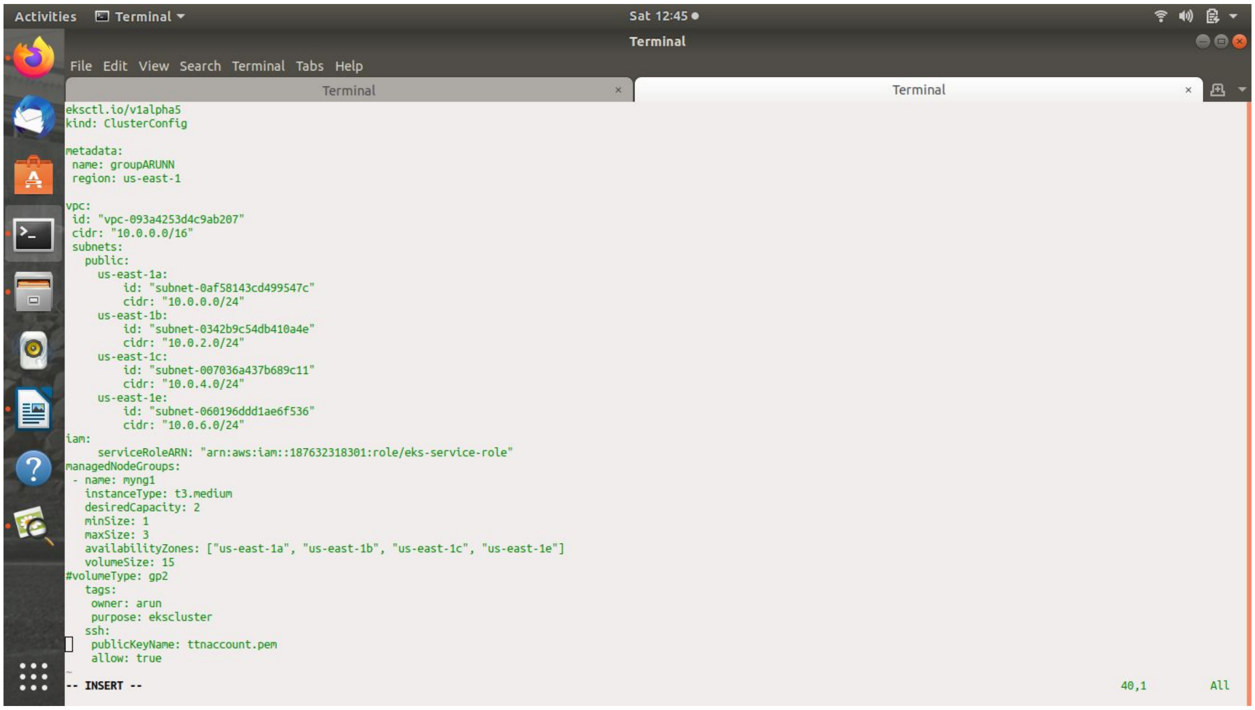
Assessment -17

EKS-1

Trainee Name : Arun Parmar
Mentor Name : Ravi Kumar
College: UPES

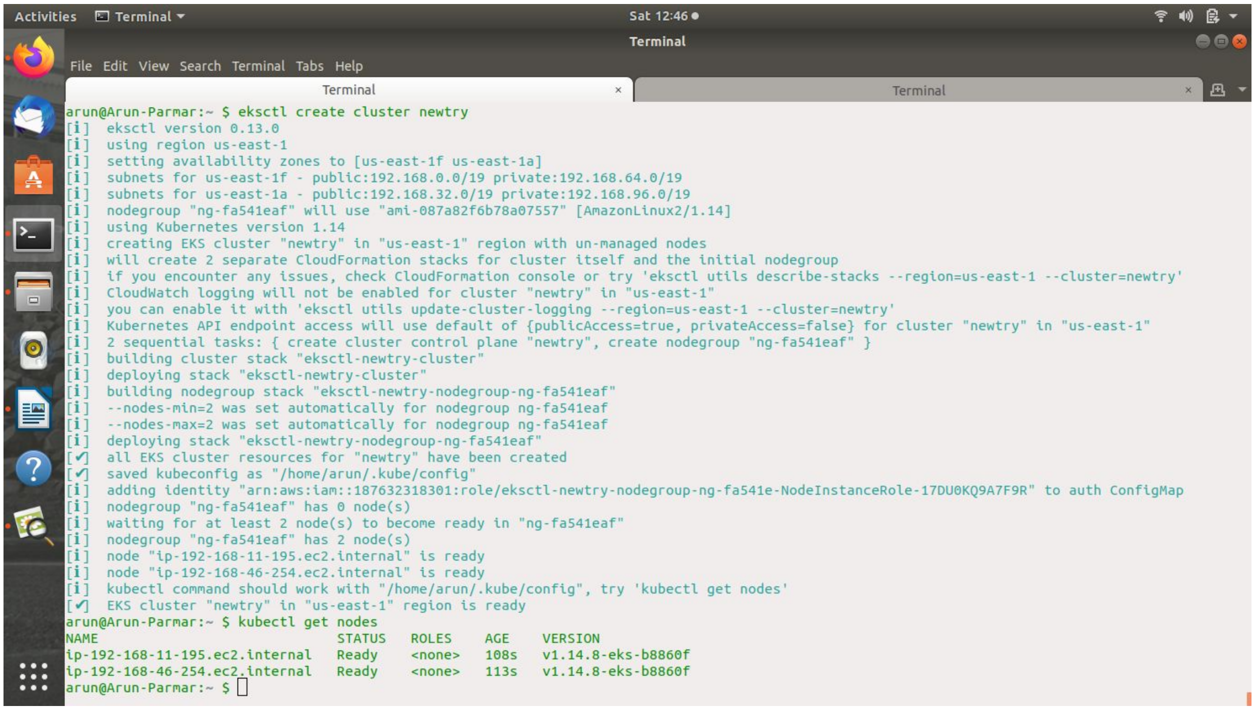
1. Create eks cluster using eksctl
   During creation, Specify
   - Cluster name
   - Kubernetes version
   - Control plane role
   - Subnets for Control Plane
   - Control Plane security Group
   - Add tag: owner, purpose on Control Plane
   - Node Group Name
   - Node Instance Role
   - Subnets for 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



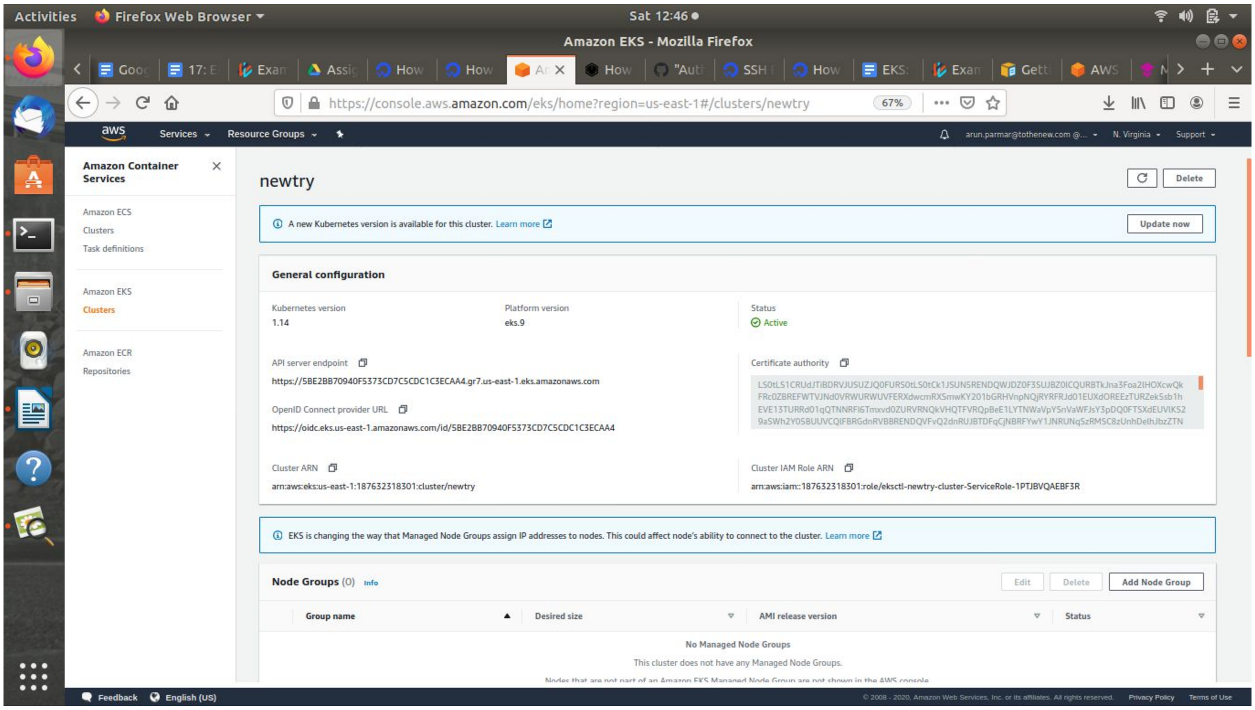
```
eksctl.io/v1alpha5
kind: ClusterConfig

metadata:
 name: groupARUNN
 region: us-east-1

vpc:
 id: "vpc-093a4253d4c9ab207"
 cidr: "10.0.0.0/16"
 subnets:
   public:
     us-east-1a:
         id: "subnet-0af58143cd499547c"
         cidr: "10.0.0.0/24"
     us-east-1b:
         id: "subnet-0342b9c54db410a4e"
         cidr: "10.0.2.0/24"
     us-east-1c:
         id: "subnet-007036a437b689c11"
         cidr: "10.0.4.0/24"
     us-east-1e:
         id: "subnet-060196ddd1ae6f536"
         cidr: "10.0.6.0/24"
iam:
     serviceRoleARN: "arn:aws:iam::187632318301:role/eks-service-role"
managedNodeGroups:
 - name: myng1
   instanceType: t3.medium
   desiredCapacity: 2
   minSize: 1
   maxSize: 3
   availabilityZones: ["us-east-1a", "us-east-1b", "us-east-1c", "us-east-1e"]
   volumeSize: 15
#volumeType: gp2
   tags:
    owner: arun
    purpose: ekscluster
   ssh:
    publicKeyName: ttnaccount.pem
    allow: true
~
-- INSERT --                                                                          40,1          All
```



```
arun@Arun-Parmar:~ $ eksctl create cluster newtry
[i]  eksctl version 0.13.0
[i]  using region us-east-1
[i]  setting availability zones to [us-east-1f us-east-1a]
[i]  subnets for us-east-1f - public:192.168.0.0/19 private:192.168.64.0/19
[i]  subnets for us-east-1a - public:192.168.32.0/19 private:192.168.96.0/19
[i]  nodegroup "ng-fa541eaf" will use "ami-087a82f6b78a07557" [AmazonLinux2/1.14]
[i]  using Kubernetes version 1.14
[i]  creating EKS cluster "newtry" in "us-east-1" region with un-managed nodes
[i]  will create 2 separate CloudFormation stacks for cluster itself and the initial nodegroup
[i]  if you encounter any issues, check CloudFormation console or try 'eksctl utils describe-stacks --region=us-east-1 --cluster=newtry'
[i]  CloudWatch logging will not be enabled for cluster "newtry" in "us-east-1"
[i]  you can enable it with 'eksctl utils update-cluster-logging --region=us-east-1 --cluster=newtry'
[i]  Kubernetes API endpoint access will use default of {publicAccess=true, privateAccess=false} for cluster "newtry" in "us-east-1"
[i]  2 sequential tasks: { create cluster control plane "newtry", create nodegroup "ng-fa541eaf" }
[i]  building cluster stack "eksctl-newtry-cluster"
[i]  deploying stack "eksctl-newtry-cluster"
[i]  building nodegroup stack "eksctl-newtry-nodegroup-ng-fa541eaf"
[i]  --nodes-min=2 was set automatically for nodegroup ng-fa541eaf
[i]  --nodes-max=2 was set automatically for nodegroup ng-fa541eaf
[i]  deploying stack "eksctl-newtry-nodegroup-ng-fa541eaf"
[✔]  all EKS cluster resources for "newtry" have been created
[✔]  saved kubeconfig as "/home/arun/.kube/config"
[i]  adding identity "arn:aws:iam::187632318301:role/eksctl-newtry-nodegroup-ng-fa541e-NodeInstanceRole-17DU0KQ9A7F9R" to auth ConfigMap
[i]  nodegroup "ng-fa541eaf" has 0 node(s)
[i]  waiting for at least 2 node(s) to become ready in "ng-fa541eaf"
[i]  nodegroup "ng-fa541eaf" has 2 node(s)
[i]  node "ip-192-168-11-195.ec2.internal" is ready
[i]  node "ip-192-168-46-254.ec2.internal" is ready
[i]  kubectl command should work with "/home/arun/.kube/config", try 'kubectl get nodes'
[✔]  EKS cluster "newtry" in "us-east-1" region is ready
arun@Arun-Parmar:~ $ kubectl get nodes
NAME                             STATUS   ROLES    AGE    VERSION
ip-192-168-11-195.ec2.internal   Ready    <none>   108s   v1.14.8-eks-b8860f
ip-192-168-46-254.ec2.internal   Ready    <none>   113s   v1.14.8-eks-b8860f
arun@Arun-Parmar:~ $ 
```



newtry

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

General configuration

Kubernetes version
1.14

Platform version
eks.9

Status
Active

API server endpoint
https://5BE2BB70940F5373CD7C5CDC1C3ECAA4.gr7.us-east-1.eks.amazonaws.com

OpenID Connect provider URL
https://oidc.eks.us-east-1.amazonaws.com/id/5BE2BB70940F5373CD7C5CDC1C3ECAA4

Certificate authority
LS0tLS1CRUdJTiBDRVJUSUZJQ0FURS0tLS0tCk1JSUN5RENDQWJDZ0F3SUJBZ0lCQURBTkJna3Foa2lHOXcwQk
FRc0ZBREFWTVJNd0VRWURWUVFERXdwcmRXSmwKY201bGRHVnpNQjRYRFRJd01EUXdOREEzTURZek5sb1h
EVE13TURRd01qQTNNRFl6Tmxvd0ZURVRNQkVHQTFVRQpBeE1LYTNWaVpYSnVaWFJsY3pDQ0FTSXdEUVlKS2
9aSWh2Y05BUUVCQlFBRGdnRVBBRENDQVFvQ2dnRUJBTDFqCjNBRFYwY1JNRUNqSzRMSC8zUnhDelhJbzZTN

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

Cluster IAM Role ARN
arn:aws:iam::187632318301:role/eksctl-newtry-cluster-ServiceRole-1PTJBVQAEBF3R

EKS is changing the way that Managed Node Groups assign IP addresses to nodes. This could affect node's ability to connect to the cluster. Learn more

Node Groups (0) Info

Group name	Desired size	AMI release version	Status

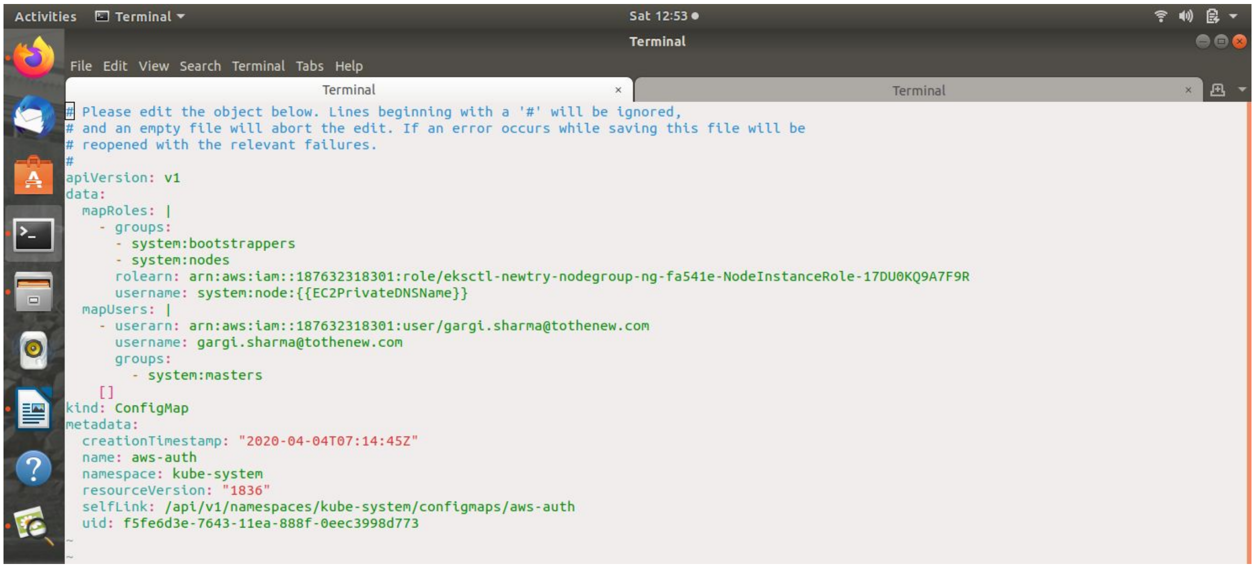
No Managed Node Groups

This cluster does not have any Managed Node Groups.

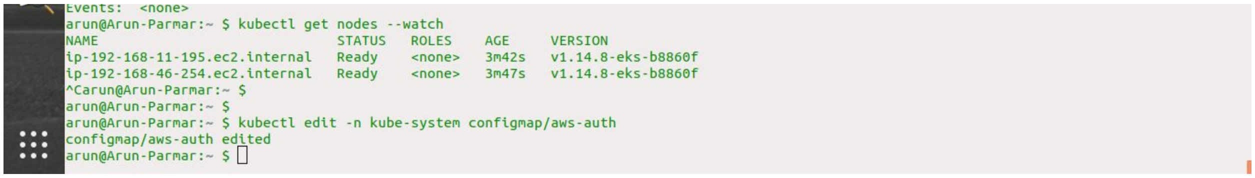
Nodes that are not part of an Amazon EKS Managed Node Group are not shown in the AWS console.

2. Authentication Management

a. Add new 2 IAM user into the cluster



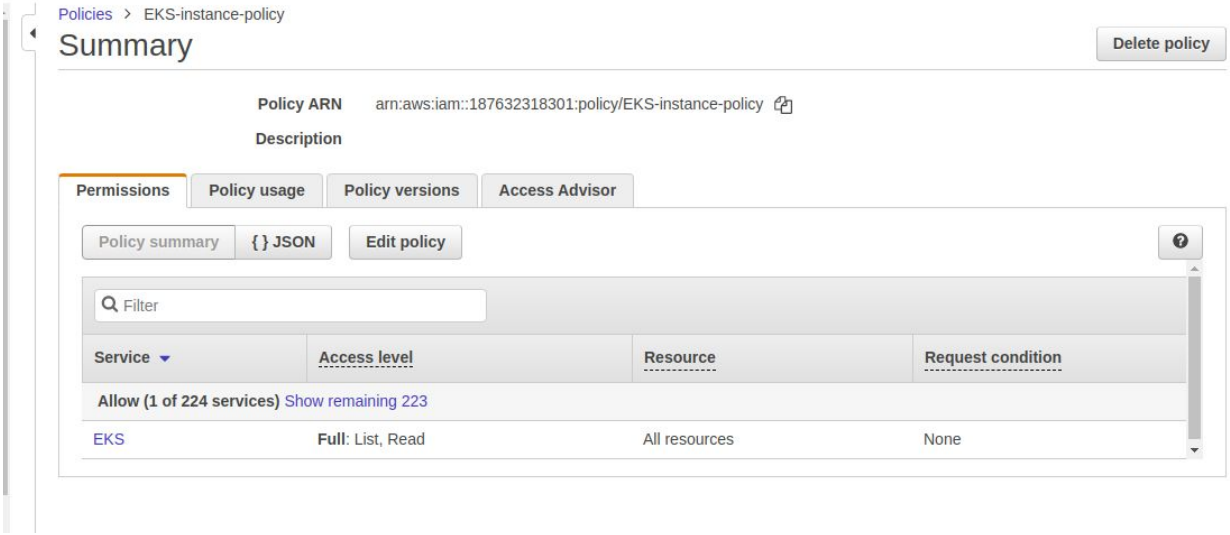
```
# Please edit the object below. Lines beginning with a '#' will be ignored,
# and an empty file will abort the edit. If an error occurs while saving this file will be
# reopened with the relevant failures.
#
apiVersion: v1
data:
  mapRoles: |
    - groups:
      - system:bootstrappers
      - system:nodes
      rolearn: arn:aws:iam::187632318301:role/eksctl-newtry-nodegroup-ng-fa541e-NodeInstanceRole-17DU0KQ9A7F9R
      username: system:node:{{EC2PrivateDNSName}}
  mapUsers: |
    - userarn: arn:aws:iam::187632318301:user/gargi.sharma@tothenew.com
      username: gargi.sharma@tothenew.com
      groups:
        - system:masters
    []
kind: ConfigMap
metadata:
  creationTimestamp: "2020-04-04T07:14:45Z"
  name: aws-auth
  namespace: kube-system
  resourceVersion: "1836"
  selfLink: /api/v1/namespaces/kube-system/configmaps/aws-auth
  uid: f5fe6d3e-7643-11ea-888f-0eec3998d773
~
~
```



```
Events:  <none>
arun@Arun-Parmar:~ $ kubectl get nodes --watch
NAME                             STATUS    ROLES    AGE     VERSION
ip-192-168-11-195.ec2.internal   Ready     <none>   3m42s   v1.14.8-eks-b8860f
ip-192-168-46-254.ec2.internal   Ready     <none>   3m47s   v1.14.8-eks-b8860f
^Carun@Arun-Parmar:~ $
arun@Arun-Parmar:~ $
arun@Arun-Parmar:~ $ kubectl edit -n kube-system configmap/aws-auth
configmap/aws-auth edited
arun@Arun-Parmar:~ $
```

b. Enable a EC2 server to access Cluster master API without using access/secret key

Creating a new policy and specifying EKS as a service



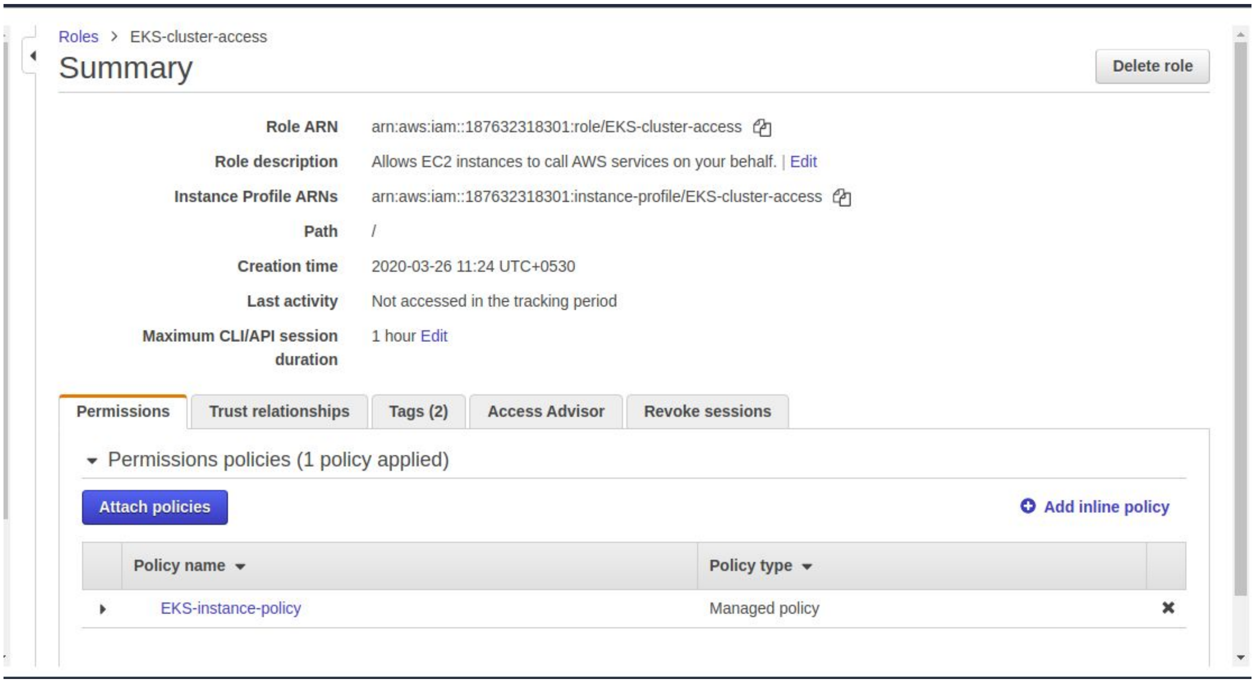
Summary

Policy ARN arn:aws:iam::187632318301:policy/EKS-instance-policy

Description

Service	Access level	Resource	Request condition
Allow (1 of 224 services) Show remaining 223			
EKS	**Full**: List, Read	All resources	None

Creating a role and attaching a policy to the role



Roles > EKS-cluster-access

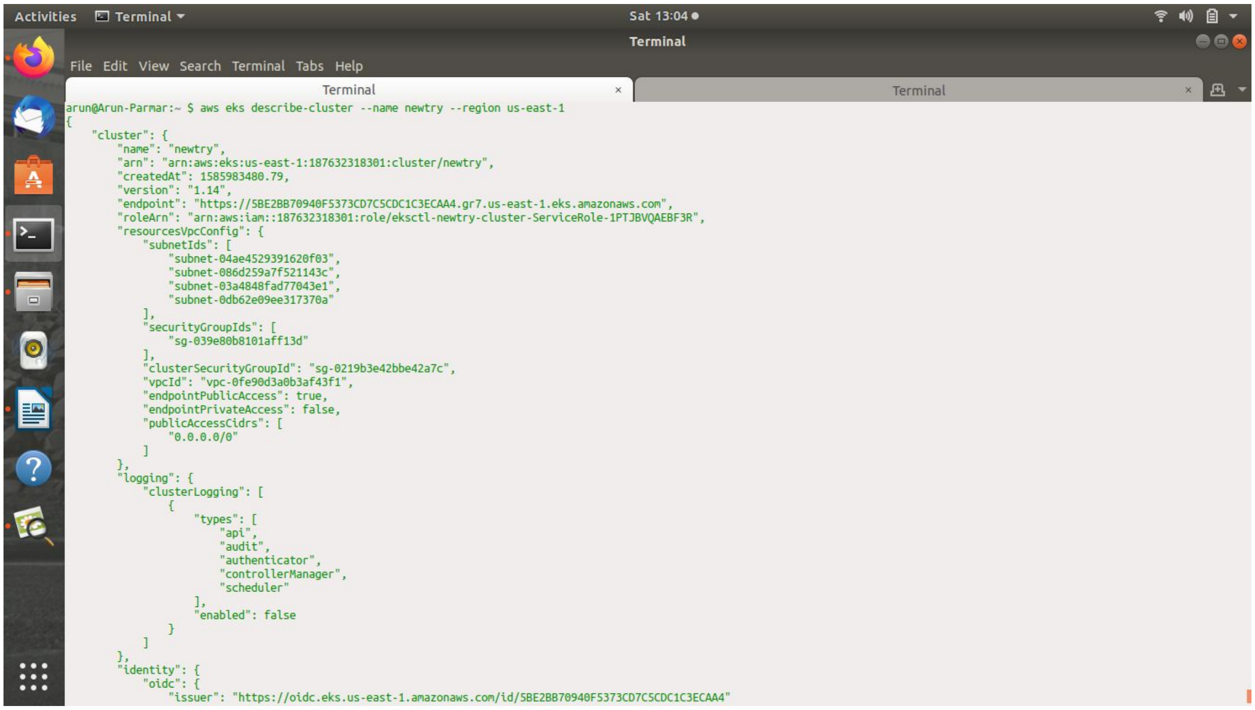
Summary

Role ARN	arn:aws:iam::187632318301:role/EKS-cluster-access
Role description	Allows EC2 instances to call AWS services on your behalf. | Edit
Instance Profile ARNs	arn:aws:iam::187632318301:instance-profile/EKS-cluster-access
Path	/
Creation time	2020-03-26 11:24 UTC+0530
Last activity	Not accessed in the tracking period
Maximum CLI/API session duration	1 hour Edit

Permissions policies (1 policy applied)

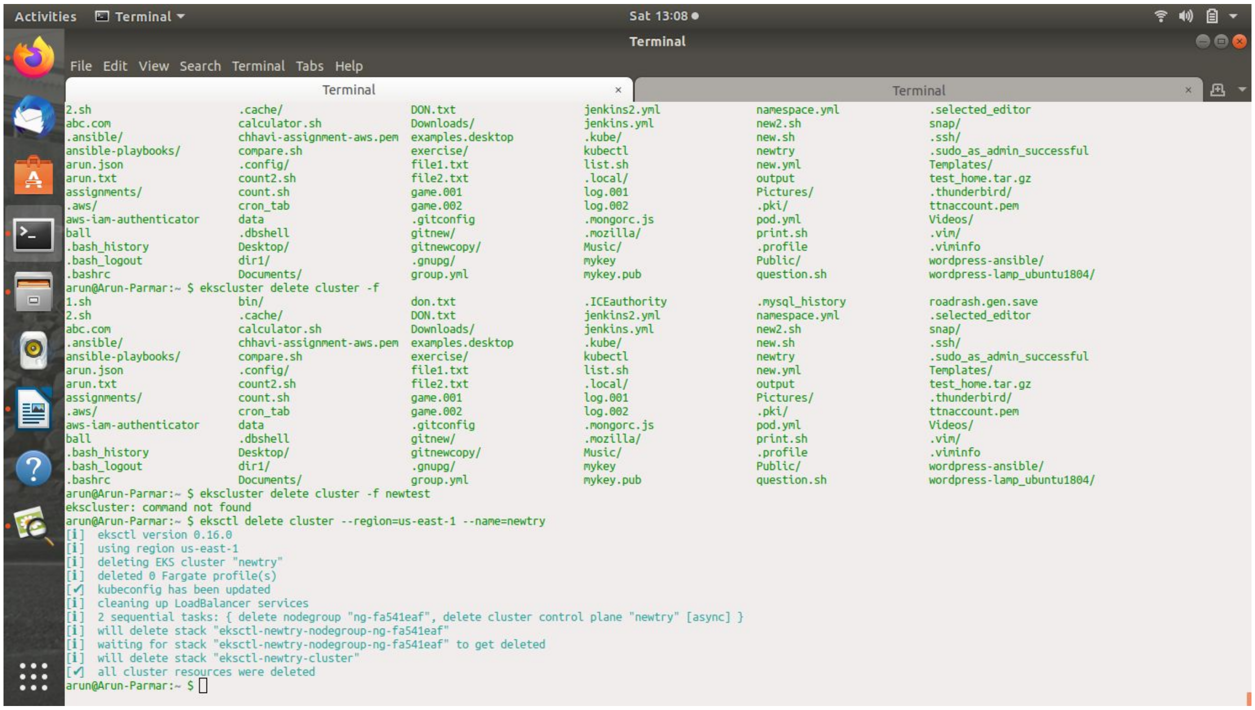
Policy name	Policy type
EKS-instance-policy	Managed policy

$$ aws eks describe-cluster --name newtry --region us-east-1



```
arun@Arun-Parmar:~ $ aws eks describe-cluster --name newtry --region us-east-1
{
    "cluster": {
        "name": "newtry",
        "arn": "arn:aws:eks:us-east-1:187632318301:cluster/newtry",
        "createdAt": 1585983480.79,
        "version": "1.14",
        "endpoint": "https://5BE2BB70940F5373CD7C5CDC1C3ECAA4.gr7.us-east-1.eks.amazonaws.com",
        "roleArn": "arn:aws:iam::187632318301:role/eksctl-newtry-cluster-ServiceRole-1PTJBVQAEBF3R",
        "resourcesVpcConfig": {
            "subnetIds": [
                "subnet-04ae4529391620f03",
                "subnet-086d259a7f521143c",
                "subnet-03a4848fad77043e1",
                "subnet-0db62e09ee317370a"
            ],
            "securityGroupIds": [
                "sg-039e80b8101aff13d"
            ],
            "clusterSecurityGroupId": "sg-0219b3e42bbe42a7c",
            "vpcId": "vpc-0fe90d3a0b3af43f1",
            "endpointPublicAccess": true,
            "endpointPrivateAccess": false,
            "publicAccessCidrs": [
                "0.0.0.0/0"
            ]
        },
        "logging": {
            "clusterLogging": [
                {
                    "types": [
                        "api",
                        "audit",
                        "authenticator",
                        "controllerManager",
                        "scheduler"
                    ],
                    "enabled": false
                }
            ]
        },
        "identity": {
            "oidc": {
                "issuer": "https://oidc.eks.us-east-1.amazonaws.com/id/5BE2BB70940F5373CD7C5CDC1C3ECAA4"
```

3. Eksctl command to terminate the stack



```
2.sh                       .cache/                    DON.txt                    jenkins2.yml               namespace.yml              .selected_editor
abc.com                    calculator.sh              Downloads/                 jenkins.yml                new2.sh                    snap/
.ansible/                  chhavi-assignment-aws.pem  examples.desktop           .kube/                     new.sh                     .ssh/
ansible-playbooks/         compare.sh                 exercise/                  kubectl                    newtry                     .sudo_as_admin_successful
arun.json                  .config/                   file1.txt                  list.sh                    new.yml                    Templates/
arun.txt                   count2.sh                  file2.txt                  .local/                    output                     test_home.tar.gz
assignments/               count.sh                   game.001                   log.001                    Pictures/                  .thunderbird/
.aws/                      cron_tab                   game.002                   log.002                    .pki/                      ttnaccount.pem
aws-iam-authenticator      data                       .gitconfig                 .mongorc.js                pod.yml                    Videos/
ball                       .dbshell                   gitnew/                    .mozilla/                  print.sh                   .vim/
.bash_history              Desktop/                   gitnewcopy/                Music/                     .profile                   .viminfo
.bash_logout               dir1/                      .gnupg/                    mykey                      Public/                    wordpress-ansible/
.bashrc                    Documents/                 group.yml                  mykey.pub                  question.sh                wordpress-lamp_ubuntu1804/
arun@Arun-Parmar:~ $ ekscluster delete cluster -f
1.sh                       bin/                       don.txt                    .ICEauthority              .mysql_history             roadrash.gen.save
2.sh                       .cache/                    DON.txt                    jenkins2.yml               namespace.yml              .selected_editor
abc.com                    calculator.sh              Downloads/                 jenkins.yml                new2.sh                    snap/
.ansible/                  chhavi-assignment-aws.pem  examples.desktop           .kube/                     new.sh                     .ssh/
ansible-playbooks/         compare.sh                 exercise/                  kubectl                    newtry                     .sudo_as_admin_successful
arun.json                  .config/                   file1.txt                  list.sh                    new.yml                    Templates/
arun.txt                   count2.sh                  file2.txt                  .local/                    output                     test_home.tar.gz
assignments/               count.sh                   game.001                   log.001                    Pictures/                  .thunderbird/
.aws/                      cron_tab                   game.002                   log.002                    .pki/                      ttnaccount.pem
aws-iam-authenticator      data                       .gitconfig                 .mongorc.js                pod.yml                    Videos/
ball                       .dbshell                   gitnew/                    .mozilla/                  print.sh                   .vim/
.bash_history              Desktop/                   gitnewcopy/                Music/                     .profile                   .viminfo
.bash_logout               dir1/                      .gnupg/                    mykey                      Public/                    wordpress-ansible/
.bashrc                    Documents/                 group.yml                  mykey.pub                  question.sh                wordpress-lamp_ubuntu1804/
arun@Arun-Parmar:~ $ ekscluster delete cluster -f newtest
ekscluster: command not found
arun@Arun-Parmar:~ $ eksctl delete cluster --region=us-east-1 --name=newtry
[i]  eksctl version 0.16.0
[i]  using region us-east-1
[i]  deleting EKS cluster "newtry"
[i]  deleted 0 Fargate profile(s)
[✓]  kubeconfig has been updated
[i]  cleaning up LoadBalancer services
[i]  2 sequential tasks: { delete nodegroup "ng-fa541eaf", delete cluster control plane "newtry" [async] }
[i]  will delete stack "eksctl-newtry-nodegroup-ng-fa541eaf"
[i]  waiting for stack "eksctl-newtry-nodegroup-ng-fa541eaf" to get deleted
[i]  will delete stack "eksctl-newtry-cluster"
[✓]  all cluster resources were deleted
arun@Arun-Parmar:~ $ 
```