apiVersion: v1

kind: Namespace

metadata:

name: sa-permissions-test

---

apiVersion: v1

kind: ServiceAccount

metadata:

name: shared-sa

namespace: sa-permissions-test

automountServiceAccountToken: true

---

apiVersion: rbac.authorization.k8s.io/v1

kind: Role

metadata:

name: shared-sa-role

namespace: sa-permissions-test

rules:

- apiGroups: [""]

resources: ["deployments", "pods", "secrets"]

verbs: ["get", "list"]

---

apiVersion: rbac.authorization.k8s.io/v1

kind: RoleBinding

metadata:

name: shared-sa-rb

namespace: sa-permissions-test

subjects:

- kind: ServiceAccount

name: shared-sa

namespace: auth

roleRef:

kind: Role

name: shared-sa-role

apiGroup: rbac.authorization.k8s.io

---

apiVersion: v1

kind: Pod

metadata:

name: deployment-viewer-pod

namespace: sa-permissions-test

spec:

serviceAccountName: shared-sa

containers:

- name: busybox

image: radial/busyboxplus:curl

command: ['sh', '-c', 'TOKEN=$(cat /var/run/secrets/kubernetes.io/serviceaccount/token); while true; do if curl -s -o /dev/null -k -m 3 -H "Authorization: Bearer $TOKEN" https://kubernetes.default.svc.cluster.local/api/v1/namespaces/auth/deployments/; then echo "[SUCCESS] Successfully viewed Deployments!"; else echo "[FAIL] Failed to view Deployments!"; fi; sleep 5; done']

---

apiVersion: v1

kind: Pod

metadata:

name: pod-viewer-pod

namespace: sa-permissions-test

spec:

serviceAccountName: shared-sa

containers:

- name: busybox

image: radial/busyboxplus:curl

command: ['sh', '-c', 'TOKEN=$(cat /var/run/secrets/kubernetes.io/serviceaccount/token); while true; do if curl -s -o /dev/null -k -m 3 -H "Authorization: Bearer $TOKEN" https://kubernetes.default.svc.cluster.local/api/v1/namespaces/auth/pods/; then echo "[SUCCESS] Successfully viewed Pods!"; else echo "[FAIL] Failed to view Pods!"; fi; sleep 5; done']