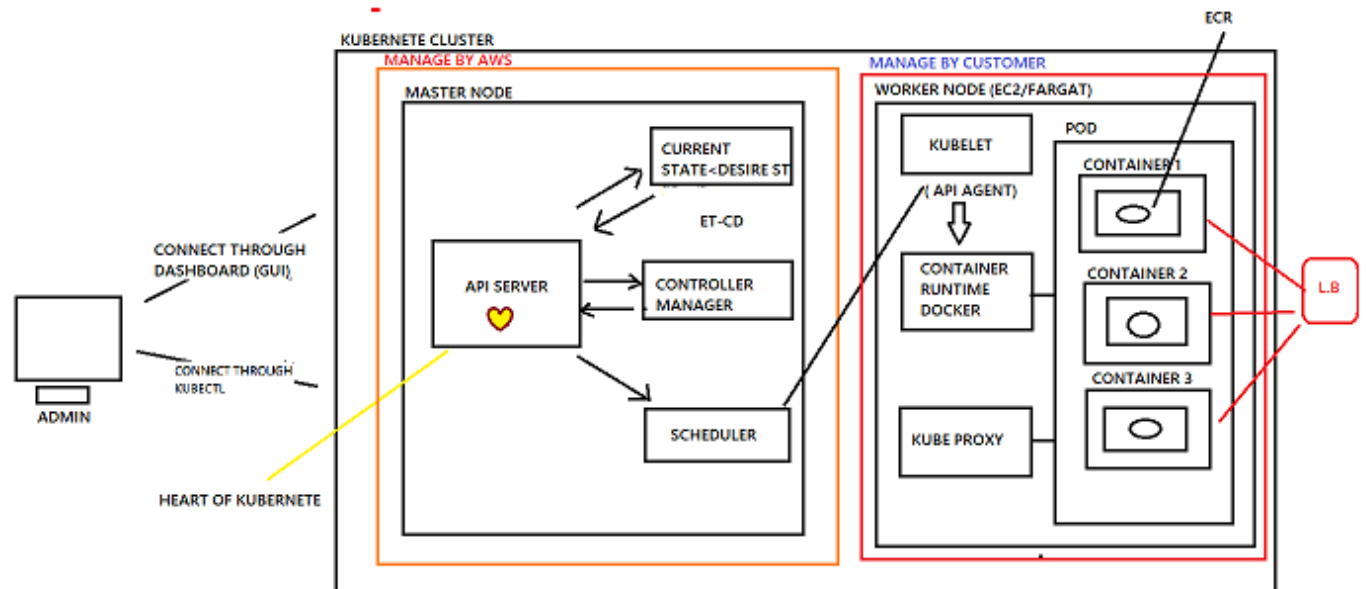


AIM- CONCEPT OF KUBERNETE IN AWS

CREATING CLUSTER ,MASTER NODE AND WORKER NODE

ARCHITECTURE



STEPS 1-

CREATE A CLUSTER

Cluster configuration [Info](#)

Name

Enter a unique name for this cluster. This property cannot be changed after the cluster is created.

The cluster name should begin with letter or digit and can have any of the following characters: the set of Unicode letters, digits, hyphens and underscores. Maximum length of 100.

Kubernetes version [Info](#)

Select Kubernetes version for this cluster.

i Kubernetes version 1.29 reaches the end of standard support on March 23, 2025. If you don't update your cluster to a later version before that date, it will automatically enter extended support. After the extended support preview ends, clusters on versions in extended support will be subject to additional fees. [Learn more](#) [↗](#).

Cluster service role [Info](#)

[Learn more](#) [↗](#).

Cluster service role [Info](#)

Select the IAM role to allow the Kubernetes control plane to manage AWS resources on your behalf. This property cannot be changed at the cluster is created. To create a new role, follow the instructions in the [Amazon EKS User Guide](#) [↗](#).



Cluster access [Info](#)

Control how IAM principals can access this cluster.

Create A IAM ROLE IN WHICH SELECTAWS SERVICE EKS AND ASSIGN
[AmazonEKSClusterPolicy](#)

Cluster access [Info](#)

Control how IAM principals can access this cluster.

Bootstrap cluster administrator access [Info](#)

Choose whether the IAM principal creating the cluster has Kubernetes cluster administrator access.

☒ **Allow cluster administrator access**
Allow cluster administrator access for your IAM principal.

☐ **Disallow cluster administrator access**
Disallow cluster administrator access for your IAM principal.

Cluster authentication mode [Info](#)

Configure which source the cluster will use for authenticated IAM principals.

- ☒ **EKS API**
The cluster will source authenticated IAM principals only from EKS access entry APIs.
- ☐ **EKS API and ConfigMap**
The cluster will source authenticated IAM principals from both EKS access entry APIs and the aws-auth ConfigMap.
- ☐ **ConfigMap**
The cluster will source authenticated IAM principals only from the aws-auth ConfigMap.

Secrets encryption [Info](#)

Once turned on, secrets encryption cannot be modified or removed.

☒ Turn on envelope encryption of Kubernetes secrets using KMS

Specify networking

Networking [Info](#)

IP address family and service IP address range cannot be changed after cluster creation.

VPC [Info](#)

Select a VPC to use for your EKS cluster resources. To create a new VPC, go to the [VPC console](#).

vpc-04643f4dea97e29fa | Default ▼



Subnets [Info](#)

Choose the subnets in your VPC where the control plane may place elastic network interfaces (ENIs) to facilitate communication with your cluster. To create a new subnet, go to the corresponding page in the [VPC console](#).

Select subnets ▼



subnet-0886539ca2b844d31 ✕
us-east-1b 172.31.0.0/20

subnet-02c5d405a7b08401b ✕
us-east-1f 172.31.64.0/20

subnet-0e3cc9d94044f8c92 ✕
us-east-1a 172.31.32.0/20

subnet-0eb6fce940480b9ee ✕
us-east-1d 172.31.16.0/20

subnet-09cc10383c3868dff ✕
us-east-1c 172.31.80.0/20

subnet-0cc8f51b300fa5982 ✕
us-east-1e 172.31.48.0/20

create a new security group, go to the corresponding page in the [VPC console](#).

Select security groups ▼



Choose cluster IP address family [Info](#)

Specify the IP address type for pods and services in your cluster.

☒ IPv4

☐ IPv6

☐ Configure Kubernetes service IP address range [Info](#)

Specify the range from which cluster services will receive IP addresses.

Cluster endpoint access [Info](#)

Configure access to the Kubernetes API server endpoint.

☒ Public

The cluster endpoint is accessible from outside of your VPC. Worker node traffic will leave your VPC to connect to the endpoint.

☐ Public and private

The cluster endpoint is accessible from outside of your VPC. Worker node traffic to the endpoint will stay within your VPC.

☐ Private

CloudWatch [Info](#)

i You can enable CloudWatch Observability in your clusters through the CloudWatch Observability add-on. After your cluster is created, navigate to the add-ons tab and install CloudWatch Observability add-on to enable CloudWatch Application Signals and Container Insights and start ingesting telemetry into CloudWatch.

Control plane logging [Info](#)

Send audit and diagnostic logs from the Amazon EKS control plane to CloudWatch Logs.

- ☐ **API server**
Logs pertaining to API requests to the cluster.
- ☐ **Audit**
Logs pertaining to cluster access via the Kubernetes API.
- ☐ **Authenticator**
Logs pertaining to authentication requests into the cluster.
- ☐ **Controller manager**
Logs pertaining to state of cluster controllers.

- ☐ **API server**
Logs pertaining to API requests to the cluster.
- ☐ **Audit**
Logs pertaining to cluster access via the Kubernetes API.
- ☐ **Authenticator**
Logs pertaining to authentication requests into the cluster.
- ☐ **Controller manager**
Logs pertaining to state of cluster controllers.
- ☐ **Scheduler**
Logs pertaining to scheduling decisions.

Cancel

Previous

Next

- Step 3
[Configure observability](#)
- Step 4
Select add-ons
- Step 5
Configure selected add-ons settings
- Step 6
Review and create

CoreDNS [Info](#) ☒

Enable service discovery within your cluster.

Category
networking

☒ Installed by default

kube-proxy [Info](#) ☒

Enable service networking within your cluster.

Category
networking

☒ Installed by default

Amazon VPC CNI [Info](#) ☒

Enable pod networking within your cluster.

Category
networking

☒ Installed by default

Amazon EKS Pod Identity Agent [Info](#) ☒

Install EKS Pod Identity Agent to use EKS Pod Identity to grant AWS IAM permissions to pods through Kubernetes service accounts.

Category
security

Amazon GuardDuty EKS Runtime Monitoring [Info](#) ☐

Install EKS Runtime Monitoring add-on within your cluster. Ensure to enable EKS Runtime Monitoring within Amazon GuardDuty.

Category
security

CoreDNS [Info](#)

Category
networking

Status
✔ Installed by default

Version
Select the version for this add-on.

v1.11.1-eksbuild.4 ▼

kube-proxy [Info](#)

Category
networking

Status
✔ Installed by default

Version
Select the version for this add-on.

v1.29.0-eksbuild.1 ▼

Amazon VPC CNI [Info](#)

Category
networking

Status
✔ Installed by default

Version
Select the version for this add-on.

v1.16.0-eksbuild.1 ▼

Amazon EKS Pod Identity Agent [Info](#)

Remove add-on

Category
security

Status
✔ Ready to install

Version
Select the version for this add-on.

v1.2.0-eksbuild.1 ▼

Cancel

Previous

Next

Selected add-ons version

Add-on name	Version
coredns	v1.11.1-eksbuild.4
Add-on name	Version
kube-proxy	v1.29.0-eksbuild.1
Add-on name	Version
vpc-cni	v1.16.0-eksbuild.1
Add-on name	Version
eks-pod-identity-agent	v1.2.0-eksbuild.1

Cancel

Previous

Create

< 1 >

	Cluster name	Status	Kubernetes version	Support type	Provider
<input type="radio"/>	cluster-bicky	Active	1.29	Standard support until March 23, 2025	EKS

STEP 2 – NOW CREATE WORKER NODE

us-east-1:console.aws.amazon.com/eks/home?region=us-east-1#/clusters/cluster-123456789012/selected-tab=cluster-compute-tab

Gmail YouTube All Books

Services Search [Alt+S]

EC2 VPC S3 AWS Auto Scaling Simple Queue Service Simple Notification Service Key Management Service CloudTrail Amazon EventBridge RDS IAM Lambda DynamoDB

Amazon Elastic Kubernetes Service

Clusters **New**

- Amazon EKS Anywhere
 - Enterprise Subscriptions **New**
- Related services
 - Amazon ECR
 - AWS Batch

Documentation

Submit feedback

Status: Active Kubernetes version: 1.29 Support type: Standard support until March 23, 2025 Provider: EKS

< Overview Resources **Compute** Networking Add-ons Access Observability Upgrade insights Update history >

Nodes (0) [Info](#)

< 1 >

Node name	Instance type	Node group	Created	Status
No Nodes				
This cluster does not have any Nodes, or you don't have permission to view them.				

Node groups (0) [Info](#)

Edit Delete Add node group

Group name	Desired size	AMI release version	Launch template	Status
------------	--------------	---------------------	-----------------	--------

Node group configuration

These properties cannot be changed after the node group is created.

Name
Assign a unique name for this node group.

The node group name should begin with letter or digit and can have any of the following characters: the set of Unicode letters, digits, hyphens and underscores. Maximum length of 63.

Node IAM role [Info](#)
Select the IAM role that will be used by the nodes. To create a new role, go to the [IAM console](#).

The selected role must not be used by a self-managed node group as this could lead to a service interruption upon managed node group deletion.

[Learn more](#)

HERE ALSO CREATE WORKER NODE and also assign one role for that where basic permission will be given

workernode [Info](#)

Allows EC2 instances to call AWS services on your behalf.


Delete

Summary

Edit

Creation date
April 01, 2024, 12:17 (UTC+05:30)












ARN
 am:aws:iam::905418179079:role/workernode

Instance profile ARN
 arn:aws:iam::905418179079:instance-profile/workernode

Last activity
 8 hours ago

Maximum session duration
1 hour

[Permissions](#) | [Trust relationships](#) | [Tags](#) | [Access Advisor](#) | [Revoke sessions](#)

 S3  AWS Auto Scaling  Simple Queue Service  Simple Notification Service  Key Management Service  CloudTrail  Amazon EventBridge  RDS  IAM  Lambda  DynamoDB >

Access (IAM)

Permissions policies (3) [Info](#)

You can attach up to 10 managed policies.



[Simulate](#)







[Remove](#)

[Add permissions](#)

Filter by Type

All types

< 1 > 

<input type="checkbox"/>	Policy name Info	Type	Attached entities
<input type="checkbox"/>	  AmazonEC2ContainerRegistryReadO...	AWS managed	1
<input type="checkbox"/>	  AmazonEKS_CNI_Policy	AWS managed	1
<input type="checkbox"/>	  AmazonEKSWorkerNodePolicy	AWS managed	1

► **Permissions boundary** (not set)

Assign a unique name for this node group.

WORKER-NODE

The node group name should begin with letter or digit and can have any of the following characters: the set of Unicode letters, digits, hyphens and underscores. Maximum length of 63.

Node IAM role [Info](#)

Select the IAM role that will be used by the nodes. To create a new role, go to the [IAM console](#).

workernode



The selected role must not be used by a self-managed node group as this could lead to a service interruption upon managed node group deletion.

[Learn more](#)

Launch template [Info](#)

These properties cannot be changed after the node group is created.

☐ Use launch template

Configure this node group using an EC2 launch template.

Node group compute configuration

These properties cannot be changed after the node group is created.

AMI type [Info](#)

Select the EKS-optimized Amazon Machine Image for nodes.

Amazon Linux 2 (AL2_x86_64)

Capacity type

Select the capacity purchase option for this node group.

On-Demand

Instance types [Info](#)

Select instance types you prefer for this node group.

t3.medium

vCPU: 2 vCPUs Memory: 4 GiB Network: Up to 5 Gigabit Max ENI: 3 Max IPs: 18



Disk size

Select the size of the attached EBS volume for each node.

20

GiB

Node group scaling configuration

Desired size

Set the desired number of nodes that the group should launch with initially.

1 nodes

Desired node size must be greater than or equal to 0

Minimum size

Set the minimum number of nodes that the group can scale in to.

1 nodes

Minimum node size must be greater than or equal to 0

Maximum size

Set the maximum number of nodes that the group can scale out to.

2 nodes

Maximum node size must be greater than or equal to 1 and cannot be lower than the minimum size

Maximum node size must be greater than or equal to 1 and cannot be lower than the minimum size

Node group update configuration [Info](#)

Maximum unavailable

Set the maximum number or percentage of unavailable nodes to be tolerated during the node group version update.

☒ Number

Enter a number

☐ Percentage

Specify a percentage

Value

1 node

Node count must be greater than 0.

Cancel

Previous

Next

[y](#) > [Node groups](#) > Add node group

Specify networking

Node group network configuration

These properties cannot be changed after the node group is created.

Subnets [Info](#)

Specify the subnets in your VPC where your nodes will run. To create a new subnet, go to the corresponding page in the [VPC console](#).

Select subnets



subnet-0886539ca2b844d31 X

subnet-0e3cc9d94044f8c92 X

subnet-09cc10383c3868dff X

☐ Configure remote access to nodes [Info](#)

Cancel

Previous

Next

Node group update configuration

Maximum unavailable
1 node

Step 3: Networking

Edit

Node group network configuration

Subnets
subnet-0886539ca2b844d31
subnet-0e3cc9d94044f8c92
subnet-09cc10383c3868dff

Configure remote access to nodes
off

Cancel

Previous

Create

No Nodes

This cluster does not have any Nodes, or you don't have permission to view them.

Node groups (1) Info

Edit

Delete

Add node group

	Group name	Desired size	AMI release version	Launch template	Status
	WORKER-NODE	1	1.29.0-20240315	-	Creating

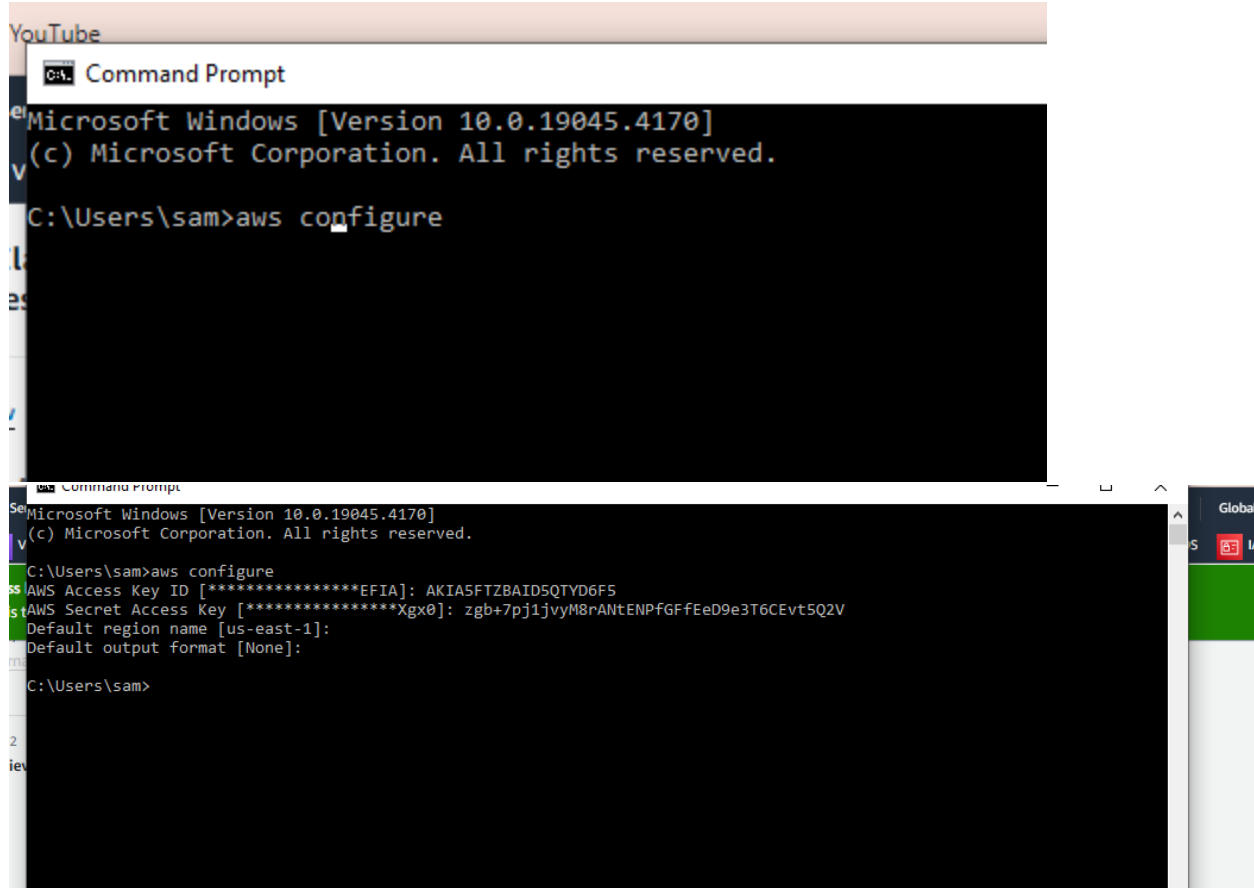
Fargate profiles (0) Info

Edit

Delete

Add Fargate profile

Now Connect with install and first do aws configure to use aws service and then install kubectl version



```
Microsoft Windows [Version 10.0.19045.4170]
(c) Microsoft Corporation. All rights reserved.

C:\Users\sam>aws configure

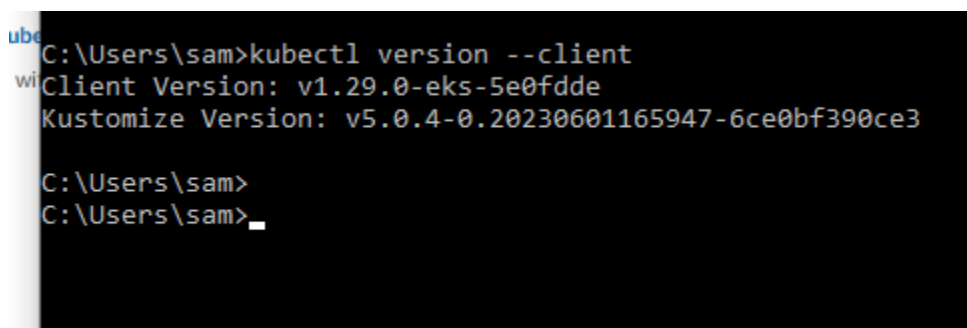
C:\Users\sam>aws configure
AWS Access Key ID [*****EFIA]: AKIA5FTZBAID5QTYD6F5
AWS Secret Access Key [*****Xgx0]: zgb+7pj1jvyM8rAntENPFGFFeE9e3T6CEvt5Q2V
Default region name [us-east-1]:
Default output format [None]:

C:\Users\sam>
```

NOW INSTALL KUBECTL

SO FOR THAT FOLLOW THESE DOCUMENTATION

<https://docs.aws.amazon.com/eks/latest/userguide/install-kubectl.html>



```
C:\Users\sam>kubectl version --client
Client Version: v1.29.0-eks-5e0fdde
Kustomize Version: v5.0.4-0.20230601165947-6ce0bf390ce3

C:\Users\sam>
C:\Users\sam>
```

So I had done onstallment of kubectl now configure kubectl

Cmd

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

aws eks update-kubeconfig --region us-east-1 --name [cluster-bicky](#)

```
C:\Users\sam>aws eks update-kubeconfig --region us-east-1 --name cluster-bicky
Updated context arn:aws:eks:us-east-1:905418179079:cluster/cluster-bicky in C:\Users\sam\.kube\config
C:\Users\sam>
```

next cmd –

kubectl get svc

```
C:\Users\sam>kubectl get svc
NAME          TYPE          CLUSTER-IP    EXTERNAL-IP    PORT(S)    AGE
kubernetes    ClusterIP     10.100.0.1    <none>         443/TCP    11h
C:\Users\sam>
```

next cmd –

Test if you can run command on your cluster using kubectl

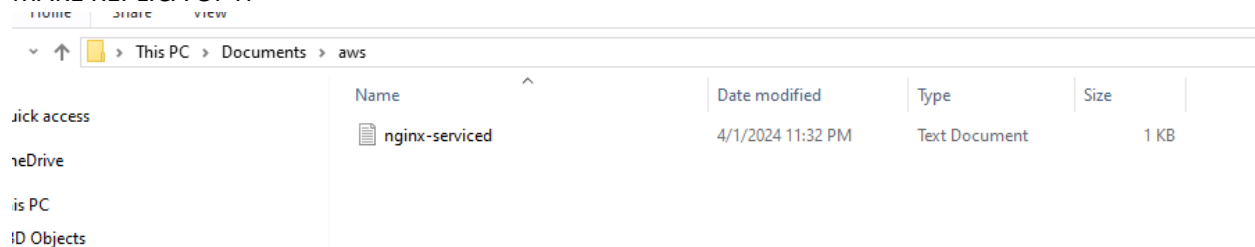
cmd- kubectl get nodes

```
C:\Users\sam>kubectl get nodes
NAME                                STATUS    ROLES    AGE    VERSION
ip-172-31-47-100.ec2.internal      Ready    <none>   56m    v1.29.0-eks-5e0fdde
C:\Users\sam>
```

now Appy deployment of manifest and service

first you need to save the NGINX SERVICE YAML FILE AS WELL AS NGINX SERICE YAML FILE

SAVE NGINX SERVICE YAML FILE ,BASICALLY WE ARE SAYING TO MAKE PULL IMAGE OF NGINX AND MAKE REPLICA OF IT



apiVersion: v1

kind: Service

metadata:

name: nginx-service

spec:

selector:

app: nginx

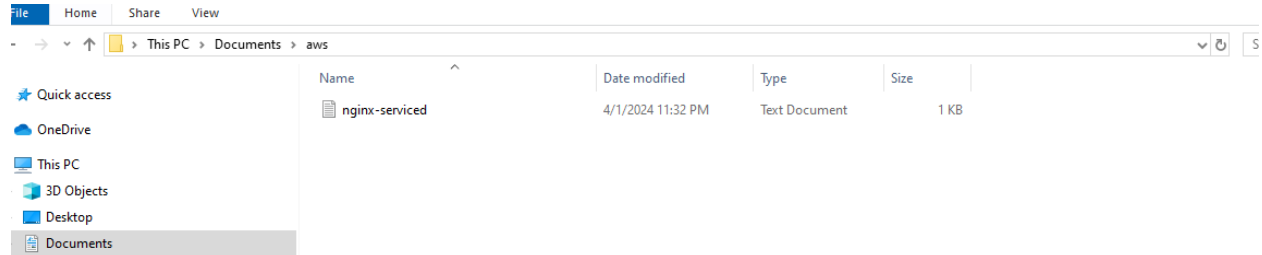
ports:

- protocol: TCP

port: 80

targetPort: 80

type: LoadBalancer



now COPY THE PATH AND IN SIMILAR MANNER SAVE THE NGNIX DEPLOYMENT YAML FILE

NGNIX DEPLOYMENT YAML FILE

apiVersion: apps/v1

kind: Deployment

metadata:

name: nginx-deployment

spec:

replicas: 3

selector:

matchLabels:

app: nginx

template:

metadata:

labels:

app: nginx

spec:

containers:

- name: nginx

image: nginx:latest

ports:

- containerPort: 80

SAVE IT AS nginx-deployment.yaml

NGINX SERVICE YAML FILE

apiVersion: v1

kind: Service

metadata:

name: nginx-service

spec:

selector:

app: nginx

ports:

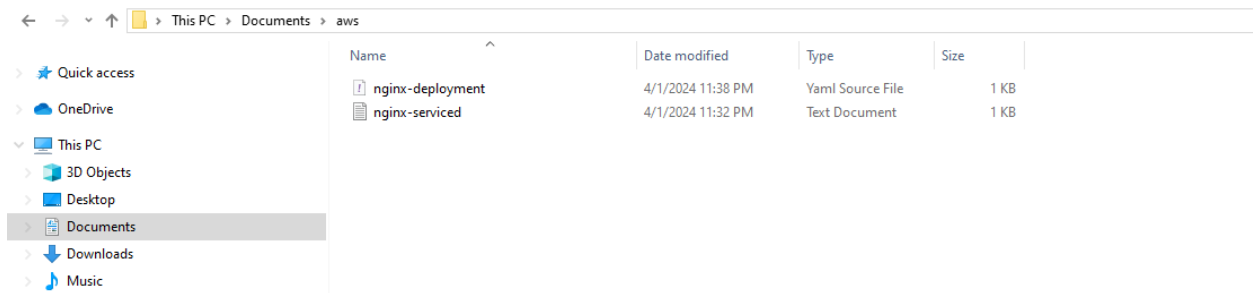
- protocol: TCP

port: 80

targetPort: 80

type: LoadBalancer

SAVE THESE FILE AS `nginx-service.yaml` AND IN SAVE LOCATION WHERE YOUR KUBECTL IS STORE AND DEPLOYMENT YAML FILE IS STORE



NOW Apply deployment of manifest and service

First go to the path where you install kubectl exe

The screenshot shows a Windows File Explorer window titled "kubectl.exe - Search Results in This PC". The search bar at the top contains "kubectl.exe". The left sidebar shows the navigation pane with "This PC" selected. The main area displays five search results:

File Name	Path	Type	Date modified	Size
kubectl.exe.sha256	C:\Users\sam\Documents	SHA256 File	4/1/2024 11:44 PM	77 bytes
kubectl!	C:\Users\sam\Documents	Application	4/1/2024 11:43 PM	48.6 MB
kubectl.exe.sha256	C:\Users\sam	SHA256 File	4/1/2024 12:50 PM	77 bytes
kubectl.execurl	C:\Users\sam	Application	4/1/2024 12:50 PM	326 bytes
kubectl!	C:\Users\sam	Application	4/1/2024 12:49 PM	48.6 MB

Go to the path now

```
error: the path "nginx-deployment.yaml" does not exist
C:\Users\sam>cd C:\Users\sam
C:\Users\sam>kubectl apply -f nginx-deployment.yaml
deployment.apps/nginx-deployment created
C:\Users\sam>
```

Used cmd - `kubectl apply -f nginx-service.yaml`

```
C:\Users\sam>kubect1 apply -f nginx-service.yaml
service/nginx-service created

C:\Users\sam>
```

So now go to worker node and check whether the 3 replica is create or not

For checking these go to cluster select cluster and the go to worker node

And select your node

Services Search [All+5] N. Virginia Vicky Omprakash Sharma

PC S3 AWS Auto Scaling Simple Queue Service Simple Notification Service Key Management Service CloudTrail Amazon EventBridge RDS IAM Lambda DynamoDB

elastic Service

Anywhere

Descriptions New

es

in

ack

Nodes (1) Info

Filter Nodes by property or value

Node name	Instance type	Node group	Created	Status
ip-172-31-47-100.ec2.internal	t3.medium	WORKER-NODE	Created 3 hours ago	Ready

Node groups (1) Info

Edit Delete Add node group

Group name	Desired size	AMI release version	Launch template	Status
WORKER-NODE	1	1.29.0-20240315	-	Active

Fargate profiles (0) Info

Edit Delete Add Fargate profile

Details **Nodes** Health issues 0 Kubernetes labels Update config Kubernetes taints Update history Tags

Nodes (1) Info

Filter Nodes by property or value

Node name	Instance type	Node group	Created	Status
ip-172-31-47-100.ec2.internal	t3.medium	WORKER-NODE	Created 3 hours ago	Ready

rice

re

ons New

Pods (8) Info

Name	Status	Created	IP
nginx-deployment-7c79c4bf97-2ck6f	Running	an hour ago	172.31.41.133
nginx-deployment-7c79c4bf97-bt7t2	Running	an hour ago	172.31.37.218
nginx-deployment-7c79c4bf97-xn4kf	Running	an hour ago	172.31.41.39
aws-node-pswvc	Running	3 hours ago	172.31.47.100
coredns-54d6f577c6-9cxp9	Running	12 hours ago	172.31.37.32
coredns-54d6f577c6-dnzvz	Running	12 hours ago	172.31.46.96
eks-pod-identity-agent-2srxw	Running	3 hours ago	172.31.47.100
kube-proxy-bprnz	Running	3 hours ago	172.31.47.100

We successfully get replicas now check load balancer is made or not

Load balancers (1)

Elastic Load Balancing scales your load balancer capacity automatically in response to changes in incoming traffic.

Actions ▾

Create load balancer ▾

Filter load balancers

<input type="checkbox"/>	Name ▾	DNS name ▾	State ▾	VPC ID ▾	Availability Zones ▾	Type ▾
<input type="checkbox"/>	a5858f4c2ae9b4d9d8...	a5858f4c2ae9b4d9d8ef50...	-	vpc-04643f4dea97e29fa	6 Availability Zones	classic

▾	Availability Zones ▾	Type ▾	Date created ▾
643f4dea97e29fa	6 Availability Zones	classic	April 2, 2024, 01:20 (U...