Create a service account to access your storage 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/)

≡ Google Cloud 🗈 baya.in 👻	Q Search Products, resources, docs (/)		ii 5. 4	0 : 🔇
• 🙆 Welcome	۵			•
• You're working in baya.in Dashboard Recommendations	query in BigQuery 💽 Create a GKE clus	ter Create a storage bucket	•	
Quick access				
RPI APIs & Services	🕑 IAM & Admin	© Billing	Compute Engine	
	Privacy Polic	y · Terms of Service		

- a. Select hamburger menu in top left corner.
- b. Select IAM & Admin.
- c. Select Service Accounts.

Ţ	Google Cloud	baya.in	- (Q Search	Products, resources, docs (/)				🌲 🥹 i 🥵
a	Cloud overview	>	IAM Identity & Or	rganization	N.				
	View all products		Policy Troub	-					
PINN	ED		Policy Analy Organizatior						
API	APIs & Services	>	Service Acco	ounts	<mark>−c</mark>				
-	Billing			entity Federatior					
θ	IAM & Admin	>	Labels Tags						
$\sum_{i=1}^{n}$	Marketplace	b	Settings		Create a GKE clust	ter 🛨 Create a s	storage bucket		
۲	Compute Engine	~	Privacy & Se Identity-Awa						
٢	Kubernetes Engine	>	Roles						
	Cloud Storage	>	Audit Logs						
<u>(</u>	BigQuery	>	Manage Res Create a Pro		M & Admin	🕢 Billing	0	Compute Engine	
11	VPC network	>	Asset Invent	tory					
)>	Cloud Run		Essential Co	ontacts	Privacy Polic	· Terms of Service			

2. CREATE A PROJECT

- a. Provide Project name
- b. Specify the Organization
- c. Select the Location
- d. Click CREATE

≡ Google Cloud	Q Search Products, resources, docs (/)		ii	>.	۰	?		٢
New Project								
Project name * NewProject Project ID: newproject-363011. It cannot be chang	ed later. EDIT							
Organization * • • • • • • • • • • • • • • • • • •								
Location * baya.in Parent organization or folder	BROWSE							
CREATE CANCEL								

3. Create a service account

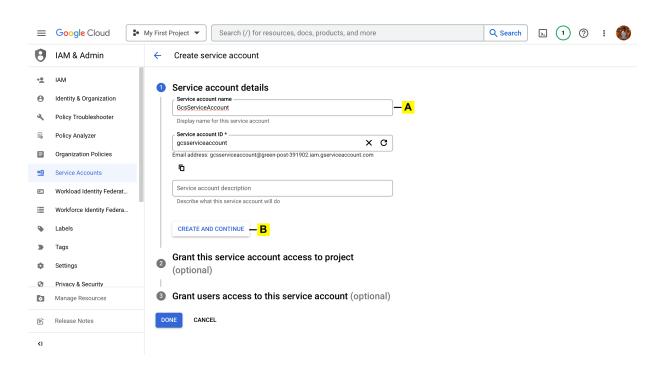
a. Click CREATE SERVICE ACCOUNT.

=	Google Cloud So NewF	roject ▼ Q Search Products, resources, docs (/)	ii 🛛 🌲 0 i 🍕
θ	IAM & Admin	Service accounts + CREATE SERVICE ACCOUNT	🗐 HELP ASSISTANT 🛛 🗢 LEARN
÷ <u>e</u>	IAM	Service accounts for project "NewProject"	
Θ	Identity & Organization	A service account represents a Google Cloud service identity, such as code running on Compute Engine VMs, App Engine apps, or systems run	ning outside Google. Learn more about service accounts.
٩	Policy Troubleshooter	Organization policies can be used to secure service accounts and block risky service account features, such as automatic IAM Grants, key cre Learn more about service account organization policies.	ation/upload, or the creation of service accounts entirely.
Ę	Policy Analyzer	Filter Enter property name or value	Ø III
	Organization Policies	Finter Enter property name or value Email Status Name Description Key ID Key creation date OAuth 2 Client ID	
연고	Service Accounts	No rows to display	PINION
	Workload Identity Federation		
۹	Labels		
	Tags		
۰	Settings		
ø	Manage Resources		
Ē	Release Notes		
<1			

4. On the service account details window.

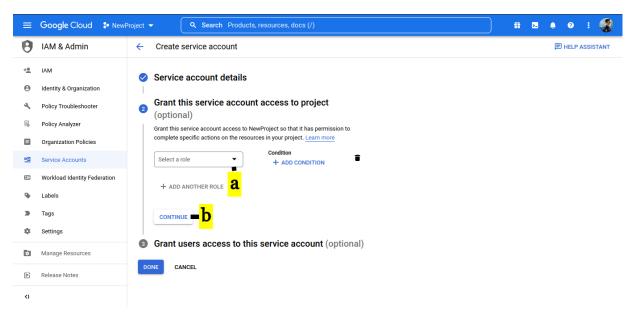
A. Provide Service account name

B. Click CREATE AND CONTINUE

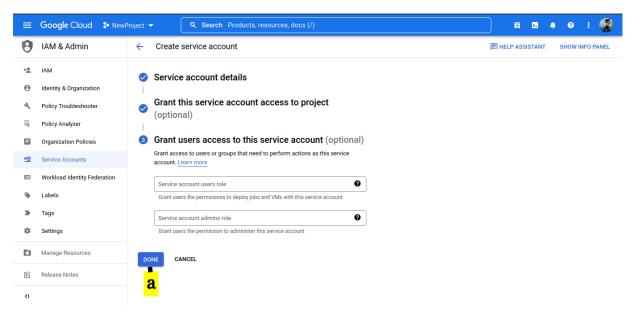


- 5. Grant this service account access to project.
 - a. Leave this empty

b. Click CONTINUE



- 6. Grant users access to this service account (optional)
 - a. Click DONE



7. On service account window.

- A. Click on Action button denoted by three dots
- **B. Select Manage Keys**

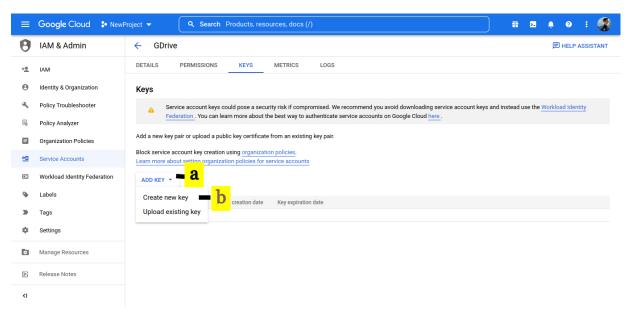
COPY. Copy the email id (This id should be copied at this stage as it will not be visible later. This id will be used for Assigning Permissions)

≡	Google Cloud	My First Project 🔻	Search (/) for resour	rces, docs, pro	ducts, and more			Q Search	b 1	0	: 🎲
θ	IAM & Admin	Service accou	nts + CREATE S	SERVICE ACCOUN	NT 👕 DELETE	* MANAGE ACCESS	C RE	FRESH			🗢 LEARN
+•	IAM	Service accou	nts for project "My F	irst Project"							
Θ	Identity & Organization	A service account re accounts.	presents a Google Cloud servic	e identity, such as	code running on Compute	Engine VMs, App Engine	apps, or syst	ems running outsid	e Google. <mark>Learn m</mark>	ore abou	it service
٩	Policy Troubleshooter		can be used to secure service about service account organiza		ck risky service account fe	atures, such as automatic	IAM Grants,	key creation/uploa	d, or the creation o	f service	accounts
R	Policy Analyzer	entirely. <u>Lean more</u>	about service account organize	ation policies. Es							
	Organization Policies	\Xi Filter Ente	r property name or value							0	ш
연	Service Accounts	Email		Status	Name 个	Description	Key ID	Key creation date			Actions
œ	Workload Identity Federat	post-	erviceaccount@green-	Senabled 🔮	GcsServiceAccount		No keys		110551968		∶– <mark>А</mark>
≔	Workforce Identity Federa		iam.gserviceaccount.com						Manage det Manage per		ins
•	Labels	Cop	<mark>y</mark>						Manage key		
	Tags								View metric	s	
\$	Settings								View logs		
Ø	Privacy & Security								Disable		
Ø	Manage Resources								Delete		
Ē	Release Notes										
<1											

8. Create a key

a. ADD KEY

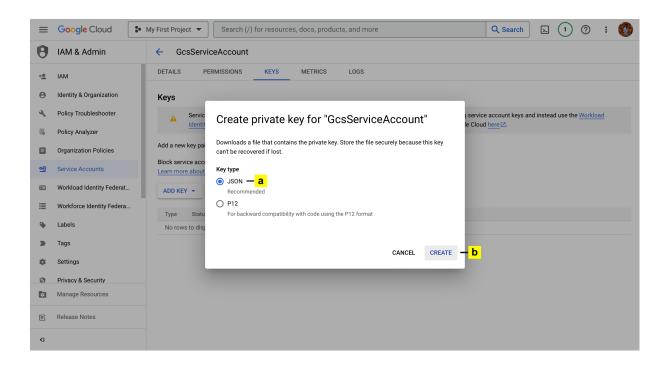
b. Create new key



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)



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.

₹	Google Cloud	* N	1y First Project 🔻 Search	(/) for resources, docs, products,	and more	Q Search	曲	D	?	:	T
A	Cloud overview Products & solutions	> >	IAM Identity & Organization Policy Troubleshooter	LE TO CREATE ROLE FROM SEL	ECTION	E HELP ASSISTAN	IT SI	How Info P	ANEL	⊜ ⊥	EARN
pinne RPI	APIs & Services	>	Policy Analyzer Organization Policies Service Accounts	at you can assign to principals. You c an existing role and adjust its permis							
	Billing		Workload Identity Federation	e or value	Used in	Status			0		
θ	IAM & Admin	>	Tags	cket	Custom	Enabled	:				
È	Marketplace		Settings	registry.createOnPushRepoAdmin	Artifact Registry	Enabled	:				
<u> </u>	Marketplace		Privacy & Security	registry.createOnPushWriter	Artifact Registry	Enabled	:				
۲	Compute Engine	>	Identity-Aware Proxy	oval Approver	Access Approval	Enabled	:				
Â	Kubernetes Engine	>	Roles - B	oval Config Editor	Access Approval	Enabled	:				
\sim	Raberneteo Engine	·		oval Invalidator	Access Approval	Enabled	:				
	Cloud Storage	>	Audit Logs	oval Viewer	Access Approval	Enabled	:				
()	BigQuery	>	Manage Resources	ext Manager Admin	Access Context Manager	Enabled	:				
\sim	bigguery	ŕ	Create a Project	ext Manager Editor	Access Context Manager	Enabled	:				
1	VPC network	>	Essential Contacts	ext Manager Reader	Access Context Manager	Enabled	:				
>>	Cloud Run		Asset Inventory	sparency Admin	Organization Policy	Enabled	:				
11			Quotas	in	Actions	Enabled	:				
\$	SQL		Groups	<u>er</u>	Actions	Enabled	:				
ns·//c	onsole cloud google com/jam	-admin/i	am?project=green-post-391902	jsis Viewer	Other	Enabled	:				

C. Click on Create Role

≡	Google Cloud	 My First Pro 	oject 🔻	Search (/) for resources, docs, products,	and more	Q Search	đ	>-	1	?	: (Ì
0	IAM & Admin	Roles		+ CREATE ROLE	ECTION	E HELP ASSISTA	NT	SHOW	INFO PA	NEL	🗢 LEA	ARN
÷ <u>•</u>	IAM	Roles	s for "N	C ly First Project" project								
Θ	Identity & Organization A role is a group of permissions that you can assign to principals. You can create a role											
عر	and add permissions to it, or copy an existing role and adjust its permissions. Learn Policy Troubleshooter more [2]											
II.	Policy Analyzer	ΞF	ilter Ente	er property name or value						0	III	
	Organization Policies		Туре	Title	Used in	Status						
헌	Service Accounts		₿	Access to Bucket	Custom	Enabled	:					
_			Θ	roles/artifactregistry.createOnPushRepoAdmin	Artifact Registry	Enabled	÷					
81	Workload Identity Federat		Ο	roles/artifactregistry.createOnPushWriter	Artifact Registry	Enabled	:					
۰	Labels		0	Access Approval Approver	Access Approval	Enabled	÷					
	Tags		Ο	Access Approval Config Editor	Access Approval	Enabled	:					
_	1490		Ο	Access Approval Invalidator	Access Approval	Enabled	:					
\$	Settings		0	Access Approval Viewer	Access Approval	Enabled	:					
0	Privacy & Security		0	Access Context Manager Admin	Access Context Manager	Enabled	:					
	Identity-Aware Proxy		0	Access Context Manager Editor	Access Context Manager	Enabled	:					
			0	Access Context Manager Reader	Access Context Manager	Enabled	i					
*	Manage Resources		o	Access Transparency Admin	Organization Policy	Enabled	:					
Ē	Release Notes		o	Actions Admin	Actions	Enabled	:					
_			O	Actions Viewer	Actions	Enabled	:					
<۱	onsole.cloud.google.com/iam-a			A stivity Apolysis Viewer	Other	Enabled	:					

Fill the Title and Create a Custom ID

D. Click on Add Permissions

≡	Google Cloud	Search (/) for resources, docs, products, and more	Q Search	毌		1 (?		T				
0	IAM & Admin	← Create Role				E ۲	IELP A	SSIST	ANT				
+0	IAM	Custom roles let you group permissions and assign them to principals in your project or											
Θ	Identity & Organization	organization. You can manually select permissions or import permissions from another role. Learn more											
٩	Policy Troubleshooter	Title * Custom Role											
110	Policy Analyzer	11 / 100 characters											
	Organization Policies	Created on: 2023-08-21											
연	Service Accounts	22 / 256 characters	22 / 256 characters										
82	Workload Identity Federat	D * CustomRole120											
۹	Labels	A Role launch stage											
	Tags	Alpha D ·											
\$	Settings	+ ADD PERMISSIONS											
0	Privacy & Security												
	Identity-Aware Proxy	No assigned permissions											
¢	Manage Resources	Filter Enter property name or value											
È	Release Notes	Permission ↑ Status											
< I		No rows to display								,			

E. Click on ADD

≡	Google Cloud	My First Project 🔻	Se	arch (/) for resources, docs,	products, and mo	pre	Q Search	击	>.	0	?	: (
θ	IAM & Admin	← Create R	ole							F	3 HELP	ASSISTAN	vт
÷ <u>e</u>	IAM	04010111101001	Add	permissions									
Θ	Identity & Organization	organization. Y role. <u>Learn mo</u>	Filter n	ermissions by role		•	1						
4	Policy Troubleshooter	Custom Role	- inter p	ermasions by role		·	J -						
	Policy Analyzer		ŦΡ	ilter object (8) Enter proper	ty name or value	× 0 III							
	Organization Policies	Description –		Permission 个	Status								
연필	Service Accounts	Created on. 2	~	storage.objects.create	Supported								
	Service Accounts			storage.objects.delete	Supported								
	Workload Identity Federat	_ ID *		storage.objects.get	Supported								
•	Labels	CustomRole		storage.objects.getlamPolicy	Supported								
	200010	C Role launch st	Image: A start of the start	storage.objects.list	Supported								
	Tags	Alpha		storage.objects.setlamPolicy	Supported								
\$	Settings	+ ADD PE	~	storage.objects.update	Supported								
0	Privacy & Security	T ADD PE				11 - 17 of 17 🗶 📏							
	Identity-Aware Proxy	No assigr				E.							
6	Manage Resources	= Filter											
Ē	Release Notes	Pertuss		Status									
<1		No rows to disp		one might be appreciated with and	obacked by third or	retion							

F. Click on CREATE

≡	Google Cloud	🗣 My First Project 🔻	Search (/) f	or resources, docs, pro	ducts, and mor	e
0	IAM & Admin	← Create F	Role			
+•	IAM	Alpha				•
Θ	Identity & Organization	+ ADD PERM	ISSIONS			
٩	Policy Troubleshooter	6 assigned	permissions			
Ę	Policy Analyzer		er property name or		Ø	
	Organization Policies		sion 个	Status	U	
어린	Service Accounts	🔽 storage	e.buckets.get	Supported		
	Workload Identity Federat	Storage	e.objects.create	Supported		
≡	Workforce Identity Federa		e.objects.delete e.objects.get	Supported Supported		
•	Labels	_	e.objects.list	Supported		
	Tags	storage	e.objects.update	Supported		
•	Settings Manage Resources	These	permissions contai	be associated with and ch in the third party's service a		
Ē	Release Notes	the pe	rmission prefix.			
<۱		F - CREATE C	ANCEL			

- 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**

≡	Google Cloud	 My First Project ▼ Search (/) for resources, docs, products, and more Q. Search ① ② : 	
	Cloud Storage	← Bucket details C REFRESH ■ HELP ASSISTANT SLEAF	N
•	Buckets	secondtestingcopy24051998	
ш	Monitoring	Location Storage class Public access Protection	
•	Settings	us (multiple regions in United States) Standard Not public None	
		OBJECTS CONFIGURATION PERMISSIONS PROTECTION LIFECYCLE OBSERVABILITY INVENTORY REPORTS	_
		Public access Access control Not public Uniform: No object-level ACLs enabled 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 (2) 90 days left to change this setting Principals restricted from bucket access: allUsers, allAuthenticatedUsers 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 (2) REMOVE PUBLIC ACCESS PREVENTION SWITCH TO FINE-GRAINED	
) <u>.</u>	Marketplace	Permissions	
Ē	Release Notes	VIEW BY B NCIPALS VIEW BY ROLES	
<1		+ GRANT ACCESS - REMOVE ACCESS	

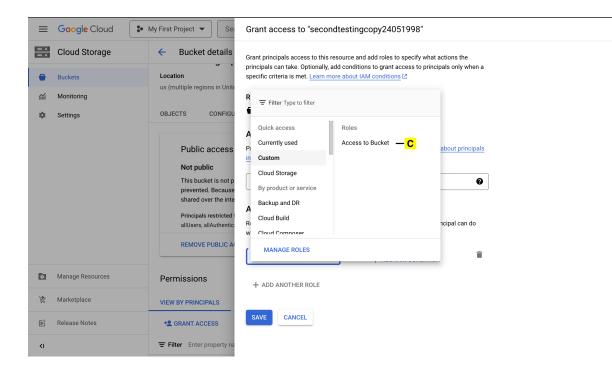
14. Add Principal

A. Paste the Service Account Email copied in STEP 7

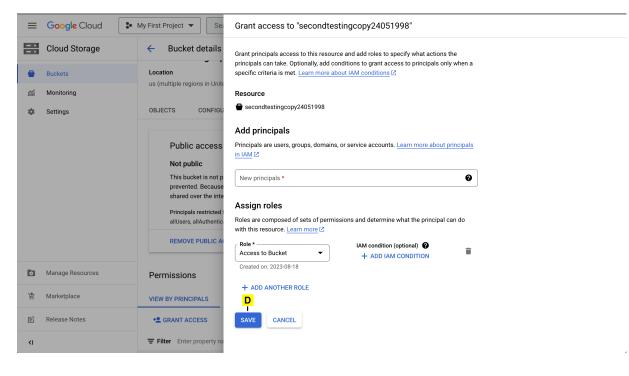
B. Choose the Custom IAM Role created in STEP 10

≡	Google Cloud *	My First Project 🔻 Sea	Grant access to "secondtestingcopy24051998"
	Cloud Storage	← Bucket details	Grant principals access to this resource and add roles to specify what actions the
•	Buckets	Location us (multiple regions in Unite	principals can take. Optionally, add conditions to grant access to principals only when a specific criteria is met. Learn more about IAM conditions [2]
	Monitoring	de (maniple regione in emit	Resource
ф	Settings	OBJECTS CONFIGU	escondtestingcopy24051998
		_	Add principals
		Public access	Principals are users, groups, domains, or service accounts. Learn more about principals in IAM [2]
		Not public	
		This bucket is not p	New principals *
		prevented. Because shared over the inte	
		Principals restricted	Assign roles
		allUsers, allAuthentic	Roles are composed of sets of permissions and determine what the principal can do with this resource. Learn more [2]
		REMOVE PUBLIC A	IAM condition (optional)
			Select a role * + ADD IAM CONDITION
	Manage Resources	Permissions	+ ADD ANOTHER ROLE
)\$	Marketplace	VIEW BY PRINCIPALS	
Ē	Release Notes	* GRANT ACCESS	SAVE CANCEL
<1		\Xi Filter Enter property na	

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



D. Click on SAVE



The principal will be added and will be listed below.

≡	Google Cloud	My First Project	▼ Search (/) for resources, docs, proc	lucts, and mor	e	Q Search	Ť	D	?	: (Ċ
- 1	Cloud Storage	← Buck	et details				C REFRESH			🗢 LEA	۱RN
	Buckets	REMO	VE PUBLIC ACCESS PREVENTION	LIC ACCESS PREVENTION		NE-GRAINED					
ണ് ന	Monitoring Settings	Permissic	ns								
		VIEW BY PRINCIPALS VIEW BY ROLES ** GRANT ACCESS -* REMOVE ACCESS = Filter Enter property name or value III									
		🔲 Туре	Principal 个	Name	R	ble		Inheritance	e		
		[] 연	bucketlevelaccess@green-post- 391902.iam.gserviceaccount.com	BucketLe	evelAccess A	ccess to Bucket				ľ	
			Editors of project: green-post-391902		SI	orage Legacy Bucke	t Owner			1	
					SI	orage Legacy Object	Owner				
			Owners of project: green-post-391902		SI	orage Legacy Bucket	t Owner			1	
¢	Manage Resources				SI	orage Legacy Object	Owner				
*	Marketplace	[] 역	testingbucketlevelaccess@green-post- 391902.iam.gserviceaccount.com	testingbu	ucketlevelaccess A	ccess to Bucket		🐓 My Fir	rst Project		
			Viewers of project: green-post-391902		SI	orage Legacy Bucket	t Reader			1	
Ē	Release Notes				SI	orage Legacy Object	Reader				
<1											