**8: Verify EKS Cluster & Nodes**

**Verify Nodegroups subnets to confirm EC2 Instances are in Public Subnet**

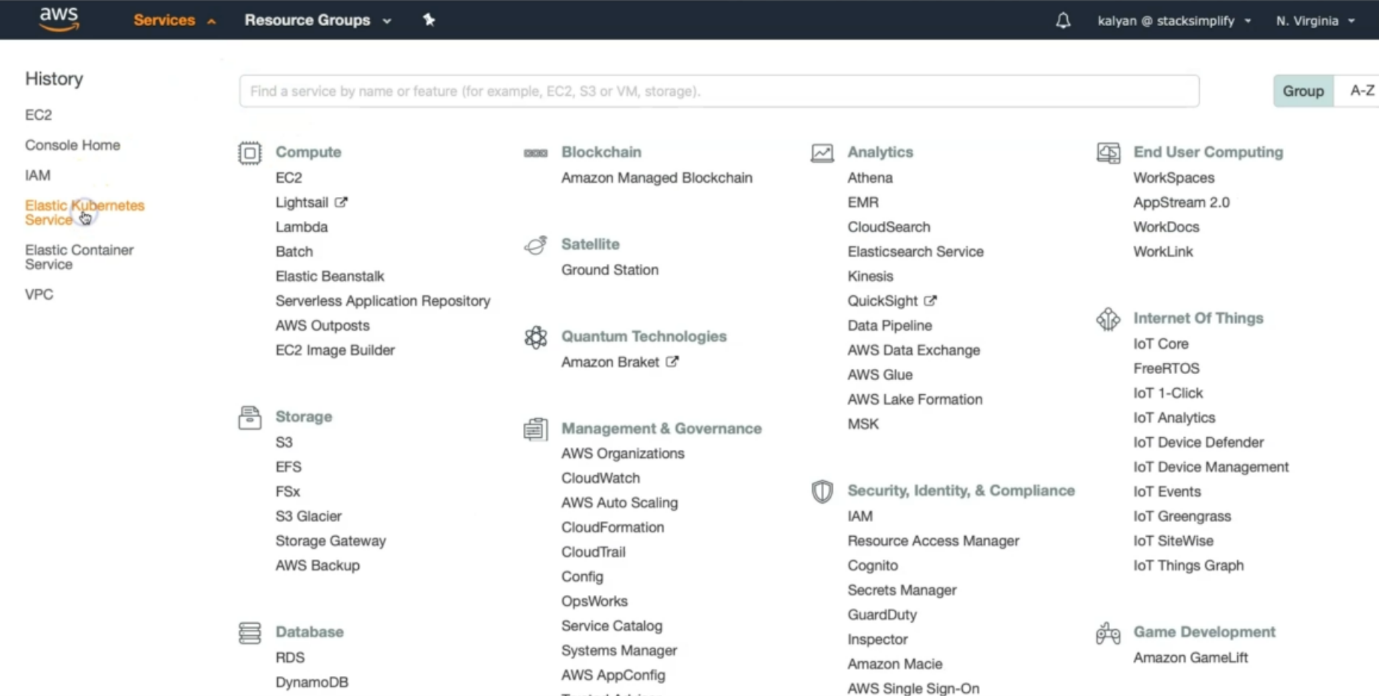
--- Verify the node group subnet to ensure it created in public subnets

I, Go to Services -> EKS -> eksdemo -> eksdemo1-ng1-public

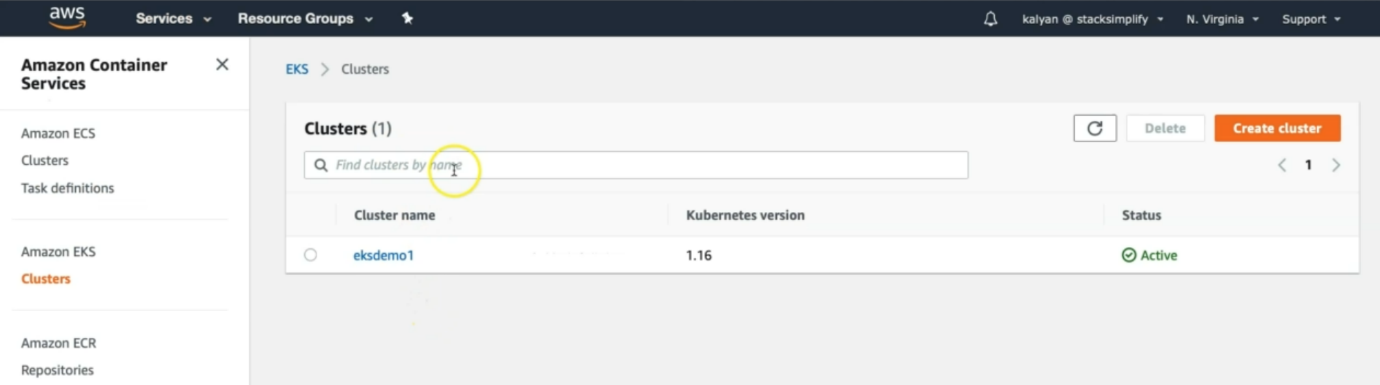
ii, Click on Associated subnet in Details tab

iii, Click on Route Table Tab.

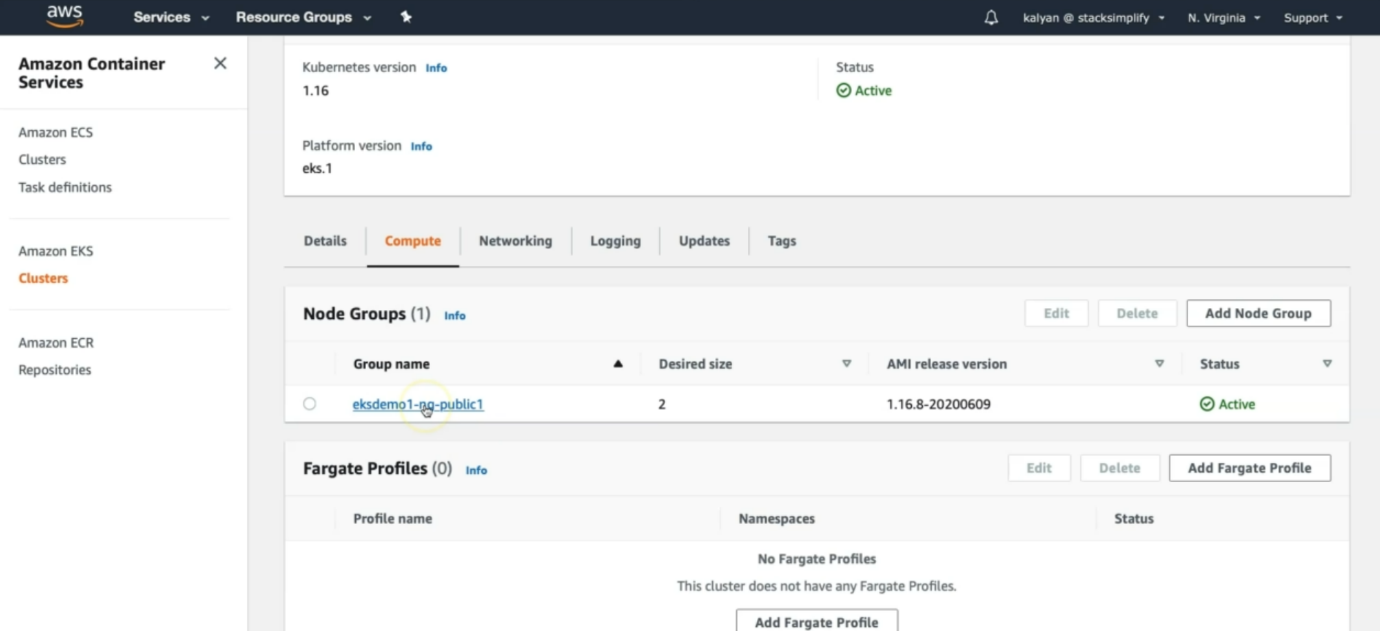
Iv, We should see that internet route via Internet Gateway (0.0.0.0/0 -> igw-xxxxxxxx)



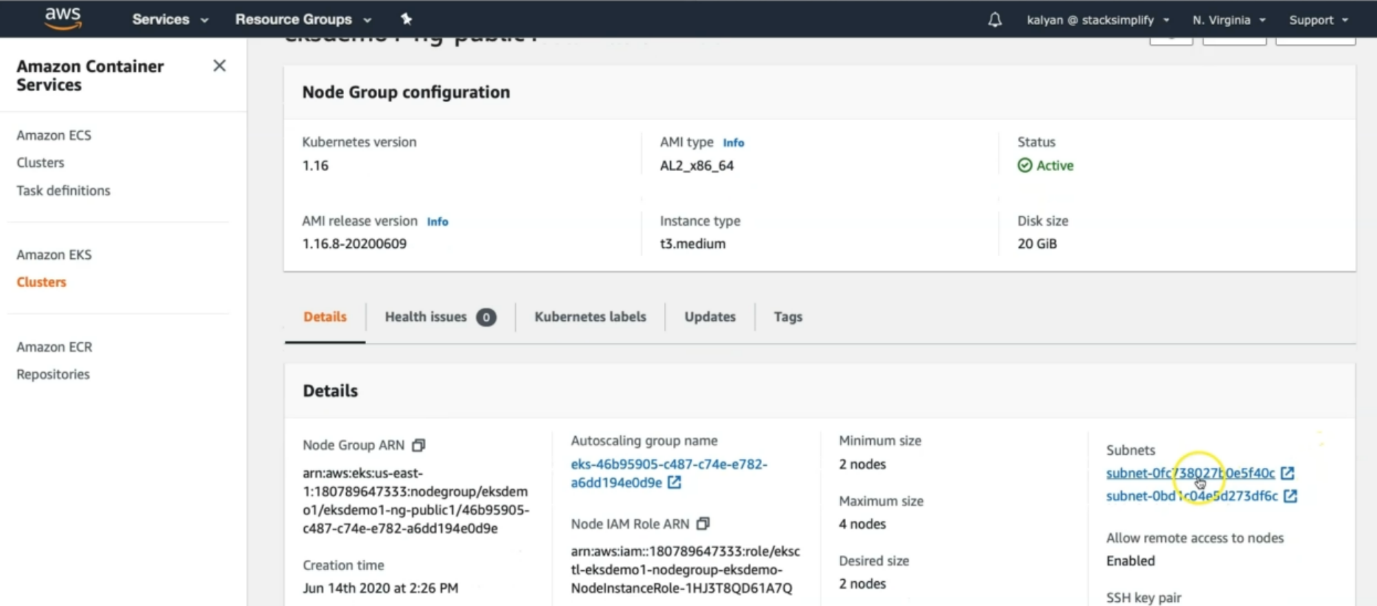
--- click on elastic kubernetes service,



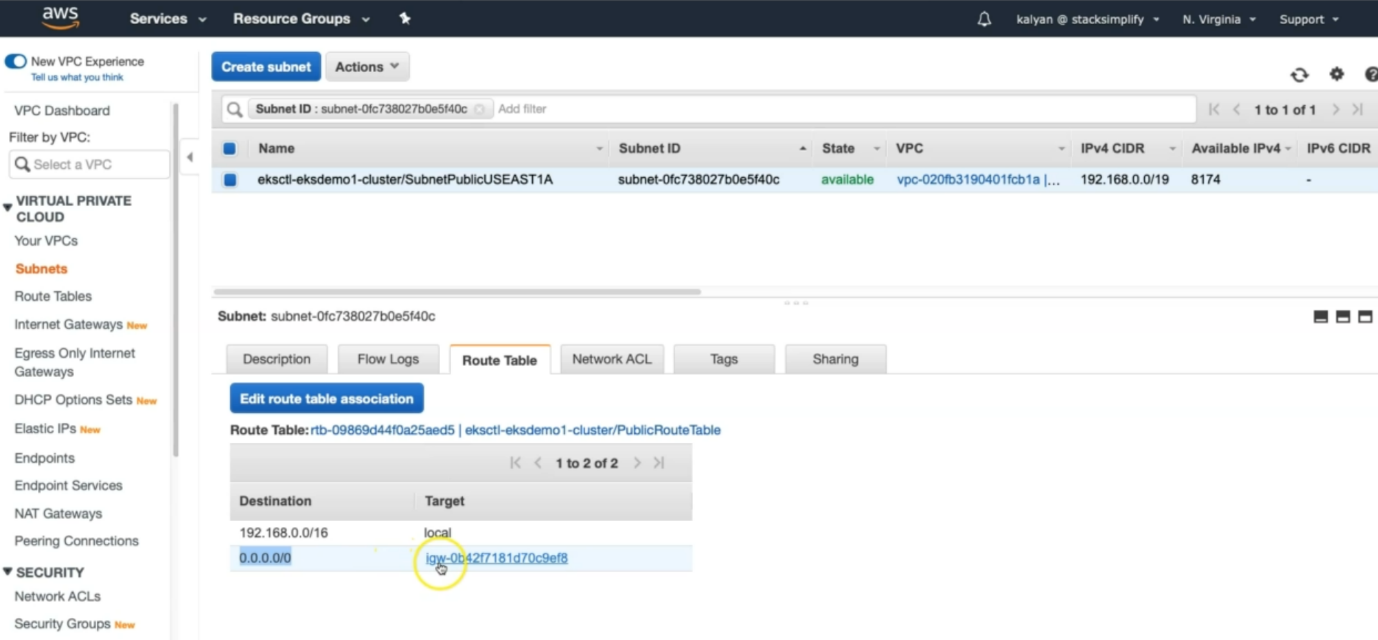
--- click on the cluster name.



--- click on the node group name.



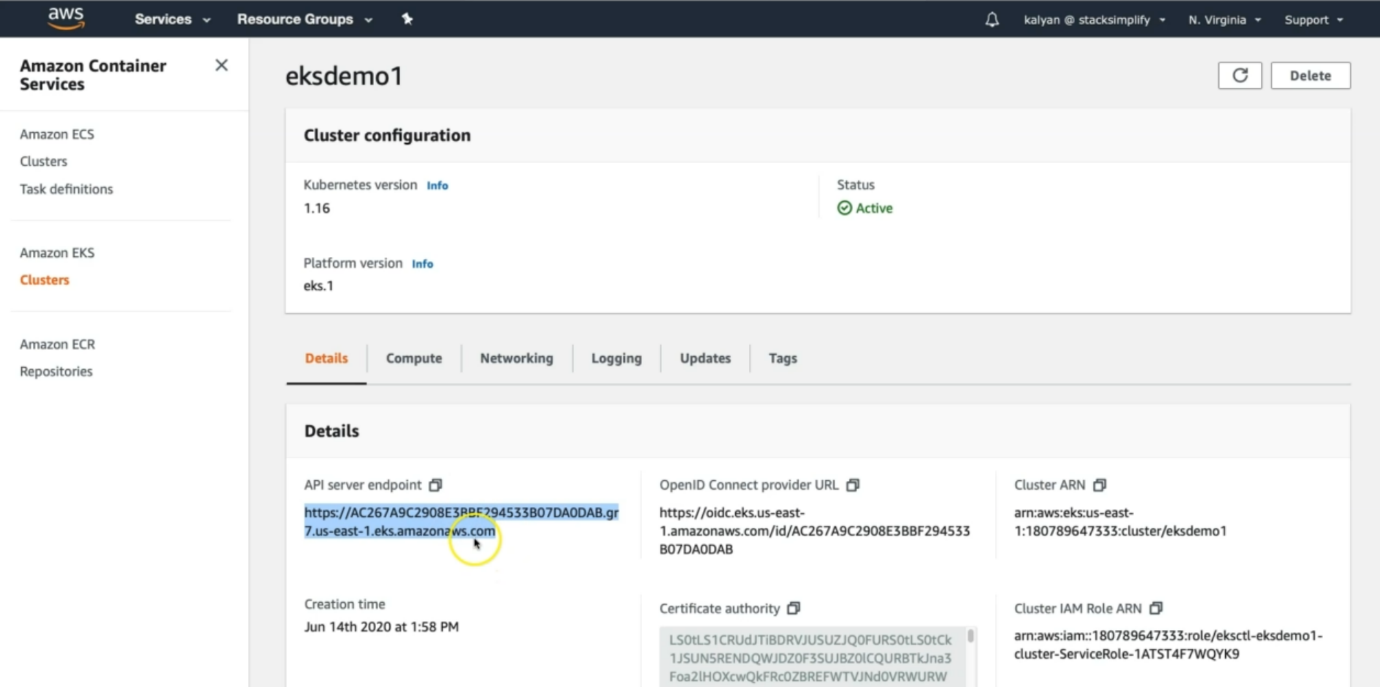
--- click on the subnets and it will take us to the vpc tab. It is also created autoscaling group.



--- now you can see that subnet is attached with internet gate way so it is public subnet.

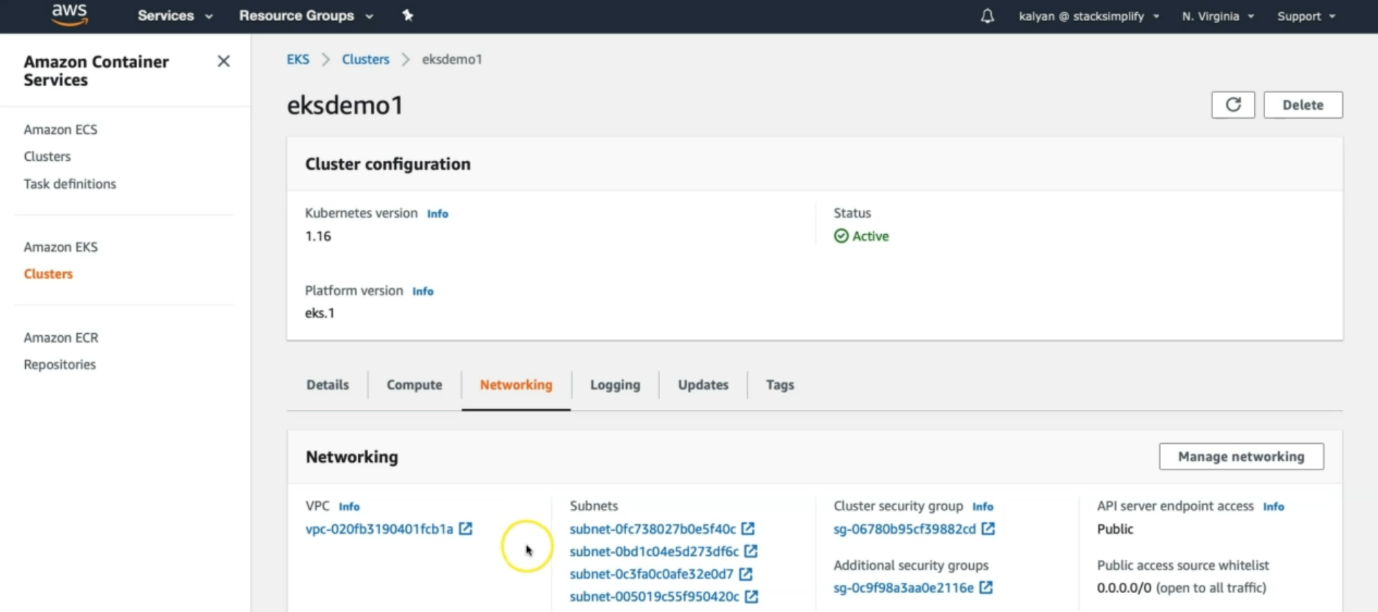
**Verify Cluster, NodeGroup in EKS Management Console**

--- Go to Services -> Elastic Kubernetes Service -> eksdemo1

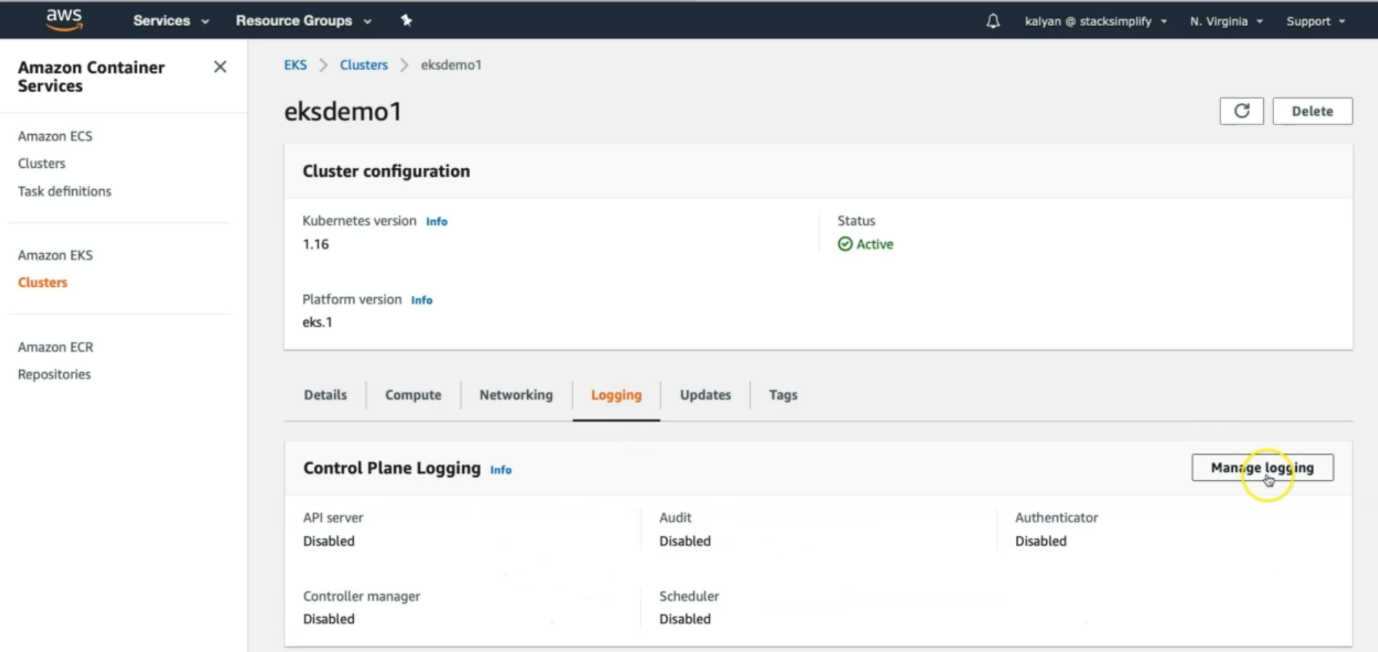


--- this is thee kube api server end point.

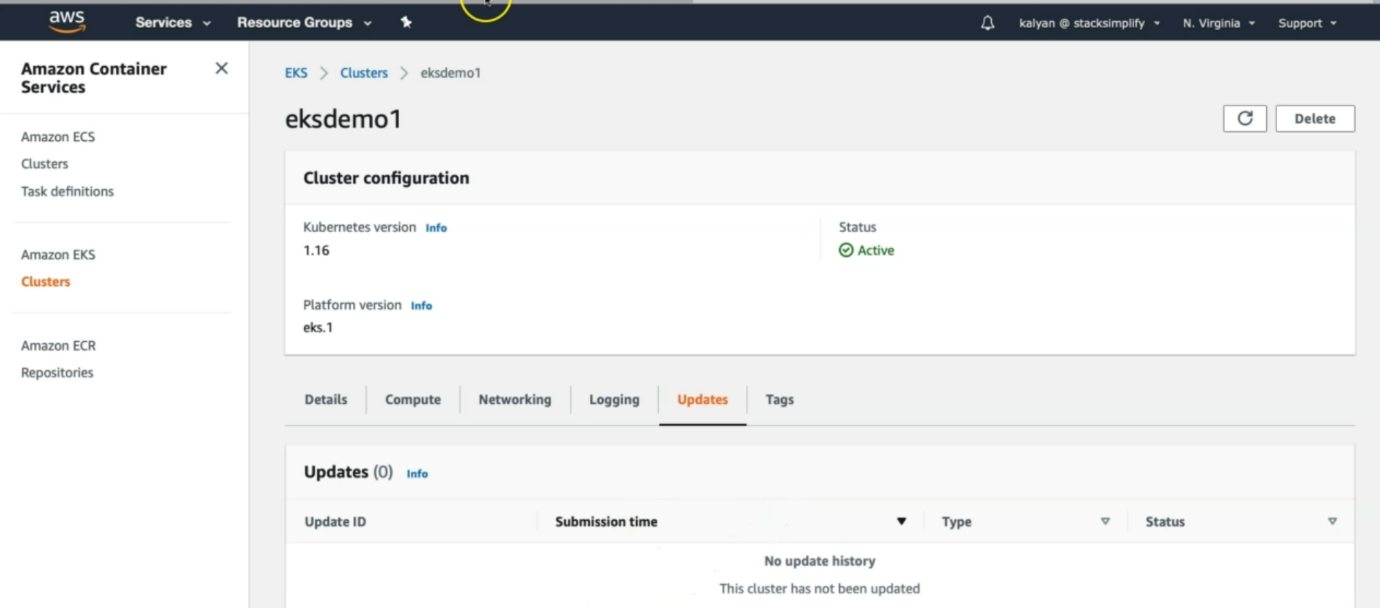
--- the second one is the openID connect provider URL.



--- here we can see the networking information of cluster.



--- you can see the logging information here. By default, it is disabled. If you want then we can enable it.



--- any new updated then those updates you can see here.

**List Worker Nodes**

**# List EKS clusters**

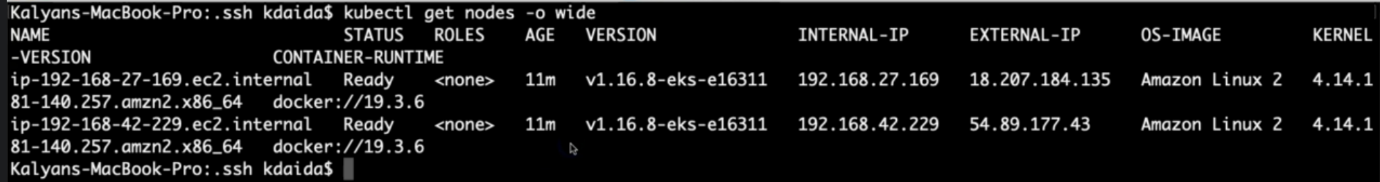
--- **eksctl get cluster**

**# List NodeGroups in a cluster**

--- **eksctl get nodegroup --cluster=<clusterName>**

**# List Nodes in current kubernetes cluster**

--- **kubectl get nodes -o wide**



**# Our kubectl context should be automatically changed to new cluster**

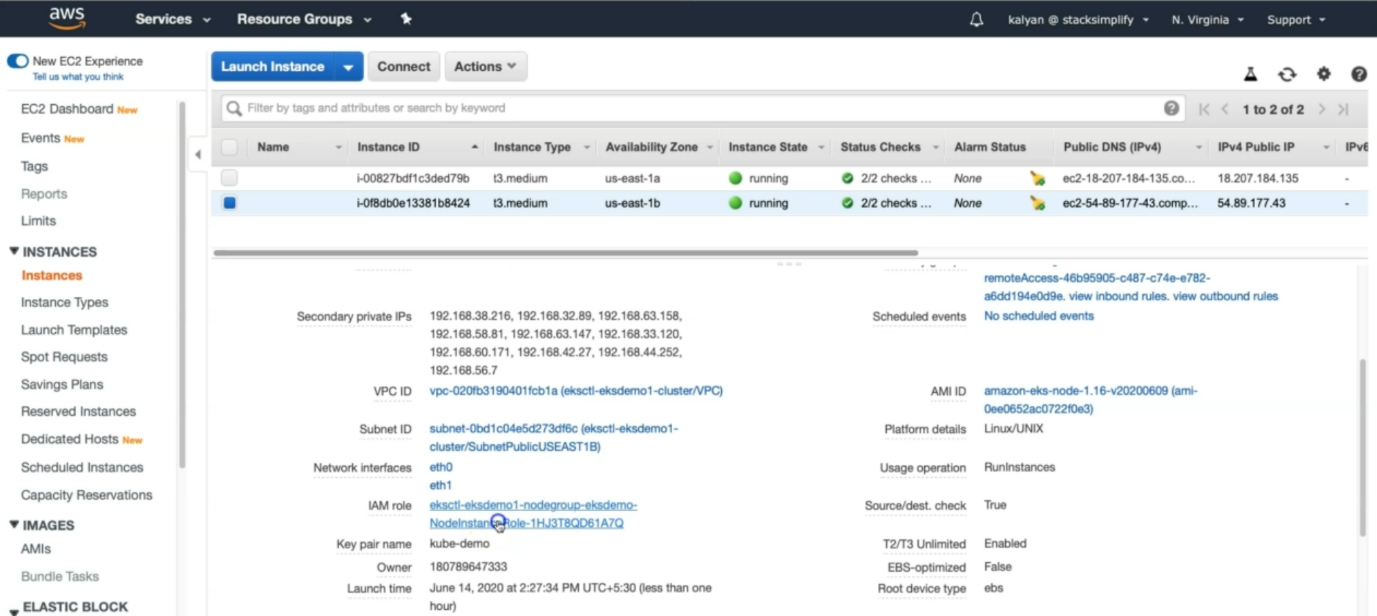
--- **kubectl config view –minify** – to see current config context.



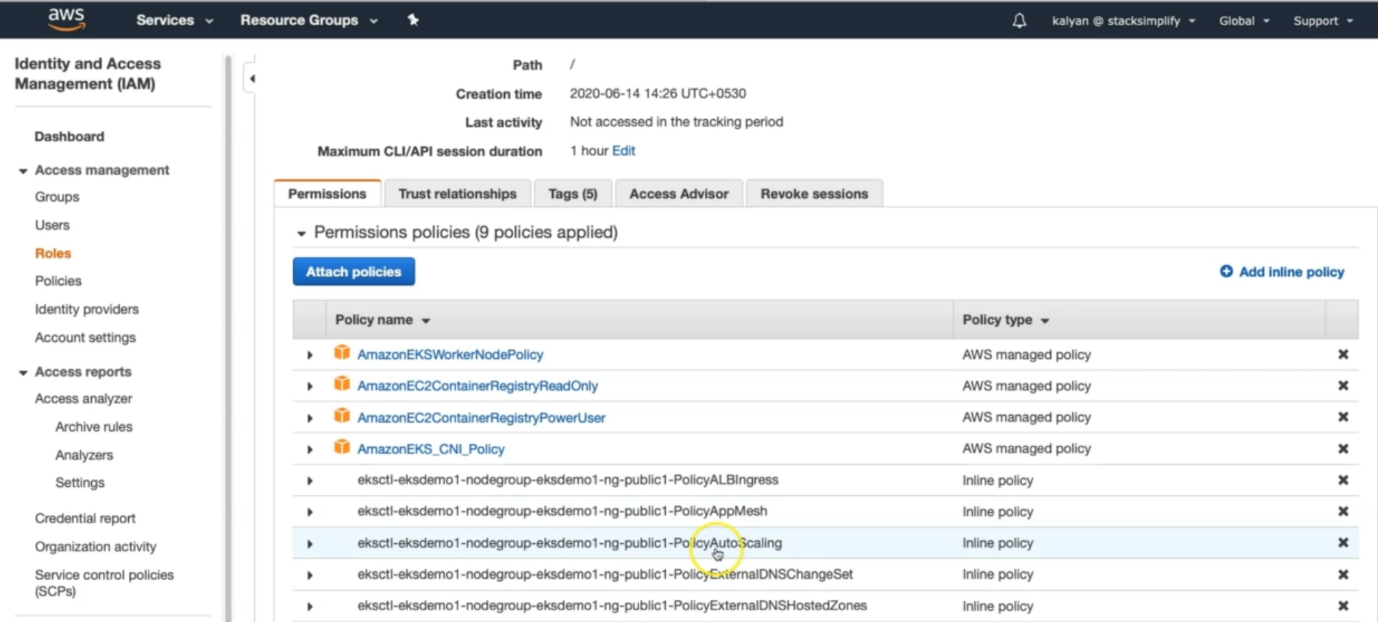
**Verify Worker Node IAM Role and list of Policies**

--- **note** – while creating cluster and node groups we assigned some I am roles. Here we will verify them.

--- Go to Services -> EC2 -> Worker Nodes



--- Click on IAM Role associated to EC2 Worker Nodes. It will take us to the iam role tab.

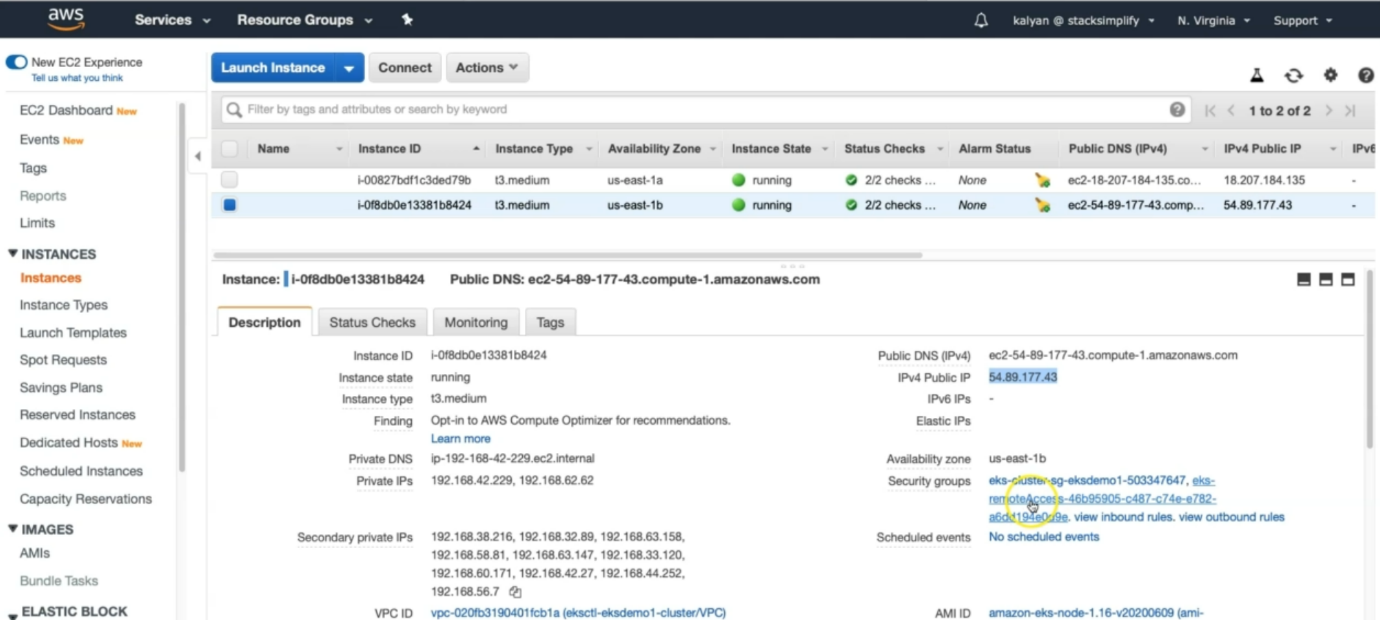


--- here you can see the all the policies which are associated with node groups.

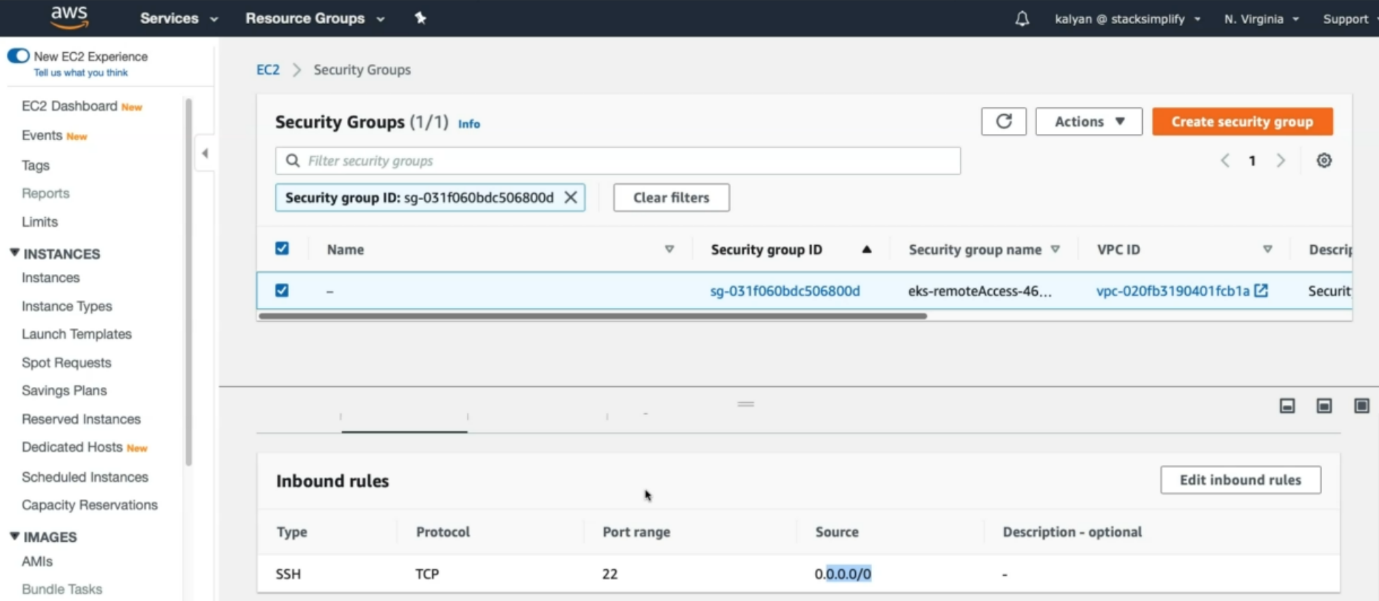
**Verify Security Group Associated to Worker Nodes**

--- **Go to Services -> EC2 -> Worker Nodes**

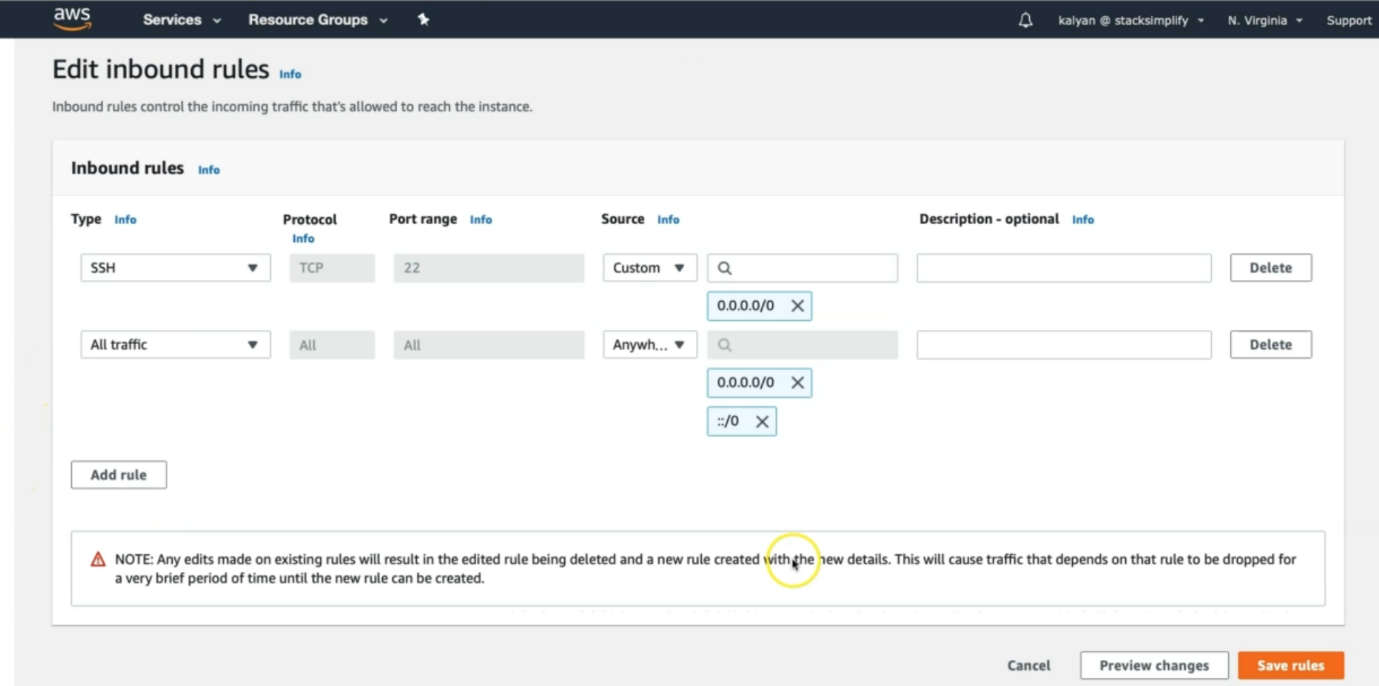
--- note - Click on Security Group associated to EC2 Instance which contains remote in the name.



--- you can see that the security group name contains remote in it. So click on that security group name.

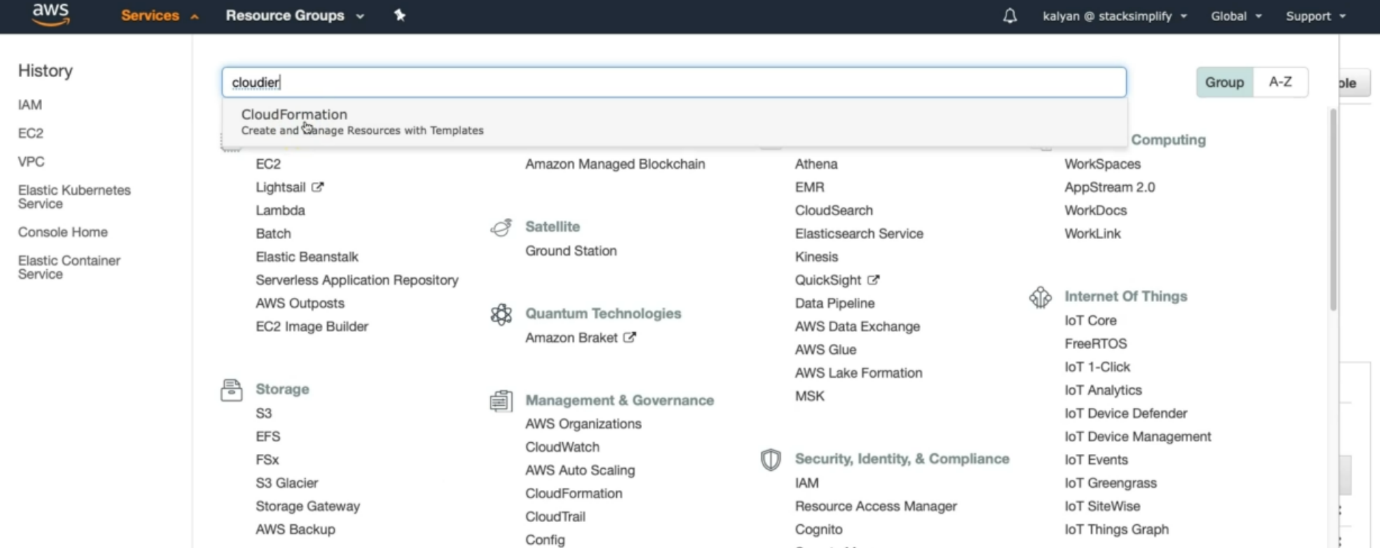


--- **note** – in the inbound rules it opened for port 22 over internet that is why we are able to connect the worker node.

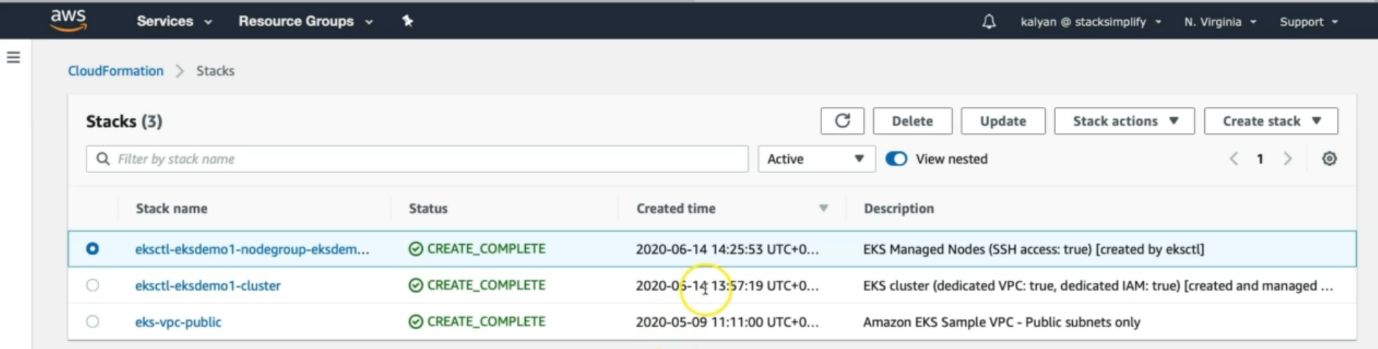


--- allow all traffic from anywhere.

**Verify CloudFormation Stacks**

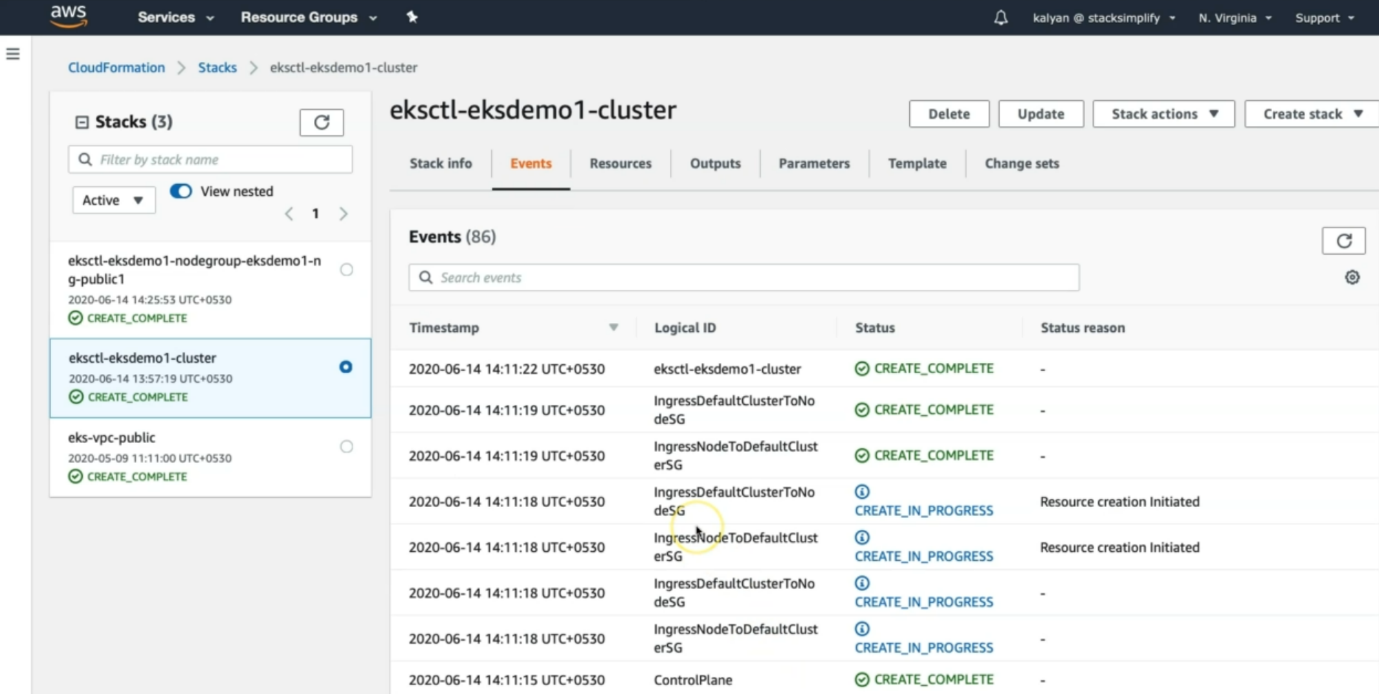


--- click on cloudformation.



--- the above 1st 2 things I created today.

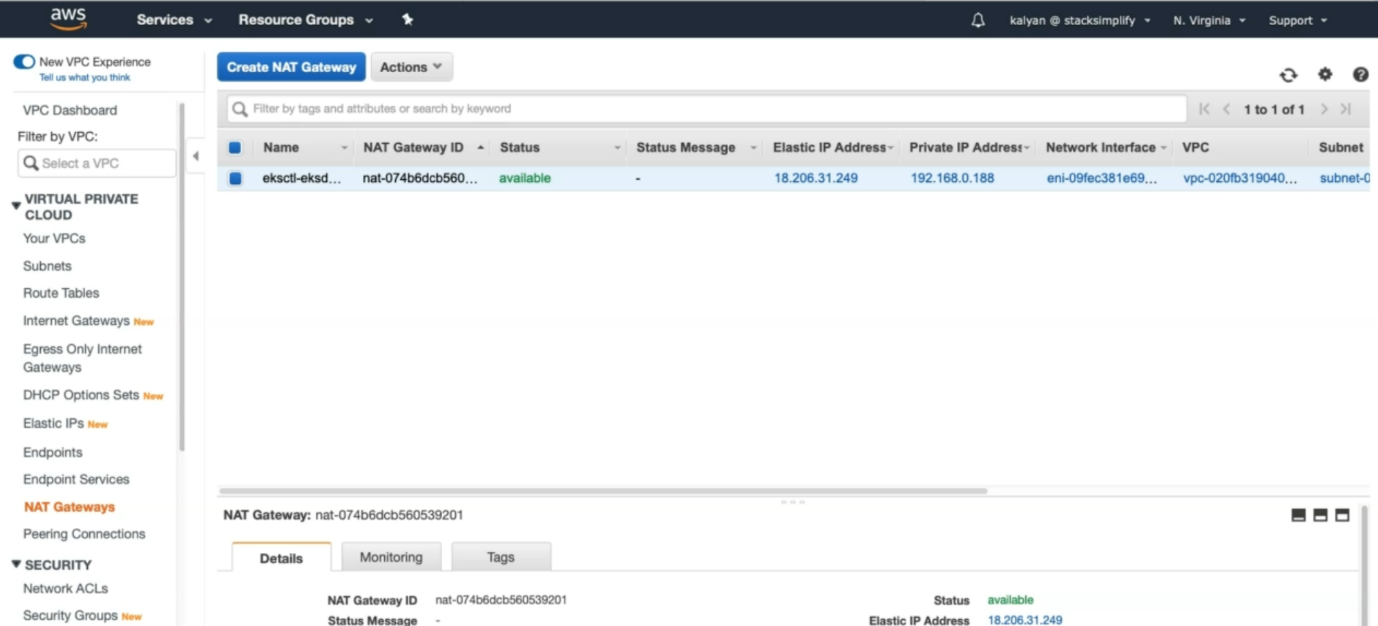
--- **click on the eksctl-eksdemo1-cluster** – click on that option, when executed created cluster command, it will create some events…etc.



--- it will create nat gate way, route tables…etc. it will create lot stuff under events.

--- **output** – under output, you will find kube api server end point.

**NateGateWay**



--- by default, it created single nat gateway but you can have the option to create high availability nat gateway or you can even disable the nat gateway. These are the important things which we need to know.

Login to Worker Node using Keypair kube-demo

Login to worker node

# For MAC or Linux or Windows10

ssh -i kube-demo.pem ec2-user@<Public-IP-of-Worker-Node>

# For Windows 7

Use putty