Module 5: Securing the Cluster

MCQ Scenarios

Module – 5

[Scenario - 1]

Consider the following yaml file for a cluster role

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

[Scenario - 2]

Consider the following yaml file snippet for a RoleBinding

```
subjects:
- kind: Group
  name: system:serviceaccounts:frontend
  apiGroup: rbac.authorization.k8s.io
```


[Scenario - 3]

Consider the following yaml file for a cluster role

```
apiVersion: networking.k8s.io/v1
kind: NetworkPolicy
metadata:
  name: networkpolicy-nginx
spec:
  podSelector:
    matchLabels:
      run: nginx
  ingress:
  - from:
    - podSelector:
        matchLabels:
          catalogue-pod: "true"
```