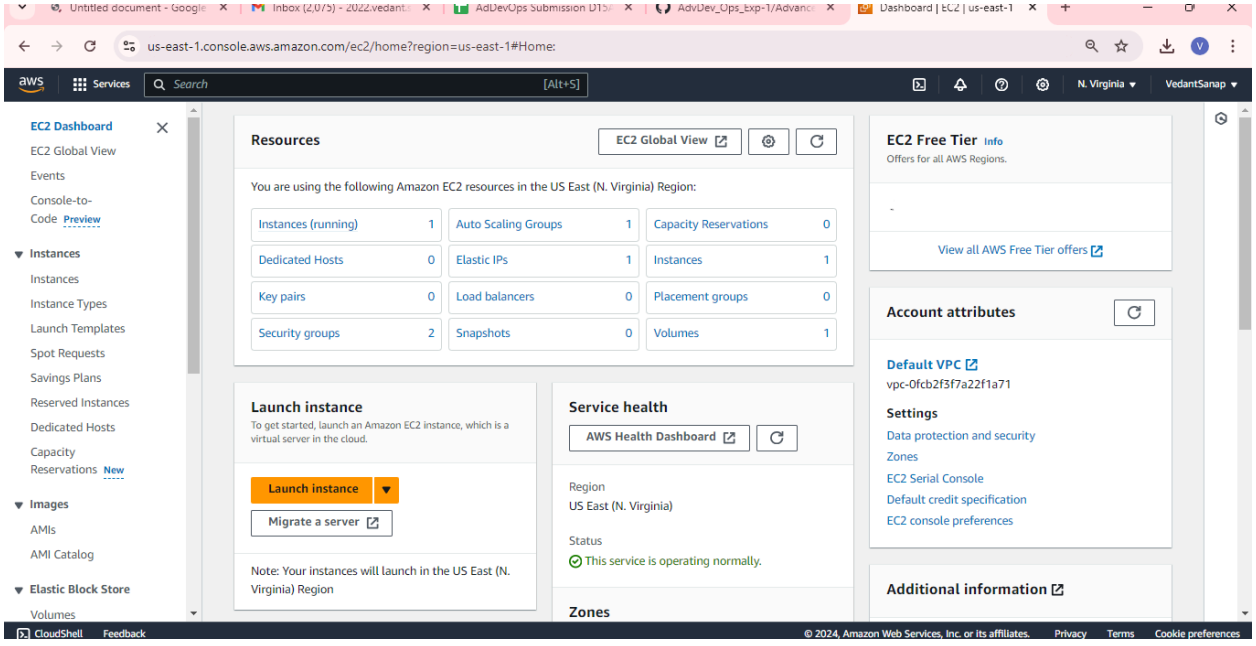
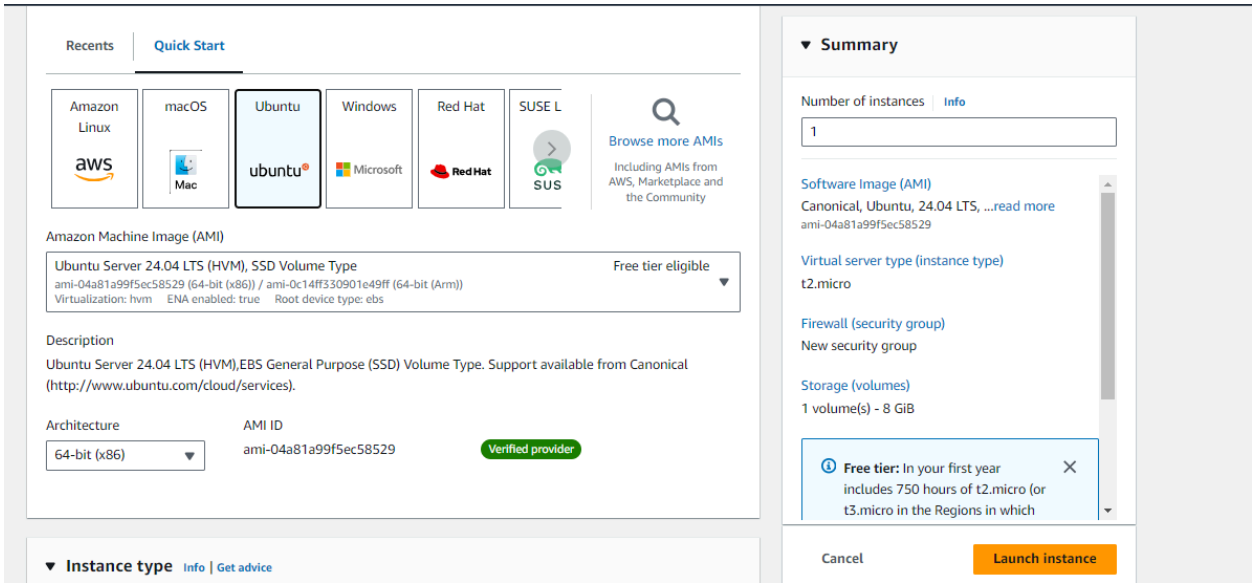
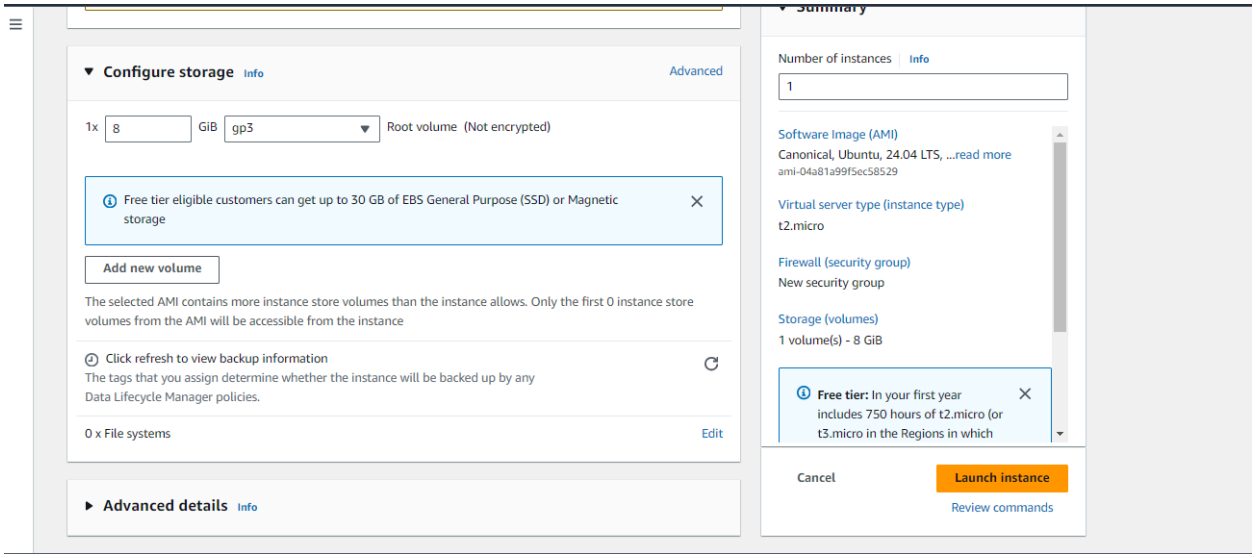
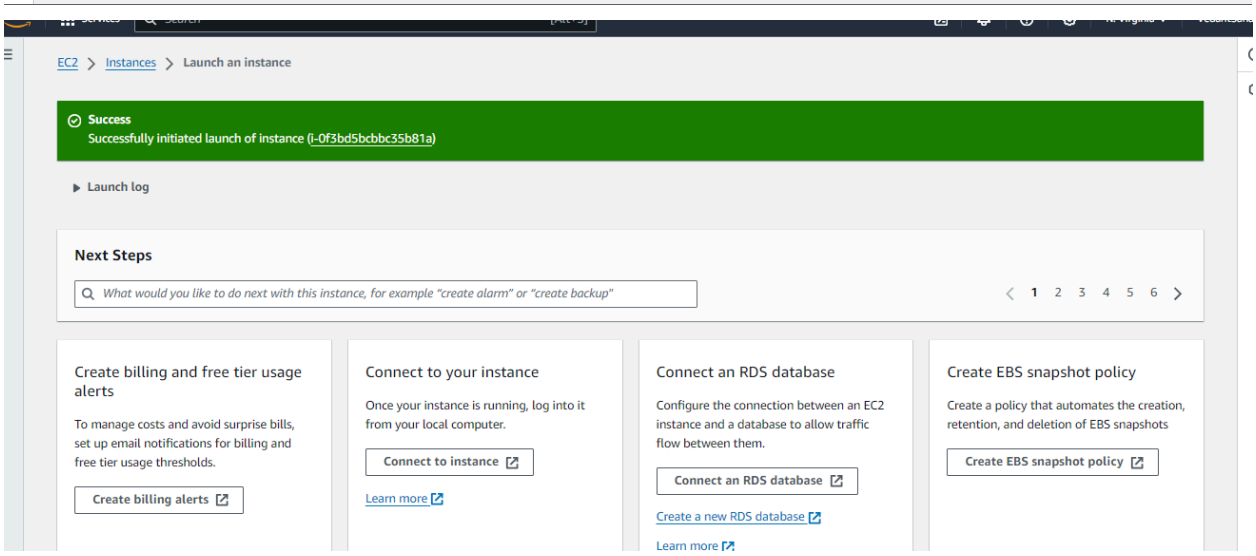
Experiment 01

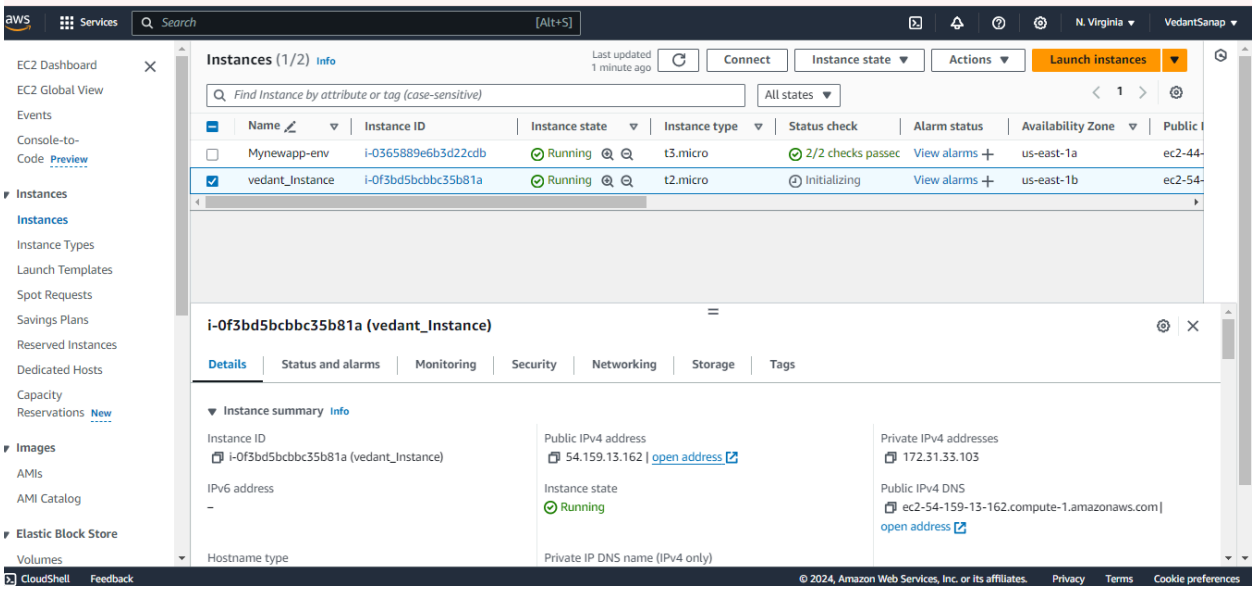
a) To develop a website and host it on your local machine on a VM

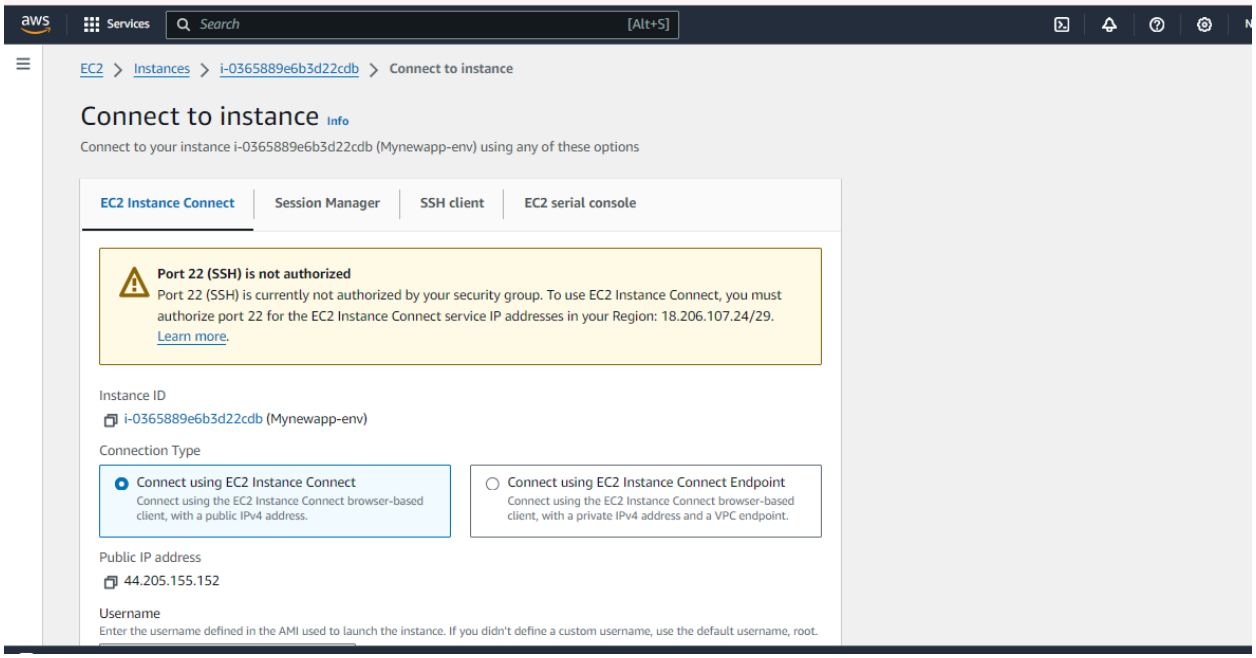





Configure storage Info
Advanced
1x 8 GiB gp3 Root volume (Not encrypted)
Free tier eligible customers can get up to 30 GB of EBS General Purpose (SSD) or Magnetic storage
Add new volume
The selected AMI contains more instance store volumes than the instance allows. Only the first 0 instance store volumes from the AMI will be accessible from the instance
Click refresh to view backup information
The tags that you assign determine whether the instance will be backed up by any Data Lifecycle Manager policies.
0 x File systems
Edit
Advanced details Info
Number of instances Info
1
Software Image (AMI)
Canonical, Ubuntu, 24.04 LTS, ...read more
ami-04a81a99f5ec58529
Virtual server type (instance type)
t2.micro
Firewall (security group)
New security group
Storage (volumes)
1 volume(s) - 8 GiB
Free tier: In your first year includes 750 hours of t2.micro (or t3.micro in the Regions in which
Cancel
Launch instance
Review commands


EC2 > Instances > Launch an instance
Success
Successfully initiated launch of instance (i-0f3bd5bcbbc35b81a)
Launch log
Next Steps
What would you like to do next with this instance, for example "create alarm" or "create backup"
1 2 3 4 5 6
Create billing and free tier usage alerts
To manage costs and avoid surprise bills, set up email notifications for billing and free tier usage thresholds.
Create billing alerts
Connect to your instance
Once your instance is running, log into it from your local computer.
Connect to instance
Learn more
Connect an RDS database
Configure the connection between an EC2 instance and a database to allow traffic flow between them.
Connect an RDS database
Create a new RDS database
Learn more
Create EBS snapshot policy
Create a policy that automates the creation, retention, and deletion of EBS snapshots
Create EBS snapshot policy


Services
Search
[Alt+S]
N. Virginia
VedantSanap
EC2 Dashboard
EC2 Global View
Events
Console-to-Code Preview
Instances
Instances
Instance Types
Launch Templates
Spot Requests
Savings Plans
Reserved Instances
Dedicated Hosts
Capacity Reservations New
Images
AMIs
AMI Catalog
Elastic Block Store
Volumes
Instances (1/2) Info
Last updated 1 minute ago
Connect
Instance state
Actions
Launch instances
Find Instance by attribute or tag (case-sensitive)
All states
Name
Instance ID
Instance state
Instance type
Status check
Alarm status
Availability Zone
Mynewapp-env
i-0365889e6b3d22cdb
Running
t3.micro
2/2 checks passec
View alarms
us-east-1a
vedant_Instance
i-0f3bd5bcbbc35b81a
Running
t2.micro
Initializing
View alarms
us-east-1b
i-0f3bd5bcbbc35b81a (vedant_Instance)
Details
Status and alarms
Monitoring
Security
Networking
Storage
Tags
Instance summary Info
Instance ID
i-0f3bd5bcbbc35b81a (vedant_Instance)
IPv6 address
–
Hostname type
Public IPv4 address
54.159.13.162 | open address
Instance state
Running
Private IP DNS name (IPv4 only)
Private IPv4 addresses
172.31.33.103
Public IPv4 DNS
ec2-54-159-13-162.compute-1.amazonaws.com|
open address
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

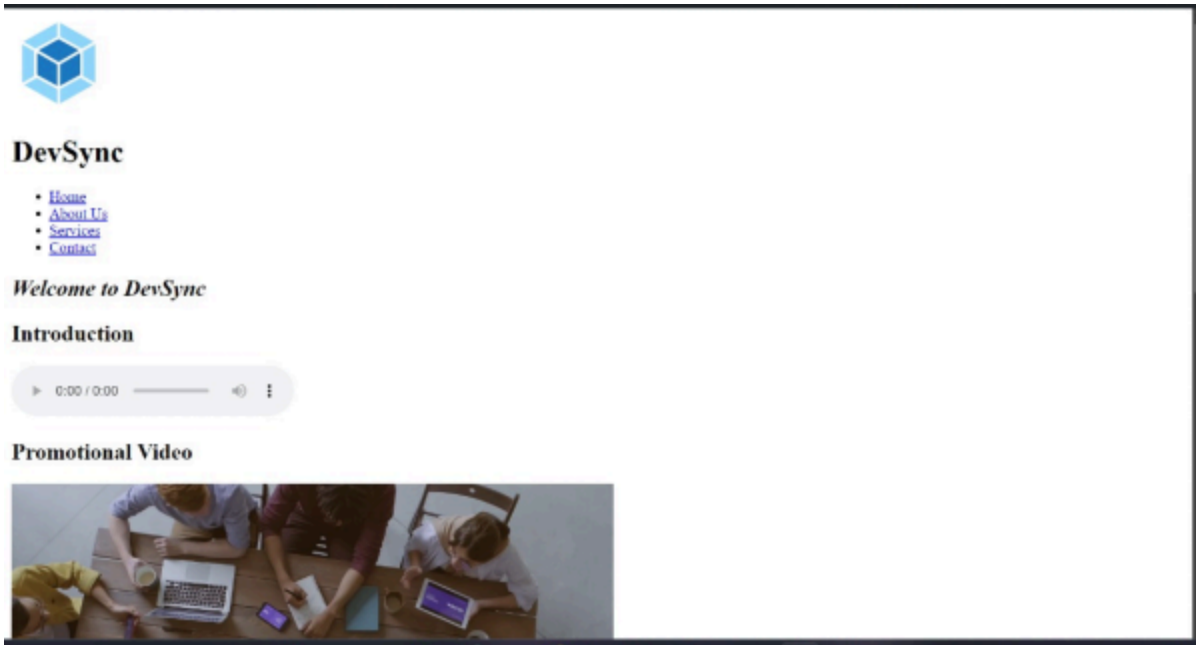



```
supra>ssh -i "supra-key.pem" ubuntu@3.110.164.61
Welcome to Ubuntu 24.04 LTS (GNU/Linux 6.8.0-1009-aws x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/pro

 System information as of Mon Aug  5 14:53:57 UTC 2024

  System load:  0.01              Processes:             105
  Usage of /:   22.7% of 6.71GB   Users logged in:       0
  Memory usage: 20%               IPv4 address for enX0: 172.31.6.34
  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-172-31-6-34:~$ sudo apt update && sudo apt upgrade -y
Hit:1 http://ap-south-1.ec2.archive.ubuntu.com/ubuntu noble InRelease
Get:2 http://ap-south-1.ec2.archive.ubuntu.com/ubuntu noble-updates InRelease [126 kB]
Get:3 http://ap-south-1.ec2.archive.ubuntu.com/ubuntu noble-backports InRelease [126 kB]
Get:4 http://ap-south-1.ec2.archive.ubuntu.com/ubuntu noble/universe amd64 Packages [15.0 MB]
Get:5 http://security.ubuntu.com/ubuntu noble-security InRelease [126 kB]
Get:6 http://ap-south-1.ec2.archive.ubuntu.com/ubuntu noble/universe Translation-en [5982 kB]
Get:7 http://ap-south-1.ec2.archive.ubuntu.com/ubuntu noble/universe amd64 Components [3871 kB]
Get:8 http://ap-south-1.ec2.archive.ubuntu.com/ubuntu noble/universe amd64 c-n-f Metadata [301 kB]
Get:9 http://ap-south-1.ec2.archive.ubuntu.com/ubuntu noble/multiverse amd64 Packages [269 kB]
Get:10 http://ap-south-1.ec2.archive.ubuntu.com/ubuntu noble/multiverse Translation-en [118 kB]
Get:11 http://ap-south-1.ec2.archive.ubuntu.com/ubuntu noble/multiverse amd64 Components [35.0 kB]
Get:12 http://ap-south-1.ec2.archive.ubuntu.com/ubuntu noble/multiverse amd64 c-n-f Metadata [8328 B]
Get:13 http://ap-south-1.ec2.archive.ubuntu.com/ubuntu noble-updates/main amd64 Packages [317 kB]
Get:14 http://ap-south-1.ec2.archive.ubuntu.com/ubuntu noble-updates/main Translation-en [82.7 kB]
Get:15 http://ap-south-1.ec2.archive.ubuntu.com/ubuntu noble-updates/main amd64 c-n-f Metadata [5640 B]
Get:16 http://ap-south-1.ec2.archive.ubuntu.com/ubuntu noble-updates/universe amd64 Packages [318 kB]
Get:17 http://ap-south-1.ec2.archive.ubuntu.com/ubuntu noble-updates/universe Translation-en [133 kB]
Get:18 http://ap-south-1.ec2.archive.ubuntu.com/ubuntu noble-updates/universe amd64 Components [45.0 kB]
Get:19 http://ap-south-1.ec2.archive.ubuntu.com/ubuntu noble-updates/universe amd64 c-n-f Metadata [12.5 kB]
Get:20 http://ap-south-1.ec2.archive.ubuntu.com/ubuntu noble-updates/restricted amd64 Packages [208 kB]
Get:21 http://ap-south-1.ec2.archive.ubuntu.com/ubuntu noble-updates/restricted Translation-en [40.7 kB]
Get:22 http://ap-south-1.ec2.archive.ubuntu.com/ubuntu noble-updates/restricted amd64 c-n-f Metadata [416 B]
Get:23 http://ap-south-1.ec2.archive.ubuntu.com/ubuntu noble-updates/multiverse amd64 Packages [14.1 kB]
Get:24 http://ap-south-1.ec2.archive.ubuntu.com/ubuntu noble-updates/multiverse Translation-en [3608 B]
Get:25 http://ap-south-1.ec2.archive.ubuntu.com/ubuntu noble-updates/multiverse amd64 Components [212 B]
Get:26 http://ap-south-1.ec2.archive.ubuntu.com/ubuntu noble-updates/multiverse amd64 c-n-f Metadata [532 B]
Get:27 http://ap-south-1.ec2.archive.ubuntu.com/ubuntu noble-backports/main amd64 Components [208 B]
Get:28 http://ap-south-1.ec2.archive.ubuntu.com/ubuntu noble-backports/main amd64 c-n-f Metadata [112 B]
Get:29 http://ap-south-1.ec2.archive.ubuntu.com/ubuntu noble-backports/universe amd64 Packages [10.3 kB]
Get:30 http://ap-south-1.ec2.archive.ubuntu.com/ubuntu noble-backports/universe Translation-en [10.5 kB]
Get:31 http://ap-south-1.ec2.archive.ubuntu.com/ubuntu noble-backports/universe amd64 Components [17.6 kB]
Get:32 http://ap-south-1.ec2.archive.ubuntu.com/ubuntu noble-backports/universe amd64 c-n-f Metadata [1016 B]
Get:33 http://ap-south-1.ec2.archive.ubuntu.com/ubuntu noble-backports/restricted amd64 Components [216 B]
Get:34 http://ap-south-1.ec2.archive.ubuntu.com/ubuntu noble-backports/restricted amd64 c-n-f Metadata [116 B]
```

```
No VM guests are running outdated hypervisor (qemu) binaries on this host.
ubuntu@ip-172-31-6-34:~$ sudo apt install apache2 -y
Reading package lists... Done
Building dependency tree... Done
Enabling module auth_basic.
Enabling module access_compat.
Enabling module authn_file.
Enabling module authz_user.
Enabling module alias.
Enabling module dir.
Enabling module autoindex.
Enabling module env.
Enabling module mime.
Enabling module negotiation.
Enabling module setenvif.
Enabling module filter.
Enabling module deflate.
Enabling module status.
Enabling module reqtimeout.
Enabling conf charset.
Enabling conf localized-error-pages.
Enabling conf other-vhosts-access-log.
Enabling conf security.
Enabling conf serve-cgi-bin.
Enabling site 000-default.
Created symlink /etc/systemd/system/multi-user.target.wants/apache2.service → /usr/lib/systemd/system/apache2.service.
Created symlink /etc/systemd/system/multi-user.target.wants/apache-htcacheclean.service → /usr/lib/systemd/system/apache-htcacheclean
.service.
Processing triggers for ufw (0.36.2-6) ...
Processing triggers for man-db (2.12.0-4build2) ...
Processing triggers for libc-bin (2.39-0ubuntu8.2) ...
Scanning processes...
Scanning candidates...
Scanning linux images...

Pending kernel upgrade!
```

```
*** System restart required ***
Last login: Mon Aug  5 14:53:58 2024 from 152.58.43.204
ubuntu@ip-172-31-6-34:~$ sudo mv /home/ubuntu/index.html /var/www/html/
ubuntu@ip-172-31-6-34:~$ sudo chown -R www-data:www-data /var/www/html
ubuntu@ip-172-31-6-34:~$ sudo nano /etc/apache2/sites-available/000-default.conf
ubuntu@ip-172-31-6-34:~$ sudo a2ensite 000-default.conf
Site 000-default already enabled
ubuntu@ip-172-31-6-34:~$ sudo systemctl restart apache2
ubuntu@ip-172-31-6-34:~$ sudo apt install certbot python3-certbot-apache
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
  augeas-lenses libaugeas0 python3-acme python3-augeas
  python3-certbot python3-configargparse python3-icu
  python3-josepy python3-parsedatetime python3-rfc3339
Suggested packages:
  augeas-doc python-certbot-doc python3-certbot-nginx
  augeas-tools python-acme-doc python-certbot-apache-doc
The following NEW packages will be installed:
  augeas-lenses certbot libaugeas0 python3-acme python3-augeas
  python3-certbot python3-certbot-apache
..
Unpacking python3-parsedatetime (2.6-3) ...
Selecting previously unselected package python3-certbot.
Preparing to unpack .../08-python3-certbot_2.9.0-1_all.deb ...
Unpacking python3-certbot (2.9.0-1) ...
Selecting previously unselected package certbot.
Preparing to unpack .../09-certbot_2.9.0-1_all.deb ...
Unpacking certbot (2.9.0-1) ...
Selecting previously unselected package python3-certbot-apache.
Preparing to unpack .../10-python3-certbot-apache_2.9.0-1_all.deb ...
Unpacking python3-certbot-apache (2.9.0-1) ...
Selecting previously unselected package python3-icu.
Preparing to unpack .../11-python3-icu_2.12-1build2_amd64.deb ...
Unpacking python3-icu (2.12-1build2) ...
```

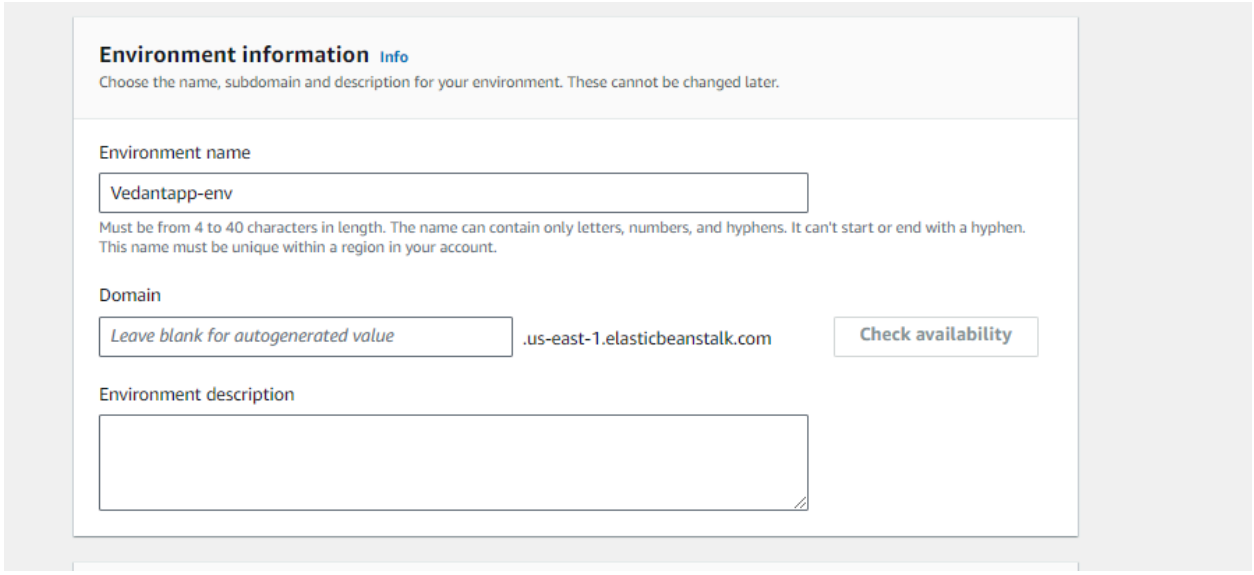


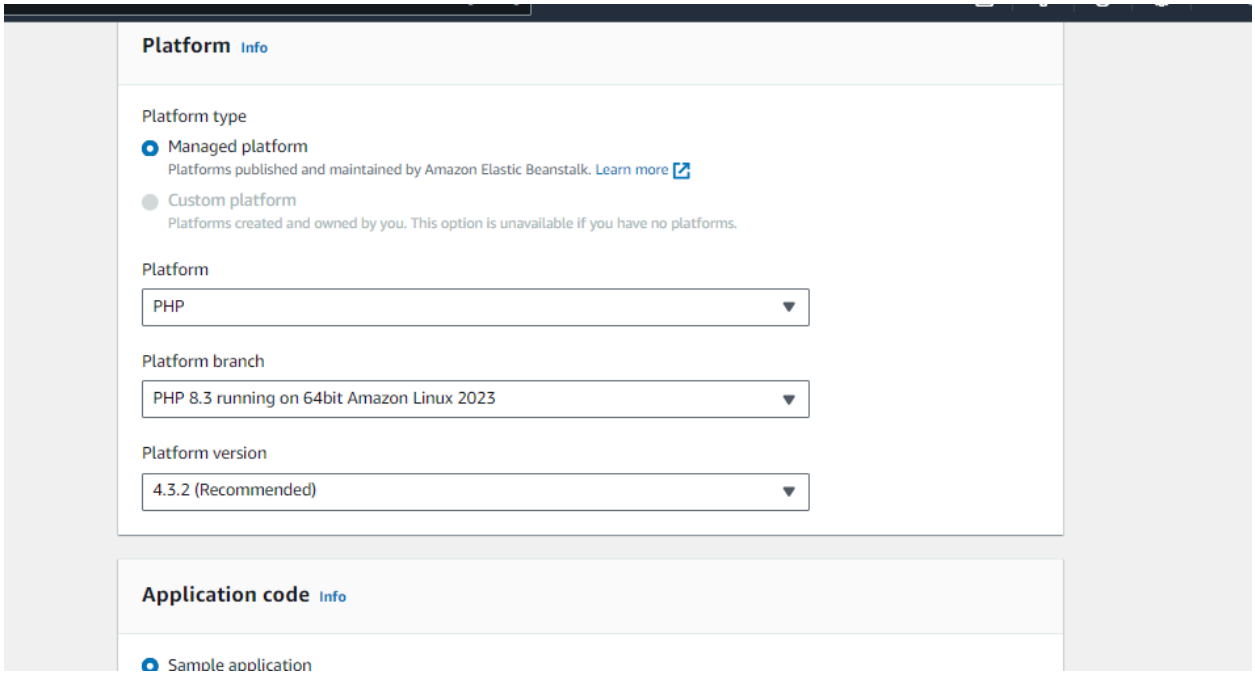
Vedant Sanap
D15A 48

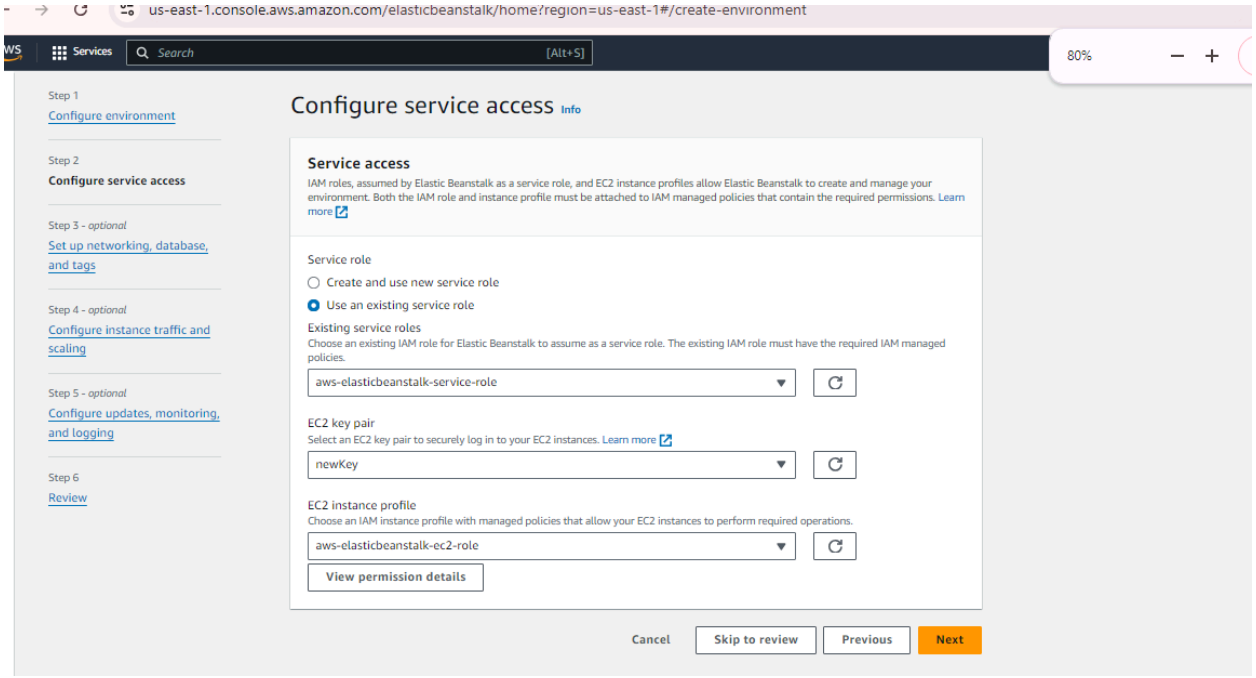
ADVANCE DEVOPS EXP-2

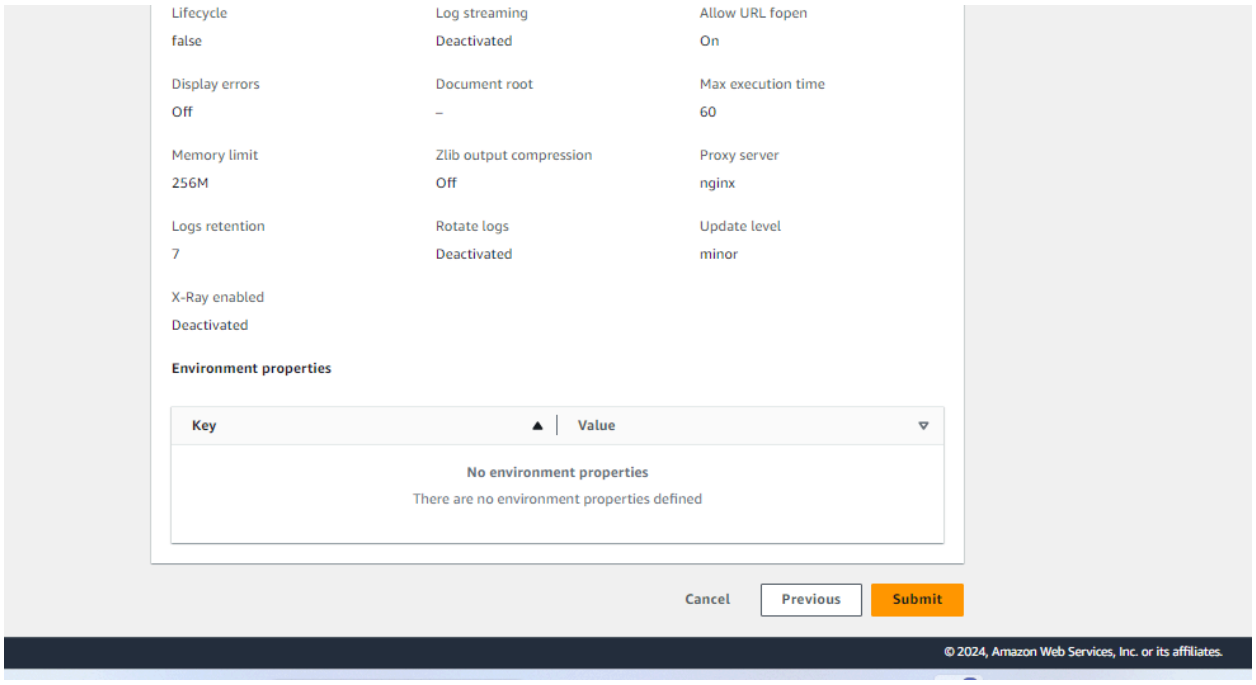
Aim: To build your application using AWS Codebuild and deploy on S3 using AWS CodePipeline deploy sample application on EC2 instance using AWS codedeploy. Code and Output : Using

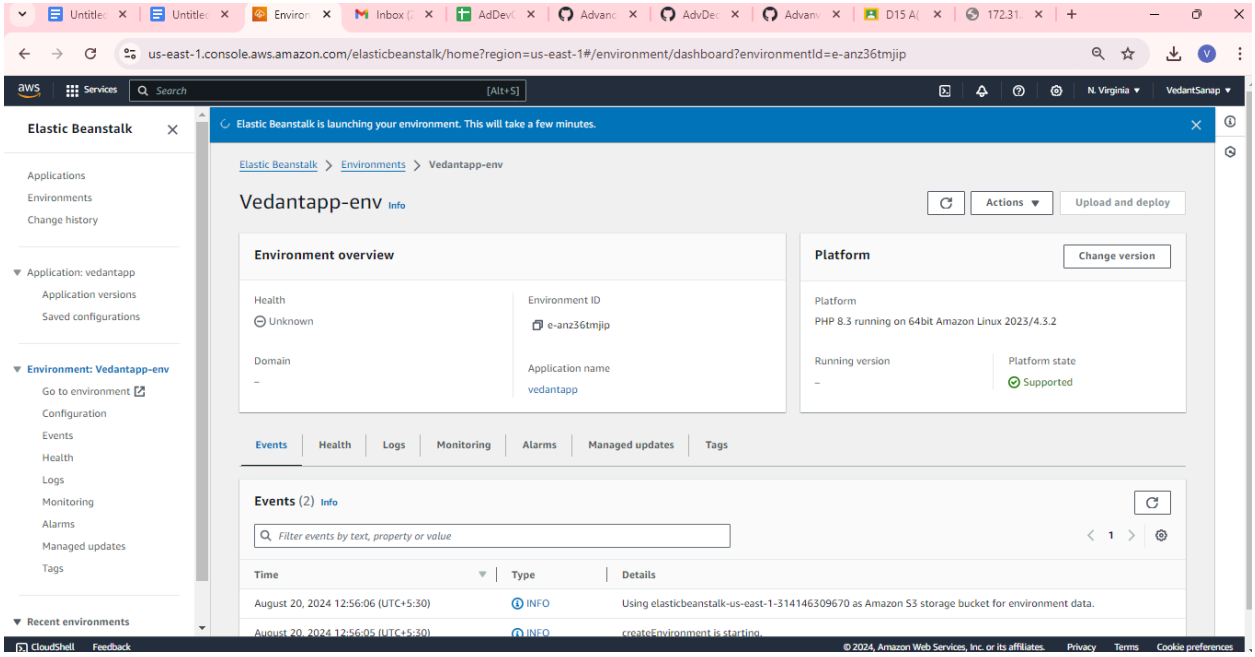
Elastic Beanstalk:

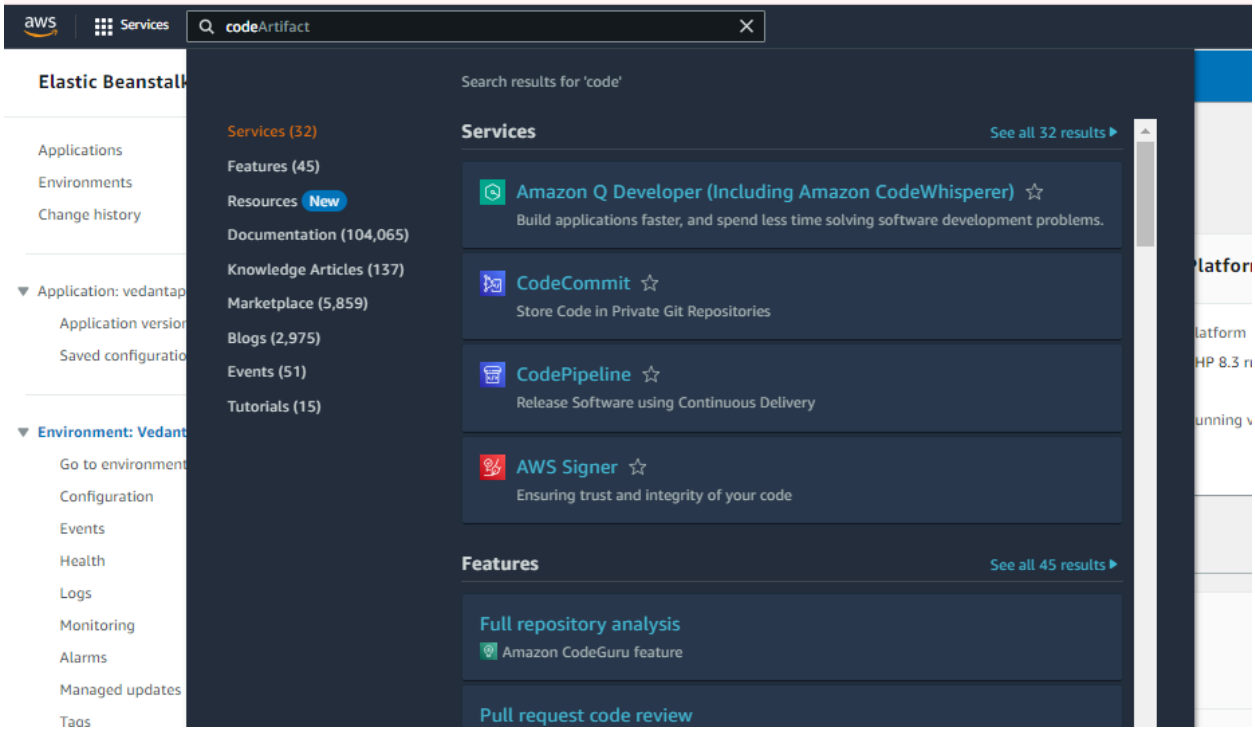


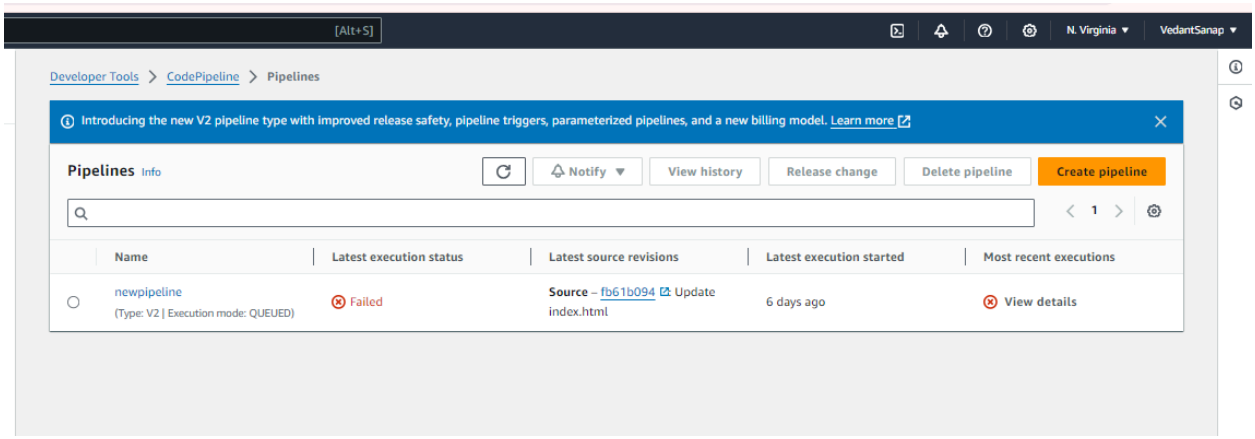


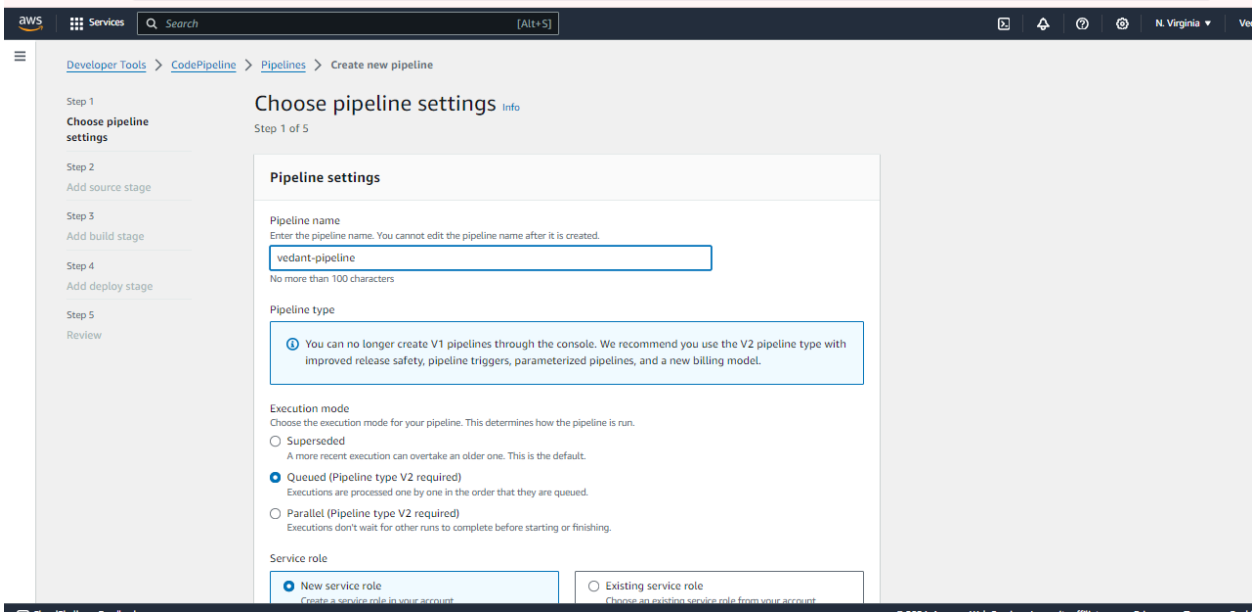

us-east-1.console.aws.amazon.com/elasticbeanstalk/home?region=us-east-1#/create-environment
Services
Search
[Alt+S]
80%
Step 1
Configure environment
Step 2
Configure service access
Step 3 - optional
Set up networking, database, and tags
Step 4 - optional
Configure instance traffic and scaling
Step 5 - optional
Configure updates, monitoring, and logging
Step 6
Review
Configure service access Info
Service access
IAM roles, assumed by Elastic Beanstalk as a service role, and EC2 instance profiles allow Elastic Beanstalk to create and manage your environment. Both the IAM role and instance profile must be attached to IAM managed policies that contain the required permissions. Learn more
Service role
Create and use new service role
Use an existing service role
Existing service roles
Choose an existing IAM role for Elastic Beanstalk to assume as a service role. The existing IAM role must have the required IAM managed policies.
aws-elasticbeanstalk-service-role
EC2 key pair
Select an EC2 key pair to securely log in to your EC2 instances. Learn more
newKey
EC2 instance profile
Choose an IAM instance profile with managed policies that allow your EC2 instances to perform required operations.
aws-elasticbeanstalk-ec2-role
View permission details
Cancel
Skip to review
Previous
Next

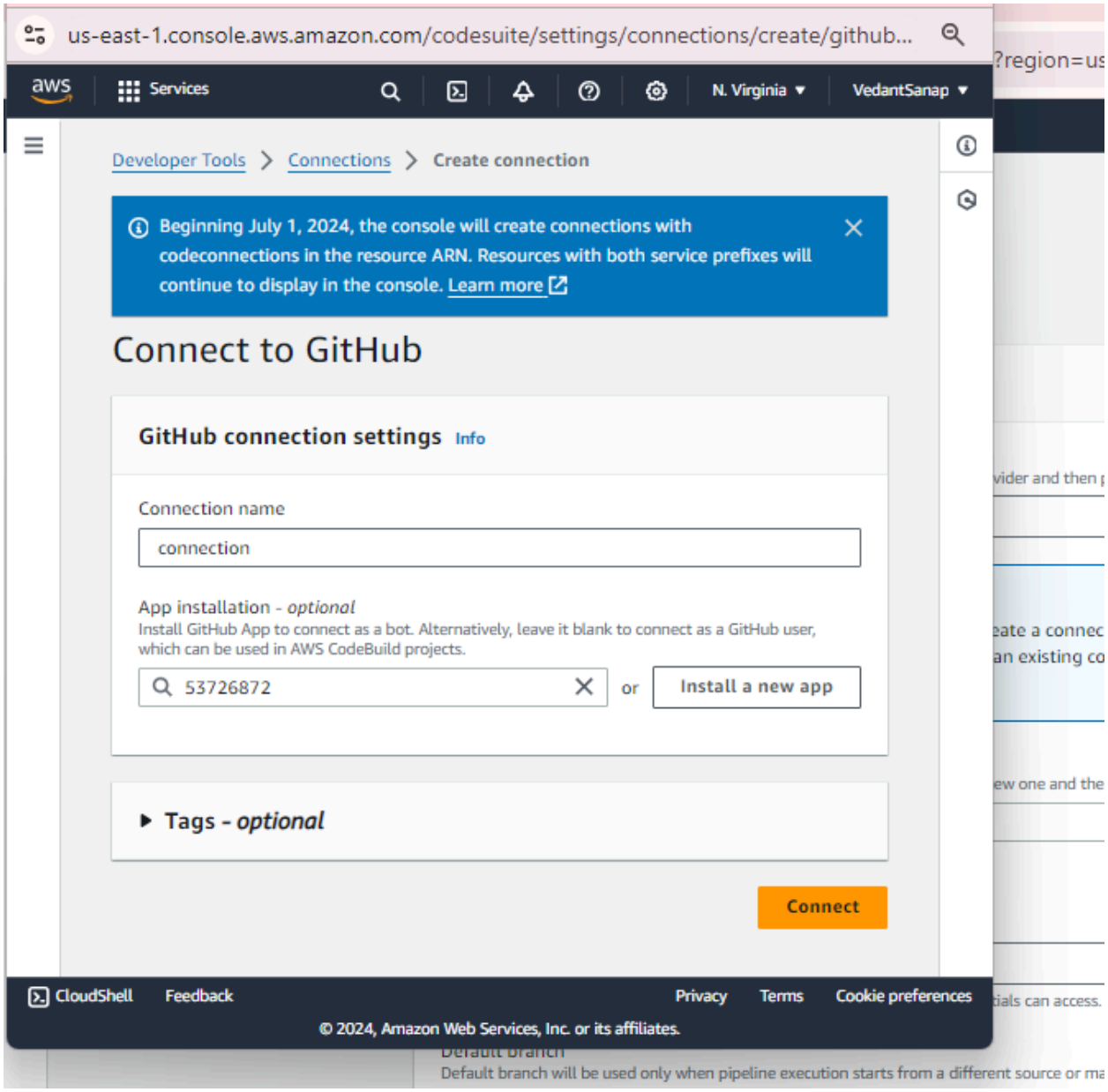

Lifecycle
false
Log streaming
Deactivated
Allow URL fopen
On
Display errors
Off
Document root
–
Max execution time
60
Memory limit
256M
Zlib output compression
Off
Proxy server
nginx
Logs retention
7
Rotate logs
Deactivated
Update level
minor
X-Ray enabled
Deactivated
Environment properties
Key
Value
No environment properties
There are no environment properties defined
Cancel
Previous
Submit
© 2024, Amazon Web Services, Inc. or its affiliates.

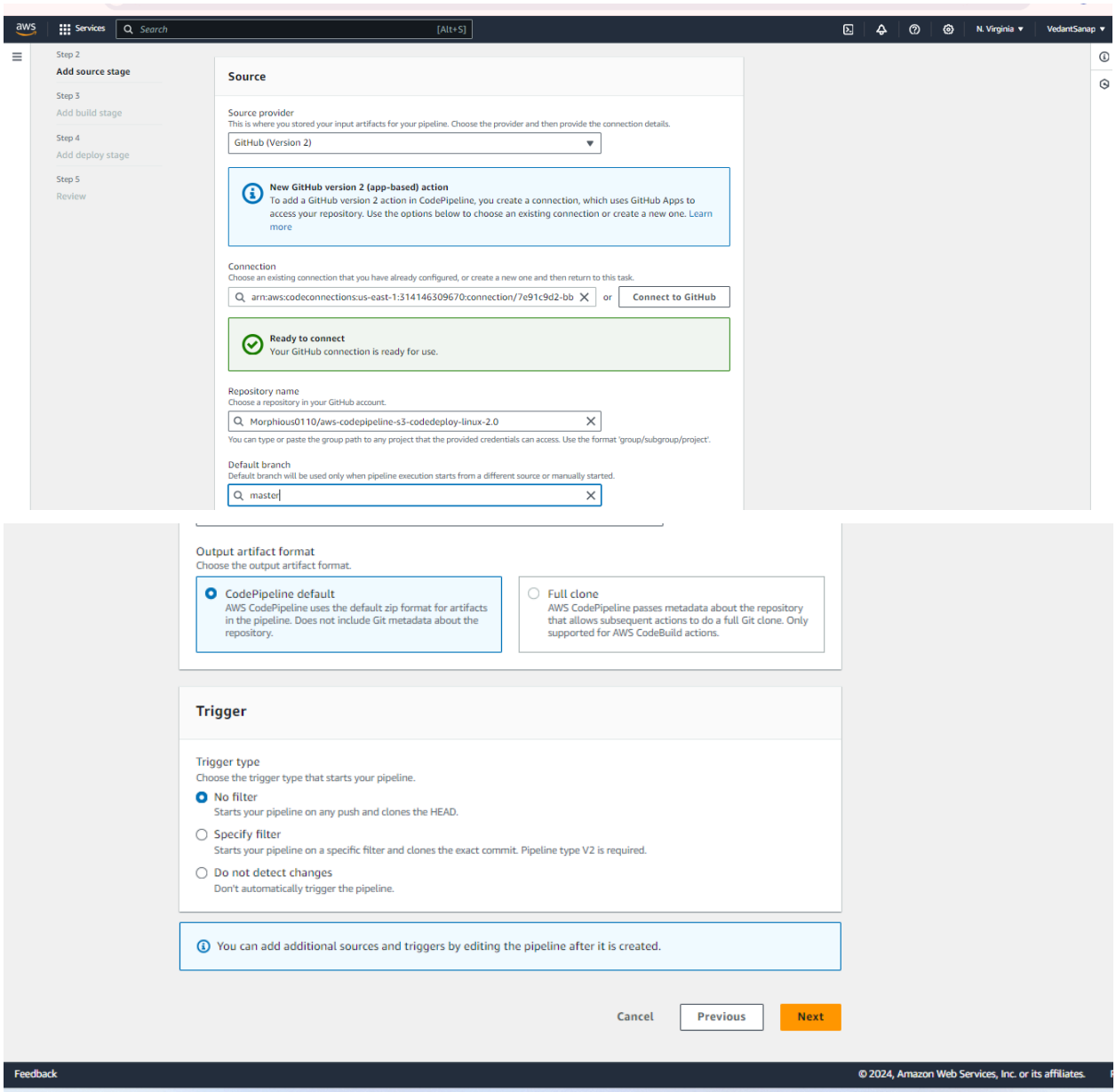

us-east-1.console.aws.amazon.com/elasticbeanstalk/home?region=us-east-1#/environment/dashboard?environmentId=e-anz36tmjip
Elastic Beanstalk is launching your environment. This will take a few minutes.
Elastic Beanstalk > Environments > Vedantapp-env
Vedantapp-env Info
Actions
Upload and deploy
Environment overview
Health
Unknown
Environment ID
e-anz36tmjip
Domain
Application name
vedantapp
Platform
Change version
Platform
PHP 8.3 running on 64bit Amazon Linux 2023/4.3.2
Running version
Platform state
Supported
Events
Health
Logs
Monitoring
Alarms
Managed updates
Tags
Events (2) Info
Filter events by text, property or value
Time
Type
Details
August 20, 2024 12:56:06 (UTC+5:30)
INFO
Using elasticbeanstalk-us-east-1-314146309670 as Amazon S3 storage bucket for environment data.
August 20, 2024 12:56:05 (UTC+5:30)
INFO
createEnvironment is starting.
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

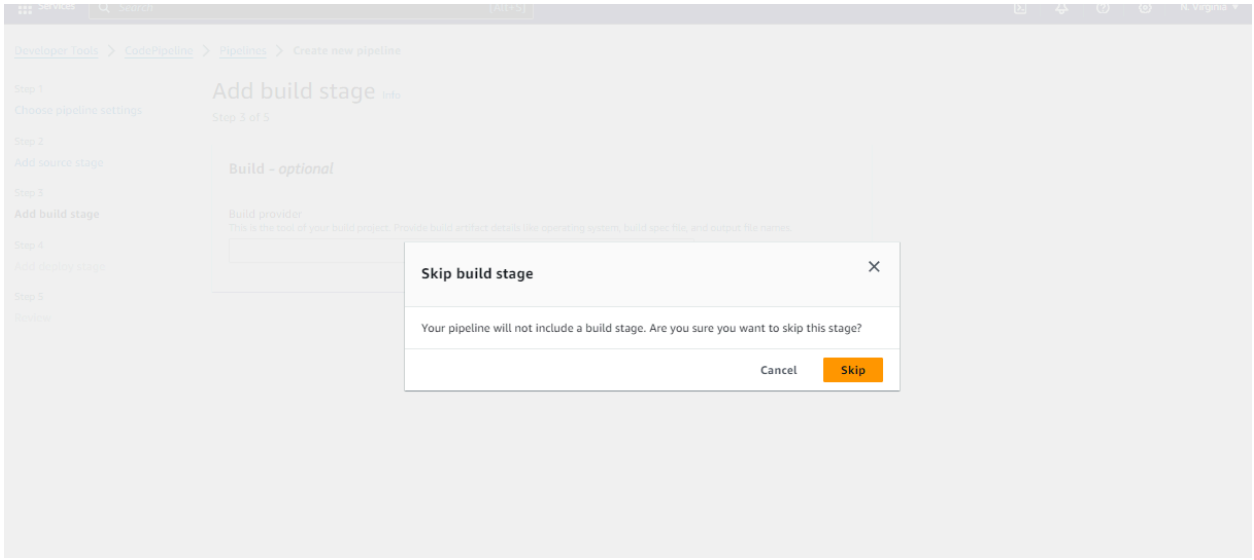

codeArtifact
Search results for 'code'
Services (32)
Features (45)
Resources New
Documentation (104,065)
Knowledge Articles (137)
Marketplace (5,859)
Blogs (2,975)
Events (51)
Tutorials (15)
Services
See all 32 results
Amazon Q Developer (Including Amazon CodeWhisperer)
Build applications faster, and spend less time solving software development problems.
CodeCommit
Store Code in Private Git Repositories
CodePipeline
Release Software using Continuous Delivery
AWS Signer
Ensuring trust and integrity of your code
Features
See all 45 results
Full repository analysis
Amazon CodeGuru feature
Pull request code review

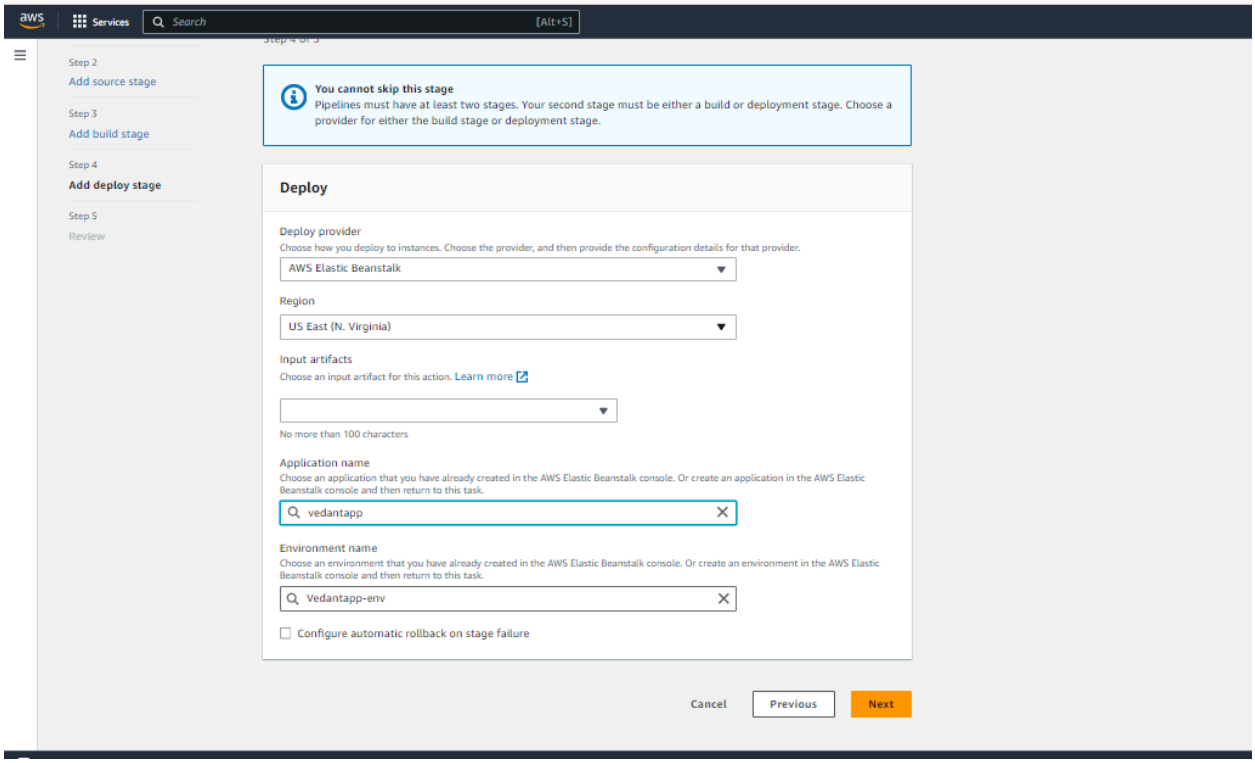

[Alt+S]
N. Virginia
VedantSanap
Developer Tools > CodePipeline > Pipelines
Introducing the new V2 pipeline type with improved release safety, pipeline triggers, parameterized pipelines, and a new billing model. Learn more
Pipelines Info
Notify
View history
Release change
Delete pipeline
Create pipeline
Name
Latest execution status
Latest source revisions
Latest execution started
Most recent executions
newpipeline
(Type: V2 | Execution mode: QUEUED)
Failed
Source – fb61b094 Update index.html
6 days ago
View details

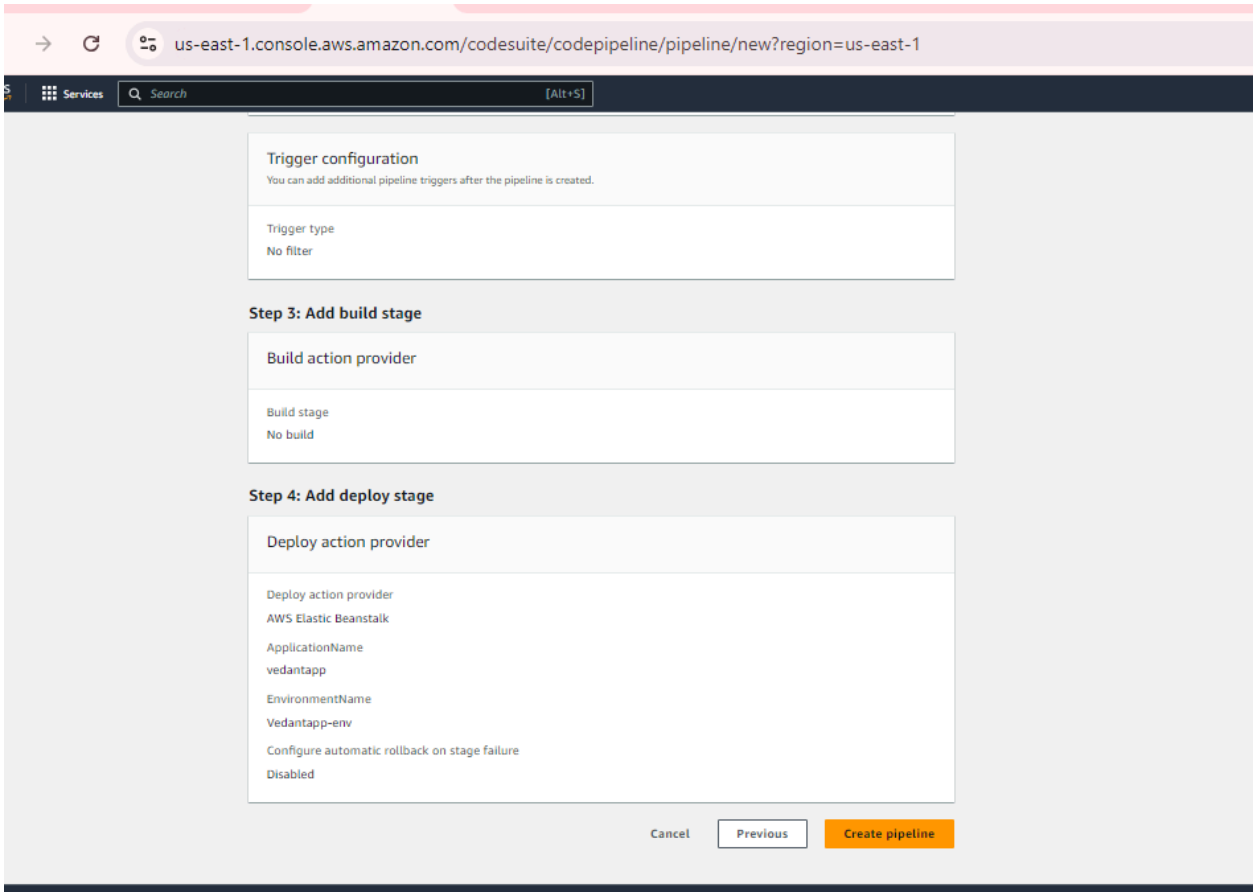

aws
Services
Search
[Alt+S]
N. Virginia
Developer Tools > CodePipeline > Pipelines > Create new pipeline
Step 1
Choose pipeline settings
Step 2
Add source stage
Step 3
Add build stage
Step 4
Add deploy stage
Step 5
Review
Choose pipeline settings Info
Step 1 of 5
Pipeline settings
Pipeline name
Enter the pipeline name. You cannot edit the pipeline name after it is created.
vedant-pipeline
No more than 100 characters
Pipeline type
You can no longer create V1 pipelines through the console. We recommend you use the V2 pipeline type with improved release safety, pipeline triggers, parameterized pipelines, and a new billing model.
Execution mode
Choose the execution mode for your pipeline. This determines how the pipeline is run.
Superseded
A more recent execution can overtake an older one. This is the default.
Queued (Pipeline type V2 required)
Executions are processed one by one in the order that they are queued.
Parallel (Pipeline type V2 required)
Executions don't wait for other runs to complete before starting or finishing.
Service role
New service role
Existing service role

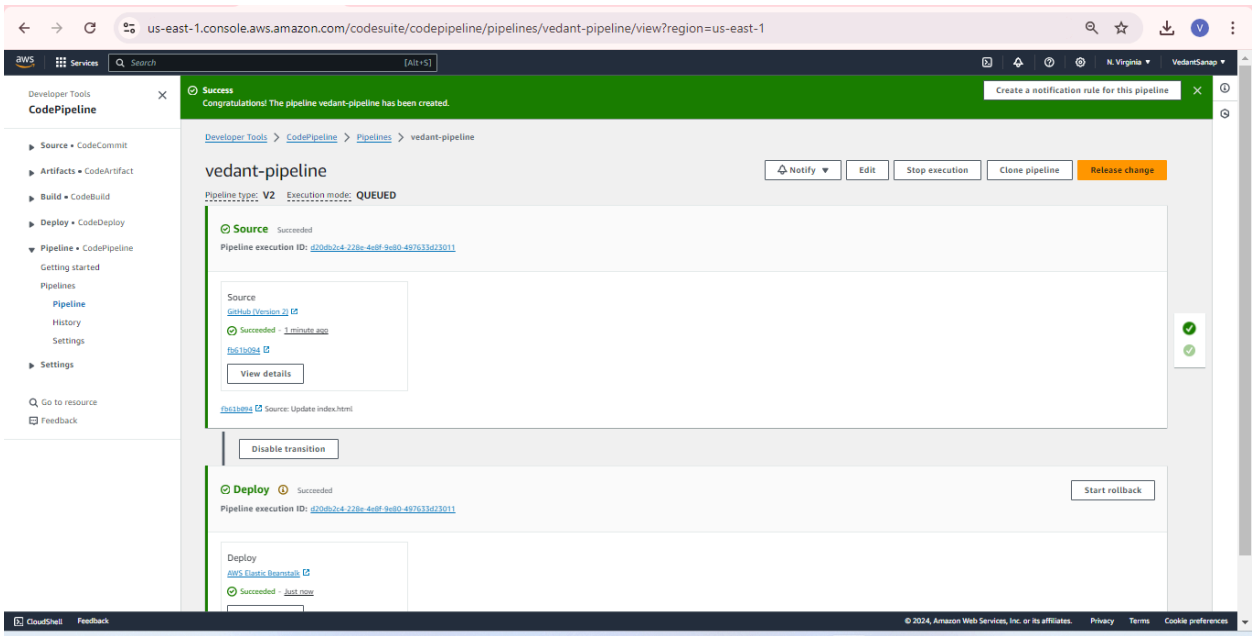

us-east-1.console.aws.amazon.com/codesuite/settings/connections/create/github...
aws
Services
N. Virginia
VedantSanap
Developer Tools
Connections
Create connection
Beginning July 1, 2024, the console will create connections with codeconnections in the resource ARN. Resources with both service prefixes will continue to display in the console. Learn more
Connect to GitHub
GitHub connection settings Info
Connection name
connection
App installation - optional
Install GitHub App to connect as a bot. Alternatively, leave it blank to connect as a GitHub user, which can be used in AWS CodeBuild projects.
53726872
or
Install a new app
Tags - optional
Connect
CloudShell
Feedback
Privacy
Terms
Cookie preferences
© 2024, Amazon Web Services, Inc. or its affiliates.

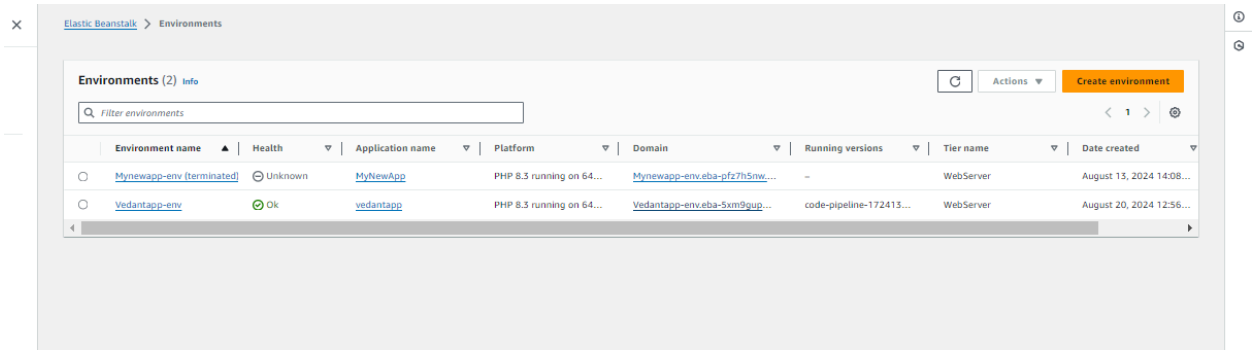

aws
Services
Search
[Alt+S]
N. Virginia
VedantSanap
Step 2
Add source stage
Step 3
Add build stage
Step 4
Add deploy stage
Step 5
Review
Source
Source provider
This is where you stored your input artifacts for your pipeline. Choose the provider and then provide the connection details.
GitHub (Version 2)
New GitHub version 2 (app-based) action
To add a GitHub version 2 action in CodePipeline, you create a connection, which uses GitHub Apps to access your repository. Use the options below to choose an existing connection or create a new one. Learn more
Connection
Choose an existing connection that you have already configured, or create a new one and then return to this task.
arn:aws:codeconnections:us-east-1:314146309670:connection/7e91c9d2-bb
or
Connect to GitHub
Ready to connect
Your GitHub connection is ready for use.
Repository name
Choose a repository in your GitHub account.
Morphious0110/aws-codepipeline-s3-codedeploy-linux-2.0
You can type or paste the group path to any project that the provided credentials can access. Use the format 'group/subgroup/project'.
Default branch
Default branch will be used only when pipeline execution starts from a different source or manually started.
master
Output artifact format
Choose the output artifact format.
CodePipeline default
AWS CodePipeline uses the default zip format for artifacts in the pipeline. Does not include Git metadata about the repository.
Full clone
AWS CodePipeline passes metadata about the repository that allows subsequent actions to do a full Git clone. Only supported for AWS CodeBuild actions.
Trigger
Trigger type
Choose the trigger type that starts your pipeline.
No filter
Starts your pipeline on any push and clones the HEAD.
Specify filter
Starts your pipeline on a specific filter and clones the exact commit. Pipeline type V2 is required.
Do not detect changes
Don't automatically trigger the pipeline.
You can add additional sources and triggers by editing the pipeline after it is created.
Cancel
Previous
Next
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.

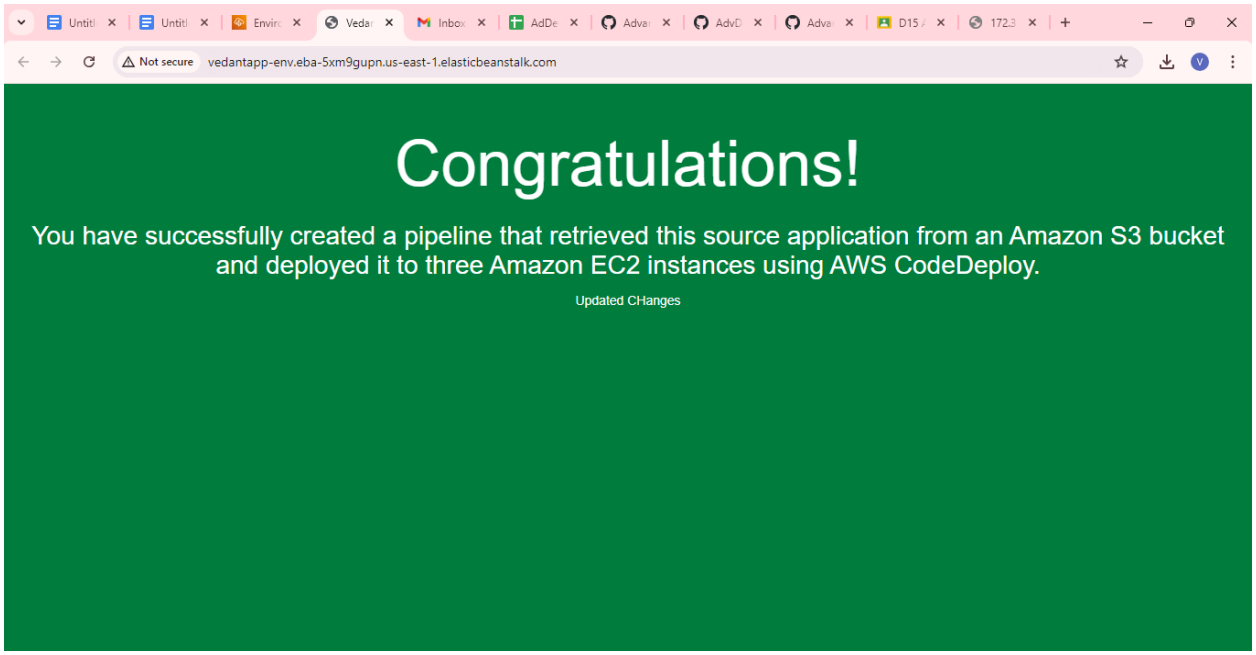

Skip build stage
Your pipeline will not include a build stage. Are you sure you want to skip this stage?
Cancel
Skip


aws
Services
Search
[Alt+S]
Step 2
Add source stage
Step 3
Add build stage
Step 4
Add deploy stage
Step 5
Review
You cannot skip this stage
Pipelines must have at least two stages. Your second stage must be either a build or deployment stage. Choose a provider for either the build stage or deployment stage.
Deploy
Deploy provider
Choose how you deploy to instances. Choose the provider, and then provide the configuration details for that provider.
AWS Elastic Beanstalk
Region
US East (N. Virginia)
Input artifacts
Choose an input artifact for this action. Learn more
No more than 100 characters
Application name
Choose an application that you have already created in the AWS Elastic Beanstalk console. Or create an application in the AWS Elastic Beanstalk console and then return to this task.
vedantapp
Environment name
Choose an environment that you have already created in the AWS Elastic Beanstalk console. Or create an environment in the AWS Elastic Beanstalk console and then return to this task.
Vedantapp-env
Configure automatic rollback on stage failure
Cancel
Previous
Next

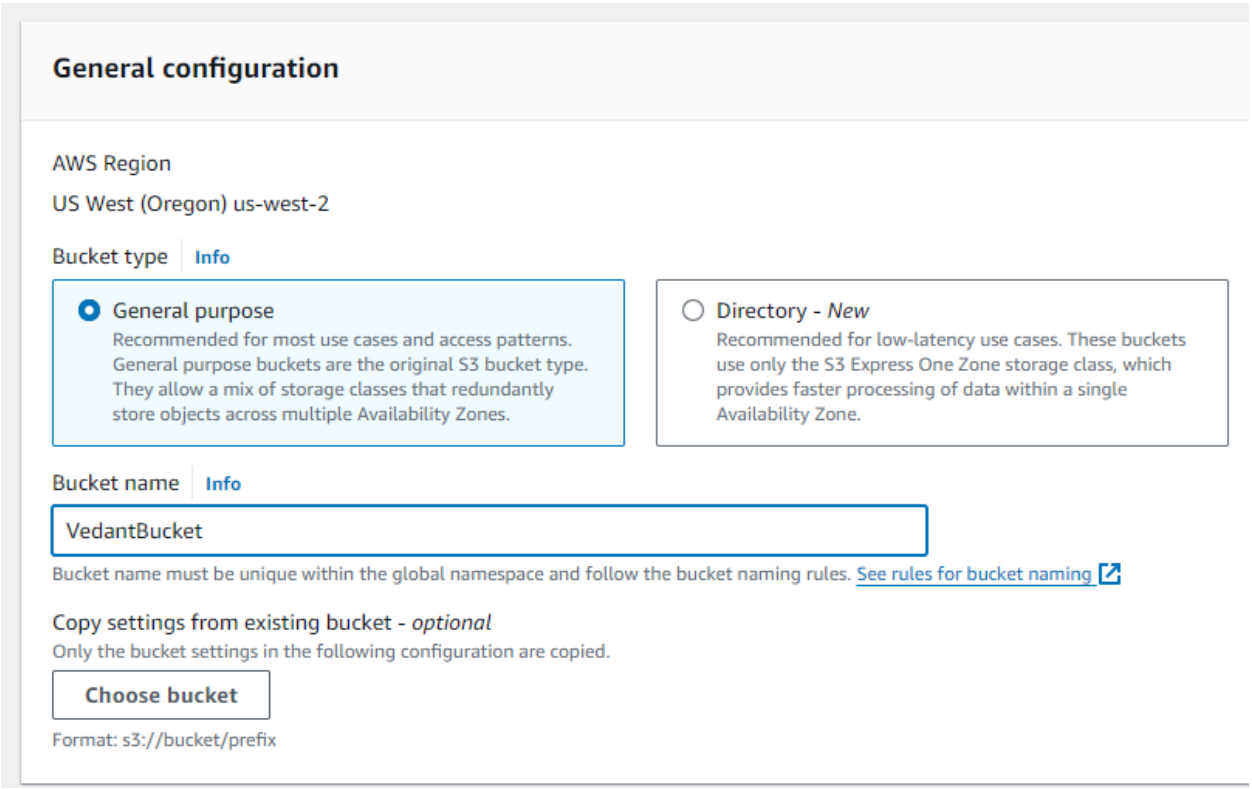

us-east-1.console.aws.amazon.com/codesuite/codepipeline/pipeline/new?region=us-east-1
Services
Search
[Alt+S]
Trigger configuration
You can add additional pipeline triggers after the pipeline is created.
Trigger type
No filter
Step 3: Add build stage
Build action provider
Build stage
No build
Step 4: Add deploy stage
Deploy action provider
Deploy action provider
AWS Elastic Beanstalk
ApplicationName
vedantapp
EnvironmentName
Vedantapp-env
Configure automatic rollback on stage failure
Disabled
Cancel
Previous
Create pipeline

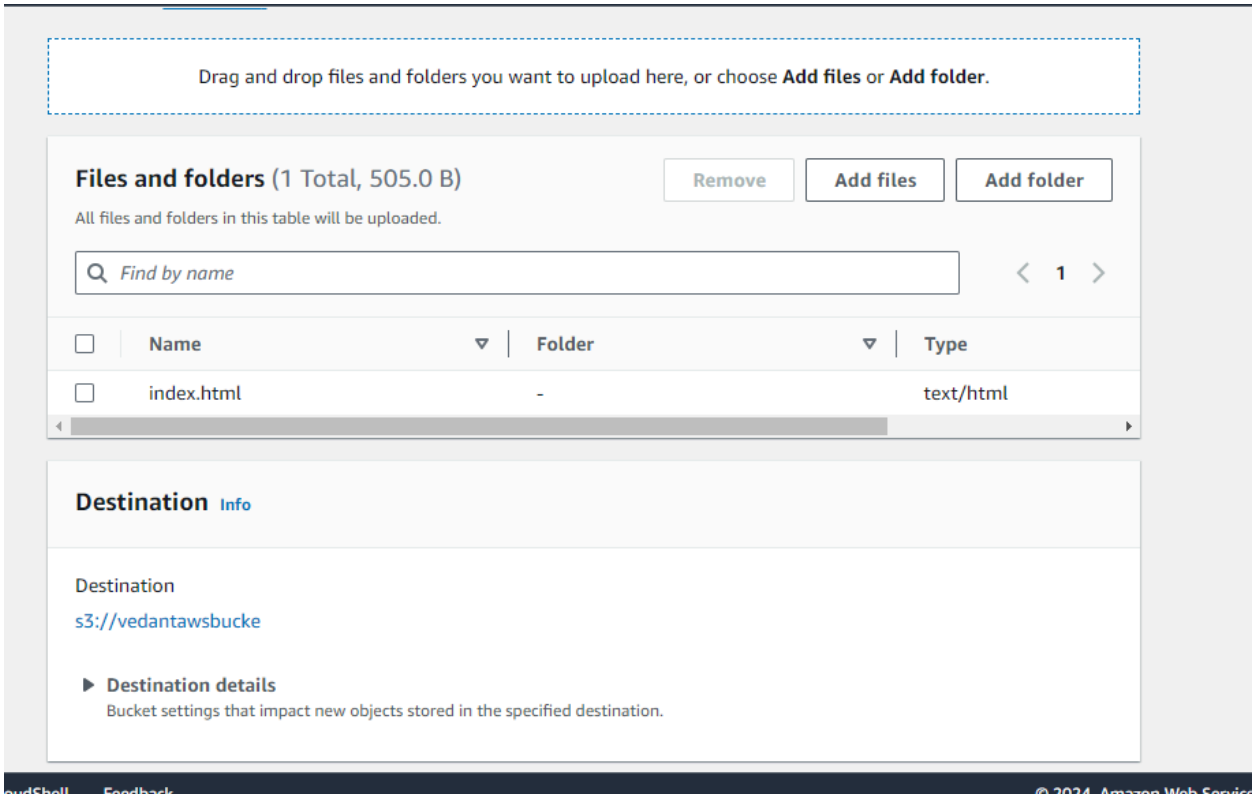

us-east-1.console.aws.amazon.com/codesuite/codepipeline/pipelines/vedant-pipeline/view?region=us-east-1
Developer Tools
CodePipeline
Success
Congratulations! The pipeline vedant-pipeline has been created.
Create a notification rule for this pipeline
Developer Tools > CodePipeline > Pipelines > vedant-pipeline
vedant-pipeline
Notify
Edit
Stop execution
Clone pipeline
Release change
Pipeline type: V2
Execution mode: QUEUED
Source
Succeeded
Pipeline execution ID: d20db2c4-228e-4e8f-9e80-497633d23011
View details
Disable transition
Deploy
Succeeded
Start rollback
Pipeline execution ID: d20db2c4-228e-4e8f-9e80-497633d23011
AWS Elastic Beanstalk
Succeeded - Just now
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

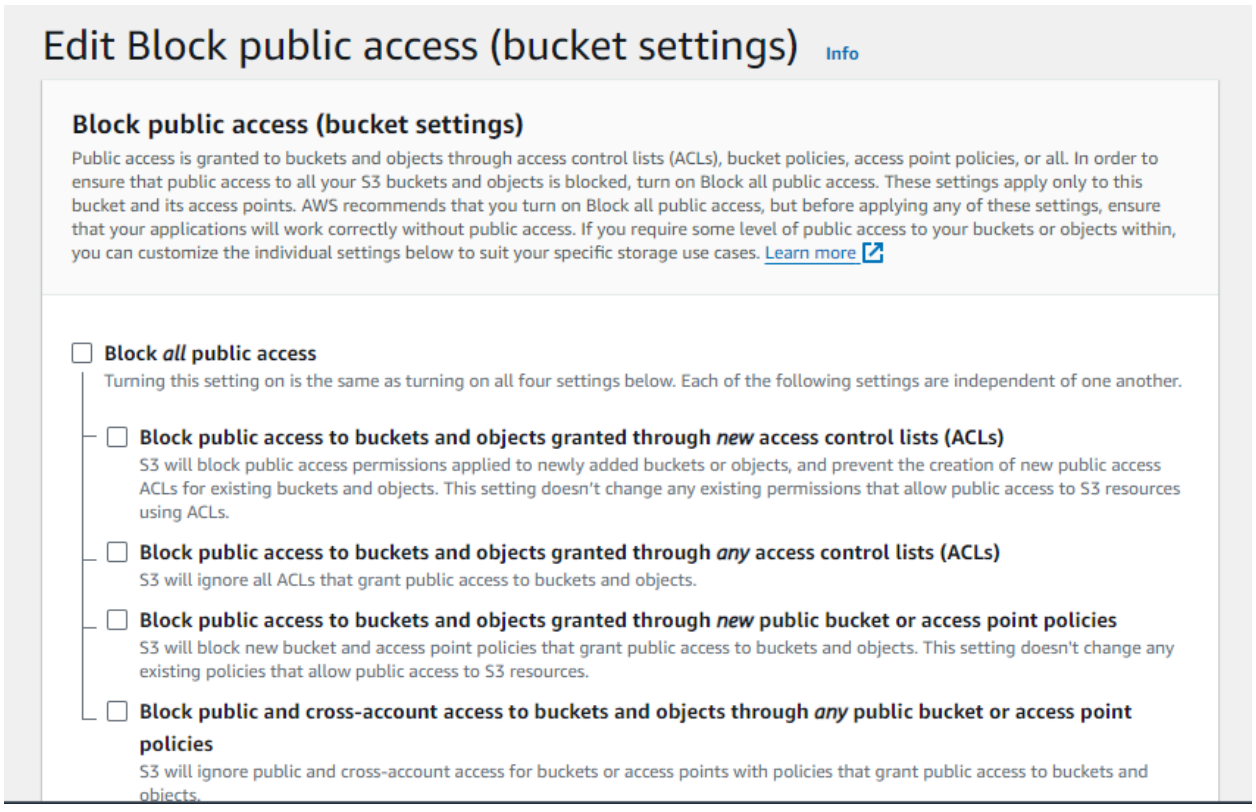

Elastic Beanstalk > Environments
Environments (2) Info
Actions
Create environment
Filter environments
Environment name
Health
Application name
Platform
Domain
Running versions
Tier name
Date created
Mynewapp-env (terminated)
Unknown
MyNewApp
PHP 8.3 running on 64...
Mynewapp-env.eba-pfz7h5nw....
–
WebServer
August 13, 2024 14:08...
Vedantapp-env
Ok
vedantapp
PHP 8.3 running on 64...
Vedantapp-env.eba-5xm9gup...
code-pipeline-172413...
WebServer
August 20, 2024 12:56...

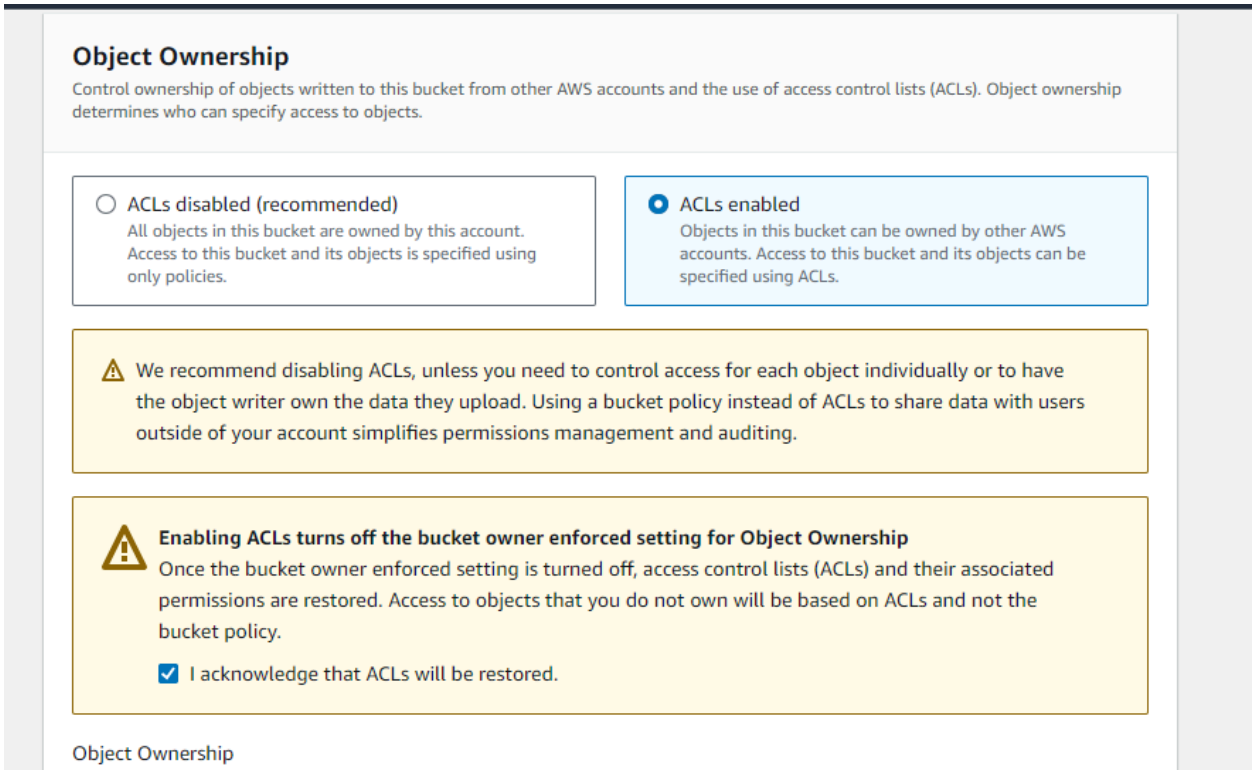

Not secure
vedantapp-env.eba-5xm9gupn.us-east-1.elasticbeanstalk.com
Congratulations!
You have successfully created a pipeline that retrieved this source application from an Amazon S3 bucket and deployed it to three Amazon EC2 instances using AWS CodeDeploy.
Updated CHanges

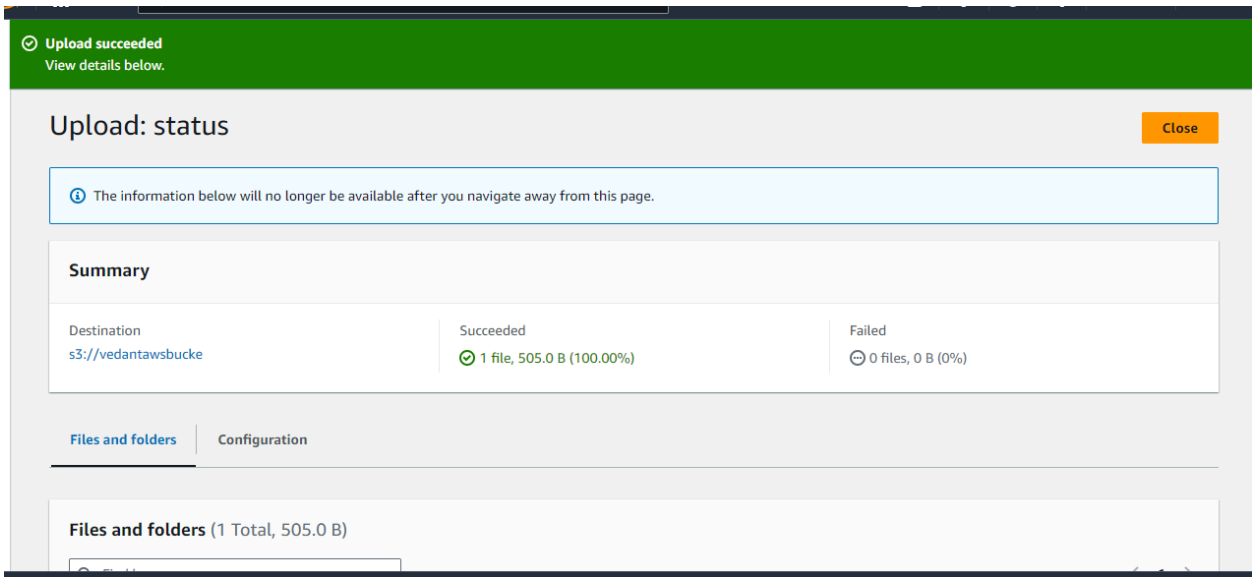
S3 Bucket :

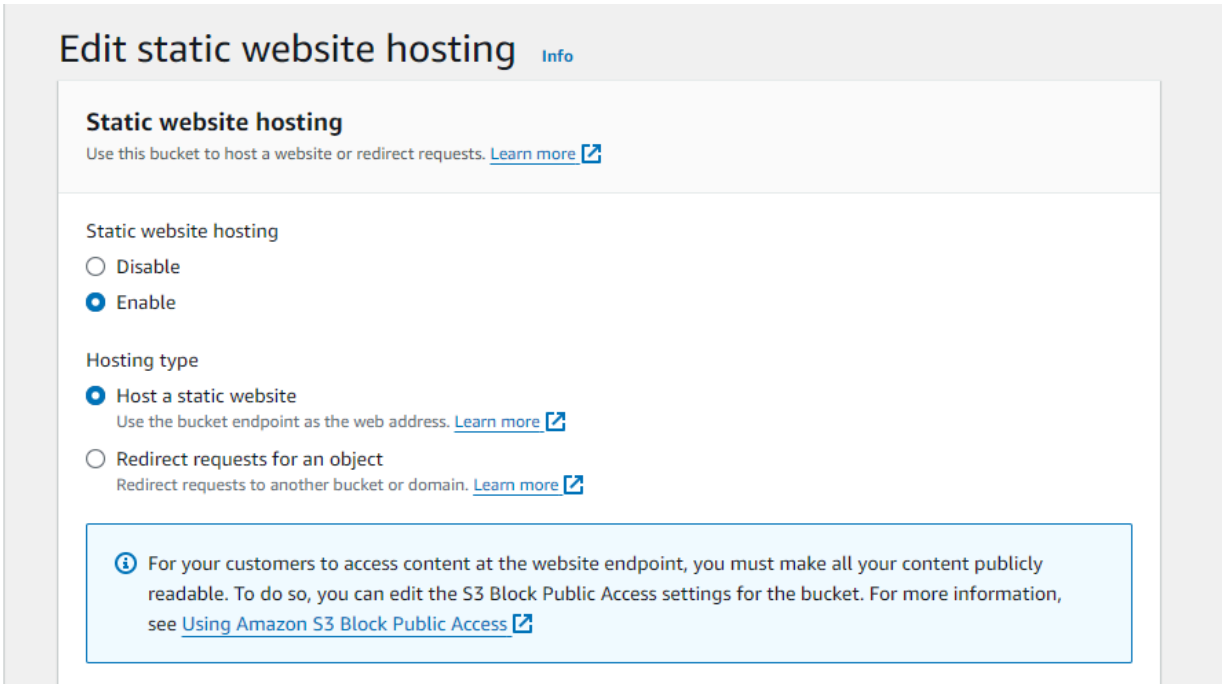

General configuration
AWS Region
US West (Oregon) us-west-2
Bucket type
Info
General purpose
Recommended for most use cases and access patterns. General purpose buckets are the original S3 bucket type. They allow a mix of storage classes that redundantly store objects across multiple Availability Zones.
Directory - New
Recommended for low-latency use cases. These buckets use only the S3 Express One Zone storage class, which provides faster processing of data within a single Availability Zone.
Bucket name
Info
VedantBucket
Bucket name must be unique within the global namespace and follow the bucket naming rules. See rules for bucket naming
Copy settings from existing bucket - optional
Only the bucket settings in the following configuration are copied.
Choose bucket
Format: s3://bucket/prefix

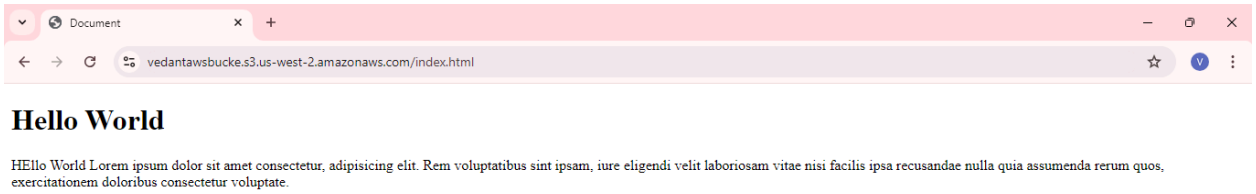

Drag and drop files and folders you want to upload here, or choose Add files or Add folder.
Files and folders (1 Total, 505.0 B)
Remove
Add files
Add folder
All files and folders in this table will be uploaded.
Find by name
1
Name
Folder
Type
index.html
-
text/html
Destination Info
Destination
s3://vedantawsbucke
Destination details
Bucket settings that impact new objects stored in the specified destination.


Edit Block public access (bucket settings) Info
Block public access (bucket settings)
Public access is granted to buckets and objects through access control lists (ACLs), bucket policies, access point policies, or all. In order to ensure that public access to all your S3 buckets and objects is blocked, turn on Block all public access. These settings apply only to this bucket and its access points. AWS recommends that you turn on Block all public access, but before applying any of these settings, ensure that your applications will work correctly without public access. If you require some level of public access to your buckets or objects within, you can customize the individual settings below to suit your specific storage use cases. Learn more
Block all public access
Turning this setting on is the same as turning on all four settings below. Each of the following settings are independent of one another.
Block public access to buckets and objects granted through new access control lists (ACLs)
S3 will block public access permissions applied to newly added buckets or objects, and prevent the creation of new public access ACLs for existing buckets and objects. This setting doesn't change any existing permissions that allow public access to S3 resources using ACLs.
Block public access to buckets and objects granted through any access control lists (ACLs)
S3 will ignore all ACLs that grant public access to buckets and objects.
Block public access to buckets and objects granted through new public bucket or access point policies
S3 will block new bucket and access point policies that grant public access to buckets and objects. This setting doesn't change any existing policies that allow public access to S3 resources.
Block public and cross-account access to buckets and objects through any public bucket or access point policies
S3 will ignore public and cross-account access for buckets or access points with policies that grant public access to buckets and objects.


Object Ownership
Control ownership of objects written to this bucket from other AWS accounts and the use of access control lists (ACLs). Object ownership determines who can specify access to objects.
ACLs disabled (recommended)
All objects in this bucket are owned by this account. Access to this bucket and its objects is specified using only policies.
ACLs enabled
Objects in this bucket can be owned by other AWS accounts. Access to this bucket and its objects can be specified using ACLs.
We recommend disabling ACLs, unless you need to control access for each object individually or to have the object writer own the data they upload. Using a bucket policy instead of ACLs to share data with users outside of your account simplifies permissions management and auditing.
Enabling ACLs turns off the bucket owner enforced setting for Object Ownership
Once the bucket owner enforced setting is turned off, access control lists (ACLs) and their associated permissions are restored. Access to objects that you do not own will be based on ACLs and not the bucket policy.
I acknowledge that ACLs will be restored.
Object Ownership


Upload succeeded
View details below.
Upload: status
Close
The information below will no longer be available after you navigate away from this page.
Summary
Destination
s3://vedantawsbucke
Succeeded
1 file, 505.0 B (100.00%)
Failed
0 files, 0 B (0%)
Files and folders
Configuration
Files and folders (1 Total, 505.0 B)


Edit static website hosting
Info
Static website hosting
Use this bucket to host a website or redirect requests. Learn more
Static website hosting
Disable
Enable
Hosting type
Host a static website
Use the bucket endpoint as the web address. Learn more
Redirect requests for an object
Redirect requests to another bucket or domain. Learn more
For your customers to access content at the website endpoint, you must make all your content publicly readable. To do so, you can edit the S3 Block Public Access settings for the bucket. For more information, see Using Amazon S3 Block Public Access


Document
vedantawsbucke.s3.us-west-2.amazonaws.com/index.html
Hello World
HEllo World Lorem ipsum dolor sit amet consectetur, adipisicing elit. Rem voluptatibus sint ipsam, iure eligendi velit laboriosam vitae nisi facilis ipsa recusandae nulla quia assumenda rerum quos, exercitationem doloribus consectetur voluptate.

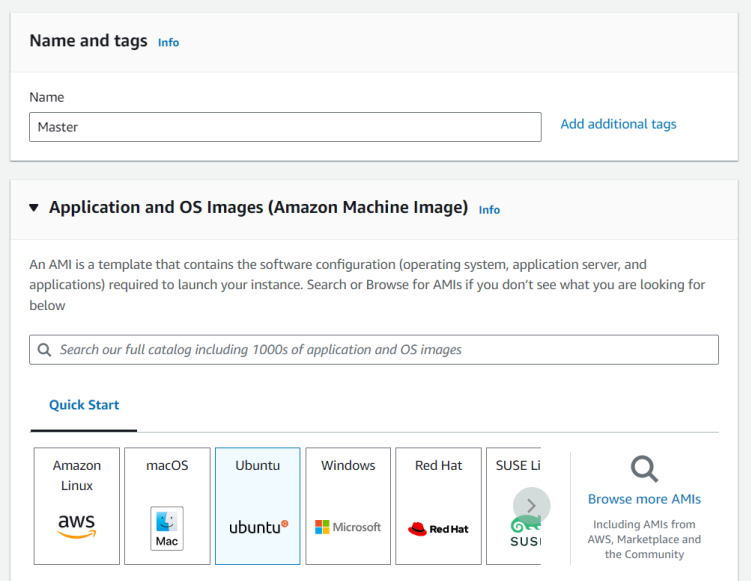
EC2 :

Experiment No 3

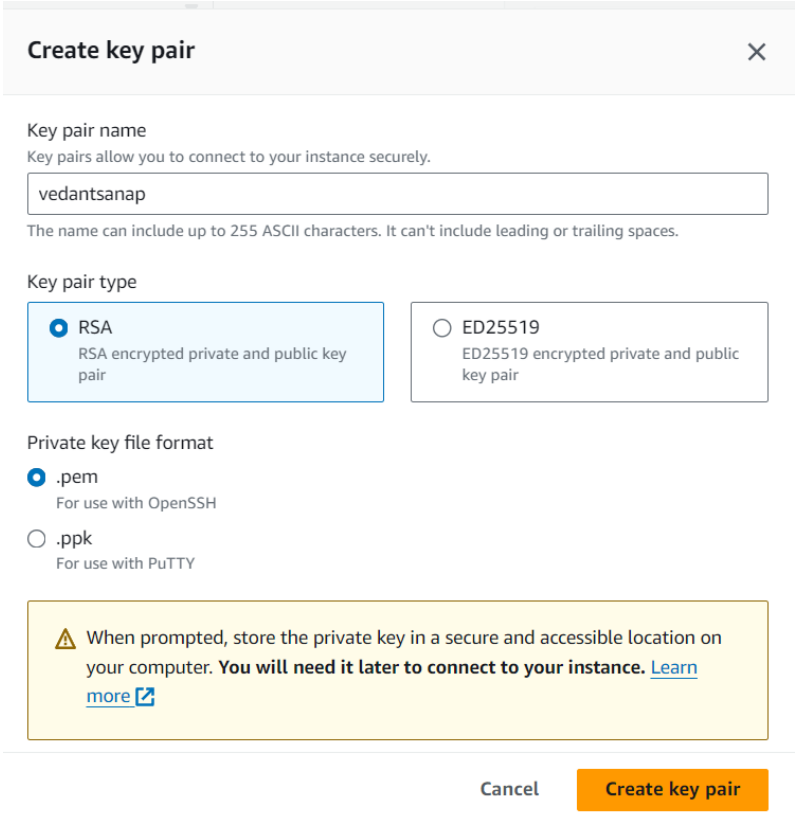
Vedant Sanap
D15A 48
Batch C

Aim- To understand the Kubernetes Cluster Architecture, install and Spin Up a Kubernetes Cluster on Linux Machines/Cloud Platforms.

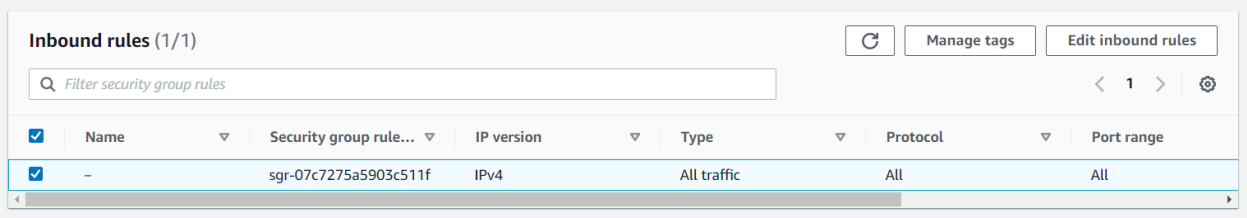
1) Launch 2 EC2 instance and select Ubuntu in AMI



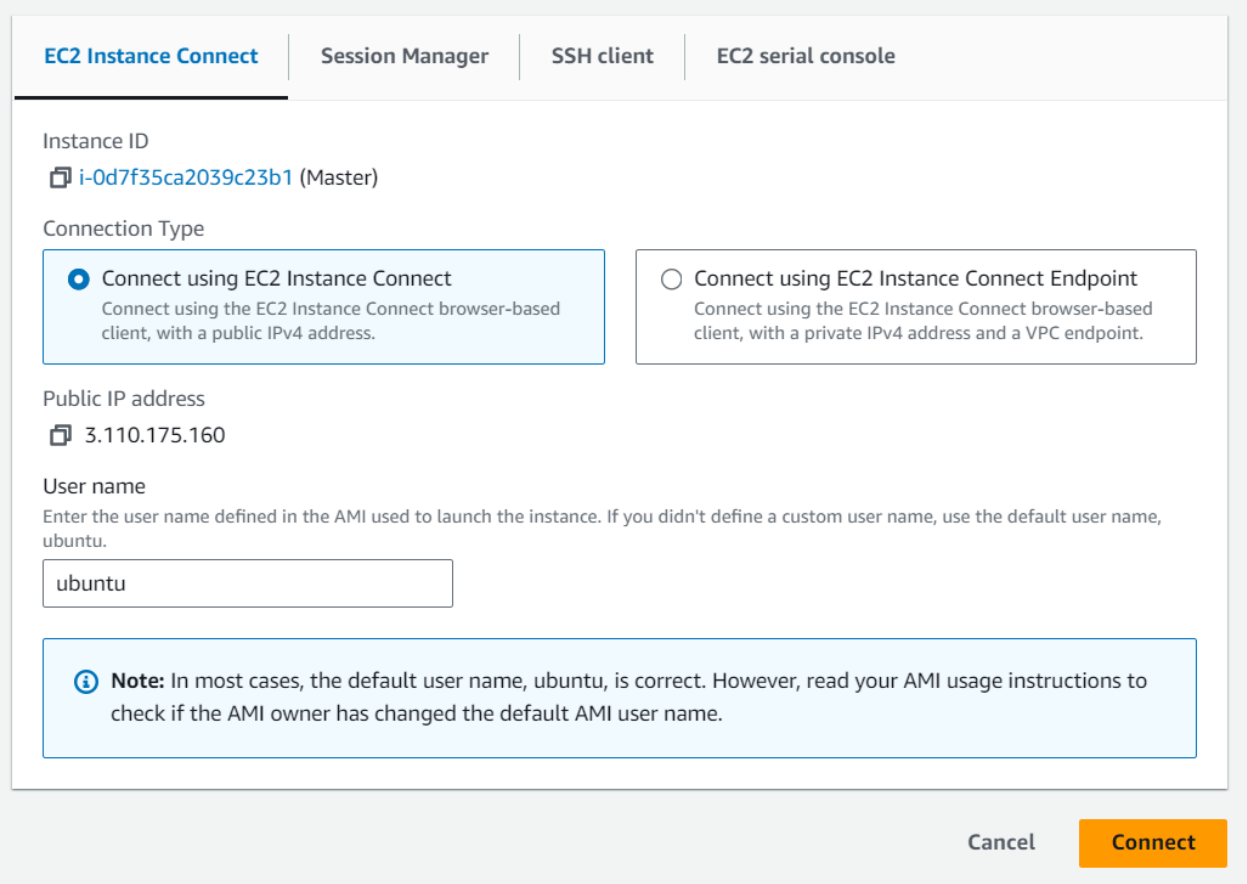
2) Create new key pair



3) In Security group select all checkbox and launch instance
4) Go to security group and edit inbound rules of both instance
5) Delete all the rules and add new rule with All traffic and Anywhere-IPv4



6) Now in running instances click on master instance and click on connect



8) Similarly connect the worker
9) Set hostname to master and worker respectively

```
ubuntu@ip-172-31-12-130:~$ sudo hostnamectl set-hostname master
ubuntu@ip-172-31-12-130:~$
```

```
ubuntu@master:~$
```

```
ubuntu@worker:~$
```

10) Use command sudo apt-get update on both master and worker CLI

sudo apt-get update on both

```
Get:24 http://ap-south-1.ec2.archive.ubuntu.com/ubuntu jammy-backports/main Translation-en [10.5 kB]
Get:25 http://ap-south-1.ec2.archive.ubuntu.com/ubuntu jammy-backports/main amd64 c-n-f Metadata [388 B]
Get:26 http://ap-south-1.ec2.archive.ubuntu.com/ubuntu jammy-backports/restricted amd64 c-n-f Metadata [1
Get:27 http://ap-south-1.ec2.archive.ubuntu.com/ubuntu jammy-backports/universe amd64 Packages [24.3 kB]
Get:28 http://ap-south-1.ec2.archive.ubuntu.com/ubuntu jammy-backports/universe Translation-en [16.4 kB]
Get:29 http://ap-south-1.ec2.archive.ubuntu.com/ubuntu jammy-backports/universe amd64 c-n-f Metadata [644
Get:30 http://ap-south-1.ec2.archive.ubuntu.com/ubuntu jammy-backports/multiverse amd64 c-n-f Metadata [1
Get:31 http://security.ubuntu.com/ubuntu jammy-security/main amd64 Packages [765 kB]
Get:32 http://security.ubuntu.com/ubuntu jammy-security/main Translation-en [165 kB]
Get:33 http://security.ubuntu.com/ubuntu jammy-security/main amd64 c-n-f Metadata [11.3 kB]
Get:34 http://security.ubuntu.com/ubuntu jammy-security/restricted amd64 Packages [826 kB]
Get:35 http://security.ubuntu.com/ubuntu jammy-security/restricted Translation-en [133 kB]
Get:36 http://security.ubuntu.com/ubuntu jammy-security/restricted amd64 c-n-f Metadata [536 B]
Get:37 http://security.ubuntu.com/ubuntu jammy-security/universe amd64 Packages [781 kB]
Get:38 http://security.ubuntu.com/ubuntu jammy-security/universe Translation-en [143 kB]
Get:39 http://security.ubuntu.com/ubuntu jammy-security/universe amd64 c-n-f Metadata [16.7 kB]
Get:40 http://security.ubuntu.com/ubuntu jammy-security/multiverse amd64 Packages [36.5 kB]
Get:41 http://security.ubuntu.com/ubuntu jammy-security/multiverse Translation-en [7060 B]
Get:42 http://security.ubuntu.com/ubuntu jammy-security/multiverse amd64 c-n-f Metadata [260 B]
Fetched 27.1 MB in 5s (5664 kB/s)
Reading package lists... Done
ubuntu@master:~$
```

11) Installing Docker on both CLI

sudo apt-get install docker.io on both

```
Done.
Created symlink /etc/systemd/system/multi-user.target.wants/docker.service → /lib/systemd/system/docker.service.
Created symlink /etc/systemd/system/sockets.target.wants/docker.socket → /lib/systemd/system/docker.socket.
Processing triggers for dbus (1.12.20-2ubuntu4.1) ...
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@master:~$
```

12) Enable Docker on both CLI and check its status

sudo systemctl enable docker

sudo systermctl status docker on both

```
No VM guests are running outdated hypervisor (qemu) binaries on this host.
ubuntu@master:~$ sudo systemctl enable docker
ubuntu@master:~$ sudo systemctl status docker
● docker.service - Docker Application Container Engine
     Loaded: loaded (/lib/systemd/system/docker.service; enabled; vendor preset: enabled)
     Active: active (running) since Sun 2023-09-17 17:23:49 UTC; 3min 30s ago
TriggeredBy: ● docker.socket
       Docs: https://docs.docker.com
   Main PID: 3050 (dockerd)
      Tasks: 7
     Memory: 33.2M
        CPU: 291ms
     CGroup: /system.slice/docker.service
             └─3050 /usr/bin/dockerd -H fd:// --containerd=/run/containerd/containerd.sock
```

DOCKER INSTALLED SUCCESSFULLY

13) Now for Installing Kubernetes (On both CLI)

sudo apt-get update

```
ubuntu@master:~$ sudo apt-get update
Hit:1 http://ap-south-1.ec2.archive.ubuntu.com/ubuntu jammy InRelease
Hit:2 http://ap-south-1.ec2.archive.ubuntu.com/ubuntu jammy-updates InRelease
Hit:3 http://ap-south-1.ec2.archive.ubuntu.com/ubuntu jammy-backports InRelease
Hit:4 http://security.ubuntu.com/ubuntu jammy-security InRelease
Reading package lists... Done
ubuntu@master:~$
```

sudo apt-get install -y apt-transport-https ca-certificates curl

```
Updating certificates in /etc/ssl/certs...
rehash: warning: skipping ca-certificates.crt,it does not contain exactly one certificate or CRL
19 added, 6 removed; done.
Setting up libcurl4:amd64 (7.81.0-1ubuntu1.13) ...
Setting up curl (7.81.0-1ubuntu1.13) ...
Processing triggers for man-db (2.10.2-1) ...
Processing triggers for libc-bin (2.35-0ubuntu3.1) ...
Processing triggers for ca-certificates (20230311ubuntu0.22.04.1) ...
Updating certificates in /etc/ssl/certs...
0 added, 0 removed; done.
Running hooks in /etc/ca-certificates/update.d...
done.
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@master:~$
```

14) Download Google cloud public signing key

sudo curl -fsSLo /usr/share/keyrings/kubernetes-archive-keyring.gpg https://dl.k8s.io/apt/doc/apt-key.gpg

```
No VM guests are running outdated hypervisor (qemu) binaries on this host.
ubuntu@master:~$ sudo curl -fsSLo /usr/share/keyrings/kubernetes-archive-keyring.gpg https://dl.k8s.io/apt/doc/apt-key.gpg
ubuntu@master:~$
```

15) Adding kubernetes apt repository

echo "deb [signed-by=/usr/share/keyrings/kubernetes-archive-keyring.gpg] https://apt.kubernetes.io/ kubernetes-xenial main" | sudo tee /etc/apt/sources.list.d/kubernetes.list

```
ubuntu@master:~$ echo "deb [signed-by=/usr/share/keyrings/kubernetes-archive-keyring.gpg] https://apt.kubernetes.io/ kubernetes-xenial main" | sudo tee /etc/apt/sources.lis
t.d/kubernetes.list
deb [signed-by=/usr/share/keyrings/kubernetes-archive-keyring.gpg] https://apt.kubernetes.io/ kubernetes-xenial main
ubuntu@master:~$
```

16) Run this 3 commands

sudo apt-get update

```
ubuntu@master:~$ sudo apt-get update
Hit:1 http://ap-south-1.ec2.archive.ubuntu.com/ubuntu jammy InRelease
Hit:2 http://ap-south-1.ec2.archive.ubuntu.com/ubuntu jammy-updates InRelease
Hit:3 http://ap-south-1.ec2.archive.ubuntu.com/ubuntu jammy-backports InRelease
Hit:4 http://security.ubuntu.com/ubuntu jammy-security InRelease
Get:5 https://packages.cloud.google.com/apt kubernetes-xenial InRelease [8993 B]
Get:6 https://packages.cloud.google.com/apt kubernetes-xenial/main amd64 Packages [69.9 kB]
Fetched 78.9 kB in 1s (53.8 kB/s)
Reading package lists... Done
ubuntu@master:~$
```

sudo apt-get install -y kubelet kubeadm kubectl

```
Setting up conntrack (1:1.4.6-2build2) ...
Setting up kubectl (1.28.2-00) ...
Setting up ebtables (2.0.11-4build2) ...
Setting up socat (1.7.4.1-3ubuntu4) ...
Setting up cri-tools (1.26.0-00) ...
Setting up kubernetes-cni (1.2.0-00) ...
Setting up kubelet (1.28.2-00) ...
Created symlink /etc/systemd/system/multi-user.target.wants/kubelet.service → /lib/systemd/system/kubelet.service.
Setting up kubeadm (1.28.2-00) ...
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@master:~$
```

sudo apt-mark hold kubelet kubeadm kubectl

```
ubuntu@master:~$ sudo apt-mark hold kubelet kubeadm kubectl
kubelet set on hold.
kubeadm set on hold.
kubectl set on hold.
ubuntu@master:~$
```

KUBERNETES INSTALLED SUCCESSFULLY

17) Kubernetes Deployment

sudo swapoff -a

```
ubuntu@master:~$ sudo swapoff -a
ubuntu@master:~$
```

18) Initialize kubernetes on Master

sudo touch "/etc/docker/daemon.json"

sudo nano "/etc/docker/daemon.json" Run this command and copy paste this

{

"exec-opts": ["native.cgroupdriver=systemd"]

}

Then press ctrl + O and enter then ctrl + X

sudo cat "/etc/docker/daemon.json"

sudo systemctl daemon-reload

sudo systemctl restart docker

sudo systemctl restart kubelet

sudo kubeadm reset

```
ubuntu@master:~$ sudo touch "/etc/docker/daemon.json"
ubuntu@master:~$ sudo nano "/etc/docker/daemon.json"
```

```
ubuntu@master:~$ sudo cat "/etc/docker/daemon.json"
{
      "exec-opts": ["native.cgroupdriver=systemd"],
      "log-driver": "json-file",
      "log-opts": {
      "max-size": "100m"
   },
       "storage-driver": "overlay2"
       }
ubuntu@master:~$
```

```
ubuntu@master:~$ sudo systemctl daemon-reload
ubuntu@master:~$ sudo systemctl restart docker
ubuntu@master:~$ sudo systemctl restart kubelet
ubuntu@master:~$ sudo kubeadm reset
W0917 18:15:57.371540   10839 preflight.go:56] [reset] WARNING: (
[reset] Are you sure you want to proceed? [y/N]: y
[preflight] Running pre-flight checks
W0917 18:16:01.329044   10839 removeetcdmember.go:106] [reset] No
[reset] Deleted contents of the etcd data directory: /var/lib/etc
[reset] Stopping the kubelet service
[reset] Unmounting mounted directories in "/var/lib/kubelet"
```

$ sudo kubeadm init --pod-network-cidr=10.244.0.0/16 --ignore-preflight-errors=all

```
ubuntu@master:~$ sudo kubeadm init --pod-network-cidr=10.244.0.0/16 --ignore-preflight-er
[init] Using Kubernetes version: v1.28.2
[preflight] Running pre-flight checks
        [WARNING NumCPU]: the number of available CPUs 1 is less than the required 2
        [WARNING Mem]: the system RAM (965 MB) is less than the minimum 1700 MB
[preflight] Pulling images required for setting up a Kubernetes cluster
[preflight] This might take a minute or two, depending on the speed of your internet conn
[preflight] You can also perform this action in beforehand using 'kubeadm config images p
W0917 18:17:31.346348   10860 checks.go:835] detected that the sandbox image "registry.k8
 It is recommended that using "registry.k8s.io/pause:3.9" as the CRI sandbox image.
[certs] Using certificateDir folder "/etc/kubernetes/pki"
[certs] Generating "ca" certificate and key
[certs] Generating "apiserver" certificate and key
[certs] apiserver serving cert is signed for DNS names [kubernetes kubernetes.default kub
 172.31.12.130]
[certs] Generating "apiserver-kubelet-client" certificate and key
[certs] Generating "front-proxy-ca" certificate and key
[certs] Generating "front-proxy-client" certificate and key
[certs] Generating "etcd/ca" certificate and key
[certs] Generating "etcd/server" certificate and key
[certs] etcd/server serving cert is signed for DNS names [localhost master] and IPs [172.
[certs] Generating "etcd/peer" certificate and key
[certs] etcd/peer serving cert is signed for DNS names [localhost master] and IPs [172.31
[certs] Generating "etcd/healthcheck-client" certificate and key
[certs] Generating "apiserver-etcd-client" certificate and key
[certs] Generating "sa" key and public key
```

kubeadm join 172.31.12.130:6443 --token 67nba2.98zekjx1ogwtrr29 --discovery-token-ca-cert-hash sha256:5d3403f5221016f77cbed1757a266467af45dc41b765ebe535f15ee058baf883

```
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 172.31.12.130:6443 --token 67nba2.98zekjx1ogwtrr29 \
        --discovery-token-ca-cert-hash sha256:5d3403f5221016f77cbed1757a266467af45dc41b765ebe535f15ee058baf883
ubuntu@master:~$
```

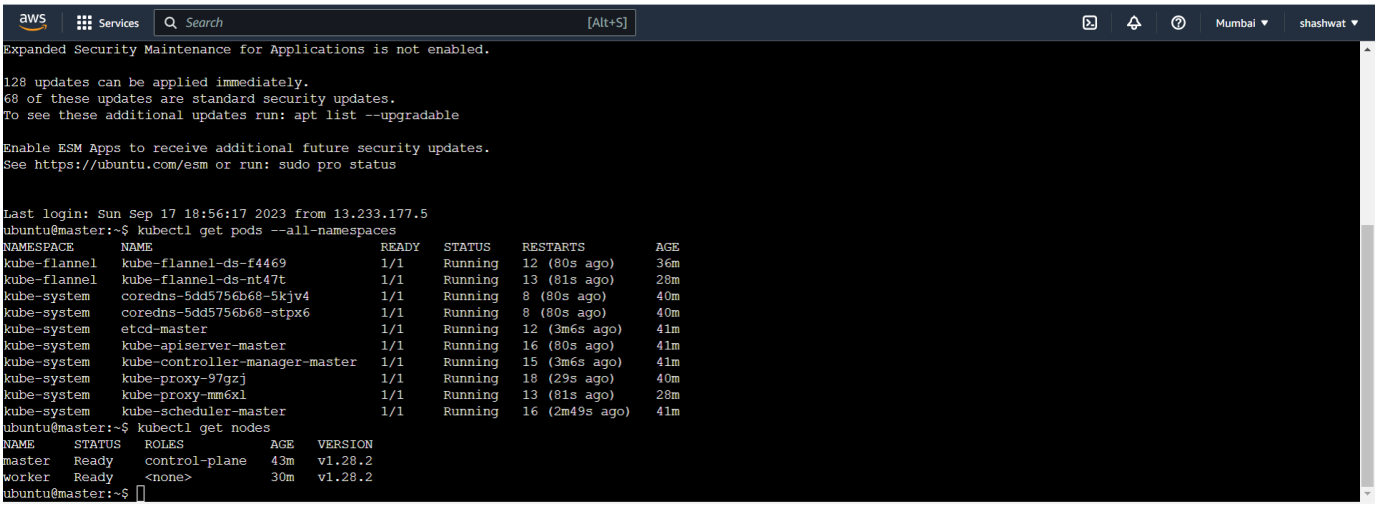
```
ubuntu@master:~$ mkdir -p $HOME/.kube
ubuntu@master:~$ sudo cp -i /etc/kubernetes/admin.conf $HOME/.kube/config
ubuntu@master:~$ sudo chown $(id -u):$(id -g) $HOME/.kube/config
ubuntu@master:~$
```

```
ubuntu@master:~$ kubectl apply -f https://github.com/flannel-io/flannel/releases/latest/download/kube-flannel.yml
namespace/kube-flannel created
serviceaccount/flannel created
clusterrole.rbac.authorization.k8s.io/flannel created
clusterrolebinding.rbac.authorization.k8s.io/flannel created
configmap/kube-flannel-cfg created
daemonset.apps/kube-flannel-ds created
ubuntu@master:~$
```

```
[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...
I0917 18:31:31.967826   11348 kubelet.go:220] [kubelet-start] preserving the crisocket information for th
I0917 18:31:31.968119   11348 patchnode.go:31] [patchnode] Uploading the CRI Socket information "unix:///
 as an annotation
I0917 18:31:31.968407   11348 cert_rotation.go:137] Starting client certificate rotation controller

This node has joined the cluster:
* Certificate signing request was sent to apiserver 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.

ubuntu@worker:~$
```

```
ubuntu@master:~$ kubectl get pods --all-namespaces
The connection to the server 172.31.12.130:6443 was refused - did you specify the right host or port?
ubuntu@master:~$
```

```
ubuntu@master:~$ kubectl get nodes
NAME     STATUS   ROLES           AGE   VERSION
master   Ready    control-plane   24m   v1.28.2
worker   Ready    <none>          11m   v1.28.2
ubuntu@master:~$
```



Conclusion:
Thus we have understood the Kubernetes Cluster Architecture, installed and spun a Kubernetes Cluster on AWS Cloud Platform.

Error:
The status of all namespaces was not showing running in the first try, but when I rebooted the master and worker instances it was successful.

Experiment No 4

Vedant Sanap
D15A 48
Batch C

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

```
Last login: Sun Sep 17 18:58:53 2023 from 13.233.177.4
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:~$
```

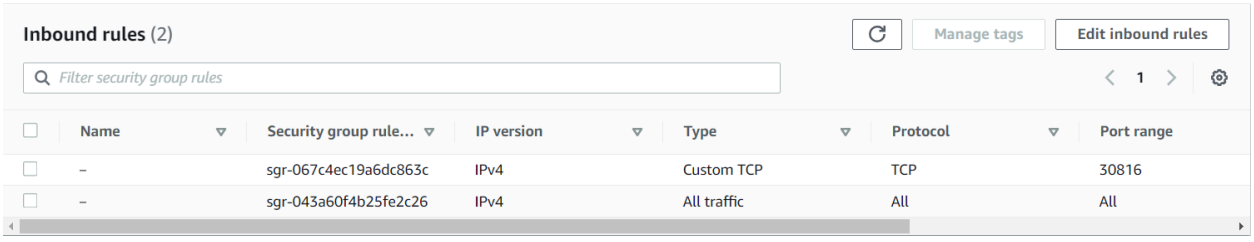
- **Run the following command to create a service named nginx that will expose the app publicly.**
  kubectl expose deploy nginx –port 80 –target-port 80 –type NodePort

```
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.**

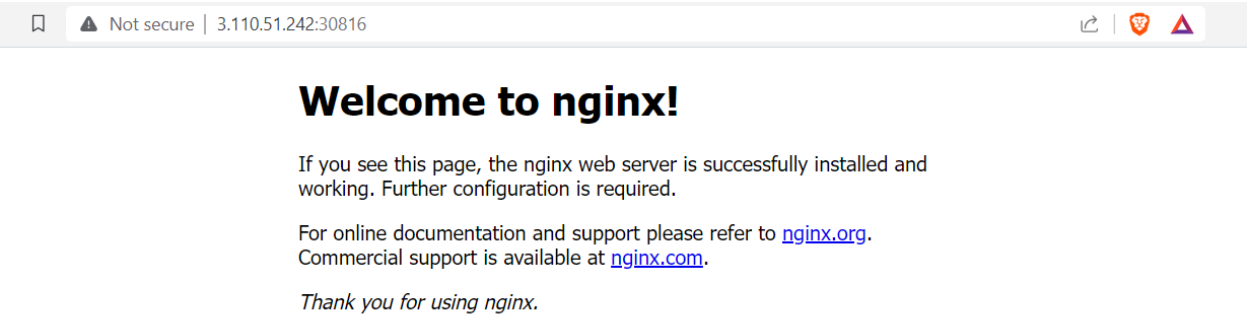


- **We can verify that the nginx page is accessible on all nodes using curl command(Worker)**

1. sudo su
2. curl worker:30816

```
Last login: Fri Sep 22 13:48:46 2023 from 13.233.177.4
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:

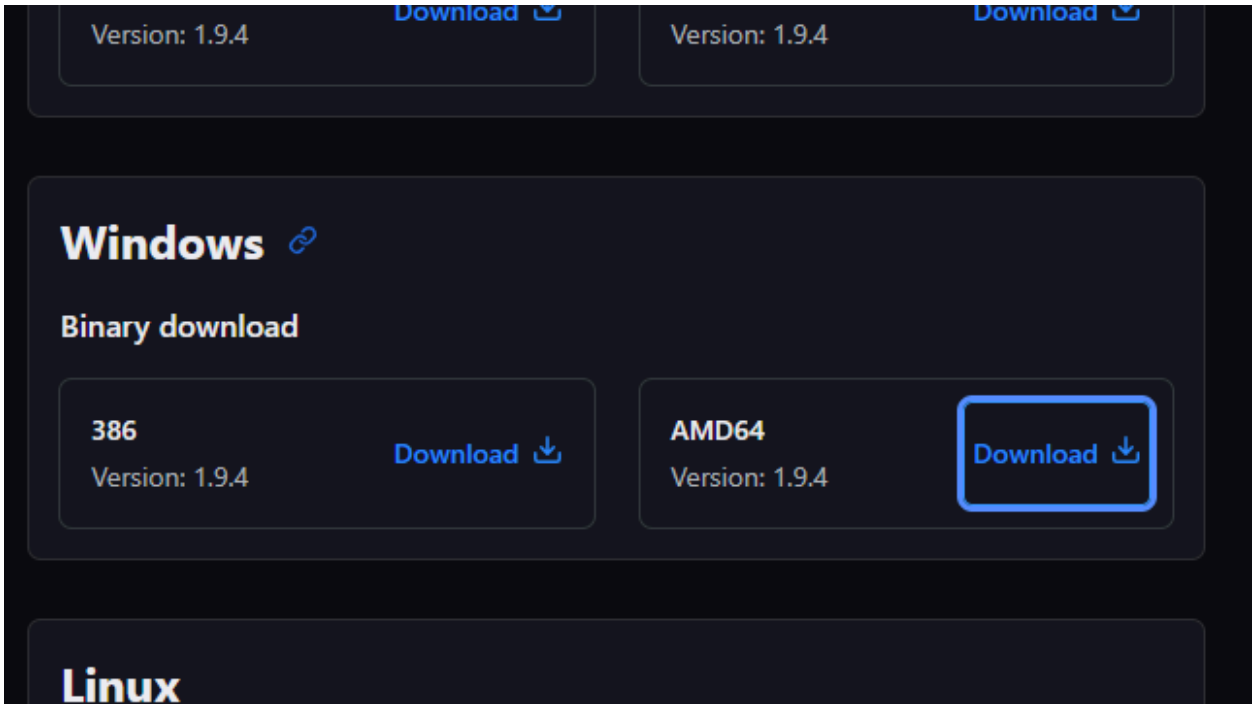
Thus, we have studied and implemented how to install Kubectl and execute Kubectl commands to manage the Kubernetes cluster and deploy.

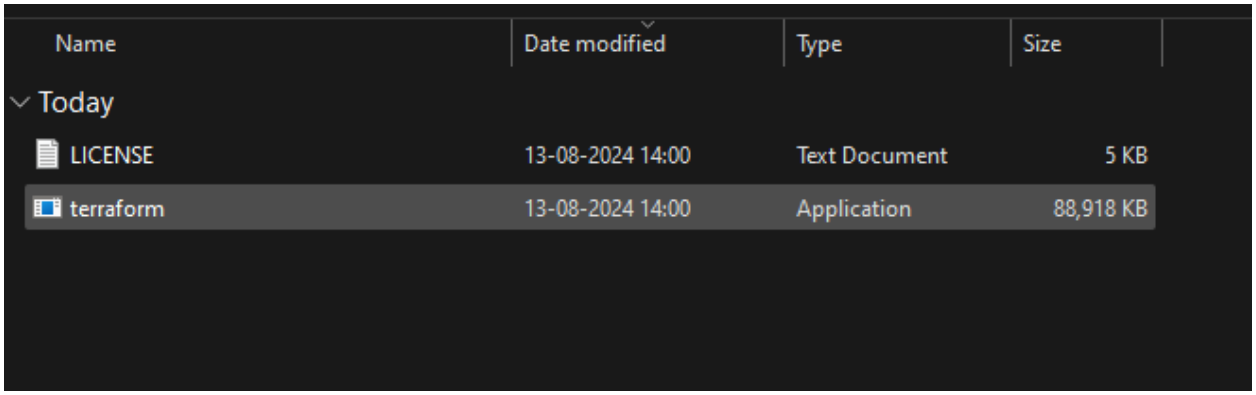
Errors:

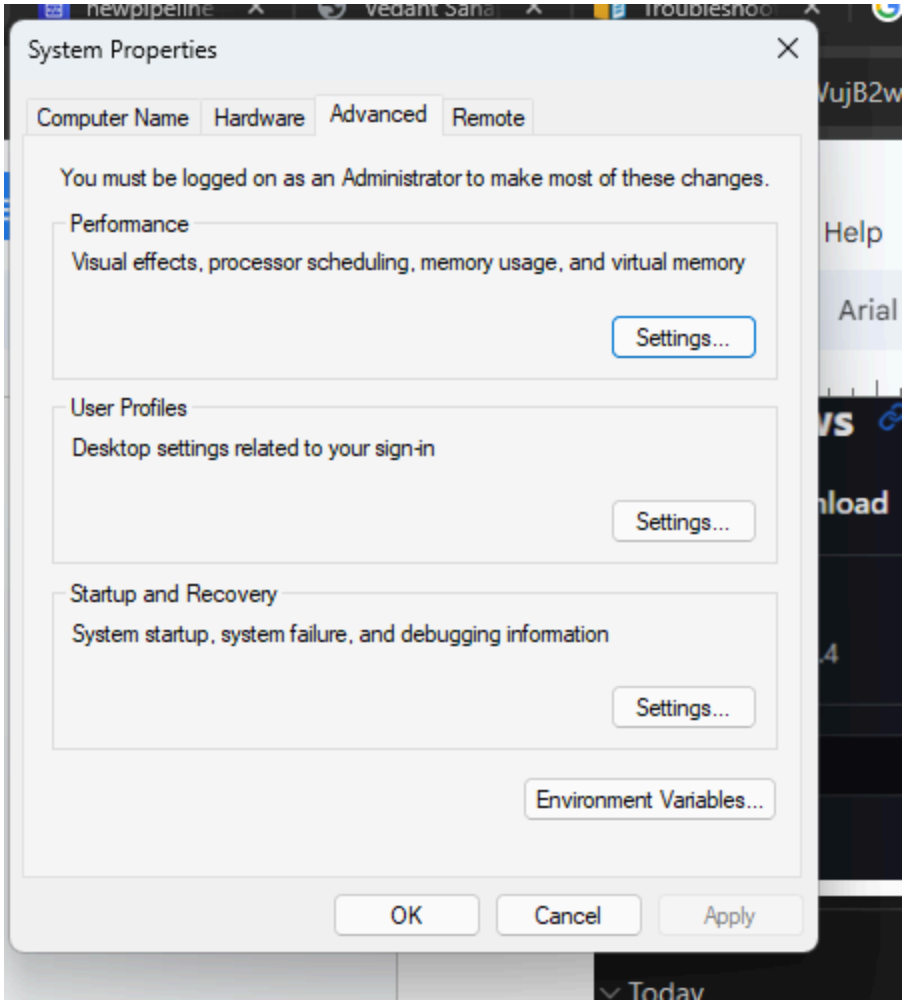
I was facing an error because I forgot to make changes in the security group of worker node.

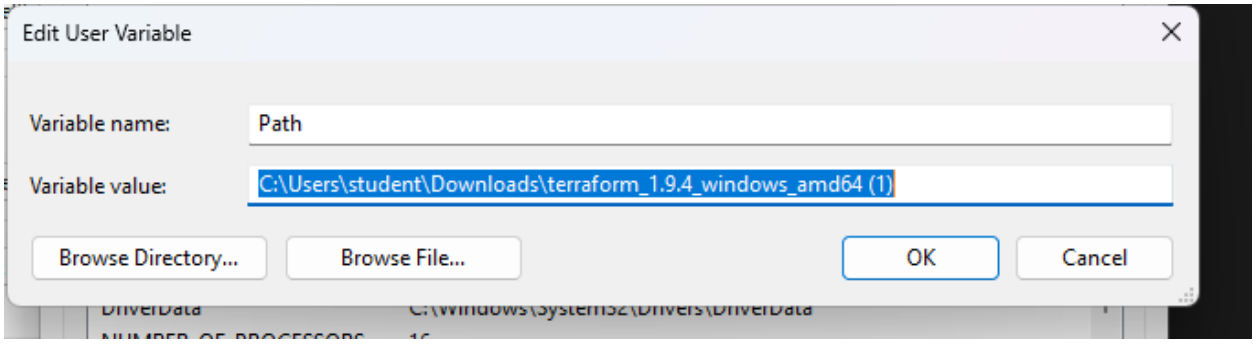
ADVANCE DEVOPS EXP-5

Vedant Sanap **D15A/48**






System Properties
Computer Name
Hardware
Advanced
Remote
You must be logged on as an Administrator to make most of these changes.
Performance
Visual effects, processor scheduling, memory usage, and virtual memory
Settings...
User Profiles
Desktop settings related to your sign-in
Settings...
Startup and Recovery
System startup, system failure, and debugging information
Settings...
Environment Variables...
OK
Cancel
Apply


Edit User Variable
Variable name:
Path
Variable value:
C:\Users\student\Downloads\terraform_1.9.4_windows_amd64 (1)
Browse Directory...
Browse File...
OK
Cancel


Windows PowerShell
System
Open
Run as administrator
Open file location
Pin to Start
Pin to taskbar

```
PS C:\Users\student> terraform
Usage: terraform [global options] <subcommand> [args]

The available commands for execution are listed below.
The primary workflow commands are given first, followed by
less common or more advanced commands.

Main commands:
  init          Prepare your working directory for other commands
  validate      Check whether the configuration is valid
  plan          Show changes required by the current configuration
  apply         Create or update infrastructure
  destroy       Destroy previously-created infrastructure

All other commands:
  console       Try Terraform expressions at an interactive command prompt
  fmt           Reformat your configuration in the standard style
  force-unlock  Release a stuck lock on the current workspace
  get           Install or upgrade remote Terraform modules
  graph         Generate a Graphviz graph of the steps in an operation
  import        Associate existing infrastructure with a Terraform resource
  login         Obtain and save credentials for a remote host
  logout        Remove locally-stored credentials for a remote host
  metadata      Metadata related commands
  output        Show output values from your root module
  providers     Show the providers required for this configuration
  refresh       Update the state to match remote systems
  show          Show the current state or a saved plan
  state         Advanced state management
  taint         Mark a resource instance as not fully functional
  test          Execute integration tests for Terraform modules
  untaint       Remove the 'tainted' state from a resource instance
  version       Show the current Terraform version
```

Vedant Sanap **D15A** **48**

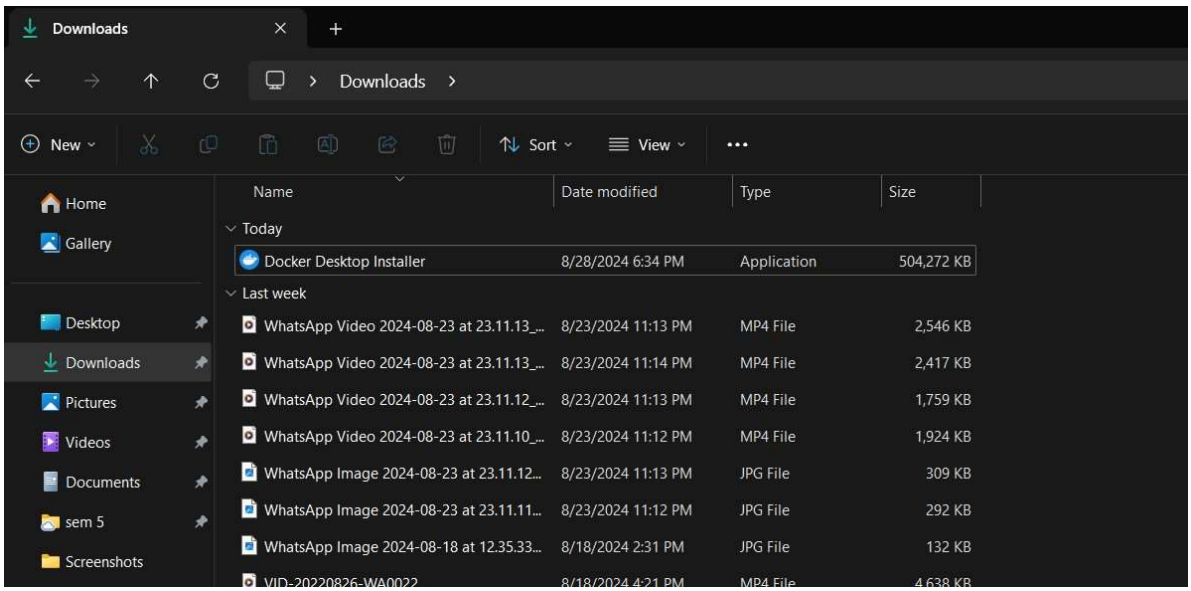
Experiment 6

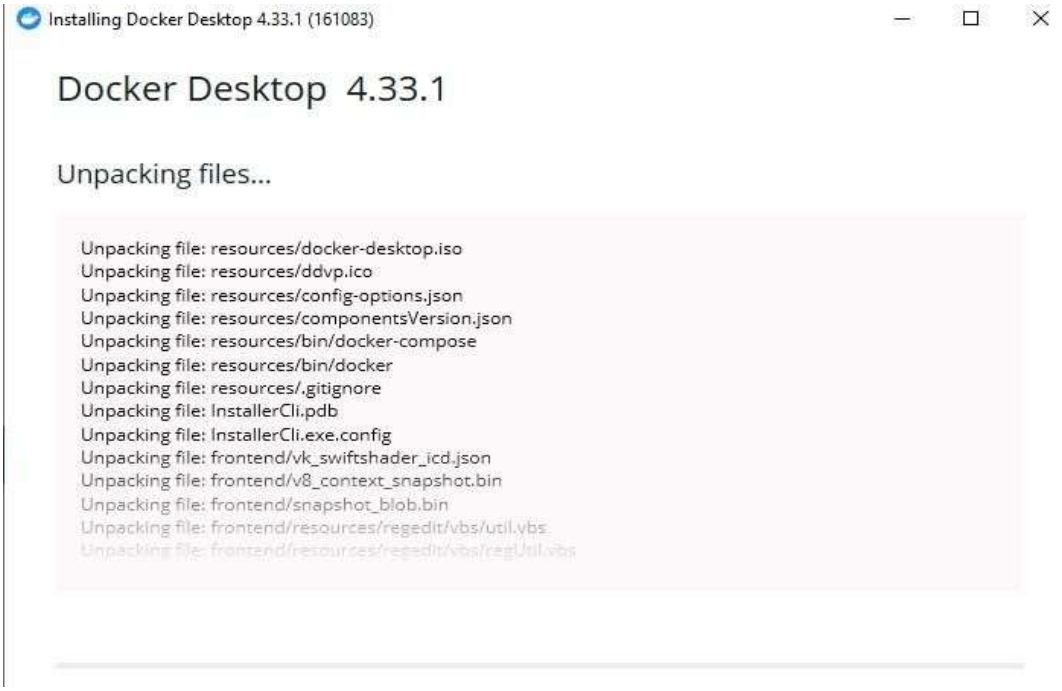
Aim:

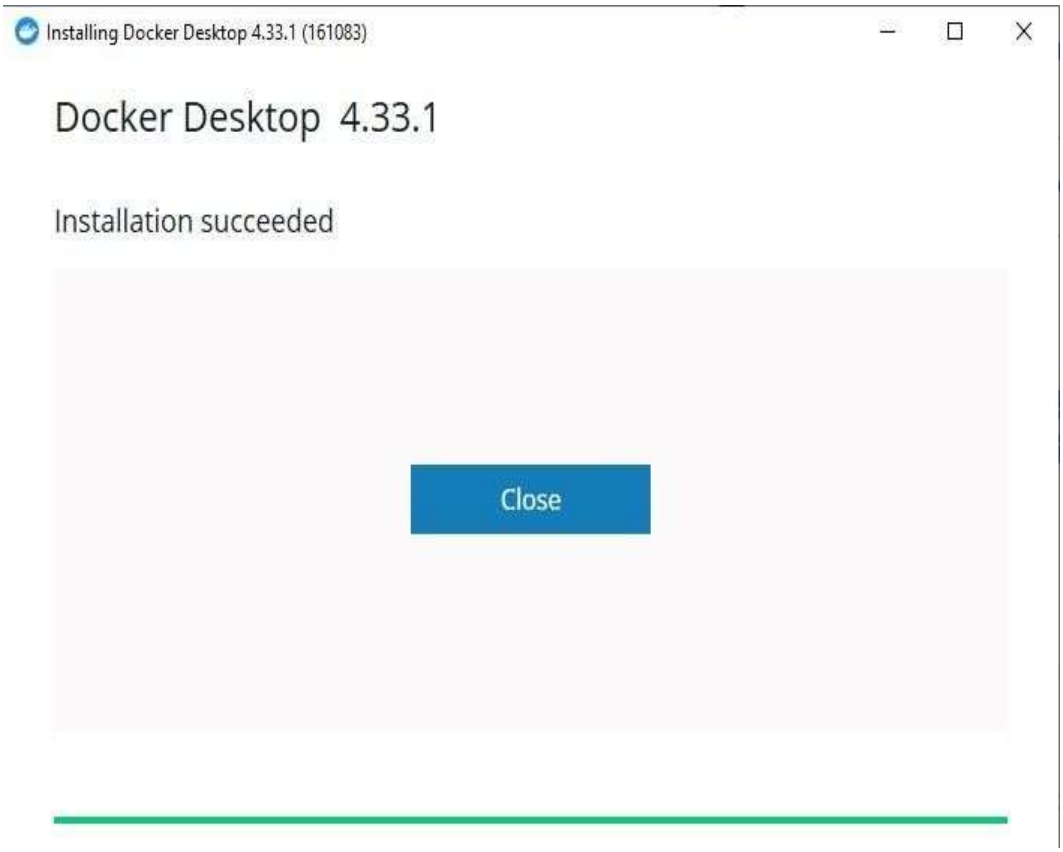
To Build, change, and destroy AWS / GCP /Microsoft Azure/ DigitalOcean infrastructure Using Terraform.(S3 bucket or Docker)

Step 1: Download Docker form www.docker.com

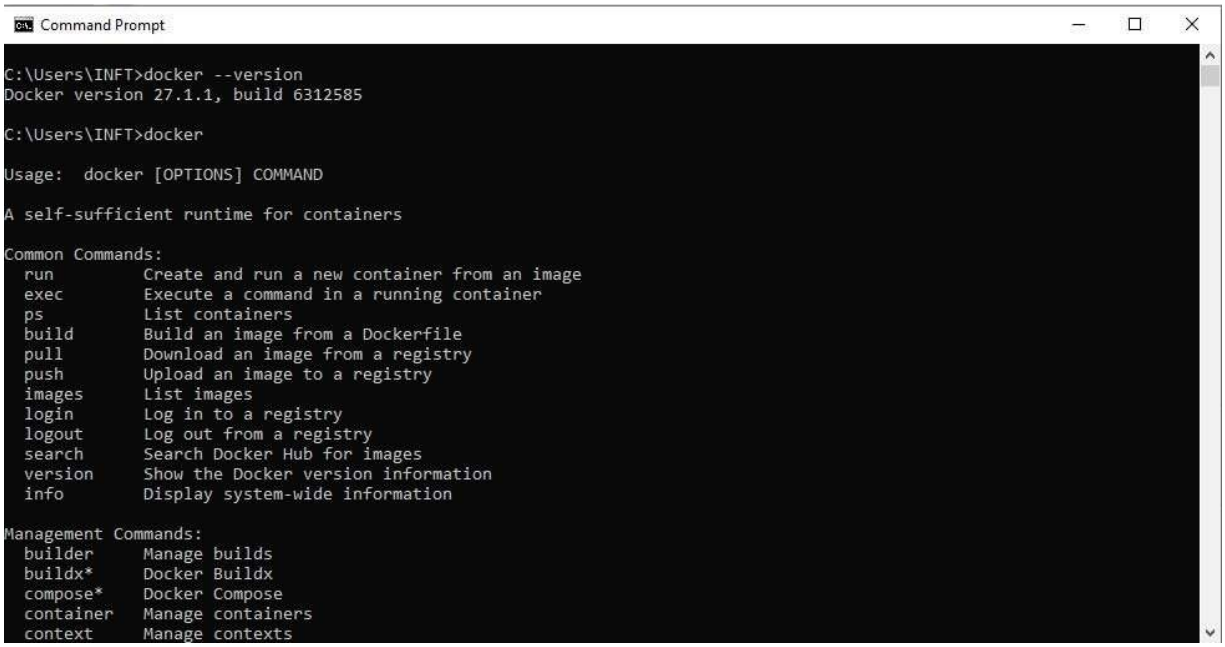
Step 2: The Docker is successfully downloaded. Now, run the docker installer and complete the installation.



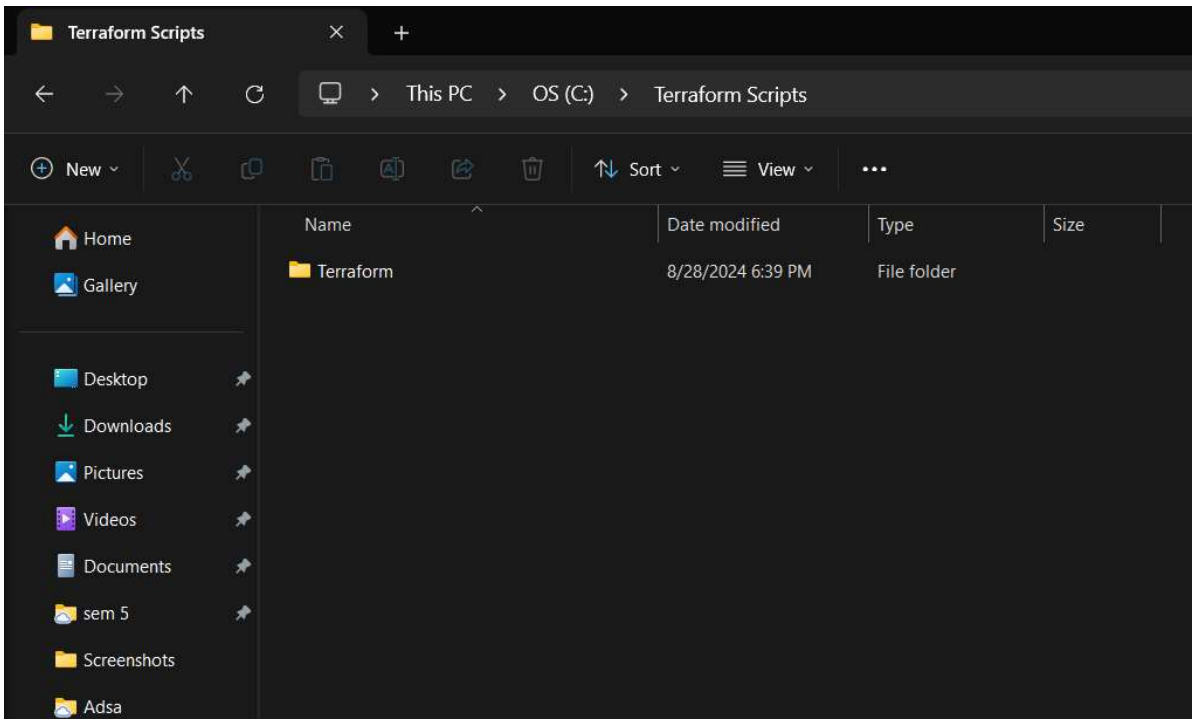

Installing Docker Desktop 4.33.1 (161083)
Docker Desktop 4.33.1
Unpacking files...
Unpacking file: resources/docker-desktop.iso
Unpacking file: resources/ddvp.ico
Unpacking file: resources/config-options.json
Unpacking file: resources/componentsVersion.json
Unpacking file: resources/bin/docker-compose
Unpacking file: resources/bin/docker
Unpacking file: resources/.gitignore
Unpacking file: InstallerCli.pdb
Unpacking file: InstallerCli.exe.config
Unpacking file: frontend/vk_swiftshader_icd.json
Unpacking file: frontend/v8_context_snapshot.bin
Unpacking file: frontend/snapshot_blob.bin
Unpacking file: frontend/resources/regedit/vbs/util.vbs


Installing Docker Desktop 4.33.1 (161083)
Docker Desktop 4.33.1
Installation succeeded
Close

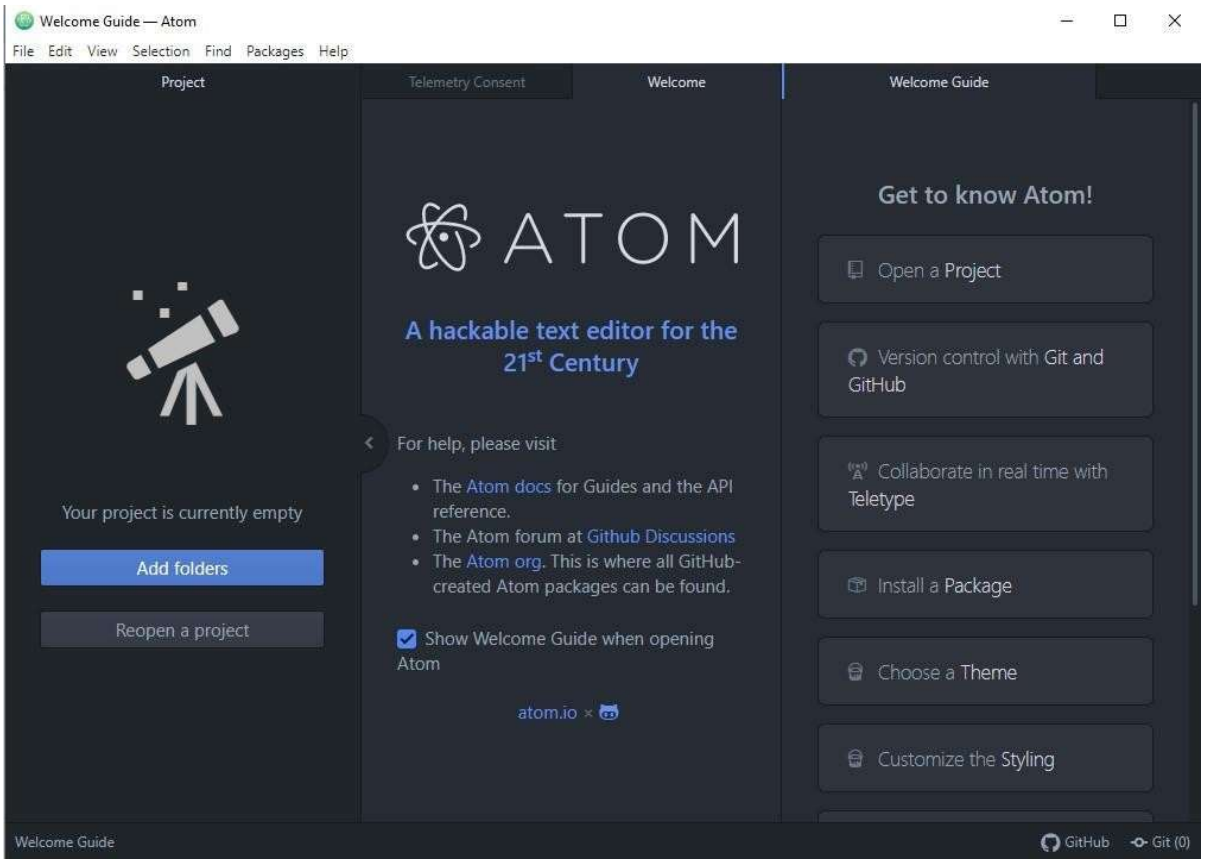
Step 3: Open Command Prompt and run as administrator. Enter the command docker –version, to check whether the docker is successfully installed.



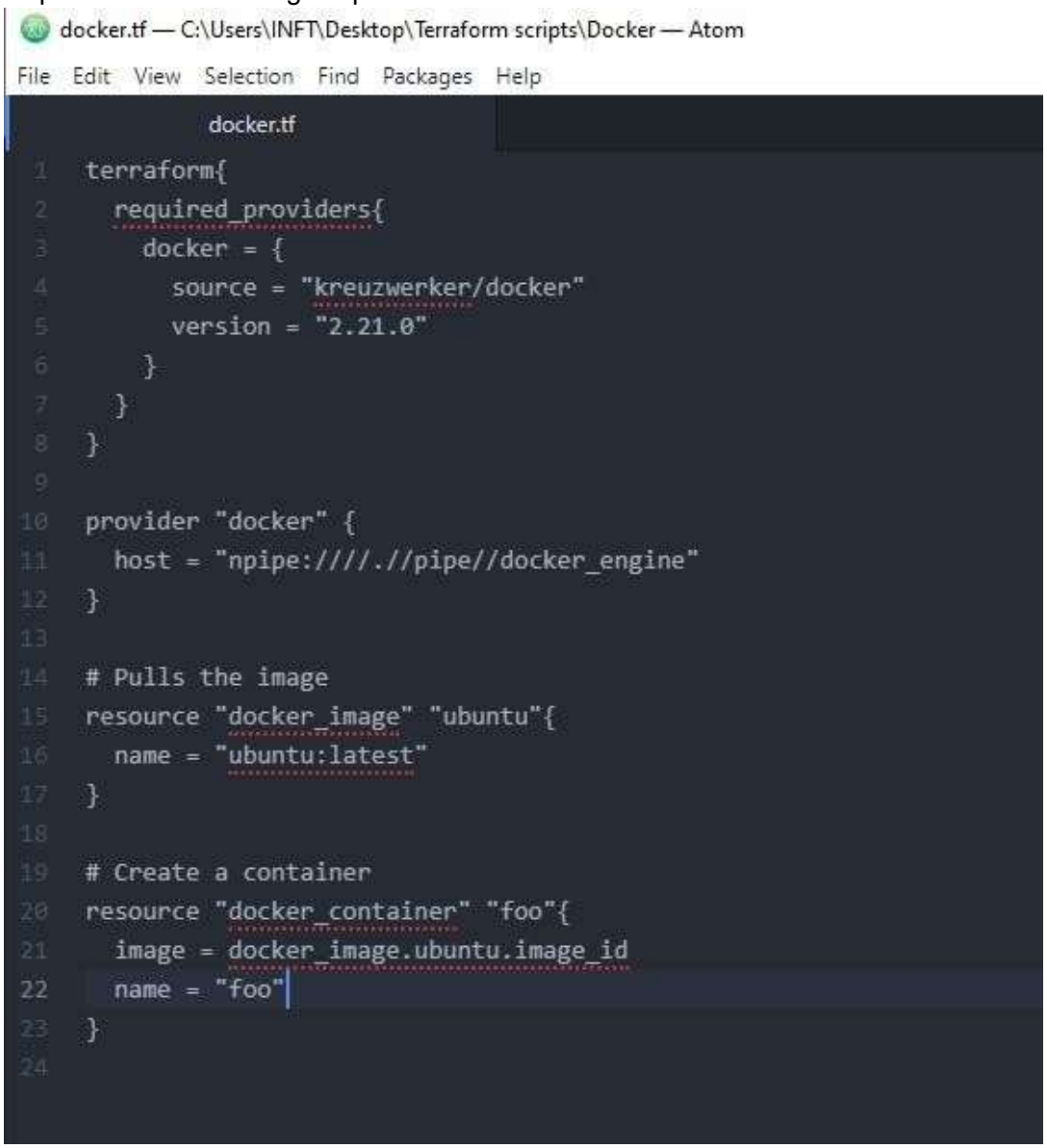
Step 4: Create a folder Terraform_scripts and inside it create a folder named Docker.



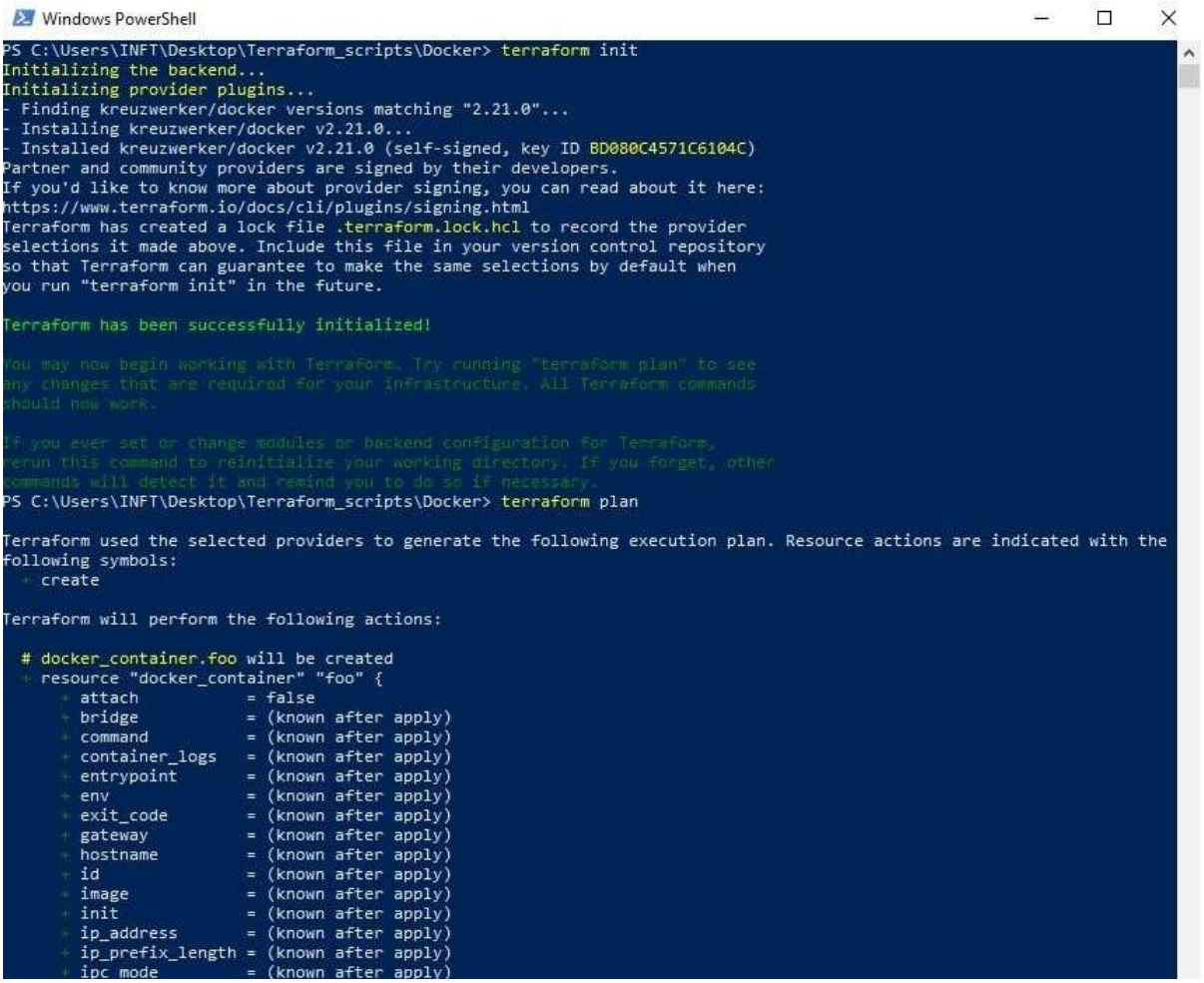
Step 5: Download Atom Editor.

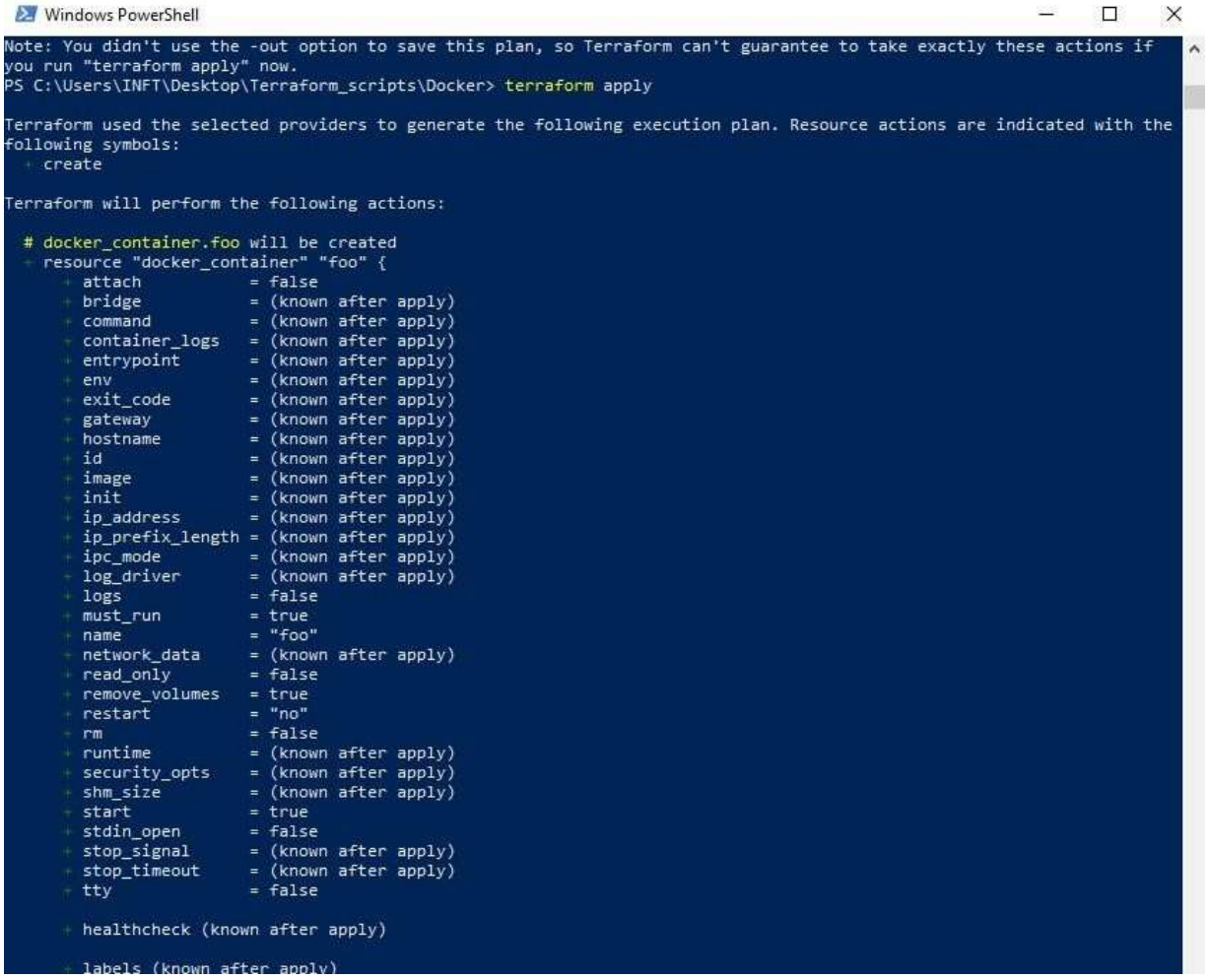


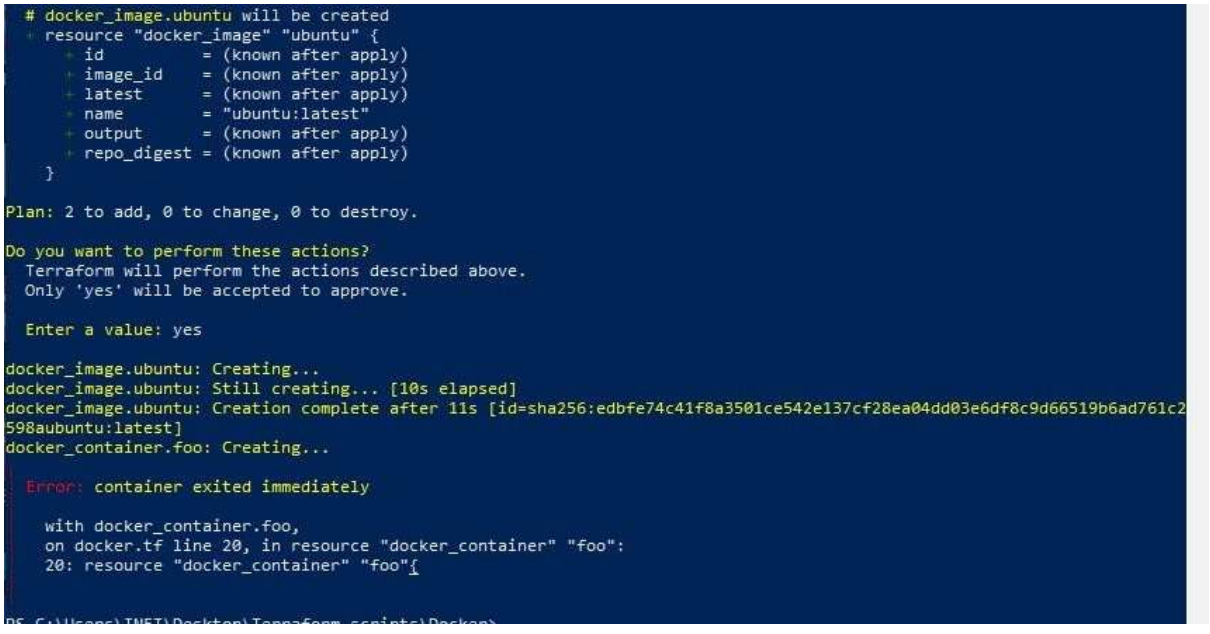
Step 6: Run the following script in the Atom Editor

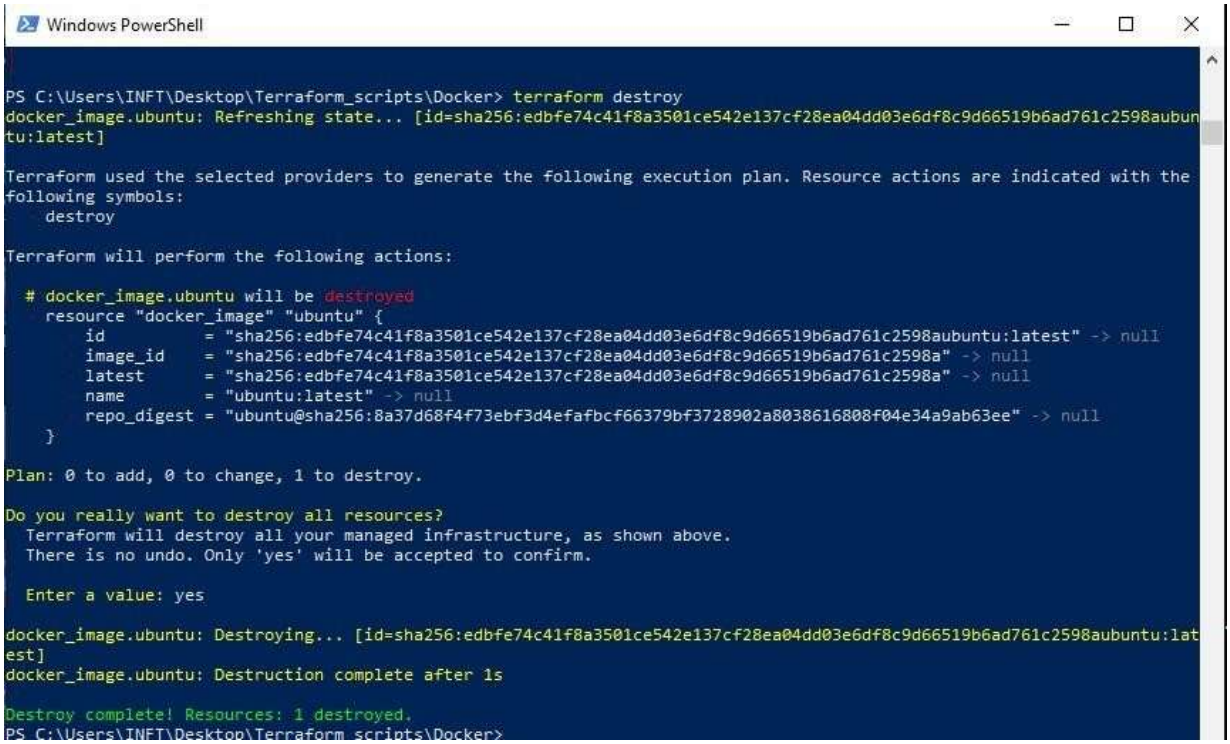


Step 7: Open Windows Explorer and run the following command terraform init, terraform plan, terraform apply, terraform destroy and docker images.




Windows PowerShell
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.
PS C:\Users\INFT\Desktop\Terraform_scripts\Docker> terraform apply
Terraform used the selected providers to generate the following execution plan. Resource actions are indicated with the following symbols:
+ create
Terraform will perform the following actions:
# docker_container.foo will be created
+ resource "docker_container" "foo" {
+ attach = false
+ bridge = (known after apply)
+ command = (known after apply)
+ container_logs = (known after apply)
+ entrypoint = (known after apply)
+ env = (known after apply)
+ exit_code = (known after apply)
+ gateway = (known after apply)
+ hostname = (known after apply)
+ id = (known after apply)
+ image = (known after apply)
+ init = (known after apply)
+ ip_address = (known after apply)
+ ip_prefix_length = (known after apply)
+ ipc_mode = (known after apply)
+ log_driver = (known after apply)
+ logs = false
+ must_run = true
+ name = "foo"
+ network_data = (known after apply)
+ read_only = false
+ remove_volumes = true
+ restart = "no"
+ rm = false
+ runtime = (known after apply)
+ security_opts = (known after apply)
+ shm_size = (known after apply)
+ start = true
+ stdin_open = false
+ stop_signal = (known after apply)
+ stop_timeout = (known after apply)
+ tty = false
+ healthcheck (known after apply)
+ labels (known after apply)


# docker_image.ubuntu will be created
+ resource "docker_image" "ubuntu" {
+ id = (known after apply)
+ image_id = (known after apply)
+ latest = (known after apply)
+ name = "ubuntu:latest"
+ output = (known after apply)
+ repo_digest = (known after apply)
}
Plan: 2 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
docker_image.ubuntu: Creating...
docker_image.ubuntu: Still creating... [10s elapsed]
docker_image.ubuntu: Creation complete after 11s [id=sha256:edbfe74c41f8a3501ce542e137cf28ea04dd03e6df8c9d66519b6ad761c2598aubuntu:latest]
docker_container.foo: Creating...
Error: container exited immediately
with docker_container.foo,
on docker.tf line 20, in resource "docker_container" "foo":
20: resource "docker_container" "foo"{


Windows PowerShell
PS C:\Users\INFT\Desktop\Terraform_scripts\Docker> terraform destroy
docker_image.ubuntu: Refreshing state... [id=sha256:edbfe74c41f8a3501ce542e137cf28ea04dd03e6df8c9d66519b6ad761c2598aubuntu:latest]
Terraform used the selected providers to generate the following execution plan. Resource actions are indicated with the following symbols:
destroy
Terraform will perform the following actions:
# docker_image.ubuntu will be destroyed
resource "docker_image" "ubuntu" {
id = "sha256:edbfe74c41f8a3501ce542e137cf28ea04dd03e6df8c9d66519b6ad761c2598aubuntu:latest" -> null
image_id = "sha256:edbfe74c41f8a3501ce542e137cf28ea04dd03e6df8c9d66519b6ad761c2598a" -> null
latest = "sha256:edbfe74c41f8a3501ce542e137cf28ea04dd03e6df8c9d66519b6ad761c2598a" -> null
name = "ubuntu:latest" -> null
repo_digest = "ubuntu@sha256:8a37d68f4f73ebf3d4efafbcf66379bf3728902a8038616808f04e34a9ab63ee" -> null
}
Plan: 0 to add, 0 to change, 1 to destroy.
Do you really want to destroy all resources?
Terraform will destroy all your managed infrastructure, as shown above.
There is no undo. Only 'yes' will be accepted to confirm.
Enter a value: yes
docker_image.ubuntu: Destroying... [id=sha256:edbfe74c41f8a3501ce542e137cf28ea04dd03e6df8c9d66519b6ad761c2598aubuntu:latest]
docker_image.ubuntu: Destruction complete after 1s
Destroy complete! Resources: 1 destroyed.
PS C:\Users\INFT\Desktop\Terraform_scripts\Docker>


Windows PowerShell
PS C:\Users\INFT\Desktop\Terraform_scripts\Docker> docker images
REPOSITORY TAG IMAGE ID CREATED SIZE
PS C:\Users\INFT\Desktop\Terraform_scripts\Docker>

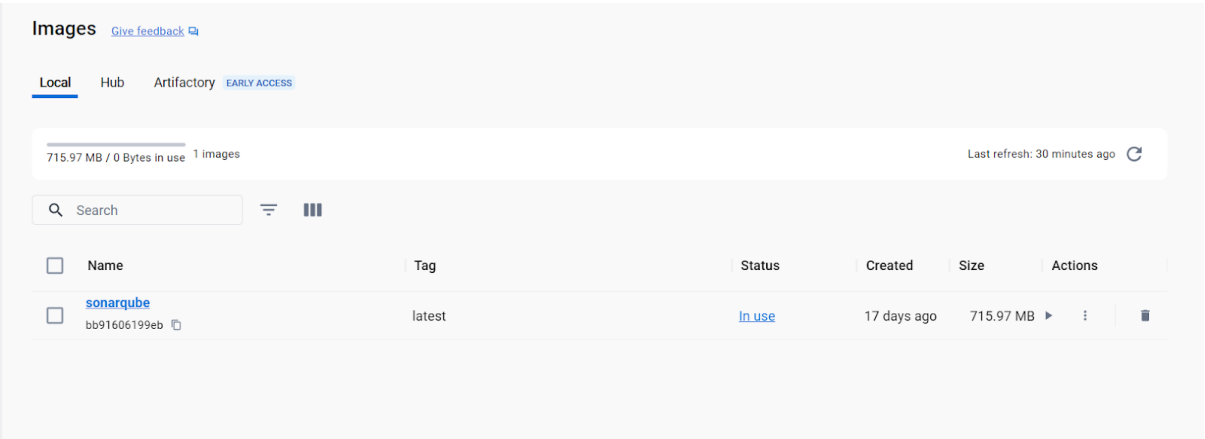
Experiment No 7

Vedant Sanap
D15A 48
Batch C

AIM: Installing SonarQube from the Docker Image

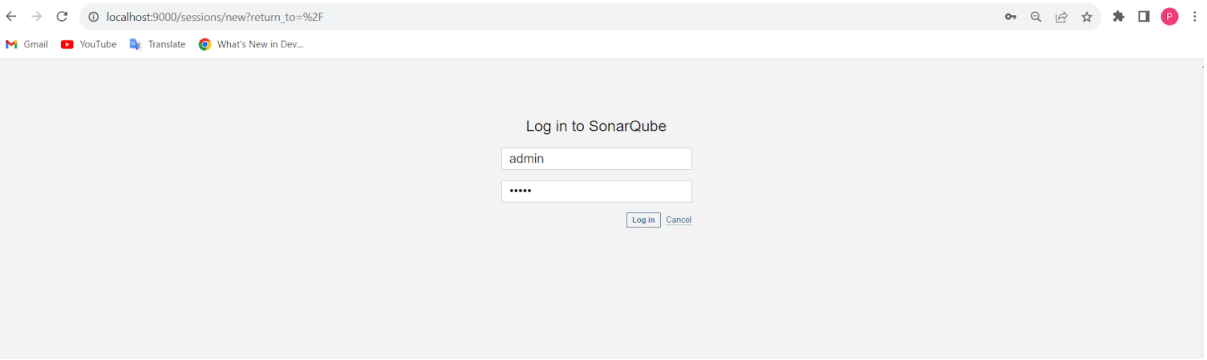
$ docker run -d --name sonarqube -e SONAR_ES_BOOTSTRAP_CHECKS_DISABLE=true -p 9000:9000
Sonarqube:latest

```
PS D:\Desktop\DockerFile> docker run -d --name sonarqube -e SONAR_ES_BOOTSTRAP_CHECKS_DISABLE=true -p 9000:9000 sonarqub
e:latest
Unable to find image 'sonarqube:latest' locally
latest: Pulling from library/sonarqube
44ba2882f8eb: Pull complete
2cabec57fa36: Pull complete
c20481384b6a: Pull complete
bf7b17ee74f8: Pull complete
38617faac714: Pull complete
b795b715553d: Pull complete
c5244f6c9231: Pull complete
Digest: sha256:1ffd122cfb37ce982289dc7f5d38bb702ba05af7b5a50f7cb077ae25e60b5b9a
Status: Downloaded newer image for sonarqube:latest
1442c4e613b25aaedec05c060f020a00802b1c6dbaa27e8c5c0dad4ed8fc1f76
```

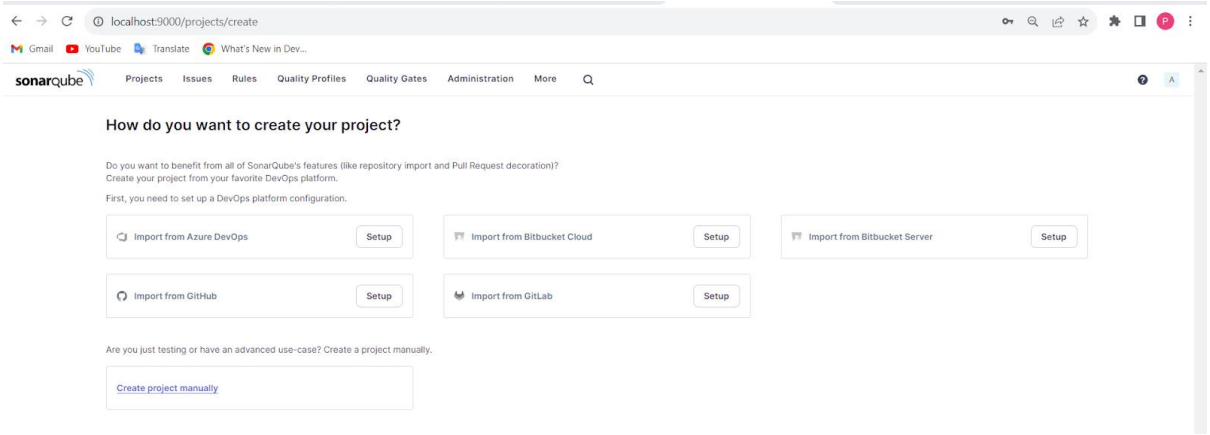


go to the SonarQube page by typing:
http://localhost:9000/ on your browser.

Installation is successful if you see this page

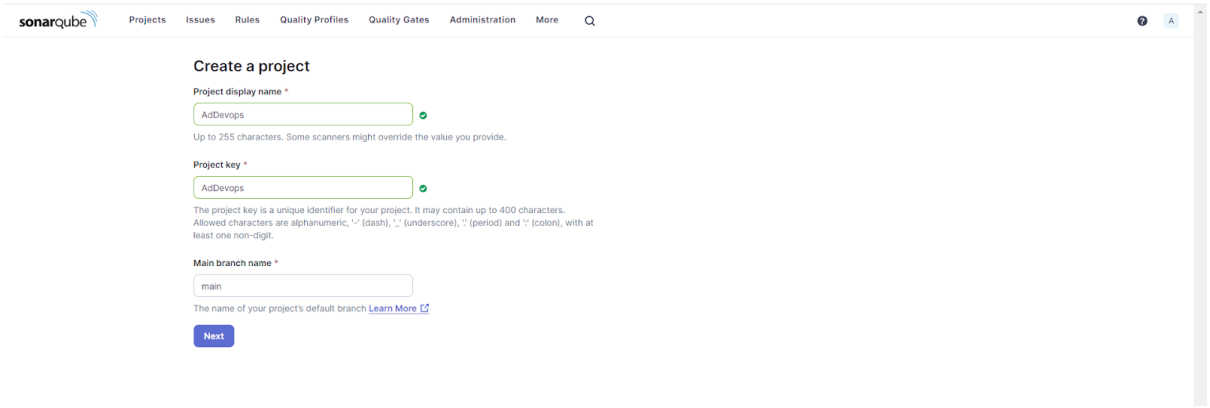


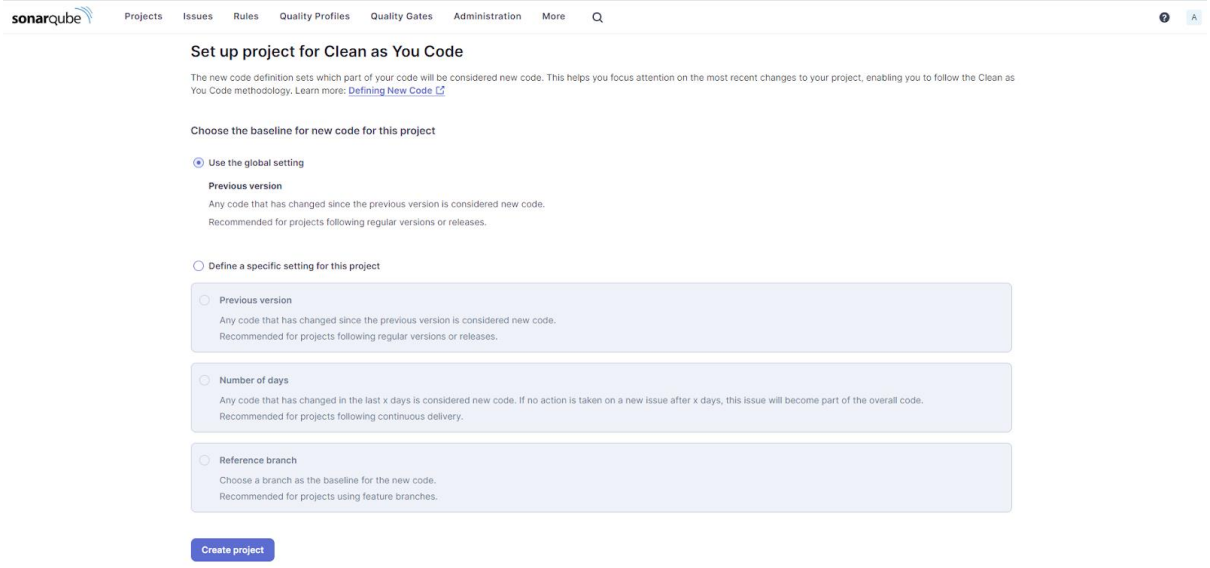
Update to new password



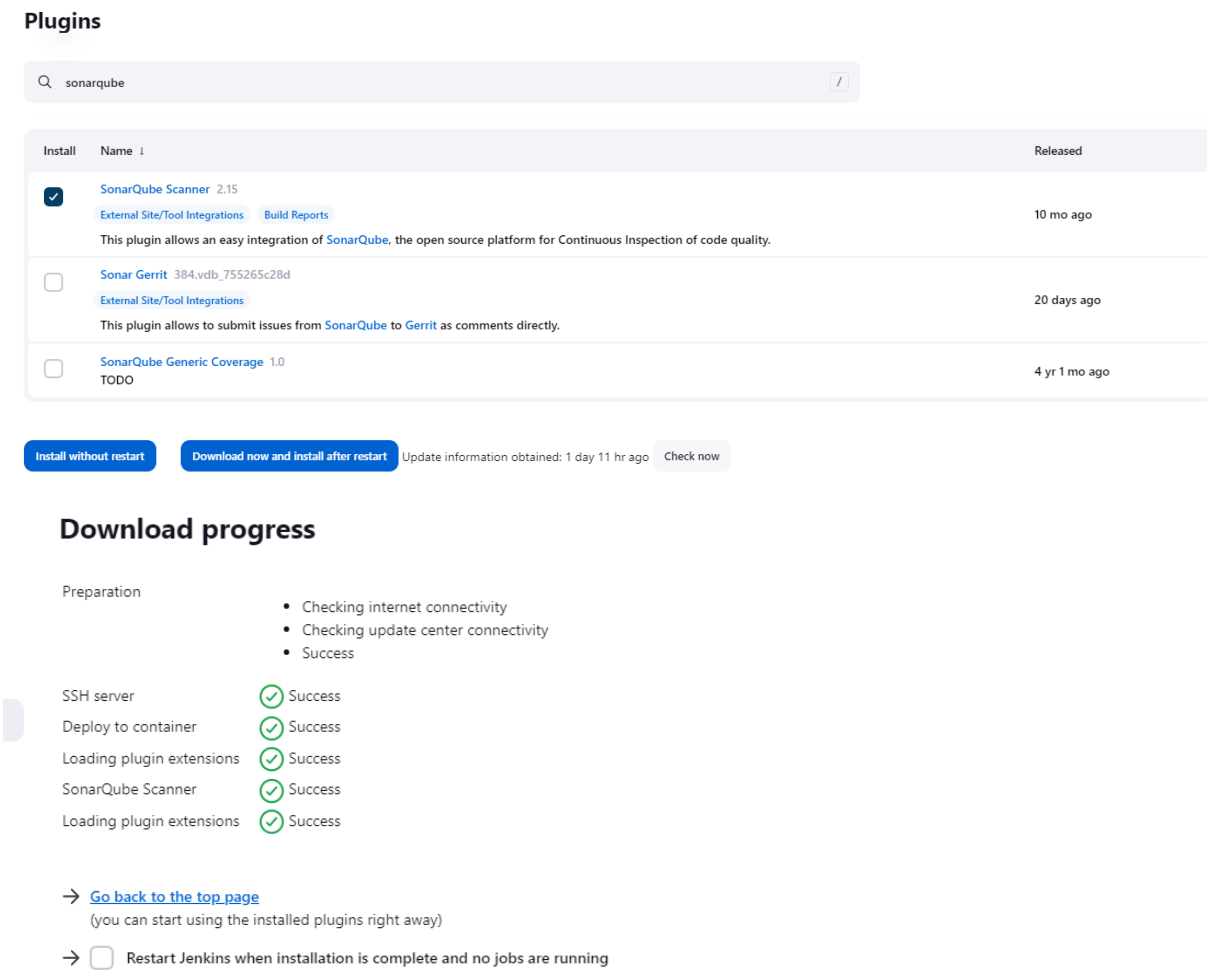
Create project manually:

Here project name is “AdDevops”

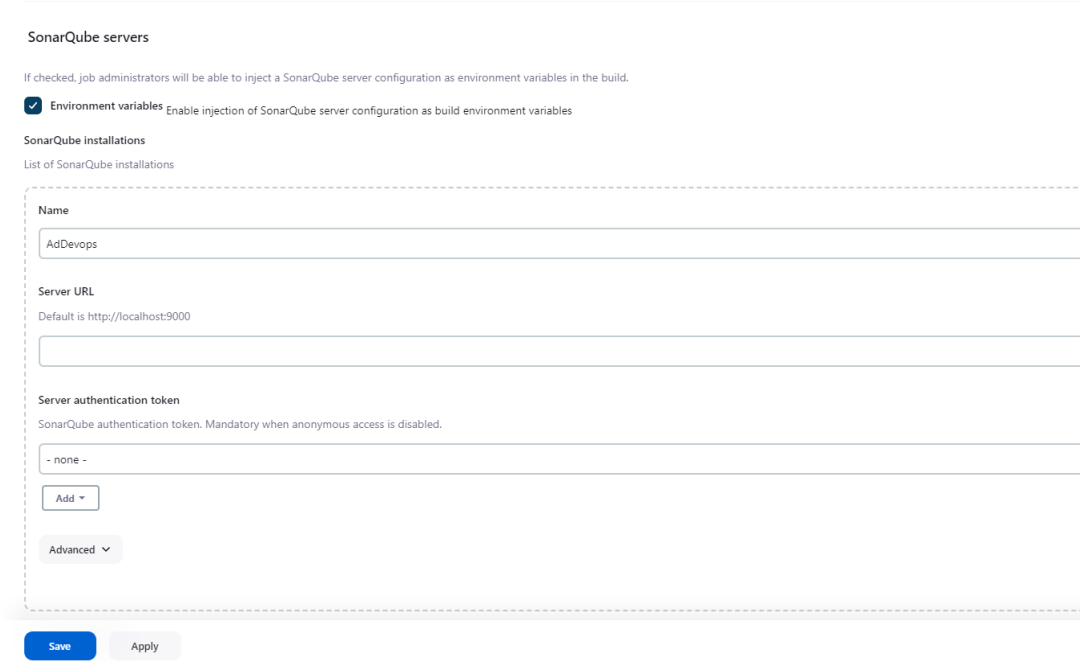




open Jenkins
Go to Dashboard ->Manage Jenkins -> Plugin Manager and search for
SonarQube Scanner under Available plugins for Jenkins and install without restart.

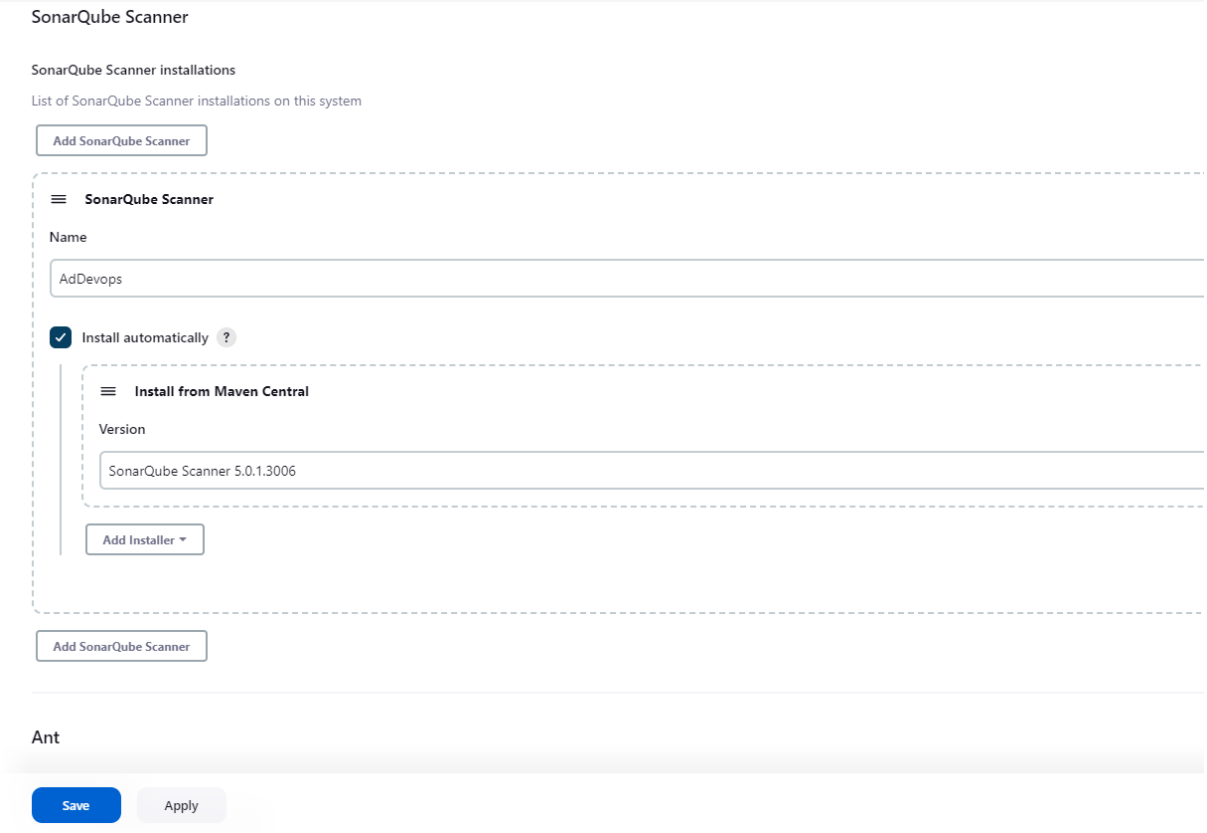


Under Jenkins ,
Dashboard -> Manage Jenkins -> Configure System ,
Look for SonarQube Servers and enter the details. Enter the Server Authentication Token if needed.

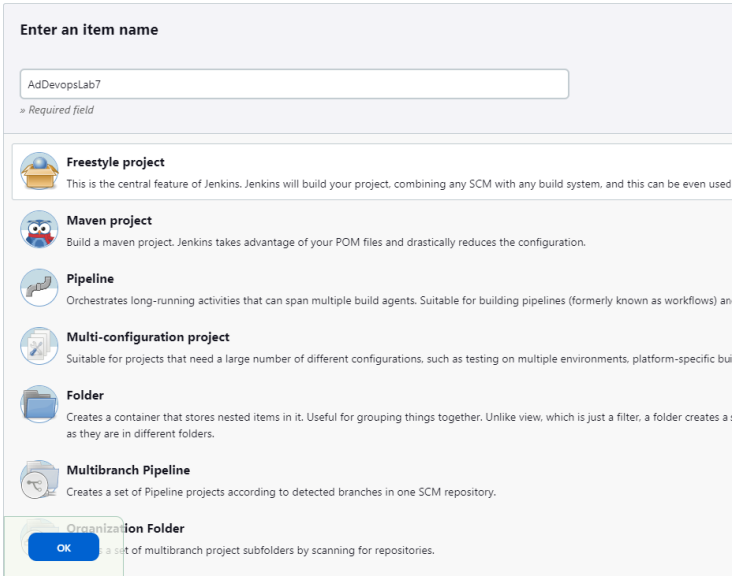


Search SonarQube Scanner under Dashboard -> Manage Jenkins -> Global Tool Configuration.

Choose the latest configuration and choose Install Automatically.

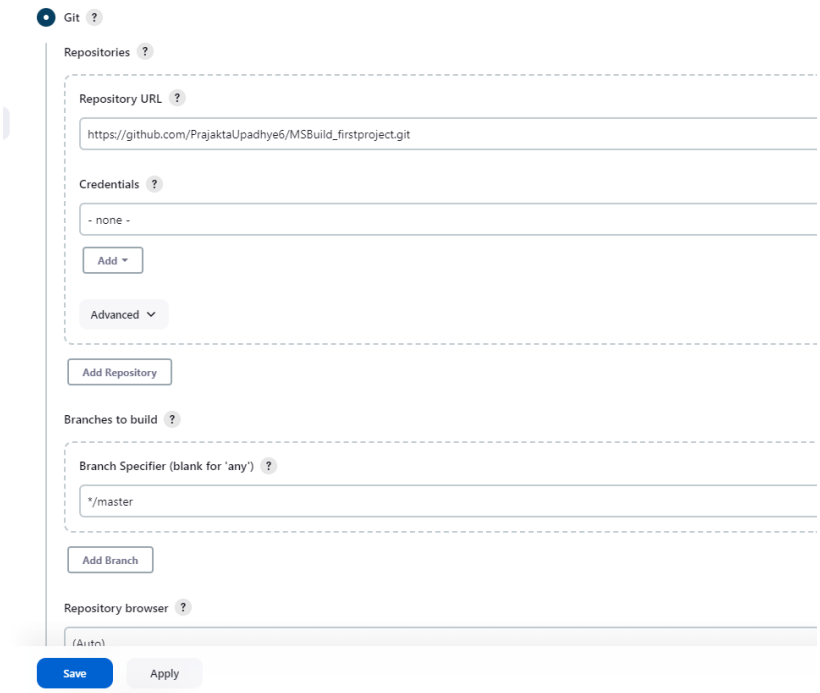


create a New Item in Jenkins, choose a freestyle project.

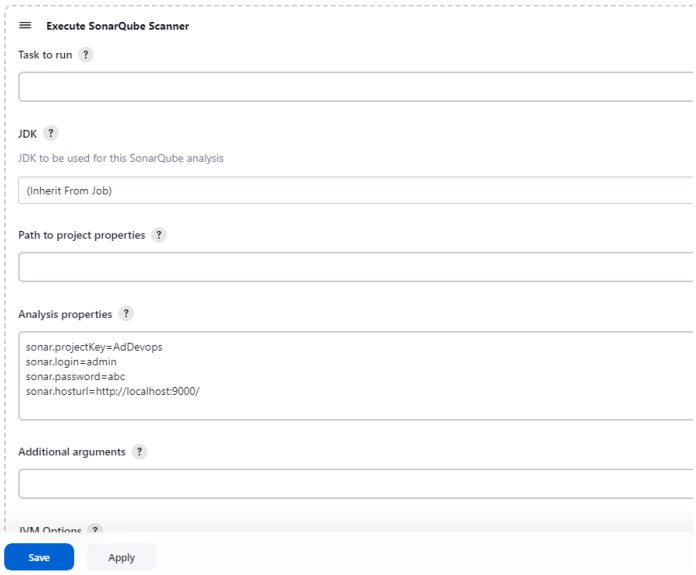


Choose this GitHub repository in Source Code Management.
https://github.com/shazforiot/MSBuild_firstproject.git

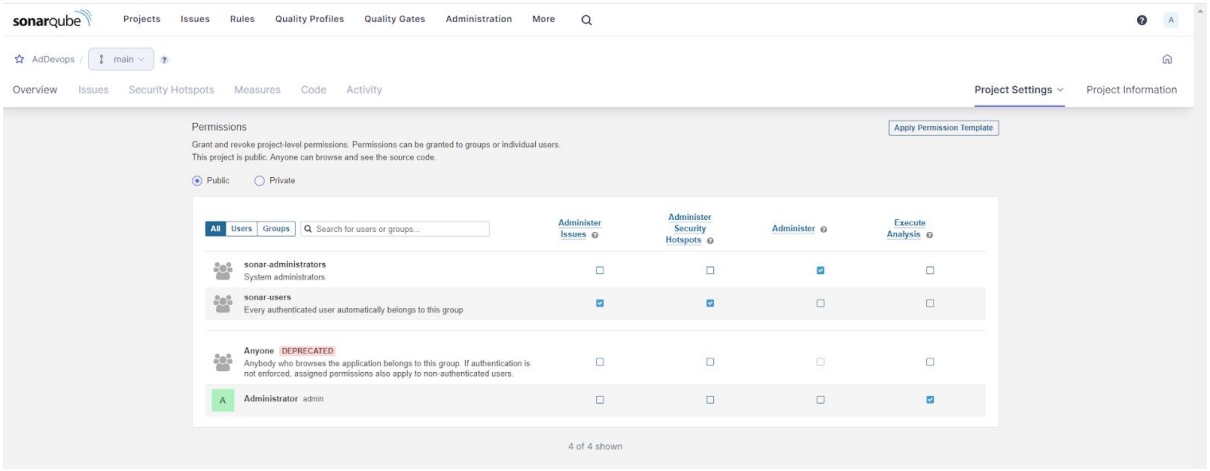
Under Build ->Execute SonarQube Scanner, enter these Analysis properties. Mention the SonarQube Project Key, Login, Password, and Host URL.
sonar.projectKey=AdDevops
sonar.login=admin
sonar.password=abc
sonar.hosturl=http://localhost:9000/



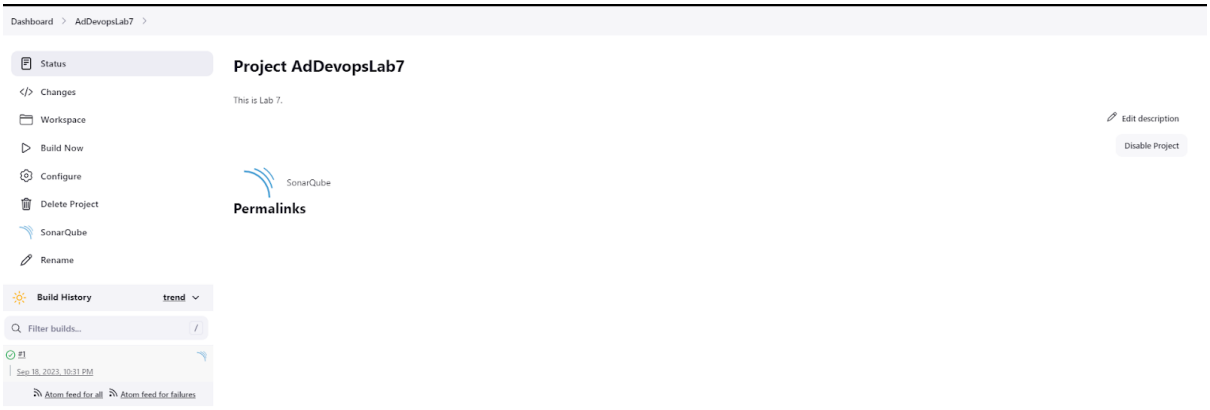
Build Steps

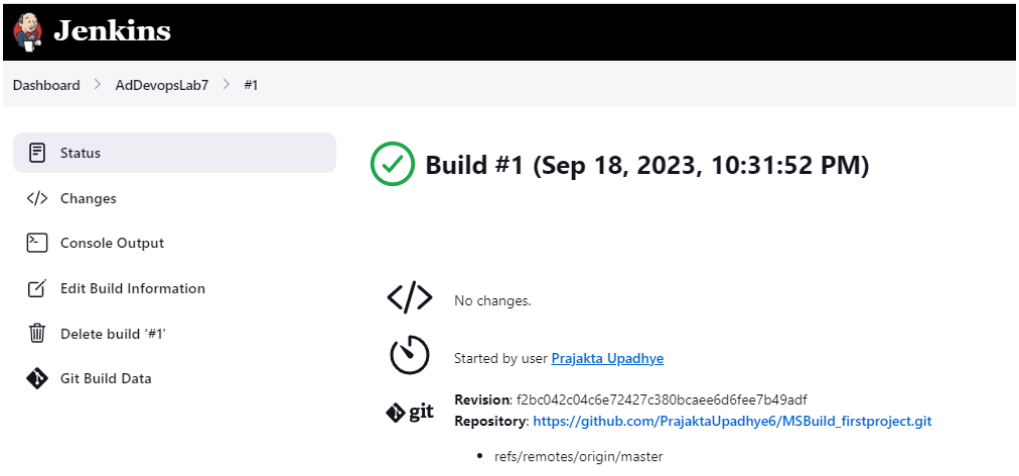


Go to http://localhost:9000/ and enter your previously created username.
Go to Permissions and grant the Admin user Execute Permissions.

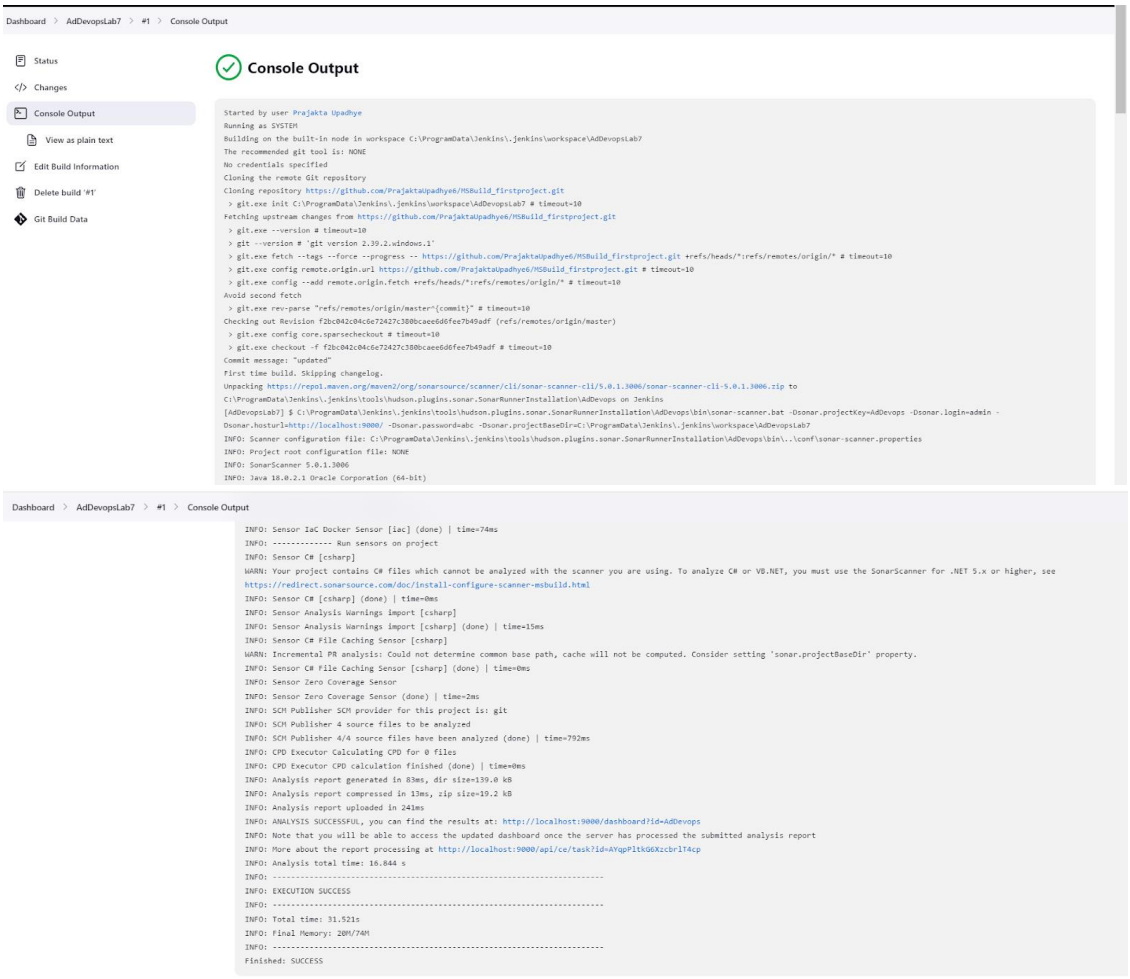


Build and Run:

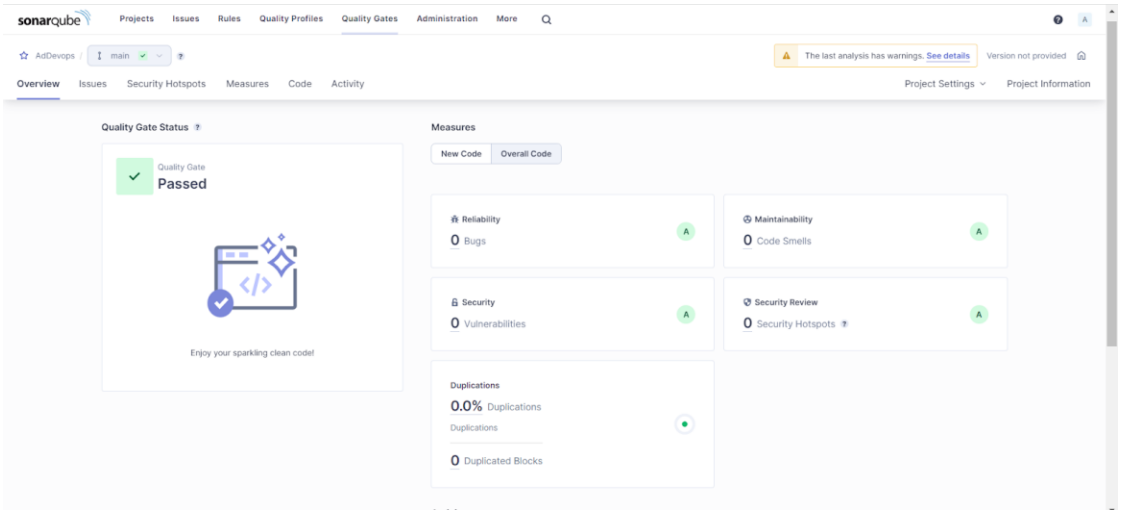




Console Output:



Project on sonarqube:



Conclusion: Thus, we have successfully installed SonarQube from Docker image.

Experiment No 8

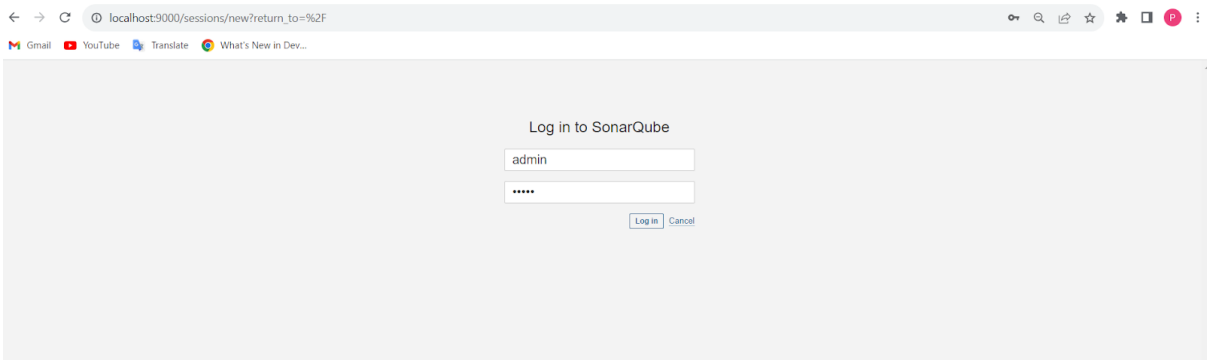
Vedant Sanap
D15A 48
Batch C

AIM: Integrating Jenkins with SonarQube.

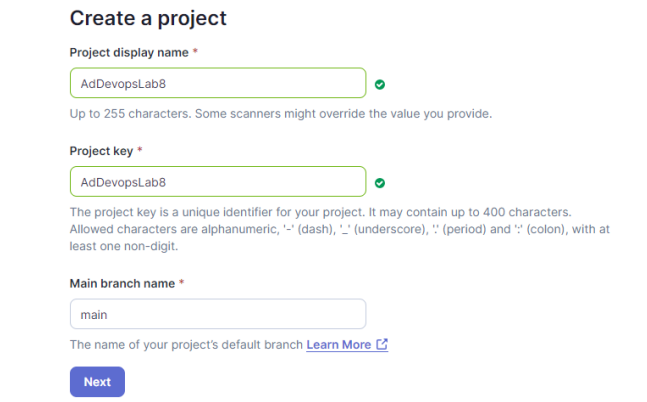
Open up Jenkins Dashboard on localhost, port 8080
Run SonarQube in a Docker container using this command -
$ docker run -d --name sonarqube -e SONAR_ES_BOOTSTRAP_CHECKS_DISABLE=true -p 9000:9000
sonarqube:latest

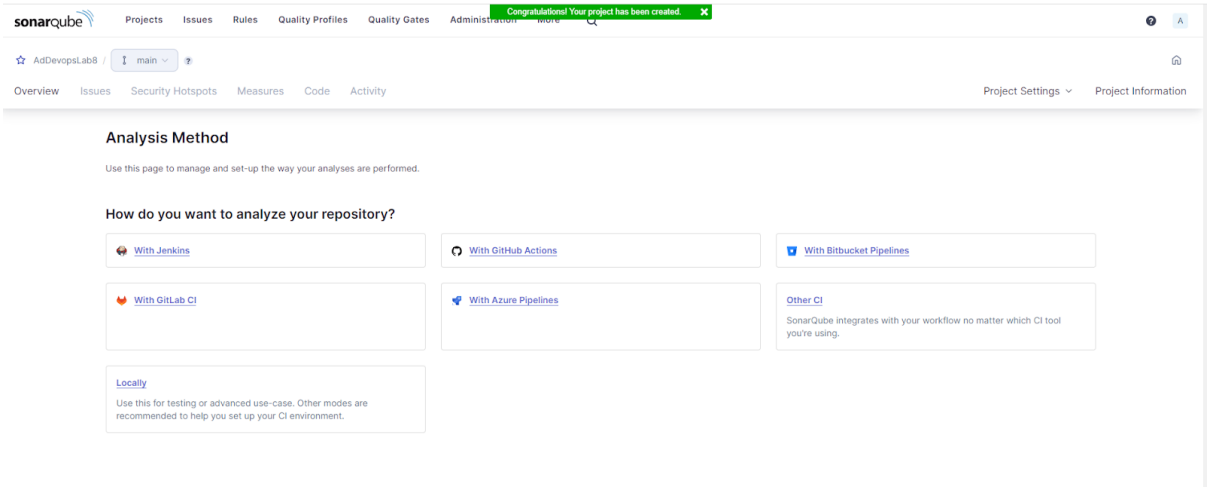
```
PS D:\Desktop\DockerFile> docker run -d --name sonarqube -e SONAR_ES_BOOTSTRAP_CHECKS_DISABLE=true -p 9000:9000 sonarqub
e:latest
Unable to find image 'sonarqube:latest' locally
latest: Pulling from library/sonarqube
44ba2882f8eb: Pull complete
2cabec57fa36: Pull complete
c20481384b6a: Pull complete
bf7b17ee74f8: Pull complete
38617faac714: Pull complete
b795b715553d: Pull complete
c5244f6c9231: Pull complete
Digest: sha256:1ffd122cfb37ce982289dc7f5d38bb702ba05af7b5a50f7cb077ae25e60b5b9a
Status: Downloaded newer image for sonarqube:latest
1442c4e613b25aaedec05c060f020a00802b1c6dbaa27e8c5c0dad4ed8fc1f76
```

sonarqube

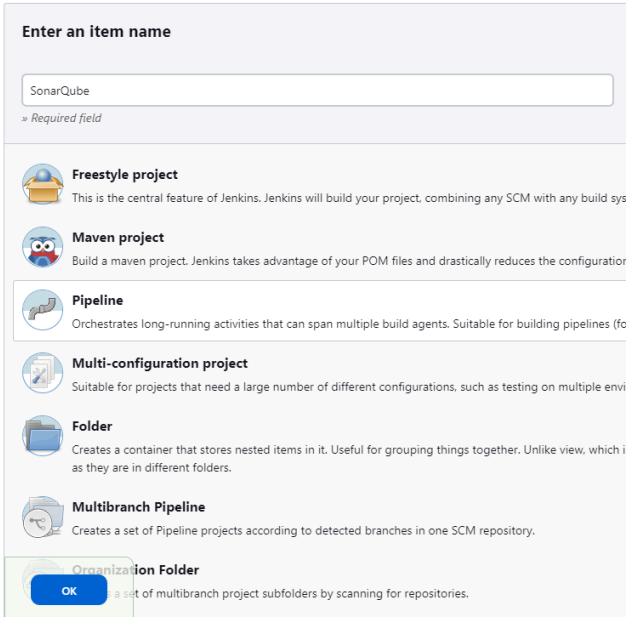


Create project manually





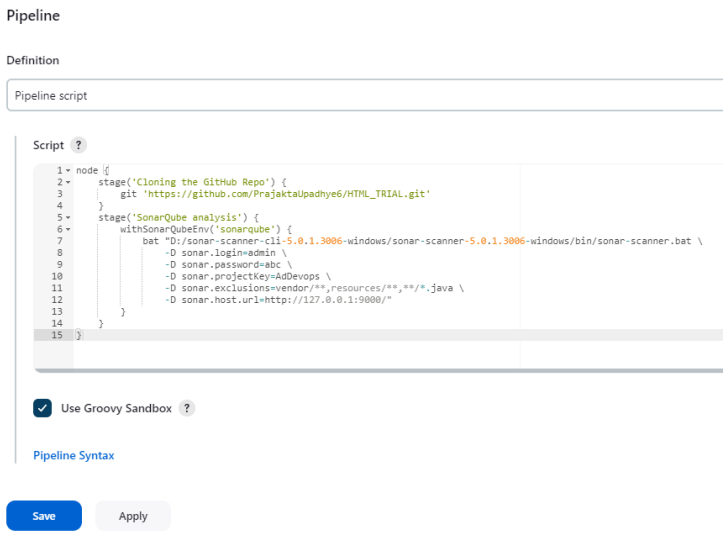
In Jenkins create a pipeline here named “SonarQube”



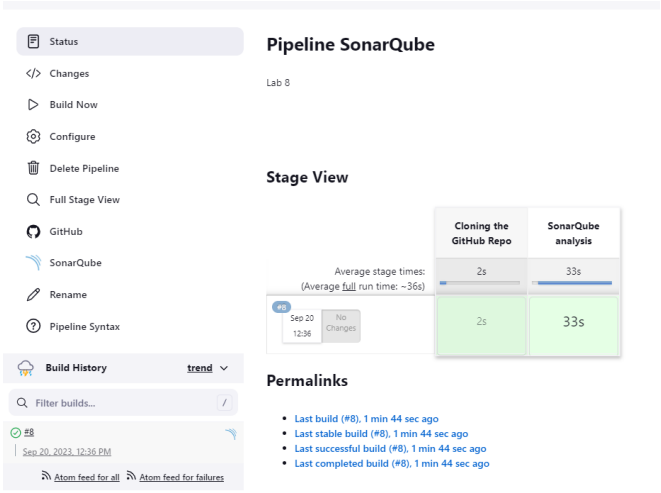
Enter the following in pipeline script:

```
node {
   stage('Cloning the GitHub Repo') {
      git 'https://github.com/PrajaktaUpadhye6/MSBuild_firstproject.git'
   }
   stage('SonarQube analysis') {
      withSonarQubeEnv('sonarqube') {
         bat "D:/sonar-scanner-cli-5.0.1.3006-windows/sonar-scanner-5.0.1.3006-
windows/bin/sonar-scanner.bat \
            -D sonar.login=admin \
            -D sonar.password=abc \
            -D sonar.projectKey=AdDevops \
            -D sonar.exclusions=vendor/**,resources/**,**/*.java \
            -D sonar.host.url=http://127.0.0.1:9000/"
      }
```

```
    }
}
```

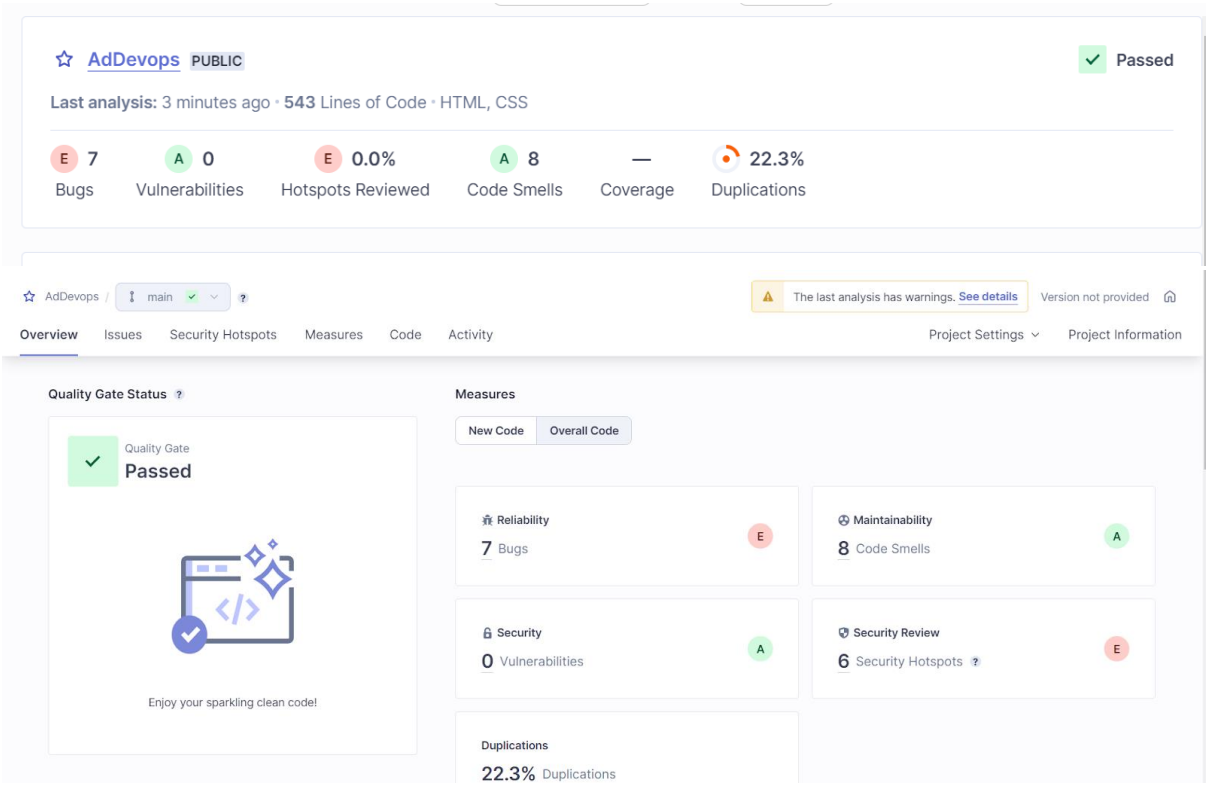


It is a java sample project which has a lot of repetitions and issues that will be detected by SonarQube.
Build and run:

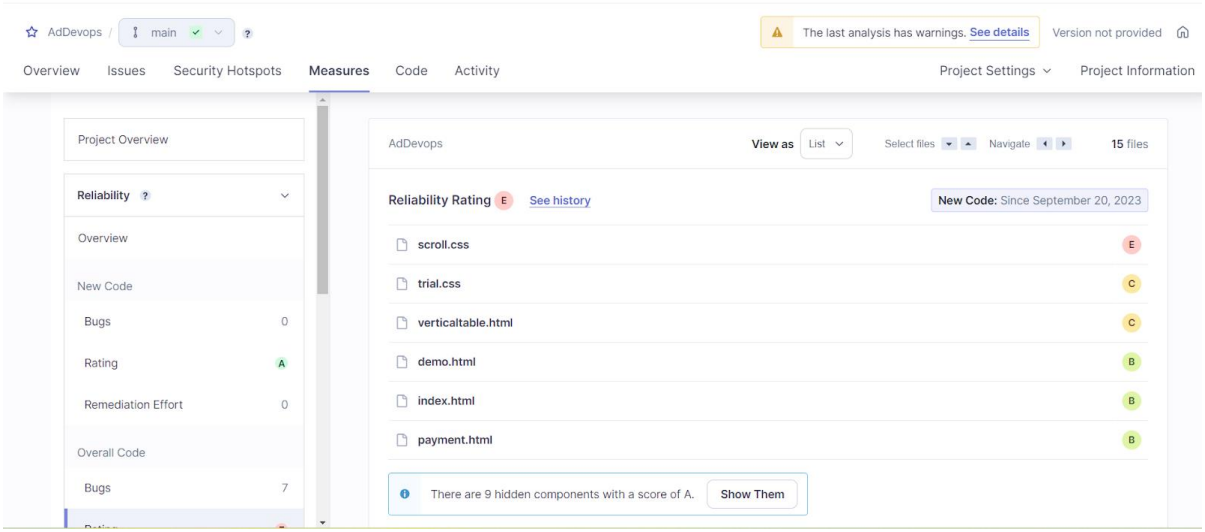


Console output:

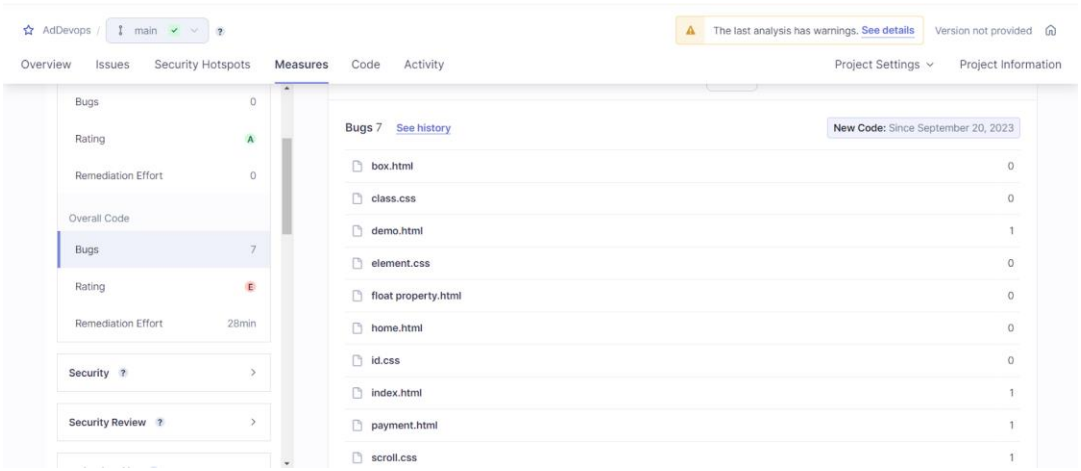
sonarqube:



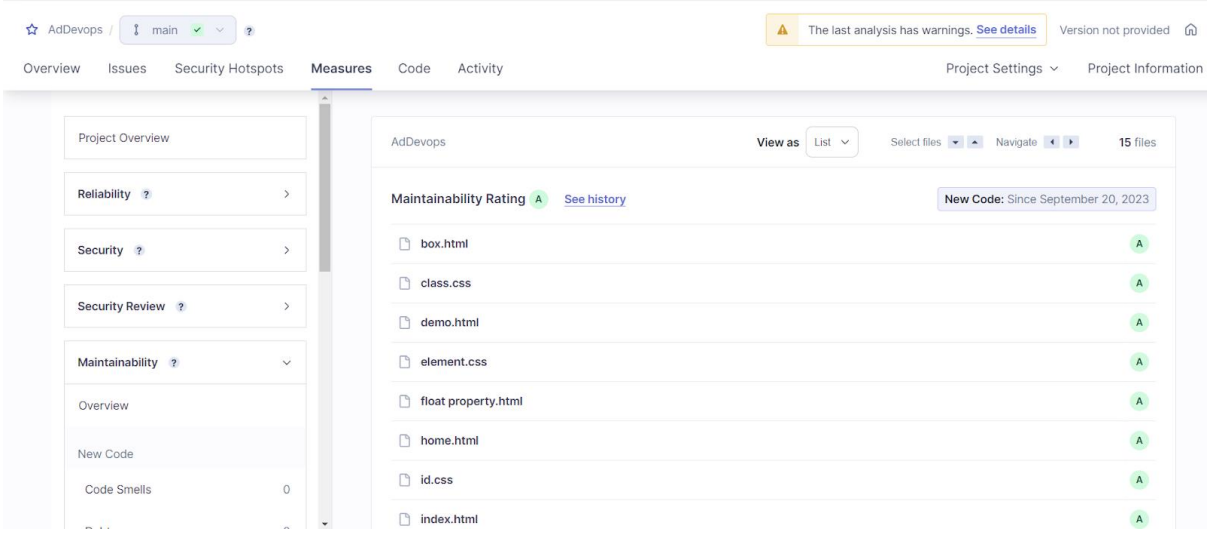
Reliability:



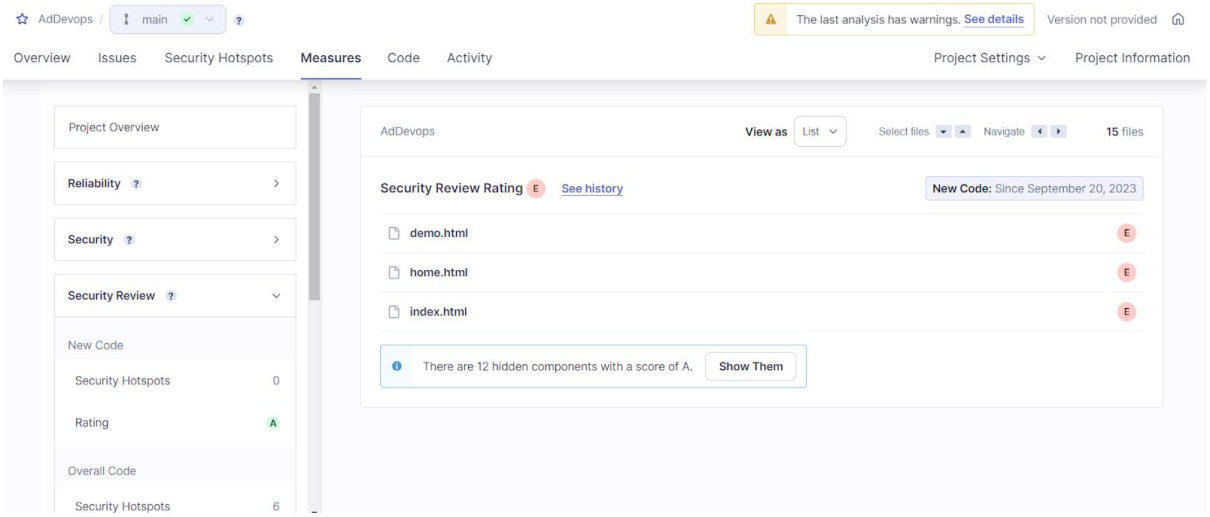
Bugs:



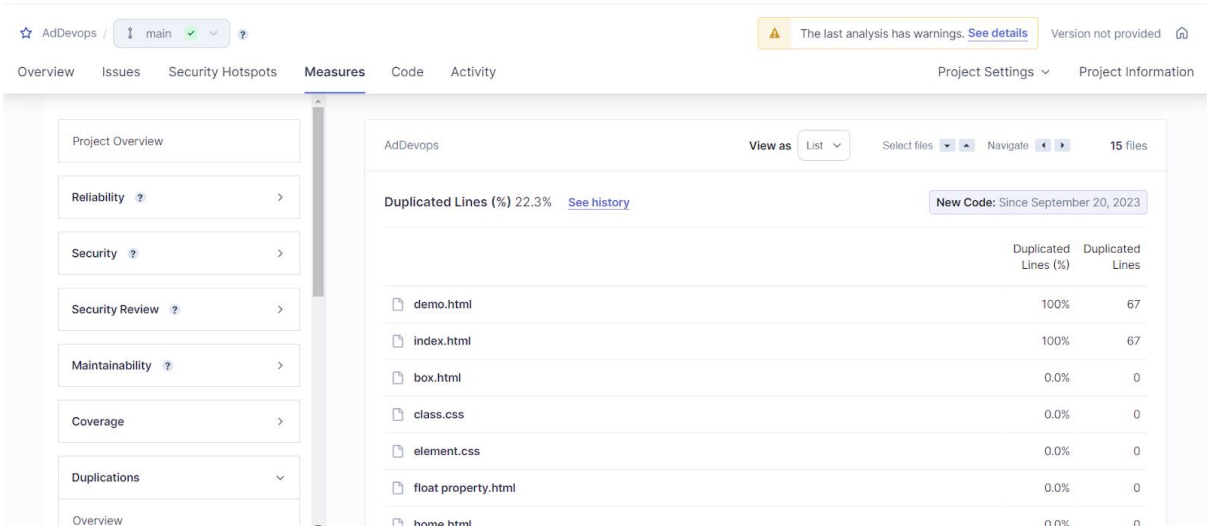
Maintanaibility:



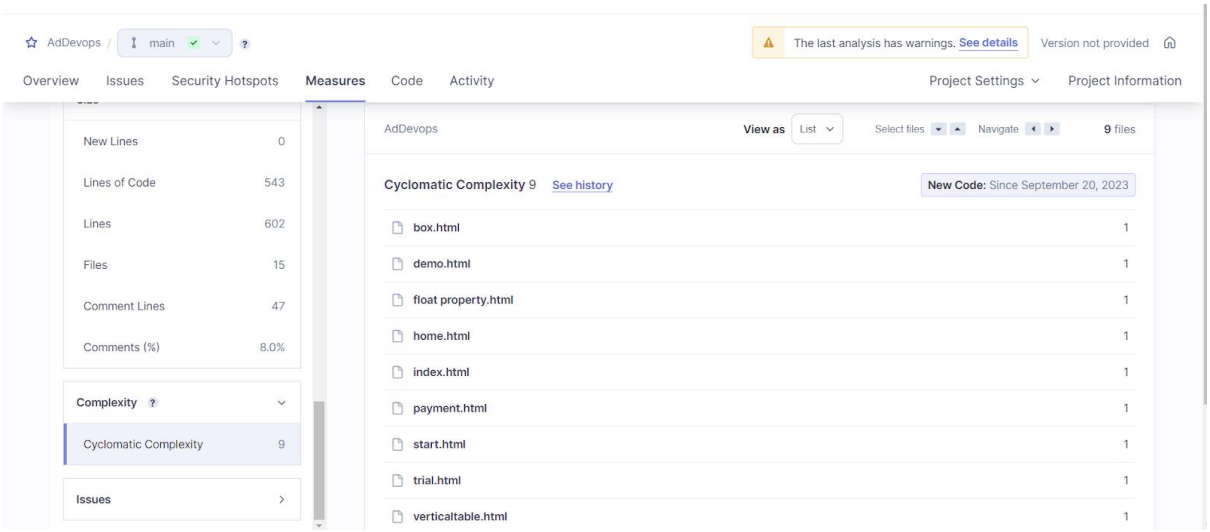
Security:



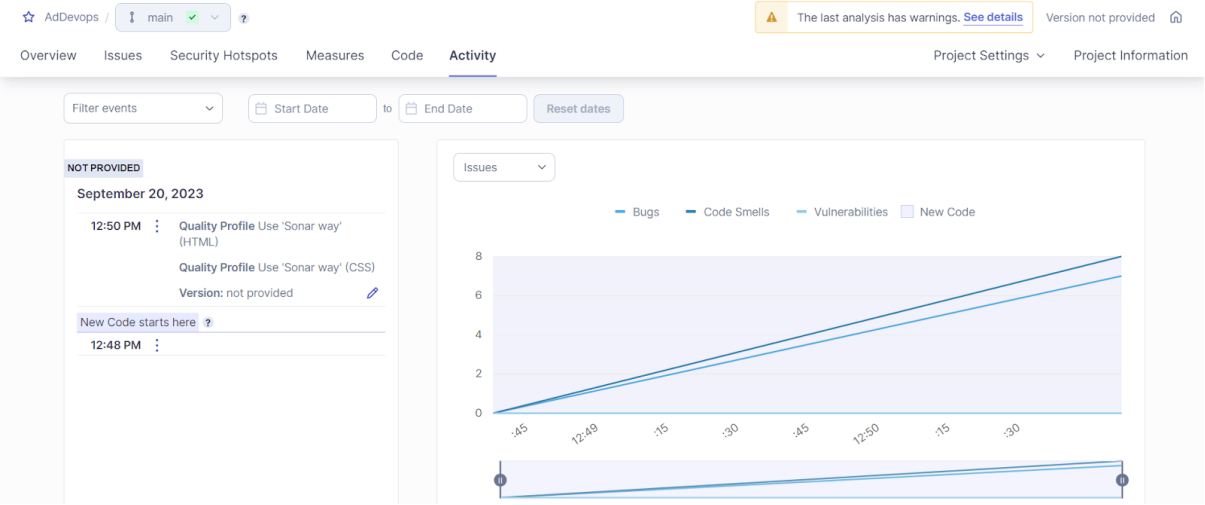
Duplications:



Cyclomatic complexity:



Activity:



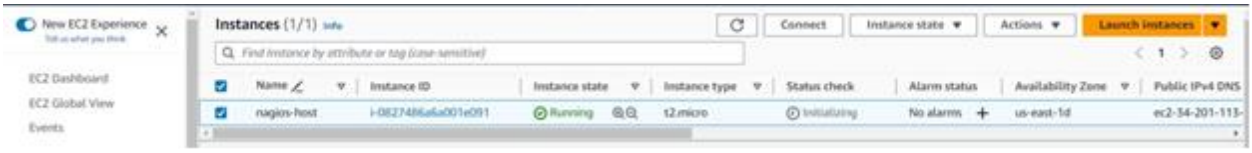
Conclusion: Thus, we have successfully integrated Jenkins with SonarQube.

Experiment No 9

Vedant Sanap
D15A 48
Batch C

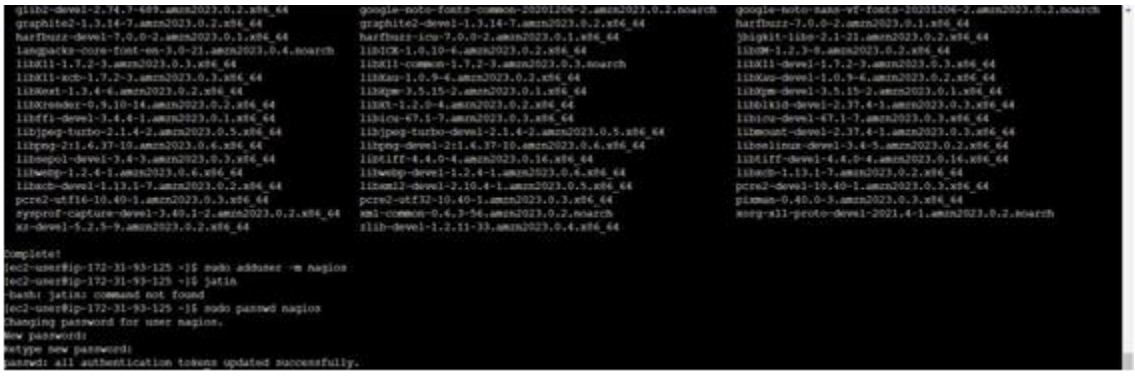
AIM: To Understand Continuous monitoring and Installation and configuration of Nagios Core, Nagios Plugins and NRPE (Nagios Remote Plugin Executor) on Linux Machine.

1)

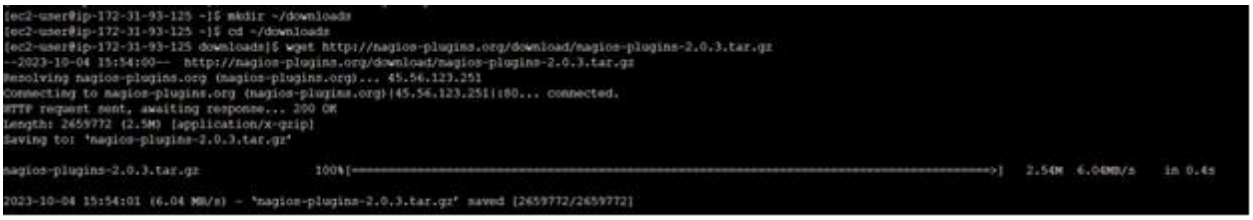


2)

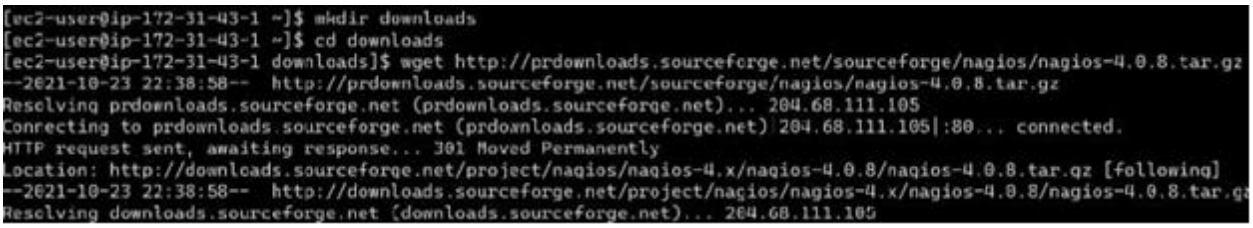
3)



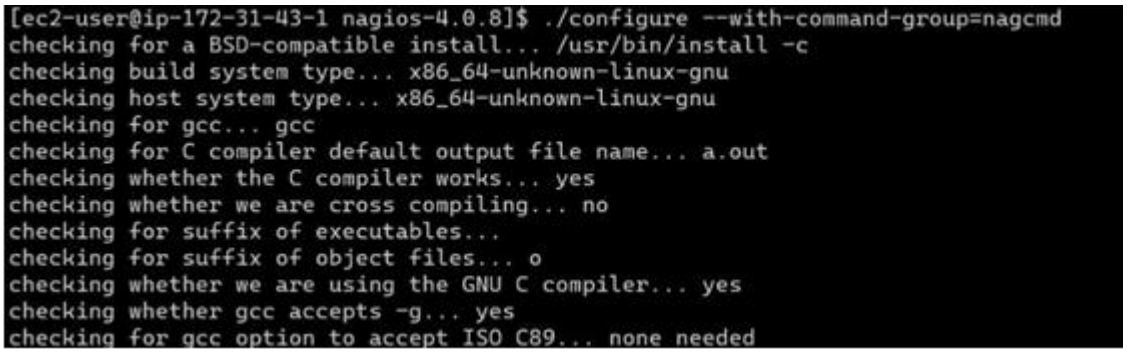
4)


[ec2-user@ip-172-31-93-125 ~]$ mkdir ~/downloads
[ec2-user@ip-172-31-93-125 ~]$ cd ~/downloads
[ec2-user@ip-172-31-93-125 downloads]$ wget http://nagios-plugins.org/download/nagios-plugins-2.0.3.tar.gz
--2023-10-04 15:54:00-- http://nagios-plugins.org/download/nagios-plugins-2.0.3.tar.gz
Resolving nagios-plugins.org (nagios-plugins.org)... 45.56.123.251
Connecting to nagios-plugins.org (nagios-plugins.org)|45.56.123.251|:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 2659772 (2.5M) [application/x-gzip]
Saving to: 'nagios-plugins-2.0.3.tar.gz'
nagios-plugins-2.0.3.tar.gz 100%[==========>] 2.54M 6.04MB/s in 0.4s
2023-10-04 15:54:01 (6.04 MB/s) - 'nagios-plugins-2.0.3.tar.gz' saved [2659772/2659772]

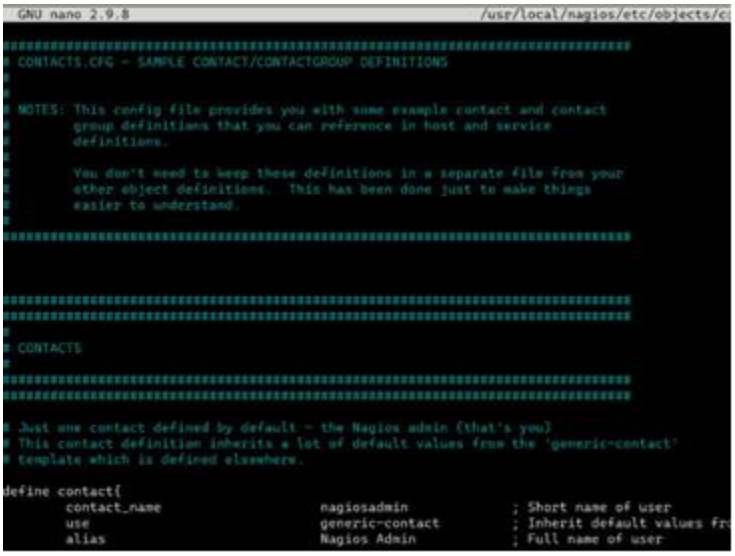
5)


[ec2-user@ip-172-31-43-1 ~]$ mkdir downloads
[ec2-user@ip-172-31-43-1 ~]$ cd downloads
[ec2-user@ip-172-31-43-1 downloads]$ wget http://prdownloads.sourceforge.net/sourceforge/nagios/nagios-4.0.8.tar.gz
--2021-10-23 22:38:58-- http://prdownloads.sourceforge.net/sourceforge/nagios/nagios-4.0.8.tar.gz
Resolving prdownloads.sourceforge.net (prdownloads.sourceforge.net)... 204.68.111.105
Connecting to prdownloads.sourceforge.net (prdownloads.sourceforge.net)|204.68.111.105|:80... connected.
HTTP request sent, awaiting response... 301 Moved Permanently
Location: http://downloads.sourceforge.net/project/nagios/nagios-4.x/nagios-4.0.8/nagios-4.0.8.tar.gz [following]
--2021-10-23 22:38:58-- http://downloads.sourceforge.net/project/nagios/nagios-4.x/nagios-4.0.8/nagios-4.0.8.tar.gz
Resolving downloads.sourceforge.net (downloads.sourceforge.net)... 204.68.111.105

6)


[ec2-user@ip-172-31-43-1 nagios-4.0.8]$ ./configure --with-command-group=nagcmd
checking for a BSD-compatible install... /usr/bin/install -c
checking build system type... x86_64-unknown-linux-gnu
checking host system type... x86_64-unknown-linux-gnu
checking for gcc... gcc
checking for C compiler default output file name... a.out
checking whether the C compiler works... yes
checking whether we are cross compiling... no
checking for suffix of executables...
checking for suffix of object files... o
checking whether we are using the GNU C compiler... yes
checking whether gcc accepts -g... yes
checking for gcc option to accept ISO C89... none needed

7)


GNU nano 2.9.8 /usr/local/nagios/etc/objects/c
# CONTACTS.CFG - SAMPLE CONTACT/CONTACTGROUP DEFINITIONS
# NOTES: This config file provides you with some example contact and contact
# group definitions that you can reference in host and service
# definitions.
# You don't need to keep these definitions in a separate file from your
# other object definitions. This has been done just to make things
# easier to understand.
# CONTACTS
# Just one contact defined by default - the Nagios admin (that's you)
# This contact definition inherits a lot of default values from the 'generic-contact'
# template which is defined elsewhere.
define contact{
contact_name nagiosadmin ; Short name of user
use generic-contact ; Inherit default values fr
alias Nagios Admin ; Full name of user

8)

```
*** Support Notes *****************************************

If you have questions about configuring or running Nagios,
please make sure that you:

     - Look at the sample config files
     - Read the documentation on the Nagios Library at:
          http://library.nagios.com

before you post a question to one of the mailing lists.
Also make sure to include pertinent information that could
help others help you.  This might include:

     - What version of Nagios you are using
     - What version of the plugins you are using
     - Relevant snippets from your config files
     - Relevant error messages from the Nagios log file

For more information on obtaining support for Nagios, visit:

       http://support.nagios.com

************************************************************

Enjoy.

[ec2-user@ip-172-31-43-1 nagios-4.0.8]$
```

9)

```
[ec2-user@ip-172-31-46-218 nagios-4.0.8]$ sudo make install-webconf
/usr/bin/install -c -m 644 sample-config/httpd.conf /etc/httpd/conf.d/nagios.conf

*** Nagios/Apache conf file installed ***
```

10)

```
[ec2-user@ip-172-31-46-218 nagios-4.0.8]$ sudo htpasswd -c /usr/local/nagios/etc/htpasswd.users nagiosadmin
New password:
Re-type new password:
Adding password for user nagiosadmin
[ec2-user@ip-172-31-46-218 nagios-4.0.8]$
```

11)

```
[ec2-user@ip-172-31-46-218 ~]$ cd ~/downloads/
[ec2-user@ip-172-31-46-218 downloads]$ tar zxvf nagios-plugins-2.0.3.tar.gz
```

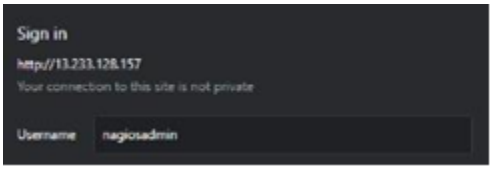
12)

```
2-user@ip-172-31-46-218 ~]$ sudo service nagios start
rting nagios (via systemctl):                              [  OK  ]
2-user@ip-172-31-46-218 ~]$
```

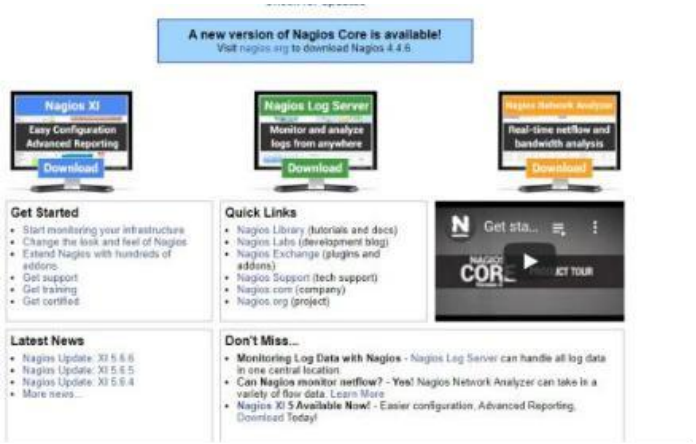
13)

```
[ec2-user@ip-172-31-46-218 ~]$ sudo systemctl status nagios
● nagios.service - LSB: Starts and stops the Nagios monitoring server
   Loaded: loaded (/etc/rc.d/init.d/nagios; bad; vendor preset: disabled)
   Active: active (running) since Sun 2021-10-24 08:05:00 UTC; 1min 21s ago
     Docs: man:systemd-sysv-generator(8)
  Process: 30073 ExecStart=/etc/rc.d/init.d/nagios start (code=exited, status
   CGroup: /system.slice/nagios.service
           ├─30094 /usr/local/nagios/bin/nagios -d /usr/local/nagios/etc/nagi
           ├─30096 /usr/local/nagios/bin/nagios --worker /usr/local/nagios/va
           ├─30097 /usr/local/nagios/bin/nagios --worker /usr/local/nagios/va
           ├─30098 /usr/local/nagios/bin/nagios --worker /usr/local/nagios/va
           ├─30099 /usr/local/nagios/bin/nagios --worker /usr/local/nagios/va
           └─30100 /usr/local/nagios/bin/nagios -d /usr/local/nagios/etc/nagi
```

14)



15)



Conclusion: Thus, we have understood continuous monitoring and Installation and configuration of Nagios Core, Nagios Plugins and NRPE (Nagios Remote Plugin Executor) on Linux Machine.

Experiment No 10

Vedant Sanap
D15A 48
Batch C

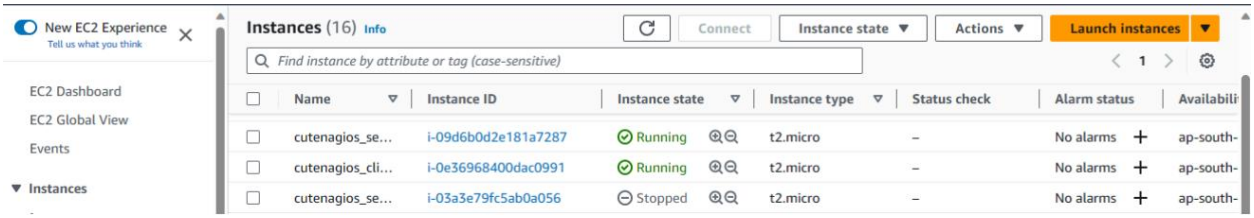
AIM: To perform Port, Service monitoring, Windows/Linux server monitoring using Nagios.

Output-

Step 1: To Confirm that Nagios is running on the server side, run this sudo systemctl status nagios on the “NAGIOS HOST”.

```
● nagios.service - Nagios Core 4.4.14
     Loaded: loaded (/lib/systemd/system/nagios.service; enabled; vendor preset: enabled)
     Active: active (running) since Sat 2023-09-30 08:54:01 UTC; 20s ago
       Docs: https://www.nagios.org/documentation
    Process: 55285 ExecStartPre=/usr/local/nagios/bin/nagios -v /usr/local/nagios/etc/nagios.cfg (code=exited, status=0/SUCCESS)
    Process: 55286 ExecStart=/usr/local/nagios/bin/nagios -d /usr/local/nagios/etc/nagios.cfg (code=exited, status=0/SUCCESS)
   Main PID: 55287 (nagios)
      Tasks: 6 (limit: 1141)
     Memory: 5.3M
        CPU: 252ms
     CGroup: /system.slice/nagios.service
             ├─55287 /usr/local/nagios/bin/nagios -d /usr/local/nagios/etc/nagios.cfg
             ├─55288 /usr/local/nagios/bin/nagios --worker /usr/local/nagios/var/rw/nagios.qh
             ├─55289 /usr/local/nagios/bin/nagios --worker /usr/local/nagios/var/rw/nagios.qh
             ├─55290 /usr/local/nagios/bin/nagios --worker /usr/local/nagios/var/rw/nagios.qh
             ├─55291 /usr/local/nagios/bin/nagios --worker /usr/local/nagios/var/rw/nagios.qh
             └─55292 /usr/local/nagios/bin/nagios -d /usr/local/nagios/etc/nagios.cfg

Sep 30 08:54:01 ip-172-31-44-151 nagios[55287]: qh: Socket '/usr/local/nagios/var/rw/nagios.qh' successfully initialized
lines 1-19
```

Step 2: To monitor a Linux machine, create an Ubuntu 20.04 server EC2 Instance in AWS.



Step 3: On client side Step-03 Make a package index update and install gcc, nagios-nrpe-server and the plugins.
sudo apt update -y
sudo apt install gcc -y
sudo apt install -y nagios-nrpe-server nagios-plugins

```
*** System restart required ***
Last login: Sat Sep 30 08:31:30 2023 from 13.233.177.3
ubuntu@ip-172-31-44-151:~$ sudo apt install gcc -y
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
gcc is already the newest version (4:11.2.0-1ubuntu1).
gcc set to manually installed.
0 upgraded, 0 newly installed, 0 to remove and 2 not upgraded.
ubuntu@ip-172-31-44-151:~$
```

```
root@ip-172-31-44-151:/home/ubuntu# sudo apt install nagios-nrpe-server nagios-plugins
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
Note, selecting 'monitoring-plugins' instead of 'nagios-plugins'
monitoring-plugins is already the newest version (2.3.1-1ubuntu4).
nagios-nrpe-server is already the newest version (4.0.3-1ubuntu2).
0 upgraded, 0 newly installed, 0 to remove and 2 not upgraded.
```

```
Get:4 http://security.ubuntu.com/ubuntu jammy-security InRelease [110 kB]
Fetched 229 kB in 1s (290 kB/s)
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
2 packages can be upgraded. Run 'apt list --upgradable' to see them.
root@ip-172-31-44-151:/home/ubuntu# sudo apt install gcc -y
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
gcc is already the newest version (4:11.2.0-1ubuntu1).
0 upgraded, 0 newly installed, 0 to remove and 2 not upgraded.
root@ip-172-31-44-151:/home/ubuntu# sudo apt install -y nagios-nrpe-server nagios-plugins
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
Note, selecting 'monitoring-plugins' instead of 'nagios-plugins'
monitoring-plugins is already the newest version (2.3.1-1ubuntu4).
nagios-nrpe-server is already the newest version (4.0.3-1ubuntu2).
0 upgraded, 0 newly installed, 0 to remove and 2 not upgraded.
```

Step 4: Open nrpe.cfg file to make changes.
sudo nano /etc/nagios/nrpe.cfg

```
  GNU nano 6.2                                  /etc/nagios/nrpe.cfg

# SERVER ADDRESS
# Address that nrpe should bind to in case there are more than one interface
# and you do not want nrpe to bind on all interfaces.
# NOTE: This option is ignored if NRPE is running under either inetd or xinetd

#server_address=127.0.0.1



# LISTEN QUEUE SIZE
# Listen queue size (backlog) for serving incoming connections.
# You may want to increase this value under high load.

#listen_queue_size=5

^G Help          ^O Write Out     ^W Where Is      ^K Cut           ^T Execute       ^C Location      M-U Undo        M-A Set Mark
^X Exit          ^R Read File     ^\ Replace       ^U Paste         ^J Justify       ^/ Go To Line    M-E Redo        M-6 Copy
```

```
  GNU nano 6.2                                  /etc/nagios/nrpe.cfg *
 95 # that are allowed to talk to the NRPE daemon. Network addresses with a bit mask
 96 # (i.e. 192.168.1.0/24) are also supported. Hostname wildcards are not currently
 97 # supported.
 98 #
 99 # Note: The daemon only does rudimentary checking of the client's IP
100 # address.  I would highly recommend adding entries in your /etc/hosts.allow
101 # file to allow only the specified host to connect to the port
102 # you are running this daemon on.
103 #
104 # NOTE: This option is ignored if NRPE is running under either inetd or xinetd
105
106 allowed_hosts=127.0.0.1,::1,13.235.0.144
107 server_address=0.0.0.0
108
109
110

^G Help          ^O Write Out     ^W Where Is      ^K Cut           ^T Execute       ^C Location      M-U Undo        M-A Set Mark
^X Exit          ^R Read File     ^\ Replace       ^U Paste         ^J Justify       ^/ Go To Line    M-E Redo        M-6 Copy
```

Step 5: Restart the NRPE server
sudo systemctl restart nagios-nrpe-server

```
Restarting services...
Service restarts being deferred:
 /etc/needrestart/restart.d/dbus.service
 systemctl restart getty@tty1.service
 systemctl restart networkd-dispatcher.service
 systemctl restart systemd-logind.service
 systemctl restart unattended-upgrades.service
 systemctl restart user@1000.service

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.
root@ip-172-31-41-41:/home/ubuntu# sudo nano /etc/nagios/nrpe.cfg
root@ip-172-31-41-41:/home/ubuntu# sudo nano /etc/nagios/nrpe.cfg
root@ip-172-31-41-41:/home/ubuntu# sudo systemctl restart nagios-nrpe-server
root@ip-172-31-41-41:/home/ubuntu# sudo systemctl status nagios-nrpe-server
● nagios-nrpe-server.service - Nagios Remote Plugin Executor
```

```
root@ip-172-31-41-41:/home/ubuntu# sudo systemctl status nagios-nrpe-server
● nagios-nrpe-server.service - Nagios Remote Plugin Executor
     Loaded: loaded (/lib/systemd/system/nagios-nrpe-server.service; enabled; vendor preset: enabled)
     Active: active (running) since Sat 2023-09-30 09:27:17 UTC; 6s ago
       Docs: http://www.nagios.org/documentation
   Main PID: 7349 (nrpe)
      Tasks: 1 (limit: 1141)
     Memory: 1.5M
        CPU: 9ms
     CGroup: /system.slice/nagios-nrpe-server.service
             └─7349 /usr/sbin/nrpe -c /etc/nagios/nrpe.cfg -f

Sep 30 09:27:17 ip-172-31-41-41 systemd[1]: nagios-nrpe-server.service: Deactivated successfully.
Sep 30 09:27:17 ip-172-31-41-41 systemd[1]: Stopped Nagios Remote Plugin Executor.
Sep 30 09:27:17 ip-172-31-41-41 systemd[1]: Started Nagios Remote Plugin Executor.
Sep 30 09:27:17 ip-172-31-41-41 nrpe[7349]: Starting up daemon
Sep 30 09:27:17 ip-172-31-41-41 nrpe[7349]: Server listening on 0.0.0.0 port 5666.
Sep 30 09:27:17 ip-172-31-41-41 nrpe[7349]: Listening for connections on port 5666
Sep 30 09:27:17 ip-172-31-41-41 nrpe[7349]: Allowing connections from: 127.0.0.1,::1,13.235.0.144
root@ip-172-31-41-41:/home/ubuntu#
```

Step 6: On the server run this command
ps -ef | grep nagios

```
root@ip-172-31-44-151:/home/ubuntu# ps -ef | grep nagios
nagios     55287       1  0 08:54 ?        00:00:00 /usr/local/nagios/bin/nagios -d /usr/local/nagios/etc/nagios.cfg
nagios     55288   55287  0 08:54 ?        00:00:00 /usr/local/nagios/bin/nagios --worker /usr/local/nagios/var/rw/nagios.qh
nagios     55289   55287  0 08:54 ?        00:00:00 /usr/local/nagios/bin/nagios --worker /usr/local/nagios/var/rw/nagios.qh
nagios     55290   55287  0 08:54 ?        00:00:00 /usr/local/nagios/bin/nagios --worker /usr/local/nagios/var/rw/nagios.qh
nagios     55291   55287  0 08:54 ?        00:00:00 /usr/local/nagios/bin/nagios --worker /usr/local/nagios/var/rw/nagios.qh
nagios     55292   55287  0 08:54 ?        00:00:00 /usr/local/nagios/bin/nagios -d /usr/local/nagios/etc/nagios.cfg
nagios     56327       1  0 08:58 ?        00:00:00 /usr/sbin/nrpe -c /etc/nagios/nrpe.cfg -f
root       60903   60158  0 09:32 pts/1    00:00:00 grep --color=auto nagios
root@ip-172-31-44-151:/home/ubuntu# sudo su
root@ip-172-31-44-151:/home/ubuntu# mkdir /usr/local/nagios/etc/objects/monitorhosts
root@ip-172-31-44-151:/home/ubuntu# mkdir /usr/local/nagios/etc/objects/monitorhosts/linuxhosts
```

Step 7: Become a root user and create 2 folders 1.sudo su 2.mkdir /usr/local/nagios/etc/objects/monitorhosts 3.mkdir /usr/local/nagios/etc/objects/monitorhosts/linuxhosts Copy the sample localhost.cfg file to linuxhost folder 4.cp /usr/local/nagios/etc/objects/localhost.cfg /usr/local/nagios/etc/objects/monitorhosts/linuxhosts/linuxserver.cfg

```
root@ip-172-31-44-151:/home/ubuntu# cp /usr/local/nagios/etc/objects/localhost.cfg /usr/local/nagios/etc/objects/monitorhosts/linuxhos
ts/linuxserver.cfg
root@ip-172-31-44-151:/home/ubuntu# nano /usr/local/nagios/etc/objects/monitorhosts/linuxhosts/linuxserver.cfg
```

Step 8: Open linuxserver.cfg using nano and make the following changes
nano /usr/local/nagios/etc/objects/monitorhosts/linuxhosts/linuxserver.cfg Change the hostname to linux server (EVERYWHERE ON THE FILE) Change address to the public IP address of your LINUX CLIENT.

```
  GNU nano 6.2                  /usr/local/nagios/etc/objects/monitorhosts/linuxhosts/linuxserver.cfg
##############################################################################

# Define a host for the local machine

define host {

    use                     linux-server            ; Name of host template to use
                                                    ; This host definition will inherit all variables that are defined
                                                    ; in (or inherited by) the linux-server host template definition.
    host_name               localhost
    alias                   localhost
    address                 127.0.0.1
}


]
^G Help          ^O Write Out     ^W Where Is      ^K Cut           ^T Execute       ^C Location      M-U Undo         M-A Set Mark
^X Exit          ^R Read File     ^\ Replace       ^U Paste         ^J Justify       ^/ Go To Line    M-E Redo         M-6 Copy
```

i-03a3e79fc5ab0a056 (cutenagios_server)

```
  GNU nano 6.2                  /usr/local/nagios/etc/objects/monitorhosts/linuxhosts/linuxserver.cfg *
##############################################################################
#
# HOST GROUP DEFINITION
#
##############################################################################

# Define an optional hostgroup for Linux machines

define hostgroup {

    hostgroup_name          linux-servers           ; The name of the hostgroup
    alias                   Linux Servers           ; Long name of the group
    members                 localhost               ; Comma separated list of hosts that belong to this group
}


^G Help          ^O Write Out     ^W Where Is      ^K Cut           ^T Execute       ^C Location      M-U Undo         M-A Set Mark
^X Exit          ^R Read File     ^\ Replace       ^U Paste         ^J Justify       ^/ Go To Line    M-E Redo         M-6 Copy
```

Change hostgroup_name under hostgroup to linux-servers1

Step 9: Open the Nagios Config file and add the following line nano /usr/local/nagios/etc/nagios.cfg Add this line cfg_dir=/usr/local/nagios/etc/objects/monitorhosts/

```
  GNU nano 6.2                            /usr/local/nagios/etc/nagios.cfg *
# You can also tell Nagios to process all config files (with a .cfg
# extension) in a particular directory by using the cfg_dir
# directive as shown below:

#cfg_dir=/usr/local/nagios/etc/servers
#cfg_dir=/usr/local/nagios/etc/printers
#cfg_dir=/usr/local/nagios/etc/switches
#cfg_dir=/usr/local/nagios/etc/routers
cfg_dir=/usr/local/nagios/etc/objects/monitorhosts/



# OBJECT CACHE FILE
# This option determines where object definitions are cached when
# Nagios starts/restarts.  The CGIs read object definitions from
Save modified buffer?
 Y Yes
 N No            ^C Cancel
```

Step 10: Verify the configuration files.

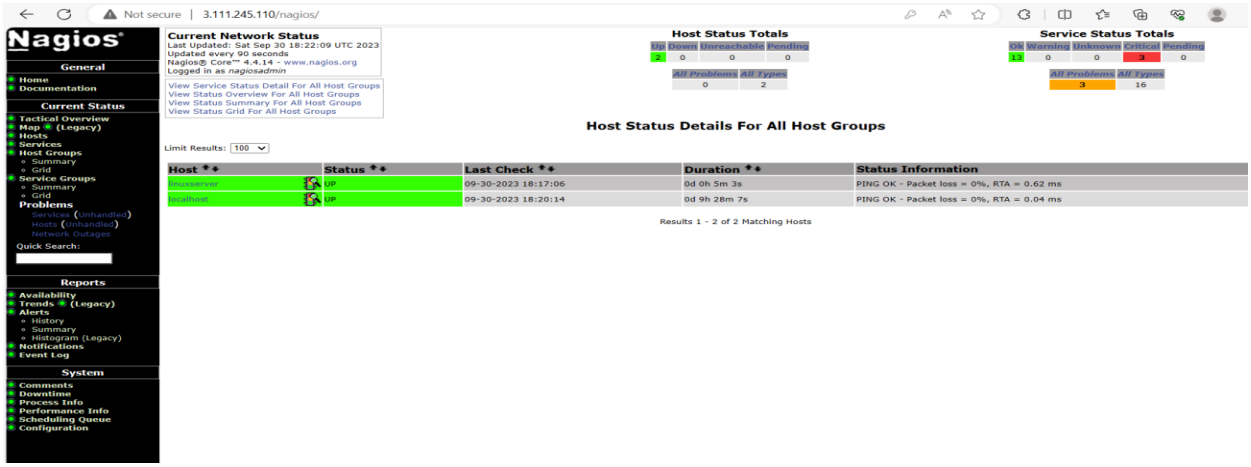
```
root@ip-172-31-44-151:/home/ubuntu# nano /usr/local/nagios/etc/objects/monitorhosts/linuxhosts/linuxserver.cfg
root@ip-172-31-44-151:/home/ubuntu#    /usr/local/nagios/bin/nagios -v /usr/local/nagios/etc/nagios.cfg

Nagios Core 4.4.14
Copyright (c) 2009-present Nagios Core Development Team and Community Contributors
Copyright (c) 1999-2009 Ethan Galstad
Last Modified: 2023-08-01
License: GPL

Website: https://www.nagios.org
Reading configuration data...
   Read main config file okay...
   Read object config files okay...

Running pre-flight check on configuration data...

Checking objects...
        Checked 8 services.
        Checked 1 hosts.
        Checked 1 host groups.
        Checked 1 contacts.
        Checked 1 contact groups.
        Checked 24 commands.
        Checked 5 time periods.
        Checked 0 host escalations.
        Checked 0 service escalations.
Checking for circular paths...
        Checked 1 hosts
        Checked 0 service dependencies
        Checked 0 host dependencies
        Checked 5 timeperiods
Checking global event handlers...
Checking obsessive compulsive processor commands...
Checking misc settings...

Total Warnings: 0
Total Errors:   0

Things look okay - No serious problems were detected during the pre-flight check
root@ip-172-31-44-151:/home/ubuntu# nano /usr/local/nagios/etc/nagios.cfg
```

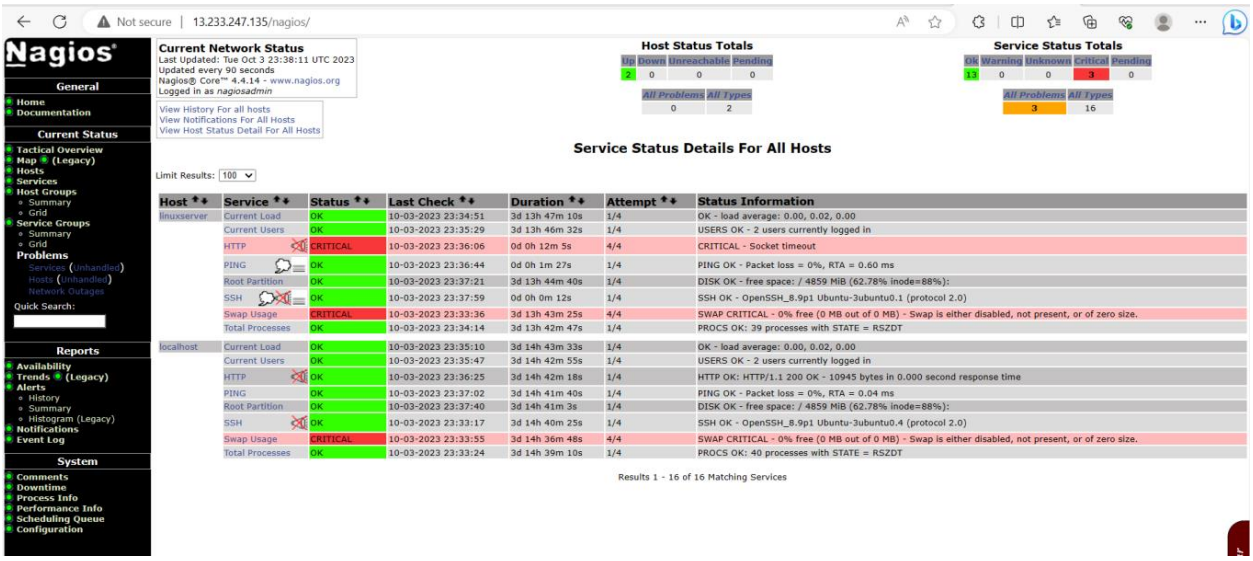
Step 11: Restart the nagios service service nagios restart

Sudo systemctl status nagios

```
● nagios.service - Nagios Core 4.4.14
     Loaded: loaded (/lib/systemd/system/nagios.service; enabled; vendor preset: enabled)
     Active: active (running) since Sat 2023-09-30 08:54:01 UTC; 20s ago
       Docs: https://www.nagios.org/documentation
    Process: 55285 ExecStartPre=/usr/local/nagios/bin/nagios -v /usr/local/nagios/etc/nagios.cfg (code=exited, status=0/SUCCESS)
    Process: 55286 ExecStart=/usr/local/nagios/bin/nagios -d /usr/local/nagios/etc/nagios.cfg (code=exited, status=0/SUCCESS)
   Main PID: 55287 (nagios)
      Tasks: 6 (limit: 1141)
     Memory: 5.3M
        CPU: 252ms
     CGroup: /system.slice/nagios.service
             ├─55287 /usr/local/nagios/bin/nagios -d /usr/local/nagios/etc/nagios.cfg
             ├─55288 /usr/local/nagios/bin/nagios --worker /usr/local/nagios/var/rw/nagios.qh
             ├─55289 /usr/local/nagios/bin/nagios --worker /usr/local/nagios/var/rw/nagios.qh
             ├─55290 /usr/local/nagios/bin/nagios --worker /usr/local/nagios/var/rw/nagios.qh
             ├─55291 /usr/local/nagios/bin/nagios --worker /usr/local/nagios/var/rw/nagios.qh
             └─55292 /usr/local/nagios/bin/nagios -d /usr/local/nagios/etc/nagios.cfg

Sep 30 08:54:01 ip-172-31-44-151 nagios[55287]: qh: Socket '/usr/local/nagios/var/rw/nagios.qh' successfully initialized
lines 1-19
```

Step 12: Now, check your nagios dashboard and you'll see a new host being added.




Not secure | 13.233.247.135/nagios/
Nagios
General
Home
Documentation
Current Status
Tactical Overview
Map (Legacy)
Hosts
Services
Host Groups
Summary
Grid
Service Groups
Summary
Grid
Problems
Services (Unhandled)
Hosts (Unhandled)
Network Outages
Quick Search:
Reports
Availability
Trends (Legacy)
Alerts
History
Summary
Histogram (Legacy)
Notifications
Event Log
System
Comments
Downtime
Process Info
Performance Info
Scheduling Queue
Configuration
Current Network Status
Last Updated: Tue Oct 3 23:38:11 UTC 2023
Updated every 90 seconds
Nagios® Core™ 4.4.14 - www.nagios.org
Logged in as nagiosadmin
View History For all hosts
View Notifications For All Hosts
View Host Status Detail For All Hosts
Host Status Totals
Up Down Unreachable Pending
2 0 0 0
All Problems All Types
0 2
Service Status Totals
Ok Warning Unknown Critical Pending
13 0 0 3 0
All Problems All Types
3 16
Service Status Details For All Hosts
Limit Results: 100
Host Service Status Last Check Duration Attempt Status Information
linuxserver Current Load OK 10-03-2023 23:34:51 3d 13h 47m 10s 1/4 OK - load average: 0.00, 0.02, 0.00
Current Users OK 10-03-2023 23:35:29 3d 13h 46m 32s 1/4 USERS OK - 2 users currently logged in
HTTP CRITICAL 10-03-2023 23:36:06 0d 0h 12m 5s 4/4 CRITICAL - Socket timeout
PING OK 10-03-2023 23:36:44 0d 0h 1m 27s 1/4 PING OK - Packet loss = 0%, RTA = 0.60 ms
Root Partition OK 10-03-2023 23:37:21 3d 13h 44m 40s 1/4 DISK OK - free space: / 4859 MiB (62.78% inode=88%):
SSH OK 10-03-2023 23:37:59 0d 0h 0m 12s 1/4 SSH OK - OpenSSH_8.9p1 Ubuntu-3ubuntu0.1 (protocol 2.0)
Swap Usage CRITICAL 10-03-2023 23:33:36 3d 13h 43m 25s 4/4 SWAP CRITICAL - 0% free (0 MB out of 0 MB) - Swap is either disabled, not present, or of zero size.
Total Processes OK 10-03-2023 23:34:14 3d 13h 42m 47s 1/4 PROCS OK: 39 processes with STATE = RSZDT
localhost Current Load OK 10-03-2023 23:35:10 3d 14h 43m 33s 1/4 OK - load average: 0.00, 0.02, 0.00
Current Users OK 10-03-2023 23:35:47 3d 14h 42m 55s 1/4 USERS OK - 2 users currently logged in
HTTP OK 10-03-2023 23:36:25 3d 14h 42m 18s 1/4 HTTP OK: HTTP/1.1 200 OK - 10945 bytes in 0.000 second response time
PING OK 10-03-2023 23:37:02 3d 14h 41m 40s 1/4 PING OK - Packet loss = 0%, RTA = 0.04 ms
Root Partition OK 10-03-2023 23:37:40 3d 14h 41m 3s 1/4 DISK OK - free space: / 4859 MiB (62.78% inode=88%):
SSH OK 10-03-2023 23:33:17 3d 14h 40m 25s 1/4 SSH OK - OpenSSH_8.9p1 Ubuntu-3ubuntu0.4 (protocol 2.0)
Swap Usage CRITICAL 10-03-2023 23:33:55 3d 14h 36m 48s 4/4 SWAP CRITICAL - 0% free (0 MB out of 0 MB) - Swap is either disabled, not present, or of zero size.
Total Processes OK 10-03-2023 23:33:24 3d 14h 39m 10s 1/4 PROCS OK: 40 processes with STATE = RSZDT
Results 1 - 16 of 16 Matching Services

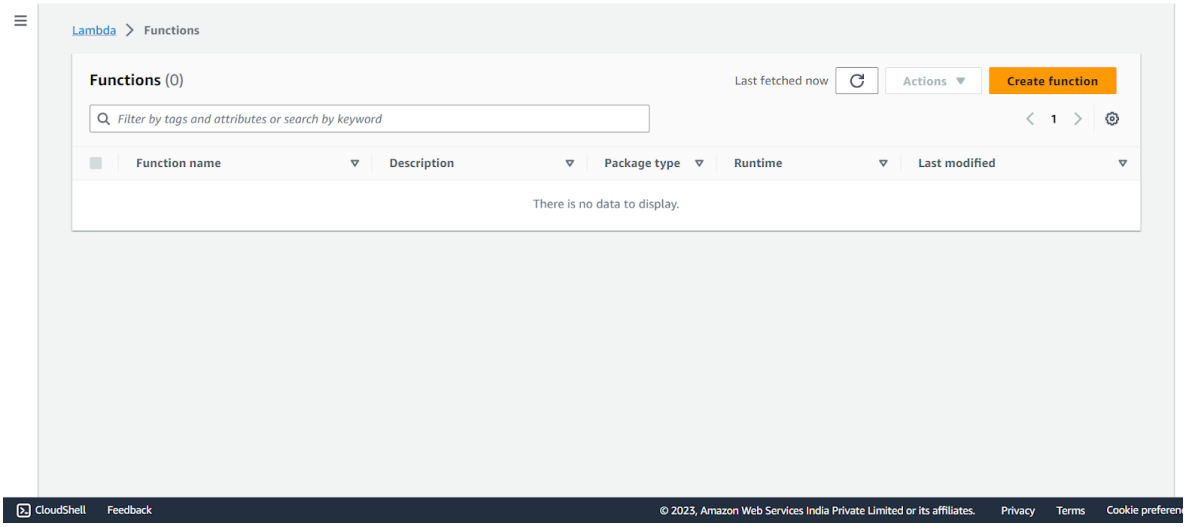
Experiment No 11

Vedant Sanap
D15A 48
Batch C

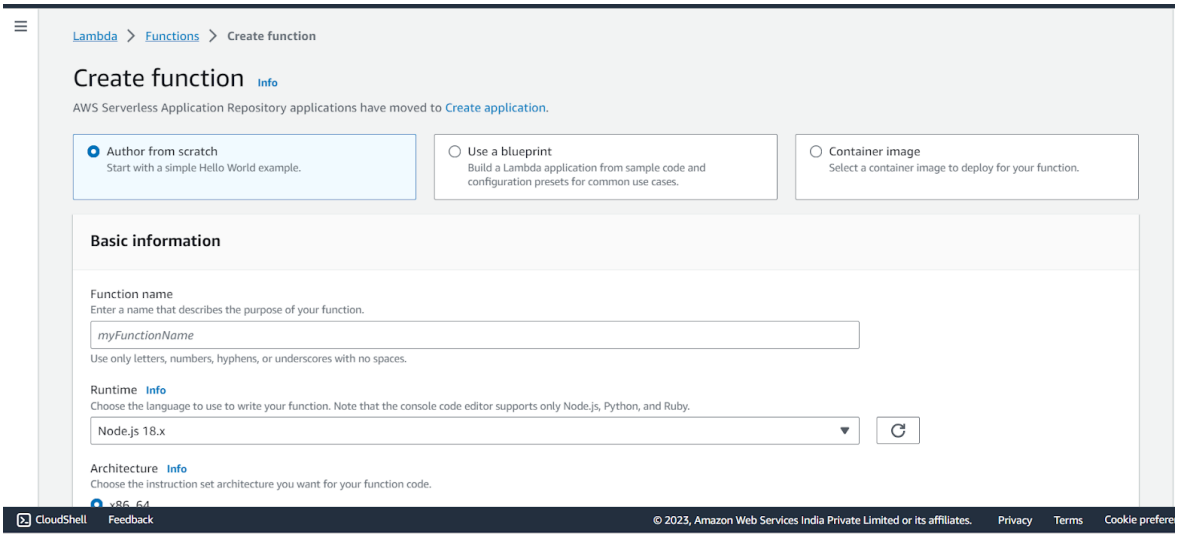
AIM: To understand AWS Lambda, its workflow, various functions and create your first Lambda functions using Python / Java / Nodejs.

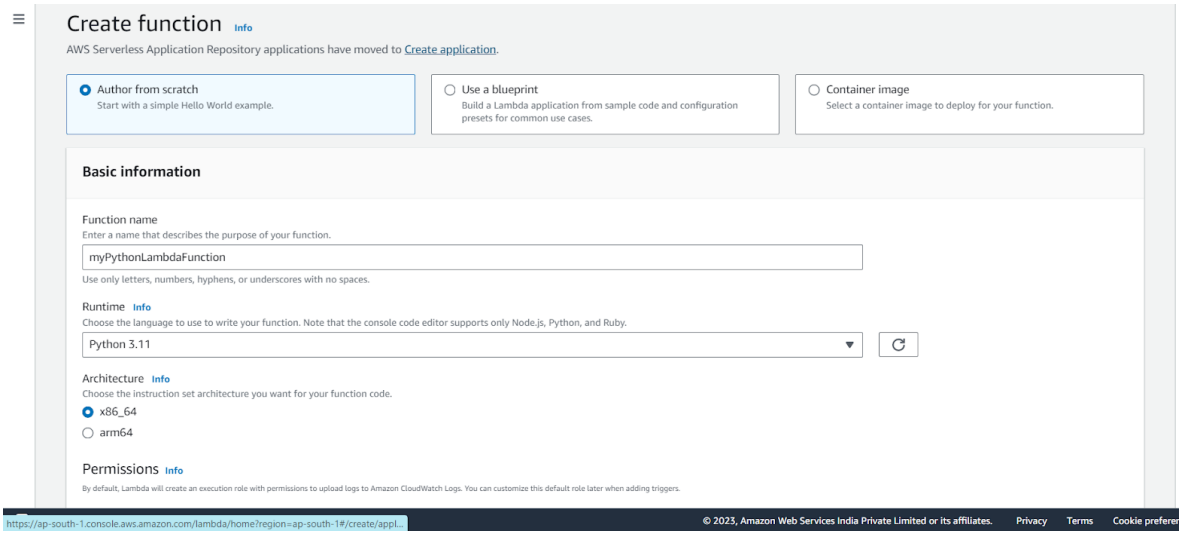
Steps to create an AWS Lambda function

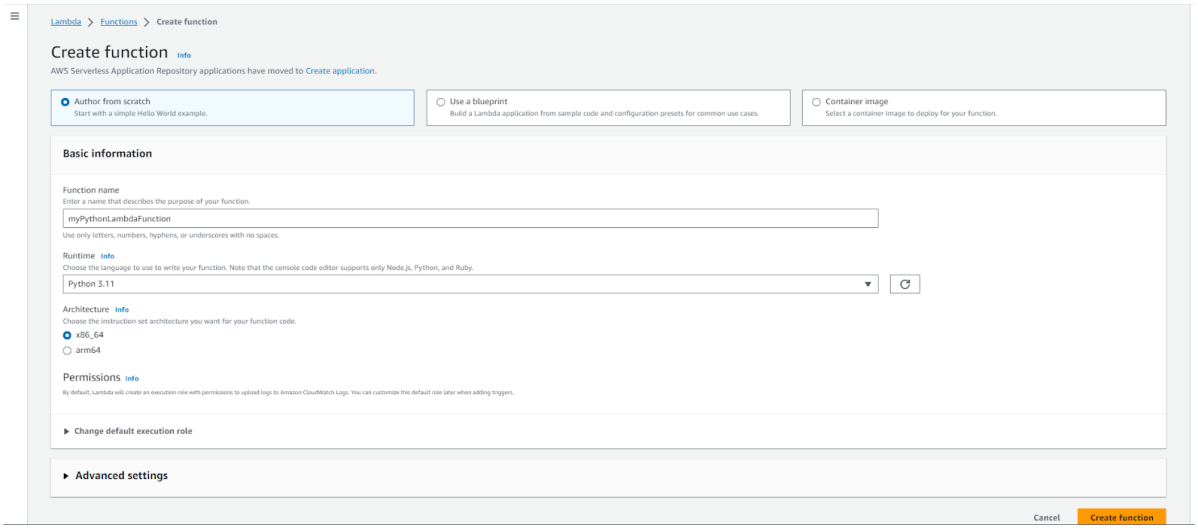
Step 1:Open up the Lambda Console and click on the Create button.
Be mindful of where you create your functions since Lambda is region-dependent.



2. Choose to create a function from scratch or use a blueprint, i.e templates defined by AWS for you with all configuration presets required for the most common use cases.
Then, choose a runtime env for your function, under the dropdown, you can see all the options AWS supports, Python, Nodejs, .NET and Java being the most popular ones.
After that, choose to create a new role with basic Lambda permissions if you don't have an existing one.

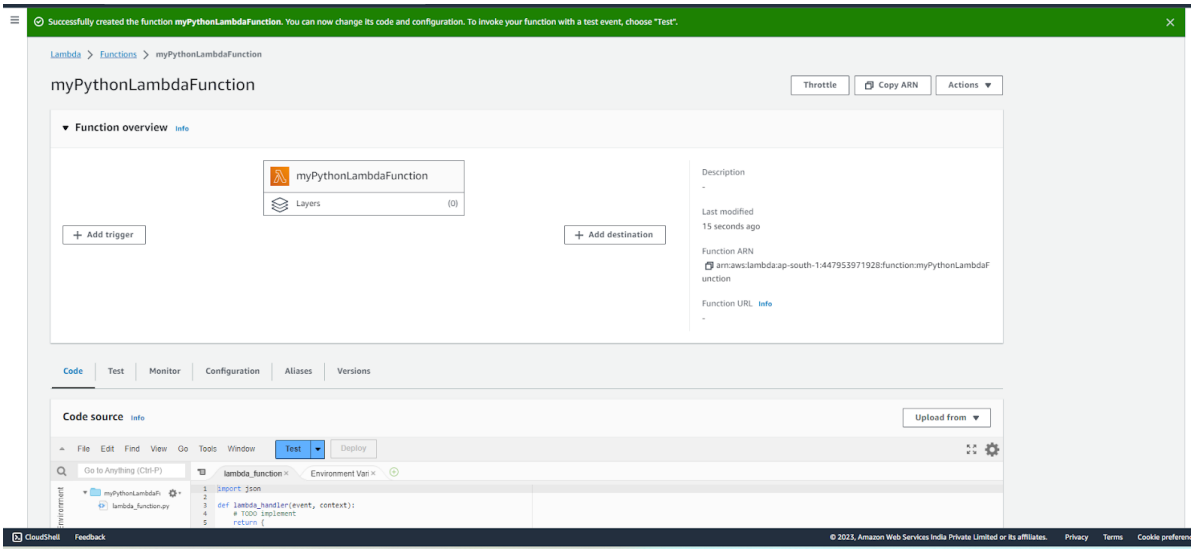


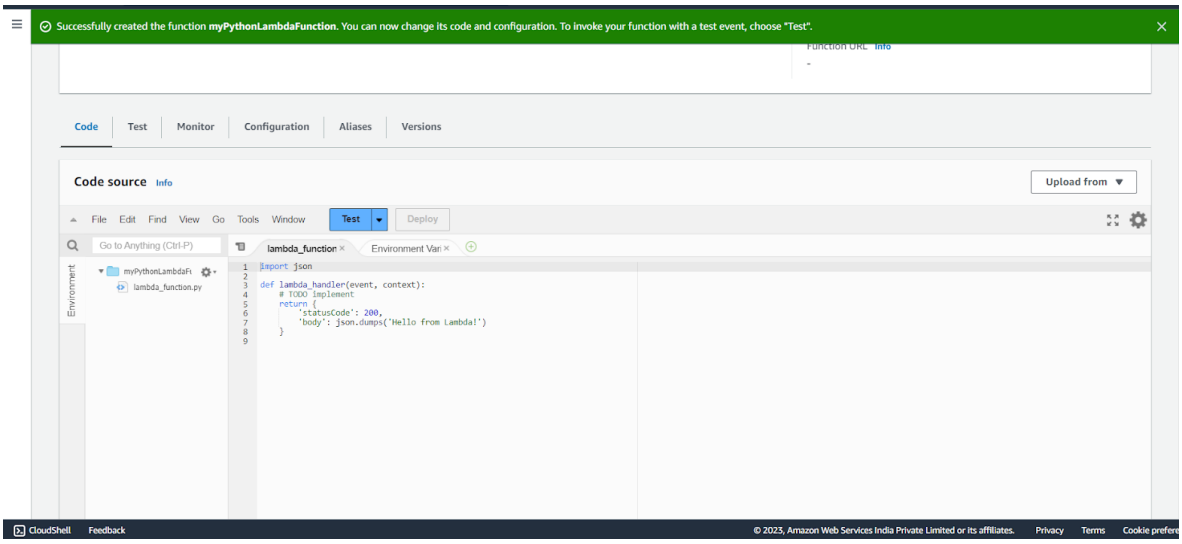




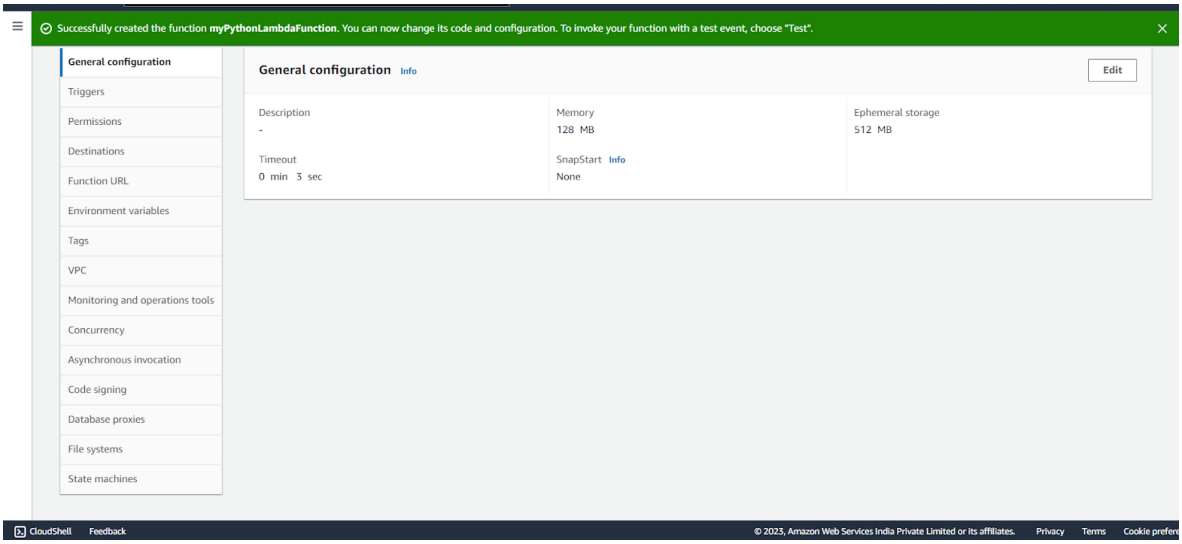
Click on the Create button.

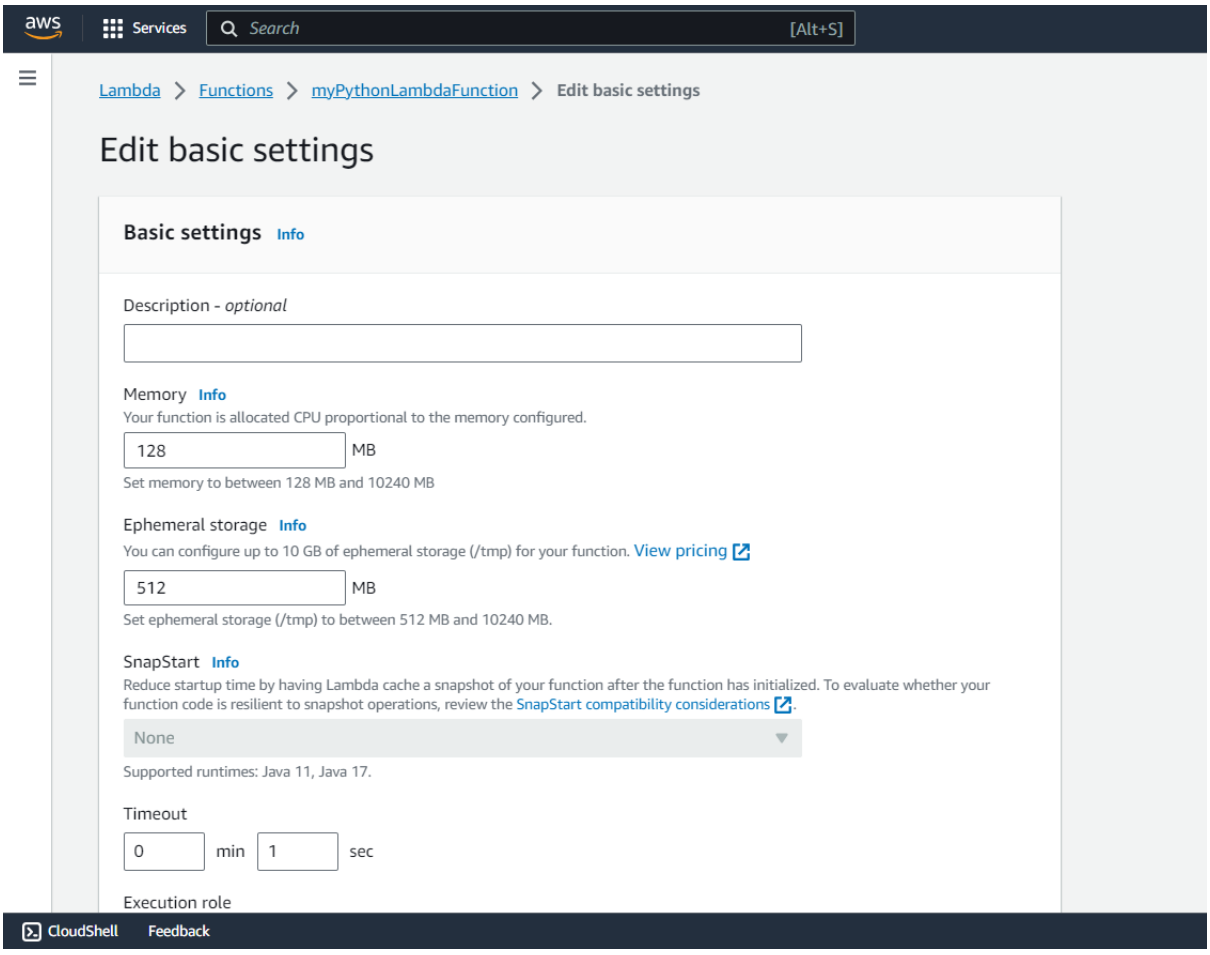
3. This process will take a while to finish and after that, you'll get a message that your function was successfully created.



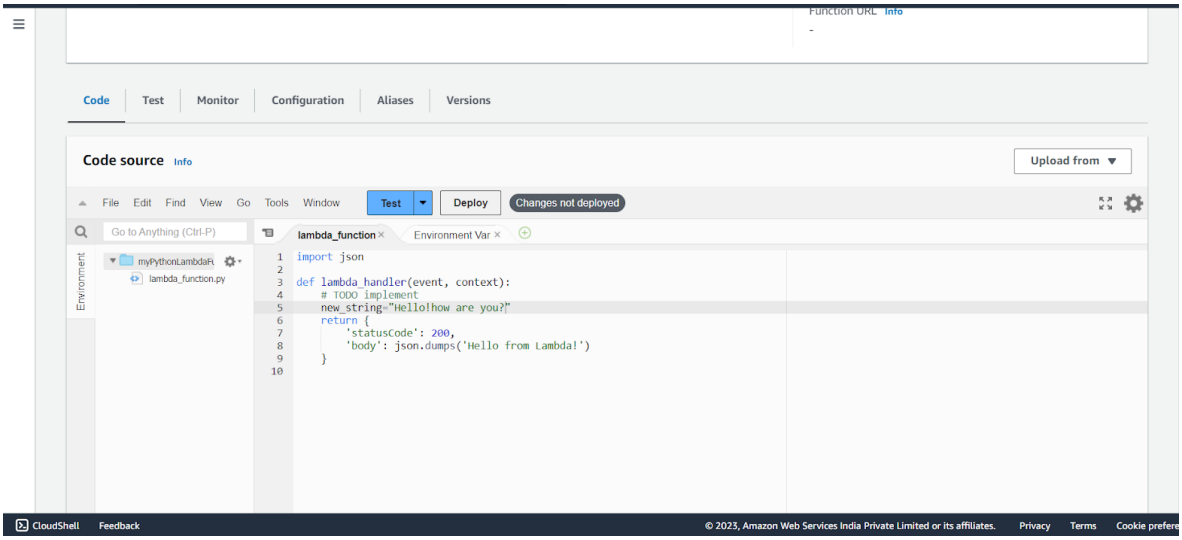


4. To change the configuration, open up the Configuration tab and under General Configuration, choose Edit.
Here, you can enter a description and change Memory and Timeout. I've changed the Timeout period to 1 sec since that is sufficient for now.

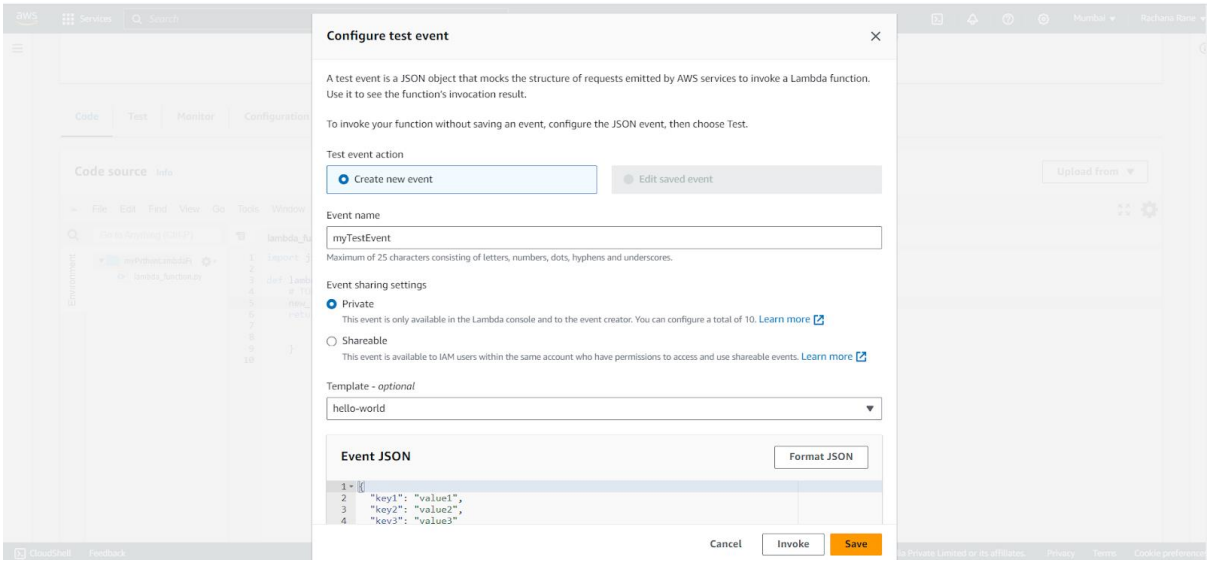




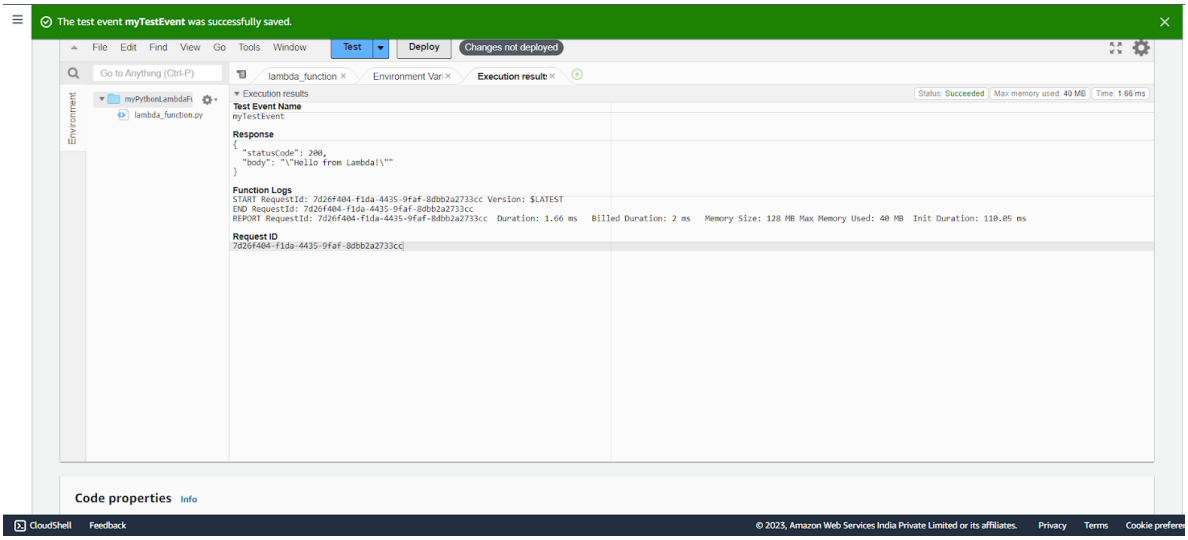
5. You can make changes to your function inside the code editor. You can also upload a zip file of your function or upload one from an S3 bucket if needed.
Press Ctrl + S to save the file and click Deploy to deploy the changes.

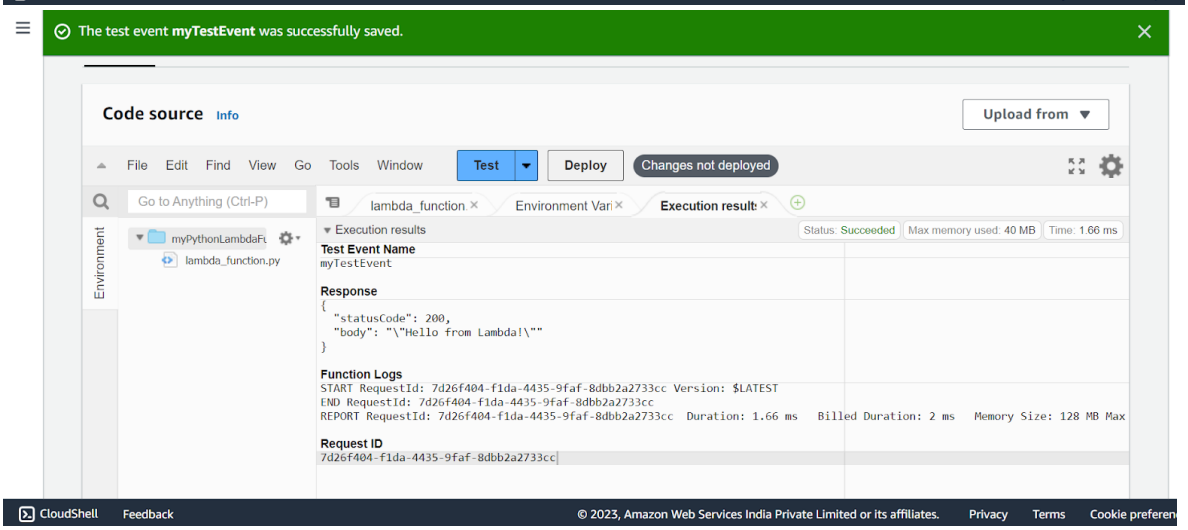


6. Click on Test and you can change the configuration, like so. If you do not have anything in the request body, it is important to specify two curly braces as valid JSON, so make sure they are there.



7. Now click on Test and you should be able to see the results.



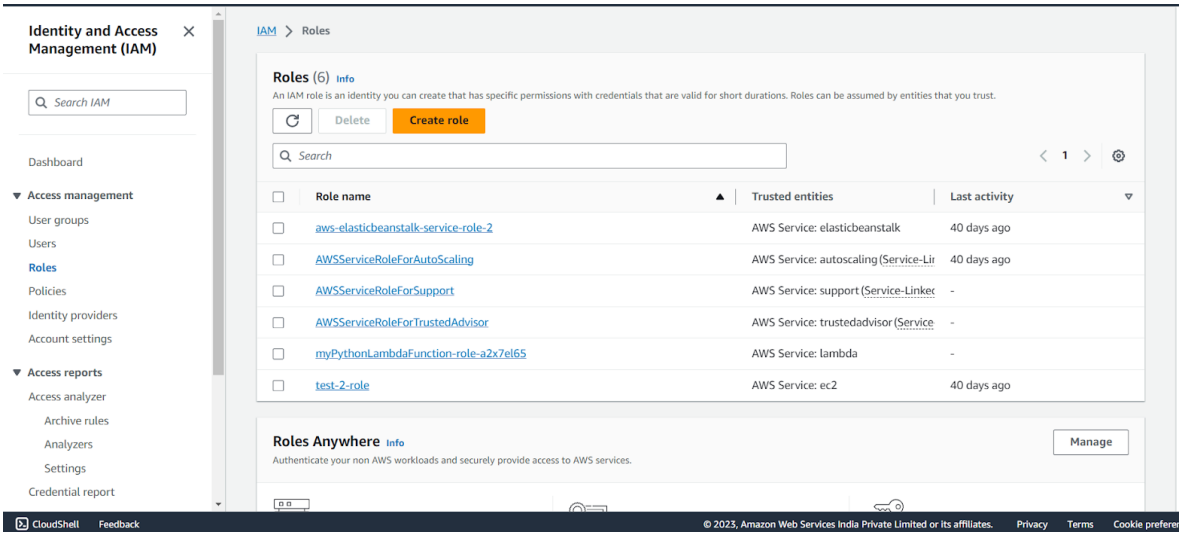


Conclusion: Thus, we understood AWS Lambda, its workflow, various functions and created our first Lambda functions using Python / Java / Nodejs.

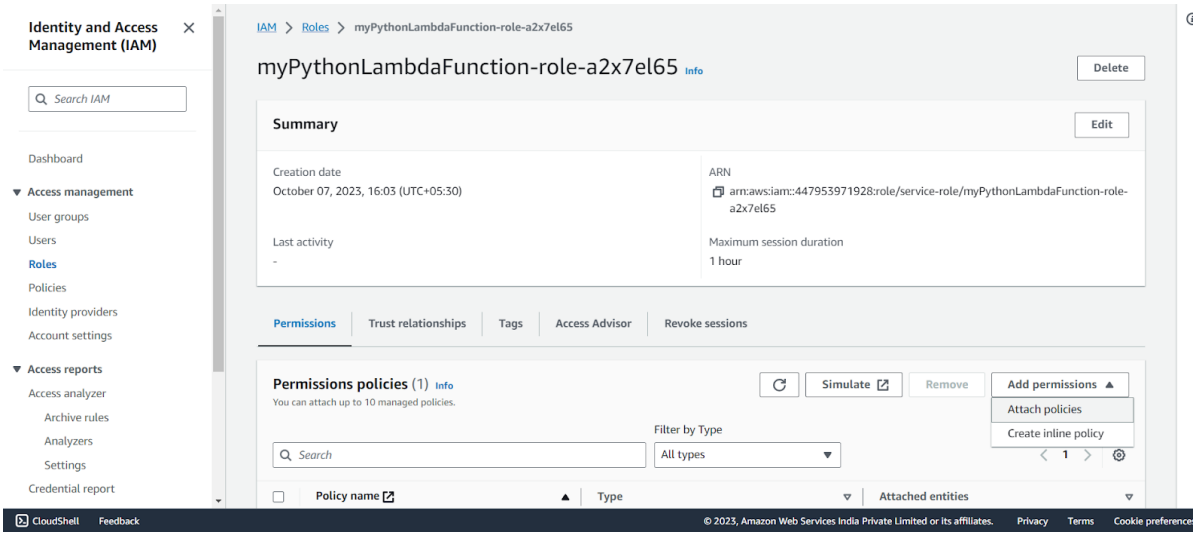
Experiment No 12

Vedant Sanap
D15A 48
Batch C

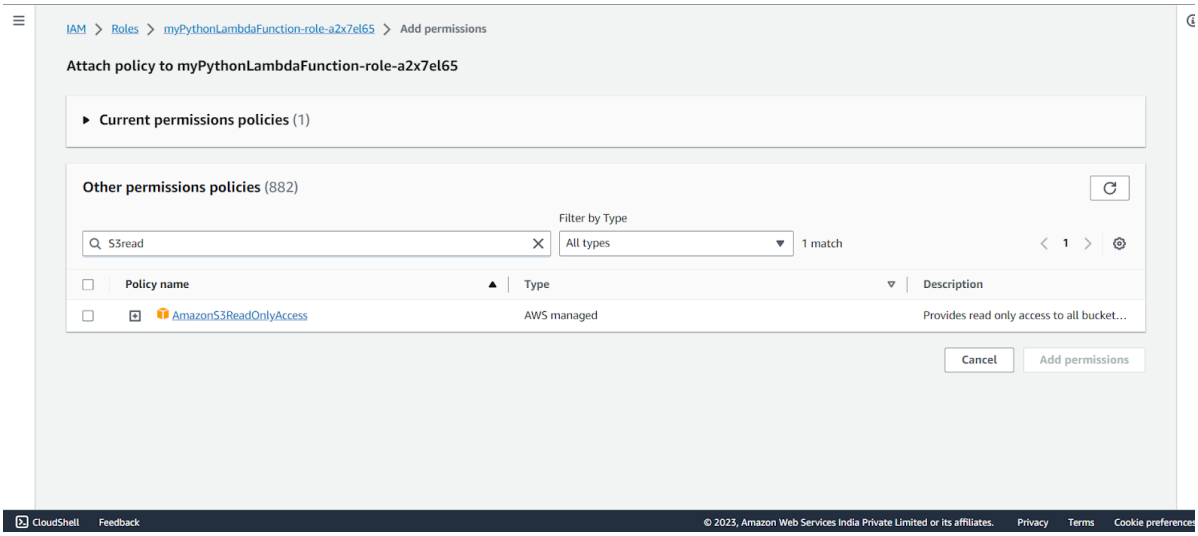
Step 1: Open up the IAM Console and under Roles, choose the Role we previously created for the Python Lambda Function (You can find your role name configuration of your Lambda function).



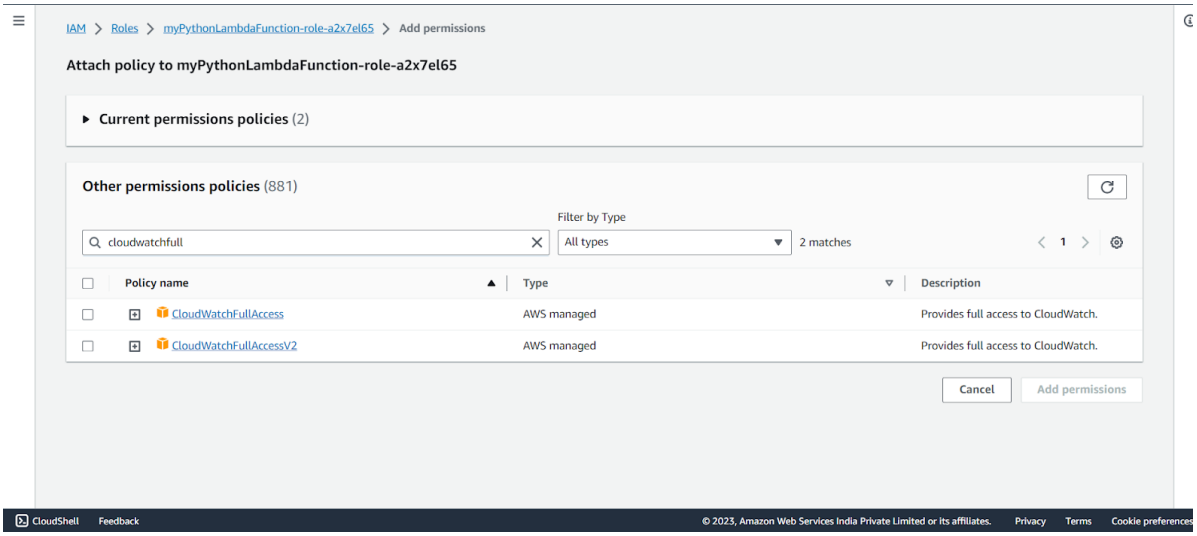
Step 2: Under Attach Policies, add S3-ReadOnly and CloudWatchFull permissions to this role.



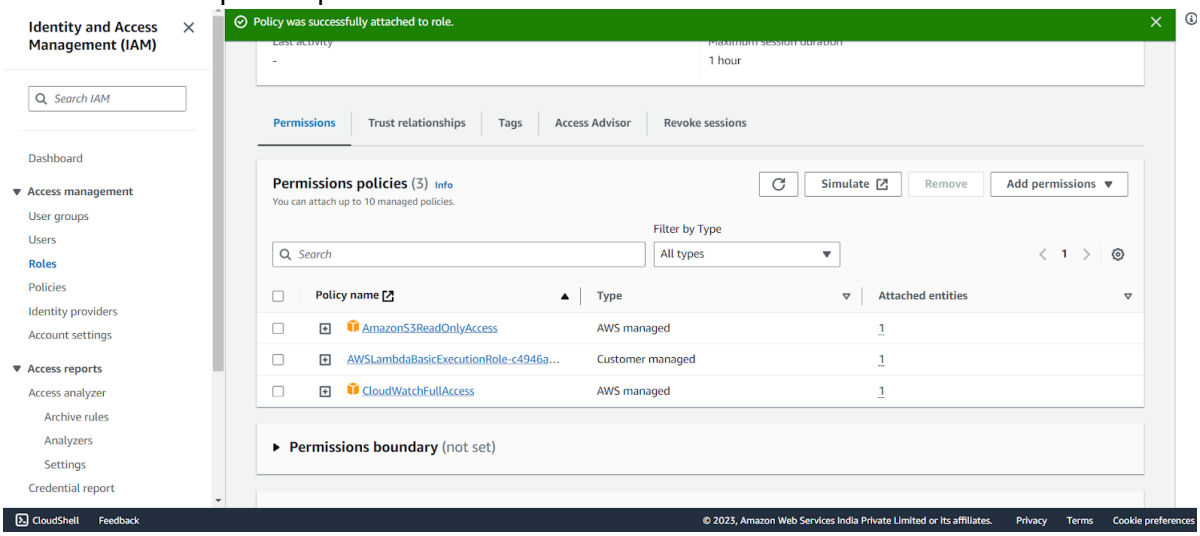
S3-ReadOnly



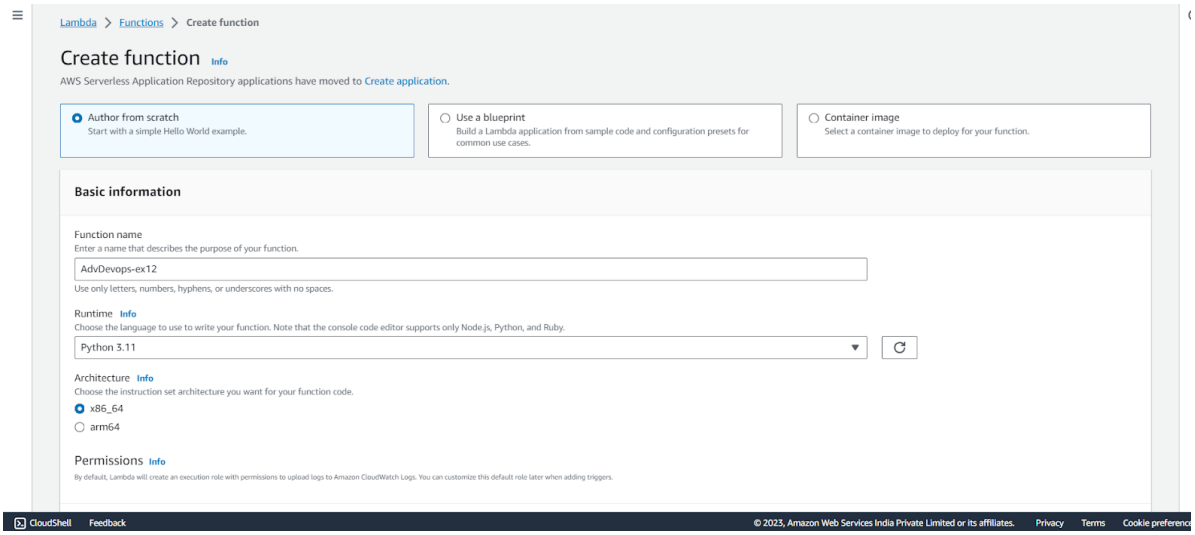
CloudWatchFull



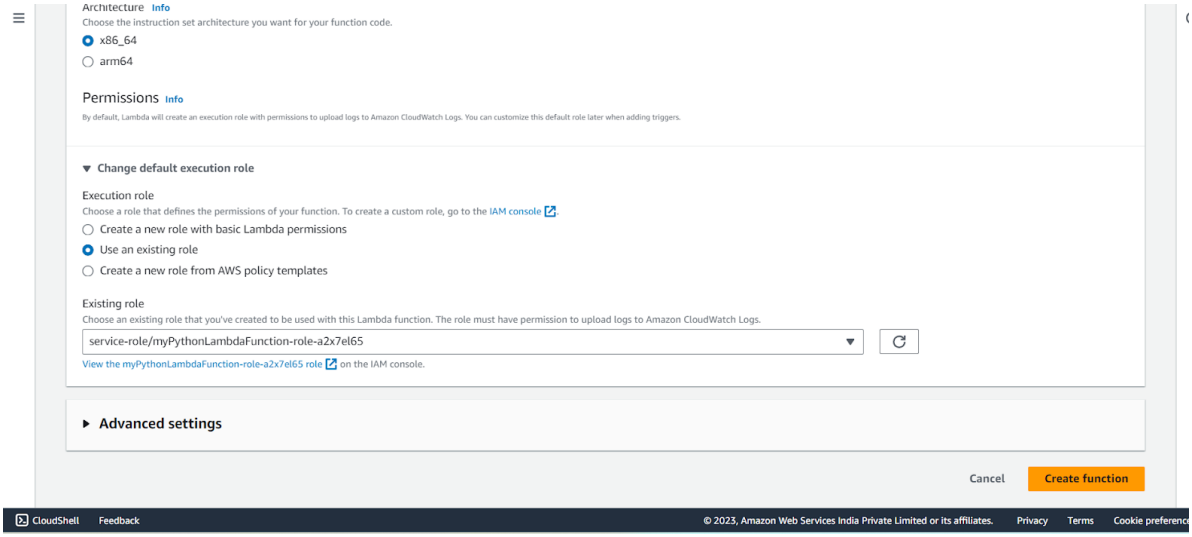
After successful attachment of policy you will see something like this you will be able to see the updated policies.



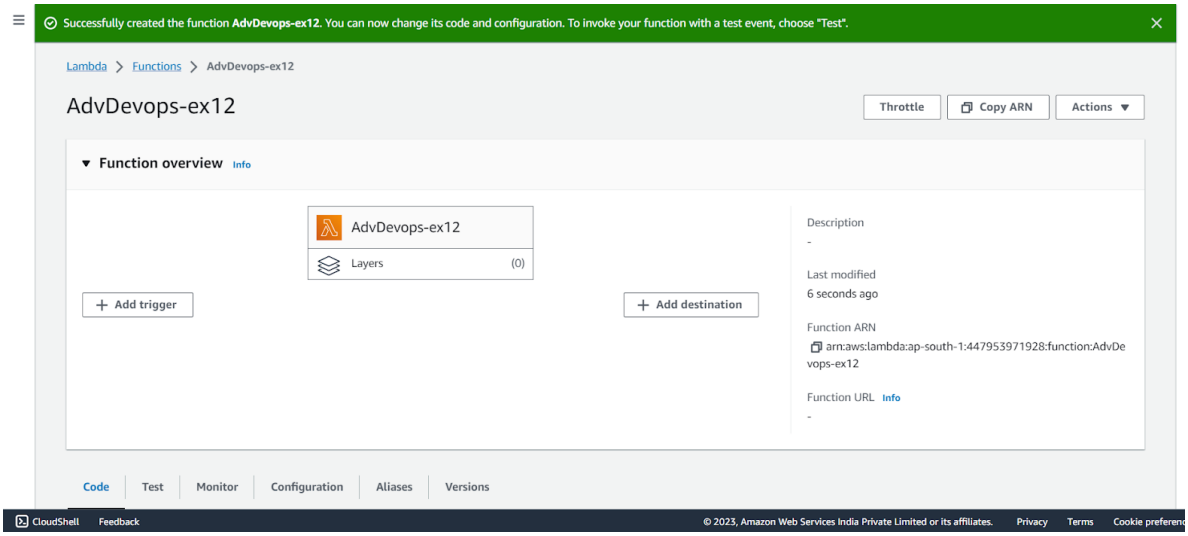
Step 3: Open up AWS Lambda and create a new Python function.



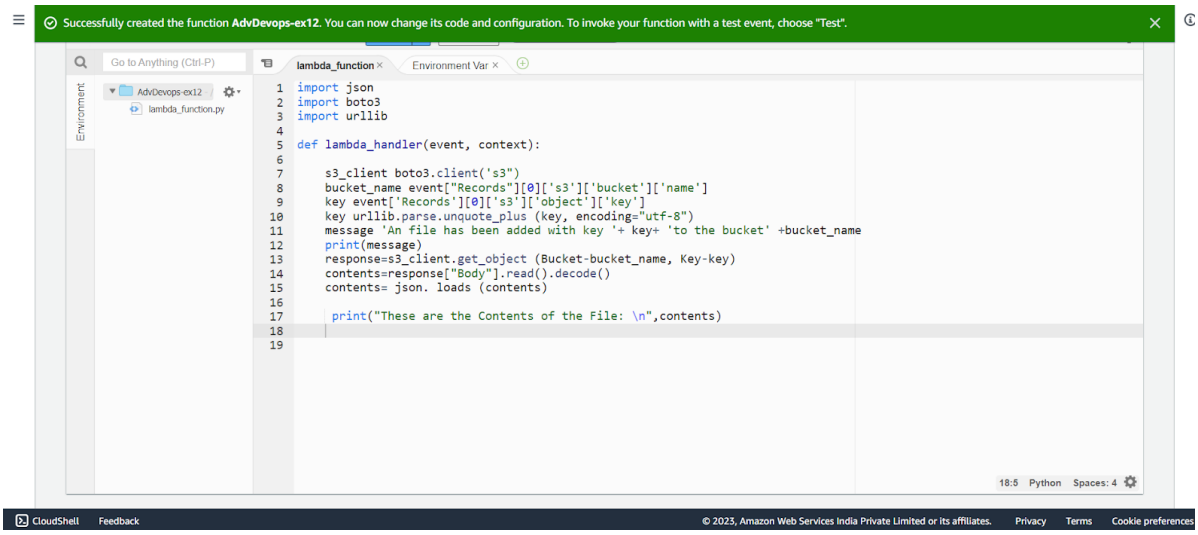
Under Execution Role, choose the existing role, then select the one which was previously created and to which we just added permissions.



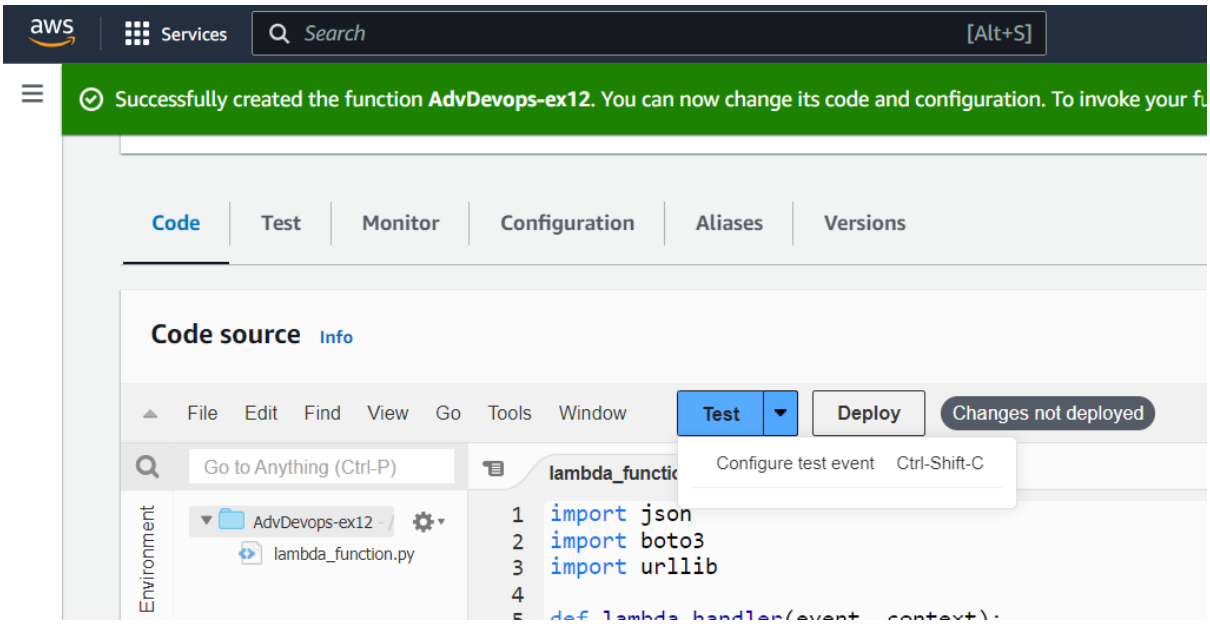
Step 4: The function is up and running.

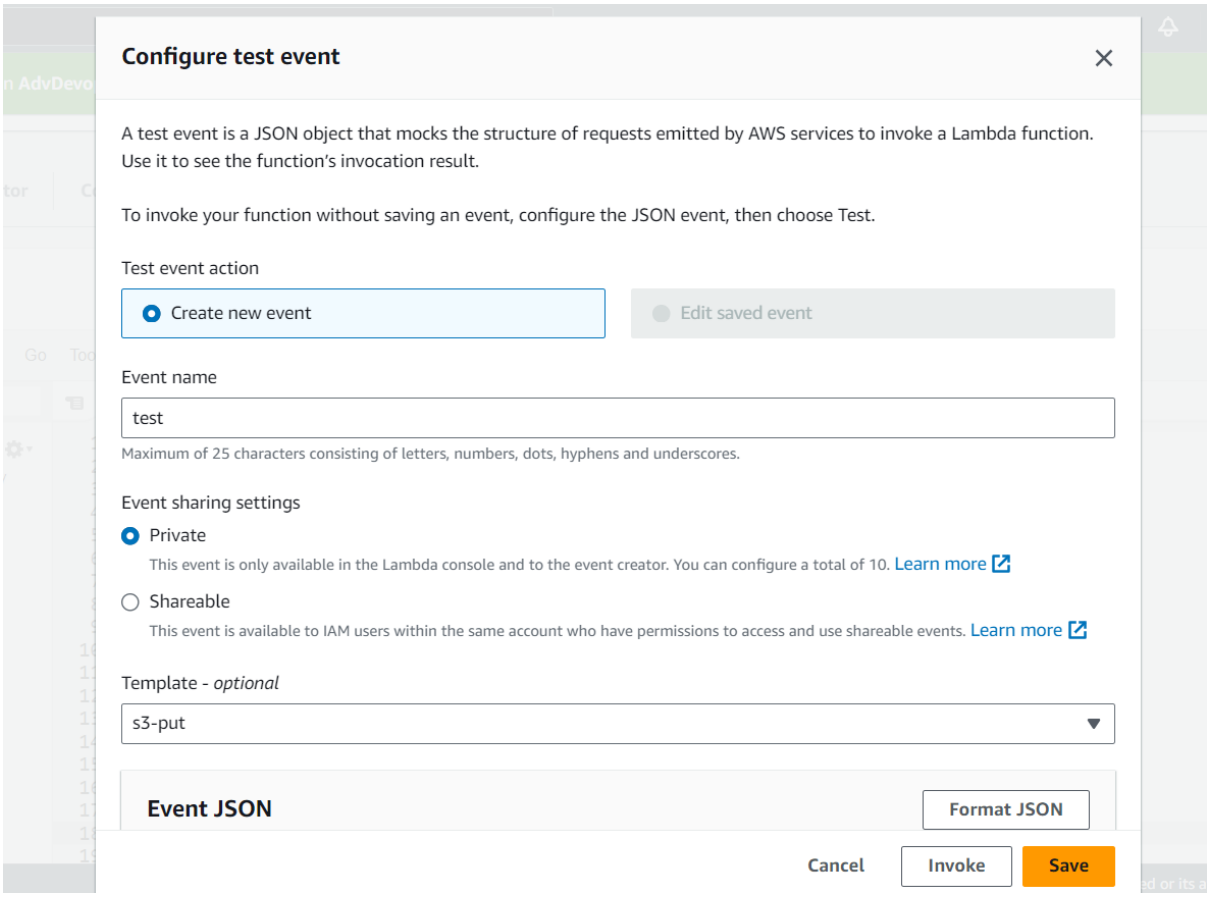


Step 5: Make the following changes to the function and click on the deploy button. This code basically logs a message and logs the contents of a JSON file which is uploaded to an S3 Bucket and then deploy the code.



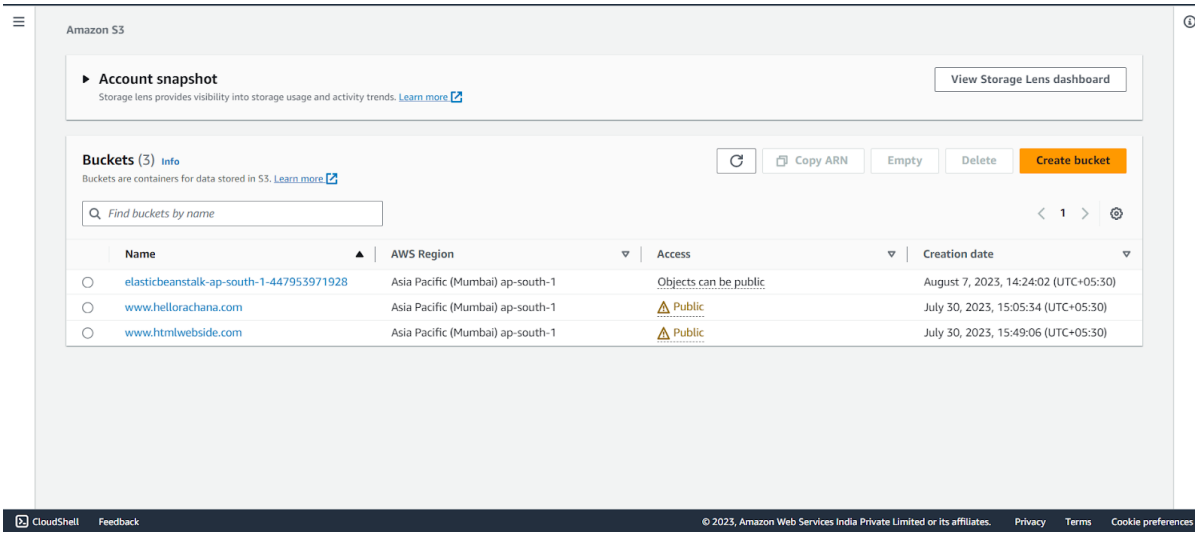
Step 6: Click on Test and choose the ‘S3 Put’ Template.



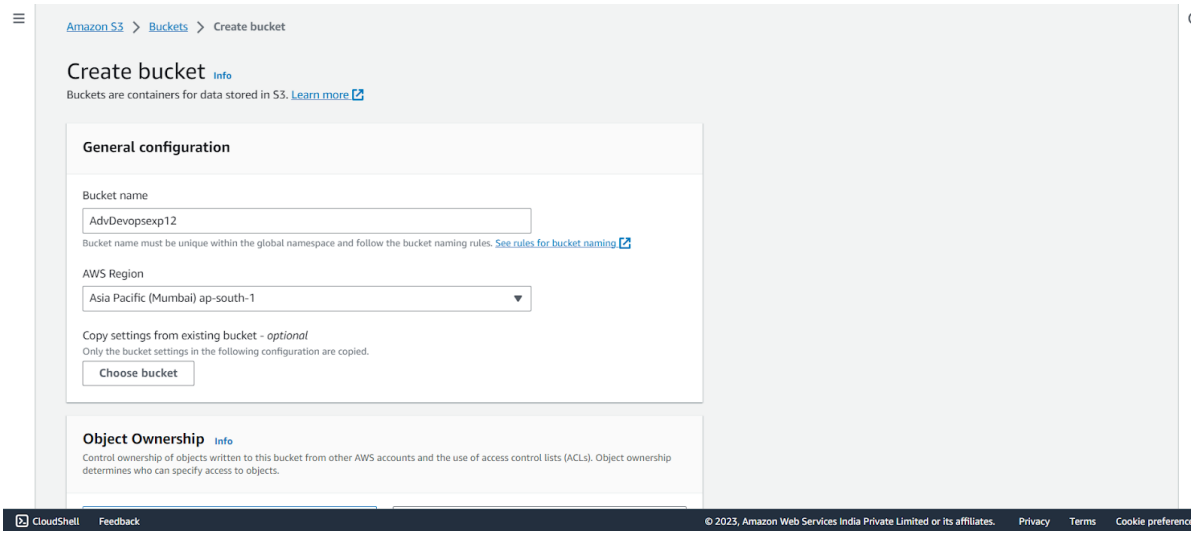


And Save it.

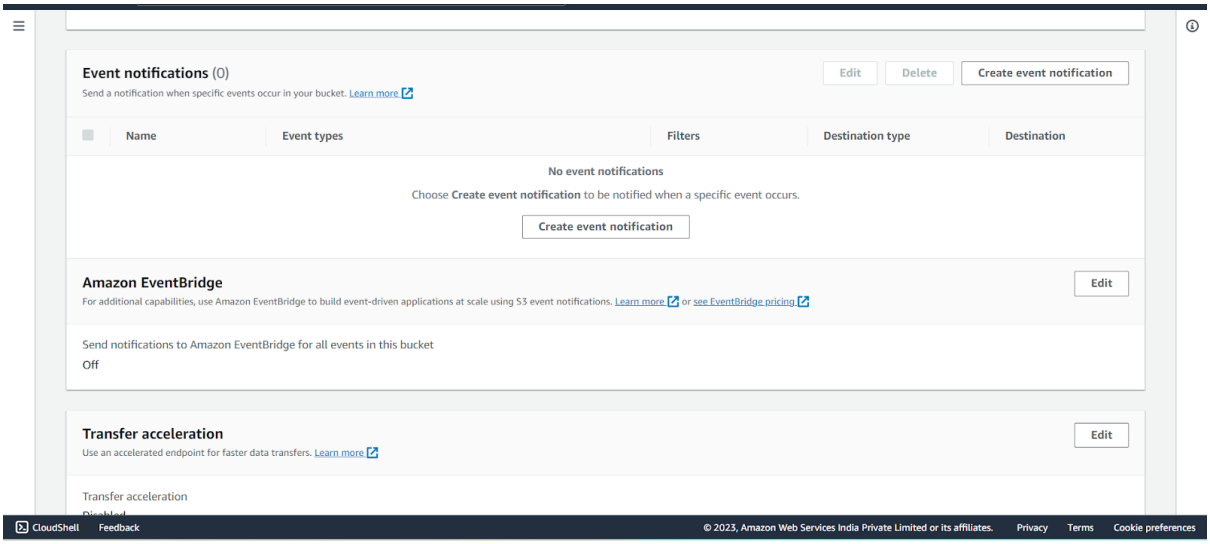
Step 7: Open up the S3 Console and create a new bucket.



Step 8: With all general settings, create the bucket in the same region as the function.

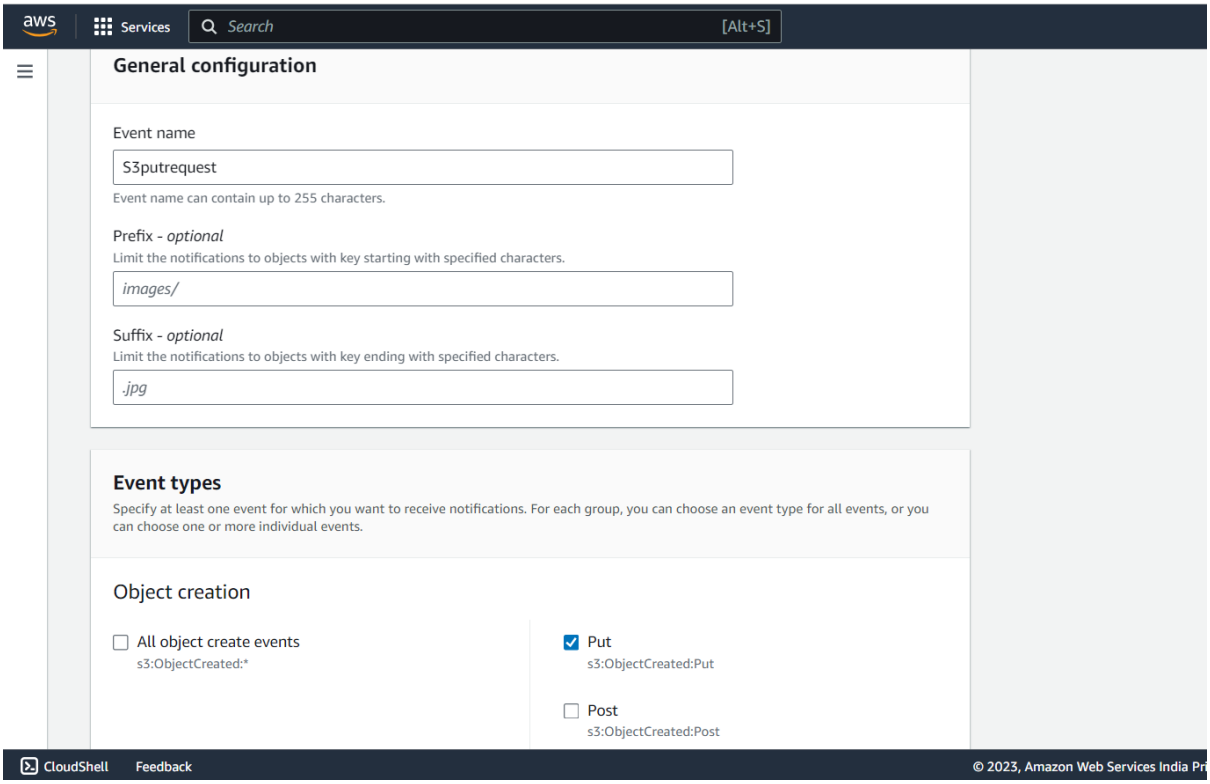


Step 9: Click on the created bucket and under properties, look for events.

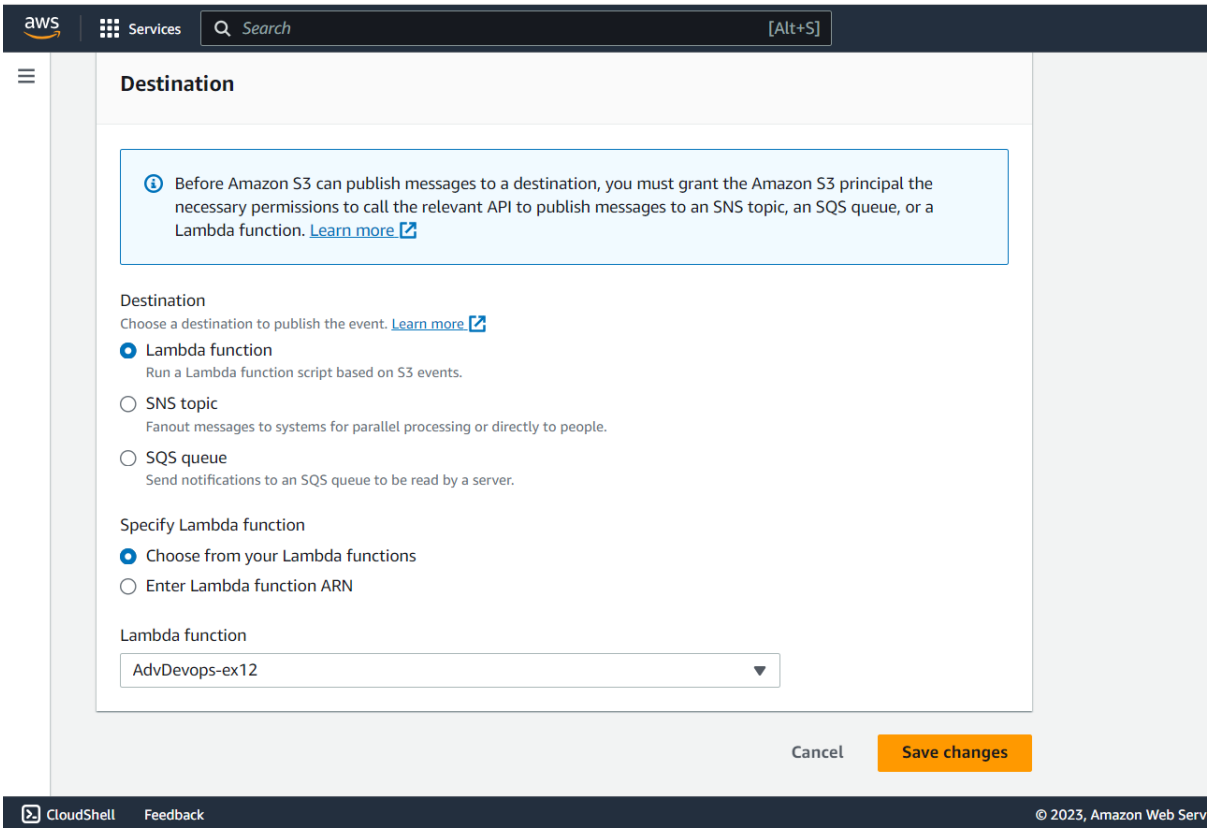


Click on Create Event Notification.

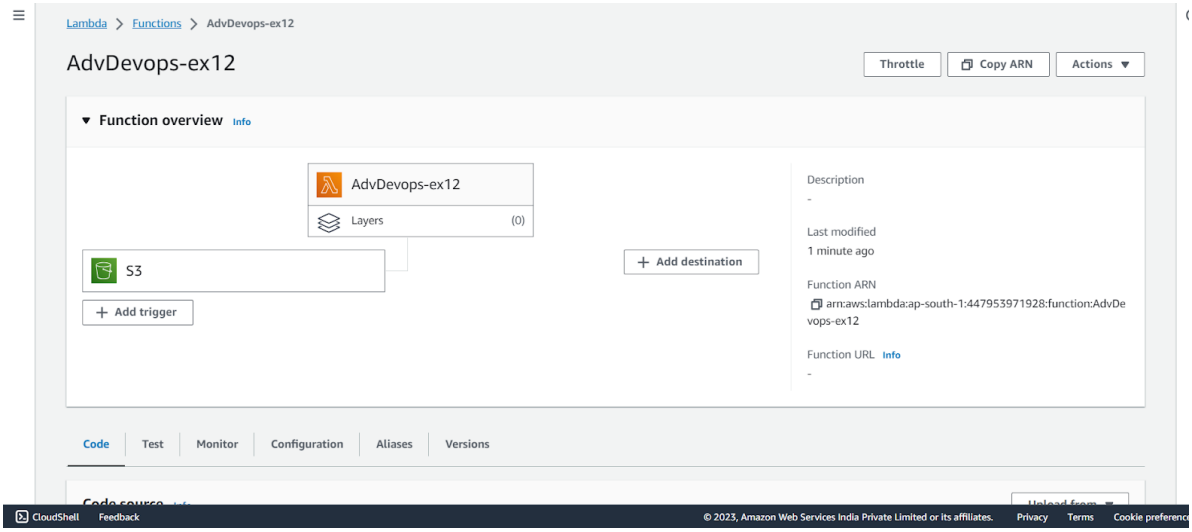
Step 10: Mention an event name and check Put under event types.



Choose Lambda function as destination and choose your lambda function and save the changes.

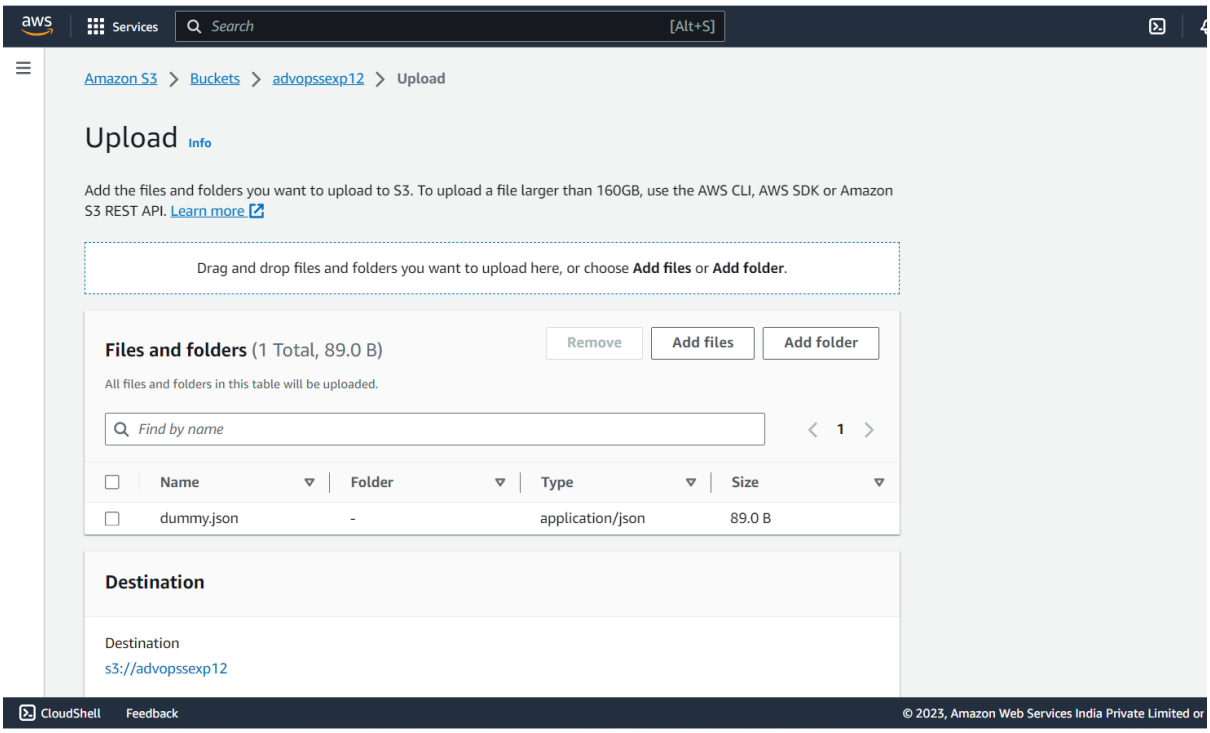


Step 11: Refresh the Lambda function console and you should be able to see an S3 Trigger in the overview.

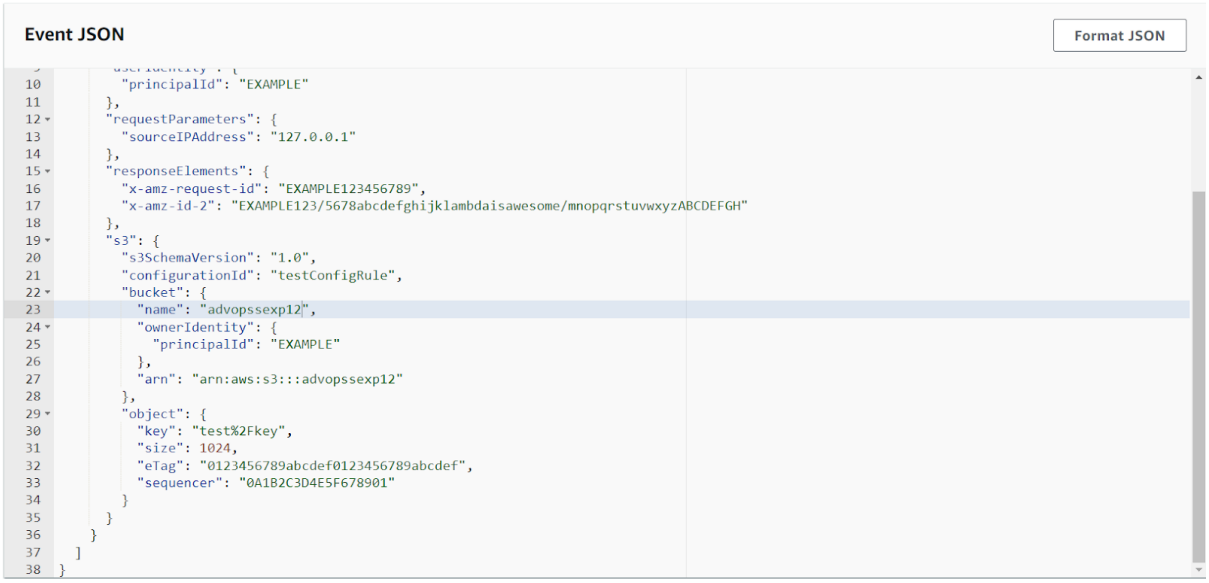


Step 12: Now, create a dummy JSON file locally.

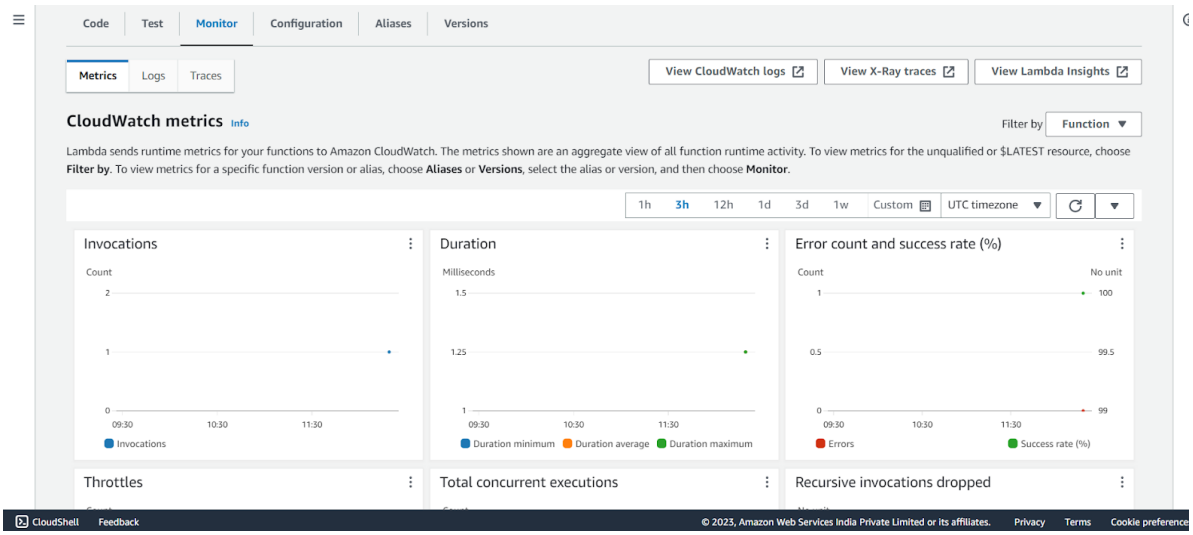
Step 13: Go back to your S3 Bucket and click on Add Files to upload a new file.
Step 14: Select the dummy data file from your computer and click Upload.



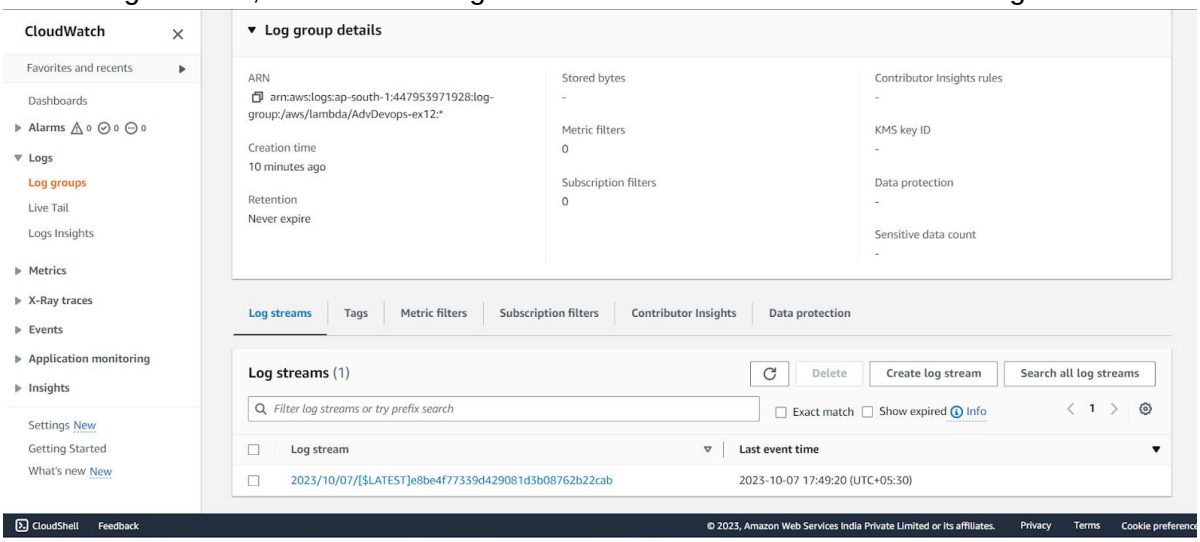
Step 15: After this make the necessary changes in the Test configuration file which we created it previously by replacing the Bucket Name and the ARN of Bucket.



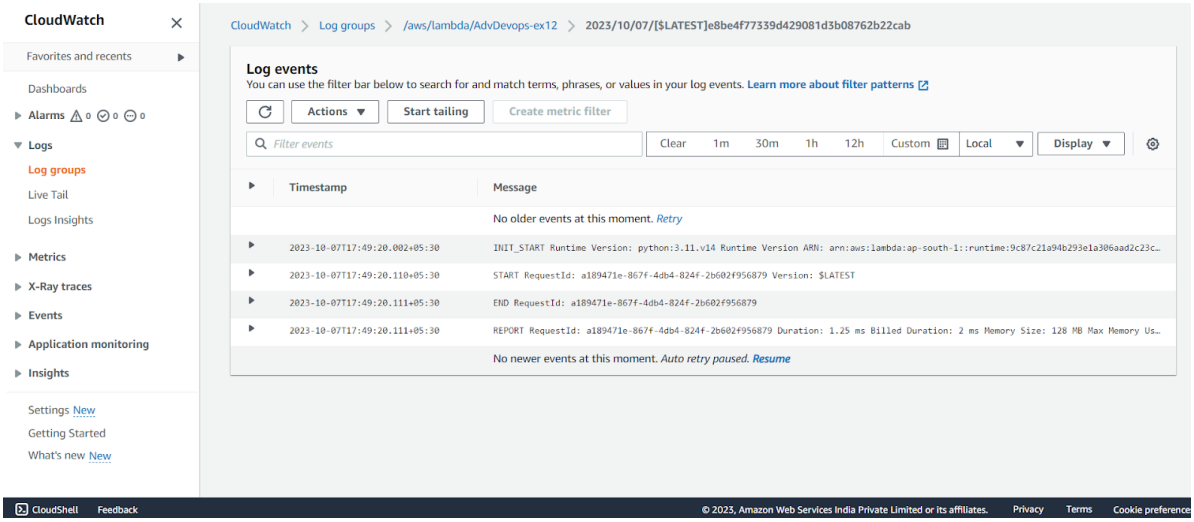
Step 16: Go back to your Lambda function , Refresh it and check the Monitor tab.



Under Log streams, click on View logs in Cloudwatch to check the Function logs.



Step 17: Click on this log Stream that was created to view what was logged by your function.



Conclusion: Thus, we have created a Lambda function which logs “An Image has been added” once you add an object to a specific bucket in S3.