

HSBC Fund Rebalancing Project

Deployment Guideline

April 3rd, 2019

Team REST

Aurora (Yutian) Qiu

Cathy Leung

Leo Cheng

Leo (Jixing) Li

Shaw (Xiao) Lu

Stanley Ye

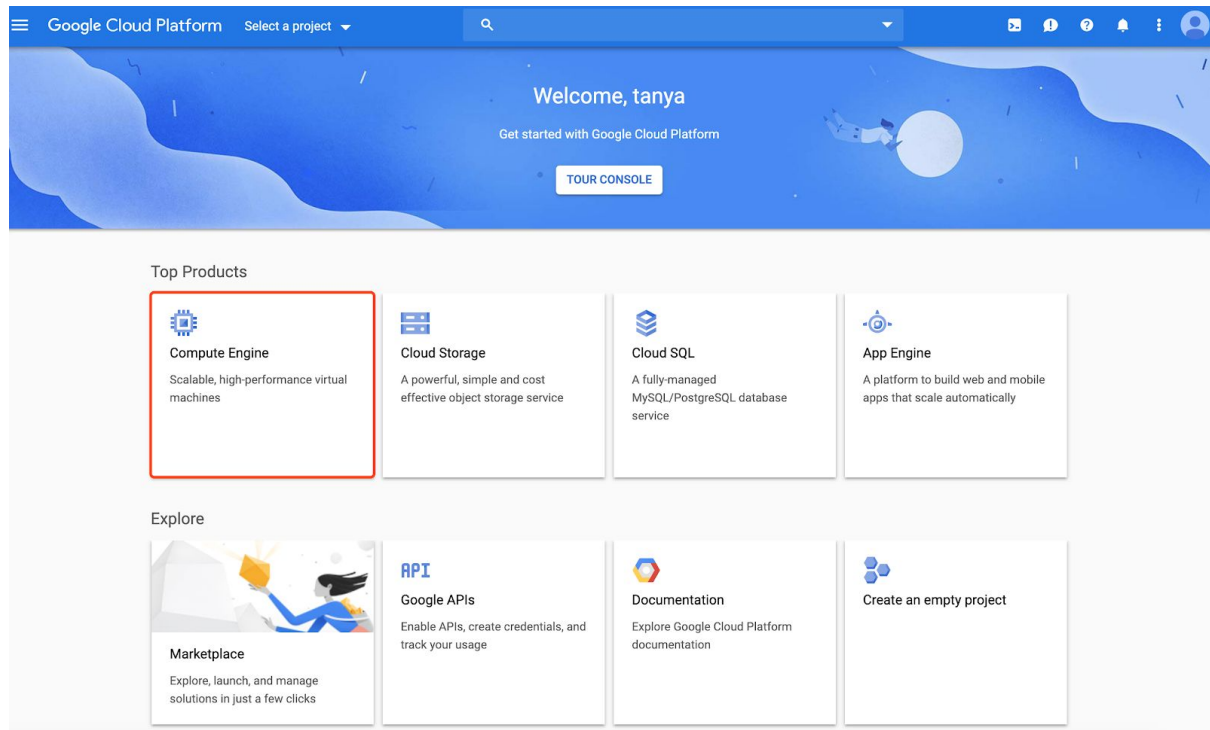
Tanya (Yi) Tan

Table of Contents

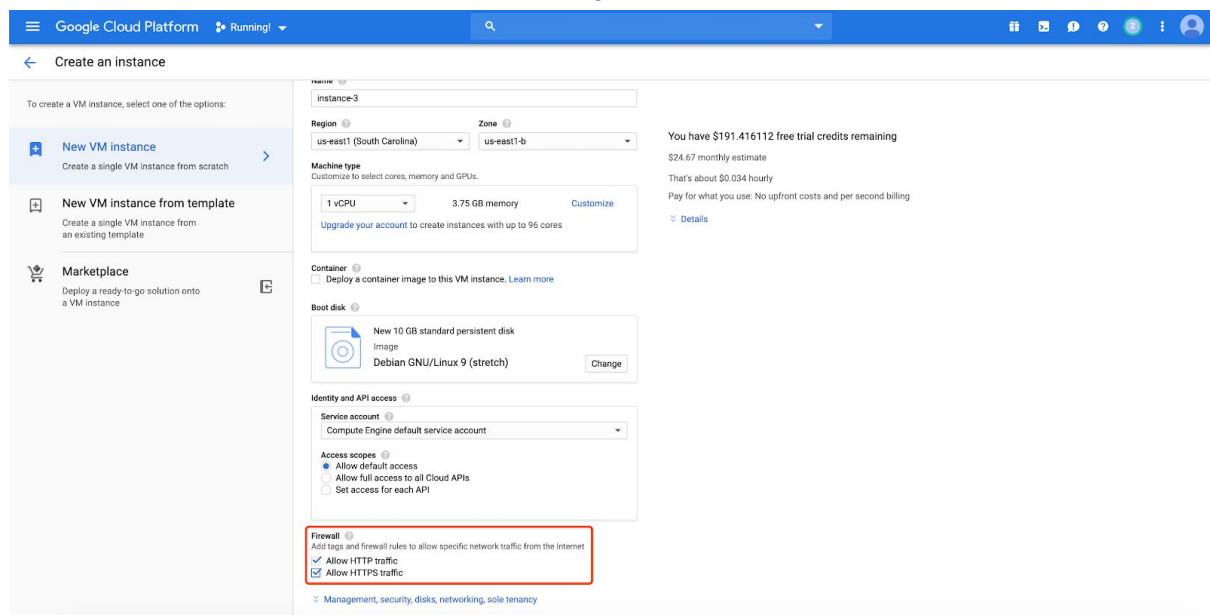
Table of Contents	2
Frontend & Backend Deployment	3
Appendix I: Database Deployment	6
Appendix II: Firewall Rule Configurations	13

Frontend & Backend Deployment

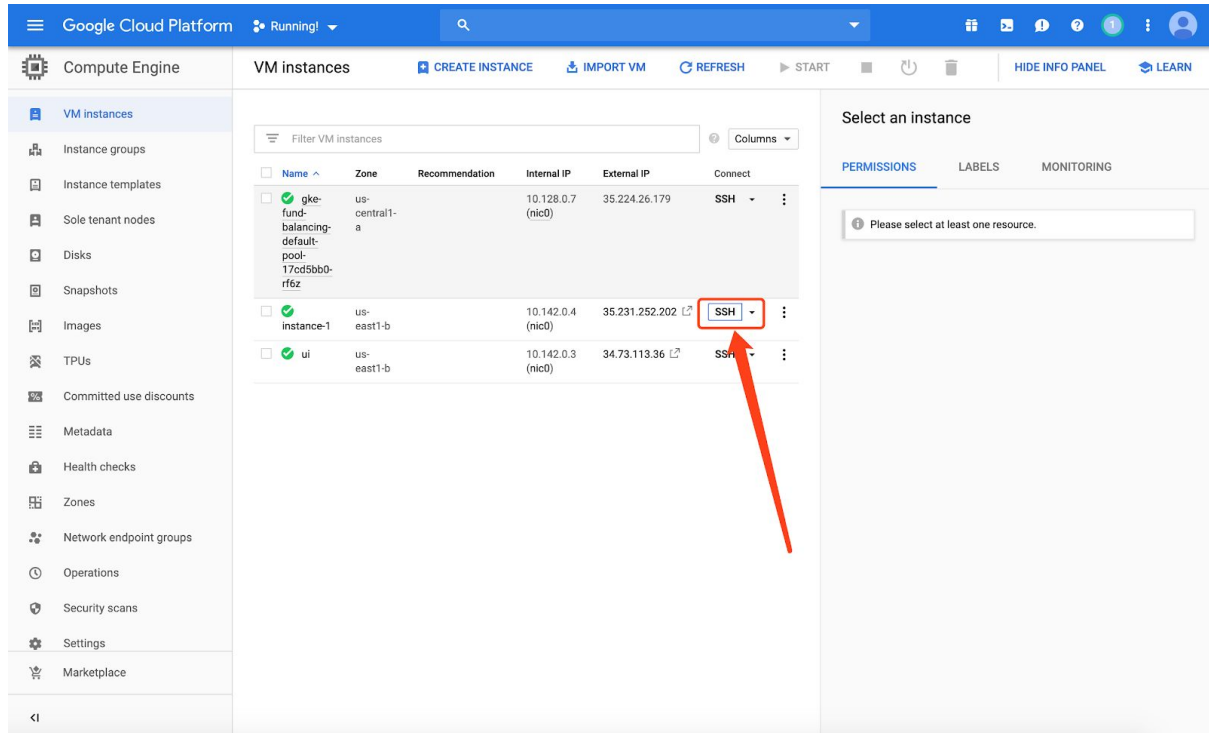
1. Open the website: <https://console.cloud.google.com/> and navigate to “Compute Engine”.



2. Select “Create Instance”. In the configuration page, check “Allow HTTP traffic” and “Allow HTTPS traffic” boxes and keep the rest setting as default. Then, click “Create”.



3. Choose the VM instance you just created and click **ssh** as shown in the screenshot and the virtual terminal window will popup.



4. In the virtual terminal window, use the following commands to install Git, Java, and Nodejs (for the first time usage):

```
sudo apt install git
sudo apt install default-jdk
curl -sL https://deb.nodesource.com/setup_11.x | sudo bash -
sudo apt-get install -y nodejs
sudo npm install -g npm@latest
```

5. Then in the virtual terminal window, clone the codebase from GitLab.

```
git clone https://[username]@gitlab.com/cpsc319-2018w2/hsbc/rest/fund-rebalancing.git
```

Note: replace the [username] with your Gitlab user name.

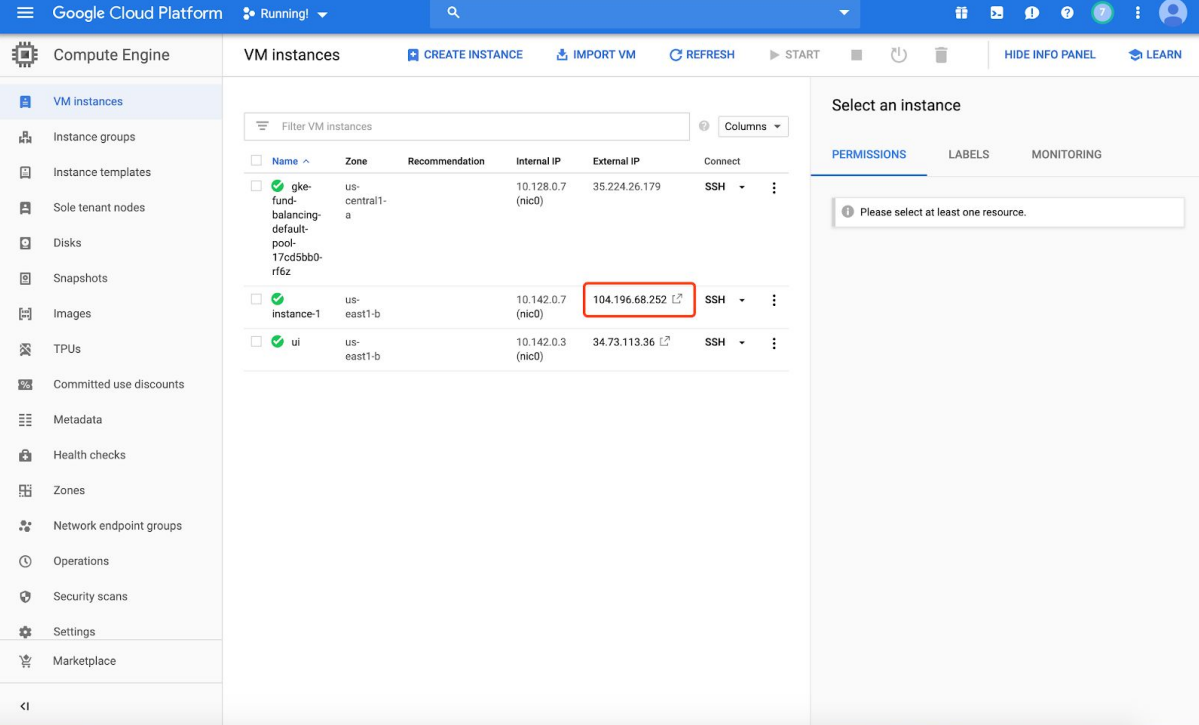
Then enter the password.

6. Create database instance and change the database server URL in the codebase. Steps are provided in the appendix, the end of this file.

7. Change the backend server url to the current VM instance IP using commands:

```
cd ~/fund-rebalancing/src/main/react/src
```

Then, use an editor to change the **HOST_IP** variable in the *constant.js* file to the public IP address of current VM instance, eg: '34.73.113.36' (the backend server url team REST is currently using). The example current VM instance IP address can be found in the VM Instances page as indicated by the red box below.



The screenshot shows the Google Cloud Platform interface for VM instances. The left sidebar lists various resources, and the main panel displays a table of VM instances. The table has columns for Name, Zone, Recommendation, Internal IP, External IP, and Connect. The 'instance-1' row is highlighted, and its 'External IP' (104.196.68.252) is enclosed in a red box. The right sidebar shows the 'Select an instance' panel with tabs for PERMISSIONS, LABELS, and MONITORING.

Name	Zone	Recommendation	Internal IP	External IP	Connect
gke-fund-balancing-default-pool-17cd5bb0-rf6z	us-central1-a		10.128.0.7 (nic0)	35.224.26.179	SSH
instance-1	us-east1-b		10.142.0.7 (nic0)	104.196.68.252	SSH
ui	us-east1-b		10.142.0.3 (nic0)	34.73.113.36	SSH

8. In the virtual terminal window, run the deployment script using commands:

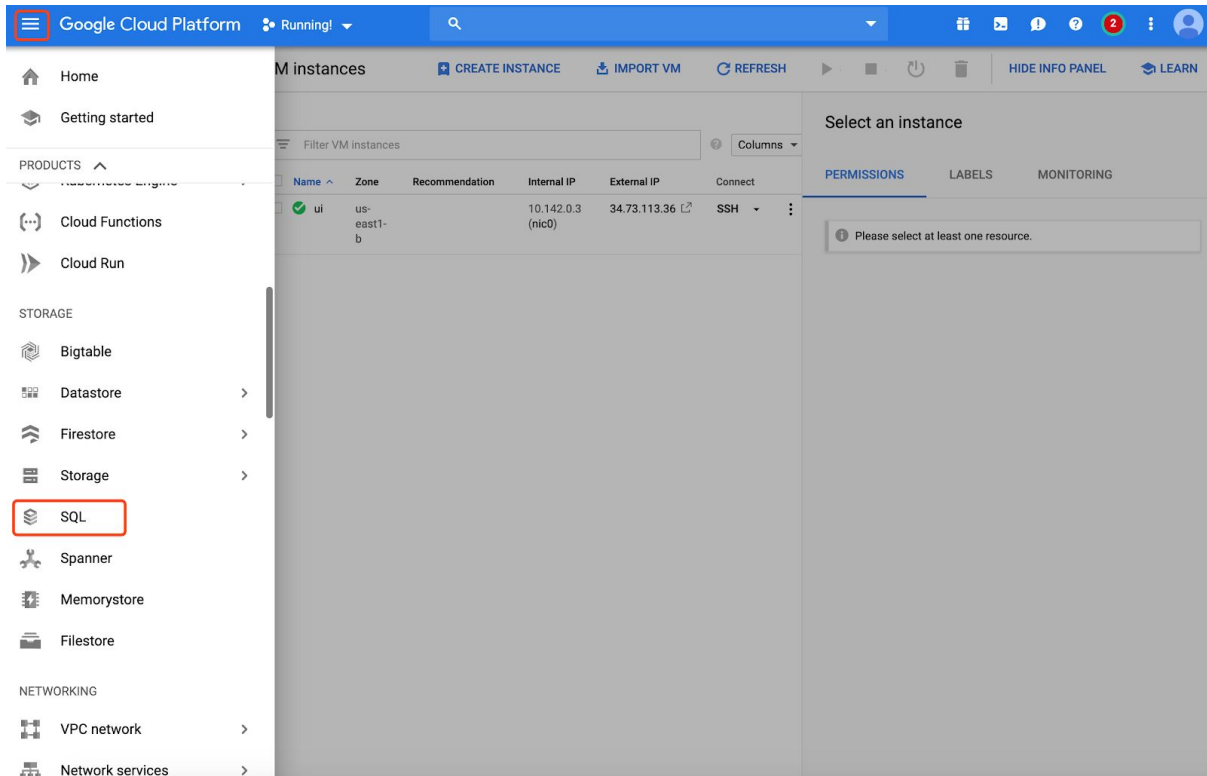
```
cd ~/fund-rebalancing
chmod +x deployment.sh
./deployment.sh
```

9. Once all these steps has completed, the application is hosted at GCP URL:

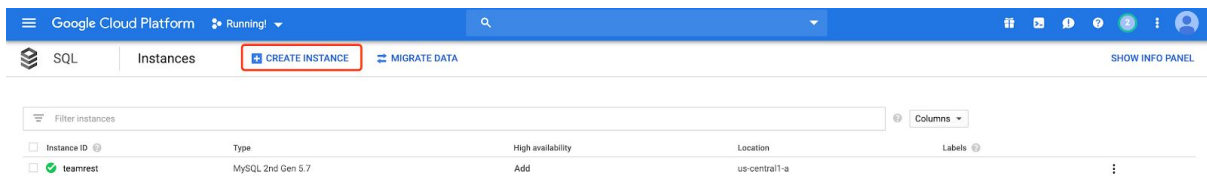
[http://\[public_ip_address_of_vm\]:3000](http://[public_ip_address_of_vm]:3000)

Appendix 1: Database Deployment

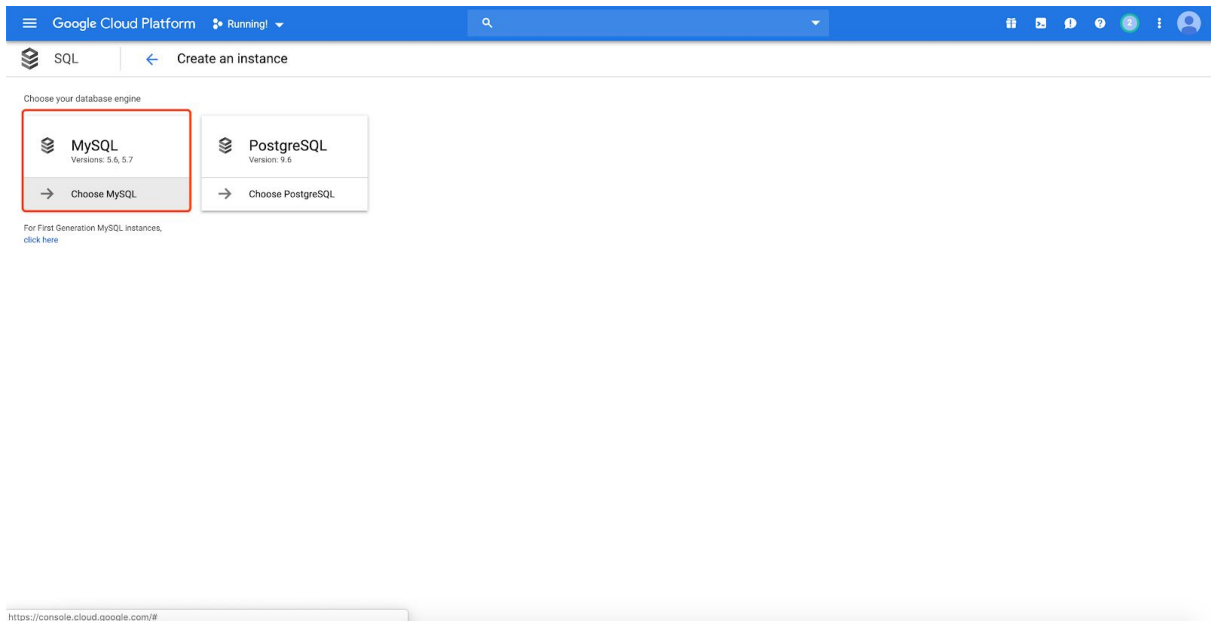
1) Click the navigation button on the top left corner, and choose “SQL” from the panel.



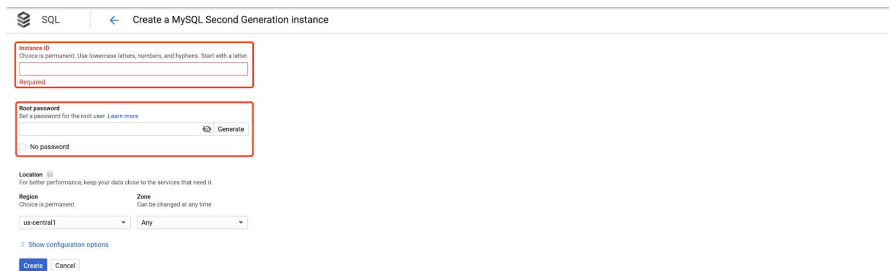
2) Click on “Create Instance”



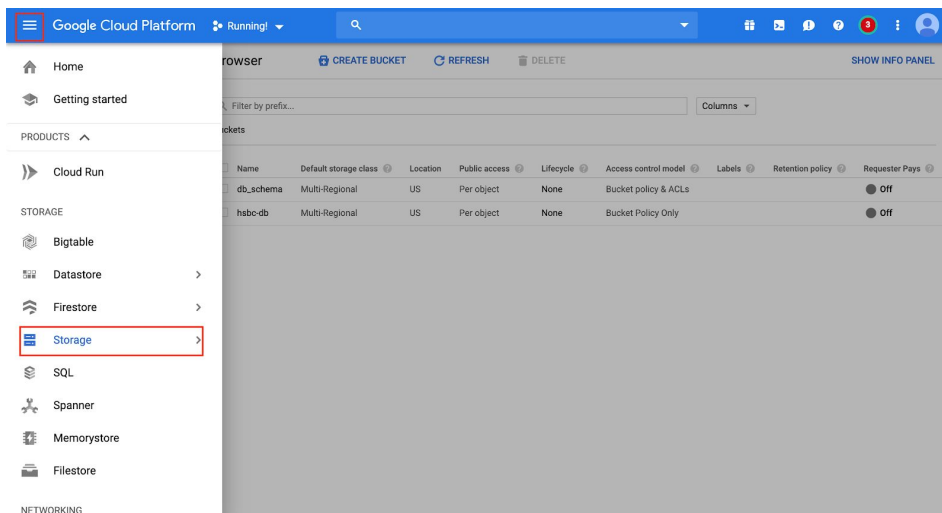
3) And click “Choose MySQL”



4) Fill in the instance ID and the root password, then click on “Create”. Note: this step may take a few minutes to complete.



5) Click the navigation button on the top left corner again and select “Storage”



6) Click “Create Bucket” and enter a Name for this bucket and click “Creat

Create a bucket

Name ⓘ
Must be unique across Cloud Storage. If you're serving website content, enter the website domain as the name.

Default storage class
Objects added to this bucket are assigned the selected storage class by default. An object's storage class and bucket location affect its geo-redundancy, availability, and costs. You can set storage classes for individual objects in gcloud. [Learn more](#)

ⓘ Nearline and Coldline data in multi-regional locations is now stored geo-redundantly. New locations nam4 and eu4 (available in beta) enable co-location of compute and storage for high performance with geo-redundancy. [Learn more](#)

☒ Multi-Regional
☐ Regional
☐ Nearline
☐ Coldline

Location
United States (multiple regions in the United States)

[Compare storage classes](#)

Storage cost	Retrieval cost	Class A operations ⓘ	Class B operations ⓘ
\$0.026 per GB-month	Free	\$0.005 per 1,000 ops	\$0.0004 per 1,000 ops

Access control model
Choose how you'll control access to this bucket's objects. [Learn more](#)

☐ Set permissions uniformly at bucket-level (Bucket Policy Only)
Enforces the bucket's IAM policy without object ACLs. May help prevent unintended access. If selected, this option becomes permanent after 90 days.

☒ Set object-level and bucket-level permissions
Enforces the IAM policy and object ACLs for more granular control of object access.

☒ Show advanced settings

Create **Cancel**

7) Upload the database schema file into the bucket. You can download the file from GitLab [here](https://gitlab.com/cpsc319-2018w2/hsbc/rest/fund-rebalancing/blob/master/src/mysql/hsbc_db.sql). (If you don't have gitLab account, you can get this file from sourcecode: https://gitlab.com/cpsc319-2018w2/hsbc/rest/fund-rebalancing/blob/master/src/mysql/hsbc_db.sql)

Bucket details [EDIT BUCKET](#) [REFRESH BUCKET](#)

db_schema

[Objects](#) [Overview](#) [Permissions](#) [Bucket Lock](#)

Upload files **Upload folder** **Create folder** **Manage holds** **Delete**

🔍 Filter by prefix...

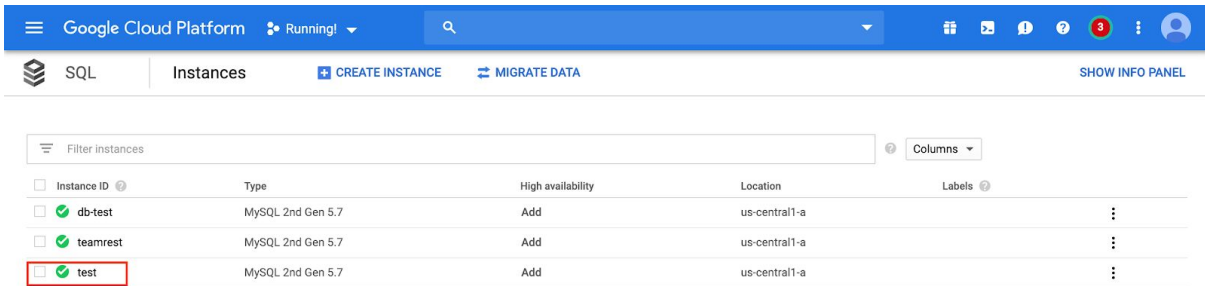
Buckets / db_schema

<input type="checkbox"/>	Name	Size	Type	Storage class	Last modified	Public access ⓘ	Encryption ⓘ	Retention expiration date ⓘ	Holds ⓘ
<input checked="" type="checkbox"/>	hsbc_db.sql	5.06 KB	application/octet-stream	Multi-Regional	4/3/19, 11:55:58 PM UTC-7	Not public	Google-managed key	–	None

Upload 1 of 1 complete

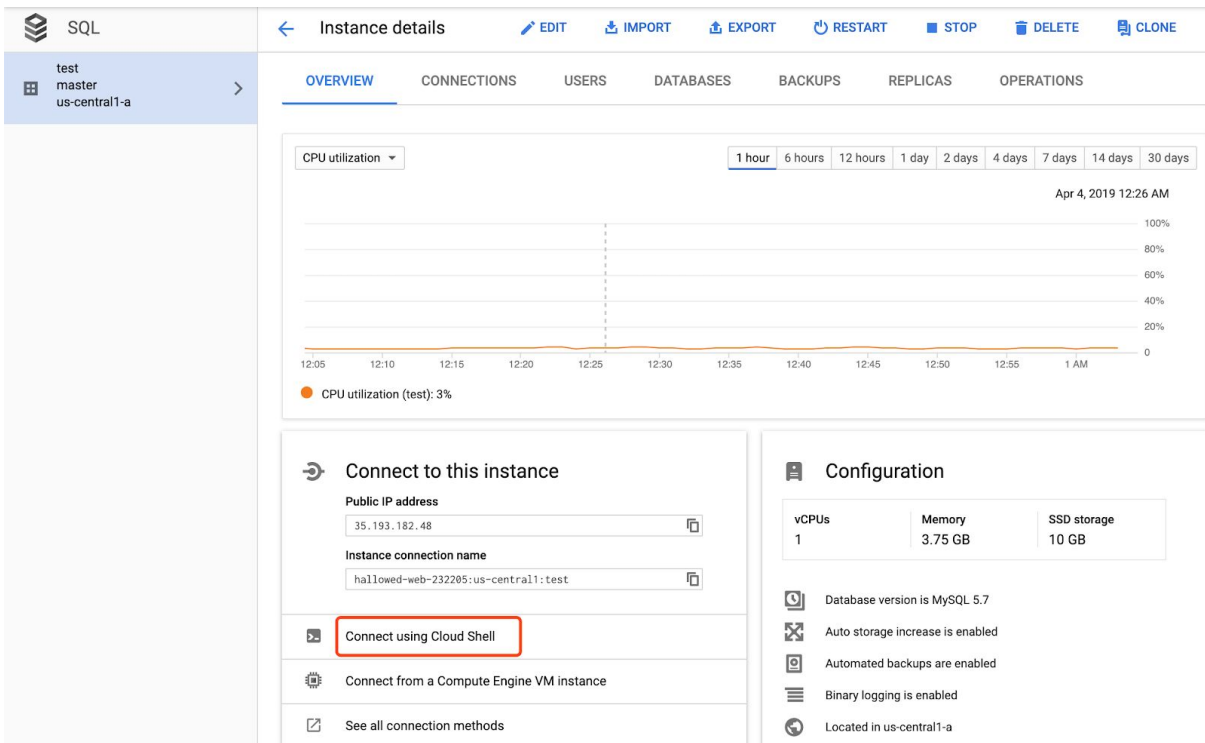
hsbc_db.sql	Finished
-------------	----------

8) Navigate back to SQL main page by clicking the navigation button on the top left corner again and select “SQL”. On the main page, click on the instance you just created.



Instance ID	Type	High availability	Location	Labels
db-test	MySQL 2nd Gen 5.7	Add	us-central1-a	
teamrest	MySQL 2nd Gen 5.7	Add	us-central1-a	
test	MySQL 2nd Gen 5.7	Add	us-central1-a	

9) In the instance details page, click on “Connect using Cloud Shell”



Instance details | EDIT | IMPORT | EXPORT | RESTART | STOP | DELETE | CLONE

OVERVIEW | CONNECTIONS | USERS | DATABASES | BACKUPS | REPLICAS | OPERATIONS

CPU utilization (test): 3%

Connect to this instance

Public IP address: 35.193.182.48

Instance connection name: hallowed-web-232285-us-central1:test

Connect using Cloud Shell

Connect from a Compute Engine VM instance

See all connection methods

Configuration

vCPUs	Memory	SSD storage
1	3.75 GB	10 GB

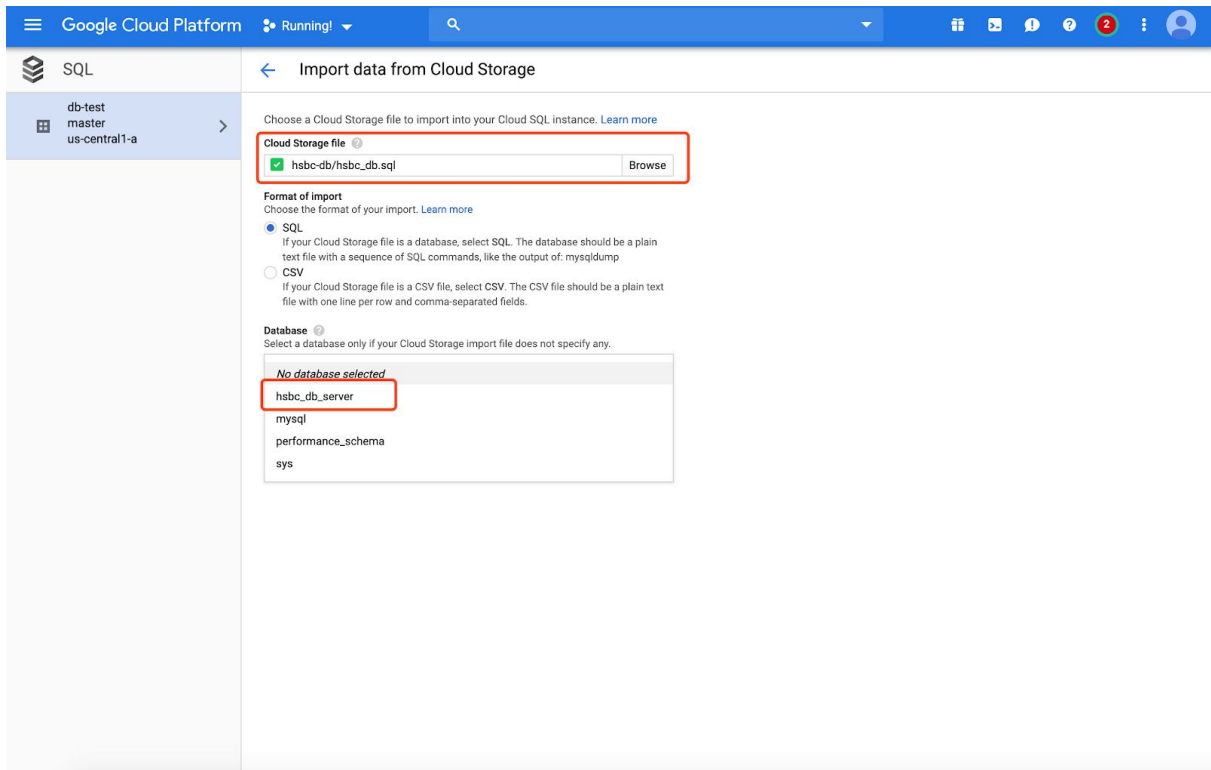
- Database version is MySQL 5.7
- Auto storage increase is enabled
- Automated backups are enabled
- Binary logging is enabled
- Located in us-central1-a

10) A terminal window will popup at the bottom of the detail page, press “Enter” key. Then input the password and press “Enter” again. Once login, enter command: `create database hsbcb_db_server`; and press “Enter”. You can close the terminal window now.

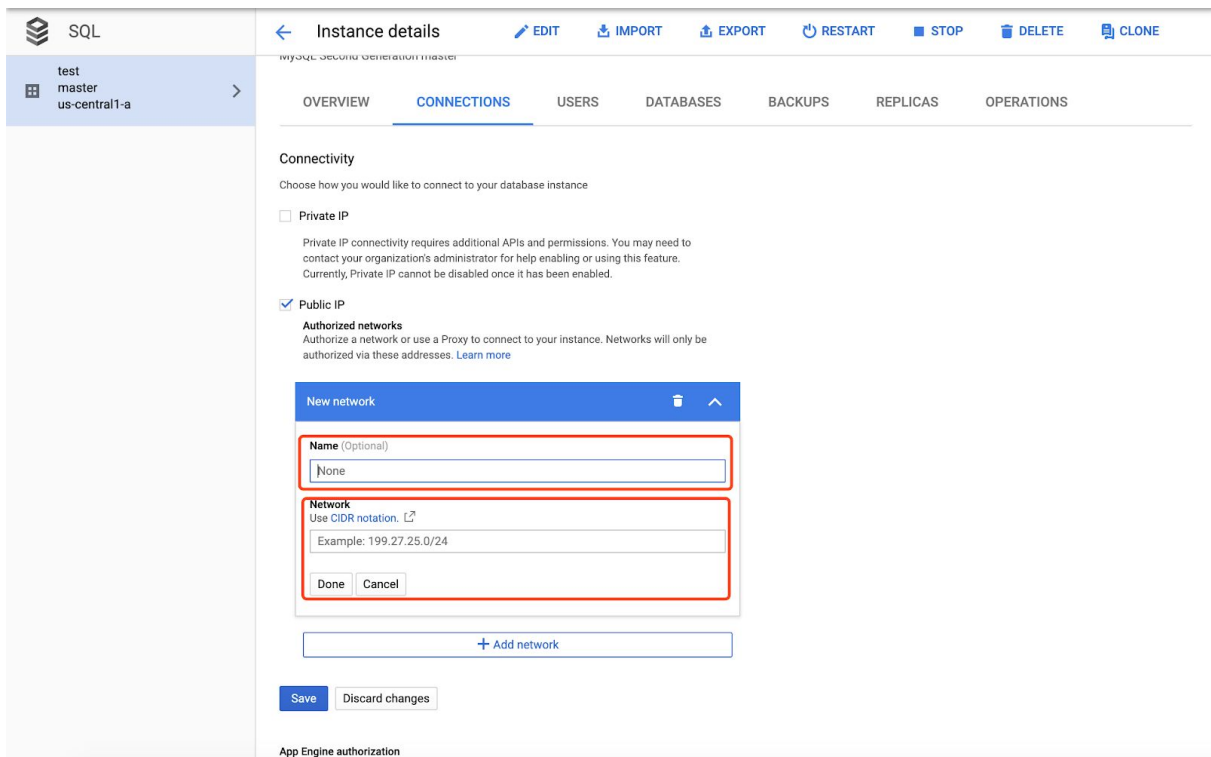
The screenshot shows the Google Cloud Platform interface for a SQL instance named 'db-test' in the 'master' region and 'us-central1-a' zone. The instance is running. The 'Instance details' tab is active, showing a CPU utilization graph for 'db-test' at 8%. Below the graph, there are sections for 'Connect to this instance' and 'Configuration'. The 'Connect to this instance' section shows the public IP address as 104.197.68.7 and the instance connection name. The 'Configuration' section shows 1 vCPU, 3.75 GB memory, and 10 GB SSD storage. At the bottom, there is a terminal window showing the command prompt and the execution of the 'gcloud sql connect' command, which successfully connects to the database.

11) Click on “Import” icon in the navigation bar. In “Cloud Storage File”, select the schema file you uploaded earlier. In “Database”, choose the database “hsbc_db_server”. Then, click “Import” button to import the database schema into the database.

The screenshot shows the Google Cloud Platform interface for a SQL instance named 'test' in the 'master' region and 'us-central1-a' zone. The instance is running. The 'Instance details' tab is active, showing a CPU utilization graph for 'test' at 100%. Below the graph, there are sections for 'Connect to this instance' and 'Configuration'. The 'Connect to this instance' section shows the public IP address as 35.193.182.48 and the instance connection name as 'hallowed-web-232205:us-central1:test'. The 'Configuration' section shows 1 vCPU, 3.75 GB memory, and 10 GB SSD storage. Below the configuration, there are several status indicators: 'Database version is MySQL 5.7', 'Auto storage increase is enabled', 'Automated backups are enabled', and 'Binary logging is enabled'.



12) When importing is done. In the Instance Details page, click on “Connections”, then click “Add Network” to add a new network rule by given a name and network mask (You can specify your IP address, or just simply use 0.0.0.0/0). Click “Done” and then click “Save”.



The database connection setup has finished. Now, remember the public IP address, username, and password, go to the file in the codebase:

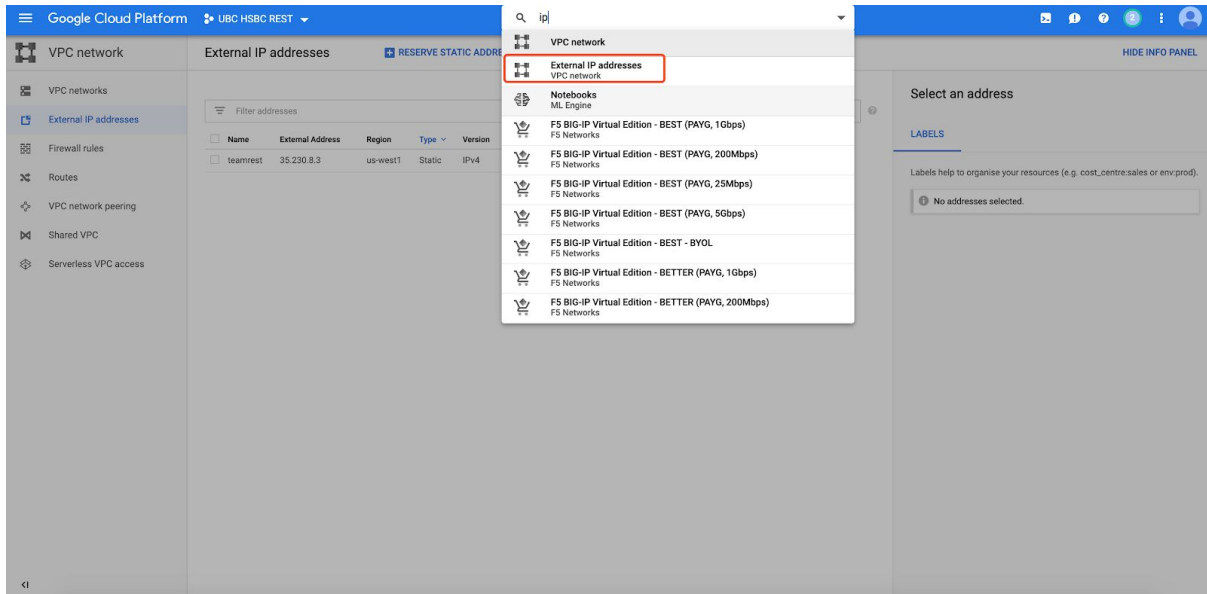
~/fund-rebalancing/src/main/java/Util/DatabaseConnection.java

Update `GOOGLE_DB_URL`, `GOOGLE_DB_USERNAME`, and `GOOGLE_DB_PASSWORD` variables with the public IP address, username and password you just created. Then use maven to rebuild the jar in the main folder of the codebase `~/fund-rebalancing` by running following commands:

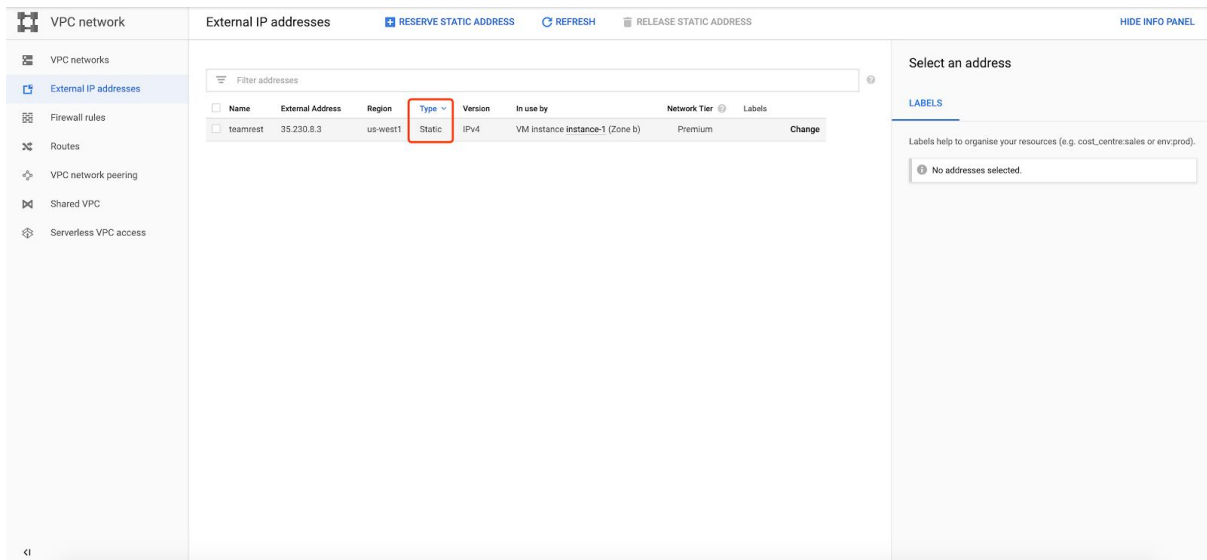
```
sudo apt install maven
mvn -Dmaven.test.skip=true package
cd ~/fund-rebalancing
mvn package
```

Appendix 2: Firewall Rule Configurations

1. Search “IP address”, click on “External IP addresses”.



2. Change the type of IP address to “Static”.



3. Click on “Firewall Rules” on the left panel.

The screenshot shows the Google Cloud Platform console interface. On the left sidebar, under the 'VPC network' section, 'Firewall rules' is highlighted with a red rectangular box. The main content area is titled 'External IP addresses' and includes buttons for 'RESERVE STATIC ADDRESS', 'REFRESH', and 'RELEASE STATIC ADDRESS'. Below these is a search bar and a table of external IP addresses. The table has columns: Name, External Address, Region, Type, Version, In use by, Network Tier, and Labels. One entry is visible: 'teamrest' with address '35.230.8.3' in the 'us-west1' region, static type, IPv4 version, used by 'VM instance instance-1 (Zone b)', and 'Premium' network tier. To the right of the table is a 'Select an address' section with a 'LABELS' tab and a message 'No addresses selected.'

Name	External Address	Region	Type	Version	In use by	Network Tier	Labels
teamrest	35.230.8.3	us-west1	Static	IPv4	VM instance instance-1 (Zone b)	Premium	

4. Click on “Create firewall rule”.

The screenshot shows the Google Cloud Platform console interface for 'Firewall rules'. The left sidebar has 'Firewall rules' selected. The main content area has a title 'Firewall rules' and buttons for 'CREATE FIREWALL RULE', 'REFRESH', and 'DELETE'. Below the buttons is a description: 'Firewall rules control incoming or outgoing traffic to an instance. By default, incoming traffic from outside your network is blocked. Learn more' and a note: 'Note: App Engine firewalls are managed here.' Below this is a search bar and a table of firewall rules. The table has columns: Name, Type, Targets, Filters, Protocols/ports, Action, Priority, and Network. The rules listed are: 'default-allow-http', 'default-allow-https', 'instance-1-egress', 'instance-1-ingress', 'default-allow-icmp', 'default-allow-internal', 'default-allow-rdp', and 'default-allow-ssh'.

Name	Type	Targets	Filters	Protocols/ports	Action	Priority	Network
default-allow-http	Ingress	http-server	IP ranges: 0.0.0.0/0	tcp:80	Allow	1000	default
default-allow-https	Ingress	https-server	IP ranges: 0.0.0.0/0	tcp:443	Allow	1000	default
instance-1-egress	Ingress	Apply to all	IP ranges: 0.0.0.0/0	all	Allow	1000	default
instance-1-ingress	Ingress	Apply to all	IP ranges: 0.0.0.0/0	all	Allow	1000	default
default-allow-icmp	Ingress	Apply to all	IP ranges: 0.0.0.0/0	icmp	Allow	65534	default
default-allow-internal	Ingress	Apply to all	IP ranges: 10.128.0.0/9	tcp:0-65535 udp:0-65535 icmp	Allow	65534	default
default-allow-rdp	Ingress	Apply to all	IP ranges: 0.0.0.0/0	tcp:3389	Allow	65534	default
default-allow-ssh	Ingress	Apply to all	IP ranges: 0.0.0.0/0	tcp:22	Allow	65534	default

5. Give a name of the rule. **Create one rule for ingress traffic and one for egress separately.** Choose “All instances in the network” in Targets. Fill the IP ranges with “0.0.0.0/0” and Choose “Allow all” for protocols and ports. Then click on “Create”.

Screenshot 1: Initial 'Create a firewall rule' form

- Name:** lowercase, no spaces
- Description (Optional):**
- Logs:** On (selected), Off
- Network:** default
- Priority:** 1000
- Direction of traffic:** Ingress (selected), Egress
- Action on match:** Allow (selected), Deny
- Targets:** Specified target tags
- Target tags:**
- Source filter:** IP ranges
- Source IP ranges:** for example, 0.0.0.0/0, 192.168.2.0/24

Screenshot 2: Completed 'Create a firewall rule' form

- Direction of traffic:** Ingress (selected), Egress
- Action on match:** Allow (selected), Deny
- Targets:** Specified target tags
- Target tags:**
- Source filter:** IP ranges
- Source IP ranges:** for example, 0.0.0.0/0, 192.168.2.0/24
- Second source filter:** None
- Protocols and ports:** Allow all (selected), Specified protocols and ports
 - tcp: 20, 50-60
 - udp: all
 - Other protocols: protocols, comma separated, e.g. ssh, scp
- Buttons:** Create, Cancel