

# Manage IAM users and roles

EKS clusters use IAM users and roles to control access to the cluster. The rules are implemented in a config map called `aws-auth`. `eksctl` provides commands to read and edit this config map.

Get all identity mappings:

```
eksctl get iamidentitymapping --cluster <clusterName> --region=<region>
```

Get all identity mappings matching an arn:

```
eksctl get iamidentitymapping --cluster <clusterName> --region=<region> --arn arn:aws:iam::123456:role/testing-role
```

Create an identity mapping:

```
eksctl create iamidentitymapping --cluster <clusterName> --region=<region> --arn arn:aws:iam::123456:role/testing --group system:masters --username admin
```

The identity mappings can also be specified in ClusterConfig:

```
---
apiVersion: eksctl.io/v1alpha5
kind: ClusterConfig

metadata:
  name: cluster-with-iamidentitymappings
  region: us-east-1

iamIdentityMappings:
  - arn: arn:aws:iam::000000000000:role/myAdminRole
    groups:
      - system:masters
    username: admin
    noDuplicateARNs: true # prevents shadowing of ARNs

  - arn: arn:aws:iam::000000000000:user/myUser
    username: myUser
    noDuplicateARNs: true # prevents shadowing of ARNs

  - serviceName: emr-containers
    namespace: emr # serviceName requires namespace


  - account: "000000000000" # account must be configured with no other options

nodeGroups:
  - name: ng-1
    instanceType: m5.large
    desiredCapacity: 1
```

```
eksctl create iamidentitymapping -f cluster-with-iamidentitymappings.yaml
```

Delete an identity mapping:

```
eksctl delete iamidentitymapping --cluster <clusterName> --region=<region> --arn arn:aws:iam::123456:role/testing
```

 **Note**

Above command deletes a single mapping FIFO unless `--all` is given in which case it removes all matching. Will warn if more mappings matching this role are found.

Create an account mapping:

```
eksctl create iamidentitymapping --cluster <clusterName> --region=<region> --account user-account
```

Delete an account mapping:

```
eksctl delete iamidentitymapping --cluster <clusterName> --region=<region> --account user-account
```

Was this page helpful?



