How to solve Error creating Service: googleapi: Error 403: Permission 'iam.serviceaccounts.actAs' denied on service account

Ask Question

Asked 1 year, 5 months ago Modified 9 months ago Viewed 5k times Part of Google Cloud Collective

4

I've been trying to create a public cloud run invoker policy and bind that to my cb_app cloud run service so that it can be exposed. I've created a custom service and assigned it cloud admin role. But getting this error

```
Error: Error creating Service: googleapi: Error 403: Permission 'iam.serviceaccounts.actAs' denied on service account app-worker@samuel-django-project.iam.gserviceaccount.com (or it may not exist).
```

Here are the configs

```
resource "google_cloud_run_service_iam_member" "domain" {
  service = google_cloud_run_service.cb_app.name
  location = google_cloud_run_service.cb_app.location
  role = "roles/run.admin"
  member = "serviceAccount:${var.service_account}"
}
#create service account to run service
resource "google_service_account" "cb_app" {
    account_id    = "app-worker"
    display_name  = "app worker"
}
```

And in app service, I have this

```
spec {
      # Use locked down Service Account
      service_account_name = google_service_account.cb_app.email
```

Any ideas on how to solve this?

terraform google-cloud-run service-accounts terraform-provider-gcp google-iam

Share Follow

asked Jul 29, 2021 at 16:38
Shammir
825 ● 3 ● 16 ● 30

What is the content of ${var.service_account}? – CaioT Jul 29, 2021 at 17:31

Add a comment

3 Answers

Sorted by: Highest score (default)

2

When you create a resoure such as Cloud Run, you have the option to attach a service account to the resource.

The following error means that the identity (user or service account) that Terraform is using does not have permission to attach the service account to the resource.

> Error: Error creating Service: googleapi: Error 403: Permission 'iam.serviceaccounts.actAs' denied on service account app-worker@samuel-django-project.iam.gserviceaccount.com (or it may not exist).

The solution is to add the role **roles/iam.serviceAccountUser** to the identity that Terraform is running under. You do not specify the identity in your question. The identity could be a user account or a service account. Go to the Google Cloud Console -> IAM. Find the identity and add the role.

You can also use the CLI **gcloud**. The exact command arguments depend on the identity type.

For a user account:

```
gcloud projects add-iam-policy-binding PROJECT_ID \
--member='user:someone@gmail.com' \
--role='roles/iam.serviceAccountUser'
```

For a service account:

```
gcloud projects add-iam-policy-binding PROJECT_ID \
--member='serviceAccount:myserviceaccount@PROJECT_ID.iam.gserviceaccount.com' \
--role='roles/iam.serviceAccountUser'
```

Share Follow

answered Jul 30, 2021 at 6:41

John Hanley
69.5k ● 6 ● 75 ● 137

Add a comment

0

Possible solution to this issue if you're encountering it while **applying Terraform in Google Cloud Shell**.

I also encountered a very similar error:

```
Error: googleapi: Error 403: Missing necessary permission enter code hereiam.serviceA
on the service account mr-service-account-sa@mr-project.iam.gserviceaccount.com.
Grant the role 'roles/iam.serviceAccountUser' to $MEMBER on the service
account mr-service-account-sa@mr-project.iam.gserviceaccount.com.
You can do that by running 'gcloud iam service-accounts
add-iam-policy-binding mr-service-account-sa@mr-project.iam.gserviceaccount.com --mem
--role=roles/iam.serviceAccountUser'.
In case the member is a service account please use the prefix 'serviceAccount:' inste
```

I think this error message is deceptive/misleading.

My solution:

- **was not** to give the "Service Account User" role to mr-service-account-sa@mr-project.iam.gserviceaccount.com
- **was not** to give the "Service Account User" role to the Terrform deployment service account.
- **was** to give the "Service Account User" role to my own personal GCP account.

It seems like Cloud Shell uses a mixture of authorisation accounts when applying Terraform. In some cases it uses the service account defined in the provider and at other times it uses your own GCP OAuth account.

Share Follow

edited Nov 19, 2021 at 10:18

answered Nov 19, 2021 at 10:06

FreeZey
2,223 ● 3 ● 11 ● 22

Add a comment

0

I ran this code:

```
gcloud config set auth/impersonate_service_account [SA_FULL_EMAIL]
```

and it worked for me.

Share Follow

edited Apr 15, 2022 at 20:02

Ethan
852 ● 7 ● 18 ● 31

answered Apr 14, 2022 at 11:12

Nawfal Osman
1 ● 1

Add a comment

Your Answer

Sign up or log in

Sign up using Google

Sign up using Facebook

Sign up using Email and Password

Post as a guest

Name

Email

Required, but never shown

Post Your Answer *By clicking "Post Your Answer", you agree to our terms of service, privacy policy and cookie policy*

Not the answer you're looking for? Browse other questions tagged terraform google-cloud-run service-accounts terraform-provider-gcp google-iam or ask your own question.

raggedleft does not work for last column in Table
Find the first run of numbers summing to n
Identify this part: two 2x2 plates connected by a strip
Would a summer camp responsible for caring for a child have any alternative other than refunding money if child intentionally misbehaves?
Do authors prefer to see reviewer reports before a decision?
Do Bracers of Archery make weapon attacks magical for overcoming resistance to non-magical attacks?
How is the US "six month club" list determined?
I want to write a LaTeX document in Yiddish
3.6 V Zener diodes clamping at 2.3 V
How do I justify a world where drones are commonplace but computers remain large?
Optimizing Python BFS Code
Conjecture: If circular coins of any sizes are in a convex polygonal frame, with each coin touching exactly one edge, then all the coins can move
Is there any particular advice on crank-bolt lubrication I should know?
Question feed