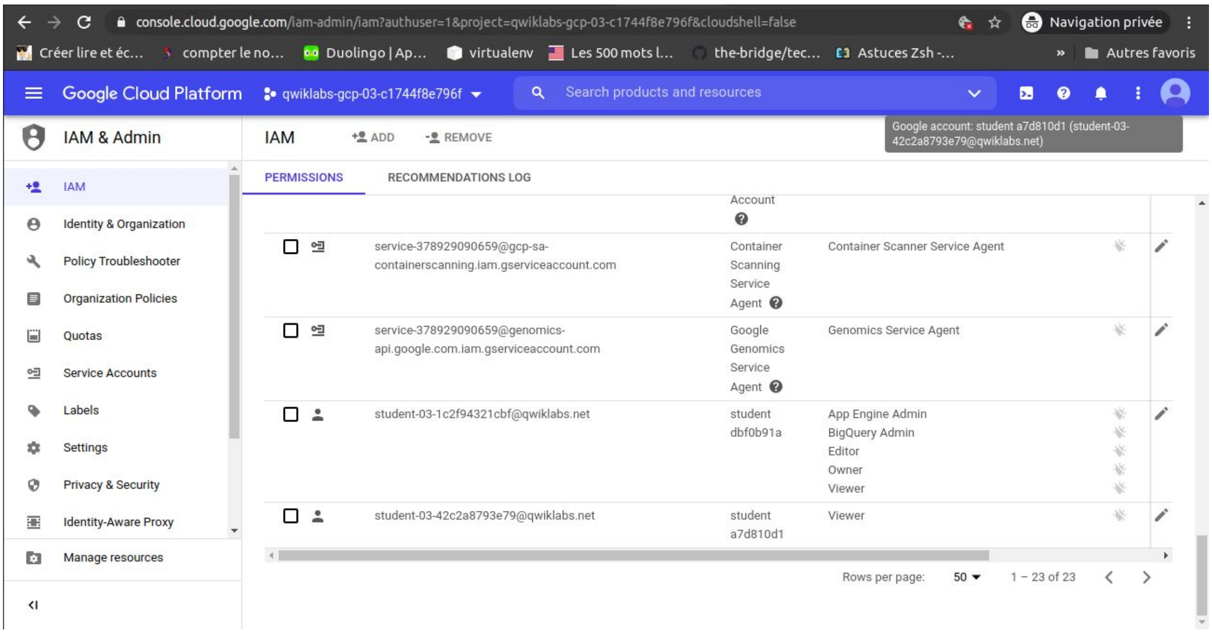
Cloud IAM

Lab objectives

- Use cloud IAM to implement access control
- Restrict access to a specific features or resources
- Use the Service Account User role

We achieved these goals in several steps:

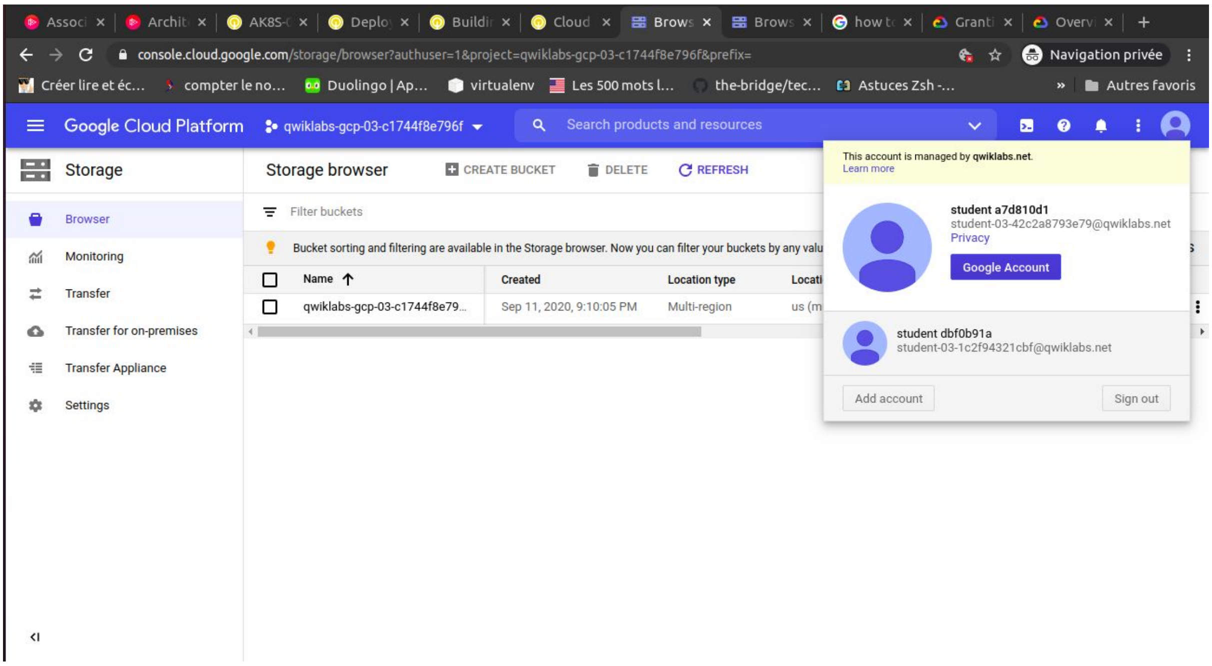
step 1: **Setup for two users**
In this step, we created two user accounts: username1 and username2. We first created the username1 account and then we added the username2 account. After this, we remarked that the username1 had the project owner and can modify the different users roles while the username2 just had the project viewer and couldn't then perform any action on the project; he could just view it. We can see at the bottom the screenshot below, the two users with their respective roles (the before last user is the principal and the last user on the list is the secondary user):



		Account	
☐	service-378929090659@gcp-sa-containerscanning.iam.gserviceaccount.com	Container Scanning Service Agent	Container Scanner Service Agent
☐	service-378929090659@genomics-api.google.com.iam.gserviceaccount.com	Google Genomics Service Agent	Genomics Service Agent
☐	student-03-1c2f94321cbf@qwiklabs.net	student dbf0b91a	App Engine Admin BigQuery Admin Editor Owner Viewer
☐	student-03-42c2a8793e79@qwiklabs.net	student a7d810d1	Viewer

[the two users with their role]

Step2: Upload file for testing
In this step we uploaded a file that we renamed to **sample.txt** in some bucket that we created in the cloud storage. We do this with the username1 account. We then switched to a username2 account and saw that this one can view the object we previously uploaded in the project. **This confirmed to us that the username2 has a project view rôle**.



console.cloud.google.com/storage/browser?authuser=1&project=qwiklabs-gcp-03-c1744f8e796f&prefix=

Bucket sorting and filtering are available in the Storage browser. Now you can filter your buckets by any valu

Name	Created	Location type	Locati
qwiklabs-gcp-03-c1744f8e79...	Sep 11, 2020, 9:10:05 PM	Multi-region	us (m

This account is managed by **qwiklabs.net**.
Learn more

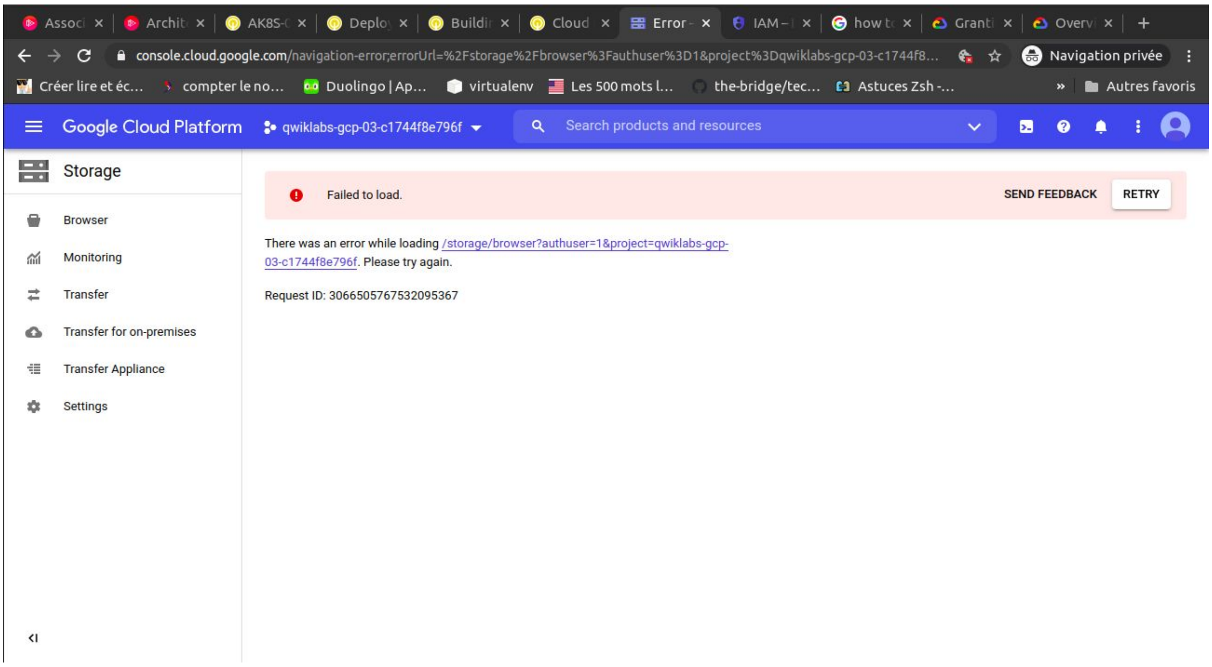
student a7d810d1
student-03-42c2a8793e79@qwiklabs.net
Privacy

student dbf0b91a
student-03-1c2f94321cbf@qwiklabs.net

[username2 could the object created by username1]

Step 3: Remove project access

In this step, we just remove the project viewer role for username2. And then when trying to access our sample file with username2, we got an error: Username2 still has a google cloud account but has not access to the project. **Username2 therefore cannot view the project or any of the project resources.**



console.cloud.google.com/navigation-error;errorUrl=%2Fstorage%2Fbrowser%3Fauthuser%3D1%26project%3Dqwiklabs-gcp-03-c1744f8...

Failed to load.

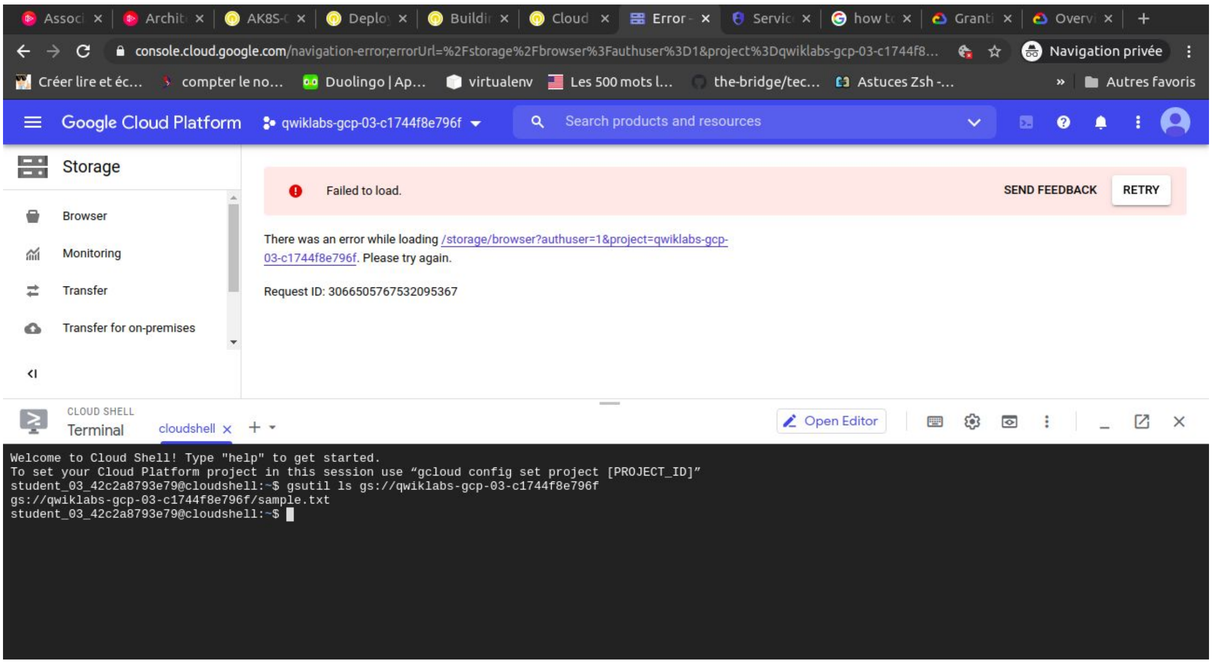
There was an error while loading /storage/browser?authuser=1&project=qwiklabs-gcp-03-c1744f8e796f. Please try again.

Request ID: 3066505767532095367

[username2 couldn't see the bucket content after removing his permission]

Step 4: Add storage access

We added **storage object view** permission for username2 and he were able to list our bucket objects from the cloud shell.


console.cloud.google.com/navigation-error;errorUrl=%2Fstorage%2Fbrowser%3Fauthuser%3D1&project%3Dqwiklabs-gcp-03-c1744f8...
Google Cloud Platform
qwiklabs-gcp-03-c1744f8e796f
Search products and resources
Storage
Browser
Monitoring
Transfer
Transfer for on-premises
SEND FEEDBACK
RETRY
CLOUD SHELL
Terminal
cloudshell
Open Editor

Failed to load.

There was an error while loading /storage/browser?authuser=1&project=qwiklabs-gcp-03-c1744f8e796f. Please try again.

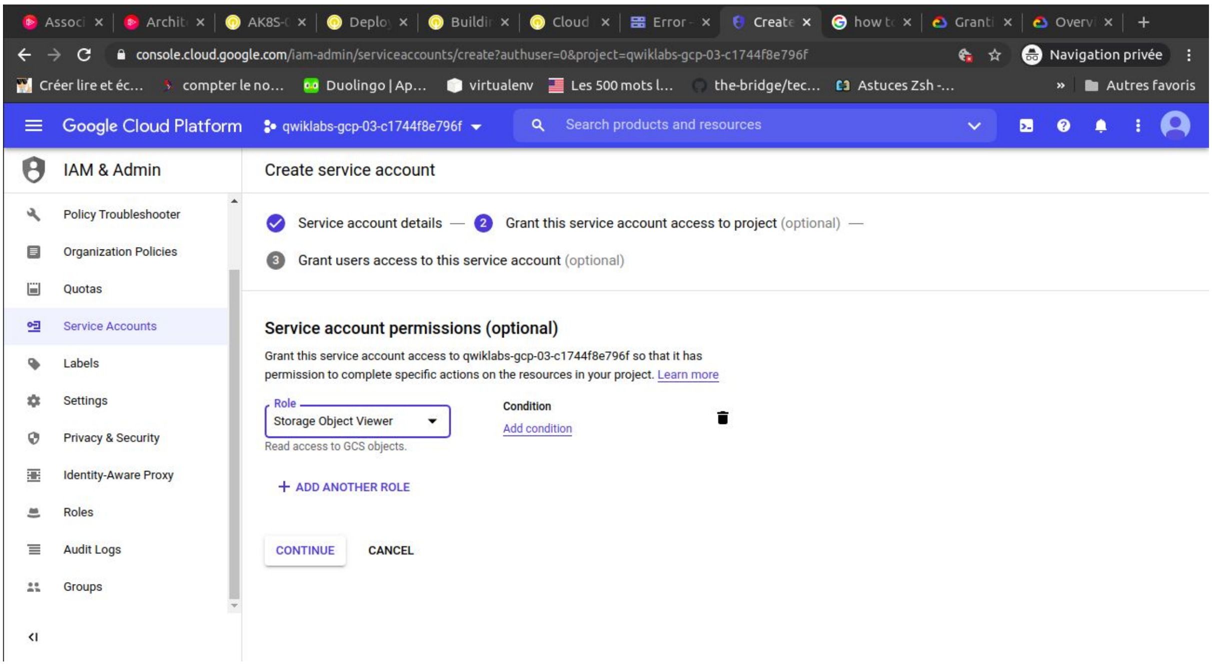
Request ID: 3066505767532095367

```
Welcome to Cloud Shell! Type "help" to get started.
To set your Cloud Platform project in this session use “gcloud config set project [PROJECT_ID]”
student_03_42c2a8793e79@cloudshell:~$ gsutil ls gs://qwiklabs-gcp-03-c1744f8e796f
gs://qwiklabs-gcp-03-c1744f8e796f/sample.txt
student_03_42c2a8793e79@cloudshell:~$
```

[listing bucket objects with username2]

Step5: Setup the service account user

In this last step, we created a service account user with **storage object view** permission. We then granted this service account user role to everyone at some fake company that we created.



Create service account

Service account details — 2 Grant this service account access to project (optional) —

3 Grant users access to this service account (optional)

Service account permissions (optional)

Grant this service account access to qwiklabs-gcp-03-c1744f8e796f so that it has permission to complete specific actions on the resources in your project. Learn more

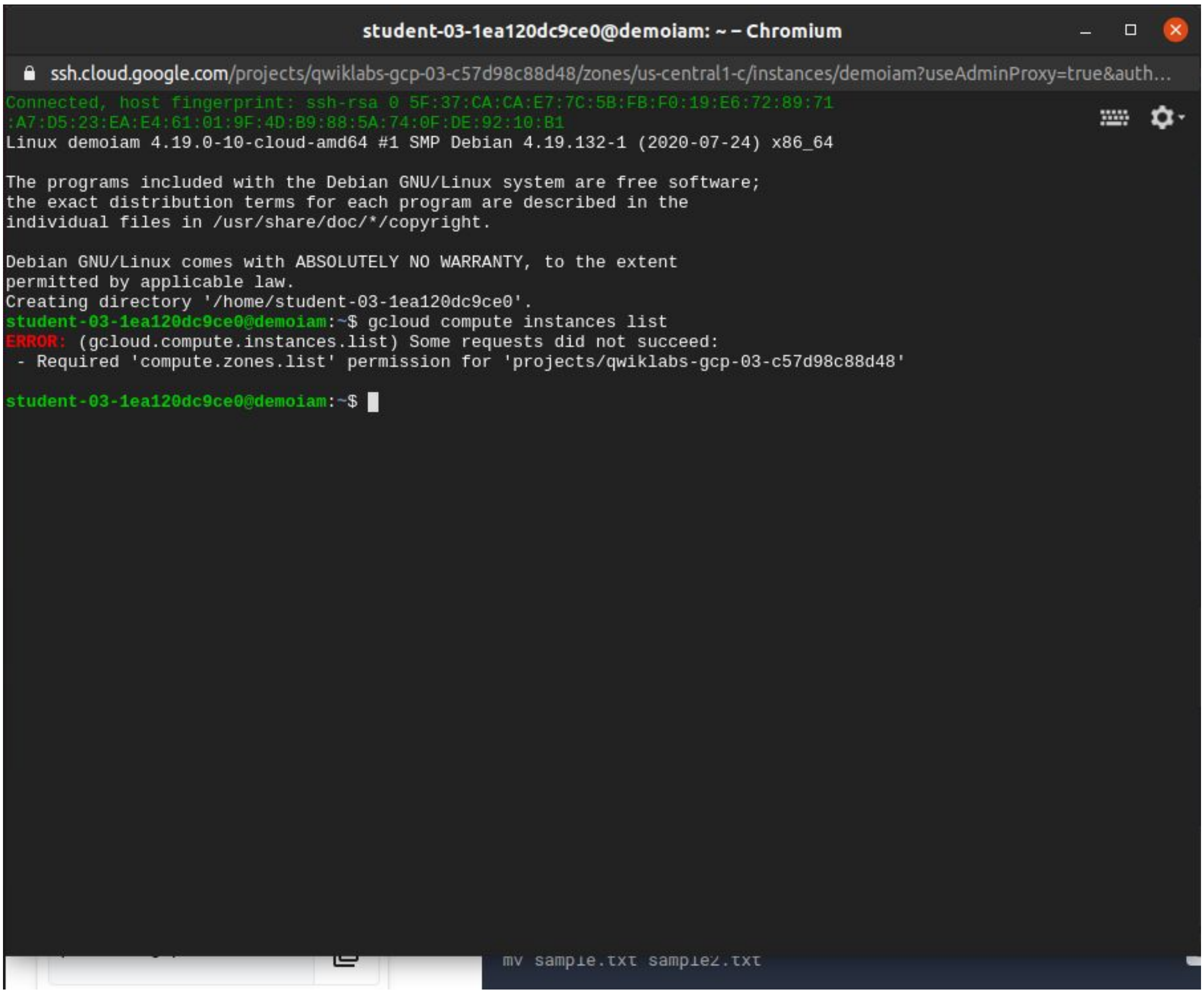
Role: Storage Object Viewer

Read access to GCS objects.

Condition: Add condition

[Creating service account]

We also gave them the computer engine admin role. To explore the service account user role, we created a vm instance with the service account user and connected to it via ssh. From the ssh window, we were just able to copy from the bucket. We were not able to list compute instances, or copy into the bucket as shown on the screenshot below:


student-03-1ea120dc9ce0@demoiam: ~ – Chromium
ssh.cloud.google.com/projects/qwiklabs-gcp-03-c57d98c88d48/zones/us-central1-c/instances/demoiam?useAdminProxy=true&auth...

```
Connected, host fingerprint: ssh-rsa 0 5F:37:CA:CA:E7:7C:5B:FB:F0:19:E6:72:89:71
:A7:D5:23:EA:E4:61:01:9F:4D:B9:88:5A:74:0F:DE:92:10:B1
Linux demoiam 4.19.0-10-cloud-amd64 #1 SMP Debian 4.19.132-1 (2020-07-24) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Creating directory '/home/student-03-1ea120dc9ce0'.
student-03-1ea120dc9ce0@demoiam:~$ gcloud compute instances list
ERROR: (gcloud.compute.instances.list) Some requests did not succeed:
 - Required 'compute.zones.list' permission for 'projects/qwiklabs-gcp-03-c57d98c88d48'

student-03-1ea120dc9ce0@demoiam:~$ 
```

```
mv sample.txt sample2.txt
```

[unable to list project compute instances]

This is due to the service account user role. It just allowed access to the bucket objects and this is why we could copy files from the bucket. But the service account user does not include the others actions such as write, update….this is why we couldn't even copy files to the bucket.