Lab 15: RBAC

Training Goals Covered:

- Define a Role and RoleBinding for pods view only.
- Explore the behaviour.

Steps:

1. Create a Service Account to represent a user. The Service Account should be defined as bob.

Shell

```
kubectl create serviceaccount bob
```

2. Create a Role defining the only actions to be performed on pods are get, list and watch.

Shell

```
apiVersion: rbac.authorization.k8s.io/v1
kind: Role
metadata:
  namespace: default
  name: pod-viewer
rules:
- apiGroups: [""]
  resources: ["pods"]
  verbs: ["get","list","watch"]
```

3. Create a RoleBinding to bind the Service Account to the defined Role.

Shell

```
apiVersion: rbac.authorization.k8s.io/v1
kind: RoleBinding
metadata:
  name: read-pods-bob
  namespace: default
subjects:
- kind: ServiceAccount
  name: bob
  namespace: default
roleRef:
  kind: Role
  name: pod-viewer
  apiGroup: rbac.authorization.k8s.io
```

4. Use the command **kubectl auth can-i** to explore the permissions defined.

Shell

```
kubectl auth can-i list pods --as=system:serviceaccount:default:bob
```

→ *Can Bob list pods?* **Yes**

Shell

```
kubectl auth can-i delete pods --as=system:serviceaccount:default:bob
```

→ *Can Bob list pods?* **No**

Shell

```
kubectl auth can-i get secrets --as=system:serviceaccount:default:bob
```

→ *Can Bob view Secrets?* **No**

5. Delete Resources.