

Experiment No 4

Name: Mayur Jaiswal

Roll No: 26

Div: D15B

AIM: To install Kubectl and execute Kubectl commands to manage the Kubernetes cluster and deploy Your First Kubernetes Application.

- Running the application on the cluster

kubectl create deployment nginx --image=nginx

```
ubuntu@master:~$ kubectl create deployment nginx --image=nginx
deployment.apps/nginx created
ubuntu@master:~$
```

- Verifying the deployment using command

kubectl get deployments

```
ubuntu@master:~$ kubectl get deployments
NAME      READY   UP-TO-DATE   AVAILABLE   AGE
nginx     1/1     1            1           47s
ubuntu@master:~$
```

- Run the following command to create a service named nginx that will expose the app publicly.

kubectl expose deploy nginx --port 80 --target-port 80 --type NodePort

```
ubuntu@master:~$ kubectl expose deploy nginx --port 80 --target-port 80 --type NodePort
service/nginx exposed
ubuntu@master:~$
```

- Run this command to see the summary of the service and ports exposed.

kubectl get services

```
ubuntu@master:~$ kubectl get services
NAME         TYPE        CLUSTER-IP   EXTERNAL-IP   PORT(S)          AGE
kubernetes   ClusterIP   10.96.0.1    <none>        443/TCP          4d14h
nginx        NodePort    10.103.96.233 <none>        80:30816/TCP     67s
ubuntu@master:~$
```

- Add the port which is displayed i.e 30816 (will differ for each device) in the inbound rules of the security group of the worker.

The image shows two screenshots of the AWS Management Console. The top screenshot displays the 'Key pairs (2)' page, showing a table with two key pairs: 'vockey' and 'mayur'. The bottom screenshot displays the 'Security Groups (7)' page, showing a table with seven security groups. Both screenshots include the AWS navigation sidebar on the left and the top navigation bar with the user's profile and region (N. Virginia).

Key pairs (2)

Name	Type	Created	Fingerprint	ID
vockey	rsa	2024/07/24 09:35 GMT+5:30	54:aa:2d:cc:74:38:a4:eb:f5:66:12:6c...	key-076e4f0ec3e18528a
mayur	rsa	2024/10/15 19:15 GMT+5:30	55:d1:c7:6f:00:d5:e9:90:9f:73:e2:d...	key-088430597bb7ce54c

Security Groups (7)

Name	Security group ID	Security group name	VPC ID	Description
-	sg-0b6fb42acdef0bfc4	mayuropops	vpc-0e1ae88992574a815	devops
-	sg-061652699cfe57654	launch-wizard-4	vpc-0e1ae88992574a815	launch-wiz
-	sg-0ce34492b892cfa22	launch-wizard-1	vpc-0e1ae88992574a815	launch-wiz
-	sg-0ce23e457ec5f1fc5	mayurdevops	vpc-0e1ae88992574a815	hello
-	sg-0967cb2ca4e76404a	launch-wizard-3	vpc-0e1ae88992574a815	launch-wiz

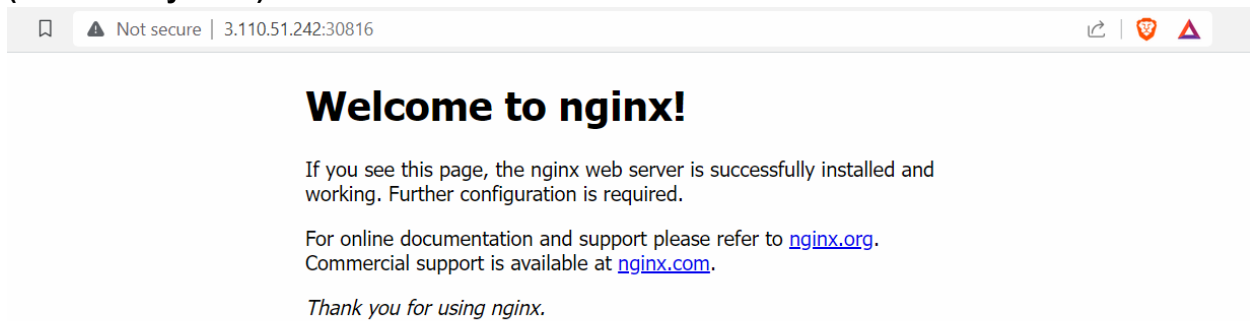
- We can verify that the nginx page is accessible on all nodes using curl command(Worker)
 1. sudo su
 2. curl worker:30816

```
ubuntu@worker:~$ sudo su
root@worker:/home/ubuntu# curl worker:30816
<!DOCTYPE html>
<html>
<head>
<title>Welcome to nginx!</title>
<style>
html { color-scheme: light dark; }
body { width: 35em; margin: 0 auto;
font-family: Tahoma, Verdana, Arial, sans-serif; }
</style>
</head>
<body>
<h1>Welcome to nginx!</h1>
<p>If you see this page, the nginx web server is successfully installed and
working. Further configuration is required.</p>

<p>For online documentation and support please refer to
<a href="http://nginx.org/">nginx.org</a>.<br/>
Commercial support is available at
<a href="http://nginx.com/">nginx.com</a>.</p>

<p><em>Thank you for using nginx.</em></p>
</body>
</html>
root@worker:/home/ubuntu#
```

Open a new tab in browser and paste the public IP address followed by :port number (30816 in my case)



Conclusion:

Thus, we have studied and implemented how to install Kubectl and execute Kubectl commands to manage the Kubernetes cluster and deploy.