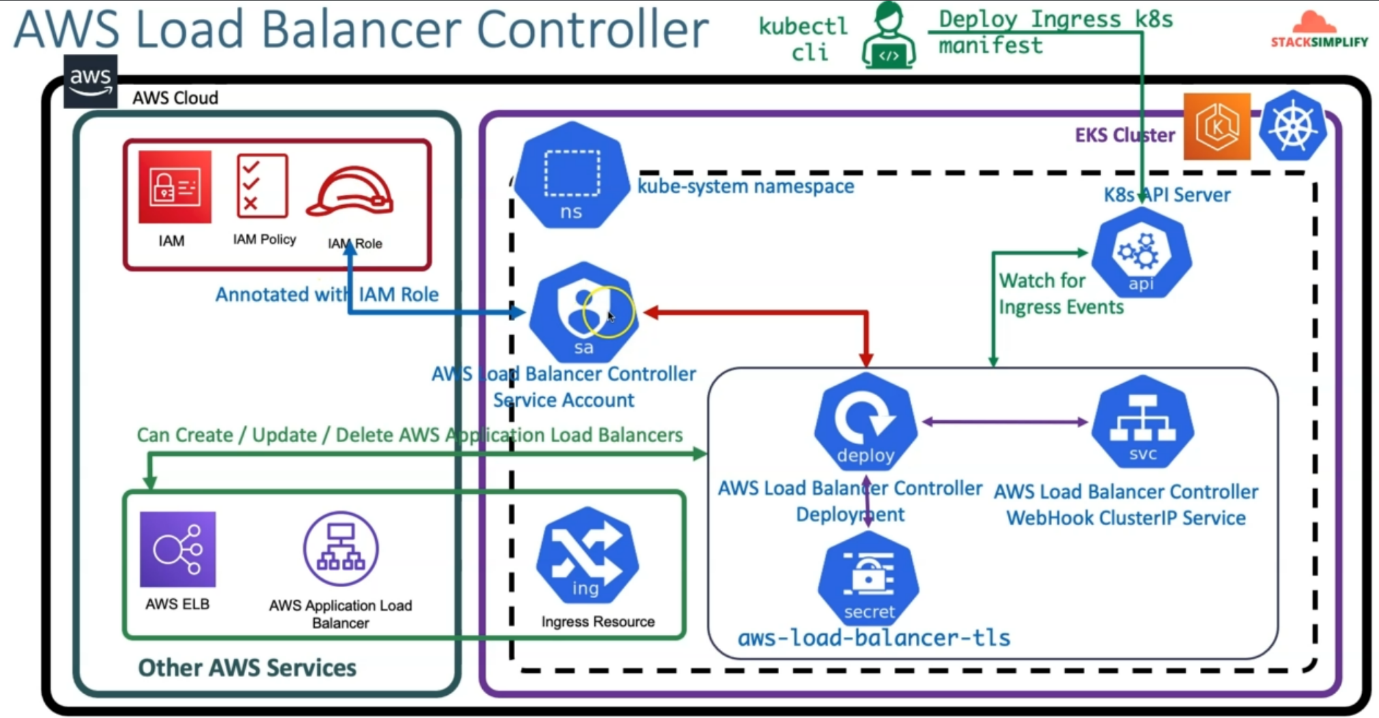
**03. Create IAM Policy, IAM Role, k8s service account and annotate it with I**

--- **Reference** - <https://github.com/stacksimplify/aws-eks-kubernetes-masterclass/tree/master/08-NEW-ELB-Application-LoadBalancers/08-01-Load-Balancer-Controller-Install>



--- here we are going to create IAM, IAM policy, IAM Role and also create AWS load balancer controller service account in kubernetes and annotate that respective service account with respective IAM Role.

**Create IAM Policy**

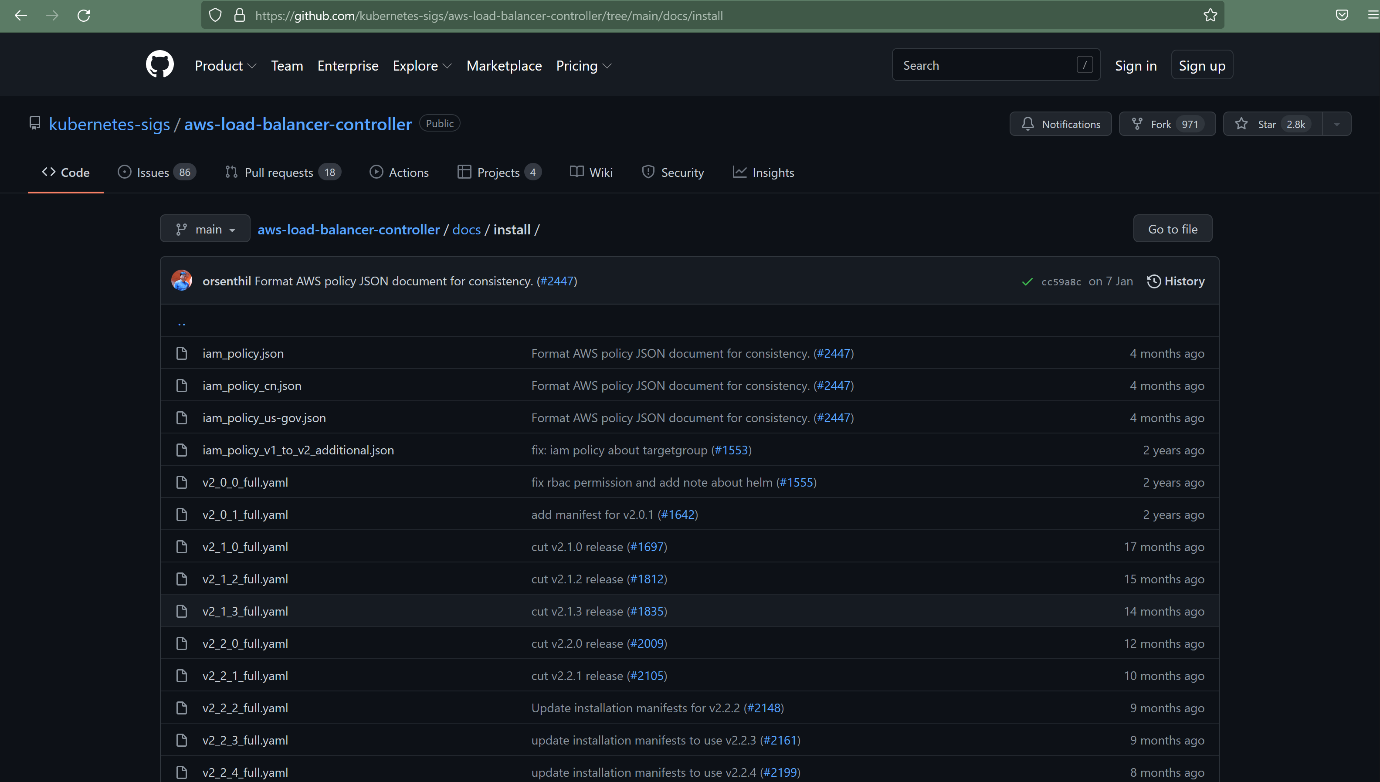
--- Create IAM policy for the AWS Load Balancer Controller that allows it to make calls to AWS APIs on your behalf.

--- As on today 2.3.1 is the latest Load Balancer Controller

--- We will download always latest from main branch of Git Repo

--- AWS Load Balancer Controller Main Git repo - <https://github.com/kubernetes-sigs/aws-load-balancer-controller>

--- <https://github.com/kubernetes-sigs/aws-load-balancer-controller/tree/main/docs/install>



--- **note** – in the above location, you will find latest **iam\_policy.json files**. You can also download specific versions of iam\_plicy.json files.

**# Change Directory**

--- **cd 08-NEW-ELB-Application-LoadBalancers/**

--- **cd 08-01-Load-Balancer-Controller-Install**

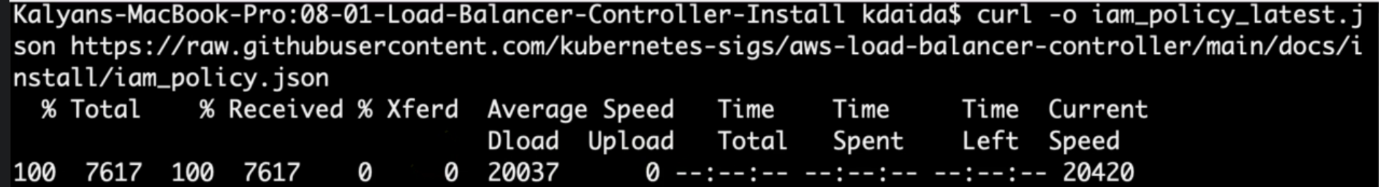
**# Delete files before download (if any present)**

--- **rm iam\_policy\_latest.json**

**# Download IAM Policy**

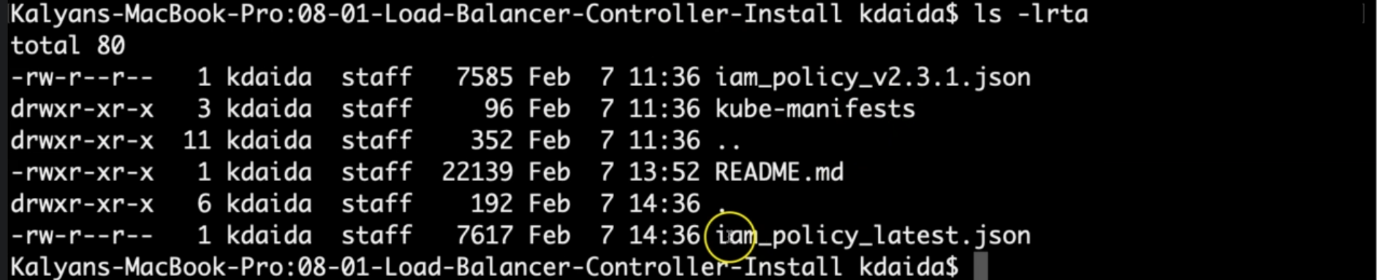
**## Download latest**

--- **curl -o iam\_policy\_latest.json** [**https://raw.githubusercontent.com/kubernetes-sigs/aws-load-balancer-controller/main/docs/install/iam\_policy.json**](https://raw.githubusercontent.com/kubernetes-sigs/aws-load-balancer-controller/main/docs/install/iam_policy.json)



**## Verify latest**

--- **ls -lrta**



--- **note** – the latest one downloaded.

**## Download specific version**

--- **curl -o iam\_policy\_v2.3.1.json https://raw.githubusercontent.com/kubernetes-sigs/aws-load-balancer-controller/v2.3.1/docs/install/iam\_policy.json**

**# Create IAM Policy using policy downloaded**

--- **aws iam create-policy \**

**--policy-name AWSLoadBalancerControllerIAMPolicy \**

**--policy-document file://iam\_policy\_latest.json**

**## Sample Output**

**Kalyans-MacBook-Pro:08-01-Load-Balancer-Controller-Install kdaida$ aws iam create-policy \**

**> --policy-name AWSLoadBalancerControllerIAMPolicy \**

**> --policy-document file://iam\_policy\_latest.json**

**{**

**"Policy": {**

**"PolicyName": "AWSLoadBalancerControllerIAMPolicy",**

**"PolicyId": "ANPASUF7HC7S52ZQAPETR",**

**"Arn": "arn:aws:iam::180789647333:policy/AWSLoadBalancerControllerIAMPolicy",**

**"Path": "/",**

**"DefaultVersionId": "v1",**

**"AttachmentCount": 0,**

**"PermissionsBoundaryUsageCount": 0,**

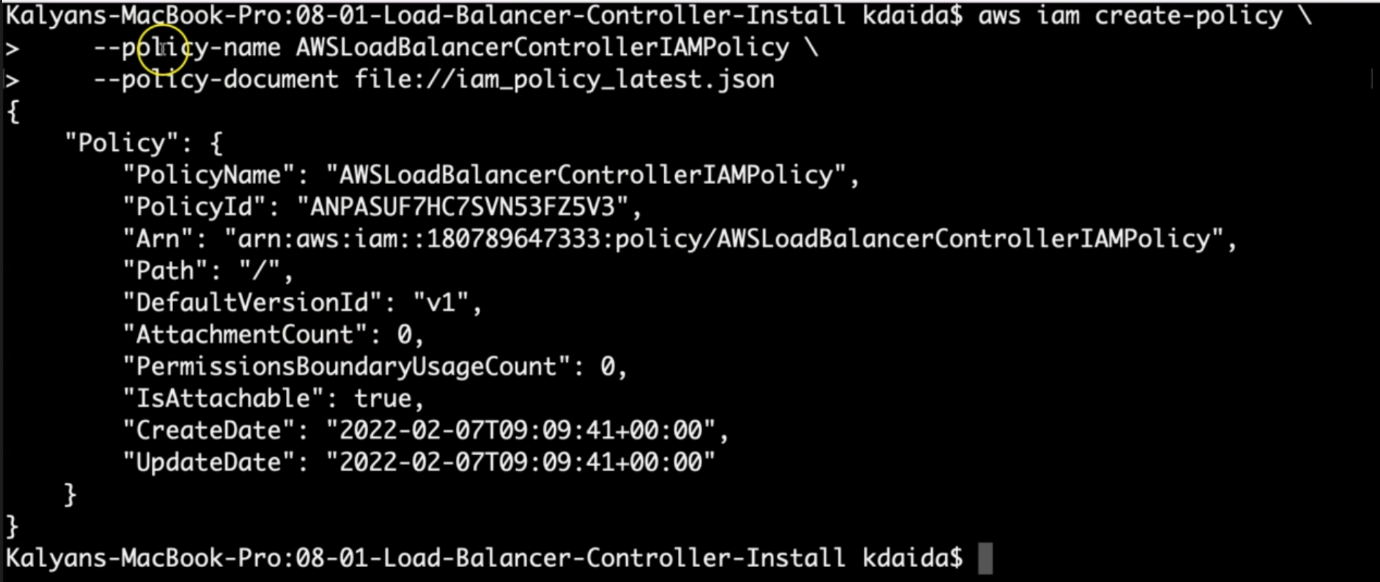
**"IsAttachable": true,**

**"CreateDate": "2022-02-02T04:51:21+00:00",**

**"UpdateDate": "2022-02-02T04:51:21+00:00"**

**}**

**}**



--- **note** – you should be in the file location directory and execute the above command.

--- **Important Note:** If you view the policy in the AWS Management Console, you may see warnings for ELB. These can be safely ignored because some of the actions only exist for ELB v2. You do not see warnings for ELB v2.

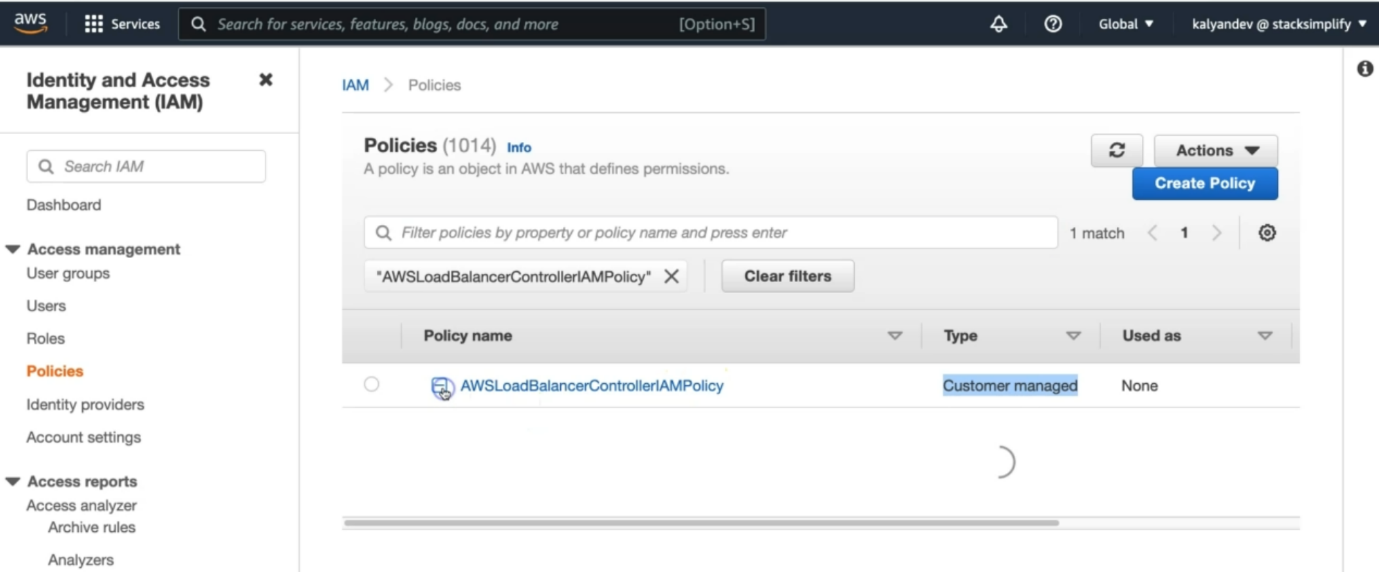
--- **Make a note of Policy ARN** - Make a note of Policy ARN as we are going to use that in next step when creating IAM Role.

**# Policy ARN**

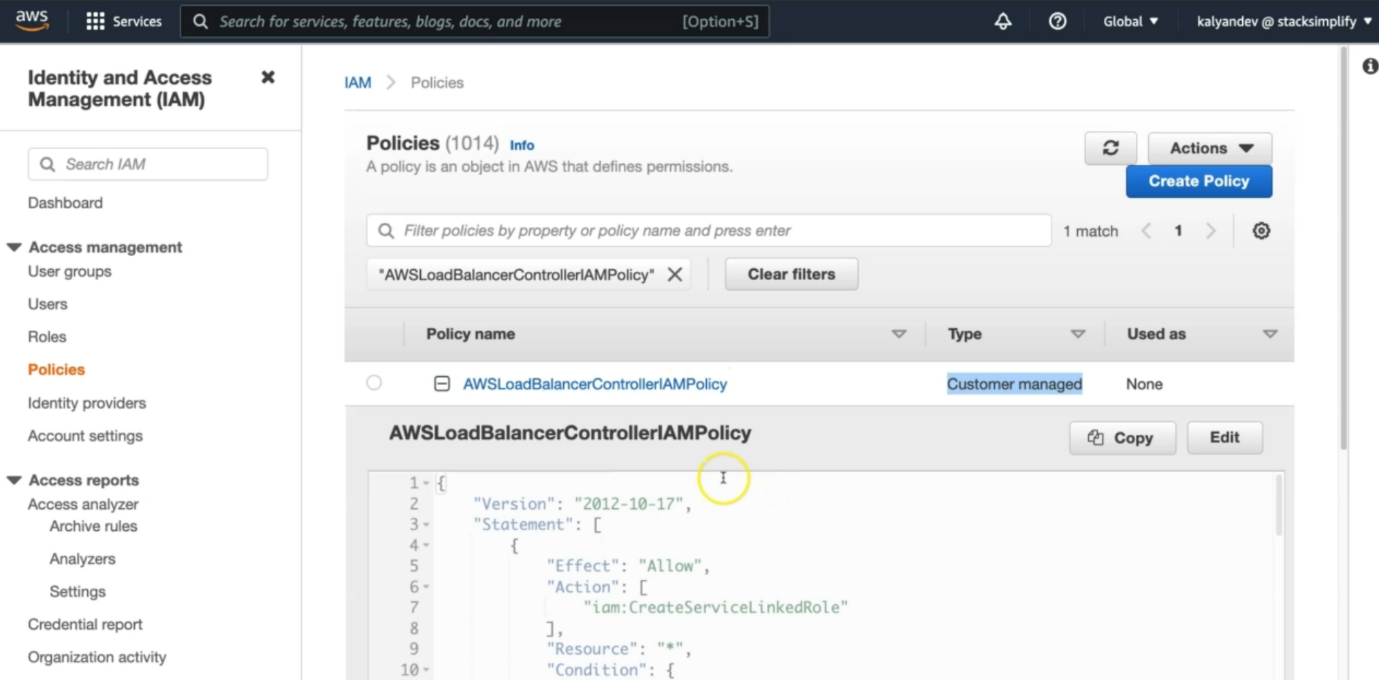
Policy ARN: arn:aws:iam::180789647333:policy/AWSLoadBalancerControllerIAMPolicy

--- **180789647333** – this is aws account id.

**Verify policy is created in aws or not**



--- **note** – the policy is created under policy section which is customer managed policy. Click on the policy name.



--- **note** – that is the policy code. Here you will find the policy information.

**Create an IAM role for the AWS LoadBalancer Controller and attach the role to the Kubernetes service account**

--- Applicable only with eksctl managed clusters

--- This command will create an AWS IAM role

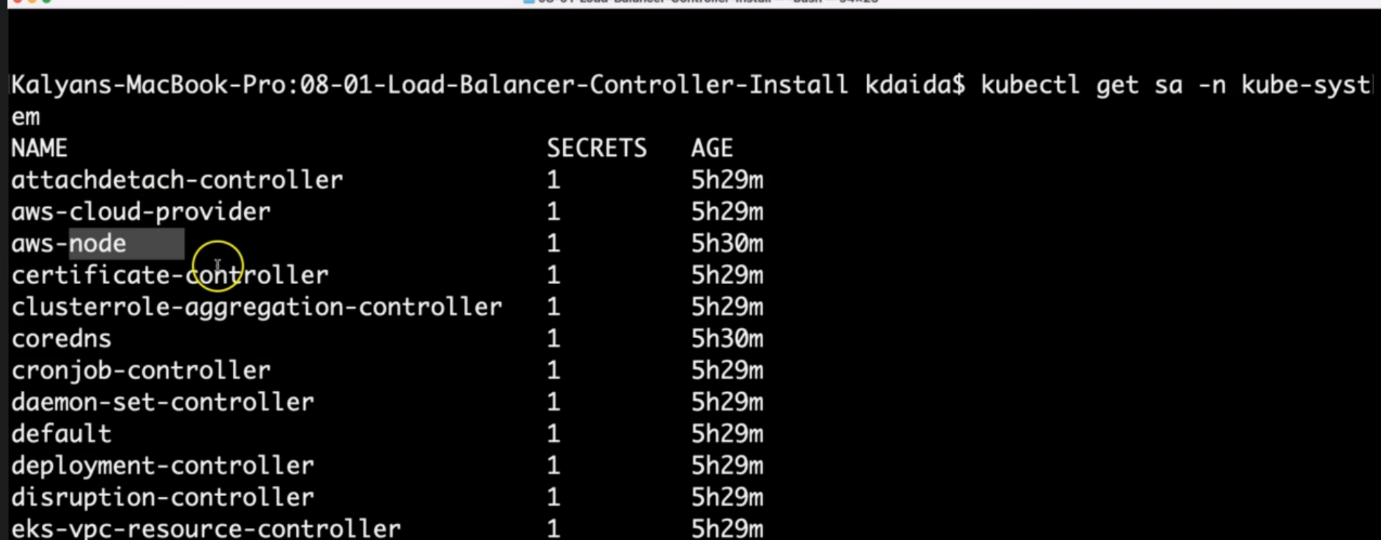
--- This command also will create Kubernetes Service Account in k8s cluster

--- In addition, this command will bound IAM Role created and the Kubernetes service account created

**Create IAM Role using eksctl**

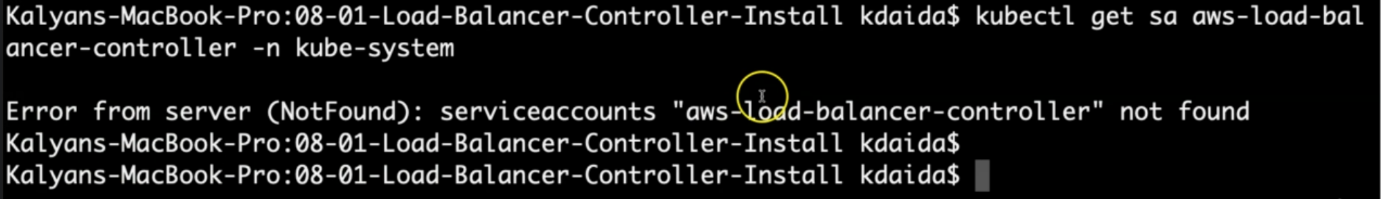
**# Verify if any existing service account**

--- **kubectl get sa -n kube-system**



--- **note** – we are verifying the service account is present in kube-system. Here with aws, we could not find service account in kube-system.

--- **kubectl get sa aws-load-balancer-controller -n kube-system**



--- **note** – we can also search the service account by its name in the kube-system.

--- **Observation:** Nothing with name "aws-load-balancer-controller" should exist

**# Template**

--- **eksctl create iamserviceaccount \**

**--cluster=my\_cluster \ # my cluster name**

**--namespace=kube-system \ # we are creating service account in kube-system name space.**

**--name=aws-load-balancer-controller \ #Note: K8S Service Account Name that need to be bound to newly created IAM Role**

**--attach-policy-arn=arn:aws:iam::111122223333:policy/AWSLoadBalancerControllerIAMPolicy \ # we are attaching the policy which is created by us previously.**

**--override-existing-serviceaccounts \**

**--approve**

**# Replaced name, cluster and policy arn (Policy arn we took note in step-02)**

--- **eksctl create iamserviceaccount \**

**--cluster=eksdemo1 \**

**--namespace=kube-system \**

**--name=aws-load-balancer-controller \**

**--attach-policy-arn=arn:aws:iam::180789647333:policy/AWSLoadBalancerControllerIAMPolicy \**

**--override-existing-serviceaccounts \**

**--approve**

**# Sample Output for IAM Service Account creation**

--- **eksctl create iamserviceaccount \**

**> --cluster=eksdemo1 \**

**> --namespace=kube-system \**

**> --name=aws-load-balancer-controller \**

**> --attach-policy-arn=arn:aws:iam::180789647333:policy/AWSLoadBalancerControllerIAMPolicy \**

**> --override-existing-serviceaccounts \**

**> --approve**

2022-02-02 10:22:49 [ℹ] eksctl version 0.82.0

2022-02-02 10:22:49 [ℹ] using region us-east-1

2022-02-02 10:22:52 [ℹ] 1 iamserviceaccount (kube-system/aws-load-balancer-controller) was included (based on the include/exclude rules)

2022-02-02 10:22:52 [!] metadata of serviceaccounts that exist in Kubernetes will be updated, as --override-existing-serviceaccounts was set

2022-02-02 10:22:52 [ℹ] 1 task: {

2 sequential sub-tasks: {

create IAM role for serviceaccount "kube-system/aws-load-balancer-controller",

create serviceaccount "kube-system/aws-load-balancer-controller",

} }2022-02-02 10:22:52 [ℹ] building iamserviceaccount stack "eksctl-eksdemo1-addon-iamserviceaccount-kube-system-aws-load-balancer-controller"

2022-02-02 10:22:53 [ℹ] deploying stack "eksctl-eksdemo1-addon-iamserviceaccount-kube-system-aws-load-balancer-controller"

2022-02-02 10:22:53 [ℹ] waiting for CloudFormation stack "eksctl-eksdemo1-addon-iamserviceaccount-kube-system-aws-load-balancer-controller" #

2022-02-02 10:23:10 [ℹ] waiting for CloudFormation stack "eksctl-eksdemo1-addon-iamserviceaccount-kube-system-aws-load-balancer-controller"

2022-02-02 10:23:29 [ℹ] waiting for CloudFormation stack "eksctl-eksdemo1-addon-iamserviceaccount-kube-system-aws-load-balancer-controller"

2022-02-02 10:23:32 [ℹ] created serviceaccount "kube-system/aws-load-balancer-controller"

**Verify using eksctl cli**

**# Get IAM Service Account**

--- **eksctl get iamserviceaccount --cluster eksdemo1**

**# Sample Output**

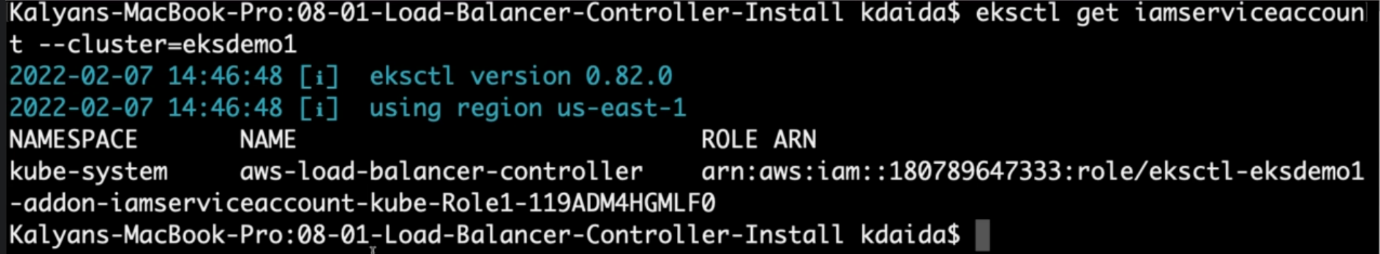
--- **eksctl get iamserviceaccount --cluster eksdemo1**

**2022-02-02 10:23:50 [ℹ] eksctl version 0.82.0**

**2022-02-02 10:23:50 [ℹ] using region us-east-1**

**NAMESPACE NAME ROLE ARN**

**kube-system aws-load-balancer-controller arn:aws:iam::180789647333:role/eksctl-eksdemo1-addon-iamserviceaccount-kube-Role1-1244GWMVEAKEN**



--- **note** – this service account is associated with IAM role arn.

--- **Observation**: You can see that newly created Role ARN is added in Annotations confirming that AWS IAM role bound to a Kubernetes service account

**## Sample Output**

--- **kubectl describe sa aws-load-balancer-controller -n kube-system**

**Name: aws-load-balancer-controller**

**Namespace: kube-system**

**Labels: app.kubernetes.io/managed-by=eksctl**

**Annotations: eks.amazonaws.com/role-arn: arn:aws:iam::180789647333:role/eksctl-eksdemo1-addon-iamserviceaccount-kube-Role1-1244GWMVEAKEN**

**Image pull secrets: <none>**

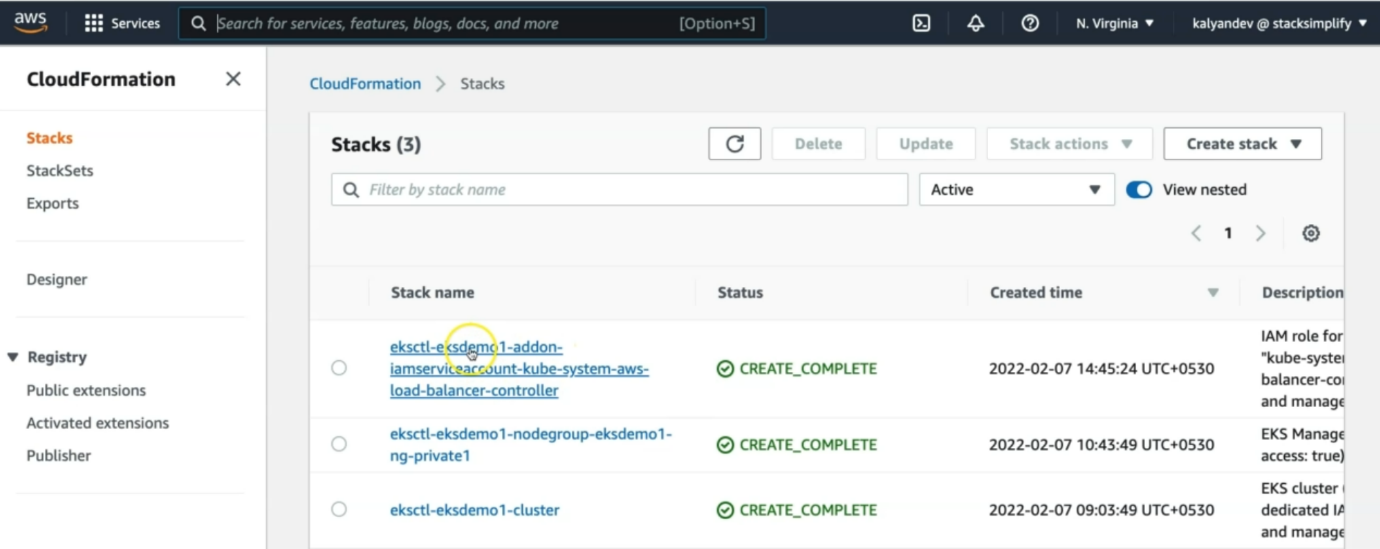
**Mountable secrets: aws-load-balancer-controller-token-5w8th**

**Tokens: aws-load-balancer-controller-token-5w8th**

**Events: <none>**

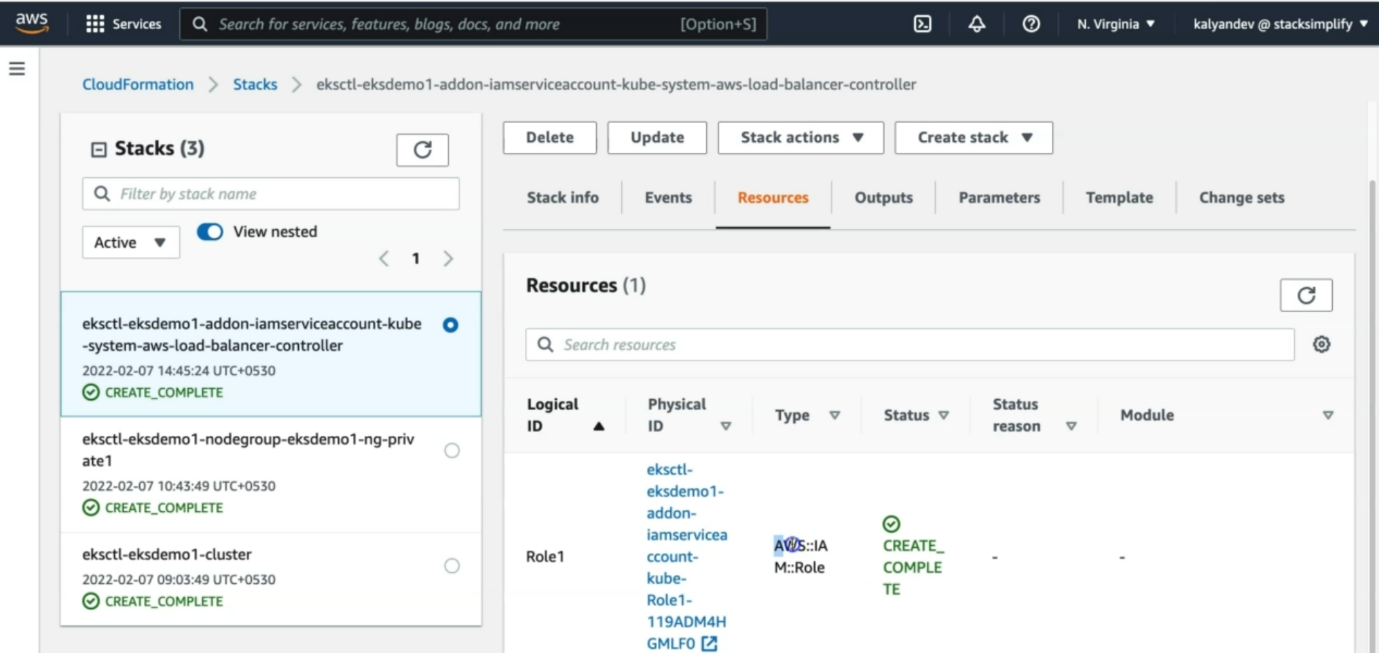
**Verify CloudFormation Template eksctl created & IAM Role**

--- go to Services -> CloudFormation

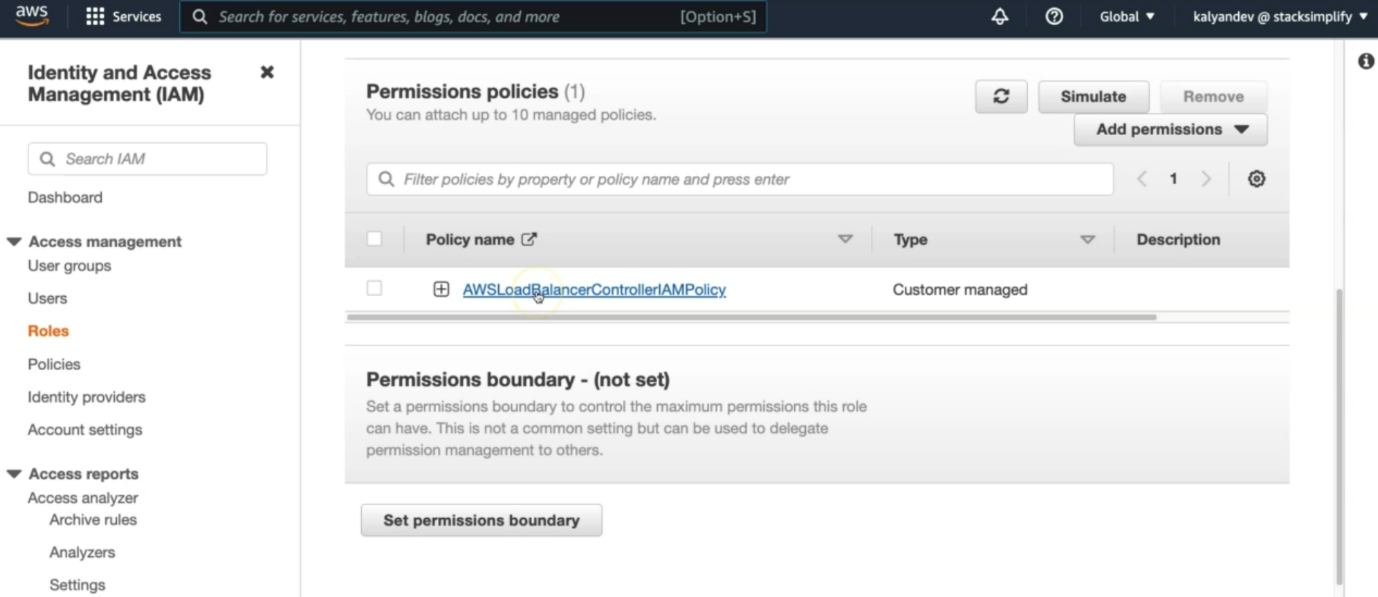


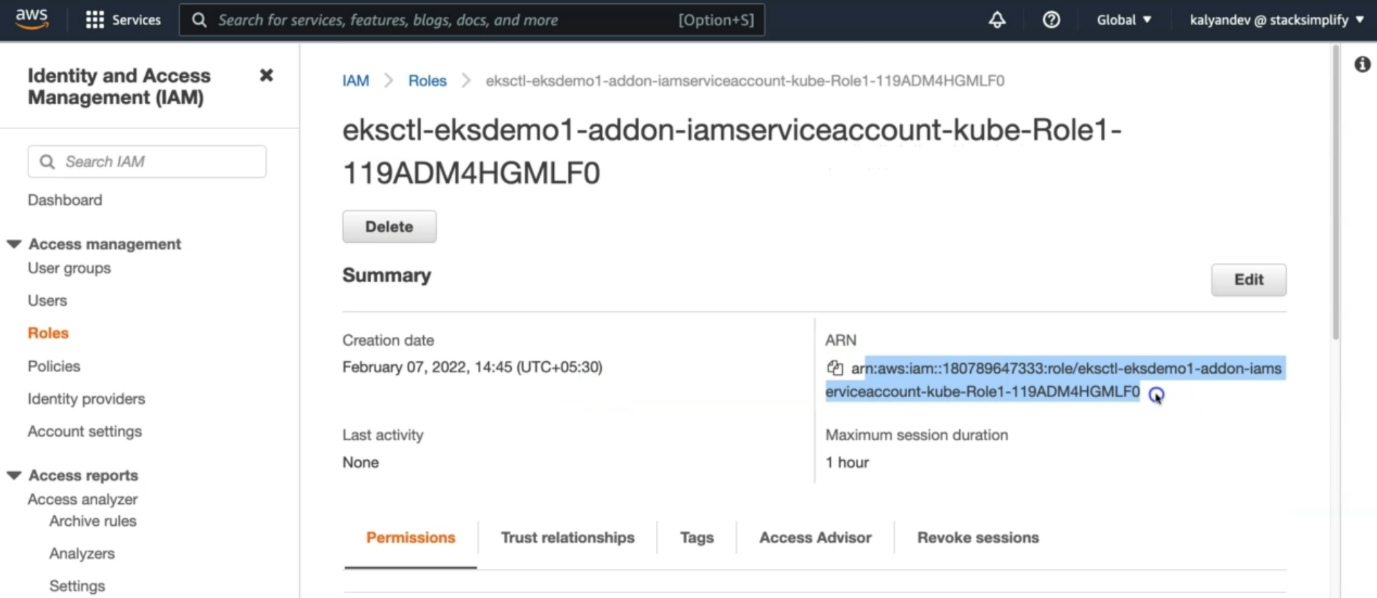
--- CFN Template Name: eksctl-eksdemo1-addon-iamserviceaccount-kube-system-aws-load-balancer-controller. Click on that name.

--- Click on Resources tab



--- Click on link in Physical Id to open the IAM Role



--- **note** – this is the IAM role, it had created. 

--- note – this is the arn, which is associated with the IAM role.

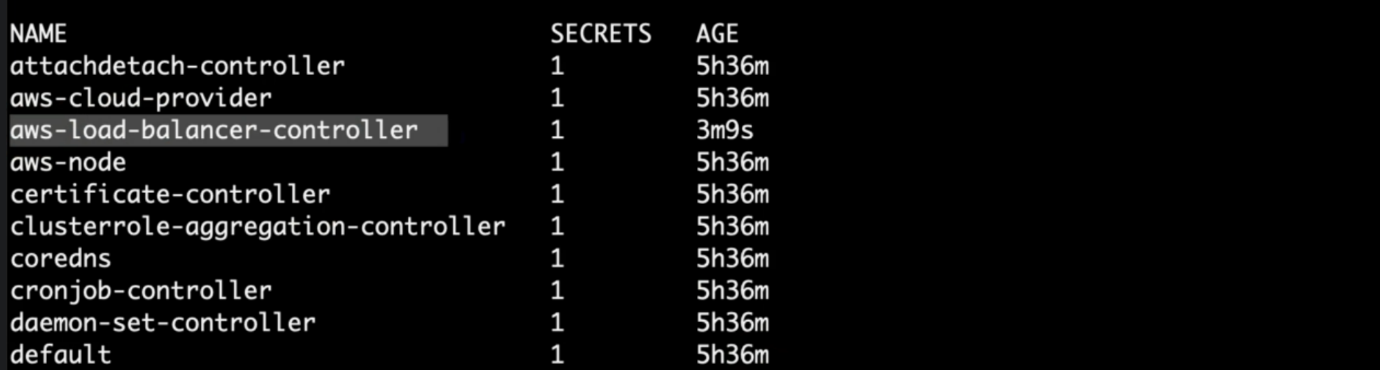
--- click on permission tab.

--- Verify it has eksctl-eksdemo1-addon-iamserviceaccount-kube-Role1-WFAWGQKTAVLR associated

**Verify k8s Service Account using kubectl**

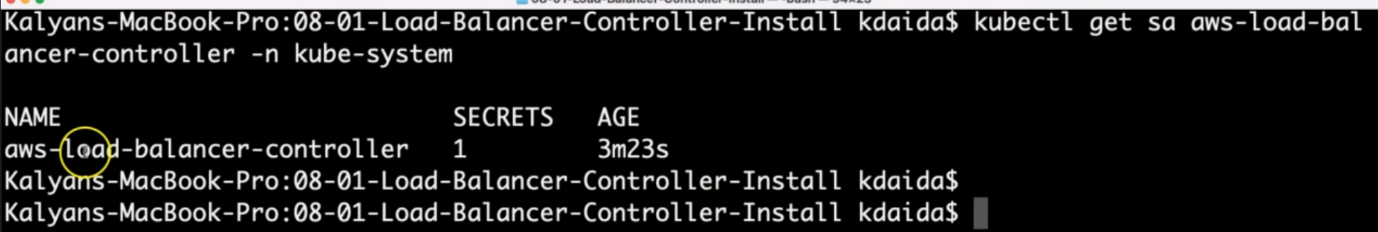
**# Verify if any existing service account**

--- **kubectl get sa -n kube-system**



--- **note** – service is created under name space kube-system.

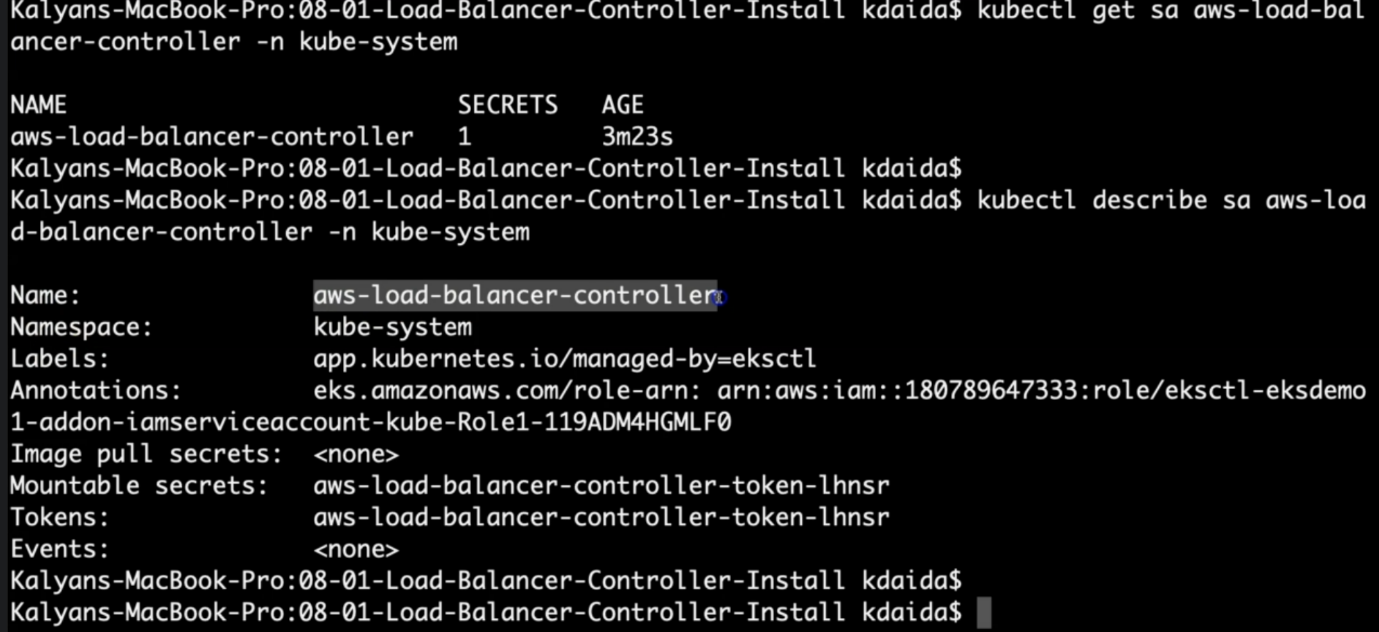
--- **kubectl get sa aws-load-balancer-controller -n kube-system** – searching account by its name.



--- **Observation**: We should see a new Service account created. We can also see the age of the service account.

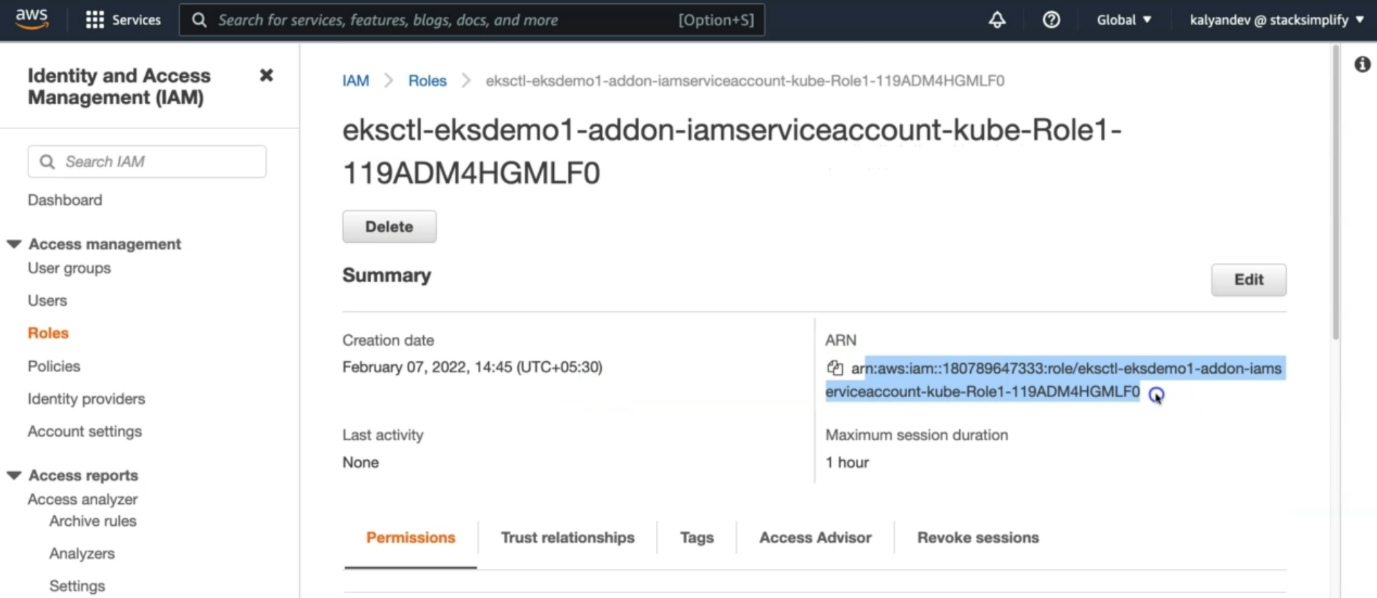
**# Describe Service Account aws-load-balancer-controller**

--- kubectl describe sa aws-load-balancer-controller -n kube-system

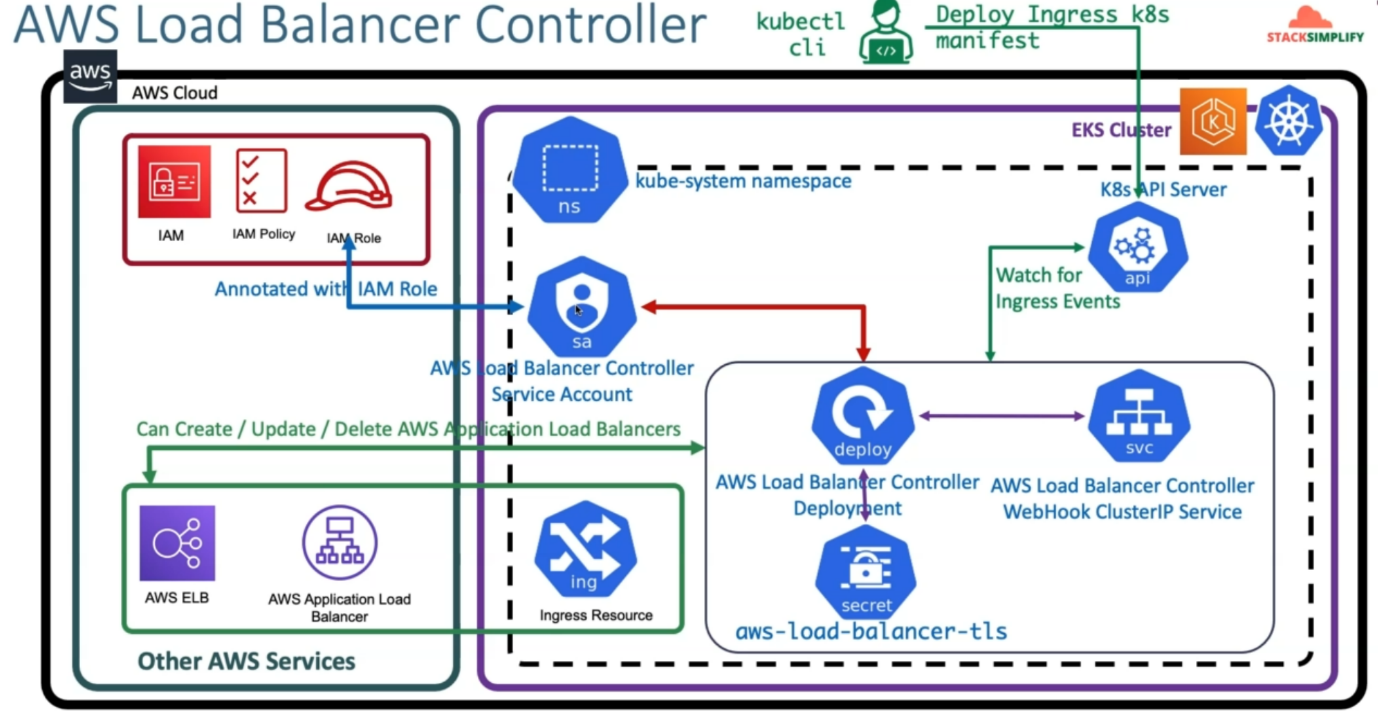


--- **note** – we could see the role arn, when we describe service account.

--- **note** - this confirms that the aws IAM role is bound to kubernetes service account.



**What we have done so far**



--- so far, we have done IAM, IAM Policy, IAM Role and AWS load balancer controller service account. In the next lesion we will Install AWS Load balancer controller using HELM.