Steps to implement Hands-on Project - Mission 1

Amazon Web Services

- Access AWS console and go to IAM service
- Under Access management, Click in "Users", then "Add user" and create a programmatic user "**terraform-en-1**"
- On Set permissions, click on "Attach existing policies directly" button.
- Select AmazonS3FullAccess.
- Click on Next: Tags
- Click on Next: Review
- Click on Create user
- Click on Download .csv
- After download, rename .csv to accessKeys.csv

Google Cloud Platform (GCP)

- CLICK HERE to download the hands-on files.
- Access GCP Console and open Cloud Shell
- Upload accessKeys.csv and .zip hands-on file to GCP Cloud Shell
- Hands-on files preparation

```
mkdir mission1_en mv mission1.zip mission1_en cd mission1_en unzip
mission1.zip mv ~/accessKeys.csv mission1/en cd mission1/en chmod +x *.sh
```

- Run the following commands to prepare AWS and GCP environment. Authorize when asked.

```
./aws_set_credentials.sh accessKeys.csv gcloud config set project
<project_id>
```

- Execute the command below

```
./gcp_set_project.sh
```

- Enable the Container Registry API, Kubernetes Engine API and the Cloud SQL API

```
gcloud services enable containerregistry.googleapis.com gcloud services
enable container.googleapis.com gcloud services enable
sqladmin.googleapis.com
```

IMPORTANT (DO NOT SKIP):

- **Before executing the Terraform commands, open the Google Editor and update the file tcb_aws_storage.tf replacing the bucket name with an unique name (AWS requires unique bucket names).**
  - Open the tcb_aws_storage.tf using Google Editor
  - On line 4 of the file tcb_aws_storage.tf:
    - Replace xxxx with your name initials plus two random numbers: Example: luxxy-covid-testing-system-pdf-en-jr29

- Run the following commands to finish provision infrastructure steps

```
cd ~/mission1_en/mission1/en/terraform/ terraform init terraform plan
terraform apply Type Yes and go ahead.
```

- Once the CloudSQL instance is provisioned, access the Cloud SQL service
- Click on your Cloud SQL instance.

- On the left side, under Primary Instance, click on **Connections**.
- Under **Instance IP assignment**, enable Private IP.
    - Click **Set up Connection** and **Use an automatically allocated IP range in your network**.
    - Click **Continue**
    - Click **Create Connection** and **wait a minutes.**
- Under **Associated networking**, select "Default"
- Under **Authorized Networks**, click "Add Network".
- Under **New Network**, enter the following information:
    - **Name:** Public Access (For testing purposes only)
    - Network:** 0.0.0.0/0
    - Click **Done**.

PS: For production environments, it is recommended to use only the Private Network for database access.
⚠️ Never grant public network access (0.0.0.0/0) to production databases.

- After that, click on Save and wait to conclude the update.