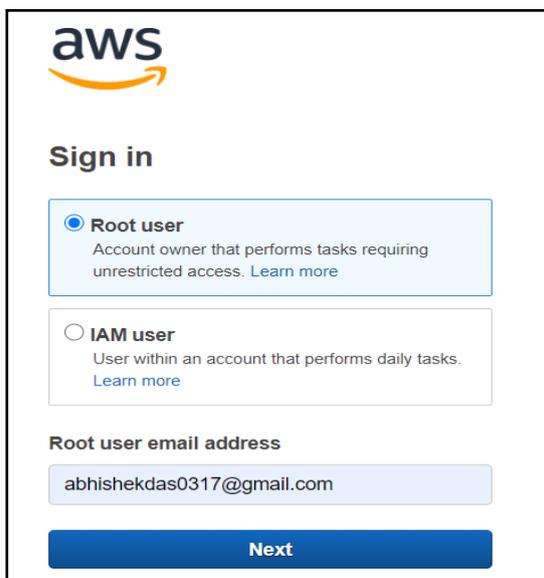


01: EC2 INSTANCE CREATION

AWS EC2 instance: An EC2 instance is a virtual server in Amazon's Elastic Compute Cloud (EC2) for running applications on the Amazon Web Services (AWS) infrastructure.

Process launch EC2 instance:

1. Sign in to the AWS Management Console.



aws

Sign in

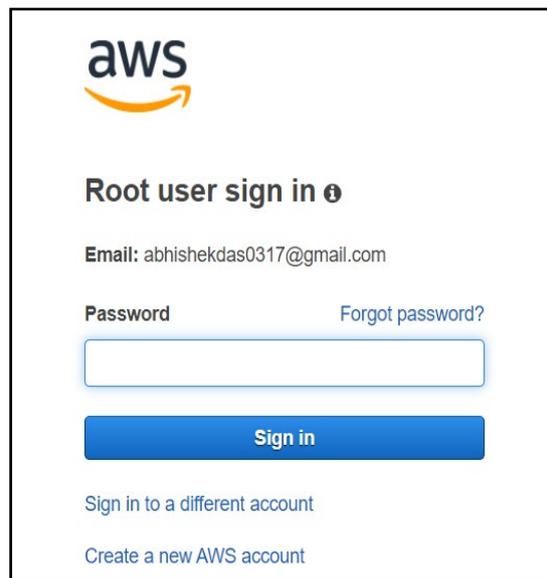
Root user
Account owner that performs tasks requiring unrestricted access. [Learn more](#)

IAM user
User within an account that performs daily tasks. [Learn more](#)

Root user email address

abhishekdas0317@gmail.com

Next



aws

Root user sign in

Email: abhishekdas0317@gmail.com

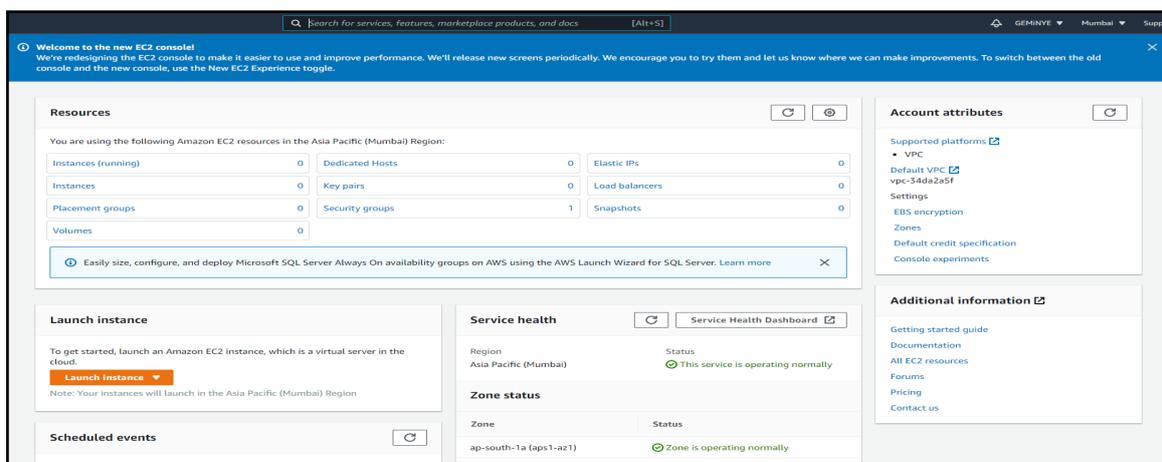
Password [Forgot password?](#)

Sign in

[Sign in to a different account](#)

[Create a new AWS account](#)

2. Choose EC2 from compute services and click on launch instance.



Welcome to the new EC2 console! We're redesigning the EC2 console to make it easier to use and improve performance. We'll release new screens periodically. We encourage you to try them and let us know where we can make improvements. To switch between the old console and the new console, use the New EC2 Experience toggle.

Resources

You are using the following Amazon EC2 resources in the Asia Pacific (Mumbai) Region:

Instances (running)	0	Dedicated Hosts	0	Elastic IPs	0
Instances	0	Key pairs	0	Load balancers	0
Placement groups	0	Security groups	1	Snapshots	0
Volumes	0				

[Easily size, configure, and deploy Microsoft SQL Server Always On availability groups on AWS using the AWS Launch Wizard for SQL Server. Learn more](#)

Launch instance

To get started, launch an Amazon EC2 instance, which is a virtual server in the cloud.

Launch instance

Note: Your instances will launch in the Asia Pacific (Mumbai) Region

Scheduled events

Service health

Region: Asia Pacific (Mumbai) | Status: ✔ This service is operating normally

Zone status

Zone	Status
ap-south-1a (ap-s1-az1)	✔ Zone is operating normally

Account attributes

Supported platforms

- VPC
- Default VPC: vpc-34da2a5f

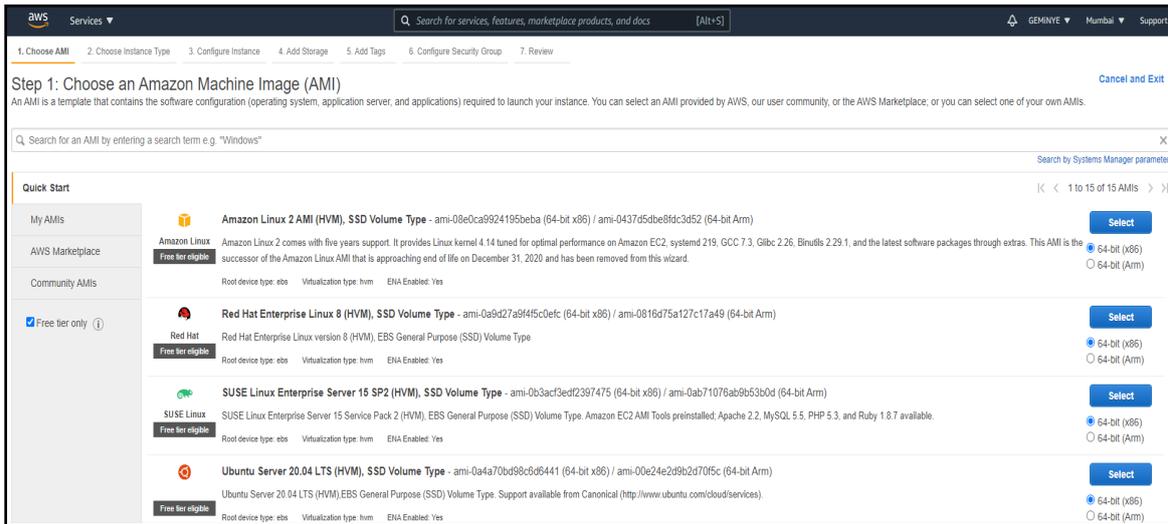
Settings

- EBS encryption
- Zones
- Default credit specification
- Console experiments

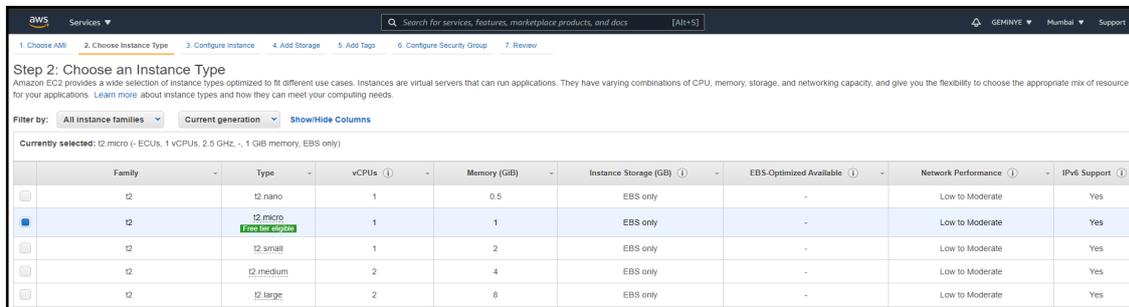
Additional information

- Getting started guide
- Documentation
- All EC2 resources
- Forums
- Pricing
- Contact us

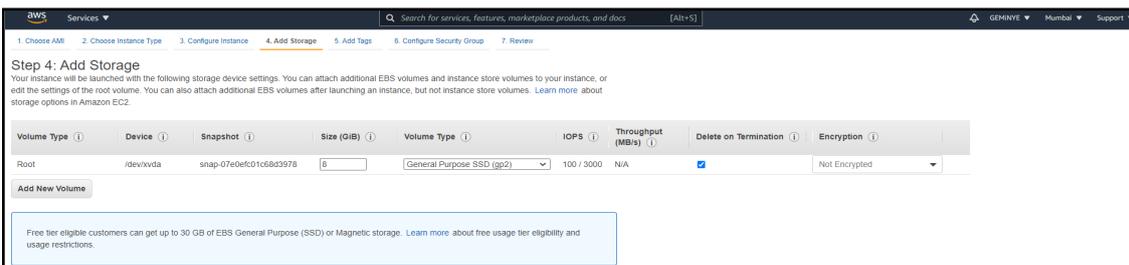
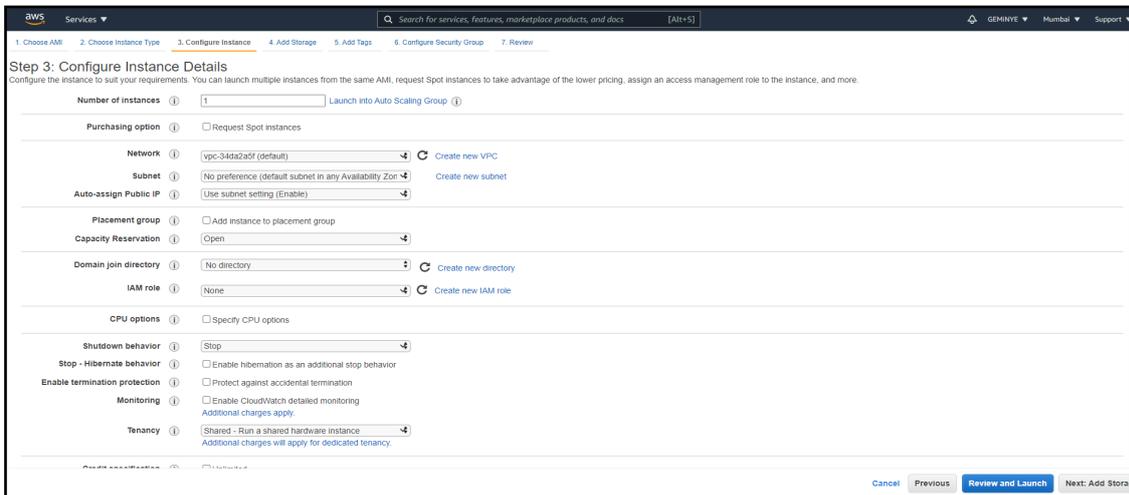
3. Tick on free tier and select AMI AMZON from free tier services.



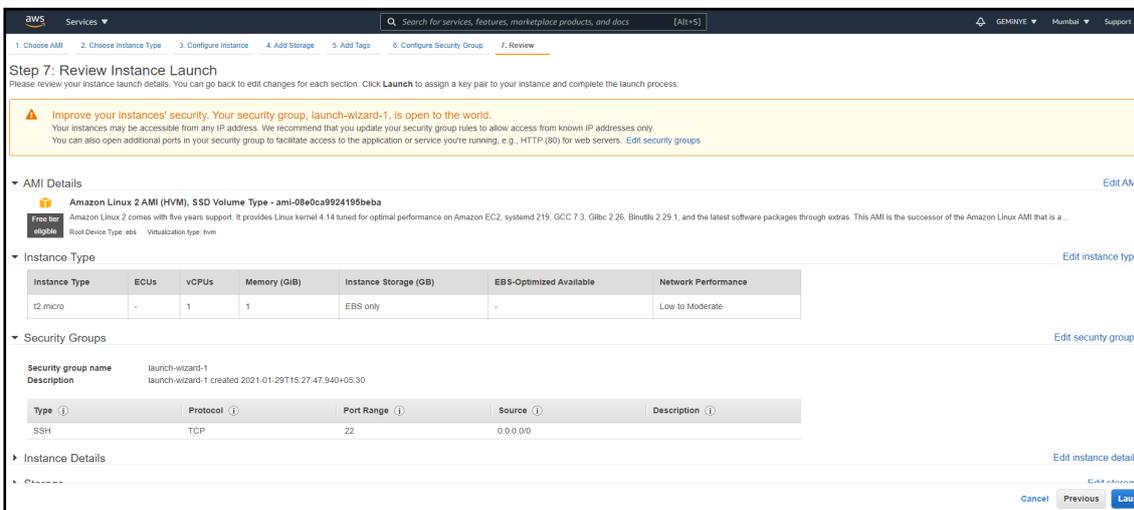
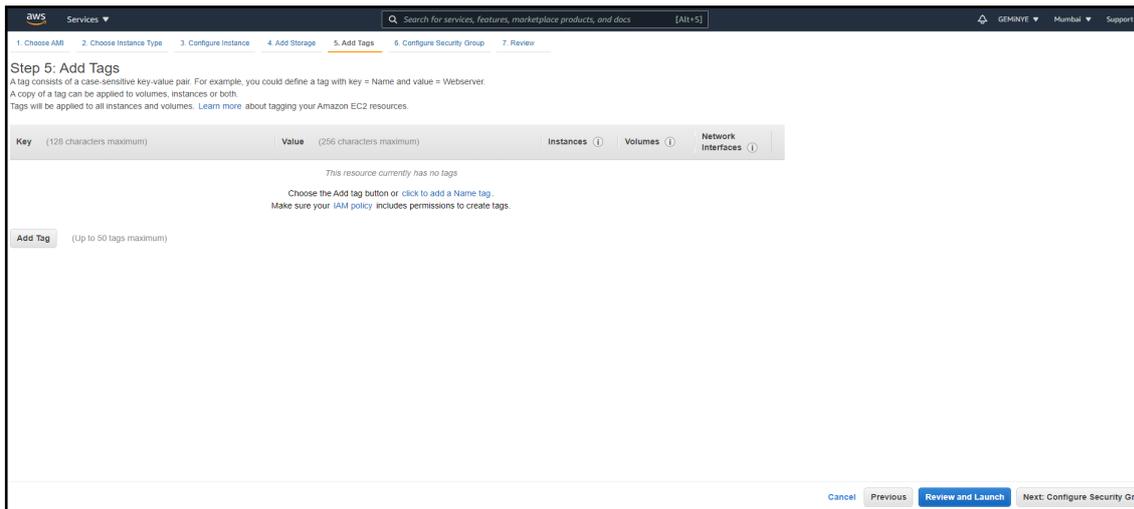
4. Choose free tier 1cpu 1gh ram (t2 micro).



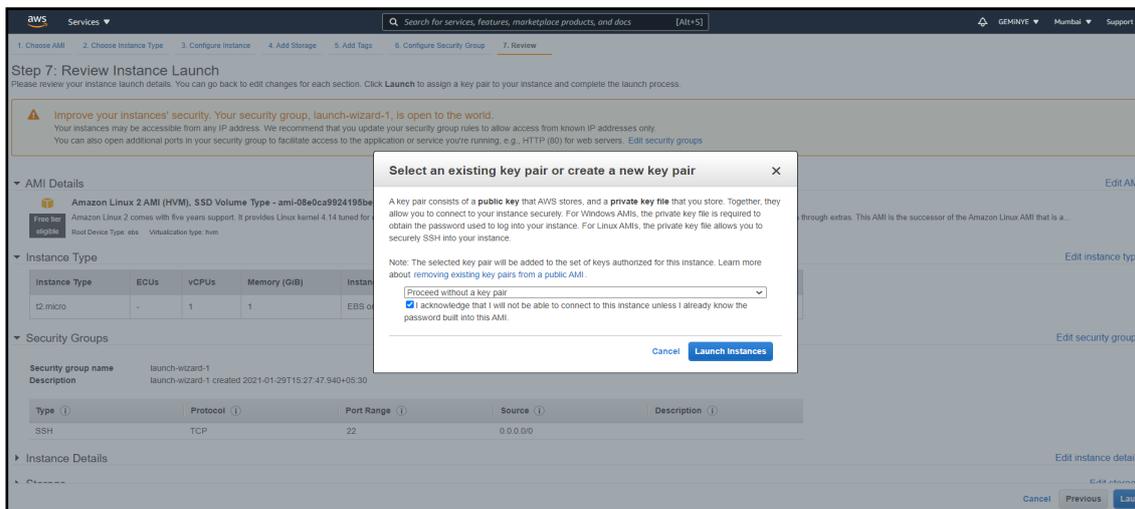
5. Configure instance detail and add storage.



6. Click on review and launch.



7. Continue without a key pair.



8. Click on launch Instance.

Launch Status

✔ Your instances are now launching
The following instance launches have been initiated: i-02f5dbfc98c80f88d [View launch log](#)

ℹ Get notified of estimated charges
Create billing alerts to get an email notification when estimated charges on your AWS bill exceed an amount you define (for example, if you exceed the free usage tier).

How to connect to your instances
Your instances are launching, and it may take a few minutes until they are in the **running** state, when they will be ready for you to use. Usage hours on your new instances will start immediately and continue to accrue until you stop or terminate your instances. Click **View Instances** to monitor your instances' status. Once your instances are in the **running** state, you can **connect** to them from the Instances screen. [Find out: how to connect to your instances.](#)

Here are some helpful resources to get you started

- [How to connect to your Linux instance](#)
- [Learn about AWS Free Usage Tier](#)
- [Amazon EC2: User Guide](#)
- [Amazon EC2: Discussion Forum](#)

While your instances are launching you can also

- [Create status check alarms](#) to be notified when these instances fail status checks. (Additional charges may apply)
- [Create and attach additional EBS volumes](#) (Additional charges may apply)
- [Manage security groups](#)

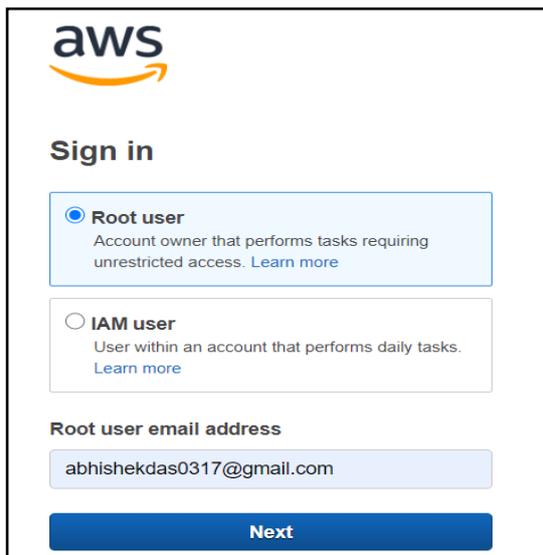
[View Instances](#)

02: Creating VPC

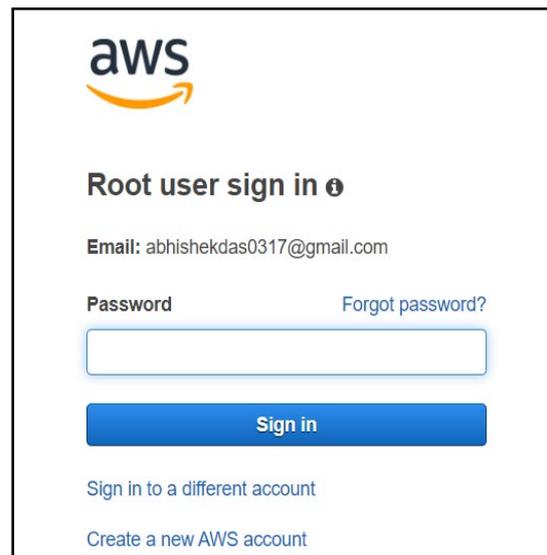
VPC (Virtual Private Cloud): Amazon Virtual Private Cloud (Amazon VPC) enables you to launch Amazon Web Services (AWS) resources into a virtual network you've defined. This virtual network resembles a traditional network that you'd operate in your own data centre, with the benefits of using the scalable infrastructure of AWS.

Process to configure VPC:

1. Sign in to the AWS Management Console.

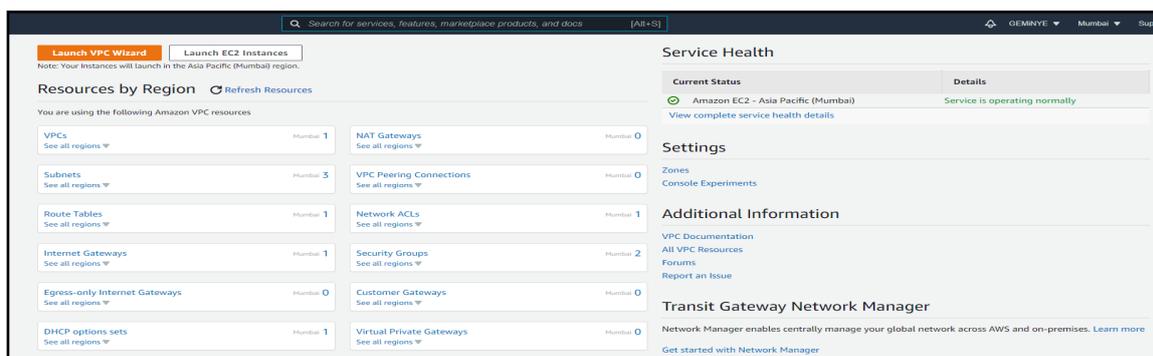


The screenshot shows the AWS Sign in page. At the top is the AWS logo. Below it is the heading 'Sign in'. There are two radio button options: 'Root user' (selected) and 'IAM user'. The 'Root user' option includes the text 'Account owner that performs tasks requiring unrestricted access. Learn more'. The 'IAM user' option includes 'User within an account that performs daily tasks. Learn more'. Below these options is a field for 'Root user email address' containing 'abhishekdas0317@gmail.com'. At the bottom is a blue 'Next' button.



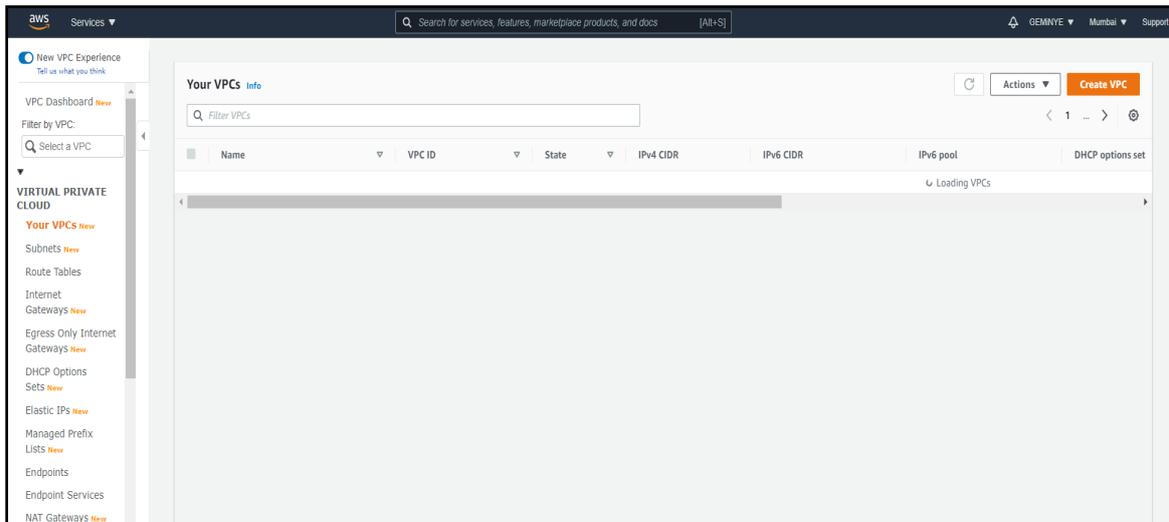
The screenshot shows the AWS Root user sign in page. At the top is the AWS logo. Below it is the heading 'Root user sign in'. The email field is filled with 'abhishekdas0317@gmail.com'. There is a 'Forgot password?' link. Below the email field is a password input field. At the bottom is a blue 'Sign in' button. Below the button are two links: 'Sign in to a different account' and 'Create a new AWS account'.

2. Open VPC from services under networking.

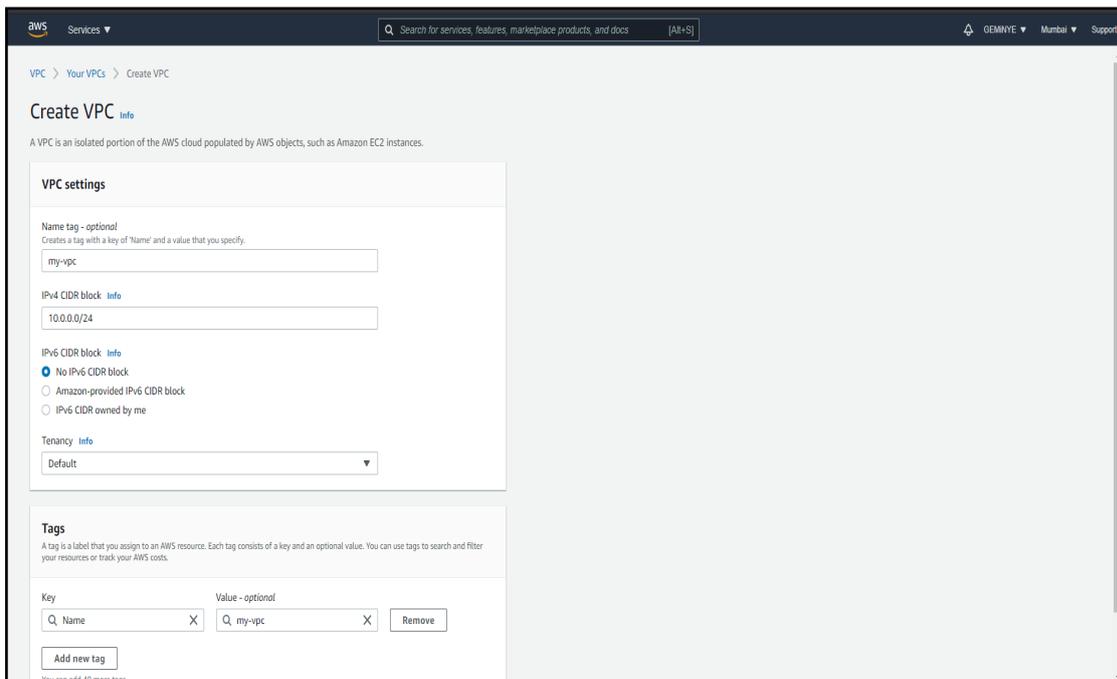


The screenshot shows the AWS Management Console interface. At the top, there is a search bar and navigation elements. Below the search bar, there are two tabs: 'Launch VPC Wizard' (selected) and 'Launch EC2 Instances'. A note states: 'Note: Your Instances will launch in the Asia Pacific (Mumbai) region.' Below this is the 'Resources by Region' section, which lists various AWS services and their counts for the Mumbai region. The services listed are: VPCs (1), Subnets (3), Route Tables (1), Internet Gateways (1), Egress-only Internet Gateways (0), DHCP options sets (1), NAT Gateways (0), VPC Peering Connections (0), Network ACLs (1), Security Groups (2), Customer Gateways (0), and Virtual Private Gateways (0). On the right side, there is a 'Service Health' section showing the status of 'Amazon EC2 - Asia Pacific (Mumbai)' as 'Service is operating normally'. Below that is a 'Settings' section with links for 'Zones' and 'Console Experiments'. At the bottom right, there is an 'Additional Information' section with links for 'VPC Documentation', 'All VPC Resources', 'Forums', and 'Report an Issue'. At the very bottom right, there is a 'Transit Gateway Network Manager' section with a brief description and a 'Get started with Network Manager' link.

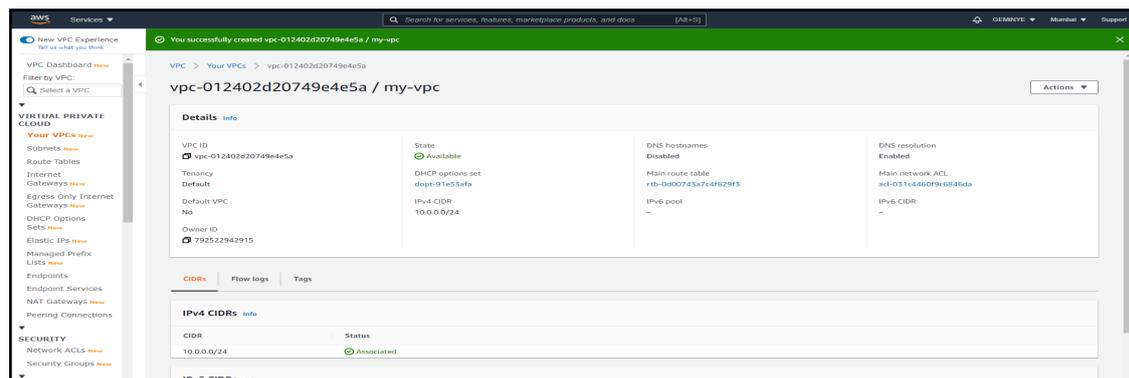
3. Click on your VPC and create VPC.



4. Configure VPC using name of VPC and IP range.



5. Check VPC status.

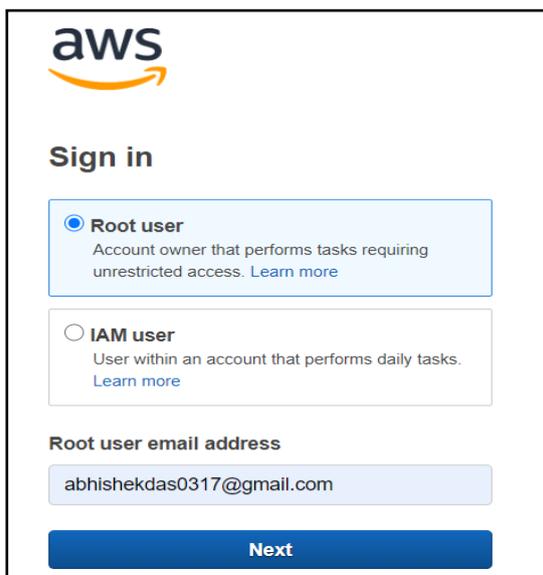


03: Configure Subnet

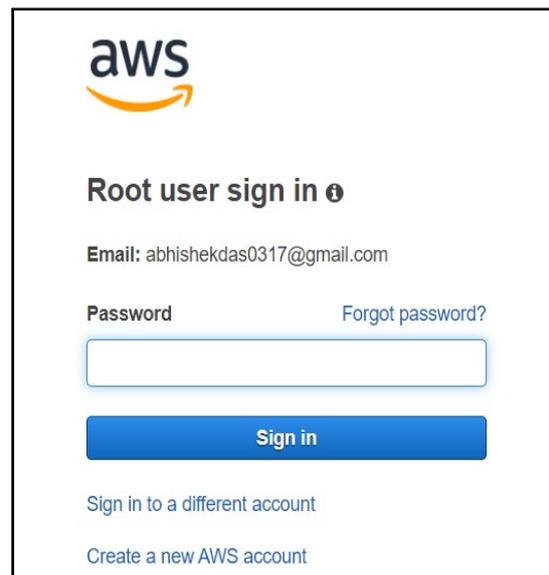
About Subnet: Subnet is a logical subdivision of an IP network. The practice of dividing a network into two or more networks is called subnetting. AWS provides two types of subnetting one is Public which allow the internet to access the machine and another is private which is hidden from the internet.

Process to configure Subnet:

1. Sign in to the AWS Management Console.

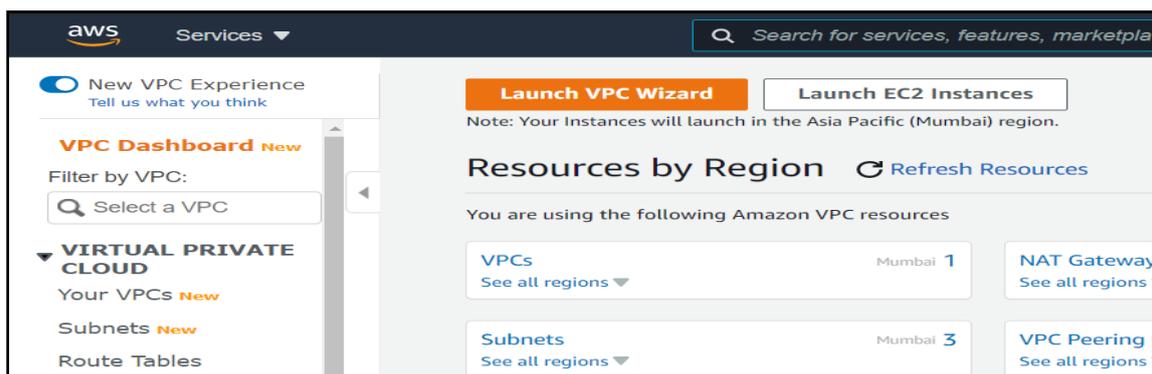


The screenshot shows the AWS Sign in page. At the top is the AWS logo. Below it is the heading "Sign in". There are two radio button options: "Root user" (selected) and "IAM user". The "Root user" option includes the text "Account owner that performs tasks requiring unrestricted access. [Learn more](#)". The "IAM user" option includes the text "User within an account that performs daily tasks. [Learn more](#)". Below these options is a field for "Root user email address" containing the email "abhishekdas0317@gmail.com". At the bottom is a blue "Next" button.

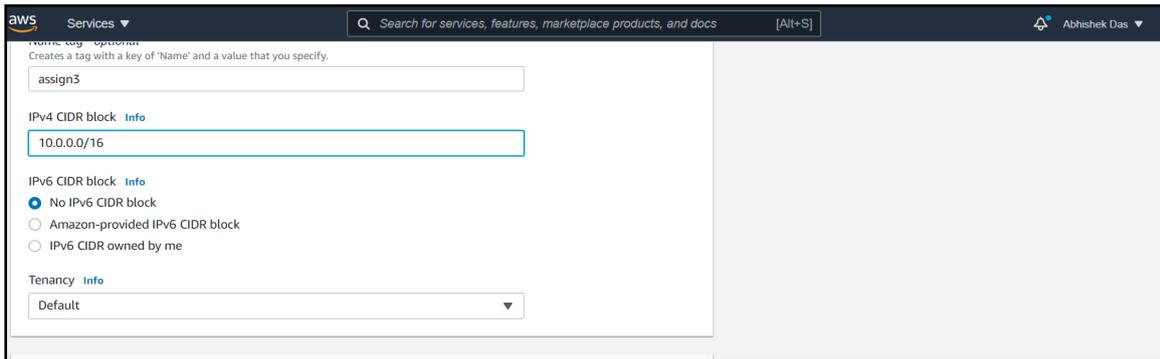
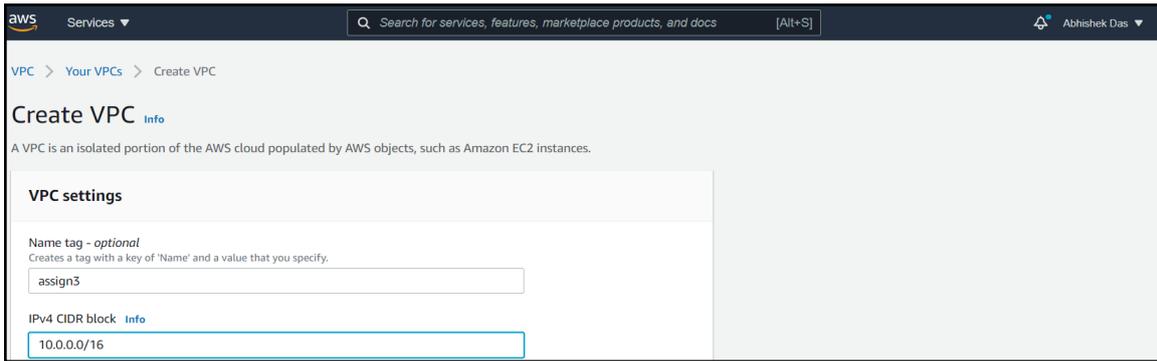


The screenshot shows the AWS Root user sign in page. At the top is the AWS logo. Below it is the heading "Root user sign in". There is an "Email" field containing "abhishekdas0317@gmail.com" and a "Password" field. To the right of the password field is a link "Forgot password?". Below the password field is a blue "Sign in" button. At the bottom are two links: "Sign in to a different account" and "Create a new AWS account".

2. Click on VPC from service and configure it by providing name, IPv4 CIDR block and click on create VPC.

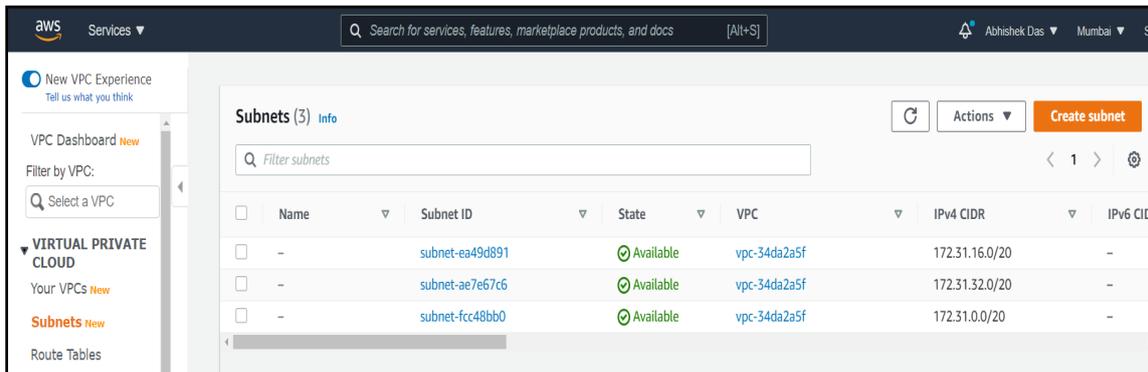


The screenshot shows the AWS Management Console. At the top is the AWS logo and "Services" dropdown. Below it is a search bar. The main content area is titled "Resources by Region" and shows a summary of VPC resources in the Mumbai region. It includes buttons for "Launch VPC Wizard" and "Launch EC2 Instances". Below the summary are two cards: "VPCs" (1 in Mumbai) and "Subnets" (3 in Mumbai). To the right are links for "NAT Gateway" and "VPC Peering". On the left side, there is a sidebar with a "VPC Dashboard" link and a search filter for VPCs.

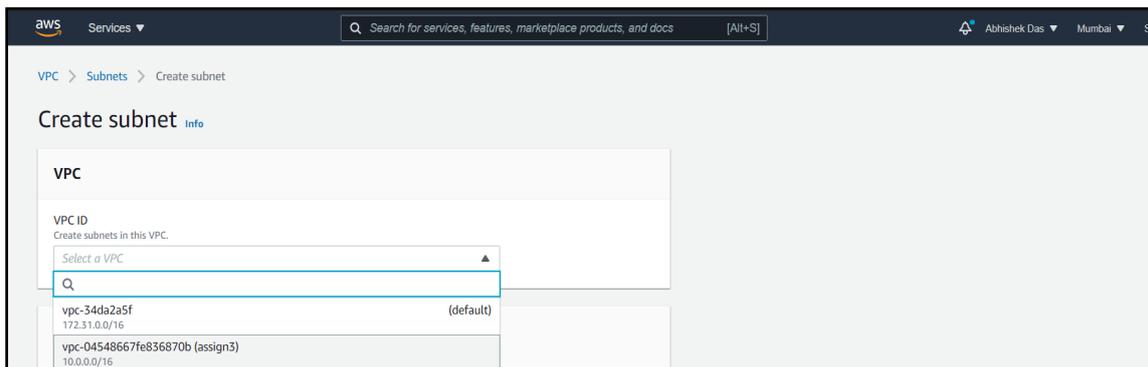


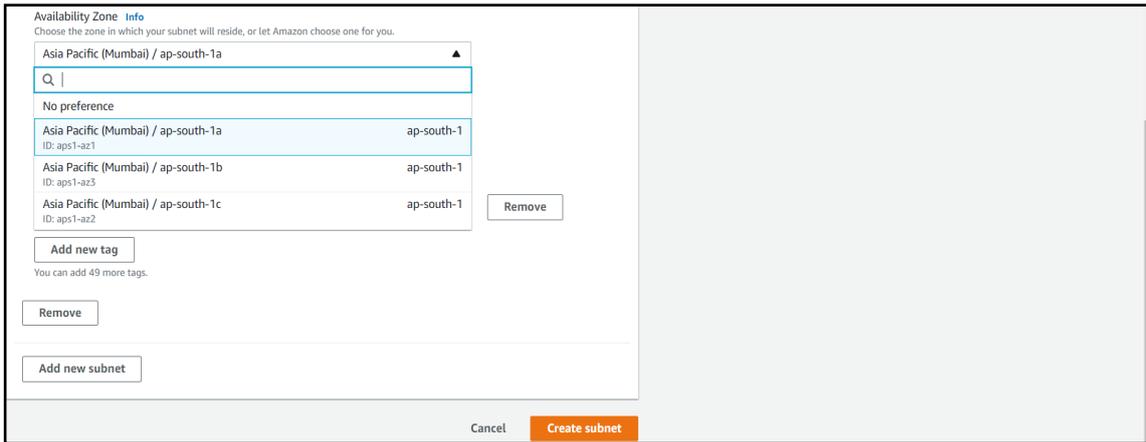
Configuration of Private Subnet

3. Now click on Subnet to configure private subnet.



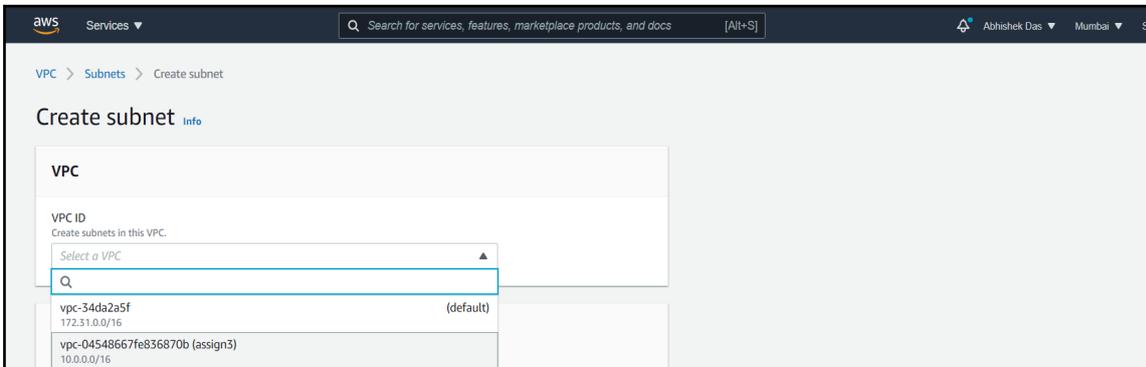
4. Provide VPC ID and availability zone then click on create Subnet.



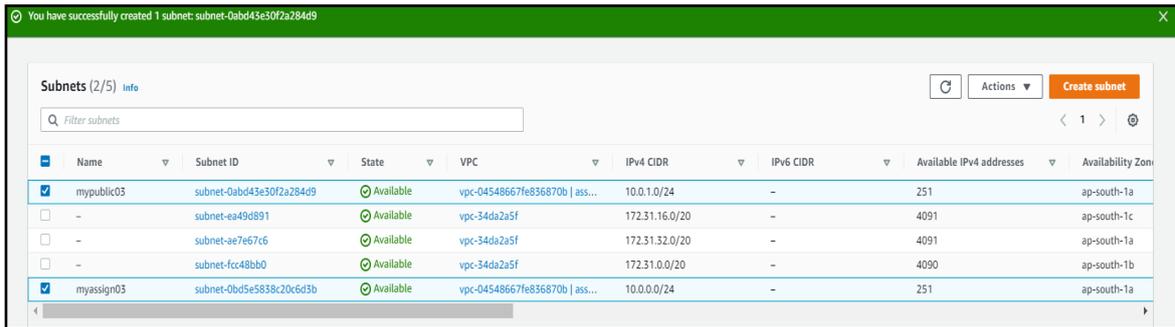


Configuration of Public Subnet

- Now again click on Subnet to create Public Subnet provide VPC ID and availability zone also provide IPv4 CIDR no as **10.0.1.0/26** to make it public.

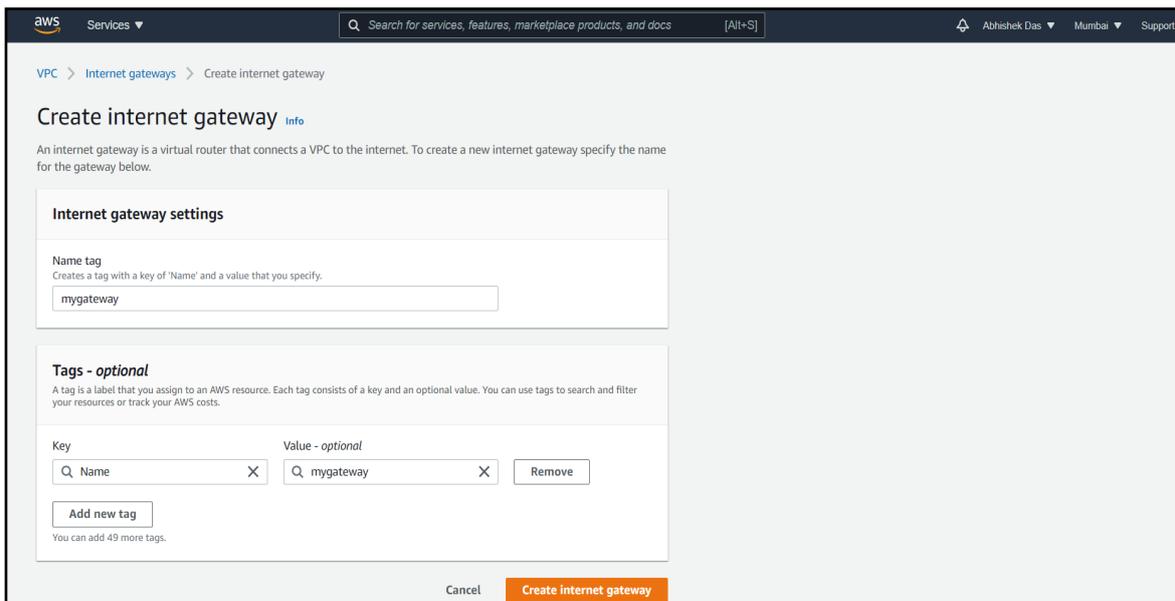


6. Then click on create subnet.

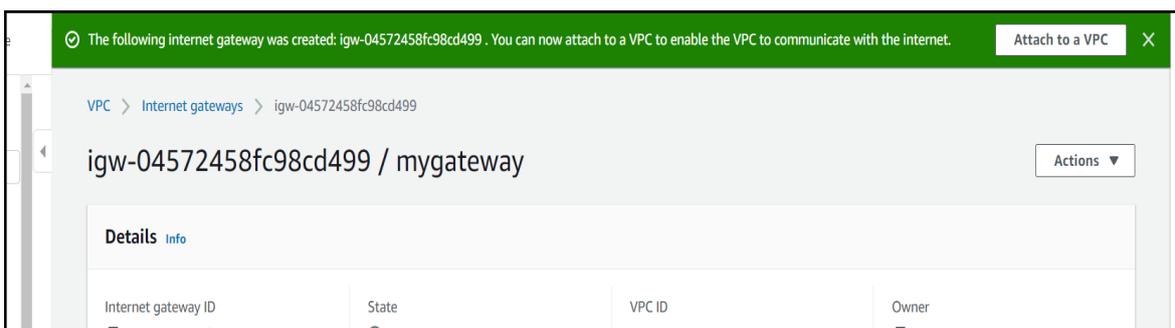


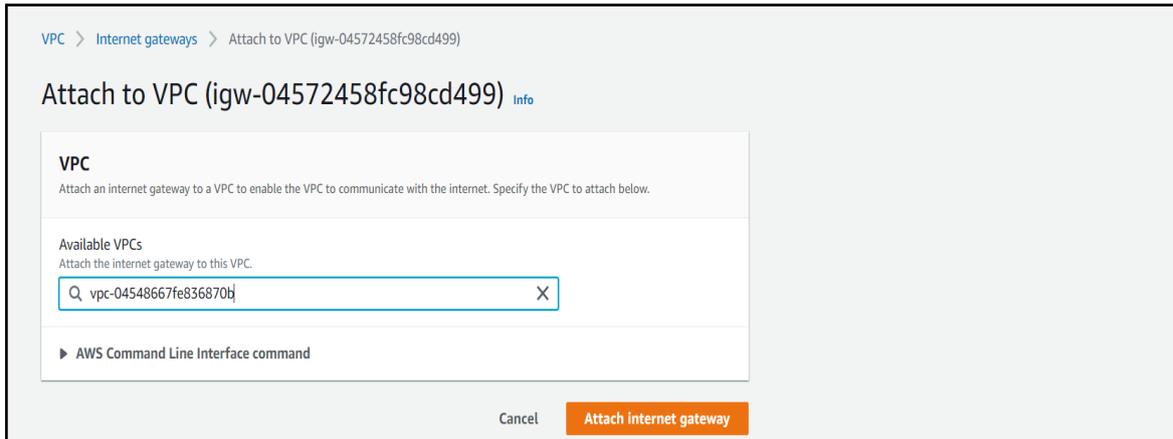
Configuration of Internet Gateway

7. Now click on Internet gateway and write its tag name then click on create Internet gateway.



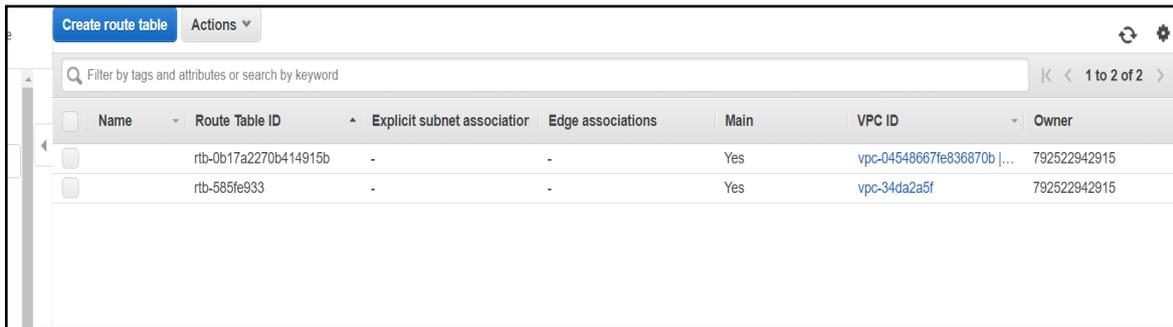
8. Then click on attach to a VPC and browse the VPC and select attach Internet Gateway.





Configuration of Route Table

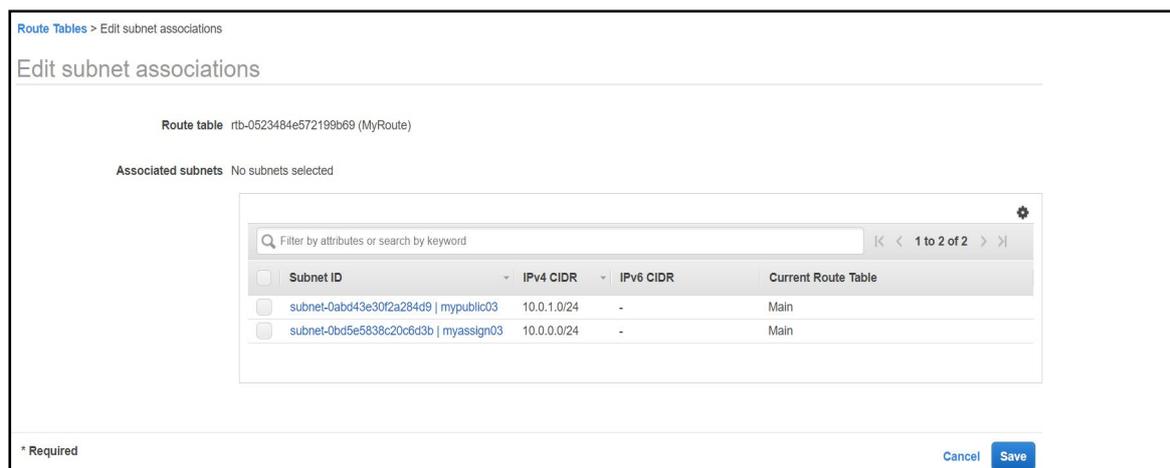
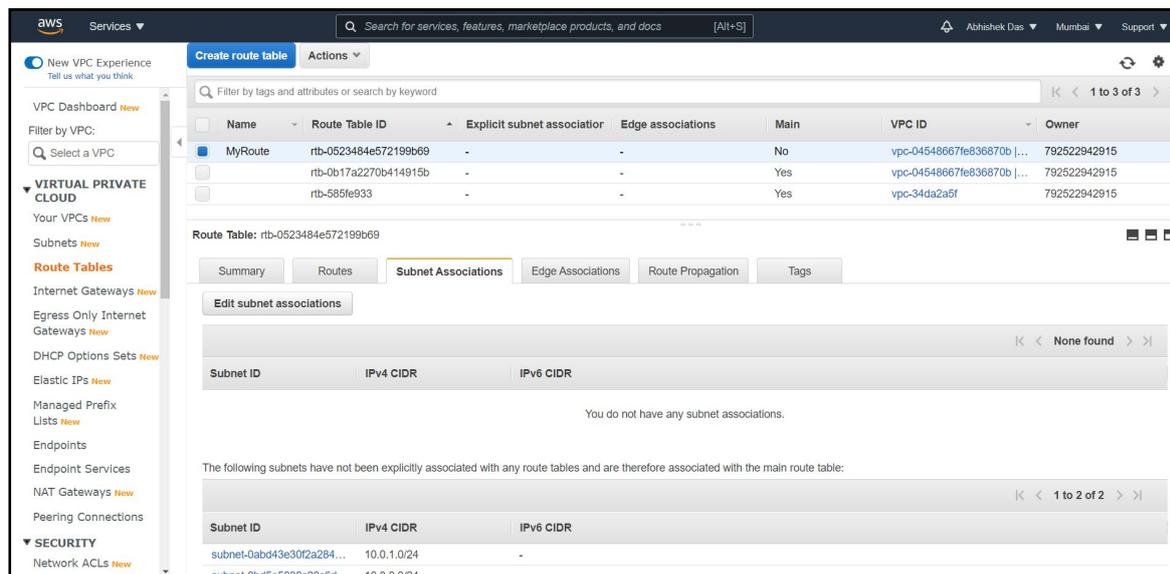
9. Click on Route Table and click on Create route table.



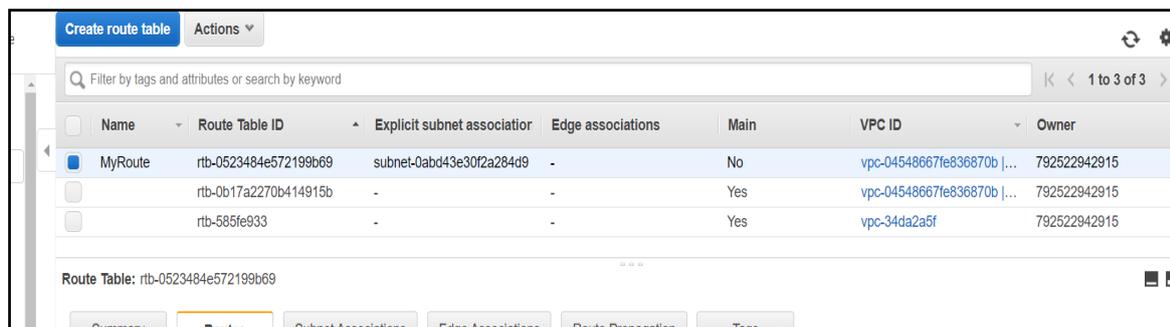
10. Provide its Name tag and browse VPC. Then click on Create.



11. Then go to Subnet Association under its detail and select public subnet and click on save.



12. Now go to Route and click on Add Route and give its Destination and target.



Route Tables > Edit routes

Edit routes

Destination	Target	Status	Propagated
10.0.0.0/16	local	active	No
0.0.0.0/0	igw-		No

Add route

* Required

Cancel Save routes

13. Open EC2 service then where we can find our custom VPC, Subnet.

1. Choose AMI 2. Choose Instance Type 3. Configure Instance 4. Add Storage 5. Add Tags 6. Configure Security Group 7. Review

Step 3: Configure Instance Details

Configure the instance to suit your requirements. You can launch multiple instances from the same AMI, request Spot instances to take advantage of the lower pricing, assign an access management role to the instance, and more.

Number of instances: 1 [Launch into Auto Scaling Group](#)

Purchasing option: Request Spot instances

Network: vpc-34da2a5f (default) [Create new VPC](#)

Subnet: vpc-34da2a5f (default) [Create new subnet](#)

Auto-assign Public IP: Use subnet setting (Enable)

Placement group: Add instance to placement group

Capacity Reservation: Open

Domain join directory: No directory [Create new directory](#)

IAM role: None [Create new IAM role](#)

CPU options: Specify CPU options

Shutdown behavior: Stop

Stop - Hibernate behavior: Enable hibernation as an additional stop behavior

Enable termination protection: Protect against accidental termination

Cancel Previous **Review and Launch** Next: Add Storage

1. Choose AMI 2. Choose Instance Type 3. Configure Instance 4. Add Storage 5. Add Tags 6. Configure Security Group 7. Review

Step 3: Configure Instance Details

Configure the instance to suit your requirements. You can launch multiple instances from the same AMI, request Spot instances to take advantage of the lower pricing, assign an access management role to the instance, and more.

Number of instances: 1 [Launch into Auto Scaling Group](#)

Purchasing option: Request Spot instances

Network: vpc-04548667fe836870b | assign3 [Create new VPC](#)

Subnet: subnet-0abd43e3072a284d9 | mypublic03 | ap-south-1 [Create new subnet](#)

Auto-assign Public IP: Use subnet setting (Disable)

Placement group: Add instance to placement group

Capacity Reservation: Open

Domain join directory: No directory [Create new directory](#)

IAM role: None [Create new IAM role](#)

CPU options: Specify CPU options

Shutdown behavior: Stop

Stop - Hibernate behavior: Enable hibernation as an additional stop behavior

Cancel Previous **Review and Launch** Next: Add Storage

04: EBS

About EBS (Elastic Block Store): Amazon Elastic Block Store (EBS) is an easy to use, high-performance, block-storage service designed for use with Amazon Elastic Compute Cloud (EC2) for both throughput and transaction intensive workloads at any scale.

Process to Configure EBS:

1. Sign in to the AWS Management Console.

aws

Sign in

Root user
Account owner that performs tasks requiring unrestricted access. [Learn more](#)

IAM user
User within an account that performs daily tasks. [Learn more](#)

Root user email address

abhishekdas0317@gmail.com

Next

aws

Root user sign in

Email: abhishekdas0317@gmail.com

Password [Forgot password?](#)

Sign in

[Sign in to a different account](#)

[Create a new AWS account](#)

2. Now go to EC2 service and click on volume. Then click on Create Volume.

aws Services

Search for services, features, marketplace products, and docs [Alt+S]

Abhishek Das Mumbai Support

Resources

You are using the following Amazon EC2 resources in the Asia Pacific (Mumbai) Region:

Instances (running)	0	Dedicated Hosts	0
Elastic IPs	0	Instances	0
Key pairs	0	Load balancers	0
Placement groups	0	Security groups	8
Snapshots	0	Volumes	0

Launch instance

To get started, launch an Amazon EC2 instance, which is a virtual server in the cloud.

Launch instance

Note: Your instances will launch in the Asia Pacific (Mumbai) Region

Service health

Service Health Dashboard

Region: Asia Pacific (Mumbai) Status: ✔ This service is operating normally

Account attributes

Supported platforms

- VPC
- Default VPC vpc-34da2a5f

Settings

- EBS encryption
- Zones
- Default credit specification
- Console experiments

Explore AWS

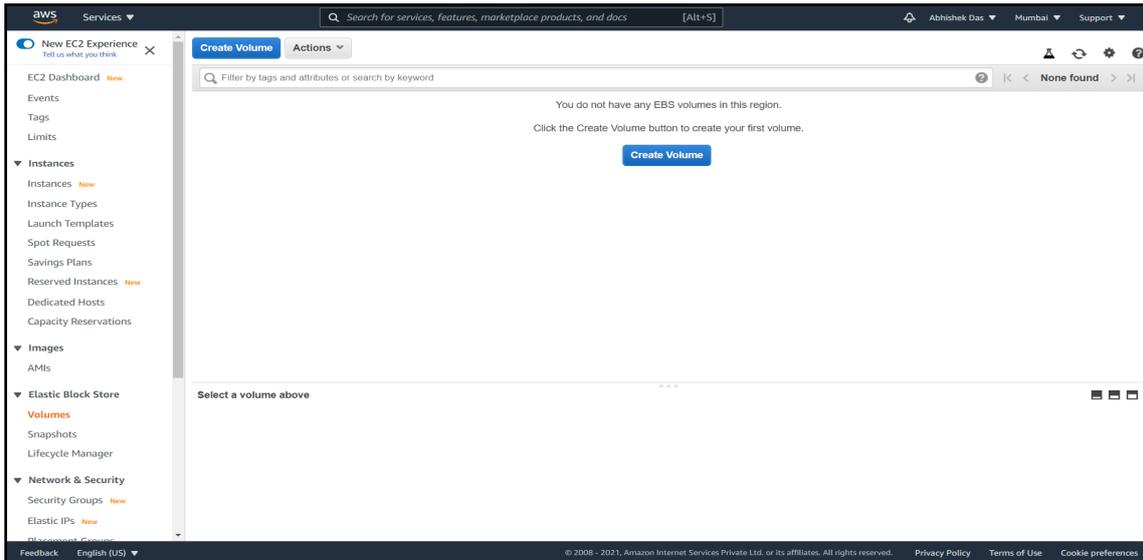
Get Up to 40% Better Price Performance

T4g instances deliver the best price performance for burstable general purpose workloads in Amazon EC2. [Learn more](#)

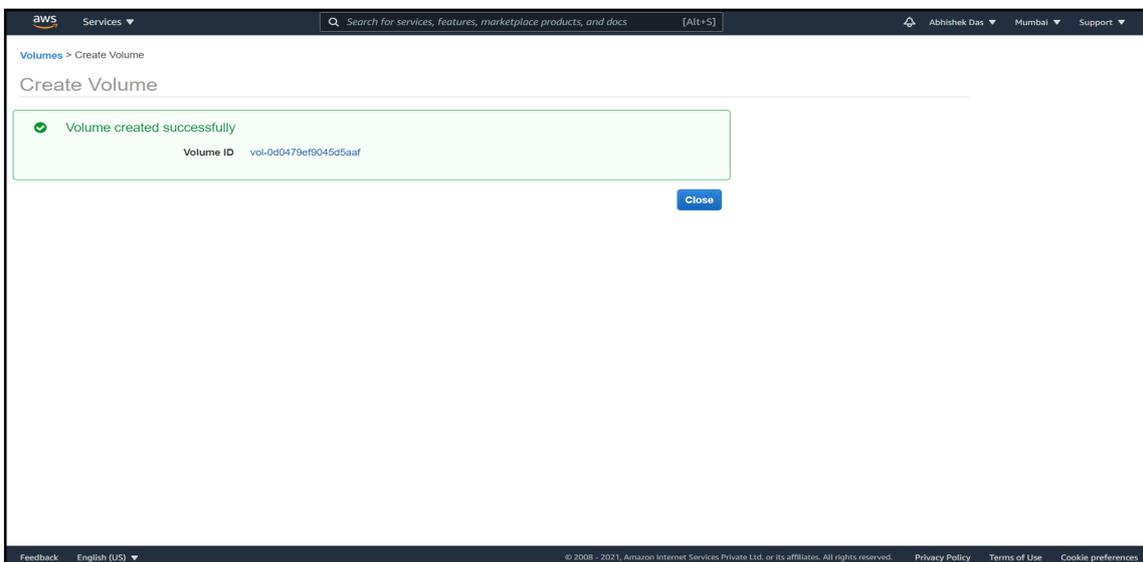
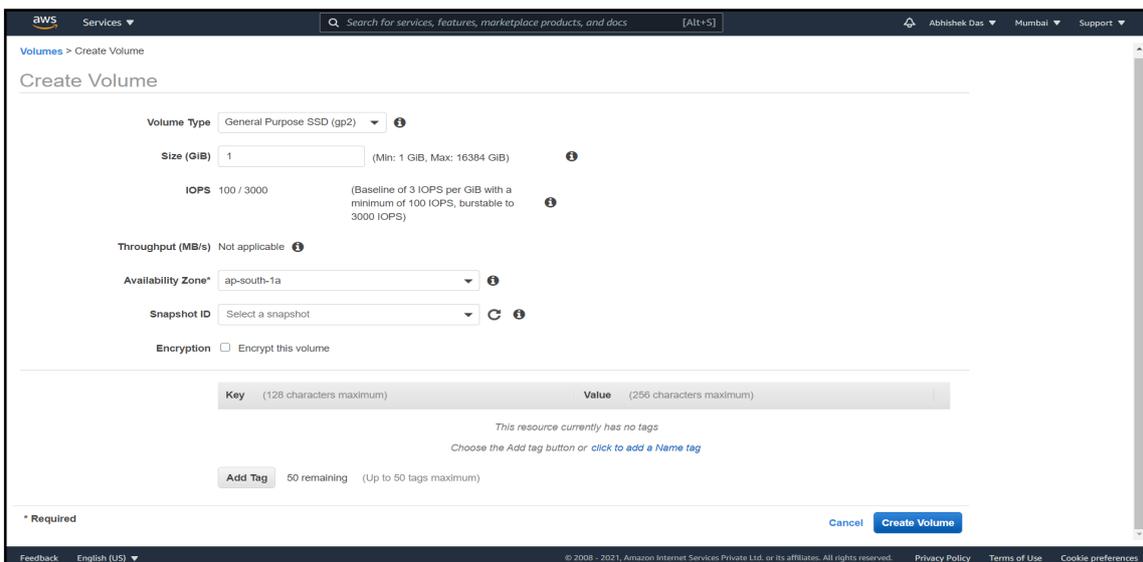
Enable Best Price-Performance with AWS Graviton2

AWS Graviton2 powered EC2 instances enable up to 40% better price performance for a broad spectrum of cloud workloads. [Learn more](#)

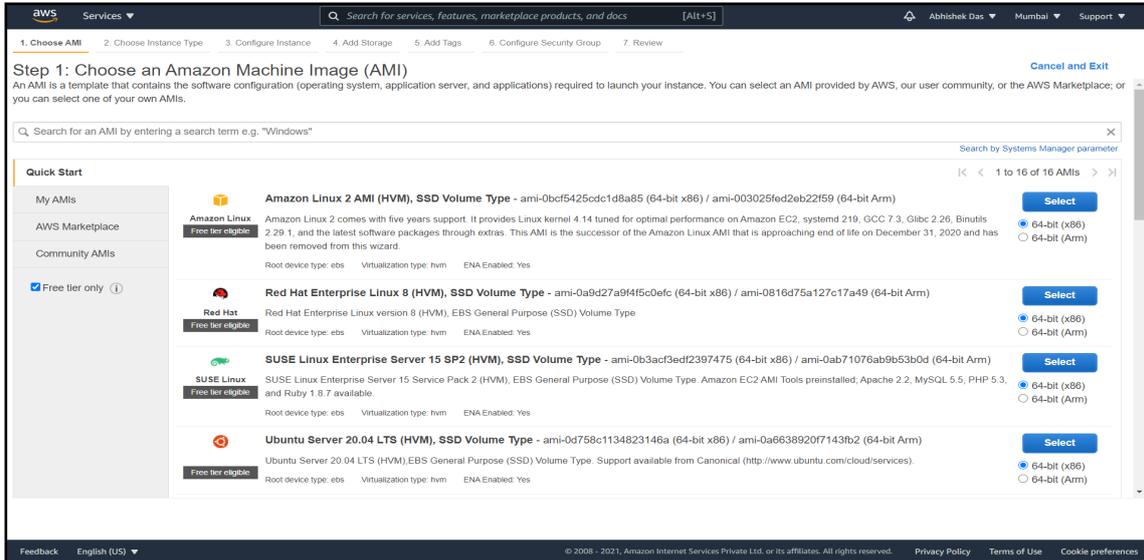
© 2008 - 2021, Amazon Internet Services Private Ltd. or its affiliates. All rights reserved. Privacy Policy Terms of Use Cookie pr



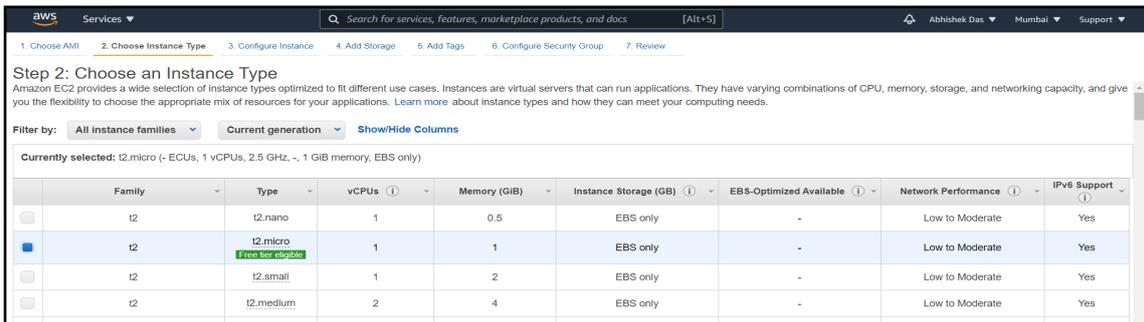
3. Provide its size and click on Create Volume.



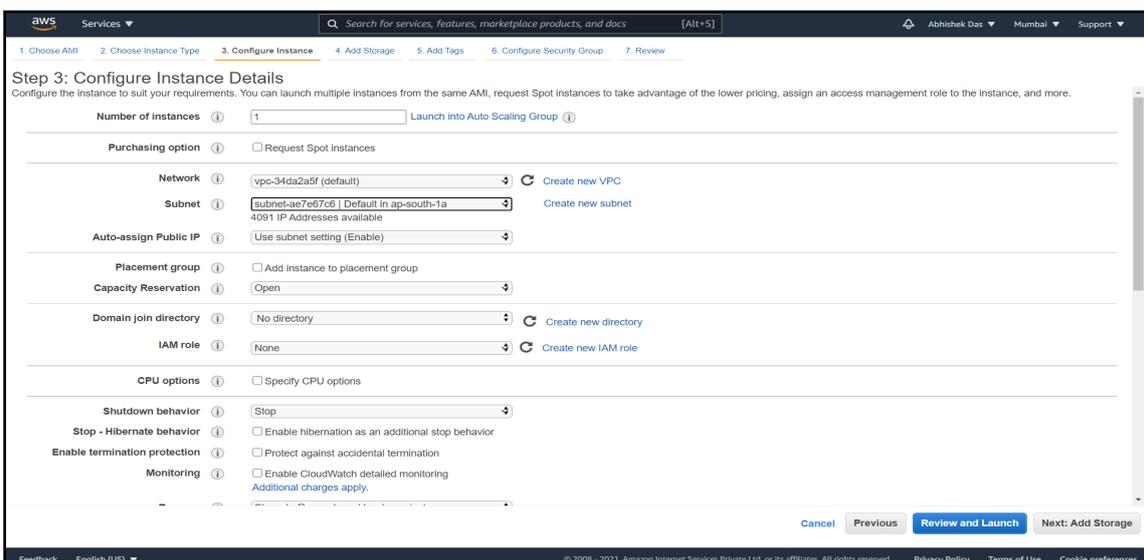
- After volume creation, create a EC2 instance.
- Select its Machine image as a “Free tier only”.



6. Select its Instance Type.



7. Now configure its Instance Detail and give subnet on same location.



8. Now Add Storage.

The screenshot shows the 'Step 4: Add Storage' configuration page in the AWS Management Console. The page is titled 'Step 4: Add Storage' and includes a sub-header 'Your instance will be launched with the following storage device settings. You can attach additional EBS volumes and instance store volumes to your instance, or edit the settings of the root volume. You can also attach additional EBS volumes after launching an instance, but not instance store volumes. Learn more about storage options in Amazon EC2.'

The configuration table is as follows:

Volume Type	Device	Snapshot	Size (GiB)	Volume Type	IOPS	Throughput (MB/s)	Delete on Termination	Encryption
Root	/dev/xvda	snap-0b55bb79ac67ade6	8	General Purpose SSD (gp2)	100 / 3000	N/A	<input checked="" type="checkbox"/>	Not Encrypted

Below the table is an 'Add New Volume' button and a note: 'Free tier eligible customers can get up to 30 GB of EBS General Purpose (SSD) or Magnetic storage. Learn more about free usage tier eligibility and usage restrictions.'

9. Now continue without pairing key.

The screenshot shows a dialog box titled 'Select an existing key pair or create a new key pair'. The dialog contains the following text:

A key pair consists of a **public key** that AWS stores, and a **private key file** that you store. Together, they allow you to connect to your instance securely. For Windows AMIs, the private key file is required to obtain the password used to log into your instance. For Linux AMIs, the private key file allows you to securely SSH into your instance.

Note: The selected key pair will be added to the set of keys authorized for this instance. Learn more about [removing existing key pairs from a public AMI](#).

Choose an existing key pair
Select a key pair
No key pairs found

No key pairs found
You don't have any key pairs. Please create a new key pair by selecting the **Create a new key pair** option above to continue.

Buttons: Cancel, Launch Instances

10. Now again go to volume and select previously created volume and in action select "Attach volume".

The screenshot shows the AWS Management Console 'Volumes' page. The 'Actions' menu is open, and 'Attach Volume' is selected. The volume details for 'vol-0d0479e9f9045d5aaf' are displayed below.

Name	Volume Type	IOPS	Throughput	Snapshot	Created	Availability Zone	State	Alarm Status
gp2	gp2	100	-	snap-0b55bb7...	April 3, 2021 at 7:42...	ap-south-1a	in-use	None
gp2	gp2	100	-	-	April 3, 2021 at 7:40...	ap-south-1a	available	None

Volume details for 'vol-0d0479e9f9045d5aaf':

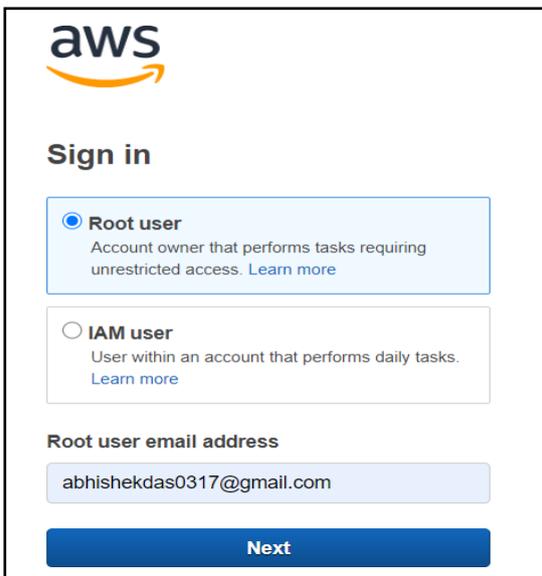
Description	Status Checks	Monitoring	Tags
Volume ID: vol-0d0479e9f9045d5aaf	Alarm status: None	Outposts ARN: -	
Snapshot: -	Availability Zone: ap-south-1a	Size: 1 GiB	
Encryption: Not Encrypted	KMS Key ID: -	Created: April 3, 2021 at 7:40:44 AM UTC+5:30	
		State: available	
		Attachment information:	
		Volume type: gp2	

05: LOAD BALANCER

About Load Balancer: Load Balancer provides basic load balancing across multiple Amazon EC2 instances and operates at both the request level and the connection level. Classic Load Balancer is intended for applications that were built within the EC2-Classic network.

Process to Configure Load Balancer:

1. Sign in to the AWS Management Console.



aws

Sign in

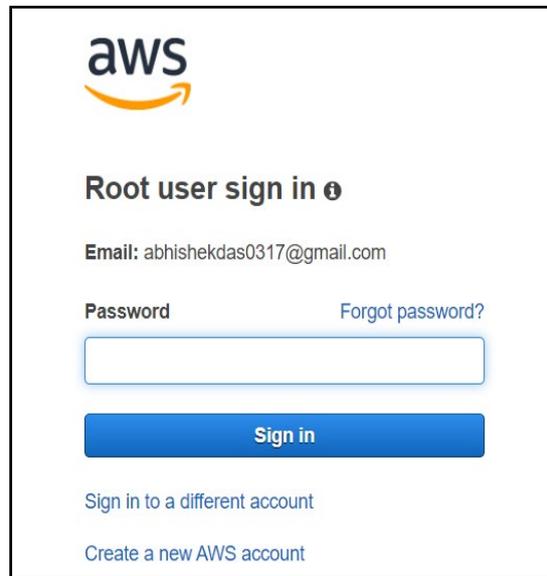
Root user
Account owner that performs tasks requiring unrestricted access. [Learn more](#)

IAM user
User within an account that performs daily tasks. [Learn more](#)

Root user email address

abhishekdas0317@gmail.com

Next



aws

Root user sign in

Email: abhishekdas0317@gmail.com

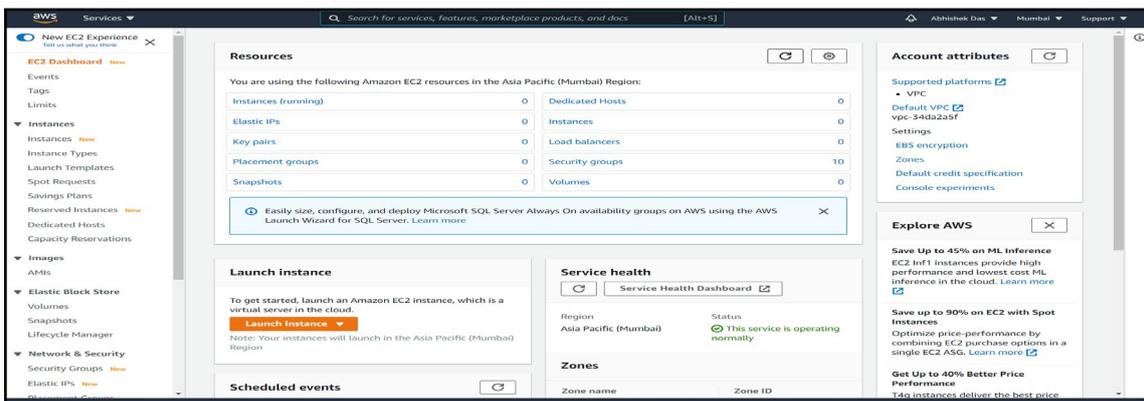
Password [Forgot password?](#)

Sign in

[Sign in to a different account](#)

[Create a new AWS account](#)

2. Go to EC2 instance creation from service and create instance using free tier.



aws

Search for services, features, marketplace products, and docs. [Alt+S]

Abhishek Das Mumbai Support

Resources

You are using the following Amazon EC2 resources in the Asia Pacific (Mumbai) Region:

Instances (running)	0	Dedicated Hosts	0
Elastic IPs	0	Instances	0
Key pairs	0	Load balancers	0
Placement groups	0	Security groups	10
Snapshots	0	Volumes	0

Launch instance

To get started, launch an Amazon EC2 instance, which is a virtual server in the cloud.

Launch instance

Note: Your instances will launch in the Asia Pacific (Mumbai) Region.

Service health

Region: Asia Pacific (Mumbai) Status: This service is operating normally

Account attributes

Supported platforms

- VPC

Default VPC vpc-34d2a25f

Settings

EBS encryption

Zones

Default credit specification

Console experiments

Explore AWS

Save up to 45% on ML inference

EC2 In1 instances provide high performance and lowest cost ML inference in the cloud. [Learn more](#)

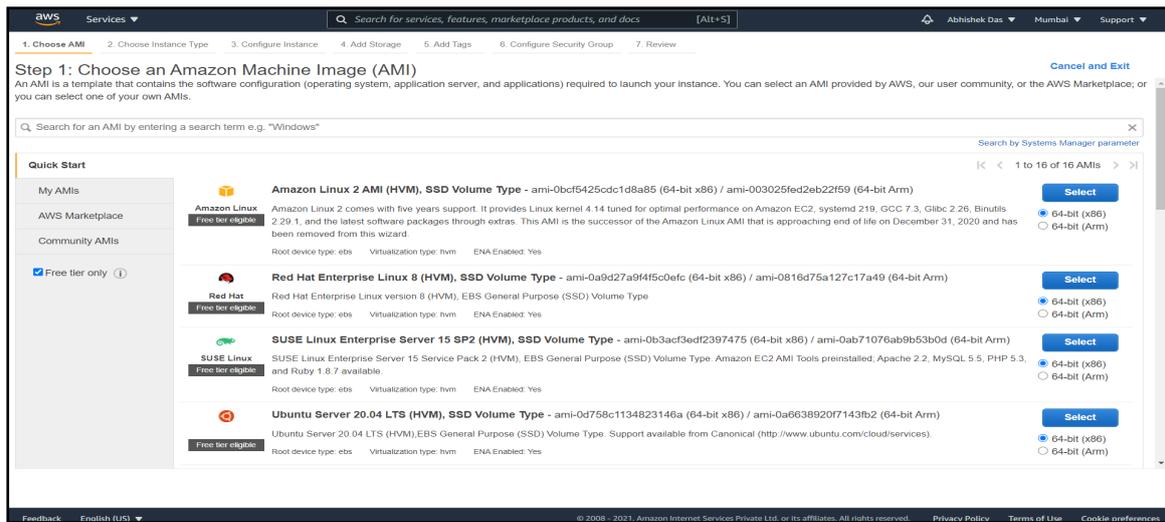
Save up to 90% on EC2 with Spot Instances

Optimize price-performance by combining EC2 purchase options in a single EC2 ASG. [Learn more](#)

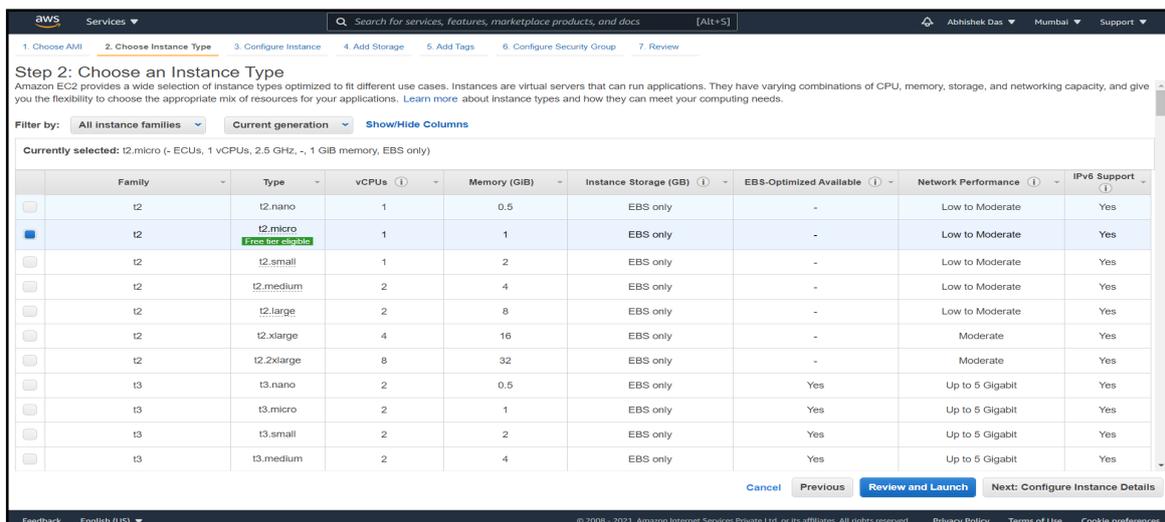
Get Up to 40% Better Price Performance

T4g instances deliver the best price

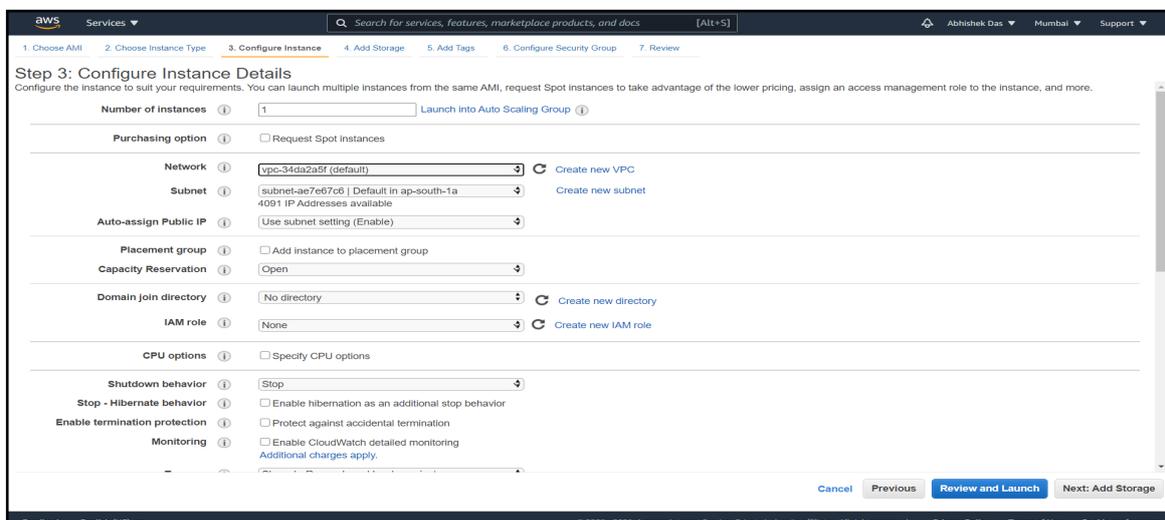
3. Select Machine Image to Free tier only.



4. Then Select Instance Type.



5. In Instance detail select Subnet of one zone.



6. Now Configure security group by providing type (http, https).

Step 6: Configure Security Group

A security group is a set of firewall rules that control the traffic for your instance. On this page, you can add rules to allow specific traffic to reach your instance. For example, if you want to set up a web server and allow Internet traffic to reach your instance, add rules that allow unrestricted access to the HTTP and HTTPS ports. You can create a new security group or select from an existing one below. [Learn more about Amazon EC2 security groups.](#)

Assign a security group: Create a new security group
 Select an existing security group

Security group name:
Description:

Type	Protocol	Port Range	Source	Description
SSH	TCP	22	Custom 0.0.0.0/0	e.g. SSH for Admin Desktop
HTTP	TCP	80	Custom 0.0.0.0/0, ::/0	e.g. SSH for Admin Desktop
HTTPS	TCP	443	Custom 0.0.0.0/0, ::/0	e.g. SSH for Admin Desktop

Warning
Rules with source of 0.0.0.0/0 allow all IP addresses to access your instance. We recommend setting security group rules to allow access from known IP addresses only.

[Cancel](#) [Previous](#) [Review and Launch](#)

7. Then continue without security pair key.

Step 7: Review Instance Launch

Please review your instance launch details. You can go back to edit changes for each section. Click **Launch** to assign a key pair to your instance and complete the launch process.

Warning Improve your instances' security. Your security group, launch-wizard-8, is open to the world. Your instances may be accessible from any IP address. We recommend that you update your security group rules to allow access from known IP addresses only. You can also open additional ports in your security group.

Select an existing key pair or create a new key pair

A key pair consists of a **public key** that AWS stores, and a **private key file** that you store. Together, they allow you to connect to your instance securely. For Windows AMIs, the private key file is required to obtain the password used to log into your instance. For Linux AMIs, the private key file allows you to securely SSH into your instance.

Note: The selected key pair will be added to the set of keys authorized for this instance. Learn more about removing existing key pairs from a public AMI.

I acknowledge that I will not be able to connect to this instance unless I already know the password built into this AMI.

[Cancel](#) [Launch Instances](#)

8. Similarly create another instance but choose different Subnet during configuration instance detail.

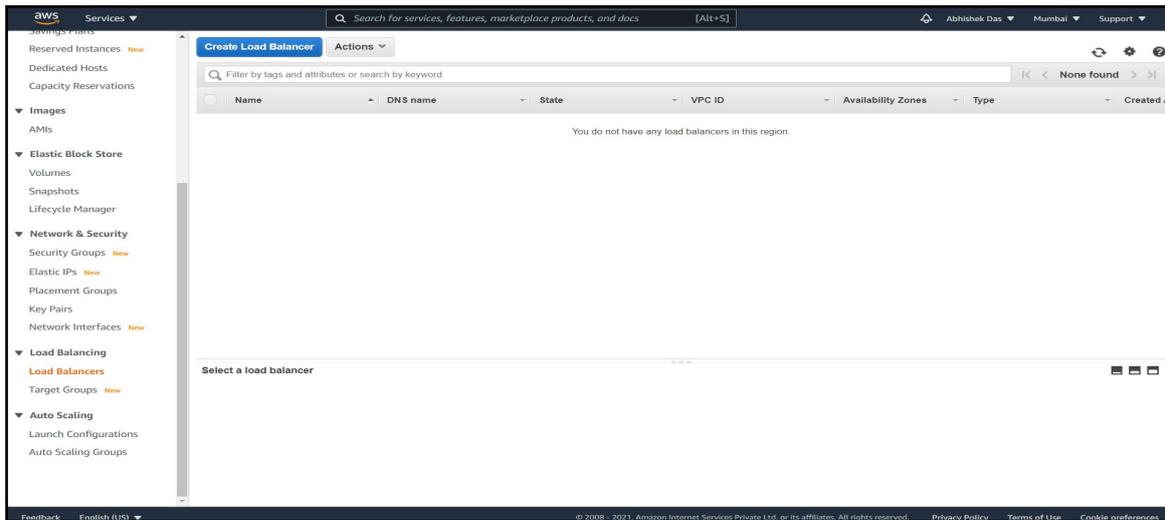
Instances (2) Info

Filter instances

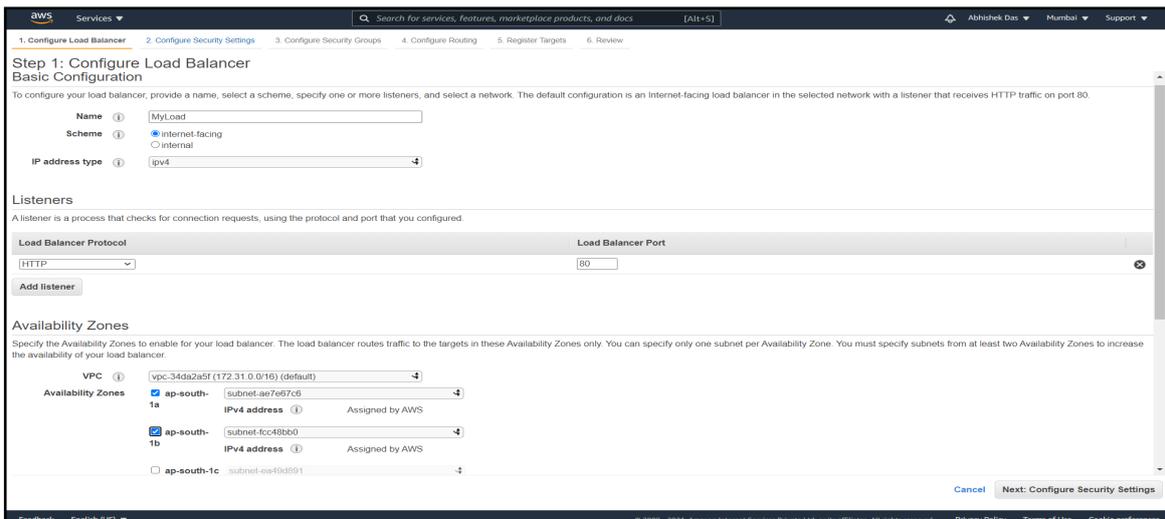
Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone	Public IPv4 DNS
-	i-06f06aaef9b7ab68	Running	t2.micro	Initializing	No alarms	ap-south-1a	ec2-35-154-4-53.a
-	i-0ed130c9581133020	Running	t2.micro	Initializing	No alarms	ap-south-1b	ec2-13-232-232-8

[Connect](#) [Instance state](#) [Actions](#) [Launch Instances](#)

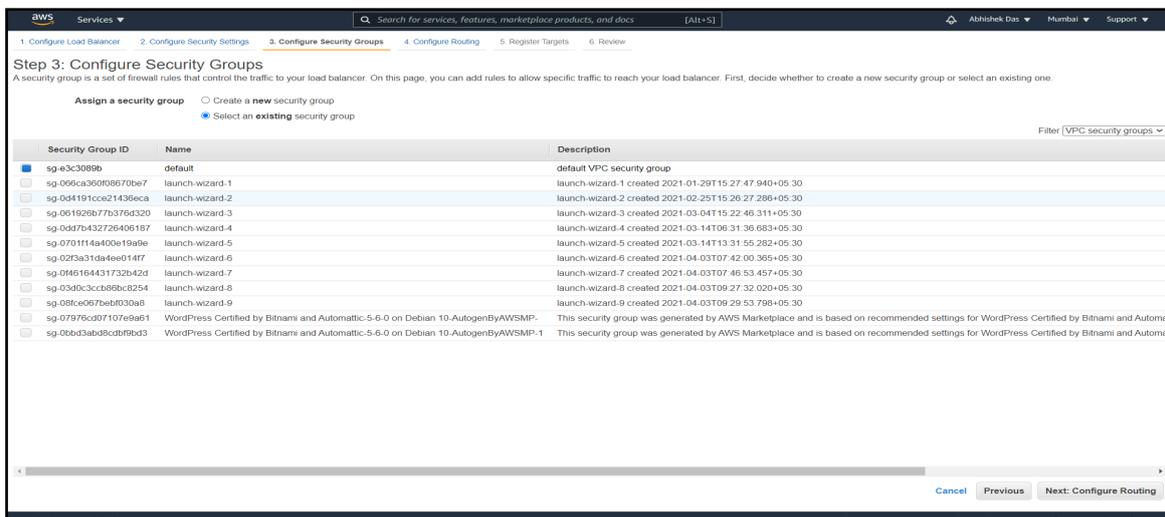
9. Now click on Load Balancer.



10. Then click on Application Load Balancer and provide its name, VPC, availability zone (choose two).



11. Choose default security group.



12. Now configure Routing by providing its target name. Then click on next select one instance and register it.

Step 4: Configure Routing
Your load balancer routes requests to the targets in this target group using the protocol and port that you specify, and performs health checks on the targets using these health check settings. The target group you specify in this step will apply to all of the listeners configured on this load balancer; you can edit the listeners and add listeners after the load balancer is created.

Target group

Target group:

Name:

Target type:
 Instance
 IP
 Lambda function

Protocol:

Port:

Protocol version:
 HTTP1
Send requests to targets using HTTP/1.1. Supported when the request protocol is HTTP/1.1 or HTTP/2.
 HTTP2
Send requests to targets using HTTP/2. Supported when the request protocol is HTTP/2 or gRPC, but gRPC-specific features are not available.
 gRPC
Send requests to targets using gRPC. Supported when the request protocol is gRPC.

Health checks

Protocol:

Path:

Advanced health check settings

[Cancel](#) [Previous](#) [Next: Register Targets](#)

Step 5: Register Targets
Register targets with your target group. If you register a target in an enabled Availability Zone, the load balancer starts routing requests to the targets as soon as the registration process completes and the target passes the initial health checks.

Registered targets
To deregister instances, select one or more registered instances and then click Remove.

Instance	Name	Port	State	Security groups	Zone
No instances available.					

Instances
To register additional instances, select one or more running instances, specify a port, and then click Add. The default port is the port specified for the target group. If the instance is already registered on the specified port, you must specify a different port.

on port

Search Instances

Instance	Name	State	Security groups	Zone	Subnet ID	Subnet CIDR
<input type="checkbox"/>	i-09f63aaaf9b7ab698	running	launch-wizard-8	ap-south-1a	subnet-ae7e6766	172.31.32.0/20
<input type="checkbox"/>	i-0ed130c9581133020	running	launch-wizard-9	ap-south-1b	subnet-4c482bb0	172.31.0.0/20

[Cancel](#) [Previous](#) [Next: Review](#)

Step 5: Register Targets
Register targets with your target group. If you register a target in an enabled Availability Zone, the load balancer starts routing requests to the targets as soon as the registration process completes and the target passes the initial health checks.

Registered targets
To deregister instances, select one or more registered instances and then click Remove.

Instance	Name	Port	State	Security groups	Zone
<input checked="" type="checkbox"/>	i-09f63aaaf9b7ab698	80	running	launch-wizard-8	ap-south-1a

Instances
To register additional instances, select one or more running instances, specify a port, and then click Add. The default port is the port specified for the target group. If the instance is already registered on the specified port, you must specify a different port.

on port

Search Instances

Instance	Name	State	Security groups	Zone	Subnet ID	Subnet CIDR
<input checked="" type="checkbox"/>	i-09f63aaaf9b7ab698	running	launch-wizard-8	ap-south-1a	subnet-ae7e6766	172.31.32.0/20
<input type="checkbox"/>	i-0ed130c9581133020	running	launch-wizard-9	ap-south-1b	subnet-4c482bb0	172.31.0.0/20

[Cancel](#) [Previous](#) [Next: Review](#)

Step 6: Review

Please review the load balancer details before continuing.

- Load balancer**
 - Name: MyLoad
 - Scheme: internet-facing
 - Listeners: Port 80 - Protocol HTTP
 - IP address type: ipv4
 - VPC: vpc-34da2a5f
 - Subnets: subnet-ae7e67c6, subnet-fcc48bb0
 - Tags
- Security groups**
 - Security groups: sg-e3c3089b
- Routing**
 - Target group: New target group
 - Target group name: Target01
 - Port: 80
 - Target type: instance
 - Protocol: HTTP
 - Protocol version: HTTP1
 - Health check protocol: HTTP
 - Path: /
 - Health check port: traffic port
 - Healthy threshold: 5
 - Unhealthy threshold: 2
 - Timeout: 5
 - Interval: 30
 - Success codes: 200
- Targets**
 - Instances: i-06f06aaaf5b7ab69.80

Buttons: Cancel, Previous, Create

Load Balancer Creation Status

Successfully created load balancer

Load balancer MyLoad was successfully created.

Note: It might take a few minutes for your load balancer to be fully set up and ready to route traffic, and for the targets to complete the registration process and pass the initial health checks.

Suggested next steps

- Discover other services that you can integrate with your load balancer. Visit the **Integrated services** tab within MyLoad.
- Consider using AWS Global Accelerator to further improve the availability and performance of your applications. [AWS Global Accelerator console](#)

Close

Create Load Balancer

Name	DNS name	State	VPC ID	Availability Zones	Type	Created At
MyLoad	MyLoad-1583204894 ap-sou...	provisioning	vpc-34da2a5f	ap-south-1a, ap-south-1b	application	April 3, 2021 at 9:35:48 AM ...

Load balancer: MyLoad

Description | Listeners | Monitoring | Integrated services | Tags

Basic Configuration

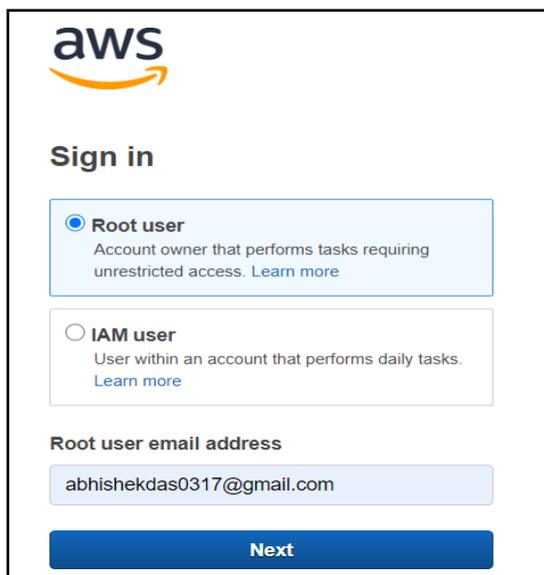
- Name: MyLoad
- ARN: arn:aws:elasticloadbalancing:ap-south-1:782522942915:loadbalancer/app/MyLoad:c053791c515c877e
- DNS name: MyLoad-1583204894 ap-south-1.elb.amazonaws.com (A Record)
- State: provisioning
- Type: application
- Scheme: internet-facing
- IP address type: ipv4
- VPC: vpc-34da2a5f
- Availability Zones: subnet-ae7e67c6 - ap-south-1a, subnet-fcc48bb0 - ap-south-1b
- Hosted zone: ZP97RFLXTNZK

06: AWS LAMBDA

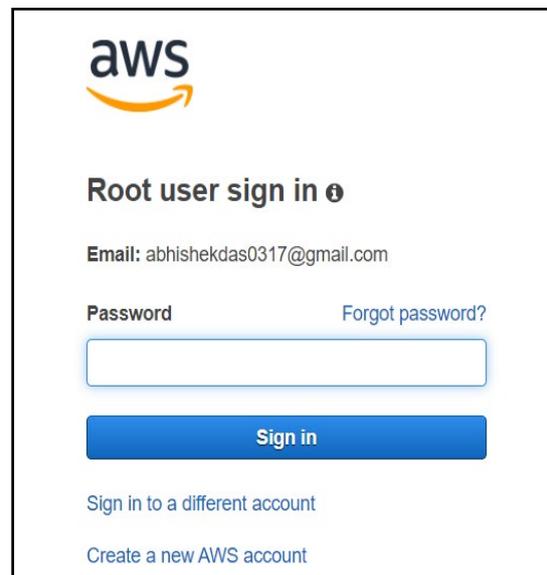
About AWS Lambda: AWS Lambda is a serverless compute service that lets you run code without provisioning or managing servers, creating workload-aware cluster scaling logic, maintaining event integrations, or managing runtimes.

Process to Configure AWS Lambda:

1. Sign in to the AWS Management Console.

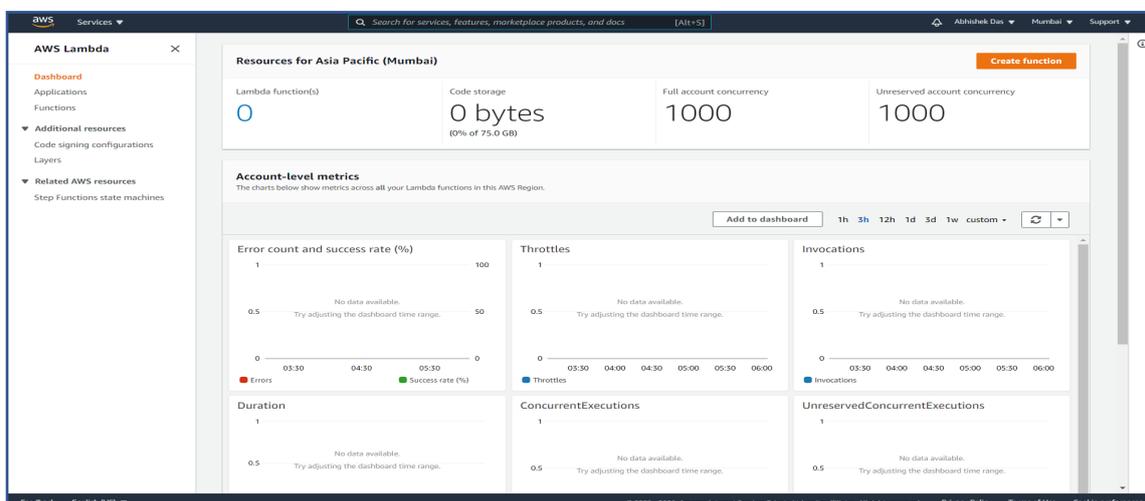


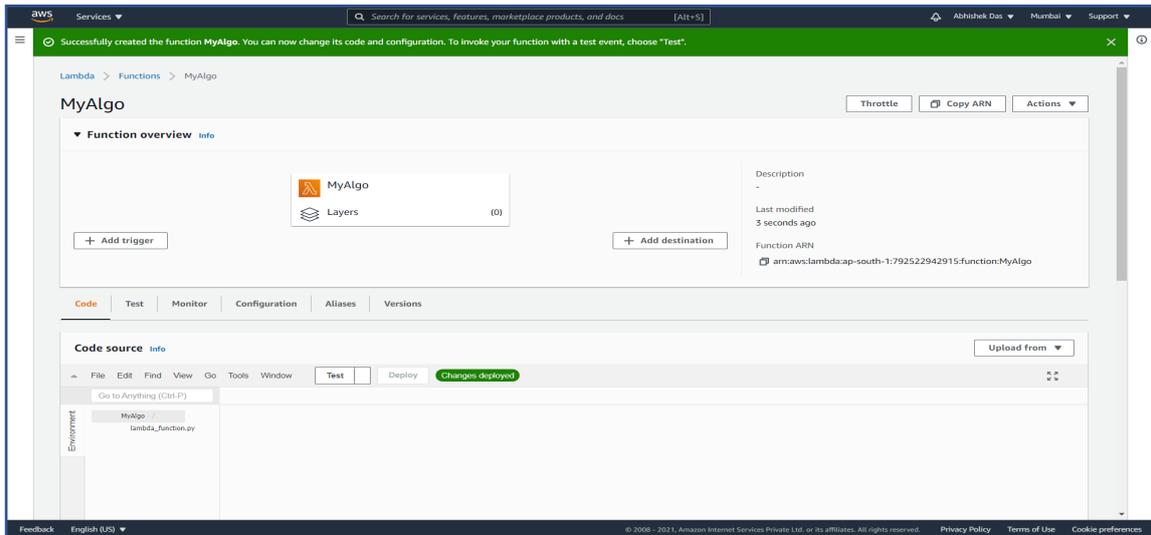
The screenshot shows the AWS Sign in page. At the top is the AWS logo. Below it is the heading "Sign in". There are two radio button options: "Root user" (selected) and "IAM user". The "Root user" option includes the text "Account owner that performs tasks requiring unrestricted access. [Learn more](#)". The "IAM user" option includes "User within an account that performs daily tasks. [Learn more](#)". Below these options is a text input field for "Root user email address" containing "abhishekdas0317@gmail.com". At the bottom is a blue "Next" button.



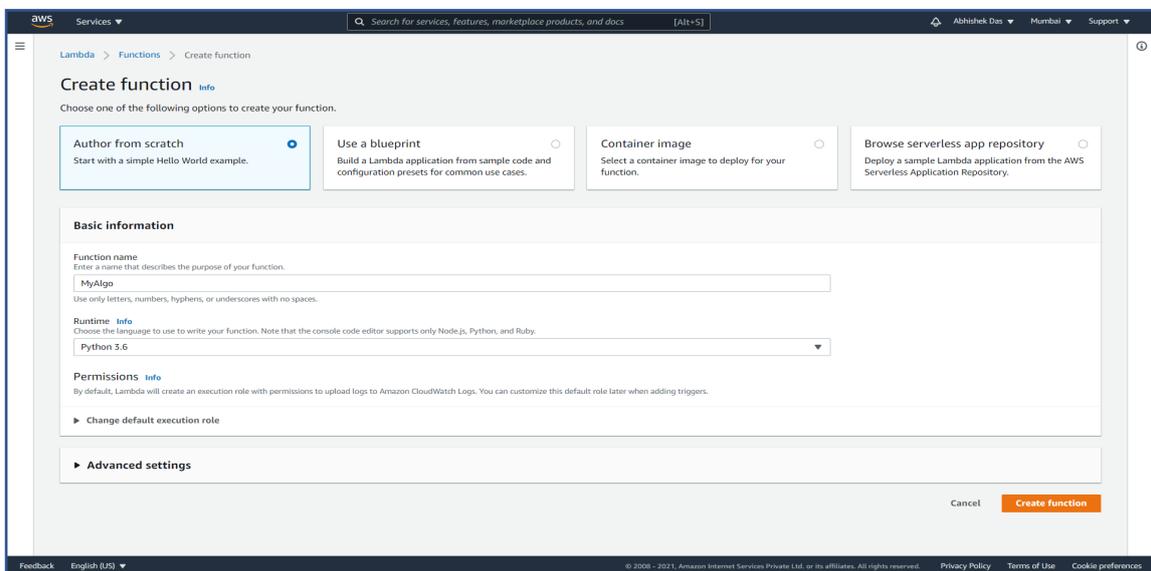
The screenshot shows the AWS Root user sign in page. At the top is the AWS logo. Below it is the heading "Root user sign in". There is an "Email" field containing "abhishekdas0317@gmail.com" and a "Password" field. A "Forgot password?" link is next to the password field. Below the password field is a blue "Sign in" button. At the bottom are two links: "Sign in to a different account" and "Create a new AWS account".

2. Open Lambda from service.

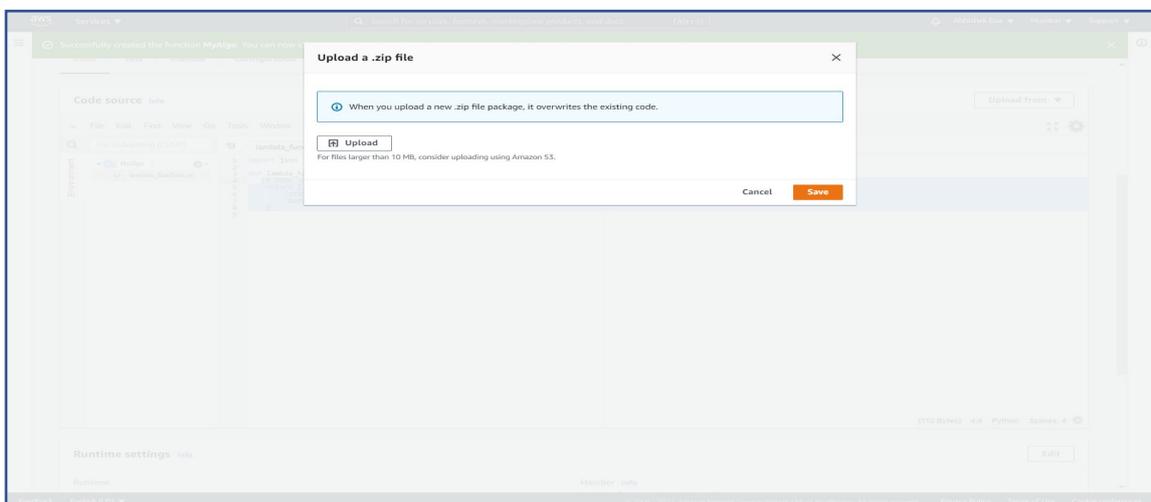




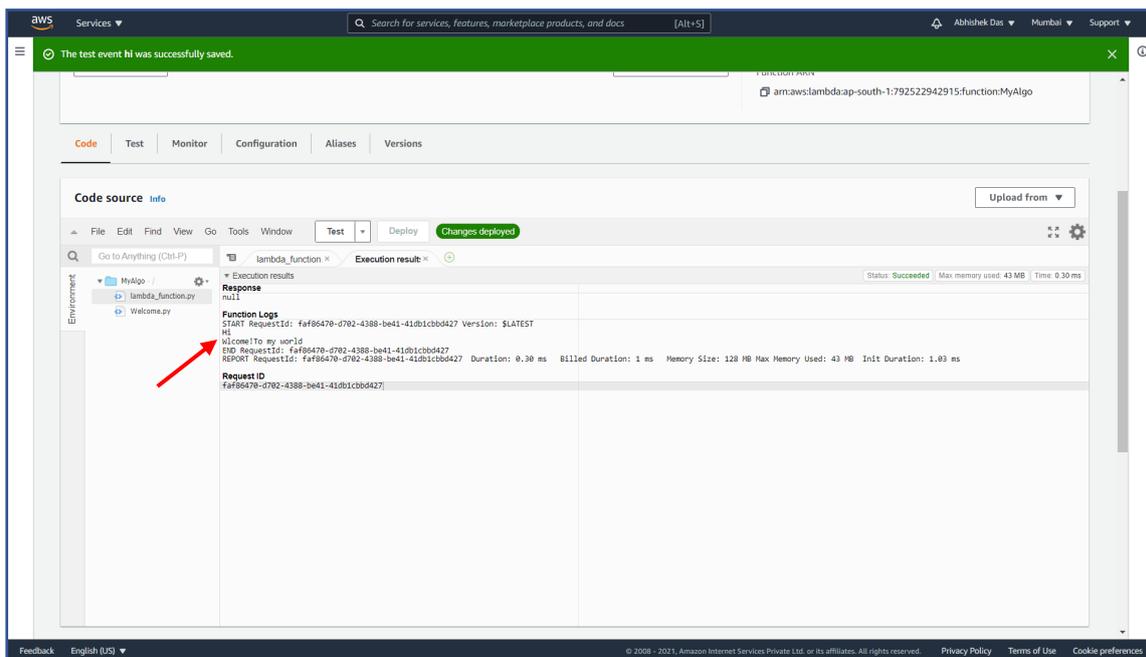
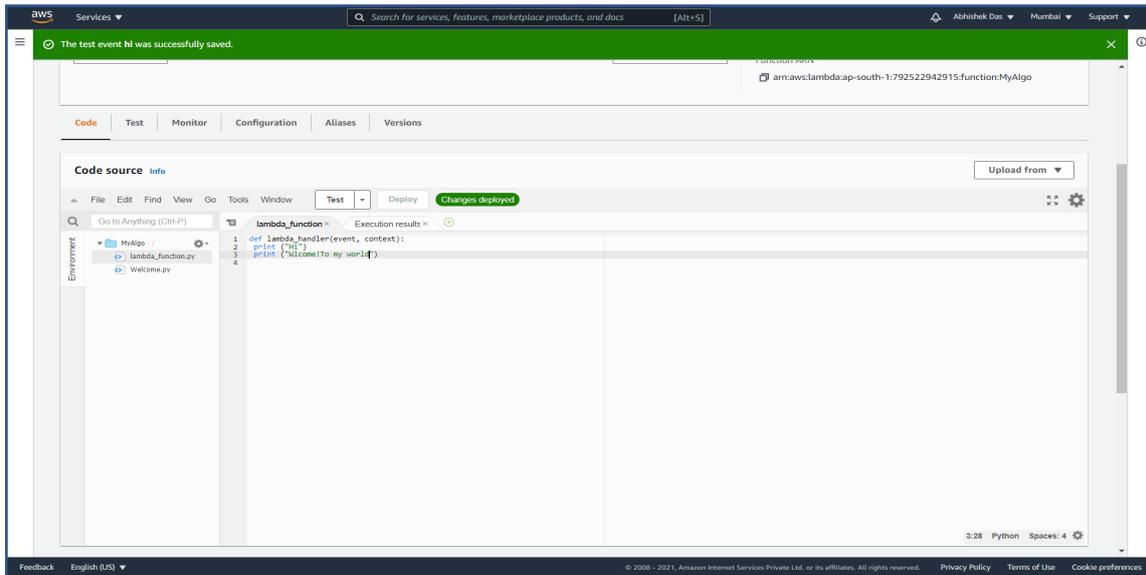
3. Click on Create function and provide function name, runtime.



4. Now we execute our code and even upload our code file from S3 bucket also.



5. Now go to text editor type your code and test it.

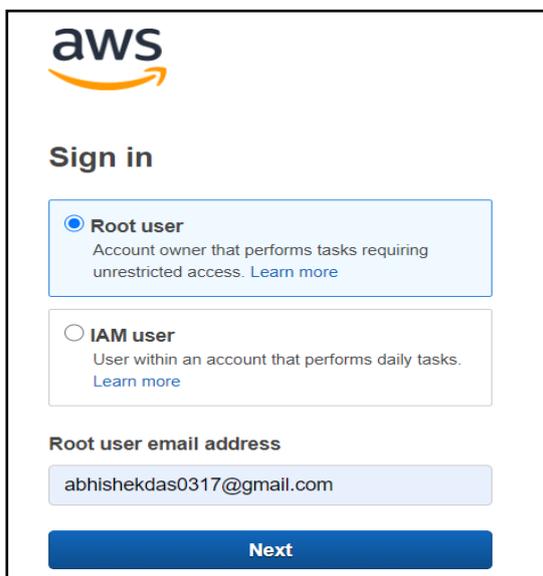


07: Auto Scaling

About Auto Scaling: AWS Auto Scaling monitors your applications and automatically adjusts capacity to maintain steady, predictable performance at the lowest possible cost. Using AWS Auto Scaling, it's easy to setup application scaling for multiple resources across multiple services in minutes.

Process to Configure Auto Scaling:

1. Sign in to the AWS Management Console.



aws

Sign in

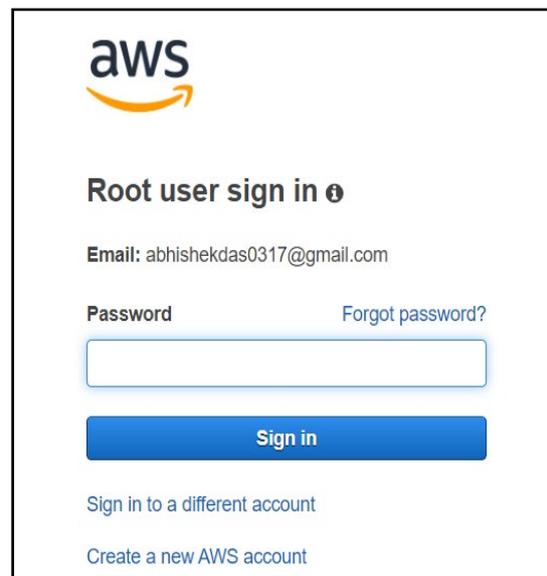
Root user
Account owner that performs tasks requiring unrestricted access. [Learn more](#)

IAM user
User within an account that performs daily tasks. [Learn more](#)

Root user email address

abhishekdas0317@gmail.com

Next



aws

Root user sign in

Email: abhishekdas0317@gmail.com

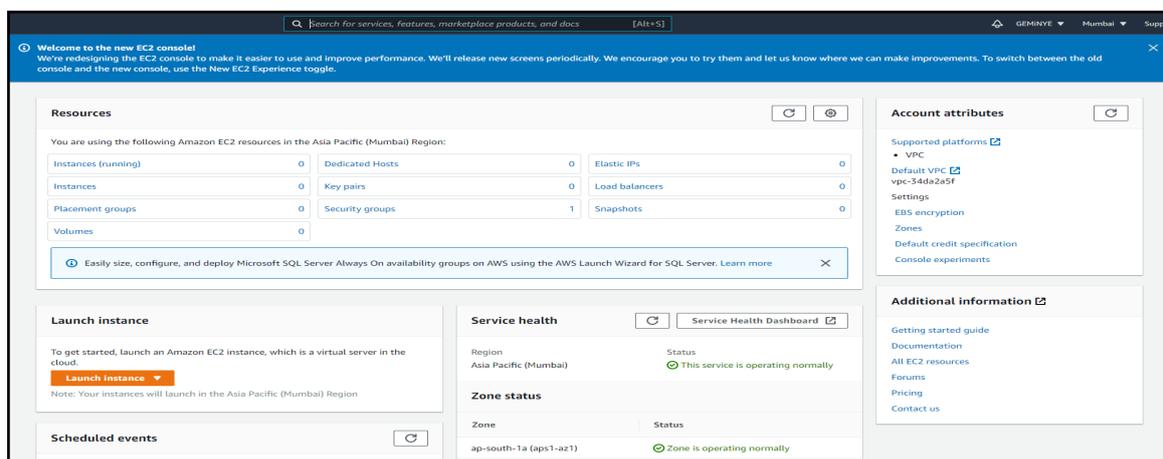
Password [Forgot password?](#)

Sign in

[Sign in to a different account](#)

[Create a new AWS account](#)

2. Choose EC2 from compute services and click on launch instance.



Welcome to the new EC2 console! We're redesigning the EC2 console to make it easier to use and improve performance. We'll release new screens periodically. We encourage you to try them and let us know where we can make improvements. To switch between the old console and the new console, use the new EC2 Experience toggle.

Resources

You are using the following Amazon EC2 resources in the Asia Pacific (Mumbai) Region:

Instances (running)	0	Dedicated Hosts	0	Elastic IPs	0
Instances	0	Key pairs	0	Load balancers	0
Placement groups	0	Security groups	1	Snapshots	0
Volumes	0				

[Easily size, configure, and deploy Microsoft SQL Server Always On availability groups on AWS using the AWS Launch Wizard for SQL Server. \[Learn more\]\(#\)](#)

Launch instance

To get started, launch an Amazon EC2 Instance, which is a virtual server in the cloud.

Launch instance

Note: Your instances will launch in the Asia Pacific (Mumbai) Region.

Scheduled events

Service health

Region: Asia Pacific (Mumbai) Status: ✔ This service is operating normally

Zone status

Zone	Status
ap-south-1a (aps1-a21)	✔ Zone is operating normally

Account attributes

Supported platforms: [VPC](#), [Default VPC](#), [vpc-3461a2a5f](#)

Settings: [EBS encryption](#), [Zones](#), [Default credit specification](#), [Console experiments](#)

Additional information

[Getting started guide](#), [Documentation](#), [All EC2 resources](#), [Forums](#), [Pricing](#), [Contact us](#)

3. Tick on free tier and select AMI AMZON from free tier services.

Step 1: Choose an Amazon Machine Image (AMI)

Search for an AMI by entering a search term e.g. "Windows"

Quick Start

- Amazon Linux 2 AMI (HVM), SSD Volume Type** - ami-08e0ca9924195beba (64-bit x86) / ami-0437d5dbef8c3d52 (64-bit Arm) **Select**
- Red Hat Enterprise Linux 8 (HVM), SSD Volume Type** - ami-0a9d27a9f45c0efc (64-bit x86) / ami-0816d75a127c17a49 (64-bit Arm) **Select**
- SUSE Linux Enterprise Server 15 SP2 (HVM), SSD Volume Type** - ami-0b3ac3edf2397475 (64-bit x86) / ami-0ab71076ab9b53b0d (64-bit Arm) **Select**
- Ubuntu Server 20.04 LTS (HVM), SSD Volume Type** - ami-0a4a70bd98c6db441 (64-bit x86) / ami-00e24e2d9b2d705c (64-bit Arm) **Select**

4. Choose free tier 1cpu 1gh ram (t2 micro).

Step 2: Choose an Instance Type

Amazon EC2 provides a wide selection of instance types optimized to fit different use cases. Instances are virtual servers that can run applications. They have varying combinations of CPU, memory, storage, and networking capacity, and give you the flexibility to choose the appropriate mix of resources for your applications.

Filter by: All instance families, Current generation, Show/Hide Columns

Currently selected: 12 micro (-, ECUs, 1 vCPUs, 2.5 GHz, -, 1 GiB memory, EBS only)

Family	Type	vCPUs	Memory (GiB)	Instance Storage (GiB)	EBS-Optimized Available	Network Performance	IPv6 Support
t2	t2.nano	1	0.5	EBS only	-	Low to Moderate	Yes
t2	t2.micro Free tier eligible	1	1	EBS only	-	Low to Moderate	Yes
t2	t2.small	1	2	EBS only	-	Low to Moderate	Yes
t2	t2.medium	2	4	EBS only	-	Low to Moderate	Yes
t2	t2.large	2	8	EBS only	-	Low to Moderate	Yes

5. Configure instance detail and add storage.

Step 3: Configure Instance Details

Configure the instance to suit your requirements. You can launch multiple instances from the same AMI, request Spot instances to take advantage of the lower pricing, assign an access management role to the instance, and more.

- Number of instances: 1
- Purchasing option: Request Spot instances
- Network: vpc-34da2a5f (default)
- Subnet: No preference (default subnet in any Availability Zone)
- Auto-assign Public IP: Use subnet setting (Enable)
- Placement group: Add instance to placement group
- Capacity Reservation: Open
- Domain join directory: No directory
- IAM role: None
- CPU options: Specify CPU options
- Shutdown behavior: Stop
- Stop - Hibernate behavior: Enable hibernation as an additional stop behavior
- Enable termination protection: Protect against accidental termination
- Monitoring: Enable CloudWatch detailed monitoring
- Tenancy: Shared - Run a shared hardware instance

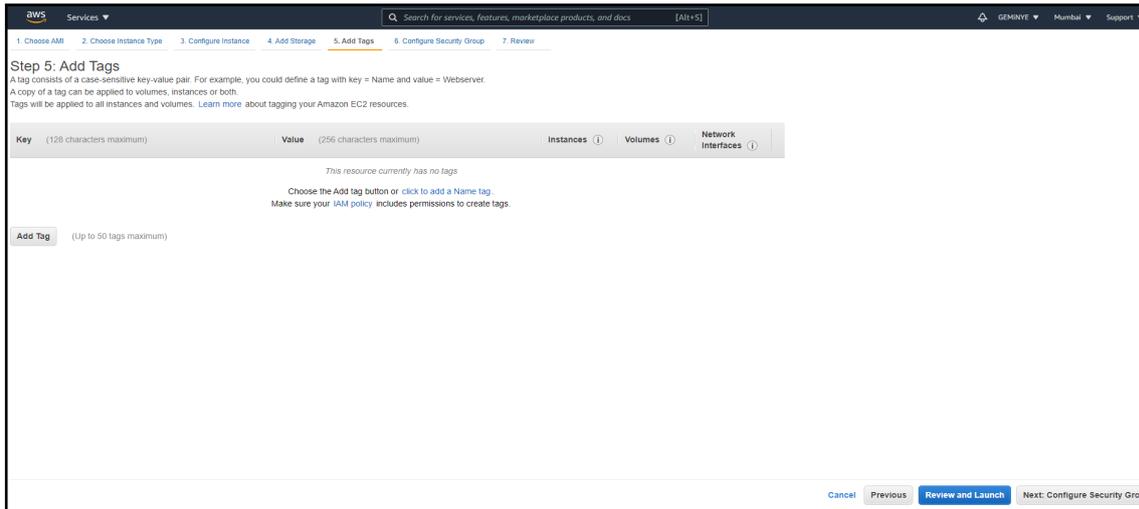
Step 4: Add Storage

Your instance will be launched with the following storage device settings. You can attach additional EBS volumes and instance store volumes to your instance, or edit the settings of the root volume. You can also attach additional EBS volumes after launching an instance, but not instance store volumes.

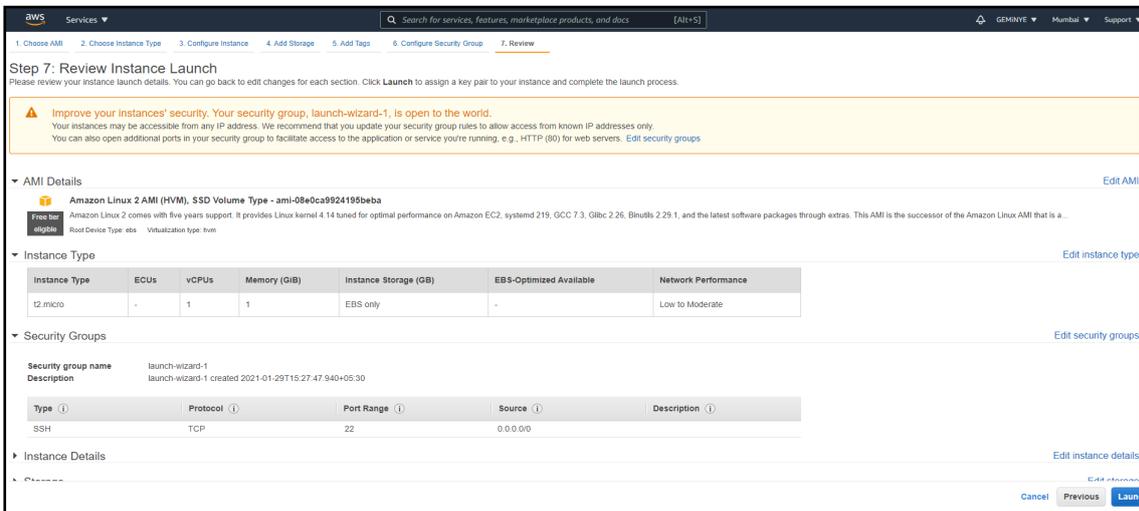
Volume Type	Device	Snapshot	Size (GiB)	Volume Type	IOPS	Throughput (MiB/s)	Delete on Termination	Encryption
Root	/dev/xvda	snap-07e0ef01c68d3978	8	General Purpose SSD (gp2)	100 / 3000	N/A	<input checked="" type="checkbox"/>	Not Encrypted

Free tier eligible customers can get up to 30 GB of EBS General Purpose (SSD) or Magnetic storage.

6. Click on review and launch.

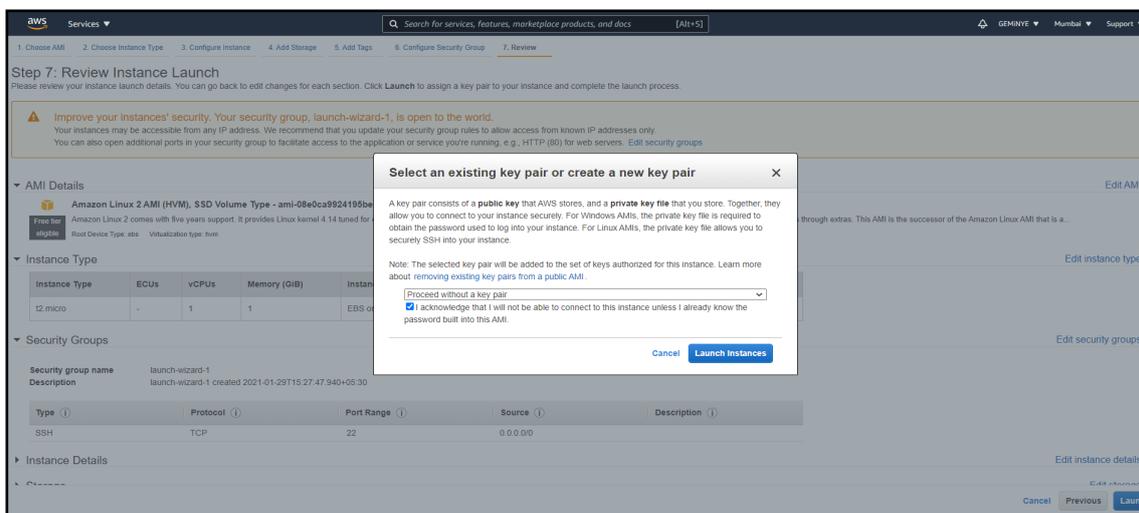


The screenshot shows the 'Step 5: Add Tags' page in the AWS console. It includes a breadcrumb trail from 'Choose AMI' to 'Add Tags'. The main content area has a table with columns for 'Key', 'Value', 'Instances', 'Volumes', and 'Network Interfaces'. Below the table, there is an 'Add Tag' button and a note: 'This resource currently has no tags. Choose the Add tag button or click to add a Name tag. Make sure your IAM policy includes permissions to create tags.' At the bottom right, there are 'Cancel', 'Previous', 'Review and Launch', and 'Next: Configure Security Group' buttons.



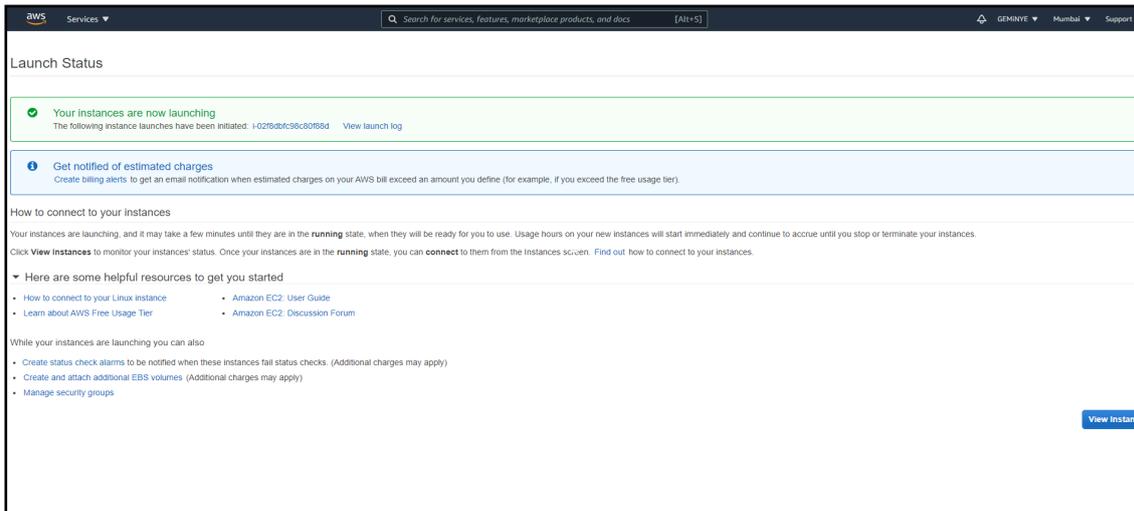
The screenshot shows the 'Step 7: Review Instance Launch' page. It features a warning banner: 'Improve your instances' security. Your security group, launch-wizard-1, is open to the world. Your instances may be accessible from any IP address. We recommend that you update your security group rules to allow access from known IP addresses only. You can also open additional ports in your security group to facilitate access to the application or service you're running, e.g., HTTP (80) for web servers. Edit security groups'. Below this, there are sections for 'AMI Details' (Amazon Linux 2 AMI), 'Instance Type' (t2.micro), and 'Security Groups' (launch-wizard-1). At the bottom right, there are 'Cancel', 'Previous', and 'Launch' buttons.

7. Continue without a key pair.

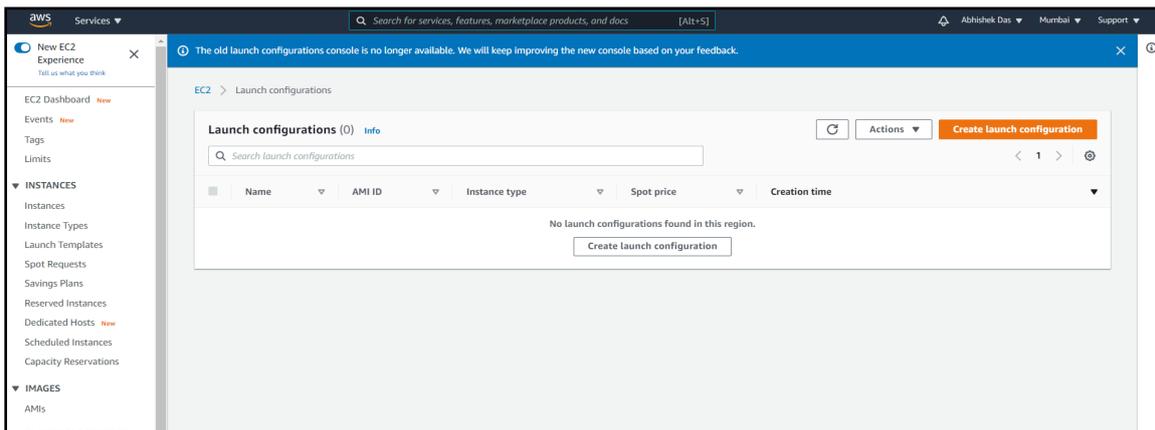


This screenshot is similar to the previous one but includes a modal dialog box titled 'Select an existing key pair or create a new key pair'. The dialog explains that a key pair consists of a public key and a private key file. It offers a dropdown menu with the option 'Proceed without a key pair' selected. Below the dropdown, there is a checked checkbox: 'I acknowledge that I will not be able to connect to this instance unless I already know the password built into this AMI.' The dialog has 'Cancel' and 'Launch Instances' buttons.

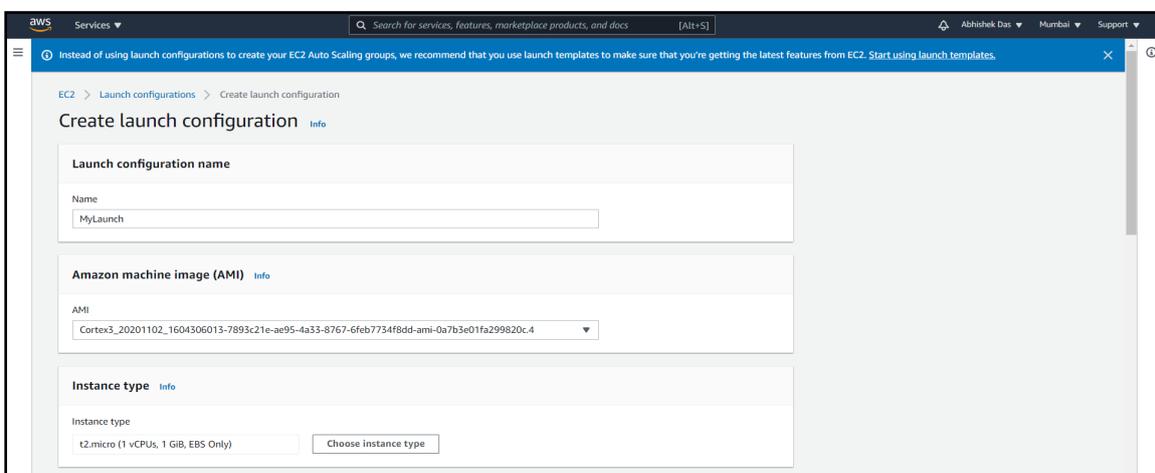
8. Click on launch Instance.



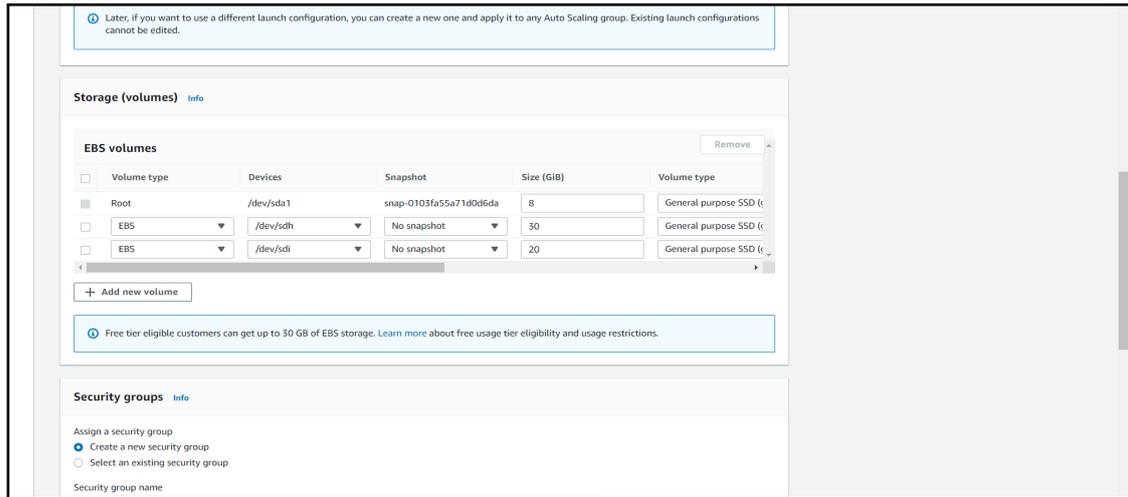
9. Now click on Launch Configuration under Auto Scaling and create Launch Configuration.



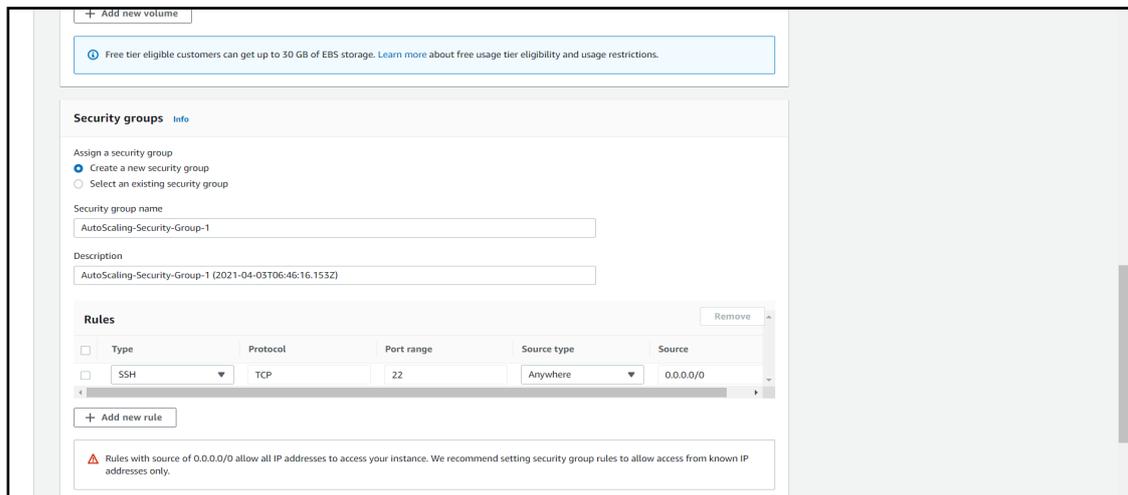
10. Then provide Name, AMI, Instance Type.



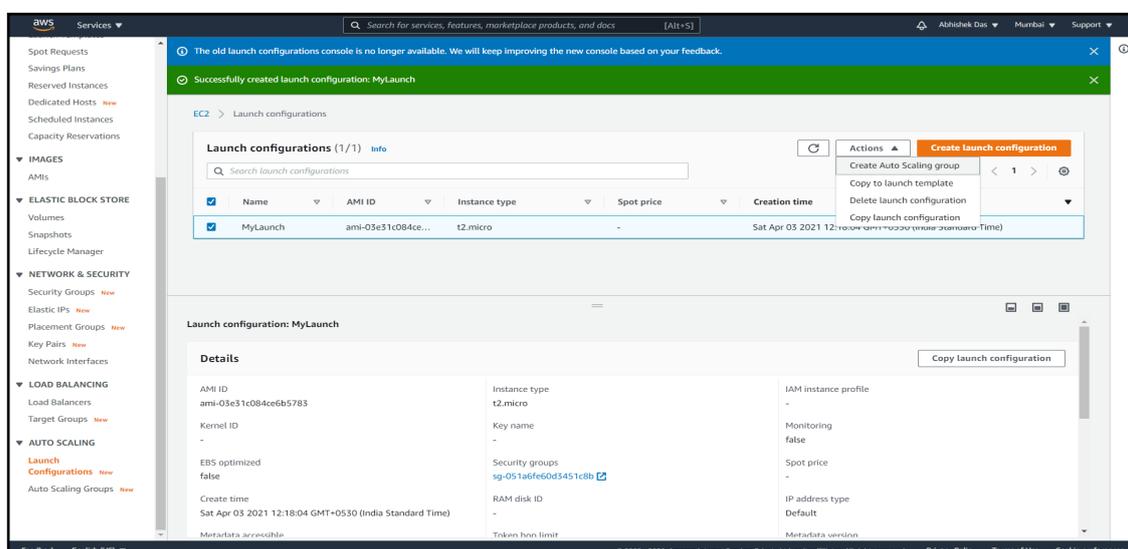
11. We can extend volumes (EBS).



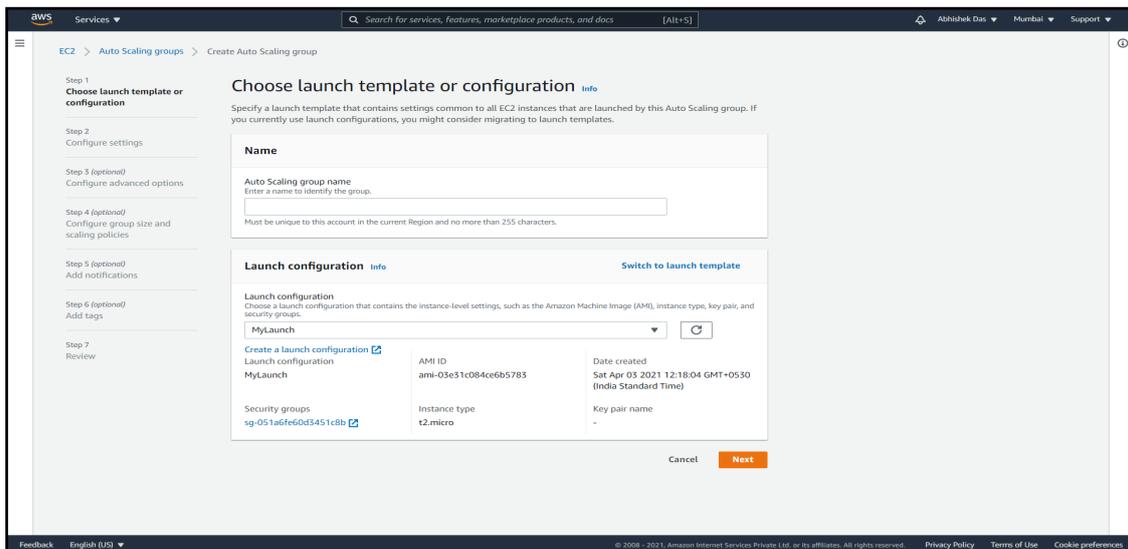
12. Now select Security Groups and click on Create Launch Configuration.



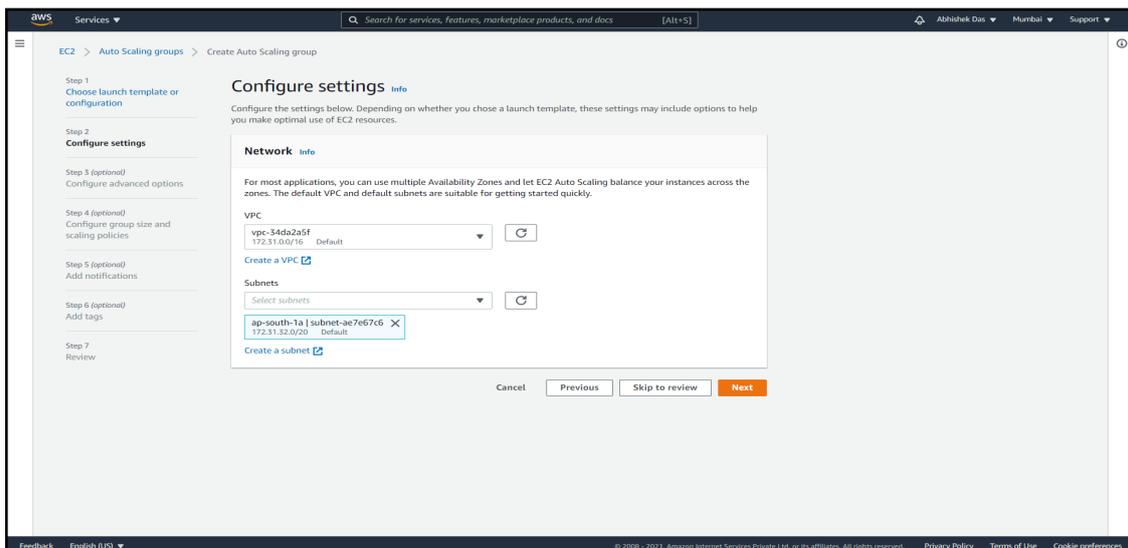
13. Then select that configuration and click on Action and select create auto scaling group.



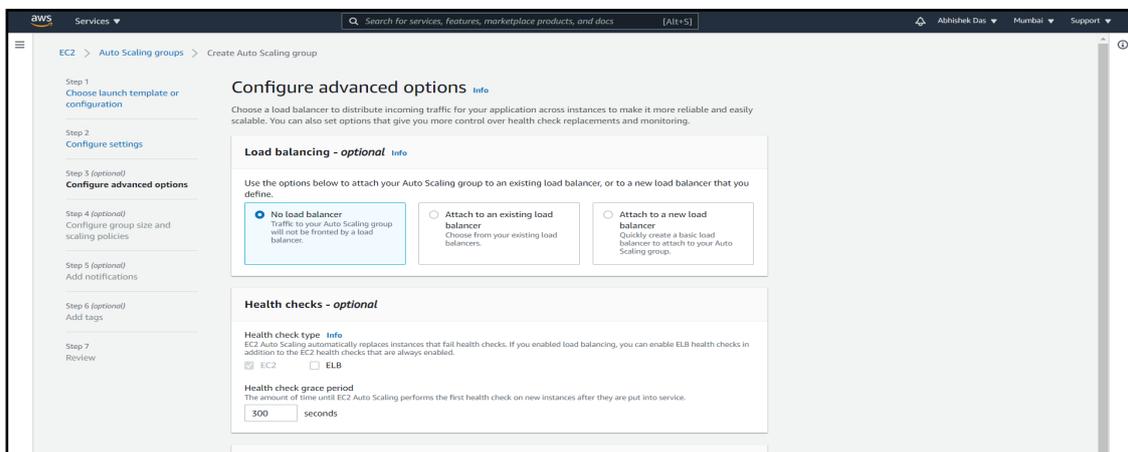
14. Provide Security group name and click next.



15. Select VPC and Subnet and click next.



16. Then select Load Balancing and click next.



17. In configure group size and autoscaling policies set Maximum capacity as 2 and click next.

The screenshot shows the AWS console interface for configuring an Auto Scaling group. The page title is "Configure group size and scaling policies". The left sidebar shows a progress bar with steps: Step 1 (Choose launch template or configuration), Step 2 (Configure settings), Step 3 (optional, Configure advanced options), Step 4 (optional, Configure group size and scaling policies - currently active), Step 5 (optional, Add notifications), Step 6 (optional, Add tags), and Step 7 (Review). The main content area includes:

- Group size - optional**: A section with a description: "Specify the size of the Auto Scaling group by changing the desired capacity. You can also specify minimum and maximum capacity limits. Your desired capacity must be within the limit range." It contains three input fields: "Desired capacity" (value: 1), "Minimum capacity" (value: 1), and "Maximum capacity" (value: 1).
- Scaling policies - optional**: A section with a description: "Choose whether to use a scaling policy to dynamically resize your Auto Scaling group to meet changes in demand." It has two radio buttons: "Target tracking scaling policy" (unselected) and "None" (selected).
- Instance scale-in protection - optional**: A section that is currently empty.

18. Now add tags and click next.

The screenshot shows the "Add tags" step in the AWS console. The left sidebar shows the progress bar with Step 4 (Configure group size and scaling policies) completed and Step 5 (Add tags) active. The main content area includes:

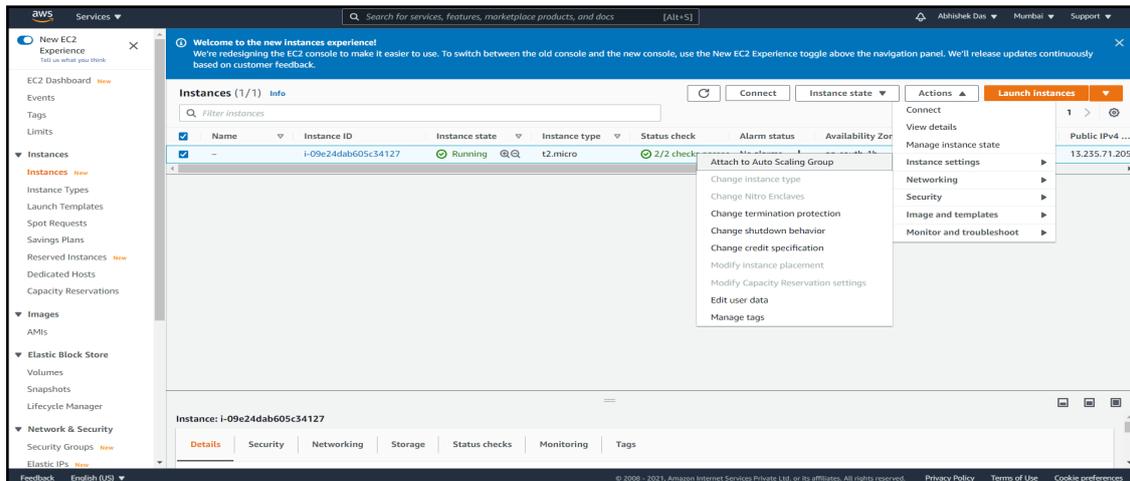
- Add tags**: A section with a description: "Add tags to help you search, filter, and track your Auto Scaling group across AWS. You can also choose to automatically add these tags to instances when they are launched." Below this is a blue informational box: "You can optionally choose to add tags to instances (and their attached EBS volumes) by specifying tags in your launch template. We recommend caution, however, because the tag values for instances from your launch template will be overridden if there are any duplicate keys specified for the Auto Scaling group." Below the box is a "Tags (0)" section with an "Add tag" button and "50 remaining" text.

19. Review your settings and click on finish.

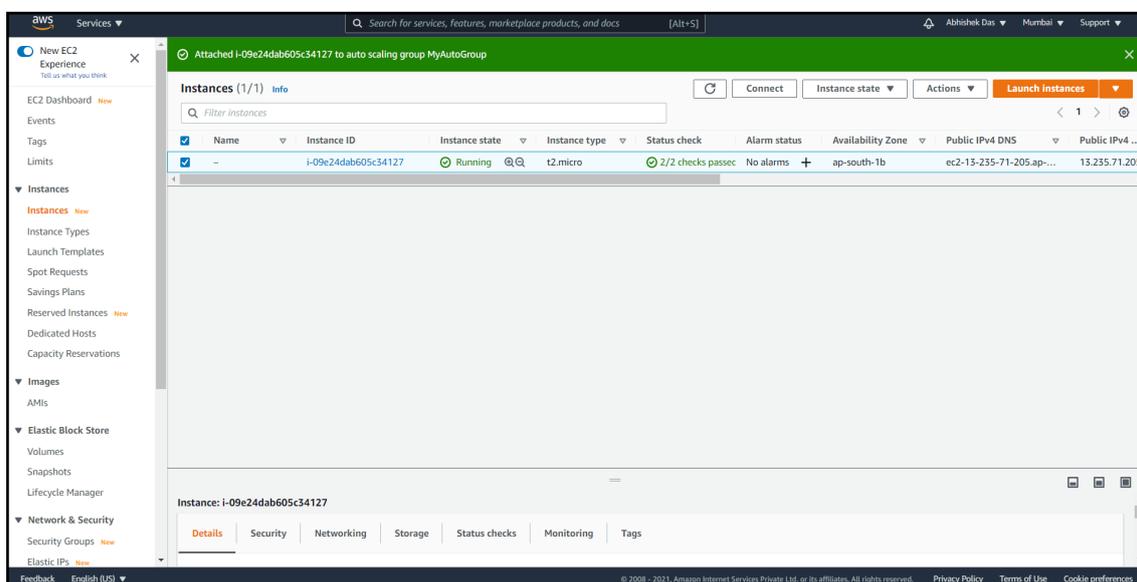
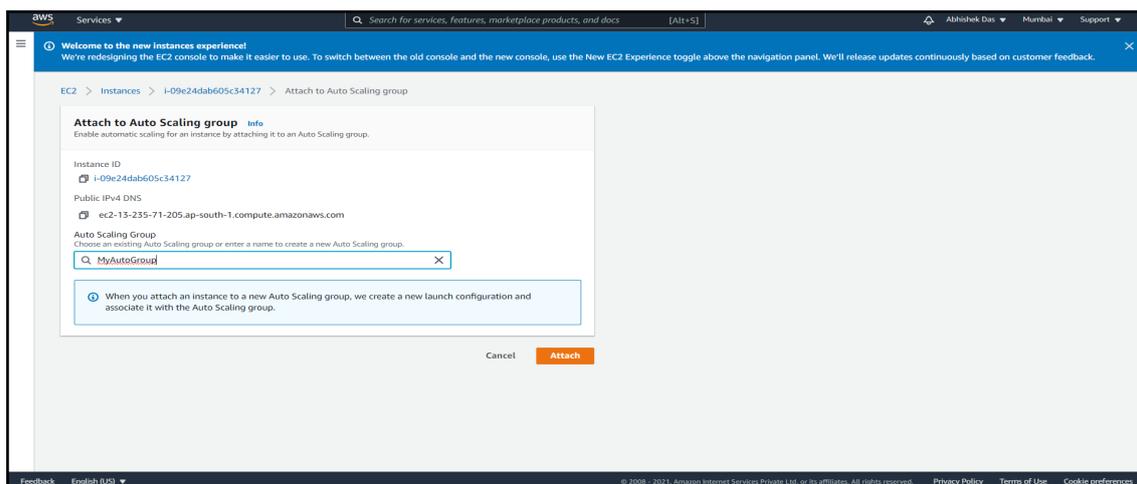
The screenshot shows the "Review" step in the AWS console. The left sidebar shows the progress bar with Step 5 (Add tags) completed and Step 7 (Review) active. The main content area includes:

- Review**: A section with a description: "Review your configuration before creating the Auto Scaling group." It contains three summary cards, each with an "Edit" button:
 - Step 1: Choose launch template or configuration**: Shows "Group details" (Auto Scaling group name: MyAutoGroup) and "Launch configuration" (MyLaunch).
 - Step 2: Configure settings**: Shows "Network" details: VPC (vpc-34da2a5f), Availability Zone (ap-south-1a), Subnet (subnet-ae7e67c6), and IP address (172.31.32.0/20).
 - Step 3: Configure advanced options**: Shows "Load balancing" details.

20. Then go to EC2 Dashboard and click on the instance and click on Action >> Instance Settings >> Attach auto scaling group.



21. Provide Security group name and click on Attach.

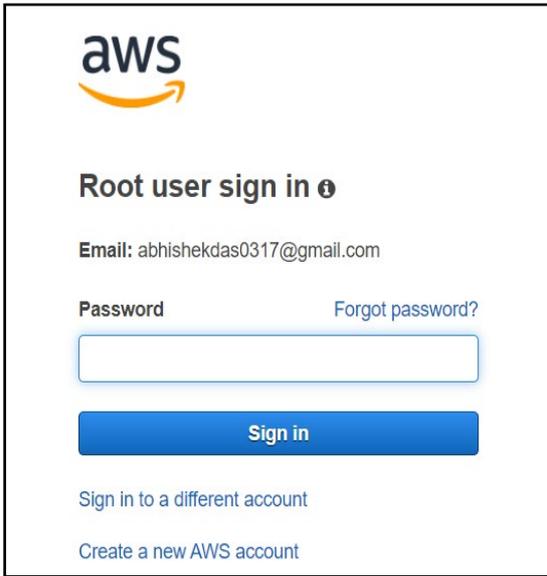
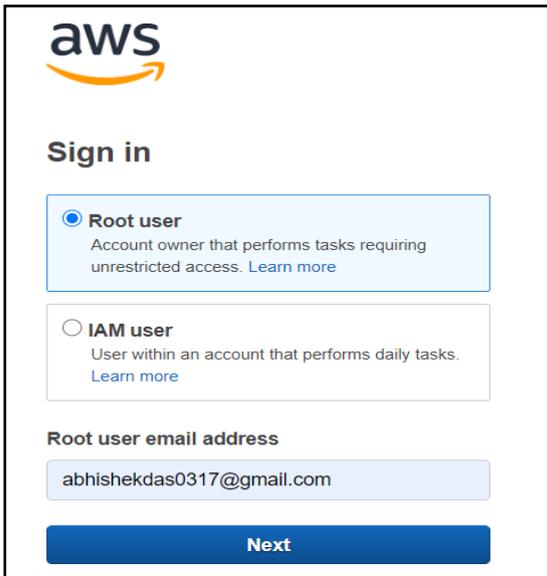


08: Cloud Watch

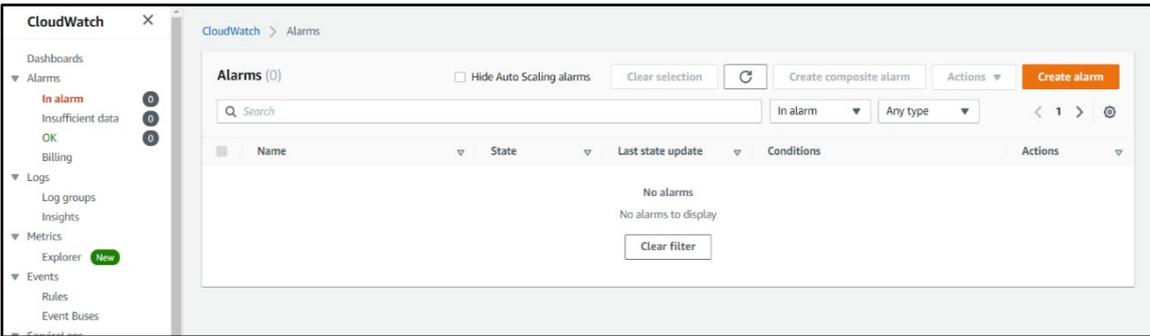
About Cloud Watch: Amazon CloudWatch is a monitoring and management service that provides data and actionable insights for AWS, hybrid, and on-premises applications and infrastructure resources. With CloudWatch, you can collect and access all your performance and operational data in form of logs and metrics from a single platform.

Process to Configure Cloud Watch:

1. Sign in to the AWS Management Console.



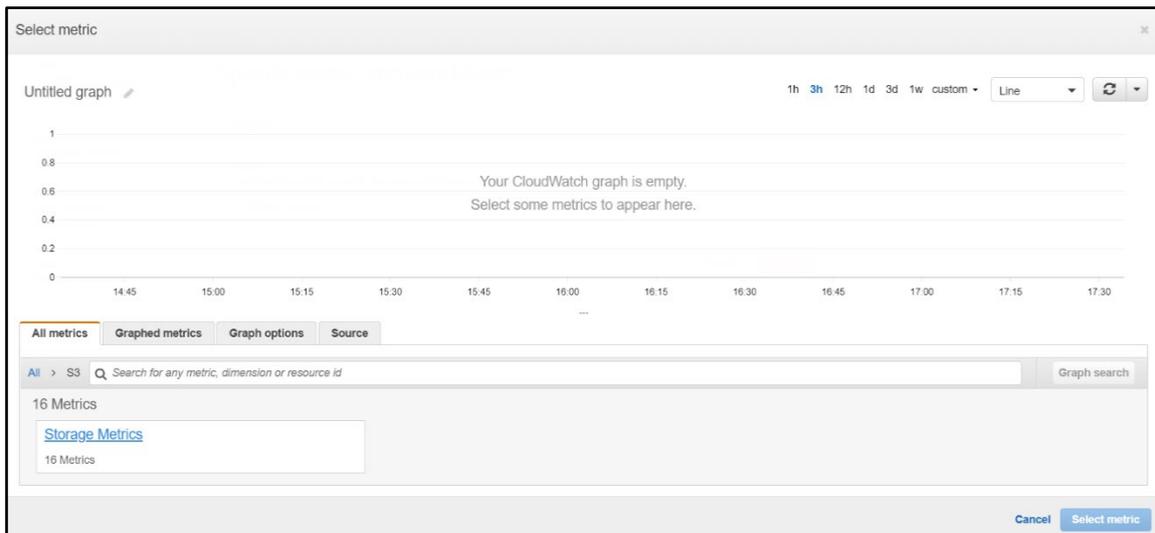
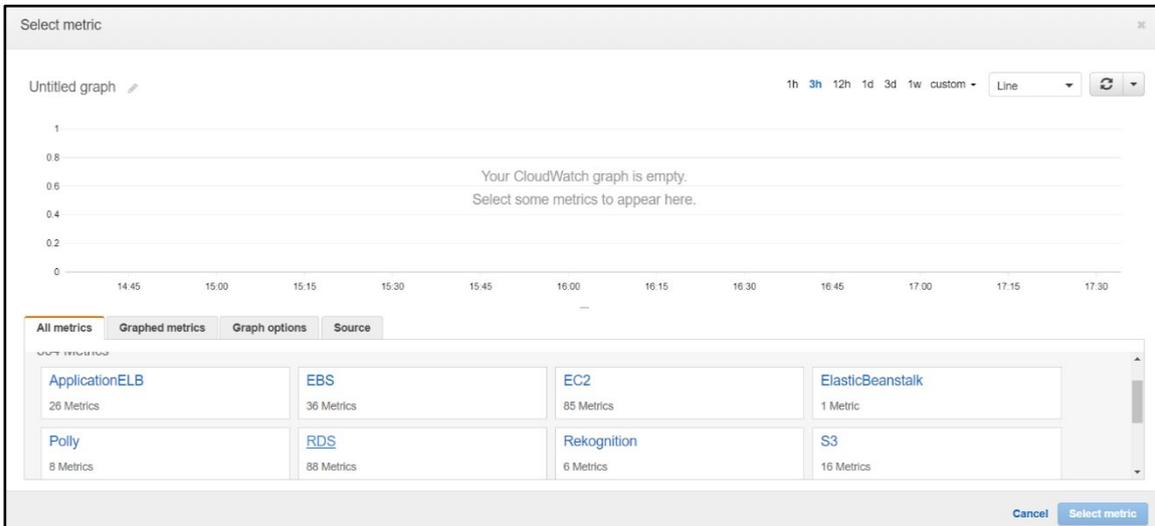
2. Click on CloudWatch from service and then click on "In alarm".



3. Now click on Create alarm and do configuration.



4. Then select matrix by setting for S3. So, select S3.



5. Now select storage matrix as well as bucket.

Select metric

Untitled graph 1h 3h 12h 1d 3d 1w custom Line ↺ ↻

Your CloudWatch graph is empty.
Select some metrics to appear here.

All metrics **Graphed metrics** Graph options Source

All > S3 > Storage Metrics Graph search

BucketName (16)	StorageType	Metric Name
<input type="checkbox"/> AbhishekDas4499	StandardStorage	BucketSizeBytes
<input type="checkbox"/> AbhishekDas0317	AllStorageTypes	NumberOfObjects

Cancel Select metric

6. Then edit matrix condition and configure threshold type, alarm condition and threshold value.

CloudWatch > Alarms > Create alarm

Step 1 **Specify metric and conditions**

Step 2 Configure actions

Step 3 Add name and description

Step 4 Preview and create

Specify metric and conditions

Metric Edit

Graph
This alarm will trigger when the blue line goes above the red line for 1 datapoints within 1 day.

Count

Namespace

Metric name

StorageType

BucketName

Statistic ×

Period

Conditions

Threshold type

Static
Use a value as a threshold

Anomaly detection
Use a band as a threshold

Whenever NumberOFObjects is...

Define the alarm condition.

Greater
> threshold

Greater/Equal
≥ threshold

Lower/Equal
≤ threshold

Lower
< threshold

than...

Define the threshold value.

Must be a number

▶ Additional configuration

Cancel Next

7. Click on next and select alarm trigger.

CloudWatch > Alarms > Create alarm

Step 1
Specify metric and conditions

Step 2
Configure actions

Step 3
Add name and description

Step 4
Preview and create

Configure actions

Notification

Alarm state trigger
Define the alarm state that will trigger this action. Remove

In alarm
The metric or expression is outside of the defined threshold.

OK
The metric or expression is within the defined threshold.

Insufficient data
The alarm has just started or not enough data is available.

Select an SNS topic
Define the SNS (Simple Notification Service) topic that will receive the notification.

Select an existing SNS topic

Create new topic

Use topic ARN

Send a notification to...

Only email lists for this account are available.

Add notification

8. Create SNS for notification and write the topic name.

CloudWatch > Alarms > Create alarm

Step 1
Specify metric and conditions

Step 2
Configure actions

Step 3
Add name and description

Step 4
Preview and create

Configure actions

Notification

Alarm state trigger
Define the alarm state that will trigger this action. Remove

In alarm
The metric or expression is outside of the defined threshold.

OK
The metric or expression is within the defined threshold.

Insufficient data
The alarm has just started or not enough data is available.

Select an SNS topic
Define the SNS (Simple Notification Service) topic that will receive the notification.

Select an existing SNS topic

Create new topic

Use topic ARN

Send a notification to...

Only email lists for this account are available.

Add notification

9. For email notification provide email id and then click on create topic.

Preview and create

Select an SNS topic
Define the SNS (Simple Notification Service) topic that will receive the notification.

Select an existing SNS topic

Create new topic

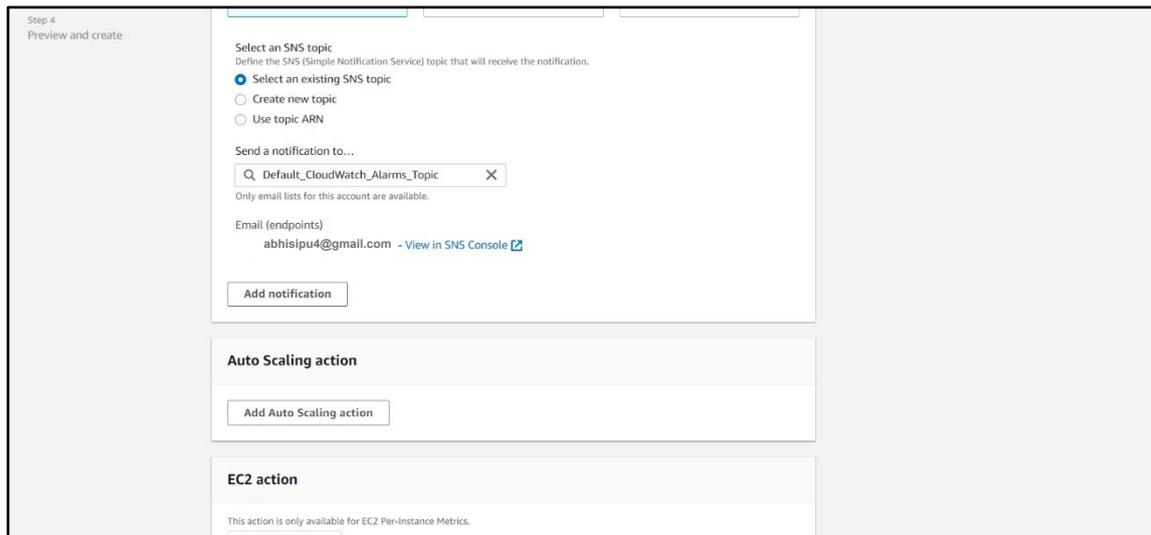
Use topic ARN

Create a new topic...
The topic name must be unique.

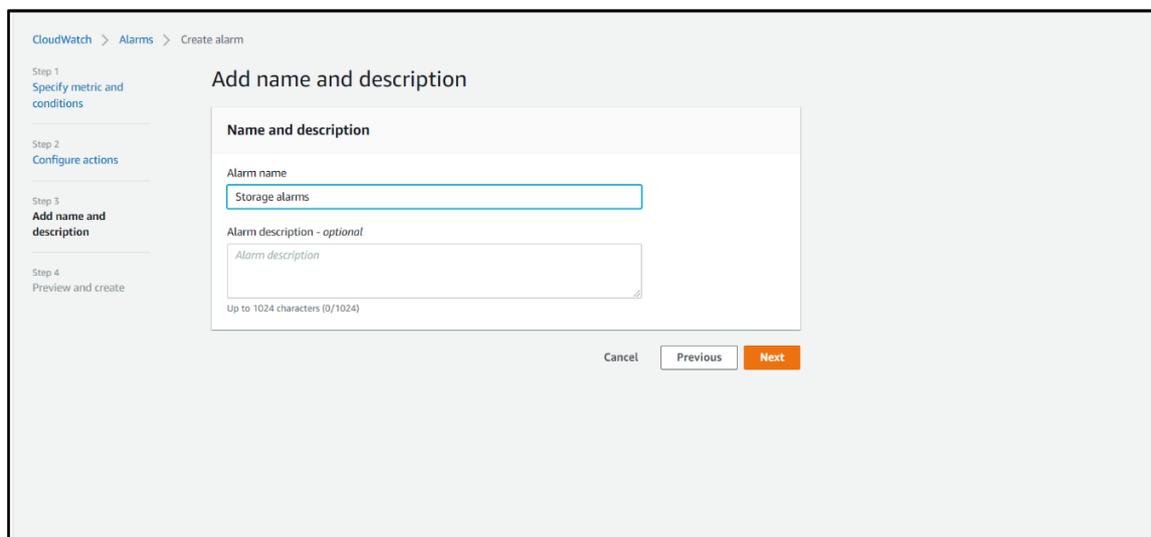
SNS topic names can contain only alphanumeric characters, hyphens (-) and underscores (_).

Email endpoints that will receive the notification...
Add a comma-separated list of email addresses. Each address will be added as a subscription to the topic above.

user1@example.com, user2@example.com



10. Click on next and write alarm name.



11. Again, click on next and create alarm.

12. Our alarm is successfully created for confirmation we have to go to our email and confirm its subscription.

13. Then CloudWatch created successfully.

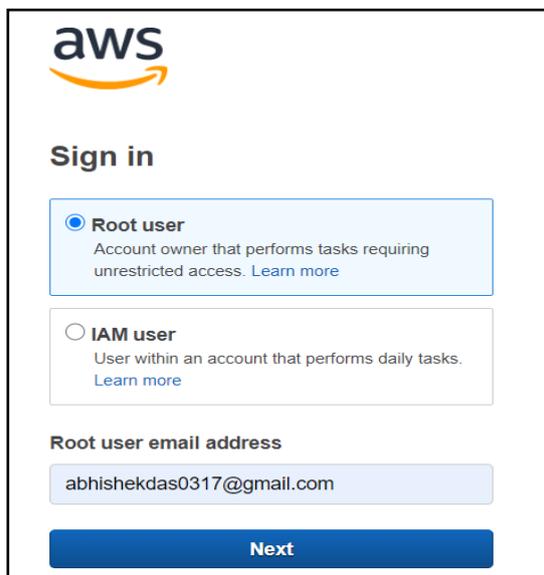
14. In case your bucket size increases then threshold size will also change correspondingly and notify in your email.

09: Amazon RDS

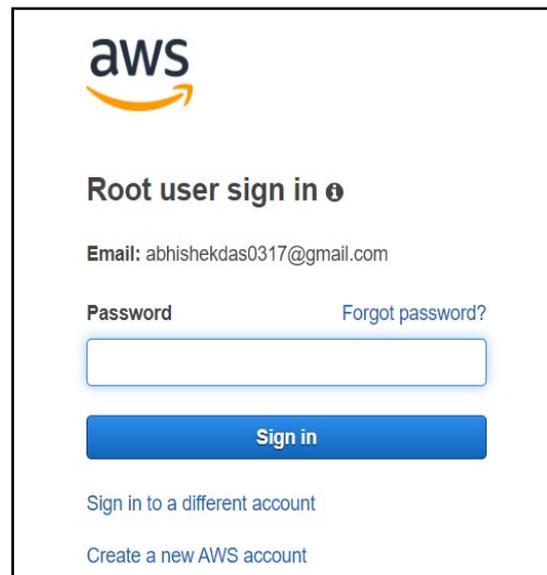
About Amazon RDS: Amazon Relational Database Service (Amazon RDS) makes it easy to set up, operate, and scale a relational database in the cloud. It provides cost-efficient and resizable capacity while automating time-consuming administration tasks such as hardware provisioning, database setup, patching and backups.

Process to Configure Amazon RDS:

1. Sign in to the AWS Management Console.

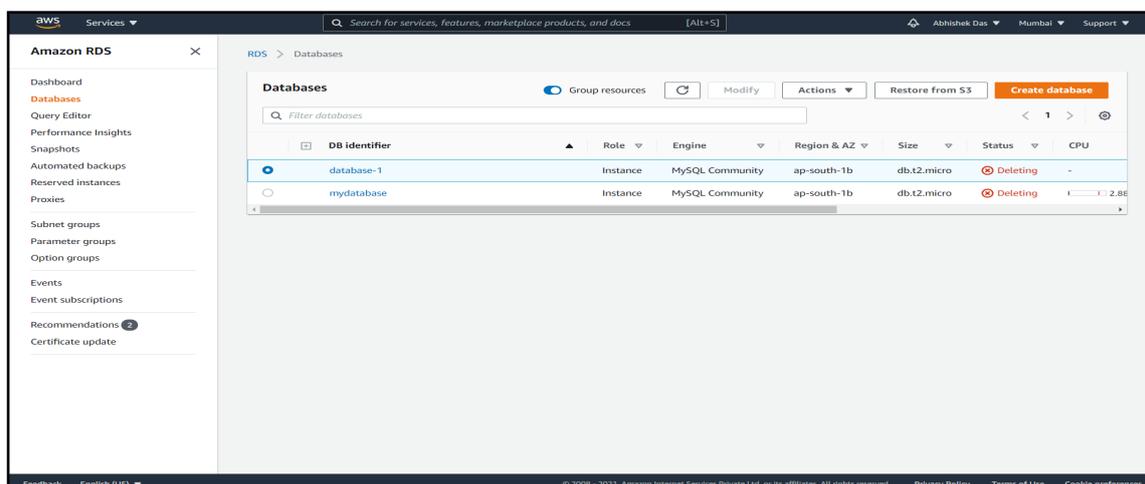


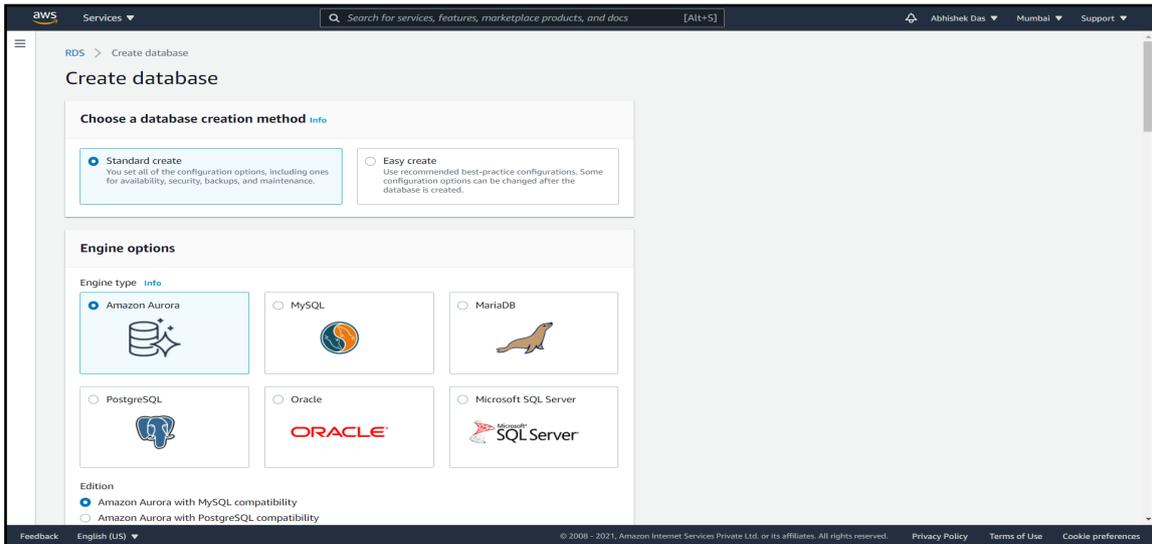
The screenshot shows the AWS Sign in page. At the top is the AWS logo. Below it is the 'Sign in' heading. There are two radio button options: 'Root user' (selected) and 'IAM user'. The 'Root user' option is described as 'Account owner that performs tasks requiring unrestricted access. Learn more'. The 'IAM user' option is described as 'User within an account that performs daily tasks. Learn more'. Below these options is a text input field for 'Root user email address' containing 'abhishekdas0317@gmail.com'. At the bottom is a blue 'Next' button.



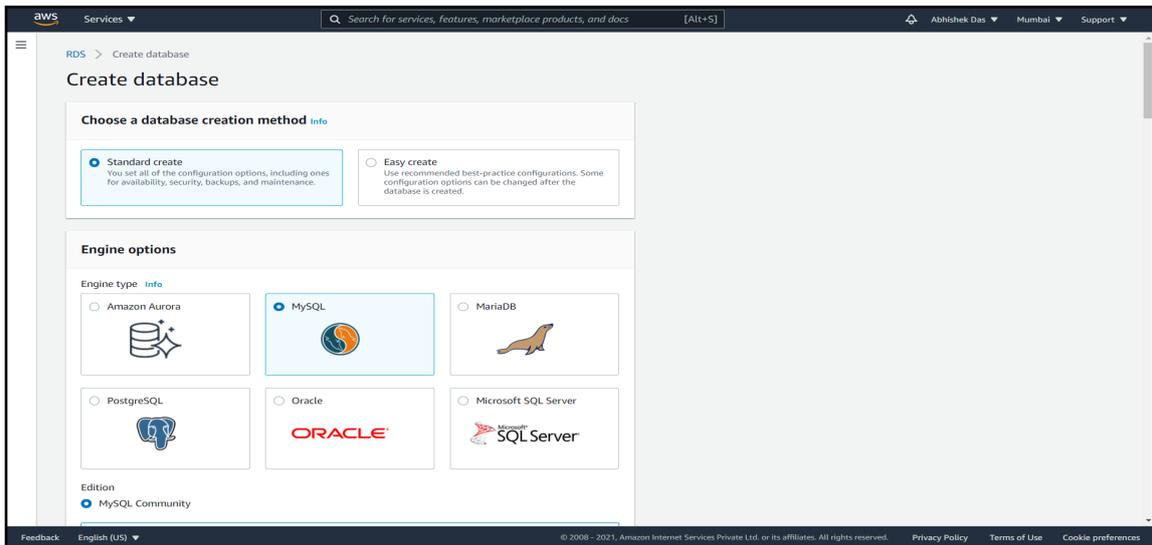
The screenshot shows the AWS Root user sign in page. At the top is the AWS logo. Below it is the heading 'Root user sign in'. There is an 'Email' field containing 'abhishekdas0317@gmail.com' and a 'Forgot password?' link. Below the email field is a 'Password' field. At the bottom is a blue 'Sign in' button. Below the button are two links: 'Sign in to a different account' and 'Create a new AWS account'.

2. Open RDS from services and click on create Database.

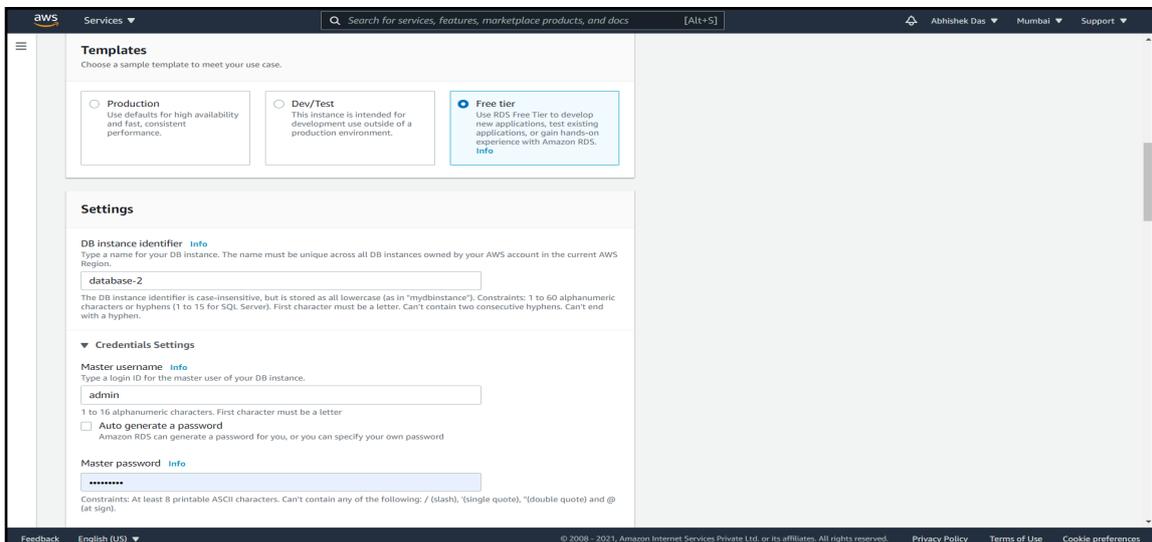




3. Then select MySQL database and select its version.



4. Now select Free Tier Template.



5. And in settings provide its name, master username, password.

The screenshot shows the 'Settings' page in the AWS Management Console. The 'DB instance identifier' field contains 'mydatabase007'. Under 'Credentials Settings', the 'Master username' field contains 'admin'. The 'Auto generate a password' checkbox is unchecked. The 'Master password' field contains a masked password. The 'Confirm password' field also contains a masked password. The 'DB instance class' section is partially visible at the bottom.

6. Select instance type and Storage.

The screenshot shows the 'DB instance class' selection page. A dropdown menu is open, showing various instance classes. The 'db.t2.micro' class is selected. The page also shows the 'Maximum storage threshold' section with a value of '1000' GIB.

The screenshot shows the 'Storage' configuration page. The 'Storage type' is set to 'General Purpose (SSD)'. The 'Allocated storage' is set to '20' GIB. The 'Storage autoscaling' checkbox is checked. The 'Maximum storage threshold' is set to '1000' GIB. The 'Availability & durability' section shows the 'Multi-AZ deployment' options, with 'Create a standby instance' selected.

7. In Connectivity, allow public access and also choose subnet group and VPC security group.

The screenshot shows the 'Connectivity' configuration page in the AWS console. It includes sections for 'Virtual private cloud (VPC)', 'Subnet group', 'Public access', and 'VPC security group'. The 'Public access' section has the 'Yes' radio button selected. The 'VPC security group' section has 'Choose existing' selected, with 'default' chosen from the dropdown menu.

Virtual private cloud (VPC) Info
VPC that defines the virtual networking environment for this DB instance.
Default VPC (vpc-34da2a5f)
Only VPCs with a corresponding DB subnet group are listed.

After a database is created, you can't change the VPC selection.

Subnet group Info
DB subnet group that defines which subnets and IP ranges the DB instance can use in the VPC you selected.
default-vpc-34da2a5f

Public access Info
 Yes
Amazon EC2 instances and devices outside the VPC can connect to your database. Choose one or more VPC security groups that specify which EC2 instances and devices inside the VPC can connect to the database.
 No
RDS will not assign a public IP address to the database. Only Amazon EC2 instances and devices inside the VPC can connect to your database.

VPC security group
Choose a VPC security group to allow access to your database. Ensure that the security group rules allow the appropriate incoming traffic.
 Choose existing
Choose existing VPC security groups
 Create new
Create new VPC security group

Existing VPC security groups
Choose VPC security groups
default

8. After complete review, click on Create database.

The screenshot shows the 'Additional configuration' and 'Estimated monthly costs' sections of the AWS RDS console. The 'Additional configuration' section includes options for 'Password authentication', 'Password and IAM database authentication', and 'Password and Kerberos authentication'. The 'Estimated monthly costs' section provides information about the Amazon RDS Free Tier and lists the resources included for 12 months.

Password authentication
Authenticates using database passwords.

Password and IAM database authentication
Authenticates using the database password and user credentials through AWS IAM users and roles.

Password and Kerberos authentication (not available for this version)
Choose a directory in which you want to allow authorized users to authenticate with this DB instance using Kerberos Authentication.

Additional configuration
Database options, backup enabled, backtrack disabled, Enhanced Monitoring disabled, maintenance, CloudWatch Logs, delete protection disabled

Estimated monthly costs
The Amazon RDS Free Tier is available to you for 12 months. Each calendar month, the free tier will allow you to use the Amazon RDS resources listed below for free:
• 750 hrs of Amazon RDS in a Single-AZ db.t2.micro Instance.
• 20 GB of General Purpose Storage (SSD).
• 20 GB for automated backup storage and any user-initiated DB Snapshots.
[Learn more about AWS Free Tier.](#)
When your free usage expires or if your application use exceeds the free usage tiers, you simply pay standard, pay-as-you-go service rates as described in the [Amazon RDS Pricing page.](#)

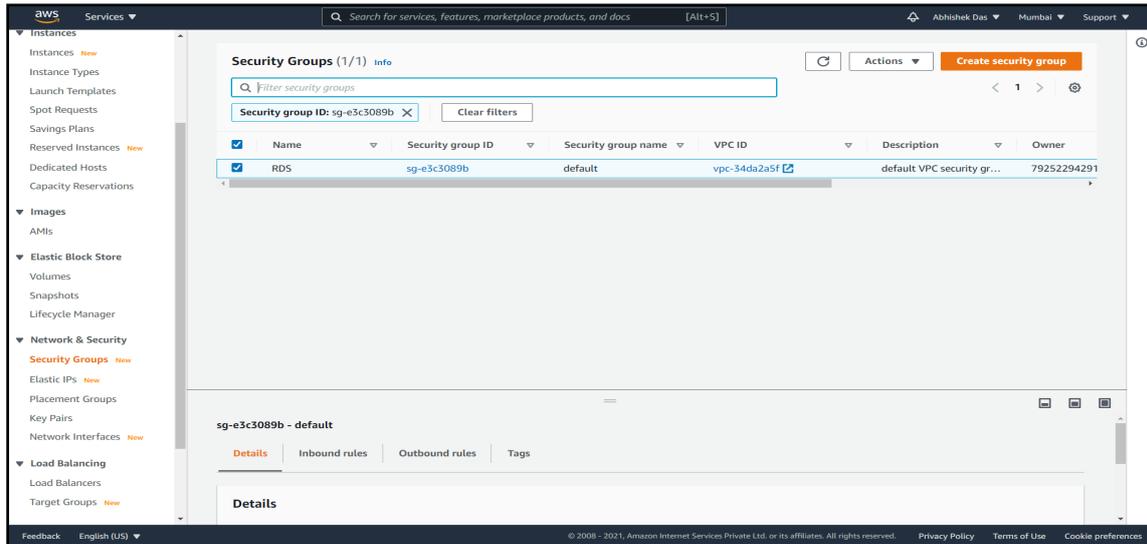
You are responsible for ensuring that you have all of the necessary rights for any third-party products or services that you use with AWS services.

Cancel **Create database**

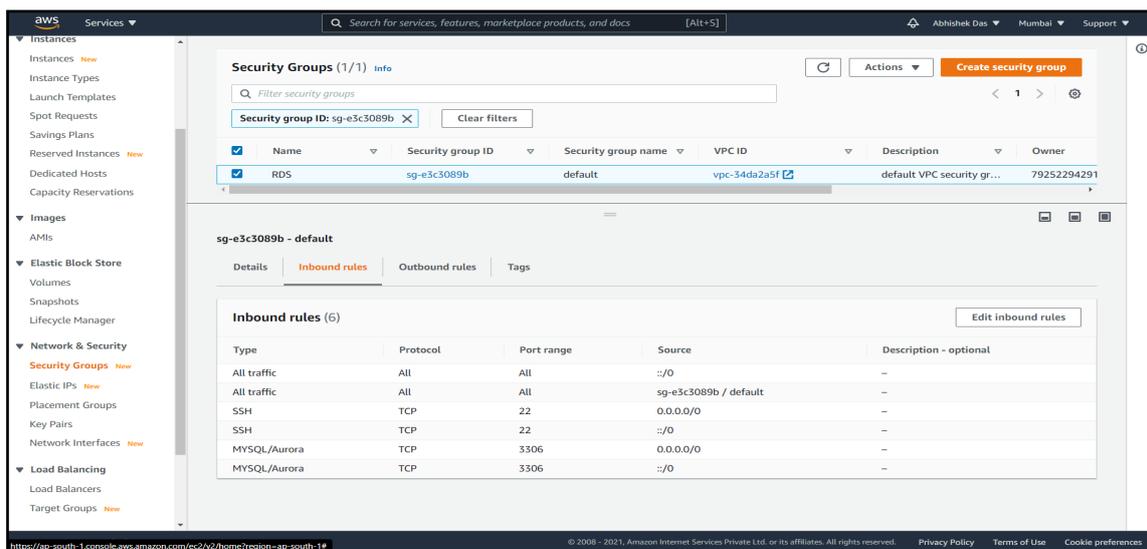
The screenshot shows the 'Amazon RDS' console with the 'Databases' view selected. A table lists the database instances, including the identifier, role, engine, region, size, status, and CPU.

DB identifier	Role	Engine	Region & AZ	Size	Status	CPU
mydatabase007	Instance	MySQL Community	ap-south-1b	db.t2.micro	Creating	-

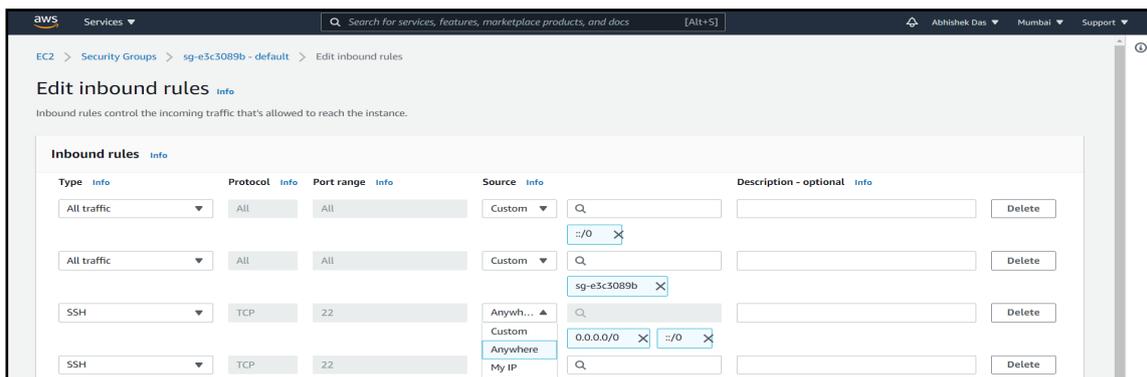
9. Then go to EC2 and click on security group.



10. Now select Inbound rules and click on Edit Inbound rules.

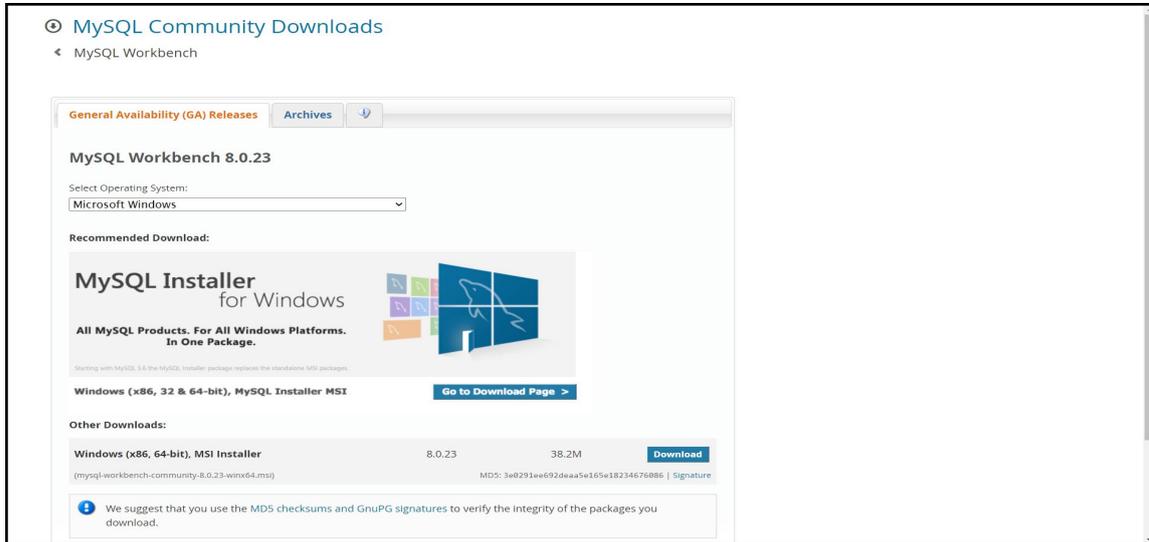


11. Add SSH and edit source to Anywhere.

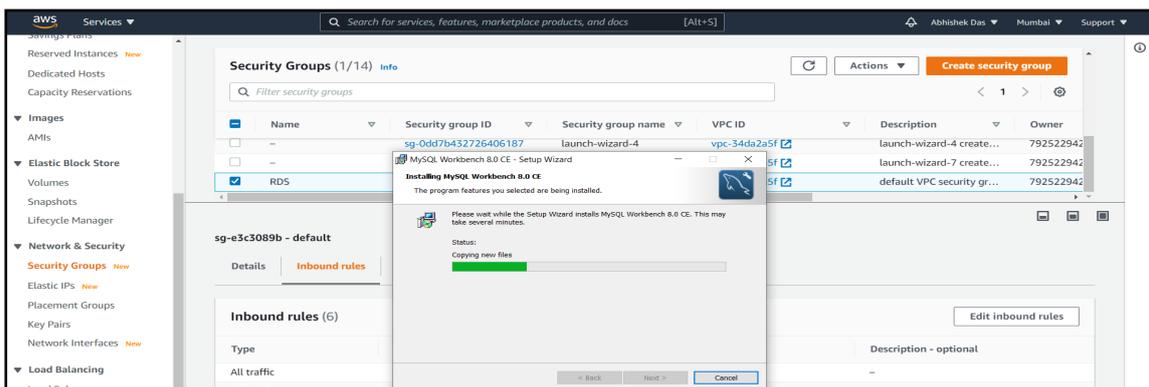
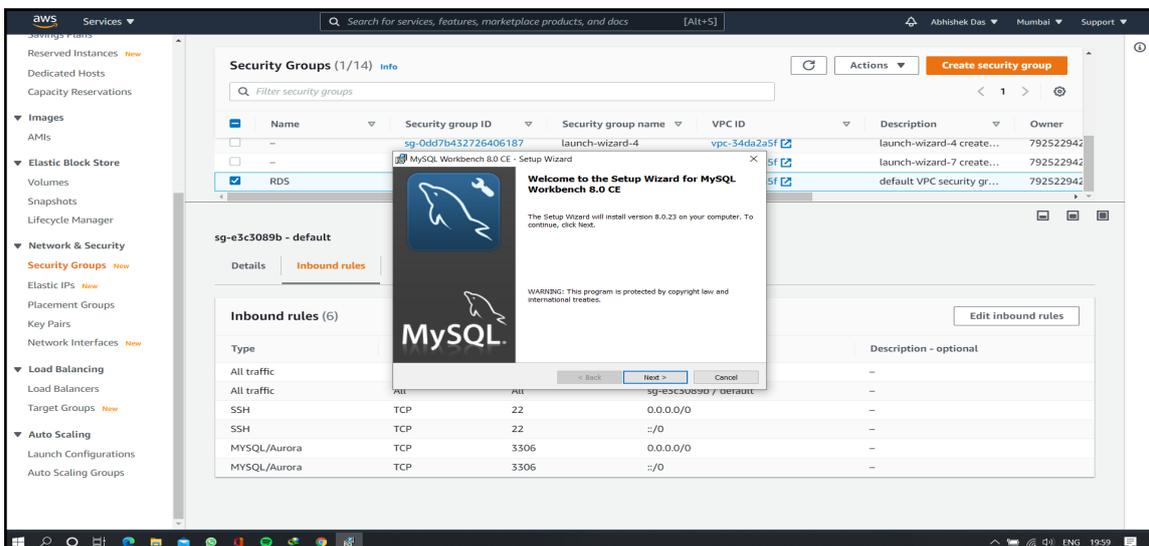


12. Now browse this site

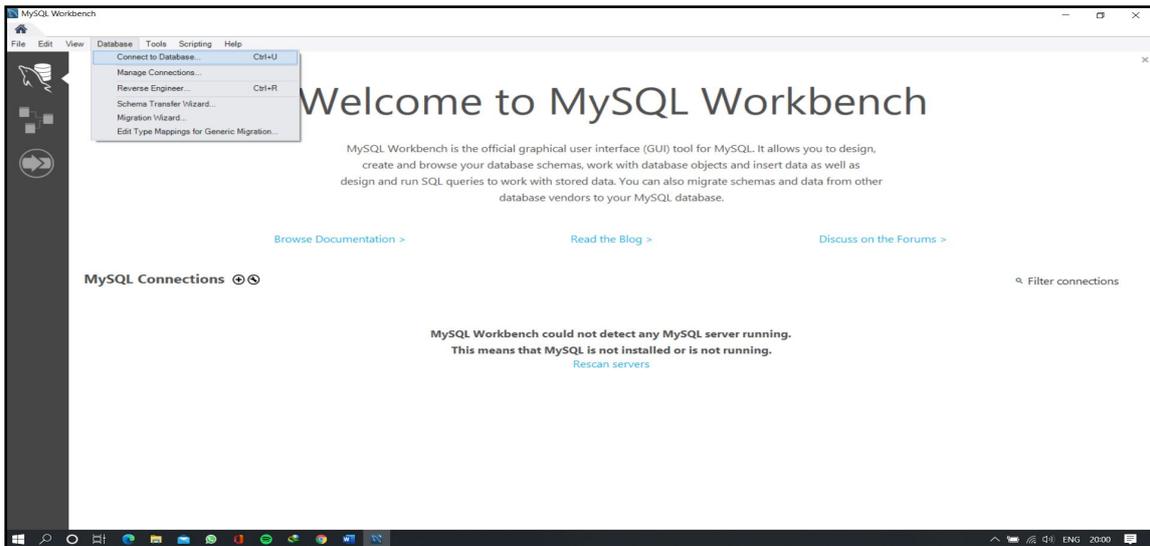
<https://dev.mysql.com/downloads/workbench/> “and download MySQL installer.



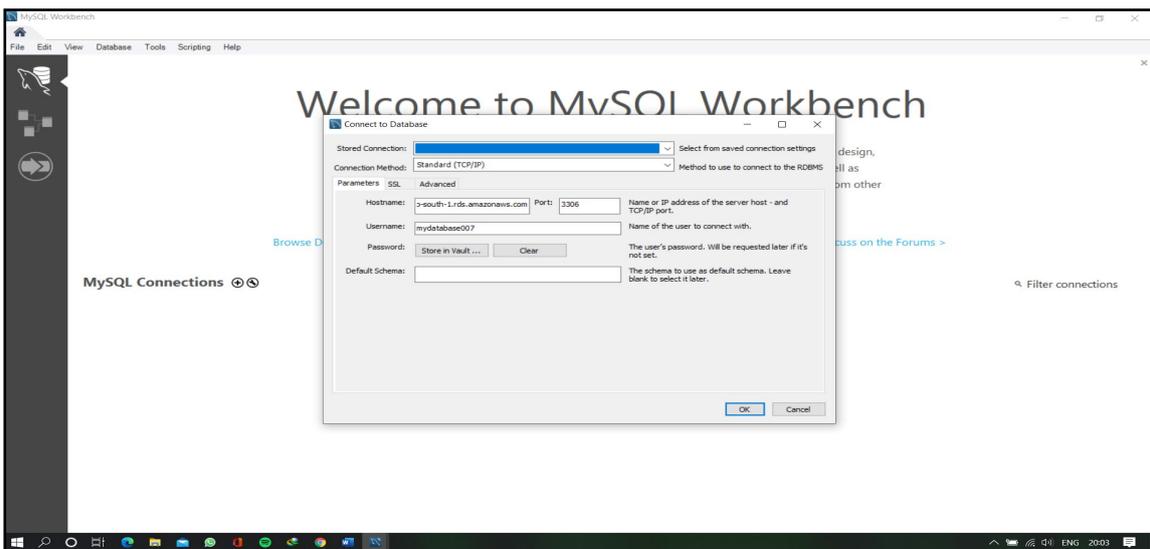
13. Then install MySQL and launch it.



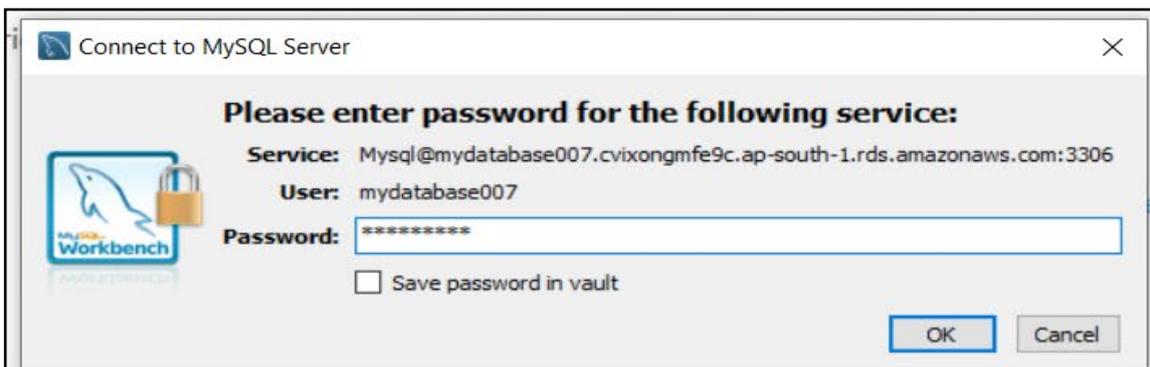
14. Then click on database >> connect database.



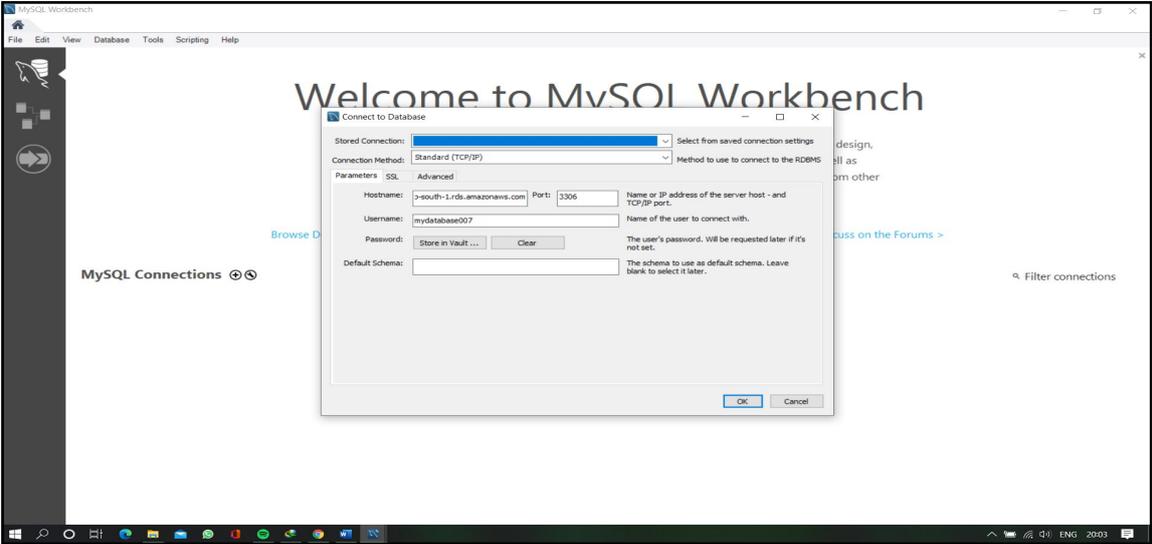
15. Now enter end point and password.



16. Then click on connect.



17. After successful connection we can create database.



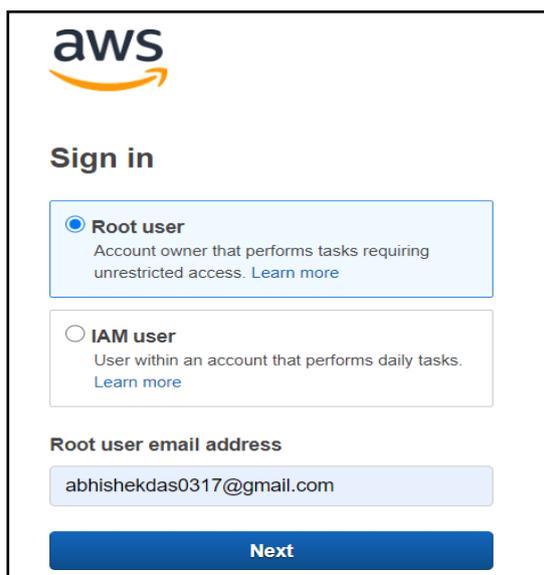
10: AWS CLI

About AWS CLI (Command Line Interface):

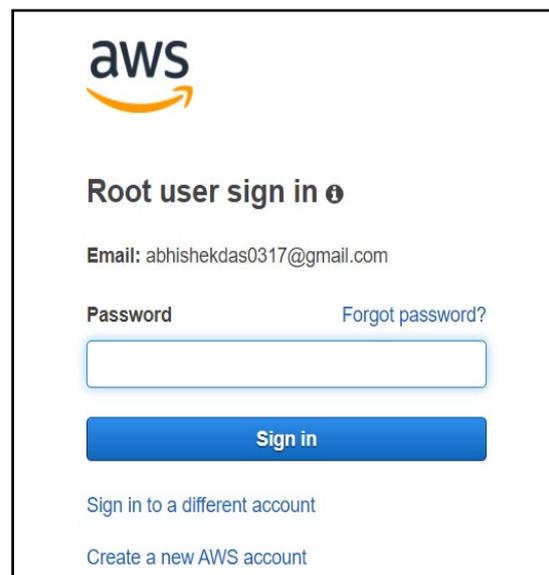
AWS Command Line Interface (CLI) is a unified tool to manage your AWS services. With just one tool to download and configure, you can control multiple AWS services from the command line and automate them through scripts.

Process to Configure Amazon CLI:

1. Sign in to the AWS Management Console.

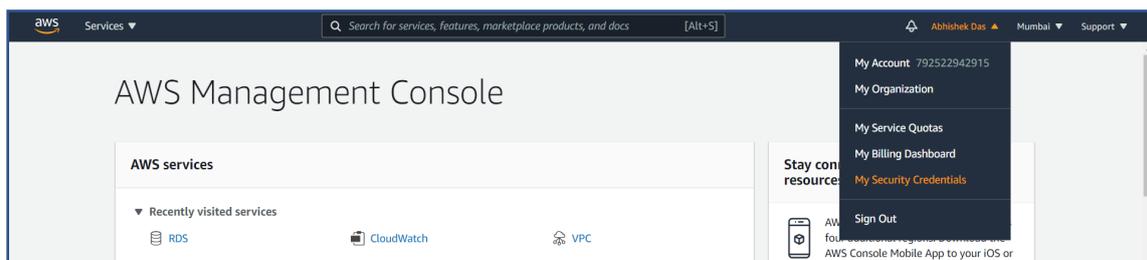


The screenshot shows the AWS Sign in page. At the top is the AWS logo. Below it is the heading "Sign in". There are two radio button options: "Root user" (selected) and "IAM user". The "Root user" option has a description: "Account owner that performs tasks requiring unrestricted access. Learn more". The "IAM user" option has a description: "User within an account that performs daily tasks. Learn more". Below these options is a text input field for "Root user email address" containing "abhishekdas0317@gmail.com". At the bottom is a blue "Next" button.

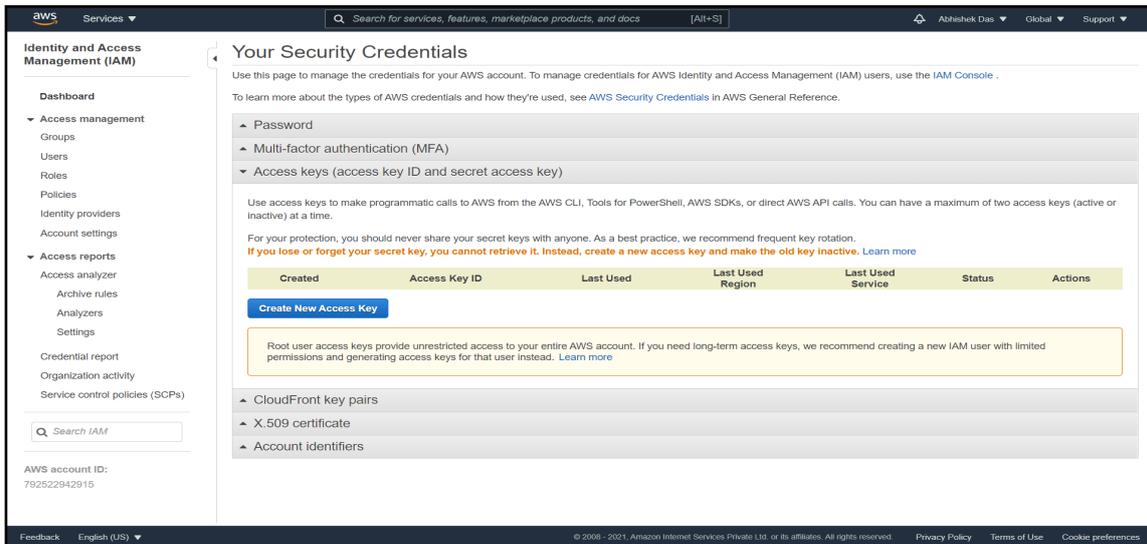


The screenshot shows the AWS Root user sign in page. At the top is the AWS logo. Below it is the heading "Root user sign in". There is a text input field for "Email" containing "abhishekdas0317@gmail.com". Below that is a "Password" input field with a "Forgot password?" link. At the bottom is a blue "Sign in" button. Below the button are two links: "Sign in to a different account" and "Create a new AWS account".

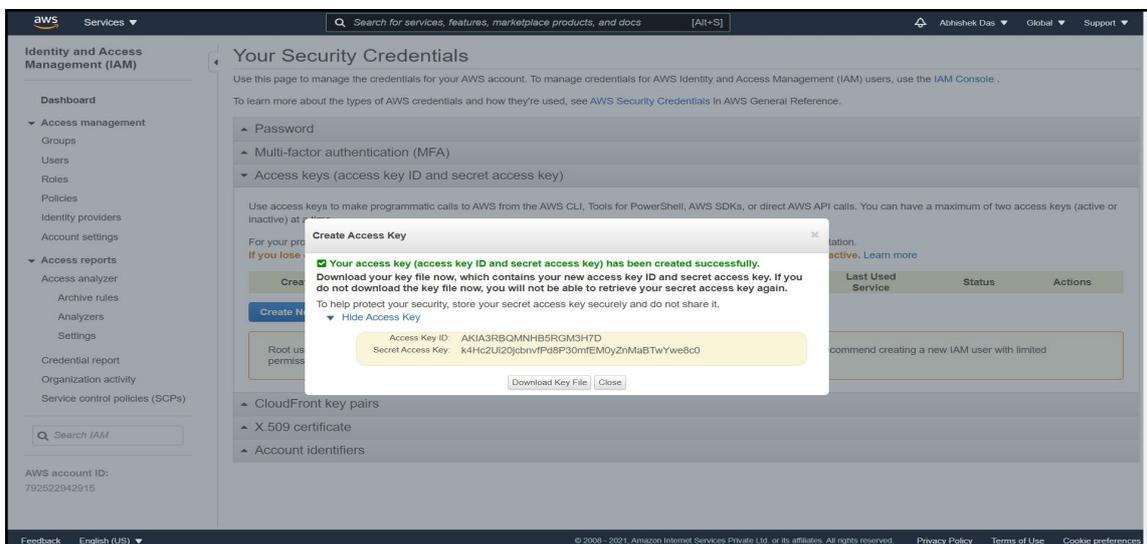
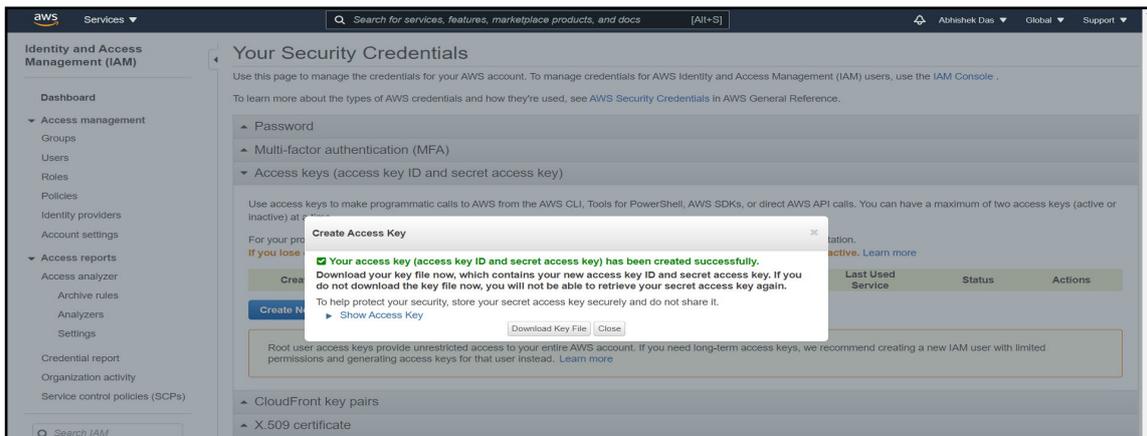
2. In Dashboard, go to My Security Credential.



3. Then click on Access Key and Create New Access Key.



4. Now click Show Access Key, then it will show Access key ID as well as Secret Access Key.



5. Now search for Aws Command Line Interface, Download and install it.

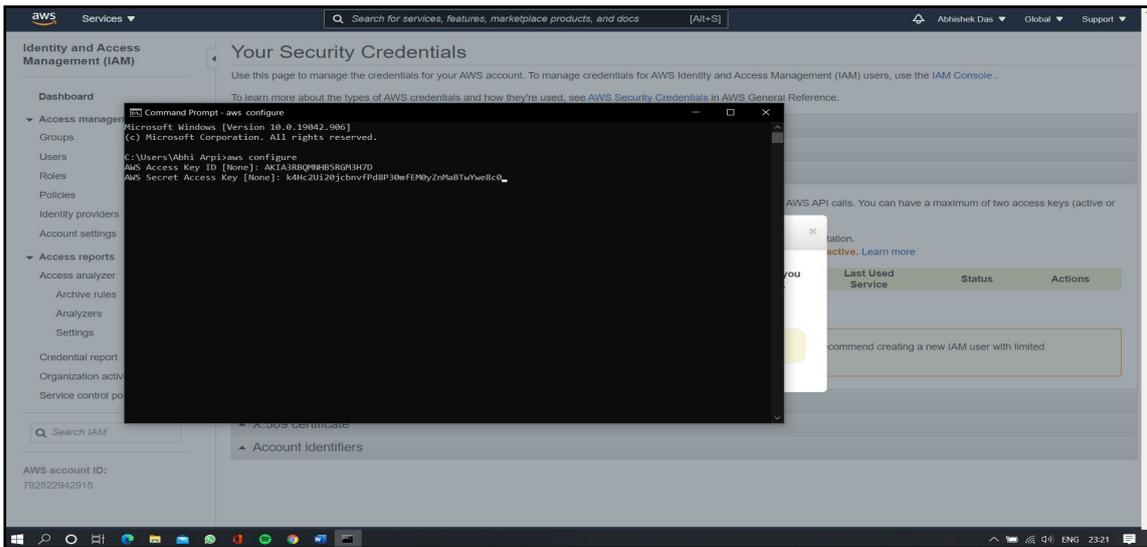
The screenshot shows the AWS website's 'AWS Command Line Interface' page. The page title is 'AWS Command Line Interface'. Below the title, there is a brief description: 'The AWS Command Line Interface (CLI) is a unified tool to manage your AWS services. With just one tool to download and configure, you can control multiple AWS services from the command line and automate them through scripts.' Below this, there are four icons with links: 'Getting Started', 'CLI Reference', 'GitHub Project', and 'Community Forum'. On the right side, there are sections for 'Windows', 'MacOS', 'Linux', 'Amazon Linux', and 'Release Notes'. At the bottom, there is a section for 'aws-shell (Developer Preview)'.

The screenshot shows the same AWS website page as above, but with a 'AWS Command Line Interface v2 Setup Wizard' window open in the foreground. The window title is 'AWS Command Line Interface v2 Setup' and it says 'Welcome to the AWS Command Line Interface v2 Setup Wizard'. It also says 'The Setup Wizard will install AWS Command Line Interface v2 on your computer. Click Next to continue or Cancel to exit the Setup Wizard.' The window has 'Back', 'Next', and 'Cancel' buttons.

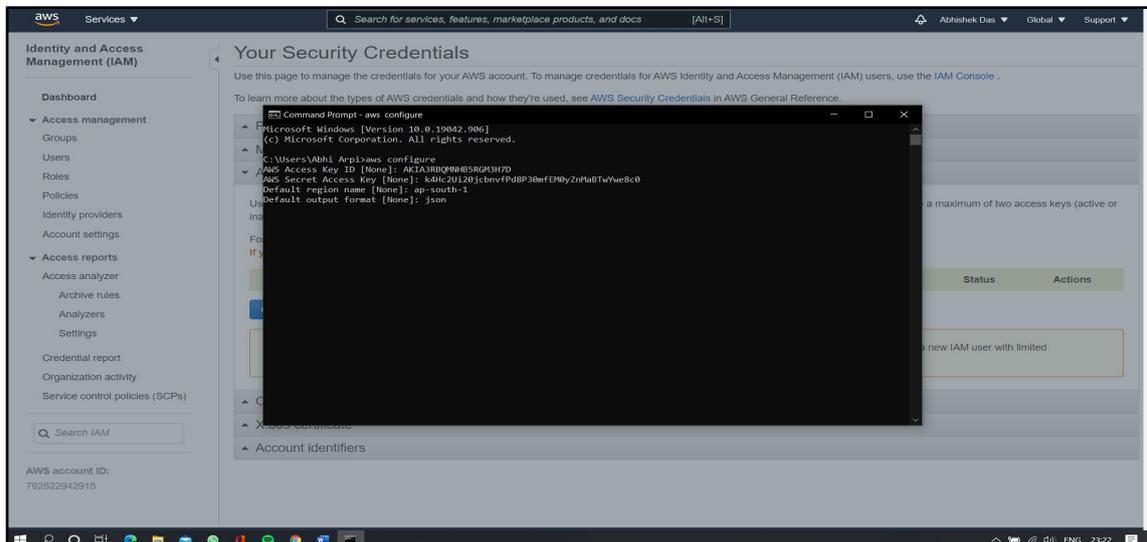
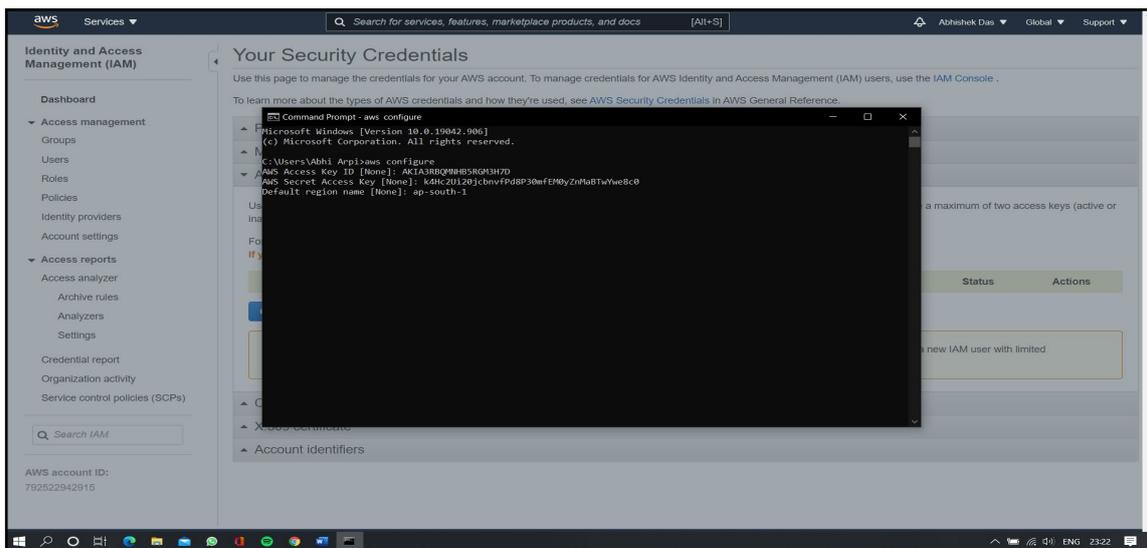
6. Then Open Command Line and type “aws configuration”.

The screenshot shows the same AWS website page as above, but with a 'Command Prompt' window open in the foreground. The window title is 'Command Prompt' and it shows the following text: 'Microsoft Windows [Version 10.0.19042.986] (c) Microsoft Corporation. All rights reserved. C:\Users\Abhi Arpi>aws configure'. The window has a standard Windows title bar with minimize, maximize, and close buttons.

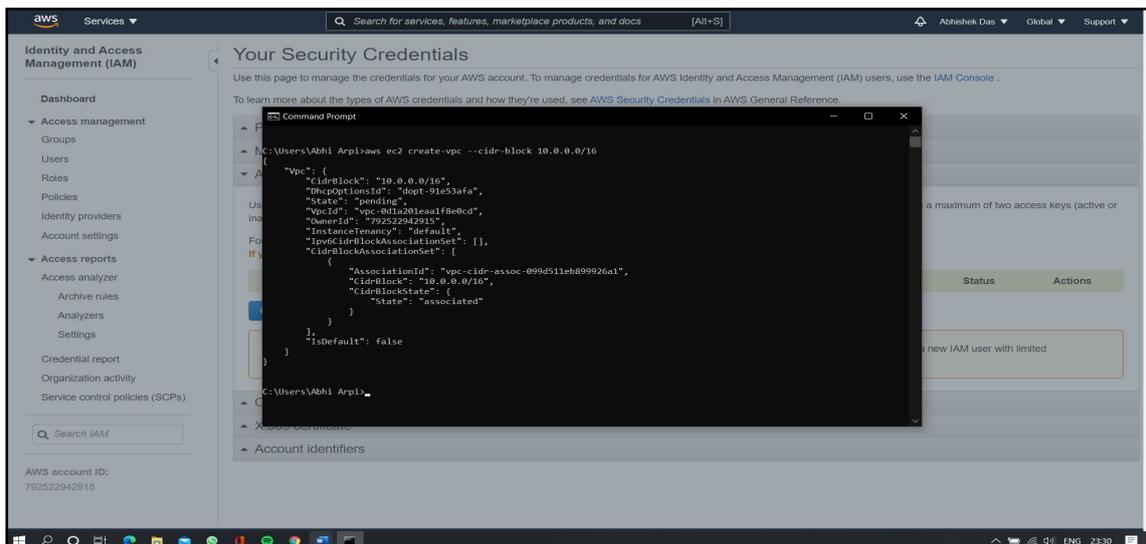
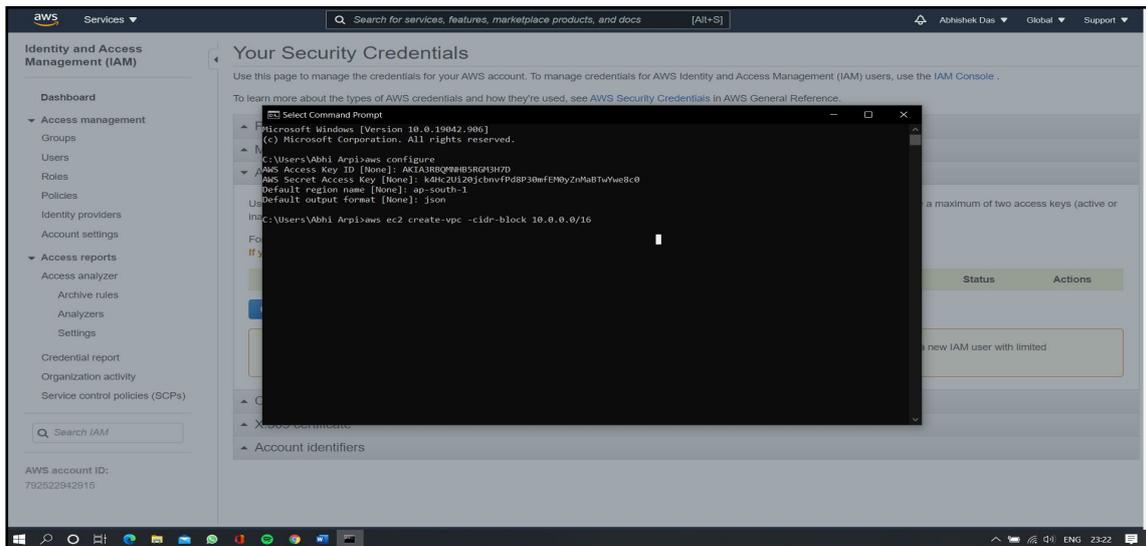
7. Then Provide Access key ID and Secret Access key.



8. Provide Region Name and output format.



9. Then type “aws ec2 create-vpc –cidr-block 10.0.0.0/16”.



10. Successfully your VPC has been created through command line.

