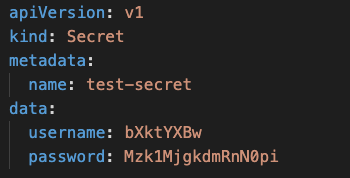
Lab 6.4 Using Secrets

1. Encode username and password

**echo -n 'john@gmail.com' | base64**

**echo -n 'password' | base64**

1. Create a secrets.yml file as below:



1. Create the Secret

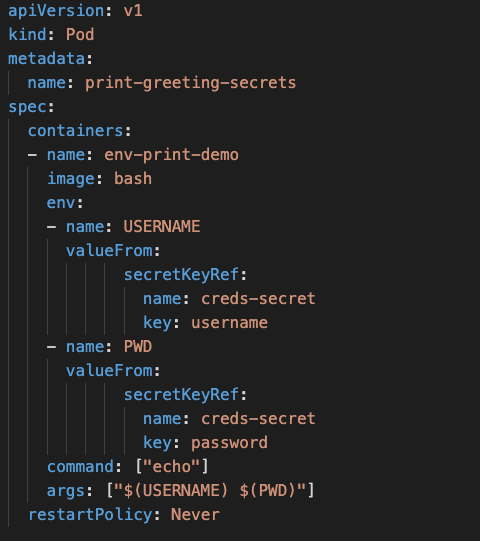
**kubectl create -f secrets.yml**

1. Check the Secret that got created

**kubectl get secrets**

**kubectl describe secret/creds-secret**

1. Create a pod-definition.yml file as below

****

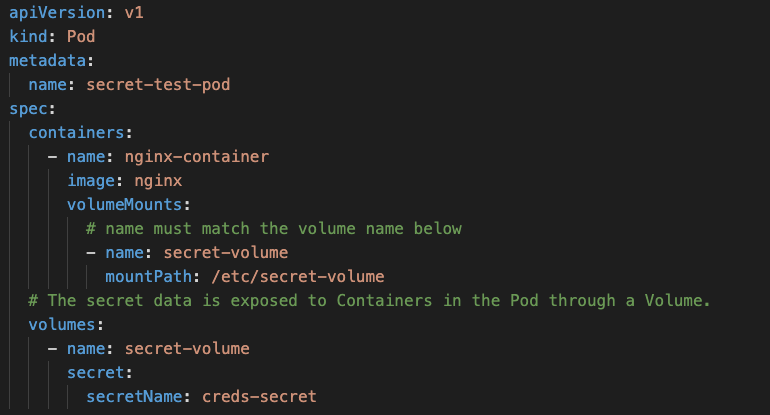
1. Create the pod

**kubectl create -f pod-definition.yml**

1. Check the Logs

**kubectl logs -f print-greeting-secrets**

1. A pod can also access secrets data through a Volume. Create another pod using pod2-definition.yml file

****

1. Create the Pod

**kubectl create -f pod2—definition.yml**

1. Check If the pod is created successfully

**kubectl get pods**

1. Get a shell into the Container that is running in your Pod:

**kubectl exec -it secret-test-pod -- /bin/bash**

1. The secret data is exposed to the Container through a Volume mounted under /etc/secret-volume. In your shell, list the files in the /etc/secret-volume directory:

**ls /etc/secret-volume**

1. In your shell, display the contents of the username and password files:

**echo "$( cat /etc/secret-volume/username )"**

**echo "$( cat /etc/secret-volume/password )"**