# 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/)

≡ Google Cloud 🗈 baya.in 👻	<b>Q</b> Search Products, resources, docs (/)		ii 🗅 🌲	0 : 🔇
• 🙆 Welcome	۰	•	•	,
You're working in baya.in <u>Dashboard</u> <u>Recommendations</u>		•	•	
Create a VM Run a Quick access	query in BigQuery	ter 🖬 Create a storage bucket		
RPI APIs & Services	C IAM & Admin	G Billing	() Compute Engine	
	Privacy Polic	cy · Terms of Service		

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

Ŧ	Google Cloud	🖽 baya.in 🕚	- Q Search	Products, resources, docs (/)			) 👬 尾 I	• • : 🔇
a	Cloud overview	>	IAM	N				
	View all products		Policy Troubleshooter					
PINN	ED		Policy Analyzer Organization Policies					
API	APIs & Services	>	Service Accounts	<mark>−c</mark>				
-	Billing		Workload Identity Federation					
θ	IAM & Admin	>	Labels Tags					
$\sum_{i=1}^{n}$	Marketplace	b	Settings	Create a GKE cluster	Create a storage bucket			
۲	Compute Engine	~	Privacy & Security					
٢	Kubernetes Engine	>	Roles					
	Cloud Storage	>	Audit Logs					
<u>(</u>	BigQuery	>	Manage Resources Create a Project	M & Admin	<ul> <li>Billing</li> </ul>	🗊 Comp	oute Engine	
11	VPC network	>	Asset Inventory					
)>	Cloud Run		Essential Contacts	Privacy Policy -	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 (/)			>.	۰	?						
New Project	New Project											
Project name * NewProject Project ID: newproject-363011. It cannot be chang	ed later. EDIT											
Organization * Contraction to attach it to a project. This selection can't be changed later.												
Location * baya.in Parent organization or folder	BROWSE - C.											
CREATE CANCEL												

### 3. Create a service account

a. Click CREATE SERVICE ACCOUNT.

=	Google Cloud Se New	Project 🗸 🔍 Q. Search Products, resources, docs (/)
θ	IAM & Admin	Service accounts + CREATE SERVICE ACCOUNT 🖀 DELETE 🔩 MANAGE ACCESS C REFRESH 🖻 HELP ASSISTANT S 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 running 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 creation/upload, or the creation of service accounts entirely. Learn more about service account organization policies.
	Policy Analyzer	
	Organization Policies	Filter     Enter property name or value     III       Fmail     Status     Name 1     Description       Key ID     Key (D)     Key creation date     OAuth 2 Client ID       Actions
연	Service Accounts	No rows to display
	Workload Identity Federation	
	Labels	
	Tags	
٠	Settings	
¢	Manage Resources	
È	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 resources	s, docs, produ	ucts, and more			Q Search	» (1	?	: 🎲
θ	IAM & Admin	Service acco	unts -	+ CREATE SER	VICE ACCOUNT	T 🝵 DELETE	* MANAGE ACCESS	C RE	EFRESH			🗢 LEARN
+•	IAM	Service acco	unts for proje	ect "My Firs	t Project"							
Θ	Identity & Organization	A service account account	represents a Google	e Cloud service id	entity, such as c	ode running on Compute	e Engine VMs, App Engine	apps, or sys	tems running outsi	de Google. <mark>Learn</mark>	more abo	ut service
٩	Policy Troubleshooter	Organization polici	es can be used to s	ecure service acc	counts and block	risky service account fe	eatures, such as automatic	c IAM Grants	s, key creation/uploa	ad, or the creation	of service	e accounts
R	Policy Analyzer			ount organization	ponoico.							
	Organization Policies	\Xi Filter En	ter property name	or value							0	III
연	Service Accounts	Email		:	Status	Name 个	Description	Key ID	Key creation date	e OAuth 2 C	lient ID	Actions
	Workload Identity Federat	□ <u>e</u> gc post-	sserviceaccount@	)green-	Senabled 🔮	GcsServiceAccount		No keys		11055196	883309	∃– <mark>A</mark>
≔	Workforce Identity Federa	39190	2.iam.gserviceacc	count.com						Manage d	etaiis ermissio	ons
۰	Labels	Co	<mark>ру</mark>							Manage k	eys —	B
	Tags									View metr	ics	
•	Settings									View logs		
a	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	:• 1	My First Project 🔻 Sea	arch (/) for resources, docs, products	, and more	Q Search	<del>1</del> D	1	?	: (	
A III	Cloud overview Products & solutions	> >	IAM Identity & Organization Policy Troubleshooter	.e ि CREATE ROLE FROM SEL	ECTION	E HELP ASSISTAN	t show	INFO PAI	NEL	S LEA	<b>RN</b>
pinni <b>Api</b>	ED APIs & Services	>	Organization Policies Service Accounts Workload Identity Federation	at you can assign to principals. You an existing role and adjust its permis	can create a role ssions. <u>Learn</u>				0		
	Billing		Labels		Used in	Status					
Θ	IAM & Admin	>	Tags	<u>cket</u>	Custom	Enabled	:				
<u>ب</u>	Marketplace		Settings	registry.createOnPushRepoAdmin	Artifact Registry	Enabled	÷				
0.0	manophaco		Privacy & Security	registry.createOnPushWriter	Artifact Registry	Enabled	:				
۲	Compute Engine	>	Identity-Aware Proxy	oval Approver	Access Approval	Enabled	:				
俞	Kubernetes Engine	>	Bolos - B	oval Config Editor	Access Approval	Enabled	:				
$\sim$		-	Noies — B	oval Invalidator	Access Approval	Enabled	:				
	Cloud Storage	>	Audit Logs	oval Viewer	Access Approval	Enabled	:				
(1)	BigQuery	>	Manage Resources	ext Manager Admin	Access Context Manager	Enabled	:				
~	Digquery	,	Create a Project	ext Manager Editor	Access Context Manager	Enabled	:				
	VPC network	>	Essential Contacts	ext Manager Reader	Access Context Manager	Enabled	:				
11	Cloud Run		Asset Inventory	parency Admin	Organization Policy	Enabled	:				
11	oloud Kull		Quotas	<u>in</u>	Actions	Enabled	:				
\$	SQL		Groups	er	Actions	Enabled	:				
https://c	onsole.cloud.google.com/iam	-admin,	/iam?project=green-post-39190	2 sis Viewer	Other	Enabled	:				

### C. Click on Create Role

≡	Google Cloud	<ul> <li>My First Project </li> </ul>	Search (/) for resources, docs, products	s, and more	Q Search	1 🛛 🚺	: 👘
θ	IAM & Admin	Roles	+ CREATE ROLE	LECTION	E HELP ASSISTANT	SHOW INFO PANEL	IEARN
+ <u>e</u>	IAM	Roles for "	C My First Project" project				
Θ	Identity & Organization	A role is a group	of permissions that you can assign to principals. You	can create a role			
٩	Policy Troubleshooter	and add permiss <u>more</u> [2	ions to it, or copy an existing role and adjust its perm	issions. <u>Learn</u>			
B	Policy Analyzer	〒 Filter Er	ter property name or value			0	ш
	Organization Policies	П Туре	Title	Used in	Status		
에	Service Accounts		Access to Bucket	Custom	Enabled	i	
_			roles/artifactregistry.createOnPushRepoAdmin	Artifact Registry	Enabled	i .	
82	Workload Identity Federat		roles/artifactregistry.createOnPushWriter	Artifact Registry	Enabled	i	
•	Labels		Access Approval Approver	Access Approval	Enabled	i	
	Tags		Access Approval Config Editor	Access Approval	Enabled	l .	
_	lago		Access Approval Invalidator	Access Approval	Enabled		
\$	Settings		Access Approval Viewer	Access Approval	Enabled	i i i i i i i i i i i i i i i i i i i	
Ø	Privacy & Security		Access Context Manager Admin	Access Context Manager	Enabled	l	
	Identific Access Descus		Access Context Manager Editor	Access Context Manager	Enabled	i .	
	Identity-Aware Proxy		Access Context Manager Reader	Access Context Manager	Enabled	l .	
\$	Manage Resources		Access Transparency Admin	Organization Policy	Enabled	ł	
Ē	Release Notes		Actions Admin	Actions	Enabled	1	
			Actions Viewer	Actions	Enabled	í .	
<i https://c</i 	onsole.cloud.google.com/iam-ad	min/analyzer?project=gr	een-post-391902	Other	Enabled	i	

# 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							
82	Workload Identity Federat	ID *							
۹	Labels	Role launch stane							
	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 <b>↑</b> Status							
<b>&lt;</b> I		No rows to display							,

E. Click on ADD

≡	Google Cloud	My First Project 🔻	Sea	arch (/) for resources,	docs, products	, and more			Q Search	毌	>-	0	?	**	
θ	IAM & Admin	← Create R	ole						-			E	) HELP A	ASSIST	TANT
••	IAM	Custom roles I	Add	permissions											
Θ	Identity & Organization	organization. Y role. <u>Learn mo</u>	<b>F</b> :1												
٩	Policy Troubleshooter	Title *	Custom Role												
R	Policy Analyzer	Custom Role	ŦF	lter object 😮 Enter	r property name o	r value	× 0	ш							
	Organization Policies	Description -		Permission 个	Status	:									
<b>~</b> ]	Service Accounts	Created on: 2		storage.objects.create	Suppo	orted									
	Service Accounts			storage.objects.delete	Suppo	orted									
	Workload Identity Federat	( ID *		storage.objects.get	Suppo	orted									
•	Labels	CustomRole		storage.objects.getlam	Policy Suppo	orted									
· ·		C Role launch st	✓	storage.objects.list	Suppo	orted									
	Tags	Alpha		storage.objects.setlaml	Policy Suppo	orted									
-	Settings		<b>~</b>	storage.objects.update	e Suppo	orted									
Ø	Privacy & Security	TADDPE					11 – 17 of 17	< >							
H	Identity-Aware Proxy	No assigr						E.							
	Manage Resources	= Filter					CANCEL	ADD							
Ē	Release Notes	No rows to displ	av .l.	Status											
<1		Come			uith and sheeled l	hu shind nonsi									

# F. Click on CREATE

≡	Google Cloud	ly First Project 🔻 Search (/) for resources, do	ocs, products, and more	Q Search	Q Search	Q Search (13) (?)	Q Search > (13) (?)	Q Search (13) ? :	Q Search > (13) (? :	Q Search (13) ? :	Q Search 📐 (13) 🕐 👯 🃢	Q Search 📐 13 🤊 👯 🌍
0	IAM & Admin	← Create Role										
+•	IAM	Alpha	•									
Θ	Identity & Organization	+ ADD PERMISSIONS										
۹,	Policy Troubleshooter	6 assigned permissions										
	Policy Analyzer	= Filter Enter property name or value	0 III									
	Organization Policies	Permission ↑ Status										
	Service Accounts	storage.buckets.get Supported										
æ	Workload Identity Federat	storage.objects.create Supported										
		storage.objects.delete Supported										
=	workforce identity Federa	storage.objects.get Supported										
۹	Labels	<ul> <li>storage.objects.list</li> <li>Supported</li> </ul>										
	Tags	storage.objects.update Supported										
	Sattinge	Some permissions might be associated with	h and checked by third parties.									
۵	Manage Resources	These permissions contain the third party's the permission prefix.	service and domain name in									
Ē	Release Notes											
<۱	F	CREATE CANCEL										

- 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	<ul> <li>My First Project ▼</li> <li>Search (/) for resources, docs, products, and more</li> <li>Q. Search</li> <li>① ② :</li> </ul>	
	Cloud Storage	← Bucket details C REFRESH ■ HELP ASSISTANT \$LEAF	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)       Odays left to change this setting         Principals restricted from bucket access: all/Users, all/Uhenticated/Users       All 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 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	principals can take. Optionally, aud conditions to grant access to principals only when a specific criteria is met. Learn more about IAM conditions [2]
<b></b>	Monitoring	us (multiple regions in oniti	Resource
ф	Settings	OBJECTS CONFIGU	econdtestingcopy24051998
			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
		REMOVE PUBLIC A	with this resource. Learn more 2
			Select a role *   Select a role *  ADD IAM CONDITION
¢	Manage Resources	Permissions	+ ADD ANOTHER ROLE
*	Marketplace	VIEW BY PRINCIPALS	
Ē	Release Notes	* GRANT ACCESS	SAVE CANCEL
<1		= 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 Fir	st Project	•	Search (/) for resources, docs, products, and more			(	<b>२</b> Search	毌	>-	1	?	:	1
- •	Cloud Storage		÷	Buck	et de	etails				н 🏾	HELP	ASSISTA	ANT	S LE	ARN	
•	Buckets			REMO	VE PU	BLIC ACCESS PREVENTION										
<b>M</b>	Monitoring		_					Switchite	FINE-OR							
\$	Settings		Permissions													
		VIEW BY PRINCIPALS VIEW BY ROLES														
			+ GRANT ACCESS REMOVE ACCESS													
			Filter Enter property name or value											0		
				Туре	Prin	cipal 🛧	Name		Role			Inf	neritance			
				<u>에</u>	buc 391	ketlevelaccess@green-post- 902.iam.gserviceaccount.com	BucketL	evelAccess	Access	to Bucket					ľ	
					Edit	ors of project: green-post-391902			Storage	Legacy Bucke	et Owner				ľ	
									Storage	Legacy Objec	t Owner					
				**	Ow	ners of project: green-post-391902			Storage	Legacy Bucke	et Owner				ľ	_
۵	Manage Resources								Storage Legacy Object Owner							
*	Marketplace			<del>ک</del> ا	tes1 391	ingbucketlevelaccess@green-post- 902.iam.gserviceaccount.com	testingb	ucketlevelaccess	Access	to Bucket			My Firs	t Projec		
					Vie	wers of project: green-post-391902			Storage	Legacy Bucke	et Reader				ï	
Ē	🖹 Release Notes								Storage	Legacy Objec	t Reader					
<1																