**Managing Users and RBAC in EKS**

Create an user in IAM and copy Access Key id and secret in notepad for further reference

example : modeldev

**Create an Admin user to access Kubernetes cluster with all permissions**

1.**Config map “aws-auth” should be update with the IAM user details as show below**

|  |
| --- |
| kubectl get cm -n kube-system  kubectl get cm -n kube-system aws-auth -o yaml >aws-auth-configmap.yaml |

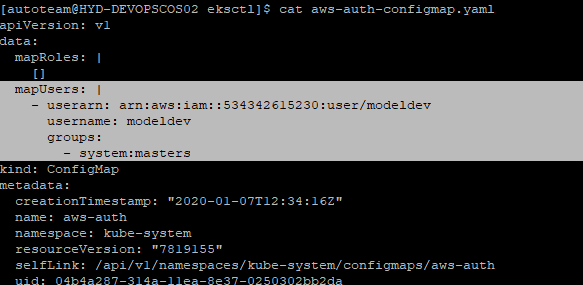
**2.In UI fetch arn of user that got created**

arn:aws:iam::534342615230:user/modeldev

**3.Edit the config map yaml wit the user arn/username details as show below**

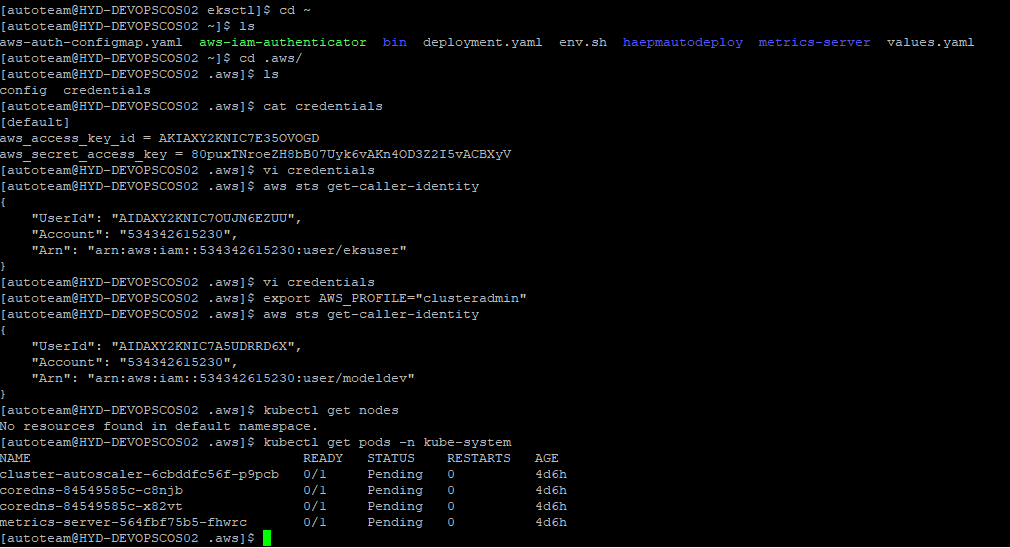
Snippet:

|  |
| --- |
| mapUsers: |  - userarn: arn:aws:iam::534342615230:user/modeldev  username: modeldev  groups:  - **system:masters** |

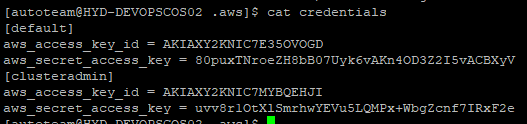


4. **Update the yaml and apply and verify with below commands**

|  |
| --- |
| kubectl apply -f aws-auth-configmap.yaml -n kube-system    kubectl get cm -n kube-system aws-auth    kubectl describe cm aws-auth -n kube-system |



**5.Update the Aws credentials file with new user details**



**6. Switch the AWS user with below commands**

|  |
| --- |
| export AWS\_PROFILE="clusteradmin"  aws sts get-caller-identity  [autoteam@HYD-DEVOPSCOS02 .aws]$ aws sts get-caller-identity  {  "UserId": "AIDAXY2KNIC7A5UDRRD6X",  "Account": "534342615230",  "Arn": "arn:aws:iam::534342615230:user/modeldev"  } |

**7. User with master access has been created and can access all the Kubernetes resources**

|  |
| --- |
| Kubectl get node  Kubectl get pods/ns/service |

**Create Read only User**

Create an user in IAM and copy Access Key id and secret

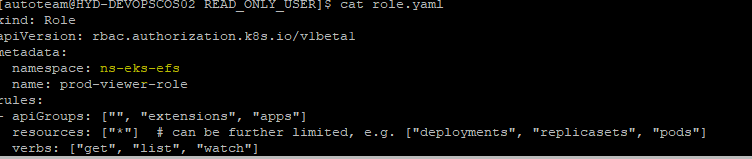
example : eksreadonly

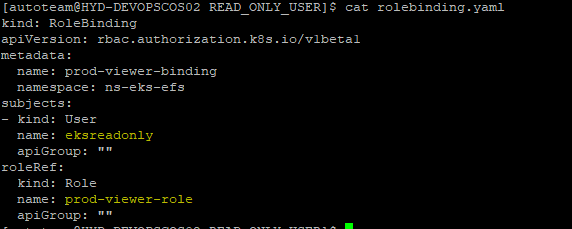
**Create an Read only user to restrict Kubernetes cluster access specific to Namespcacr**

**In UI fetch arn of user that got created**

|  |
| --- |
| arn:aws:iam::534342615230:user/eksreadonly |

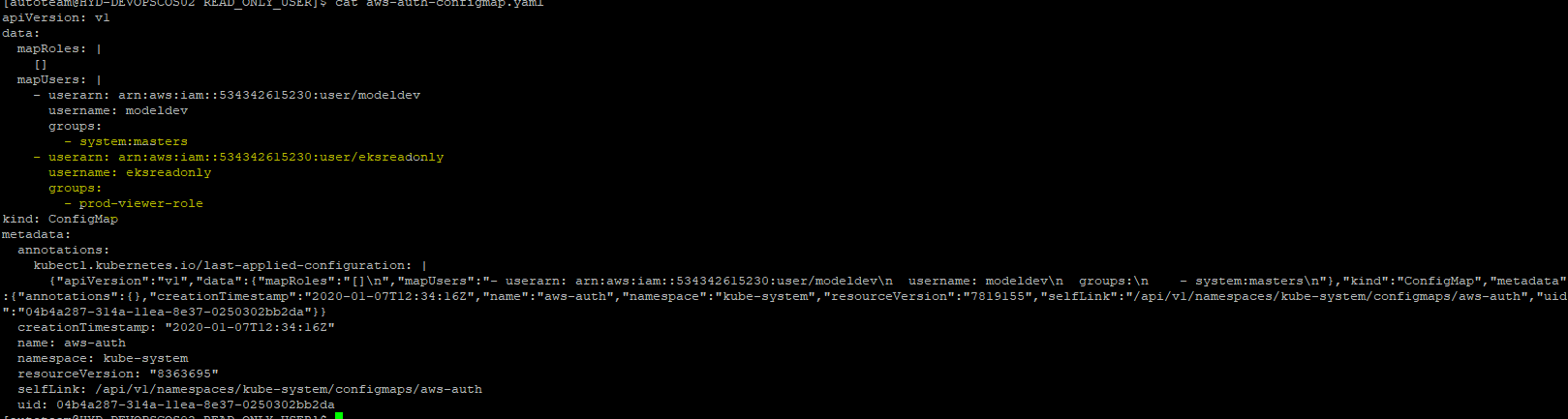
**Create role and role binding**





|  |
| --- |
| kubectl apply -f role.yaml  role.rbac.authorization.k8s.io/prod-viewer-role created  kubectl apply -f rolebinding.yaml  rolebinding.rbac.authorization.k8s.io/prod-viewer-binding created |

**3.Edit the config map yaml wit the user arn/username details as show below**



4. **Update the yaml and apply and verify with below commands**

|  |
| --- |
| kubectl apply -f aws-auth-configmap.yaml -n kube-system    kubectl get cm -n kube-system aws-auth    kubectl describe cm aws-auth -n kube-system |

5. **Switch the AWS user with below commands**

|  |
| --- |
| export AWS\_PROFILE="eksreadonly "  aws sts get-caller-identity |

**7. User with master access has been created and can access all the Kubernetes resources**

|  |
| --- |
| Kubectl get node  **Error from server (Forbidden): nodes is forbidden: User "eksreadonly" cannot list resource "nodes" in API group "" at the cluster scope**  Kubectl get pods/ns/service  **Error from server (Forbidden): pods is forbidden: User "eksreadonly" cannot list resource "pods" in API group "" in the namespace "default"**  kubectl get pods -n ns-eks-efs  **NAME READY STATUS RESTARTS AGE**  **efs-provisioner-6cd557fd6c-g7phc 0/1 Pending 0 4d6h**  **mc-web-5667fbd6d-lcxmd 0/1 Pending 0 4d6h**  **mc-web-5667fbd6d-xkbdk 0/1 Pending 0 4d6h** |

