Kubernetes RBAC(Role Based access control)

create 3 role in RBAC

1.Admin

2.General

3.others

Need to do the action

1.First we need to create service account

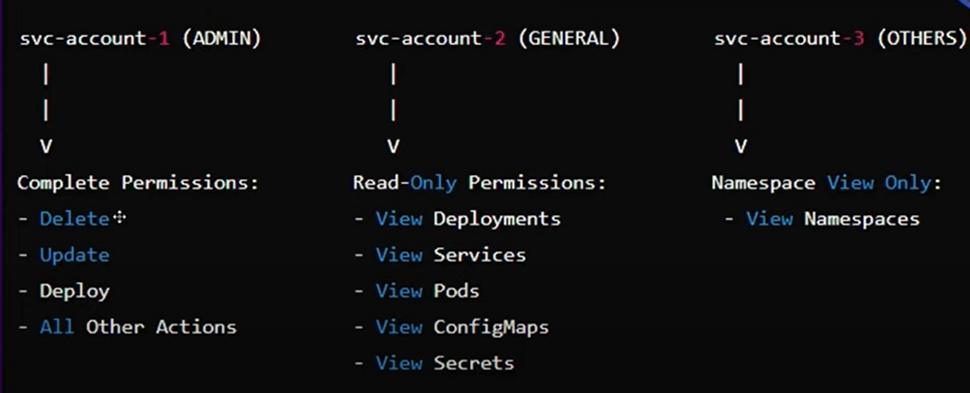
2.We need create cluster role 1.admin 2. general 3.other

3.we need to assign the cluster role to service account through role binding

Role have 2 types

1.roles

2.clusterrole



**Admin-sa.yaml:**

apiVersion: v1

kind: ServiceAccount

metadata:

name: admin

namespace: default

---

apiVersion: rbac.authorization.k8s.io/v1

kind: ClusterRole

metadata:

name: admin-role

rules:

- apiGroups: ["\*"] # Grants access to all API groups

resources: ["\*"] # Grants access to all resource types

verbs: ["\*"] # Grants all actions (get, list, create, delete, etc.)

---

apiVersion: rbac.authorization.k8s.io/v1

kind: ClusterRoleBinding

metadata:

name: admin-rolebinding

subjects:

- kind: ServiceAccount

name: admin

namespace: default

roleRef:

kind: ClusterRole

name: admin-role

apiGroup: rbac.authorization.k8s.io

**general-sa.yaml**

apiVersion: v1

kind: ServiceAccount

metadata:

name: general

namespace: default

---

apiVersion: rbac.authorization.k8s.io/v1

kind: Role

metadata:

name: general-read-only

namespace: default

rules:

- apiGroups: ["apps"]

resources: ["deployments"]

verbs: ["get", "list", "watch"]

- apiGroups: [""]

resources: ["pods", "services", "configmaps", "secrets"]

verbs: ["get", "list", "watch"]

---

apiVersion: rbac.authorization.k8s.io/v1

kind: RoleBinding

metadata:

name: general-read-only-binding

namespace: default

subjects:

- kind: ServiceAccount

name: general

namespace: default

roleRef:

kind: Role

name: general-read-only

apiGroup: rbac.authorization.k8s.io