

Maryam Taherzadeh

week 11 homework

19529

Q4 ==> 7.5. Using Secrets to pass sensitive data to containers

- Introducing the default token Secret
- **Kubectl get secrets**

```
Welcome to Cloud Shell! Type "help" to get started.  
Your Cloud Platform project in this session is set to phonic-axle-307118.  
Use "gcloud config set project [PROJECT_ID]" to change to a different project.  
taherzadeh19529@cloudshell:~ (phonic-axle-307118)$ kubectl get secrets  
NAME          TYPE           DATA   AGE  
default-token-ct8sw  kubernetes.io/service-account-token  3      4h22m  
taherzadeh19529@cloudshell:~ (phonic-axle-307118)$
```

kubectl describe secrets

```
taherzadeh19529@cloudshell:~ (phonic-axle-307118)$ kubectl describe secrets  
Name:         default-token-ct8sw  
Namespace:    default  
Labels:       <none>  
Annotations:  kubernetes.io/service-account.name: default  
              kubernetes.io/service-account.uid: e4c94af3-7e26-4f8b-b3b6-7f75e5cb7777  
Type:        kubernetes.io/service-account-token  
  
Data  
=====  
ca.crt:     1159 bytes  
namespace:  7 bytes  
token:      eyJhbGciOiJSUzI1NiIsImtpZCI6IzXuktHOGxmNk5UczFLMHPmQWhqd1hpdkVjehJPYm0TzFKQUppYYThfdzAifQ .eyJpc3MiOiJrdWJlcem5ldGVzL3NlcnZpY2VhY2NvdW50Iiwi a3ViZXJuZXrlcy5pbvy9zZXJ2aWN1YWNjb3VldG9uYW1lc3BhY2UiO1JxkZWzhdwk07ivia3ViZXJuZxplcypby0xZXJ2aWN1YWNjb3VldG9uZWNvZXQubmFtZCI6imRlZmF1bHQtdC9r2WAtV3Q4c3eiLCJrdWJlcem51dGVzLmlvL3NlcnZpY2VhY2NvdW50I5N1cnZpY2UtiYWNjb3VldG9uYW1lIjo1ZGVmYXVdcIsImtlYmvYbmV0ZXhuaW8vc2VydmljZWFjY291bnQvc2VydmljZS1hY2NvdW50LvpZC16InU0YzX0YwYzLTd1MjYtNGY4Yi1iM212LTdmNzV1NWN1Nzc3NyisInN1Yi16InN5c3RlbTpzZXJ2aWN1YWNjb3VudG5uYWh0Om0RlZmf1bRQlfQ .voYVhQEd5tKZGpLJUJtc70V3h8mcM593XFb-dh_GgCRVcWh7-Dla876a0ucx-N5T2AteLRQw1RHmZGACMuDA9r9 siT2115JkcxOhLzdvdo5 -yG9gmsmpBtCah-QdRlKzSpNRb146gEHc6w7dbQKq8E3h2R6p3v0SwansJ1IN4NuucuNPdfd4-oYfSQj1gAGjUXZssFVuqx1n5aGXe3Er_Fo1CVigzMqryea_rKlqVtNtwUw1F7LR1OZdr5TN9w1O2_SejQW61Rs_6sqik4iryd4-55dlq9r9drZ9ro4VUqh3qVB6G6pGEVt2q3515nFir7ugrFlaxsvWOEA  
taherzadeh19529@cloudshell:~ (phonic-axle-307118)$
```

-**kubectl get po**

-**kubectl exec fortune-configmap-volume ls /var/run/secrets/kubernetes.io/serviceaccount/**

```
taherzadeh19529@cloudshell:~ (phonic-axle-307118)$ kubectl get po
NAME                   READY   STATUS    RESTARTS   AGE
fortune-args-from-configmap   2/2     Running   0          3h51m
fortune-configmap-volume     2/2     Running   0          106m
fortune-configmap-volume-with-items 2/2     Running   0          130m
taherzadeh19529@cloudshell:~ (phonic-axle-307118)$ kubectl exec fortune-configmap-volume ls /var/run/secrets/kubernetes.io/serviceaccount/
kubectl exec [POD] [COMMAND] is DEPRECATED and will be removed in a future version. Use kubectl exec [POD] -- [COMMAND] instead.
Defaulting container name to html-generator.
Use 'kubectl describe pod/fortune-configmap-volume -n default' to see all of the containers in this pod.
ca.crt
namespace
token
```

- Creating a Secret

-**openssl genrsa -out https.key 2048**

```
taherzadeh19529@cloudshell:~ (phonic-axle-307118)$ openssl genrsa -out https.key 2048
Generating RSA private key, 2048 bit long modulus (2 primes)
.....+++++
.....+++++
e is 65537 (0x010001)
```

-**openssl req -new -x509 -key https.key -out https.cert -days 3650 -subj /CN=www.kubia-example.com**

```
taherzadeh19529@cloudshell:~ (phonic-axle-307118)$ openssl req -new -x509 -key https.key -out https.cert -days 3650 -subj /CN=www.kubia-example.com
taherzadeh19529@cloudshell:~ (phonic-axle-307118)$ echo bar >foo
taherzadeh19529@cloudshell:~ (phonic-axle-307118)$ kubectl create secret generic fortune-https \
>   --from-file=https.key \
>   --from-file=https.cert \
>   --from-file=foo
secret/fortune-https created
taherzadeh19529@cloudshell:~ (phonic-axle-307118)$
```

```
taherzadeh19529@cloudshell:~ (phonic-axle-307118)$ kubectl get secrets
NAME          TYPE        DATA   AGE
default-token-ct8sw  kubernetes.io/service-account-token  3      5h10m
fortune-https   Opaque      3      33m
taherzadeh19529@cloudshell:~ (phonic-axle-307118)$
```

- Comparing ConfigMaps and Secrets

```
uid: 2d5516c8-5b44-4f91-8906-30ala78b37c0
taherzadeh19529@cloudshell:~ (phonic-axle-307118)$ kubectl get secret fortune-https -o yaml
apiVersion: v1
data:
  foo: YmfYcG==

  https.certificate: LS01LS1CRU4J71BDRVJUSUZQ0FUR801L80C1K1JSURJVENDQWdc0F2E3UBjZ01VZV1Z1ZzznZUHNIVN3c0t1k0kvY1Z3RvUw0d0RRWv2l0l1pJzHgJ7kFR8UwKQ1FBd
Q1EWwNQndTTFWUfFd1ZMwQpTc1Mw1lzbhMwV1Y0Wnxz42JWwXZMw1J0P1U1WwEBSXmHkF7T1tReaDgQV1sT120wEwRfTXmNFT7FwBw5Xu1dPwv536Hr7Z1lCd4dwMVwVQw1dVmQz
ZDNwBxNdx1sabXvF2v/F3CmJHWXZMw1J0ULJ0k1q05C2ZtxaGtRz13M5-JDUVVGQPF0FREBfNSU1CQ2l0fFRUE1EfkonPoau1YXMu5t0G0x1s3pwSTF7VFMwF5FJM22zNkg
ONP3iznXVn8OUVE4NZEpxzAtTxVJUqpwVBN0szYnVwawv5kdh4pM001lmpNWdgtYmtKcJwvZ5EsS2ZzOpH1T0x0M40s21l1t14PGCMwza2TdnasVv53JLTQ1NwtMTFwV01lCm
h3RDF3UmYQzd5exNZEcxTS1Sc0Vaq1j15R251N03C1NwWp1O3k1Ohb18v8y91K1Bi1YlFn0USE1UOXTKaW1JcXhM3FnEqN1Y3d(e1lGU1Z3QVFSGVhd0t1DXbuSkx1amZxGtHn
yHam2Gv1tY1c2We6l1bF1VV-Es4apDx0wdr98VkvXyTV66ikhNWFl1lenhvzZ2R5Y2GxGaJhshbDmC3nM2z9PmVEVocd1j5JHNC11xV3jocnfpa0DEyTRyndJBEFQJU1hM13
VVRBZEJnT1Z1UTRFRMdRvURFUv1.60mbnvqTc1Z1TnP1Xh1Q1Uz1bEzENHFRXcSHz2RFSZMpcQm43Rm9yURFUv1.60qvvTc1Z1TnP1Xh1Q1Uz1bEzENHFRXcDEd11EV1wFvTfRSCSCCVV3Qxd
FGqovekFOQmdrcWhraUcd5dBCQVFr2kF8T0NBuUUVBbjRPTG8wR2437ENDcG5vYXVDDwWWTUhoeG52bmwxSKNEML1d0CmFc0JUW91IRF2oE1nMs1V68Cv3b1v0zExjV0VpdvBvTfAx0U11ZX
kvT1V1UEhd1dF2ZzddqHgqwa0pFWHb528KQXdybXh3b1vc1JPW1M2MVf2WkxFY1B2WF1xRV24ZEFmWx0c05ZzzJHHRVUS1pJdJdoyTxhZUzpTm5vOVFkdwEa1arSHZEEznAwk09EnVR
3FtnzMFtFFHTVNLakpRd09beUhNzLmncV2zXWD2aWh1v3dYHkV4Mj2sdD2pcM61d29KM2zaeHTJldkttaKQmmp5YXMoTHFy3J3LkVCKxExwHplMl0rdG0xdE13bVdhYS9wMhHfZT1n
SC91MYKZKX4KNUd1RkpxXjZBjBuCVVleFN1t7QWQWfQrOsakhuY1AraWJRHd1b0tBRWmNTX-9Pqt1S0t1UVORCBDRVJUSUZQfQfURS0t1LS0tCg==
  https.key: LS0tIS1CRUdJ1BSU0EgUFJJKVFKURVktLS0tQgNSU1FQEFQKFBS0NBUUVNURBZJxJdtgRNWJDm5t0Gokb3pw5TdFwHfWePRJM2RzNxgOn1p1zNvxVnBoUEV4Cj
  https.certificate: LS0tIS1CRUdJ1BSU0EgUFJJKVFKURVktLS0tQgNSU1FQEFQKFBS0NBUUVNURBZJxJdtgRNWJDm5t0Gokb3pw5TdFwHfWePRJM2RzNxgOn1p1zNvxVnBoUEV4Cj
BucVlVeI1TU1Q9WfQgK0RsakhuY1AraWJRHd1b0tBRWmNTX-9Pqt1S0t1UVORCBDRVJUSUZQfQfURS0t1LS0tCg==
  https.key: LS0tIS1CRUdJ1BSU0EgUFJJKVFKURVktLS0tQgNSU1FQEFQKFBS0NBUUVNURBZJxJdtgRNWJDm5t0Gokb3pw5TdFwHfWePRJM2RzNxgOn1p1zNvxVnBoUEV4Cj
  https.certificate: LS0tIS1CRUdJ1BSU0EgUFJJKVFKURVktLS0tQgNSU1FQEFQKFBS0NBUUVNURBZJxJdtgRNWJDm5t0Gokb3pw5TdFwHfWePRJM2RzNxgOn1p1zNvxVnBoUEV4Cj
  https.key: LS0tIS1CRUdJ1BSU0EgUFJJKVFKURVktLS0tQgNSU1FQEFQKFBS0NBUUVNURBZJxJdtgRNWJDm5t0Gokb3pw5TdFwHfWePRJM2RzNxgOn1p1zNvxVnBoUEV4Cj
  https.certificate: LS0tIS1CRUdJ1BSU0EgUFJJKVFKURVktLS0tQgNSU1FQEFQKFBS0NBUUVNURBZJxJdtgRNWJDm5t
```

- Using the Secret in a pod

```
taherzadeh19529@cloudshell:~ (phonic-axle-307118)$ kubectl edit configmap fortune-config
configmap/fortune-config edited
taherzadeh19529@cloudshell:~ (phonic-axle-307118)$ kubectl describe configmap fortune-config
Name:           fortune-config
Namespace:      default
Labels:         <none>
Annotations:   <none>
Data
=====
my-nginx-config.conf:
----  
server {
    listen          80;
    listen          443 ssl;
    server_name    www.kubia-example.com;
    ssl_certificate certs/https.cert;
    ssl_certificate_key certs/https.key;
    ssl_protocols   TLSv1 TLSv1.1 TLSv1.2;
    ssl_ciphers     HIGH:!aNULL:!MD5;

    location / {
        root   /usr/share/nginx/html;
        index  index.html index.htm;
    }
}

sleep-interval:
----  
25
Events:  <none>
```

```
taherzadeh19529@cloudshell:~ (phonic-axle-307118)$ vim fortune-pod-https.yaml
taherzadeh19529@cloudshell:~ (phonic-axle-307118)$ cat fortune-pod-https.yaml
apiVersion: v1
kind: Pod
metadata:
  name: fortune-https
spec:
  containers:
  - image: taherzadeh19529/fortune
    name: html-generator
    env:
    - name: INTERVAL
      valueFrom:
        configMapKeyRef:
          name: fortune-config
          key: sleep-interval
    volumeMounts:
    - name: html
      mountPath: /var/www/html
  - image: nginx:alpine
    name: web-server
    volumeMounts:
    - name: html
      mountPath: /usr/share/nginx/html
      readOnly: true
    - name: config
      mountPath: /etc/nginx/conf.d
      readOnly: true
    - name: certs
      mountPath: /etc/nginx/certs/
      readOnly: true
  ports:
  - containerPort: 80
  - containerPort: 443
  volumes:
  - name: html
    emptyDir: {}
```

```
taherzadeh19529@cloudshell:~ (phonic-axle-307118)$ kubectl create -f fortune-pod-https.yaml
pod/fortune-https created
taherzadeh19529@cloudshell:~ (phonic-axle-307118)$ kubectl get po
NAME                      READY   STATUS    RESTARTS   AGE
fortune-args-from-configmap   2/2     Running   0          4h26m
fortune-configmap-volume      2/2     Running   0          142m
fortune-configmap-volume-with-items 2/2     Running   0          165m
fortune-https                 2/2     Running   0          8s
taherzadeh19529@cloudshell:~ (phonic-axle-307118)$ █
```

```
taherzadeh19529@cloudshell:~ (phonic-axle-307118)$ kubectl port-forward fortune-https 8443:443 &
[1] 1204
taherzadeh19529@cloudshell:~ (phonic-axle-307118)$ Forwarding from 127.0.0.1:8443 -> 443
```

Create a new cloudshell terminal:

- Understanding secret volumes are stored in memory

```
taherzadeh19529@cloudshell:~ (phonic-axle-307118)$ kubectl exec fortune-https -c web-server -- mount | grep certs  
tmpfs on /etc/nginx/certs type tmpfs (ro,relatime)  
taherzadeh19529@cloudshell:~ (phonic-axle-307118)$
```

-image pull Secrets

- Creating a Secret for authenticating with a Docker registry

```
taherzadeh19529@cloudshell:~ (phonic-axle-307118)$ docker login  
Authenticating with existing credentials...  
WARNING! Your password will be stored unencrypted in /home/taherzadeh19529/.docker/config.json.  
Configure a credential helper to remove this warning. See  
https://docs.docker.com/engine/reference/commandline/login/#credentials-store  
Login Succeeded
```

- Using the docker-registry Secret in a pod definition

```
apiVersion: v1  
kind: Pod  
metadata:  
  name: private-pod  
spec:  
  imagePullSecrets:  
  - name: mydockerhubsecret  
  containers:  
  - image: taherzadeh19529/fortune  
    name: main
```

```
taherzadeh19529@cloudshell:~ (phonic-axle-307118)$ vim pod-with-private-image.yaml
taherzadeh19529@cloudshell:~ (phonic-axle-307118)$ cat pod-with-private-image.yaml
apiVersion: v1
kind: Pod
metadata:
  name: private-pod
spec:
  imagePullSecrets:
  - name: mydockerhubsecret
  containers:
  - image: tahezadeh19529/fortune
    name: main
taherzadeh19529@cloudshell:~ (phonic-axle-307118)$
```

```
  name: main
taherzadeh19529@cloudshell:~ (phonic-axle-307118)$ kubectl create -f pod-with-private-image.yaml
pod/private-pod created
taherzadeh19529@cloudshell:~ (phonic-axle-307118)$
```

```
taherzadeh19529@cloudshell:~ (phonic-axle-307118)$ kubectl get po
NAME          READY   STATUS    RESTARTS   AGE
fortune-args-from-configmap   2/2     Running   0          4h32m
fortune-configmap-volume      2/2     Running   0          147m
fortune-configmap-volume-with-items  2/2     Running   0          171m
fortune-https                 2/2     Running   0          5m56s
private-pod                  1/1     Running   0          7s
taherzadeh19529@cloudshell:~ (phonic-axle-307118)$ kubectl get po
NAME          READY   STATUS    RESTARTS   AGE
fortune-args-from-configmap   2/2     Running   0          4h32m
fortune-configmap-volume      2/2     Running   0          147m
fortune-configmap-volume-with-items  2/2     Running   0          171m
fortune-https                 2/2     Running   0          6m5s
private-pod                  1/1     Running   0          16s
taherzadeh19529@cloudshell:~ (phonic-axle-307118)$
```