Failed to obtain the location of the Google Cloud Storage bucket

Asked 4 years, 2 months ago   Modified 10 months ago   Viewed 5k times   ⚙ Part of Google Cloud Collective

▲

7

▼

🔖

↺

I am trying to transfer data from S3 to GCS by using a Java client but I got this error.

> Failed to obtain the location of the Google Cloud Storage (GCS) bucket ___ due to insufficient permissions. Please verify that the necessary permissions have been granted.

I am using a service account with the Project Owner role, which should grant unlimited access to all project resources.

google-cloud-storage   data-transfer

Share Improve this question

Follow

edited Oct 27, 2018 at 10:24
Son Truong
13.2k 5 29 55

asked Oct 27, 2018 at 9:23
Dmytro Kulaiev
Dmyt **251** 2 6

3 Answers

Sorted by:

Highest score (default) ⇕

▲

18

▼

🔖

✔

↺

Google Transfer Service is using an internal service account to move the data back and forth. This account is created automatically and should not be confused with the service accounts you create yourself.

You need to give this user a permission called "Legacy bucket writer".

This is written in the documentation, but it's VERY easy to miss:

https://cloud.google.com/storage-transfer/docs/configure-access

Share Improve this answer Follow

answered Oct 27, 2018 at 13:17
Dmytro Kulaiev
Dmyt **251** 2 6

Great to see you found the solution! You can accept your own answers after 48 hours of being posted – Federico Panunzio Oct 30, 2018 at 10:48

1   Also, these roles should be added on the specific source and target buckets only, not on the project level. This is what the Data Transfer service itself does, when configured manually via the GUI. – thnee May 11, 2020 at 18:53 ✎

Join Stack Overflow to find the best answer to your technical question, help others answer theirs.

Sign up   ✕

1 can use this API [cloud.google.com/storage-transfer/docs/reference/rest/v1/...](#) to get the service account
   email being used by Data transfer service. – [JD-V](#) Oct 23, 2020 at 11:59

Thanks to @thnee's comment I was able to piece together a terraform script that adds the permissions to the hidden Storage Transfer service account:

0

```
data "google_project" "project" {}

locals {
  // the project number is also available from the Project Info section on the
  Dashboard
  transfer_service_id = "project-${data.google_project.project.number}@storage-
  transfer-service.iam.gserviceaccount.com"
}

resource "google_storage_bucket" "backups" {
  location      = "us-west1"
  name          = "backups"
  storage_class = "REGIONAL"
}

data "google_iam_policy" "transfer_job" {
  binding {
    role = "roles/storage.legacyBucketReader"

    members = [
      "serviceAccount:${local.transfer_service_id}",
    ]
  }

  binding {
    role = "roles/storage.objectAdmin"

    members = [
      "serviceAccount:${local.transfer_service_id}",
    ]
  }

  binding {
    role = "roles/storage.admin"

    members = [
      "user:<GCP console user>",
      "serviceAccount:<terraform user doing updates>"
```

Note that this removes [the default acls](#) of `OWNER` and `READER` present on the bucket. This would prevent you from being able to access the bucket in the console. We therefore add the `roles/storage.admin` back to owner users and the terraform service account that's doing the change.

Share Improve this answer Follow

answered Sep 28, 2020 at 14:21

[Richard Nienaber](#)
10.1k 5   56   66

Join Stack Overflow to find the best answer to your technical question, help others answer theirs.

Sign up   ✕

0   Share   Improve this answer   Follow

answered Mar 6, 2022 at 1:47

Kyle Pennell
5,557   4   50   73

Join Stack Overflow to find the best answer to your technical question, help others answer theirs.

Sign up   ✕