

You don’t want sensitive information such as a database password or an keys kept around in clear text. Secrets provides you with a mechanism to use such information in a safe and reliable way with the following properties:

**SSH to your AWS Workstation**

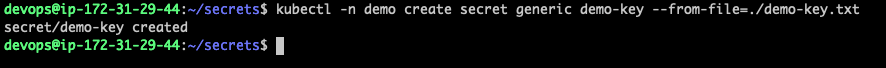
**ssh devops@<public-ip-addr**> of your Workstation  
Password is : **Dev0p$!!/**

**Replace <your-name> with your name throughout the lab.**

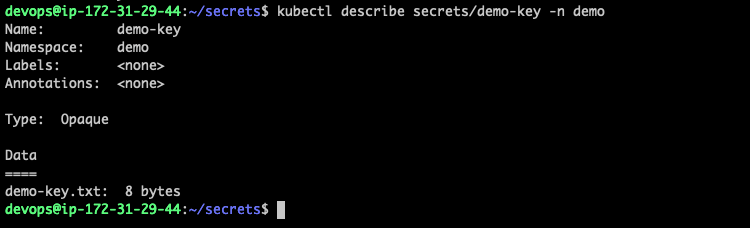
1. Create a secret key that holds a (made-up) key:

Update the “**PASSWORD**” with a desired password and <your-name> with your name.

|  |
| --- |
| $ mkdir /home/devops/secrets  $ cd /home/devops/secrets  $ echo -n "PASSWORD" > ./<your-name>-key.txt  $ kubectl -n <your-name> create secret generic <your-name>-key --from-file=./<your-name>-key.txt |



|  |
| --- |
| $ kubectl describe secrets/<your-name>-key -n <your-name> |

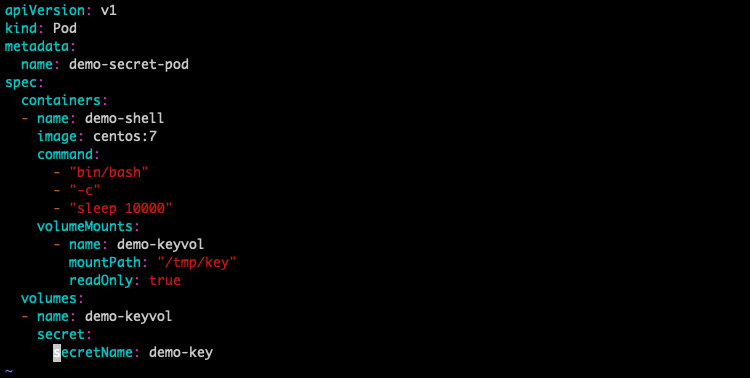


2. Now, Create a deployment object for the

|  |
| --- |
| $ vim <your-name>-pod.yaml |

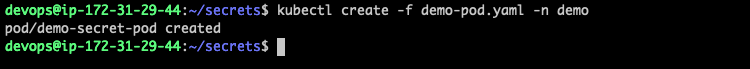
Paste the content below to the <your-name>-pod.yaml

|  |
| --- |
| apiVersion: v1 kind: Pod metadata:  name: <your-name>-secret-pod spec:  containers:  - name: <your-name>-shell  image: centos:7  command:  - "bin/bash"  - "-c"  - "sleep 10000"  volumeMounts:  - name: <your-name>-keyvol  mountPath: "/tmp/key"  readOnly: true  volumes:  - name: <your-name>-keyvol  secret:  secretName: <your-name>-key |

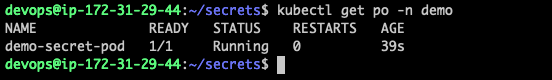


3. Create the POD by running the below command.

|  |
| --- |
| $ kubectl create -f <your-name>-pod.yaml -n <your-name> |

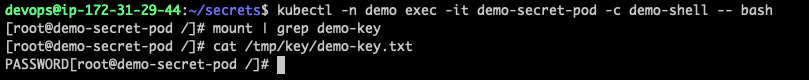


|  |
| --- |
| $ kubectl get po -n <your-name> |



4. Exec into the Container and run the below commands.

|  |
| --- |
| $ kubectl -n <your-name> exec -it <your-name>-secret-pod -c <your-name>-shell -- bash [root@demo-secret-pod /]# mount | grep <your-name>-key [root@demo-secret-pod /]# cat /tmp/key/<your-name>-key.txt |



We can Observe that the secret {PASSWORD} was copied to the pod in the above screenshot.

5. To exit out of the Container type

|  |
| --- |
| [root@demo-secret-pod /]# exit |

Note that for service accounts Kubernetes automatically creates secrets containing credentials for accessing the key and modifies your pods to use this type of secret.

6. You can remove both the pod and the secret with:

|  |
| --- |
| $ kubectl -n <your-name> delete pod/<your-name>-secret-pod secret/<your-name>-key |

