

Table of Contents

05.1g: Storage, IAM	3
5.1.1 GCP Cloud Storage	3
5.1.2 GCP Cloud Storage #1 (USGS).....	3
5.1.3 Configuring permissions	4
5.1.4 USGS data and setup.....	4
5.1.5 Python plotting code.....	4
5.1.6 GCP Cloud Storage #2 (IAM roles)	5
5.1.7 Create service account.....	5
5.1.8 Create Compute Engine VM	5
5.1.9 Service account roles (Compute)	5
5.1.10 Service account roles (Storage)	6
5.1.11 GCP Cloud Storage #3 (Python)	7
5.1.12 Python storage code	7
5.1.13 View object	7
5.1.14 Clean up	7
5.1.15 IAM and least privileges #4 (Optional)	7
05.2a: DynamoDB Guestbook.....	7
5.2.1 DynamoDB	8
5.2.2 model_dynamodb	8
5.2.3 Version 1: Ubuntu VM Python	8
5.2.4 Obtain AWS credentials	8
5.2.5 Run the application	8
5.2.6 Version 2: Ubuntu VM Docker	8
5.2.7 Run the application	8
5.2.8 Push the container image.....	9
5.2.9 Version 3: AWS Cloud9 IDE	9
5.2.10 Configure the Security Group	9
5.2.11 Run the application	9

5.2.12 Version 4: AWS EC2	10
5.2.13 Connect to the instance.....	10
5.2.14 Set up the instance.....	10
5.2.15 Visit the application	10
5.2.16 View the database	11
5.2.17 Clean-up	11
5.2g: Cloud Datastore Guestbook	12
5.2.1 Cloud Datastore	12
5.2.2 model_datastore setup.....	12
5.2.3 model_datastore	12
5.2.4 Datastore setup	12
5.2.5 Version 1: Ubuntu VM Python	12
5.2.6 Obtain GCP credentials	12
5.2.7 Run the application	12
5.2.8 Version 2: Ubuntu VM Docker	12
5.2.9 Run the application	13
5.2.10 Push the container image	13
5.2.11 Version 3: GCP Cloud Shell	13
5.2.12 Run the application	13
5.2.13 Version 4: GCP Compute Engine.....	14
5.2.14 Set up the instance.....	14
5.2.15 Visit the application	14
5.2.16 View the database	15
5.2.17 Clean up.....	15

05.1g: Storage, IAM

5.1.1 GCP Cloud Storage

5.1.2 GCP Cloud Storage #1 (USGS)

- What role is attached to the Compute Engine default service account?

Compute Admin

Permissions for project 'cloud-nurani-srirams'

These permissions affect this project and all of its resources. [Learn more](#)

☐ Include Google-provided role grants

VIEW BY PRINCIPALS VIEW BY ROLES

[GRANT ACCESS](#) [REMOVE ACCESS](#)

Filter Enter property name or value

Type	Principal	Name	Role	Security insights
<input type="checkbox"/>	40274584080-compute@developer.gserviceaccount.com	Compute Engine default service account	Compute Admin	Advanced security insight
<input type="checkbox"/>	srirams@gdx.edu	Ram Nurani Subramanyam	Owner	9975/10203 excess permissions

- Would it be sufficient for the VM to perform its functions (i.e. creating buckets and reading/writing objects in them)?

No, It wont be sufficient for the VM to perform storage related operations are not allowed in Compute Admin Role by default.

- What permissions are given by the default access scope to Cloud Storage?

The **default access scope** for Cloud Storage on a VM is **Read-only**. This means the VM can view (read) objects in Cloud Storage buckets but cannot create, modify, or delete objects or buckets.

- Would they be sufficient for the VM to perform its functions (i.e. creating buckets and reading/writing objects in them)?

No, the default Read-only access scope is not sufficient for performing operations such as creating buckets or writing objects in Cloud Storage.

- What settings are possible for setting the VM's access to the Storage API?

None, Read Only, Write Only, Read Write, Full.

- **None**: No access to Cloud Storage.
- **Read-only**: Allows the VM to view objects and bucket listings only.
- **Write-only**: Allows the VM to write objects to existing buckets but not to read or delete.
- **Read/Write**: Allows the VM to both read from and write to objects in buckets but not manage buckets.
- **Full**: Grants the VM complete access to Cloud Storage, enabling it to create, read, write, delete objects, and manage buckets (provided IAM roles allow it).

5.1.3 Configuring permissions

5.1.4 USGS data and setup

```
srirama@usgs:~/training-data-analyst/CPB100/lab2b$ head -2 earthquakes.csv
time,latitude,longitude,depth,mag,magType,nst,gap,dmin,rms,net,id,updated,place,type,horizontalError,depthError,magError,magNst,status,locationSource,magSource
2024-11-03T00:31:11.890Z,62.861,-149.6075,85,1.8,mL,,,0.18,ak,ak024e5dpk7p,2024-11-03T00:33:02.923Z,"52 km NNE of Chase, Alaska",earthquake,,0.9,,,automatic,ak,ak
```

- **What time did the latest earthquake happen?**

2024-11-03T00:31:11.890Z

- **What was the magnitude (mag)?**

1.8

- **Where was the place it happened?**

52 km NNE of Chase, Alaska

5.1.5 Python plotting code

- **Take a screenshot of the image that has been created for your lab notebook.**

Object details

Buckets > earthquake-srirams > earthquakes.png

LIVE OBJECT
VERSION HISTORY

Download
Edit Metadata
Edit Access
Delete

Overview

Type	image/png
Size	314 KB
Created	Nov 2, 2024, 5:51:38 PM
Last modified	Nov 2, 2024, 5:51:38 PM
Storage class	Standard
Custom time	—
Public URL	Not applicable
Authenticated URL	https://storage.cloud.google.com/earthquake-srirams/earthquakes.png
gsutil URI	gs://earthquake-srirams/earthquakes.png

Permissions

Public access	Not public
---------------	------------

Protection

Version history	—
Retention expiration time	None
Object retention retain until time	None
Bucket retention retain until time	None
Hold status	None
Encryption type	Google-managed

5.1.6 GCP Cloud Storage #2 (IAM roles)

5.1.7 Create service account

5.1.8 Create Compute Engine VM

5.1.9 Service account roles (Compute)

- What is the exact error message that is returned?

Some requests did not succeed.

- Required 'compute.instances.list' permission for 'projects/cloud-nurani-srirams'

```

srirams@gcs-lab-vm:~$ gcloud compute instances list
WARNING: Some requests did not succeed.
- Required 'compute.instances.list' permission for 'projects/cloud-nurani-srirams'

Listed 0 items.
srirams@gcs-lab-vm:~$ █

```

- What role needs to be added to the service account's permissions for the VM to have access to list the project's Compute Engine resources?

Compute Viewer Role

- Take a screenshot of the output for your notebook.

```

srirams@gcs-lab-vm:~$ gcloud compute instances list
NAME          ZONE     MACHINE_TYPE  PREEMPTIBLE  INTERNAL_IP  EXTERNAL_IP  STATUS
course-vm     us-west1-b  e2-medium           10.138.0.2    34.83.234.215  TERMINATED
gcs-lab-vm    us-west1-b  e2-medium           10.138.0.11   34.82.64.164   RUNNING
usgs          us-west1-b  e2-medium           10.138.0.10   34.82.64.164   RUNNING
srirams@gcs-lab-vm:~$ █

```

5.1.10 Service account roles (Storage)

- What is the exact error message that is returned?

AccessDeniedException: 403 gcs-lab@cloud-nurani-srirams.iam.gserviceaccount.com does not have storage.objects.create access to the Google Cloud Storage object. Permission 'storage.objects.create' denied on resource (or it may not exist).

```

srirams@gcs-lab-vm:~$ gsutil cp moonquakes.png gs://earthquake-srirams
Copying file://moonquakes.png [Content-Type=image/png]...
AccessDeniedException: 403 gcs-lab@cloud-nurani-srirams.iam.gserviceaccount.com does not have storage.objects.create access to the Google Cloud Storage object. Permission 'storage.objects.create' denied on resource (or it may not exist).
srirams@gcs-lab-vm:~$ █

```

- What role needs to be added to the service account's permissions for the VM to have access to add an object to a storage bucket?

Storage Object Creator

- Take a screenshot of the output for your notebook.

```

srirams@gcs-lab-vm:~$ gsutil cp moonquakes.png gs://earthquake-srirams
Copying file://moonquakes.png [Content-Type=image/png]...
/ [1 files][314.0 KiB/314.0 KiB]
Operation completed over 1 objects/314.0 KiB.
srirams@gcs-lab-vm:~$ █

```

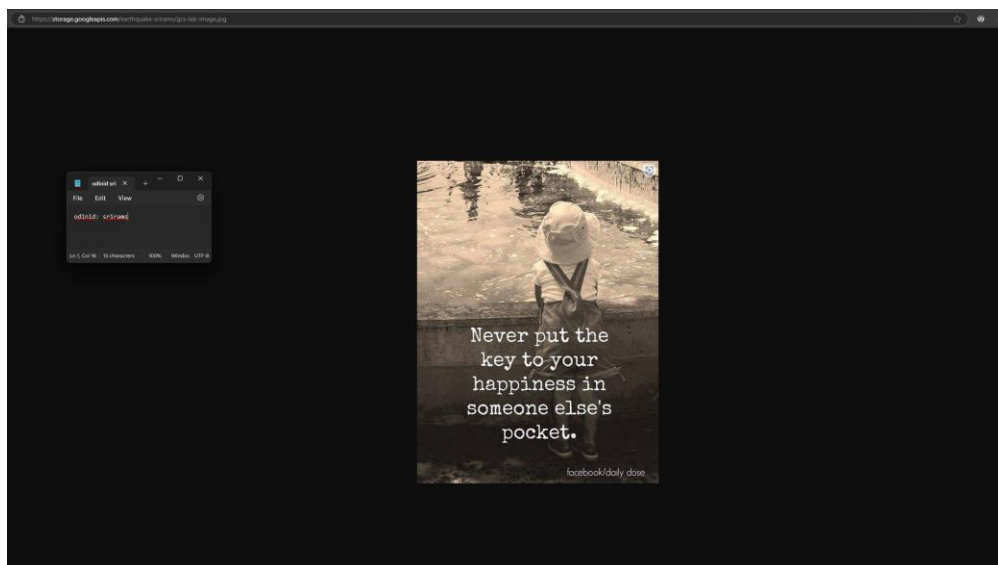
5.1.11 GCP Cloud Storage #3 (Python)

5.1.12 Python storage code

5.1.13 View object

- **Take a screenshot the shows the entire URL and the image that has been retrieved:**

<https://storage.googleapis.com/earthquake-srirams/gcs-lab-image.jpg>



5.1.14 Clean up

5.1.15 IAM and least privileges #4 (Optional)

05.2a: DynamoDB Guestbook

5.2.1 DynamoDB

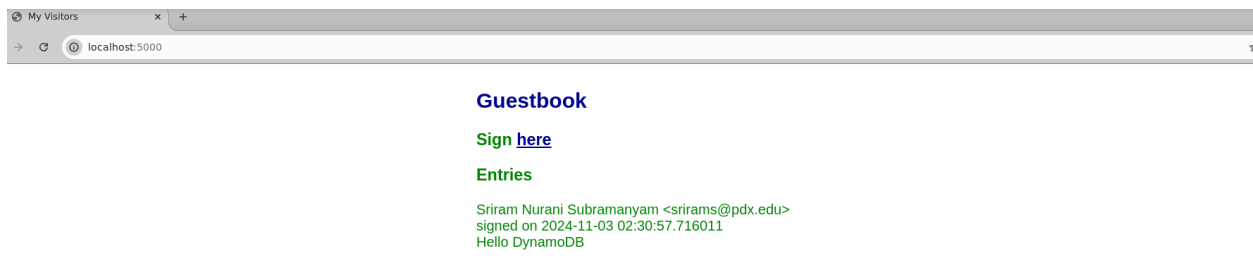
5.2.2 model_dynamodb

5.2.3 Version 1: Ubuntu VM Python

5.2.4 Obtain AWS credentials

5.2.5 Run the application

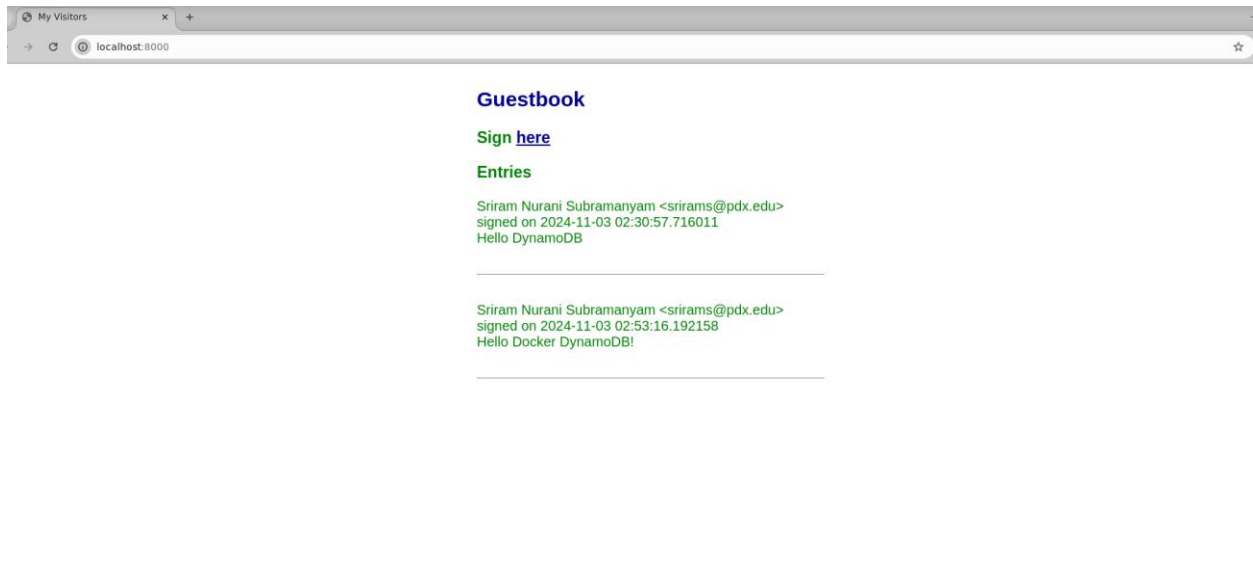
- **Take a screenshot of the output for your lab notebook.**



5.2.6 Version 2: Ubuntu VM Docker

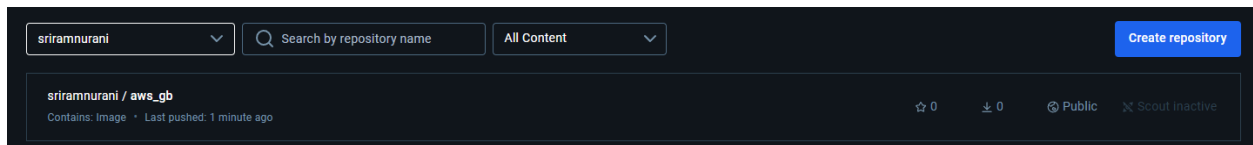
5.2.7 Run the application

- **Take a screenshot of the output for your lab notebook.**



5.2.8 Push the container image

- Take a screenshot of the container image on DockerHub.

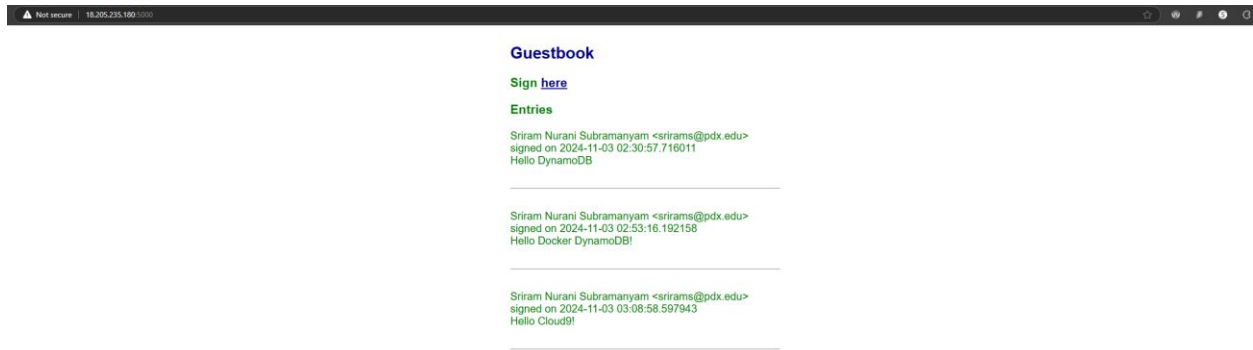


5.2.9 Version 3: AWS Cloud9 IDE

5.2.10 Configure the Security Group

5.2.11 Run the application

- Take a screenshot as before that shows your entry and the IP address in the URL bar.



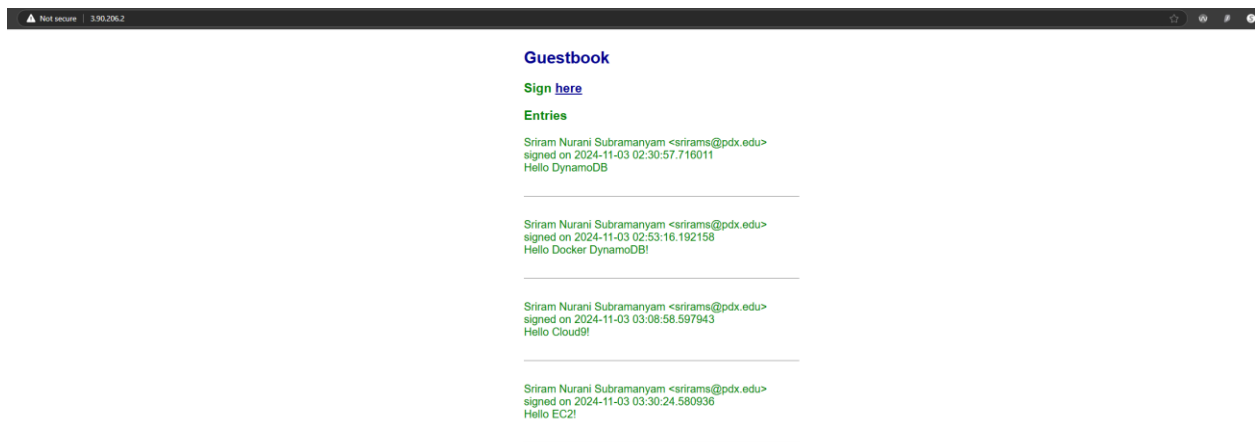
5.2.12 Version 4: AWS EC2

5.2.13 Connect to the instance

5.2.14 Set up the instance

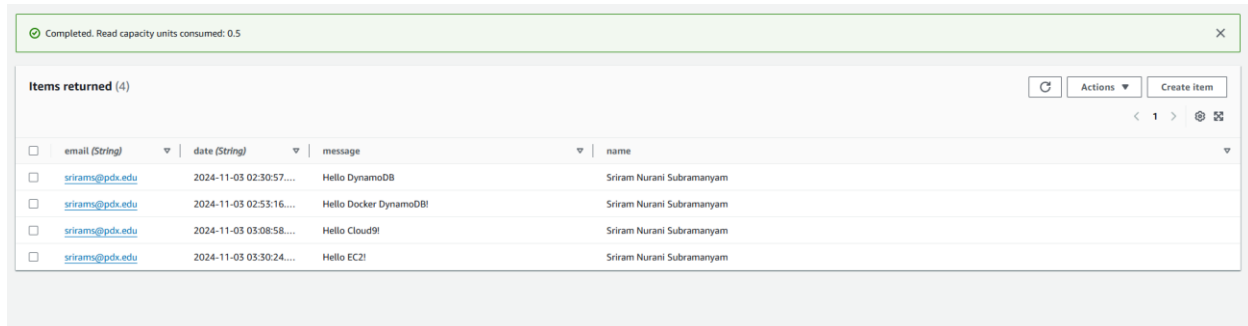
5.2.15 Visit the application

- **Take a screenshot as before that shows your entry and the IP address in the URL bar.**



5.2.16 View the database

- Take a screenshot that shows all of the guestbook entries that you added to the DynamoDB table including their timestamps.



5.2.17 Clean-up

5.2g: Cloud Datastore Guestbook

5.2.1 Cloud Datastore

5.2.2 model_datastore setup

5.2.3 model_datastore

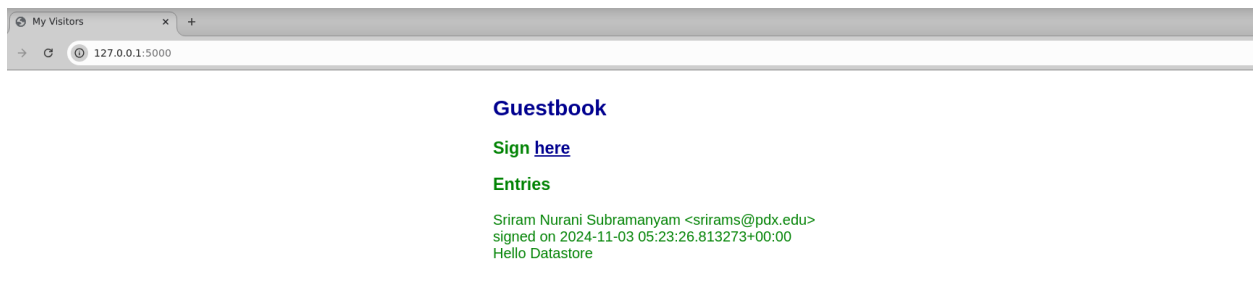
5.2.4 Datastore setup

5.2.5 Version 1: Ubuntu VM Python

5.2.6 Obtain GCP credentials

5.2.7 Run the application

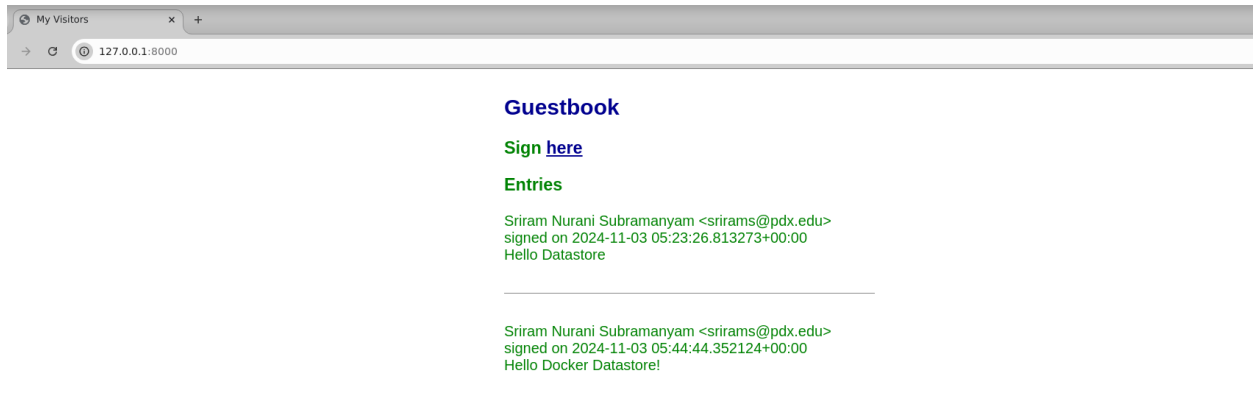
- **Take a screenshot of the output for your lab notebook.**



5.2.8 Version 2: Ubuntu VM Docker

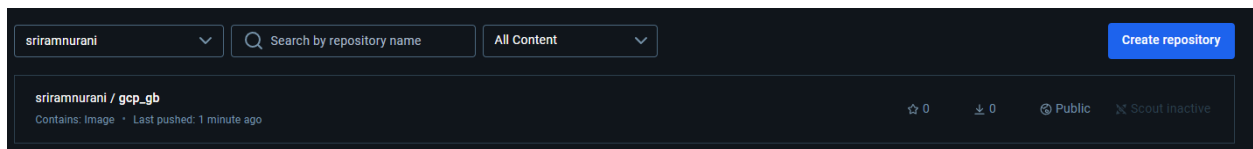
5.2.9 Run the application

- Take a screenshot of the output for your lab notebook.



5.2.10 Push the container image

- Take a screenshot of the container image on DockerHub.



5.2.11 Version 3: GCP Cloud Shell

5.2.12 Run the application

- Take a screenshot as before that shows your entry and the URL bar.

Guestbook

Sign [here](#)

Entries

Sriram Nurani Subramanyam <srirams@pdx.edu>
signed on 2024-11-03 05:58:40.519942+00:00
Hello Cloud Shell!

Sriram Nurani Subramanyam <srirams@pdx.edu>
signed on 2024-11-03 05:23:26.813273+00:00
Hello Datastore

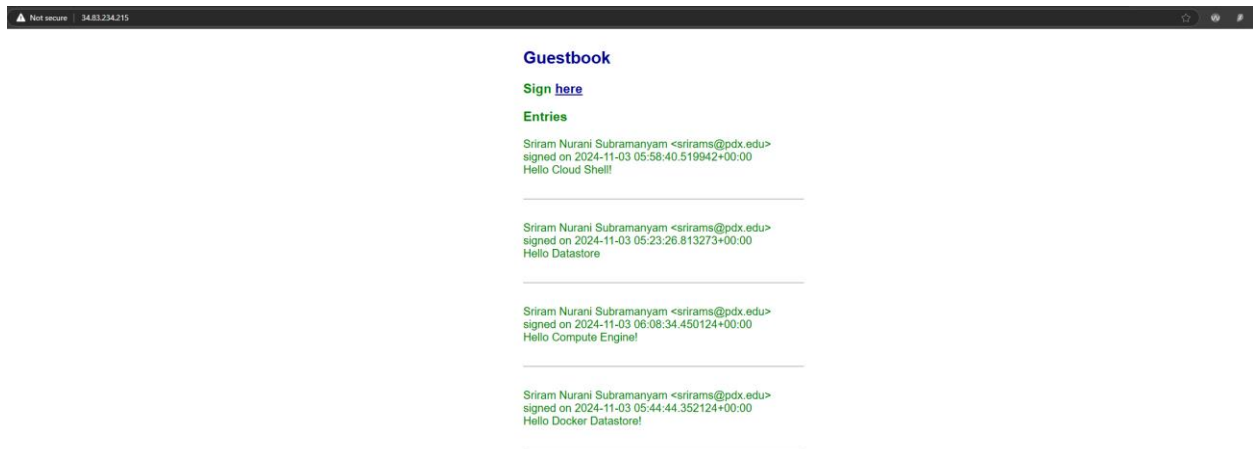
Sriram Nurani Subramanyam <srirams@pdx.edu>
signed on 2024-11-03 05:44:44.352124+00:00
Hello Docker Datastore!

5.2.13 Version 4: GCP Compute Engine

5.2.14 Set up the instance

5.2.15 Visit the application

- Take a screenshot as before that shows your entry and the IP address in the URL bar.



5.2.16 View the database

- Take a screenshot of all of the entries that have been added including their timestamps for your lab notebook.

RESULTS

ANALYSIS

Query results

Document ID	date	email	message	name
__id5632499082330112__	November 2, 2024 at 10:58:40 PM UTC-7	"srirams@pdx.edu"	"Hello Cloud Shell!"	"Sriram Nurani Subramanyam"
__id5634161670881280__	November 2, 2024 at 10:23:26 PM UTC-7	"srirams@pdx.edu"	"Hello Datastore"	"Sriram Nurani Subramanyam"
__id5642368648740864__	November 2, 2024 at 11:08:34 PM UTC-7	"srirams@pdx.edu"	"Hello Compute Engine!"	"Sriram Nurani Subramanyam"
__id5644004762845184__	November 2, 2024 at 10:44:44 PM UTC-7	"srirams@pdx.edu"	"Hello Docker Datastore!"	"Sriram Nurani Subramanyam"

5.2.17 Clean up