Andrea M. Stojanovski

Final assignment HW3

Part 0 – Everything is running

Part 1 - Secrets

The first task is to identify where the secrets are unsafely stored. To do this I inspected the files visually (there just a few) and discovered
1. MYSQL_ROOT_PASSWORD in ./db/k8/db-deployment.yaml
2. MYSQL_ROOT_PASSWORD in ./GiftcardSite/k8/django-deploy.yaml
3. SECRET_KEY in ./GiftcardSite/GifcardSite/settings.py

Then generated Kubernetes secrets and put them in the yaml files in the same order:
1. ./db/k8/secret-db.yaml for MYSQL_ROOT_PASSWORD
2. ./GiftcardSite/k8/secret-db.yaml for MYSQL_ROOT_PASSWORD (this should be linked to the above for single source of truth - I ignore this for the homework)
3. ./GiftcardSite/k8/secret-key.yaml for SECRET_KEY

Then modified the files in the first group to refer to the secrets in the second group.

MYSQL_ROOT_PASSWORD=thisisatestthing.
$ echo -n 'thisisatestthing.' | base64
Translated to base64: dGhpc2lzYXRlc3R0aGluZy4=

SECRET_KEY=kmgysa#fz+9(z1*=c0ydrjizk*7sthm2ga1z4=^61$cxcq8b$l
$ echo -n 'kmgysa#fz+9(z1*=c0ydrjizk*7sthm2ga1z4=^61$cxcq8b$l' | base64
Tranlated to base64:
a21neXNhI2Z6KzkoejEqPWMweWRyaml6ayo3c3RobTJnYTF6ND1eNjEkY3hjcThiJGw=

Finally, I put references to these secrets in the pod environments.
This is in files in the first group above.

To push the secrets:
$ kubectl apply -f ./db/k8/secret-db.yaml
$ kubectl apply -f ./GiftcardSite/k8/secret-db.yaml
$ kubectl apply -f ./GiftcardSite/k8/secret-key.yaml

Part 2 – Migration

I created a directory migr-utils where the seed.yaml and migrate.yaml are.

The containers db-migr and db-seed are copies of the original db container. I am sure this can be optimized, but this may be an overkill for an operation that is not frequent.

The admin username and password were also exposed, so I created another secret: secret-admin.yaml.

Before running these utils we have to apply the secret:

kubectl apply ./migr-utils/secret-admin.yaml

The commands are:

kubectl apply -f migrate.yaml

and

kubectl apply -f seed.yaml

Most if it is copied from manual experimentation inside the pods using $ kubectl exec -it …

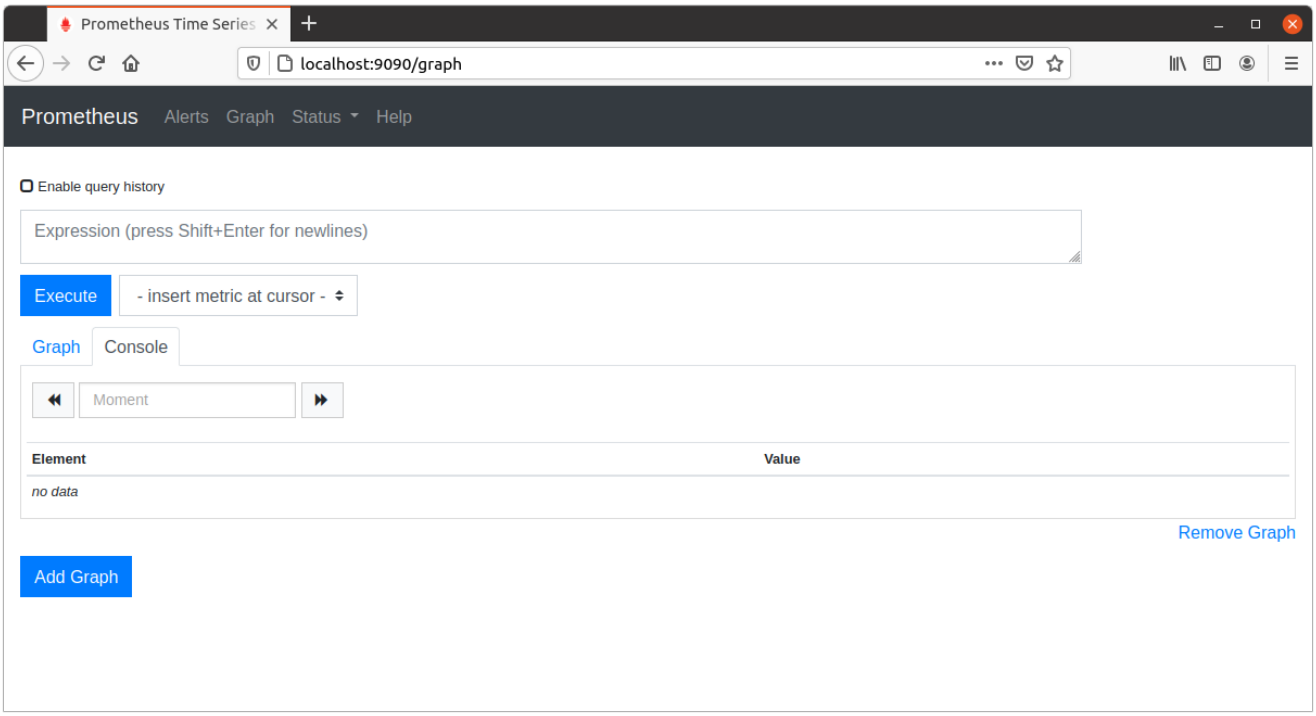
Part 3 – Monitoring

Unsafe monitoring is in views.py. Removed all lines after 16.

Added 404 error monitoring in the same place.

Installed prometheus:

sudo apt install prometheus



Prometheus installed. It has a lot of possibilities. I am pulling a configuration file off internet and trying to modify it to our needs…

To run the server:

```
./prometheus –config.file=prometheus.yml
```

Now we should put Prometheus in its own instance.