serverfault

Service account does not have storage.buckets.get access to bucket

Asked 3 years, 10 months ago Modified 1 year, 8 months ago Viewed 36k times

11

I'm trying to get a list of buckets in a project, using python like this:

```
from google.cloud import storage

storage_client = storage.Client(project='[project-id]')
bucket = storage_client.get_bucket([bucket-name])

blobs = bucket.list_blobs()

for blob in blobs:
    print(blob.name)
```

But i get an error:

```
[service-account-ID]-compute@developer.gserviceaccount.com does not have
storage.buckets.get access to [bucket-name]
```

Anyways if i try using gsutil (using the same service account):

```
gsutil ls gs://[bucket-name]
```

I can get the list of objects in the bucket... So i dont understand what is happening, any clue about what should i do?

google-cloud-platform google-cloud-storage oauth

Share Improve this question Follow

asked Mar 18, 2019 at 14:18

Dimitri

211 1 2 4

2 Answers

Sorted by:

Highest score (default)

18

GCP has the concept of *roles* and *permissions*. A *role* is something like Storage Admin (`roles/storage.admin`) and a *permission* is something like `storage.buckets.get` . Roles are made up of one or more permissions. Permissions are always granted by applying a role to a principal (user, service account, or group) -- that is, you cannot assign a permission directly to a principal.

The error you're seeing is because the permission `storage.buckets.get` is missing from the service account -- that is, none of the role(s) applied to the service account grant the storage.buckets.get permission. You can list the objects of a bucket (storage.objects.list permission) without the ability to list buckets (storage.buckets.get permission).

Therefore you need to assign a role such as `roles/storage.admin` that has the storage.buckets.get permission. You can also create a Custom Role with just that permission if you want to operate with a least-privilege model.

Share Improve this answer Follow

answered Mar 19, 2020 at 23:52
Garrett
1,282 10 16

1 Thank you @Garrett , this is the best description of roles and permissions I ever read on SO/SE. This is probably the worst understood part of working with GCP. I used to verify all changes by terraform via UI of GCP. What I discovered is that indeed - first better to understand the concepts, then try to buld up something complex from simple things. Simplicity is The King) – boldnik Oct 1, 2020 at 15:38

1 @boldnik: If you think it's a great answer, how about accepting it? :) – random_forest_fanatic Feb 18, 2021 at 20:02

I had to add the service account to the project in order to convey the permissions. – Stevko Dec 20, 2021 at 23:23

1 @Stevko -- Service accounts are objects that always exist within a single project and a service account can never be "added" to another project except by way of granting it a *role* (and thereby granting it specific *permissions*)in that project. When you say you "add[ed] the service account to the project in order to convey the permissions" I assume you mean you gave the service account in project A a role in project B – Garrett Dec 22, 2021 at 0:09

7

To add to the top answer, note that the role roles/storage.legacyBucketReader has the storage.buckets.get permission too. (See https://cloud.google.com/iam/docs/permissions-reference)

So to add that service account to that role:

```
gsutil iam ch serviceAccount:john.doe@example.com:legacyBucketReader gs://ex-bucket
```

Share Improve this answer Follow

edited May 18, 2021 at 11:42
Andrew Schulman
8,651 21 31 47

answered May 17, 2021 at 7:32
JohnFlux
71 1 1