EKS-1

ASSIGNMENT

Name – Maithely Sharma
College – University of Petroleum and Energy Studies
EmployeeID – 4057

- Create eks cluster using eksctl
    - During creation, Specify
    - Cluster name
    - Kubernetes version
    - Control plane role
    - Subnets for Control Plane
    - Control Plane security Group
    - Add tag: owner, purpose on Control Plane
    - Node Group Name
    - Node Instance Role
    - Subnets for Node Group
    - Node Instance SSH key pair
    - Node Instance Security Group
    - Node Instance Instance Type
    - Node Instance Disk
    - Add tag: owner, purpose on Node Group
    - Node Group Size: min, max

Firstly create a directory “kube” and create cluster.yml in it

```
maithely@maithely:~/Downloads$ mkdir kube
maithely@maithely:~/Downloads$ cd kube/
maithely@maithely:~/Downloads/kube$ ls
maithely@maithely:~/Downloads/kube$ mv ~/Downloads/cluster.yml .
maithely@maithely:~/Downloads/kube$ ls
cluster.yml
maithely@maithely:~/Downloads/kube$ eksctl version
[ℹ]  version.Info{BuiltAt:"", GitCommit:"", GitTag:"0.13.0"}
maithely@maithely:~/Downloads/kube$
```

Create a service role and add 2 policies for EKS

Roles > maithely-eks-role

Summary

Role ARN	arn:aws:iam::187632318301:role/maithely-eks-role
Role description	Allows EKS to manage clusters on your behalf. | Edit
Instance Profile ARNs	
Path	/
Creation time	2020-03-09 14:17 UTC+0530
Last activity	2020-03-13 23:29 UTC+0530 (2 days ago)
Maximum session duration	1 hour Edit

Permissions | **Trust relationships** | **Tags (2)** | **Access Advisor** | **Revoke sessions**

Permissions policies (2 policies applied)

Attach policies

	Policy name	Policy type
	AmazonEKSClusterPolicy	AWS managed policy
	AmazonEKSServicePolicy	AWS managed policy

Now create one more role in which you add 3 policies for instance-node

Summary

Role ARN	arn:aws:iam::187632318301:role/eksisntance-role-maithely
Role description	Allows EC2 instances to call AWS services on your behalf. | Edit
Instance Profile ARNs	arn:aws:iam::187632318301:instance-profile/eksisntance-role-maithely
Path	/
Creation time	2020-03-16 11:40 UTC+0530
Last activity	Not accessed in the tracking period
Maximum session duration	1 hour Edit

Permissions | Trust relationships | Tags (2) | Access Advisor | Revoke sessions

Permissions policies (3 policies applied)

Attach policies

Policy name	Policy type
AmazonEKSWorkerNodePolicy	AWS managed policy
AmazonEC2ContainerRegistryReadOnly	AWS managed policy
AmazonEKS_CNI_Policy	AWS managed policy

Create a cluster.yml file

```yaml
apiVersion: eksctl.io/v1alpha5
kind: ClusterConfig
metadata:
  name: maithely
  region: us-east-1
vpc:
  id: "vpc-01446cec73b675a0b"
  cidr: "192.168.0.0/16"
  subnets:
    public:
      us-east-1b:
          id: "subnet-02618d516e069dda9"
          cidr: "192.168.128.0/18"
      us-east-1c:
          id: "subnet-05128b98c1ea54979"
          cidr: "192.168.192.0/18"
      us-east-1a:
          id: "subnet-05ccb7f834d214a5a"
          cidr: "192.168.64.0/18"
iam:
  serviceRoleARN: "arn:aws:iam::187632318301:role/eksServiceRole"
```

```yaml
nodeGroups:
  - name: managed-ng-1
    instanceType: t2.micro
    minSize: 1
    desiredCapacity: 2
    maxSize: 3
    availabilityZones: ["us-east-1a","us-east-1b","us-east-1c"]
    volumeSize: 20
    iam:
      instanceProfileARN: "arn:aws:iam::187632318301:instance-profile/EKSNodeInstanceRole"
    securityGroups:
      withShared: true
      withLocal: true
      attachIDs: ['sg-07236ec4decae9d40']
    ssh:
      allow: true
      publicKeyName: 'maithely'
    tags:
      'owner': 'maithely'
      'purpose': 'bootcamp assignment'
```

Create a cluster

```
maithely@maithely:~/Downloads/kube$ eksctl create cluster -f cluster.yml
[i]  eksctl version 0.13.0
[i]  using region us-east-1
[!]  retryable error (RequestError: send request failed
caused by: Post https://ec2.us-east-1.amazonaws.com/: net/http: TLS handsha
2969ms
[✔]  using existing VPC (vpc-01446cec73b675a0b) and subnets (private:[] pub
d516e069dda9])
[!]  custom VPC/subnets will be used; if resulting cluster doesn't functior
[i]  nodegroup "managed-ng-1" will use "ami-087a82f6b78a07557" [AmazonLinux
[i]  using EC2 key pair "maithely"
[i]  using Kubernetes version 1.14
[i]  creating EKS cluster "maithely" in "us-east-1" region with un-managed
[i]  1 nodegroup (managed-ng-1) was included (based on the include/exclude
[i]  will create a CloudFormation stack for cluster itself and 1 nodegroup
[i]  will create a CloudFormation stack for cluster itself and 0 managed no
[i]  if you encounter any issues, check CloudFormation console or try 'eksc
[i]  CloudWatch logging will not be enabled for cluster "maithely" in "us-e
[i]  you can enable it with 'eksctl utils update-cluster-logging --region=u
[i]  Kubernetes API endpoint access will use default of {publicAccess=true,
[i]  2 sequential tasks: { create cluster control plane "maithely", create
[i]  building cluster stack "eksctl-maithely-cluster"
[i]  deploying stack "eksctl-maithely-cluster"
[!]  retryable error (RequestError: send request failed
caused by: Post https://cloudformation.us-east-1.amazonaws.com/: net/http:
try after delay of 43.467688ms
[!]  retryable error (RequestError: send request failed
caused by: Post https://ec2.us-east-1.amazonaws.com/: net/http: TLS handsha
.224137ms
[i]  building nodegroup stack "eksctl-maithely-nodegroup-managed-ng-1"
[i]  deploying stack "eksctl-maithely-nodegroup-managed-ng-1"
[✔]  all EKS cluster resources for "maithely" have been created
```

Now you can see after some time that a cluster is created

EKS > Clusters

New Kubernetes versions are available for 4 clusters.

Clusters (6)

Delete | Create cluster

Find clusters by name

1

Cluster name	Kubernetes version	Status
Jenkins	1.15	Active
ABCEG	1.14 Update now	Active
Group3_cluster	1.14 Update now	Active
maithely	1.14 Update now	Active
t34ak-cluster	1.15	Active
fabulous-creature-1583926076	1.14 Update now	Active

maithely

Delete

A new Kubernetes version is available for this cluster. Learn more

Update now

General configuration

Kubernetes version
1.14

Platform version
eks.9

Status
Active

API server endpoint
https://9390D7812B2F2A7F83BD05268DB37BB9.gr7.us-east-1.eks.amazonaws.com

OpenID Connect provider URL
https://oidc.eks.us-east-1.amazonaws.com/id/9390D7812B2F2A7F83BD05268DB37BB9

Certificate authority
LS0tLS1CRUdJTiBDRVJUSUZJQ0FURS0tLS0tCk1JSUN5RENDQWJDZ0F3SUJBZ0lCQURBTkJna3Foa2lHOXcwQkFRc0ZBREFWTVJNd0VRWURWUVFERXdwcmRXSmwKY201bGRHVnpNQ

Cluster ARN
arn:aws:eks:us-east-1:187632318301:cluster/maithely

Cluster IAM Role ARN
arn:aws:iam::187632318301:role/eksServiceRole

```
maithely@maithely:~/Downloads/kube$ eksctl get cluster
NAME                            REGION
ABCEG                           us-east-1
Group3_cluster                  us-east-1
Jenkins                         us-east-1
fabulous-creature-1583926076    us-east-1
maithely                        us-east-1
t34ak-cluster                   us-east-1
maithely@maithely:~/Downloads/kube$
```

```
maithely@maithely:~/Downloads/kube$ kubectl get nodes
NAME                                STATUS   ROLES    AGE   VERSION
ip-192-168-122-153.ec2.internal     Ready    <none>   50m   v1.14.8-eks-b8860f
ip-192-168-172-153.ec2.internal     Ready    <none>   50m   v1.14.8-eks-b8860f
```

```
maithely@maithely:~/Downloads/kube$ aws eks --region us-east-1 update-kubeconfig --name maithely
Added new context arn:aws:eks:us-east-1:187632318301:cluster/maithely to /home/maithely/.kube/config
maithely@maithely:~/Downloads/kube$ kubectl cluster-info
Kubernetes master is running at https://9390D7812B2F2A7F83BD05268DB37BB9.gr7.us-east-1.eks.amazonaws.com
CoreDNS is running at https://9390D7812B2F2A7F83BD05268DB37BB9.gr7.us-east-1.eks.amazonaws.com/api/v1/nam
:dns/proxy

To further debug and diagnose cluster problems, use 'kubectl cluster-info dump'.
```

```
maithely@maithely:~/Downloads/kube$ kubectl get nodes
NAME                                STATUS   ROLES    AGE    VERSION
ip-192-168-122-153.ec2.internal     Ready    <none>   134m   v1.14.8-eks-b8860f
ip-192-168-172-153.ec2.internal     Ready    <none>   134m   v1.14.8-eks-b8860f
maithely@maithely:~/Downloads/kube$
```

- AuthAuthentication Management
    - Add new 2 IAM user into the cluster
    - Enable a EC2 server to access Cluster master API without using access/secret key

For adding 2 iam user , we edit the file

```
maithely@maithely:~/Downloads/kube$ kubectl edit -n kube-system configmap/aws-auth
configmap/aws-auth edited
maithely@maithely:~/Downloads/kube$
```

Add these changes in the file

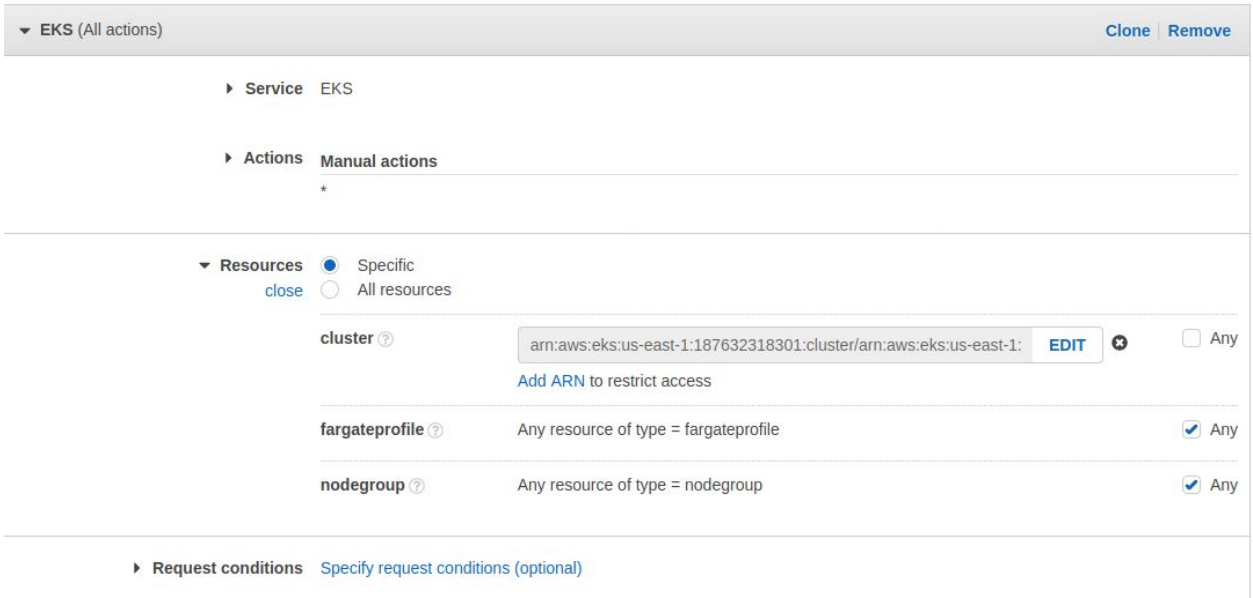
```
apiVersion: v1
data:
  mapRoles: |
    - groups:
      - system:bootstrappers
      - system:nodes
      rolearn: arn:aws:iam::187632318301:role/EKSNodeInstanceRole
      username: system:node:{{EC2PrivateDNSName}}
  mapUsers: |
    - userarn: arn:aws:iam::187632318301:user/maithely.sharma@tothenew.com
      username: maithely
      groups:
        - system-masters
    - userarn: arn:arn:aws:iam::187632318301:user/abhishek.chauhan1@tothenew.com
      username: abhishek
      groups:
        - system-masters

    []
kind: ConfigMap
metadata:
  creationTimestamp: "2020-03-16T06:28:53Z"
  name: aws-auth
  namespace: kube-system
  resourceVersion: "23011"
  selfLink: /api/v1/namespaces/kube-system/configmaps/aws-auth
  uid: 6817a890-674f-11ea-babe-02b3d18309c7
~
-- INSERT --
```

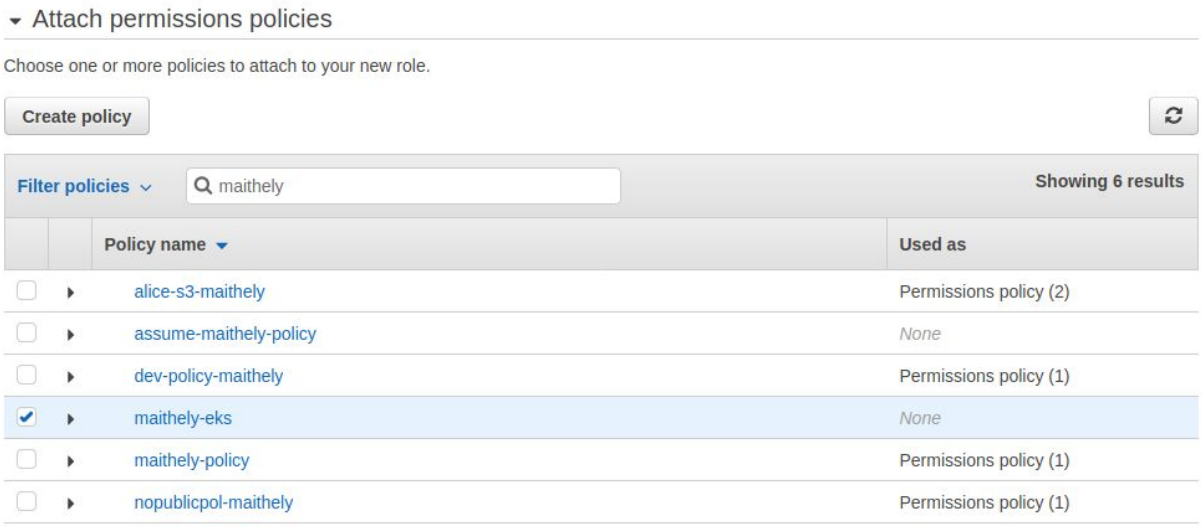
After being edited the file looks like:

```
# Please edit the object below. Lines beginning with a '#' will be ignored,
# and an empty file will abort the edit. If an error occurs while saving this file will be
# reopened with the relevant failures.
#
apiVersion: v1
data:
  mapRoles: |
    - groups:
      - system:bootstrappers
      - system:nodes
      rolearn: arn:aws:iam::187632318301:role/EKSNodeInstanceRole
      username: system:node:{{EC2PrivateDNSName}}
  mapUsers: "- userarn: arn:aws:iam::187632318301:user/maithely.sharma@tothenew.com\n
    \ username: maithely\n  groups:\n    - system-masters\n- userarn: arn:arn:aws:iam::187632318301:user/ab
hishek.chauhan1@tothenew.com\n
    \ username: abhishek\n  groups:\n    - system-masters\n\n[]    \n"
kind: ConfigMap
metadata:
  creationTimestamp: "2020-03-16T06:28:53Z"
  name: aws-auth
  namespace: kube-system
  resourceVersion: "23011"
  selfLink: /api/v1/namespaces/kube-system/configmaps/aws-auth
  uid: 6817a890-674f-11ea-babe-02b3d18309c7
```

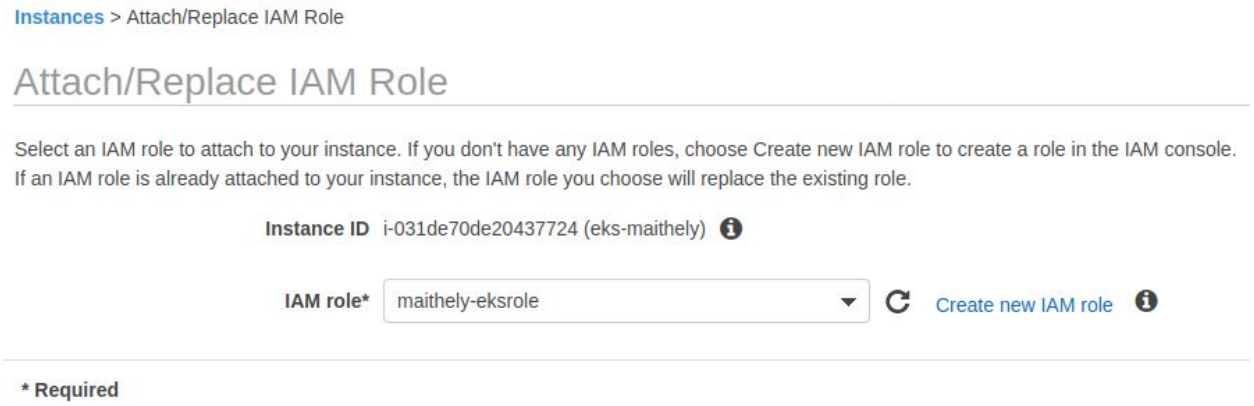
For EC2 server to access Cluster master API without using access/secret key,
create a policy



Now create a role and attach the policy created above



Attach the above created role to an instance



```
ubuntu@ip-172-31-214-226:~$ aws eks describe-cluster --name maithely --region us-east-1
{
    "cluster": {
        "name": "maithely",
        "arn": "arn:aws:eks:us-east-1:187632318301:cluster/maithely",
        "createdAt": "2020-03-16T06:16:07.337000+00:00",
        "version": "1.14",
        "endpoint": "https://9390D7812B2F2A7F83BD05268DB37BB9.gr7.us-east-1.eks.amazonaws
        "roleArn": "arn:aws:iam::187632318301:role/eksServiceRole",
        "resourcesVpcConfig": {
            "subnetIds": [
                "subnet-05ccb7f834d214a5a",
                "subnet-02618d516e069dda9",
                "subnet-05128b98c1ea54979"
            ],
            "securityGroupIds": [
                "sg-029128d1c67bf8e1f"
            ],
            "clusterSecurityGroupId": "sg-097666dafb7f4e719",
            "vpcId": "vpc-01446cec73b675a0b",
            "endpointPublicAccess": true,
            "endpointPrivateAccess": false,
            "publicAccessCidrs": [
```

- Eksctl command to terminate the stack

```
maithely@maithely:~/Downloads/kube$ eksctl delete cluster -f cluster.yml
[i]  eksctl version 0.13.0
[i]  using region us-east-1
[i]  deleting EKS cluster "maithely"
[i]  deleted 0 Fargate profile(s)
[✓]  kubeconfig has been updated
[i]  cleaning up LoadBalancer services
[i]  2 sequential tasks: { delete nodegroup "managed-ng-1", delete cluster control plane "maithely" [async] }
[i]  will delete stack "eksctl-maithely-nodegroup-managed-ng-1"
[i]  waiting for stack "eksctl-maithely-nodegroup-managed-ng-1" to get deleted
[i]  will delete stack "eksctl-maithely-cluster"
[✓]  all cluster resources were deleted
maithely@maithely:~/Downloads/kube$
```