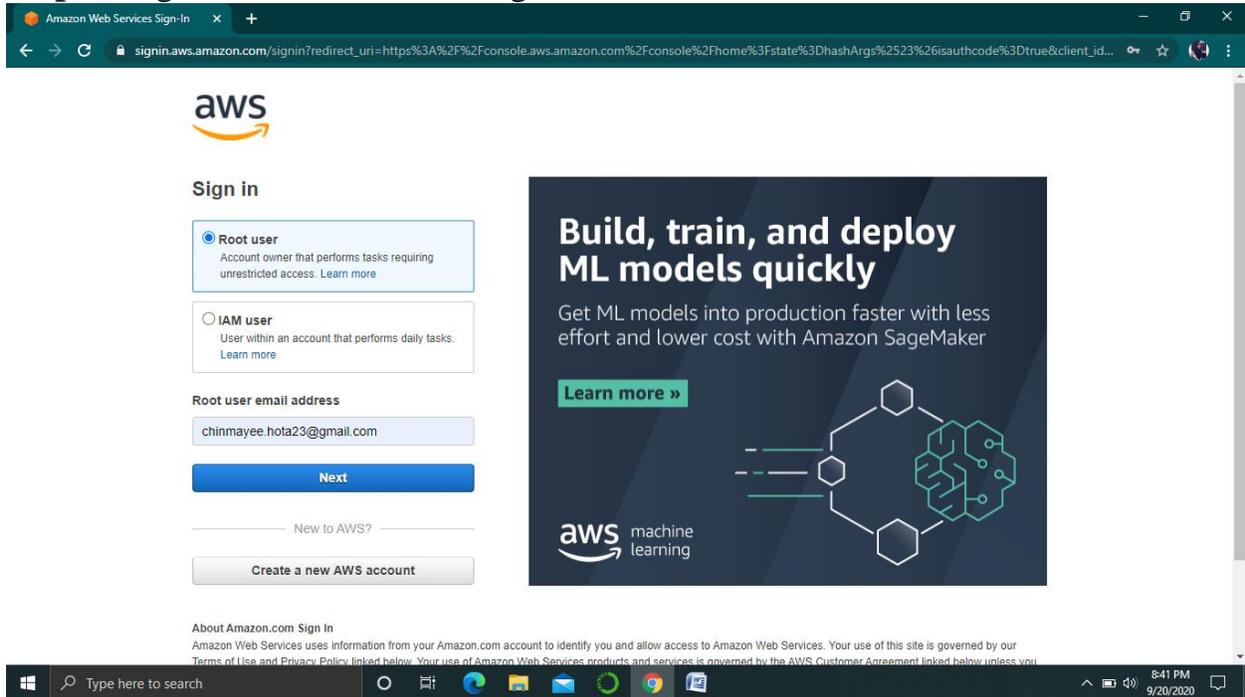
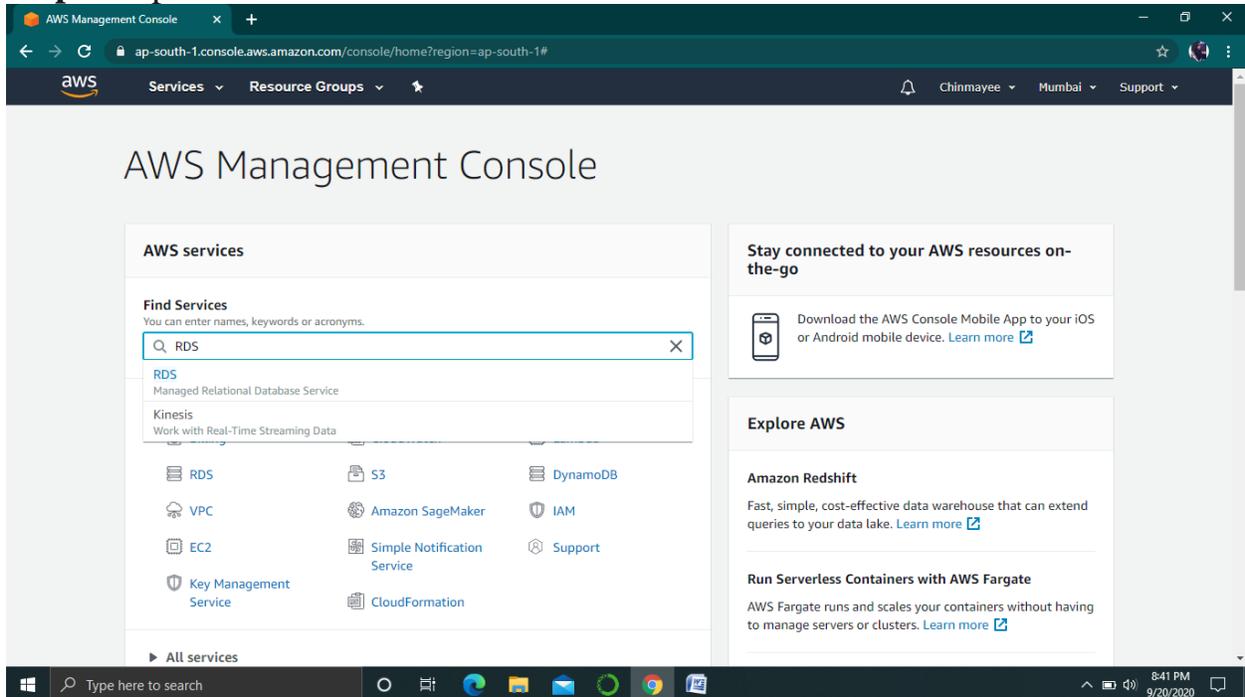


CREATING A DATABASE USING AMAZON AURORA

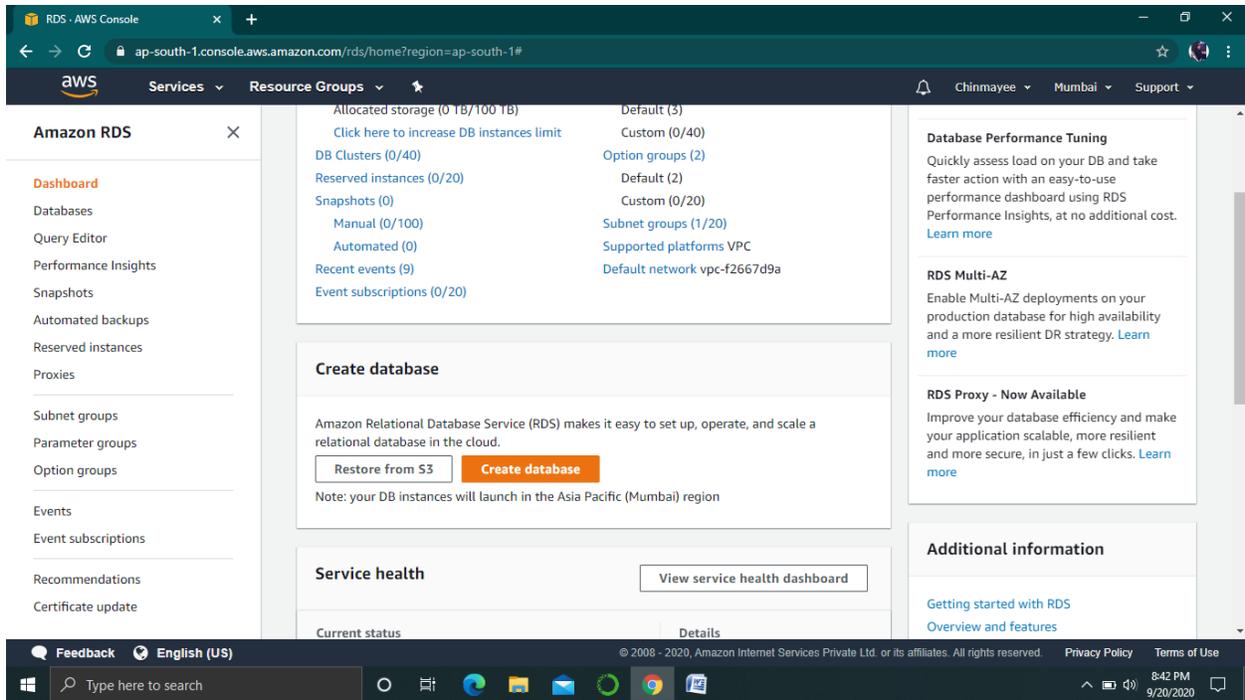
Step 1: Sign in to the AWS Management Console.



Step 2: Open the service as RDS.

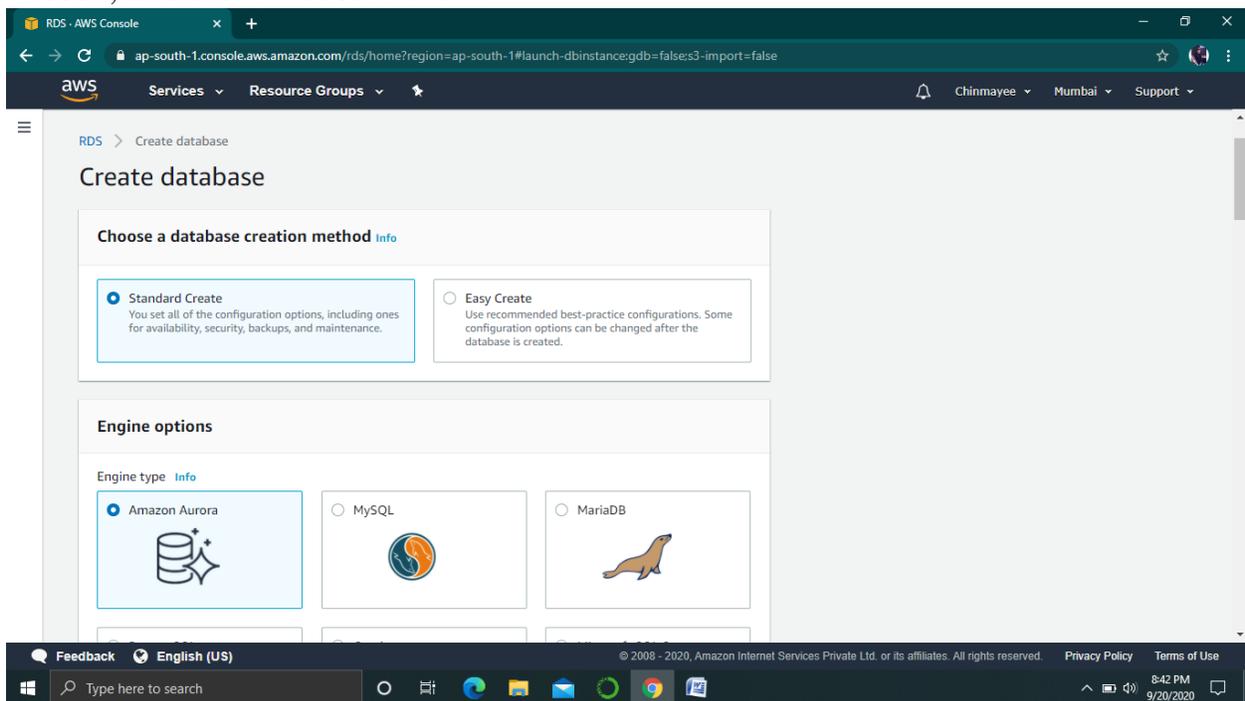


Step 3: In the navigation pane, choose Databases.

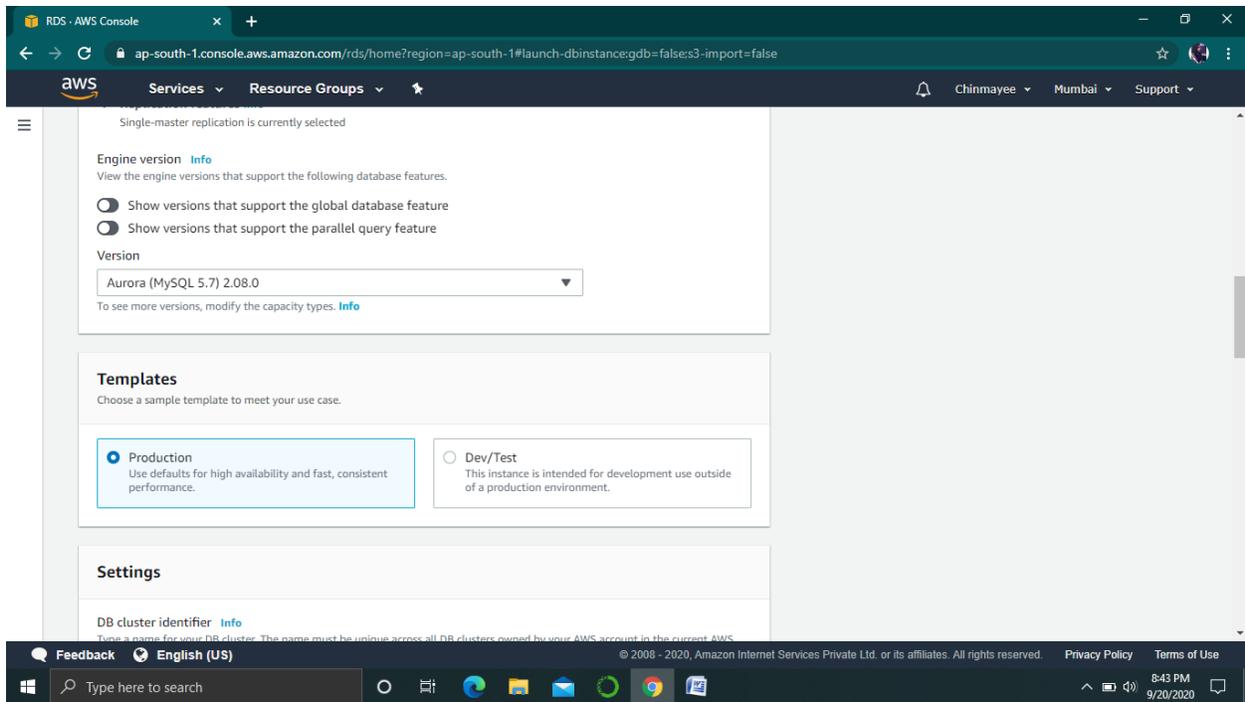


Step 4: Choose Create database.

Step 5: On the Create database page, make sure that the Standard Create option is chosen, and then choose Aurora.

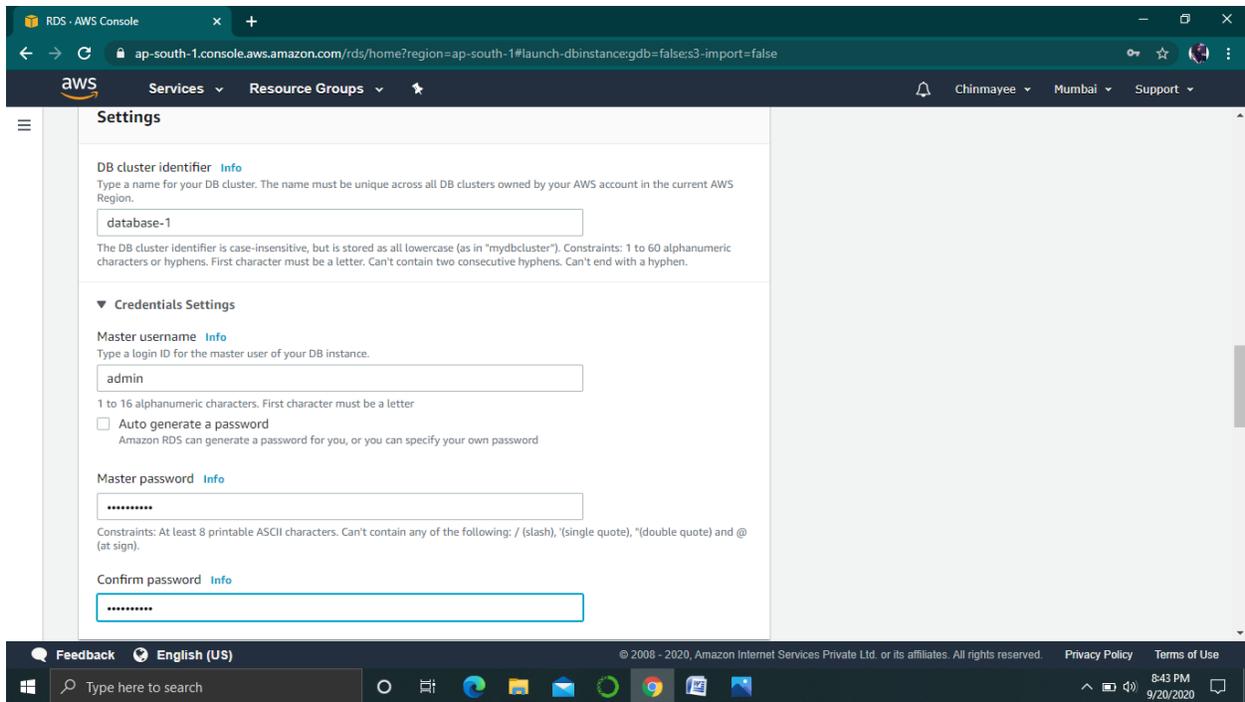


Step 6: In the Templates section, choose Production tier.



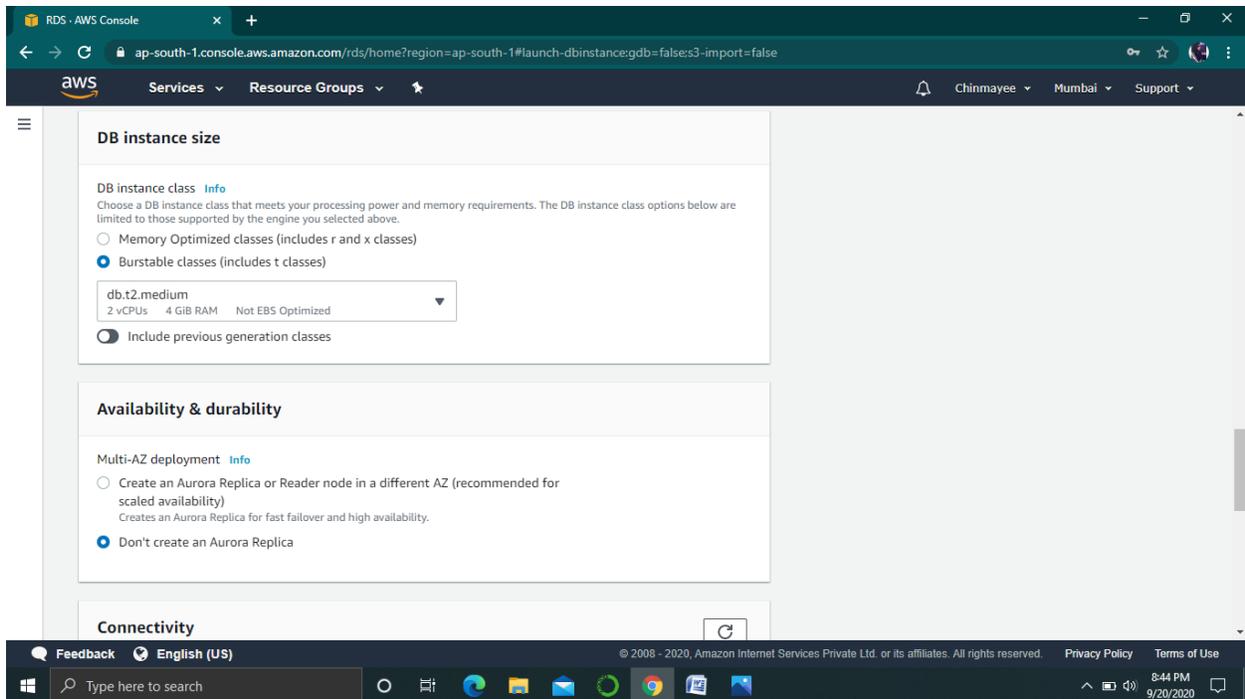
Step 7: In the Settings section, set these values:

- DB instance identifier – database-1
- Master username – admin
- Auto generate a password – Disable the option
- Master password – Choose a password.
- Confirm password – Retype the password.



Step 8: In the DB instance size section, set these values:

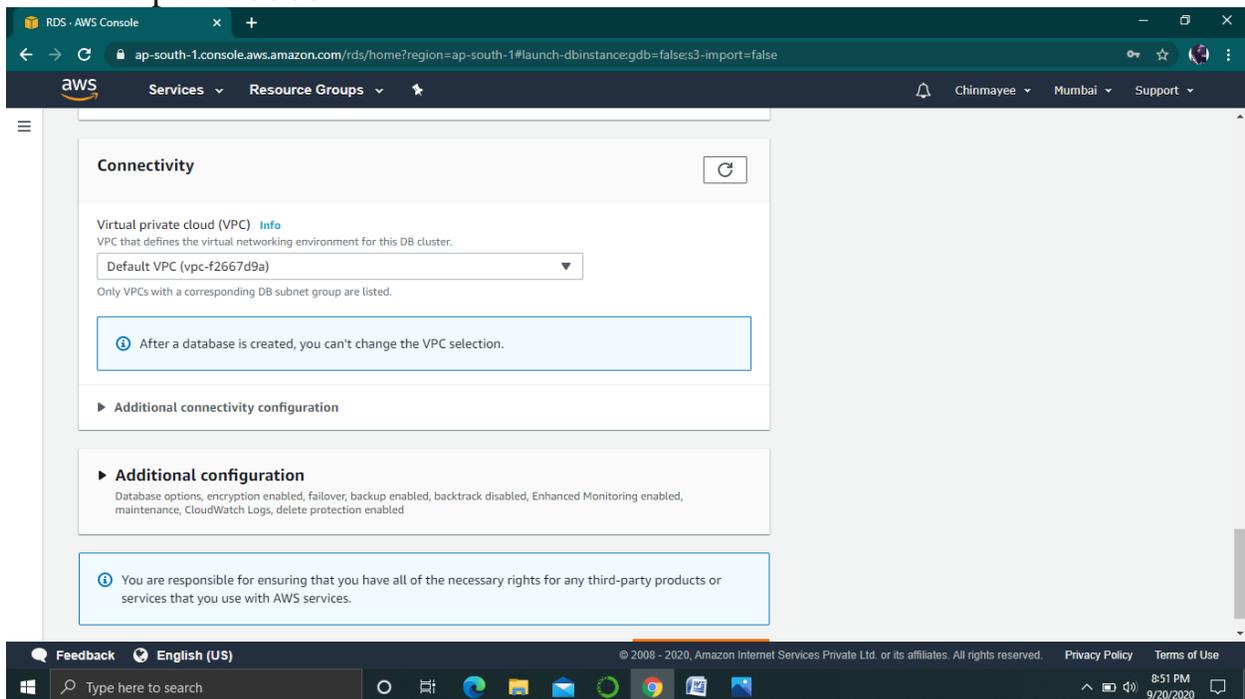
- Burstable classes (includes t classes)
- db.t2.medium



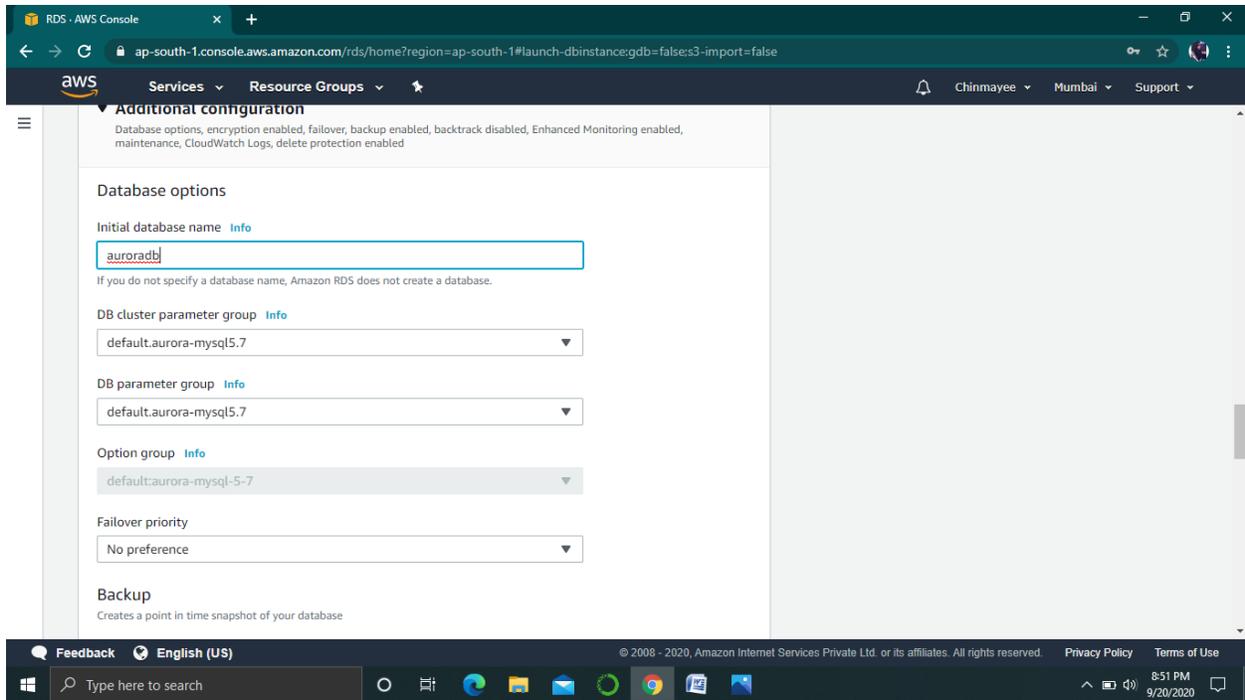
Step 9: In the Storage and Availability & durability sections, use the default values.

Step 10: In the Connectivity section, open Additional connectivity configuration and set these values:

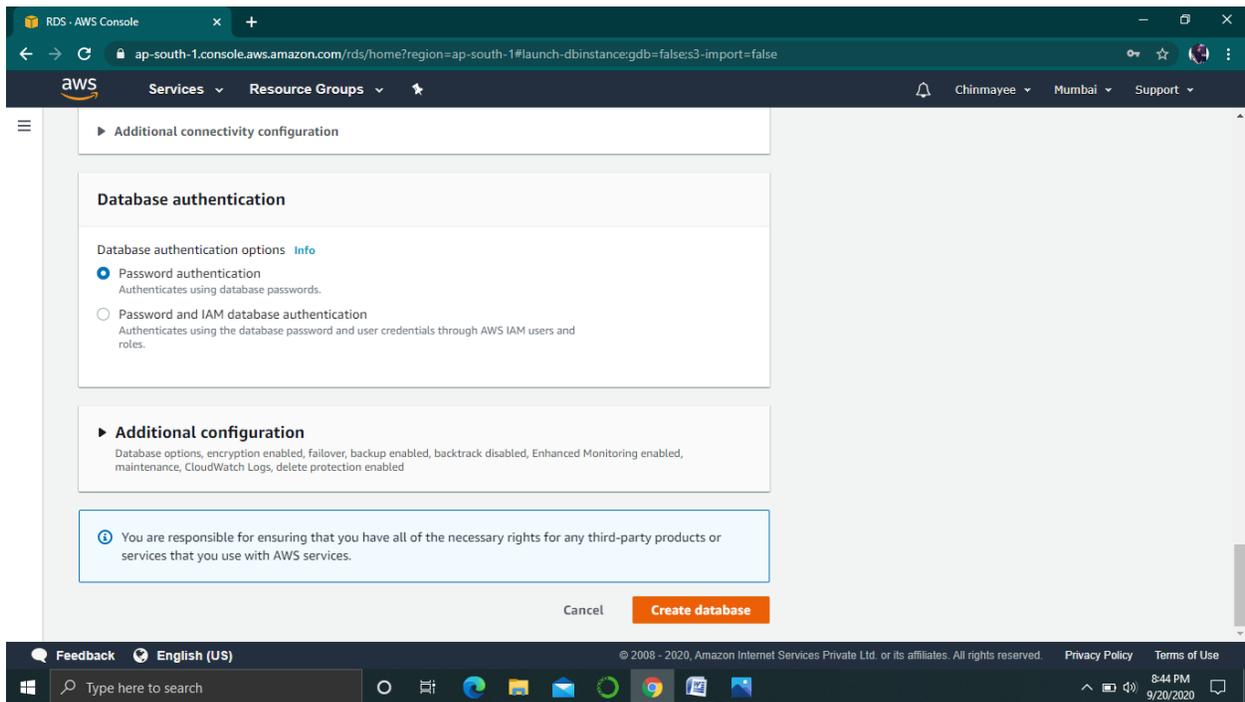
- Virtual Private Cloud (VPC) – Choose an existing VPC with both public and private subnets.
- Subnet group – The DB subnet group for the VPC, created .
- Publicly accessible – No
- VPC security groups – Choose an existing VPC security group.
- Remove other security groups, such as the default security group, by choosing the X associated with each.
- Availability zone – No Preference
- Database port – 3306



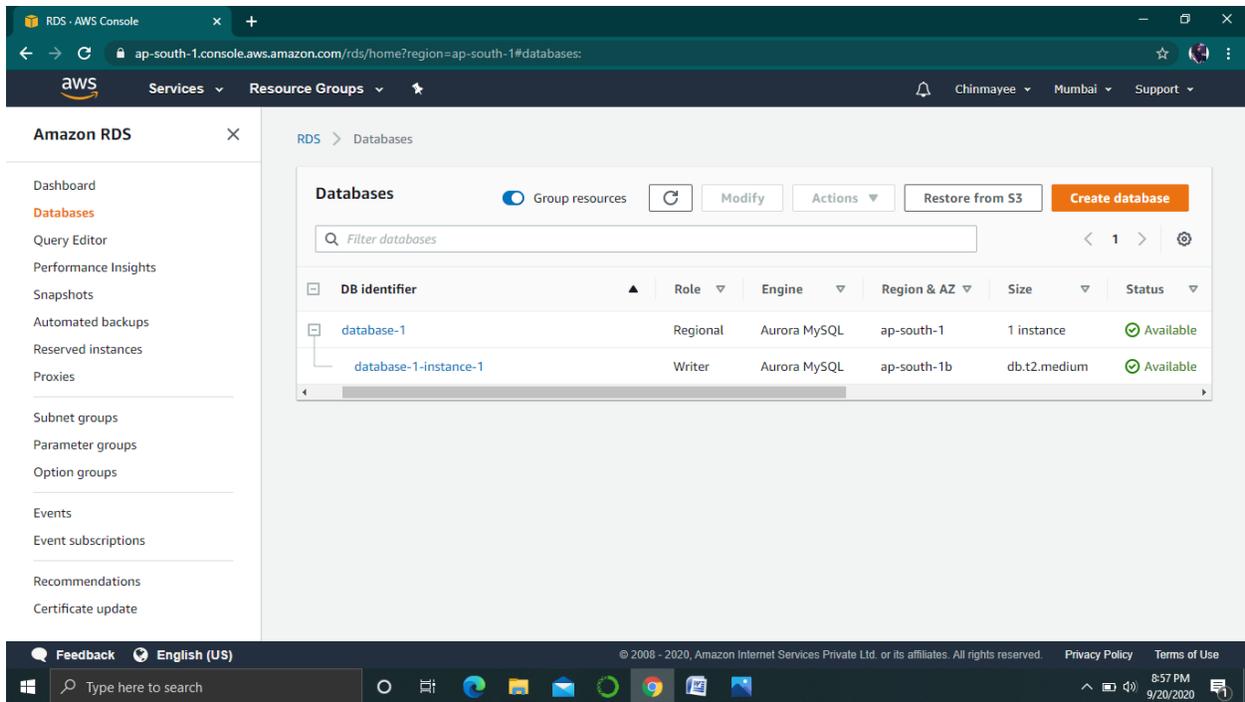
Step 11: Open the Additional configuration section, and enter auroradb for Initial database name. Keep the default settings for the other options.



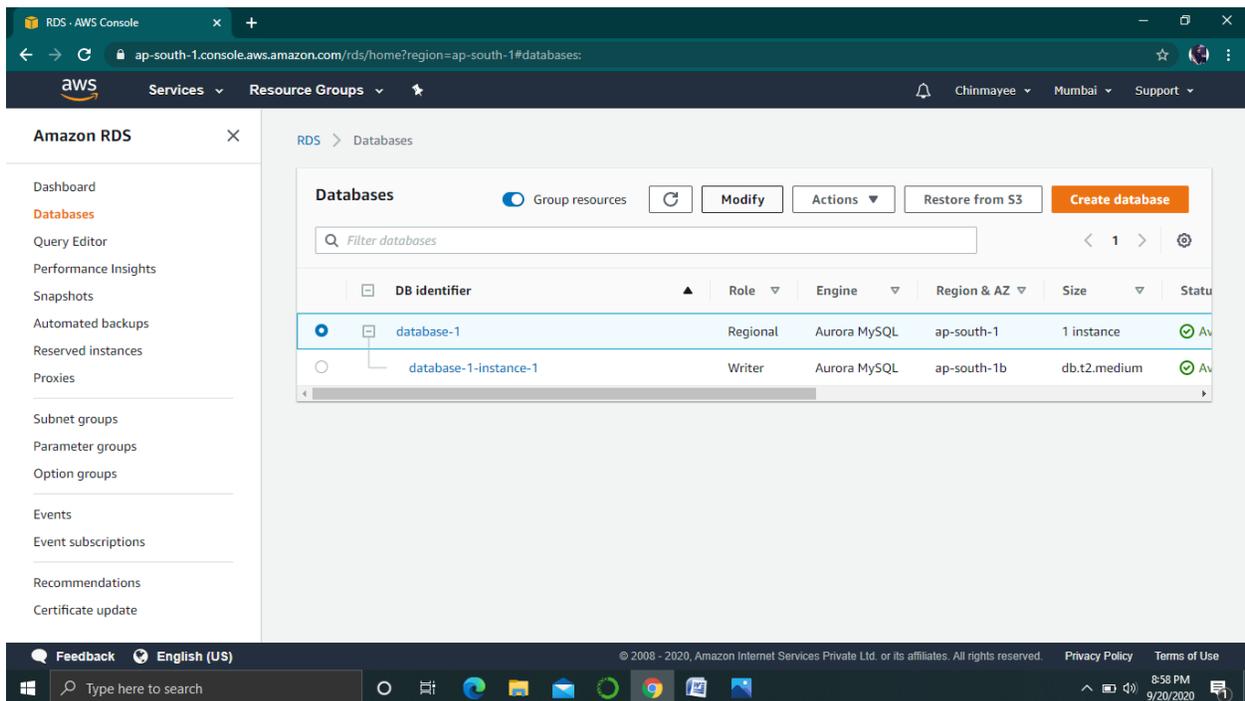
Step 12: Choose Create database to create your RDS AURORA DB instance.



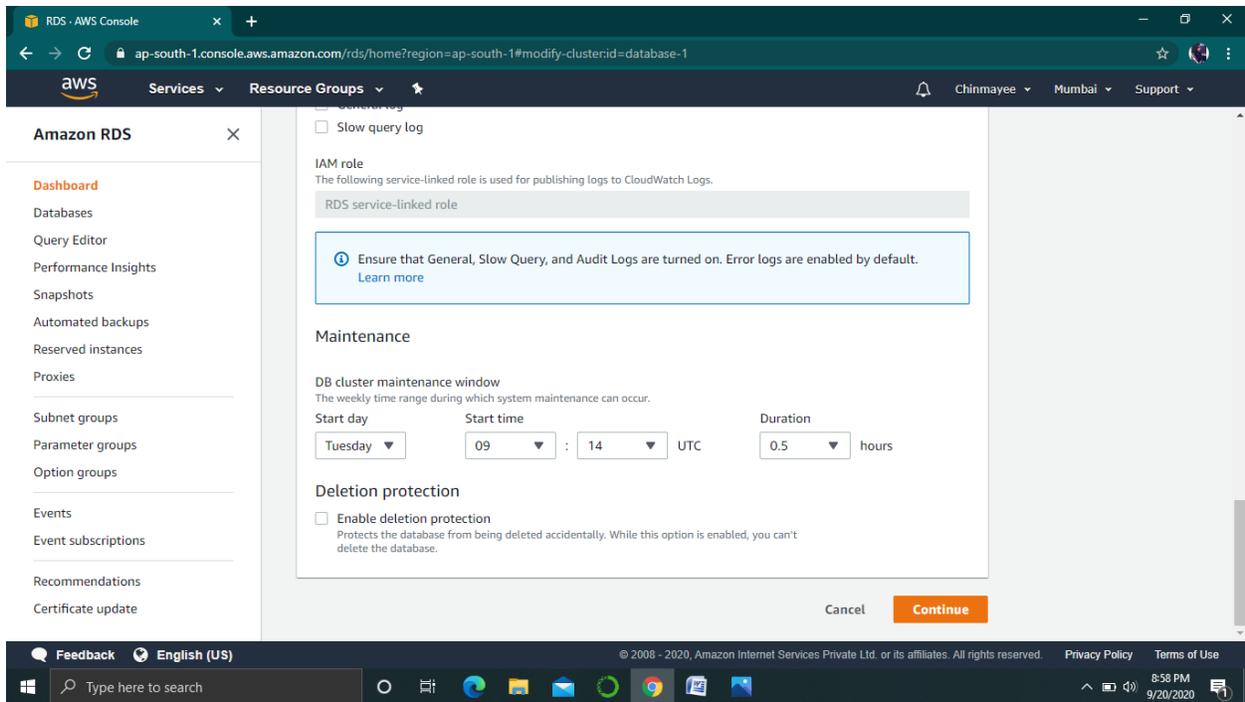
Step 13: Wait for the Status of your new DB instance to show as Available. Then choose the DB instance name to show its details.



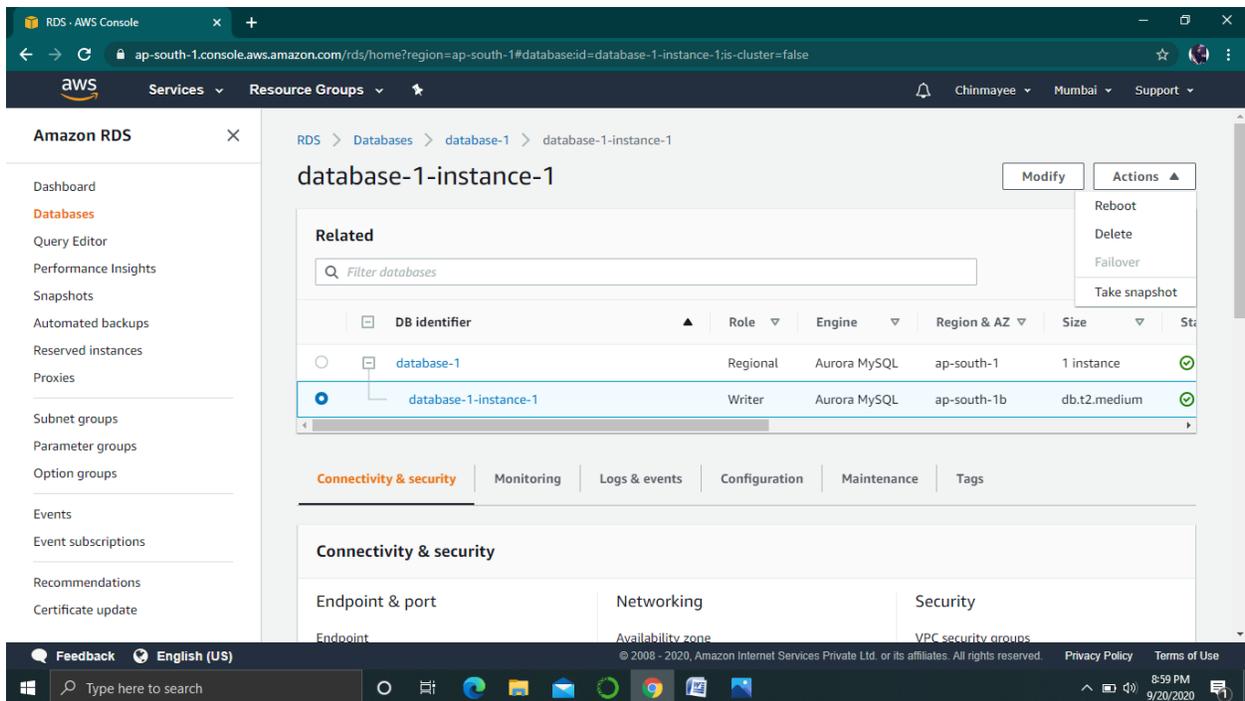
Step 14: Select the database from the dashboard and select modify.



Step 15: Disable the delete protection as we had enabled it previously and click on continue.



Step 16: Now again select the database instance from the dashboard and select actions and then click on delete.



Step 17: Confirm the dialog box for deletion.

RDS - AWS Console

ap-south-1.console.aws.amazon.com/rds/home?region=ap-south-1#databaseid=database-1-instance-1-is-cluster=false

Amazon RDS

Dashboard
Databases
Query Editor
Performance Insights
Snapshots
Automated backups
Reserved instances
Proxies
Subnet groups
Parameter groups
Option groups
Events
Event subscriptions
Recommendations
Certificate update

Delete database-1-instance-1 instance?

Are you sure you want to Delete the **database-1-instance-1** DB Instance?

Create final snapshot?
Determines whether a final DB Snapshot is created before the DB instance is deleted.

I acknowledge that upon instance deletion, automated backups, including system snapshots and point-in-time recovery, will no longer be available.

To confirm deletion, type *delete me* into the field

delete me

⚠ We strongly recommend taking a final snapshot before instance deletion since after your instance is deleted, automated backups will no longer be available.

Cancel Delete

Region & AZ	Size	St
ap-south-1	1 instance	✓
ap-south-1b	db.t2.medium	✓

© 2008 - 2020, Amazon Internet Services Private Ltd. or its affiliates. All rights reserved. Privacy Policy Terms of Use

8:59 PM 9/20/2020

CONFIGURE ELASTIC BLOCK STORE VOLUME

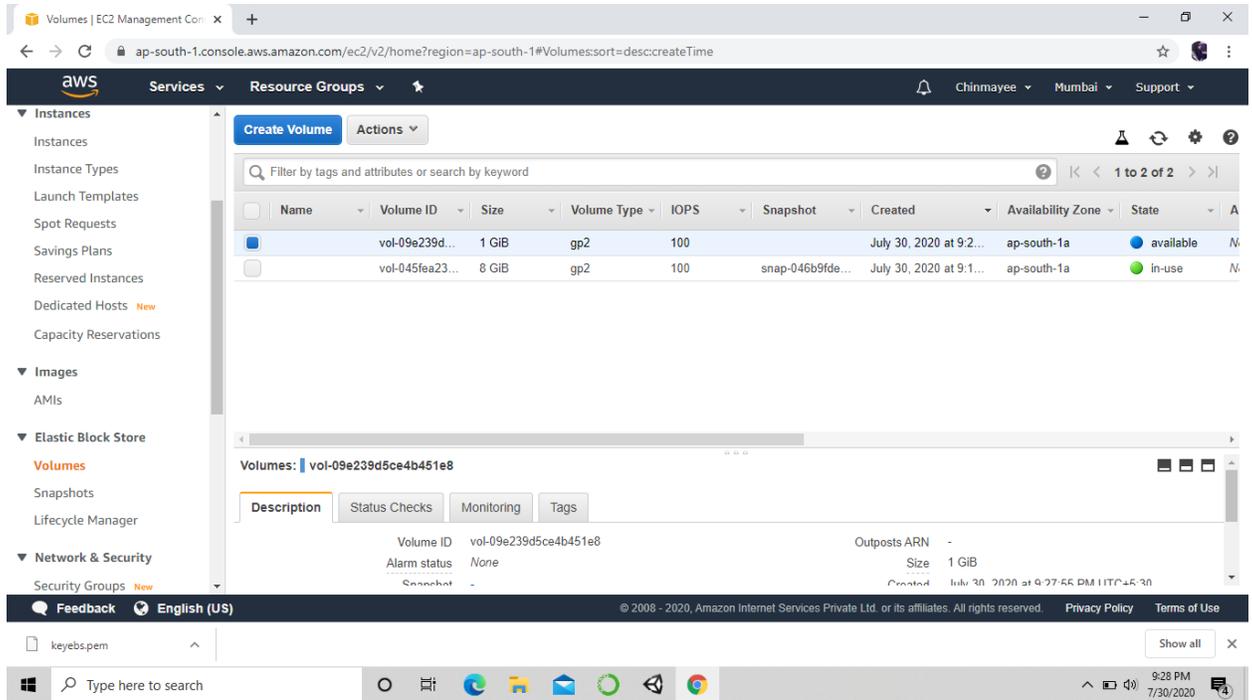
Step 1 – Create Amazon EBS volume using the following steps.

- Open the Amazon EC2 console.
- Select the region in the navigation bar where the volume is to be created.
- In the navigation pane, select Volumes, then select Create Volume.
- Provide the required information like Volume Type list, Size, IOPS, Availability zone, etc. then click the Create button.
- The volume names can be seen in the volumes list.

The screenshot displays the 'Create Volume' interface in the AWS Management Console. The configuration is as follows:

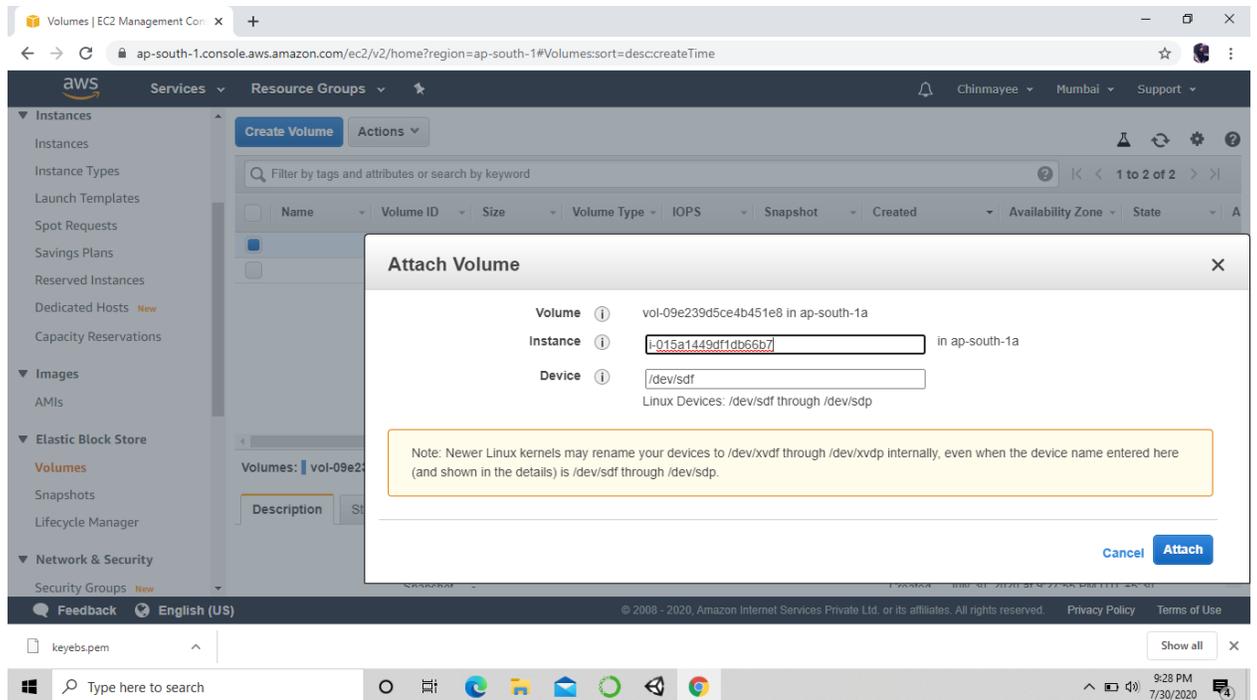
- Volume Type:** General Purpose SSD (gp2)
- Size (GiB):** 1 (Range: Min: 1 GiB, Max: 16384 GiB)
- IOPS:** 300 / 3000 (Baseline of 3 IOPS per GiB with a minimum of 100 IOPS, burstable to 3000 IOPS)
- Availability Zone:** ap-south-1a
- Throughput (MB/s):** Not applicable
- Snapshot ID:** Select a snapshot
- Encryption:** Encrypt this volume

At the bottom, there are fields for 'Key' (128 characters maximum) and 'Value' (256 characters maximum). The footer contains 'Feedback', 'English (US)', and copyright information: '© 2008 - 2020, Amazon Internet Services Private Ltd. or its affiliates. All rights reserved. Privacy Policy Terms of Use'.



Step 2 – Attach EBS Volume to an Instance using the following steps.

- Open the Amazon EC2 console.
- Select Volumes in the navigation pane. Choose a volume and click the Attach Volume option.
- An Attach Volume dialog box will open. Enter the name/ID of instance to attach the volume in the Instance field or select it from the list of suggestion options.
- Click the Attach button.
- Connect to instance and make the volume available.

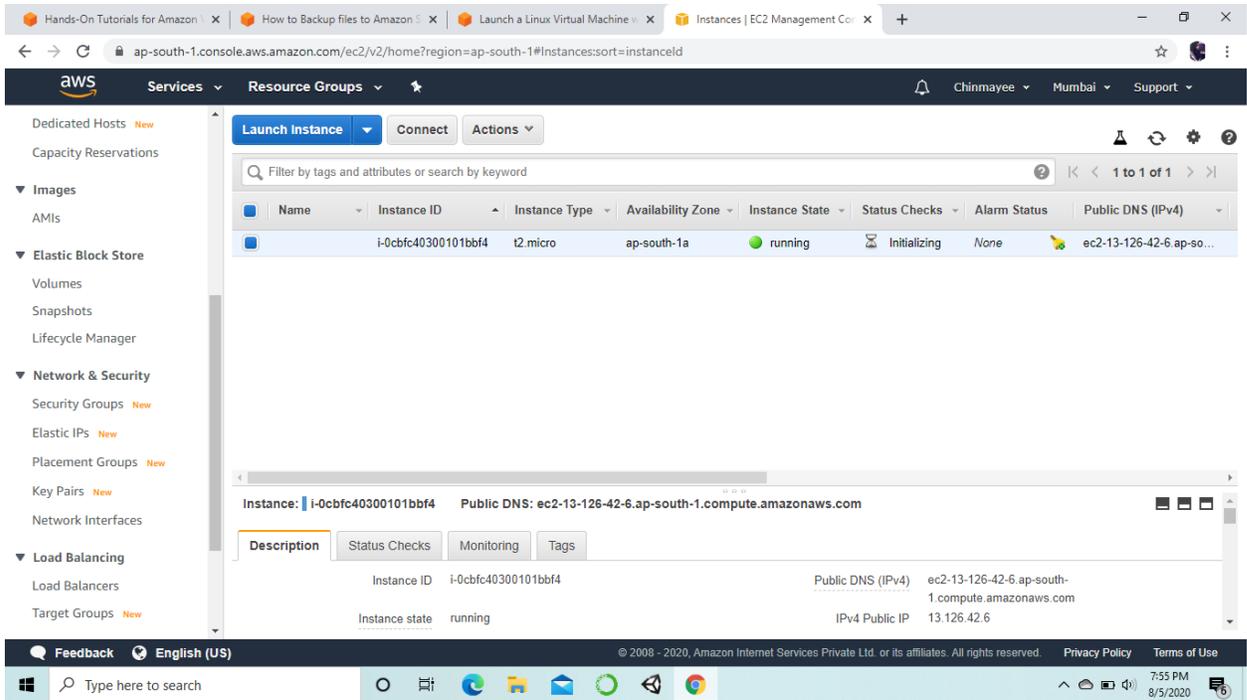


Step 3 – Detach a volume from Instance.

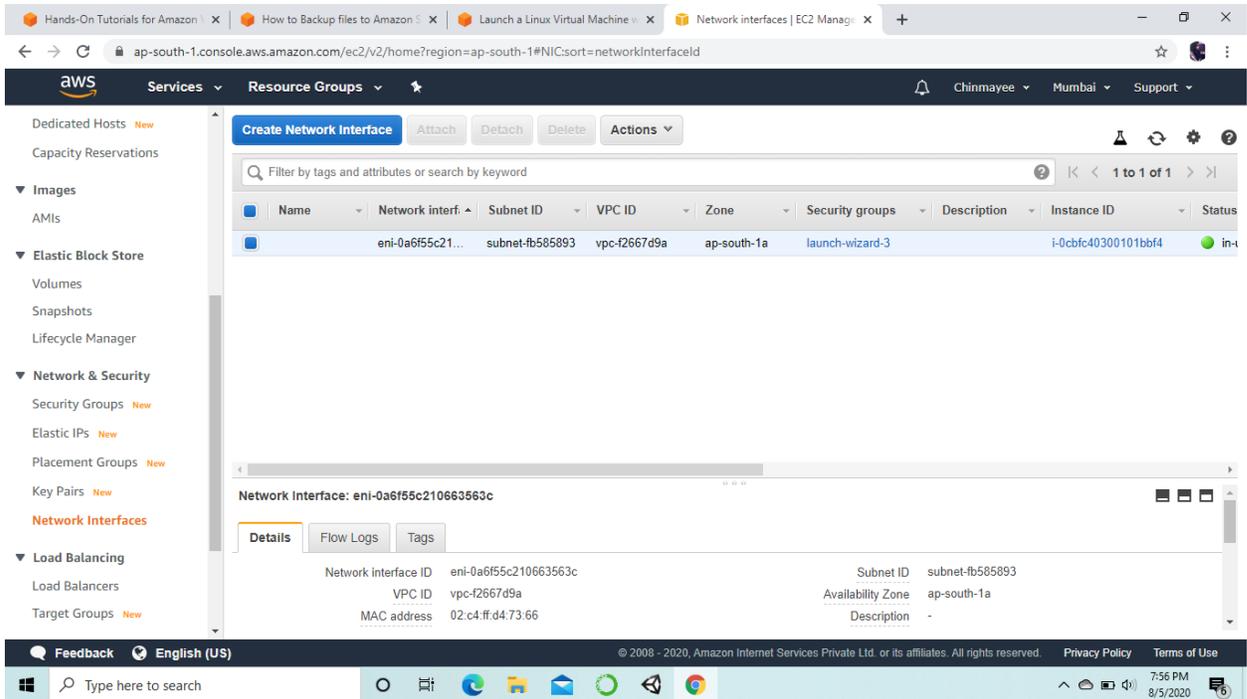
- First, use the command `/dev/sdf` in `cmd` to unmount the device.
- Open the Amazon EC2 console.
- In the navigation pane, select the Volumes option.
- Choose a volume and click the Detach Volumes option.
- A confirmation dialog box opens. Click the Yes, Detach button to confirm.

GENERATE PRIVATE IP FOR EC2 INSTANCE

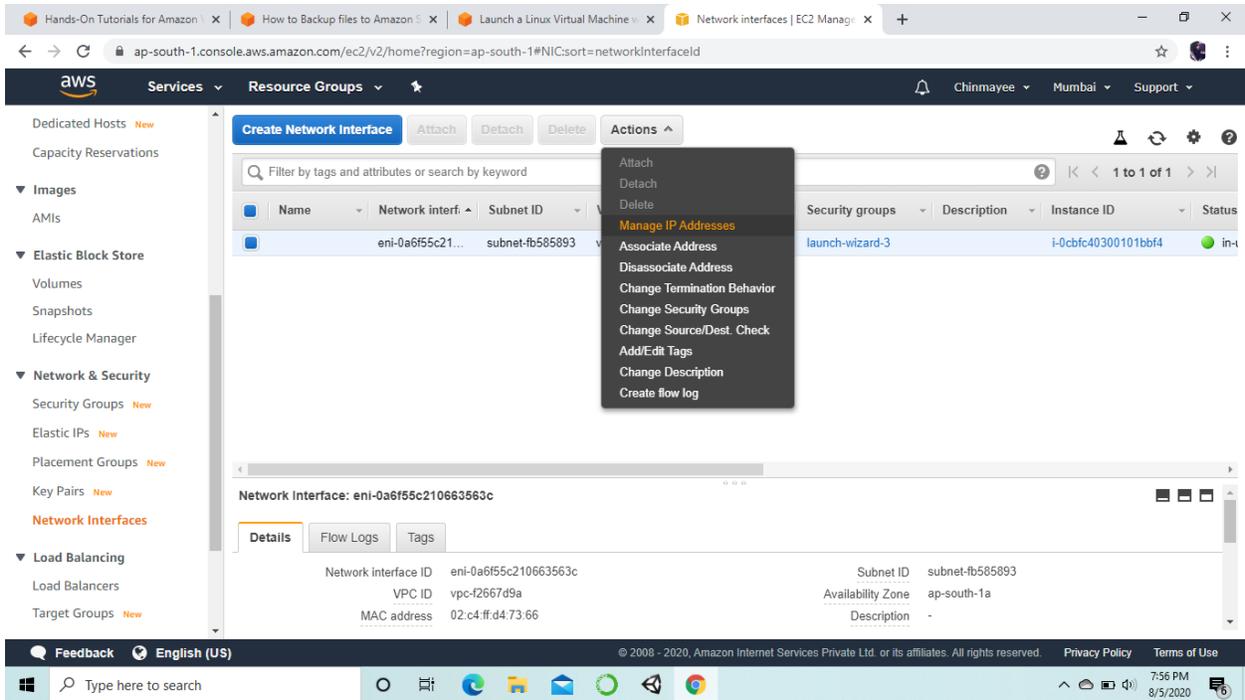
1. Login to AWS console.
2. Open the EC2 service and launch an instance.



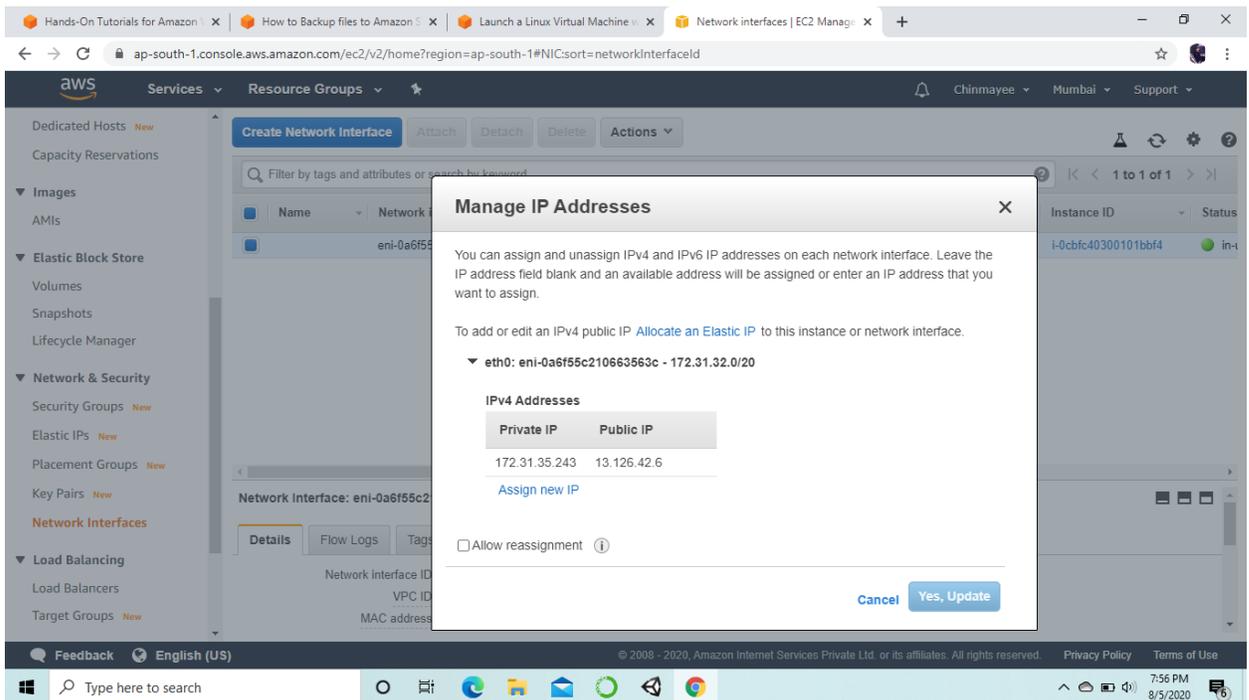
3. Under the Network and security from the dashboard, choose Network Interfaces.

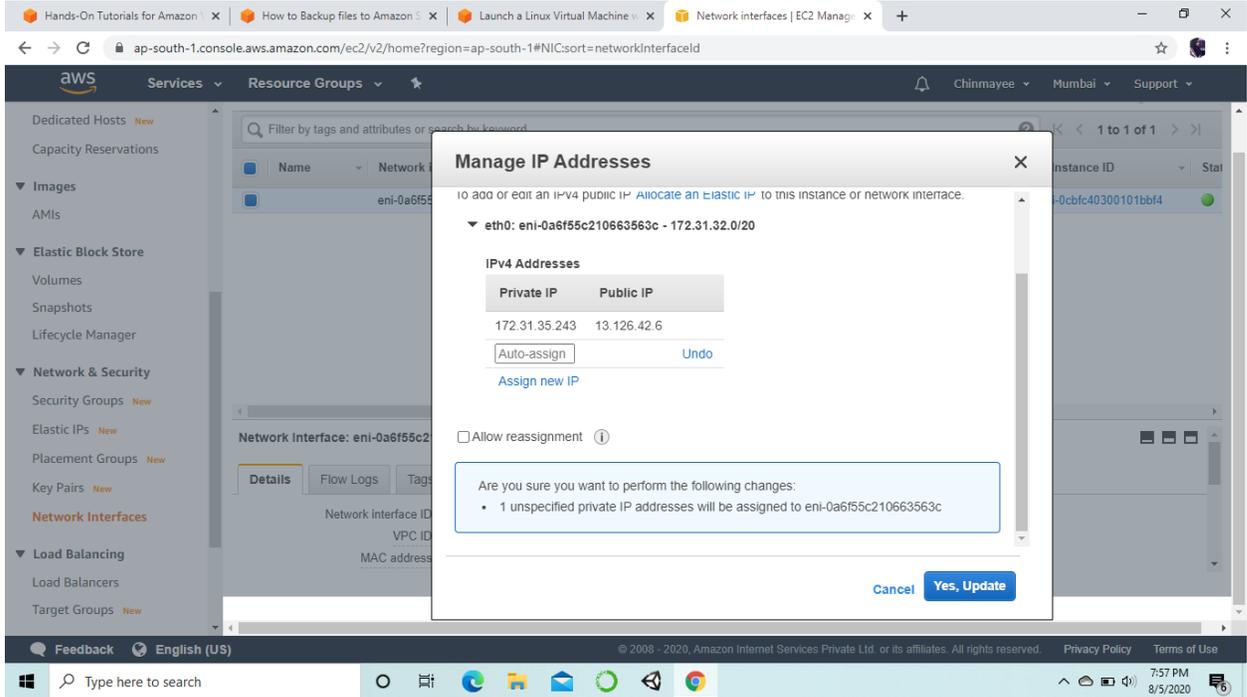


4. Choose Actions, and then choose Manage IP Addresses.

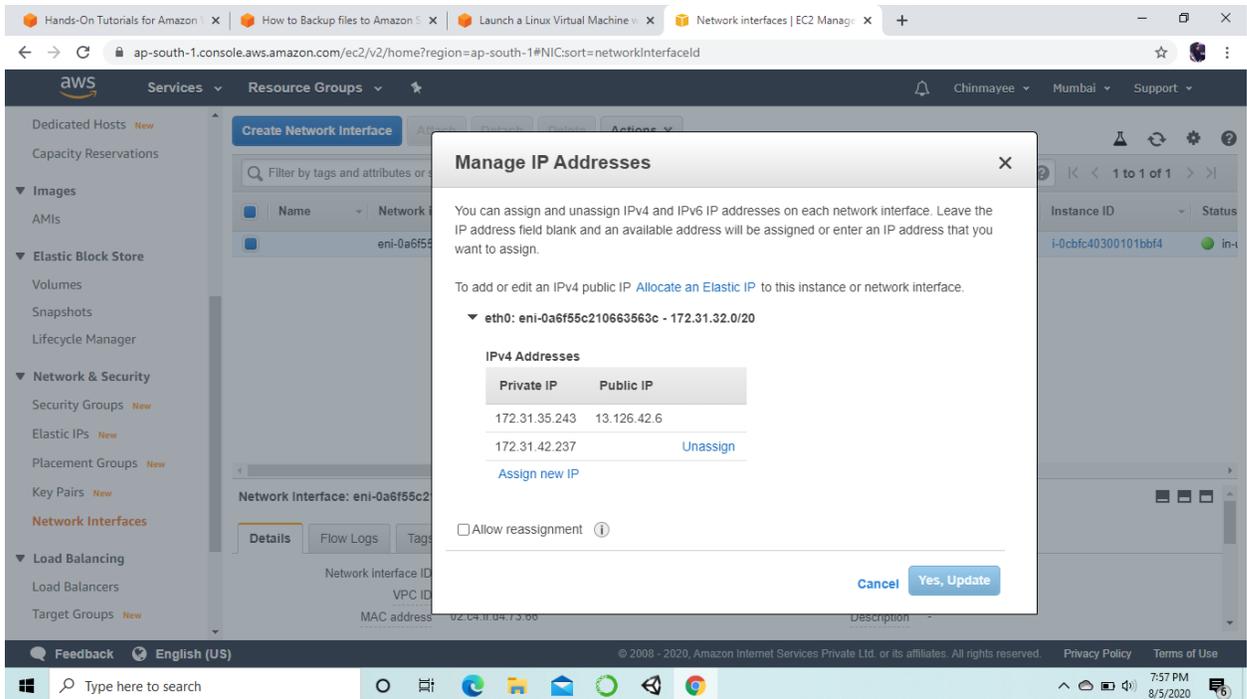


5. Assign new IP automatically.





6. Choose Yes, Update.



7. Secondary private IP is created successfully.

Hands-On Tutorials for Amazon | How to Backup files to Amazon | Launch a Linux Virtual Machine | Network interfaces | EC2 Manage

ap-south-1.console.aws.amazon.com/ec2/v2/home?region=ap-south-1#NIC:sort=networkInterfaceId

Services Resource Groups Chinmayee Mumbai Support

Dedicated Hosts **New**
Capacity Reservations

▼ Images
AMIs

▼ Elastic Block Store
Volumes
Snapshots
Lifecycle Manager

▼ Network & Security
Security Groups **New**
Elastic IPs **New**
Placement Groups **New**
Key Pairs **New**
Network Interfaces

▼ Load Balancing
Load Balancers
Target Groups **New**

Create Network Interface Attach Detach Delete Actions

Filter by tags and attributes or search by keyword

ID	Status	IPv4 Public IP	Primary private	Secondary private IPv4	IPv6 IPs	Network interface owner	Outpost ID
eni-0101bbf4	in-use	13.126.42.6*	172.31.35.243	172.31.42.237	-	914536736193	-

Network Interface: eni-0a6f55c210663563c

Details Flow Logs Tags

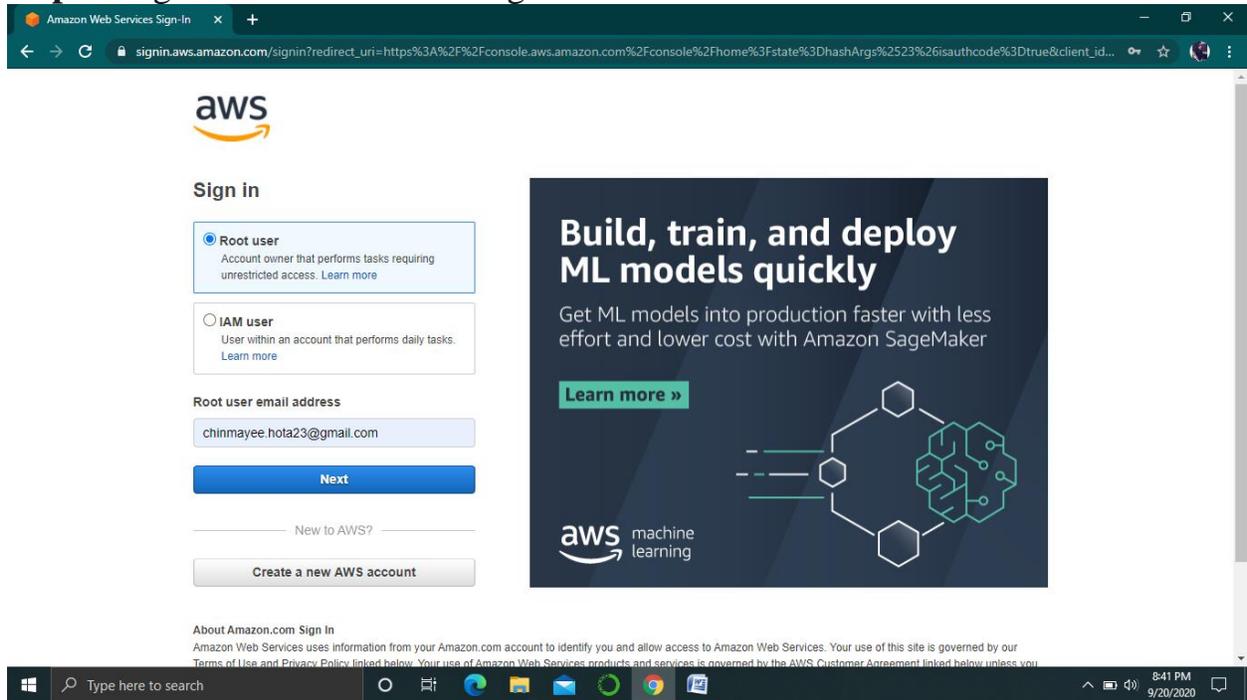
Network interface ID	eni-0a6f55c210663563c	Subnet ID	subnet-fb585893
VPC ID	vpc-f2667d9a	Availability Zone	ap-south-1a
MAC address	02:c4:ff:d4:73:66	Description	-

Feedback English (US) © 2008 - 2020, Amazon Internet Services Private Ltd. or its affiliates. All rights reserved. Privacy Policy Terms of Use

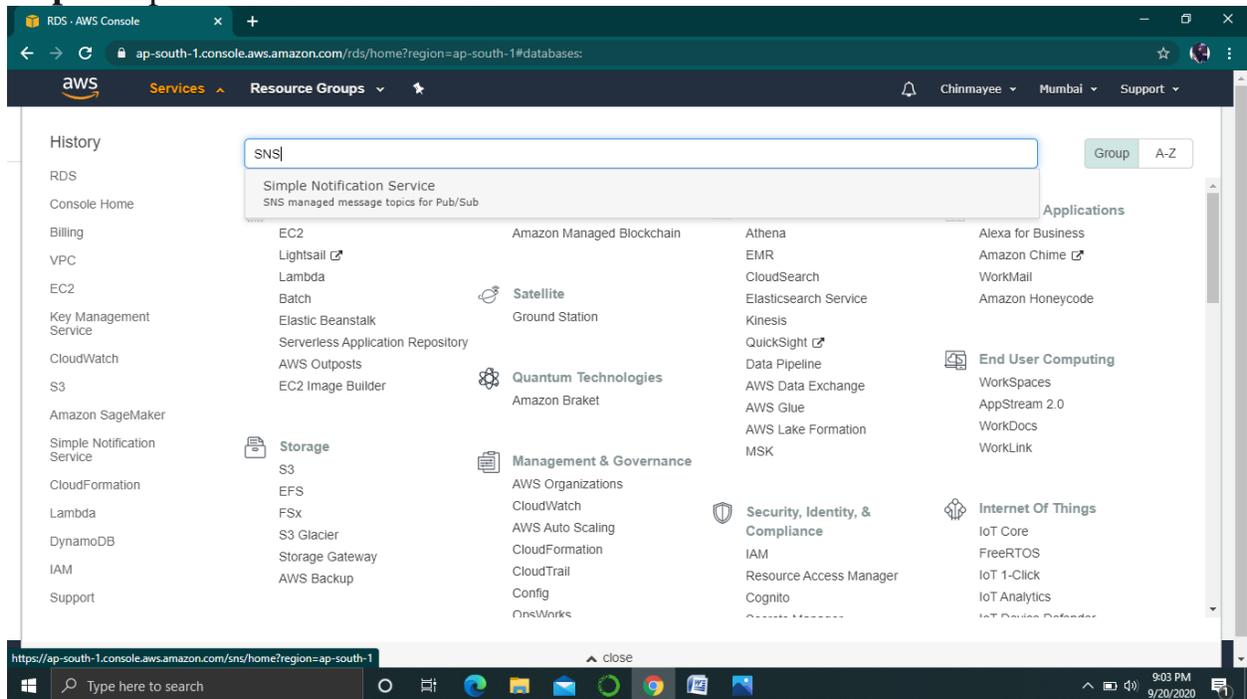
Type here to search 7:57 PM 8/5/2020

AMAZON SNS

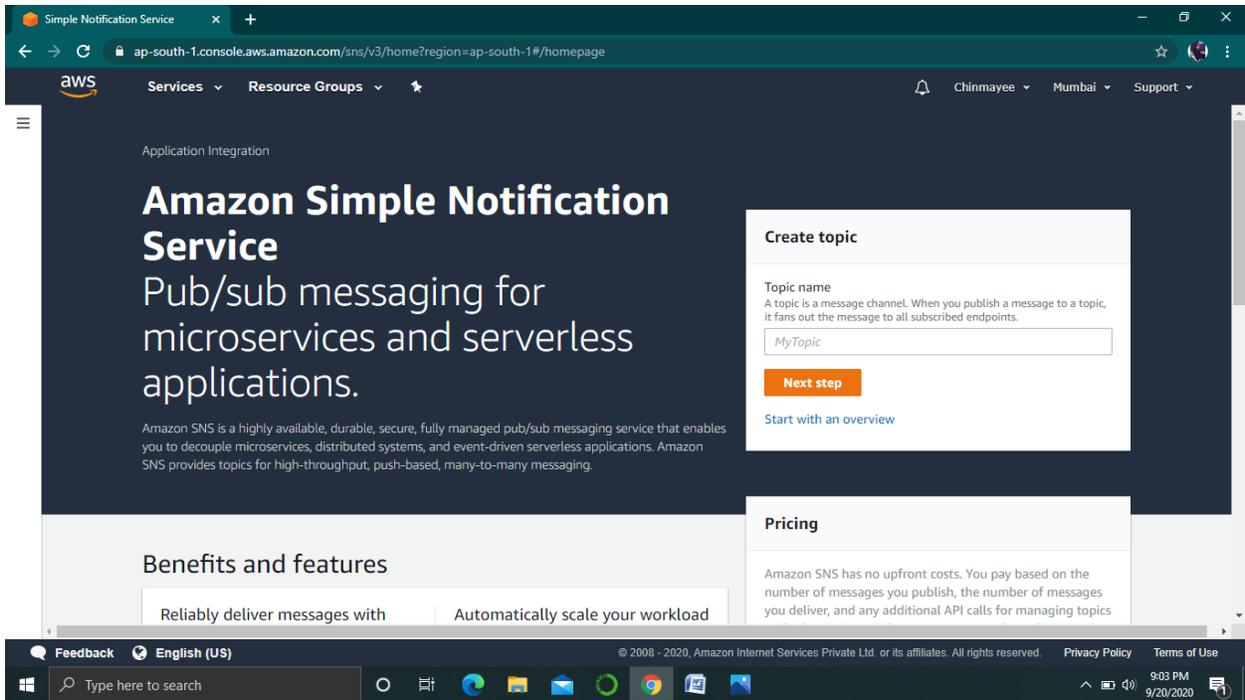
Step 1: Sign in to the AWS Management Console.



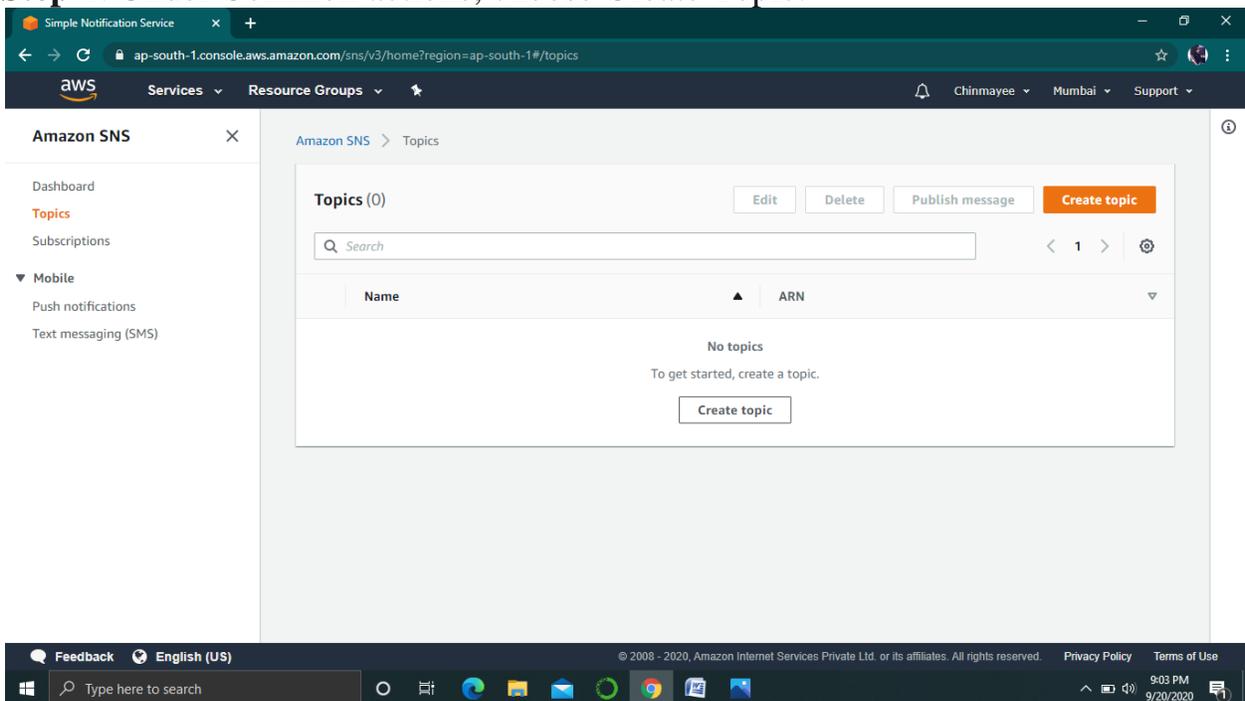
Step 2: Open the service as SNS.



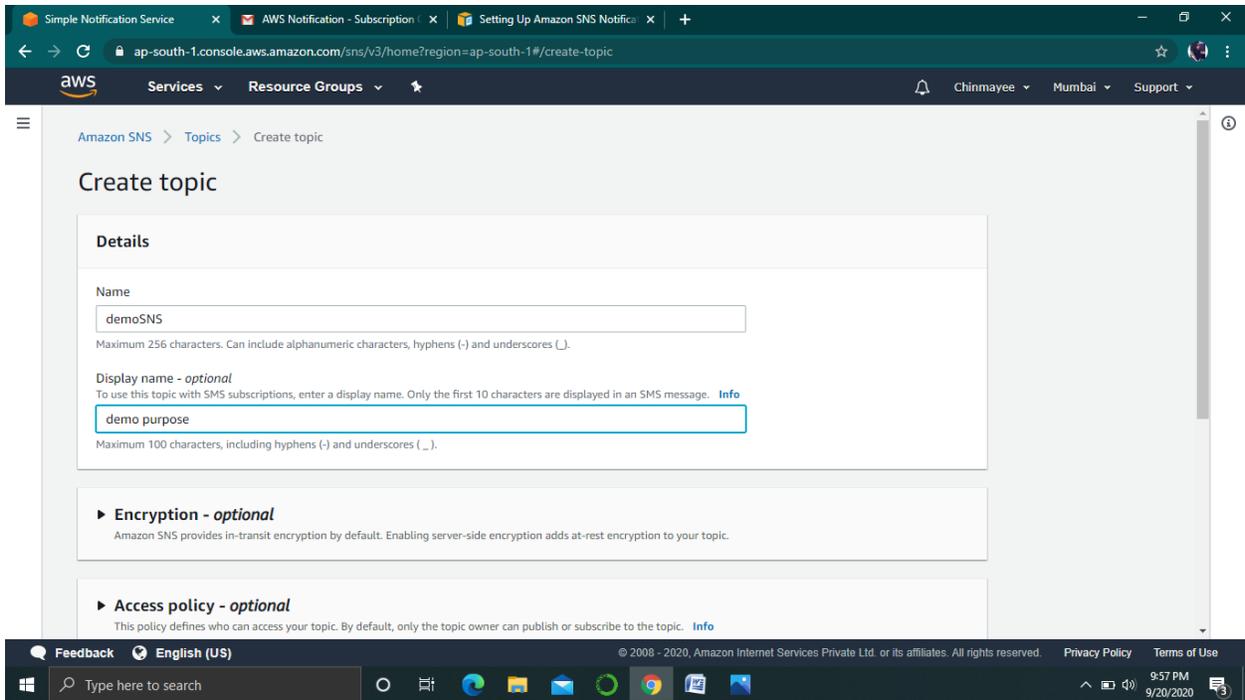
Step 3: The Amazon SNS dashboard will appear as.



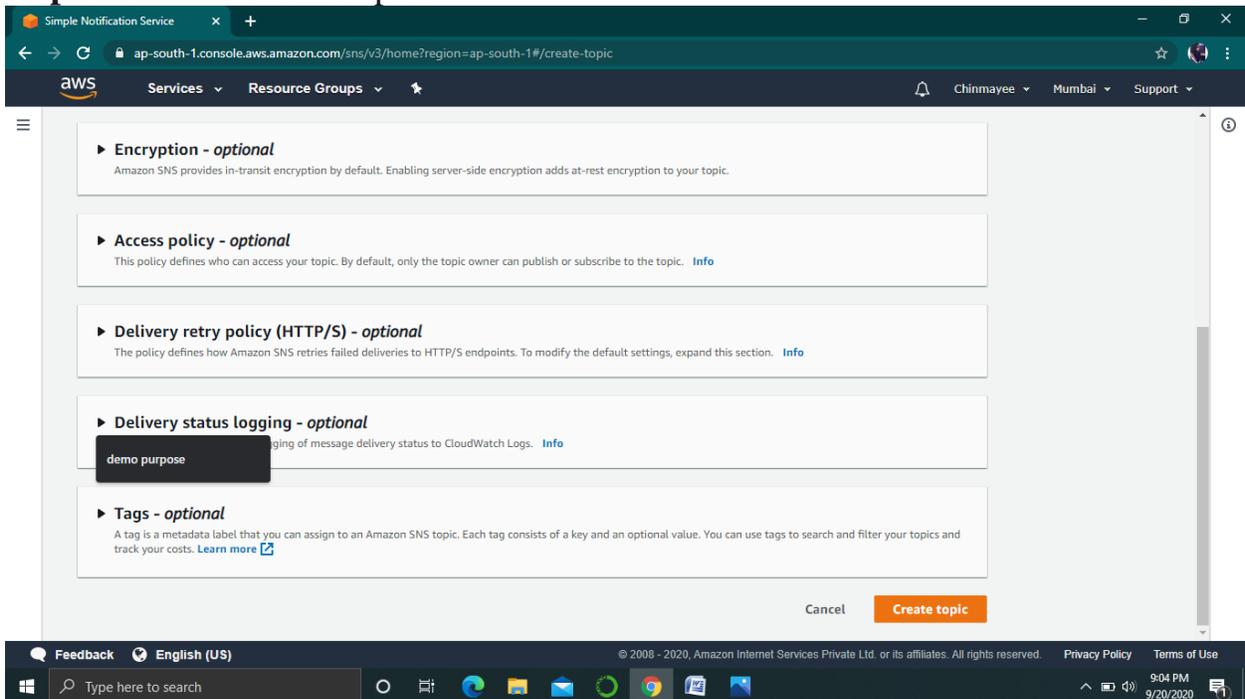
Step 4: Under Common actions, choose Create Topic.



Step 5: In the Create new topic dialog box, for Topic name, enter a name for the topic.

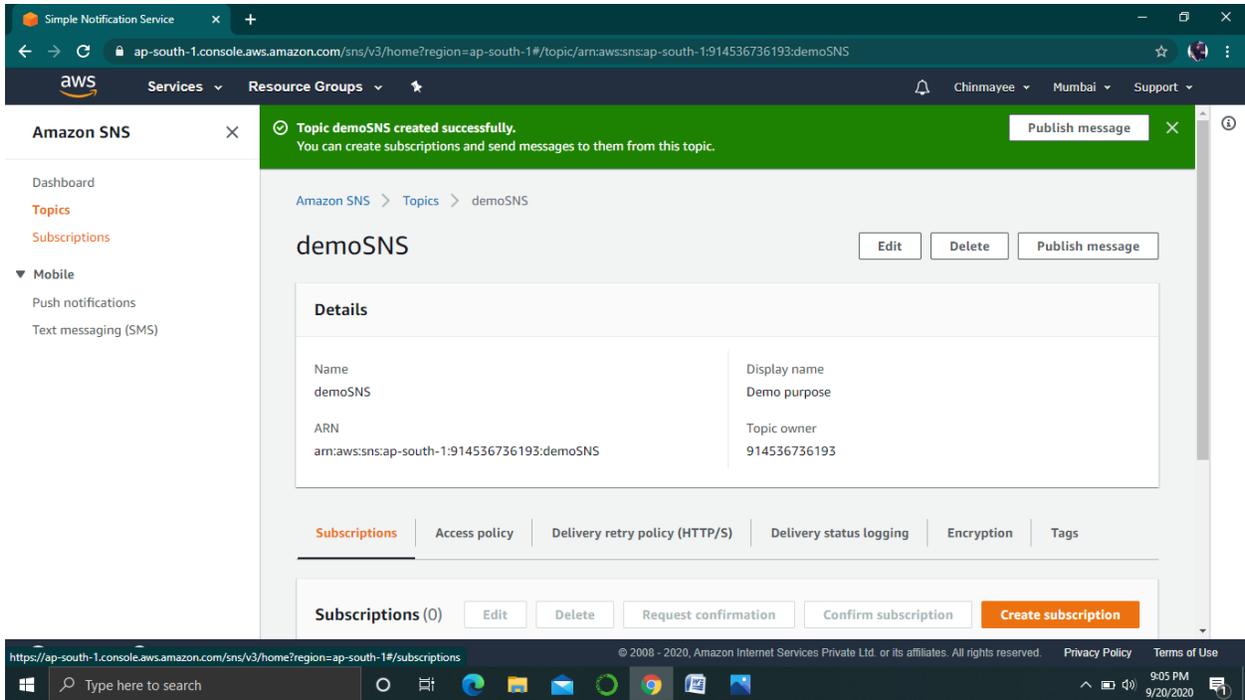


Step 6: Choose Create topic.



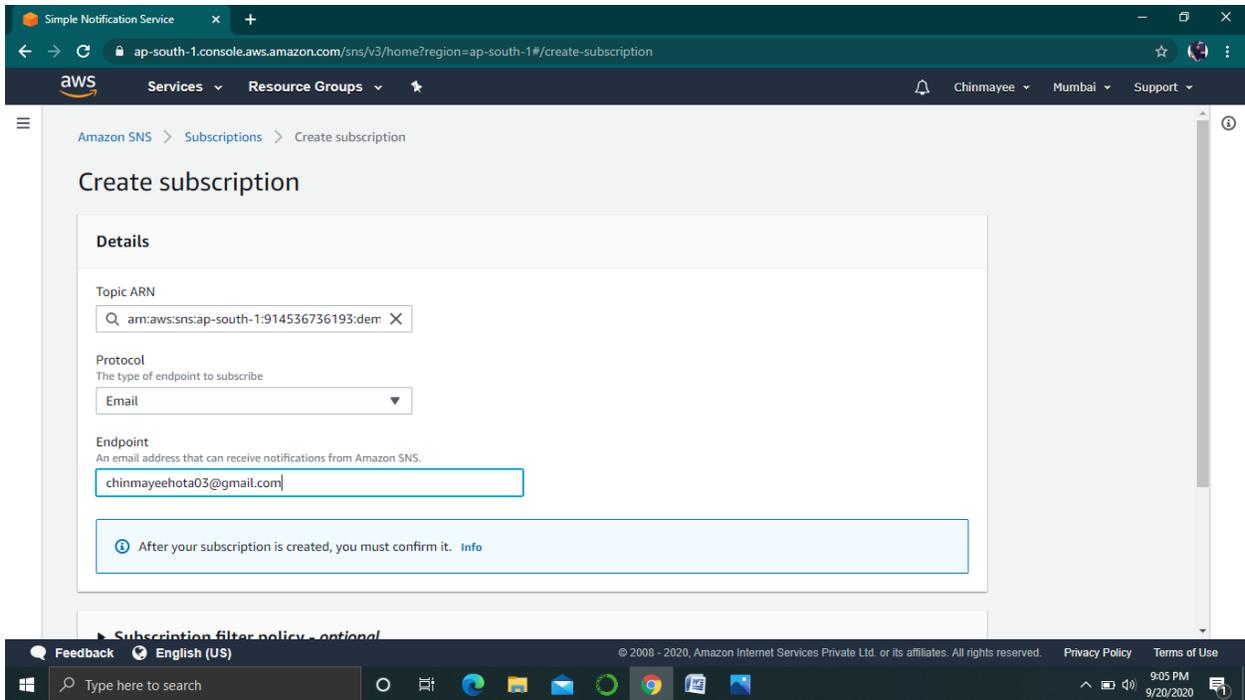
Step 7: Copy the Topic ARN for the next task.

Step 8: Check the status of the topic.

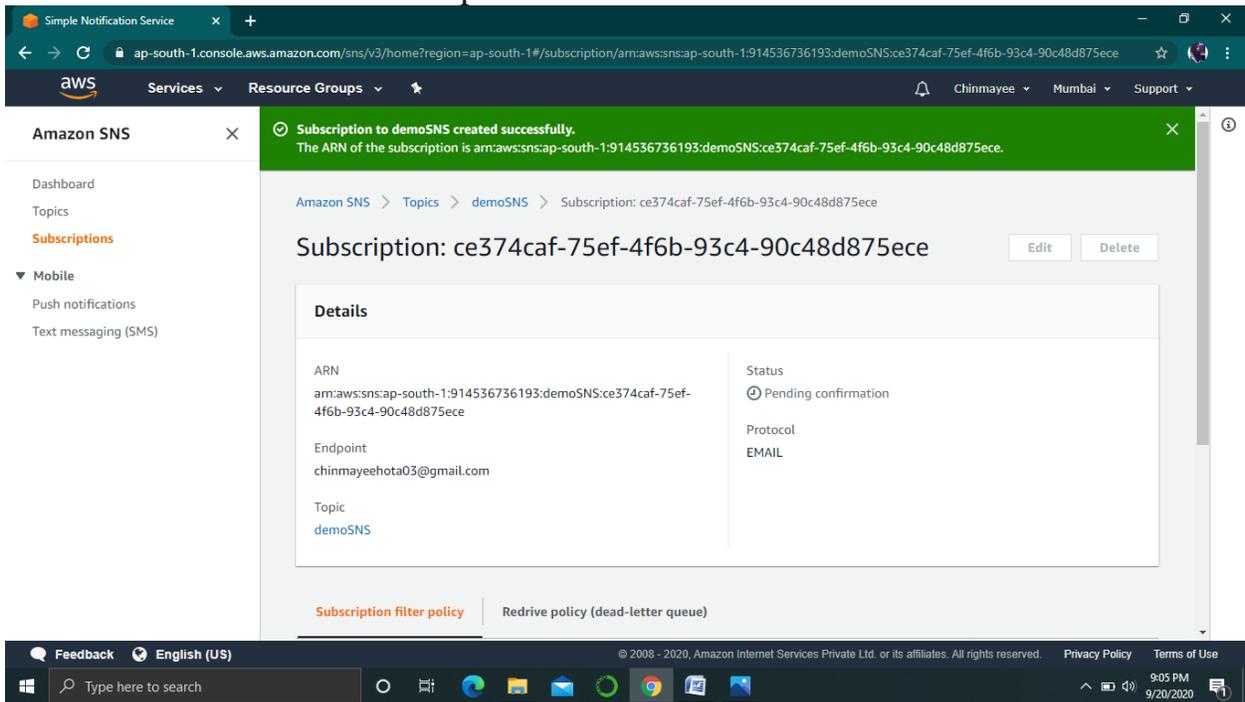


TO SUBSCRIBE TO AN SNS TOPIC

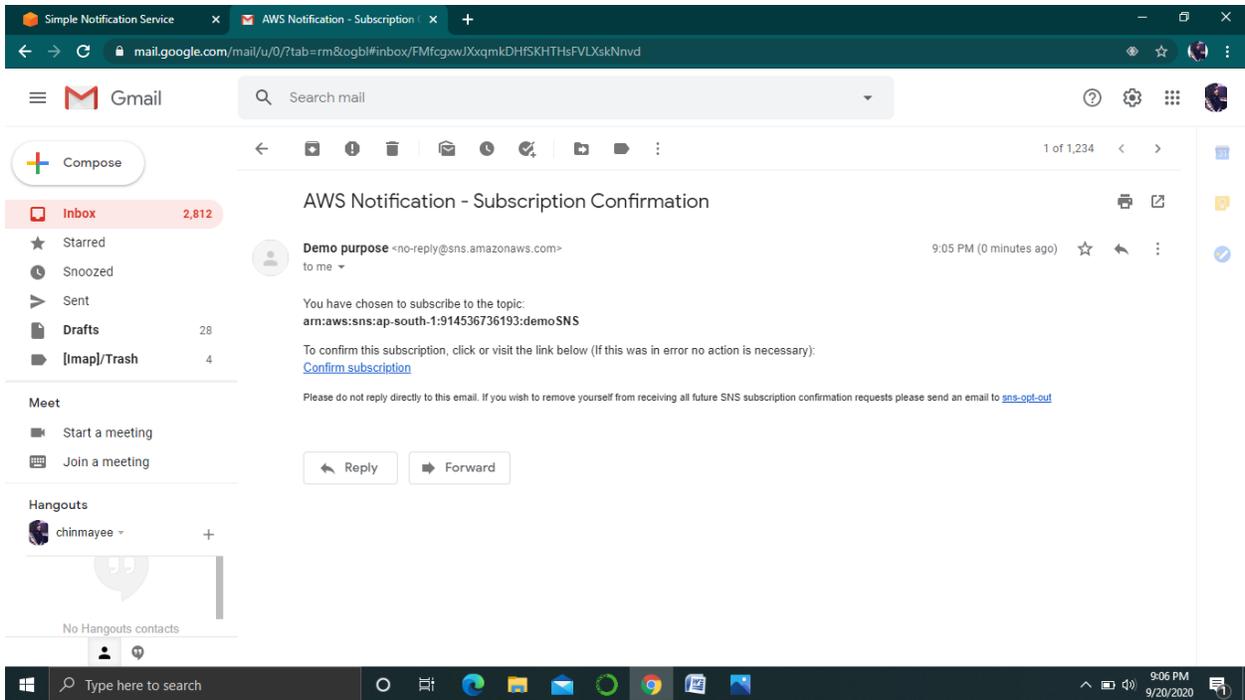
1. In the navigation pane, choose Subscriptions, Create subscription.
2. In the Create subscription dialog box, for Topic ARN, paste the topic ARN that you created in the previous task.
3. For Protocol, choose Email.



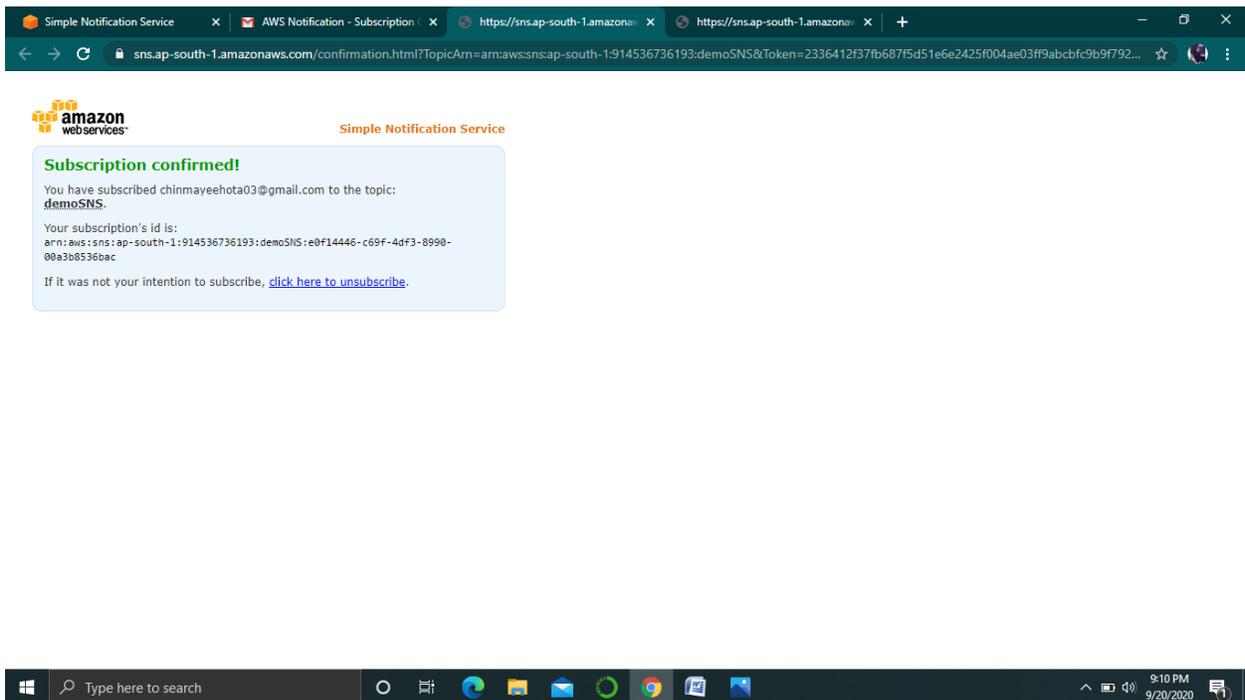
4. For Endpoint, enter an email address that you can use to receive the notification, and then choose Create subscription.



5. From your email application, open the message from AWS Notifications and confirm your subscription.



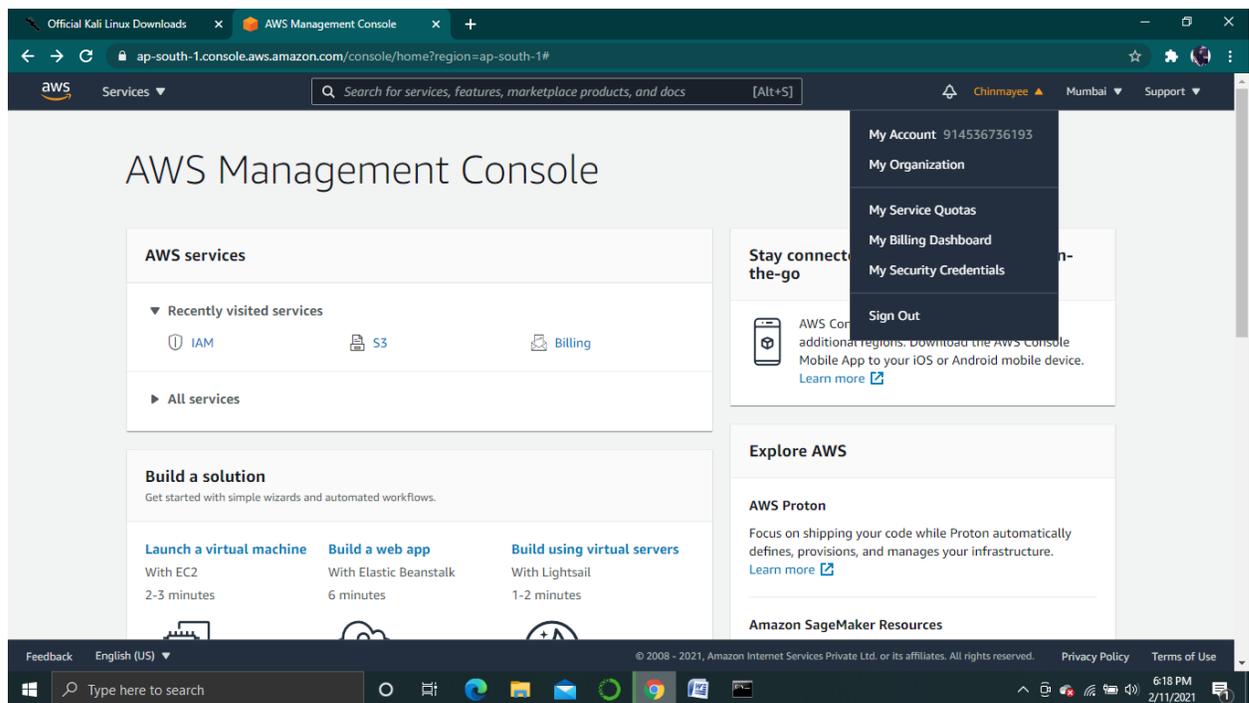
6. Your web browser displays a confirmation response from Amazon SNS.



AWS CLI FOR BUCKET CREATION

Steps to be followed:-

- 1st download AWS CLI MSI installer for Windows
- Install and run MSI installer
- Now in the search bar of your computer or laptop search for cmd to open command prompt in window.
- Now in the command prompt write a command (**aws --version**)
- Now again write a command (**aws configure**) , after enter the command it will ask for access key.
- So for access key we have to go to AWS Management Console.
- Then in the account info go to **My Security Credentials**.



- Under security credentials it has a column of Access and secret key.
- Click on Create New Access Key.

Identity and Access Management (IAM)

Dashboard

- Access management
 - Groups
 - Users
 - Roles
 - Policies
 - Identity providers
 - Account settings
- Access reports
 - Access analyzer
 - Archive rules
 - Analyzers
 - Settings
 - Credential report
 - Organization activity

Your Security Credentials

Use this page to manage the credentials for your AWS account. To manage credentials for AWS Identity and Access Management (IAM) users, use the IAM Console.

To learn more about the types of AWS credentials and how they're used, see [AWS Security Credentials](#) in AWS General Reference.

- ▲ Password
- ▲ Multi-factor authentication (MFA)
- ▼ Access keys (access key ID and secret access key)

Use access keys to make programmatic calls to AWS from the AWS CLI, Tools for PowerShell, AWS SDKs, or direct AWS API calls. You can have a maximum of two access keys (active or inactive) at a time.

For your protection, you should never share your secret keys with anyone. As a best practice, we recommend frequent key rotation.

If you lose or forget your secret key, you cannot retrieve it. Instead, create a new access key and make the old key inactive. [Learn more](#)

Created	Access Key ID	Last Used	Last Used Region	Last Used Service	Status	Actions
Jan 31st 2021	AKIAJPX4PJPHIXOLG76A	2021-02-06 13:42 UTC+0530	ap-south-1	s3	Active	Make Inactive Delete

[Create New Access Key](#)

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](#)

- Here is the Access key and Secret Key.
- Now 1st copy the Access Key and paste in the command prompt.
- Again copy Secret Key and paste it in Command prompt.
- Then it will ask for Region. So in region give the region name as **ap-south-1**.

Create Access Key

✔ Your access key (access key ID and secret access key) has been created successfully.

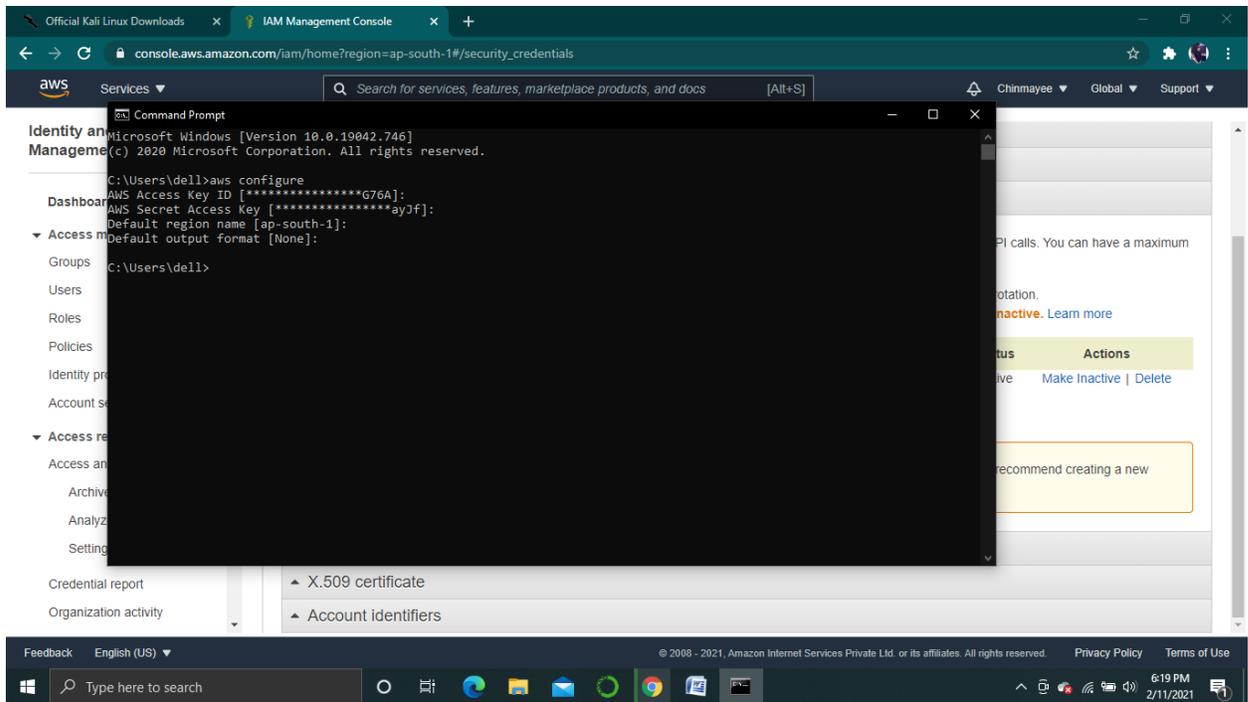
Download your key file now, which contains your new access key ID and secret access key. If you do not download the key file now, you will not be able to retrieve your secret access key again.

To help protect your security, store your secret access key securely and do not share it.

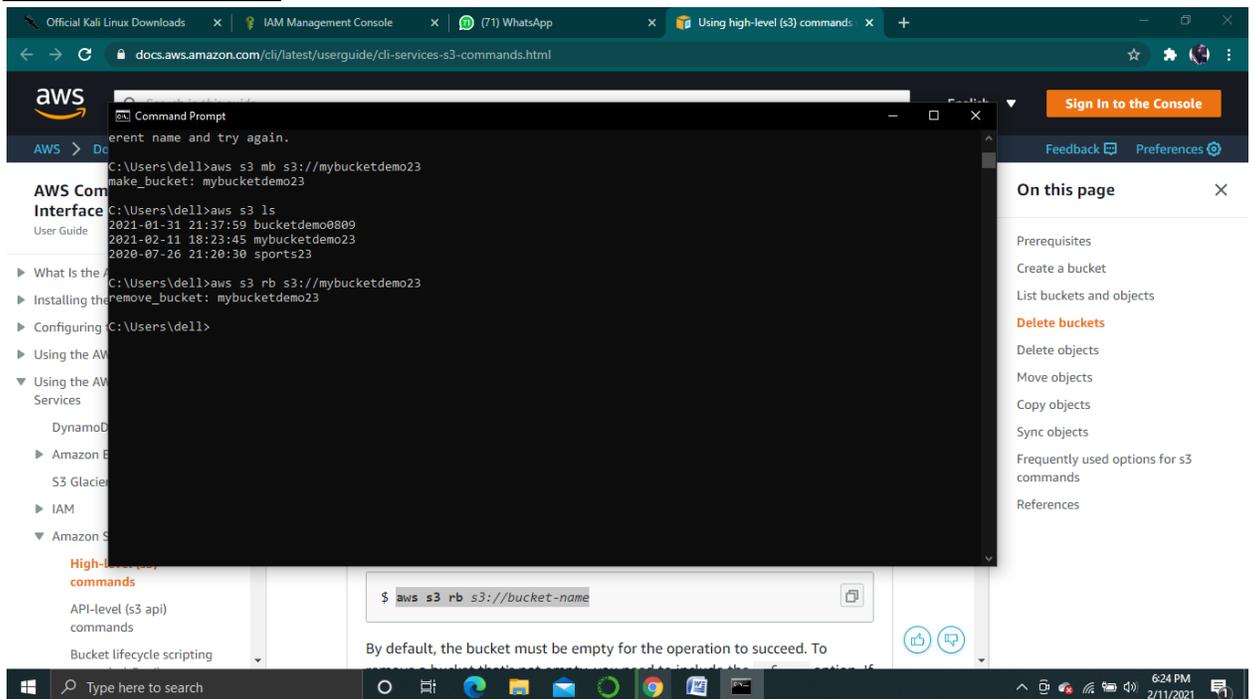
▼ Hide Access Key

Access Key ID: AKIAICYPPRCVLA7JFRPQ
Secret Access Key: NA7dD+KwRyMgs+pQ1b1zmtnHnfr9CNtWa/8a/JP

[Download Key File](#) [Close](#)

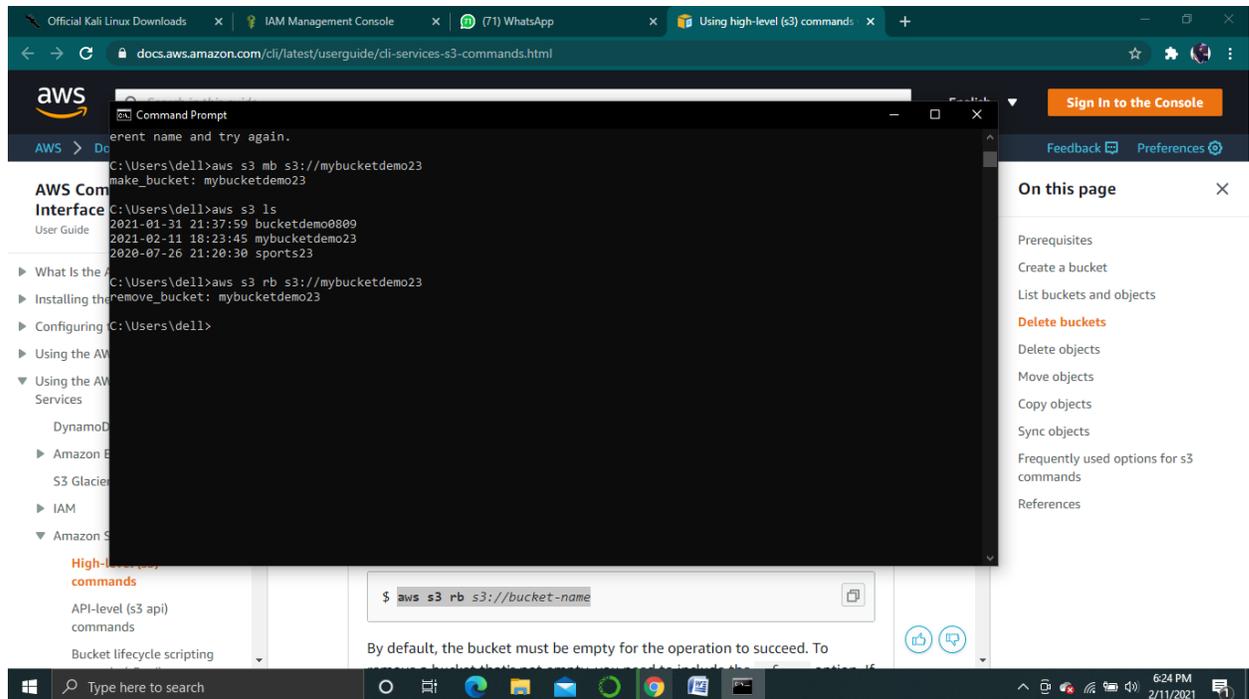


- Now to make or create a bucket we need to execute a command **aws s3 mb s3://bucket_name**



- Simultaneously check that the bucket is created in S3 service.
- Now to confirm in command prompt write a command **aws s3 ls**, it will show you all the buckets present in the s3 service.

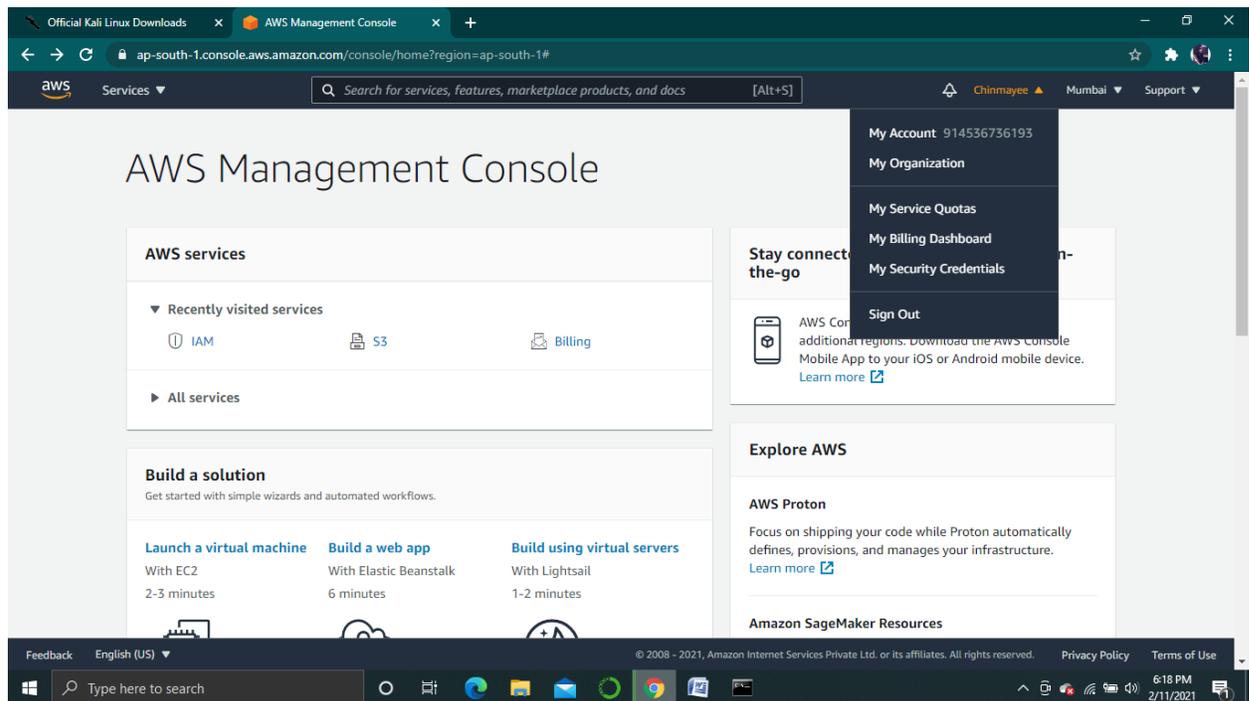
- Now Again to remove or delete the bucket execute a command **aws s3 rb s3://bucket_name**.
- Now check in the s3 service that the bucket is removed or not.
- In command prompt write command `aws s3 ls` to confirm that the bucket is deleted.



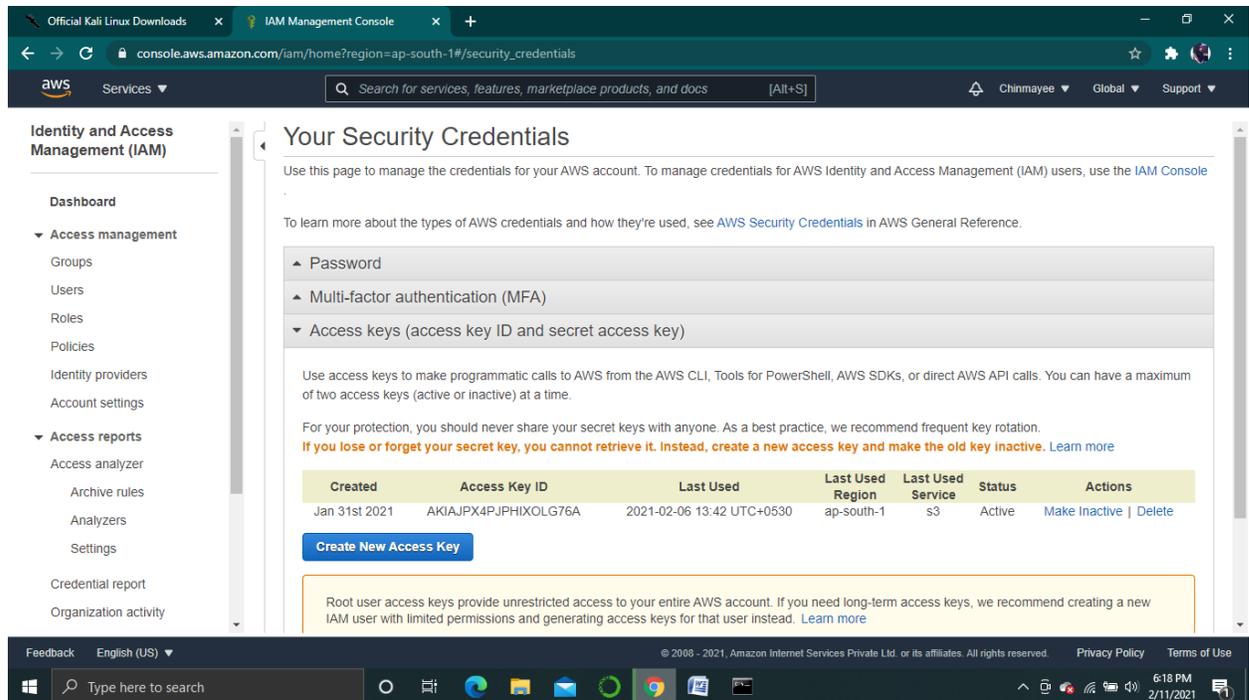
AWS CLI SETUP AND CONFIGURATION ON WINDOWS

Steps to be followed:-

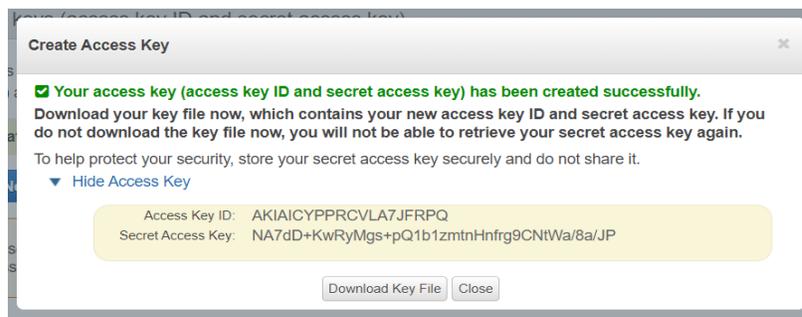
- 1st download AWS CLI MSI installer for Windows
- Install and run MSI installer
- Now in the search bar of your computer or laptop search for cmd to open command prompt in window.
- Now in the command prompt write a command (**aws --version**)
- Now again write a command (**aws configure**) , after enter the command it will ask for access key.
- So for access key we have to go to AWS Management Console.
- Then in the account info go to **My Security Credentials**.

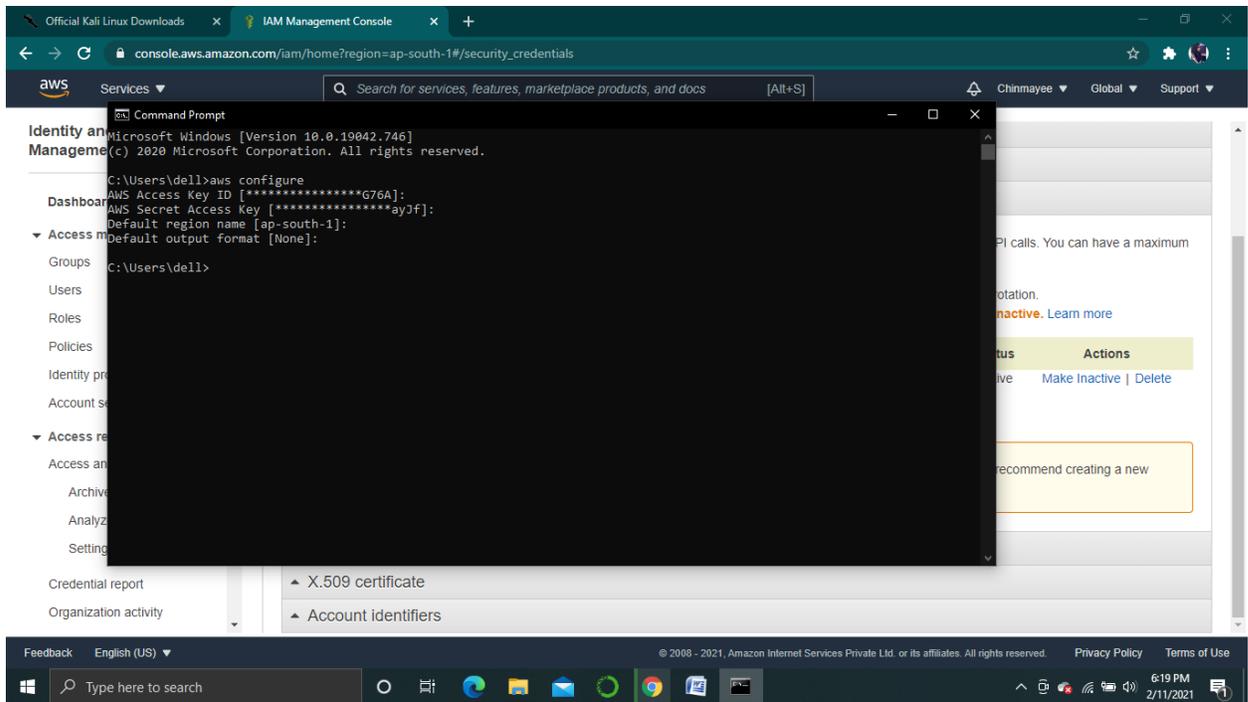


- Under security credentials it has a column of Access and secret key.
- Click on Create New Access Key.

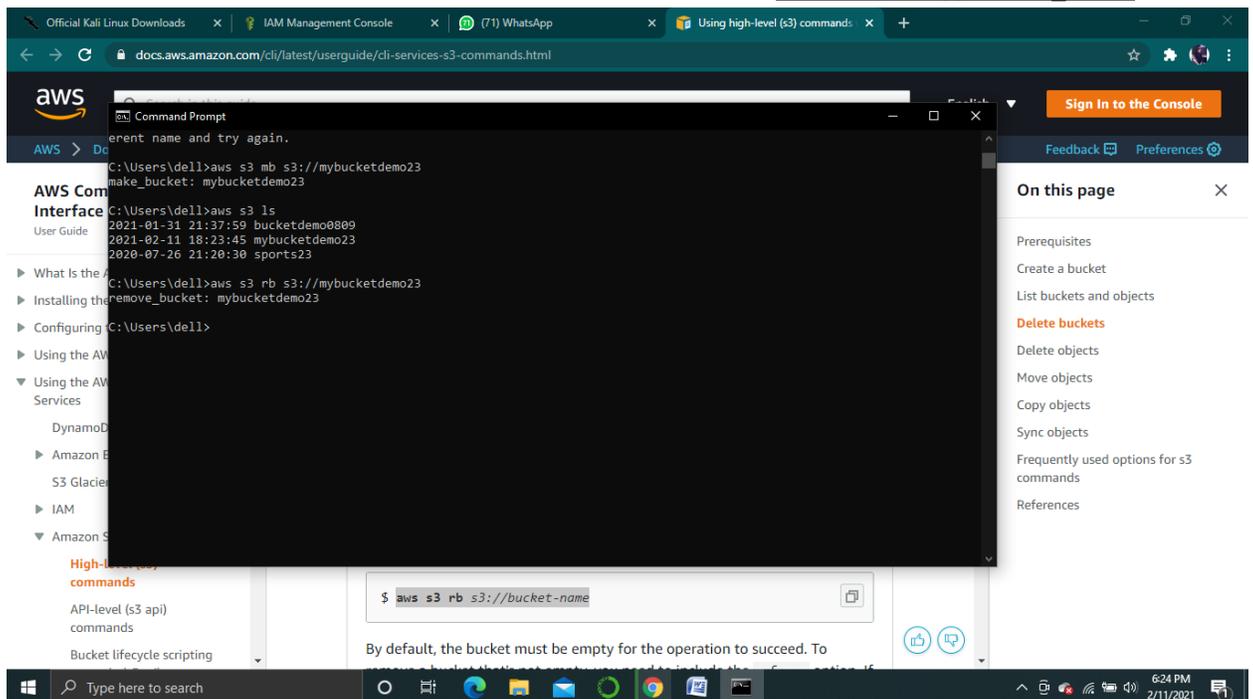


- Here is the Access key and Secret Key.
- Now 1st copy the Access Key and paste in the command prompt.
- Again copy Secret Key and paste it in Command prompt.
- Then it will ask for Region. So in region give the region name as ap-south-1.



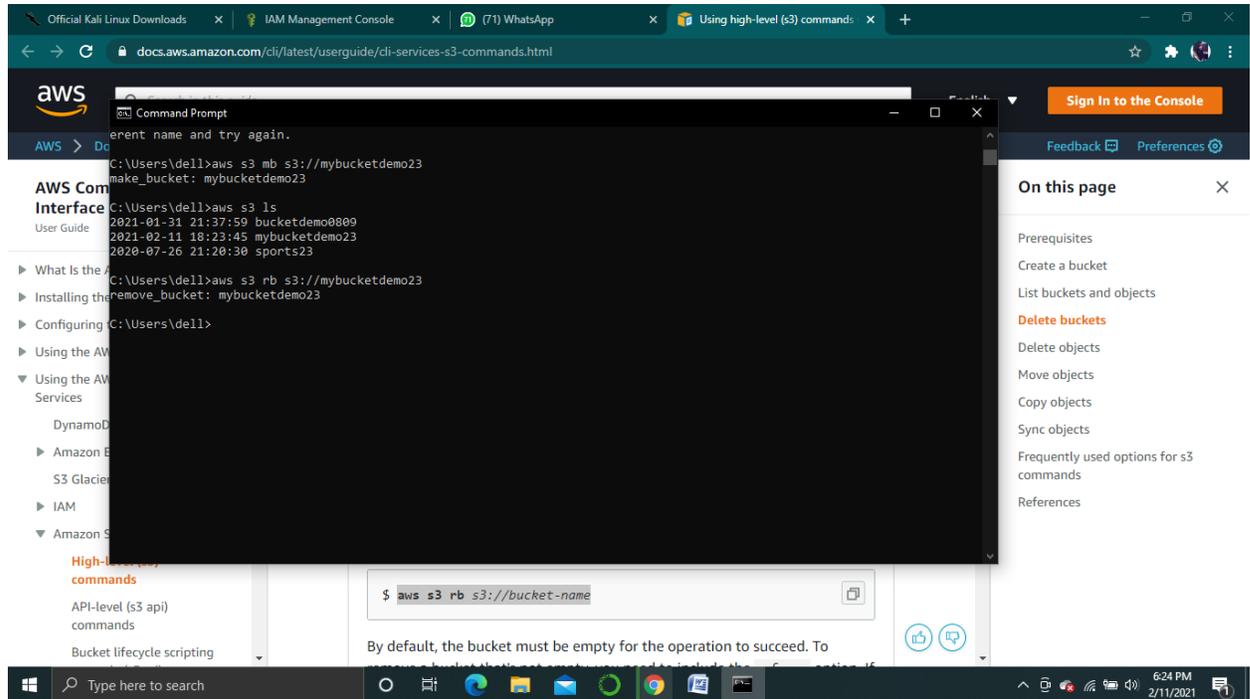


- Now to make or create a bucket we need to execute a command **`aws s3 mb s3://bucket_name`**



- Simultaneously check that the bucket is created in S3 service.
- Now to confirm in command prompt write a command `aws s3 ls`, it will show you all the buckets present in the s3 service.

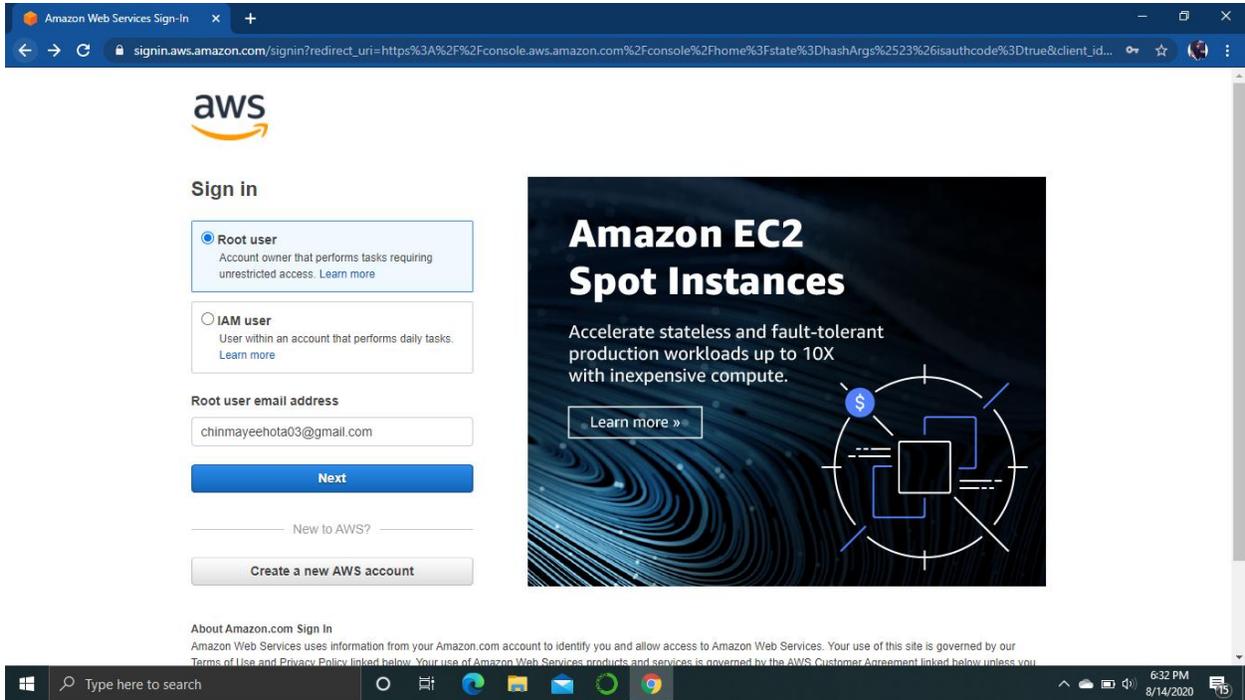
- Now Again to remove or delete the bucket execute a command **`aws s3 rb s3://bucket_name`**.
- Now check in the s3 service that the bucket is removed or not.
- In command prompt write command `aws s3 ls` to confirm that the bucket is deleted.



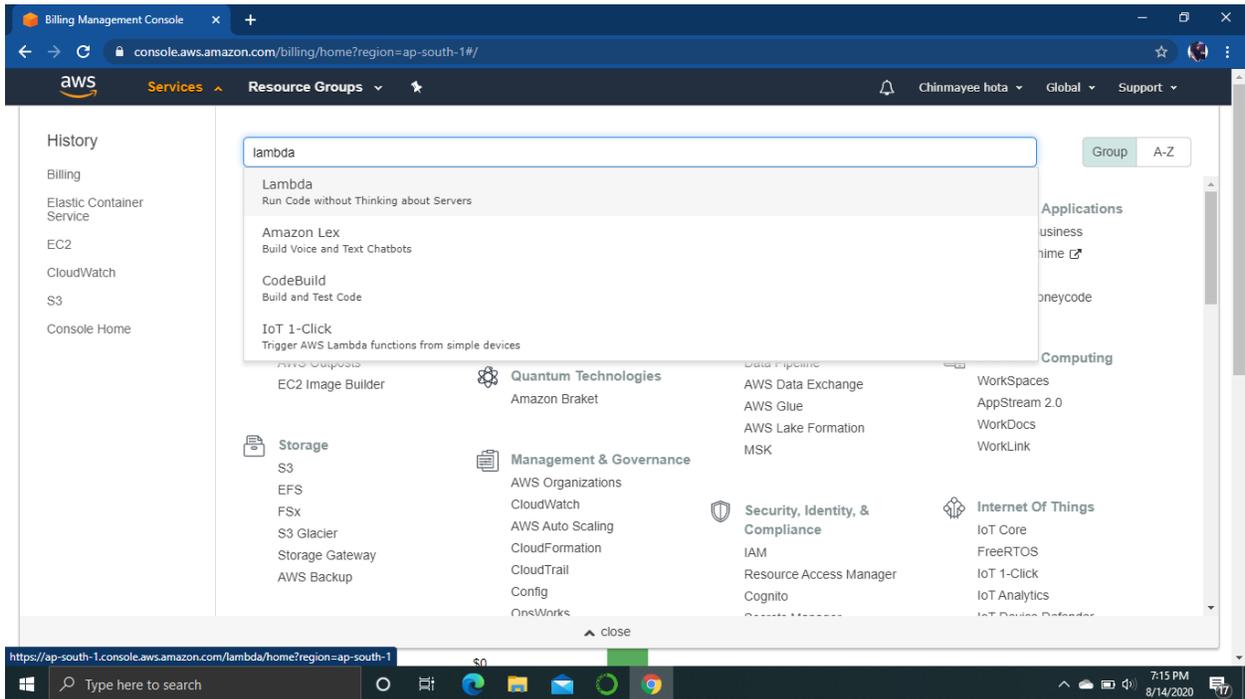
Conclusion- We have successfully created an access key and a secret key and also executed commands to create and remove buckets in command prompt.

LAMBDA FUNCTION

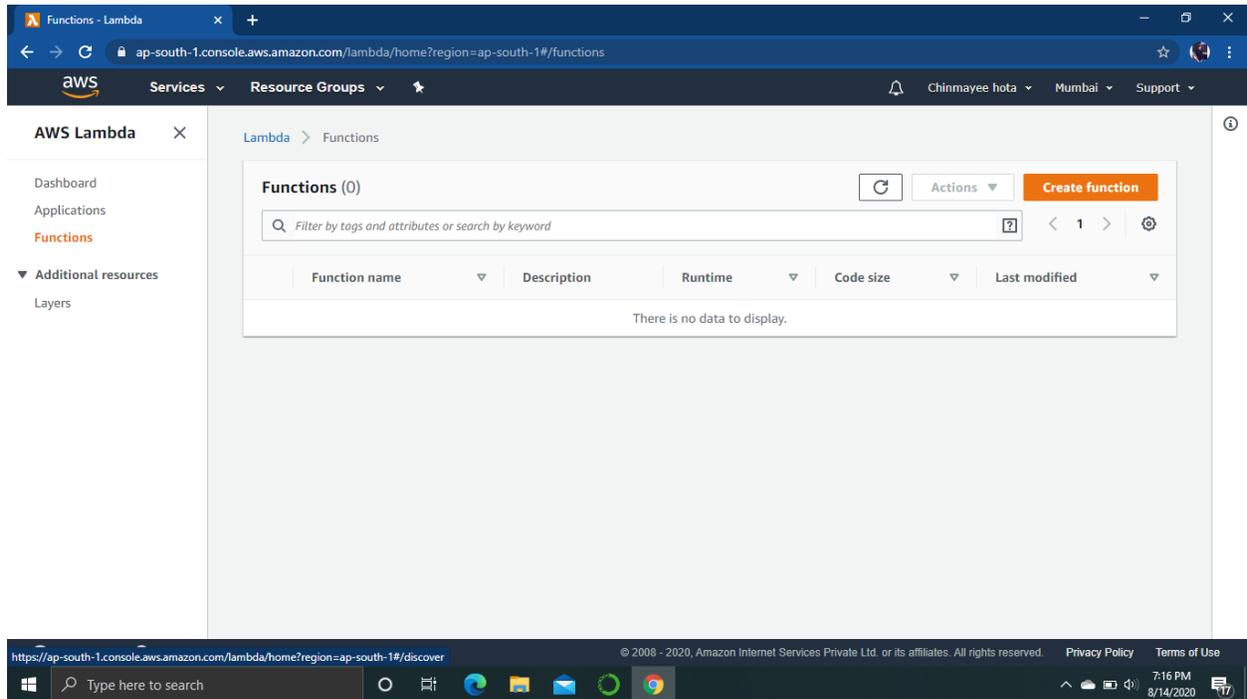
Step 1: Login to AWS console.



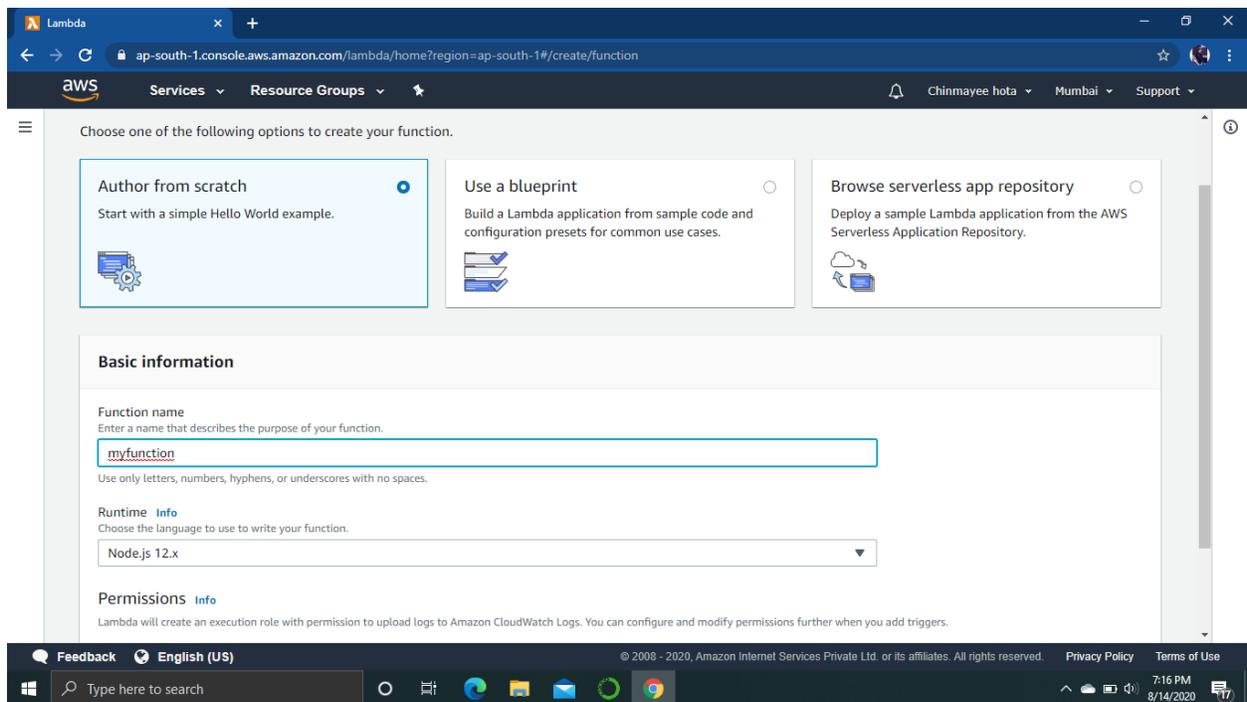
Step 2: Open the service as lambda.



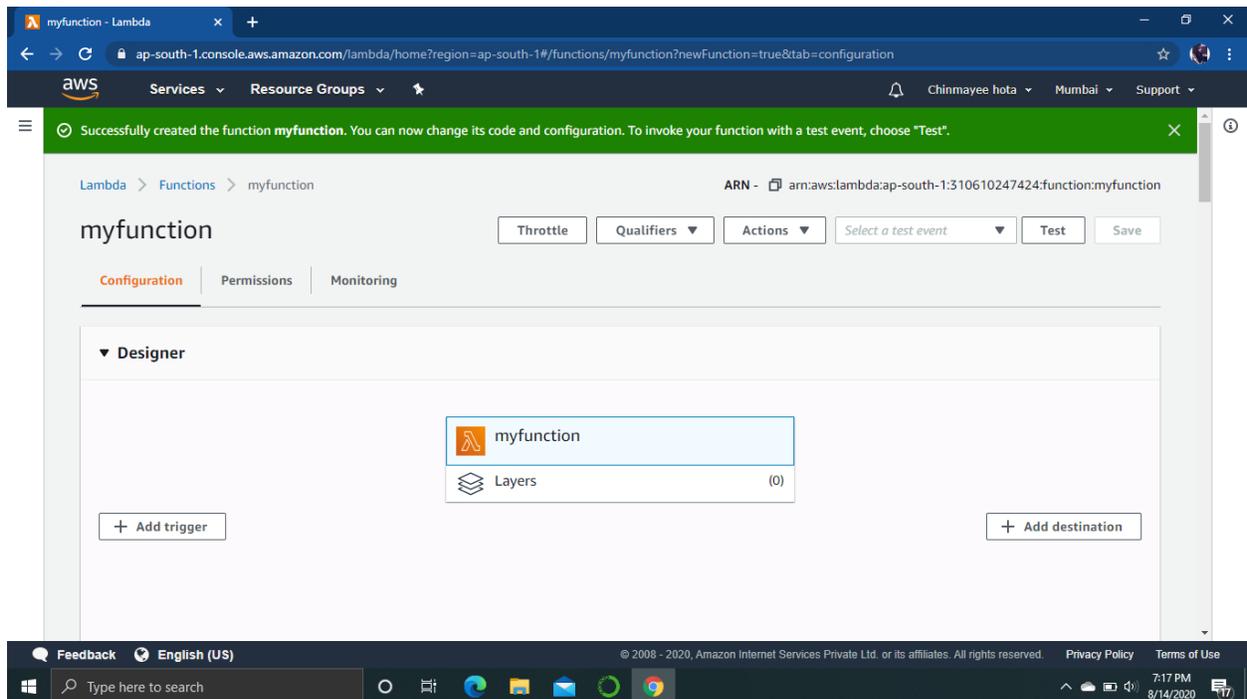
Step 3: From the dashboard select Create function.



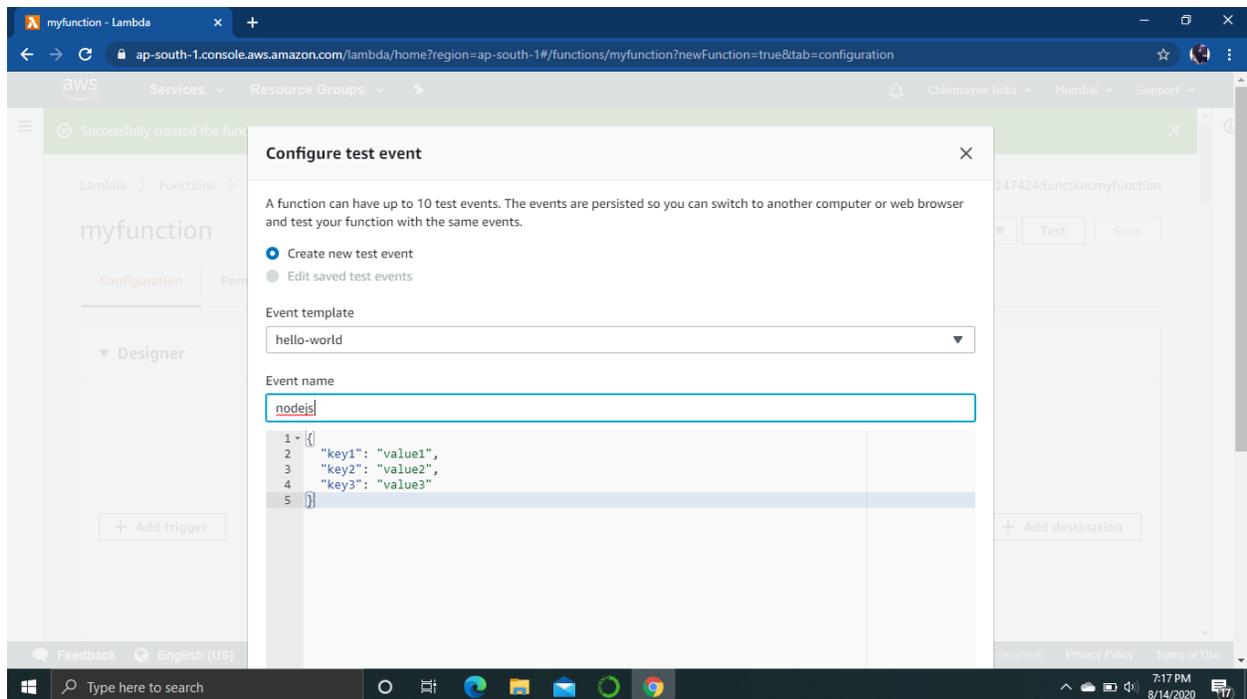
Step 4: Select author from scratch and configure the details such as function name, language to run the function as Node.js



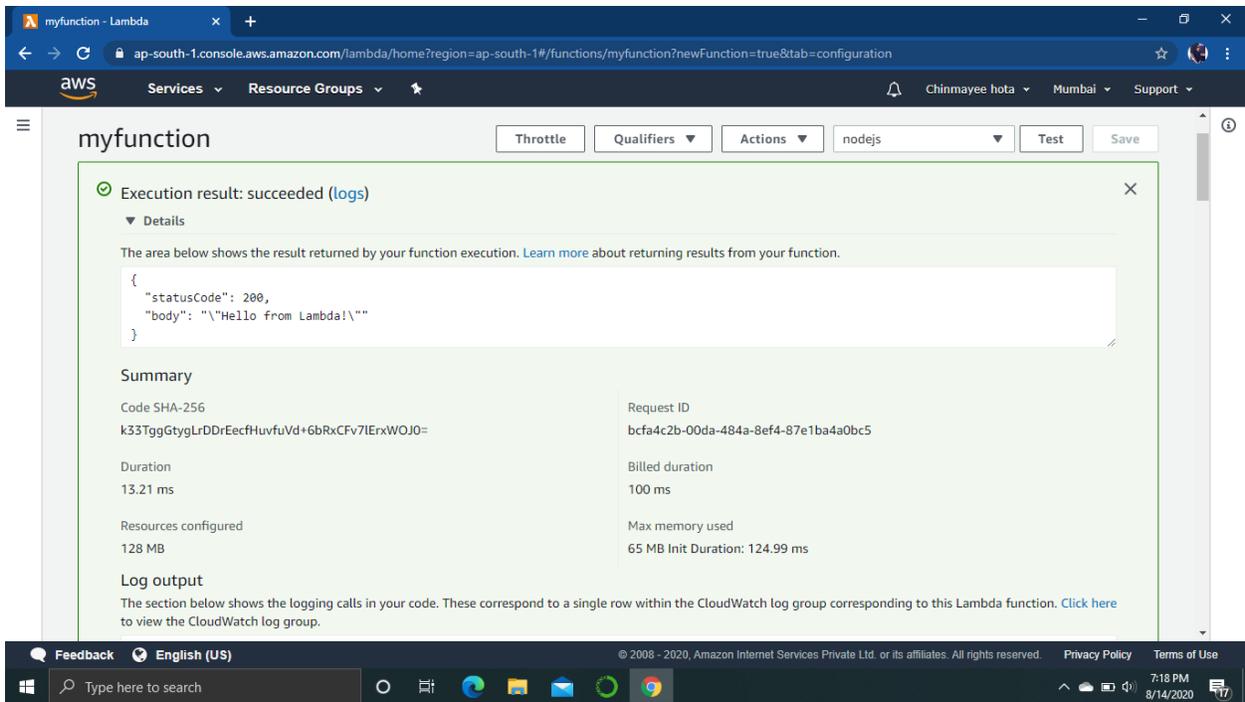
Step 4: The function is created successfully.



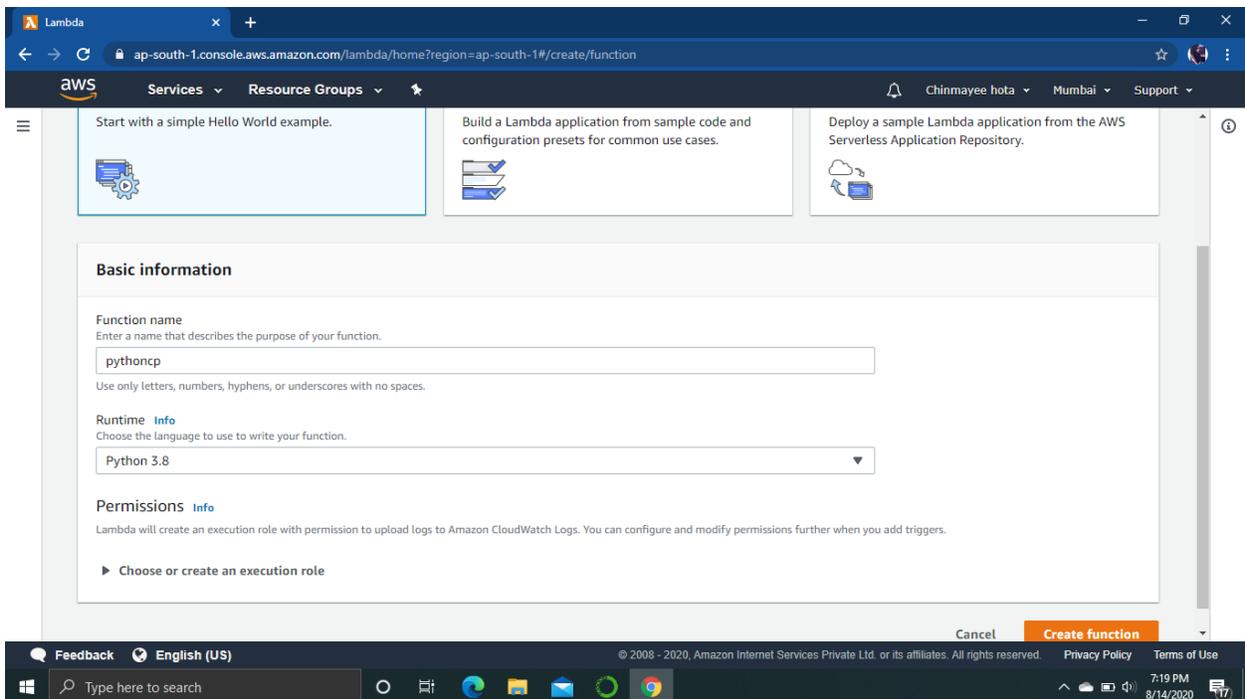
Step 5: Select test and configure test event name and all details. Then select create.



Step 6: Check the status of the event from the dashboard.



Step 7: Create another function for the language python and repeat the same process till it is executed.



pythoncp - Lambda

ap-south-1.console.aws.amazon.com/lambda/home?region=ap-south-1#/functions/pythoncp?newFunction=true&tab=configuration

Services Resource Groups

Chinmayee hota Mumbai Support

Successfully created the function **pythoncp**. You can now change its code and configuration. To invoke your function with a test event, choose "Test".

Lambda > Functions > pythoncp

ARN - arn:aws:lambda:ap-south-1:310610247424:function:pythoncp

pythoncp

Throttle Qualifiers Actions Select a test event Test Save

Configuration Permissions Monitoring

▼ Designer

pythoncp

Layers (0)

+ Add trigger + Add destination

Feedback English (US)

© 2008 - 2020, Amazon Internet Services Private Ltd. or its affiliates. All rights reserved. Privacy Policy Terms of Use

Type here to search

7:19 PM 8/14/2020

pythoncp - Lambda

ap-south-1.console.aws.amazon.com/lambda/home?region=ap-south-1#/functions/pythoncp?newFunction=true&tab=configuration

Services Resource Groups

Chinmayee hota Mumbai Support

Successfully created the function **pythoncp**. You can now change its code and configuration. To invoke your function with a test event, choose "Test".

Lambda > Functions > pythoncp

ARN - arn:aws:lambda:ap-south-1:310610247424:function:pythoncp

pythoncp

Throttle Qualifiers Actions python Test Save

Execution result: succeeded (logs)

▼ Details

The area below shows the result returned by your function execution. [Learn more](#) about returning results from your function.

```
{
  "statusCode": 200,
  "body": "\\Hello from Lambda!\\n"
}
```

Summary

Code SHA-256	Request ID
LD0MjQ04TMan6oFyOz3Y3mJqsPxm9IEhtimXGaDlb8c=	6e0f4993-84fb-4a02-828b-068ff41801db
Duration	Billed duration
1.22 ms	100 ms
Resources configured	Max memory used
128 MB	52 MB Init Duration: 129.73 ms

Feedback English (US)

© 2008 - 2020, Amazon Internet Services Private Ltd. or its affiliates. All rights reserved. Privacy Policy Terms of Use

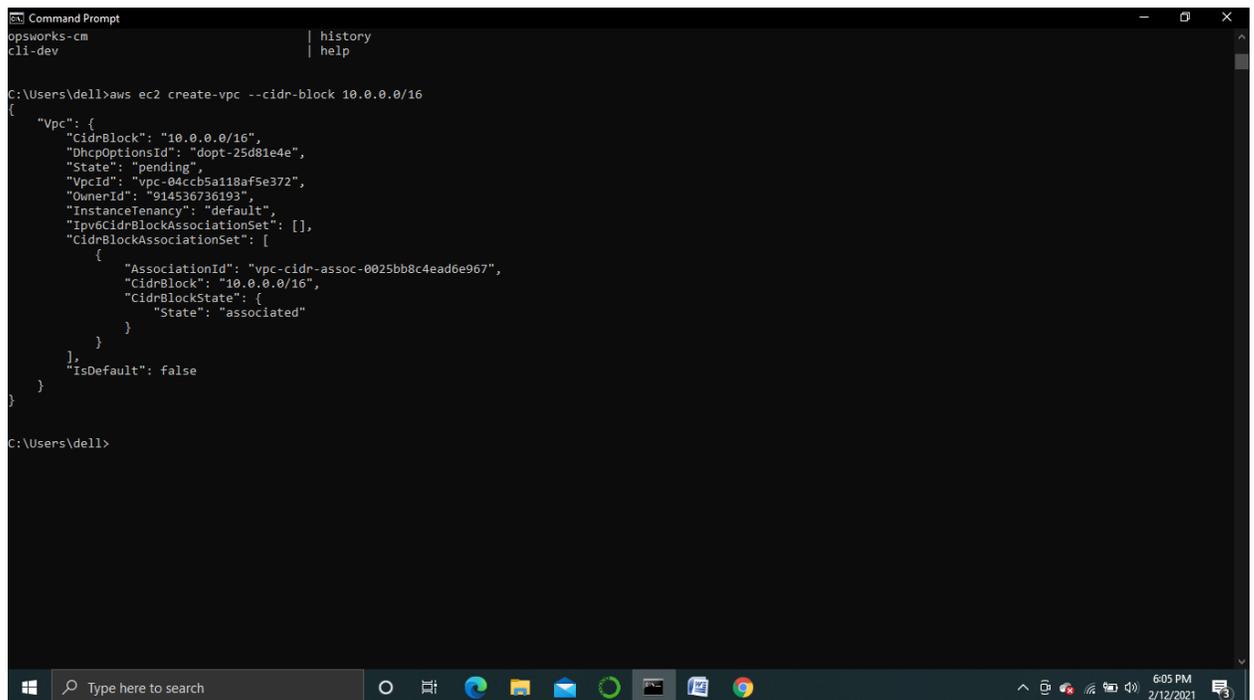
Type here to search

7:20 PM 8/14/2020

CONFIGURE SECURITY GROUPS THROUGH AWS CLI

STEPS TO FOLLOW:-

- Open the command prompt and type aws configure.
 - Give the access key id.
 - Select my security credentials from aws management console.
 - Get the access key
 - Click on new key
 - Copy the key and paste it in CLI
 - Mention the region name
 - AWS CLI is ready to take the commands.
-
- `aws ec2 create-vpc --cidr-block 10.0.0.0/16.`



```
Command Prompt
opsworks-cm | history
cli-dev | help

C:\Users\dell>aws ec2 create-vpc --cidr-block 10.0.0.0/16
{
  "Vpc": {
    "CidrBlock": "10.0.0.0/16",
    "DhcpOptionsId": "dopt-25d81e4e",
    "State": "pending",
    "VpcId": "vpc-04cc5a110af5e372",
    "OwnerId": "914536736193",
    "InstanceTenancy": "default",
    "Ipv6CidrBlockAssociationSet": [],
    "CidrBlockAssociationSet": [
      {
        "AssociationId": "vpc-cidr-assoc-0025bb8c4ead6e967",
        "CidrBlock": "10.0.0.0/16",
        "CidrBlockState": {
          "State": "associated"
        }
      }
    ],
    "IsDefault": false
  }
}

C:\Users\dell>
```

To Create SG for VPC:-

- `aws ec2 create-security-group --group-name my-sg1 --description "My security group1" --vpc-id vpc-0d0337664aaa0ab93`

```
Command Prompt
"CidrBlockState": {
  "State": "associated"
}
},
"IsDefault": false
}
}

C:\Users\dell>aws ec2 create-security-group --group-name msg1 --description "My security group1" --vpc-id vpc-04ccb5a118af5e372
{
  "GroupId": "sg-0c2ad16b484021d3d"
}

C:\Users\dell>
```

To describe:-

- `aws ec2 describe-security-groups --group-ids sg-0711db3fd7d5f5173`

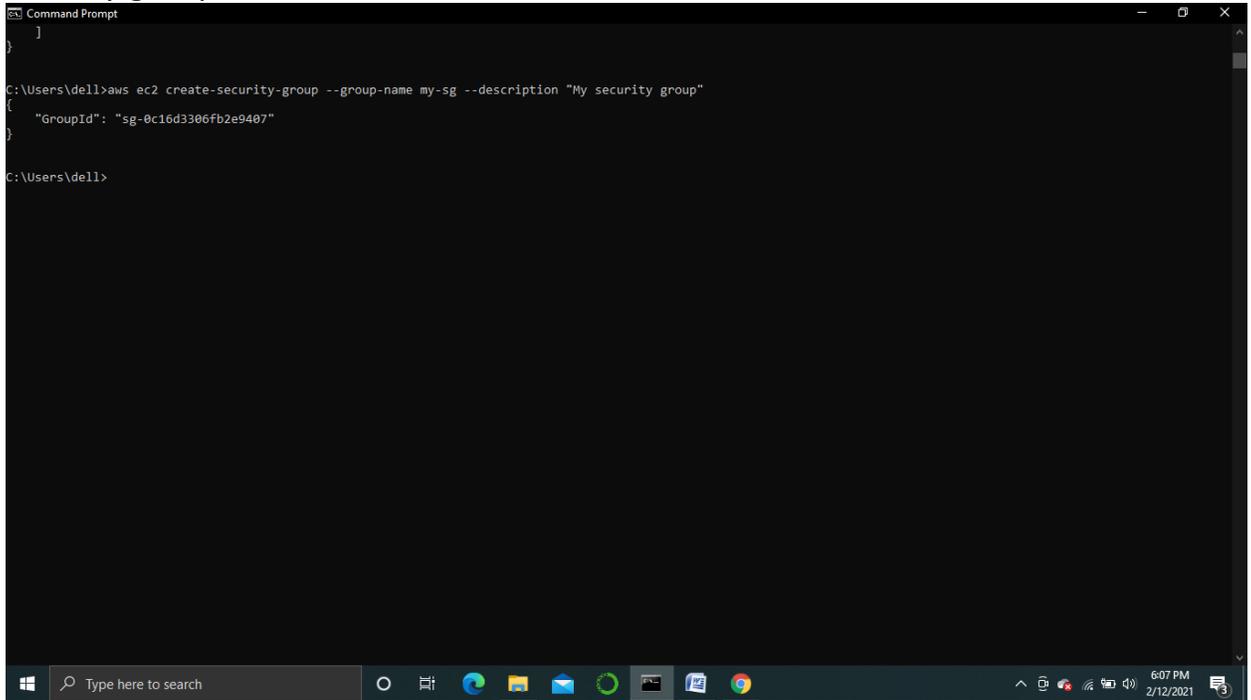
```
Command Prompt
C:\Users\dell>aws ec2 create-security-group --group-name msg1 --description "My security group1" --vpc-id vpc-04ccb5a118af5e372
{
  "GroupId": "sg-0c2ad16b484021d3d"
}

C:\Users\dell> aws ec2 describe-security-groups --group-id sg-0c2ad16b484021d3d
{
  "SecurityGroups": [
    {
      "Description": "My security group1",
      "GroupName": "msg1",
      "IpPermissions": [],
      "OwnerId": "914536736193",
      "GroupId": "sg-0c2ad16b484021d3d",
      "IpPermissionsEgress": [
        {
          "IpProtocol": "-1",
          "IpRanges": [
            {
              "CidrIp": "0.0.0.0/0"
            }
          ],
          "Ipv6Ranges": [],
          "PrefixListIds": [],
          "UserIdGroupPairs": []
        }
      ],
      "VpcId": "vpc-04ccb5a118af5e372"
    }
  ]
}

C:\Users\dell>
```

To create SG for EC2:-

- `aws ec2 create-security-group --group-name my-sg12 --description "My security group12"`



```
Command Prompt
]
}
}
C:\Users\dell>aws ec2 create-security-group --group-name my-sg --description "My security group"
{
  "GroupId": "sg-0c16d3306fb2e9407"
}
C:\Users\dell>
```

To describe :-

- `aws ec2 describe-security-groups --group-names my-sg`

```
Command Prompt
"GroupId": "sg-0c16d3306fb2e9407"
}
C:\Users\dell>aws ec2 describe-security-groups --group-names my-sg
{
  "SecurityGroups": [
    {
      "Description": "My security group",
      "GroupName": "my-sg",
      "IpPermissions": [],
      "OwnerId": "914536736193",
      "GroupId": "sg-0c16d3306fb2e9407",
      "IpPermissionsEgress": [
        {
          "IpProtocol": "-1",
          "IpRanges": [
            {
              "CidrIp": "0.0.0.0/0"
            }
          ]
        }
      ],
      "Ipv6Ranges": [],
      "PrefixListIds": [],
      "UserIdGroupPairs": []
    }
  ],
  "VpcId": "vpc-f2667d9a"
}
C:\Users\dell>
C:\Users\dell>
```

To delete the security group:-

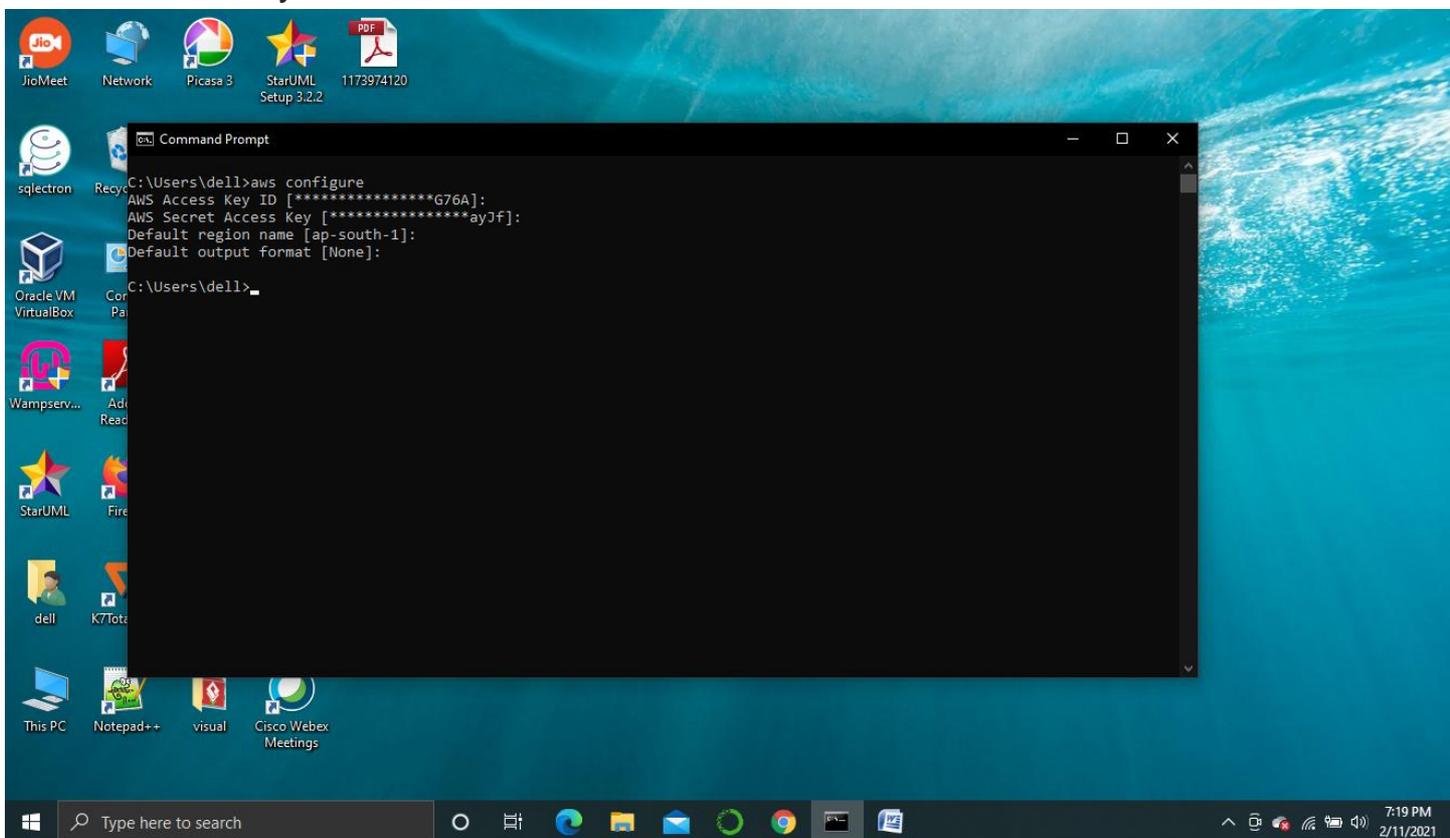
- `aws ec2 delete-security-group --group-id sg-0c16d3306fb2e9407`

```
Command Prompt
C:\Users\dell>aws ec2 delete-security-group --group-id sg-0c16d3306fb2e9407
C:\Users\dell>
```


CONFIGURE VPC THROUGH AWS CLI

STEPS TO FOLLOW:-

- Open the command prompt and type aws configure.
- Give the access key id.
- Select my security credentials from aws management console.
- Get the access key
- Click on new key
- Copy the key and paste it in CLI
- Mention the region name
- AWS CLI is ready to take the commands.



To Create VPC:-

- `aws ec2 create-vpc --cidr-block 10.0.0.0/16`

```
C:\Users\dell>aws configure
AWS Access Key ID [*****G76A]:
AWS Secret Access Key [*****ayJf]:
Default region name [ap-south-1]:
Default output format [None]:

C:\Users\dell>aws ec2 create-vpc --cidr-block 10.0.0.0/16
{
  "Vpc": {
    "CidrBlock": "10.0.0.0/16",
    "DhcpOptionsId": "dopt-25d81e4e",
    "State": "pending",
    "VpcId": "vpc-0ce18e145d0cd8231",
    "OwnerId": "914536736193",
    "InstanceTenancy": "default",
    "Ipv6CidrBlockAssociationSet": [],
    "CidrBlockAssociationSet": [
      {
        "AssociationId": "vpc-cidr-assoc-0ffbf01cbdc49885b",
        "CidrBlock": "10.0.0.0/16",
        "CidrBlockState": {
          "State": "associated"
        }
      }
    ],
    "IsDefault": false
  }
}
```

To create Subnet:-

- aws ec2 create-subnet --vpc-id vpc-2f09a348 --cidr-block 10.0.1.0/24(vpc id is created earlier)

```
    "State": "associated"
  }
},
  "IsDefault": false
}
}

C:\Users\dell>aws ec2 create-subnet --vpc-id vpc-0ce18e145d0cd8231 --cidr-block 10.0.1.0/24
{
  "Subnet": {
    "AvailabilityZone": "ap-south-1a",
    "AvailabilityZoneId": "aps1-az1",
    "AvailableIpAddressCount": 251,
    "CidrBlock": "10.0.1.0/24",
    "DefaultForAz": false,
    "MapPublicIpOnLaunch": false,
    "State": "available",
    "SubnetId": "subnet-00c63cedc554c2fce",
    "VpcId": "vpc-0ce18e145d0cd8231",
    "OwnerId": "914536736193",
    "AssignIpv6AddressOnCreation": false,
    "Ipv6CidrBlockAssociationSet": [],
    "SubnetArn": "arn:aws:ec2:ap-south-1:914536736193:subnet/subnet-00c63cedc554c2fce"
  }
}

C:\Users\dell>
```

To create internet gateway:-

- aws ec2 create-internet-gateway

```
Command Prompt
{"AvailableIpAddressCount": 251,
 "CidrBlock": "10.0.1.0/24",
 "DefaultForAz": false,
 "MapPublicIpOnLaunch": false,
 "State": "available",
 "SubnetId": "subnet-00c63cedc554c2fce",
 "VpcId": "vpc-0ce18e145d0cd8231",
 "OwnerId": "914536736193",
 "AssignIpv6AddressOnCreation": false,
 "Ipv6CidrBlockAssociationSet": [],
 "SubnetArn": "arn:aws:ec2:ap-south-1:914536736193:subnet/subnet-00c63cedc554c2fce"
}

C:\Users\dell>aws ec2 create-internet-gateway
{
  "InternetGateway": {
    "Attachments": [],
    "InternetGatewayId": "igw-05eeb1d65e361c5dd",
    "OwnerId": "914536736193",
    "Tags": []
  }
}

C:\Users\dell>
->aws ec2 create-route --route-table-id rtb-c1c8faa6 --destination-cidr-block 0.0.0.0/0 --
gateway-id igw-1ff7a07b
```

To attach the internet gateway:-

- aws ec2 attach-internet-gateway --vpc-id (enter vpc here) --internet-gateway-id (enter your internet gateway id here)

```
Command Prompt
{"MapPublicIpOnLaunch": false,
 "State": "available",
 "SubnetId": "subnet-00c63cedc554c2fce",
 "VpcId": "vpc-0ce18e145d0cd8231",
 "OwnerId": "914536736193",
 "AssignIpv6AddressOnCreation": false,
 "Ipv6CidrBlockAssociationSet": [],
 "SubnetArn": "arn:aws:ec2:ap-south-1:914536736193:subnet/subnet-00c63cedc554c2fce"
}

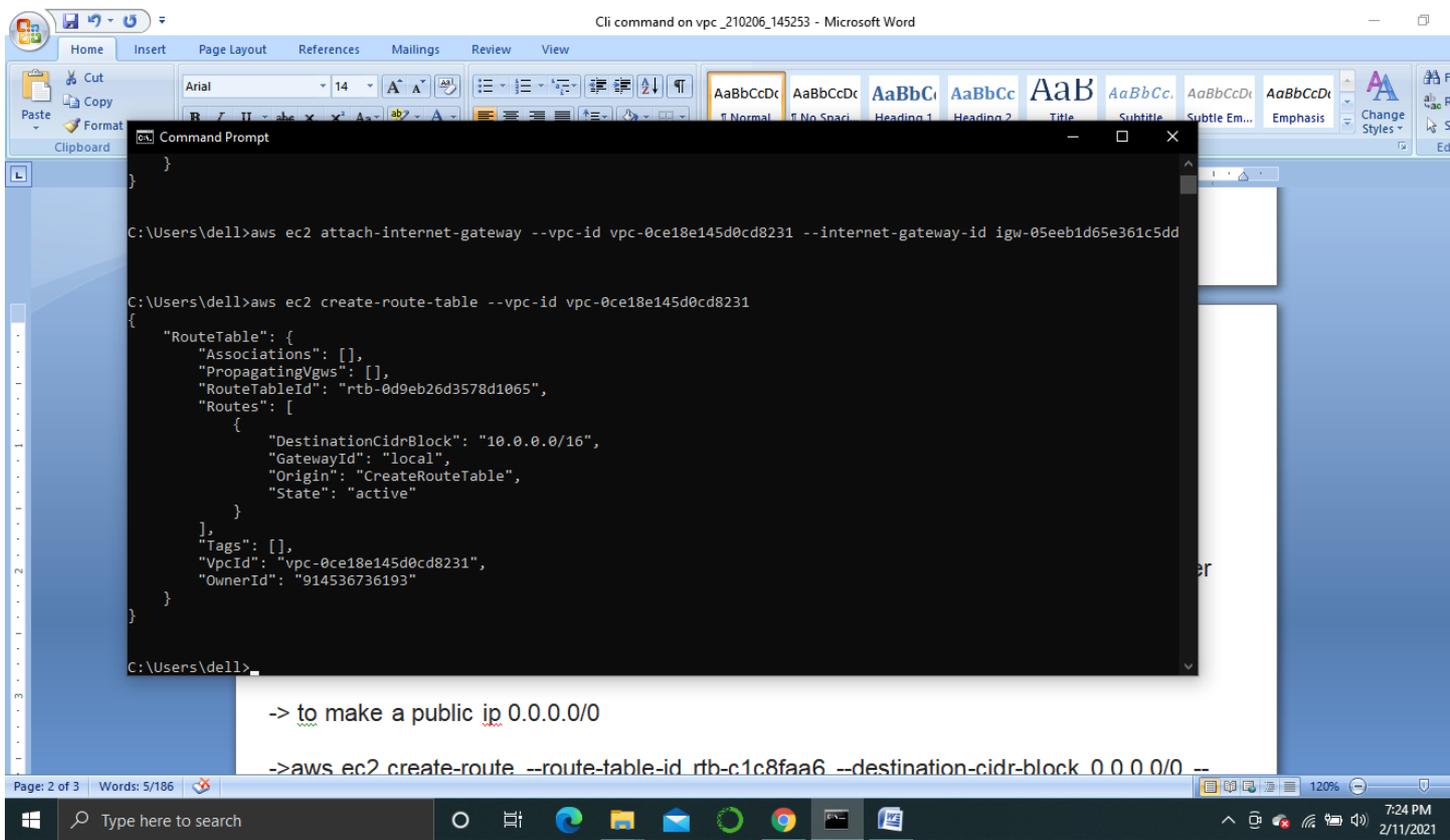
C:\Users\dell>aws ec2 create-internet-gateway
{
  "InternetGateway": {
    "Attachments": [],
    "InternetGatewayId": "igw-05eeb1d65e361c5dd",
    "OwnerId": "914536736193",
    "Tags": []
  }
}

C:\Users\dell>aws ec2 attach-internet-gateway --vpc-id vpc-0ce18e145d0cd8231 --internet-gateway-id igw-05eeb1d65e361c5dd

C:\Users\dell>
->aws ec2 attach-internet-gateway --vpc-id (enter vpc here) --internet-gateway-id (enter
your internet gateway id here.)
```

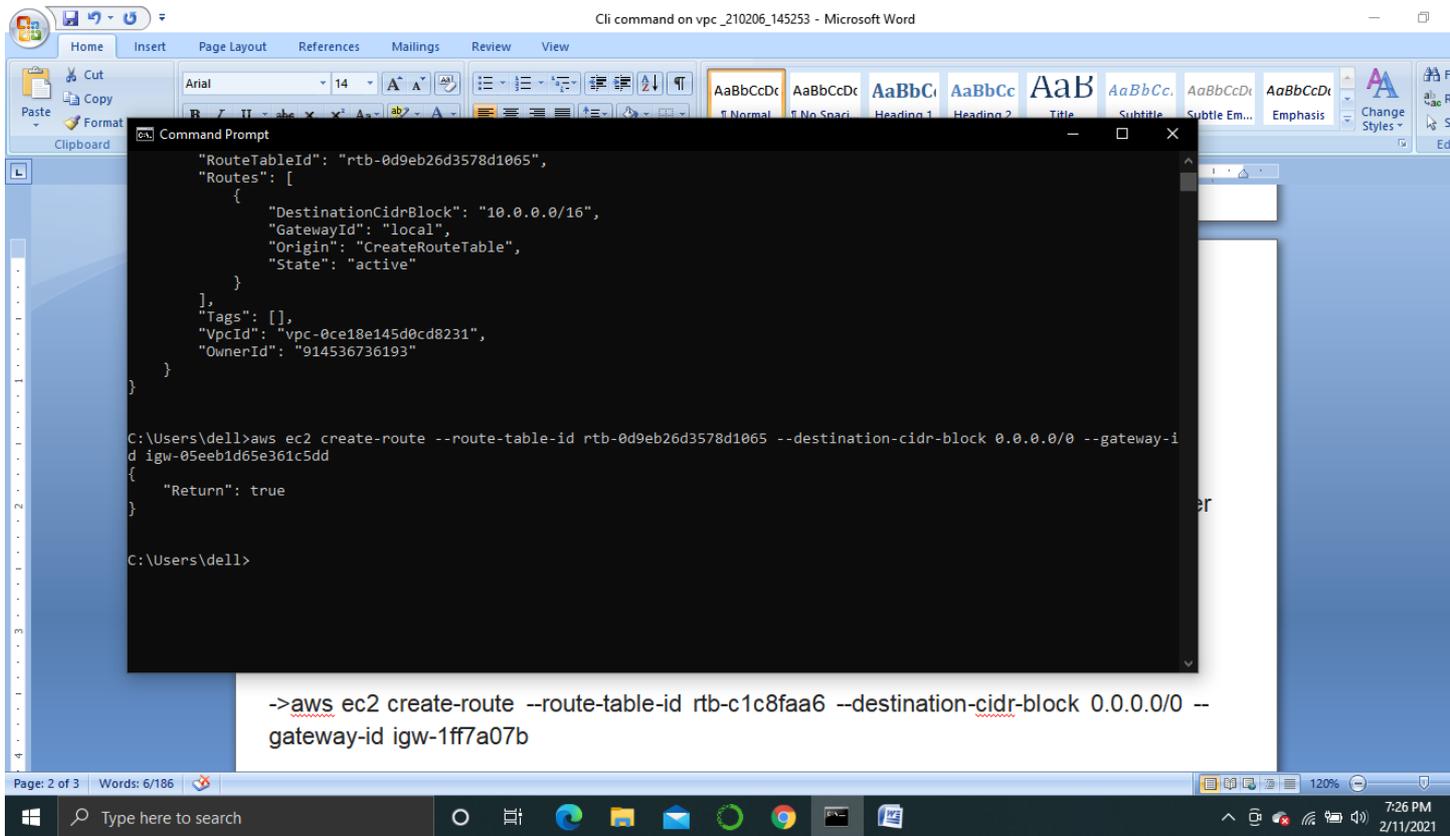
To create a route table:-

- aws ec2 create-route-table --vpc-id (enter your vpc id here)



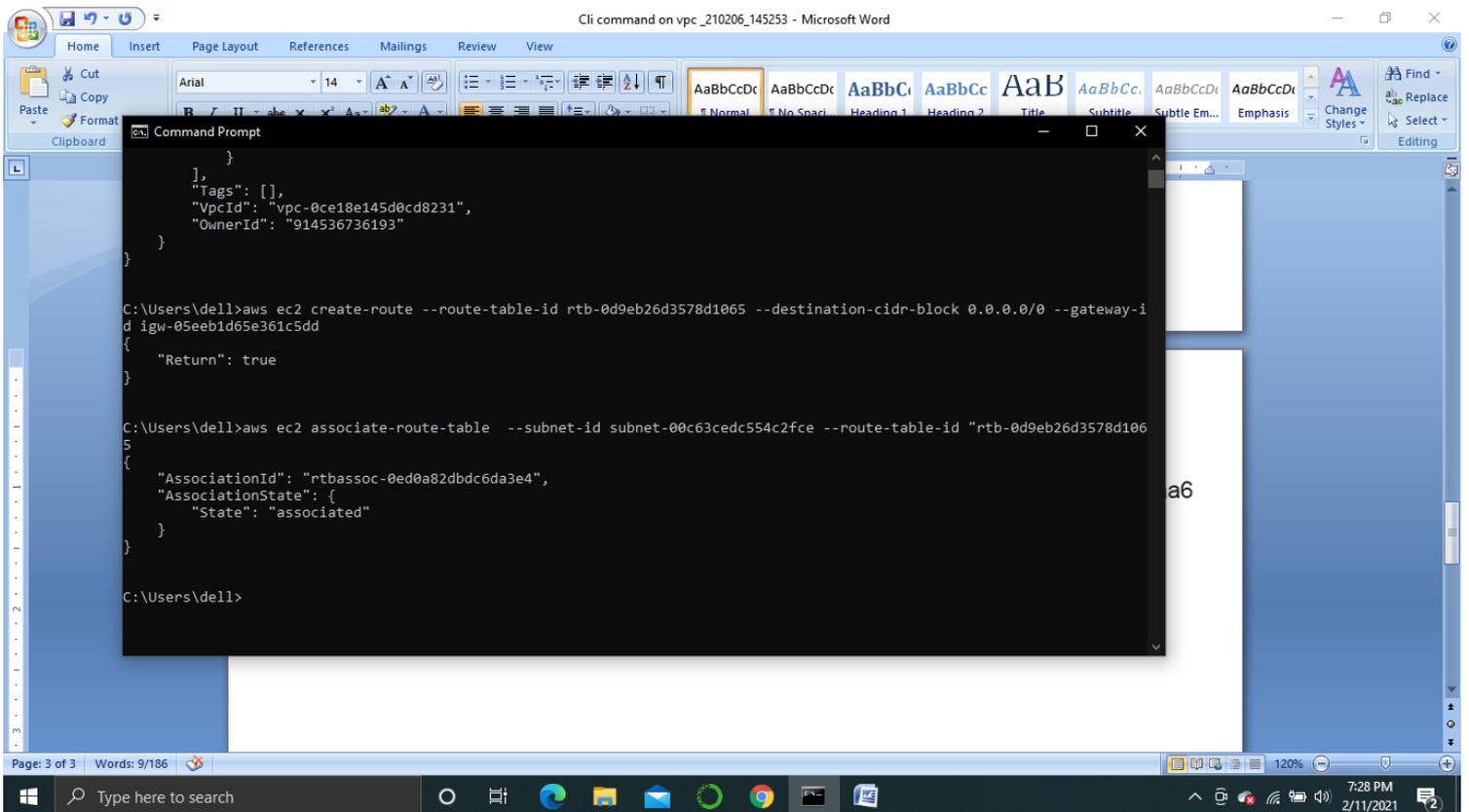
To make the Route table public:-

- `aws ec2 create-route --route-table-id rtb-c1c8faa6 --destination-cidr-block 0.0.0.0/0 -gateway-id igw-1ff7a07b`



To associate route table with subnet:-

- `aws ec2 associate-route-table --subnet-id subnet-b46032ec --route-table-id rtb-c1c8faa6`



The screenshot shows a Microsoft Word document titled "Cli command on vpc_210206_145253" with a Command Prompt window overlaid. The Command Prompt displays the following commands and their outputs:

```
C:\Users\dell>aws ec2 create-route-table --route-table-id rtb-0d9eb26d3578d1065 --destination-cidr-block 0.0.0.0/0 --gateway-id igw-05eeb1d65e361c5dd
{
  "Return": true
}

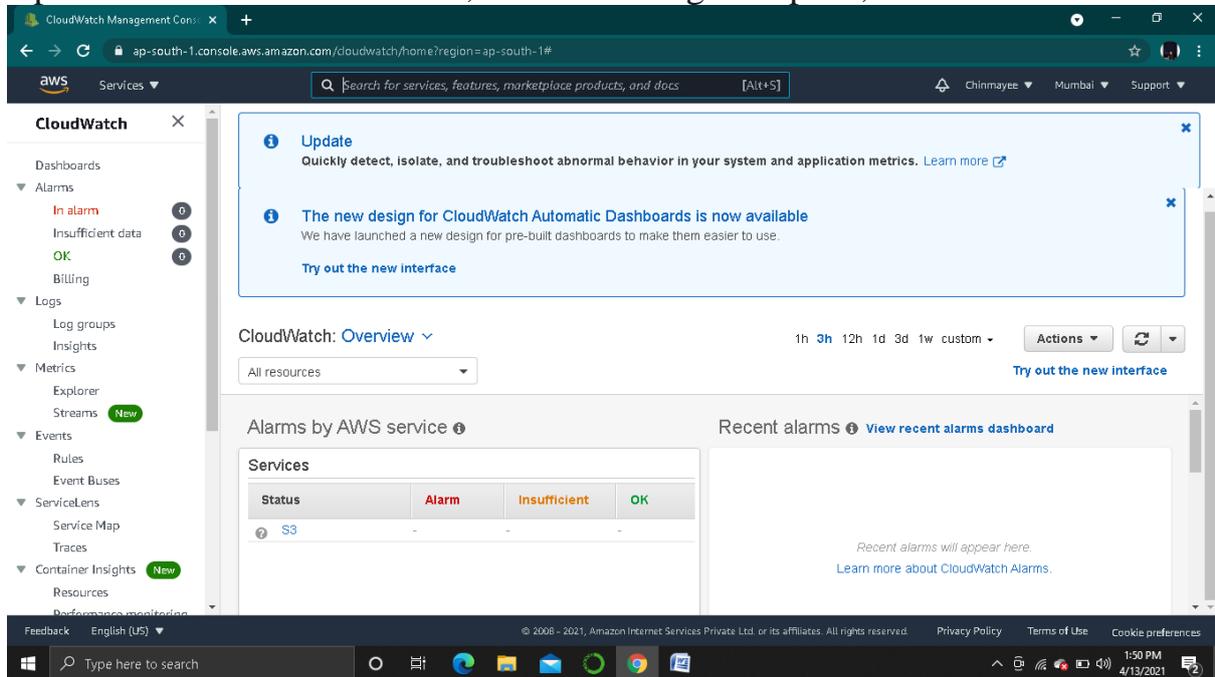
C:\Users\dell>aws ec2 associate-route-table --subnet-id subnet-00c63cedc554c2fce --route-table-id "rtb-0d9eb26d3578d1065"
{
  "AssociationId": "rtbassoc-0ed0a82dbdc6da3e4",
  "AssociationState": {
    "State": "associated"
  }
}
```

The Word document's status bar at the bottom indicates "Page: 3 of 3" and "Words: 9/186". The system tray shows the date as 2/11/2021 and the time as 7:28 PM.

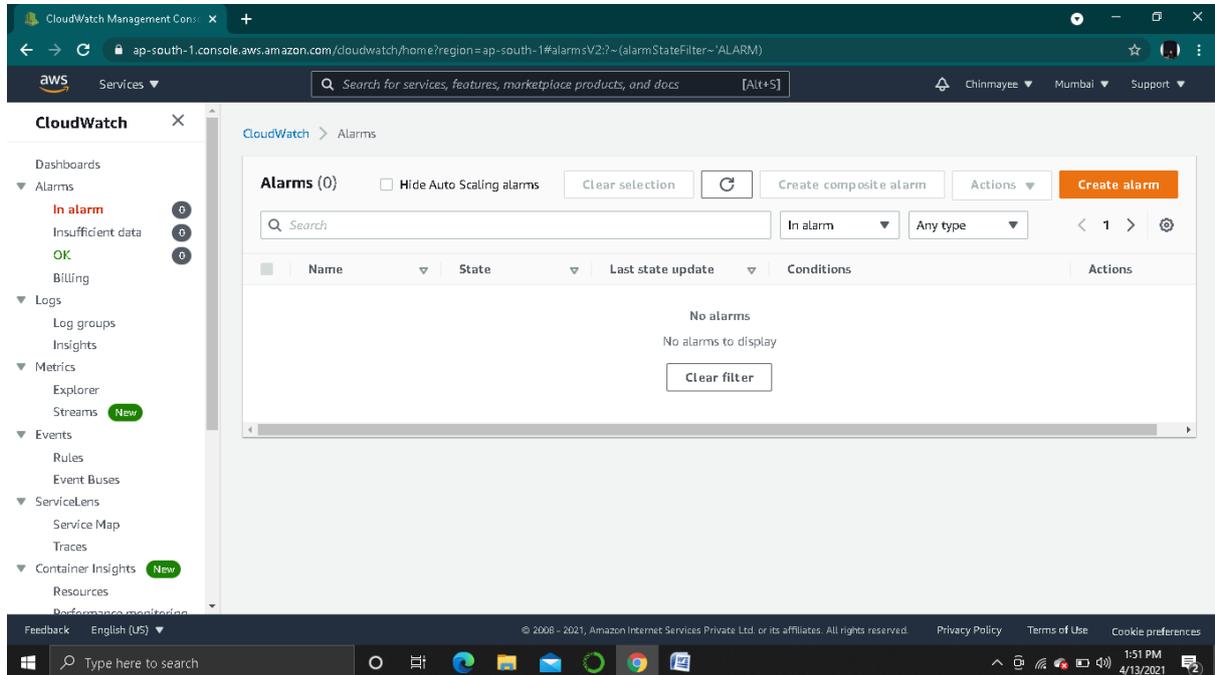
CREATE AN ALARM USING CLOUDWATCH

STEPS TO BE FOLLOWED:

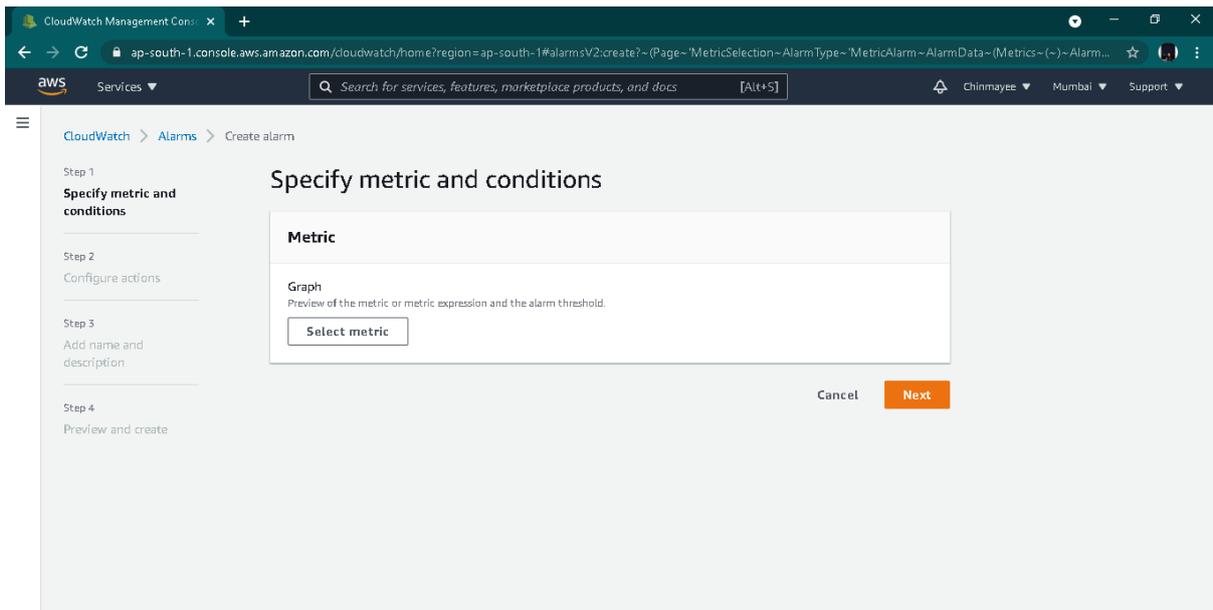
1. Open the CloudWatch console, from the navigation pane, choose Alarms.



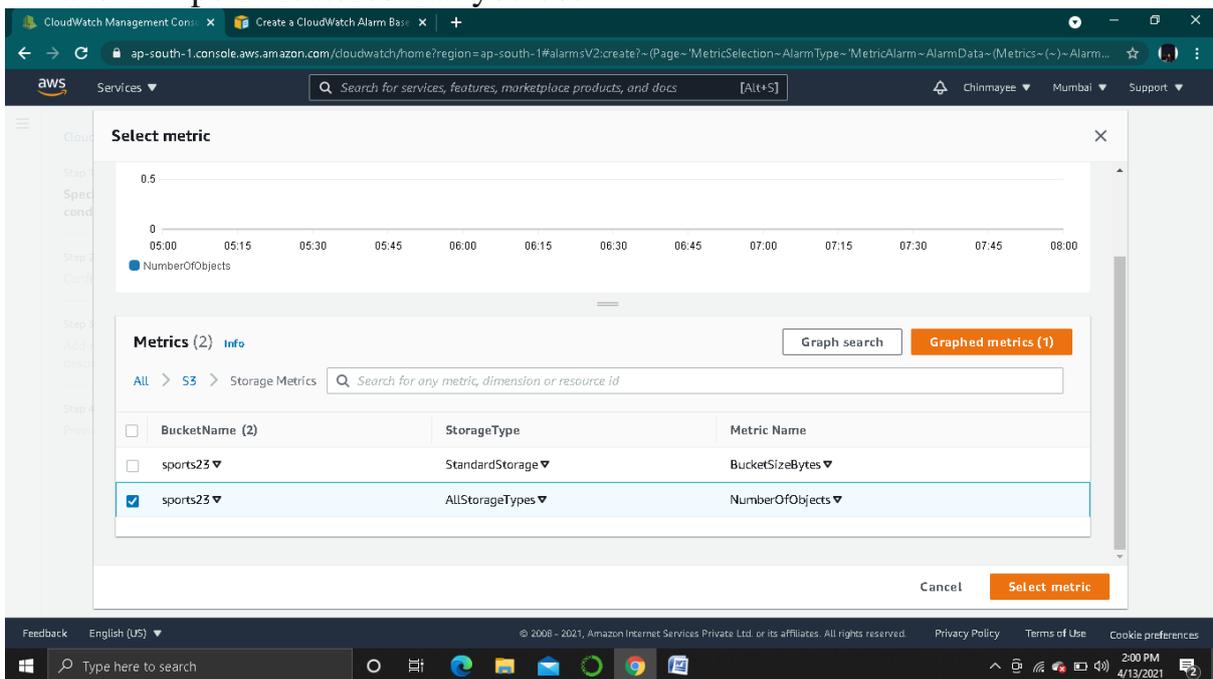
2. Choose Create alarm.



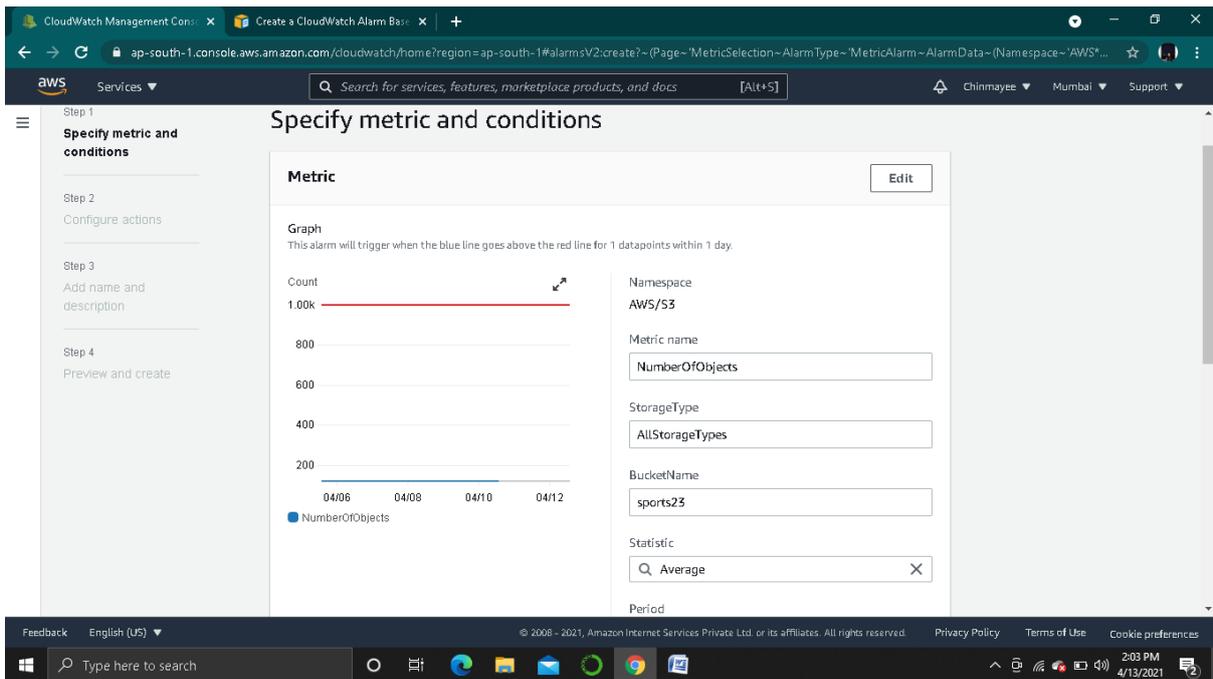
3. Choose Select metric.



4. On the All metrics tab, choose Pinpoint, and then choose the type of metric that you want to create an alarm for. The types of available metrics depends on the Amazon Pinpoint features that you use.

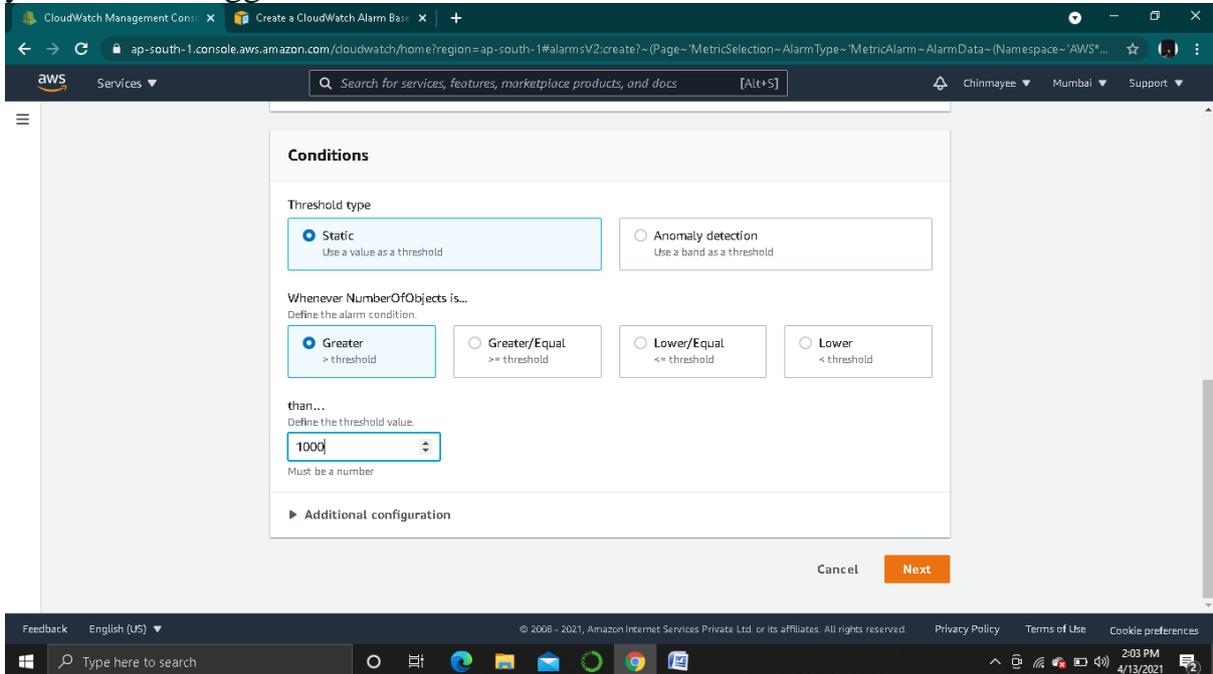


5. Select the metric that you want to create an alarm for, and then choose Select metric. The Specify metric and conditions page appears, showing a graph and other information about the metric.



6. Under Conditions, complete the following steps:

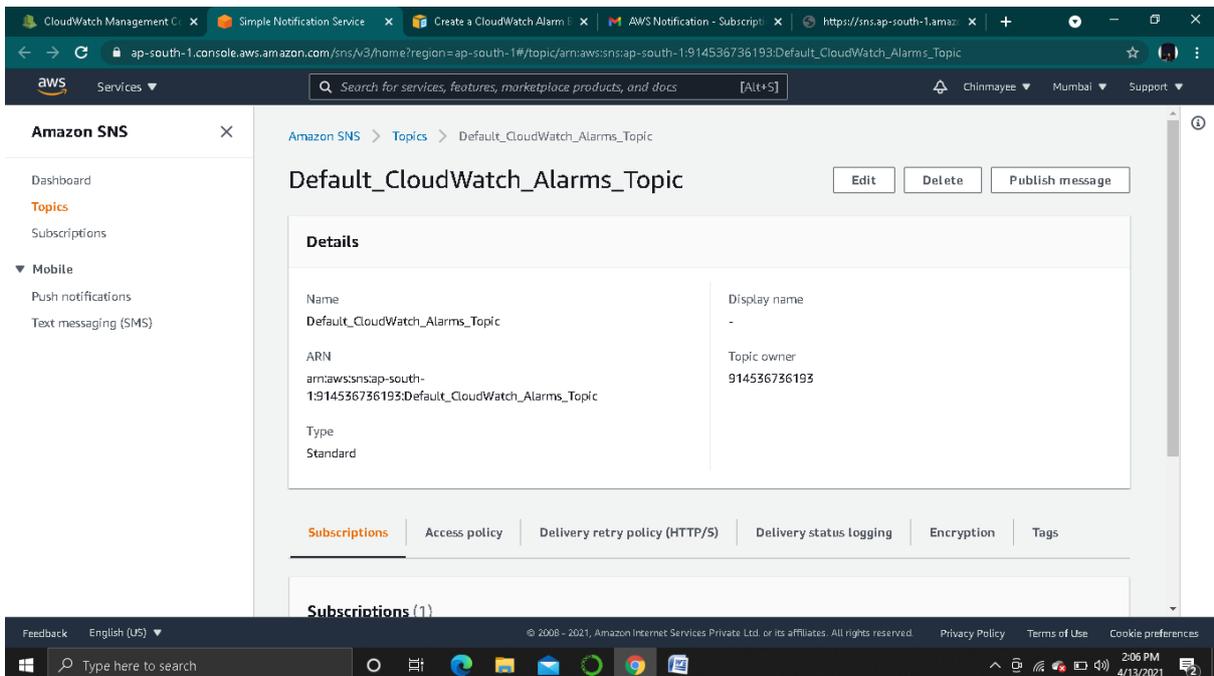
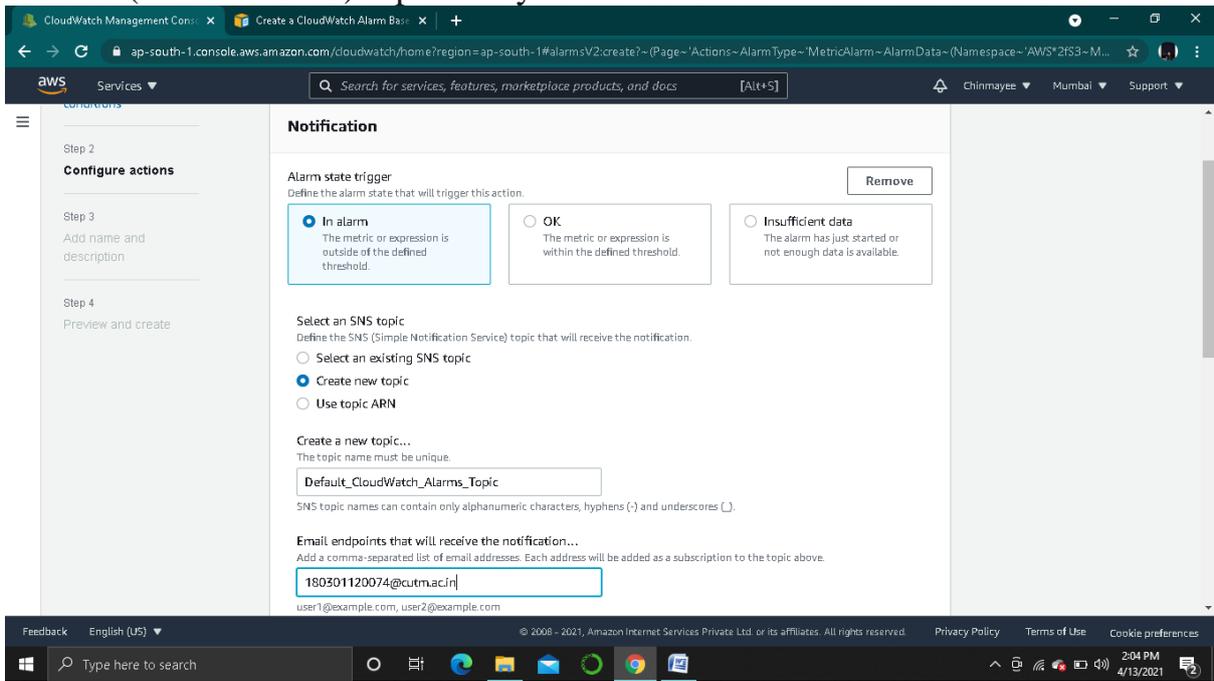
- For Threshold type, choose Static.
- For Whenever metric is, specify whether you want the value of the metric to be greater than, greater than or equal to, less than, or less than or equal to the threshold to trigger the alarm. Then, under than, enter the threshold value that you want to trigger the alarm.



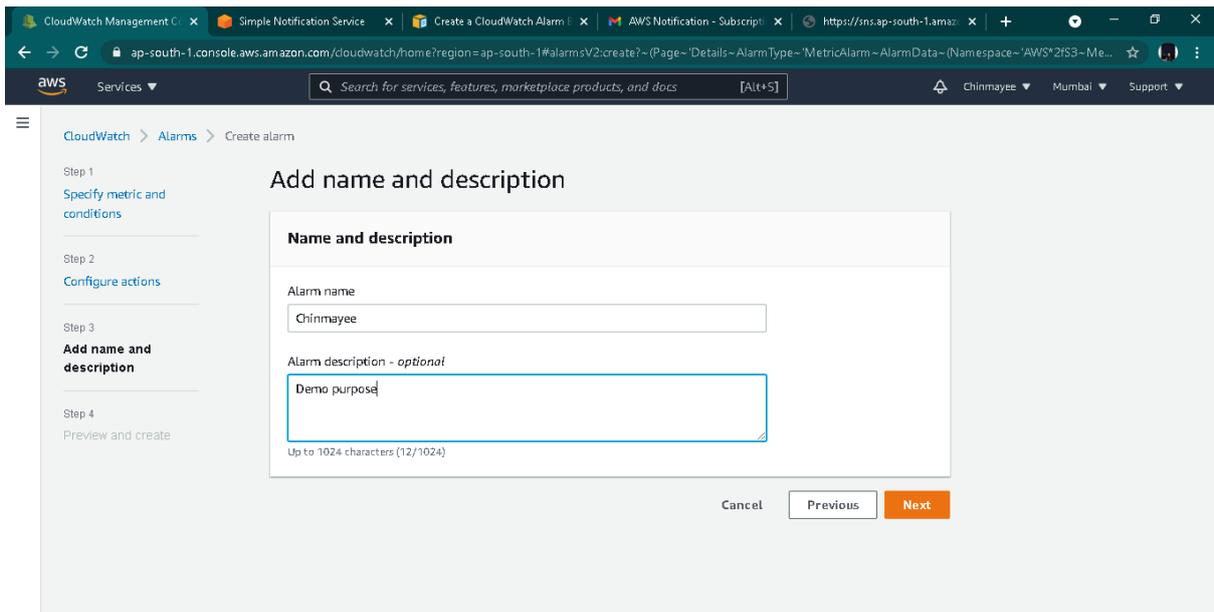
7. Under Additional configuration, complete the following steps:

- For Datapoints to alarm, enter the number of evaluation periods (datapoints) during which the metric value must meet the threshold conditions to trigger the alarm.

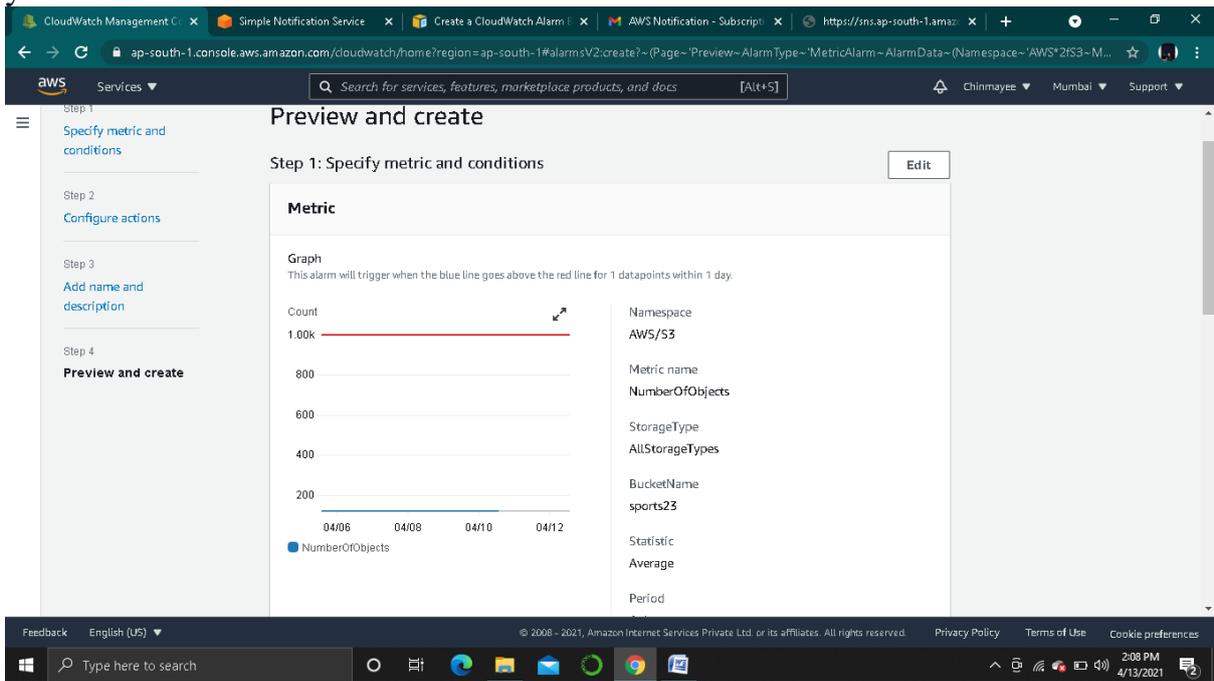
- For Missing data treatment, choose what you want the alarm to do if some data is missing.
- 8. Choose Next.
- 9. Under Notification, complete the following steps:
 - For Whenever this alarm state is, choose in Alarm.
 - For Select an SNS topic, choose or create an Amazon Simple Notification Service (Amazon SNS) topic that you want the alarm notification to be sent to.



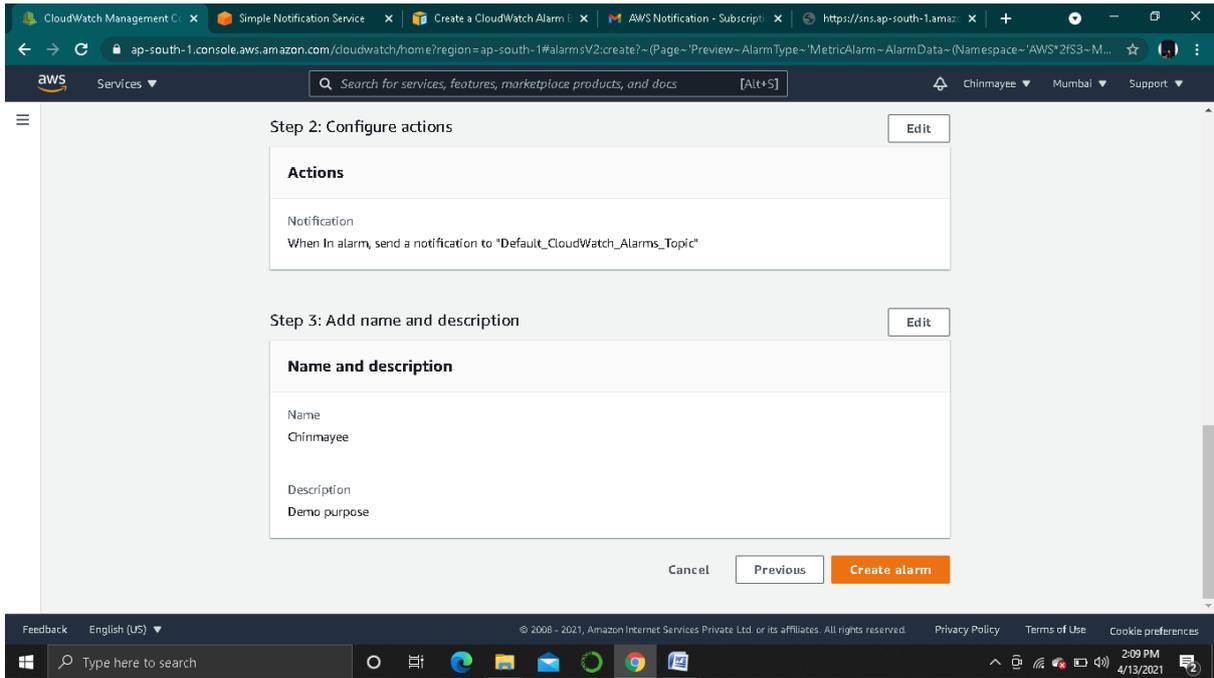
- 10. Choose Next.
- 11. Enter a name and, optionally, a description for the alarm, and then choose Next.



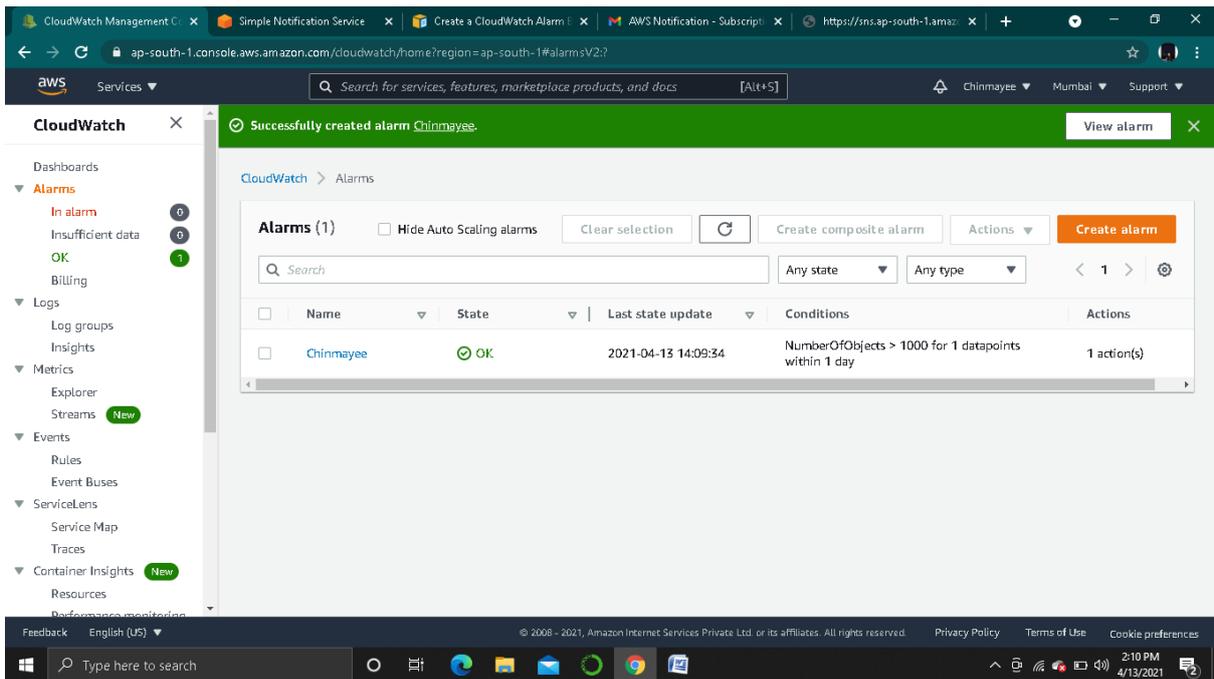
12. Under Preview and create, review and confirm that the alarm settings are what you want.



13. Choose create alarm.



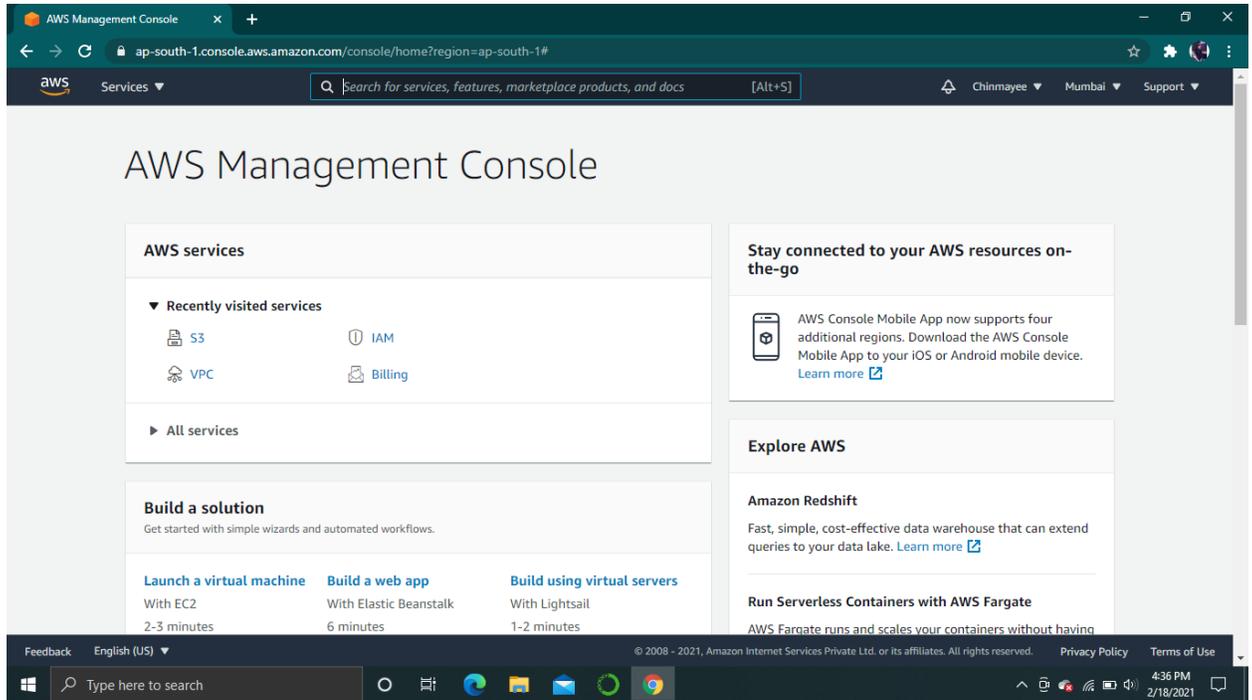
14. Review the status of the cloudwatch alarm.



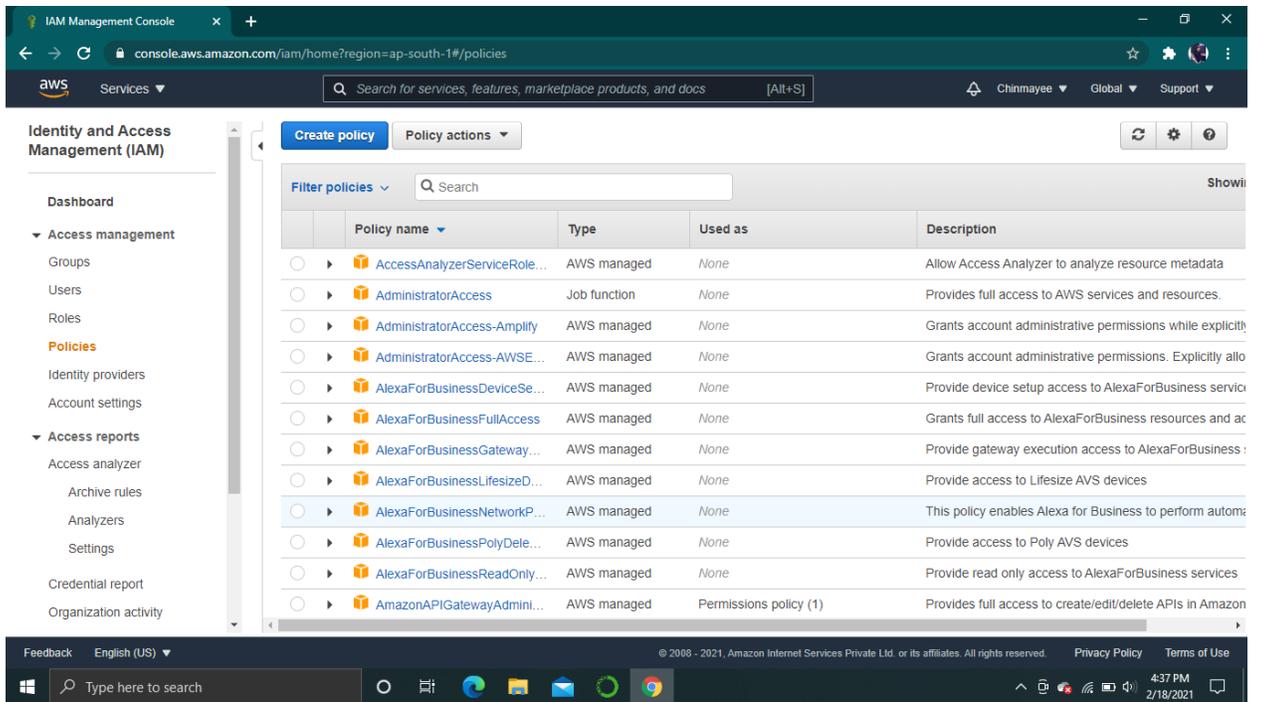
CREATE AN IAM POLICY AND ASSOCIATE A ROLE TO IT AND CONNECT IT USING EC2 INSTANCE

STEPS TO FOLLOW:-

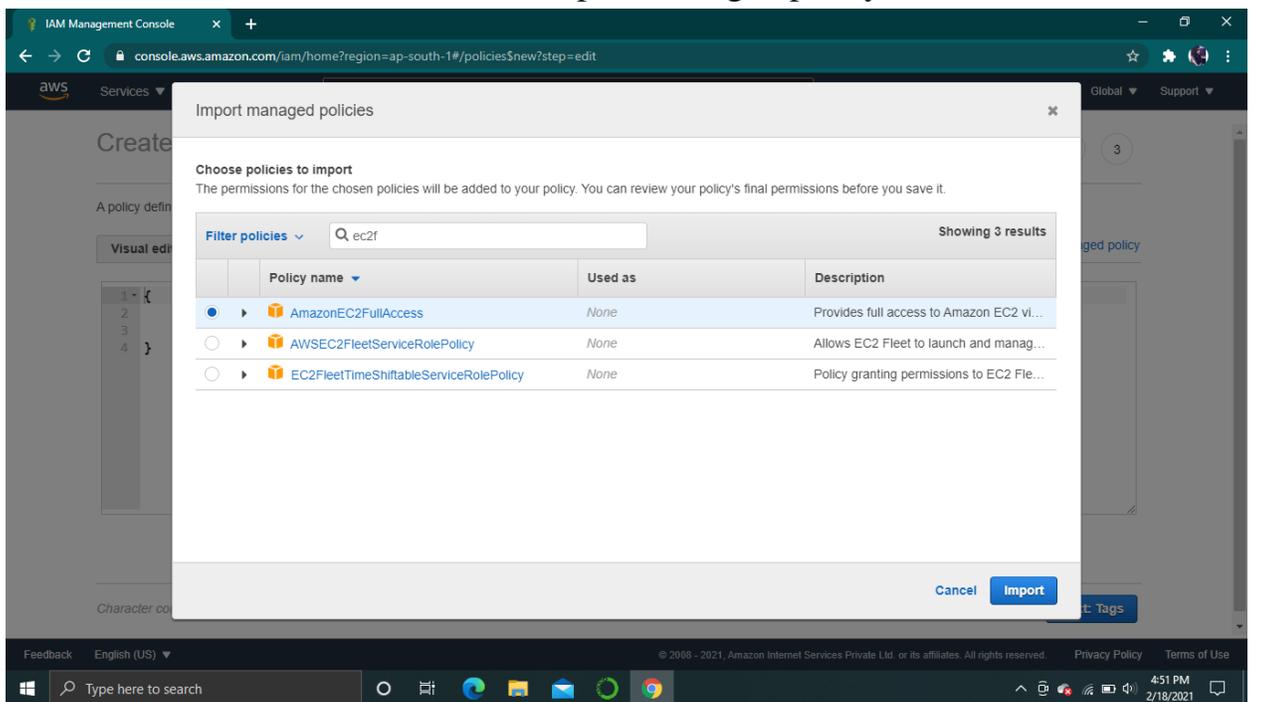
- Sign in to the AWS Management Console and open the IAM service.



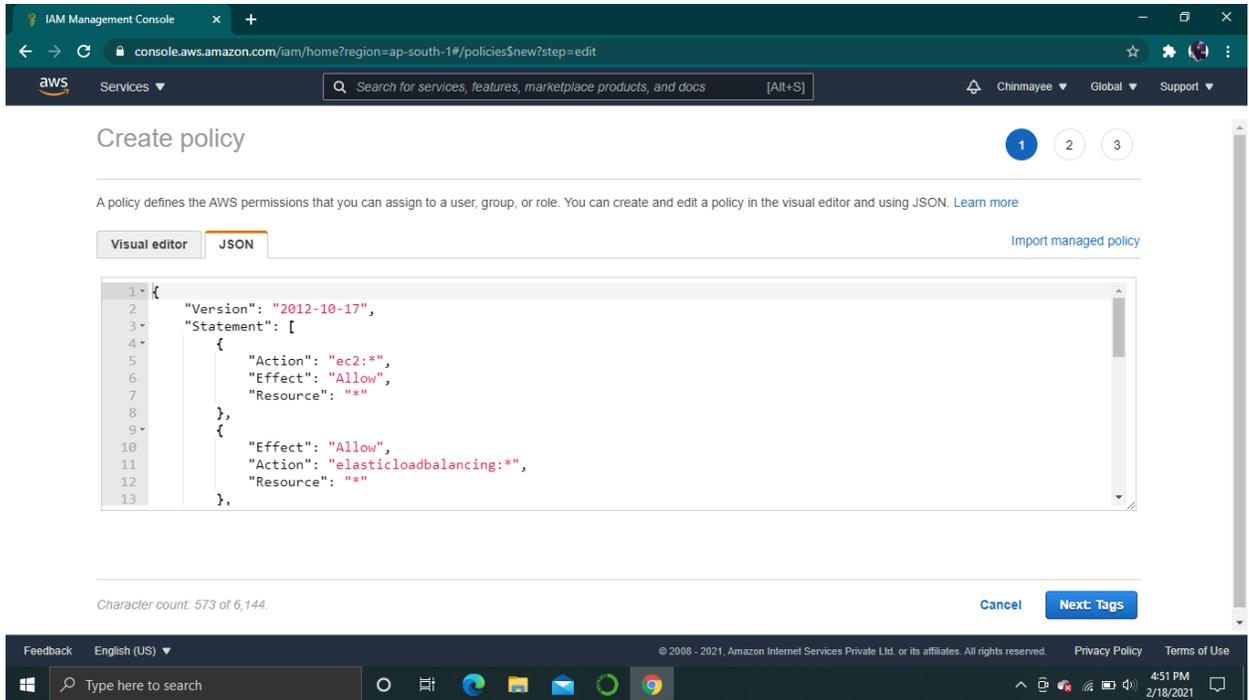
- Choose Policies, and then choose Create Policy.



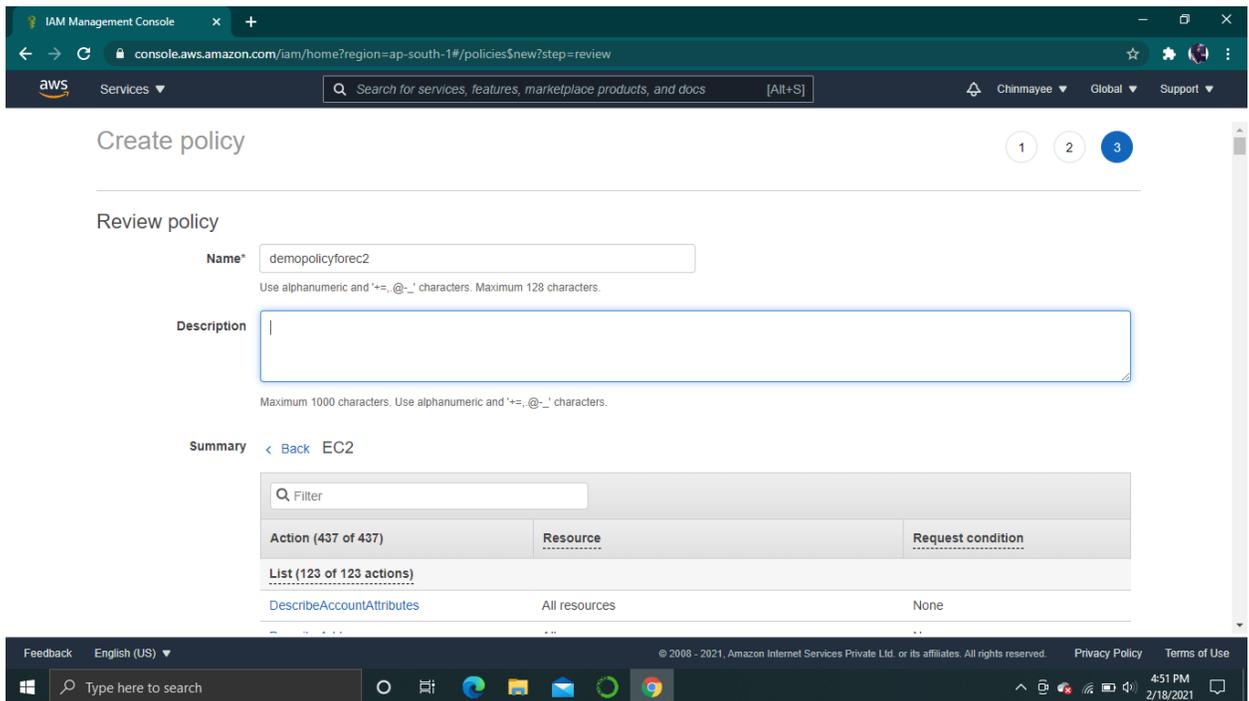
- Select the JSON format and choose import managed policy.



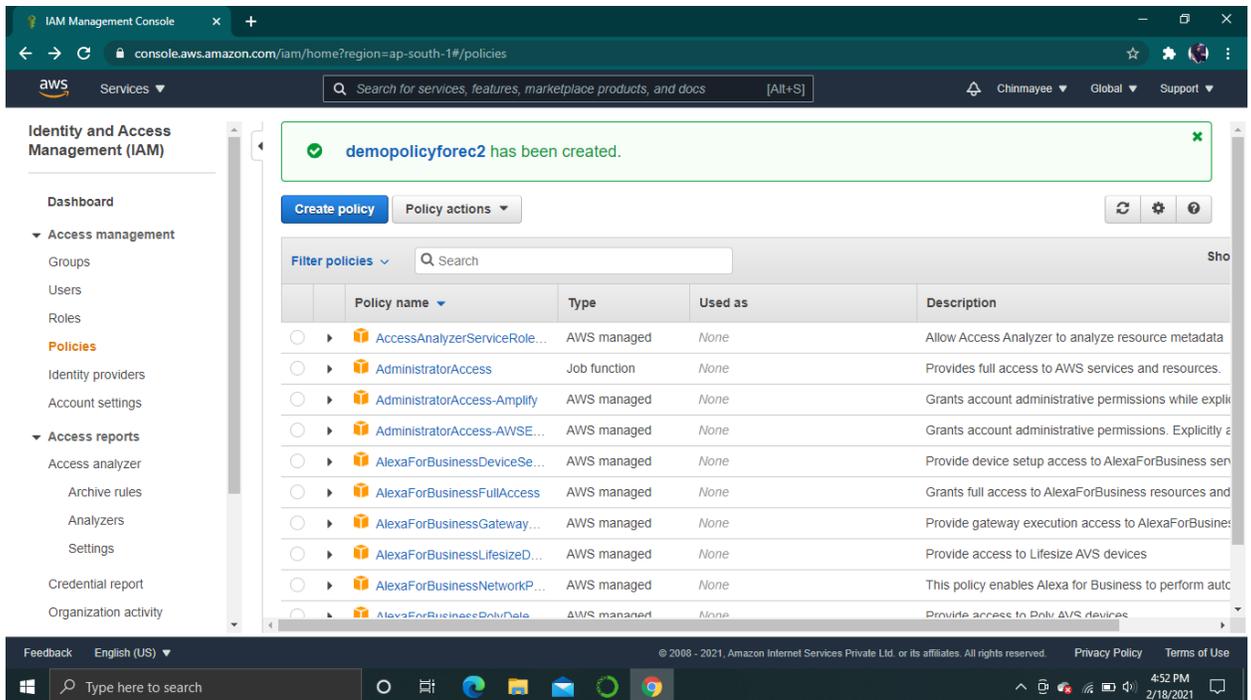
- Select AmazonEC2FullAccess and import it.



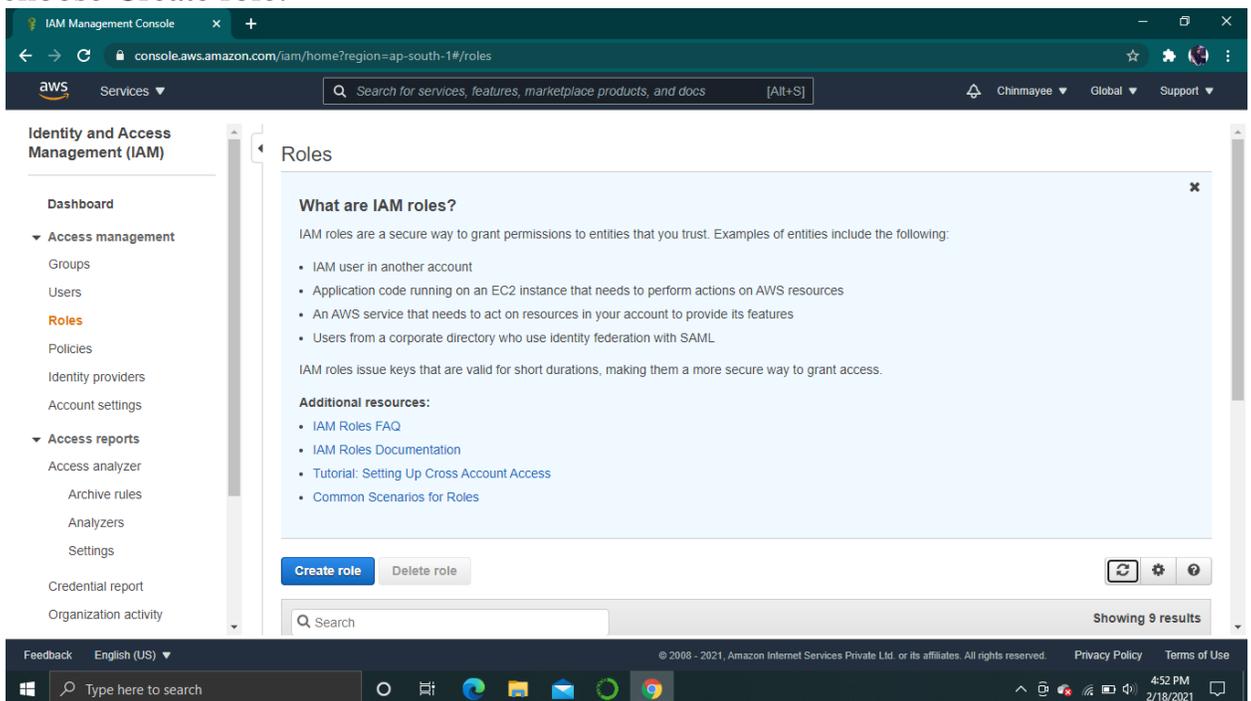
- Choose Next and define the policy with all its description and then select next.



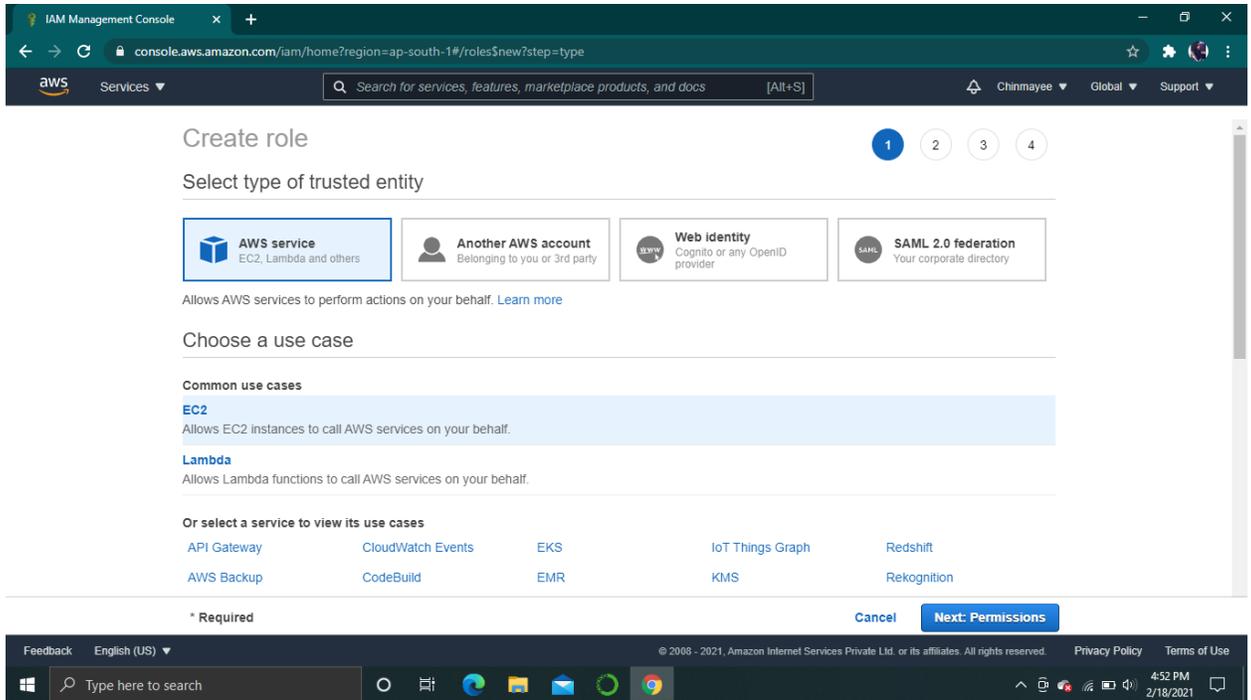
- The policy has been created.



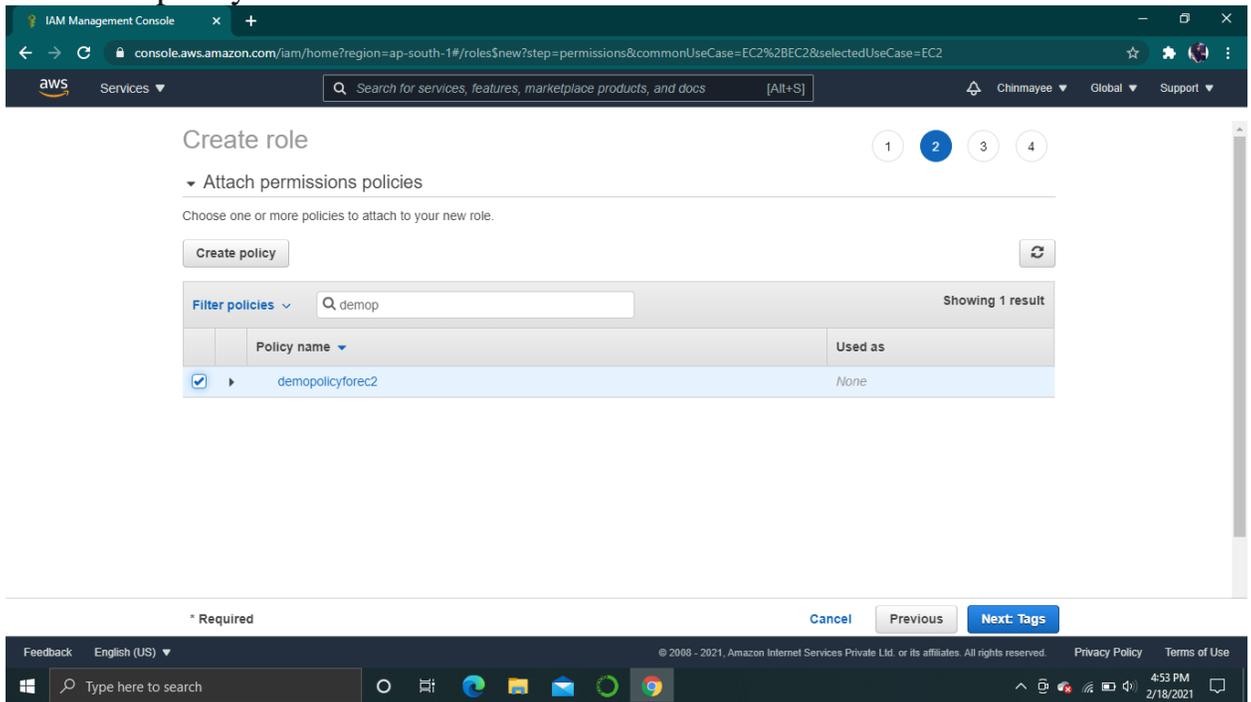
- In the navigation pane of the IAM console, choose Roles, and then choose Create role.



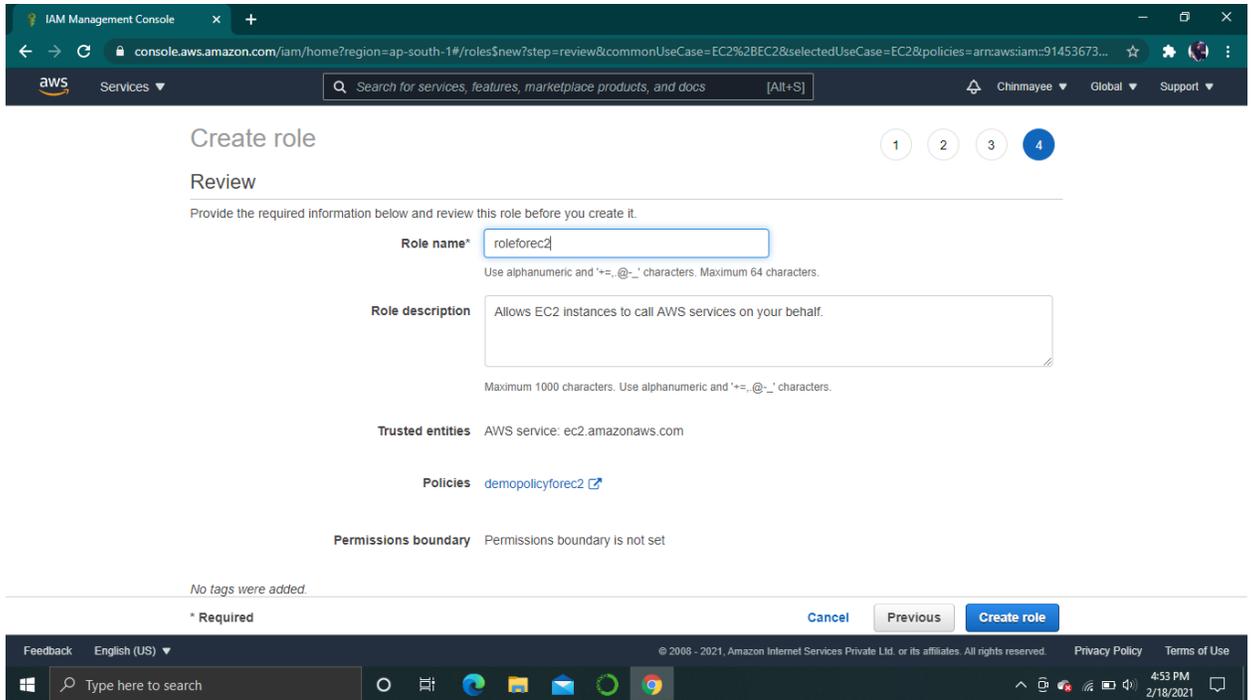
- For Select type of trusted entity, choose AWS service.
- Choose the EC2 service to allow to assume this role.



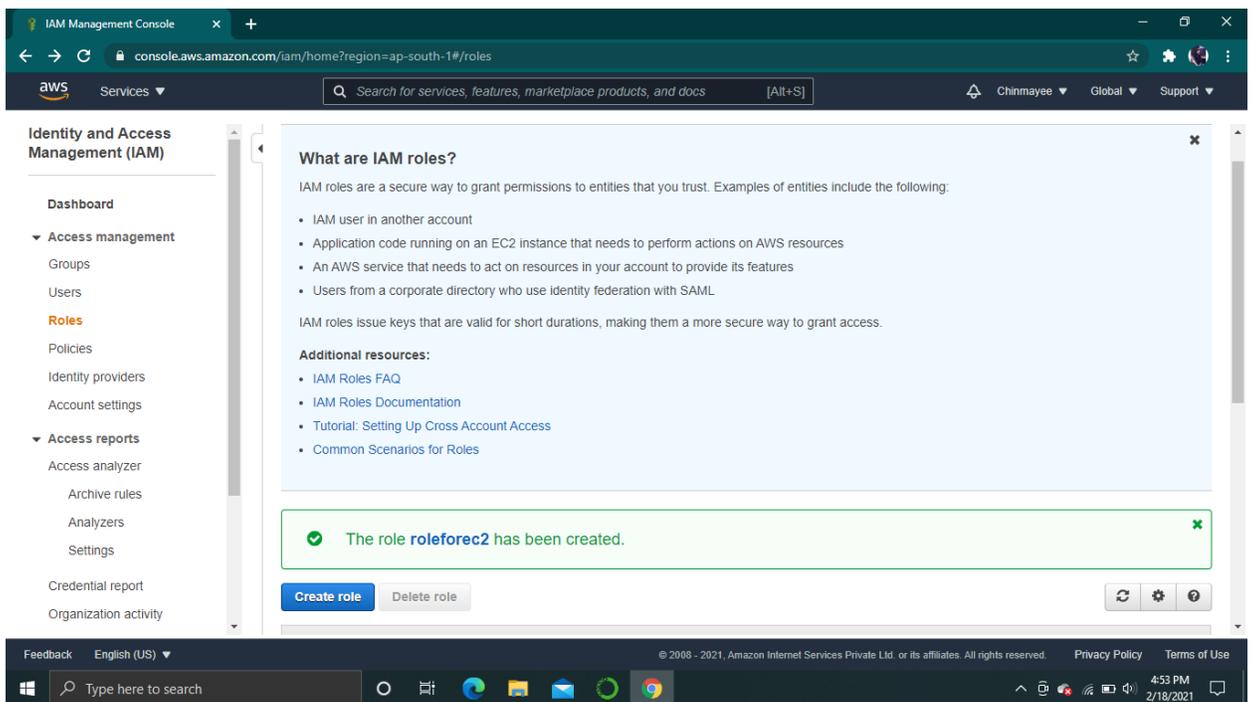
- Choose Next: Permissions.
- Select the policy created earlier.



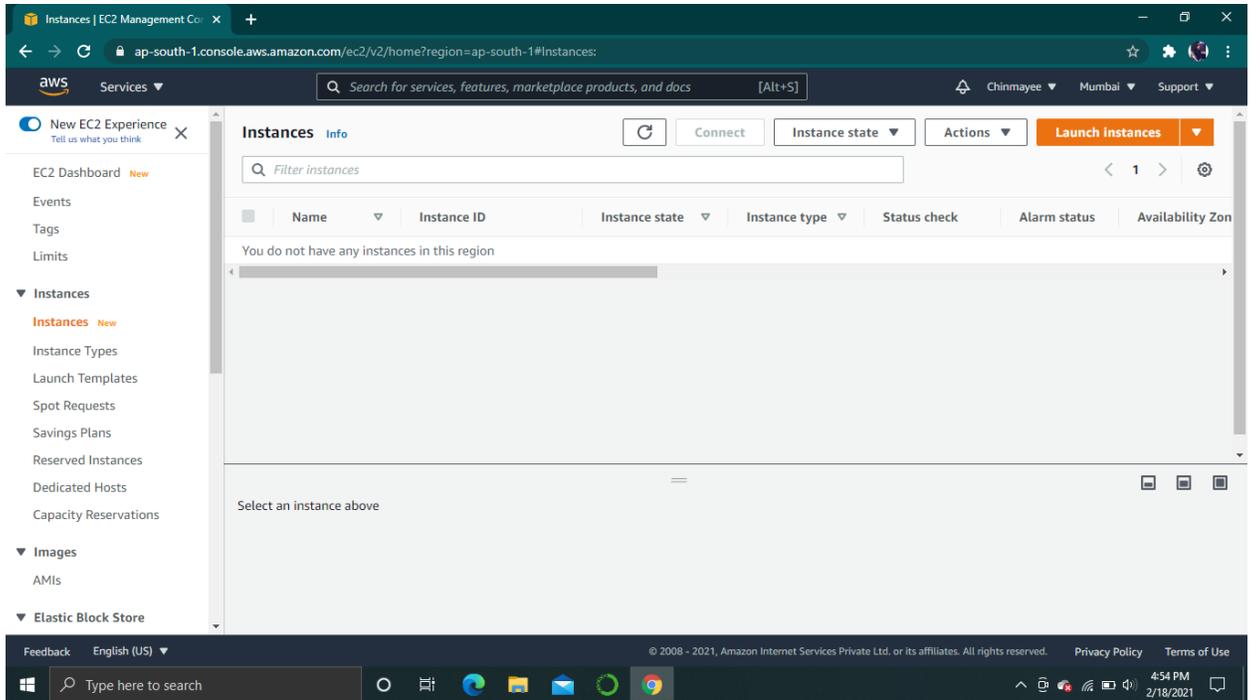
- Choose Next and define the role with all its description and then select next.



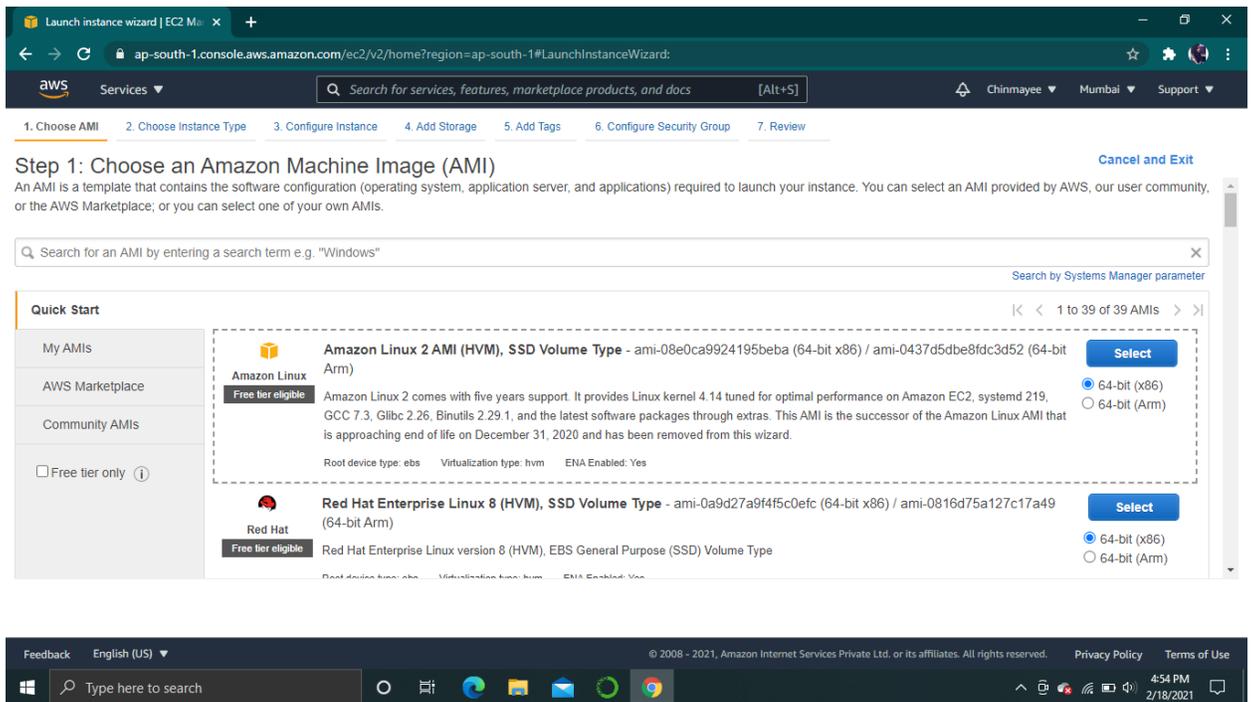
- The IAM role has now been created.



- Open the EC2 console.



- From the navigation bar, choose AMIs.



- Select the AMI, and then choose Launch.
- Choose an instance type, and then choose Next.

Launch instance wizard | EC2 M...

ap-south-1.console.aws.amazon.com/ec2/v2/home?region=ap-south-1#LaunchInstanceWizard:

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

Chinmayee Mumbai Support

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

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 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	Network Performance	IPv6 Support
<input type="checkbox"/>	t2	t2.nano	1	0.5	EBS only	-	Low to Moderate	Yes
<input checked="" type="checkbox"/>	t2	t2.micro Free tier eligible	1	1	EBS only	-	Low to Moderate	Yes
<input type="checkbox"/>	t2	t2.small	1	2	EBS only	-	Low to Moderate	Yes
<input type="checkbox"/>	t2	t2.medium	2	4	EBS only	-	Low to Moderate	Yes
<input type="checkbox"/>	t2	t2.large	2	8	EBS only	-	Low to Moderate	Yes

Cancel Previous **Review and Launch** Next: Configure Instance Details

Feedback English (US)

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

Type here to search

4:54 PM 2/18/2021

- Configure the instance details and add the IAM role to it.

Launch instance wizard | EC2 M...

ap-south-1.console.aws.amazon.com/ec2/v2/home?region=ap-south-1#LaunchInstanceWizard:

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

Chinmayee Mumbai Support

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 Launch into Auto Scaling Group

Purchasing option Request Spot instances

Network Create new VPC

Subnet Create new subnet

Auto-assign Public IP

Placement group Add instance to placement group

Capacity Reservation

Domain join directory Create new directory

IAM role Create new IAM role

None
roleforec2

Cancel Previous **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

Type here to search

4:55 PM 2/18/2021

- Select Next: Add Storage.

Launch instance wizard | EC2 M... x +

ap-south-1.console.aws.amazon.com/ec2/v2/home?region=ap-south-1#LaunchInstanceWizard:

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

Chinmayee Mumbai Support

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

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-07e0efc01c68d3978	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.

[Cancel](#) [Previous](#) [Review and Launch](#) [Next: Add Tags](#)

Feedback English (US) © 2008 - 2021, Amazon Internet Services Private Ltd. or its affiliates. All rights reserved. Privacy Policy Terms of Use

Type here to search

4:55 PM 2/18/2021

- **Configure the security group.**

Launch instance wizard | EC2 M... x +

ap-south-1.console.aws.amazon.com/ec2/v2/home?region=ap-south-1#LaunchInstanceWizard:

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

Chinmayee Mumbai Support

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

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

[Add Rule](#)

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](#)

Feedback English (US) © 2008 - 2021, Amazon Internet Services Private Ltd. or its affiliates. All rights reserved. Privacy Policy Terms of Use

Type here to search

4:55 PM 2/18/2021

- **Select review and launch the instance.**

Launch instance wizard | EC2 M... x +

ap-south-1.console.aws.amazon.com/ec2/v2/home?region=ap-south-1#LaunchInstanceWizard:

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

Chinmayee Mumbai Support

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

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.

⚠ Improve your instances' security. Your security group, launch-wizard-2, 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](#)

AMI Details [Edit AMI](#)

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...

Root Device Type: ebs Virtualization type: hvm

Instance Type [Edit 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

Cancel Previous **Launch**

Feedback English (US) © 2008 - 2021, Amazon Internet Services Private Ltd. or its affiliates. All rights reserved. Privacy Policy Terms of Use

Type here to search 4:55 PM 2/18/2021

- Confirm the status of the instance from the dashboard.

Instances | EC2 Management Co... x +

ap-south-1.console.aws.amazon.com/ec2/v2/home?region=ap-south-1#Instances:

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

Chinmayee Mumbai Support

New EC2 Experience Tell us what you think

EC2 Dashboard **New**

Events

Tags

Limits

Instances

Instances **New**

Instance Types

Launch Templates

Spot Requests

Savings Plans

Reserved Instances

Dedicated Hosts

Capacity Reservations

Images

AMIs

Instances (1/1) Info

Filter instances

Connect Instance state Actions **Launch instances**

<input checked="" type="checkbox"/>	Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone
<input checked="" type="checkbox"/>	-	i-0377f705f64715bcd	● Running	t2.micro	Initializing	No alarms +	ap-south-1b

Instance summary Info

Instance ID	Public IPv4 address	Private IPv4 addresses
i-0377f705f64715bcd	13.233.101.3 open address	172.31.15.180
Instance state	Public IPv4 DNS	Private IPv4 DNS
● Running	ec2-13-233-101-3.ap-south-	ip-172-31-15-180.ap-south-

Feedback English (US) © 2008 - 2021, Amazon Internet Services Private Ltd. or its affiliates. All rights reserved. Privacy Policy Terms of Use

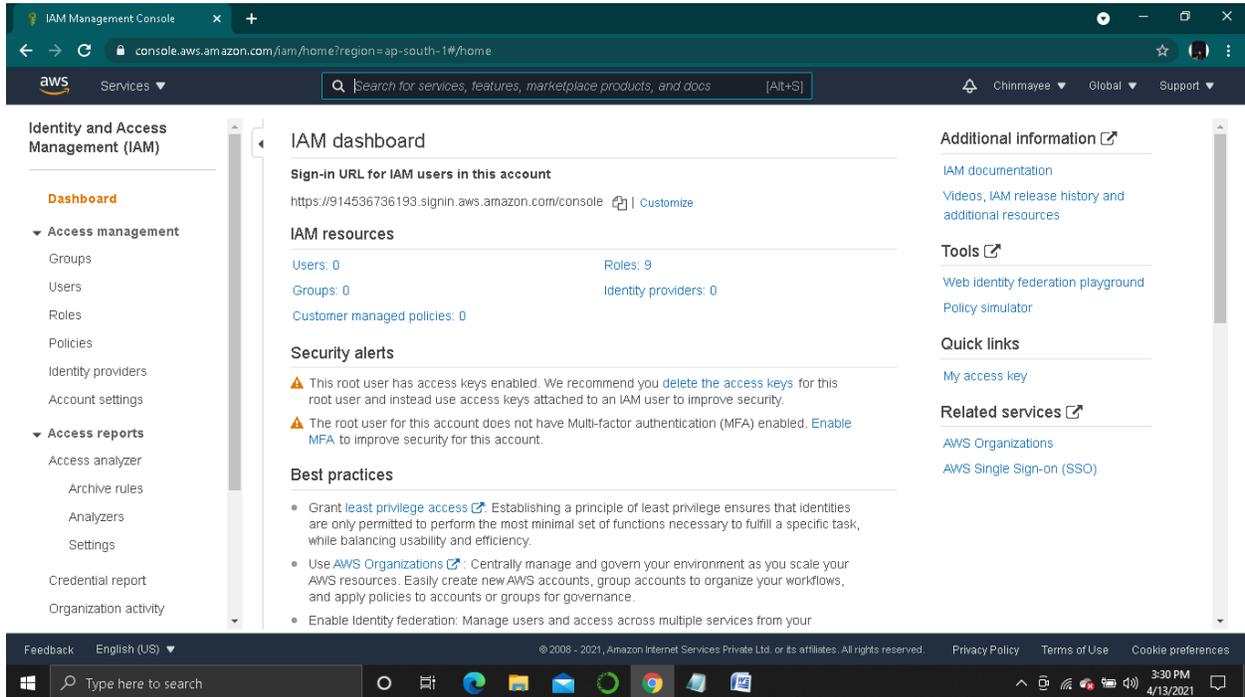
key23.pem Show all

Type here to search 4:56 PM 2/18/2021

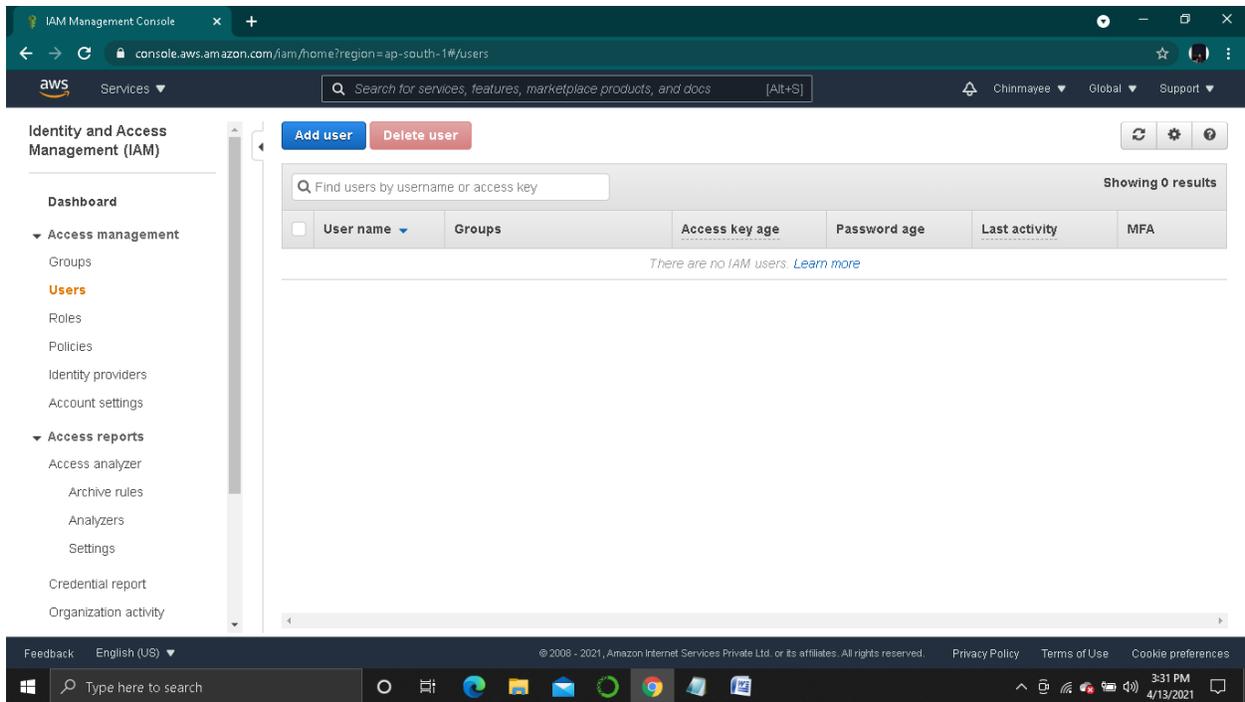
CREATE AN IAM USER AND ROLE

Steps to be Followed:-

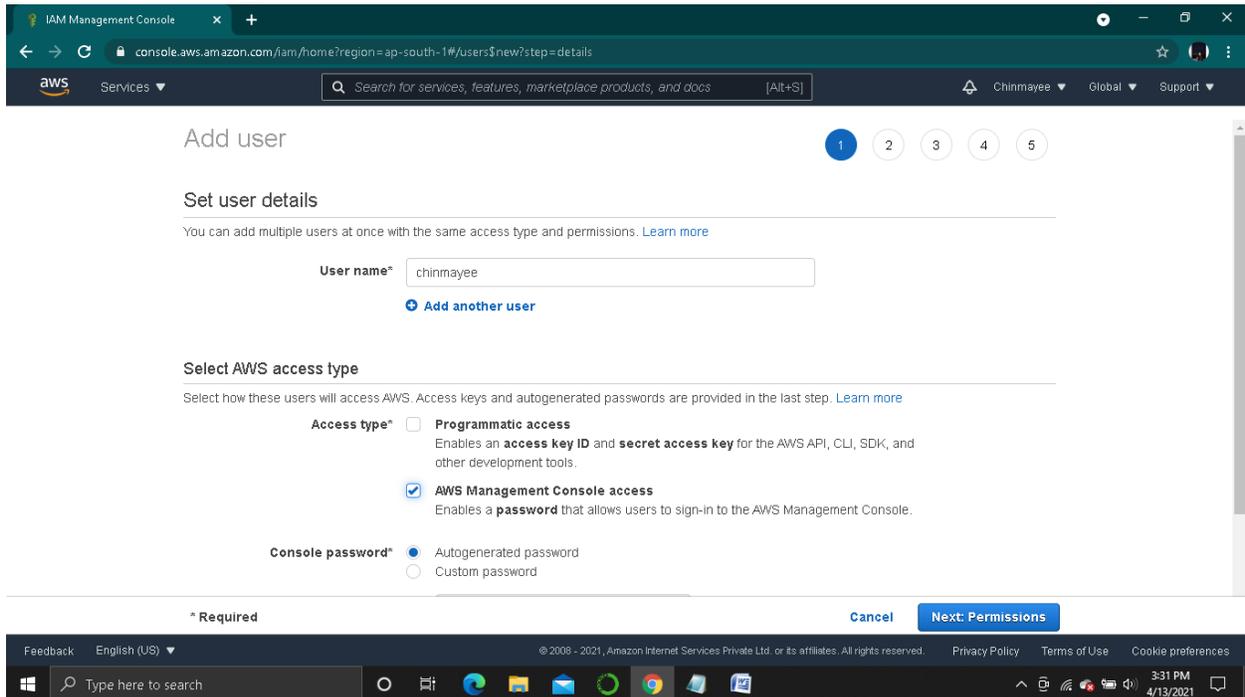
- Sign in to aws management console and search for IAM and the dashboard will appear.



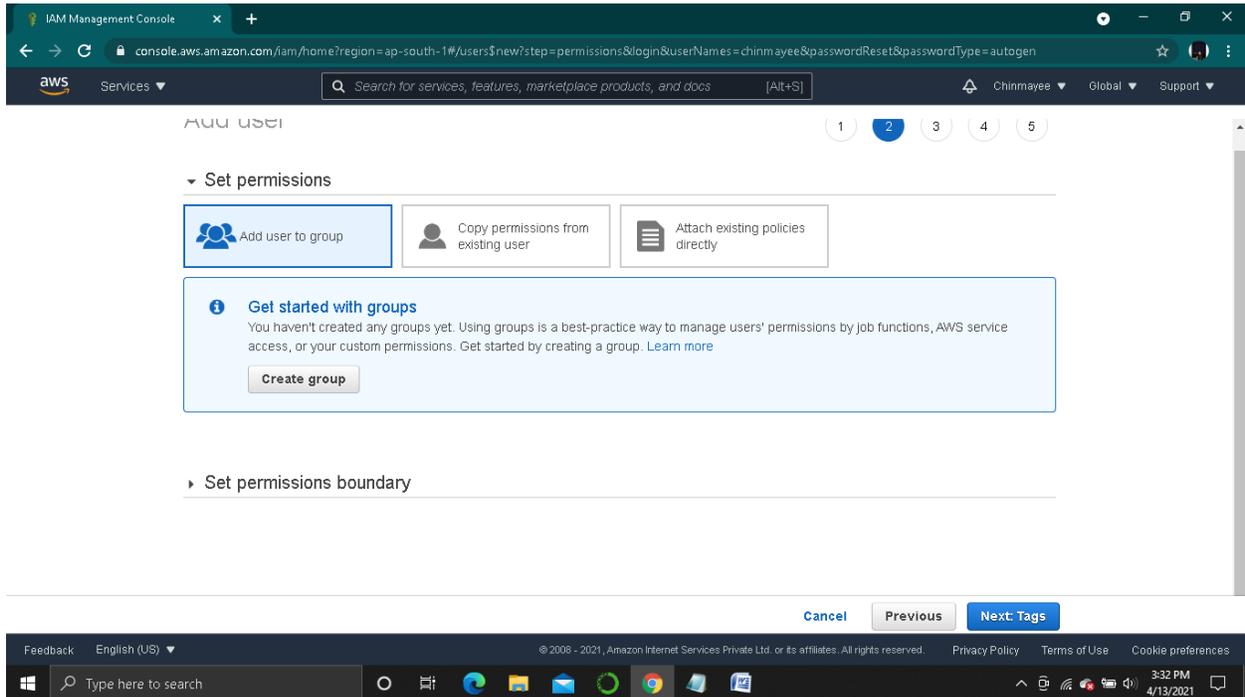
- In navigation pane choose user and then choose add user



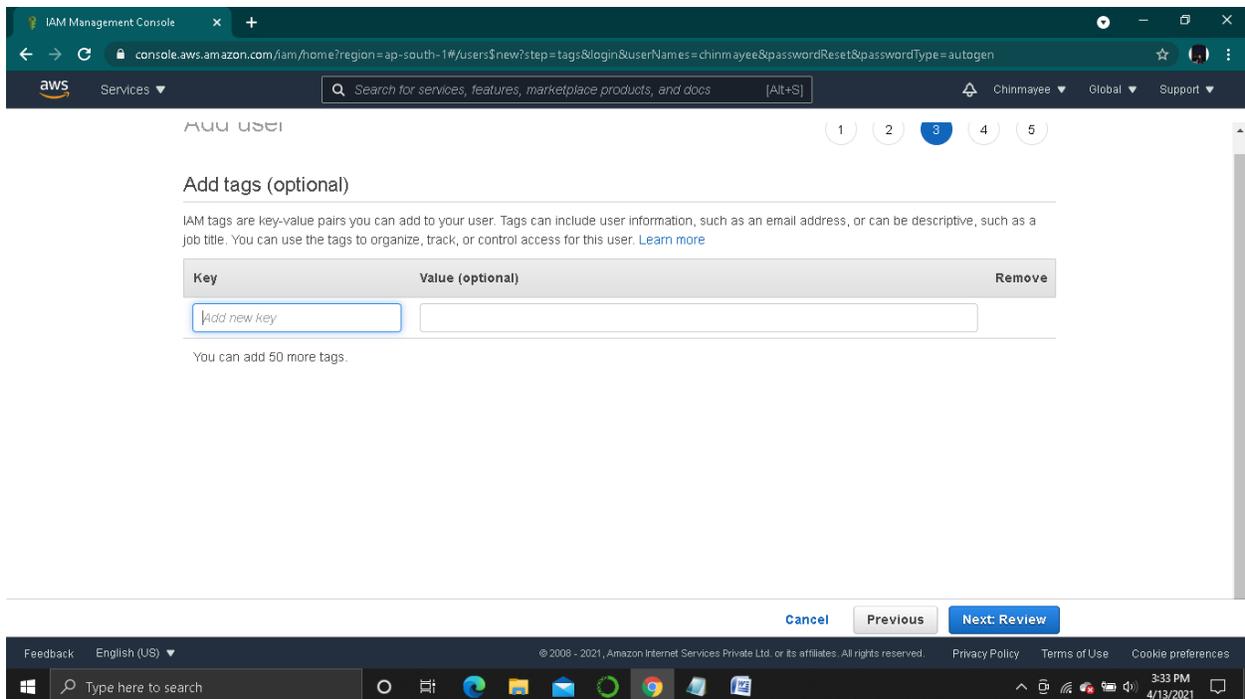
- Give the user a unique name and select the aws management console access type as aws management console access and choose auto generate password



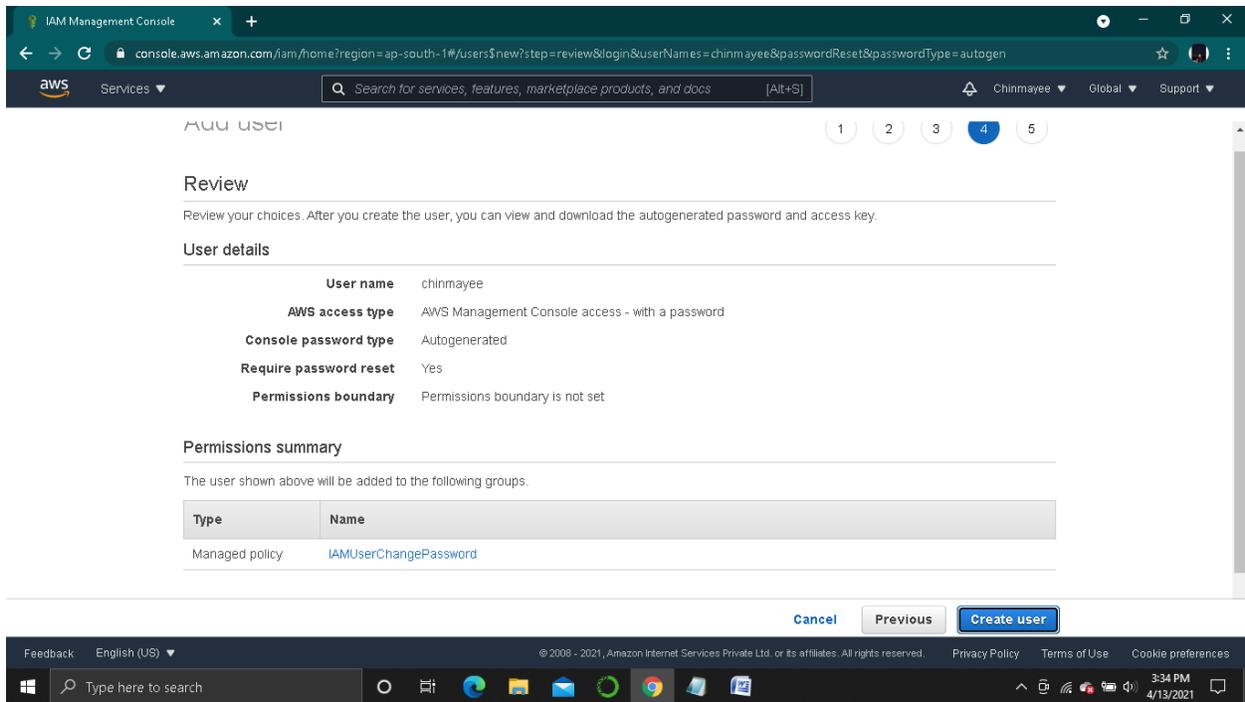
- On set permission assign a permission to set the new user



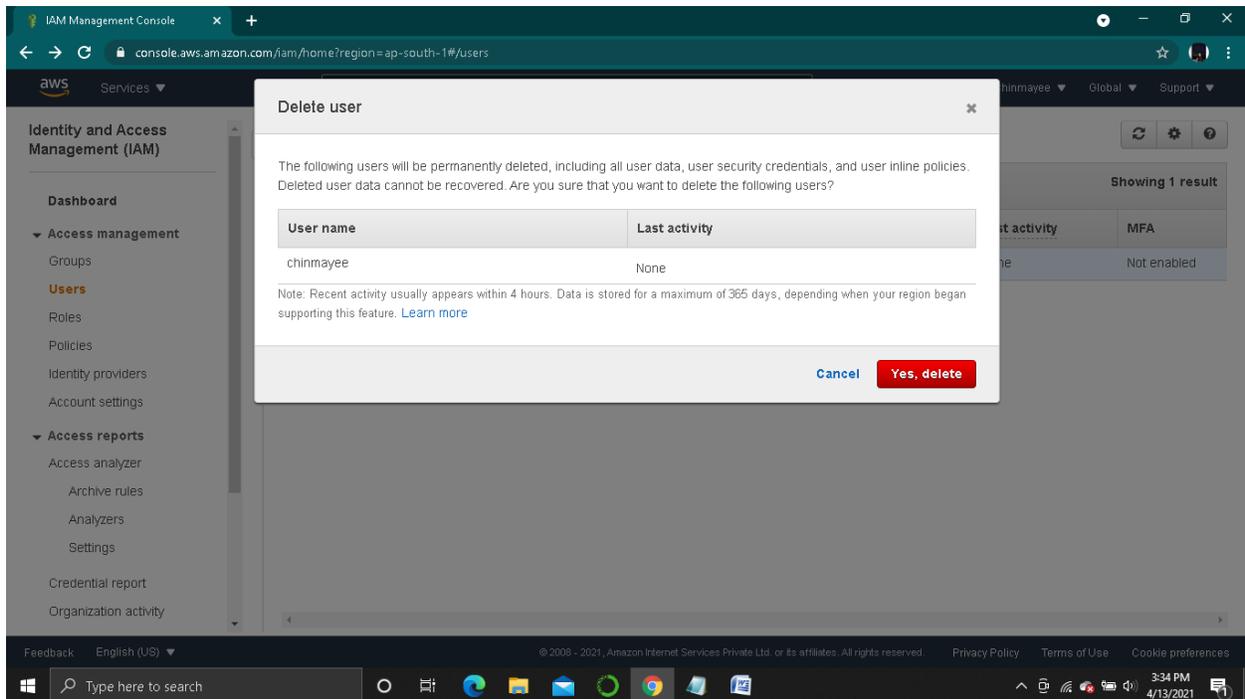
- Add a tag if required its optional and click next



- Click on create user

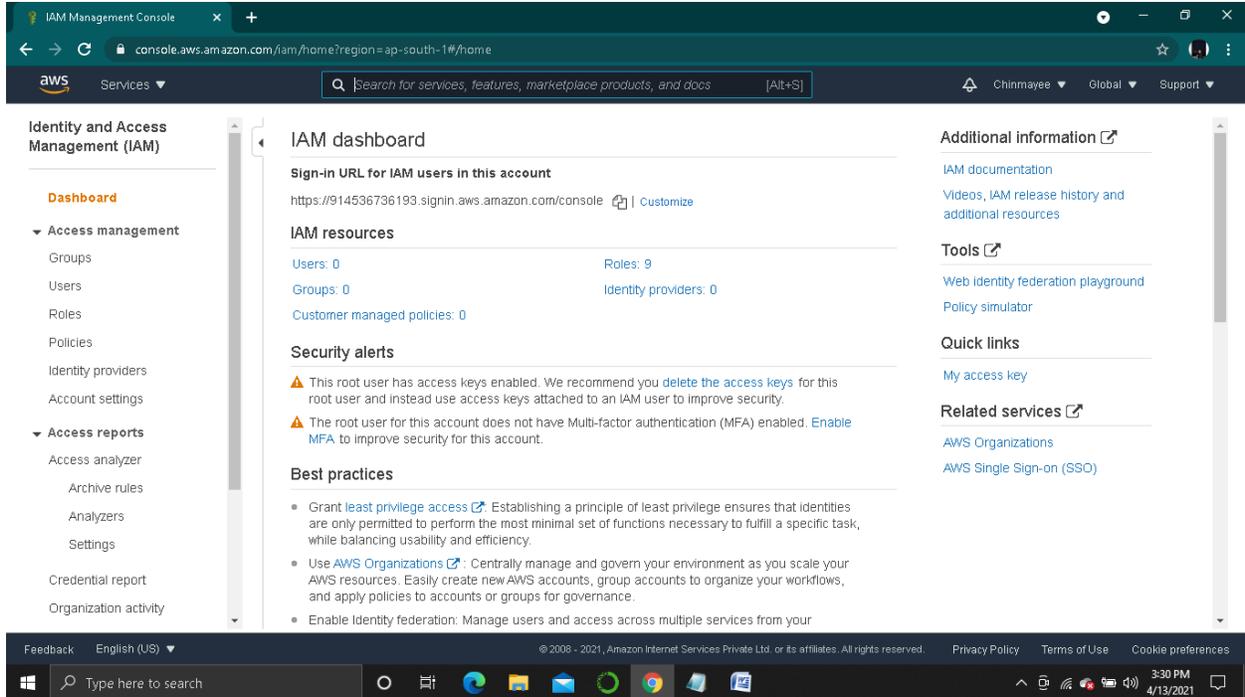


- To delete the user go to IAM console dashboard and click on delete user

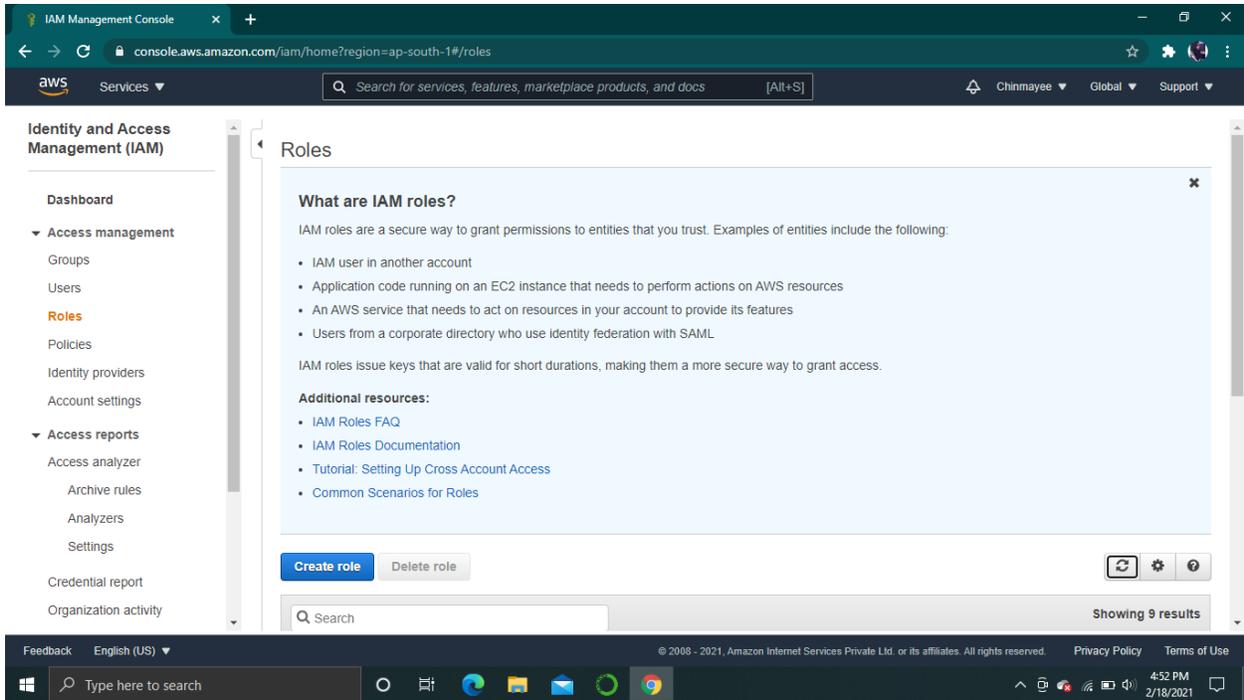


IAM ROLE

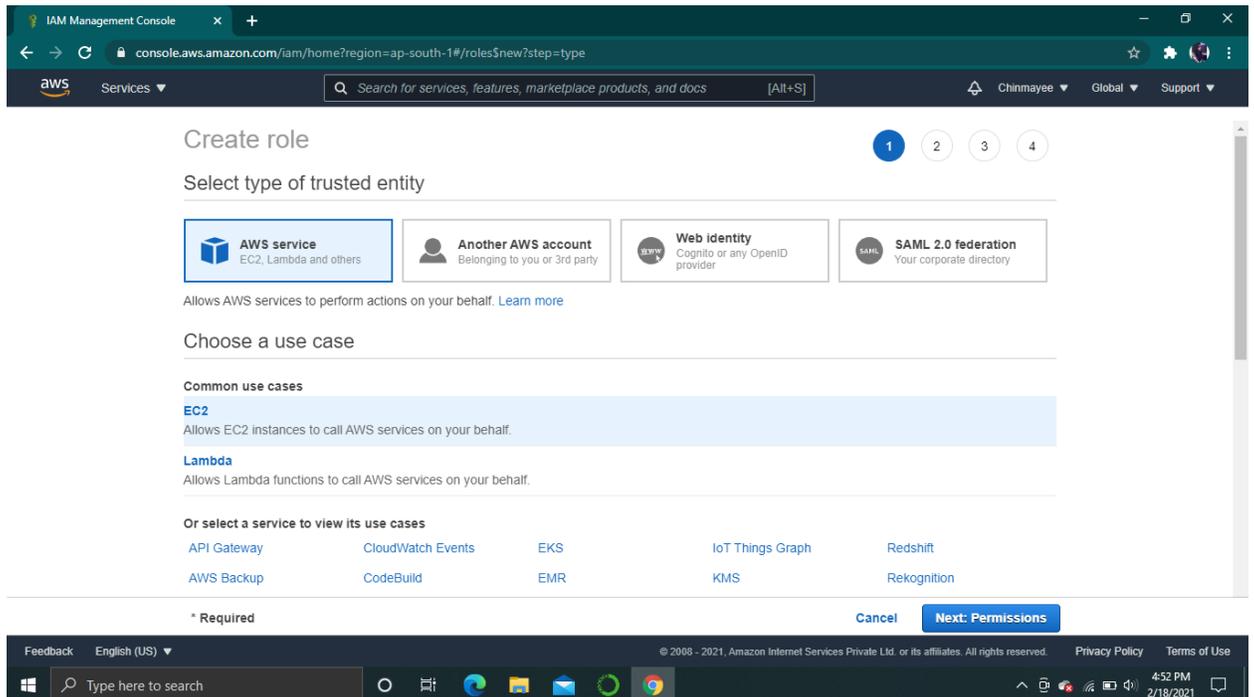
- Sign in to aws management console.



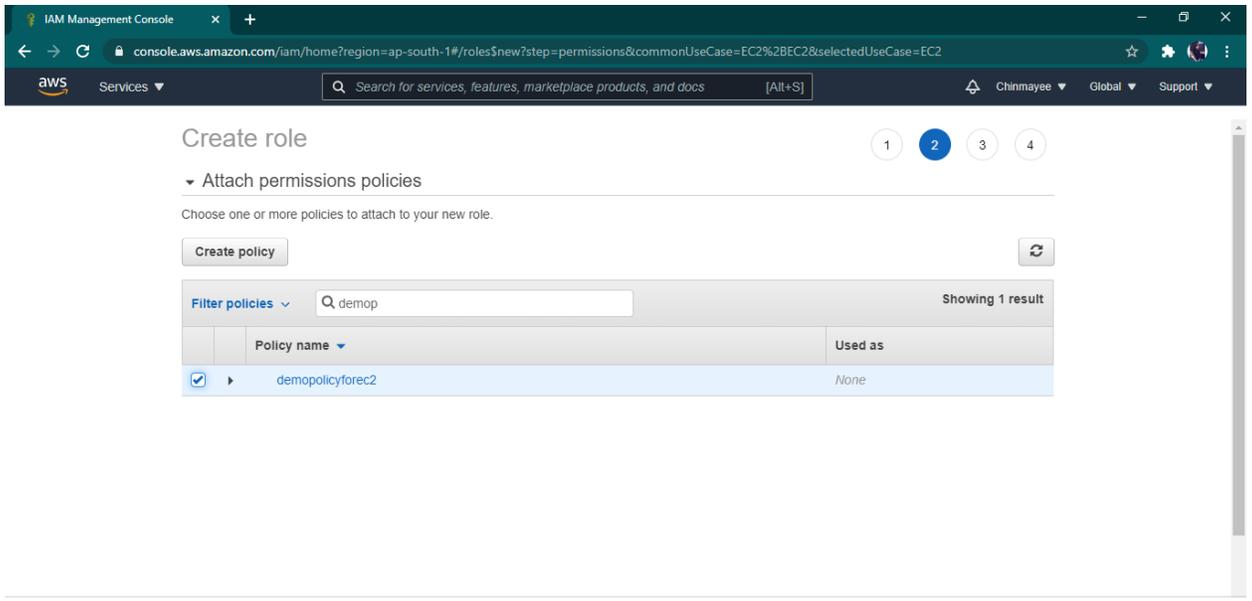
- In navigation panel choose role and then create roles.



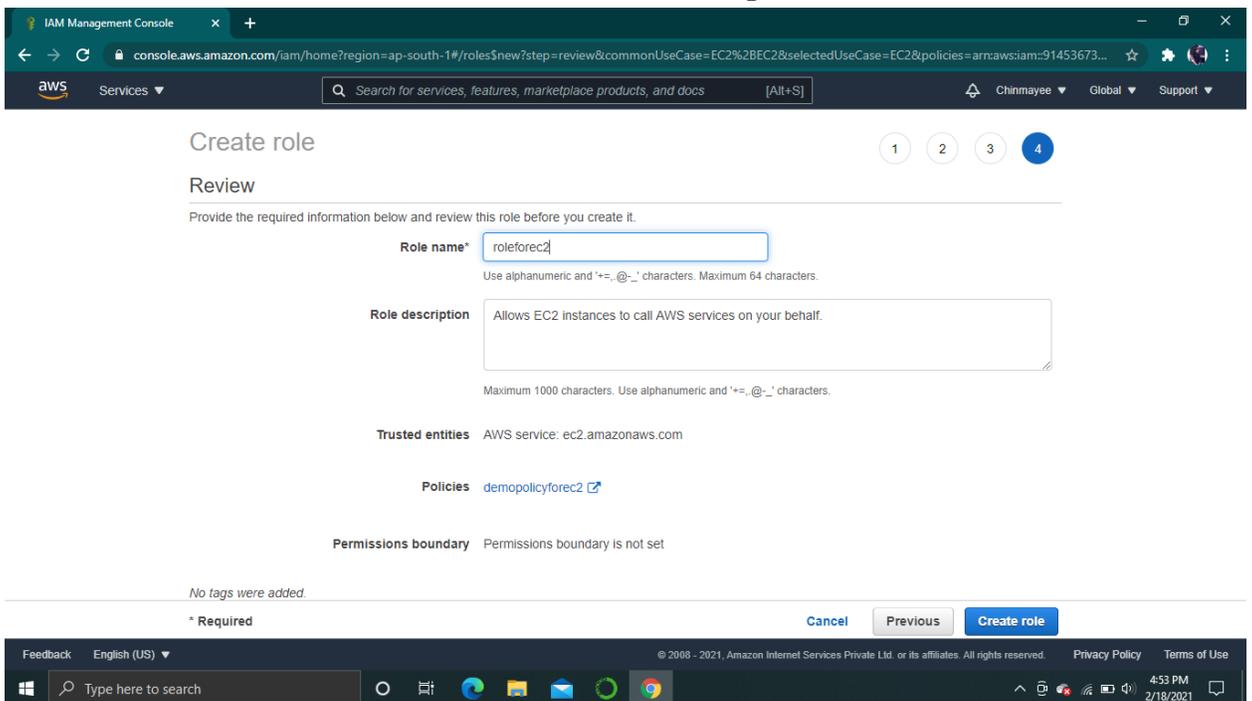
- For Select type of trusted entity, choose AWS service.
- Choose the EC2 service to allow to assume this role.



- Choose Next: Permissions.



- Choose Next and define the role with all its description and then select next.



- The IAM role has now been created.

IAM Management Console

console.aws.amazon.com/iam/home?region=ap-south-1#/roles

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

Chinmayee Global Support

Identity and Access Management (IAM)

- Dashboard
- Access management
 - Groups
 - Users
 - Roles**
 - Policies
 - Identity providers
 - Account settings
- Access reports
 - Access analyzer
 - Archive rules
 - Analyzers
 - Settings
 - Credential report
 - Organization activity

What are IAM roles?

IAM roles are a secure way to grant permissions to entities that you trust. Examples of entities include the following:

- IAM user in another account
- Application code running on an EC2 instance that needs to perform actions on AWS resources
- An AWS service that needs to act on resources in your account to provide its features
- Users from a corporate directory who use identity federation with SAML

IAM roles issue keys that are valid for short durations, making them a more secure way to grant access.

Additional resources:

- [IAM Roles FAQ](#)
- [IAM Roles Documentation](#)
- [Tutorial: Setting Up Cross Account Access](#)
- [Common Scenarios for Roles](#)

✓ The role **roleforec2** has been created.

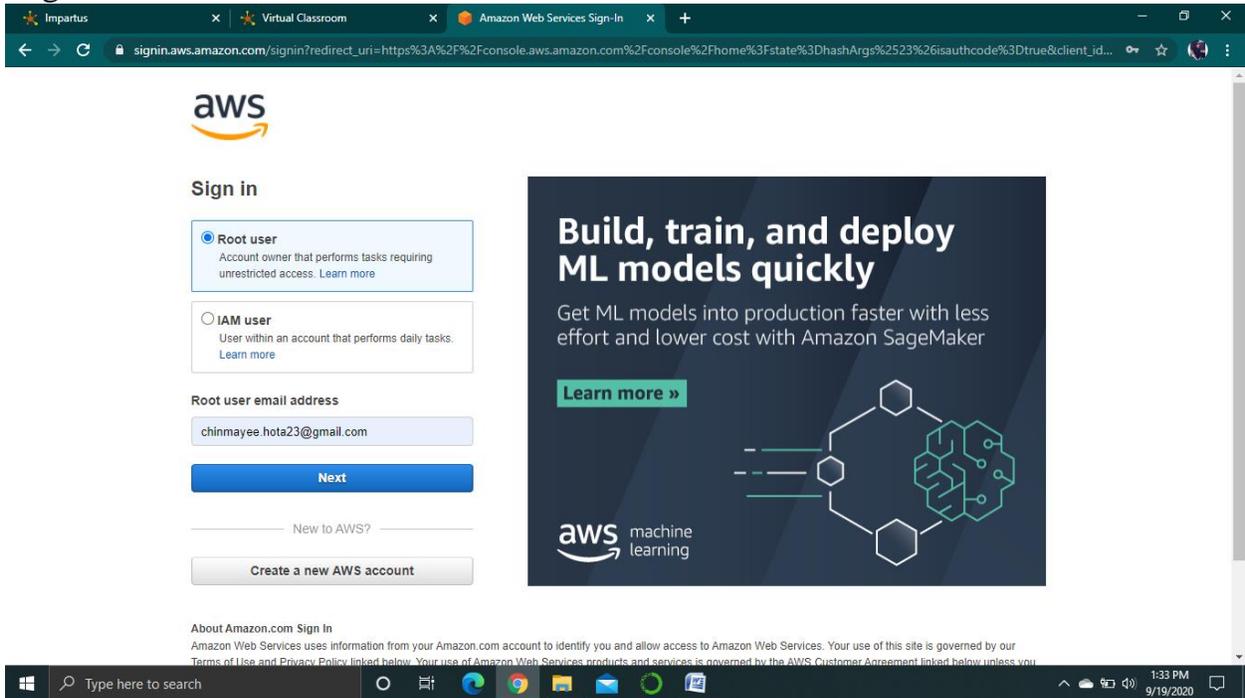
Create role Delete role

Feedback English (US) © 2008 - 2021, Amazon Internet Services Private Ltd. or its affiliates. All rights reserved. Privacy Policy Terms of Use

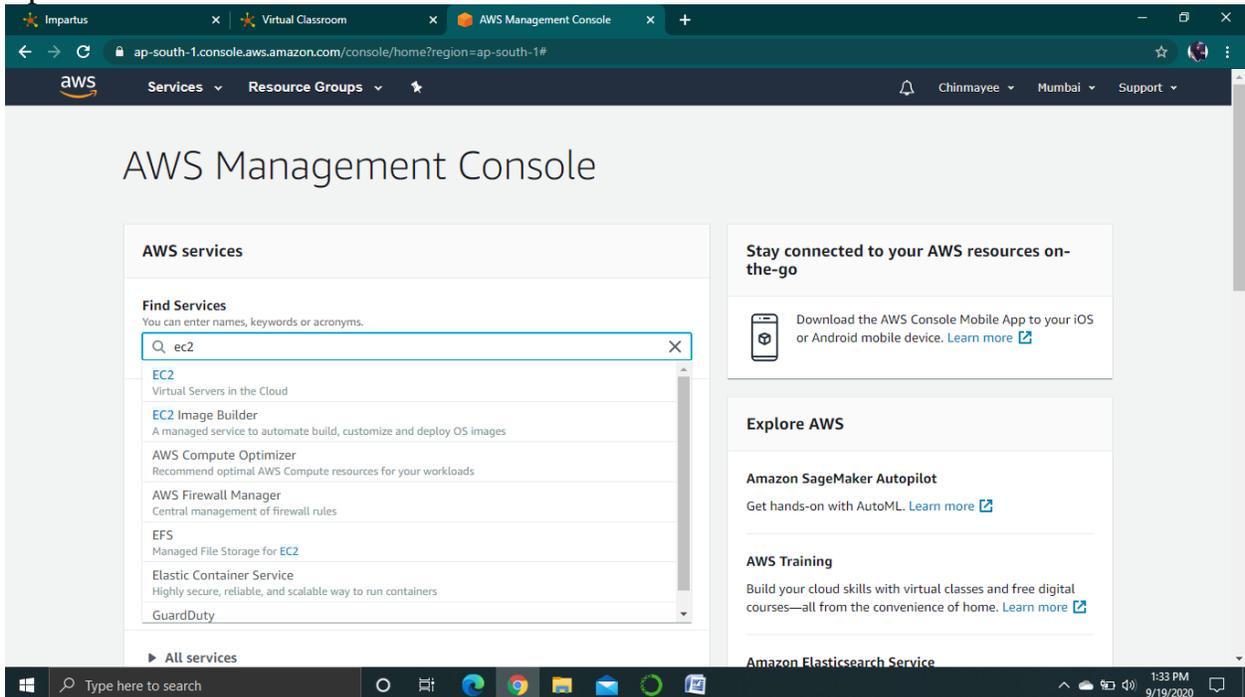
Type here to search 4:53 PM 2/18/2021

IMPLEMENTING ELASTIC LOAD BALANCING

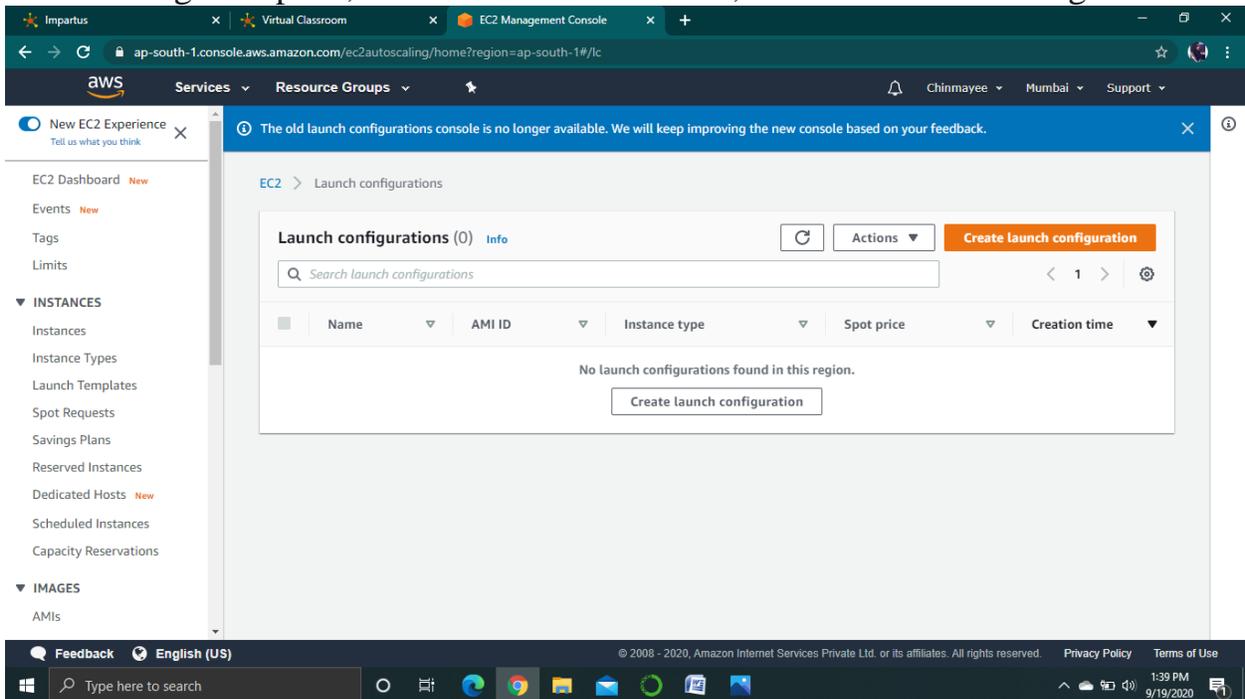
1. Login to AWS console.



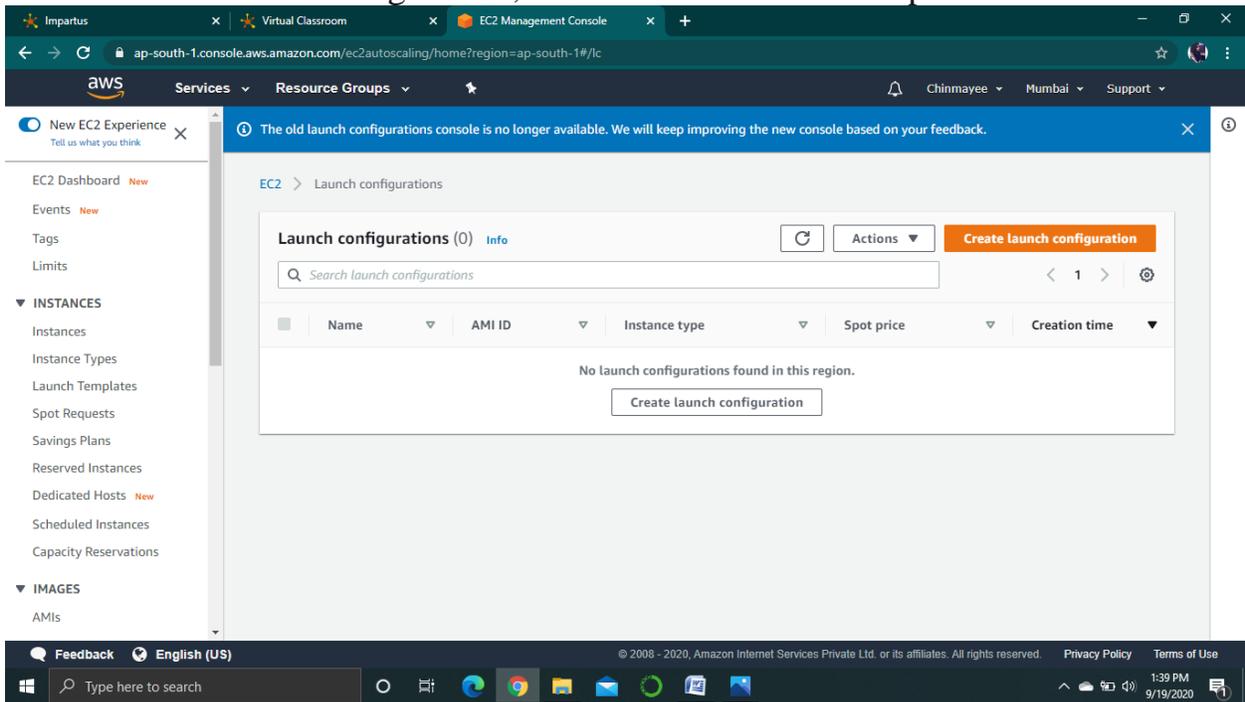
2. Open the Amazon EC2 service.



3. On the navigation pane, under AUTO SCALING, choose Launch Configurations.



4. Create a new launch configuration, and then choose Next Step.

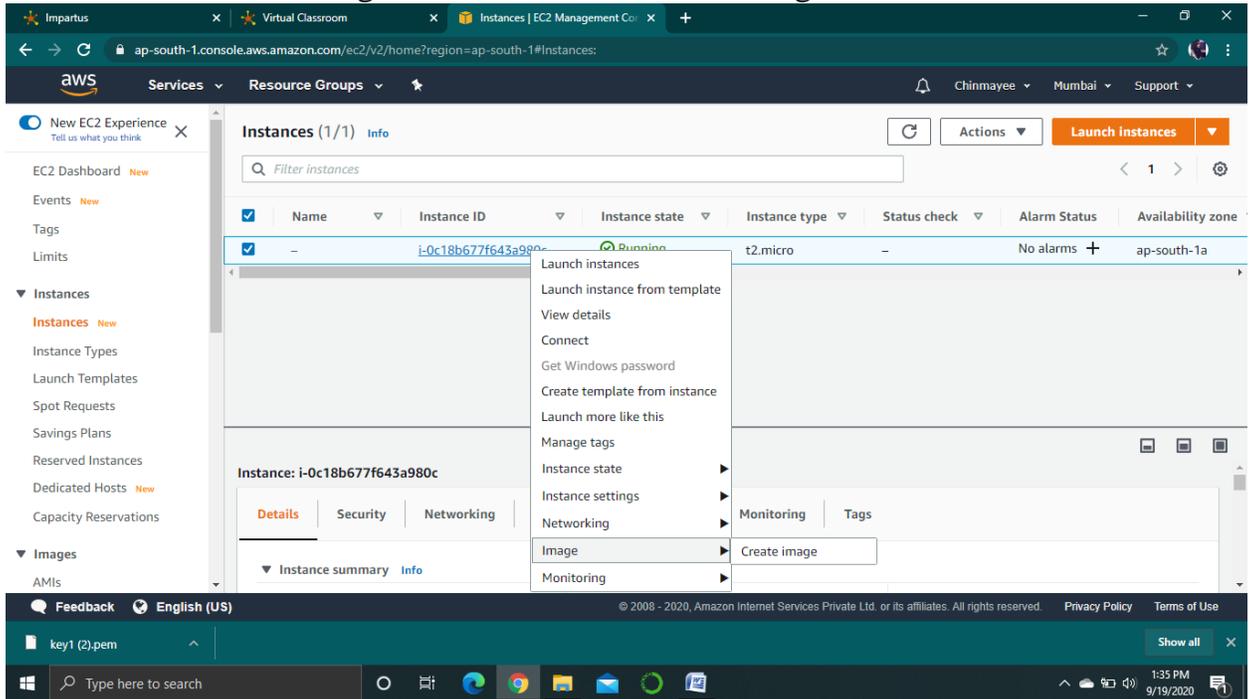


5. Configure all the details.

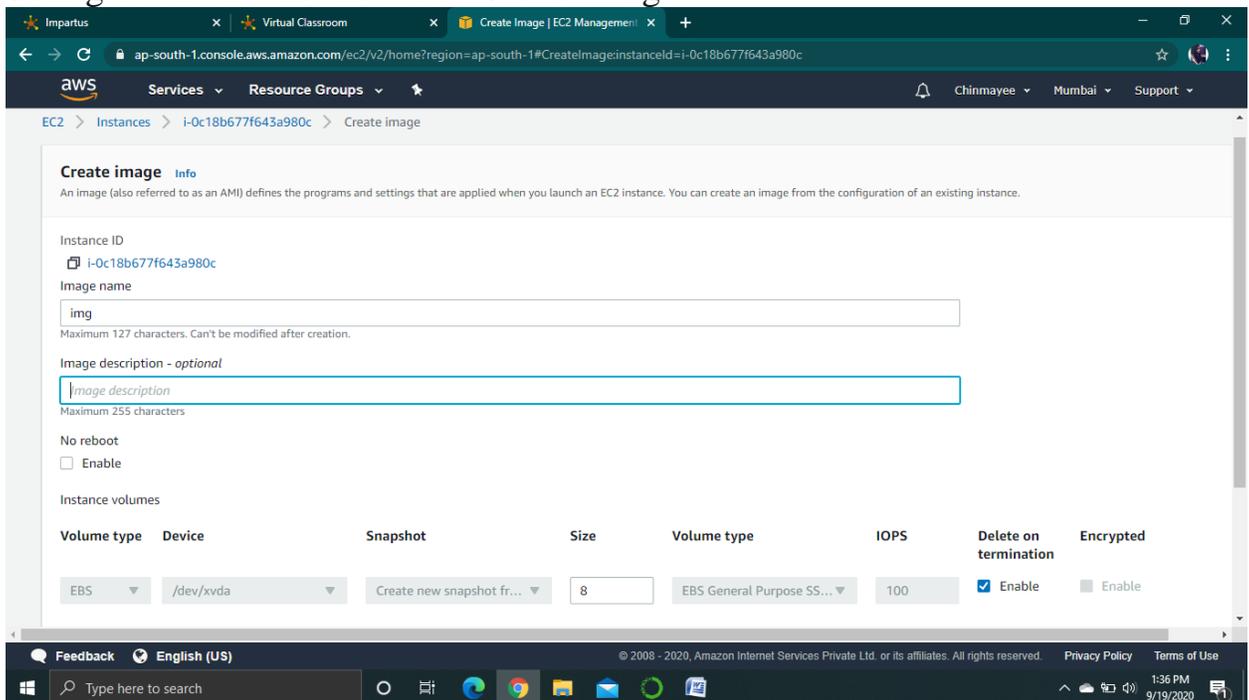
6. For selecting a free eligible AMI.

- Launch an EC2 instance.

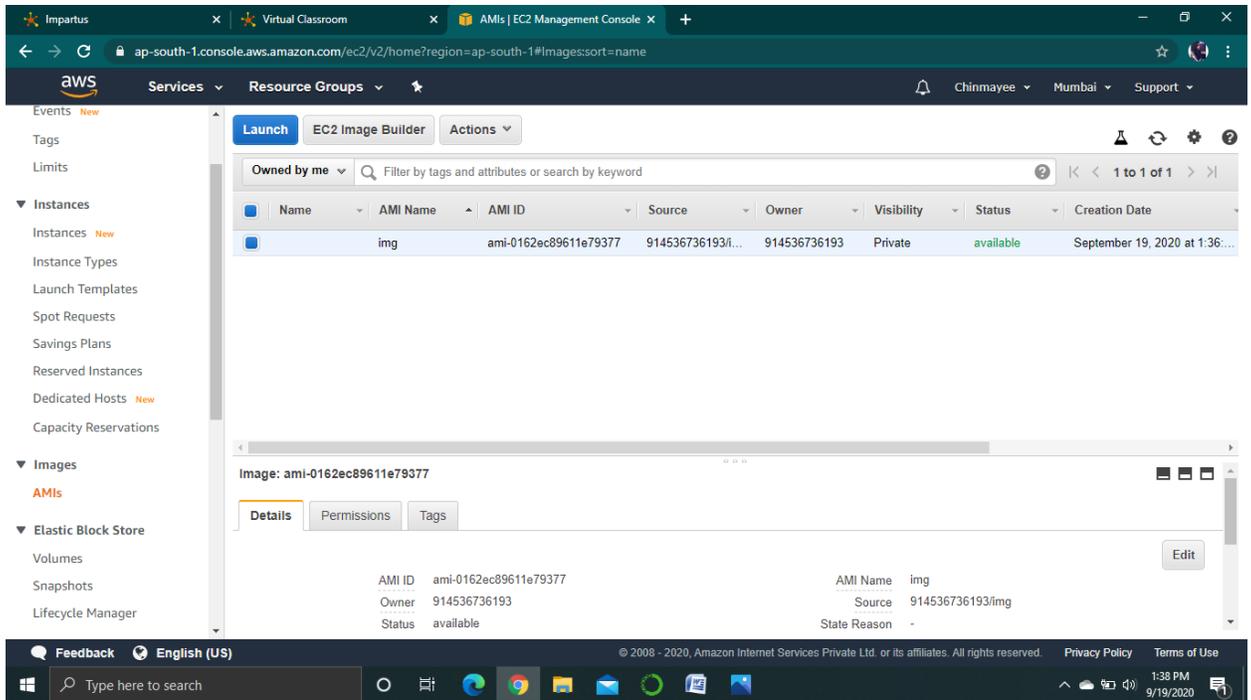
- Select the EC2 instance and choose actions.
- From actions select Image and then select Create Image.



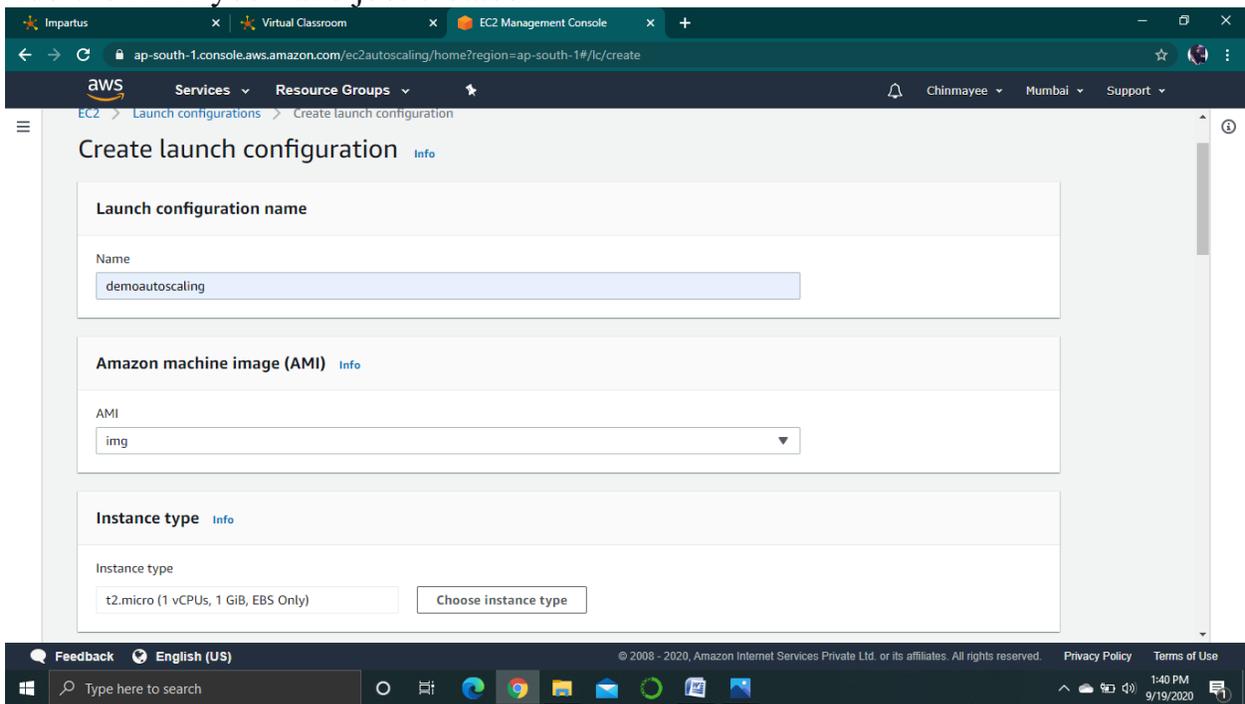
- Configure the details and select Create Image.



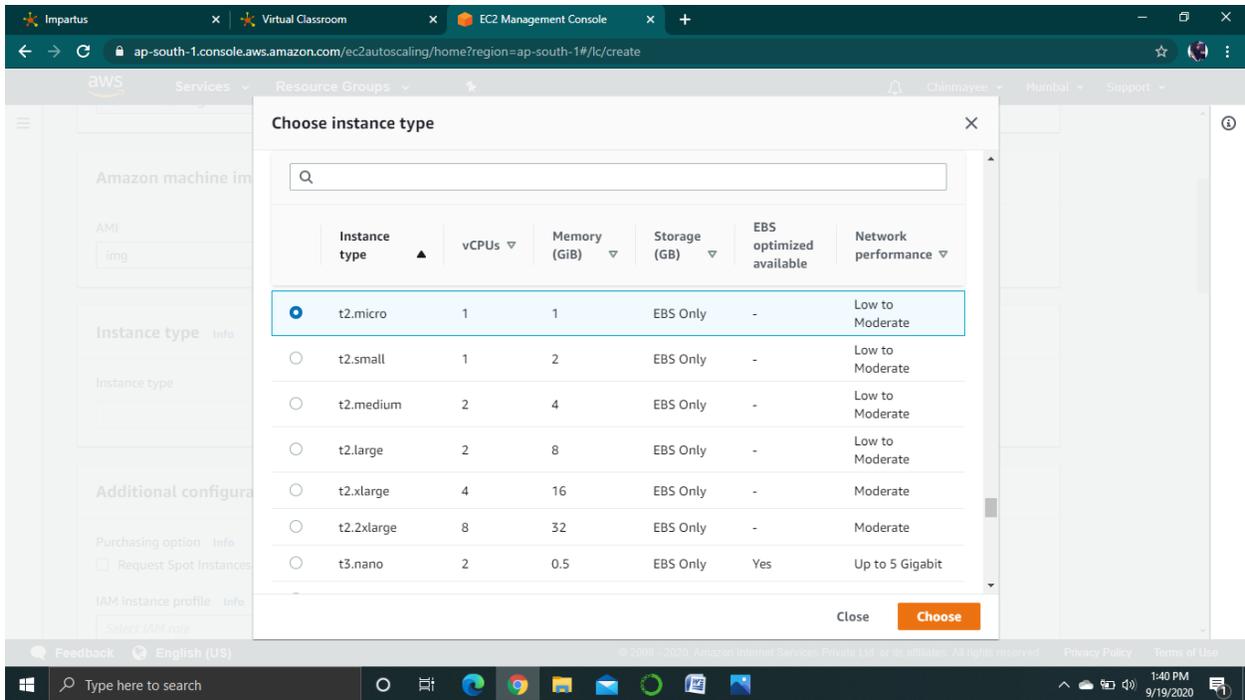
- From the AMI dashboard check the status.



7. Add the AMI you have just created.

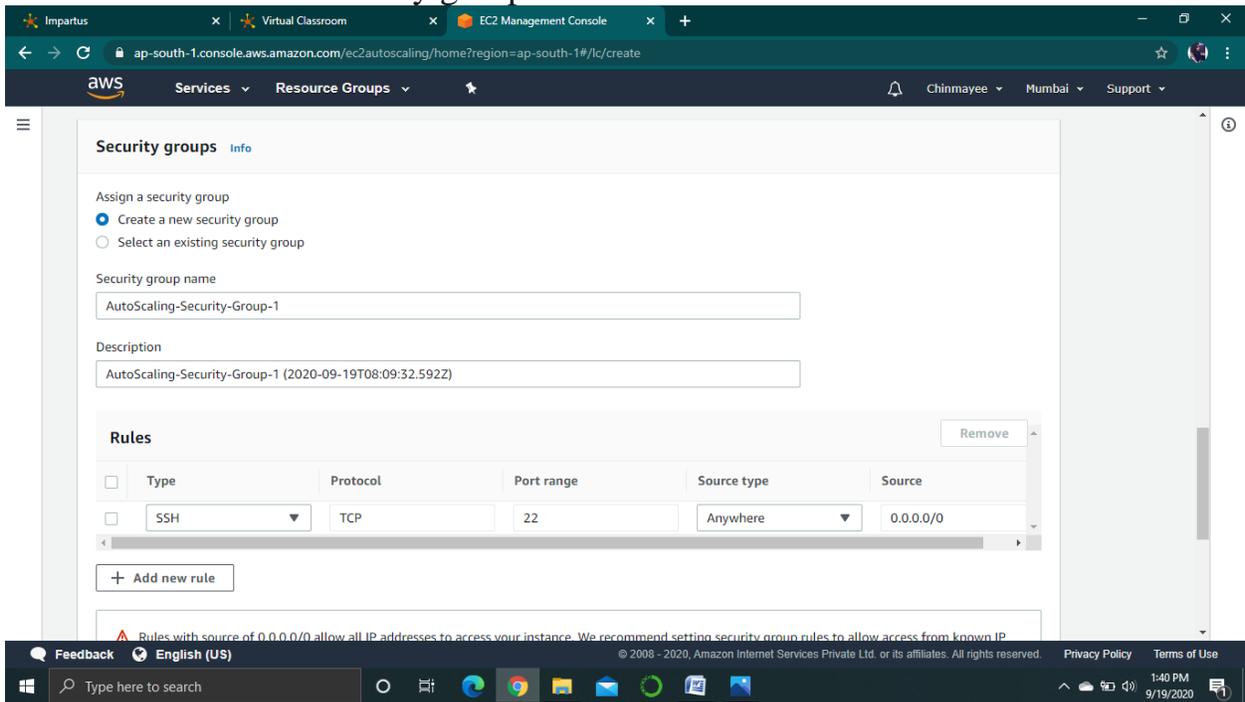


8. For the Choose Instance Type step, select a t2.micro instance.



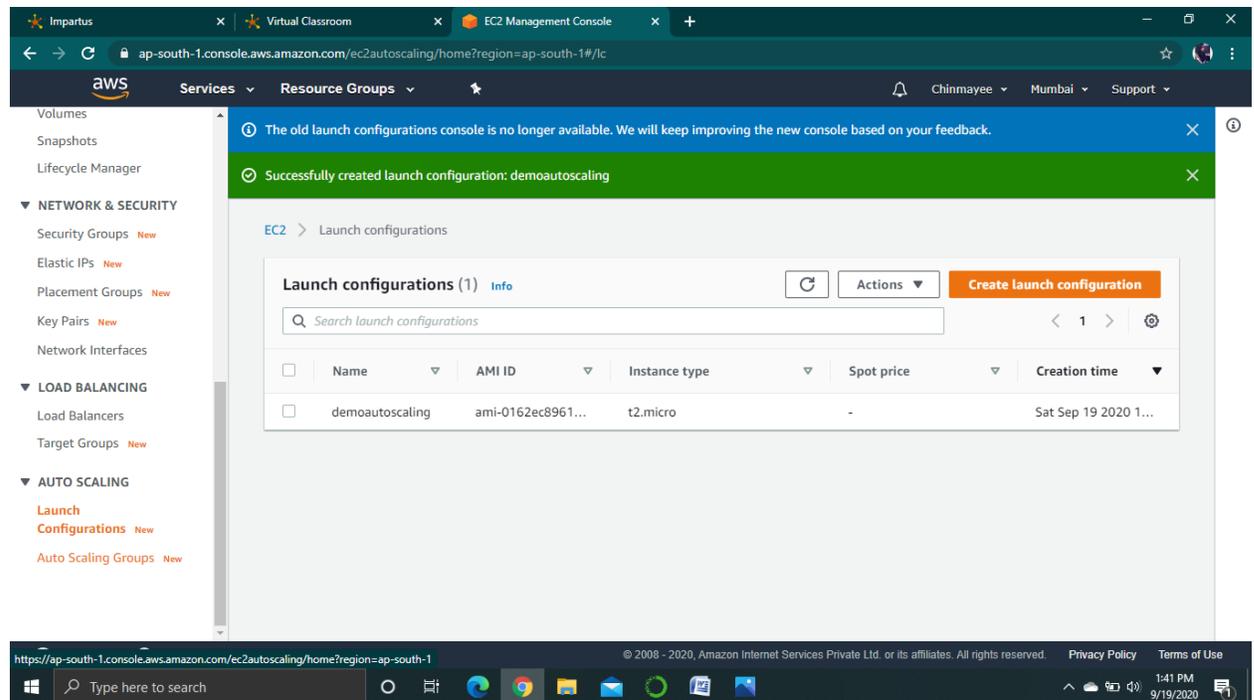
9. Choose Next: Configure details.

10. Select Create a new security group .



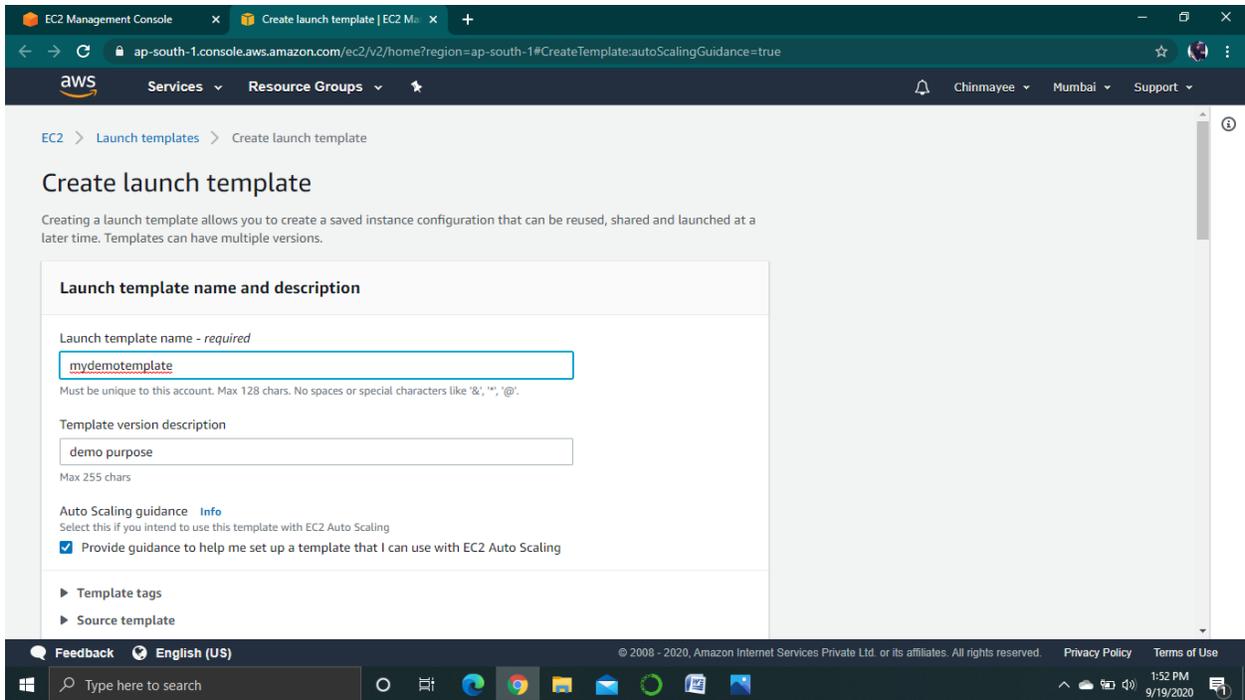
11. Choose Create launch configuration.

12. The wizard to Launch a Configuration is displayed.

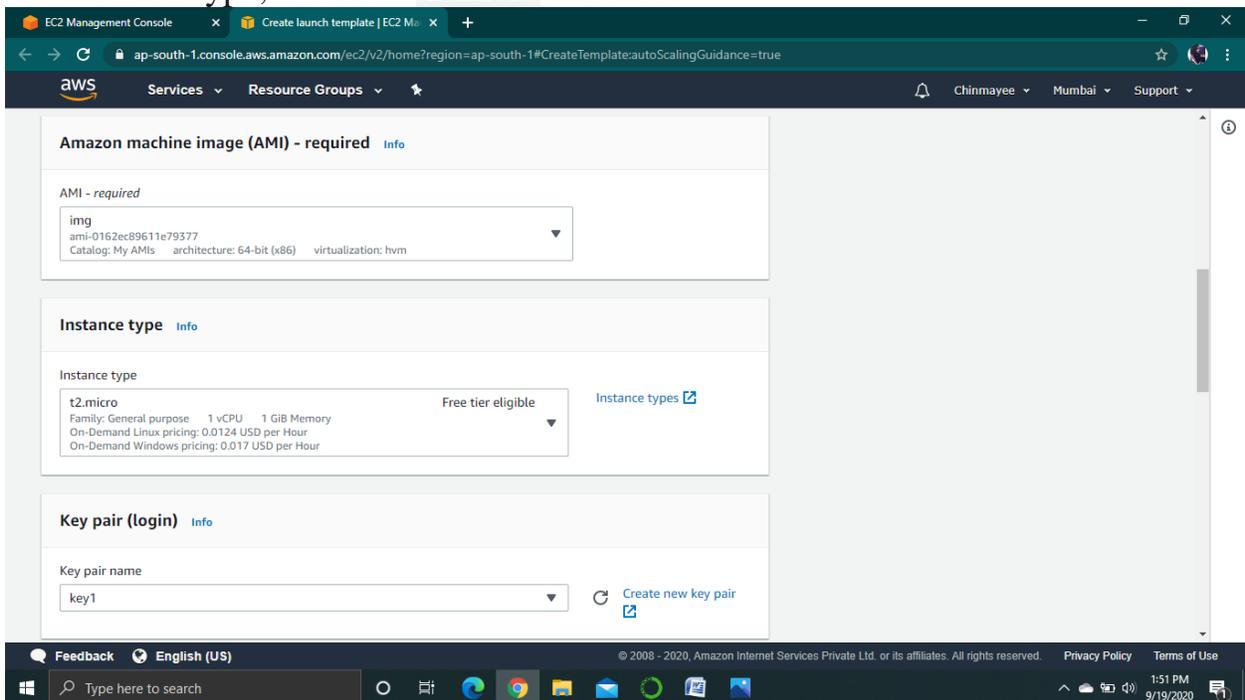


CONFIGURE A LAUNCH TEMPLATE

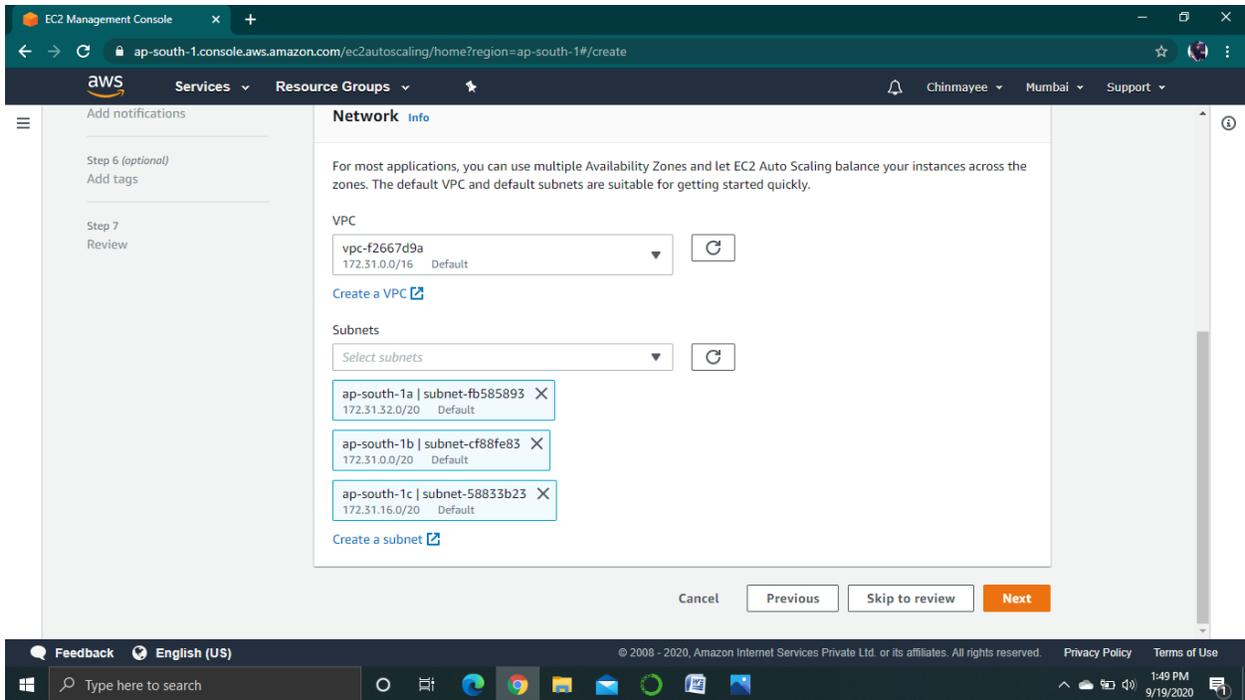
1. Login to AWS console.
2. Open the Amazon EC2 service.
3. On the navigation pane, under INSTANCES, choose Launch Templates.
4. Choose Create launch template.



5. Configure all the details.
6. For AMI ID, choose a version of AMI you have created.
7. For Instance type, choose a t2.micro instance.



8. For Key pair name, choose an existing key pair.
9. Leave Network type set to VPC.



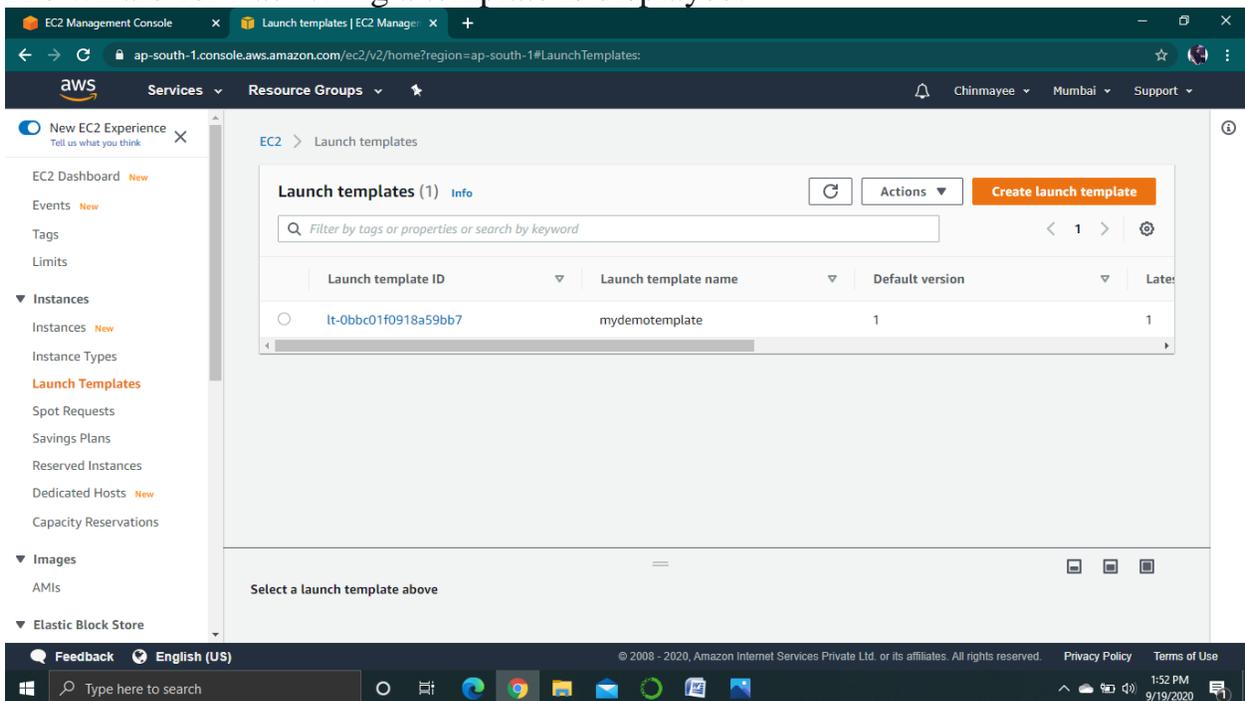
10. For Security Groups, specify the default security group for the VPC.

11. Configure default settings for EBS.

12. Leave Network Interfaces empty.

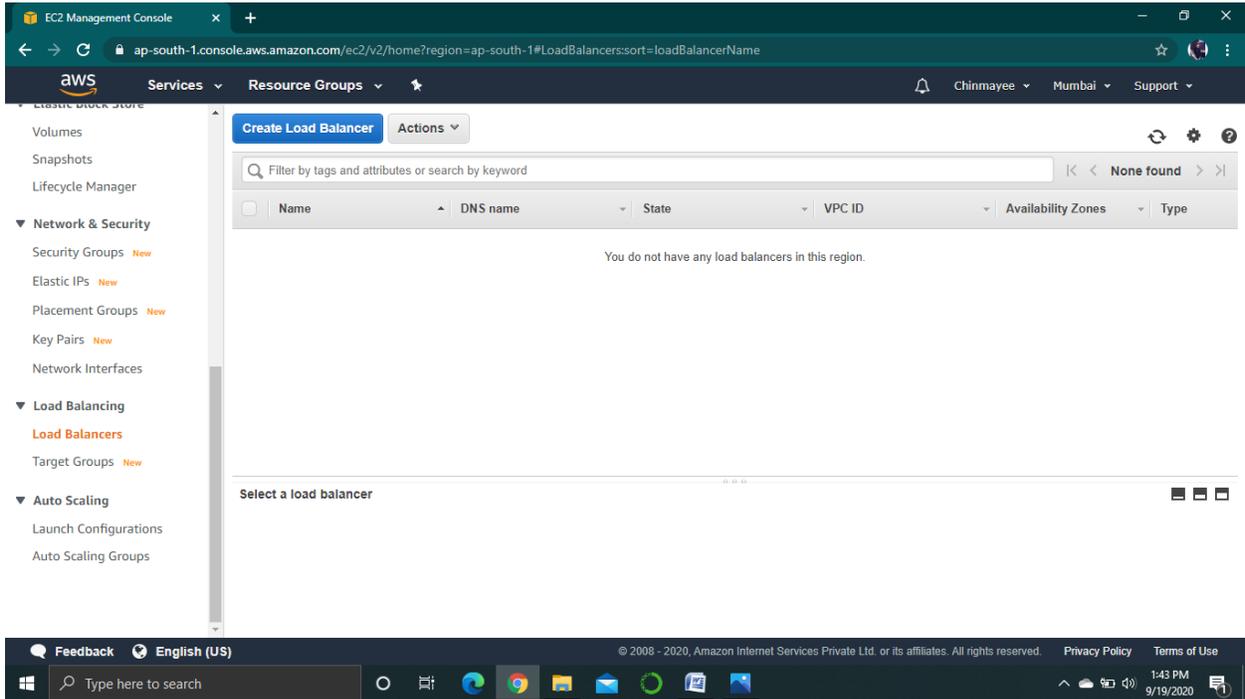
13. Scroll down and choose Create launch template.

14. The wizard for Launching a template is displayed.

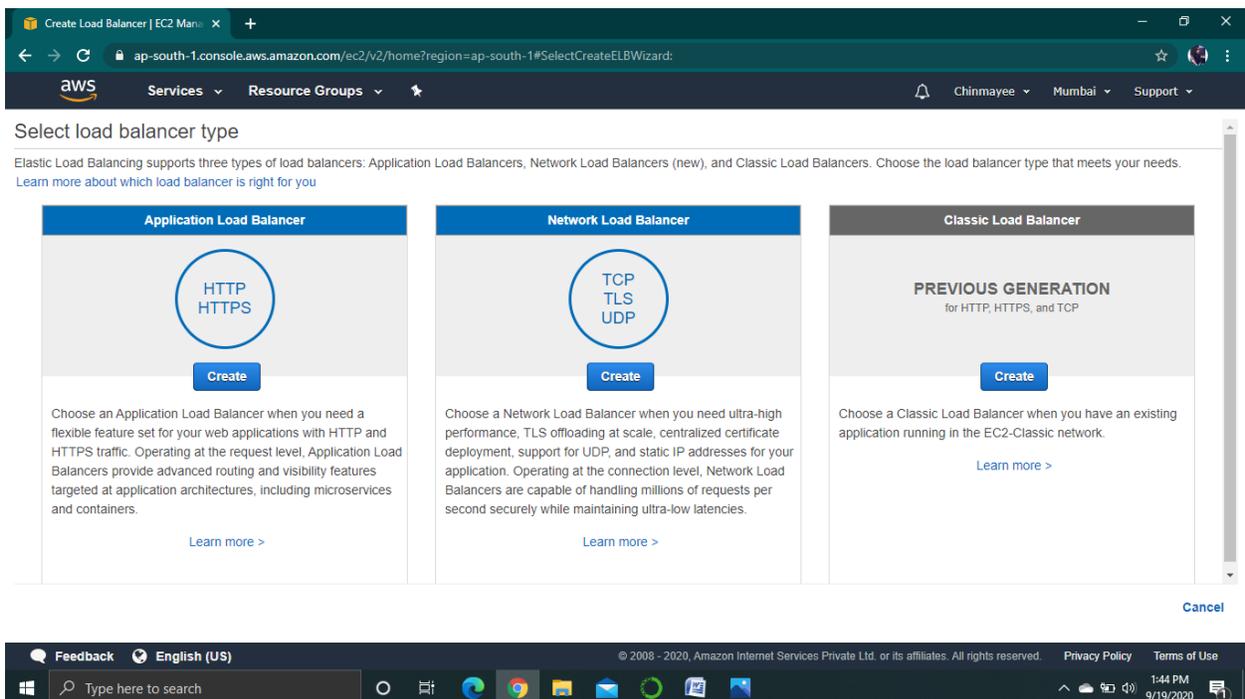


CONFIGURE LOAD BALANCING

1. Sign into AWS console and select EC2 service.
2. On the navigation pane, under LOAD BALANCING, choose Load Balancers and then choose create load balancer.



3. Choose Classic Load Balancer as the type of load balancer.



4. Define the Load Balancer and configure all its details.

1. Define Load Balancer 2. Assign Security Groups 3. Configure Security Settings 4. Configure Health Check 5. Add EC2 Instances 6. Add Tags 7. Review

Step 1: Define Load Balancer

Basic Configuration

This wizard will walk you through setting up a new load balancer. Begin by giving your new load balancer a unique name so that you can identify it from other load balancers you might create. You will also need to configure ports and protocols for your load balancer. Traffic from your clients can be routed from any load balancer port to any port on your EC2 instances. By default, we've configured your load balancer with a standard web server on port 80.

Load Balancer name:

Create LB inside:

Create an internal load balancer: (what's this?)

Enable advanced VPC configuration:

Listener Configuration:

Load Balancer Protocol	Load Balancer Port	Instance Protocol	Instance Port
HTTP	80	HTTP	80

5. Assign the default security groups and configure security settings.

1. Define Load Balancer 2. Assign Security Groups 3. Configure Security Settings 4. Configure Health Check 5. Add EC2 Instances 6. Add Tags 7. Review

Step 2: Assign Security Groups

You have selected the option of having your Elastic Load Balancer inside of a VPC, which allows you to assign security groups to your load balancer. Please select the security groups to assign to this load balancer. This can be changed at any time.

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

Filter: VPC security groups

Security Group ID	Name	Description
<input type="checkbox"/> sg-0a2a1c3d6c5875173	AutoScaling-Security-Group-1	AutoScaling-Security-Group-1 (2020-09-19T08:09:32.592Z)
<input checked="" type="checkbox"/> sg-0ca7ee69	default	default VPC security group
<input type="checkbox"/> sg-0c7a0b1db06b58f2d	launch-wizard-1	launch-wizard-1 created 2020-09-19T13:34:19.150+05:30
<input type="checkbox"/> sg-0a027b5526435aec7	WordPress Certified by Bitnami and Automattic-5-5-0 on Debian 10-AutogenByAWSMP-1	This security group was generated by AWS Marketplace and is based on recommended s

6. Configure the health check.

Create Load Balancer | EC2 Man... x +

ap-south-1.console.aws.amazon.com/ec2/v2/home?region=ap-south-1#CreateELBWizard:

Services Resource Groups

Chinmayee Mumbai Support

1. Define Load Balancer 2. Assign Security Groups 3. Configure Security Settings 4. Configure Health Check 5. Add EC2 Instances 6. Add Tags 7. Review

Step 4: Configure Health Check

Your load balancer will automatically perform health checks on your EC2 instances and only route traffic to instances that pass the health check. If an instance fails the health check, it is automatically removed from the load balancer. Customize the health check to meet your specific needs.

Ping Protocol

Ping Port

Ping Path

Advanced Details

Response Timeout seconds

Interval seconds

Unhealthy threshold

Healthy threshold

Cancel Previous Next: Add EC2 Instances

Feedback English (US)

© 2008 - 2020, Amazon Internet Services Private Ltd. or its affiliates. All rights reserved. Privacy Policy Terms of Use

Type here to search

1:47 PM 9/19/2020

7. Add the EC2 instance.

Create Load Balancer | EC2 Man... x +

ap-south-1.console.aws.amazon.com/ec2/v2/home?region=ap-south-1#CreateELBWizard:

Services Resource Groups

Chinmayee Mumbai Support

1. Define Load Balancer 2. Assign Security Groups 3. Configure Security Settings 4. Configure Health Check 5. Add EC2 Instances 6. Add Tags 7. Review

Step 5: Add EC2 Instances

The table below lists all your running EC2 Instances. Check the boxes in the Select column to add those instances to this load balancer.

VPC vpc-f2667d9a (172.31.0.0/16)

Instance	Name	State	Security groups	Zone	Subnet ID	Subnet CIDR
<input checked="" type="checkbox"/>	i-0c18b677f643a980c	running	launch-wizard-1	ap-south-1a	subnet-fb585893	172.31.32.0/20

Availability Zone Distribution

1 instance in ap-south-1a

Enable Cross-Zone Load Balancing

Enable Connection Draining seconds

Cancel Previous Next: Add Tags

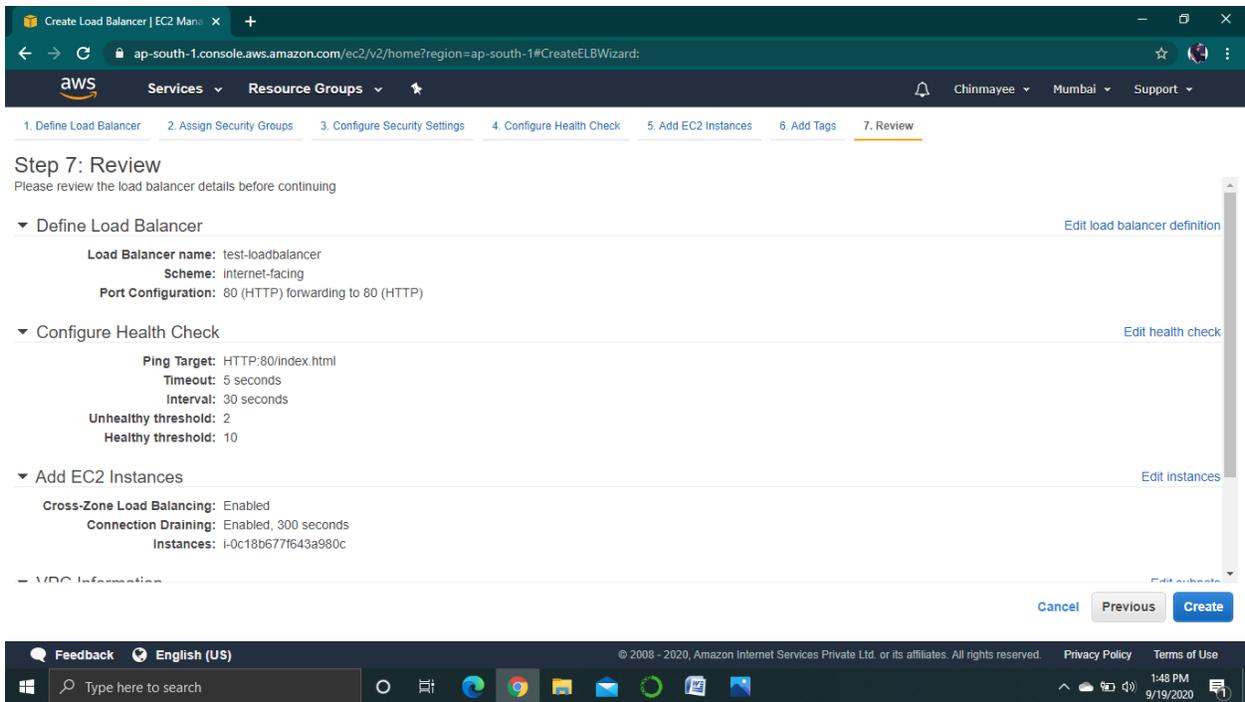
Feedback English (US)

© 2008 - 2020, Amazon Internet Services Private Ltd. or its affiliates. All rights reserved. Privacy Policy Terms of Use

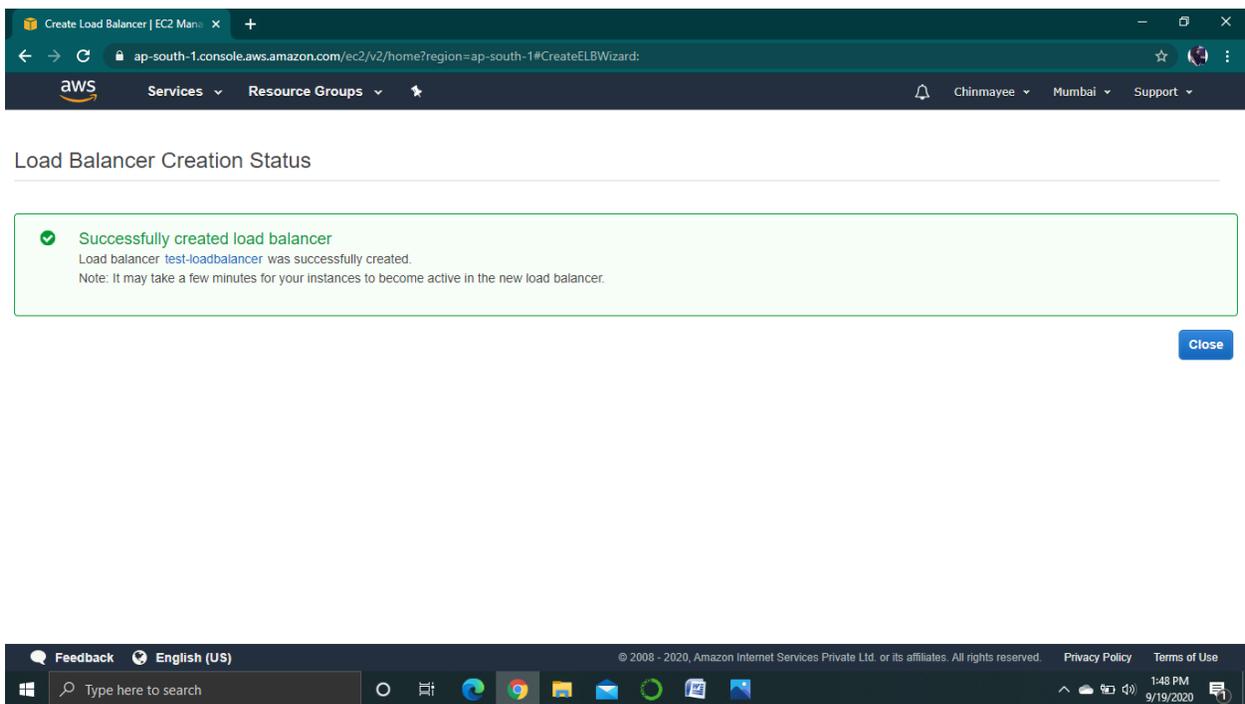
Type here to search

1:47 PM 9/19/2020

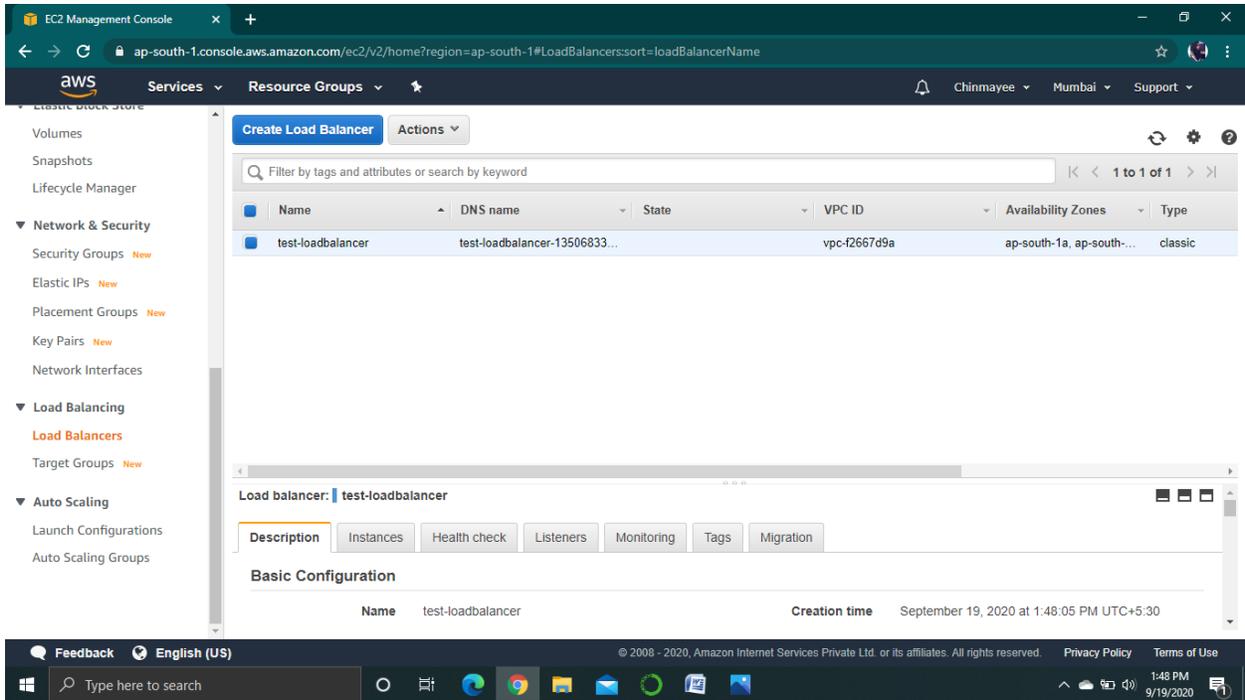
8. Add tags and click on review.



9. Check the status of the load balancer.

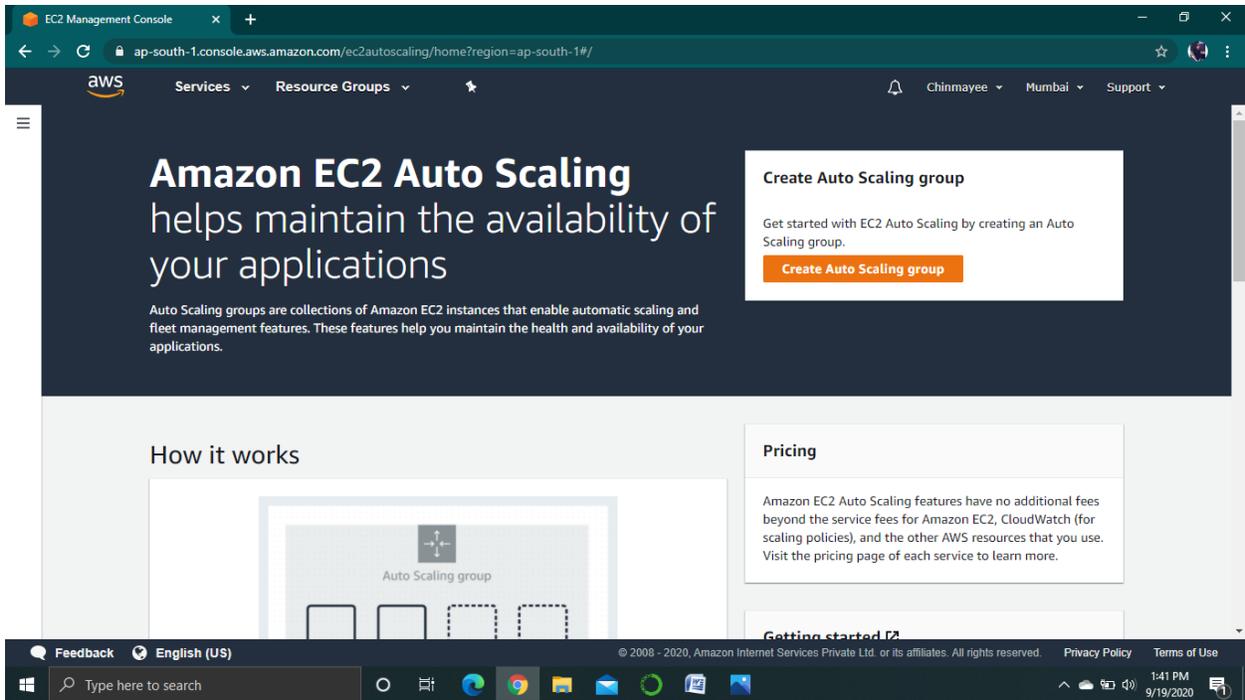


10. The load balancer created will be displayed on the dashboard.

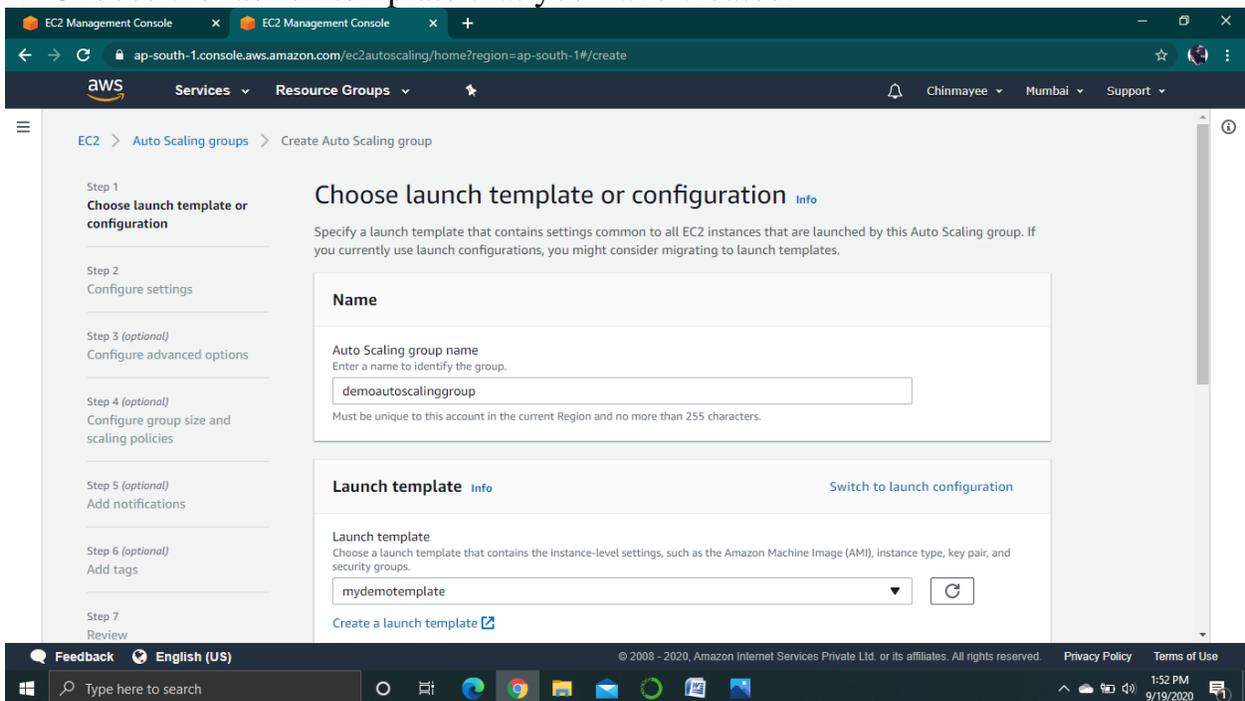


IMPLEMENTING AUTO SCALING GROUP

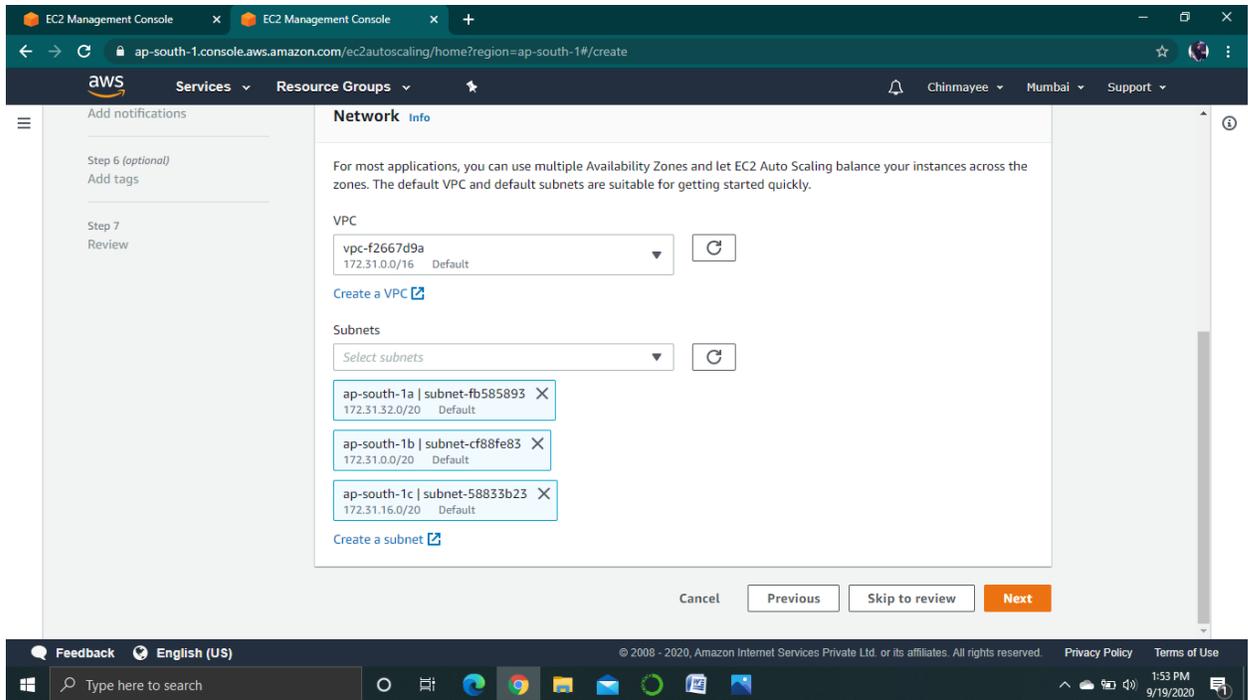
1. From EC2 dashboard, on the Auto Scaling groups page, choose Create an Auto Scaling group.



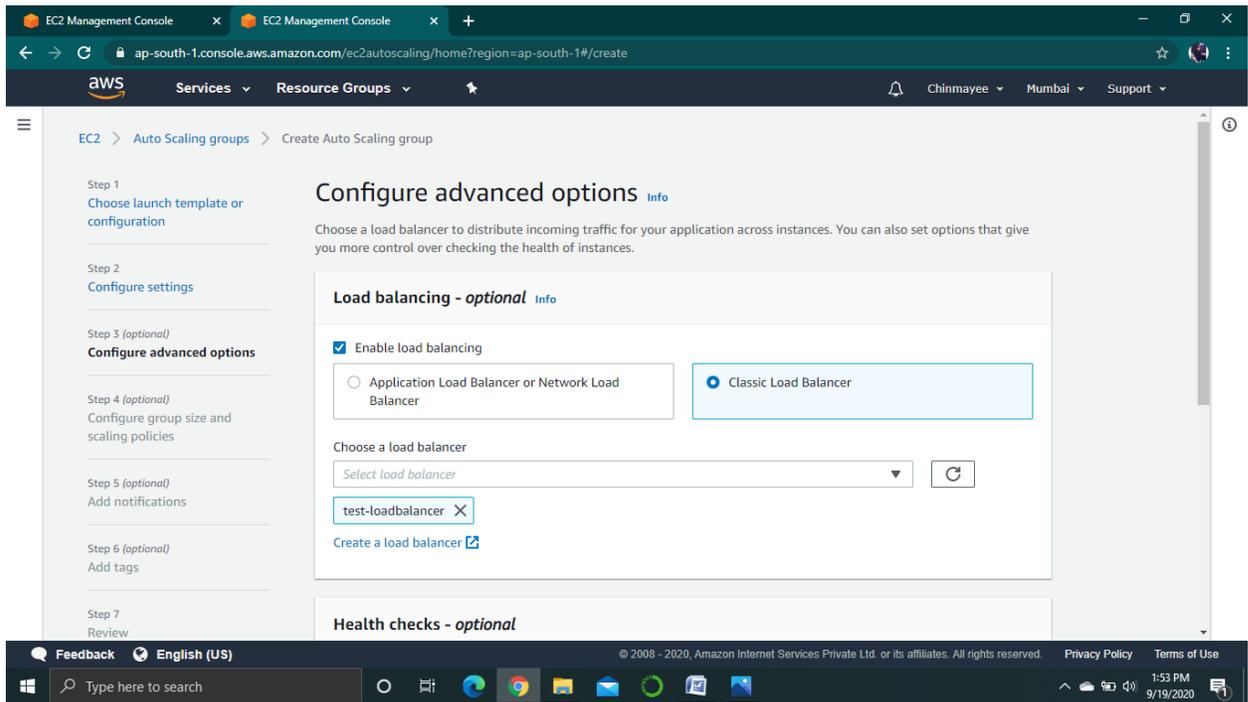
2. Choose the launch template that you have created.



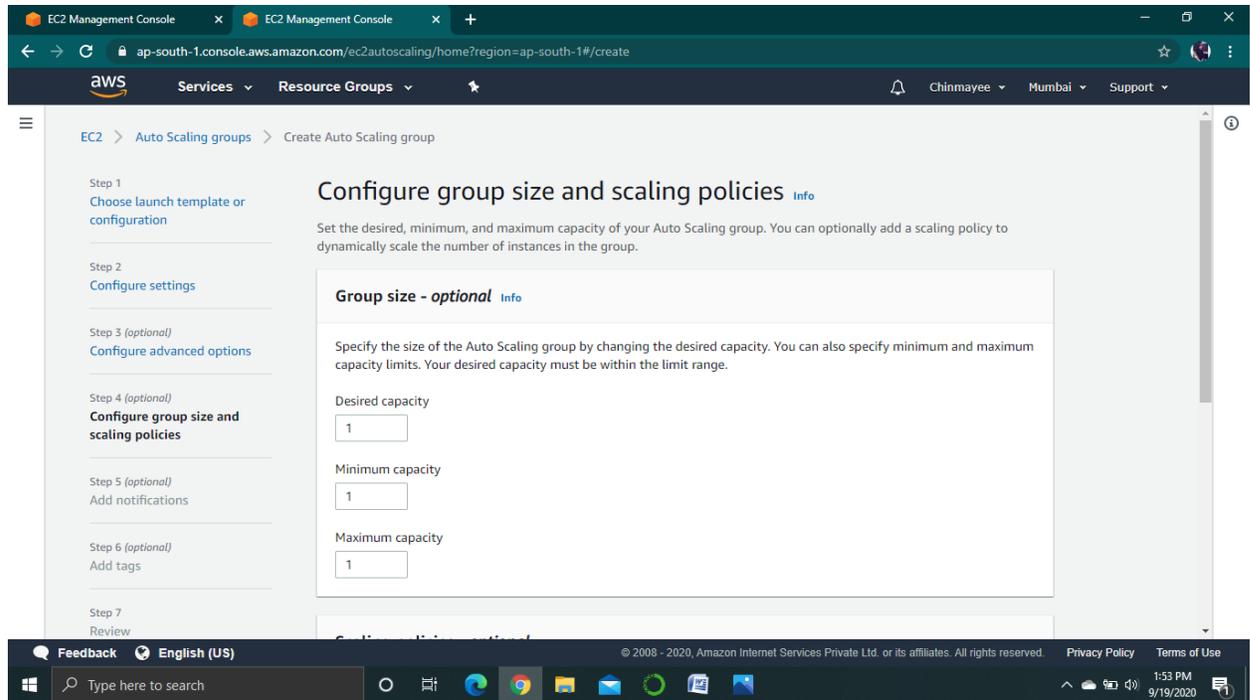
3. Choose the default version of the launch template to use when scaling out.
4. Choose Next.
5. Keep Network set to the default VPC for your chosen AWS Region.
6. For **Subnet**, choose a subnet from each Availability Zone that you want to include.



7. Enable the load balancing option and select the load balancer which you have created.

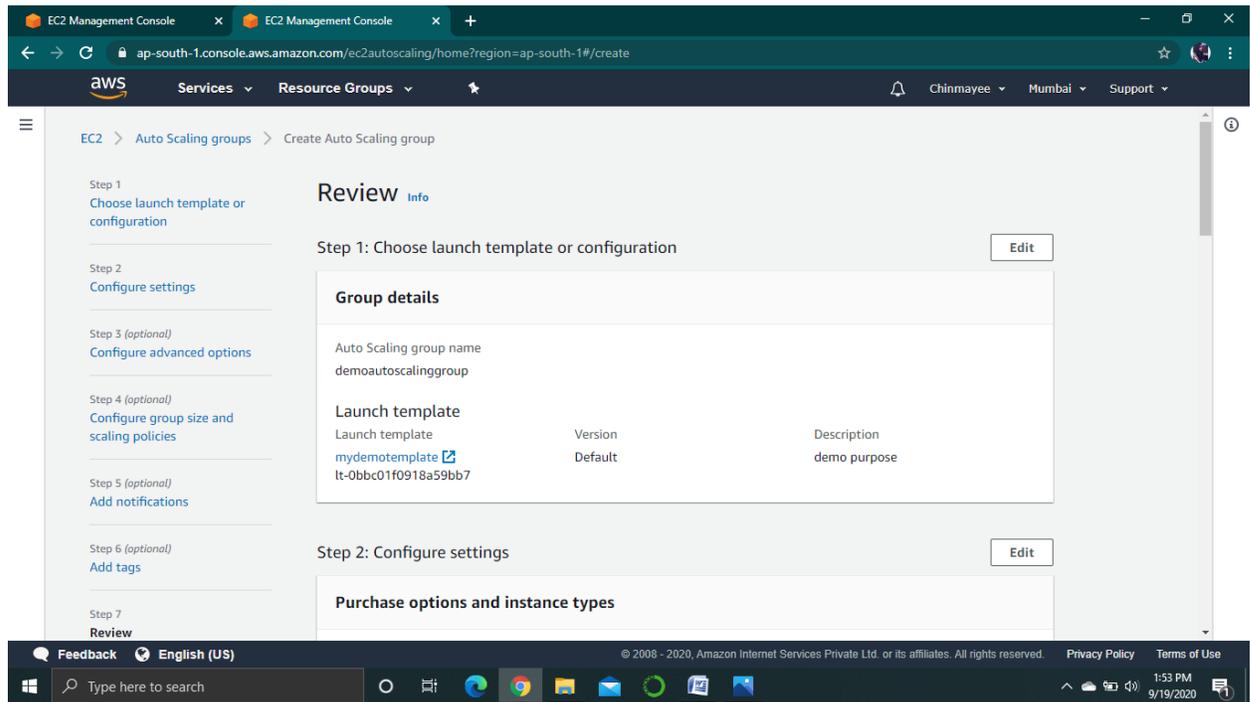


8. Configure the group size and scaling policy. Choose desired capacity as 1.

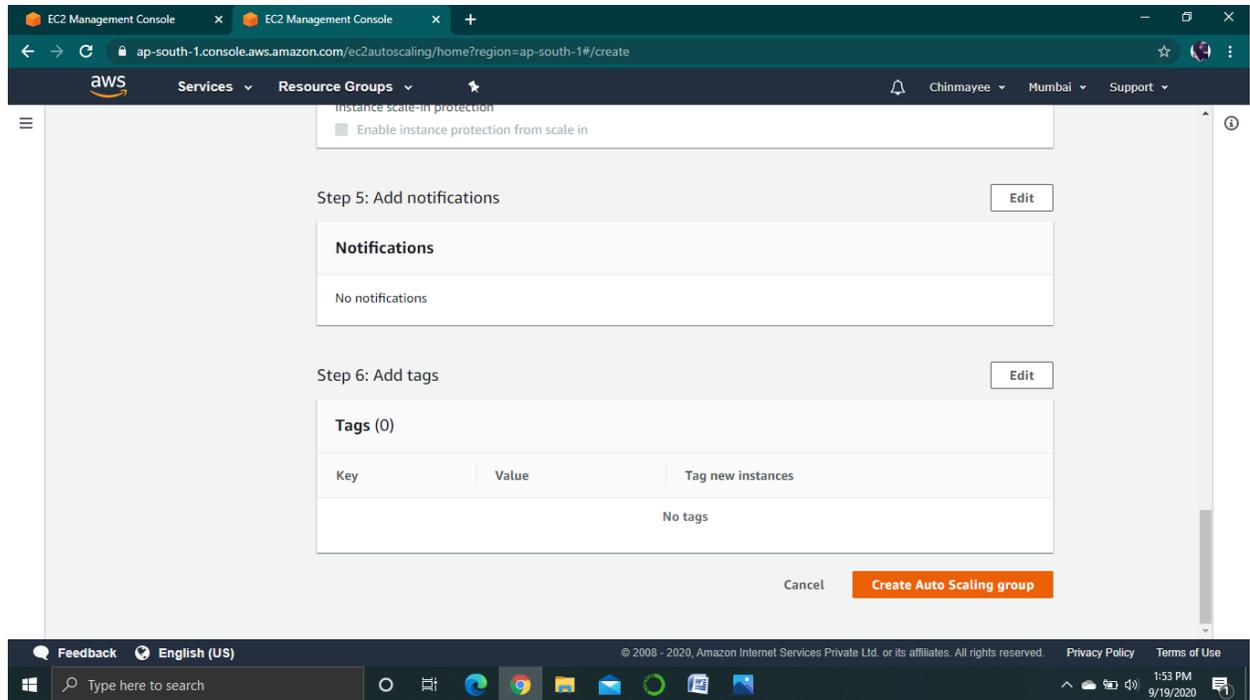


9. Notifications and tags can be added.

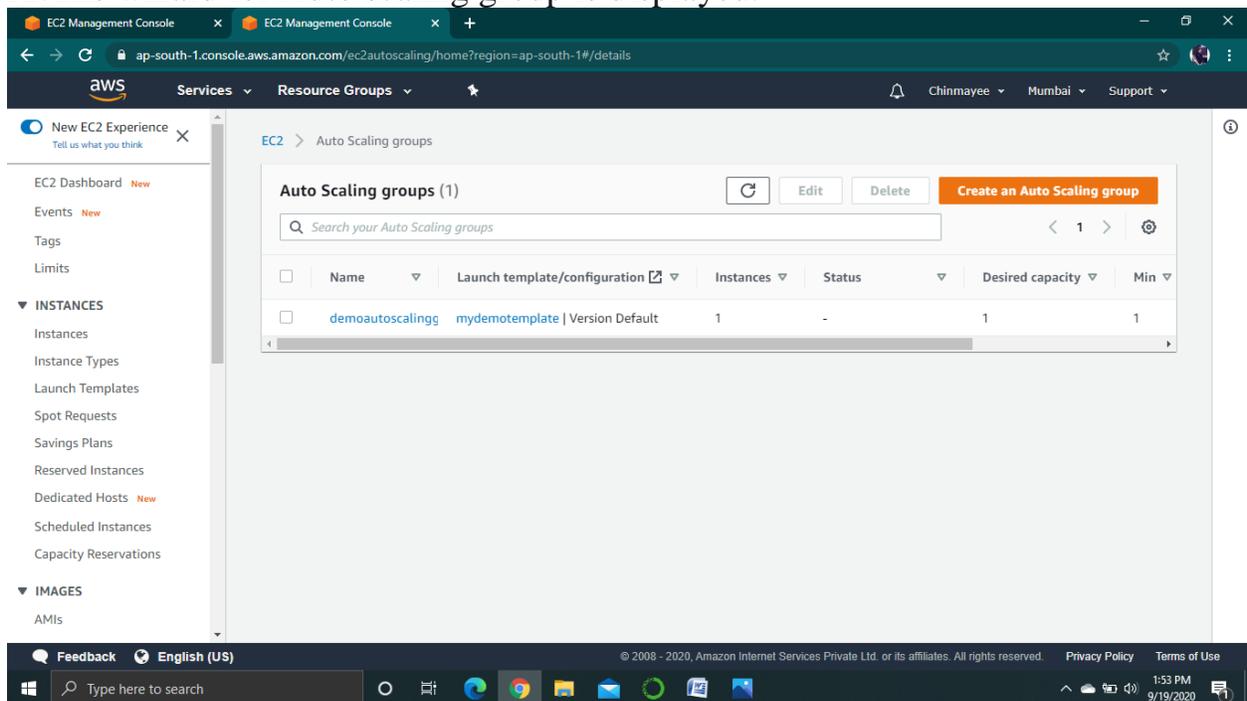
10. Choose review.



11. Choose Create Auto Scaling group.

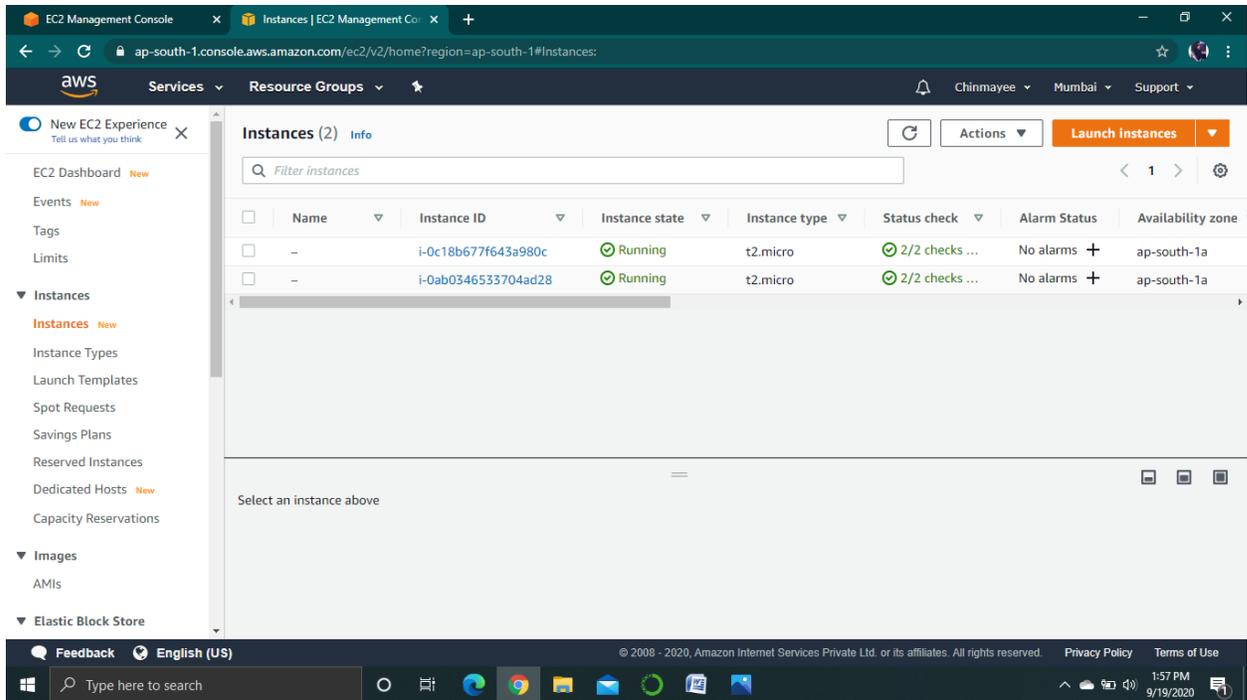


12. The wizard for Auto scaling group is displayed.



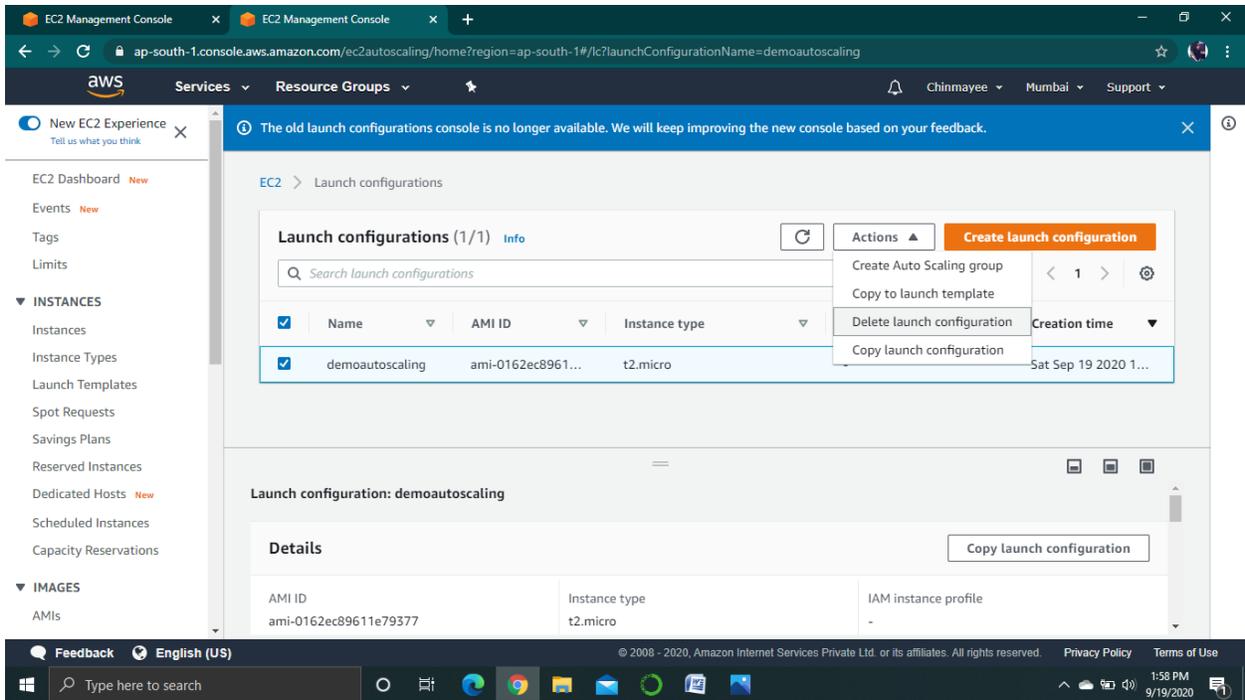
13. Verify whether Auto scaling group has created EC2 instance.

14. The instance has been launched successfully.

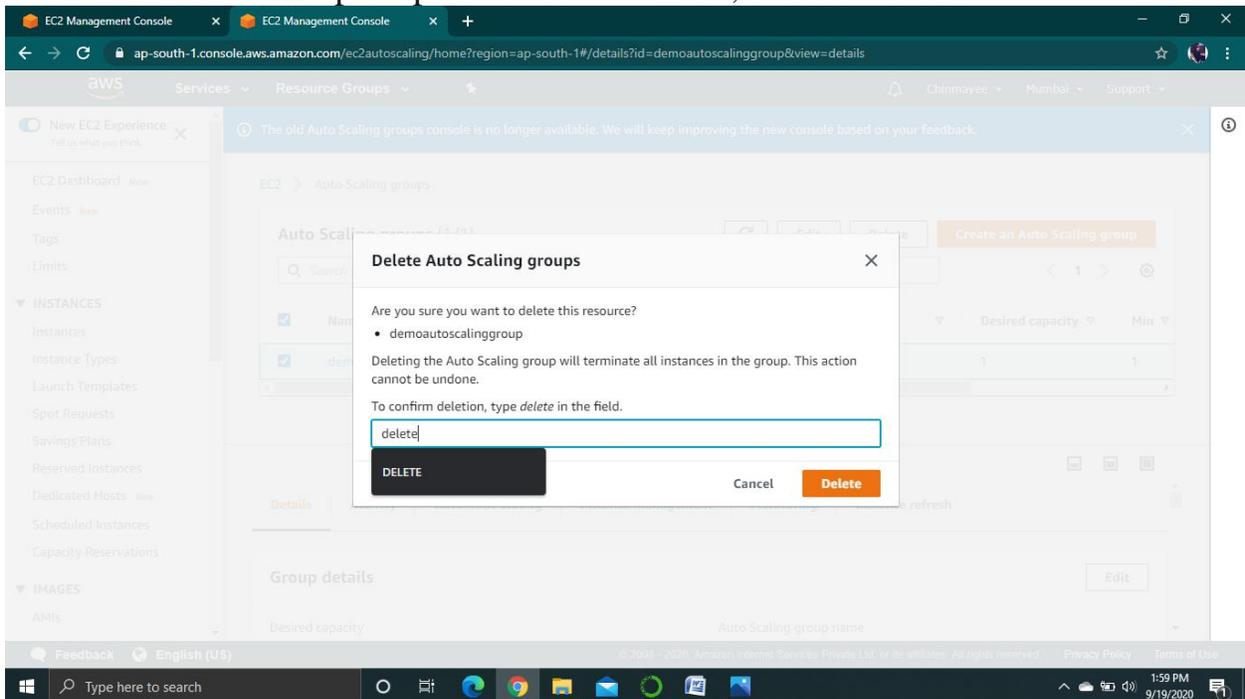


DETACHING EC2 INSTANCE FROM LOAD BALANCING

1. Open the Amazon EC2 console .
2. On the navigation pane, under AUTO SCALING, choose Auto Scaling Groups.
3. Select the check box next to your Auto Scaling group.



4. Choose Delete. When prompted for confirmation, choose Delete.

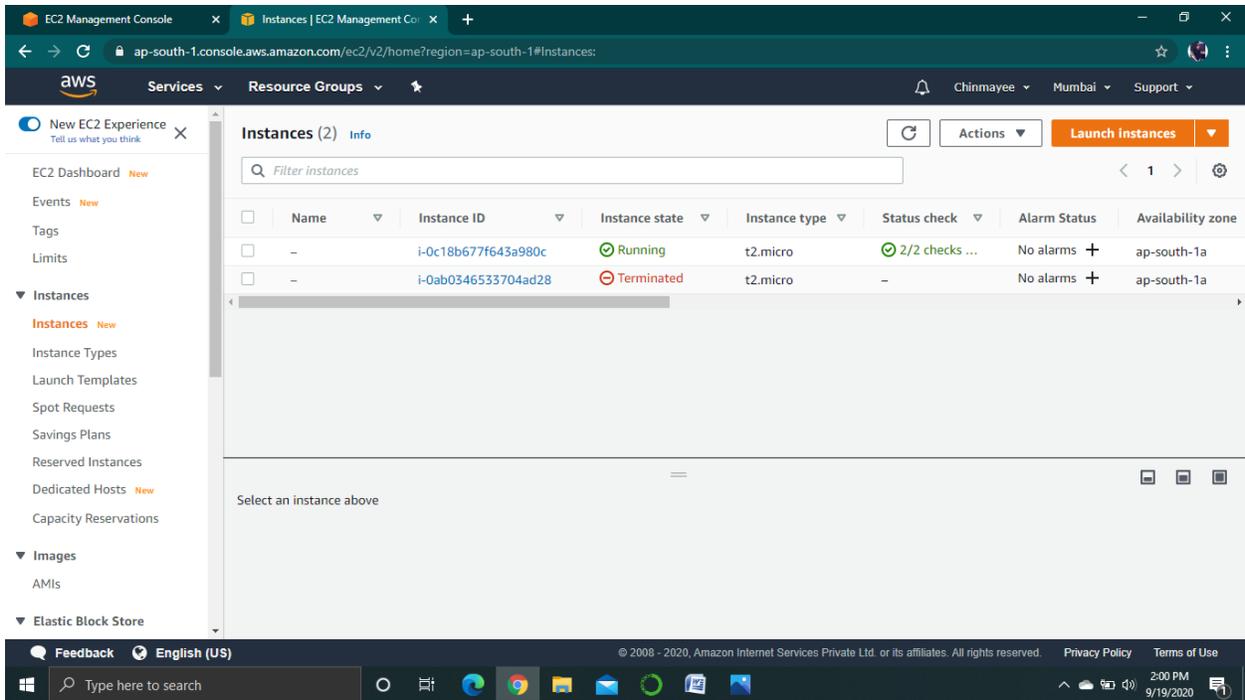


5. On the navigation pane, under AUTO SCALING, choose Launch Configuration.

6. Select the actions, and choose delete Launch Configuration.

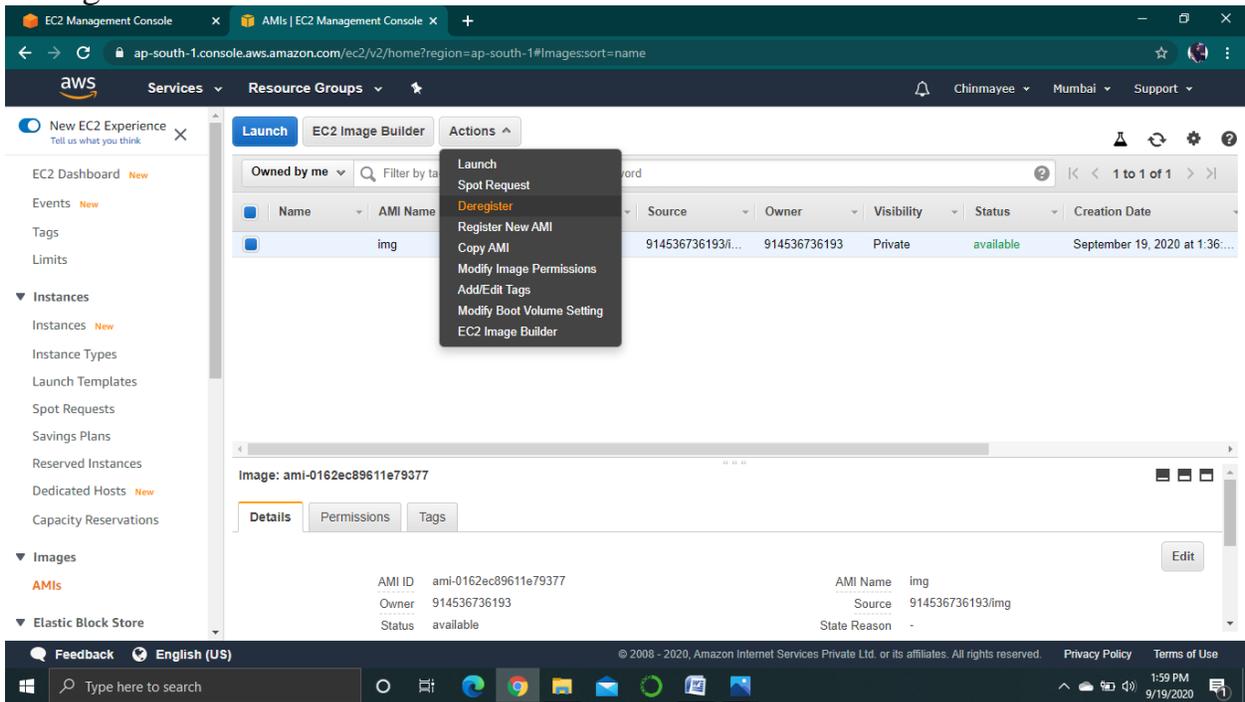
7. Choose Delete. When prompted for confirmation, choose Delete.

8. The instances created will also get terminated.



9. Terminate the instance created for AMI.

10. Deregister the AMI created.



11. Select the load balancer you have created and select actions and then delete.

EC2 Management Console

ap-south-1.console.aws.amazon.com/ec2/v2/home?region=ap-south-1#LoadBalancers:sort=loadBalancerName

Services Resource Groups

Chinmayee Mumbai Support

Filter by tags and attributes

Name	State	VPC ID	Availability Zones	Type
test-loadbalancer		vpc-f2667d9a	ap-south-1a, ap-south...	classic

Actions

- Edit health check
- Edit subnets
- Edit IP address type
- Edit instances
- Edit listeners
- Edit security groups
- Edit attributes
- Delete

Load balancer: test-loadbalancer

Description Instances Health check Listeners Monitoring Tags Migration

Basic Configuration

Name	Creation time
test-loadbalancer	September 19, 2020 at 1:48:05 PM UTC+5:30

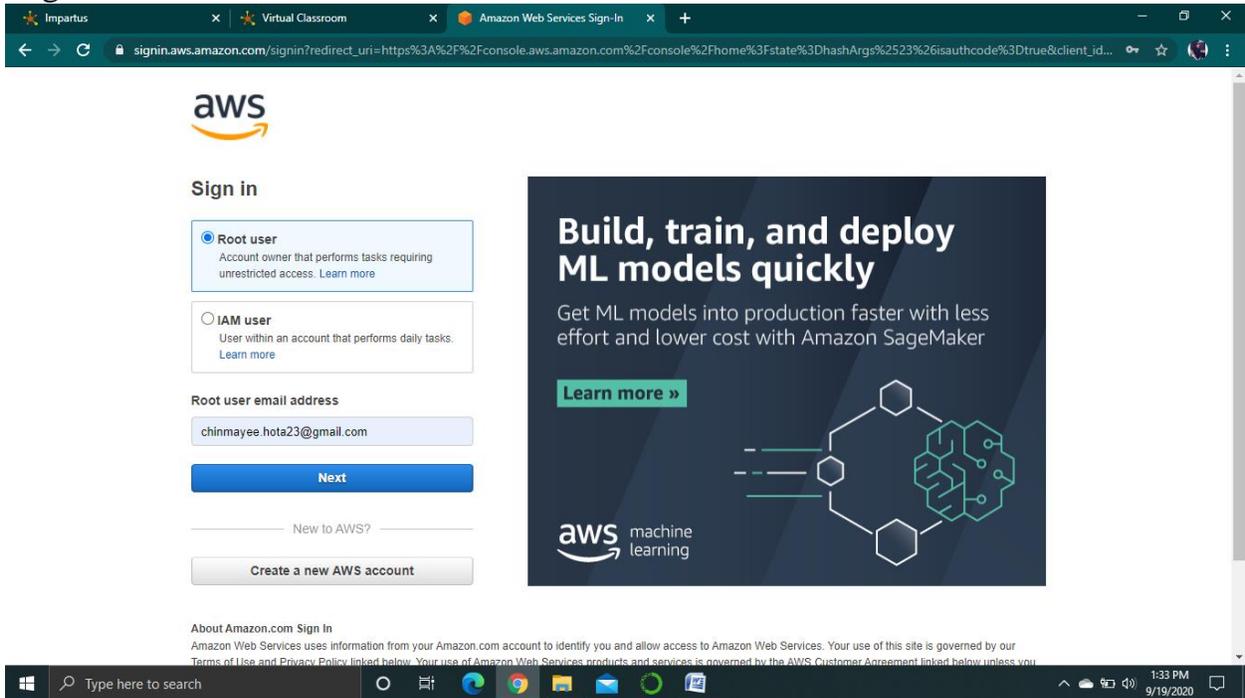
Feedback English (US)

© 2008 - 2020, Amazon Internet Services Private Ltd. or its affiliates. All rights reserved. Privacy Policy Terms of Use

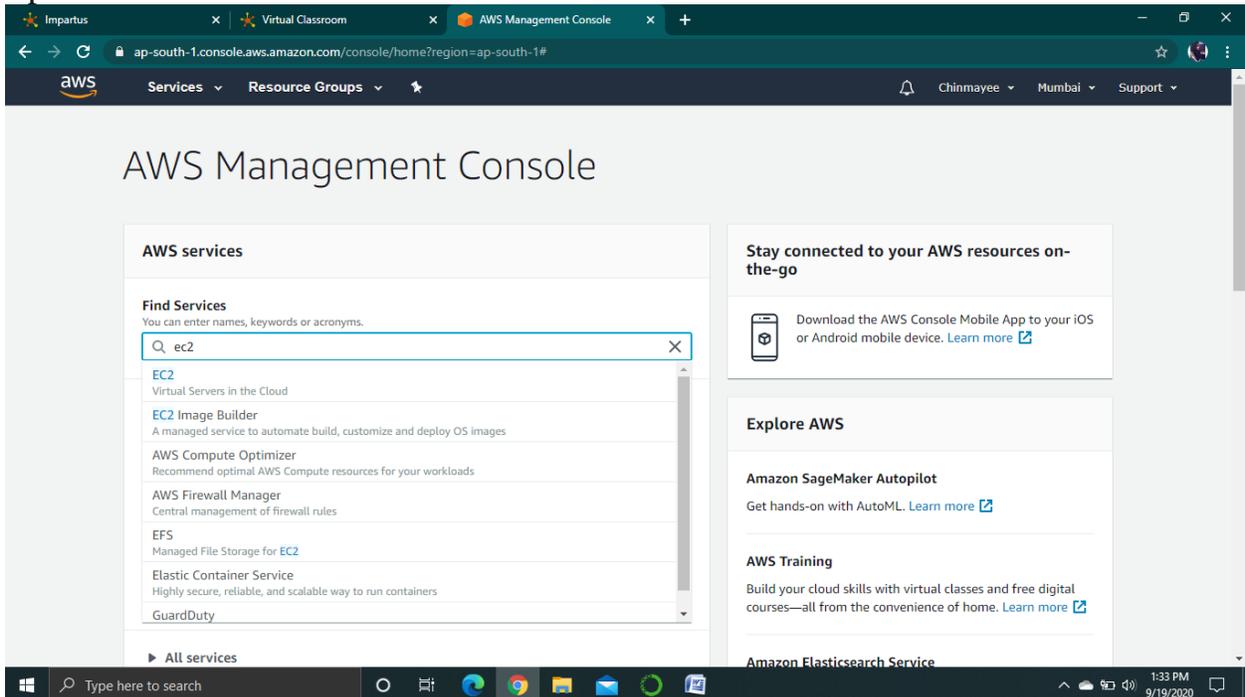
1:59 PM 9/19/2020

IMPLEMENTING ELASTIC LOAD BALANCING

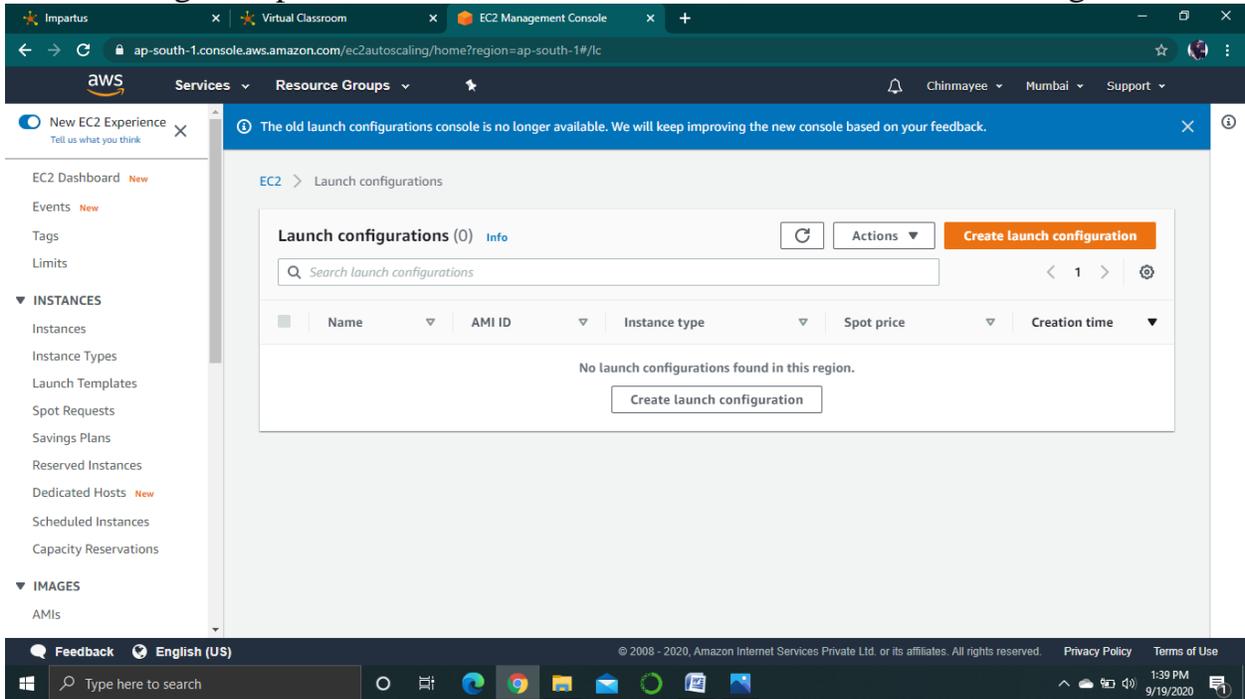
1. Login to AWS console.



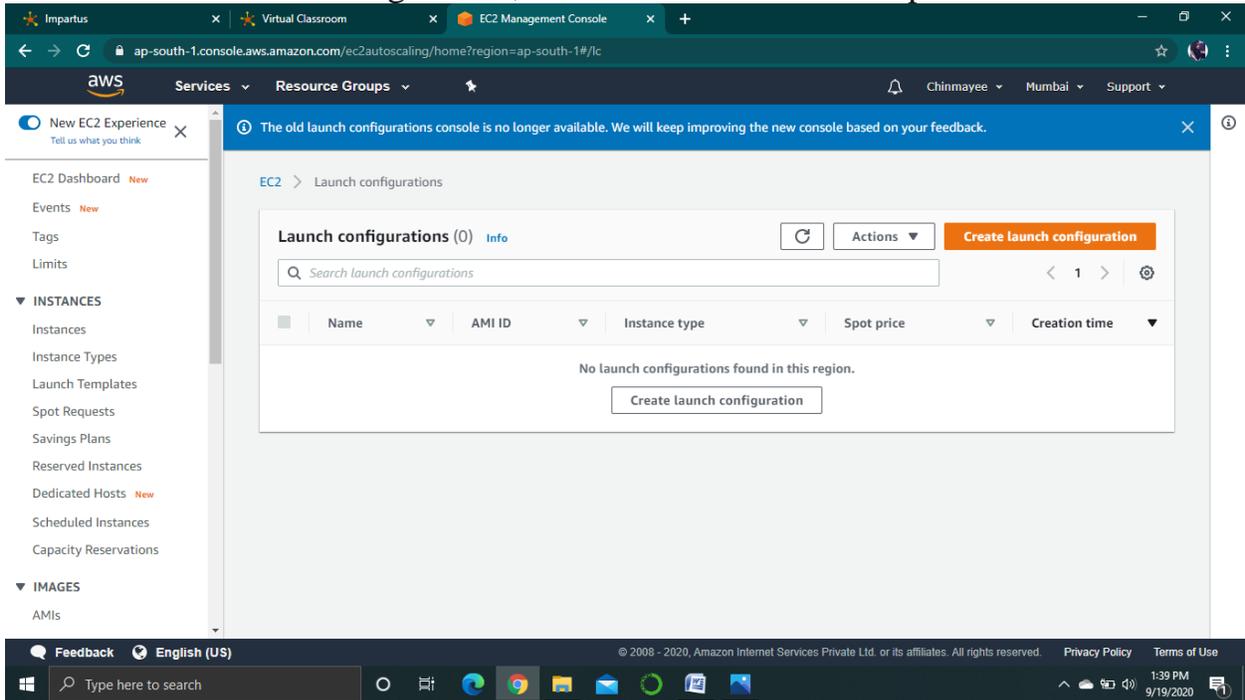
2. Open the Amazon EC2 service.



3. On the navigation pane, under AUTO SCALING, choose Launch Configurations.



4. Create a new launch configuration, and then choose Next Step.

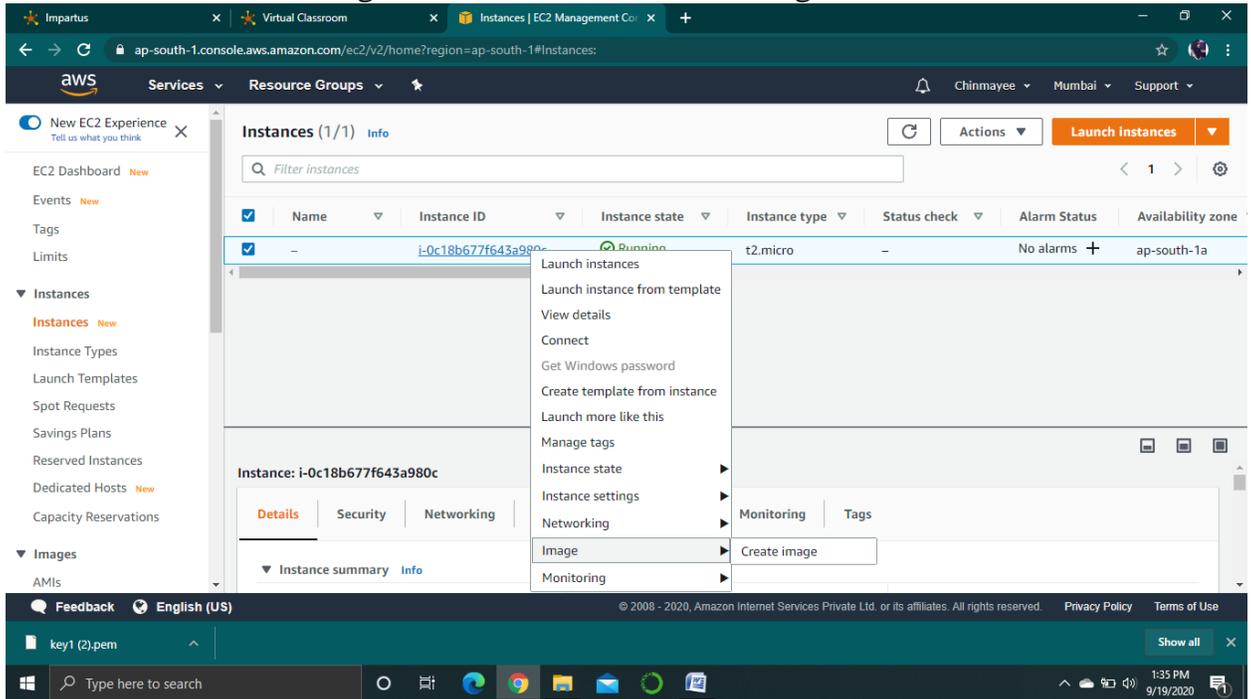


5. Configure all the details.

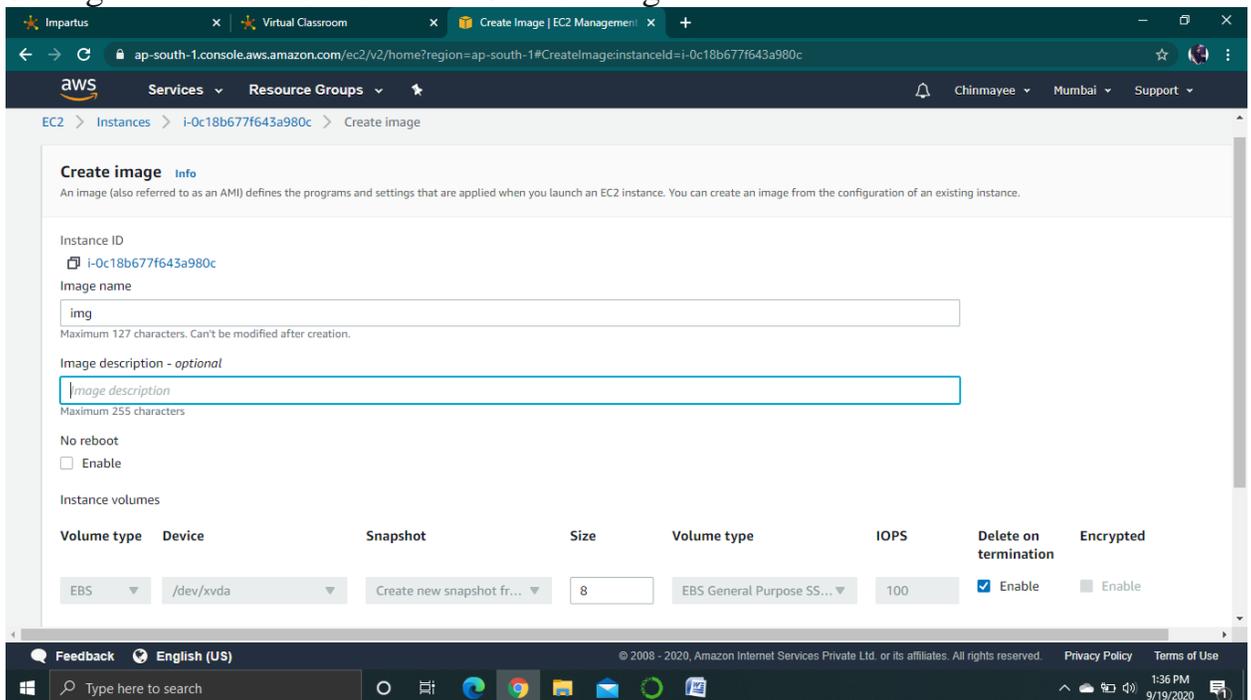
6. For selecting a free eligible AMI.

- Launch an EC2 instance.

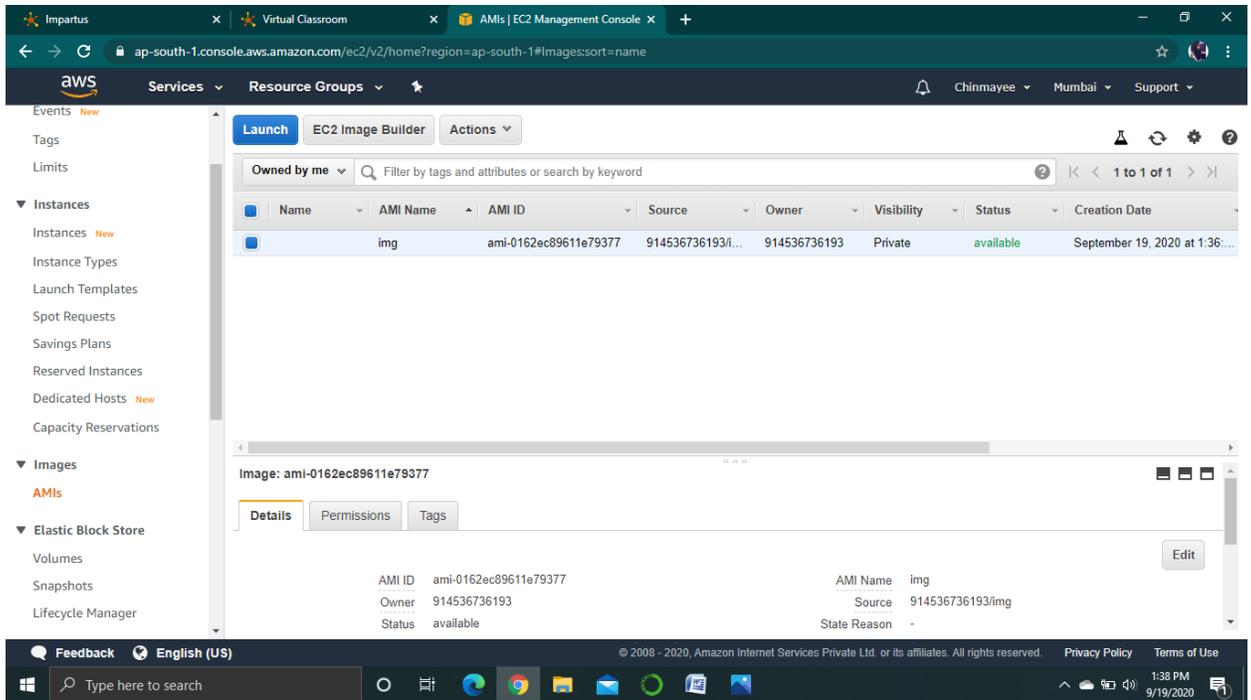
- Select the EC2 instance and choose actions.
- From actions select Image and then select Create Image.



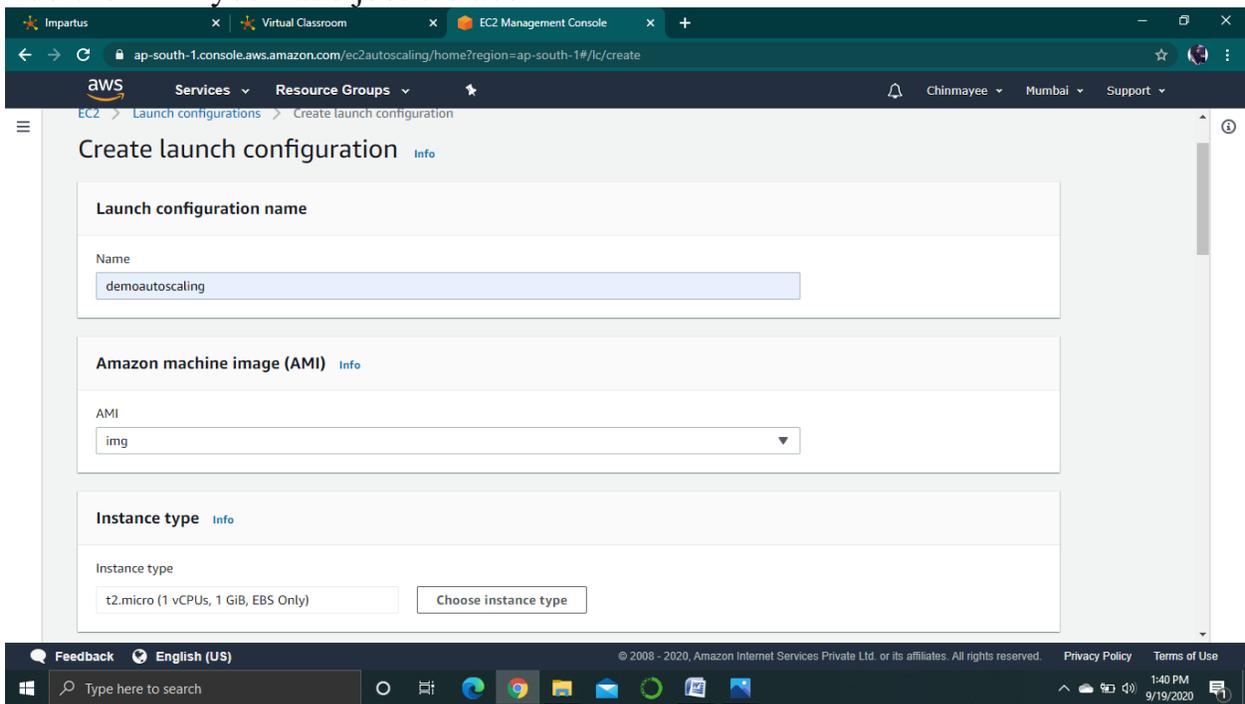
- Configure the details and select Create Image.



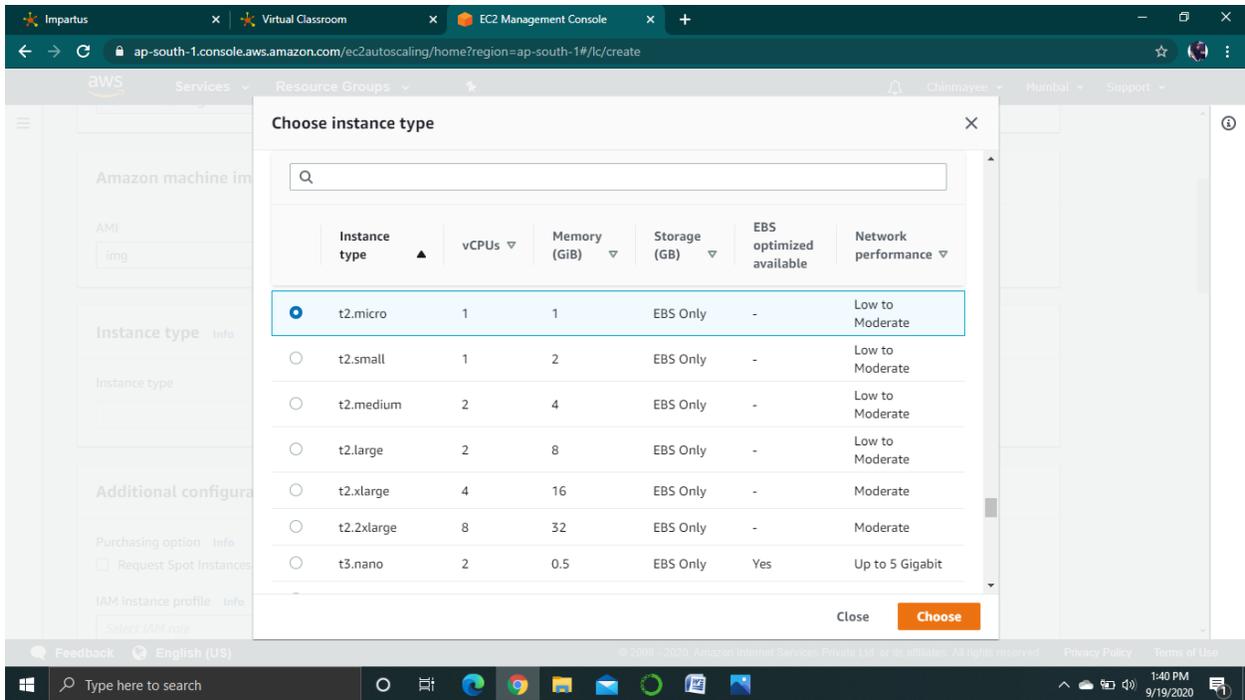
- From the AMI dashboard check the status.



7. Add the AMI you have just created.

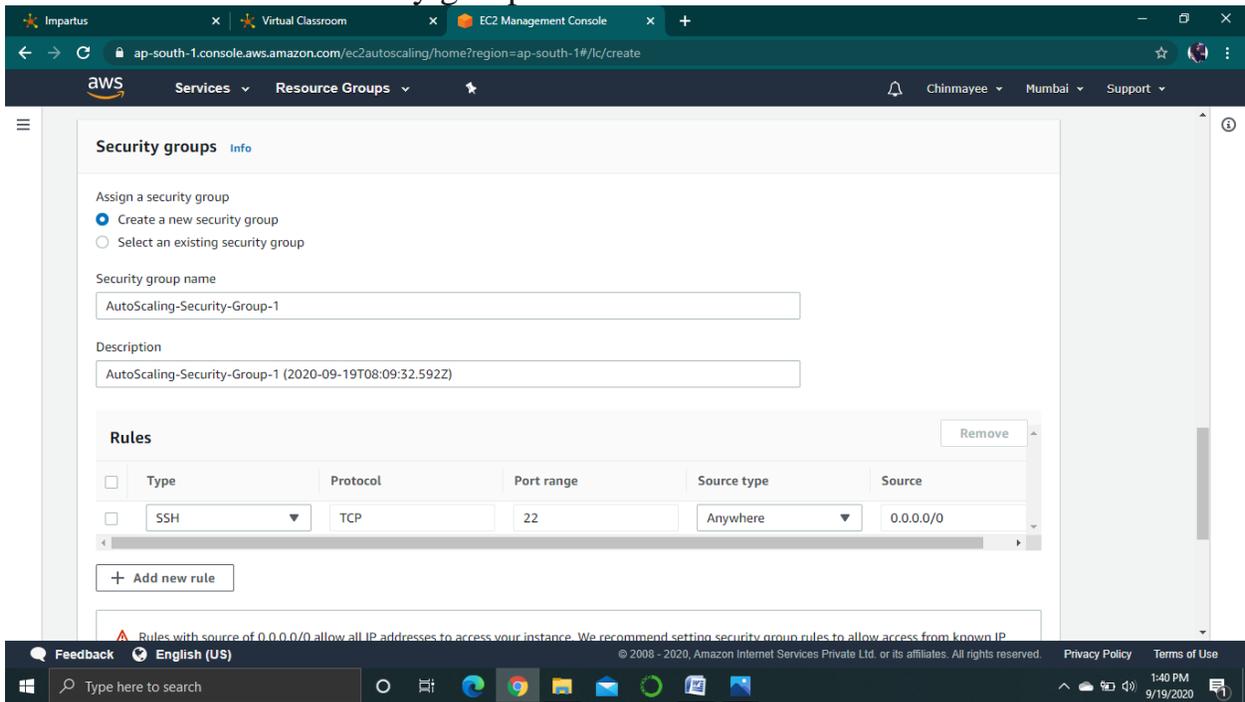


8. For the Choose Instance Type step, select a t2.micro instance.



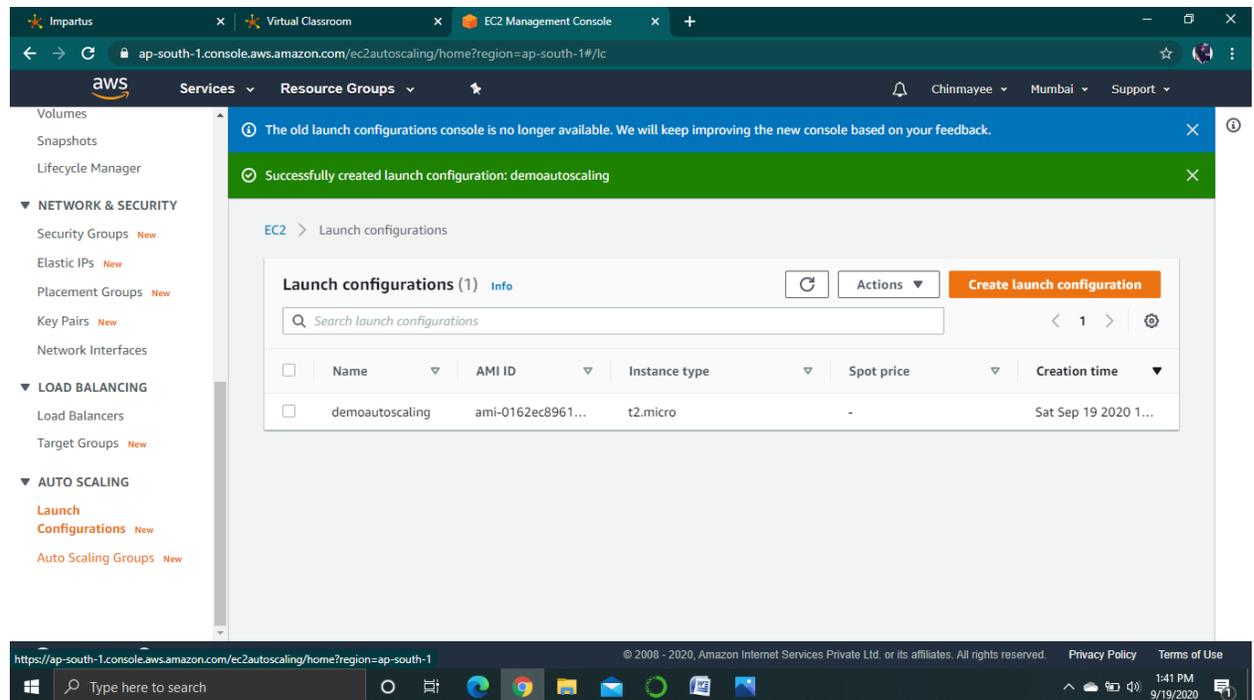
9. Choose Next: Configure details.

10. Select Create a new security group .



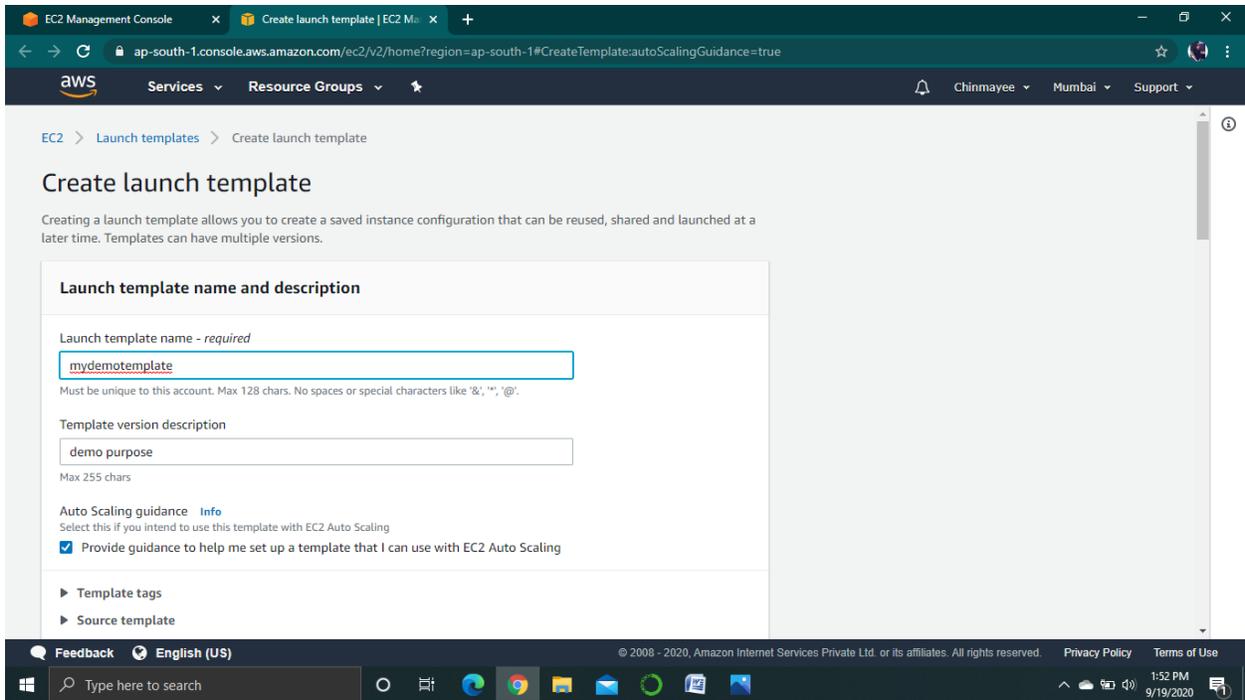
11. Choose Create launch configuration.

12. The wizard to Launch a Configuration is displayed.

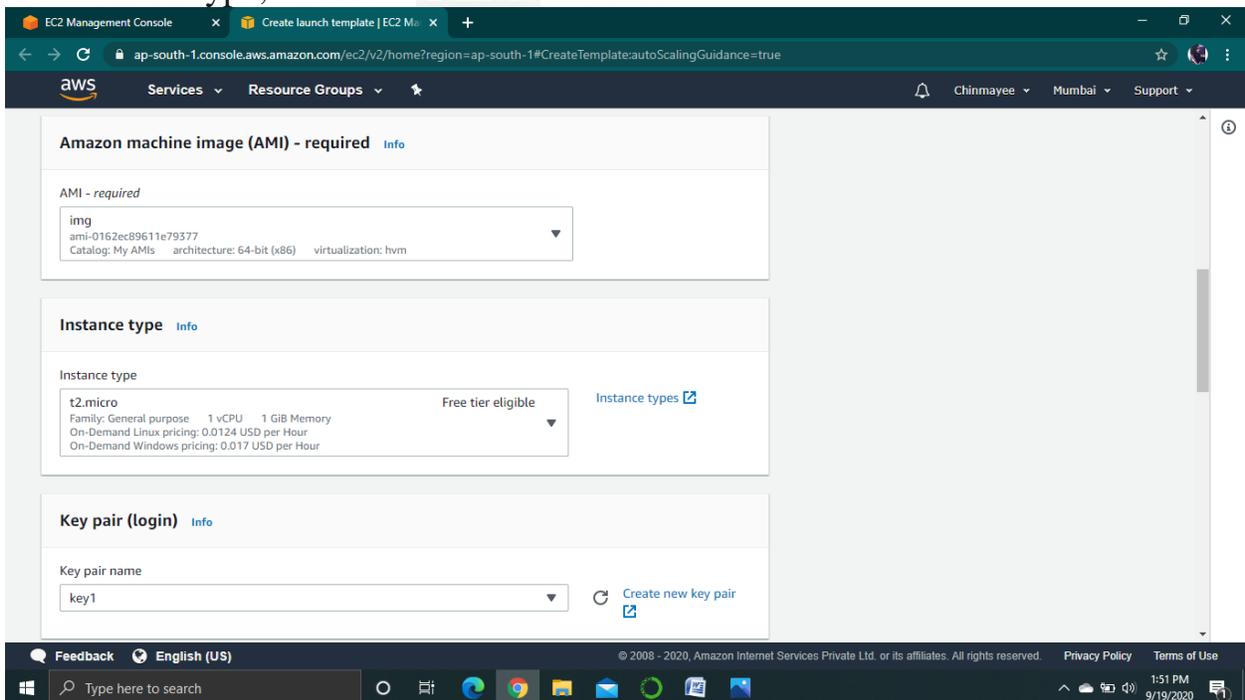


CONFIGURE A LAUNCH TEMPLATE

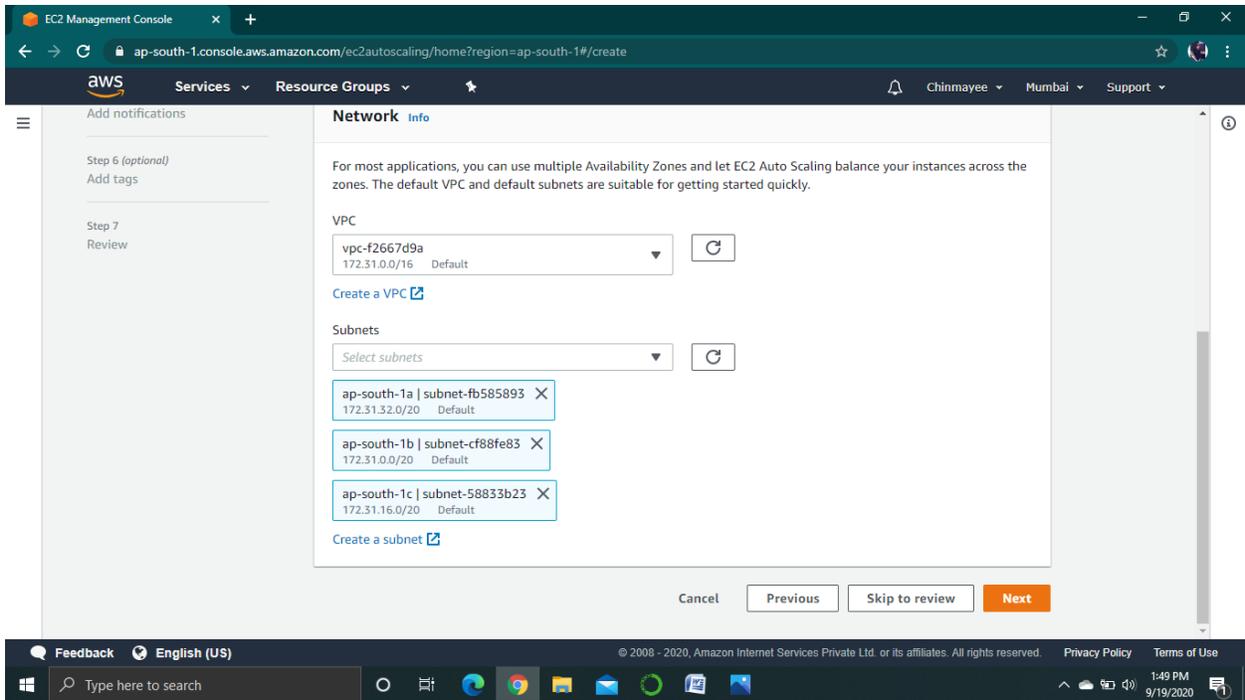
1. Login to AWS console.
2. Open the Amazon EC2 service.
3. On the navigation pane, under INSTANCES, choose Launch Templates.
4. Choose Create launch template.



5. Configure all the details.
6. For AMI ID, choose a version of AMI you have created.
7. For Instance type, choose a t2.micro instance.



8. For Key pair name, choose an existing key pair.
9. Leave Network type set to VPC.



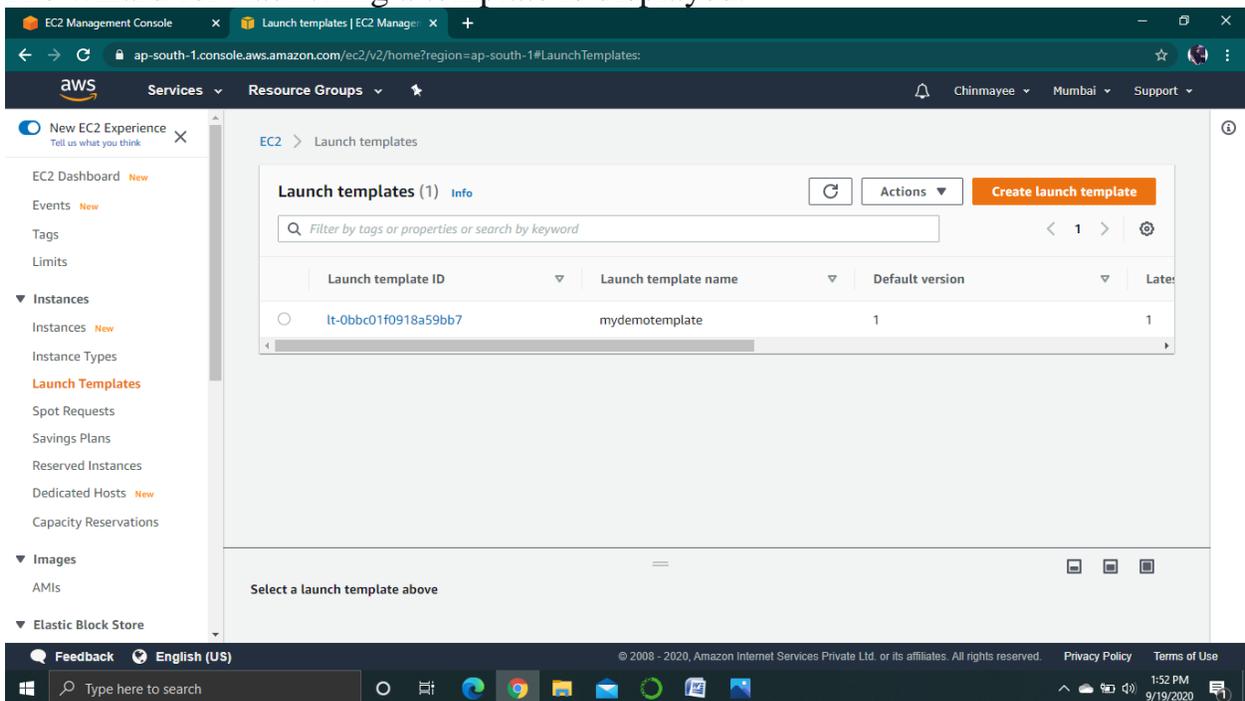
10. For Security Groups, specify the default security group for the VPC.

11. Configure default settings for EBS.

12. Leave Network Interfaces empty.

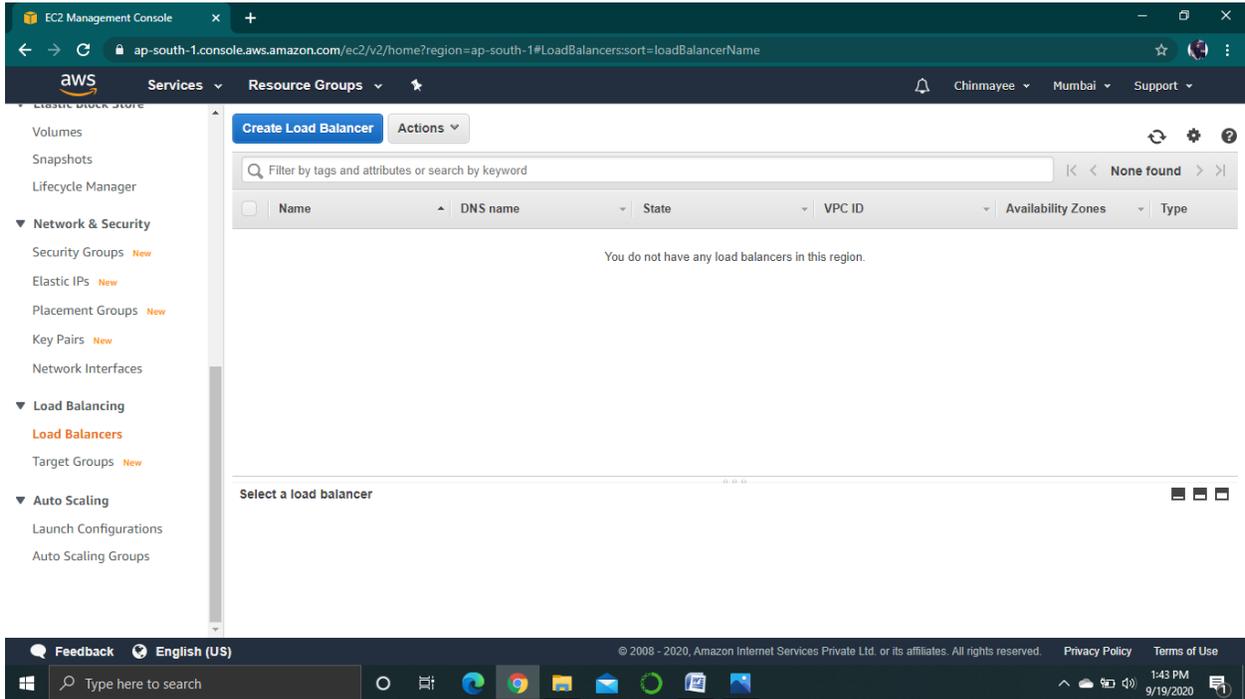
13. Scroll down and choose Create launch template.

14. The wizard for Launching a template is displayed.

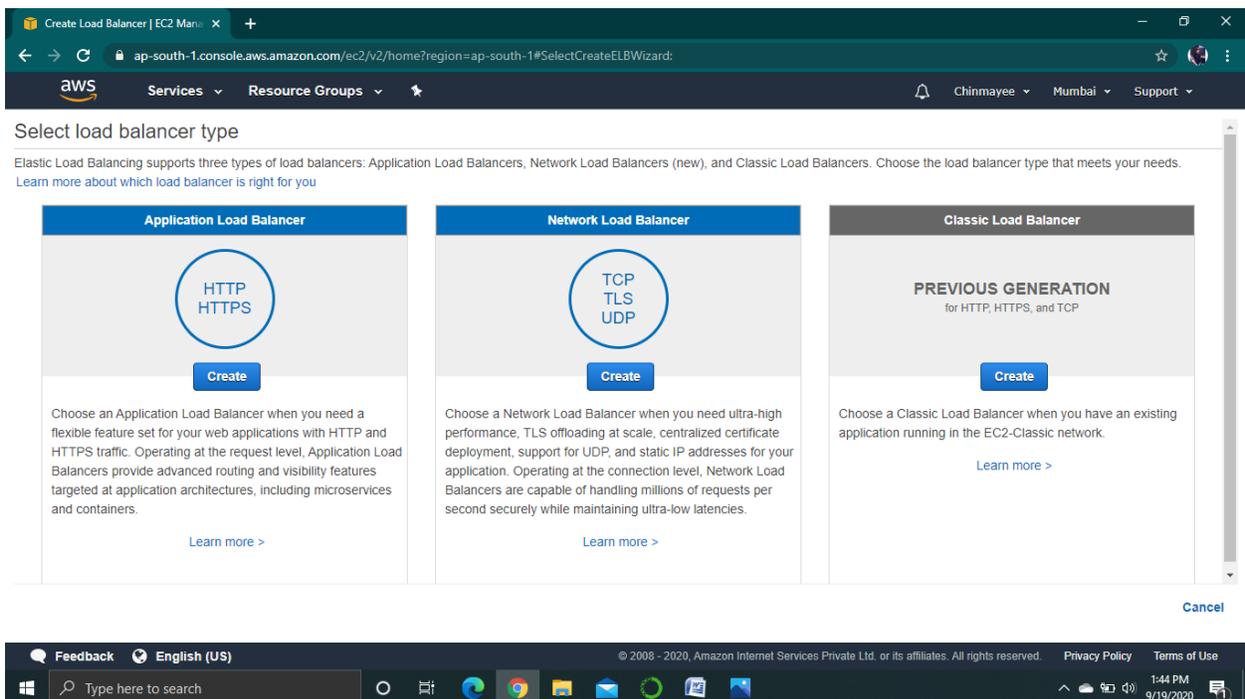


CONFIGURE LOAD BALANCING

1. Sign into AWS console and select EC2 service.
2. On the navigation pane, under LOAD BALANCING, choose Load Balancers and then choose create load balancer.



3. Choose Classic Load Balancer as the type of load balancer.



4. Define the Load Balancer and configure all its details.

1. Define Load Balancer 2. Assign Security Groups 3. Configure Security Settings 4. Configure Health Check 5. Add EC2 Instances 6. Add Tags 7. Review

Step 1: Define Load Balancer

Basic Configuration

This wizard will walk you through setting up a new load balancer. Begin by giving your new load balancer a unique name so that you can identify it from other load balancers you might create. You will also need to configure ports and protocols for your load balancer. Traffic from your clients can be routed from any load balancer port to any port on your EC2 instances. By default, we've configured your load balancer with a standard web server on port 80.

Load Balancer name:

Create LB inside:

Create an internal load balancer: (what's this?)

Enable advanced VPC configuration:

Listener Configuration:

Load Balancer Protocol	Load Balancer Port	Instance Protocol	Instance Port
HTTP	80	HTTP	80

5. Assign the default security groups and configure security settings.

1. Define Load Balancer 2. Assign Security Groups 3. Configure Security Settings 4. Configure Health Check 5. Add EC2 Instances 6. Add Tags 7. Review

Step 2: Assign Security Groups

You have selected the option of having your Elastic Load Balancer inside of a VPC, which allows you to assign security groups to your load balancer. Please select the security groups to assign to this load balancer. This can be changed at any time.

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

Filter:

Security Group ID	Name	Description
<input type="checkbox"/> sg-0a2a1c3d6c5875173	AutoScaling-Security-Group-1	AutoScaling-Security-Group-1 (2020-09-19T08:09:32.592Z)
<input checked="" type="checkbox"/> sg-0ca7ee69	default	default VPC security group
<input type="checkbox"/> sg-0c7a0b1db06b58f2d	launch-wizard-1	launch-wizard-1 created 2020-09-19T13:34:19.150+05:30
<input type="checkbox"/> sg-0a027b5526435aec7	WordPress Certified by Bitnami and Automattic-5-5-0 on Debian 10-AutogenByAWSMP-1	This security group was generated by AWS Marketplace and is based on recommended s

6. Configure the health check.

Create Load Balancer | EC2 Man... x +

ap-south-1.console.aws.amazon.com/ec2/v2/home?region=ap-south-1#CreateELBWizard:

Services Resource Groups

Chinmayee Mumbai Support

1. Define Load Balancer 2. Assign Security Groups 3. Configure Security Settings 4. Configure Health Check 5. Add EC2 Instances 6. Add Tags 7. Review

Step 4: Configure Health Check

Your load balancer will automatically perform health checks on your EC2 instances and only route traffic to instances that pass the health check. If an instance fails the health check, it is automatically removed from the load balancer. Customize the health check to meet your specific needs.

Ping Protocol

Ping Port

Ping Path

Advanced Details

Response Timeout seconds

Interval seconds

Unhealthy threshold

Healthy threshold

Cancel Previous Next: Add EC2 Instances

Feedback English (US)

© 2008 - 2020, Amazon Internet Services Private Ltd. or its affiliates. All rights reserved. Privacy Policy Terms of Use

Type here to search

1:47 PM 9/19/2020

7. Add the EC2 instance.

Create Load Balancer | EC2 Man... x +

ap-south-1.console.aws.amazon.com/ec2/v2/home?region=ap-south-1#CreateELBWizard:

Services Resource Groups

Chinmayee Mumbai Support

1. Define Load Balancer 2. Assign Security Groups 3. Configure Security Settings 4. Configure Health Check 5. Add EC2 Instances 6. Add Tags 7. Review

Step 5: Add EC2 Instances

The table below lists all your running EC2 Instances. Check the boxes in the Select column to add those instances to this load balancer.

VPC vpc-f2667d9a (172.31.0.0/16)

Instance	Name	State	Security groups	Zone	Subnet ID	Subnet CIDR
<input checked="" type="checkbox"/>	i-0c18b677f643a980c	running	launch-wizard-1	ap-south-1a	subnet-fb585893	172.31.32.0/20

Availability Zone Distribution

1 instance in ap-south-1a

Enable Cross-Zone Load Balancing

Enable Connection Draining seconds

Cancel Previous Next: Add Tags

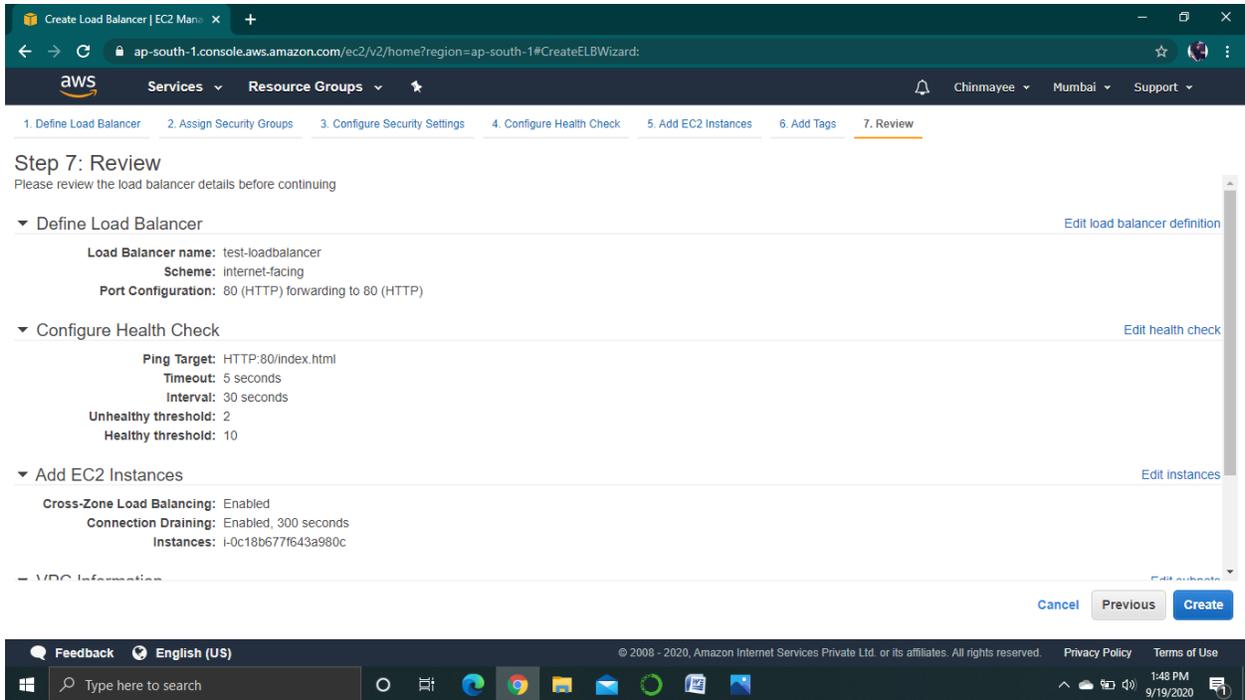
Feedback English (US)

© 2008 - 2020, Amazon Internet Services Private Ltd. or its affiliates. All rights reserved. Privacy Policy Terms of Use

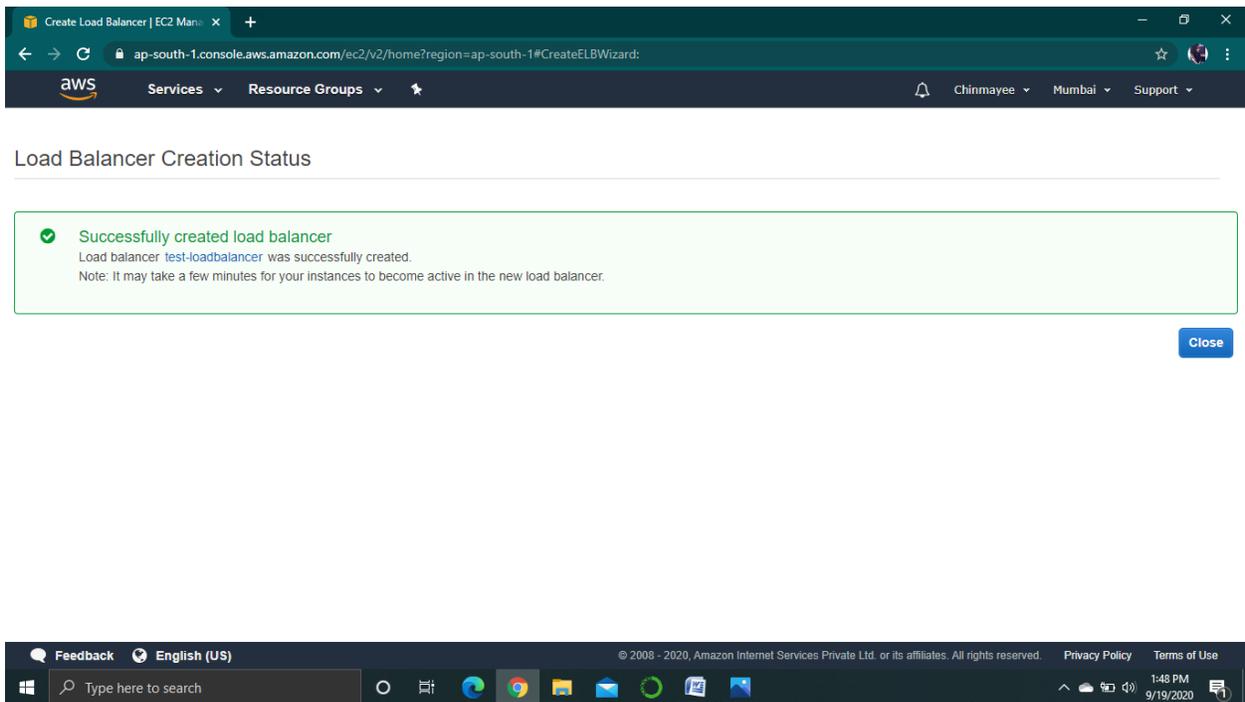
Type here to search

1:47 PM 9/19/2020

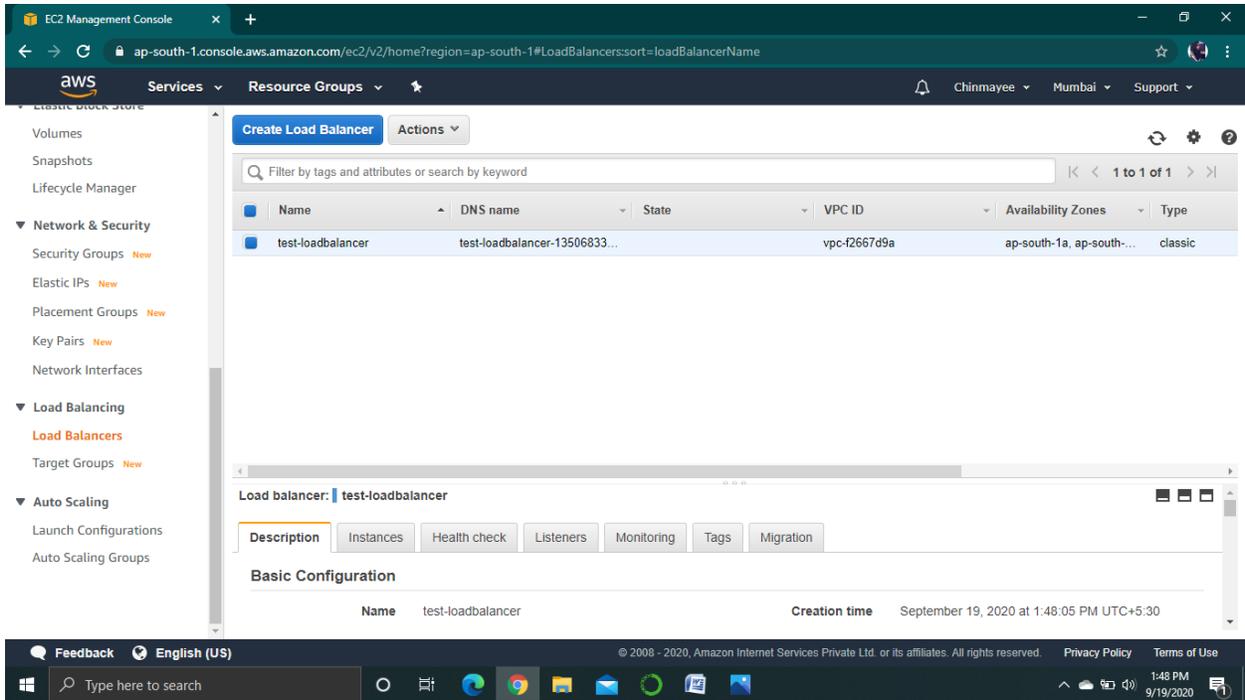
8. Add tags and click on review.



9. Check the status of the load balancer.

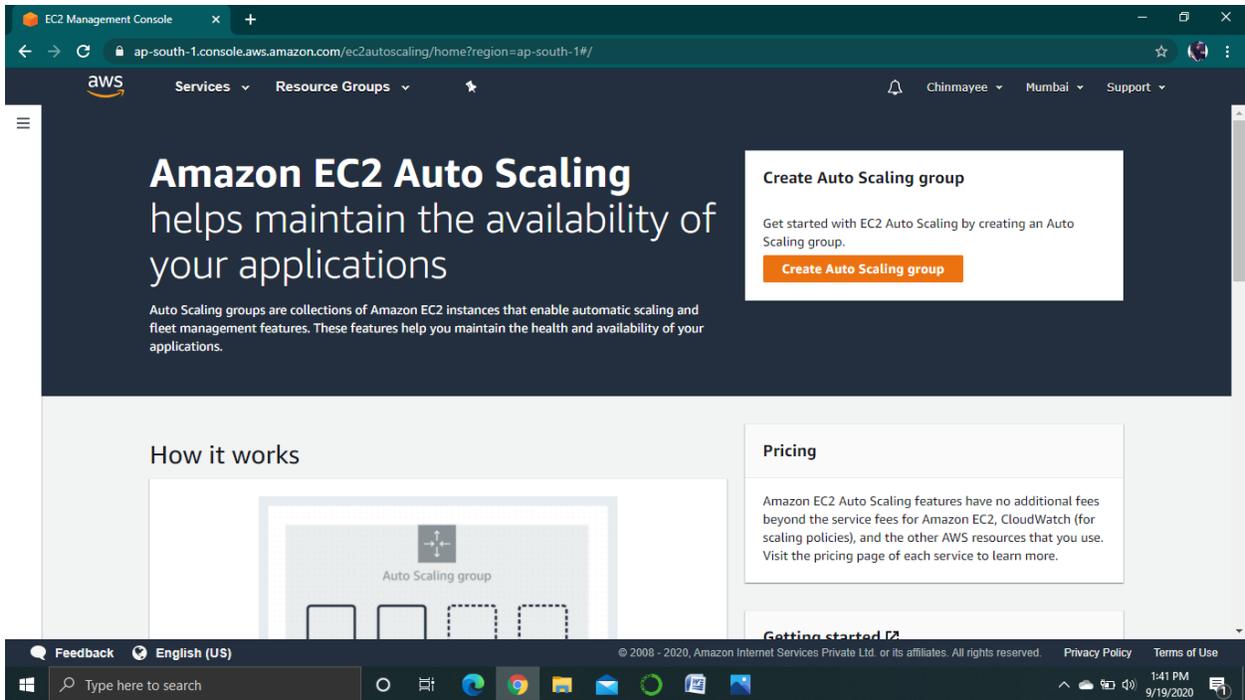


10. The load balancer created will be displayed on the dashboard.

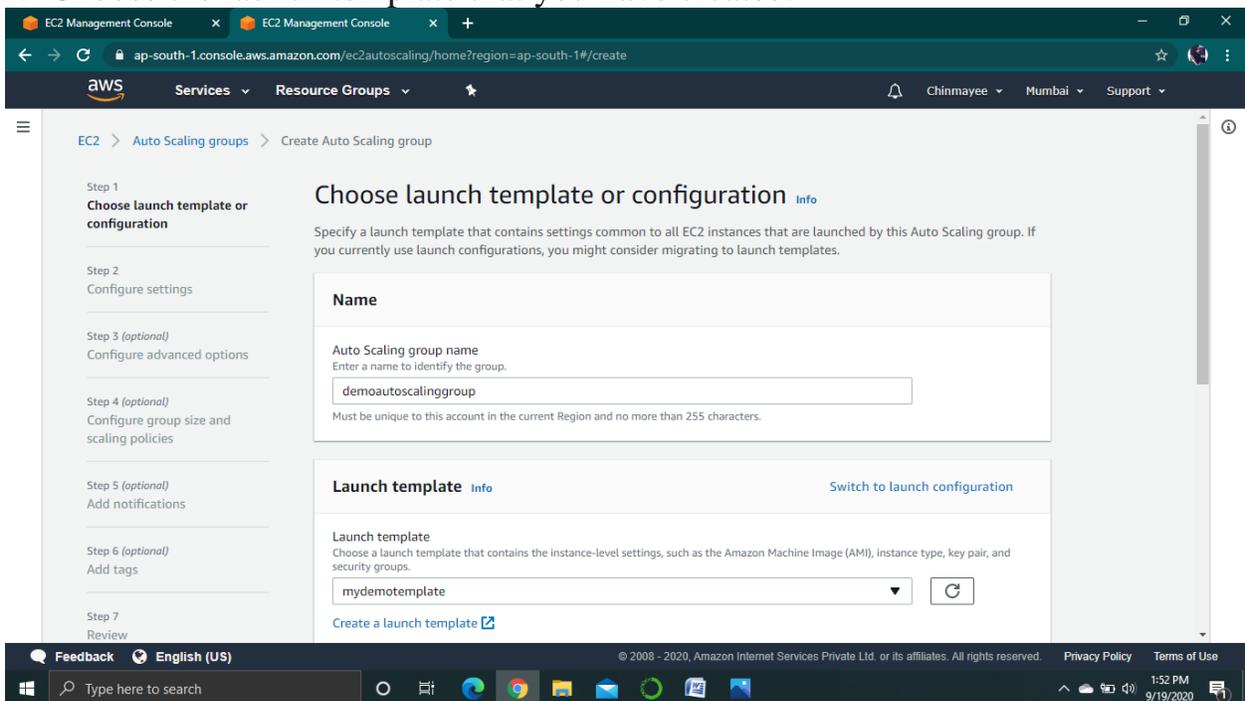


IMPLEMENTING AUTO SCALING GROUP

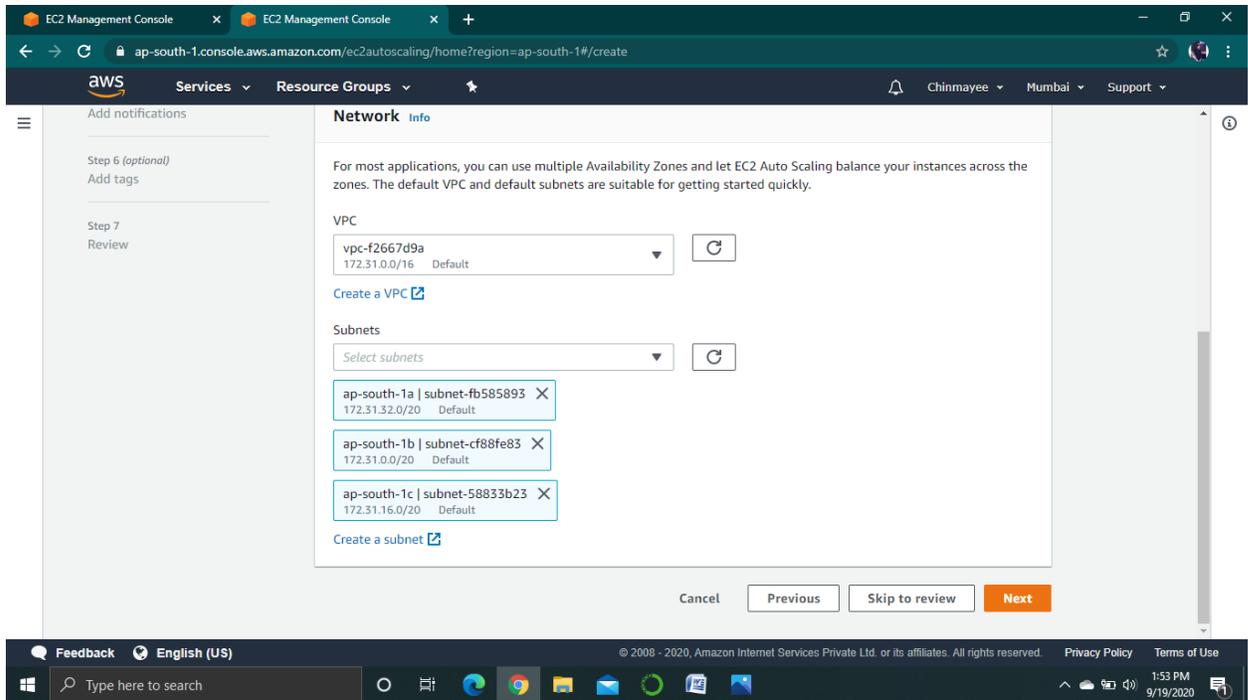
1. From EC2 dashboard, on the Auto Scaling groups page, choose Create an Auto Scaling group.



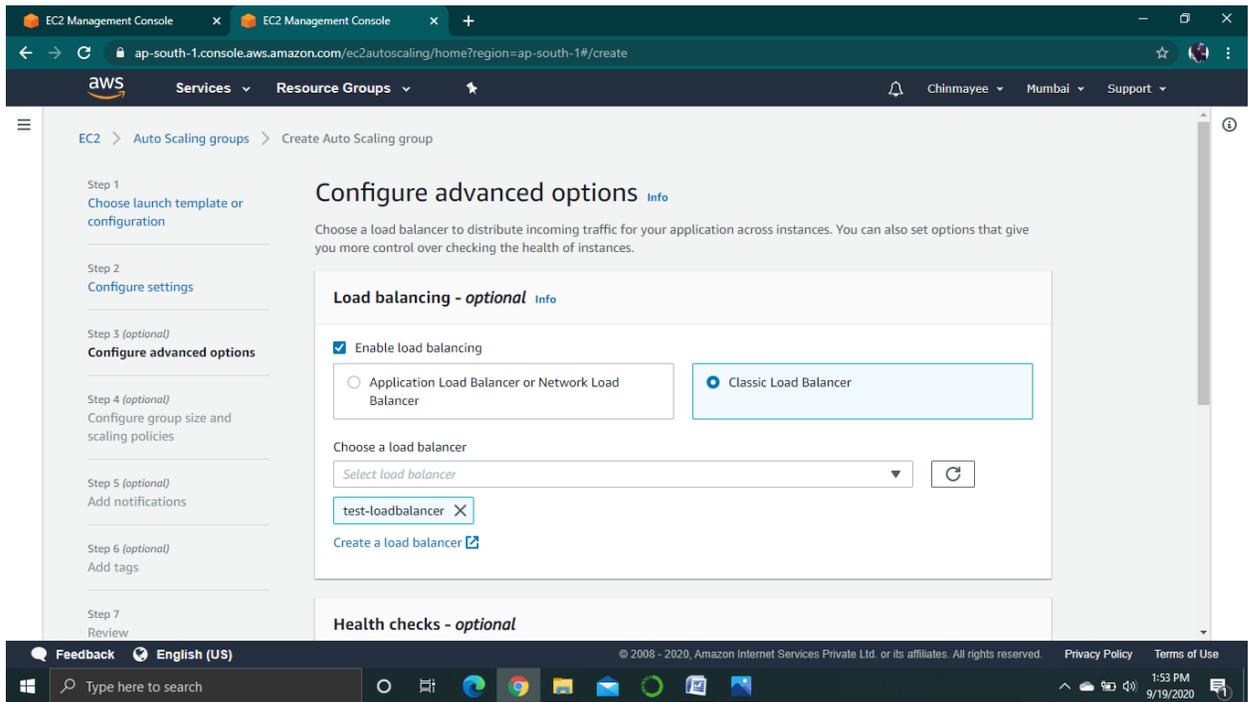
2. Choose the launch template that you have created.



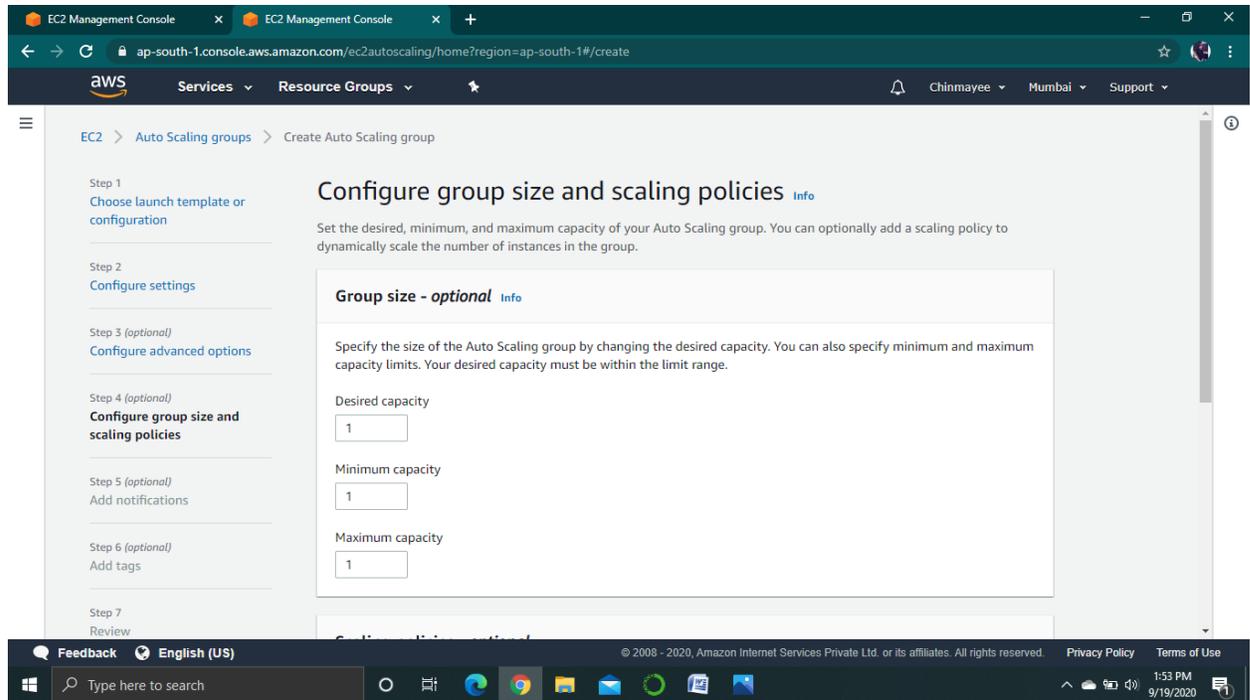
3. Choose the default version of the launch template to use when scaling out.
4. Choose Next.
5. Keep Network set to the default VPC for your chosen AWS Region.
6. For **Subnet**, choose a subnet from each Availability Zone that you want to include.



7. Enable the load balancing option and select the load balancer which you have created.

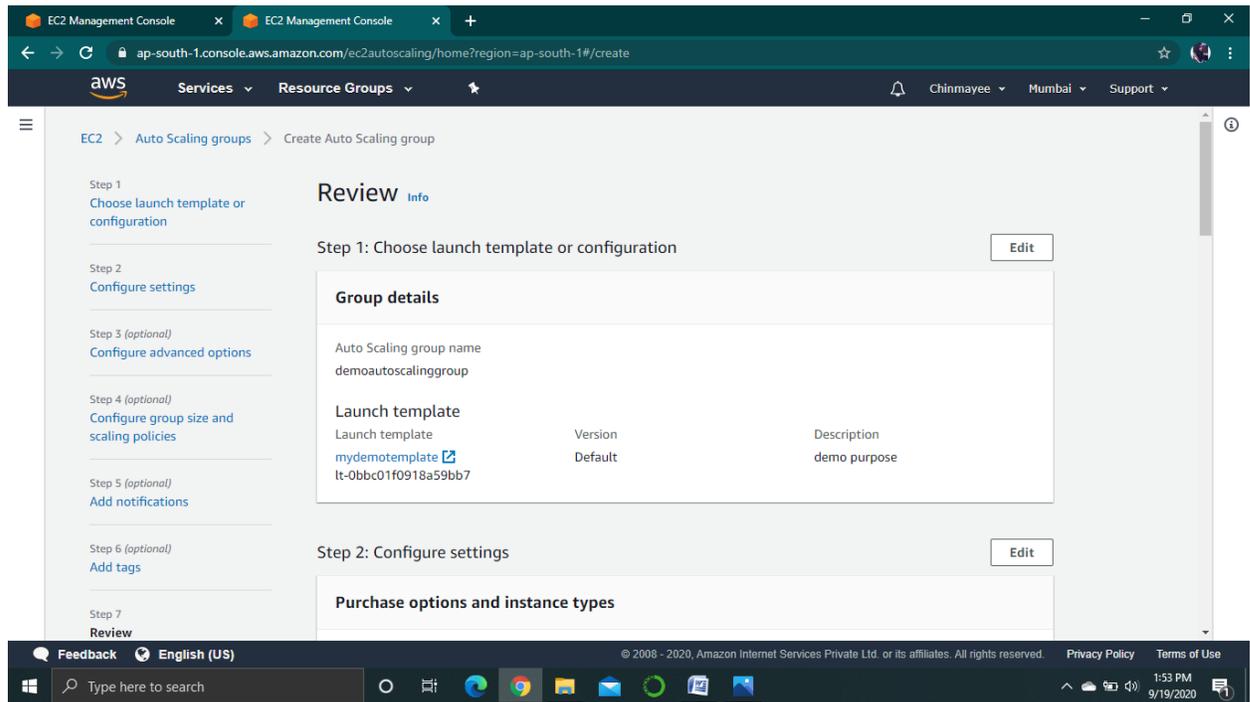


8. Configure the group size and scaling policy. Choose desired capacity as 1.

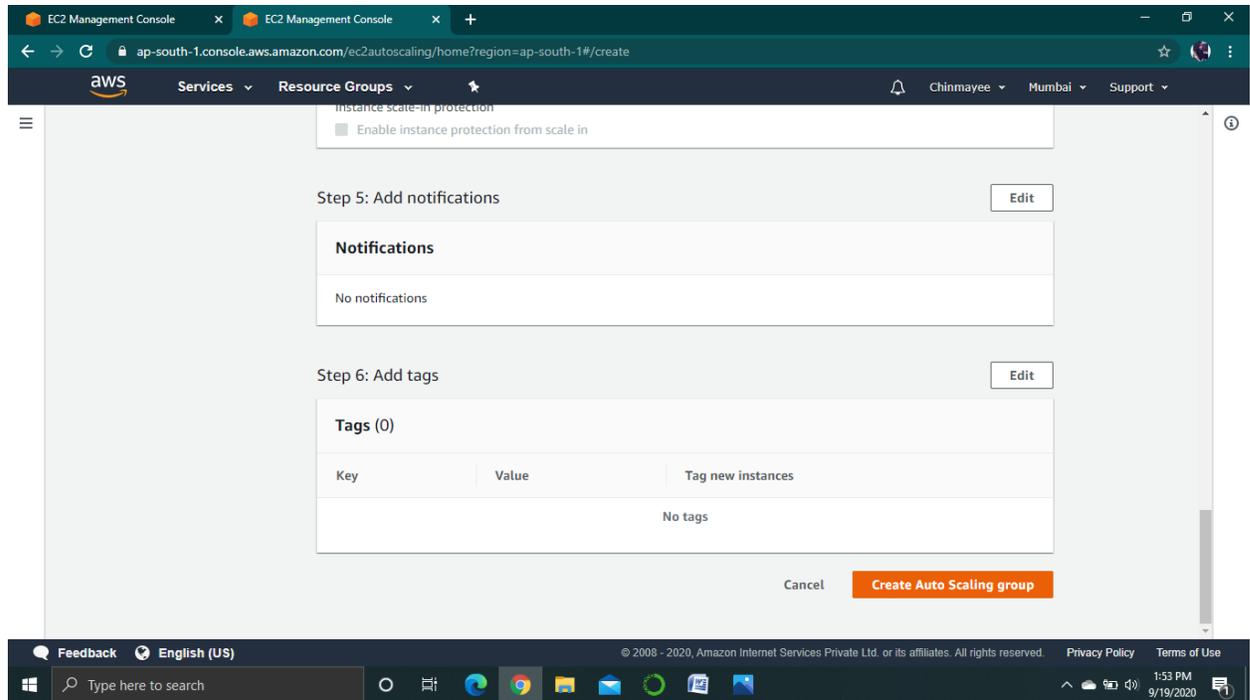


9. Notifications and tags can be added.

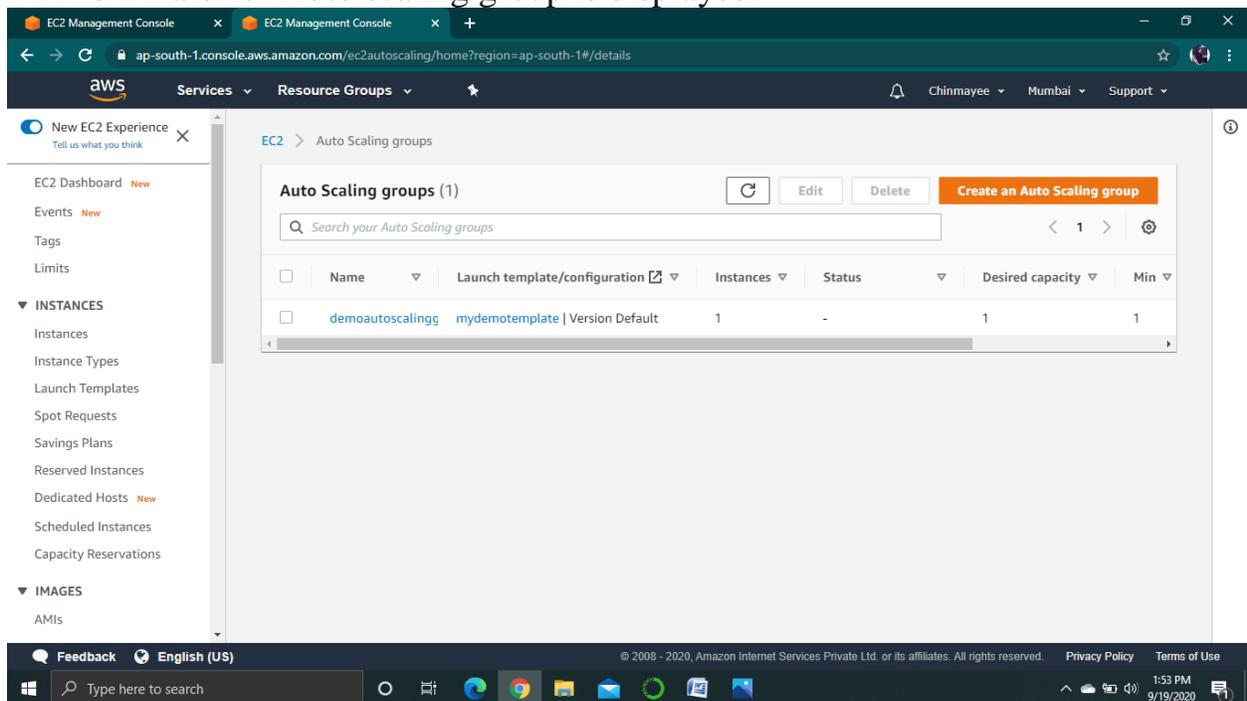
10. Choose review.



11. Choose Create Auto Scaling group.

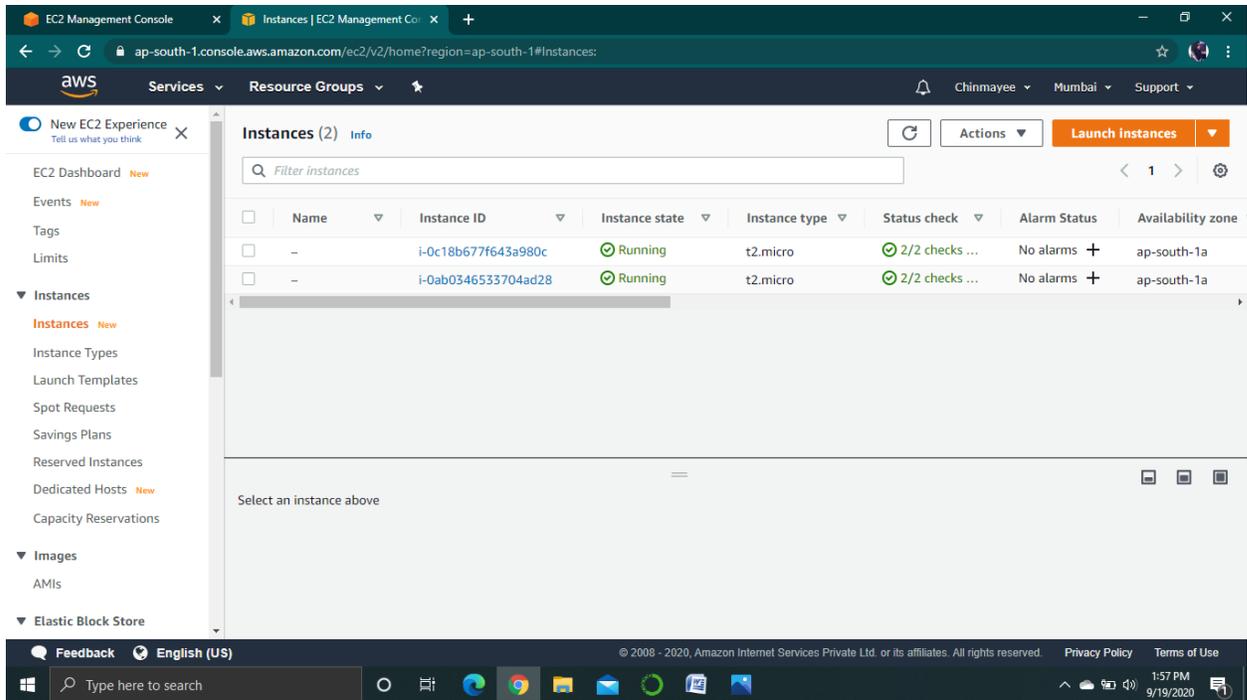


12. The wizard for Auto scaling group is displayed.



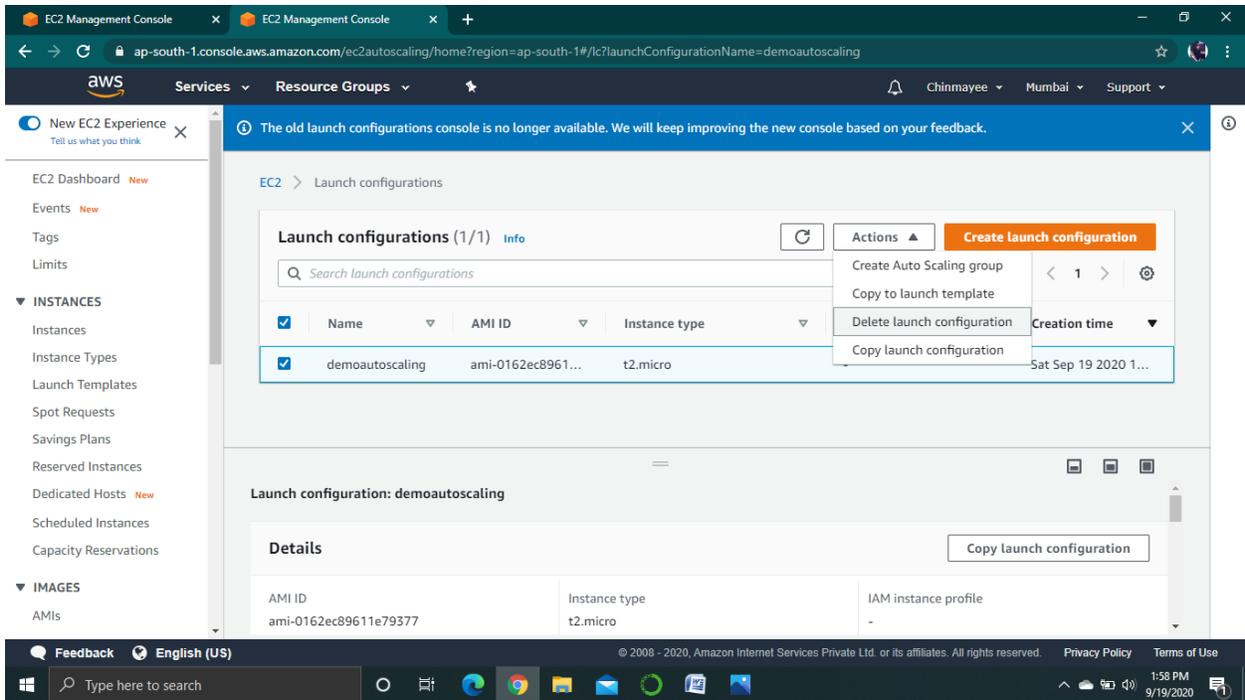
13. Verify whether Auto scaling group has created EC2 instance.

14. The instance has been launched successfully.

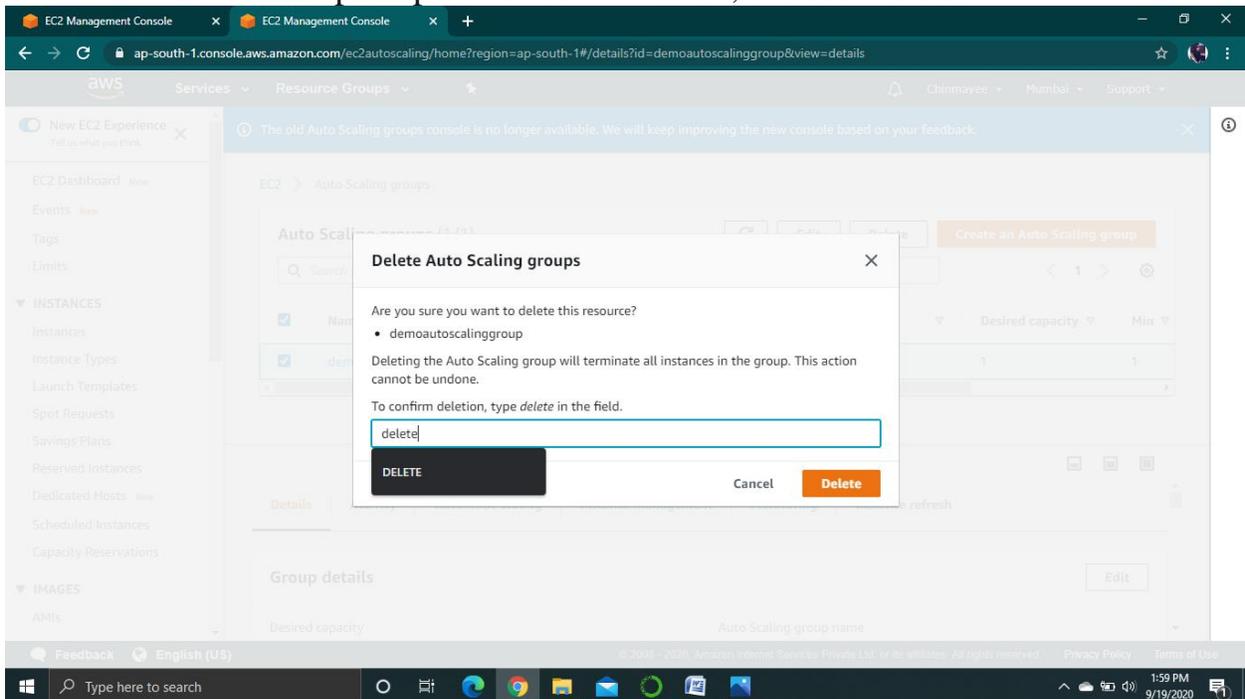


DETACHING EC2 INSTANCE FROM LOAD BALANCING

1. Open the Amazon EC2 console .
2. On the navigation pane, under AUTO SCALING, choose Auto Scaling Groups.
3. Select the check box next to your Auto Scaling group.



4. Choose Delete. When prompted for confirmation, choose Delete.

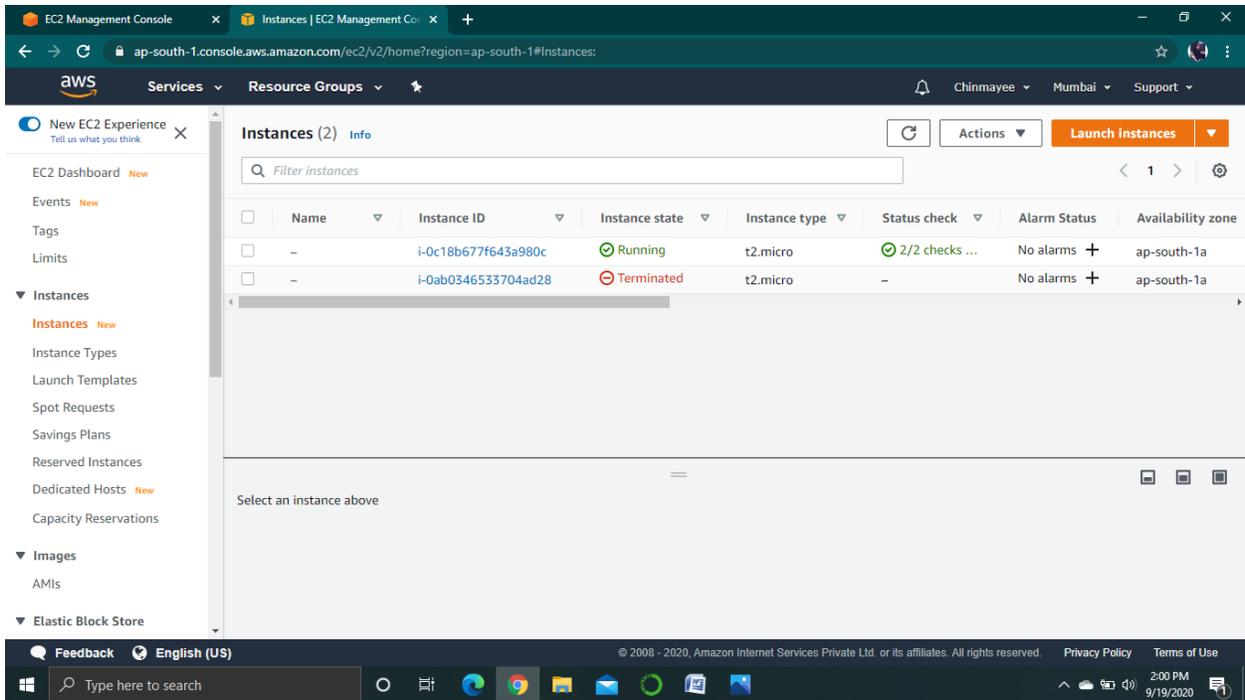


5. On the navigation pane, under AUTO SCALING, choose Launch Configuration.

6. Select the actions, and choose delete Launch Configuration.

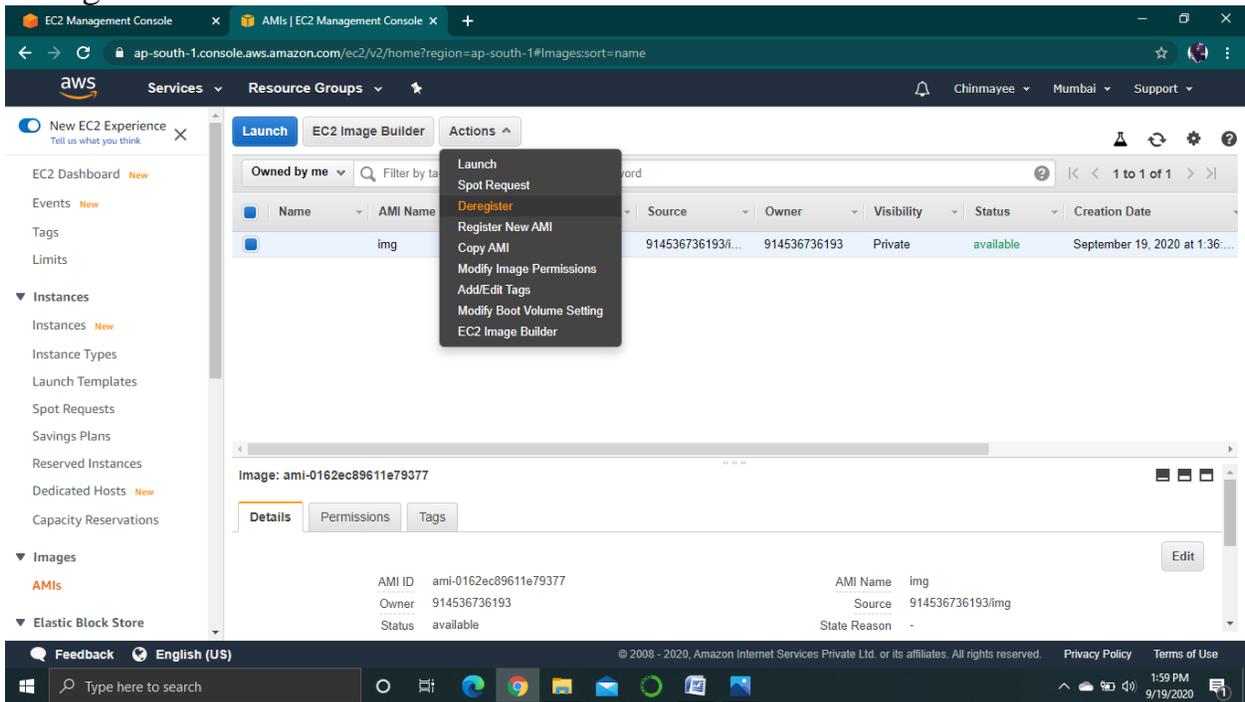
7. Choose Delete. When prompted for confirmation, choose Delete.

8. The instances created will also get terminated.



9. Terminate the instance created for AMI.

10. Deregister the AMI created.



11. Select the load balancer you have created and select actions and then delete.

EC2 Management Console

ap-south-1.console.aws.amazon.com/ec2/v2/home?region=ap-south-1#LoadBalancers:sort=loadBalancerName

Services Resource Groups

Chinmayee Mumbai Support

Filter by tags and attributes

Name	State	VPC ID	Availability Zones	Type
test-loadbalancer		vpc-f2667d9a	ap-south-1a, ap-south-...	classic

Actions

- Edit health check
- Edit subnets
- Edit IP address type
- Edit instances
- Edit listeners
- Edit security groups
- Edit attributes
- Delete

Load balancer: test-loadbalancer

Description Instances Health check Listeners Monitoring Tags Migration

Basic Configuration

Name	Creation time
test-loadbalancer	September 19, 2020 at 1:48:05 PM UTC+5:30

Feedback English (US)

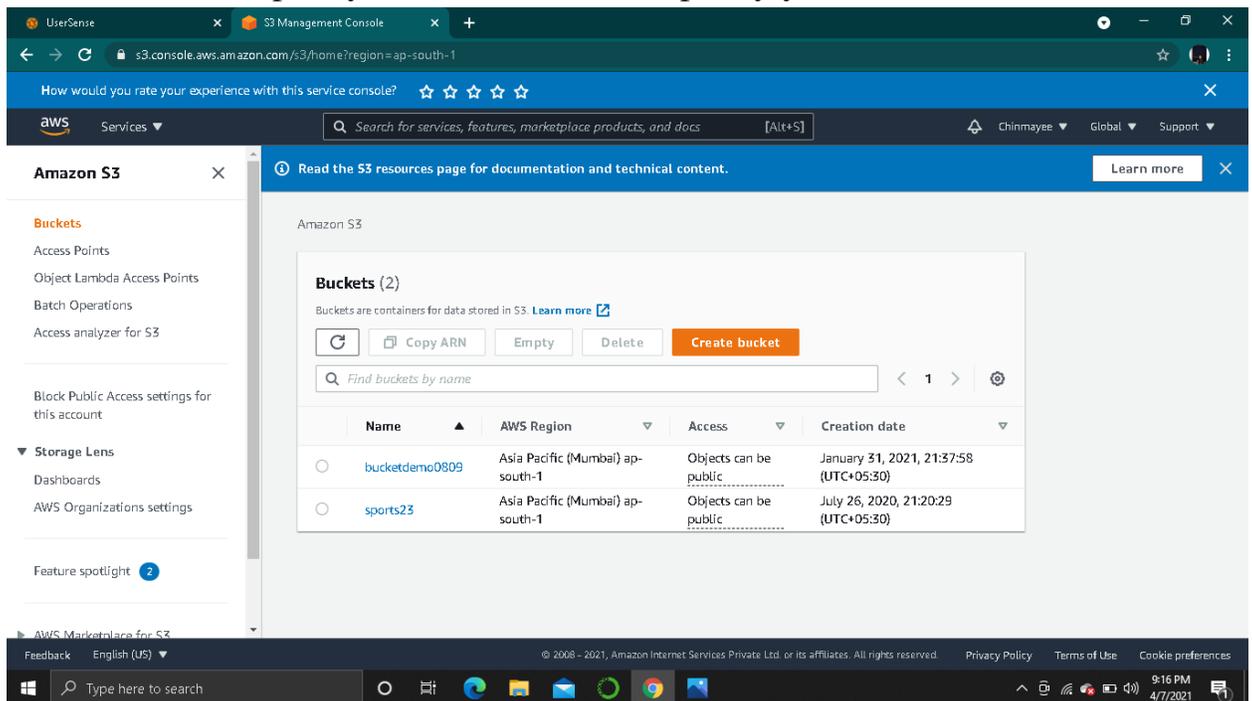
© 2008 - 2020, Amazon Internet Services Private Ltd. or its affiliates. All rights reserved. Privacy Policy Terms of Use

1:59 PM 9/19/2020

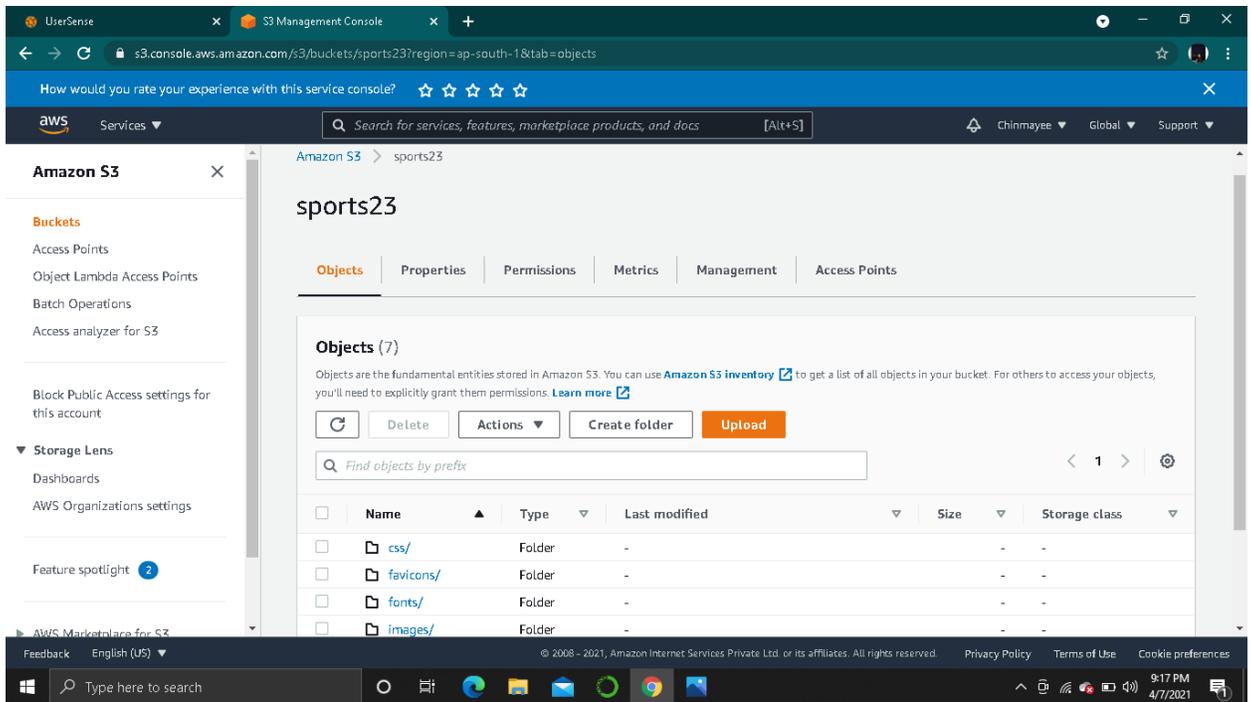
IMPLEMENTATION OF S3 BUCKET POLICY AND VERSIONING

STEPS TO BE FOLLOWED:-

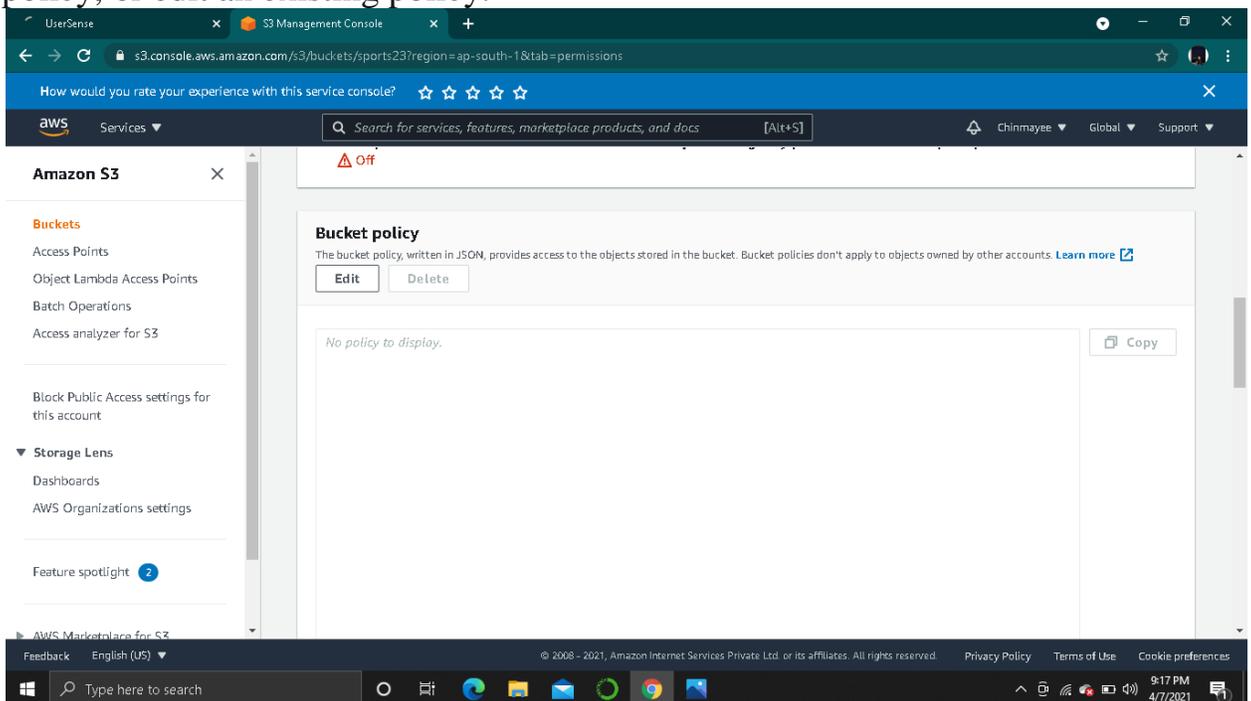
- Sign in to AWS console.
- Open the service S3.
- In the Buckets list, choose the name of the bucket that you want to create a bucket policy for or whose bucket policy you want to edit.



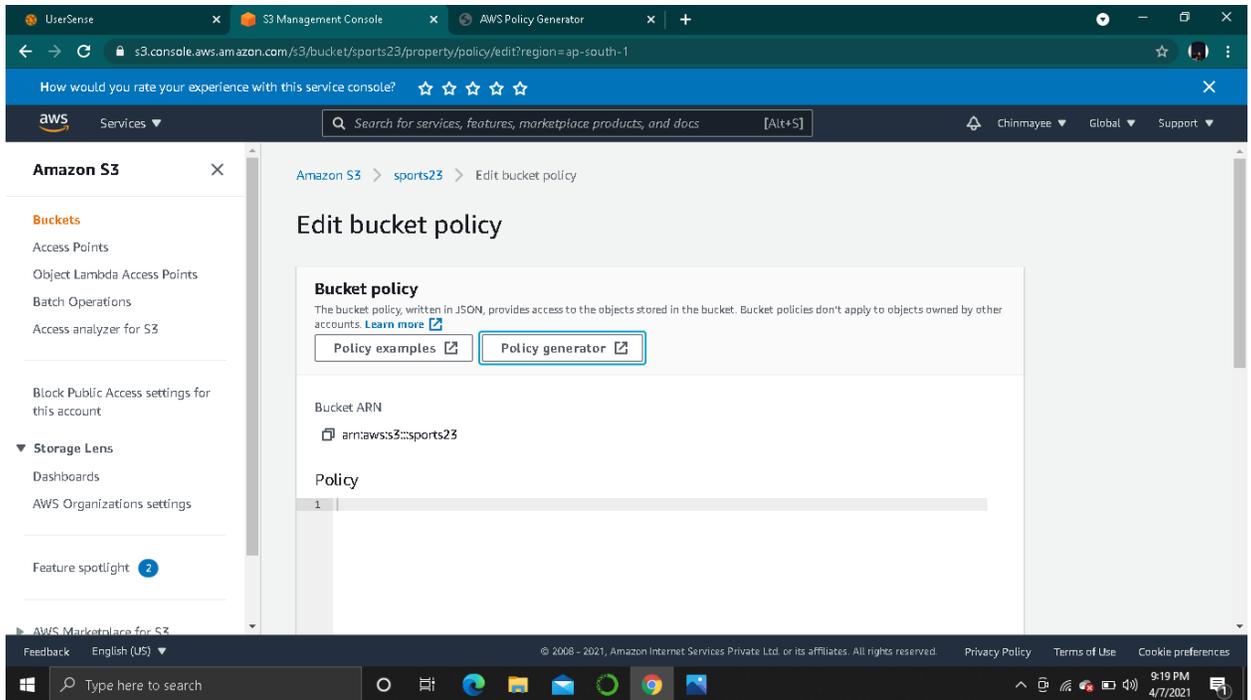
- Choose Permissions.



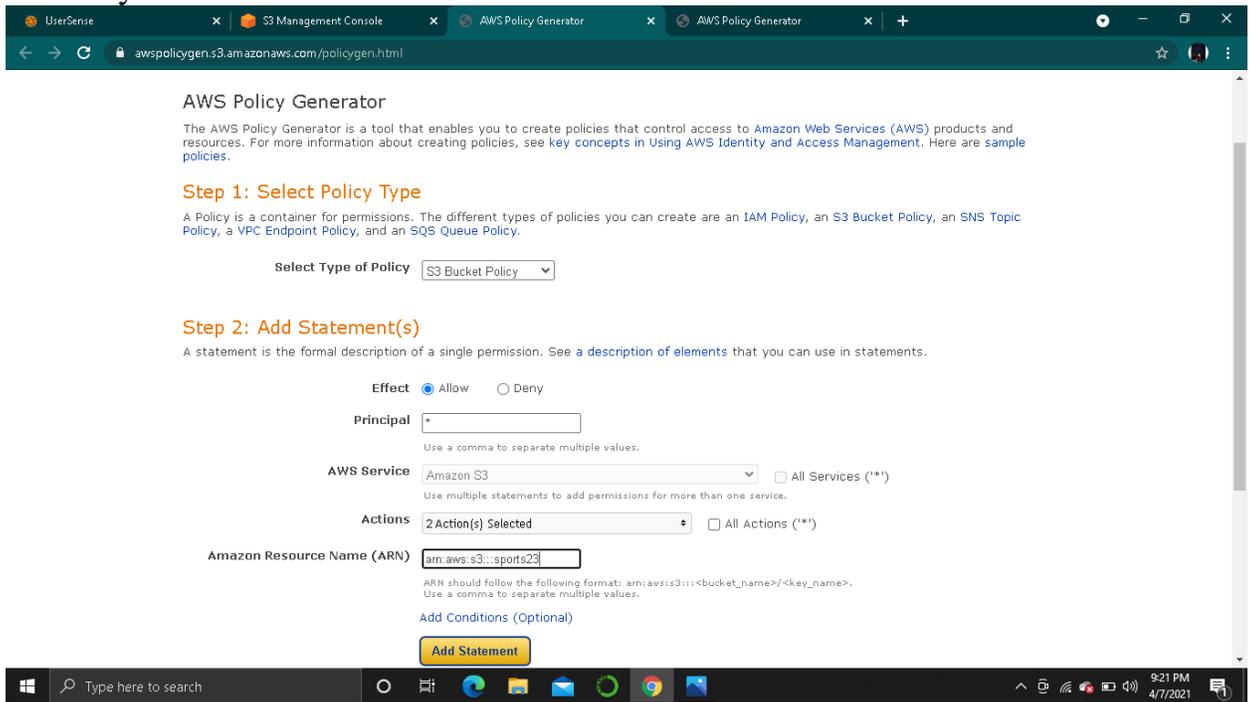
- In the Bucket policy editor text box, type or copy and paste a new bucket policy, or edit an existing policy.



- Choose Policy generator to open the AWS Policy Generator in a new window.



- On the policy generator page, select S3 Bucket Policy from the Select Type of Policy menu.



- Add one or more statements by populating the fields presented, and then choose Generate Policy.

Amazon Resource Name (ARN)

ARN should follow the following format: `arn:aws:s3:::<bucket_name>/<key_name>`.
Use a comma to separate multiple values.

Add Conditions (Optional)

Add Statement

You added the following statements. Click the button below to Generate a policy.

Principal(s)	Effect	Action	Resource	Conditions
* *	Allow	<ul style="list-style-type: none"> s3:GetObject s3:PutObject 	arn:aws:s3:::sports23	None

Step 3: Generate Policy

A policy is a document (written in the [Access Policy Language](#)) that acts as a container for one or more statements.

Generate Policy Start Over

This AWS Policy Generator is provided for informational purposes only, you are still responsible for your use of Amazon Web Services technologies and ensuring that your use is in compliance with all applicable terms and conditions. This AWS Policy Generator is provided as is without warranty of any kind, whether express, implied, or statutory. This AWS Policy Generator does not modify the applicable terms and conditions governing your use of Amazon Web Services technologies.

©2010, Amazon Web Services LLC or its affiliates. All rights reserved.

An amazon.com company

- Copy the generated policy text, and return to the Edit bucket policy page in the Amazon S3 console.

Amazon Resource Name (ARN)

ARN should follow the following format: `arn:aws:s3:::<bucket_name>/<key_name>`.

Add Conditions (Optional)

Add Statement

You added the following statements. Click the button below to Generate a policy.

Principal(s)	Effect	Action	Resource	Conditions
* *	Allow	<ul style="list-style-type: none"> s3:GetObject s3:PutObject 	arn:aws:s3:::sports23	None

Step 3: Generate Policy

A policy is a document (written in the [Access Policy Language](#)) that acts as a container for one or more statements.

Generate Policy Start Over

This AWS Policy Generator is provided for informational purposes only, you are still responsible for your use of Amazon Web Services technologies and ensuring that your use is in compliance with all applicable terms and conditions. This AWS Policy Generator is provided as is without warranty of any kind, whether express, implied, or statutory. This AWS Policy Generator does not modify the applicable terms and conditions governing your use of Amazon Web Services technologies.

©2010, Amazon Web Services LLC or its affiliates. All rights reserved.

An amazon.com company

Policy JSON Document

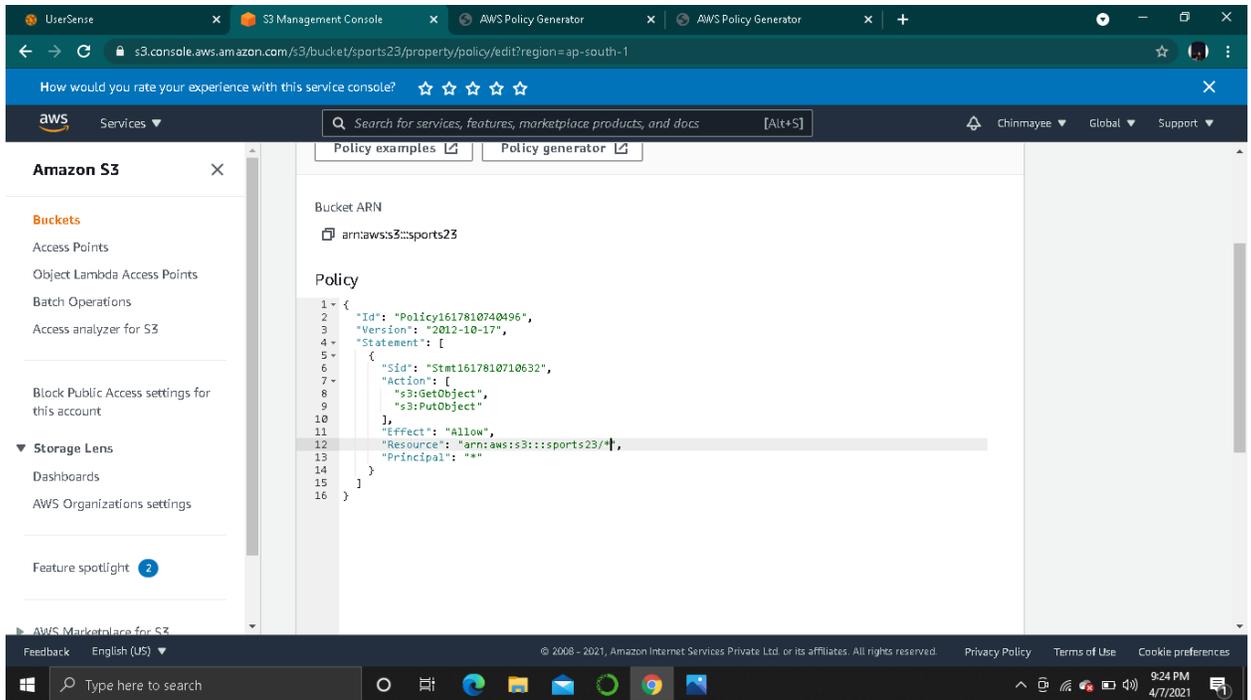
Click below to edit. To save the policy, copy the text below to a text editor. Changes made below will **not be reflected in the policy generator tool.**

```

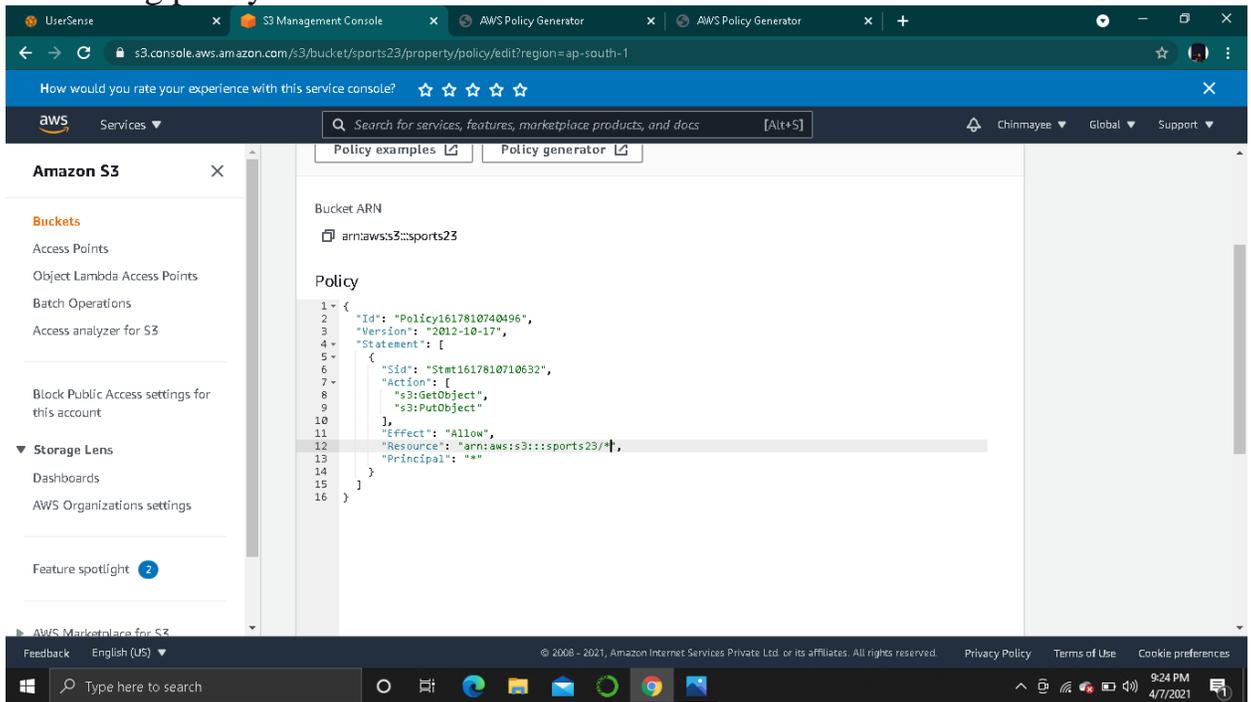
{
  "Id": "Policy1617810740498",
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "Stmt1617810710632",
      "Action": [
        "s3:GetObject",
        "s3:PutObject"
      ],
      "Effect": "Allow",
      "Resource": "arn:aws:s3:::sports23",
      "Principal": "*"
    }
  ]
}

```

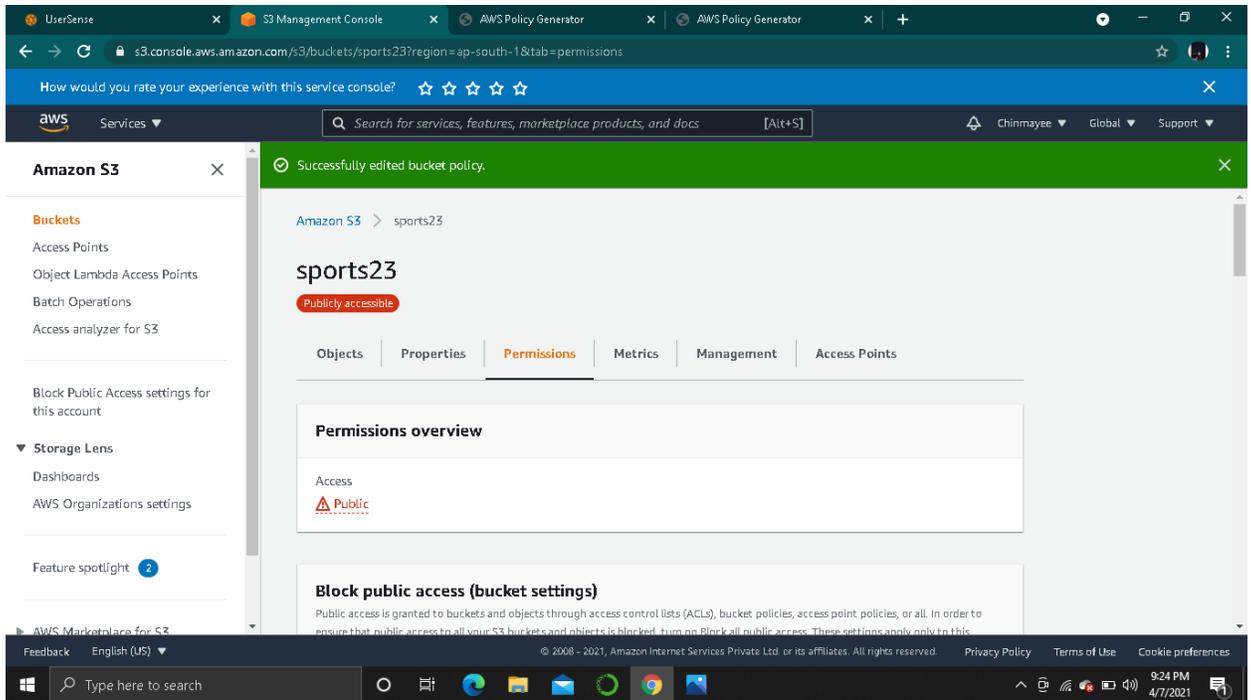
Close



- In the Policy text field, type or copy and paste a new bucket policy, or edit an existing policy.

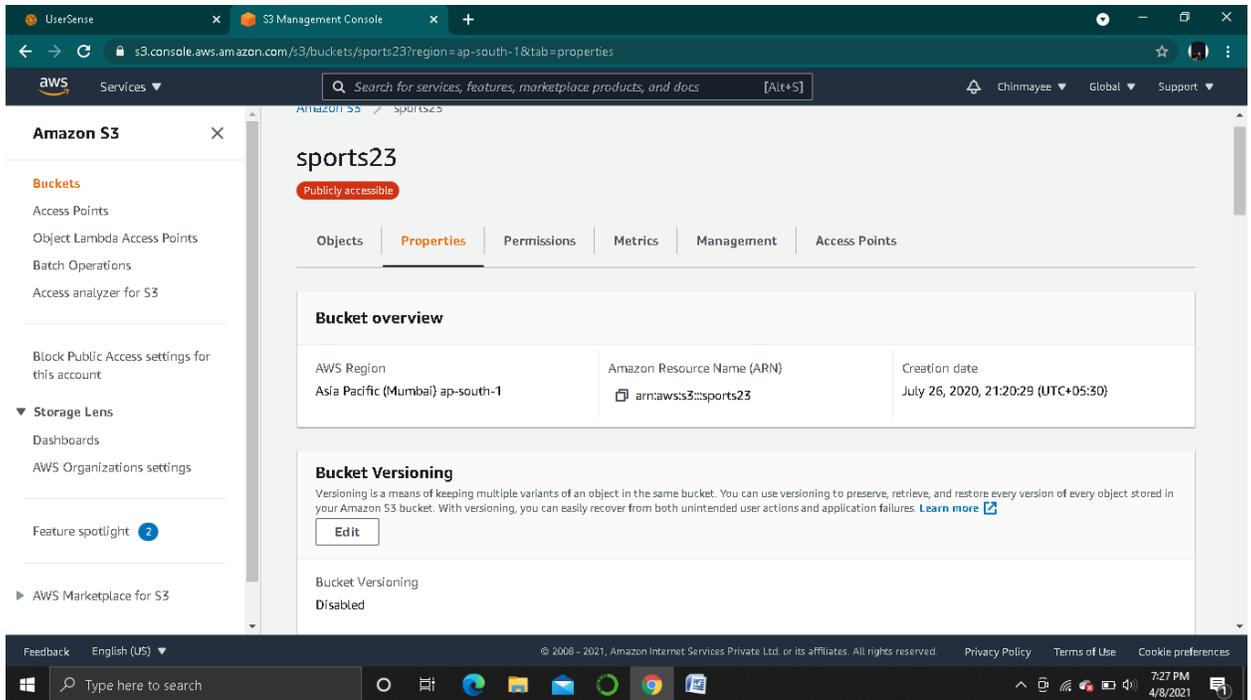


- Preview how your new policy affects public and cross-account access to your resource.
- Choose Save changes.

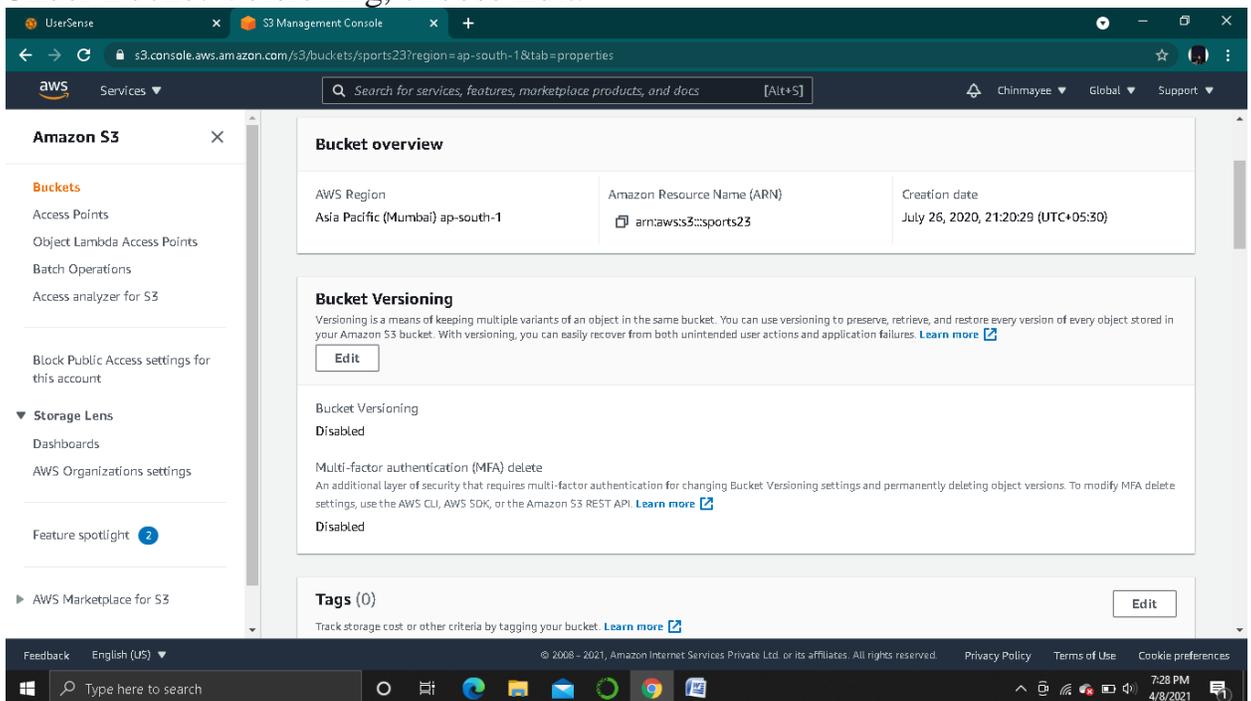


BUCKET VERSIONING

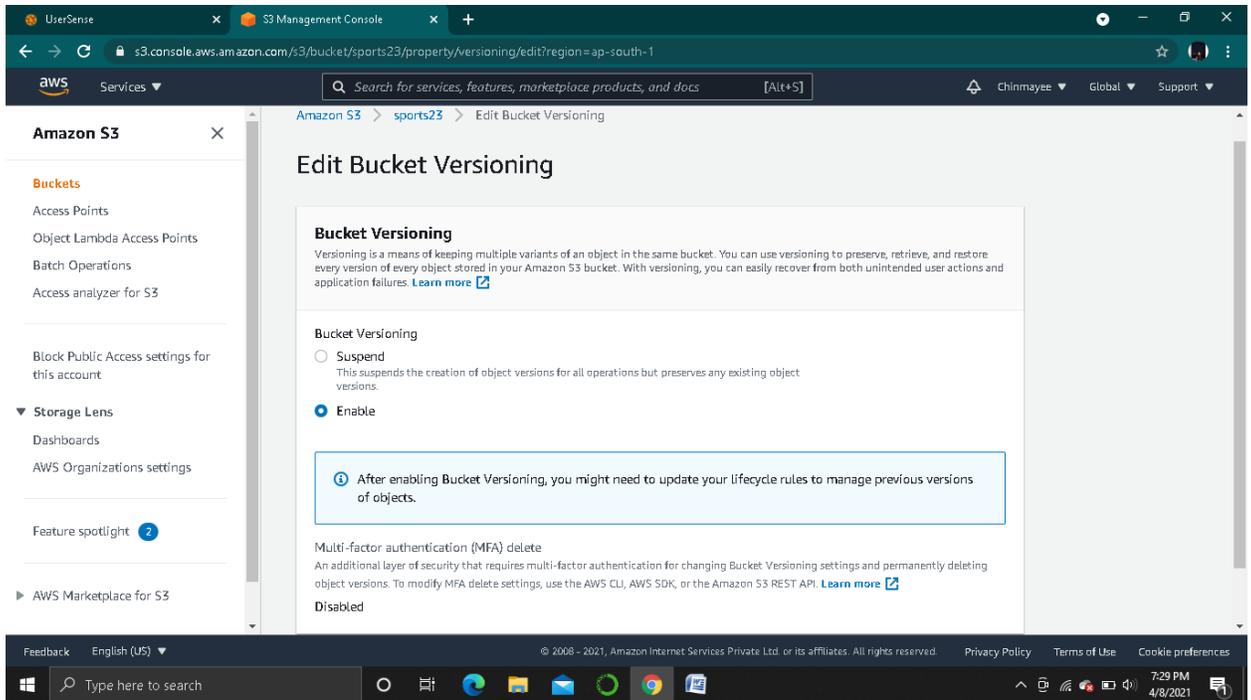
- Sign in to the AWS Management Console and open the Amazon S3.
- In the Buckets list, choose the name of the bucket that you want to enable versioning for.
- Choose Properties.



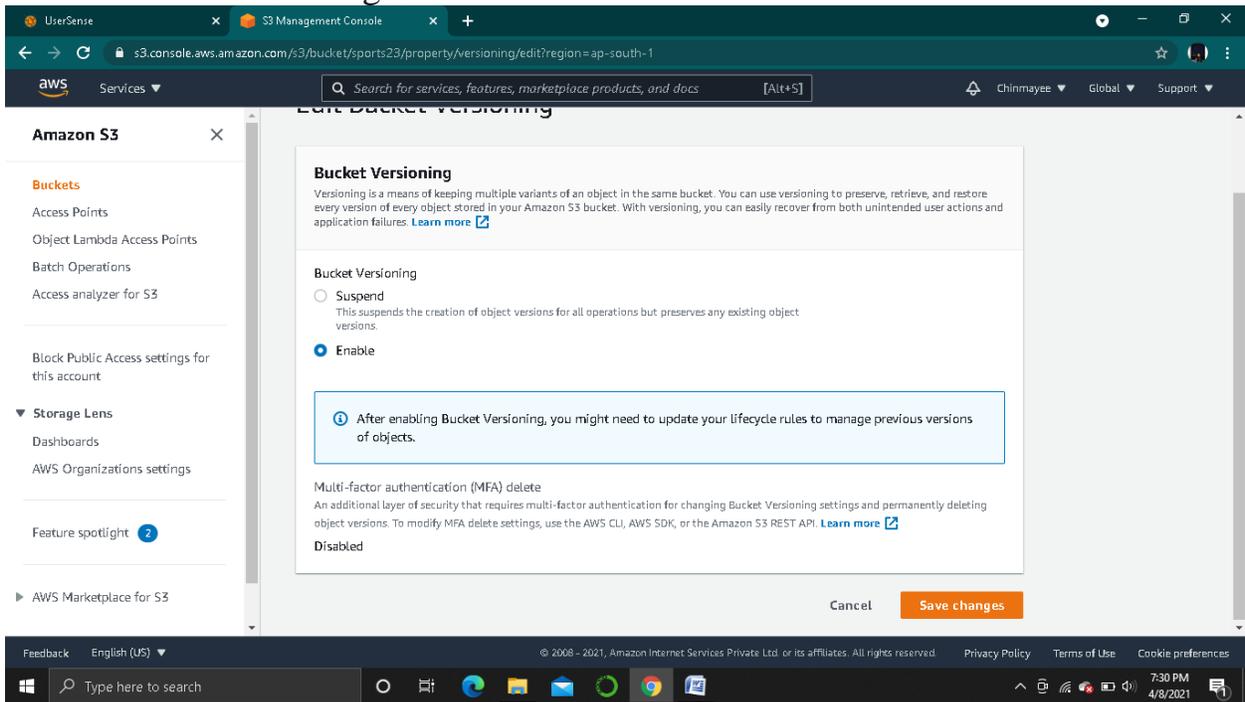
- Under Bucket Versioning, choose Edit.



- Choose Suspend or Enable.



- Choose save changes.



- The window will appear.

UserSense S3 Management Console

s3.console.aws.amazon.com/s3/buckets/sports23?region=ap-south-1&tab=properties

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

Chinmayee Global Support

Amazon S3

- Buckets
 - Access Points
 - Object Lambda Access Points
 - Batch Operations
 - Access analyzer for S3
- Block Public Access settings for this account
- Storage Lens
 - Dashboards
 - AWS Organizations settings
- Feature spotlight 2
- AWS Marketplace for S3

Successfully edited Bucket Versioning

To transition, archive, or delete older object versions, [configure lifecycle rules](#) for this bucket.

AWS Region	Amazon Resource Name (ARN)	Creation date
Asia Pacific (Mumbai) ap-south-1	arn:aws:s3:::sports23	July 26, 2020, 21:20:29 (UTC+05:30)

Bucket Versioning

Versioning is a means of keeping multiple variants of an object in the same bucket. You can use versioning to preserve, retrieve, and restore every version of every object stored in your Amazon S3 bucket. With versioning, you can easily recover from both unintended user actions and application failures. [Learn more](#)

Bucket Versioning

Enabled

Multi-factor authentication (MFA) delete

An additional layer of security that requires multi-factor authentication for changing Bucket Versioning settings and permanently deleting object versions. To modify MFA delete settings, use the AWS CLI, AWS SDK, or the Amazon S3 REST API. [Learn more](#)

Disabled

Tags (0)

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

Type here to search 7:32 PM 4/8/2021