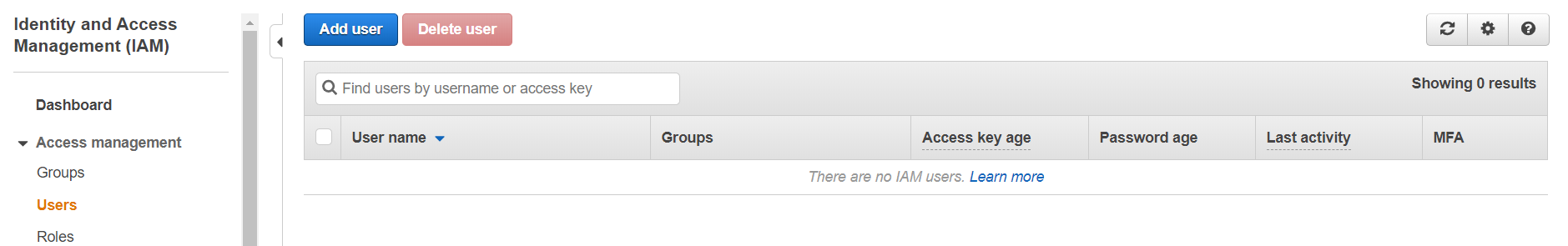
**Create Kubernates clustur with EKS**

**Prerequisits to create EKS Cluster:**

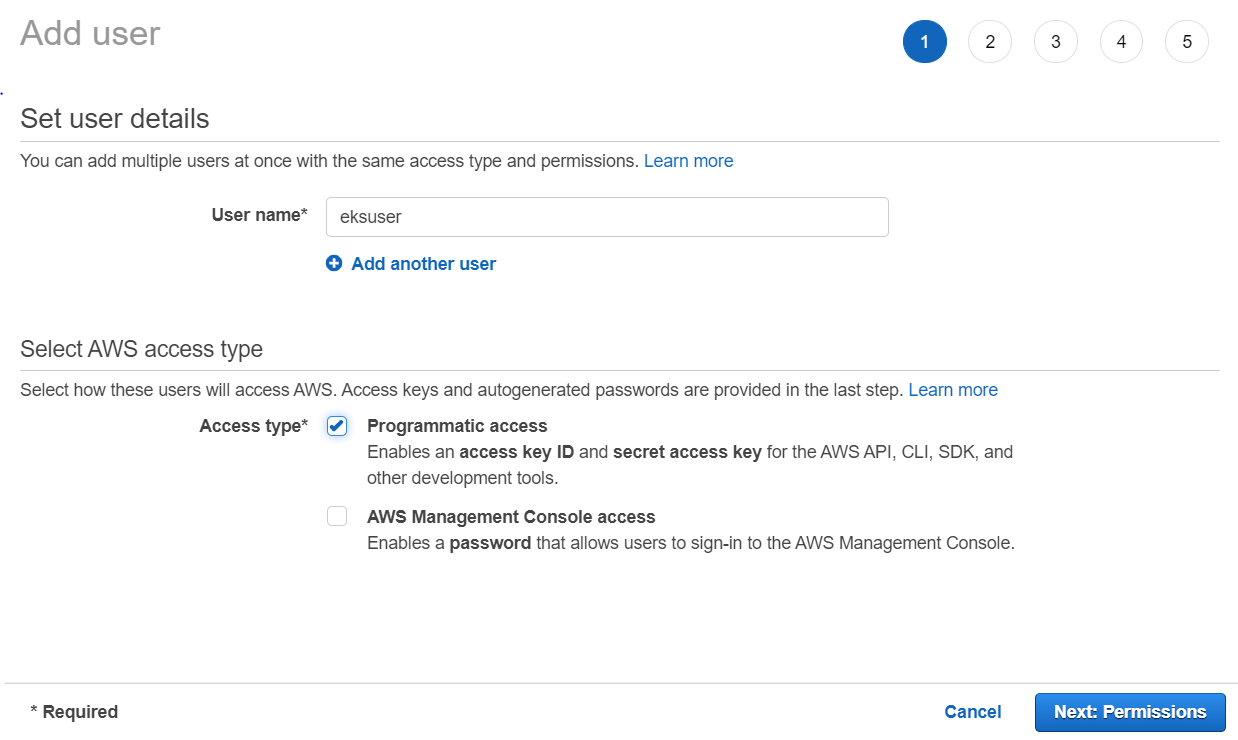
* IAM Role
* VPC
* Install and Configure kubectl
* AWSCLI

**Create user:**

Goto IAM and click on user

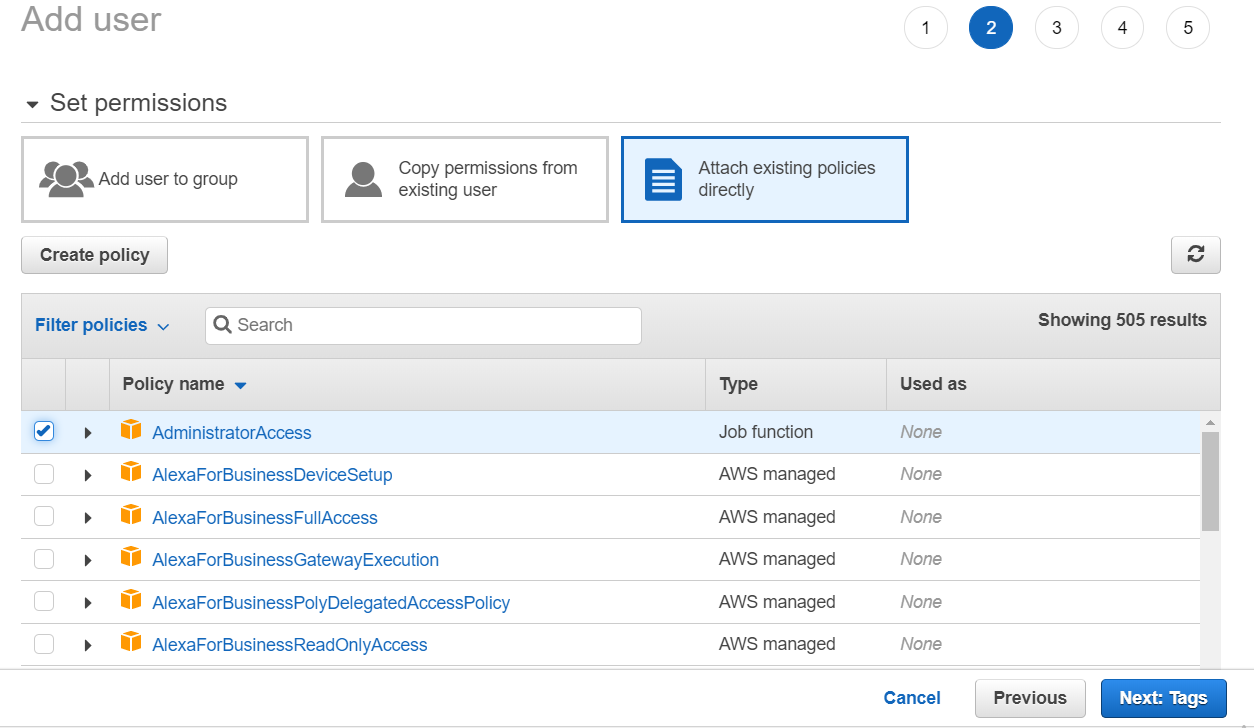


Click on Add user



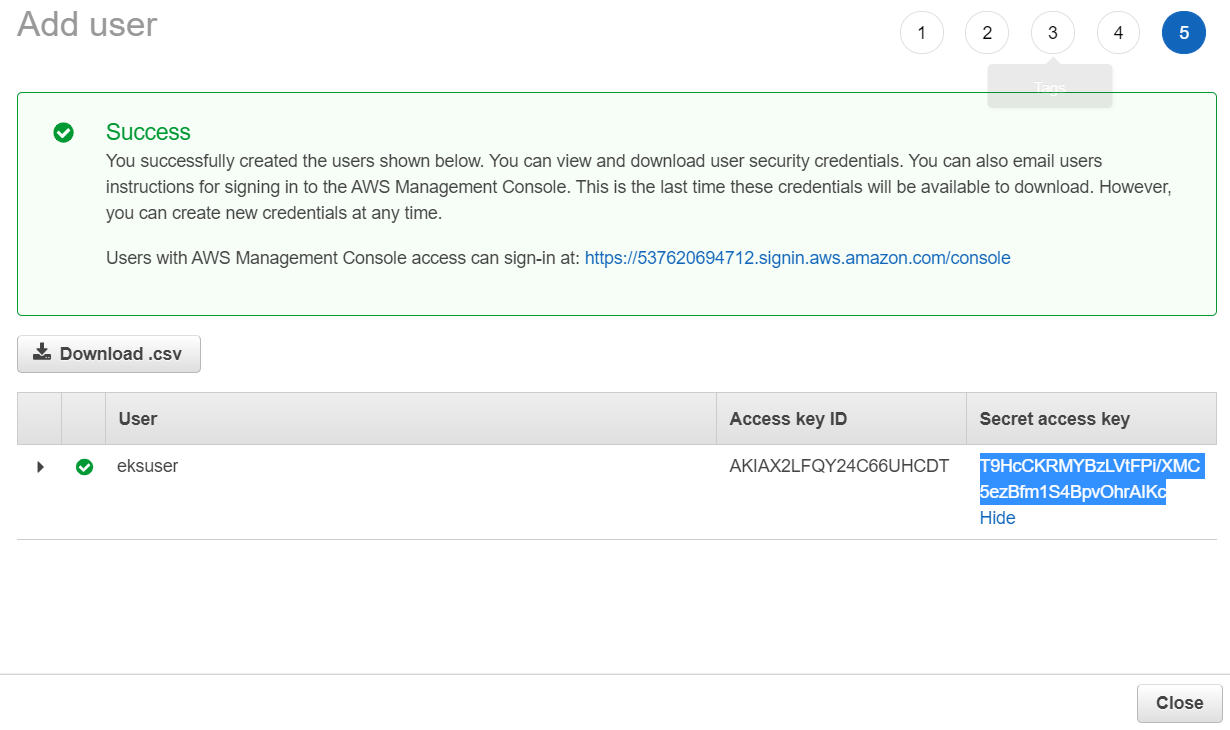
Give any name for user and check Accesstype as Programmatic access

Click on Next



Add tag as Administrator and click on next

Click on create



Here user created and copy Access key ID and Secret access key

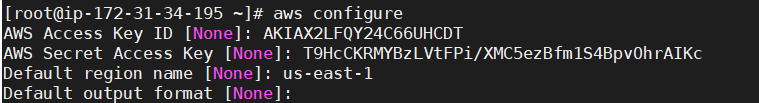
These Access Key ID and Secret access key gives to configure aws

**AWS-CLI Installation:**

yum install python2-pip –y

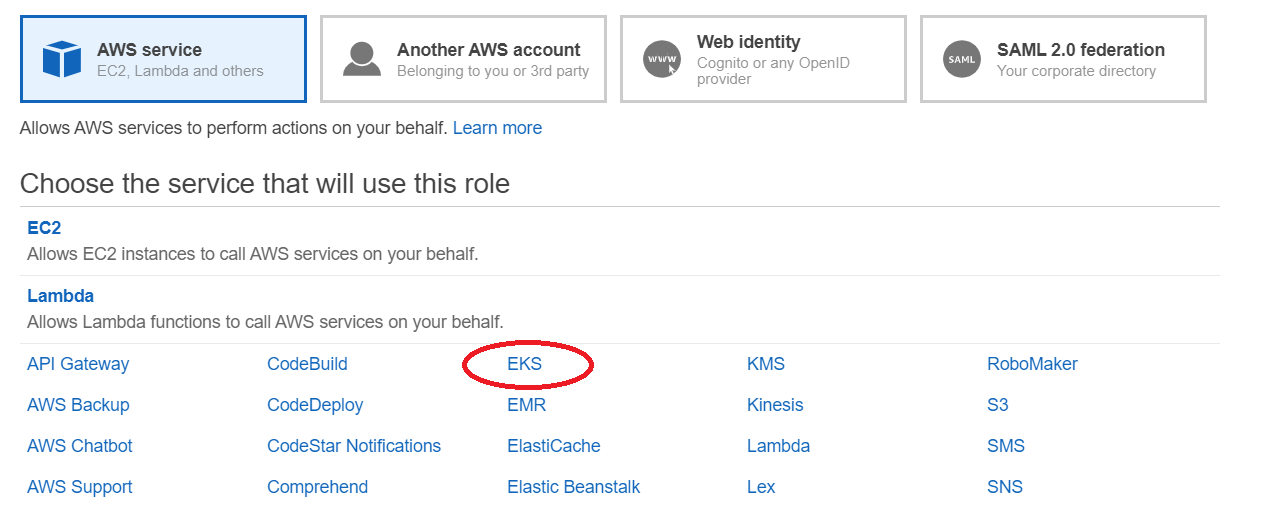
pip2 install awscli

aws configure

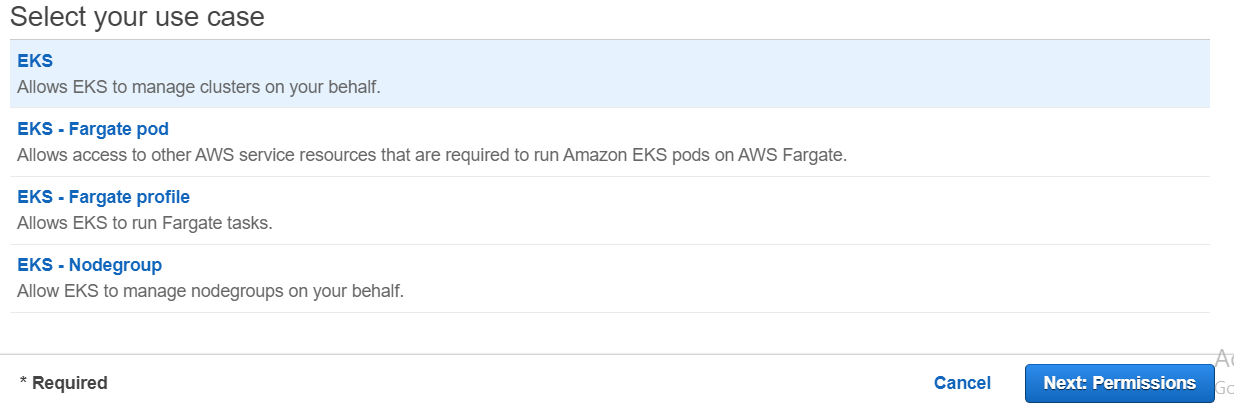


**To create Role For EKS:**

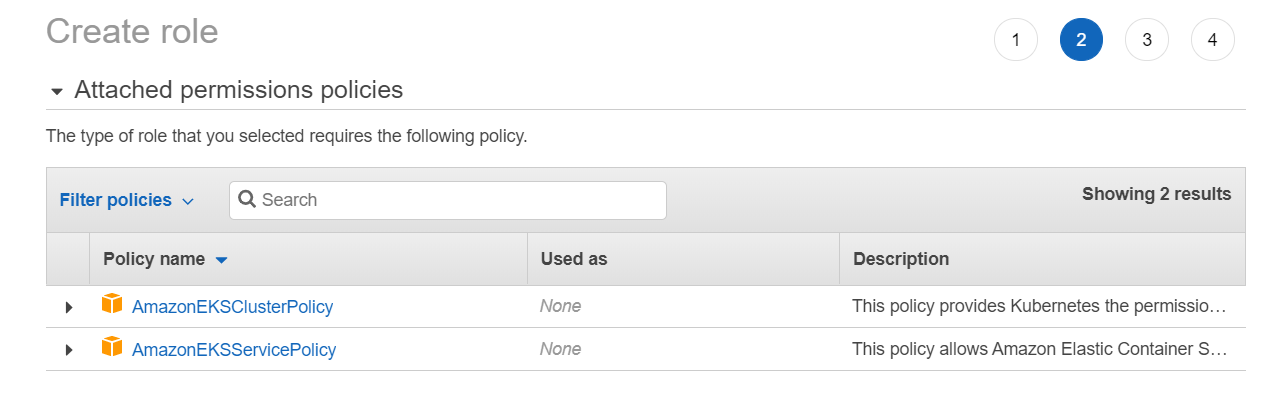
* Click on Create Role
* Click on EKS



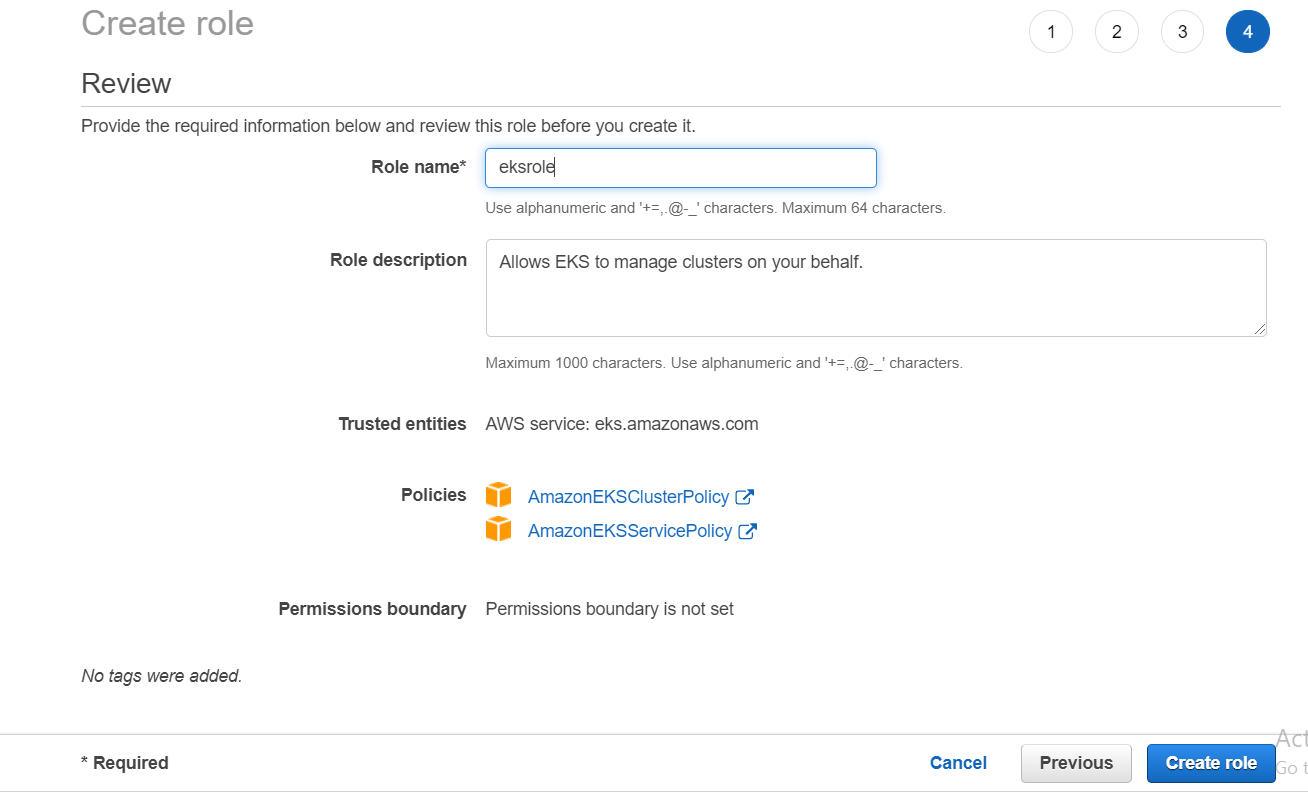
* Click on EKS again and then click on Next



* We will get window like this



* Click on Next
* Give Role Name as “eksrole” and click create role



**Kubectl**: Used for communicating with the cluster API server

curl -o kubectl https://amazon-eks.s3-us-west-2.amazonaws.com/1.14.6/2019-08-22/bin/linux/amd64/kubectl

chmod +x ./kubectl

mkdir -p $HOME/bin

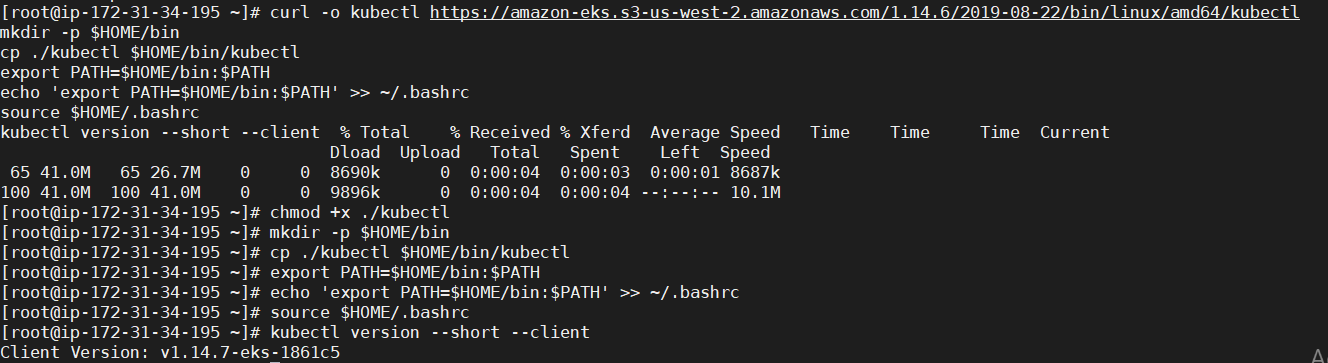
cp ./kubectl $HOME/bin/kubectl

export PATH=$HOME/bin:$PATH

echo 'export PATH=$HOME/bin:$PATH' >> ~/.bashrc

source $HOME/.bashrc

kubectl version --short --client



**AWS-IAM-Authenticator:** To allow IAM authentication with the Kubernetes cluster

curl -o aws-iam-authenticator https://amazon-eks.s3-us-west-2.amazonaws.com/1.14.6/2019-08-22/bin/linux/amd64/aws-iam-authenticator

chmod +x ./aws-iam-authenticator

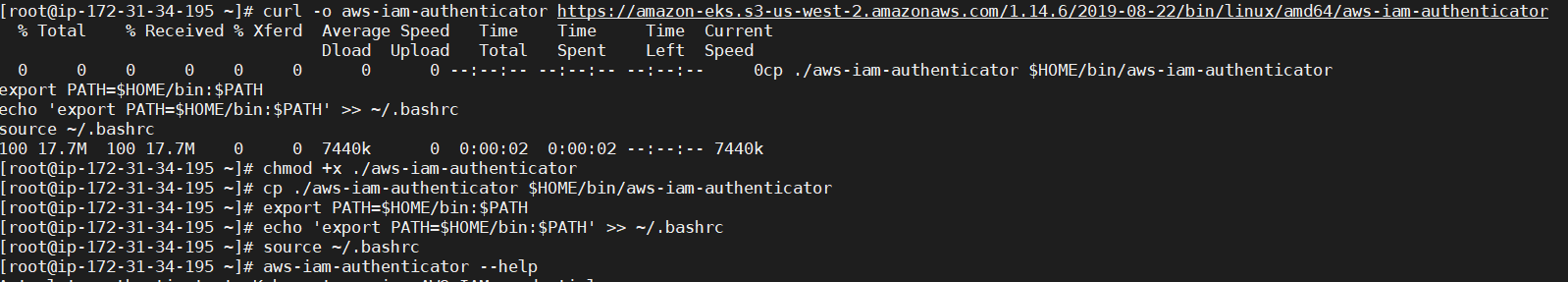
cp ./aws-iam-authenticator $HOME/bin/aws-iam-authenticator

export PATH=$HOME/bin:$PATH

echo 'export PATH=$HOME/bin:$PATH' >> ~/.bashrc

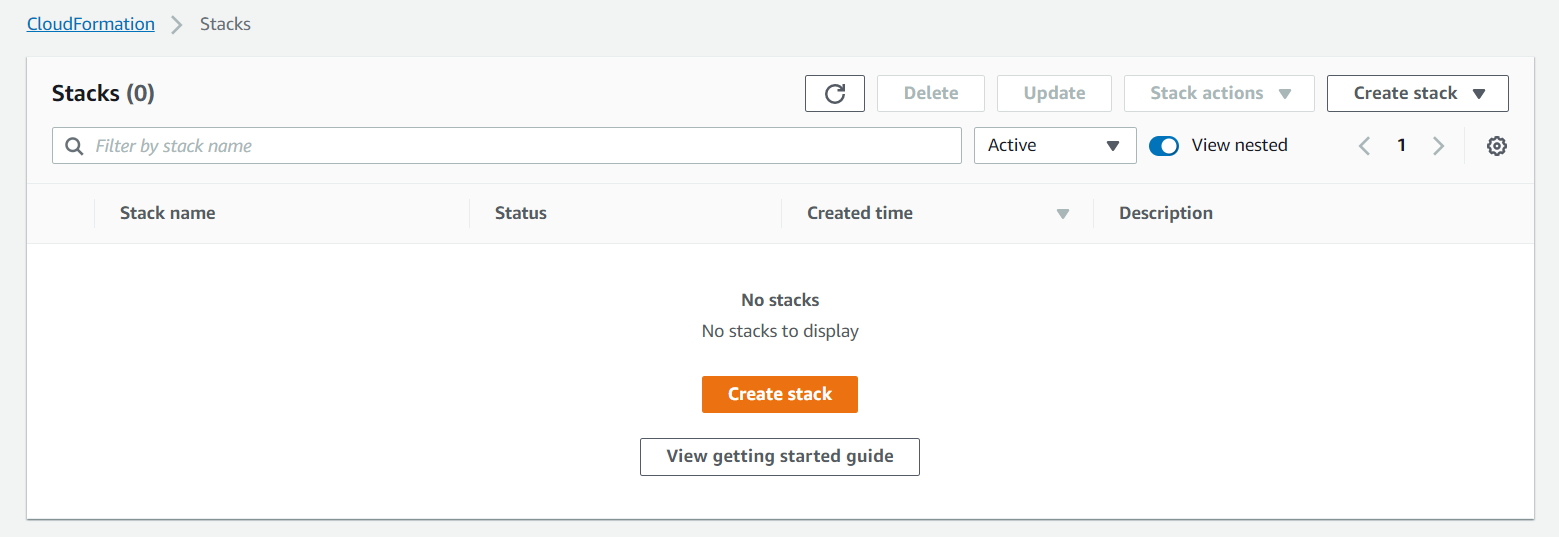
source ~/.bashrc

aws-iam-authenticator --help

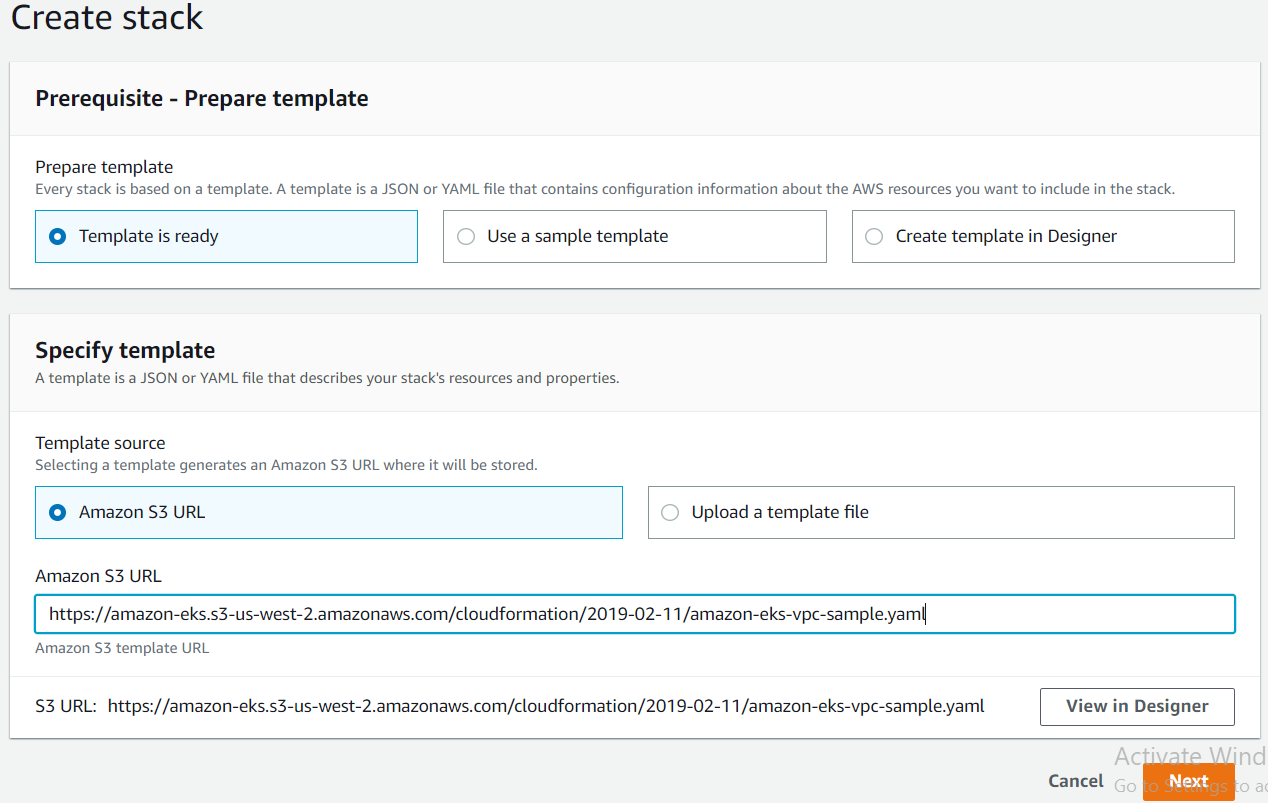


**Create VPC for EKS:**

Open Cloud Formation



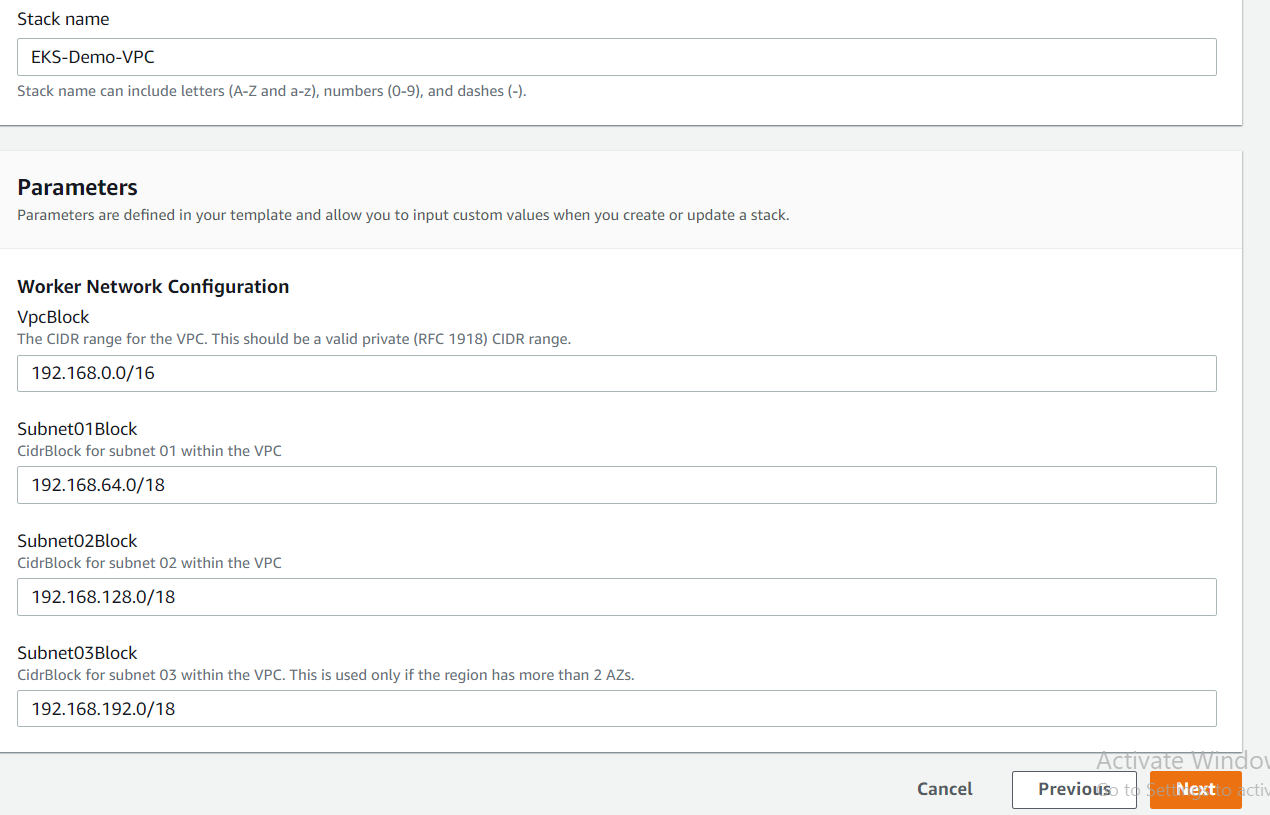
* Click on Stack



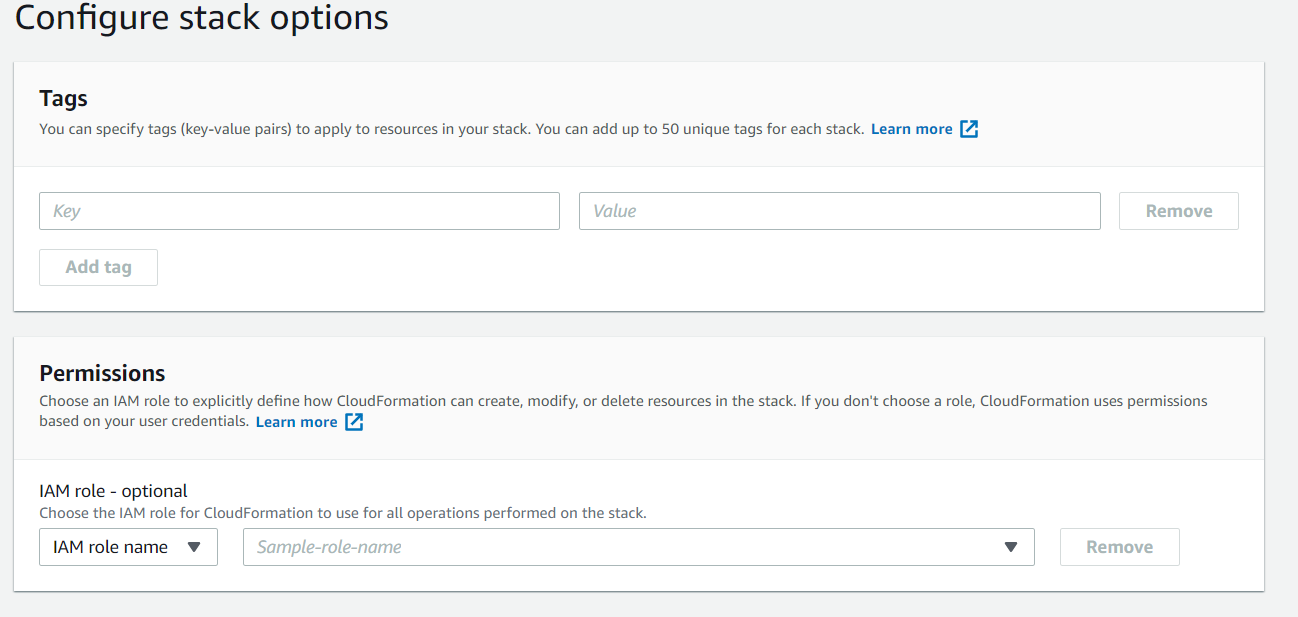
* Give Amazon S3 URL-

https://amazon-eks.s3-us-west-2.amazonaws.com/cloudformation/2019-02-11/amazon-eks-vpc-sample.yaml

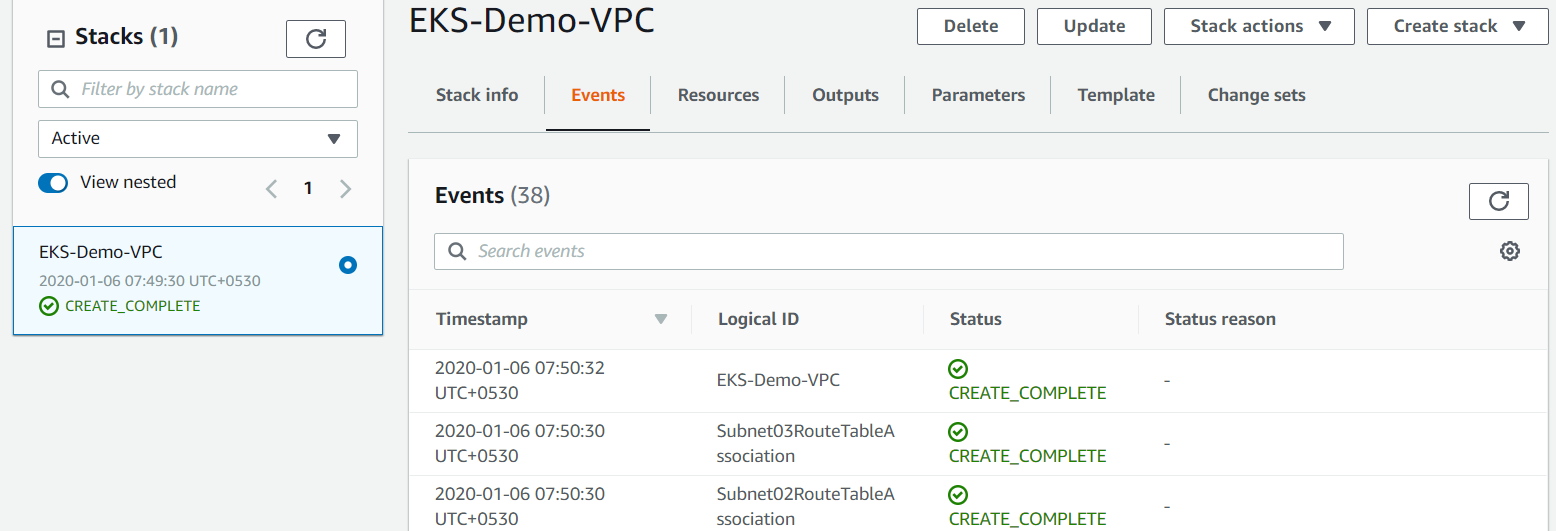
* Click on Next



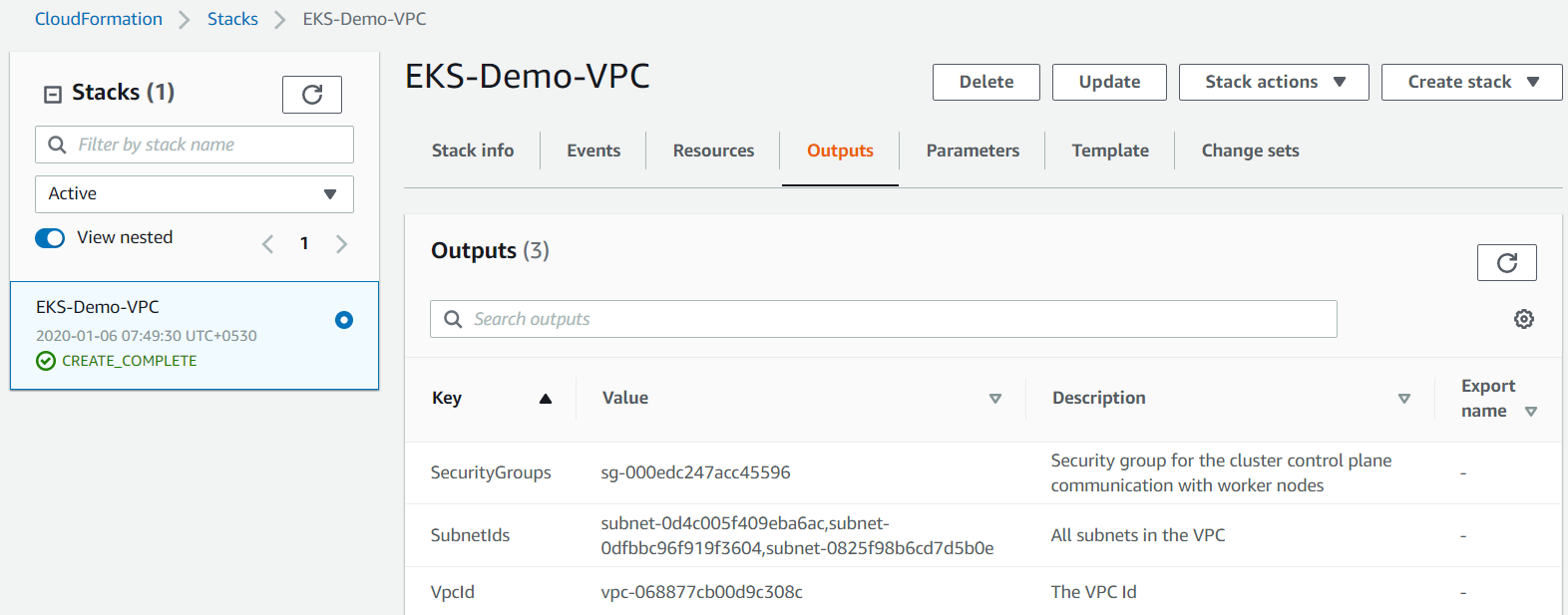
Give Stack name and click on next



Click on Next and Click on Create stack



Once complete stack creation click on outputs and check details



* The **SecurityGroups** value for the security group that was created. We need this when we create our EKS cluster; this security group is applied to the cross-account elastic network interfaces that are created in our subnets that allow the Amazon EKS control plane to communicate with our worker nodes.
* The **VpcId** for the subnets that were created. We need this when we launch our worker node group template.
* The **SubnetIds** for the subnets that were created. We need this when we create our EKS cluster; these are the subnets that our worker nodes are launched into.

**Create EKS Cluster:**

aws eks create-cluster \

--name eks-cluster \

--region us-east-1 \

--role-arn arn:aws:iam::537620694712:role/eksrole \

--resources-vpc-config subnetIds=subnet-0a2f539a235f0dd7b,subnet-01fedcb962af95dc2,subnet-05946f6e63b9511c5,securityGroupIds=sg-0abaaab7d23429e60

**Executing this command, you should see the following output in your terminal:**

{

"cluster": {

"status": "CREATING",

"logging": {

"clusterLogging": [

{

"enabled": false,

"types": [

"api",

"audit",

"authenticator",

"controllerManager",

"scheduler"

]

}

]

},

"name": "eks-cluster",

"tags": {},

"certificateAuthority": {},

"roleArn": "arn:aws:iam::537620694712:role/eksrole",

"resourcesVpcConfig": {

"vpcId": "vpc-077e064e6f416ac6a",

"subnetIds": [

"subnet-0a2f539a235f0dd7b",

"subnet-01fedcb962af95dc2",

"subnet-05946f6e63b9511c5"

],

"securityGroupIds": [

"sg-0abaaab7d23429e60"

],

"publicAccessCidrs": [

"0.0.0.0/0"

],

"endpointPublicAccess": true,

"endpointPrivateAccess": false

},

"version": "1.14",

"arn": "arn:aws:eks:us-east-1:537620694712:cluster/eks-cluster",

"platformVersion": "eks.7",

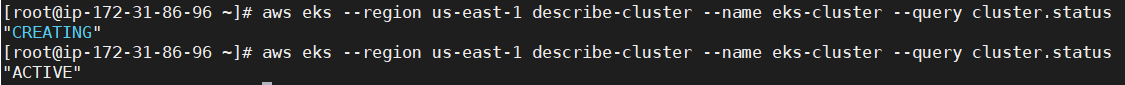
"createdAt": 1578314457.928

}

}

To check status of Cluster:

aws eks --region us-east-1 describe-cluster --name eks-cluster --query cluster.status



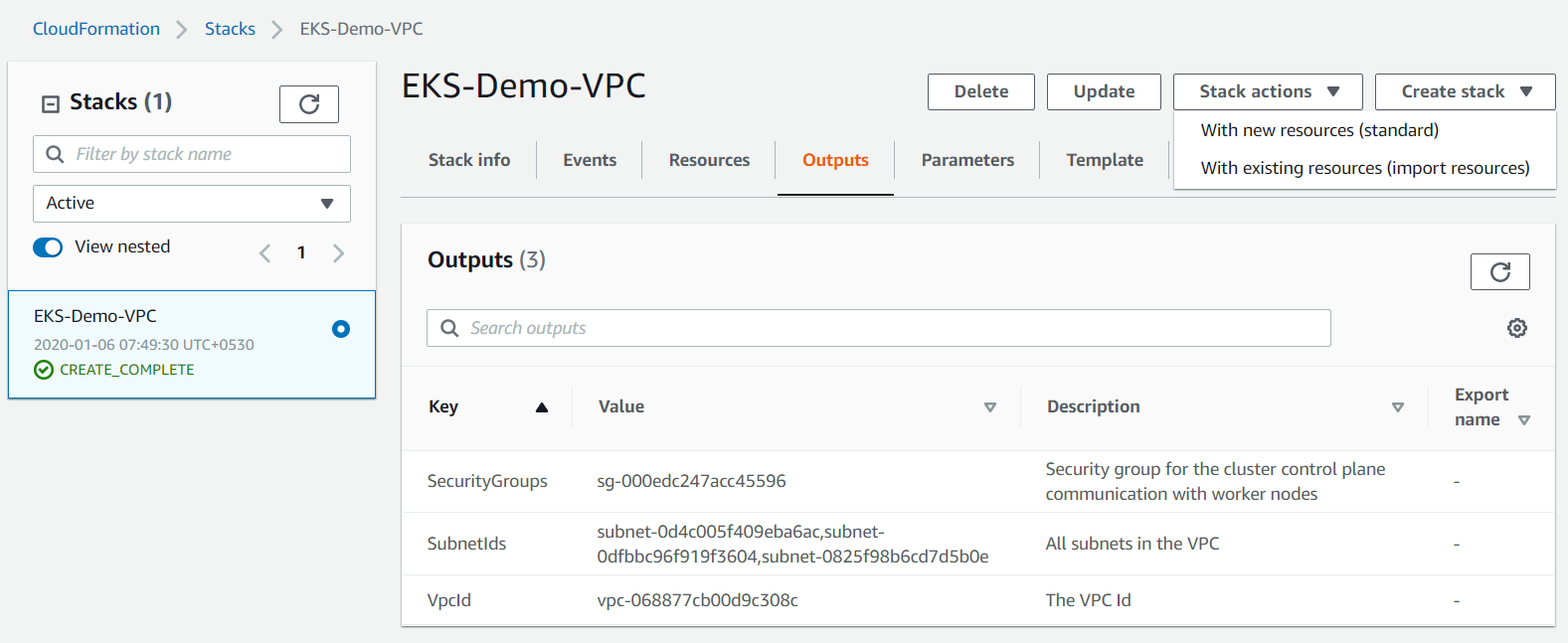
After Creation of Cluster need to Update:

aws eks --region us-east-1 update-kubeconfig --name eks-cluster

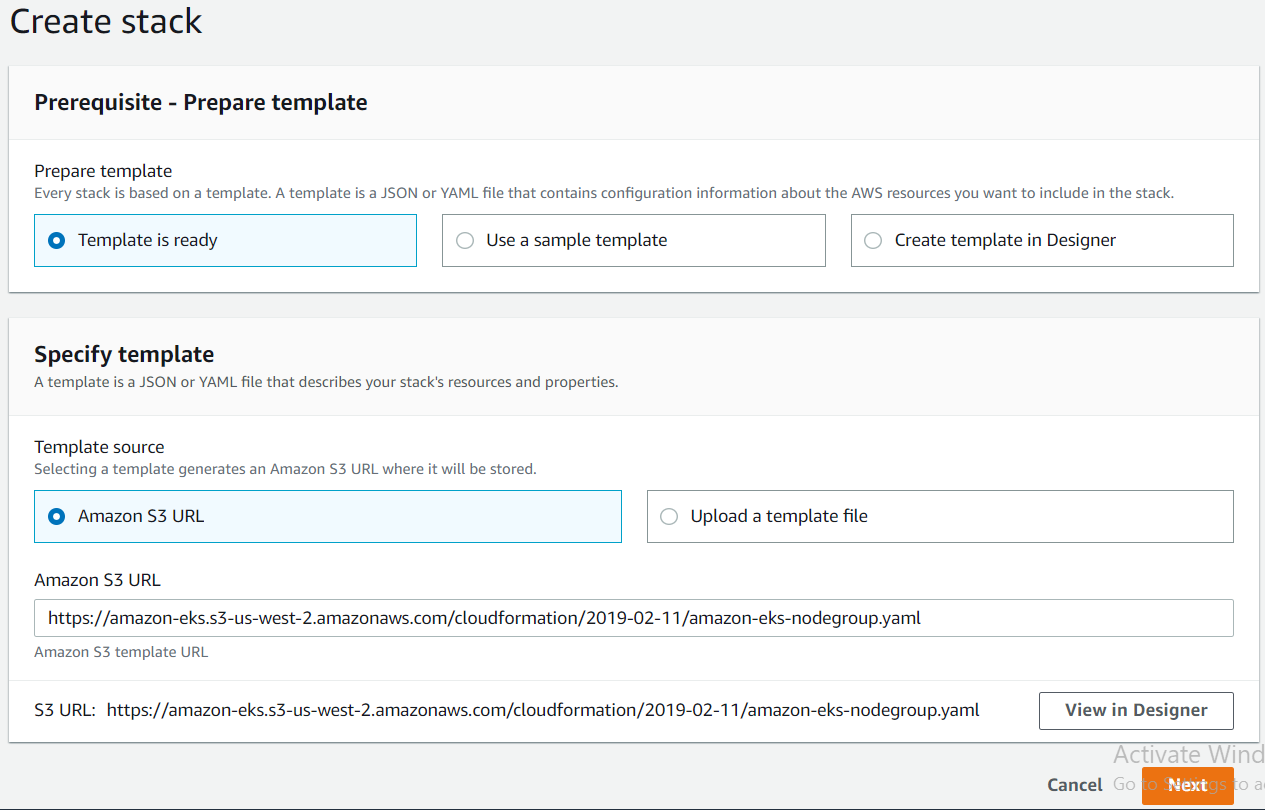
**C:\Users\hp\Desktop\Naresh\Capture.PNG**

**Launching Kubernetes worker nodes:**

Click on Create Stack



Click on with new resources



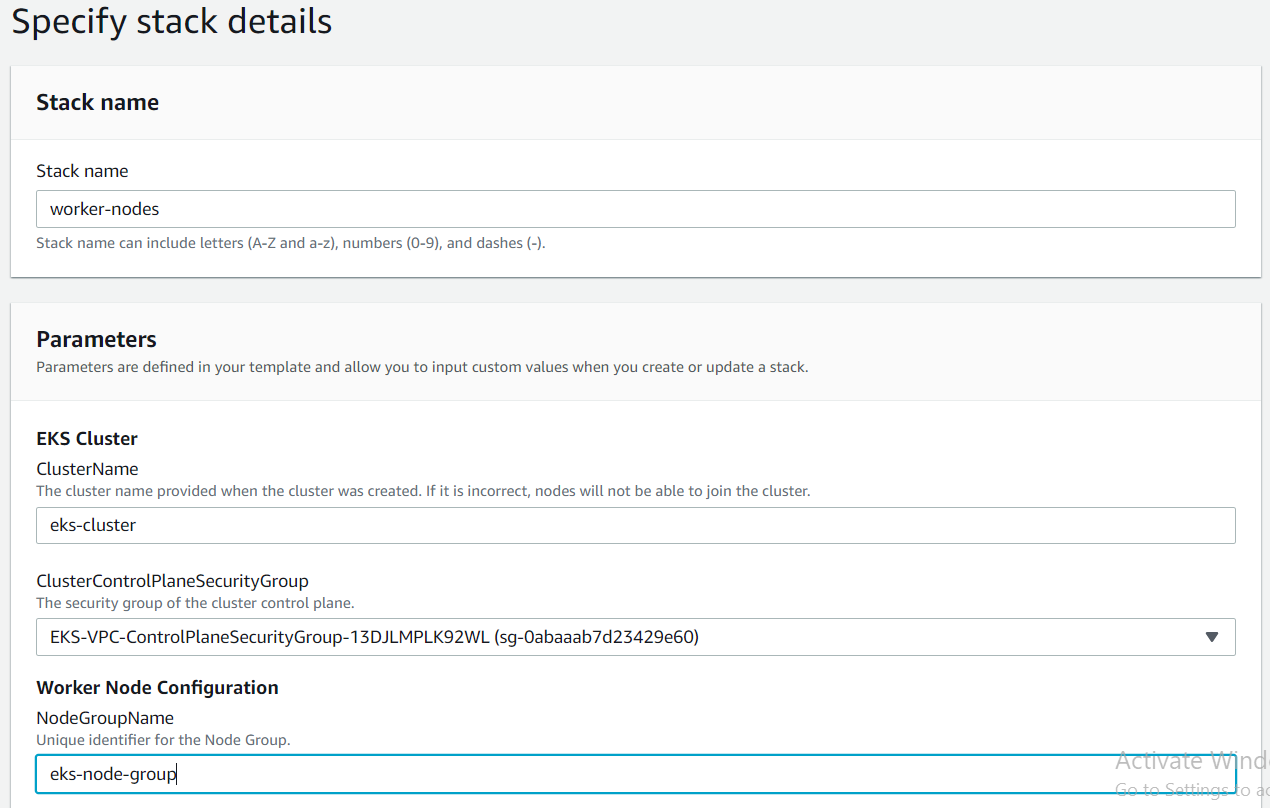
**Give below link at Amazon S3 URL to create nodes:**

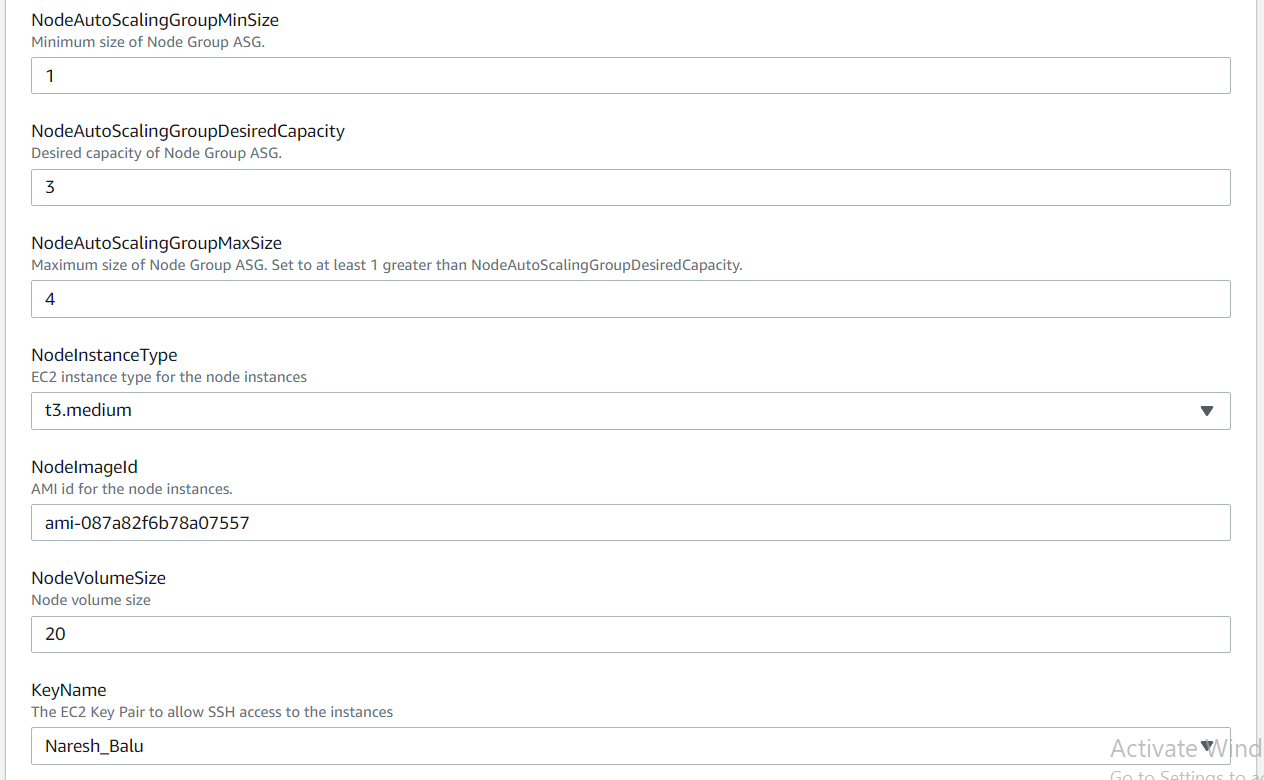
<https://amazon-eks.s3-us-west-2.amazonaws.com/cloudformation/2019-02-11/amazon-eks-nodegroup.yaml>

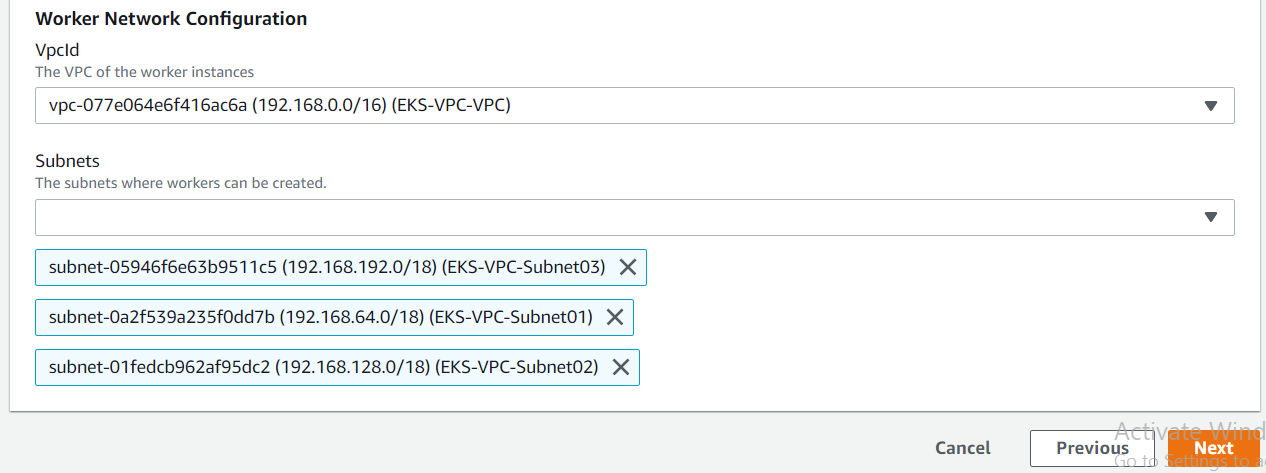
Fill details as shown below

Note: Give details for Security group, VPC and Subnets (These details we get at output of VPC creation for EKS)

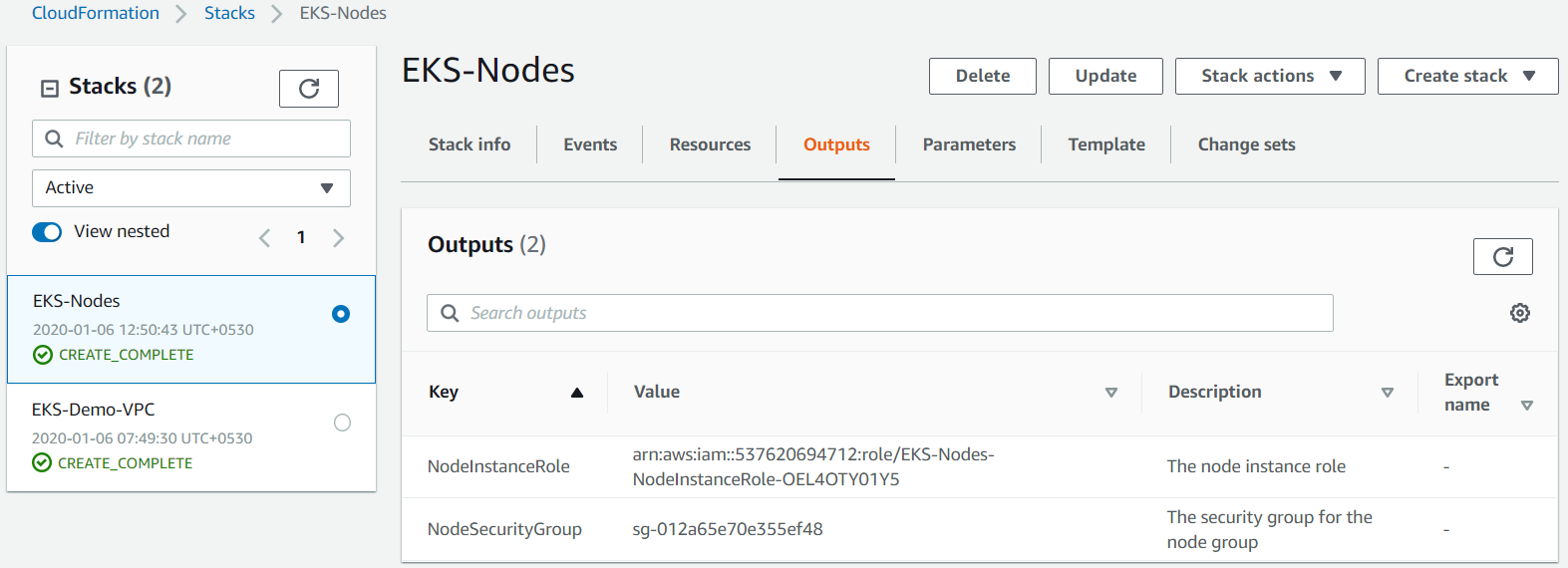
Worker Node AMI - **ami-087a82f6b78a07557** (Should give this only for US-EAST-1)







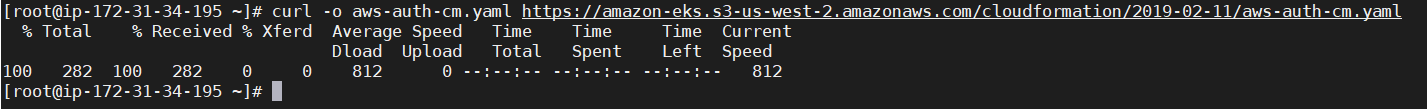
Nodes created for EKS Cluster and Copy Role **arn** (we get at output tab)

****

* **To enable worker nodes to join your cluster:**

Download the AWS authenticator configuration map

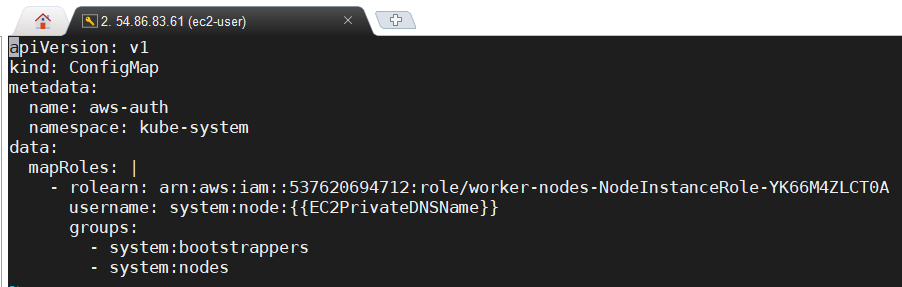
curl -o aws-auth-cm.yaml <https://amazon-eks.s3-us-west-2.amazonaws.com/cloudformation/2019-02-11/aws-auth-cm.yaml>

****

vi aws-auth-cm.yaml

Change relearn which one is created while creating worker nodes

arn:aws:iam::537620694712:role/worker-nodes-NodeInstanceRole-YK66M4ZLCT0A

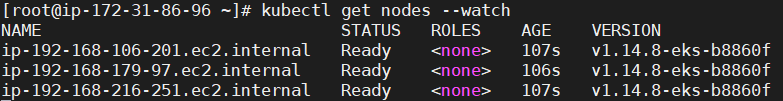
****

kubectl apply -f aws-auth-cm.yaml

**C:\Users\hp\Desktop\Naresh\Capture.PNG**

Nodes added to cluster. Check by using below command.

kubectl get nodes --watch

****