Kubernetes

Kubernetes June – 2022

Homework
Security and Policies

Stefan Veselinov

Tasks *

Note: Due to technicle issues with my main working pc, tasks are done with kind :(

```
Operating System: Debian GNU/Linux 11 (bullseye)
          Kernel: Linux 5.10.0-15-amd64
    Architecture: x86-64
```

```
vox@vox:~/SoftUni/kubernetes/M3_Security_And_Policies/homework$ free -m
               total        used        free      shared  buff/cache   available
Mem:            3781        2849         186         188         745         510
Swap:            974         974           0
```

```
model name      : Intel(R) Celeron(R) CPU  N3060  @ 1.60GHz
stepping        : 4
microcode       : 0x411
cpu MHz         : 480.000
cache size      : 1024 KB
physical id     : 0
siblings        : 2
core id         : 2
cpu cores       : 2
```

PREP: Create cluster

```
vox@vox:~/SoftUni/kubernetes/M3_Security_And_Policies/homework$ kind create cluster --config cluster.yaml --name homework
Creating cluster "homework" ...
 ✓ Ensuring node image (kindest/node:v1.24.0) 🖼
 ✓ Preparing nodes 📦 📦 📦
 ✓ Writing configuration 📜
 ✓ Starting control-plane 🕹️
 ✓ Installing CNI 🔌
 ✓ Installing StorageClass 💾
 ✓ Joining worker nodes 🚜
Set kubectl context to "kind-homework"
```

```
vox@vox:~/SoftUni/kubernetes/M3_Security_And_Policies/homework$ kubectl cluster-info --context kind-homework
Kubernetes control plane is running at https://127.0.0.1:34405
CoreDNS is running at https://127.0.0.1:34405/api/v1/namespaces/kube-system/services/kube-dns:dns/proxy
```

1. Create and register two Kubernetes uses – Ivan (ivan) and Mariana (mariana) who are part of the Gurus (gurus) group

- copy create-kube-user.sh to control plane

```
vox@vox:~/SoftUni/kubernetes/M3_Security_And_Policies/homework$ docker ps -a
CONTAINER ID   IMAGE                  COMMAND                  CREATED          STATUS                      PORTS                                                  NAMES
fd16e72bf529   kindest/node:v1.24.0   "/usr/local/bin/entr…"   40 minutes ago   Up 40 minutes               127.0.0.1:34405->6443/tcp, 0.0.0.0:8080->30001/tcp     homework-control-plane
d1d34226036f   kindest/node:v1.24.0   "/usr/local/bin/entr…"   40 minutes ago   Up 40 minutes                                                              homework-worker
2e03eb6ab77a   kindest/node:v1.24.0   "/usr/local/bin/entr…"   40 minutes ago   Up 40 minutes                                                              homework-worker2
653e8a668970   dohsimpson/weasyprint:51   "/bin/sh -c sh"          44 hours ago     Exited (137) 44 hours ago                                                  weasy
vox@vox:~/SoftUni/kubernetes/M3_Security_And_Policies/homework$ docker cp create-kube-user.sh fd16e72bf529:/create-kube-user.sh
vox@vox:~/SoftUni/kubernetes/M3_Security_And_Policies/homework$ docker exec -it fd1 bash
root@homework-control-plane:/# ls -la
total 64
drwxr-xr-x   1 root root 4096 Jun 29 14:04 .
drwxr-xr-x   1 root root 4096 Jun 29 14:04 ..
-rwxr-xr-x   1 root root    0 Jun 29 13:23 .dockerenv
lrwxrwxrwx   1 root root    7 Apr 28 00:14 bin -> usr/bin
drwxr-xr-x   2 root root 4096 Oct 11  2021 boot
-rw-r--r--   1 1000 1000 1176 Jun 29 14:01 create-kube-user.sh
drwxr-xr-x  15 root root 3340 Jun 29 13:23 dev
```

- execute create-kube-user.sh in control plane

```
root@homework-control-plane:/# ./create-kube-user.sh ivan gurus homework
Add user
Create group
Add user to group
Create a folder for the certificate
Create a private key
Generating RSA private key, 2048 bit
...............+++++
.+++++
e is 65537 (0x010001)
Create a certificate signing request
Sign the CSR with the Kubernetes CA
Signature ok
subject=CN = ivan
Getting CA Private Key
Create the user in Kubernetes
User "ivan" set.
Create context for the user as well
Context "ivan-context" created.
Create a folder to store the user co
Create a copy of config
Change ownership
```

```
root@homework-control-plane:/# ./create-kube-user.sh mariana gurus homework
Add user
Create group
groupadd: group 'gurus' already exists
Add user to group
Create a folder for the certificate related files
Create a private key
Generating RSA private key, 2048 bit long modulus (2 primes)
.....................................................................................
.....................................+++++
e is 65537 (0x010001)
Create a certificate signing request
Sign the CSR with the Kubernetes CA certificate
Signature ok
subject=CN = mariana
Getting CA Private Key
Create the user in Kubernetes
User "mariana" set.
Create context for the user as well
Context "mariana-context" created.
Create a folder to store the user configuration
Create a copy of config
Change ownership
```

- edit users .kube/config

```
apiVersion: v1
clusters:
- cluster:
    certificate-authority-data: LS0tLS1CRUdJTiBDRVJUSUZJQ0FURS
    server: https://homework-control-plane:6443
  name: homework
contexts:
- context:
    cluster: homework
    user: mariana
  name: mariana-context
current-context: mariana-context
kind: Config
preferences: {}
users:
- name: mariana
  user:
    client-certificate: /home/mariana/.certs/mariana.crt
    client-key: /home/mariana/.certs/mariana.key
```

- seting up user

```
mariana@homework-control-plane:/$ kubectl get nodes
error: error loading config file "/etc/kubernetes/admin.conf": open /etc/kubernetes/admin.conf: permission denied
mariana@homework-control-plane:/$
mariana@homework-control-plane:/$
mariana@homework-control-plane:/$ export KUBECONFIG="${HOME}/.kube/config"
mariana@homework-control-plane:/$ kubectl get nodes
Error from server (Forbidden): nodes is forbidden: User "mariana" cannot list resource "nodes" in API group "" at the cluster scope
```

2. Create a namespace named projectx

```
root@homework-control-plane:/# kubectl create namespace projectx
namespace/projectx created
root@homework-control-plane:/# kubectl get namespaces
NAME                 STATUS   AGE
default              Active   63m
kube-node-lease      Active   63m
kube-public          Active   63m
kube-system          Active   63m
local-path-storage   Active   63m
projectx             Active   6s
```

3. Create a LimitRange for the namespace to set defaults, minimum and maximum both for CPU and memory (use values that you consider suitable)

```
vox@vox:~/SoftUni/kubernetes/M3_Security_And_Policies/homework$ kubectl apply -f limit-range.yaml
limitrange/projectx-limits created
```

4. Create a ResourceQuota for the namespace to set requests and limits both for CPU and memory (use values that you consider suitable). In addition, add limits for pods, services, deployments, and replicasets (again, use values that you find appropriate)

```
vox@vox:~/SoftUni/kubernetes/M3_Security_And_Policies/homework$ kubectl apply -f resource-quota.yaml
resourcequota/projectx-quota configured
```

5. Create a custom role (devguru) which will allow the one that has it to do anything with any of the following resources pods, services, deployments, and replicasets. Grant the role to ivan and mariana (or to the group they belong to) for the namespace created earlier

```
vox@vox:~/SoftUni/kubernetes/M3_Security_And_Policies/homework$ kubectl apply -f devguru-role.yaml
role.rbac.authorization.k8s.io/devguru created
```

```
vox@vox:~/SoftUni/kubernetes/M3_Security_And_Policies/homework$ kubectl create rolebinding devguru-role --role=devguru --namespace=projectx
rolebinding.rbac.authorization.k8s.io/devguru-role created
```