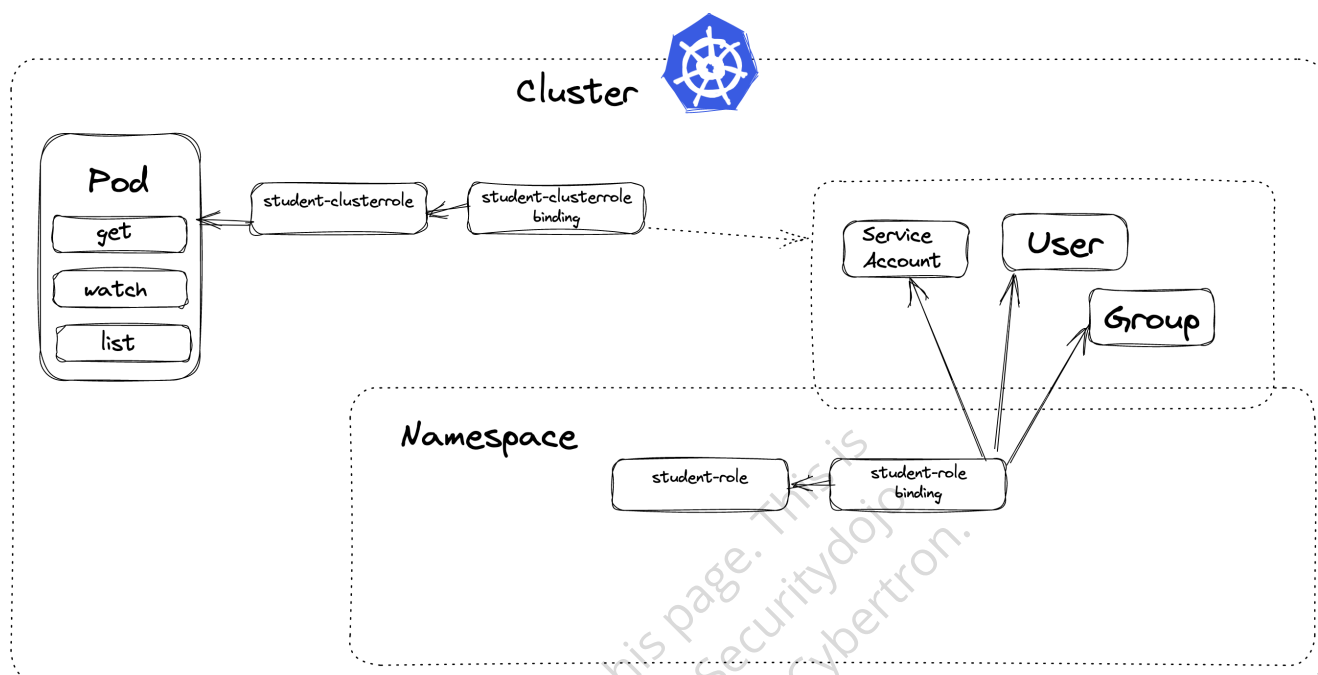


# Lab: Cluster Role & Cluster RoleBinding - Role Based Access Control



This lab creates a ClusterRole and ClusterRoleBinding in Kubernetes RBAC to grant a user named "student" read access to node resources within the entire cluster.

This is next part of the previous lab.

- Stay in the directory `3.9_authz_authn` to perform the lab.
- Create a YAML file named "student-clusterrole.yaml" and writes to it a Kubernetes Cluster Role manifest.

```

sudo bash -c "cat << EOF > student-clusterrole.yaml
apiVersion: rbac.authorization.k8s.io/v1
kind: ClusterRole
metadata:
  name: student-clusterrole
rules:
- apiGroups: ['']
  resources: ["nodes"]
  verbs: ["get", "list", "watch"]
EOF"
  
```

```
root@ip-10-0-0-62:/home/ubuntu/ workspace/course# sudo bash -c "cat << EOF > student-clusterrole.yaml
> apiVersion: rbac.authorization.k8s.io/v1
> kind: ClusterRole
> metadata:
>   name: student-clusterrole
> rules:
> - apiGroups: ['']
>   resources: ["nodes"]
>   verbs: ["get", "list", "watch"]
> EOF"
root@ip-10-0-0-62:/home/ubuntu/ workspace/course#
```

- Creates a YAML file named "student-clusterrolebinding.yaml" and writes to it a Cluster RoleBinding manifest.

```
sudo bash -c "cat << EOF > student-clusterrolebinding.yaml
apiVersion: rbac.authorization.k8s.io/v1
kind: ClusterRoleBinding
metadata:
  name: student-clusterrolebinding
roleRef:
  apiGroup: rbac.authorization.k8s.io
  kind: ClusterRole
  name: student-clusterrole
subjects:
- kind: User
  name: student
  apiGroup: rbac.authorization.k8s.io
EOF"
```

```
root@ip-10-0-0-62:/home/ubuntu/ workspace/course# sudo bash -c "cat << EOF > student-clusterrolebinding.yaml
> apiVersion: rbac.authorization.k8s.io/v1
> kind: ClusterRoleBinding
> metadata:
>   name: student-clusterrolebinding
> roleRef:
>   apiGroup: rbac.authorization.k8s.io
>   kind: ClusterRole
>   name: student-clusterrole
> subjects:
> - kind: User
>   name: student
>   apiGroup: rbac.authorization.k8s.io
> EOF"
root@ip-10-0-0-62:/home/ubuntu/ workspace/course#
root@ip-10-0-0-62:/home/ubuntu/ workspace/course#
```

- Create the Cluster Role in Kubernetes RBAC by applying the `student-clusterrole.yaml`.

```
kubectl create -f student-clusterrole.yaml
```

- Create the Cluster RoleBinding in Kubernetes RBAC by applying the `student-clusterrolebinding.yaml`.

```
kubectl create -f student-clusterrolebinding.yaml
```

```
root@ip-10-0-0-62:/home/ubuntu/ workspace/course# kubectl create -f student-clusterrole.yaml
clusterrole.rbac.authorization.k8s.io/student-clusterrole created
root@ip-10-0-0-62:/home/ubuntu/ workspace/course#
root@ip-10-0-0-62:/home/ubuntu/ workspace/course# kubectl create -f student-clusterrolebinding.yaml
clusterrolebinding.rbac.authorization.k8s.io/student-clusterrolebinding created
root@ip-10-0-0-62:/home/ubuntu/ workspace/course#
root@ip-10-0-0-62:/home/ubuntu/ workspace/course#
```

- Test whether the user "student" has permission to list nodes in the cluster.

---

Ignore the warning as nodes resource is not bound to a specific namespace and is therefore not subject to namespace-level permissions. Warning: resource 'nodes' is not namespace scoped.

---

```
kubectl auth can-i list nodes --as student
```

```
root@ip-10-0-0-62:/home/ubuntu/ workspace/course# kubectl auth can-i list nodes --as student
Warning: resource 'nodes' is not namespace scoped

yes
root@ip-10-0-0-62:/home/ubuntu/ workspace/course#
root@ip-10-0-0-62:/home/ubuntu/ workspace/course#
```