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

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

apiVersion: v1  
kind: Namespace  
metadata:  
name: backstage

**Define a Role: This role will define the permissions within the backstage namespace.**

apiVersion: [rbac.authorization.k8s.io/v1](http://rbac.authorization.k8s.io/v1)   
kind: Role  
metadata:  
namespace: backstage  
name: backstage-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"]

**Create a RoleBinding:**

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

apiVersion: [rbac.authorization.k8s.io/v1](http://rbac.authorization.k8s.io/v1)   
kind: RoleBinding  
metadata:  
name: backstage-rolebinding  
namespace: backstage  
subjects:

* kind: User  
  name: "srikar.k@kshema.co" #Replace with the actual user  
  apiGroup: [rbac.authorization.k8s.io](http://rbac.authorization.k8s.io/)   
  roleRef:  
  kind: Role  
  name: backstage-role  
  apiGroup: [rbac.authorization.k8s.io](http://rbac.authorization.k8s.io/)

**for Check**

Verify the RBAC Setup:  
Ensure that the user has the correct permissions within the backstage namespace.

**kubectl auth can-i list pods --namespace=backstage --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.  
[K8S dCOUMENTS.docx](https://dev.azure.com/Kshema/2cbbd35d-fb1d-459c-a1d1-515e60d0cf40/_apis/git/repositories/0a9d3b9b-975b-4360-a8a4-a258772efe74/Items?path=/.attachments/K8S%20dCOUMENTS-2a9177b5-4f1c-48a6-be48-bec2efddbc65.docx&download=false&resolveLfs=true&%24format=octetStream&api-version=5.0-preview.1&sanitize=true&includeContentMetadata=true&versionDescriptor.version=wikiMaster)

Complete full permission of cluster using rbac:-

* -------------------------------------------
* ---
* apiVersion: rbac.authorization.k8s.io/v1
* kind: ClusterRole
* metadata:
* name: manage-pods-namespaces
* rules:
* - apiGroups: [""]
* resources: ["pods", "namespaces"]
* verbs: ["get", "list", "watch", "create", "update", "patch", "delete"]
* ---
* apiVersion: rbac.authorization.k8s.io/v1
* kind: ClusterRoleBinding
* metadata:
* name: grant-cluster-admin
* subjects:
* - kind: User
* name: srikar.k@kshema.co
* apiGroup: rbac.authorization.k8s.io
* - kind: User
* name: sanjay.w@kshema.co
* apiGroup: rbac.authorization.k8s.io
* - kind: User
* name: yashwanth.k@kshema.co
* apiGroup: rbac.authorization.k8s.io
* roleRef:
* kind: ClusterRole
* name: manage-pods-namespaces
* apiGroup: rbac.authorization.k8s.io