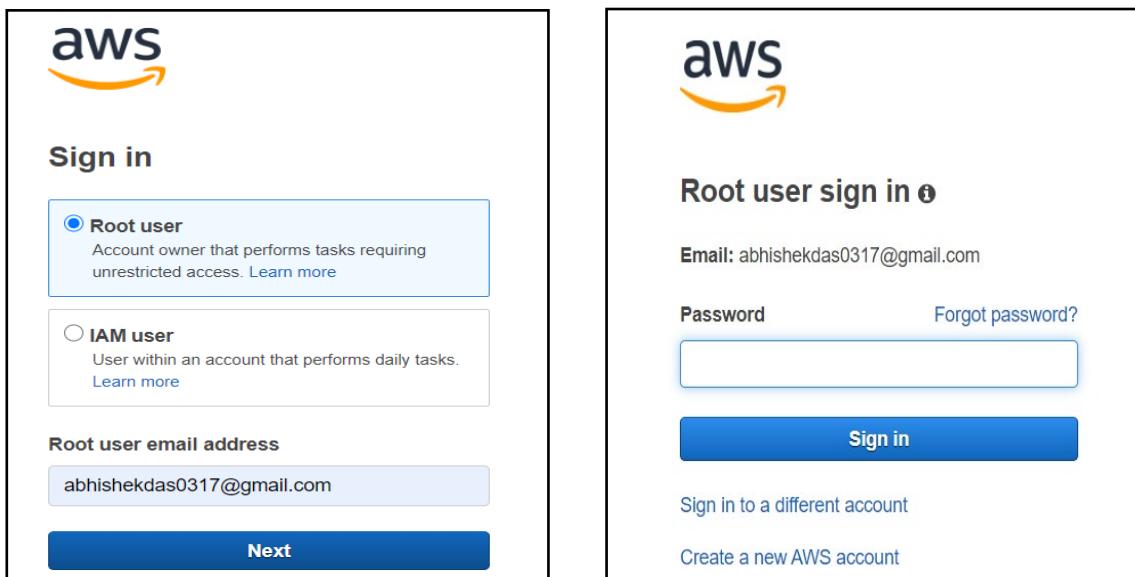


01: EC2 INSTANCE CREATION

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.



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

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

Step 1: Choose an Amazon Machine Image (AMI)

An AMI is a template that contains the software configuration (operating system, application server, and applications) required to launch your instance. You can select an AMI provided by AWS, our user community, or the AWS Marketplace; or you can select one of your own AMIs.

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

Quick Start

Category	AMI Name	Description	Root device type	Virtualization type	ENI Enabled	Action
Amazon Linux	Amazon Linux 2 AMI (HVM), SSD Volume Type - ami-08e0ca9924195beba (64-bit x86) / ami-0437d5dbe8fd3d52 (64-bit Arm)	Amazon Linux 2 comes with five years support. It provides Linux kernel 4.14 tuned for optimal performance on Amazon EC2, systemd 219, GCC 7.3, Glibc 2.26, Binutils 2.29.1, and the latest software packages through extras. This AMI is the successor of the Amazon Linux AMI that is approaching end of life on December 31, 2020 and has been removed from this wizard.	ebs	hvm	Yes	Select 64-bit (x86) 64-bit (Arm)
Red Hat	Red Hat Enterprise Linux 8 (HVM), SSD Volume Type - ami-0a9d27a9f4f5c0efc (64-bit x86) / ami-0816d75a127c17a49 (64-bit Arm)	Red Hat Enterprise Linux version 8 (HVM), EBS General Purpose (SSD) Volume Type	ebs	hvm	ENI Enabled: Yes	Select 64-bit (x86) 64-bit (Arm)
SUSE Linux	SUSE Linux Enterprise Server 15 SP2 (HVM), SSD Volume Type - ami-0b3acf3edf2397475 (64-bit x86) / ami-0ab71076ab9b53b0d (64-bit Arm)	SUSE Linux Enterprise Server 15 Service Pack 2 (HVM), EBS General Purpose (SSD) Volume Type. Amazon EC2 AMI Tools preinstalled, Apache 2.2, MySQL 5.5, PHP 5.3, and Ruby 1.8.7 available.	ebs	hvm	ENI Enabled: Yes	Select 64-bit (x86) 64-bit (Arm)
	Ubuntu Server 20.04 LTS (HVM), SSD Volume Type - ami-0a4a70bd98c6d9441 (64-bit x86) / ami-00e24e2d9b2d70f5c (64-bit Arm)	Ubuntu Server 20.04 LTS (HVM), EBS General Purpose (SSD) Volume Type. Support available from Canonical (http://www.ubuntu.com/cloud/services).	ebs	hvm	ENI Enabled: Yes	Select 64-bit (x86) 64-bit (Arm)

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. Learn more about instance types how they can meet your computing needs.

Filter by:	All instance families	Current generation	Show/Hide Columns		
Currently selected: t2.micro (- ECUs, 1 vCPUs, 2.5 GHz, ~ 1 GiB memory, EBS only)					
Family	Type	vCPUs	Memory (GiB)	Instance Storage (GB)	EBS-Optimized Available
t2	t2.nano	1	0.5	EBS only	-
<input checked="" type="checkbox"/>	t2.micro	1	1	EBS only	-
t2	t2.small	1	2	EBS only	-
t2	t2.medium	2	4	EBS only	-
t2	t2.large	2	8	EBS only	-

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	Launch into Auto Scaling Group
Purchasing option	<input type="checkbox"/> Request Spot instances	
Network	vpc-34da2a5f (default)	<input type="button"/> Create new VPC
Subnet	No preference (default subnet in any Availability Zone)	<input type="button"/> Create new subnet
Auto-assign Public IP	<input type="button"/> Use subnet setting (Enable)	
Placement group	<input type="checkbox"/> Add instance to placement group	
Capacity Reservation	<input type="button"/> Open	
Domain join directory	<input type="button"/> No directory	
IAM role	<input type="button"/> None	
CPU options	<input type="checkbox"/> Specify CPU options	
Shutdown behavior	Stop	
Stop - Hibernate behavior	<input type="checkbox"/> Enable hibernation as an additional stop behavior	
Enable termination protection	<input type="checkbox"/> Protect against accidental termination	
Monitoring	<input type="checkbox"/> 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. Learn more about storage options in Amazon EC2.

Volume Type	Device	Snapshot	Size (GiB)	Volume Type	IOPS	Throughput (MB/s)	Delete on Termination	Encryption
Root	/dev/xvda	snap-07e0fc01c6bd3978	8	General Purpose SSD (gp2)	100 / 5000	N/A	<input checked="" type="checkbox"/>	Not Encrypted

Add New Volume

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.

6. Click on review and launch.

Step 5: Add Tags

A tag consists of a case-sensitive key-value pair. For example, you could define a tag with key = Name and value = Webserver.

A copy of a tag can be applied to volumes, instances or both.

Tags will be applied to all instances and volumes. Learn more about tagging your Amazon EC2 resources.

Key (128 characters maximum) **Value** (256 characters maximum)

Instances (1) Volumes (1) Network Interfaces (1)

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.

Add Tag (Up to 50 tags maximum)

Cancel **Previous** **Review and Launch** **Next: Configure Security Group**

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.

AMI Details

Amazon Linux 2 AMI (HVM), SSD Volume Type - ami-08e0ca9924195beba

Free tier eligible Amazon Linux 2 comes with five years support. It provides Linux kernel 4.14 tuned for optimal performance on Amazon EC2, systemd 219, GCC 7.3, Glibc 2.26, Binutils 2.29.1, and the latest software packages through extras. This AMI is the successor of the Amazon Linux AMI that is a...

Instance Type

Instance Type	ECUs	vCPUs	Memory (GiB)	Instance Storage (GB)	EBS-Optimized Available	Network Performance
t2.micro	-	1	1	EBS only	-	Low to Moderate

Security Groups

Security group name launch-wizard-1
Description launch-wizard-1 created 2021-01-29T15:27:47.940+05:30

Type (1)	Protocol (1)	Port Range (1)	Source (1)	Description (1)
SSH	TCP	22	0.0.0.0/0	

Instance Details

Launch

Cancel **Previous** **Launch**

7. Continue without a key pair.

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.

AMI Details

Amazon Linux 2 AMI (HVM), SSD Volume Type - ami-08e0ca9924195beba

Free tier eligible Amazon Linux 2 comes with five years support. It provides Linux kernel 4.14 tuned for optimal performance on Amazon EC2, systemd 219, GCC 7.3, Glibc 2.26, Binutils 2.29.1, and the latest software packages through extras. This AMI is the successor of the Amazon Linux AMI that is a...

Instance Type

Instance Type	ECUs	vCPUs	Memory (GiB)	Instan...
t2.micro	-	1	1	EBS o...

Security Groups

Security group name launch-wizard-1
Description launch-wizard-1 created 2021-01-29T15:27:47.940+05:30

Type (1)	Protocol (1)	Port Range (1)	Source (1)	Description (1)
SSH	TCP	22	0.0.0.0/0	

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](#).

Proceed without a key pair
 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**

Launch

Cancel **Previous** **Launch**

8. Click on launch Instance.

The screenshot shows the AWS Launch Status page. At the top, there's a navigation bar with the AWS logo, a search bar, and account information for GEMINI Mumbai. Below the header, the main content area is titled "Launch Status". A green circular icon indicates "Your instances are now launching". Below this, a message states "The following instance launches have been initiated: i-0278dbfc98c80188d" and a link to "View launch log". There's also a section titled "Get notified of estimated charges" with a note about creating billing alerts. A "View Instances" button is present at the bottom right.

02: Creating VPC

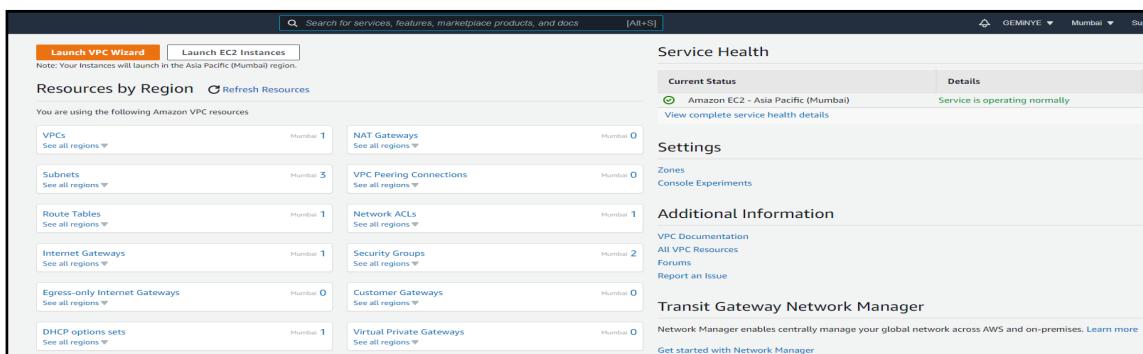
VPC (Virtual Private Cloud): Amazon Virtual Private Cloud (Amazon VPC) enables you to launch Amazon Web Services (AWS) resources into a virtual network you've defined. This virtual network resembles a traditional network that you'd operate in your own data centre, with the benefits of using the scalable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

Process to configure VPC:

1. Sign in to the AWS Management Console.

The image contains two side-by-side screenshots of the AWS sign-in interface. The left screenshot shows the 'Sign in' page with the 'aws' logo at the top. It has two radio button options: 'Root user' (selected) and 'IAM user'. Below each option is a brief description and a 'Learn more' link. A 'Root user email address' field contains the email 'abhishekdas0317@gmail.com'. At the bottom is a large blue 'Next' button. The right screenshot shows the 'Root user sign in' page with the 'aws' logo. It has fields for 'Email' (containing 'abhishekdas0317@gmail.com') and 'Password'. To the right of the password field is a 'Forgot password?' link. Below these are three links: 'Sign in to a different account', 'Create a new AWS account', and a large blue 'Sign in' button.

2. Open VPC from services under networking.



3. Click on your VPC and create VPC.

The screenshot shows the AWS VPC Dashboard. On the left, there's a sidebar with options like 'New VPC Experience', 'VPC Dashboard', 'Subnets', 'Route Tables', 'Internet Gateways', 'Egress Only Internet Gateways', 'DHCP Options Sets', 'Elastic IPs', 'Managed Prefix Lists', 'Endpoints', 'Endpoint Services', and 'NAT Gateways'. The main area is titled 'Your VPCs Info' with a search bar and a table header for 'Name', 'VPC ID', 'State', 'IPv4 CIDR', 'IPv6 CIDR', 'IPv6 pool', and 'DHCP options set'. A message at the bottom says 'Loading VPCs'.

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

The screenshot shows the 'Create VPC' configuration page. It has two main sections: 'VPC settings' and 'Tags'. In 'VPC settings', you can enter a 'Name tag - optional' (e.g., 'my-vpc'), an 'IPv4 CIDR block' (e.g., '10.0.0.0/24'), and choose an 'IPv6 CIDR block' (radio buttons for 'No IPv6 CIDR block', 'Amazon-provided IPv6 CIDR block', or 'IPv6 CIDR owned by me'). The 'Tenancy' dropdown is set to 'Default'. In the 'Tags' section, you can add key-value pairs; one tag 'Name: my-vpc' is already added. There's also a note about adding up to 10 more tags.

5. Check VPC status.

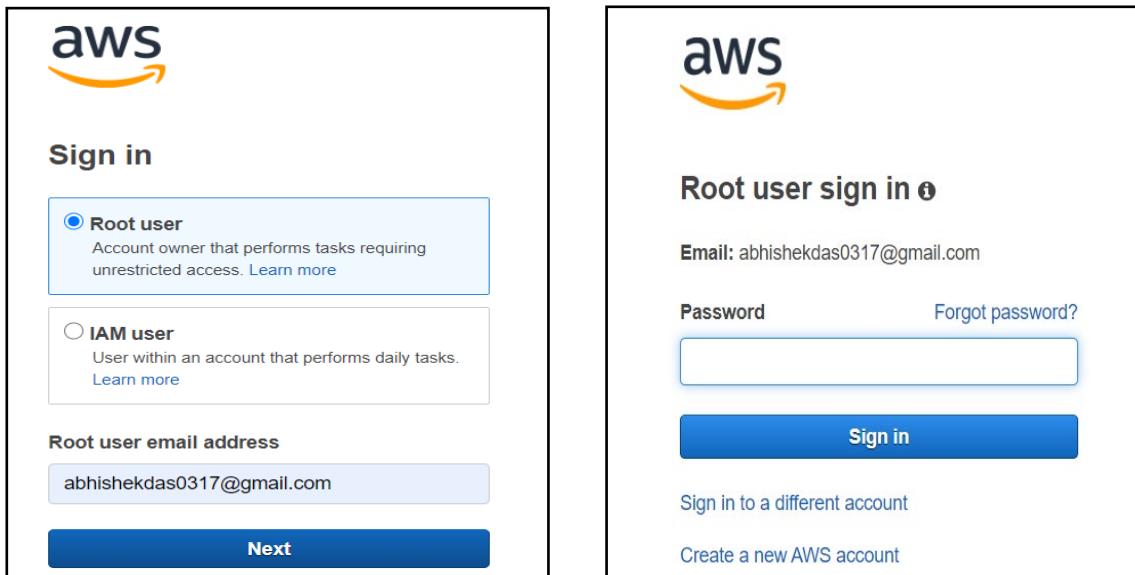
The screenshot shows the 'Details' tab of a VPC configuration page. At the top, it says 'You successfully created vpc-012402d20749e4e5a / my-vpc'. The 'Details' section shows the VPC ID ('vpc-012402d20749e4e5a'), State ('Available'), DHCP options set ('dopt-91e5sa'), IPv4 CIDR ('10.0.0.0/24'), and Owner ID ('792522942915'). Other tabs include 'CIDRs', 'Flow logs', and 'Tags'. Under 'CIDRs', there's an 'IPv4 CIDRs' section with a table for 'CIDR' and 'Status' (showing 'Associated').

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.

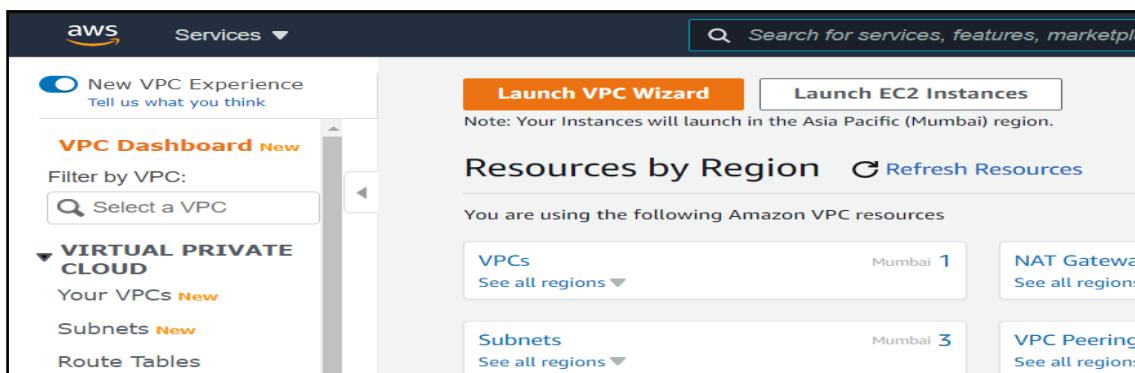
Process to configure Subnet:

1. Sign in to the AWS Management Console.



The image contains two side-by-side screenshots of the AWS sign-in interface. The left screenshot shows the 'Sign in' page with two options: 'Root user' (selected) and 'IAM user'. Below these options is a 'Root user email address' input field containing 'abhishekdas0317@gmail.com' and a 'Next' button. The right screenshot shows the 'Root user sign in' page, where the 'Email' field is filled with 'abhishekdas0317@gmail.com'. It includes fields for 'Password' and 'Forgot password?', a large 'Sign in' button, and links for '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.



VPC > Your VPCs > Create VPC

Create VPC Info

A VPC is an isolated portion of the AWS cloud populated by AWS objects, such as Amazon EC2 instances.

VPC settings

Name tag - optional
Creates a tag with a key of 'Name' and a value that you specify.
assign3

IPv4 CIDR block Info
10.0.0.0/16

Name tag - optional
Creates a tag with a key of 'Name' and a value that you specify.
assign3

IPv4 CIDR block Info
10.0.0.0/16

IPv6 CIDR block Info
 No IPv6 CIDR block
 Amazon-provided IPv6 CIDR block
 IPv6 CIDR owned by me

Tenancy Info
Default

Configuration of Private Subnet

3. Now click on Subnet to configure private subnet.

New VPC Experience
Tell us what you think

VPC Dashboard New
Filter by VPC:
Select a VPC

Subnets (3) Info

Name	Subnet ID	State	VPC	IPv4 CIDR	IPv6 CIDR
-	subnet-ea49d891	Available	vpc-34da2a5f	172.31.16.0/20	-
-	subnet-ae7e67c6	Available	vpc-34da2a5f	172.31.32.0/20	-
-	subnet-fcc48bb0	Available	vpc-34da2a5f	172.31.0.0/20	-

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

VPC > Subnets > Create subnet

Create subnet Info

VPC

VPC ID
Create subnets in this VPC.

Select a VPC

- vpc-34da2a5f (default)
- vpc-04548667fe836870b (assign3)

Availability Zone [Info](#)
 Choose the zone in which your subnet will reside, or let Amazon choose one for you.

Asia Pacific (Mumbai) / ap-south-1a	▲
<input type="text"/>	
No preference	
Asia Pacific (Mumbai) / ap-south-1a ID: aps1-az1	ap-south-1
Asia Pacific (Mumbai) / ap-south-1b ID: aps1-az3	ap-south-1
Asia Pacific (Mumbai) / ap-south-1c ID: aps1-az2	ap-south-1

[Remove](#)

[Add new tag](#)
 You can add 49 more tags.

[Remove](#)

[Add new subnet](#)

[Cancel](#) [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.

VPC Services ▾ [Search for services, features, marketplace products, and docs](#) [Alt+S] Abhishek Das Mumbai Sk

VPC > Subnets > Create subnet

Create subnet [Info](#)

VPC

VPC ID
 Create subnets in this VPC.

Select a VPC

<input type="text"/>	▲
vpc-34da2a5f 172.31.0.0/16	(default)
vpc-04548667fe836870b (assign3) 10.0.0.0/16	

Subnet settings
 Specify the CIDR blocks and Availability Zone for the subnet.

Subnet 1 of 1

Subnet name
 Create a tag with a key of 'Name' and a value that you specify.
 mypublic03
 The name can be up to 256 characters long.

Availability Zone [Info](#)
 Choose the zone in which your subnet will reside, or let Amazon choose one for you.
 Asia Pacific (Mumbai) / ap-south-1a

IPv4 CIDR block [Info](#)
 Q. 10.0.1.0/24

Tags - optional

Key	Value - optional
<input type="text"/> Name	<input type="text"/> mypublic03

[Remove](#)

[Add new tag](#)

6. Then click on create subnet.

Subnets (2/5) Info								
	Name	Subnet ID	State	VPC	IPv4 CIDR	IPv6 CIDR	Available IPv4 addresses	Availability Zone
<input checked="" type="checkbox"/>	mypublic03	subnet-0abd45e30f2a284d9	Available	vpc-04548667fe836870b ass...	10.0.1.0/24	-	251	ap-south-1a
<input type="checkbox"/>	-	subnet-ea49d891	Available	vpc-34da2a5f	172.31.16.0/20	-	4091	ap-south-1c
<input type="checkbox"/>	-	subnet-ae7e67c6	Available	vpc-34da2a5f	172.31.32.0/20	-	4091	ap-south-1a
<input type="checkbox"/>	-	subnet-fcc48bb0	Available	vpc-34da2a5f	172.31.0.0/20	-	4090	ap-south-1b
<input checked="" type="checkbox"/>	myassign03	subnet-0bd5e5838c20c6d3b	Available	vpc-04548667fe836870b ass...	10.0.0.0/24	-	251	ap-south-1a

Configuration of Internet Gateway

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

Create internet gateway [Info](#)

An internet gateway is a virtual router that connects a VPC to the internet. To create a new internet gateway specify the name for the gateway below.

Internet gateway settings

Name tag
Creates a tag with a key of 'Name' and a value that you specify.

Tags - optional
A tag is a label that you assign to an AWS resource. Each tag consists of a key and an optional value. You can use tags to search and filter your resources or track your AWS costs.

Key	Value - optional
<input type="text" value="Name"/>	<input type="text" value="mygateway"/> Remove

[Add new tag](#)
You can add 49 more tags.

[Cancel](#) [Create internet gateway](#)

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

The following internet gateway was created: igw-04572458fc98cd499. You can now attach to a VPC to enable the VPC to communicate with the internet.

[Attach to a VPC](#)

VPC > Internet gateways > igw-04572458fc98cd499

igw-04572458fc98cd499 / mygateway

[Actions ▾](#)

Details	Info
Internet gateway ID igw-04572458fc98cd499	State Detached
VPC ID	Owner

VPC > Internet gateways > Attach to VPC (igw-04572458fc98cd499)

Attach to VPC (igw-04572458fc98cd499) Info

VPC
Attach an internet gateway to a VPC to enable the VPC to communicate with the internet. Specify the VPC to attach below.

Available VPCs
Attach the internet gateway to this VPC.
 X

▶ AWS Command Line Interface command

Cancel Attach internet gateway

Configuration of Route Table

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

Create route table		Actions	
<input type="text"/>		Filter by tags and attributes or search by keyword	
Name	Route Table ID	Explicit subnet association	Edge associations
<input type="checkbox"/>	rtb-0b17a2270b414915b	-	-
<input type="checkbox"/>	rtb-585fe933	-	-

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

Route Tables > Create route table

Create route table

A route table specifies how packets are forwarded between the subnets within your VPC, the internet, and your VPN connection.

Name tag	<input type="text" value="MyRoute"/>	i
VPC*	<input type="text" value="vpc-04548667fe836870b"/>	C i
Key	(128 characters maximum)	Value (256 characters maximum)
This resource currently has no tags		
Add Tag	50 remaining (Up to 50 tags maximum)	
* Required		Cancel Create

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

Name	Route Table ID	Explicit subnet association	Edge associations	Main	VPC ID	Owner
MyRoute	rtb-0523484e572199b69	-	-	No	vpc-04548667fe836870b ...	792522942915
	rtb-0b17a2270b414915b	-	-	Yes	vpc-04548667fe836870b ...	792522942915
	rtb-585fe933	-	-	Yes	vpc-34da2a5f	792522942915

Subnet ID	IPv4 CIDR	IPv6 CIDR	Current Route Table
subnet-0abd43e30f2a284d9	10.0.1.0/24	-	Main
subnet-0bd5e5838c20c6d3b	10.0.0.0/24	-	Main

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

Name	Route Table ID	Explicit subnet association	Edge associations	Main	VPC ID	Owner
MyRoute	rtb-0523484e572199b69	subnet-0abd43e30f2a284d9	-	No	vpc-04548667fe836870b ...	792522942915
	rtb-0b17a2270b414915b	-	-	Yes	vpc-04548667fe836870b ...	792522942915
	rtb-585fe933	-	-	Yes	vpc-34da2a5f	792522942915

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

igw-04572458fc98cd499 mygateway

* 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	<input type="checkbox"/> Request Spot Instances	
Network	vpc-34da2a5f (default)	<input type="button"/> Create new VPC
Subnet	vpc-04548667fe836870b assign3	<input type="button"/> Create new subnet
Auto-assign Public IP	Use subnet setting (Enable)	
Placement group	<input type="checkbox"/> Add instance to placement group	
Capacity Reservation	Open	
Domain join directory	No directory	<input type="button"/> Create new directory
IAM role	None	<input type="button"/> Create new IAM role
CPU options	<input type="checkbox"/> Specify CPU options	
Shutdown behavior	Stop	
Stop - Hibernate behavior	<input type="checkbox"/> Enable hibernation as an additional stop behavior	
Enable termination protection	<input type="checkbox"/> 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	<input type="checkbox"/> Request Spot Instances	
Network	vpc-04548667fe836870b assign3	<input type="button"/> Create new VPC
Subnet	subnet-0abd43e30f2a284d9 mypublic03 ap-south-1a	<input type="button"/> Create new subnet
Auto-assign Public IP	subnet-0abd43e30f2a284d9 mypublic03 ap-south-1a use subnet setting (Disable)	
Placement group	<input type="checkbox"/> Add instance to placement group	
Capacity Reservation	Open	
Domain join directory	No directory	<input type="button"/> Create new directory
IAM role	None	<input type="button"/> Create new IAM role
CPU options	<input type="checkbox"/> Specify CPU options	
Shutdown behavior	Stop	
Stop - Hibernate behavior	<input type="checkbox"/> Enable hibernation as an additional stop behavior	

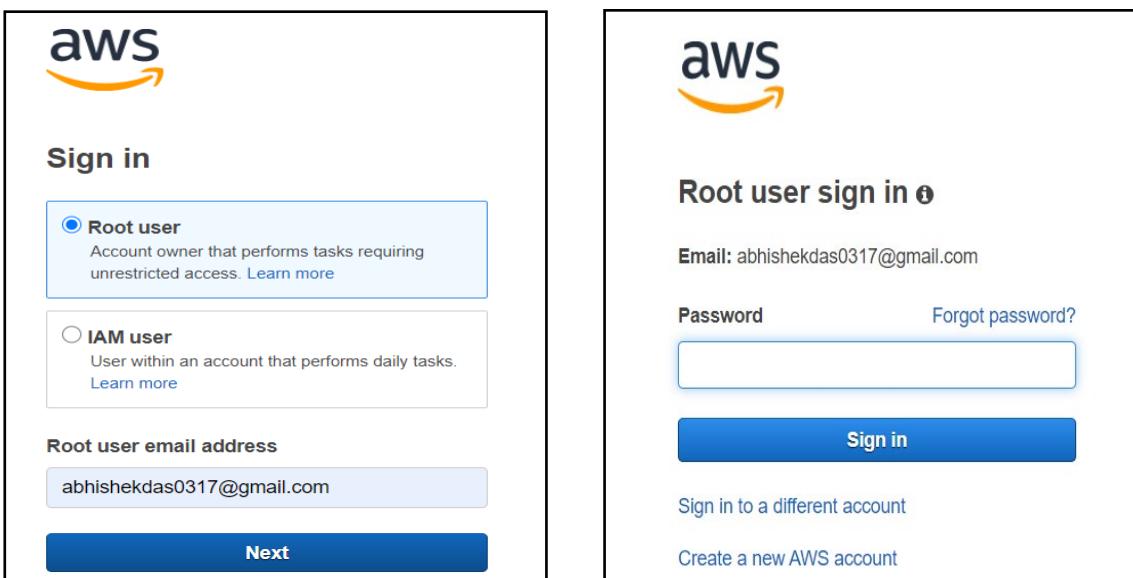
Cancel Previous Review and Launch Next: Add Storage

04: EBS

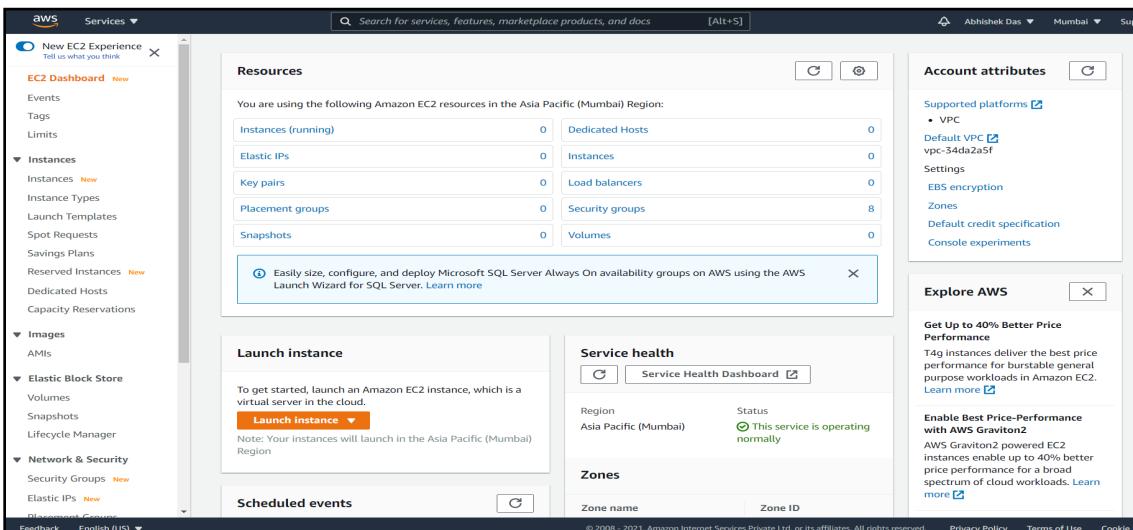
About EBS (Elastic Block Store): Amazon Elastic Block Store (EBS) is an easy to use, high-performance, block-storage service designed for use with Amazon Elastic Compute Cloud (EC2) for both throughput and transaction intensive workloads at any scale.

Process to Configure EBS:

1. Sign in to the AWS Management Console.



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



The screenshot shows the AWS EC2 service dashboard under the 'New EC2 Experience' tab. The left sidebar includes links for EC2 Dashboard, Events, Tags, Limits, Instances (with sub-links for Instances, Instance Types, Launch Templates, Spot Requests, Savings Plans, Reserved Instances), Images (AMIs), and Elastic Block Store (Volumes, Snapshots, Lifecycle Manager). The main content area is titled 'Create Volume' and displays a message: 'You do not have any EBS volumes in this region. Click the Create Volume button to create your first volume.' A large blue 'Create Volume' button is centered at the bottom of this section. The footer contains standard AWS navigation links: Feedback, English (US), Privacy Policy, Terms of Use, and Cookie preferences.

3. Provide its size and click on Create Volume.

This screenshot shows the 'Create Volume' configuration page. The form fields include:

- Volume Type: General Purpose SSD (gp2)
- Size (GiB): 1 (Min: 1 GiB, Max: 16384 GiB)
- IOPS: 100 / 3000 (Baseline of 3 IOPS per GiB with a minimum of 100 IOPS, burstable to 3000 IOPS)
- Throughput (MB/s): Not applicable
- Availability Zone*: ap-south-1a
- Snapshot ID: Select a snapshot
- Encryption: Encrypt this volume
- Tags: Key (128 characters maximum) and Value (256 characters maximum) fields, with a note: 'This resource currently has no tags. Choose the Add tag button or click to add a Name tag.'
- Add Tag button: 50 remaining (Up to 50 tags maximum)

The footer includes: Feedback, English (US), Privacy Policy, Terms of Use, and Cookie preferences.

This screenshot shows the confirmation page after a volume has been created successfully. The message 'Volume created successfully' is displayed in a green box along with the Volume ID: vol-0d0479ef9045d5aaf. A 'Close' button is located at the bottom right of the message box. The footer includes: Feedback, English (US), Privacy Policy, Terms of Use, and Cookie preferences.

4. After volume creation, create a EC2 instance.

5. Select its Machine image as a “Free tier only”.

Step 1: Choose an Amazon Machine Image (AMI)
An AMI is a template that contains the software configuration (operating system, application server, and applications) required to launch your instance. You can select an AMI provided by AWS, our user community, or the AWS Marketplace; or you can select one of your own AMIs.

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

Quick Start

My AMIs

AWS Marketplace

Community AMIs

Free tier only ⓘ

Amazon Linux 2 AMI (HVM), SSD Volume Type - ami-0bcf5425cdc1d8a85 (64-bit x86) / ami-003025fed2eb22f59 (64-bit Arm)

Amazon Linux comes with five years support. It provides Linux kernel 4.14 tuned for optimal performance on Amazon EC2, systemd 219, GCC 7.3, Glibc 2.26, Binutils 2.29.1, and the latest software packages through extras. This AMI is the successor of the Amazon Linux AMI that is approaching end of life on December 31, 2020 and has been removed from this wizard.

Root device type: ebs Virtualization type: hvm ENA Enabled: Yes

Select 64-bit (x86) 64-bit (Arm)

Red Hat Enterprise Linux 8 (HVM), SSD Volume Type - ami-0a9d27a9f4f5c0efc (64-bit x86) / ami-0816d75a127c17a49 (64-bit Arm)

Red Hat Enterprise Linux version 8 (HVM), EBS General Purpose (SSD) Volume Type

Root device type: ebs Virtualization type: hvm ENA Enabled: Yes

Select 64-bit (x86) 64-bit (Arm)

SUSE Linux Enterprise Server 15 SP2 (HVM), SSD Volume Type - ami-0b3acf3edf2397475 (64-bit x86) / ami-0ab71076ab9b53b0d (64-bit Arm)

SUSE Linux Enterprise Server 15 Service Pack 2 (HVM), EBS General Purpose (SSD) Volume Type. Amazon EC2 AMI Tools preinstalled, Apache 2.2, MySQL 5.5, PHP 5.3, and Ruby 1.8.7 available.

Root device type: ebs Virtualization type: hvm ENA Enabled: Yes

Select 64-bit (x86) 64-bit (Arm)

Ubuntu Server 20.04 LTS (HVM), SSD Volume Type - ami-0d758c1134823146a (64-bit x86) / ami-0a6638920f7143fb2 (64-bit Arm)

Ubuntu Server 20.04 LTS (HVM), EBS General Purpose (SSD) Volume Type. Support available from Canonical (<http://www.ubuntu.com/cloud/services>).

Root device type: ebs Virtualization type: hvm ENA Enabled: Yes

Select 64-bit (x86) 64-bit (Arm)

Feedback English (US) ▾

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

6. Select its Instance Type.

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. Learn more about instance types and how they can meet your computing needs.

Filter by: All instance families Current generation ShowHide Columns

Currently selected: t2.micro (~ ECUs, 1 vCPUs, 2.5 GHz, ~ 1 GiB memory, EBS only)

Family	Type	vCPUs	Memory (GiB)	Instance Storage (GB)	EBS-Optimized Available	Network Performance	IPv6 Support
t2	t2.nano	1	0.5	EBS only	-	Low to Moderate	Yes
<input checked="" type="checkbox"/>	t2.micro <small>Free tier eligible</small>	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

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

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: subnet-ae7e67c6 | Default in ap-south-1a Create new subnet
4091 IP Addresses available

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 Enable hibernation as an additional stop behavior

Stop - Hibernate behavior: Protect against accidental termination

Enable termination protection: Enable CloudWatch detailed monitoring Additional charges apply.

Monitoring: Review and Launch Next: Add Storage

Feedback English (US) ▾

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

8. Now Add Storage.

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. [Learn more about storage options in Amazon EC2.](#)

Volume Type	Device	Snapshot	Size (GiB)	Volume Type	IOPS	Throughput (MB/s)	Delete on Termination	Encryption
Root	/dev/xvda	snap-0b55bb79acf67ade6	8	General Purpose SSD (gp2)	100 / 3000	N/A	<input checked="" type="checkbox"/>	Not Encrypted

Add New Volume

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.

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](#).

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.

Cancel Launch Instances

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

Create Volume Actions ▾

Modify Volume Create Snapshot Create Lifecycle Policy Delete Volume Attach Volume Detach Volume Force Detach Volume Change Auto-Enable IO Setting Add/Edit Tags

Volume Type	IOPS	Throughput	Snapshot	Created	Availability Zone	State	Alarm Status
gp2	100	-	snap-0b55bb79acf67ade6	April 3, 2021 at 7:42...	ap-south-1a	in-use	None
gp2	100	-		April 3, 2021 at 7:40...	ap-south-1a	available	None

Volumes: vol-0d0479ef9045d5aaf

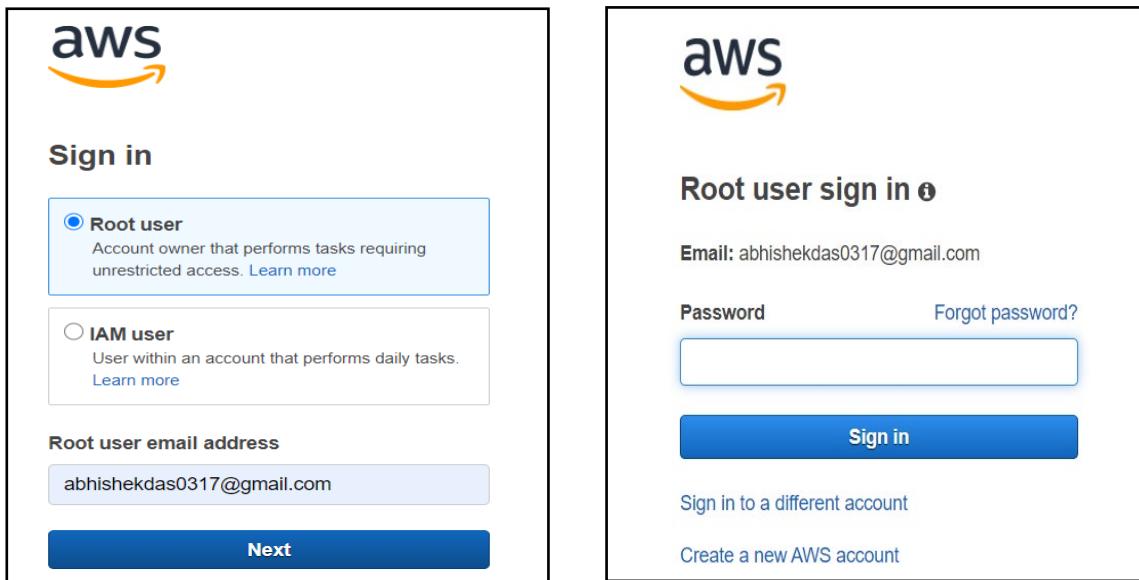
Description	Status Checks	Monitoring	Tags
Volume ID: vol-0d0479ef9045d5aaf Alarm status: None Snapshot: - Availability Zone: ap-south-1a Encryption: Not Encrypted KMS Key ID:	Outposts ARN: - Size: 1 GiB Created: April 3, 2021 at 7:40:44 AM UTC+5:30 State: available	Attachment information: Volume type: gp2	

05: LOAD BALANCER

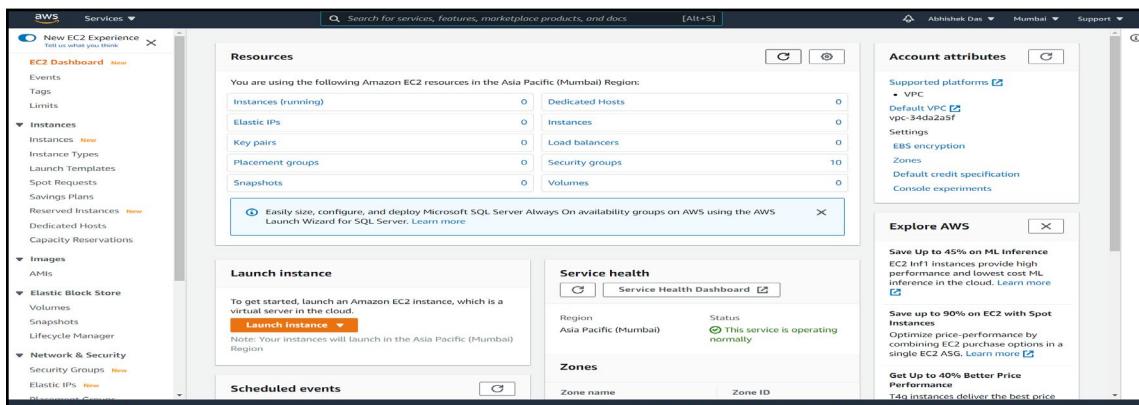
About Load Balancer: Load Balancer provides basic load balancing across multiple Amazon EC2 instances and operates at both the request level and the connection level. Classic Load Balancer is intended for applications that were built within the EC2-Classic network.

Process to Configure Load Balancer:

1. Sign in to the AWS Management Console.



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



3. Select Machine Image to Free tier only.

Step 1: Choose an Amazon Machine Image (AMI)
An AMI is a template that contains the software configuration (operating system, application server, and applications) required to launch your instance. You can select an AMI provided by AWS, our user community, or the AWS Marketplace, or you can select one of your own AMIs.

AMI Name	Description	Root device type	Virtualization type	ENAs Enabled	Select
Amazon Linux 2 AMI (HVM), SSD Volume Type - ami-0bcf5425cdc1d8a85	Amazon Linux 2 comes with five years support. It provides Linux kernel 4.14 tuned for optimal performance on Amazon EC2, systemd 219, GCC 7.3, Glibc 2.26, Binutils 2.29.1, and the latest software packages through extras. This AMI is the successor of the Amazon Linux AMI that is approaching end of life on December 31, 2020 and has been removed from this wizard.	ebs	hvm	Yes	<input checked="" type="radio"/> 64-bit (x86) <input type="radio"/> 64-bit (Arm)
Red Hat Enterprise Linux 8 (HVM), SSD Volume Type - ami-0a9d27a9f4fc0efc	Red Hat Enterprise Linux version 8 (HVM). EBS General Purpose (SSD) Volume Type	ebs	hvm	Yes	<input checked="" type="radio"/> 64-bit (x86) <input type="radio"/> 64-bit (Arm)
SUSE Linux Enterprise Server 15 SP2 (HVM), SSD Volume Type - ami-0b3acf3edf2397475	SUSE Linux Enterprise Server 15 Service Pack 2 (HVM). EBS General Purpose (SSD) Volume Type. Amazon EC2 AMI Tools preinstalled; Apache 2.2, MySQL 5.5, PHP 5.3, and Ruby 1.8.7 available.	ebs	hvm	Yes	<input checked="" type="radio"/> 64-bit (x86) <input type="radio"/> 64-bit (Arm)
Ubuntu Server 20.04 LTS (HVM), SSD Volume Type - ami-0d758c1134823146a	Ubuntu Server 20.04 LTS (HVM). EBS General Purpose (SSD) Volume Type. Support available from Canonical (http://www.ubuntu.com/cloud/services).	ebs	hvm	Yes	<input checked="" type="radio"/> 64-bit (x86) <input type="radio"/> 64-bit (Arm)

4. Then Select Instance Type.

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. Learn more about instance types and how they can meet your computing needs.

Family	Type	vCPUs	Memory (GiB)	Instance Storage (GB)	EBS-Optimized Available	Network Performance	IPv6 Support
I2	I2.nano	1	0.5	EBS only	-	Low to Moderate	Yes
I2	I2.micro	1	1	EBS only	-	Low to Moderate	Yes
I2	I2.small	1	2	EBS only	-	Low to Moderate	Yes
I2	I2.medium	2	4	EBS only	-	Low to Moderate	Yes
I2	I2.large	2	8	EBS only	-	Low to Moderate	Yes
I2	I2.xlarge	4	16	EBS only	-	Moderate	Yes
I2	I2.2xlarge	8	32	EBS only	-	Moderate	Yes
T3	T3.nano	2	0.5	EBS only	Yes	Up to 5 Gigabit	Yes
T3	T3.micro	2	1	EBS only	Yes	Up to 5 Gigabit	Yes
T3	T3.small	2	2	EBS only	Yes	Up to 5 Gigabit	Yes
T3	T3.medium	2	4	EBS only	Yes	Up to 5 Gigabit	Yes

5. In Instance detail select Subnet of one zone.

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	<input type="checkbox"/> Request Spot Instances	
Network	vpc-34da2a5f (default)	<input checked="" type="checkbox"/> Create new VPC
Subnet	subnet-ae7e6766 Default in ap-south-1a 4091 IP Addresses available	<input checked="" type="checkbox"/> Create new subnet
Auto-assign Public IP	Use subnet setting (Enable)	
Placement group	<input type="checkbox"/> Add instance to placement group	
Capacity Reservation	Open	
Domain join directory	No directory	<input checked="" type="checkbox"/> Create new directory
IAM role	None	<input checked="" type="checkbox"/> Create new IAM role
CPU options	<input type="checkbox"/> Specify CPU options	
Shutdown behavior	Stop	
Stop - Hibernate behavior	<input type="checkbox"/> Enable hibernation as an additional stop behavior	
Enable termination protection	<input type="checkbox"/> Protect against accidental termination	
Monitoring	<input type="checkbox"/> Enable CloudWatch detailed monitoring Additional charges apply.	

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

A screenshot of the AWS EC2 Step 6: Configure Security Group page. The page title is "Step 6: Configure Security Group". It displays a table of security group rules. The first rule is for SSH (Protocol TCP, Port Range 22, Source 0.0.0.0/0, Description e.g. SSH for Admin Desktop). The second rule is for HTTP (Protocol TCP, Port Range 80, Source 0.0.0.0/0, Description e.g. SSH for Admin Desktop). The third rule is for HTTPS (Protocol TCP, Port Range 443, Source 0.0.0.0/0, Description e.g. SSH for Admin Desktop). Below the table, there is a warning message: "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." At the bottom right, there are "Cancel", "Previous", and "Review and Launch" buttons.

7. Then continue without security pair key.

A screenshot of the AWS EC2 Step 7: Review Instance Launch page. The page title is "Step 7: Review Instance Launch". It shows the instance configuration details: AMI (Amazon Linux 2 AMI (HVM, SSD Volume Type)), Instance Type (t2.micro), and Security Groups (launch-wizard-8). A modal dialog titled "Select an existing key pair or create a new key pair" is open. It contains instructions: "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." It also includes a note: "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." Below the note is a dropdown menu with options: "Proceed without a key pair" (selected) and "I acknowledge that I will not be able to connect to this instance unless I already know the password built into this AMI.". At the bottom right of the modal are "Cancel" and "Launch instances" buttons. The main page has "Cancel", "Previous", and "Launch" buttons at the bottom right.

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

A screenshot of the AWS EC2 Instances page. The page title is "Instances (2) Info". It shows a table of two running instances. The first instance has an Instance ID of i-06f06aaaeef9b7ab68, is in the "Running" state, is a t2.micro type, and is in the "ap-south-1a" availability zone with a Public IPv4 DNS of ec2-35-154-4-53.a. The second instance has an Instance ID of i-0ed130c9581133020, is in the "Running" state, is a t2.micro type, and is in the "ap-south-1b" availability zone with a Public IPv4 DNS of ec2-13-232-232-82. The left sidebar shows navigation options like New EC2 Experience, EC2 Dashboard, Events, Tags, Limits, Instances, Instances Types, Launch Templates, and Spot Requests.

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 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-aef67c6, 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-06f06aaae9b7ab68:80

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](#)

Buttons: Close

Create Load Balancer

Actions

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

Basic Configuration

- Name:** My.load
- ARN:** arn:aws:elasticloadbalancing:ap-south-1:79252942915: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-aef67c6 - ap-south-1a (IPv4 address: Assigned by AWS)
 - subnet-fcc48bb0 - ap-south-1b (IPv4 address: Assigned by AWS)
- Hosted zone:** ZP97RAFLXTNZK

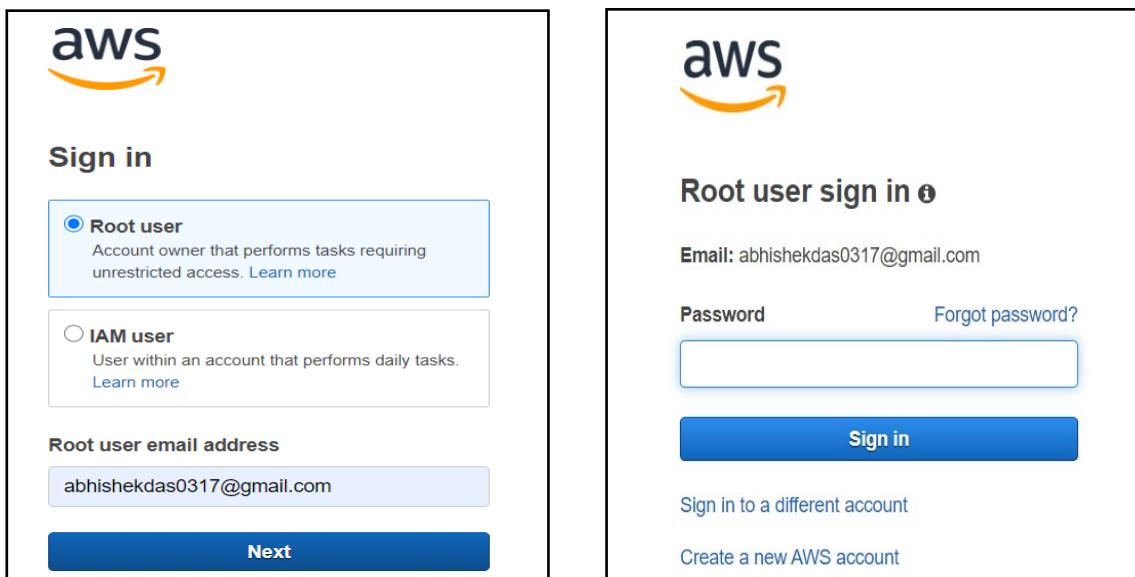
Buttons: Edit IP address type | Edit subnets

06: AWS LAMBDA

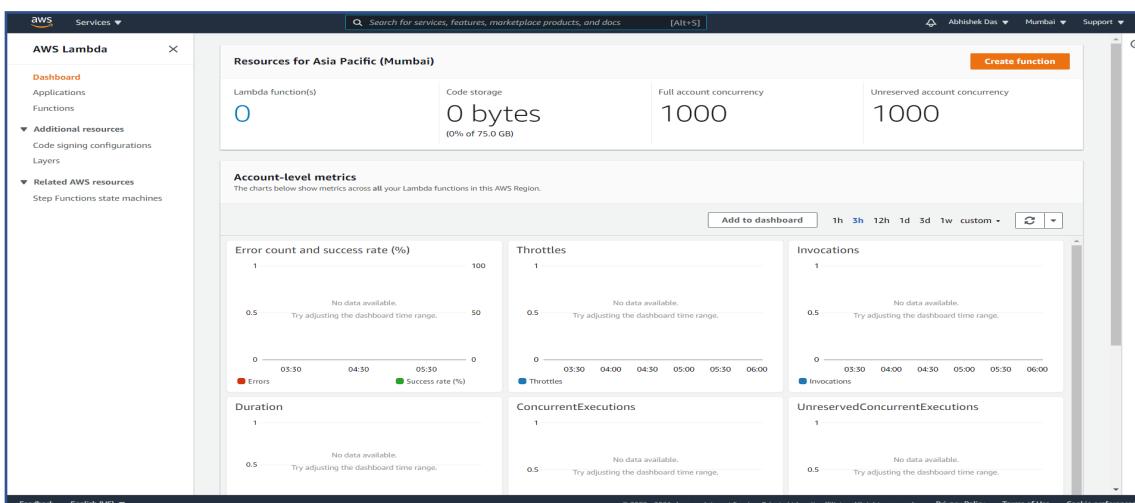
About AWS Lambda: AWS Lambda is a serverless compute service that lets you run code without provisioning or managing servers, creating workload-aware cluster scaling logic, maintaining event integrations, or managing runtimes.

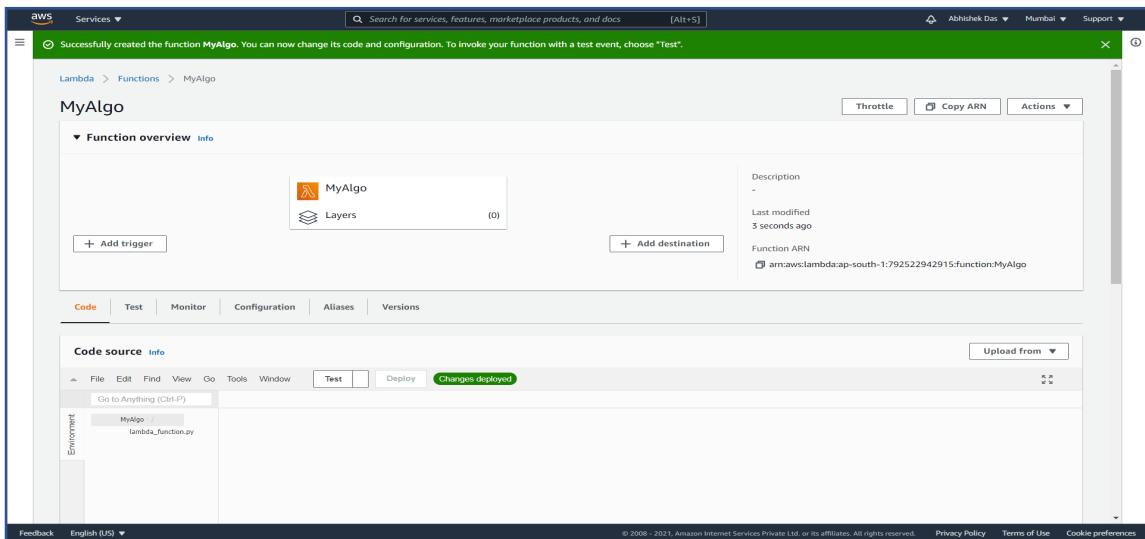
Process to Configure AWS Lambda:

1. Sign in to the AWS Management Console.

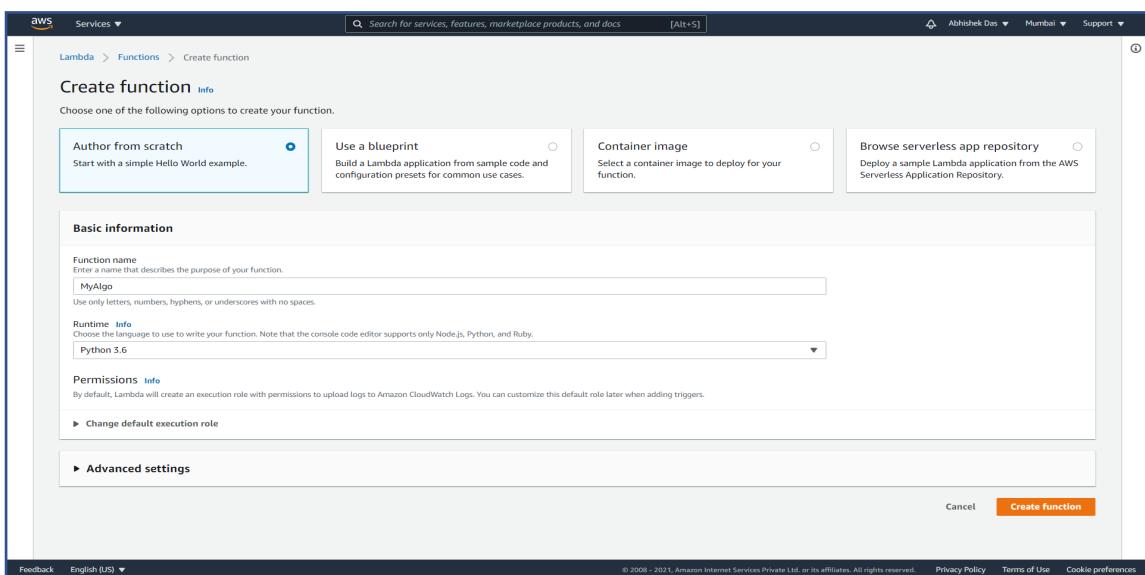


2. Open Lambda from service.

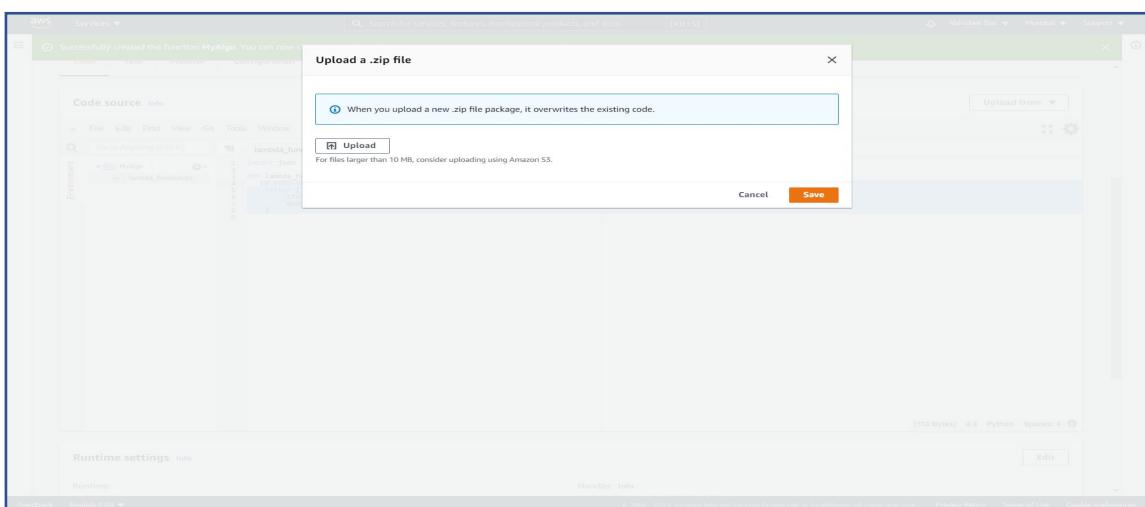




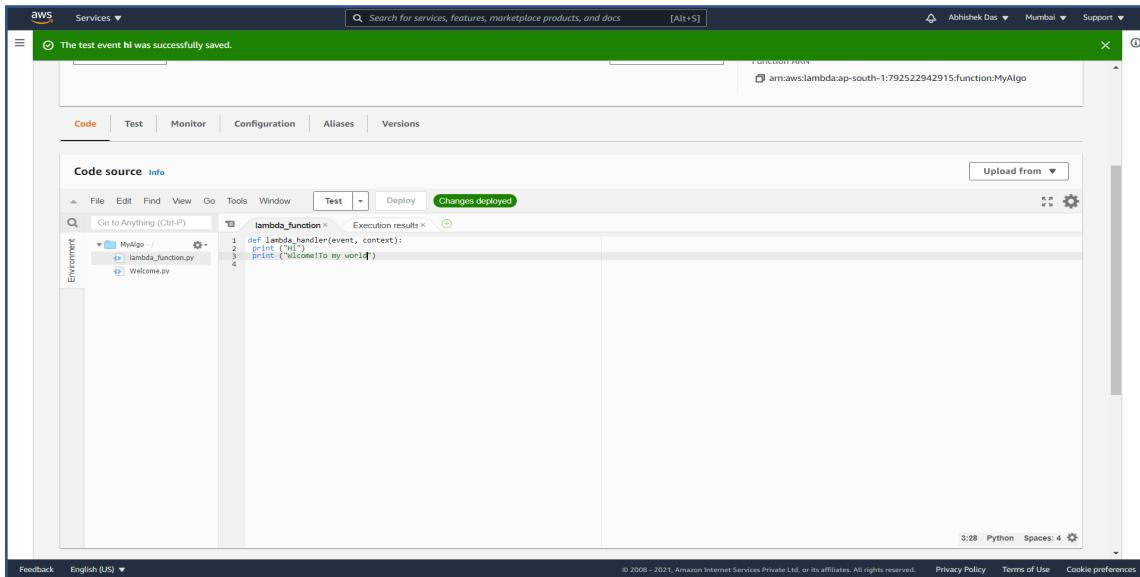
3. Click on Create function and provide function name, runtime.



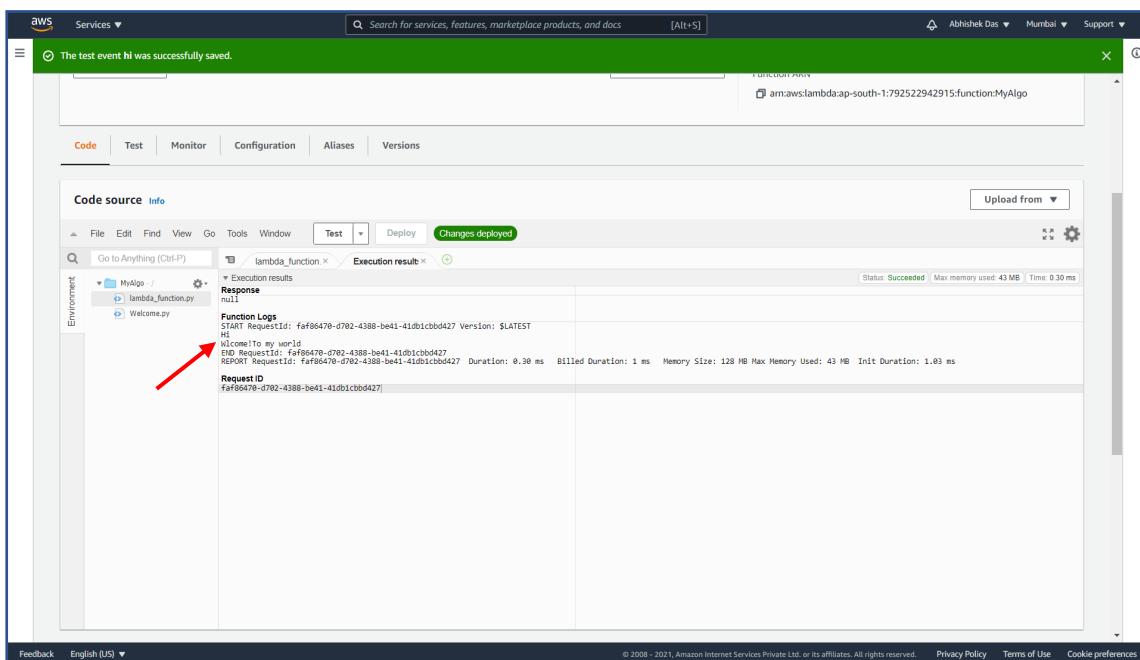
4. Now we execute our code and even upload our code file from S3 bucket also.



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



```
def lambda_handler(event, context):
    print("Hi")
    print("Welcome! To my world!")
```



The test event hi was successfully saved.

Execution result: Succeeded | Max memory used: 43 MB | Time: 0.30 ms

Response

```
nu11
```

Function Logs

```
REPORT RequestId: faf86470-d702-4388-be41-41db1cbbd427 Duration: 0.30 ms Billed Duration: 1 ms Memory Size: 128 MB Max Memory Used: 43 MB Init Duration: 1.03 ms
REPORT RequestId: faf86470-d702-4388-be41-41db1cbbd427
```

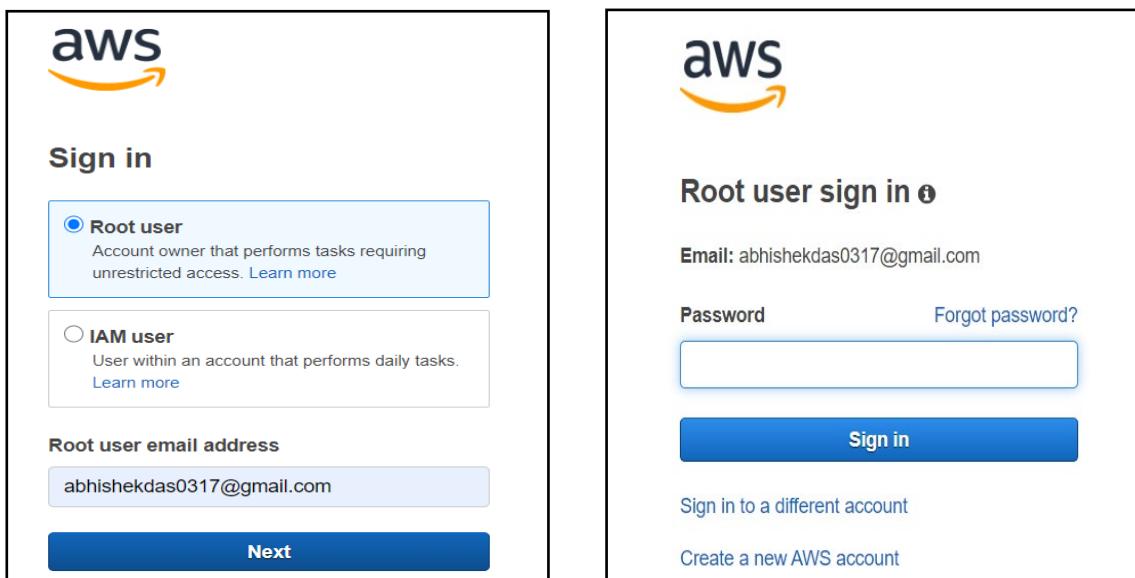
Request ID: faf86470-d702-4388-be41-41db1cbbd427

07: Auto Scaling

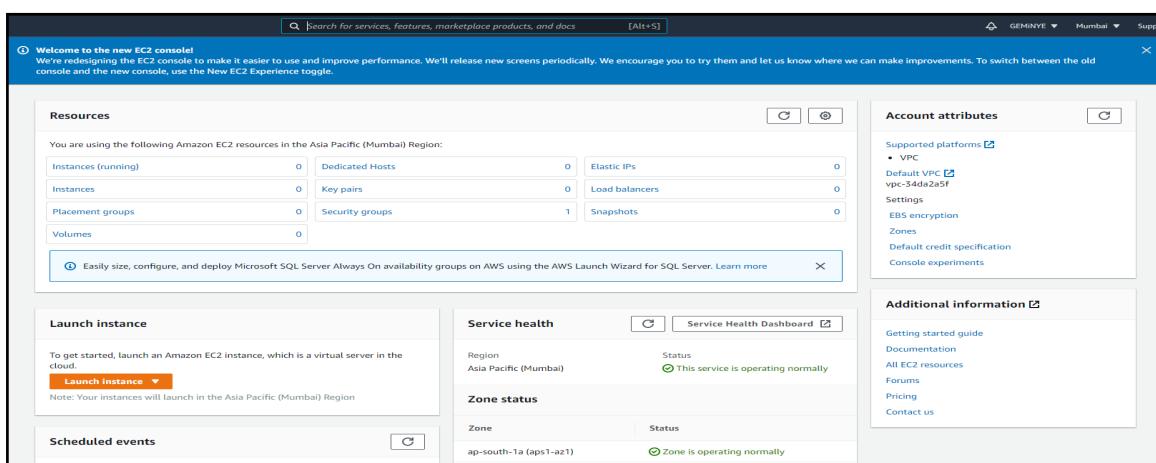
About Auto Scaling: AWS Auto Scaling monitors your applications and automatically adjusts capacity to maintain steady, predictable performance at the lowest possible cost. Using AWS Auto Scaling, it's easy to setup application scaling for multiple resources across multiple services in minutes.

Process to Configure Auto Scaling:

1. Sign in to the AWS Management Console.



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



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.

Step 5: Add Tags

A tag consists of a case-sensitive key-value pair. For example, you could define a tag with key = Name and value = Webserver.

A copy of a tag can be applied to volumes, instances or both.

Tags will be applied to all instances and volumes. Learn more about tagging your Amazon EC2 resources.

Add Tag (Up to 50 tags maximum)

Key (128 characters maximum) **Value** (256 characters maximum)

Instances Volumes Network Interfaces

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.

Cancel **Previous** **Review and Launch** **Next: Configure Security Group**

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.

AMI Details

Amazon Linux 2 AMI (HVM), SSD Volume Type - ami-08e0ca9924195beba

Free tier eligible Amazon Linux 2 comes with five years support. It provides Linux kernel 4.14 tuned for optimal performance on Amazon EC2, systemd 219, GCC 7.3, Glibc 2.26, Binutils 2.29.1, and the latest software packages through extras. This AMI is the successor of the Amazon Linux AMI that is a...

Instance Type

Instance Type	ECUs	vCPUs	Memory (GiB)	Instance Storage (GB)	EBS-Optimized Available	Network Performance
I2 micro	-	1	1	EBS only	-	Low to Moderate

Security Groups

Security group name launch-wizard-1
Description launch-wizard-1 created 2021-01-29T15:27:47.940+05:30

Type	Protocol	Port Range	Source	Description
SSH	TCP	22	0.0.0.0/0	

Instance Details

Launch

Cancel **Previous** **Launch**

7. Continue without a key pair.

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.

AMI Details

Amazon Linux 2 AMI (HVM), SSD Volume Type - ami-08e0ca9924195beba

Free tier eligible Amazon Linux 2 comes with five years support. It provides Linux kernel 4.14 tuned for optimal performance on Amazon EC2, systemd 219, GCC 7.3, Glibc 2.26, Binutils 2.29.1, and the latest software packages through extras. This AMI is the successor of the Amazon Linux AMI that is a...

Instance Type

Instance Type	ECUs	vCPUs	Memory (GiB)	Instan...
I2 micro	-	1	1	EBS o...

Security Groups

Security group name launch-wizard-1
Description launch-wizard-1 created 2021-01-29T15:27:47.940+05:30

Type	Protocol	Port Range	Source	Description
SSH	TCP	22	0.0.0.0/0	

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.

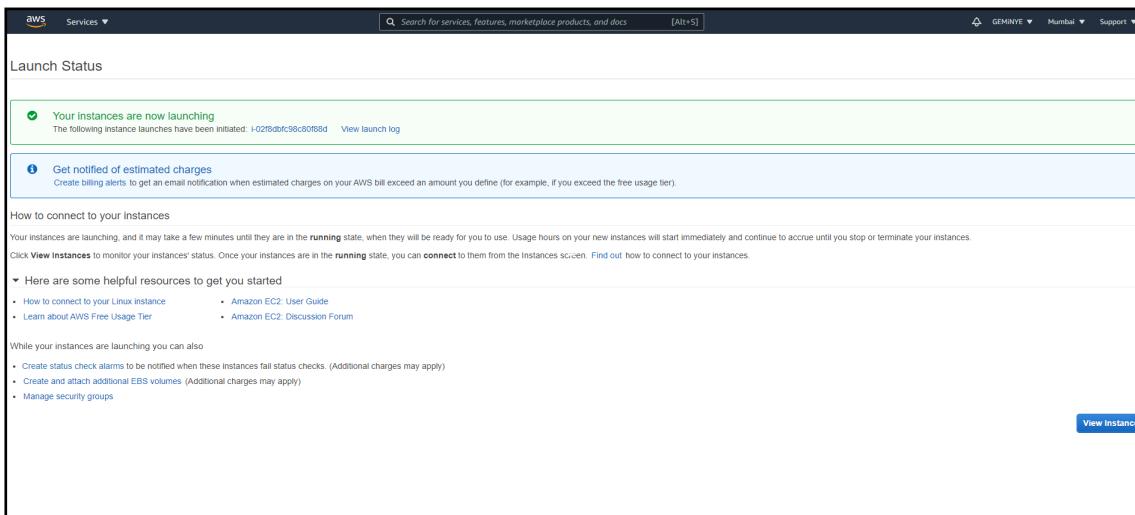
I acknowledge that I will not be able to connect to this instance unless I already know the password built into this AMI.

Cancel **Launch Instances**

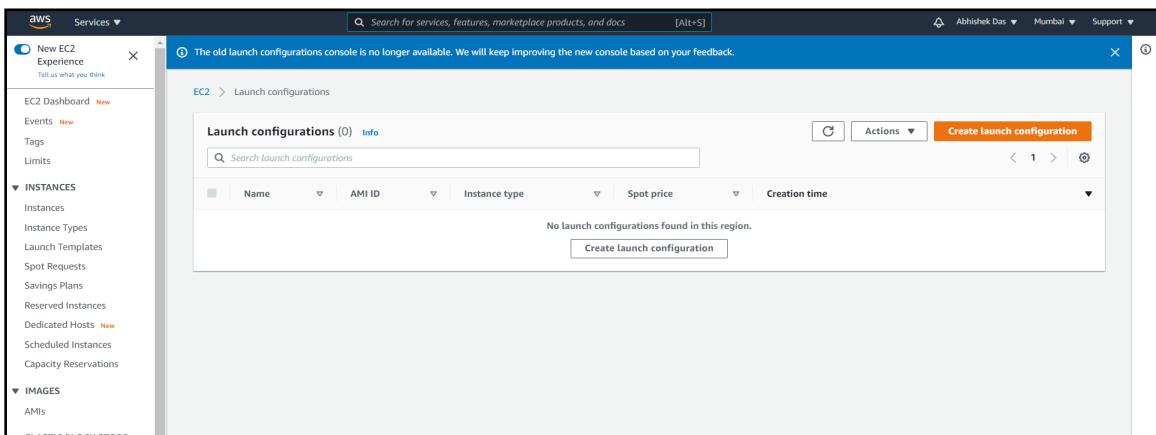
Edit instance type **Edit security groups** **Edit instance details**

Cancel **Previous** **Launch**

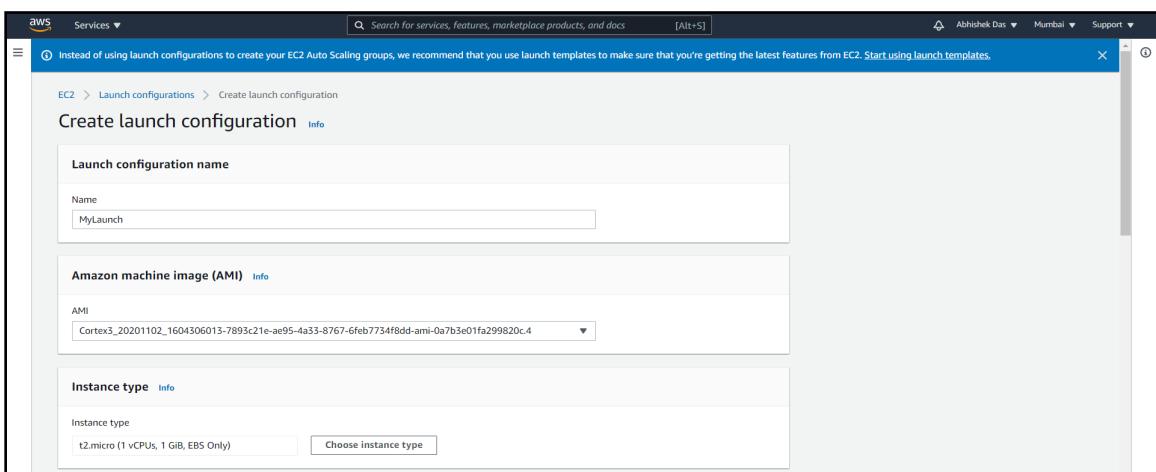
8. Click on launch Instance.



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).

The screenshot shows the 'Storage (volumes)' section of the AWS Auto Scaling configuration. It lists three volumes: 'Root' (8 GB, General purpose SSD), and two EBS volumes (30 GB and 20 GB, both General purpose SSD). A note indicates that free-tier eligible customers can get up to 30 GB of EBS storage.

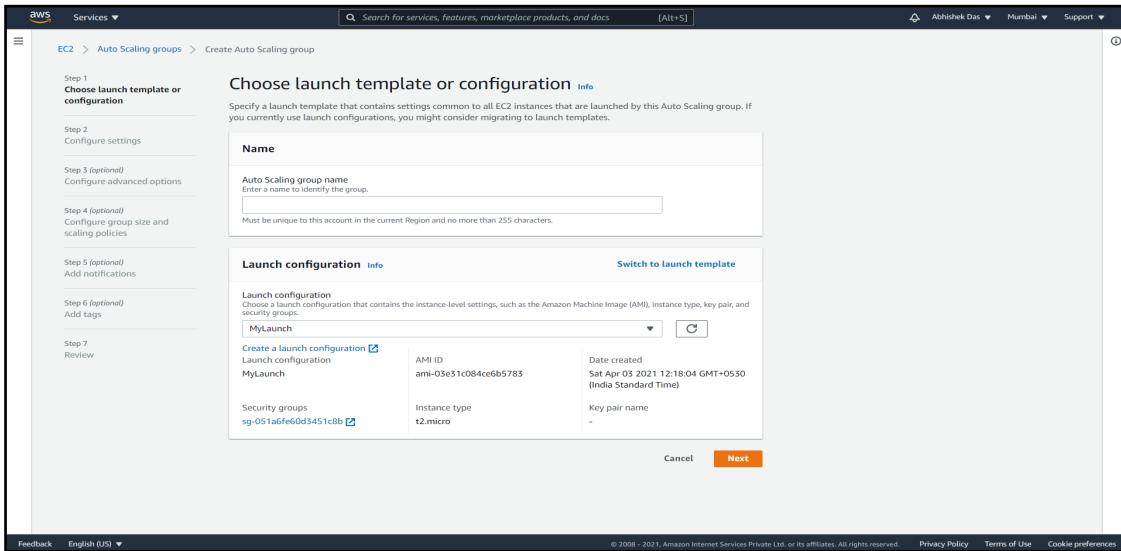
12. Now select Security Groups and click on Create Launch Configuration.

The screenshot shows the 'Security groups' section. A new security group named 'AutoScaling-Security-Group-1' is being created. It includes a rule allowing SSH traffic (TCP port 22) from anywhere. A warning message notes that rules of 0.0.0.0/0 allow all IP addresses to access the instance.

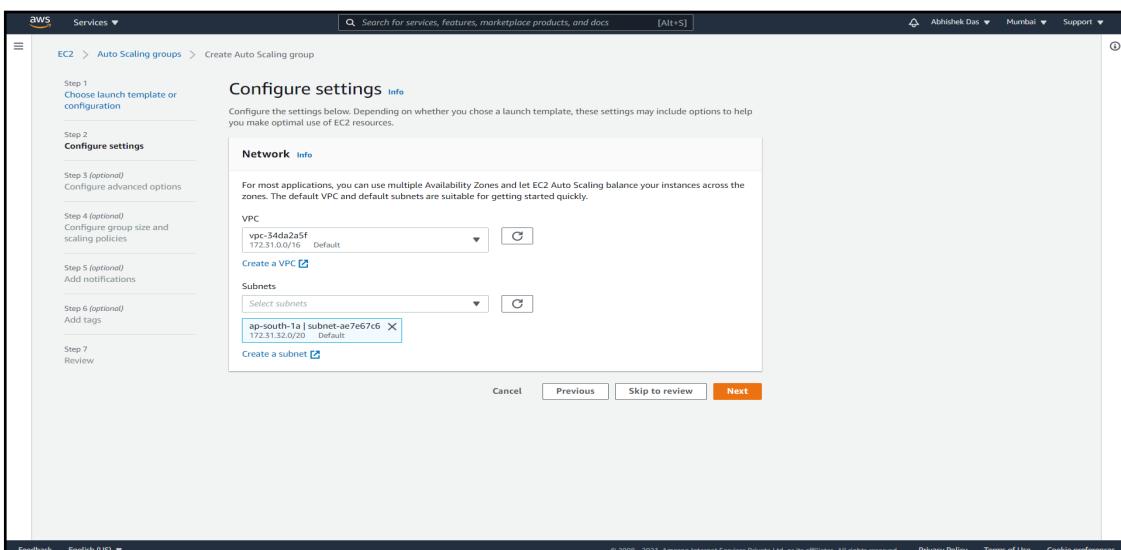
13. Then select that configuration and click on Action and select create auto scaling group.

The screenshot shows the 'Launch configurations' section. A new launch configuration named 'MyLaunch' has been successfully created. The configuration details include an AMI ID (ami-03e31c084ce...), Instance type (t2.micro), and a creation time of Sat Apr 03 2021 12:18:04 GMT+0530 (India Standard Time). The 'Actions' menu is open, showing options like 'Create Auto Scaling group', 'Copy to launch template', and 'Delete launch configuration'.

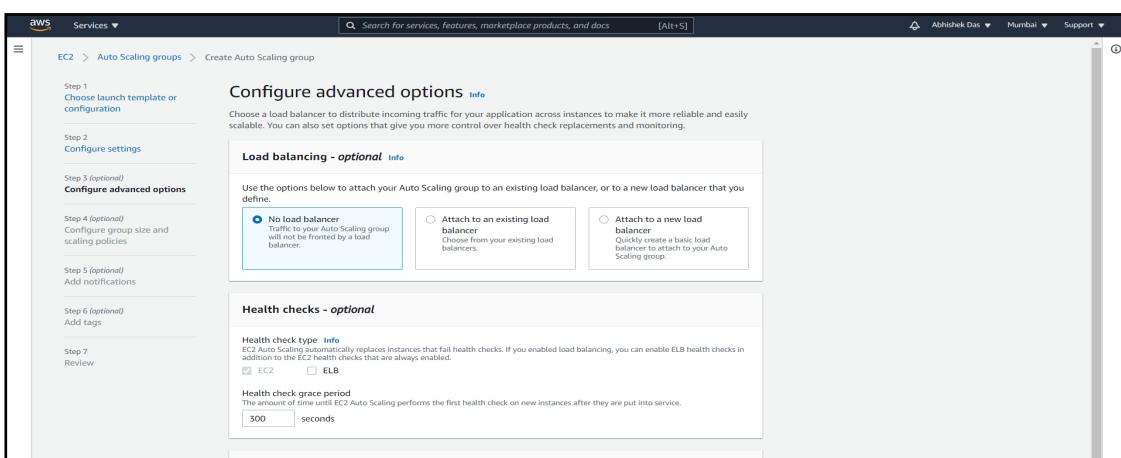
14. Provide Security group name and click next.



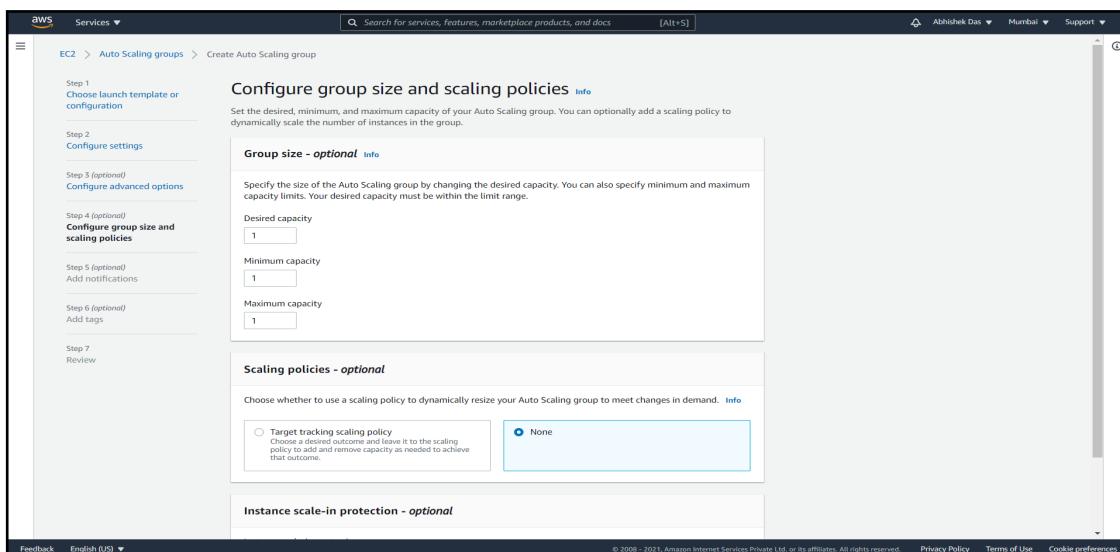
15. Select VPC and Subnet and click next.



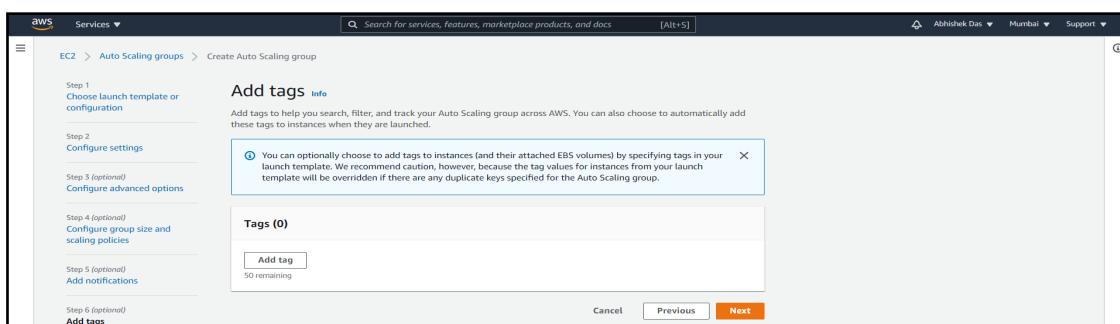
16. Then select Load Balancing and click next.



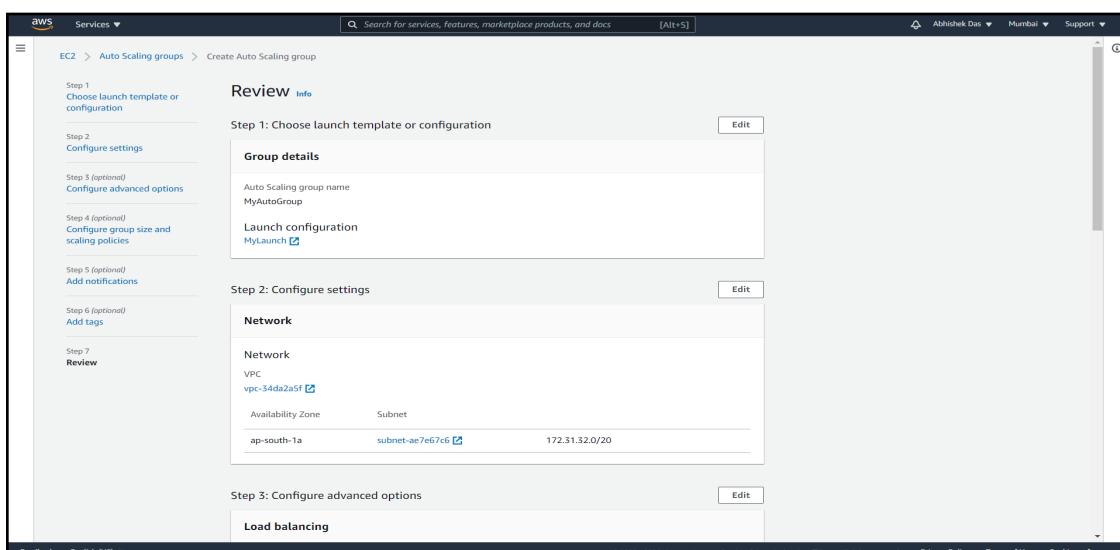
17. In configure group size and autoscaling policies set Maximum capacity as 2 and click next.



18. Now add tags and click next.



19. Review your settings and click on finish.



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

The screenshot shows the AWS EC2 Instances page. A context menu is open over an instance named 'i-09e24dab605c34127'. The 'Actions' menu is expanded, and the 'Attach to Auto Scaling Group' option is selected. Other options visible in the menu include 'Change instance type', 'Change Nitro Enclaves', 'Change termination protection', 'Change shutdown behavior', 'Change credit specification', 'Modify instance placement', 'Modify Capacity Reservation settings', 'Edit user data', and 'Manage tags'.

21. Provide Security group name and click on Attach.

The screenshot shows the 'Attach to Auto Scaling group' dialog box. It displays the instance ID 'i-09e24dab605c34127' and the public IPv4 DNS 'ec2-13-235-71-205.ap-south-1.compute.amazonaws.com'. Below these fields is a search bar containing 'MyAutoGroup'. A note at the bottom of the dialog box states: 'When you attach an instance to a new Auto Scaling group, we create a new launch configuration and associate it with the Auto Scaling group.' At the bottom right of the dialog box are 'Cancel' and 'Attach' buttons.

The screenshot shows the AWS EC2 Instances page again. The instance 'i-09e24dab605c34127' is now listed with the status 'Attached to MyAutoGroup'. The status bar at the top of the page also displays this information: 'Attached i-09e24dab605c34127 to auto scaling group MyAutoGroup'.

08: Cloud Watch

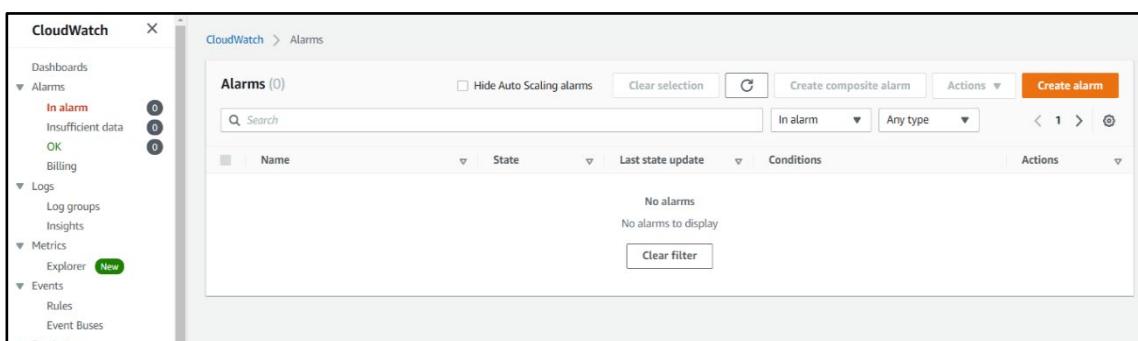
About Cloud Watch: Amazon CloudWatch is a monitoring and management service that provides data and actionable insights for AWS, hybrid, and on-premises applications and infrastructure resources. With CloudWatch, you can collect and access all your performance and operational data in form of logs and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

Process to Configure Cloud Watch:

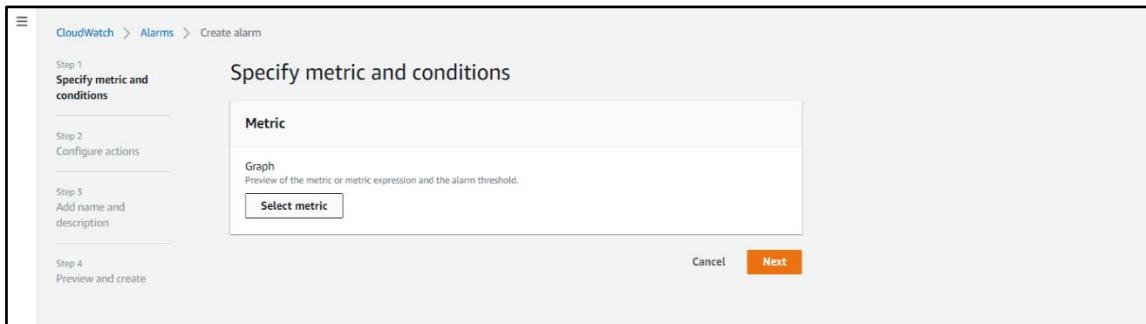
1. Sign in to the AWS Management Console.

The image consists of two side-by-side screenshots of the AWS sign-in interface. The left screenshot shows the 'Sign in' screen with the AWS logo at the top. It has two radio button options: 'Root user' (selected) and 'IAM user'. Below each option is a brief description. Underneath is a 'Root user email address' input field containing 'abhishekdas0317@gmail.com' and a blue 'Next' button. The right screenshot shows the 'Root user sign in' screen with the AWS logo. It displays the email 'abhishekdas0317@gmail.com'. There are fields for 'Password' and 'Forgot password?'. Below these is a large blue 'Sign in' button. At the bottom of the screen are links for 'Sign in to a different account' and 'Create a new AWS account'.

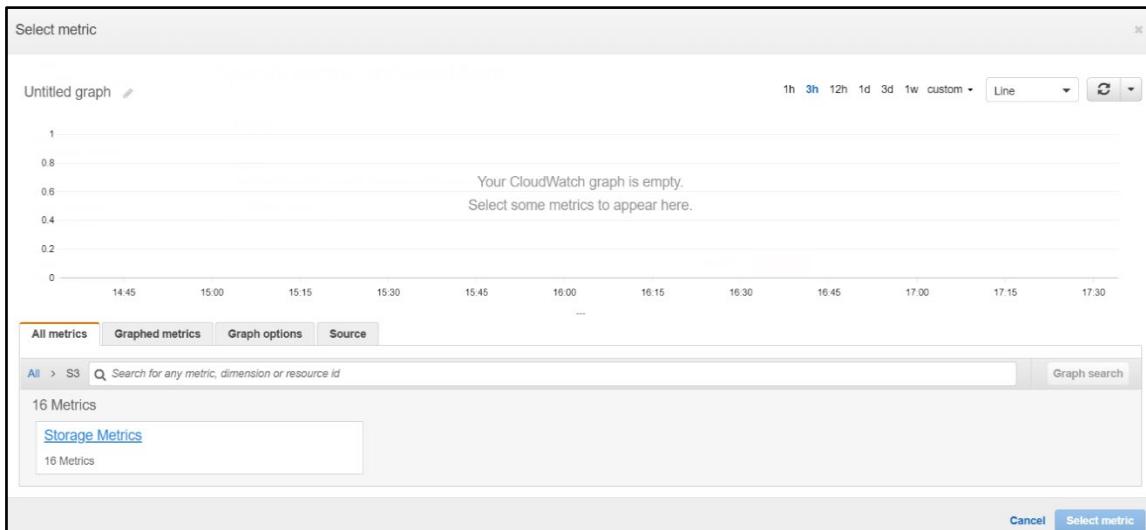
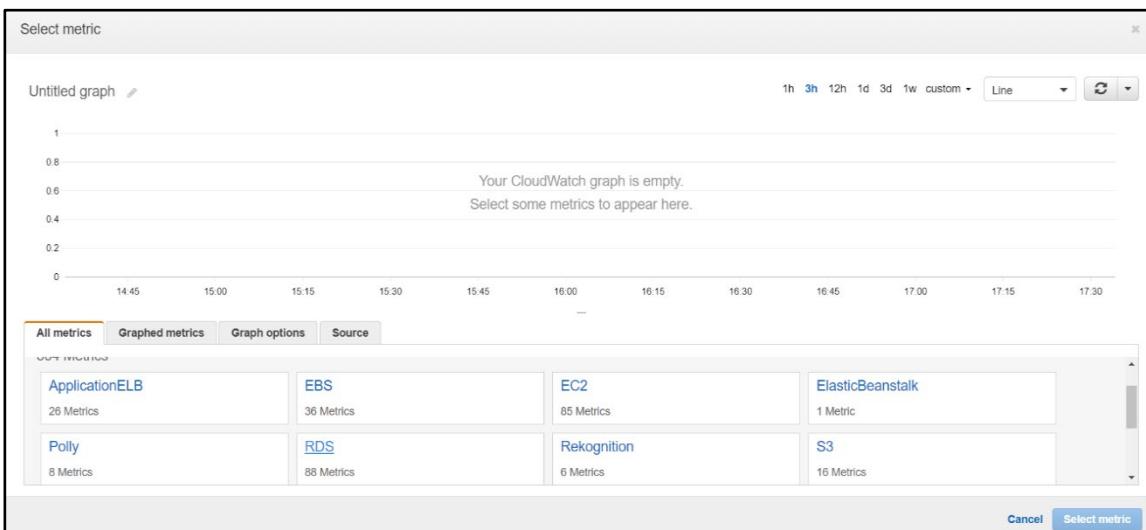
2. Click on CloudWatch from service and then click on “In alarm”.



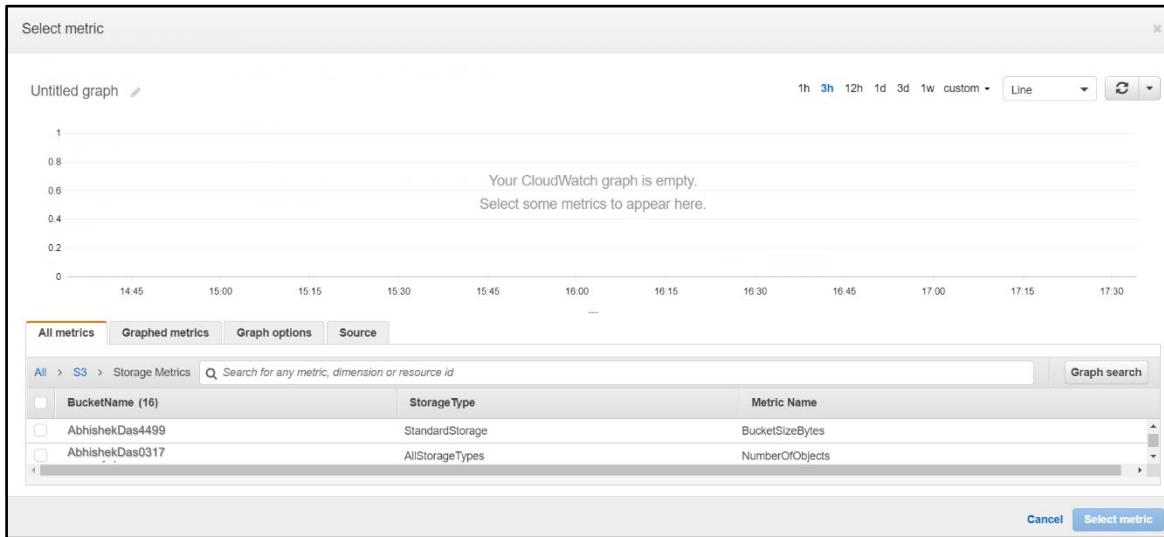
3. Now click on Create alarm and do configuration.



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



5. Now select storage matrix as well as bucket.



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

The screenshots show the 'Specify metric and conditions' step of the CloudWatch Create alarm wizard. On the left, a sidebar lists steps: Step 1 (selected), Step 2, Step 3, and Step 4. The main area shows a graph titled 'Metric' with a Y-axis from 2 to 4 and an X-axis from 02/18 to 02/24. A blue line represents the metric 'NumberOfObjects'. To the right, configuration fields include:

- Metric**: Number of Objects
- Graph**: This alarm will trigger when the blue line goes above the red line for 1 datapoints within 1 day.
- Namespace**: AWS/S3
- Metric name**: NumberOfObjects
- StorageType**: AllStorageTypes
- BucketName**: AbhishekDas0317
- Statistic**: Average
- Period**: 1 day

Conditions section:

- Threshold type**: Static (selected)
- Whenever NumberOfObjects is...**: Greater than threshold (selected)
- than...**: 1024 (input field)

7. Click on next and select alarm trigger.

The screenshot shows the 'Configure actions' step of creating a new alarm. On the left, a sidebar lists steps: Step 1 (Specify metric and conditions), Step 2 (Configure actions - highlighted in blue), Step 3 (Add name and description), and Step 4 (Preview and create). The main area is titled 'Configure actions' and 'Notification'. It shows an 'Alarm state trigger' section with three options: 'In alarm' (selected), 'OK', and 'Insufficient data'. Below this is a 'Select an SNS topic' section where 'Select an existing SNS topic' is chosen. A search bar 'Select an email list' is present, with a note that only email lists for this account are available. At the bottom is a 'Add notification' button.

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

This screenshot is identical to the one above, showing the 'Configure actions' step of creating a new alarm. The sidebar and main configuration area are the same, including the 'In alarm' selected for the alarm state trigger and the 'Select an existing SNS topic' option chosen for the notification method.

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

The screenshot shows the 'Preview and create' step of the alarm creation process. It includes sections for selecting an SNS topic (with 'Create new topic' selected and a topic name 'Default_CloudWatch_Alarms_Topic' entered), creating a new topic endpoint ('Email endpoints that will receive the notification...' with 'abhisipu4@gmail.com' listed), and a note about comma-separated email addresses. The right side of the screen is a large, empty white area.

Step 4
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

Send a notification to...

Email (endpoints)
abhisipu4@gmail.com - [View in SNS Console](#)

Add notification

Auto Scaling action

Add Auto Scaling action

EC2 action

This action is only available for EC2 Per-Instance Metrics.

10. Click on next and write alarm 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

Add name and description

Name and description

Alarm name
Storage alarms

Alarm description - optional
Alarm description
Up to 1024 characters (0/1024)

Cancel Previous Next

11. Again, click on next and create alarm.

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

13. Then CloudWatch created successfully.

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

09: Amazon RDS

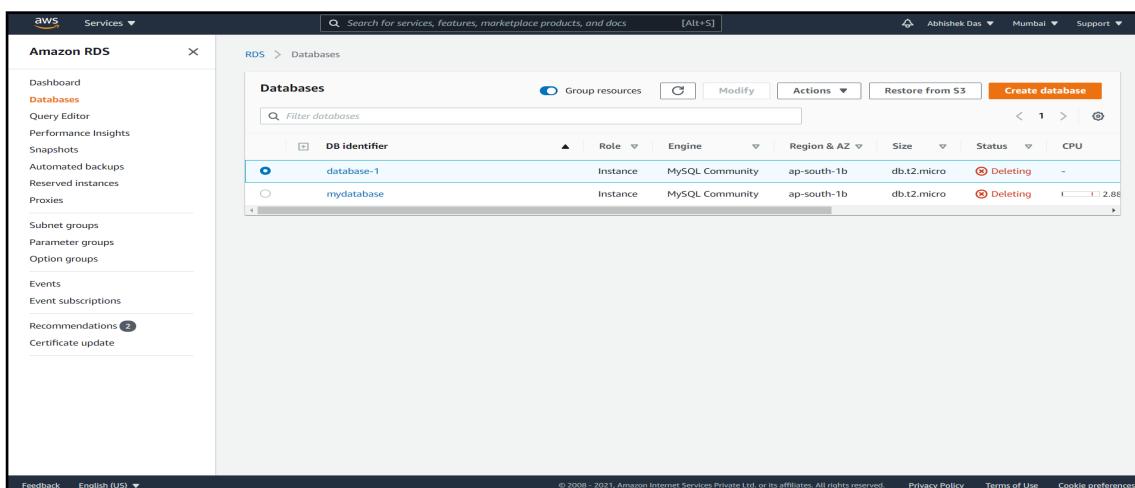
About Amazon RDS: Amazon Relational Database Service (Amazon RDS) makes it easy to set up, operate, and scale a relational database in the cloud. It provides cost-efficient and resizable capacity while automating time-consuming administration tasks such as hardware provisioning, database setup, patching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

Process to Configure Amazon RDS:

1. Sign in to the AWS Management Console.

The image contains two side-by-side screenshots of the AWS sign-in interface. The left screenshot shows the initial 'Sign in' screen with two options: 'Root user' (selected) and 'IAM user'. Below these are fields for 'Root user email address' containing 'abhishekdas0317@gmail.com' and a large blue 'Next' button. The right screenshot shows the 'Root user sign in' screen, which includes fields for 'Email' (containing 'abhishekdas0317@gmail.com') and 'Password', a 'Forgot password?' link, and a large blue 'Sign in' button. Below the sign-in form are links for 'Sign in to a different account' and 'Create a new AWS account'.

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



The screenshot shows the AWS RDS 'Create database' interface. In the 'Choose a database creation method' section, 'Standard create' is selected. In the 'Engine options' section, 'MySQL' is selected from the engine type dropdown. Other engines listed include Amazon Aurora, MariaDB, PostgreSQL, Oracle, and Microsoft SQL Server.

3. Then select MySQL database and select its version.

The screenshot shows the AWS RDS 'Create database' interface. In the 'Engine options' section, 'MySQL' is selected from the engine type dropdown. In the 'Edition' section, 'MySQL Community' is selected. Other editions listed include Amazon Aurora with MySQL compatibility and Amazon Aurora with PostgreSQL compatibility.

4. Now select Free Tier Template.

The screenshot shows the AWS RDS 'Templates' page. In the 'Templates' section, 'Free tier' is selected. In the 'Settings' section, the 'DB instance identifier' is set to 'database-2'. Under 'Credentials Settings', the 'Master username' is 'admin' and the 'Master password' is '*****'. There is also an option to 'Auto generate a password'.

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

The screenshot shows the 'Settings' tab of the AWS RDS configuration interface. It includes fields for the DB instance identifier ('mydatabase07'), master username ('admin'), master password, and confirm password. Below these, the 'DB instance class' section is visible, with the note that options are limited to those supported by the selected engine.

6. Select instance type and Storage.

The screenshot shows the 'DB instance class' selection screen. The 'Burstable classes (includes t classes)' option is selected. A dropdown menu lists various instance types, with 'db.t2.micro' currently highlighted. A tooltip for 'db.t2.micro' indicates it has 1 vCPU and 1 GiB RAM, and is Not EBS Optimized.

The screenshot shows the 'Storage' configuration screen. It includes fields for storage type ('General Purpose (SSD)'), allocated storage (set to 20 GiB), and maximum storage threshold (set to 1000 GiB). Other sections like 'Availability & durability' and 'Connectivity' are also partially visible.

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

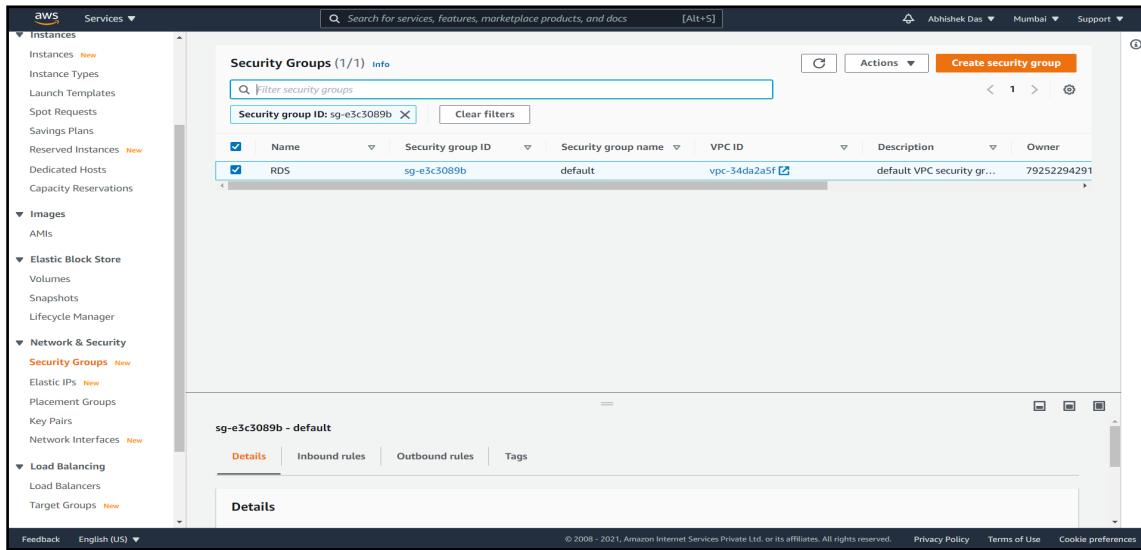
The screenshot shows the 'Connectivity' configuration step in the AWS RDS 'Create DB instance' wizard. It includes fields for selecting a VPC (Default VPC), Subnet group (default-vpc-34da2a5f), Public access (Yes), and VPC security group (Choose existing). A note indicates that after creation, the VPC cannot be changed.

8. After complete review, click on Create database.

This screenshot shows the continuation of the RDS creation wizard. It displays options for authentication (Password authentication selected), additional configuration (with a note about backup and monitoring), estimated monthly costs (free tier details), and a note about third-party product rights. At the bottom is a 'Create database' button.

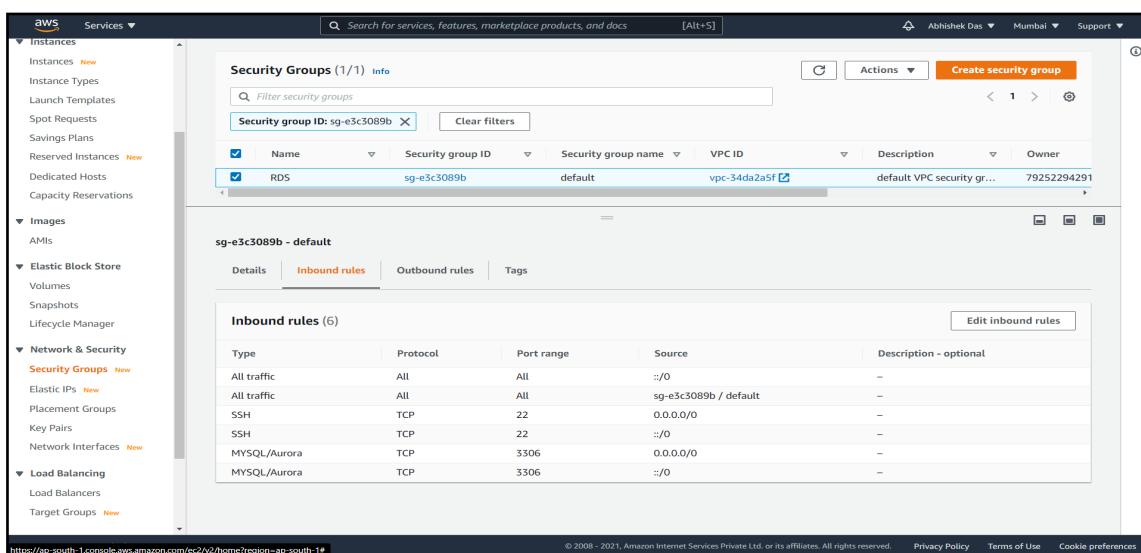
The screenshot shows the 'Databases' section of the AWS RDS console. It lists a single database named 'mydatabase007' with the following details: Instance (db.t2.micro), Engine (MySQL Community), Region & AZ (ap-south-1b), Status (Creating), and CPU (1). The left sidebar shows navigation links for Dashboard, Databases (selected), Query Editor, Performance Insights, Snapshots, Automated backups, Reserved instances, Proxies, Subnet groups, and Parameter groups.

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



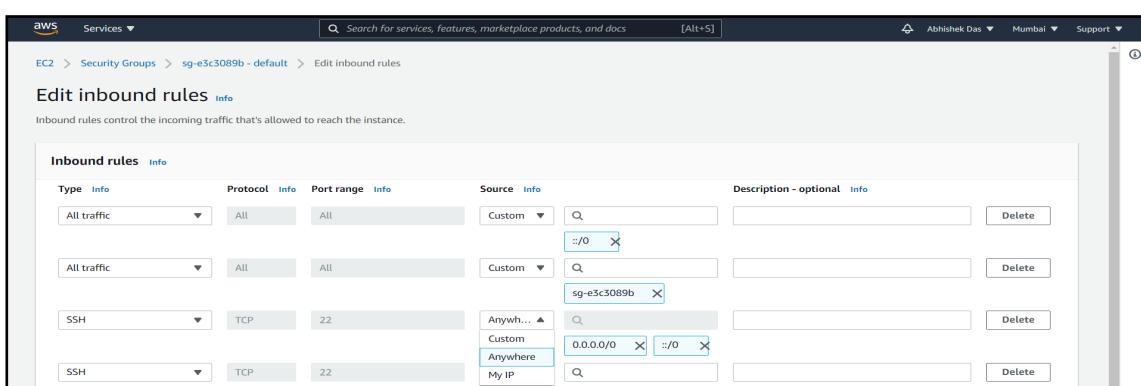
The screenshot shows the AWS Management Console with the EC2 service selected. Under the 'Instances' section, there is a link to 'Security Groups'. The main pane displays a table titled 'Security Groups (1/1) info' with one entry: 'RDS' (sg-e3c3089b). The table includes columns for Name, Security group ID, Security group name, VPC ID, Description, and Owner. Below the table, a detailed view for 'sg-e3c3089b - default' is shown, with tabs for Details, Inbound rules, Outbound rules, and Tags. The 'Inbound rules' tab is currently selected, showing a list of six rules. The first rule is 'All traffic' (Protocol: All, Port range: All, Source: ::/0, Description: optional). The second rule is 'All traffic' (Protocol: All, Port range: All, Source: sg-e3c3089b / default, Description: optional). The third and fourth rules are 'SSH' (Protocol: TCP, Port range: 22, Source: 0.0.0.0/0, Description: optional). The fifth and sixth rules are 'MySQL/Aurora' (Protocol: TCP, Port range: 3306, Source: 0.0.0.0/0, Description: optional).

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



This screenshot is identical to the previous one, showing the EC2 Security Groups page with the RDS security group selected. The 'Inbound rules' tab is highlighted. The table below shows the same six inbound rules as the previous screenshot, with the second rule ('All traffic' from sg-e3c3089b) being the target for modification.

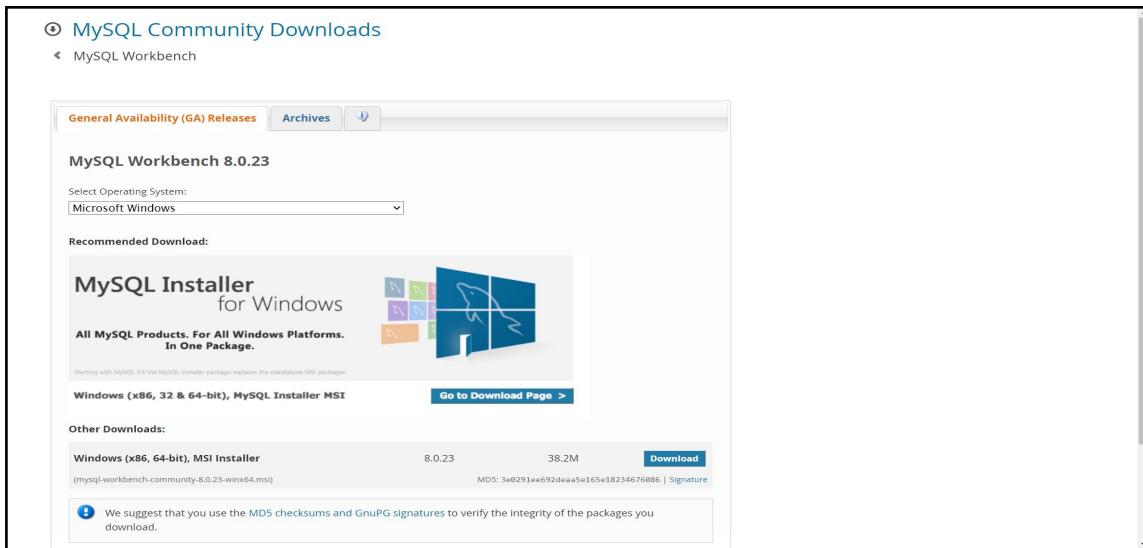
11. Add SSH and edit source to Anywhere.



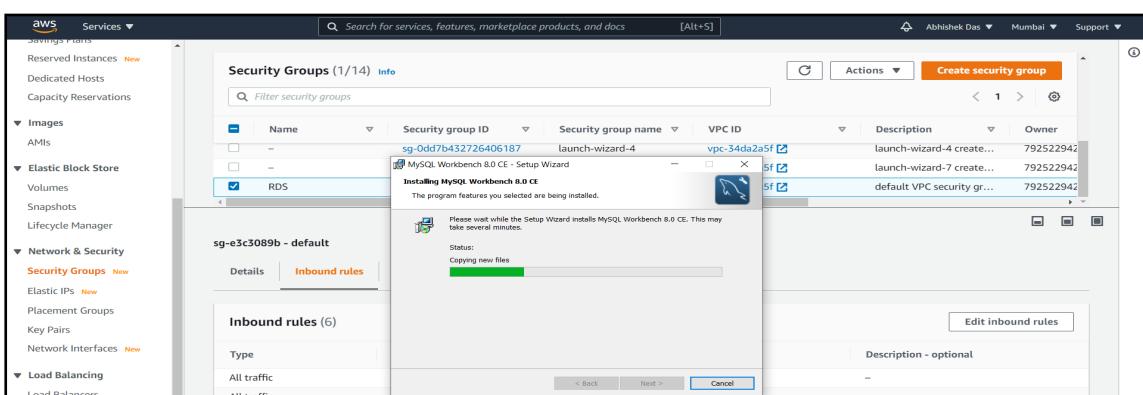
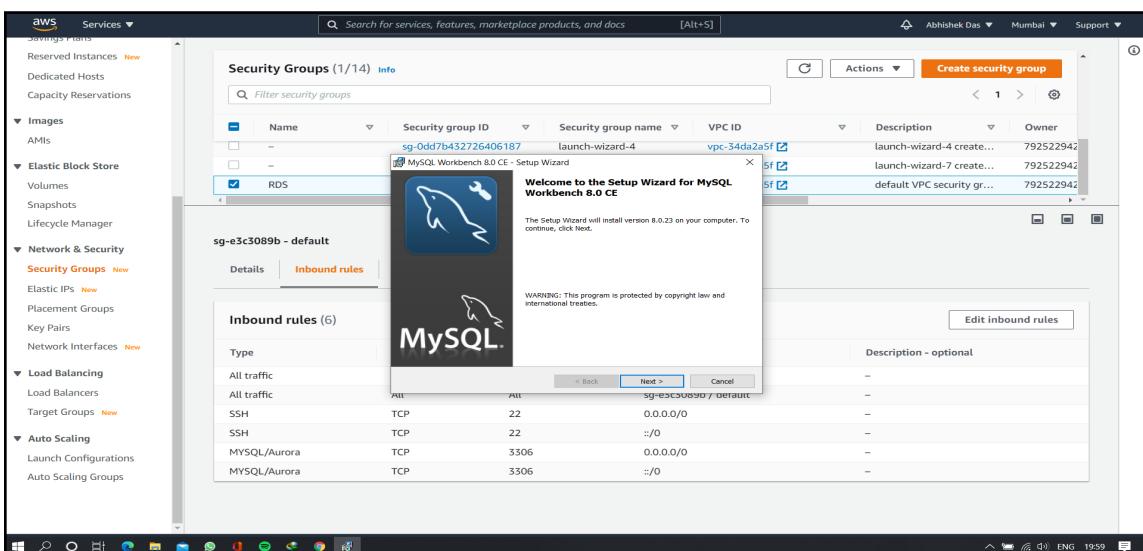
The screenshot shows the 'Edit inbound rules' dialog for the 'sg-e3c3089b - default' security group. The 'Inbound rules' table has a new row for 'SSH' (Protocol: TCP, Port range: 22). The 'Source' column for this rule is set to 'Anywhere' (Custom: 0.0.0.0/0, TCP: ::/0). There are also other rows for 'All traffic' (Protocol: All, Port range: All) with sources ::/0 and sg-e3c3089b / default.

12. Now browse this site

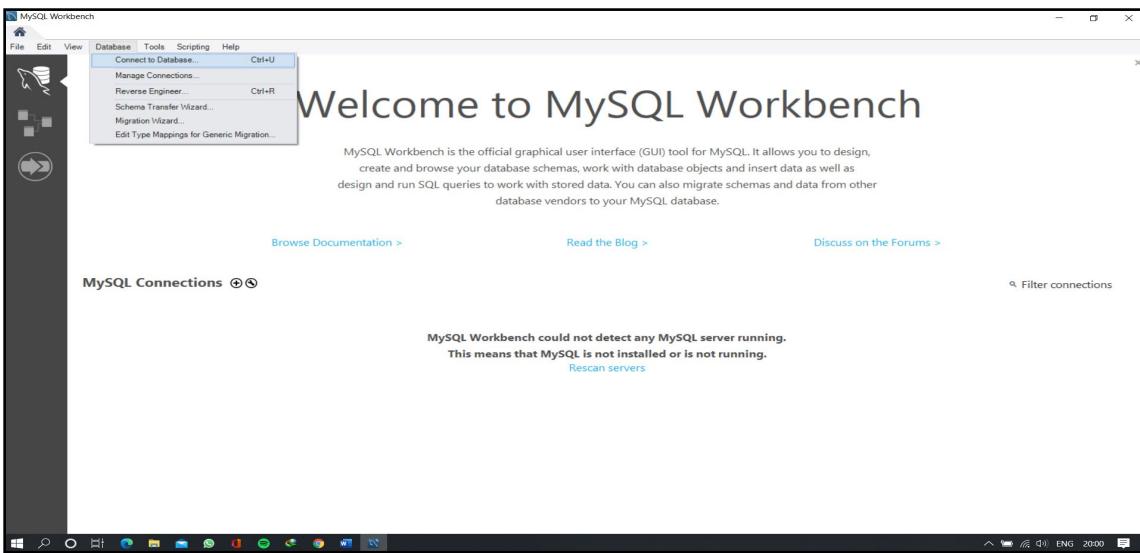
<https://dev.mysql.com/downloads/workbench/> “and download MySQL installer.



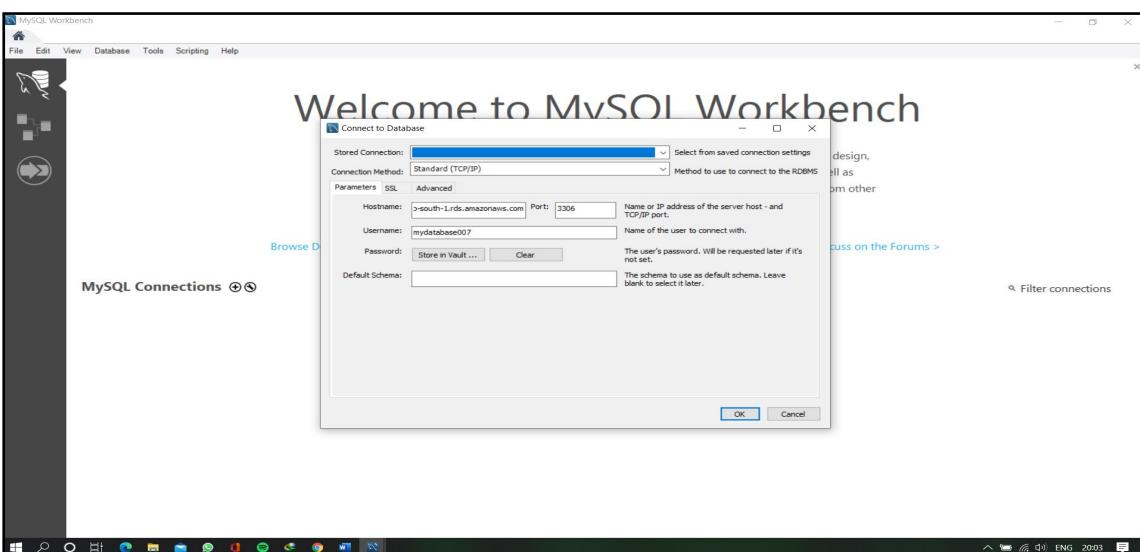
13. Then install MySQL and launch it.



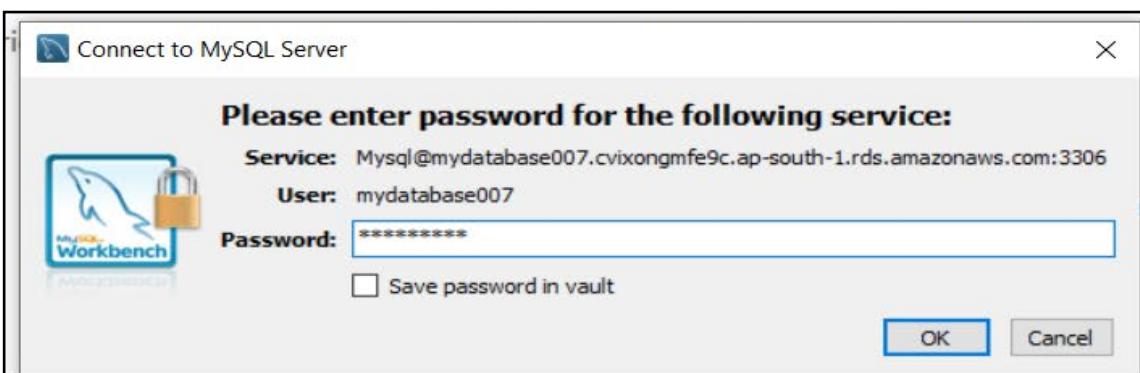
14. Then click on database >> connect database.



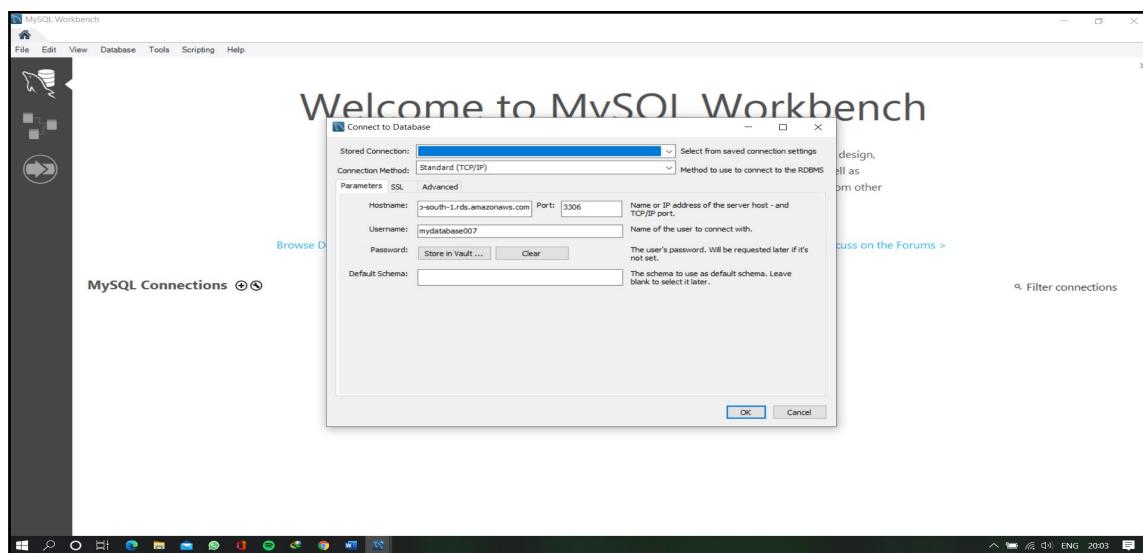
15. Now enter end point and password.



16. Then click on connect.



17. After successful connection we can create database.



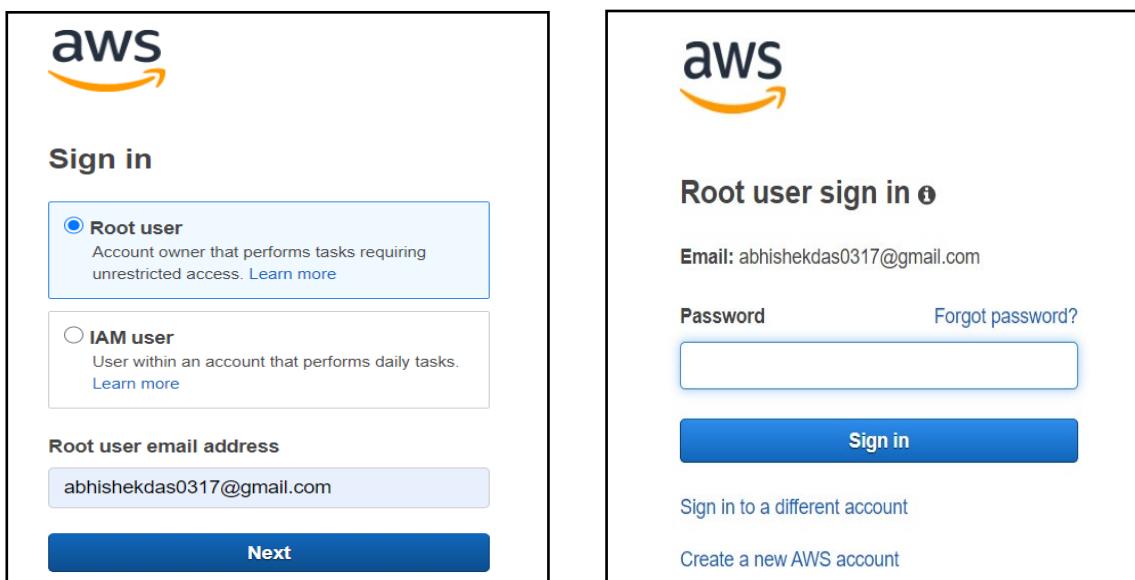
10: AWS CLI

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.

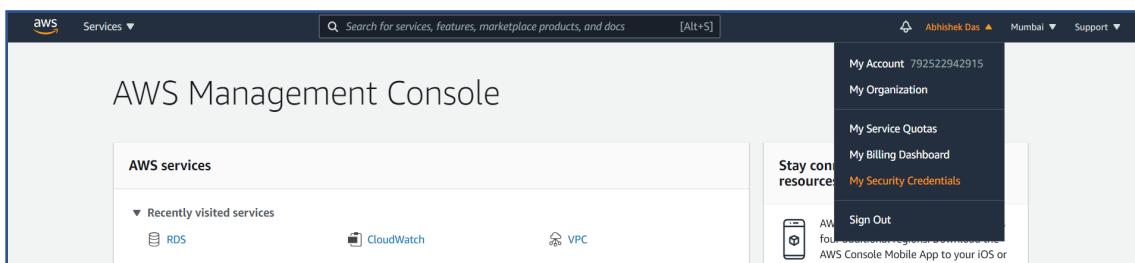
Process to Configure Amazon CLI:

1. Sign in to the AWS Management Console.



The image contains two side-by-side screenshots of the AWS sign-in interface. The left screenshot shows the initial 'Sign in' screen where the 'Root user' option is selected. It includes a field for the 'Root user email address' containing 'abhishekdas0317@gmail.com' and a large blue 'Next' button at the bottom. The right screenshot shows the 'Root user sign in' screen, which requires an 'Email' (which is already filled with 'abhishekdas0317@gmail.com') and a 'Password'. It also features a 'Forgot password?' link and a large blue 'Sign in' button.

2. In Dashboard, go to My Security Credential.



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

The screenshot shows the AWS IAM 'Your Security Credentials' page. On the left, there's a sidebar with navigation links like Dashboard, Access management, and Access reports. The main content area is titled 'Your Security Credentials' and contains sections for Password, Multi-factor authentication (MFA), and Access keys (access key ID and secret access key). A callout box highlights the 'Create New Access Key' button. Below it, a note says: 'Root user access keys provide unrestricted access to your entire AWS account. If you need long-term access keys, we recommend creating a new IAM user with limited permissions and generating access keys for that user instead. Learn more'. The 'Access keys' section has a table with columns: Created, Access Key ID, Last Used, Last Used Region, Last Used Service, Status, and Actions. There are also links for CloudFront key pairs, X.509 certificate, and Account identifiers.

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

This screenshot shows the same 'Your Security Credentials' page after a new access key has been created. A modal dialog box is open, stating 'Your access key (access key ID and secret access key) has been created successfully.' It includes instructions to download the key file and a 'Show Access Key' button. The 'Create Access Key' button is also visible on the page. The rest of the interface is similar to the first screenshot, with the 'Access keys' table and other sidebar options.

This screenshot shows the 'Your Security Credentials' page again, but now with the newly created access key details displayed. A modal dialog box shows the 'Access Key ID' (AKIA3RBQMNHB5RGm3H7D) and 'Secret Access Key' (k4Hc2U20jcbnrvPd8P30mfEMOyZnMaBTwYwe8c0). Below the dialog, there are buttons for 'Download Key File' and 'Close'. The rest of the page remains consistent with the previous screenshots.

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

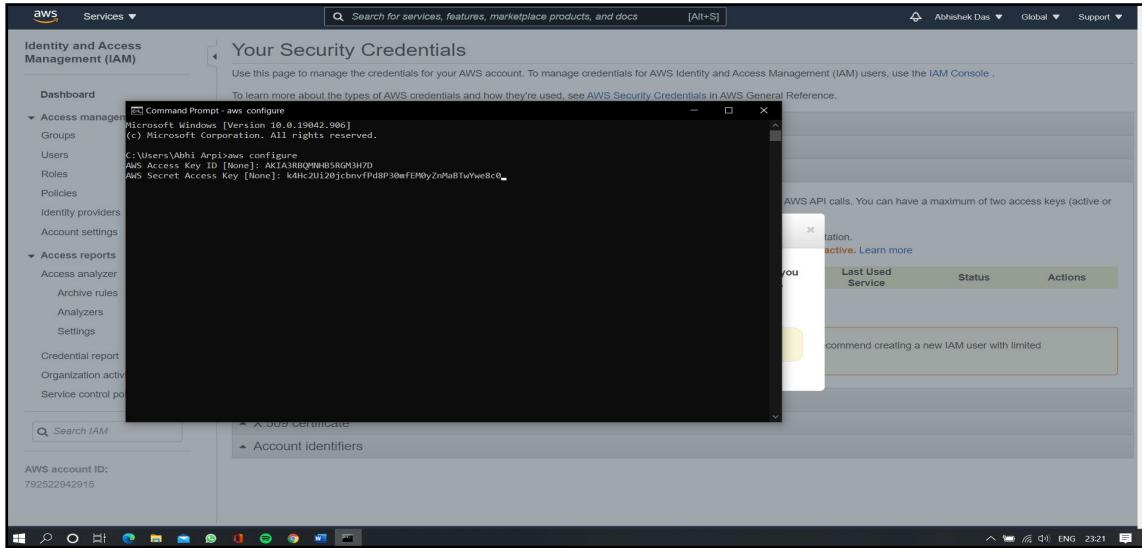
The screenshot shows the AWS Command Line Interface (CLI) v2 landing page. At the top, there's a navigation bar with links for Products, Solutions, Pricing, Documentation, Learn, Partner Network, AWS Marketplace, Customer Enablement, Events, Explore More, Contact Sales, Support, English, My Account, and a prominent orange "Sign In to the Console" button. Below the navigation is a sidebar with "RESOURCES" and a section for "AWS Command Line Interface". Under "RELATED LINKS", there are links for Documentation, Tools, and Release Notes. A button for "Get Started with AWS for Free" and a "Create Free Account" button are also present. The main content area features the title "AWS Command Line Interface" in orange. It describes the CLI as a unified tool for managing AWS services via the command line. It highlights new features like improved installers and AWS Single Sign-On (SSO). Below this, there are four icons: "Getting Started" (a large number 1), "CLI Reference", "GitHub Project", and "Community Forum". To the right, there are sections for "Windows", "MacOS", "Linux", and "Amazon Linux", each with download links. A "aws-shell (Developer Preview)" section at the bottom provides information about the command-line shell program.

This screenshot shows the "AWS Command Line Interface v2 Setup Wizard" window. The title bar says "AWS Command Line Interface v2 Setup". The main content area displays the first step of the wizard, which asks if the user wants to install the AWS CLI. It includes a progress bar showing "Step 1 of 10" and a note that the setup will install the AWS CLI v2 on the computer. Buttons for "Back", "Next", and "Cancel" are visible. To the right of the wizard window, the same sidebar and main content area from the previous screenshot are visible, including the "aws-shell (Developer Preview)" section.

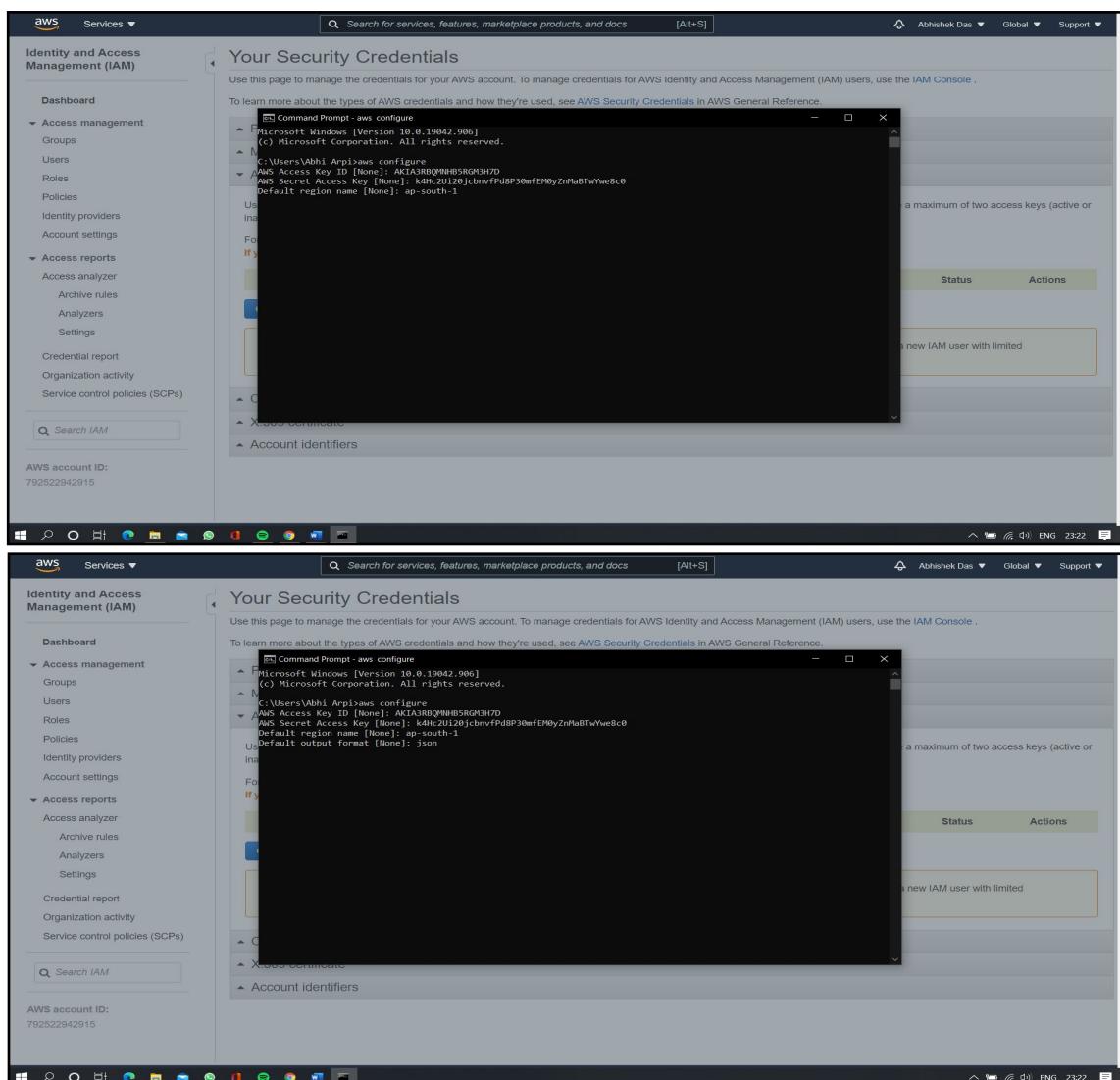
6. Then Open Command Line and type “aws configuration”.

This screenshot shows a Microsoft Command Prompt window titled "Command Prompt". The prompt shows the user has typed "aws configure". The right side of the screen displays the "aws-shell (Developer Preview)" section from the previous screenshots, which explains the aws-shell command and its convenience features for both new and advanced users. It also includes links for "Release Notes" and "Amazon Linux AMI".

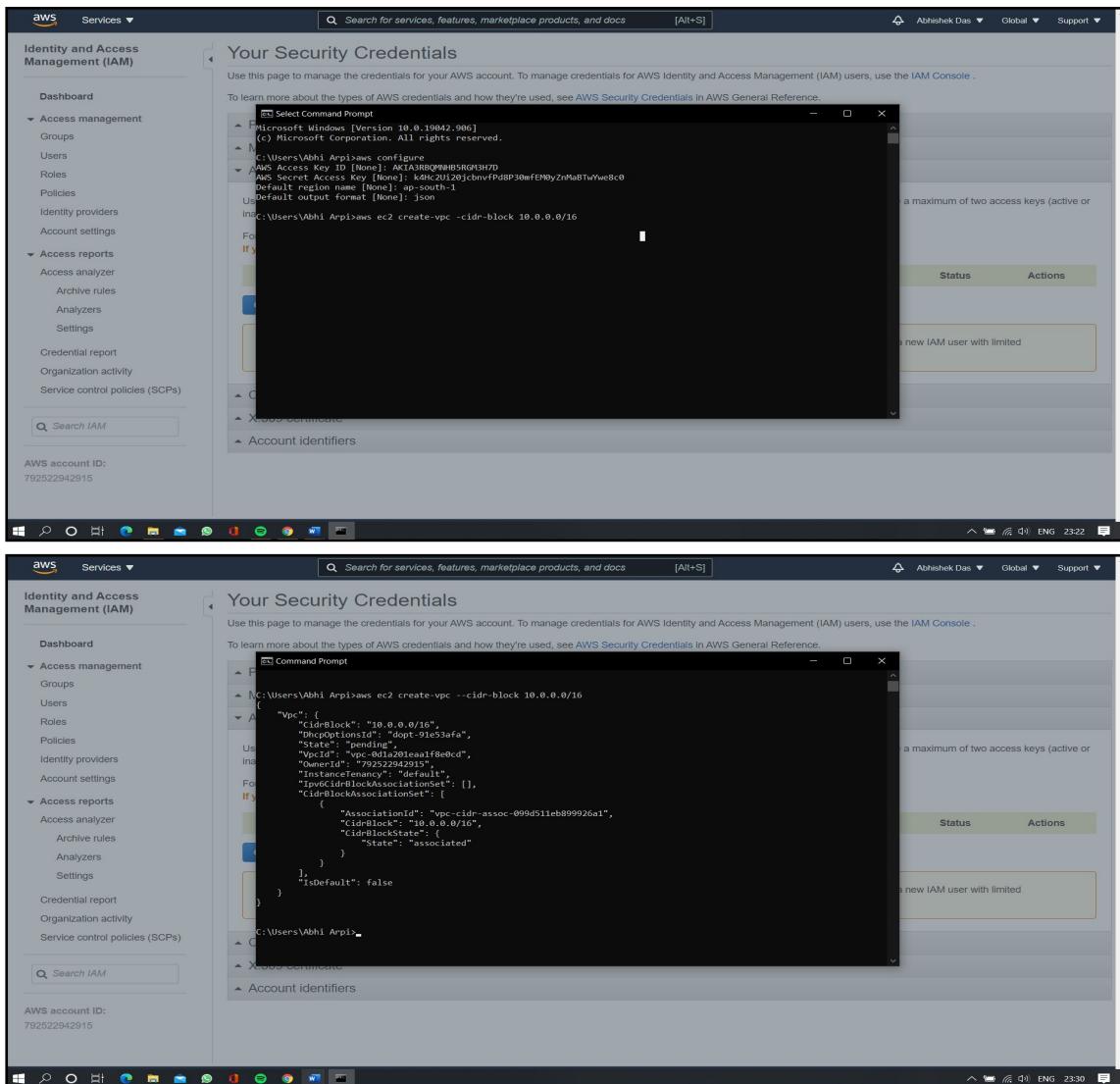
7. Then Provide Access key ID and Secret Access key.



8. Provide Region Name and output format.



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



The image contains two side-by-side screenshots of the AWS IAM Security Credentials page. Both screenshots show a Command Prompt window in the foreground displaying the command "aws ec2 create-vpc --cidr-block 10.0.0.0/16". The background shows the IAM console with a list of access keys for the user 'Abhishek Das'. The first screenshot has a timestamp of 23:22, and the second has a timestamp of 23:30.

```
C:\Users\Abhi>aws ec2 create-vpc --cidr-block 10.0.0.0/16
```

```
M:\Users\Abhi>aws ec2 create-vpc --cidr-block 10.0.0.0/16
```

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

