

Project: Capstone 2

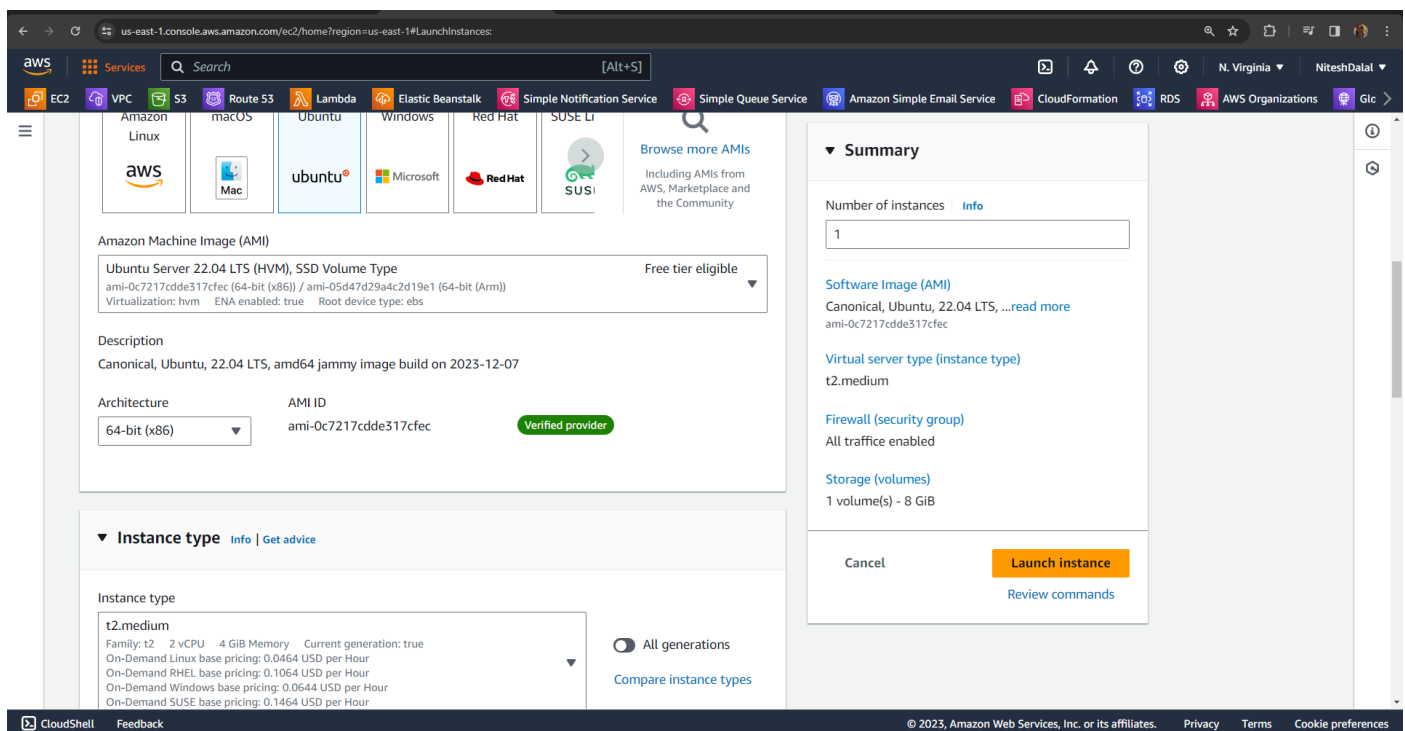
You are hired as a DevOps Engineer for Analytics Pvt Ltd. This company is a product based organization which uses Docker for their containerization needs within the company. The final product received a lot of traction in the first few weeks of launch. Now with the increasing demand, the organization needs to have a platform for automating deployment, scaling and operations of application containers across clusters of hosts. As a DevOps Engineer, you need to implement a DevOps lifecycle such that all the requirements are implemented without any change in the Docker containers in the testing environment. Up until now, this organization used to follow a monolithic architecture with just 2 developers. The product is present on: <https://github.com/hshar/website.git>

Following are the specifications of the lifecycle:

1. Git workflow should be implemented. Since the company follows a monolithic architecture of development, you need to take care of version control. The release should happen only on the 25th of every month.
2. CodeBuild should be triggered once the commits are made in the master branch.
3. The code should be containerized with the help of the Dockerfile. The Dockerfile should be built every time if there is a push to GitHub. Create a custom Docker image using a Dockerfile.
4. As per the requirement in the production server, you need to use the Kubernetes cluster and the containerized code from Docker Hub should be deployed with 2 replicas. Create a NodePort service and configure the same for port 30008.
5. Create a Jenkins Pipeline script to accomplish the above task.
6. For configuration management of the infrastructure, you need to deploy the configuration on the servers to install necessary software and configurations.
7. Using Terraform, accomplish the task of infrastructure creation in the AWS cloud provider.

Solution:

1. The very first task to perform is to create a Jenkins master ec2 instance where we will install and ansible & terraform tools. For resource management & configuration management. So, for that I am using a t2.medium instance with Ubuntu ami.



2. Now connect to instance and try installing terraform from official documentation.

```
us-east-1.console.aws.amazon.com/ec2-instance-connect/ssh?connType=standard&instanceId=i-0107956b2b5a53381&osUser=ubuntu&region=us-east-1&sshPort=22#/  
aws | Services | Search [Alt+S]  
EC2 VPC S3 Route 53 Lambda Elastic Beanstalk Simple Notification Service Simple Queue Service Amazon Simple Email Service CloudFormation RDS AWS Organizations  
Memory usage: 5% IPv4 address for eth0: 172.31.62.21  
Swap usage: 0%  
Expanded Security Maintenance for Applications is not enabled.  
0 updates can be applied immediately.  
Enable ESM Apps to receive additional future security updates.  
See https://ubuntu.com/esm or run: sudo pro status  
The list of available updates is more than a week old.  
To check for new updates run: sudo apt update  
The programs included with the Ubuntu system are free software;  
the exact distribution terms for each program are described in the  
individual files in /usr/share/doc/*/copyright.  
Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by  
applicable law.  
To run a command as administrator (user "root"), use "sudo <command>".  
See "man sudo_root" for details.  
ubuntu@ip-172-31-62-21:~$ wget -O- https://apt.releases.hashicorp.com/gpg | sudo gpg --dearmor -o /usr/share/keyrings/hashicorp-archive-keyring.gpg  
echo "deb [signed-by=/usr/share/keyrings/hashicorp-archive-keyring.gpg] https://apt.releases.hashicorp.com $(lsb_release -cs) main" | sudo tee /etc/apt/sources.list.d/hashicorp.list  
sudo apt update && sudo apt install terraform -y  
i-0107956b2b5a53381 (Machine-1)  
PublicIPs: 18.214.87.179 PrivateIPs: 172.31.62.21
```

3. Next task is to create all other resources, so for that we will create a main.tf file.

```
us-east-1.console.aws.amazon.com/ec2-instance-connect/ssh?connType=standard&instanceId=i-0107956b2b5a53381&osUser=ubuntu&region=us-east-1&sshPort=22#/  
aws | Services | Search [Alt+S]  
EC2 VPC S3 Route 53 Lambda Elastic Beanstalk Simple Notification Service Simple Queue Service Amazon Simple Email Service CloudFormation RDS AWS Organizations  
GNU nano 6.2 main.tf *  
provider "aws" {  
    region = "us-east-1"  
}  
resource "aws_instance" "K8-M" {  
    ami = "ami-0c7217cdde317cfec"  
    instance_type = "t2.medium"  
    key_name = "N_Virgina_6june"  
    tags = {  
        Name = "M-3"  
    }  
}  
resource "aws_instance" "K8-S1" {  
    ami = "ami-0c7217cdde317cfec"  
    instance_type = "t2.micro"  
    key_name = "N_Virgina_6june"  
    tags = {  
        Name = "M-2"  
    }  
}  
resource "aws_instance" "K8-S2" {  
    ami = "ami-0c7217cdde317cfec"  
    instance_type = "t2.micro"  
    key_name = "N_Virgina_6june"  
    tags = {  
        Name = "M-4"  
    }  
}  
^G Help ^O Write Out ^W Where Is ^K Cut ^T Execute ^C Location M-U Undo M-A Set Mark M-] To Bracket M-Q Previous  
^X Exit ^R Read File ^N Replace ^U Paste ^J Justify ^Y Go To Line M-B Redo M-G Copy ^_ Where Was M-W Next  
i-0107956b2b5a53381 (Machine-1)  
PublicIPs: 18.214.87.179 PrivateIPs: 172.31.62.21
```

4. Now let's first initialize the terraform by terraform init command.

```
ubuntu@ip-172-31-62-21:~$ terraform init
```

Initializing the backend...

Initializing provider plugins...

```
- Finding latest version of hashicorp/aws...
- Installing hashicorp/aws v5.31.0...
- Installed hashicorp/aws v5.31.0 (signed by HashiCorp)
```

Terraform has created a lock file `.terraform.lock.hcl` to record the provider selections it made above. Include this file in your version control repository so that Terraform can guarantee to make the same selections by default when you run "terraform init" in the future.

Terraform has been successfully initialized!

You may now begin working with Terraform. Try running "terraform plan" to see any changes that are required for your infrastructure. All Terraform commands should now work.

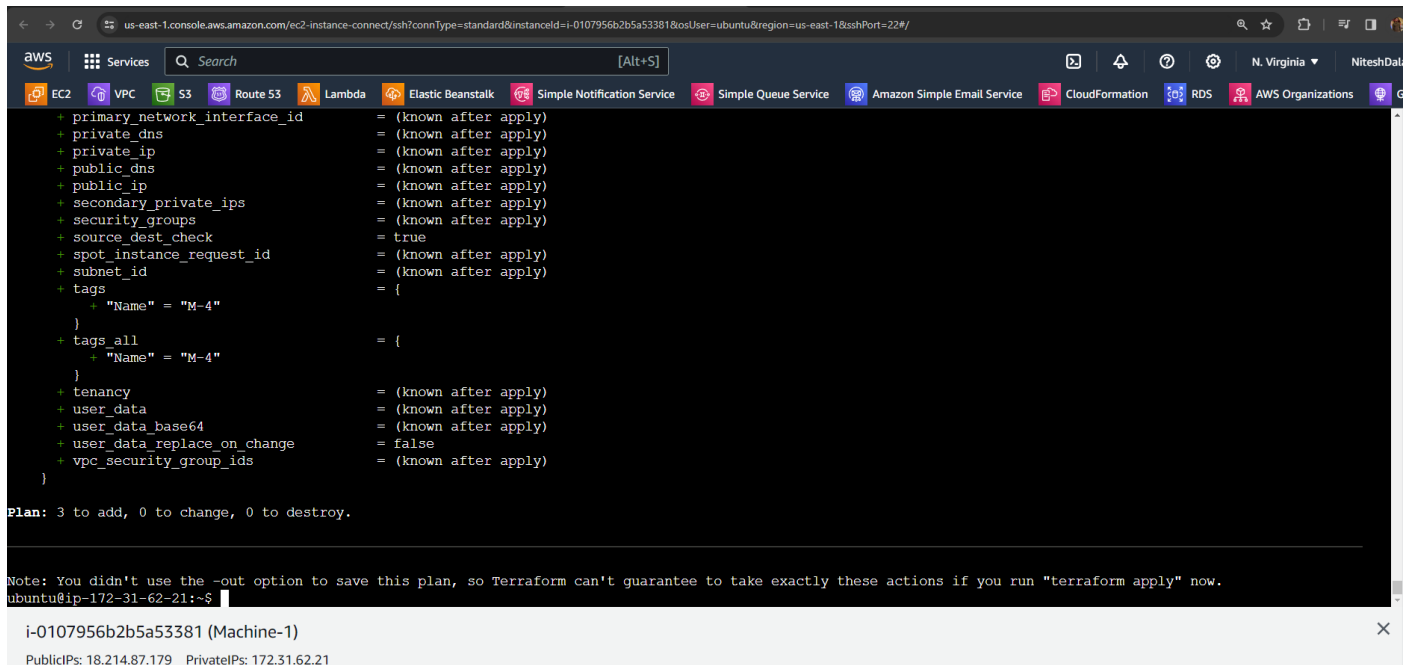
If you ever set or change modules or backend configuration for Terraform, rerun this command to reinitialize your working directory. If you forget, other commands will detect it and remind you to do so if necessary.

```
ubuntu@ip-172-31-62-21:~$
```

i-0107956b2b5a53381 (Machine-1)

PublicIPs: 18.214.87.179 PrivateIPs: 172.31.62.21

5. Now run the terraform plan command.



The screenshot shows the AWS Management Console interface. The top navigation bar includes the AWS logo, a search bar, and various service icons like EC2, VPC, S3, Route 53, Lambda, Elastic Beanstalk, Simple Notification Service, Simple Queue Service, Amazon Simple Email Service, CloudFormation, RDS, and AWS Organizations. The main content area displays the Terraform plan output for an EC2 instance. The plan shows that 3 resources will be added, 0 will be changed, and 0 will be destroyed. The resources listed include primary_network_interface_id, private_dns, private_ip, public_dns, public_ip, secondary_private_ips, security_groups, source_dest_check, spot_instance_request_id, subnet_id, tags, tags_all, tenancy, user_data, user_data_base64, user_data_replace_on_change, and vpc_security_group_ids. The plan is summarized as: Plan: 3 to add, 0 to change, 0 to destroy. A note at the bottom states: Note: You didn't use the -out option to save this plan, so Terraform can't guarantee to take exactly these actions if you run "terraform apply" now. The terminal output at the bottom shows the command: ubuntu@ip-172-31-62-21:~\$

```
us-east-1.console.aws.amazon.com/ec2-instance-connect/ssh?connType=standard&instanceId=i-0107956b2b5a53381&osUser=ubuntu&region=us-east-1&sshPort=22#/

aws Services Search [Alt+S]

EC2 VPC S3 Route 53 Lambda Elastic Beanstalk Simple Notification Service Simple Queue Service Amazon Simple Email Service CloudFormation RDS AWS Organizations

+ primary_network_interface_id = (known after apply)
+ private_dns                  = (known after apply)
+ private_ip                   = (known after apply)
+ public_dns                   = (known after apply)
+ public_ip                    = (known after apply)
+ secondary_private_ips        = (known after apply)
+ security_groups               = (known after apply)
+ source_dest_check            = true
+ spot_instance_request_id     = (known after apply)
+ subnet_id                    = (known after apply)
+ tags                         = {
+   "Name" = "M-4"
+ }
+ tags_all                     = {
+   "Name" = "M-4"
+ }
+ tenancy                      = (known after apply)
+ user_data                    = (known after apply)
+ user_data_base64             = (known after apply)
+ user_data_replace_on_change = false
+ vpc_security_group_ids       = (known after apply)
}

Plan: 3 to add, 0 to change, 0 to destroy.

Note: You didn't use the -out option to save this plan, so Terraform can't guarantee to take exactly these actions if you run "terraform apply" now.
ubuntu@ip-172-31-62-21:~$
```

i-0107956b2b5a53381 (Machine-1)

PublicIPs: 18.214.87.179 PrivateIPs: 172.31.62.21

6. Now let's run the terraform apply command.

```
us-east-1.console.aws.amazon.com/ec2-instance-connect/ssh?connType=standard&instanceId=i-0107956b2b5a53381&osUser=ubuntu@region=us-east-1&sshPort=22#/  
aws | Services | Search [Alt+S]  
EC2 VPC S3 Route 53 Lambda Elastic Beanstalk Simple Notification Service Simple Queue Service Amazon Simple Email Service CloudFormation RDS AWS Organizations  
}   
Plan: 3 to add, 0 to change, 0 to destroy.  
  
Do you want to perform these actions?  
Terraform will perform the actions described above.  
Only 'yes' will be accepted to approve.  
  
Enter a value: yes  
  
aws_instance.K8-M: Creating...  
aws_instance.K8-S1: Creating...  
aws_instance.K8-S2: Creating...  
aws_instance.K8-M: Still creating... [10s elapsed]  
aws_instance.K8-S1: Still creating... [10s elapsed]  
aws_instance.K8-S2: Still creating... [10s elapsed]  
aws_instance.K8-M: Still creating... [20s elapsed]  
aws_instance.K8-S1: Still creating... [20s elapsed]  
aws_instance.K8-S2: Still creating... [20s elapsed]  
aws_instance.K8-S1: Creation complete after 21s [id=i-0f20dfd1cc14573b7]  
aws_instance.K8-M: Still creating... [30s elapsed]  
aws_instance.K8-S2: Still creating... [30s elapsed]  
aws_instance.K8-S2: Creation complete after 31s [id=i-015ce882be8fab2e5]  
aws_instance.K8-M: Still creating... [40s elapsed]  
aws_instance.K8-M: Still creating... [50s elapsed]  
aws_instance.K8-M: Creation complete after 52s [id=i-0585a8ffd70552d61]  
  
Apply complete! Resources: 3 added, 0 changed, 0 destroyed.  
ubuntu@ip-172-31-62-21:~$  
  
i-0107956b2b5a53381 (Machine-1)  
PublicIPs: 18.214.87.179 PrivateIPs: 172.31.62.21
```

7. Now next task is to install ansible on Jenkins master to create the desired configuration of software's. Will follow the official documentation only.

```
us-east-1.console.aws.amazon.com/ec2-instance-connect/ssh?connType=standard&instanceId=i-0107956b2b5a53381&osUser=ubuntu@region=us-east-1&sshPort=22#/  
aws | Services | Search [Alt+S]  
EC2 VPC S3 Route 53 Lambda Elastic Beanstalk Simple Notification Service Simple Queue Service Amazon Simple Email Service CloudFormation RDS AWS Organizations  
Setting up python3-requests-ntlm (1.1.0-1.1) ...  
Setting up python3-winnm (0.3.0-2) ...  
Setting up ansible (8.7.0-1ppa-jammy) ...  
Setting up python3-paramiko (2.9.3-0ubuntu1) ...  
Processing triggers for man-db (2.10.2-1) ...  
Scanning processes...  
Scanning linux images...  
  
Running kernel seems to be up-to-date.  
  
No services need to be restarted.  
  
No containers need to be restarted.  
  
No user sessions are running outdated binaries.  
  
No VM guests are running outdated hypervisor (qemu) binaries on this host.  
ubuntu@ip-172-31-62-21:~$ ansible --version  
ansible [core 2.15.8]  
  config file = /etc/ansible/ansible.cfg  
  configured module search path = ['/home/ubuntu/.ansible/plugins/modules', '/usr/share/ansible/plugins/modules']  
  ansible python module location = /usr/lib/python3/dist-packages/ansible  
  ansible collection location = /home/ubuntu/.ansible/collections:/usr/share/ansible/collections  
  executable location = /usr/bin/ansible  
  python version = 3.10.12 (main, Nov 20 2023, 15:14:05) [GCC 11.4.0] (/usr/bin/python3)  
  jinja version = 3.0.3  
  libyaml = True  
ubuntu@ip-172-31-62-21:~$  
  
i-0107956b2b5a53381 (Machine-1)  
PublicIPs: 18.214.87.179 PrivateIPs: 172.31.62.21
```

8. After the ansible installation we will create password-less SSH connection b/w master machine i.e. M-1 and all others.

```
ubuntu@ip-172-31-61-47:~$ cd .ssh  
ubuntu@ip-172-31-61-47:~/.ssh$ sudo nano authorized_keys  
ubuntu@ip-172-31-61-47:~/.ssh$  
  
i-0585a8ffd70552d61 (M-3)  
PublicIPs: 54.144.199.142 PrivateIPs: 172.31.61.47
```

9. Now checking the connection.

```

ubuntu@ip-172-31-20-202:~$ ansible -m ping all
172.31.24.97 | SUCCESS => {
  "ansible_facts": {
    "discovered_interpreter_python": "/usr/bin/python3"
  },
  "changed": false,
  "ping": "pong"
}
172.31.5.32 | SUCCESS => {
  "ansible_facts": {
    "discovered_interpreter_python": "/usr/bin/python3"
  },
  "changed": false,
  "ping": "pong"
}
172.31.2.13 | SUCCESS => {
  "ansible_facts": {
    "discovered_interpreter_python": "/usr/bin/python3"
  },
  "changed": false,
  "ping": "pong"
}
ubuntu@ip-172-31-20-202:~$ ls

```

i-038f9216b2e5f96b1 (M-1)
PublicIPs: 3.17.141.0 PrivateIPs: 172.31.20.202

10. Now creating three shell scripts to install the configuration.

```

ubuntu@ip-172-31-23-144:~$ cat w1.sh
sudo apt update
sudo apt install openjdk-11-jdk -y
sudo wget -O /usr/share/keyrings/jenkins-keyring.asc \
  https://pkg.jenkins.io/debian/jenkins.io-2023.key
echo deb [signed-by=/usr/share/keyrings/jenkins-keyring.asc] \
  https://pkg.jenkins.io/debian binary/ | sudo tee \
  /etc/apt/sources.list.d/jenkins.list > /dev/null
sudo apt-get update
sudo apt-get install jenkins -y
ubuntu@ip-172-31-23-144:~$ cat w24.sh
sudo apt-get update
sudo apt-get install docker.io -y
sudo apt update
sudo apt upgrade -y
sudo apt install -y curl apt-transport-https ca-certificates software-properties-common
curl -s https://packages.cloud.google.com/apt/doc/apt-key.gpg | sudo apt-key add -
sudo add-apt-repository "deb http://apt.kubernetes.io/ kubernetes-xenial main"
sudo swapoff -a
sudo apt update
sudo apt install -y kubelet kubeadm kubectl
ubuntu@ip-172-31-23-144:~$ cat w3.sh
sudo apt-get update
sudo apt install openjdk-11-jdk -y
sudo apt-get install docker.io -y
sudo apt update
sudo apt upgrade -y
sudo apt install -y curl apt-transport-https ca-certificates software-properties-common
curl -s https://packages.cloud.google.com/apt/doc/apt-key.gpg | sudo apt-key add -
sudo add-apt-repository "deb http://apt.kubernetes.io/ kubernetes-xenial main"
sudo swapoff -a
sudo apt update
sudo apt install -y kubelet kubeadm kubectl

```

11. Creating a play.yaml file to execute this scripts.

```

---
- name: installing jenkins and java
  hosts: localhost
  become: true
  tasks:
    - name: executing script w1.sh
      script: w1.sh
- name: installing java, docker and k8s
  hosts: master
  become: true
  tasks:
    - name: executing w3.sh
      script: w3.sh
- name: installing k8s and docker in k8s slaves
  hosts: slave
  become: true
  tasks:
    - name: executing script w24.sh
      script: w24.sh

```

12. Successful execution of ansible playbook file complete.

```

ubuntu@ip-172-31-20-202:~$ ansible-playbook play.yaml

PLAY [installing jenkins and java] *****

TASK [Gathering Facts] *****
ok: [localhost]

TASK [executing script w1.sh] *****
changed: [localhost]

PLAY [installing java, docker and k8s] *****

TASK [Gathering Facts] *****
ok: [172.31.24.97]

TASK [executing w3.sh] *****
changed: [172.31.24.97]

PLAY [installing k8s and docker in k8s slaves] *****

TASK [Gathering Facts] *****
ok: [172.31.5.32]
ok: [172.31.2.13]

TASK [executing script w24.sh] *****
changed: [172.31.5.32]

```

i-038f9216b2e5f96b1 (M-1)

PublicIPs: 3.17.141.0 PrivateIPs: 172.31.20.202

13. Now to go to our Kubernetes master machine which is M-3 and initialize the cluster.

```

[bootstrap-token] Configured RBAC rules to allow Node Bootstrap tokens to get nodes
[bootstrap-token] Configured RBAC rules to allow Node Bootstrap tokens to post CSRs in order for nodes to get long term certificate credentials
[bootstrap-token] Configured RBAC rules to allow the csrapprover controller automatically approve CSRs from a Node Bootstrap Token
[bootstrap-token] Configured RBAC rules to allow certificate rotation for all node client certificates in the cluster
[bootstrap-token] Creating the "cluster-info" ConfigMap in the "kube-public" namespace
[kubelet-finalize] Updating "/etc/kubernetes/kubelet.conf" to point to a rotatable kubelet client certificate and key
[addons] Applied essential addon: CoreDNS
[addons] Applied essential addon: kube-proxy

Your Kubernetes control-plane has initialized successfully!

To start using your cluster, you need to run the following as a regular user:

  mkdir -p $HOME/.kube
  sudo cp -i /etc/kubernetes/admin.conf $HOME/.kube/config
  sudo chown $(id -u):$(id -g) $HOME/.kube/config

Alternatively, if you are the root user, you can run:

  export KUBECONFIG=/etc/kubernetes/admin.conf

You should now deploy a pod network to the cluster.
Run "kubectl apply -f [podnetwork].yaml" with one of the options listed at:
  https://kubernetes.io/docs/concepts/cluster-administration/addons/

Then you can join any number of worker nodes by running the following on each as root:

kubeadm join 172.31.24.97:6443 --token 2f6ycy.uvriu22qx2ypvobe \
--discovery-token-ca-cert-hash sha256:4162d7b980f104895bae15eb4c3dc5526a16cd0a7fe2b58d74fdccda136dfe8a

```

i-060a066b2fe4e793f (M-3)

PublicIPs: 3.133.97.99 PrivateIPs: 172.31.24.97

14. Once done run these 3 commands as normal user in M-3.

```
ubuntu@ip-172-31-24-97:~$ mkdir -p $HOME/.kube
ubuntu@ip-172-31-24-97:~$ sudo cp -i /etc/kubernetes/admin.conf $HOME/.kube/config
ubuntu@ip-172-31-24-97:~$ sudo chown $(id -u):$(id -g) $HOME/.kube/config
ubuntu@ip-172-31-24-97:~$ kubectl apply -f https://github.com/weaveworks/weave/releases/download/v2.8.1/weave-daemonset-k8s.yaml
serviceaccount/weave-net created
clusterrole.rbac.authorization.k8s.io/weave-net created
clusterrolebinding.rbac.authorization.k8s.io/weave-net created
role.rbac.authorization.k8s.io/weave-net created
rolebinding.rbac.authorization.k8s.io/weave-net created
daemonset.apps/weave-net created
```

15. In slave machine M-2&4 enter the token from master machine to join the network. But as root user.

```
ubuntu@ip-172-31-2-13:~$ sudo su
root@ip-172-31-2-13:/home/ubuntu# kubeadm join 172.31.24.97:6443 --token 2f6ycy.uvriu22qx2ypvobe \
> --discovery-token-ca-cert-hash sha256:4162d7b980f104895bae15eb4c3dc5526a16cd0a7fe2b58d74fdccda136dfe8a
[preflight] Running pre-flight checks
[preflight] Reading configuration from the cluster...
[preflight] FYI: You can look at this config file with 'kubectl -n kube-system get cm kubeadm-config -o yaml'
[kubelet-start] Writing kubelet configuration to file "/var/lib/kubelet/config.yaml"
[kubelet-start] Writing kubelet environment file with flags to file "/var/lib/kubelet/kubeadm-flags.env"
[kubelet-start] Starting the kubelet
[kubelet-start] Waiting for the kubelet to perform the TLS Bootstrap...

This node has joined the cluster:
* Certificate signing request was sent to apiservert and a response was received.
* The Kubelet was informed of the new secure connection details.

Run 'kubectl get nodes' on the control-plane to see this node join the cluster.

root@ip-172-31-2-13:/home/ubuntu#
```

i-09417e11874c7473b (M-4)

PublicIPs: 3.17.174.149 PrivateIPs: 172.31.2.13

```
ubuntu@ip-172-31-5-32:~$ sudo su
root@ip-172-31-5-32:/home/ubuntu# kubeadm join 172.31.24.97:6443 --token 2f6ycy.uvriu22qx2ypvobe \
> --discovery-token-ca-cert-hash sha256:4162d7b980f104895bae15eb4c3dc5526a16cd0a7fe2b58d74fdccda136dfe8a
[preflight] Running pre-flight checks
[preflight] Reading configuration from the cluster...
[preflight] FYI: You can look at this config file with 'kubectl -n kube-system get cm kubeadm-config -o yaml'
[kubelet-start] Writing kubelet configuration to file "/var/lib/kubelet/config.yaml"
[kubelet-start] Writing kubelet environment file with flags to file "/var/lib/kubelet/kubeadm-flags.env"
[kubelet-start] Starting the kubelet
[kubelet-start] Waiting for the kubelet to perform the TLS Bootstrap...

This node has joined the cluster:
* Certificate signing request was sent to apiservert and a response was received.
* The Kubelet was informed of the new secure connection details.

Run 'kubectl get nodes' on the control-plane to see this node join the cluster.

root@ip-172-31-5-32:/home/ubuntu#
```

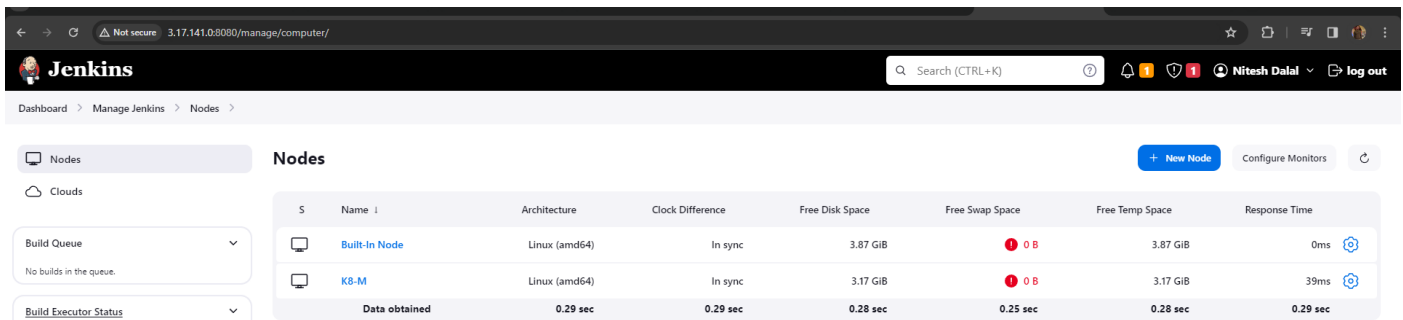
i-09bb5811236e6ef62 (M-2)

PublicIPs: 3.137.183.91 PrivateIPs: 172.31.5.32

16. Now next task is to setup Jenkins dashboard from port 8080 of master machine i.e. M-1.

The screenshot shows the Jenkins web interface. The top bar has the Jenkins logo, a search bar, and a user profile for 'Nitesh Dalal' with a 'log out' button. The left sidebar lists 'Dashboard' as the active page, along with 'New Item', 'People', 'Build History', 'Manage Jenkins', and 'My Views'. The main area is titled 'Welcome to Jenkins!' and contains a message: 'This page is where your Jenkins jobs will be displayed. To get started, you can set up distributed builds or start building a software project.' Below this, there's a section 'Start building your software project' with a 'Create a job' button. Another section 'Set up a distributed build' includes buttons for 'Set up an agent', 'Configure a cloud', and a link to 'Learn more about distributed builds'. On the left, there are two status boxes: 'Build Queue' (showing 'No builds in the queue') and 'Build Executor Status' (showing two 'Idle' executors).

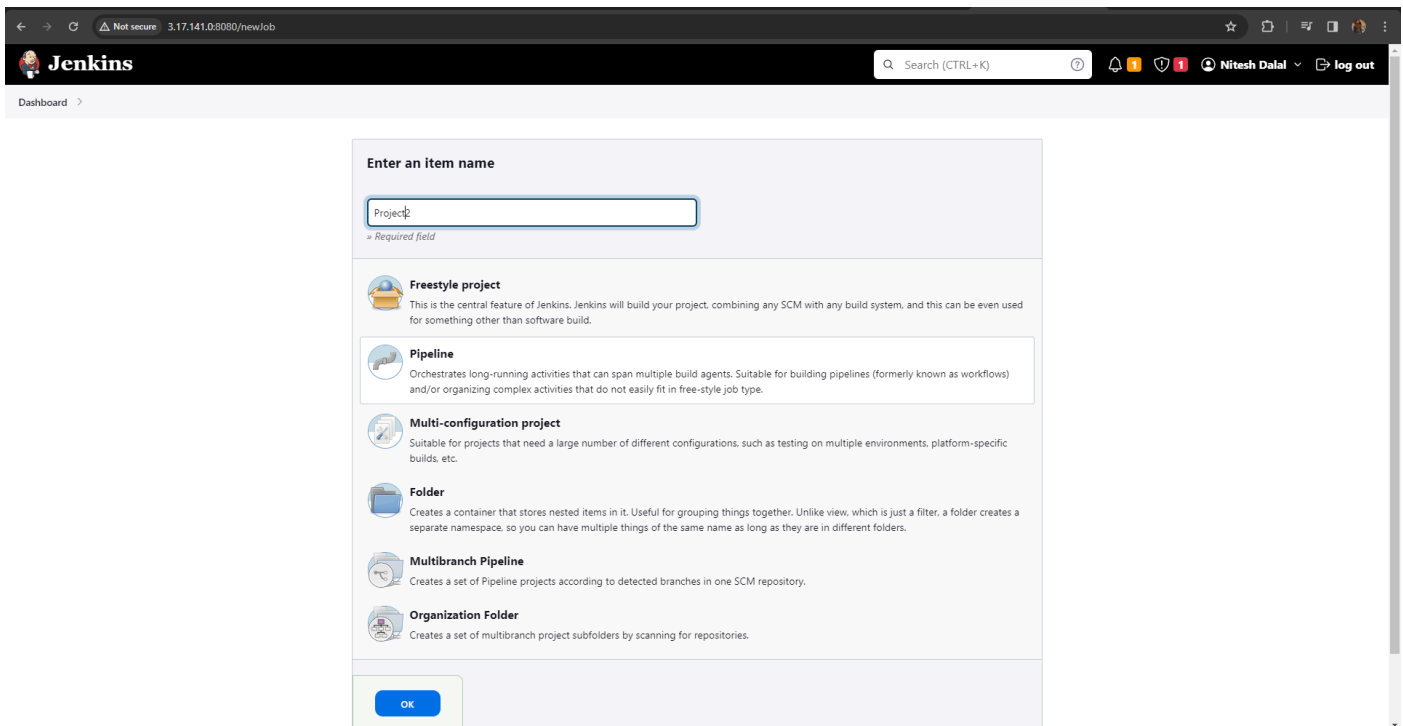
17. Add your M-3 machine as a node in Jenkins dashboard.



The screenshot shows the Jenkins 'Nodes' page. On the left, there are filters for 'Nodes' (selected), 'Build Queue' (showing 'No builds in the queue'), and 'Build Executor Status'. The main table lists two nodes: 'Built-In Node' and 'K8-M'. Both are Linux (amd64) architecture, in sync, with 3.87 GiB and 3.17 GiB of free disk space respectively. The 'Data obtained' row shows performance metrics for each node.

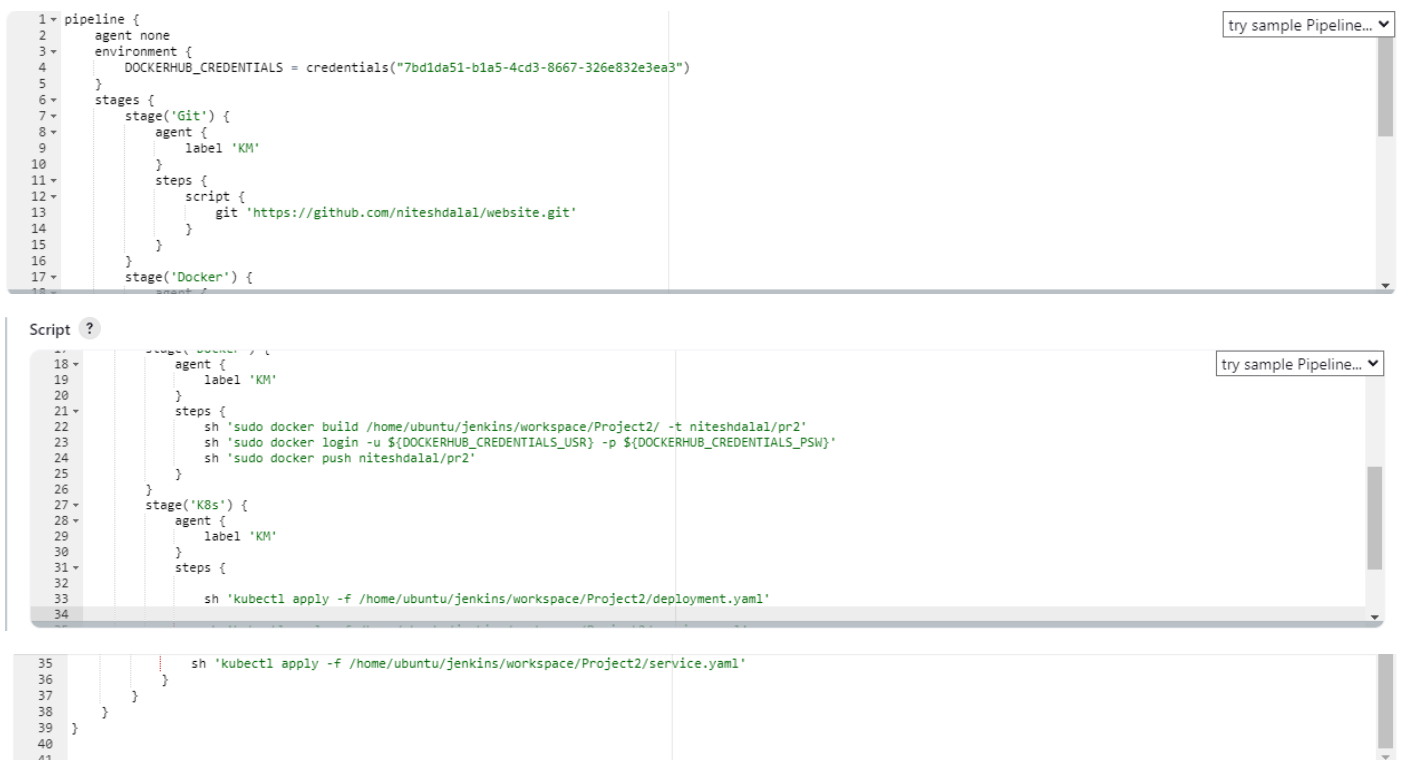
S	Name	Architecture	Clock Difference	Free Disk Space	Free Swap Space	Free Temp Space	Response Time
1	Built-In Node	Linux (amd64)	In sync	3.87 GiB	0 B	3.87 GiB	0ms
2	K8-M	Linux (amd64)	In sync	3.17 GiB	0 B	3.17 GiB	39ms
Data obtained		0.29 sec	0.29 sec	0.28 sec	0.25 sec	0.28 sec	0.29 sec

18. Now next we will create a job in Jenkins as a Pipeline.



The screenshot shows the 'Enter an item name' dialog in Jenkins. The 'Item name' field contains 'Project2'. Below the field, there are several project type options: 'Freestyle project', 'Pipeline', 'Multi-configuration project', 'Folder', 'Multibranch Pipeline', and 'Organization Folder'. The 'Pipeline' option is selected.

19. Now we create a script for the pipeline, and also enable the github trigger.

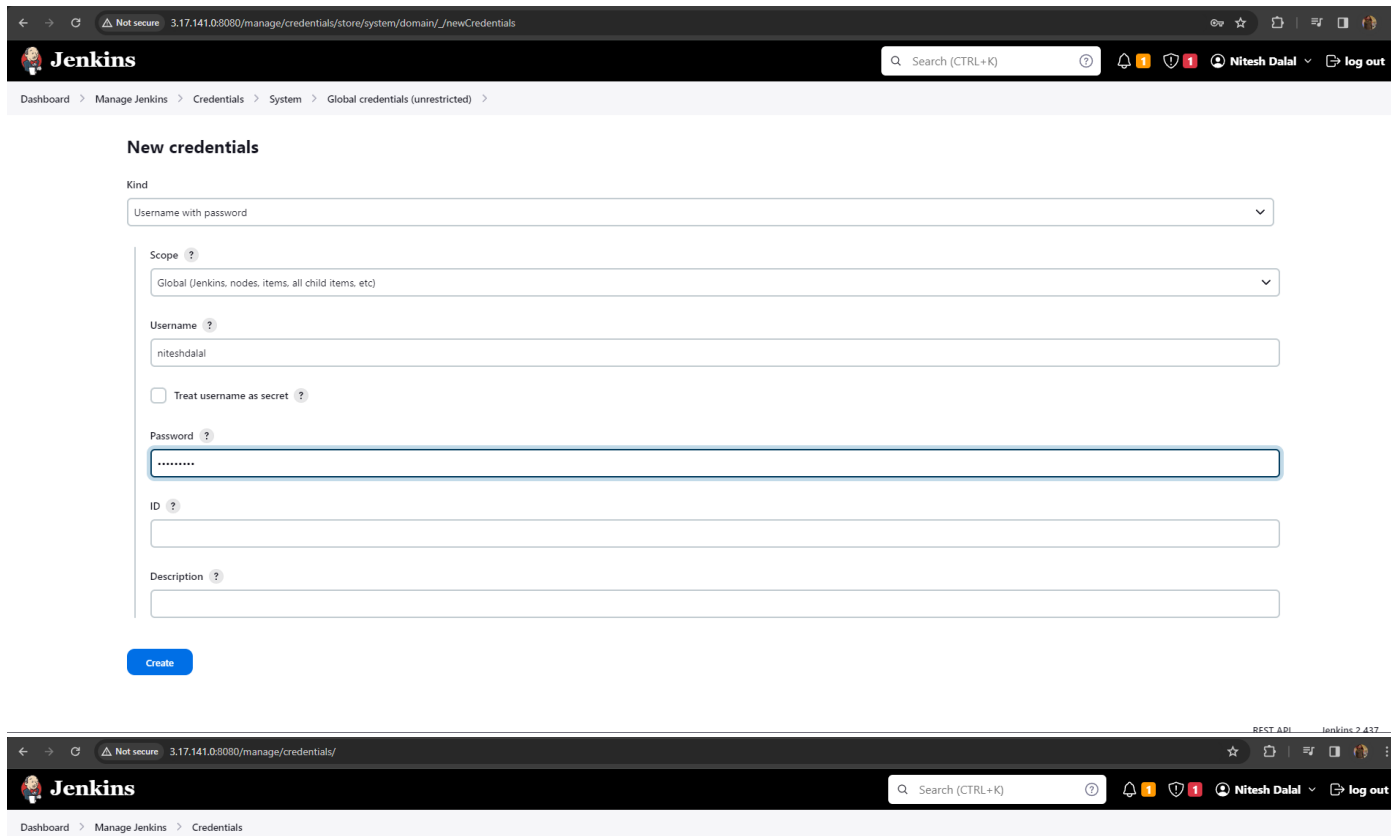


The screenshot shows the Jenkins Pipeline script editor. The script is as follows:

```

1 pipeline {
2   agent none
3   environment {
4     DOCKERHUB_CREDENTIALS = credentials("7bd1da51-b1a5-4cd3-8667-326e832e3ea3")
5   }
6   stages {
7     stage('Git') {
8       agent {
9         label 'KM'
10      }
11      steps {
12        script {
13          git 'https://github.com/niteshdalal/website.git'
14        }
15      }
16    }
17    stage('Docker') {
18      agent {
19        label 'KM'
20      }
21      steps {
22        sh 'sudo docker build /home/ubuntu/jenkins/workspace/Project2/ -t niteshdalal/pr2'
23        sh 'sudo docker login -u ${DOCKERHUB_CREDENTIALS_USR} -p ${DOCKERHUB_CREDENTIALS_PSW}'
24        sh 'sudo docker push niteshdalal/pr2'
25      }
26    }
27    stage('K8s') {
28      agent {
29        label 'KM'
30      }
31      steps {
32        sh 'kubectl apply -f /home/ubuntu/jenkins/workspace/Project2/deployment.yaml'
33      }
34    }
35    stage('Service') {
36      agent {
37        label 'KM'
38      }
39      steps {
40        sh 'kubectl apply -f /home/ubuntu/jenkins/workspace/Project2/service.yaml'
41      }
42    }
43  }
44 }
45 
```


20. Since, we need our Dockerhub username & password for pushing the image to dockerhub. For this we will create a credential variable in Jenkins dashboard. It will be used in groovy script in Jenkins pipeline.



The screenshot shows the Jenkins 'New credentials' form. The 'Kind' is set to 'Username with password'. The 'Scope' is 'Global (Jenkins, nodes, items, all child items, etc)'. The 'Username' is 'niteshdalal'. The 'Password' is masked with dots. The 'ID' is empty. The 'Description' is empty. A 'Create' button is at the bottom.

Kind: Username with password

Scope: Global (Jenkins, nodes, items, all child items, etc)

Username: niteshdalal

☐ Treat username as secret

Password:

ID:

Description:

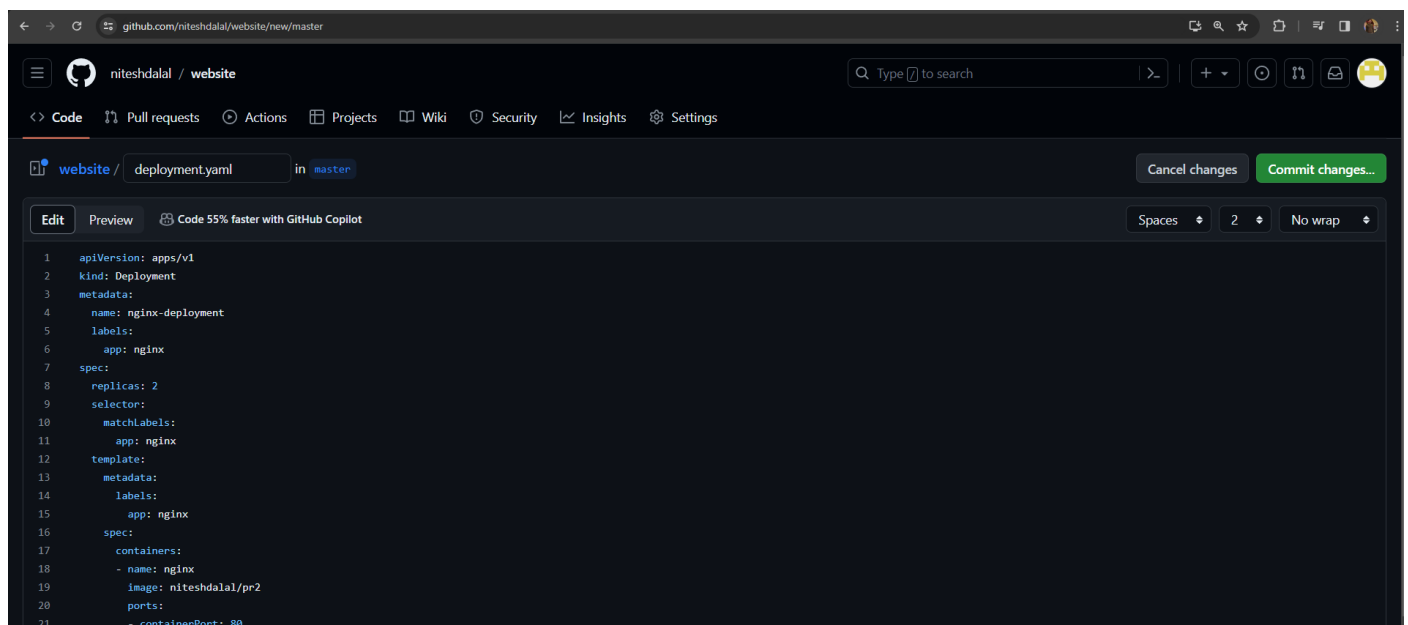
Create

Credentials

T	P	Store	I	Domain	ID	Name
		System		(global)	a587d6dd-f91d-4564-b34b-2e1be1dff5a5	ubuntu
		System		(global)	7bd1da51-b1a5-4cd3-8667-326e832e3ea3	niteshdalal/*****

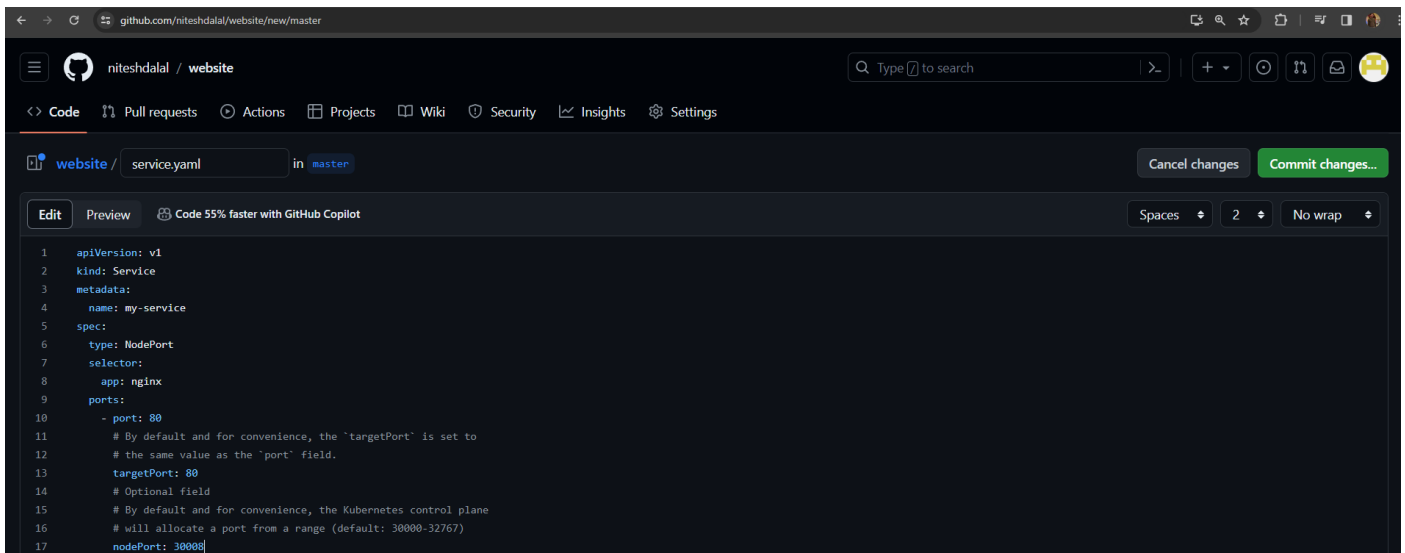
Stores scoped to Jenkins

21. Now we will create two manifest file on github. One for deployment and one for service.

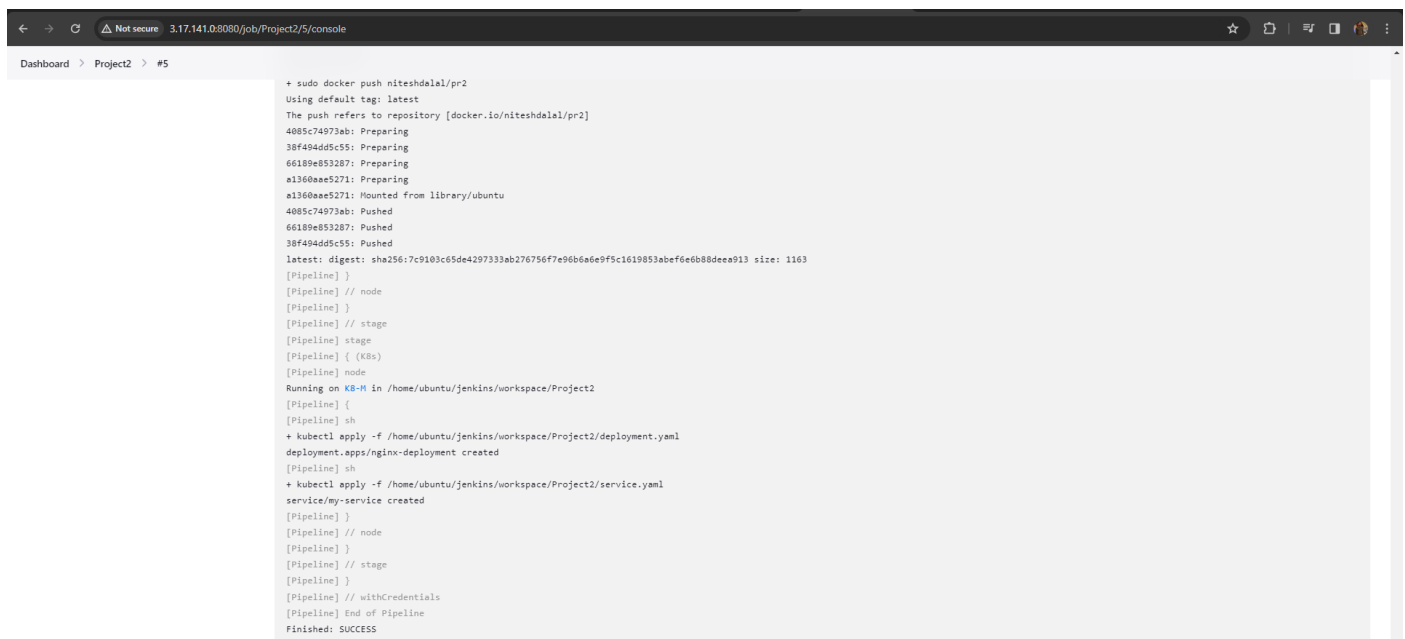


The screenshot shows a GitHub repository named 'website' by 'niteshdalal'. The file 'deployment.yaml' is selected. The code is as follows:

```
1 apiVersion: apps/v1
2 kind: Deployment
3 metadata:
4   name: nginx-deployment
5   labels:
6     app: nginx
7 spec:
8   replicas: 2
9   selector:
10    matchLabels:
11      app: nginx
12   template:
13     metadata:
14       labels:
15         app: nginx
16     spec:
17       containers:
18         - name: nginx
19           image: niteshdalal/pr2
20           ports:
21             - containerPort: 80
```



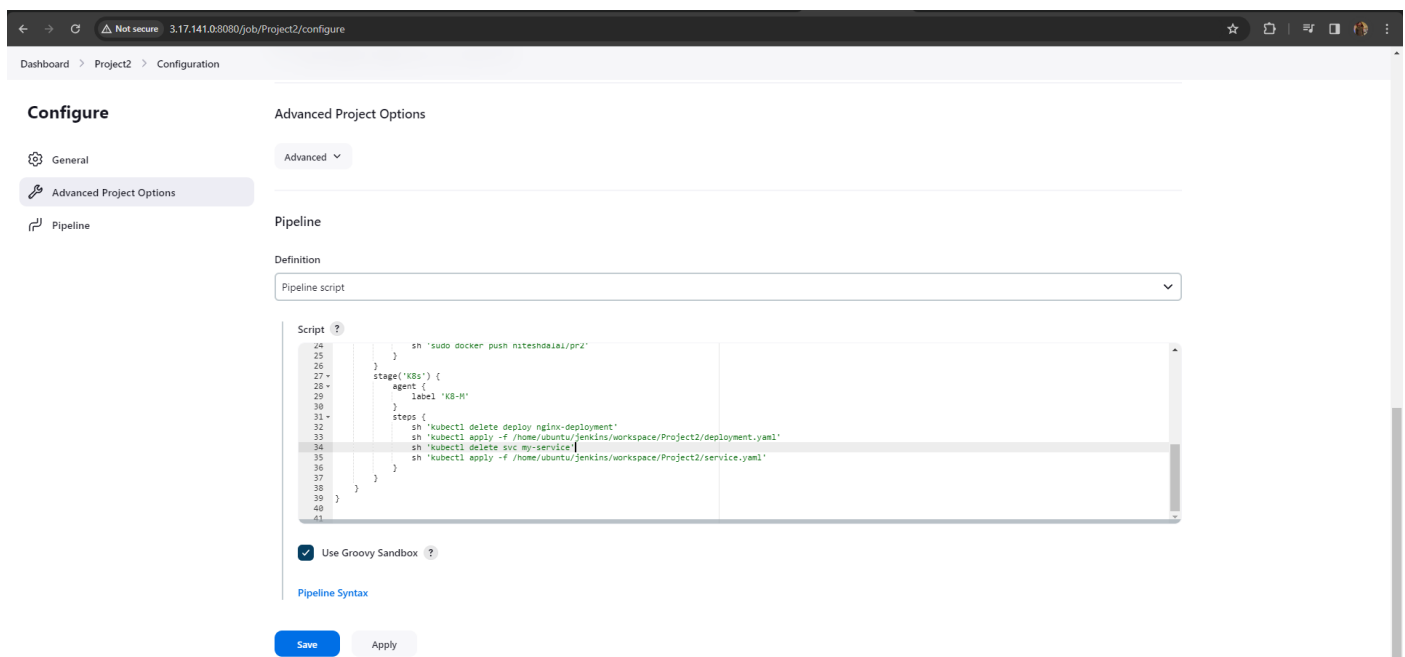
22. Once done go ahead and do you first build.



23. If it runs successfully then you should be able to see the website of public IP of worker2&4 followed by the service port 30008.



24. Now to avoid error of container already exists. We need to modify the groovy script. I added two lines to force kubernetes to delete old deployment & service every time a new changes occur.



25. Also let's create a webhook for project to ensure code build run automatically.

github.com/niteshdalal/website/settings/hooks/new

General

Access

Collaborators

Moderation options

Code and automation

Branches

Tags

Rules

Actions

Webhooks

Environments

Codespaces

Pages

Security

Code security and analysis

Deploy keys

Secrets and variables

Integrations

GitHub Apps

Webhooks / Add webhook

We'll send a POST request to the URL below with details of any subscribed events. You can also specify which data format you'd like to receive (JSON, x-www-form-urlencoded, etc). More information can be found in [our developer documentation](#).

Payload URL *

http://3.17.141.0:8080/github-webhook

Content type

application/x-www-form-urlencoded

Secret

Which events would you like to trigger this webhook?

☒ Just the push event.

☐ Send me everything.

☐ Let me select individual events.

☒ **Active**

We will deliver event details when this hook is triggered.

Add webhook

26. Let's try changing website content to see if code build triggers job automatically.

github.com/niteshdalal/website/edit/master/index.html

niteshdalal / website

Code Pull requests Actions Projects Wiki Security Insights Settings

Files

master

Go to file

images

Dockerfile

deployment.yaml

index.html

service.yaml

website / index.html in master

Cancel changes Commit changes...

Edit Preview Code 55% faster with GitHub Copilot

Spaces 2 No wrap

```
1 <html>
2 <head>
3 <title> Intellipaat </title>
4 </head>
5 <body style = "background-image:url('images/github3.jpg'); background-size: 100%">
6 <h2 ALIGN-CENTER>Hello world! From Nitesh</h2>
7 </body>
8 </html>
9
```

See the H2 content got changed.

