**Assignment 23 – Kubernetes Test Questions 12**

Date: 30 May 2024

Name: Mohamad Haffiz Bin Mohd Hissham

**Questions:**

1.

Create a pod named **secretpod1**, using image **nginx**.

* Setup the secret **secret1** as a **volume mount** on the pod at path **/etc/secret1**
* **Verify** that the **secret** was created with the **correct data**

2.

Create a **yaml file** to create a secret named **secret2**, with key value pairs

* **user2=my\_user2**
* **password2=P@ssword2**

**Verify** that the secret was created with the **correct** **data**

**References:**

* [Secrets | Kubernetes](https://kubernetes.io/docs/concepts/configuration/secret/#docker-config-secrets)
* [Managing Secrets using kubectl | Kubernetes](https://kubernetes.io/docs/tasks/configmap-secret/managing-secret-using-kubectl/)
* [ConfigMaps | Kubernetes](https://kubernetes.io/docs/concepts/configuration/configmap/)

**Question 1:**

1. Create a secret **secret1**, **kubectl create secret generic secret1 --from-literal=username=my\_user1**
   1. A screen shot of a computer

      Description automatically generated
2. Create a YAML file for **secretpod1**, **nano secretpod1.yaml**
   1. Apply the YAML file written, **k apply -f secretpod1.yaml**

apiVersion: v1

kind: Pod

metadata:

  name: secretpod1

spec:

  containers:

    - name: pod

      image: nginx

      command: ['sh', '-c', 'cat /etc/secret1/username && sleep 3600']

      volumeMounts:

        - name: secret-volume

          mountPath: /etc/secret1

          readOnly: true

  volumes:

    - name: secret-volume

      secret:

        secretName: secret1

* 1. A screen shot of a computer

     Description automatically generated

1. Verify that the secret created. View username **via** **exec command**, **kubectl exec -it secretpod1 -- cat /etc/secret1/username**
   1. A black background with white text

      Description automatically generated

**Question 2:**

1. Create a **YAML file** to **create a secret** named **secret2**, **nano 2.yaml**

apiVersion: v1

kind: Secret

metadata:

  name: secret2

type: Opaque

data:

  user2: bXlfdXNlcjI=

  password2: UEBzc3dvcmQy

* 1. **bXlfdXNlcjI=** is my\_user2 in base64
  2. **bXlfdXNlcjI=** is P@ssword2 in base64

1. Verify that the secret. View the **username2** and **password2** created
   1. A screen shot of a computer

      Description automatically generated
   2. A screenshot of a computer

      Description automatically generated
   3. **kubectl get secret secret2 -o yaml**
      1. A computer screen shot of a black screen

         Description automatically generated
   4. Or use **JSONPath** to view the user2 and password2 created
      1. **kubectl get secret secret2 -o jsonpath='{.data.password2}' | base64 –decode**
      2. **controlplane $ kubectl get secret secret2 -o jsonpath='{.data.user2}' | base64 --decode**
      3. A screenshot of a computer program

         Description automatically generated