GCE Service Account with Compute Instance Admin permissions

Asked 4 years, 7 months ago Modified 1 year, 2 months ago Viewed 8k times

Part of Google Cloud Collective

7

I have setup a compute instance called to run cronjobs on Google Compute engine using a service account with the following roles:

```
Custom Compute Image User + Deletion rights
Compute Admin
Compute Instance Admin (beta)
Kubernetes Engine Developer
Logs Writer
Logs Viewer
Pub/Sub Editor
Source Repository Reader
Storage Admin
```

Unfortunately, when I ssh into this cronjob runner instance and then run:

```
sudo gcloud compute --project  {REDACTED} instances create e-latest \
    --zone {REDACTED} --machine-type n1-highmem-8 --subnet default \
    --maintenance-policy TERMINATE  \
    --scopes  https://www.googleapis.com/auth/cloud-platform \
    --boot-disk-size 200  \
    --boot-disk-type pd-standard --boot-disk-device-name e-latest \
    --image {REDACTED} --image-project {REDACTED} \
    --service-account NAME_OF_SERVICE_ACCOUNT \
    --accelerator type=nvidia-tesla-p100,count=1 --min-cpu-platform Automatic
```

I get the following error:

> The user does not have access to service account {NAME_OF_SERVICE_ACCOUNT}. User: {NAME_OF_SERVICE_ACCOUNT} . Ask a project owner to grant you the iam.serviceAccountUser role on the service account.

Is there some other privilege besides compute instance admin that I need to be able to create instances with my instance?

Further notes: (1) when I try to not specify `--service-account` the error is the same except that the service account my user doesn't have access to is the default '51958873628-compute@developer.gserviceaccount.com'. (2) adding/removing sudo doesn't change anything

google-compute-engine google-iam

Sam Shleifer
1,596 2 15 26

3 Answers

Sorted by:

Highest score (default)

5

Creating an instance that uses a service account requires you have the compute.instances.setServiceAccount permission on that service account. To make this work, grant the iam.serviceAccountUser role to your service account (either on the entire project or on the specific service account you want to be able to create instances with).

Share Follow

answered Jun 6, 2018 at 20:18

David
9,127 1 20 52

4

Find out who you are first

- if you are using Web UI: what **email** address did you use to login?
- if you are using local `gcloud` or `terraform`: find the json file that contains your credentials for gcloud (often named similarly to `myproject*.json`) and see if it contains the **email**: `grep client_email myproject*.json`

GCP IAM change

1. Go to https://console.cloud.google.com
2. Go to IAM
3. Find your **email** address
4. Member -> Edit -> Add Another Role -> type in the role name `Service Account User` -> Add

(You can narrow it down with a Condition, but lets keep it simple for a while).

Share Follow

edited Nov 4, 2021 at 15:42

answered Jul 21, 2020 at 20:29

kubanczyk
4,721 1 37 52

0

Make sure that NAME_OF_SERVICE_ACCOUNT is service account from current project.

If you change project ID, and don't change NAME_OF_SERVICE_ACCOUNT, then you will encounter this error.

This can be checked on Google Console -> IAM & Admin -> IAM. Then look for service name

Share Follow

answered Aug 8, 2020 at 6:04

Karol Zlot

2,079 1 17 33