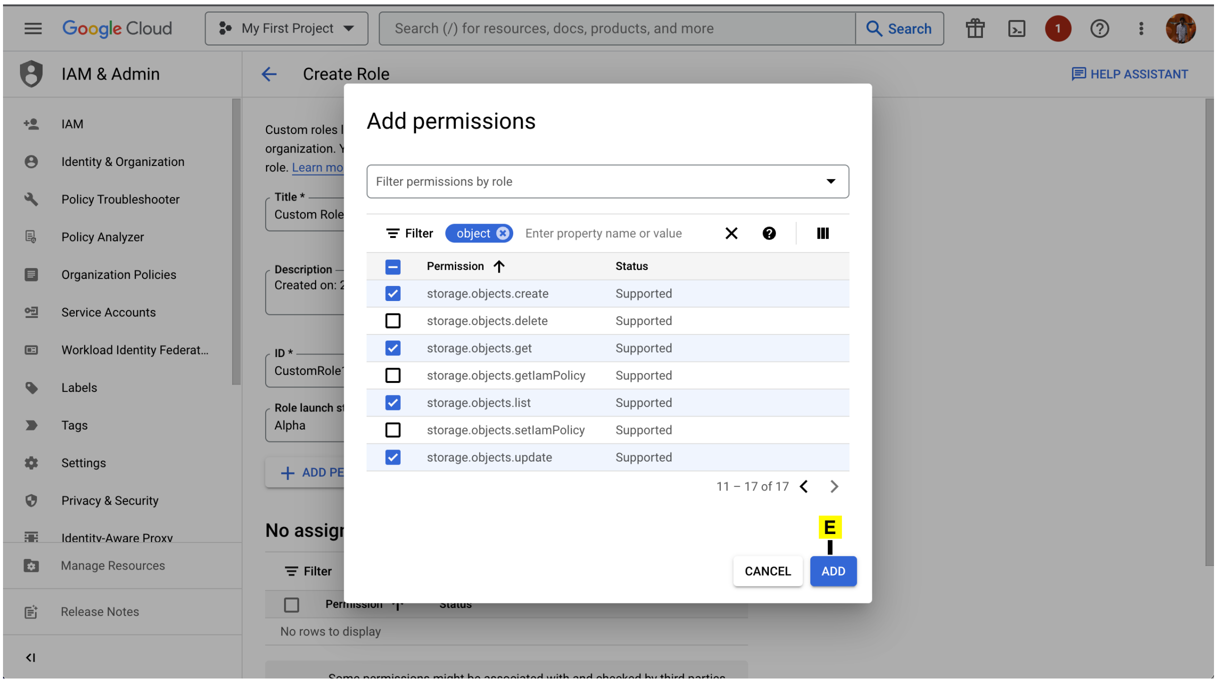
No assigned permissions

□	Permission	Status

No rows to display

Some permissions might be associated with and checked by third parties

E. Click on ADD



Add permissions

Filter permissions by role

Filter: object — Enter property name or value

	Permission	Status
☑	storage.objects.create	Supported
□	storage.objects.delete	Supported
☑	storage.objects.get	Supported
□	storage.objects.getIamPolicy	Supported
☑	storage.objects.list	Supported
□	storage.objects.setIamPolicy	Supported
☑	storage.objects.update	Supported

11 – 17 of 17

Title *: Custom Role

Description: Created on: 2

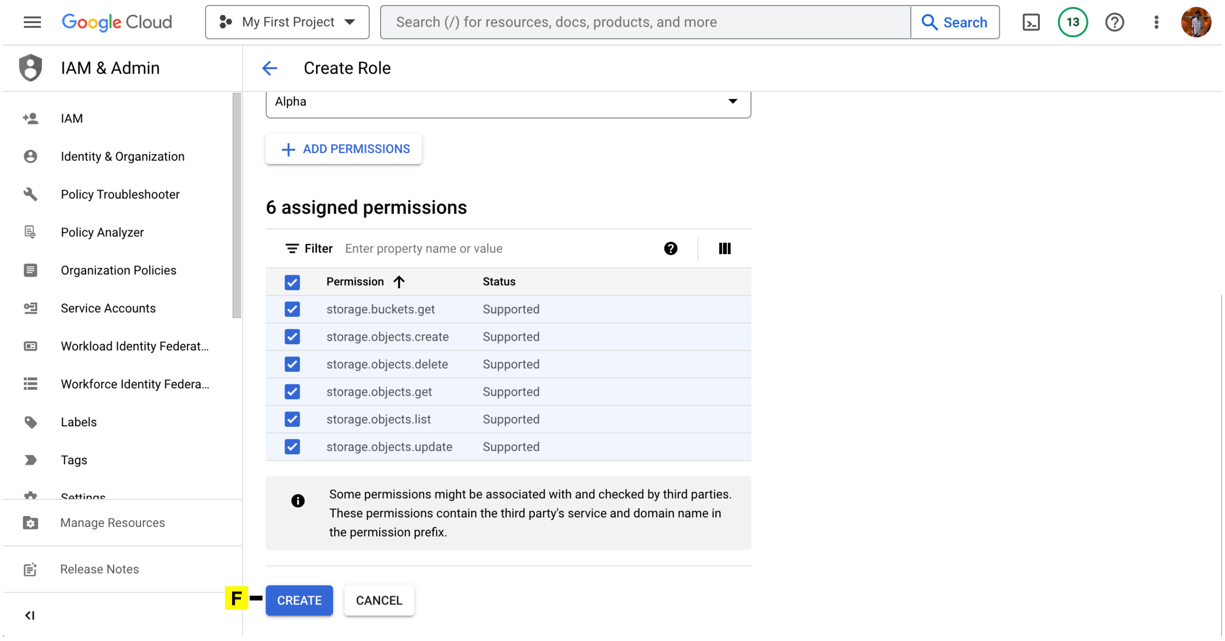
ID *: CustomRole

Role launch stage: Alpha

No assign

No rows to display

F. Click on CREATE



Alpha

6 assigned permissions

Filter: Enter property name or value

	Permission	Status
☑	storage.buckets.get	Supported
☑	storage.objects.create	Supported
☑	storage.objects.delete	Supported
☑	storage.objects.get	Supported
☑	storage.objects.list	Supported
☑	storage.objects.update	Supported

Some permissions might be associated with and checked by third parties. These permissions contain the third party's service and domain name in the permission prefix.

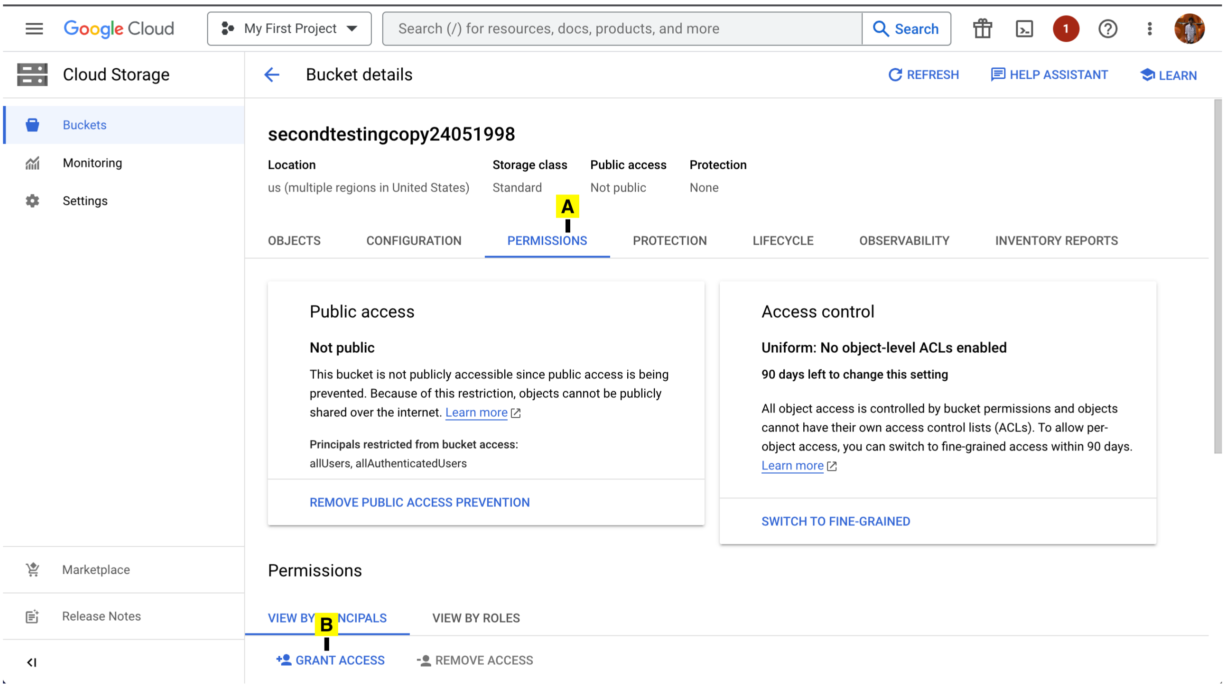
11. Find the Bucket you want to add permissions to in the Buckets section in Cloud Storage.

12. Click on the Bucket name to open its details page.

13. Add Permissions

A. Click on Permissions

B. Grant Access



Bucket details

secondtestingcopy24051998

Location	Storage class	Public access	Protection
us (multiple regions in United States)	Standard	Not public	None

OBJECTS CONFIGURATION PERMISSIONS PROTECTION LIFECYCLE OBSERVABILITY INVENTORY REPORTS

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

REMOVE PUBLIC ACCESS PREVENTION

Access control

Uniform: No object-level ACLs enabled

90 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

SWITCH TO FINE-GRAINED

Permissions

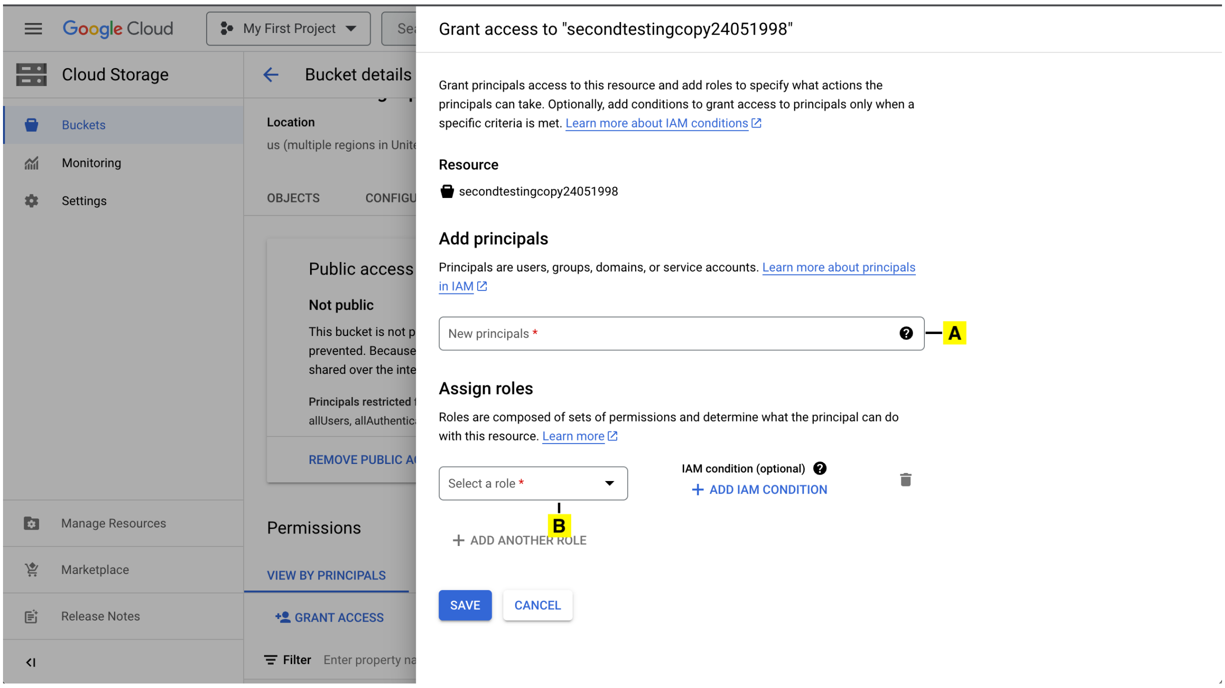
VIEW BY PRINCIPALS VIEW BY ROLES

GRANT ACCESS REMOVE ACCESS

14. Add Principal

A. Paste the Service Account Email copied in STEP 7

B. Choose the Custom IAM Role created in STEP 10



Grant access to "secondtestingcopy24051998"

Grant principals access to this resource and add roles to specify what actions the principals can take. Optionally, add conditions to grant access to principals only when a specific criteria is met. Learn more about IAM conditions

Resource

secondtestingcopy24051998

Add principals

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

New principals *

Assign roles

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

Select a role *

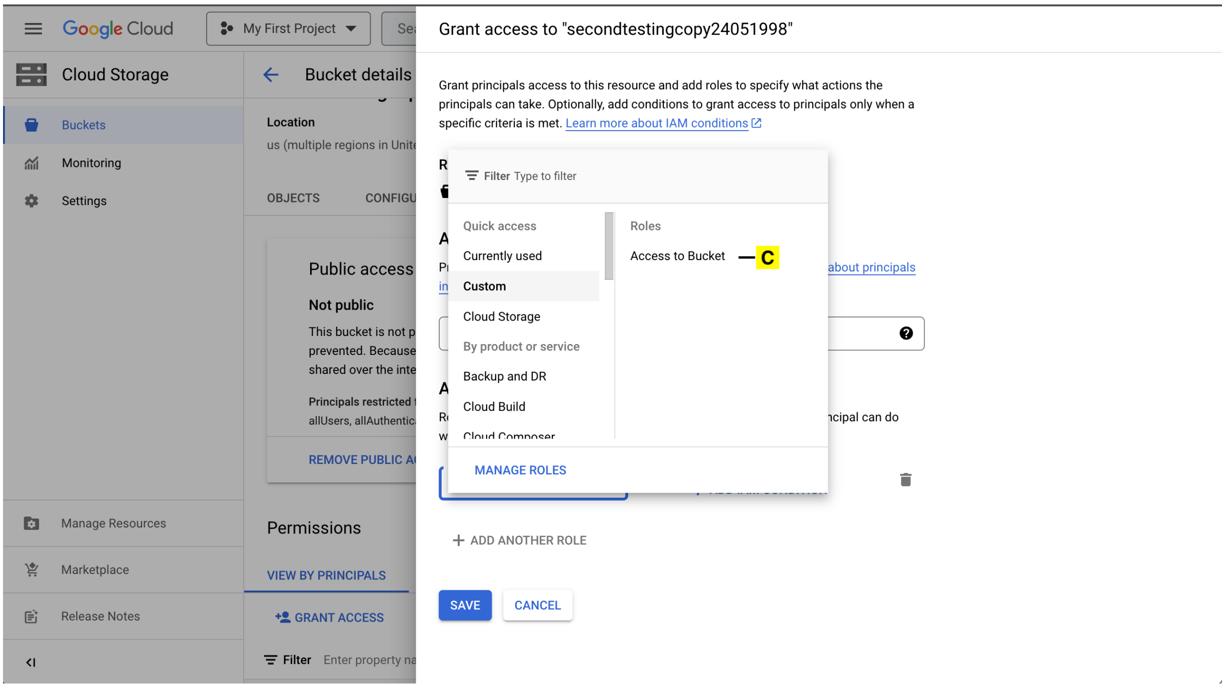
IAM condition (optional)

ADD IAM CONDITION

ADD ANOTHER ROLE

SAVE CANCEL

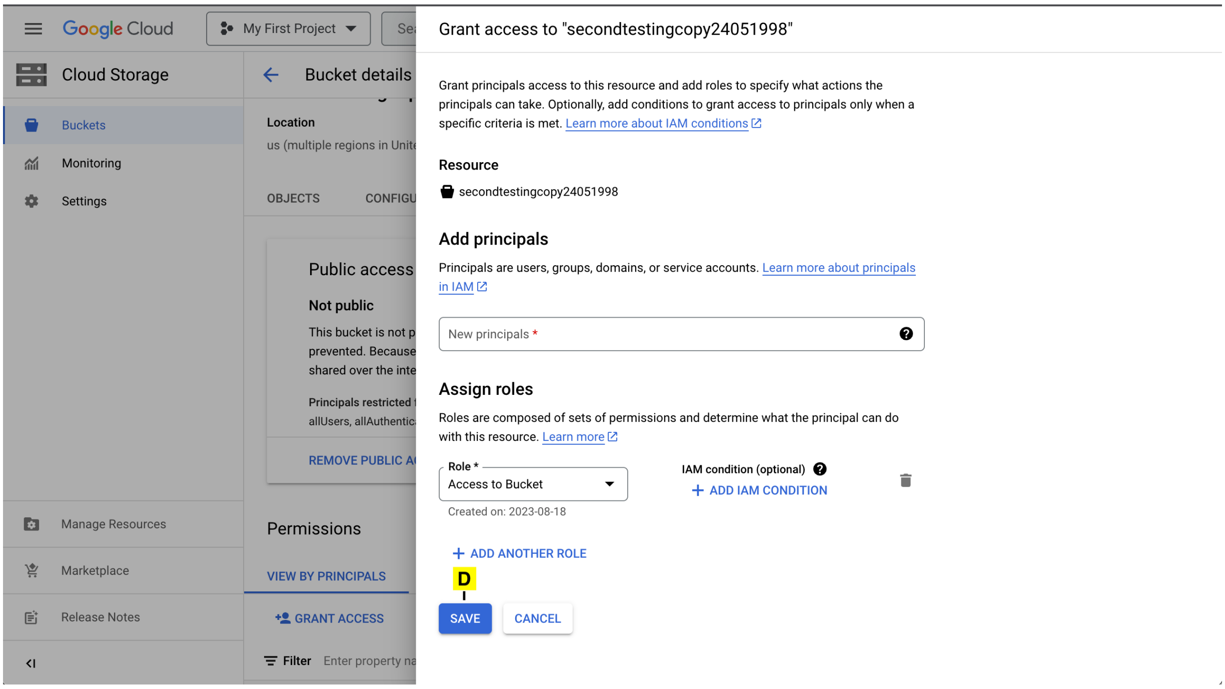
C. The custom role will be listed under Custom Group.



Grant access to "secondtestingcopy24051998"

Grant principals access to this resource and add roles to specify what actions the principals can take. Optionally, add conditions to grant access to principals only when a specific criteria is met. Learn more about IAM conditions

D. Click on SAVE



Grant access to "secondtestingcopy24051998"

Grant principals access to this resource and add roles to specify what actions the principals can take. Optionally, add conditions to grant access to principals only when a specific criteria is met. Learn more about IAM conditions

Resource

secondtestingcopy24051998

Add principals

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

New principals *

Assign roles

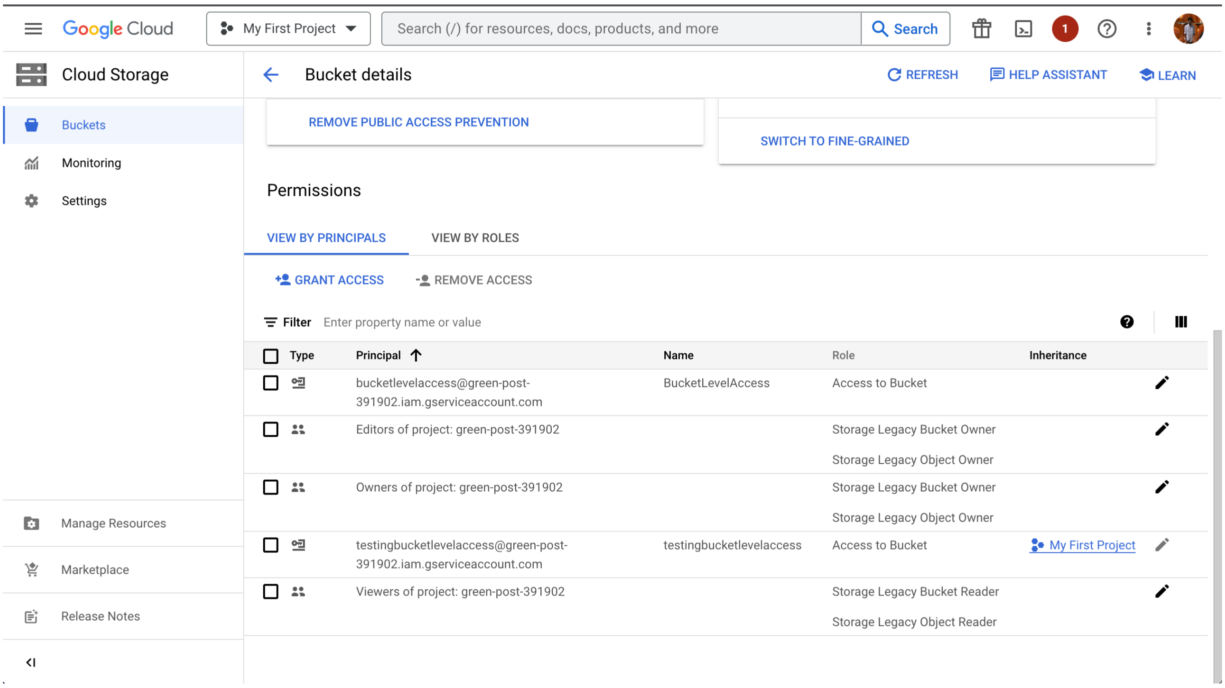
Roles are composed of sets of permissions and determine what the principal can do with this resource. Learn more

Role *: Access to Bucket

Created on: 2023-08-18

IAM condition (optional)

The principal will be added and will be listed below.



Bucket details

Permissions

□ Type	Principal ↑	Name	Role	Inheritance
□	bucketlevelaccess@green-post-391902.iam.gserviceaccount.com	BucketLevelAccess	Access to Bucket	
□	Editors of project: green-post-391902		Storage Legacy Bucket Owner Storage Legacy Object Owner	
□	Owners of project: green-post-391902		Storage Legacy Bucket Owner Storage Legacy Object Owner	
□	testingbucketlevelaccess@green-post-391902.iam.gserviceaccount.com	testingbucketlevelaccess	Access to Bucket	My First Project
□	Viewers of project: green-post-391902		Storage Legacy Bucket Reader Storage Legacy Object Reader	