To set up Role-Based Access Control (RBAC) for a single namespace in an Azure Kubernetes Service (AKS) cluster, specifically for the SonarQube namespace, you’ll need to create a role and role binding. Here’s a step-by-step guide:

1. Create a Namespace (if you haven’t already):

apiVersion: v1

kind: Namespace

metadata:

name: sonarqube

2. Define a Role:

This role will define the permissions within the sonarqube namespace.

apiVersion: rbac.authorization.k8s.io/v1

kind: Role

metadata:

namespace: sonarqube

name: sonarqube-role

rules:

- apiGroups: [""]

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

verbs: ["get", "list", "watch", "create", "update", "patch", "delete"]

- apiGroups: ["apps"]

resources: ["deployments"]

verbs: ["get", "list", "watch", "create", "update", "patch", "delete"]

3. Create a RoleBinding:

This role binding will assign the role to a user, group, or service account.

apiVersion: rbac.authorization.k8s.io/v1

kind: RoleBinding

metadata:

name: sonarqube-rolebinding

namespace: sonarqube

subjects:

- kind: User

name: "your-username" # Replace with the actual user

apiGroup: rbac.authorization.k8s.io

roleRef:

kind: Role

name: sonarqube-role

apiGroup: rbac.authorization.k8s.io

4. Apply the Configurations:

Apply the namespace, role, and role binding to your cluster.

kubectl apply -f namespace.yaml

kubectl apply -f role.yaml

kubectl apply -f rolebinding.yaml

5. Verify the RBAC Setup:

Ensure that the user has the correct permissions within the sonarqube namespace.

kubectl auth can-i list pods --namespace=sonarqube --as=your-username

Replace "your-username" with the actual username or service account you want to grant access to. If you’re using a group or a service account instead of a user, adjust the subjects field in the RoleBinding accordingly.