

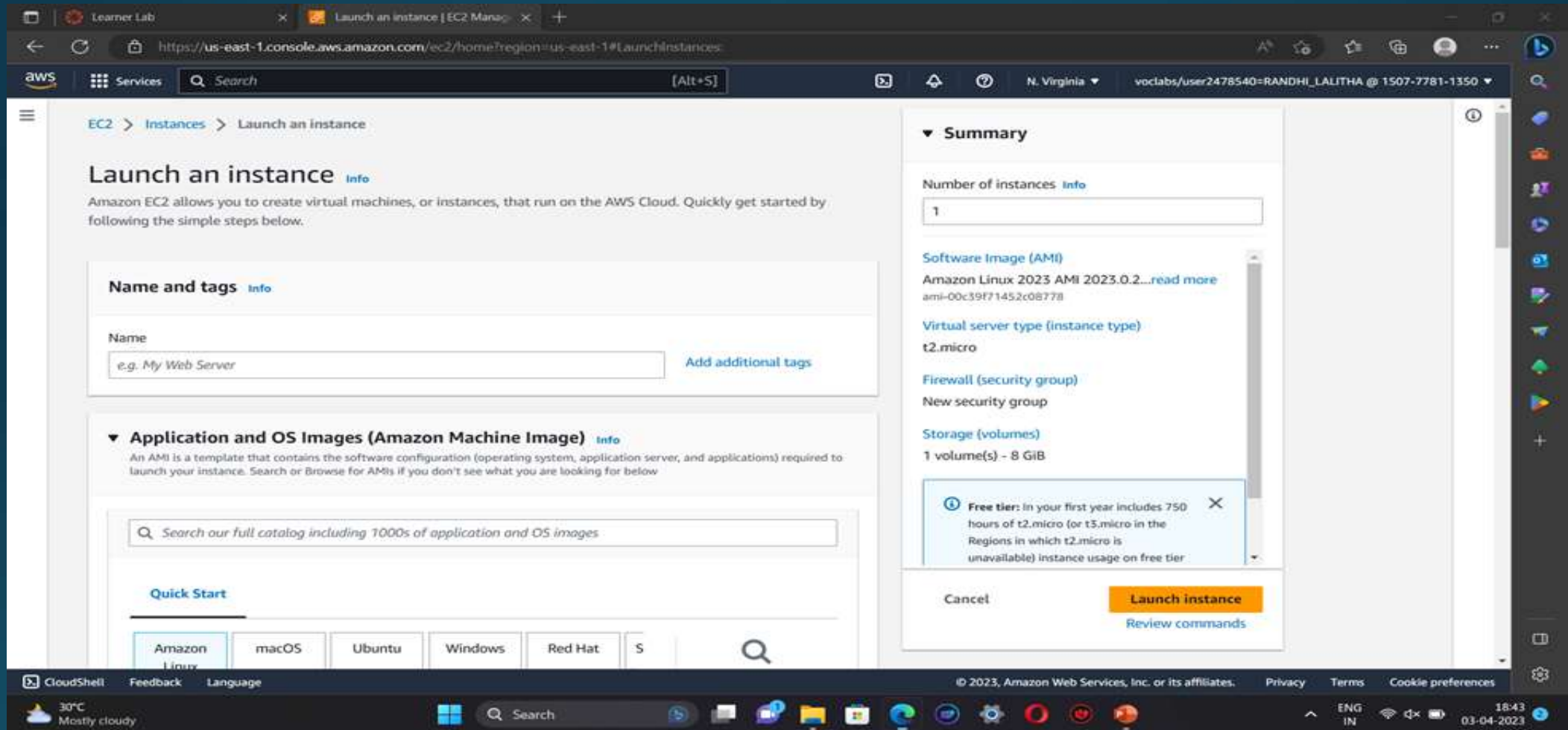
# AWS (AMAZON WEB SERVICES)

T.LIKHITA

20A31A05F7

AMAZON EC2 INSTANCE

**Step-1: Go to AWS services , click EC2 and then select 'launch instances'.**



Step-2: Name the instance, select an AMI(LINUX,WINOWS server) , select a key pair and click launch instance.

Search our full catalog including 1000s of application and OS images

### Quick Start

Amazon Linux

macOS

Ubuntu

Windows

Red Hat

[Browse more AMIs](#)

Including AMIs from AWS, Marketplace and the Community

Amazon Machine Image (AMI)

Microsoft Windows Server 2022 Base

Free tier eligible

ami-0e38fa17744b2f6a5 (64-bit (x86))

Virtualization: hvm ENA enabled: true Root device type: ebs

Description

Microsoft Windows Server 2022 Full Locale English AMI provided by Amazon

Architecture	AMI ID
--------------	--------

### Summary

Number of instances [Info](#)

1

[Software Image \(AMI\)](#)

Microsoft Windows Server 2022 ...[read more](#)

ami-0e38fa17744b2f6a5

[Virtual server type \(instance type\)](#)

t2.micro

[Firewall \(security group\)](#)

New security group

[Storage \(volumes\)](#)

Cancel

Launch instance

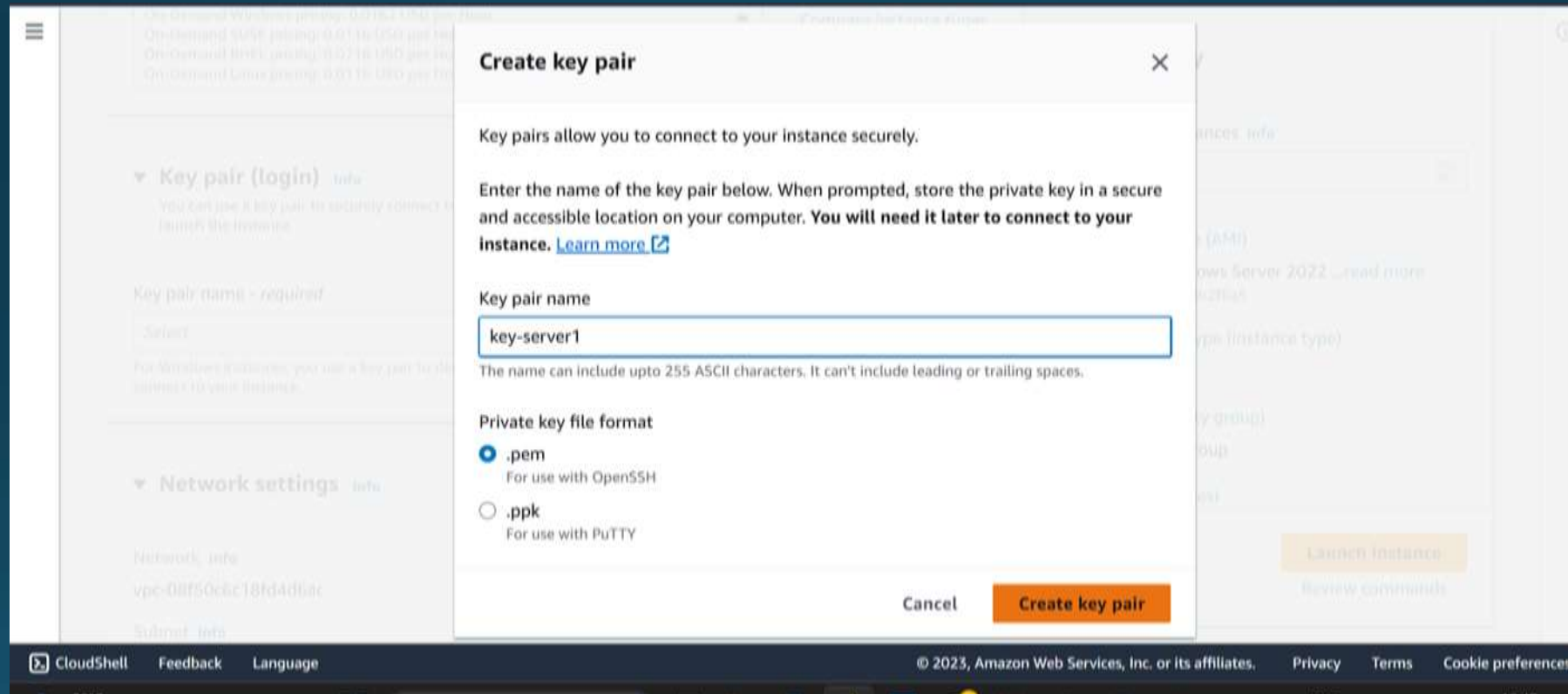
[Review commands](#)

CloudShell Feedback Language

© 2023, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

**Step-3:** For linux-select ppk key and for windows server-select pem key.

**Step-4:** If a key pair is not available create a new key.



The screenshot shows the AWS CloudShell interface with a 'Create key pair' modal dialog box open. The dialog box has a title bar with a close button (X). Inside, it explains that key pairs allow secure connection to instances. It prompts the user to enter a key pair name, with a text input field containing 'key-server1'. Below the name field, it states that the name can include up to 255 ASCII characters and cannot have leading or trailing spaces. Under 'Private key file format', there are two radio button options: '.pem' (selected) for use with OpenSSH, and '.ppk' for use with PuTTY. At the bottom of the dialog are 'Cancel' and 'Create key pair' buttons. The background shows the CloudShell sidebar with sections for 'Key pair (login)' and 'Network settings', and a footer with 'CloudShell', 'Feedback', 'Language', and copyright information for Amazon Web Services, Inc. (© 2023).

**Create key pair**

Key pairs allow you to connect to your instance securely.

Enter the name of the key pair below. When prompted, store the private key in a secure and accessible location on your computer. **You will need it later to connect to your instance.** [Learn more](#)

Key pair name

key-server1

The name can include upto 255 ASCII characters. It can't include leading or trailing spaces.

Private key file format

☒ .pem  
For use with OpenSSH

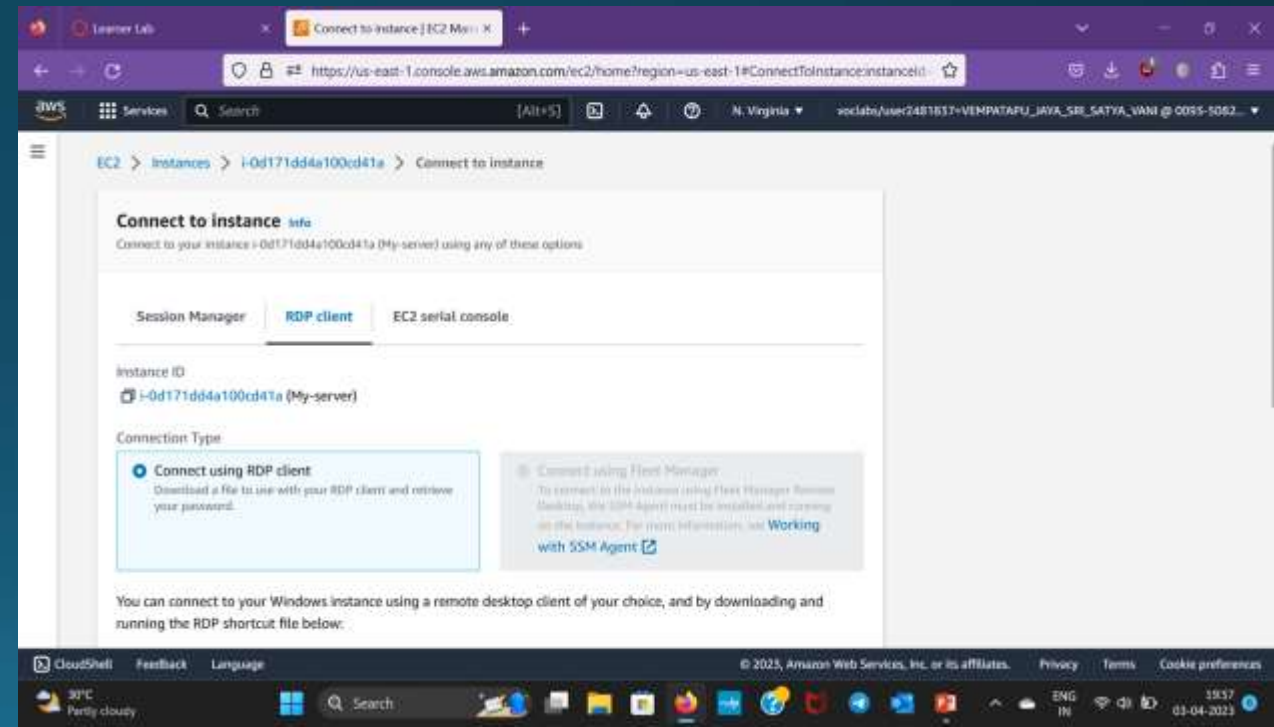
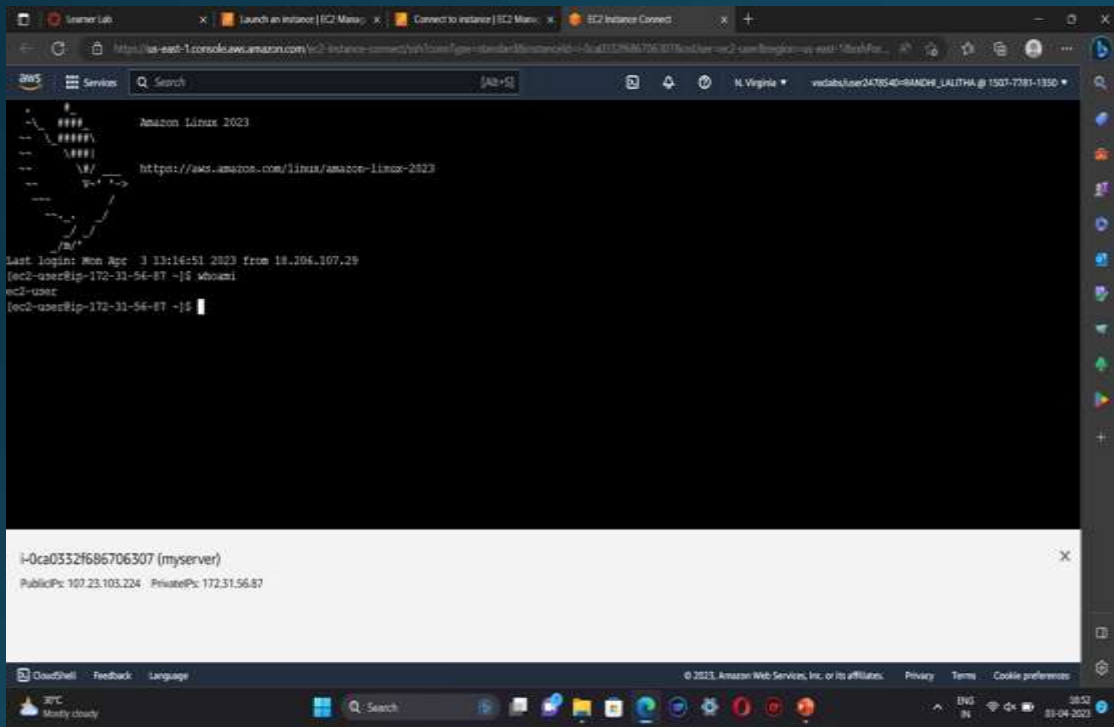
☐ .ppk  
For use with PuTTY

Cancel Create key pair

CloudShell Feedback Language © 2023, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

**Step-5:** For linux-click connect to instance you will be redirected to the CLI (or) open the putty file configure it to not timeout, and configure putty session. This will redirects you to the CLI.

For windows server-click connect→RDP client→ get password→ upload private key→ decrypt password. Open rdp file and enter the password.



**Step 6:** This will redirect you to the windows server.

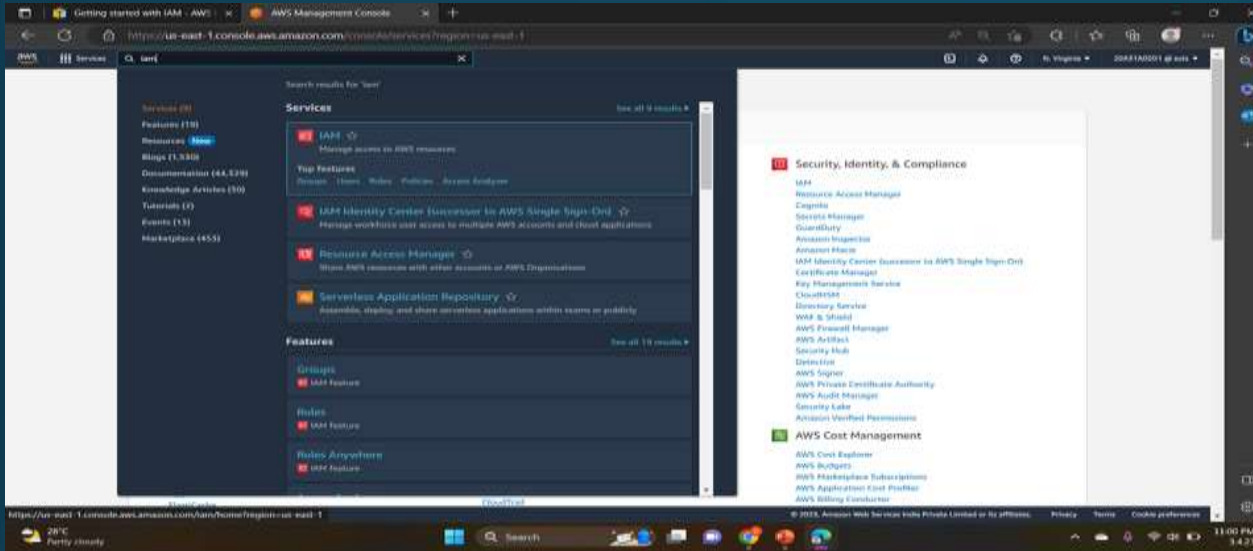
**Step 7:** Terminate the instance



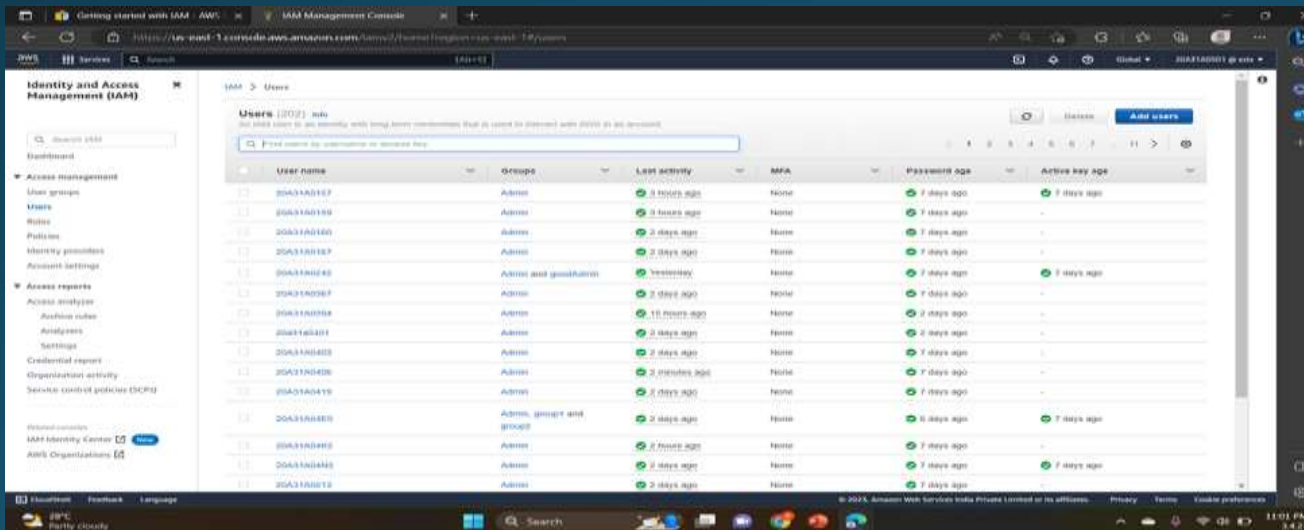
# AWS IDENTITY AND ACCESS MANAGEMENT (IAM)



Step 1 :On the **Console Home** page, select the **IAM** service.



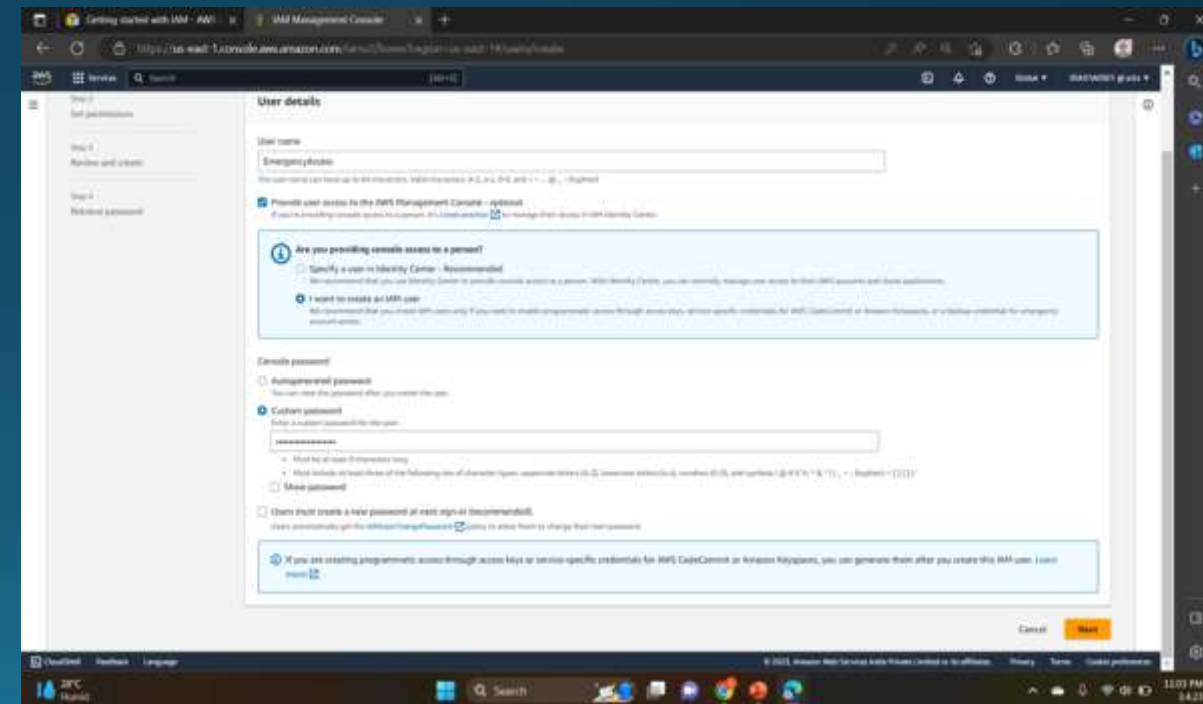
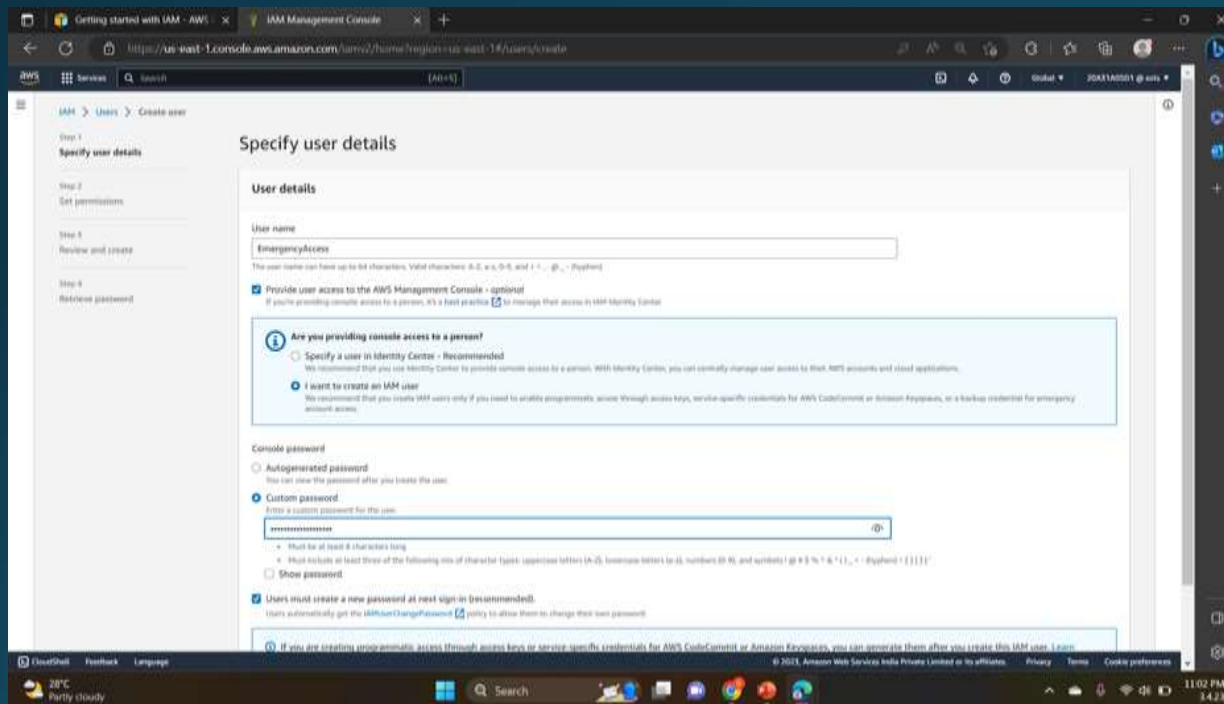
Step 2.In the navigation pane, select **Users** and then select **Add users**.



Step 3: For Username, enter EmergencyAccess and ,Select the check box next to **Provide user access to the AWS Management Console– optional**and then choose **I want to create an IAM user.**

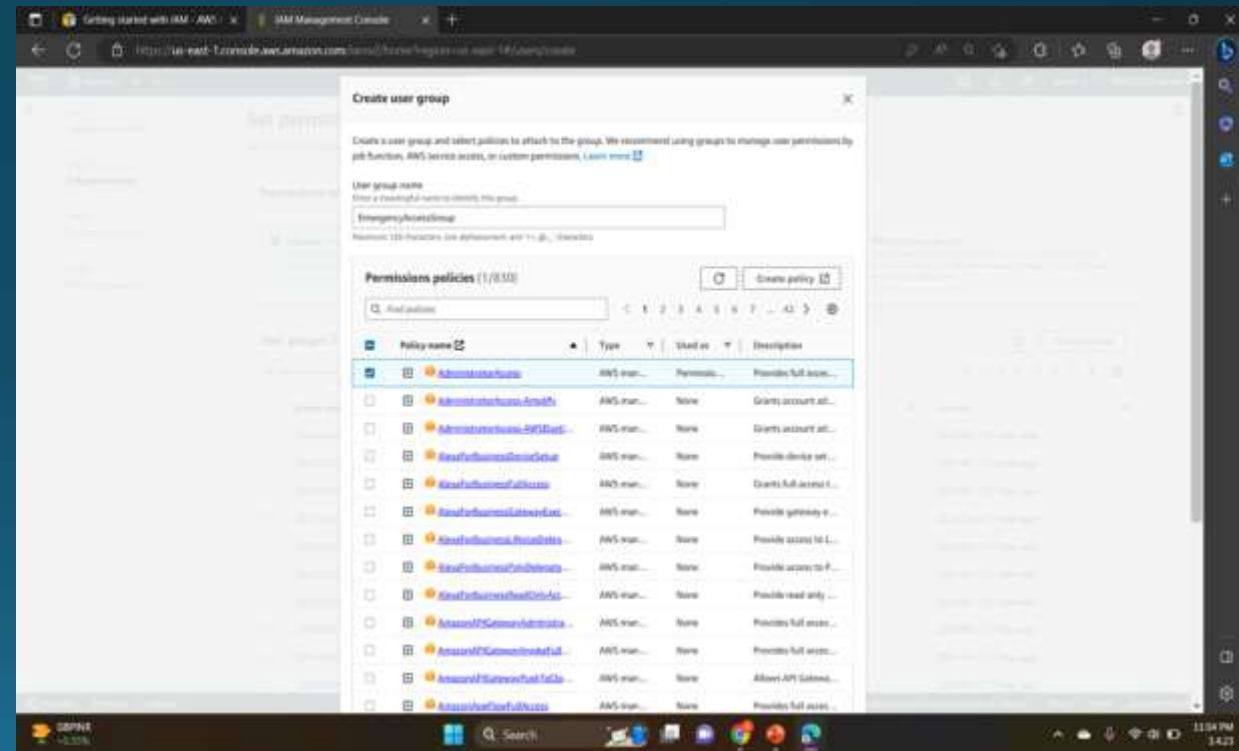
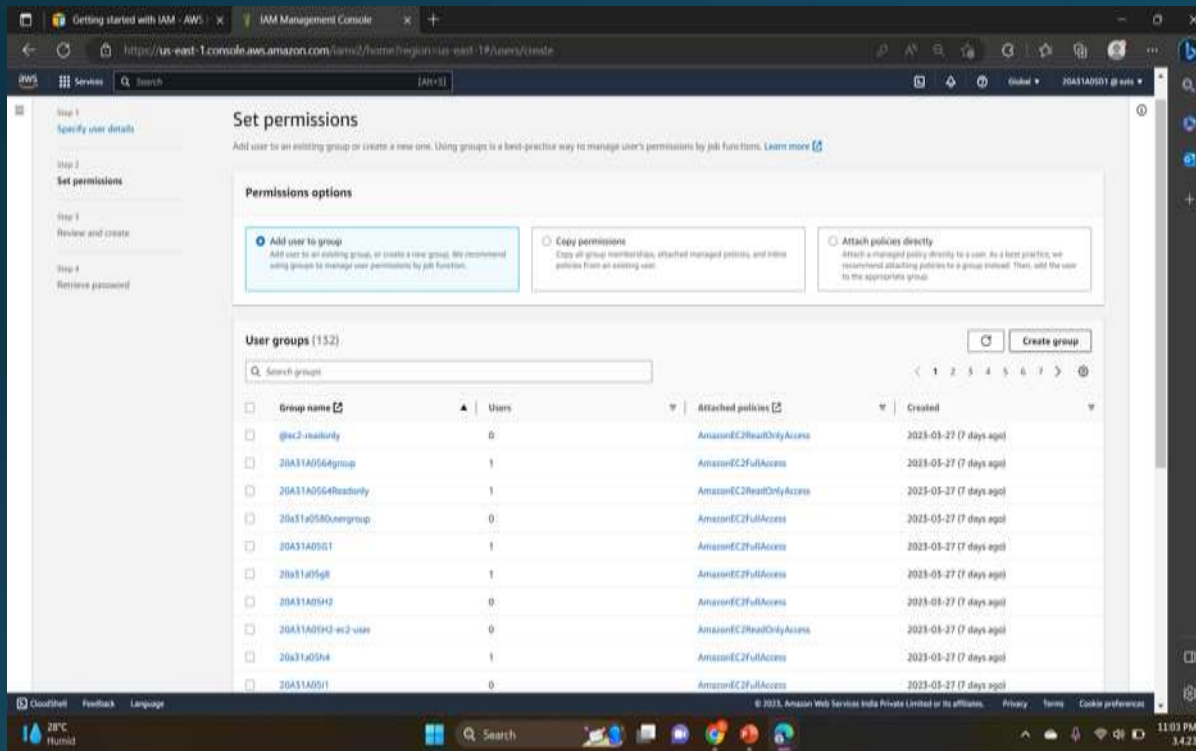
Step 4. Under **Console password**, select **Custom Password** and create your own password.

Step 5. Clear the check box next to **User must create a new password at next sign-in (recommended).** Then click on **Next.**



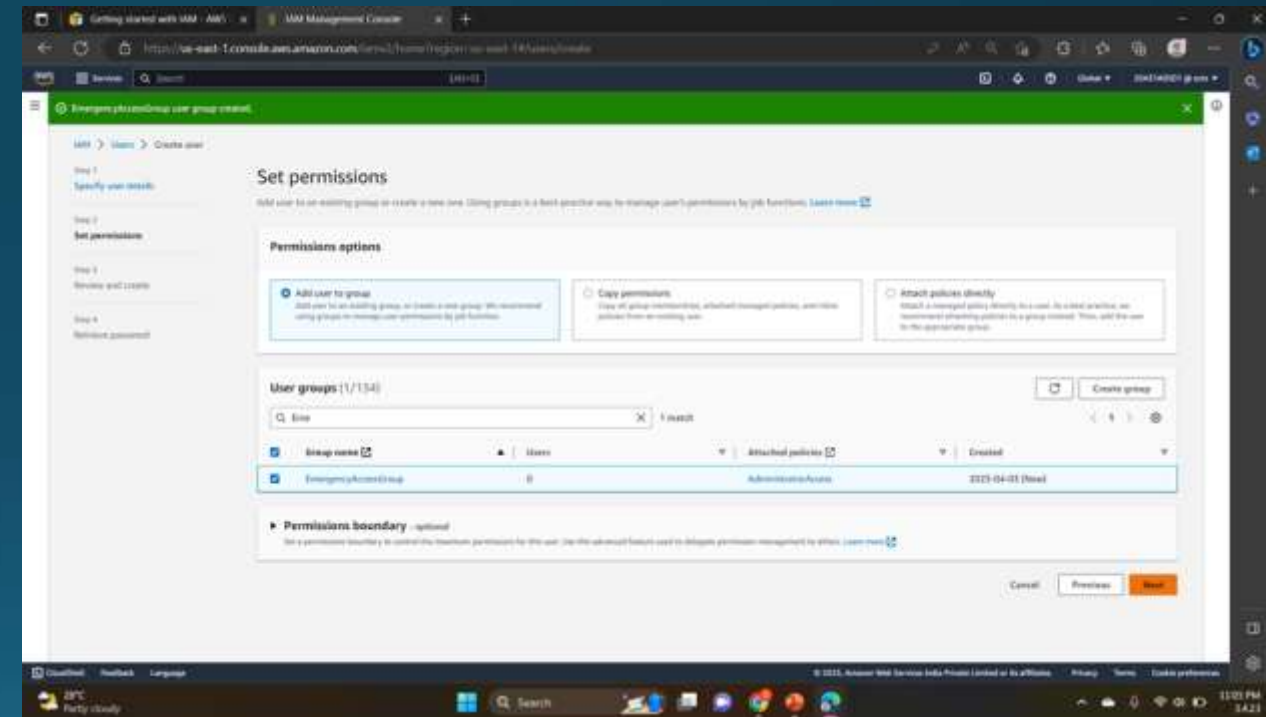
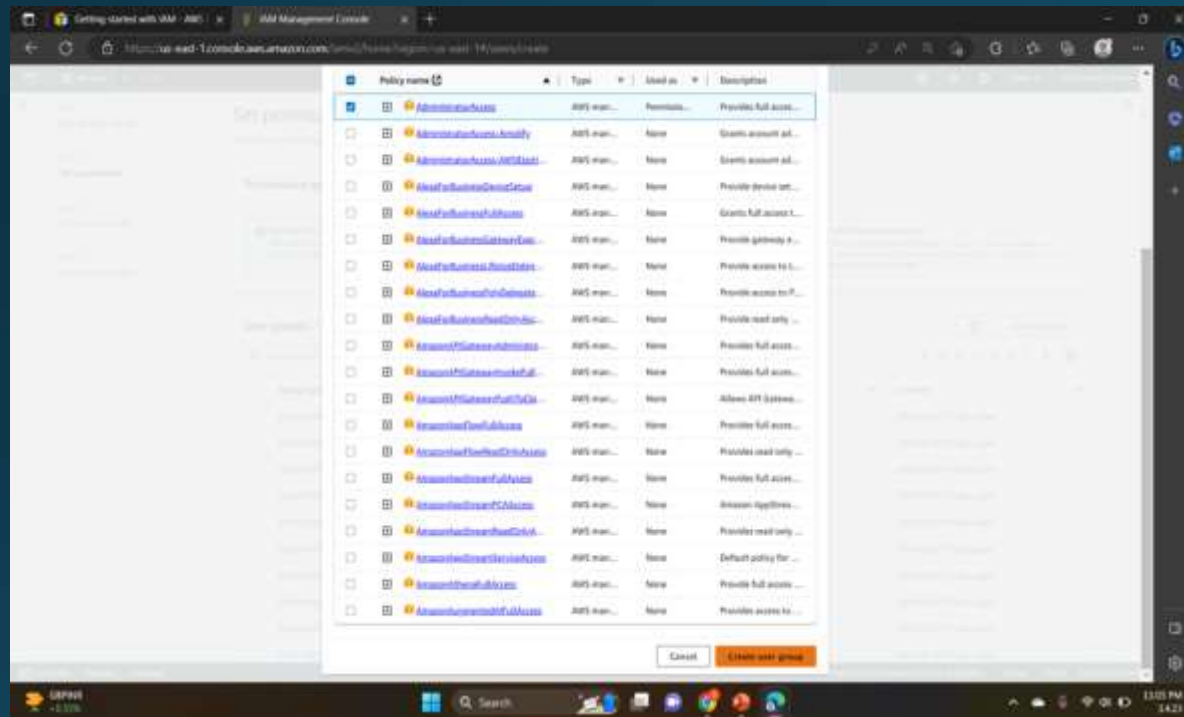
**Step 6. On the Set permissions page, under Permissions options, select Add user to group. Then, under User groups, select Create group.**

**Step 7. On the Create user group page, in User group name, enter EmergencyAccessGroup. Then, under Permissions policies, select AdministratorAccess.**



**Step 9. Select **Next** to proceed to the Review and create page.**

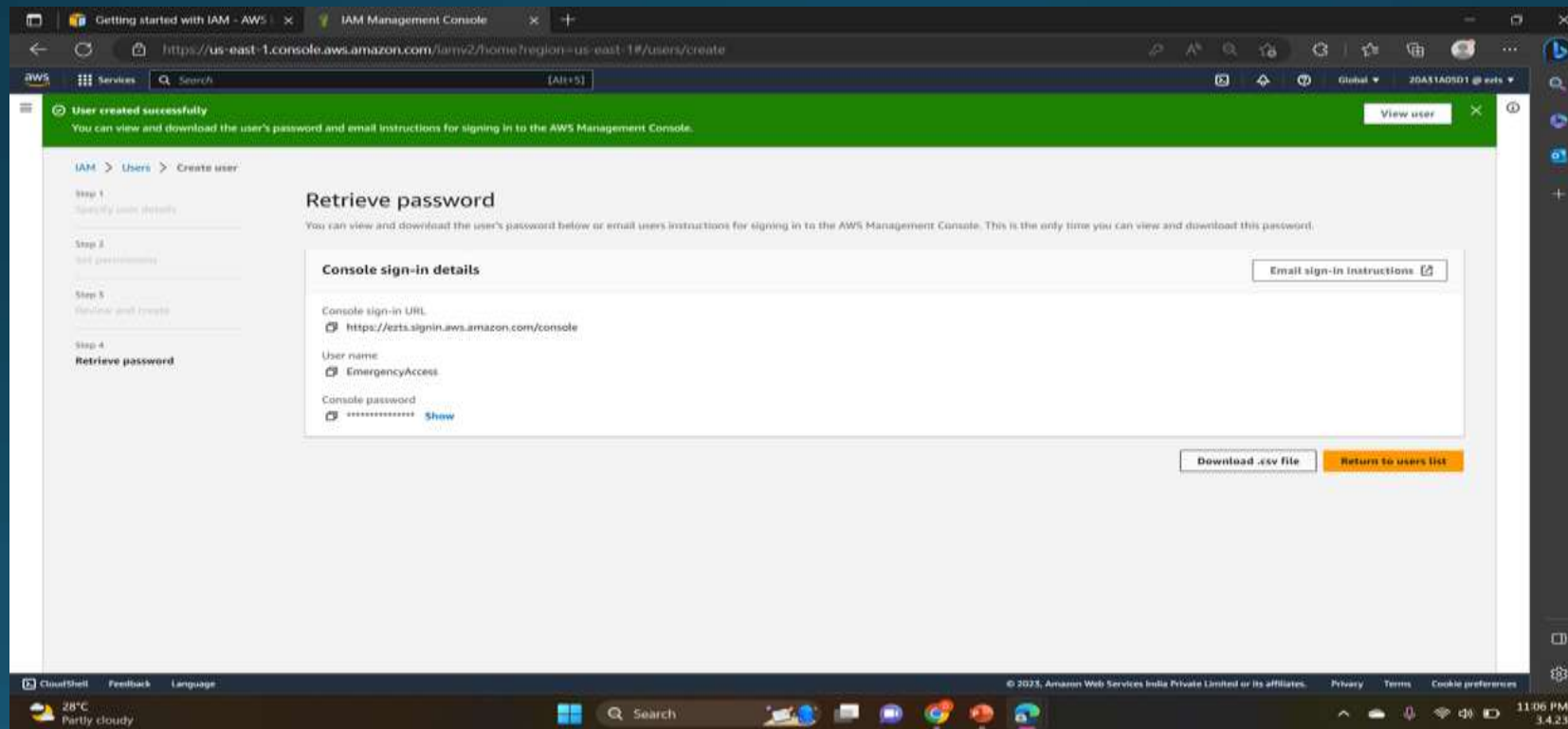
**Step 9. Select **Next** to proceed to the Review and create page.**



**Step 10:** On the **Review and create** page, review the list of user group memberships to be added to the new user. When you are ready to proceed, select **Create user**.

**Step 11:** On the **Retrieve password** page, select **Download .csv file** to save a .csv file with the user credential information (Connection URL, user name, and password).

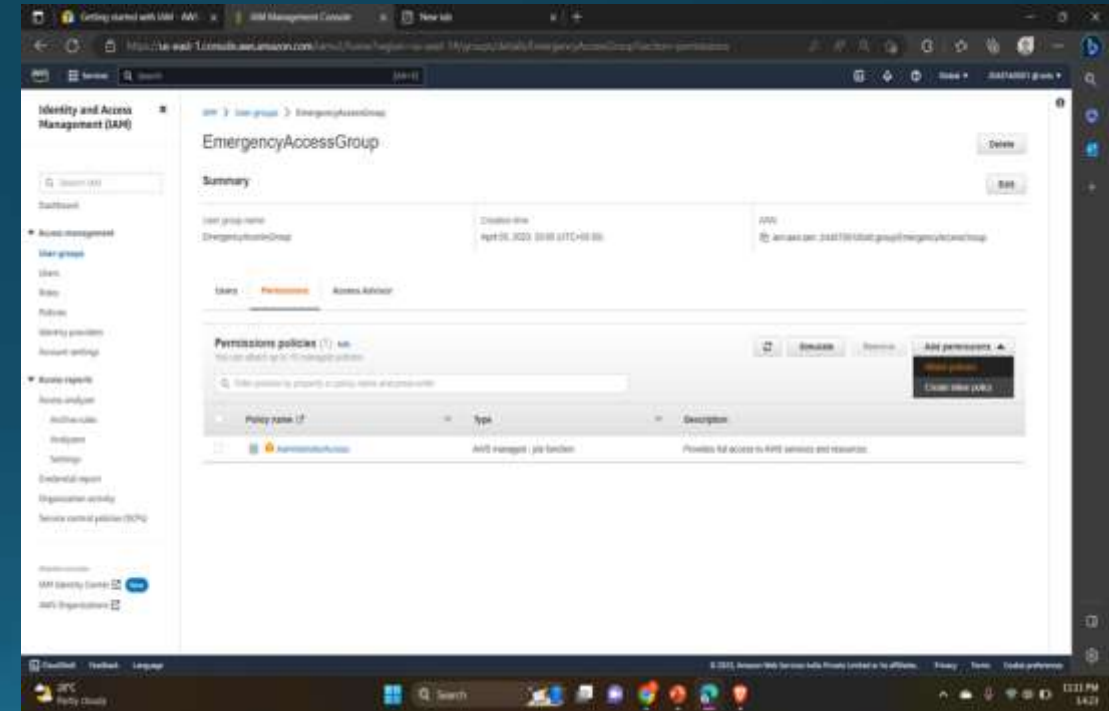
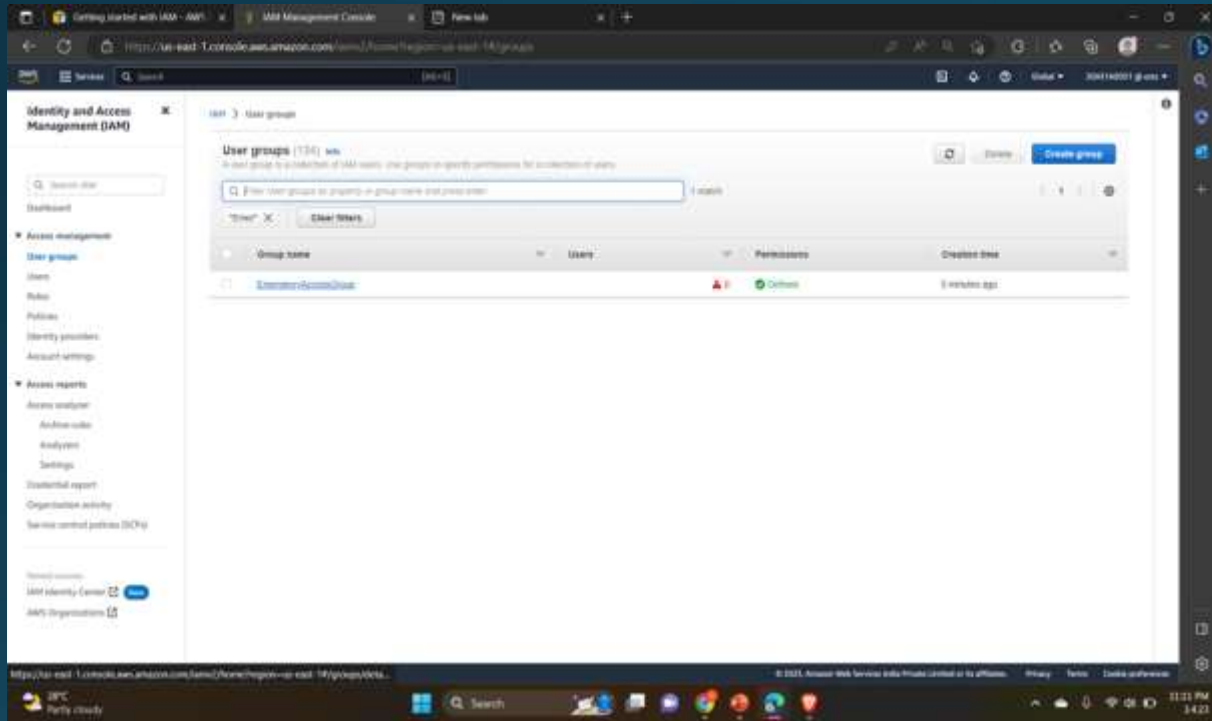
**Step 12:** Save this file to use if you need to sign-in to IAM and do not have access to your federated identity provider.



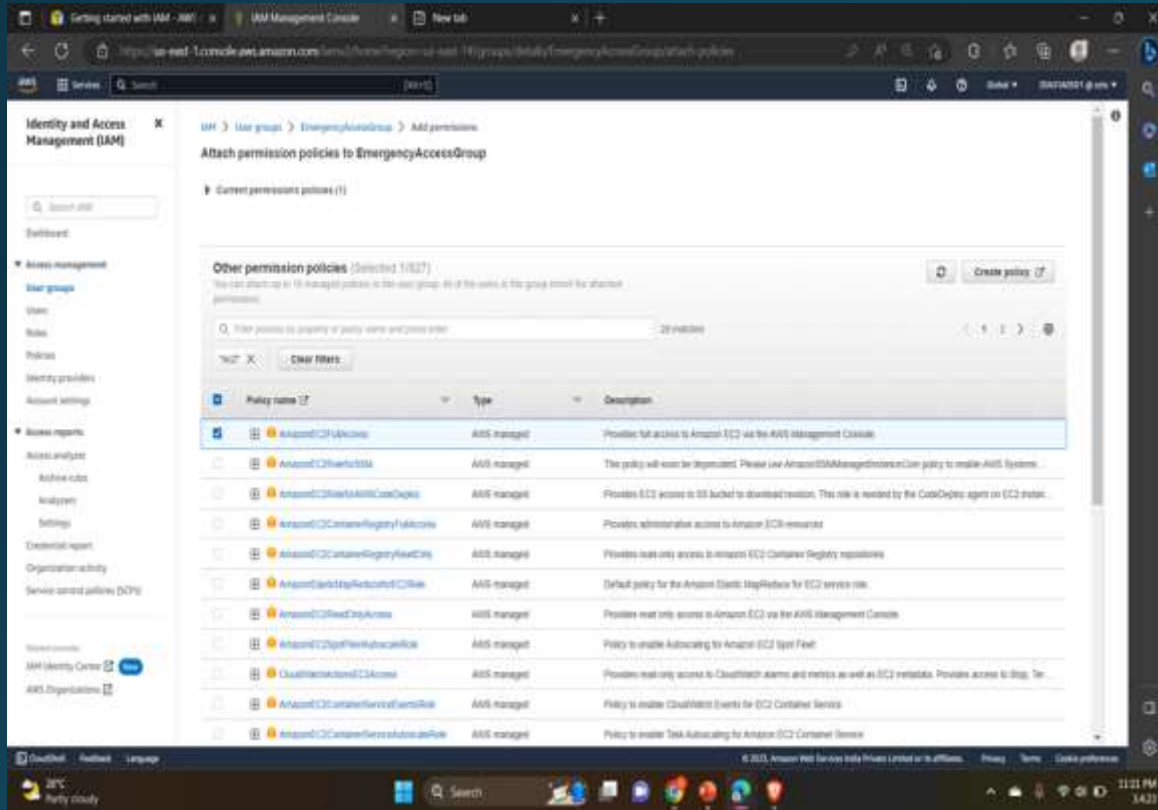


**Step 13:** If you want to add permissions to the user group, then go to **User groups** and click on the respective **User group**.

**Step 14:** Go to **Permissions** → **All permissions** → **Attach policies**

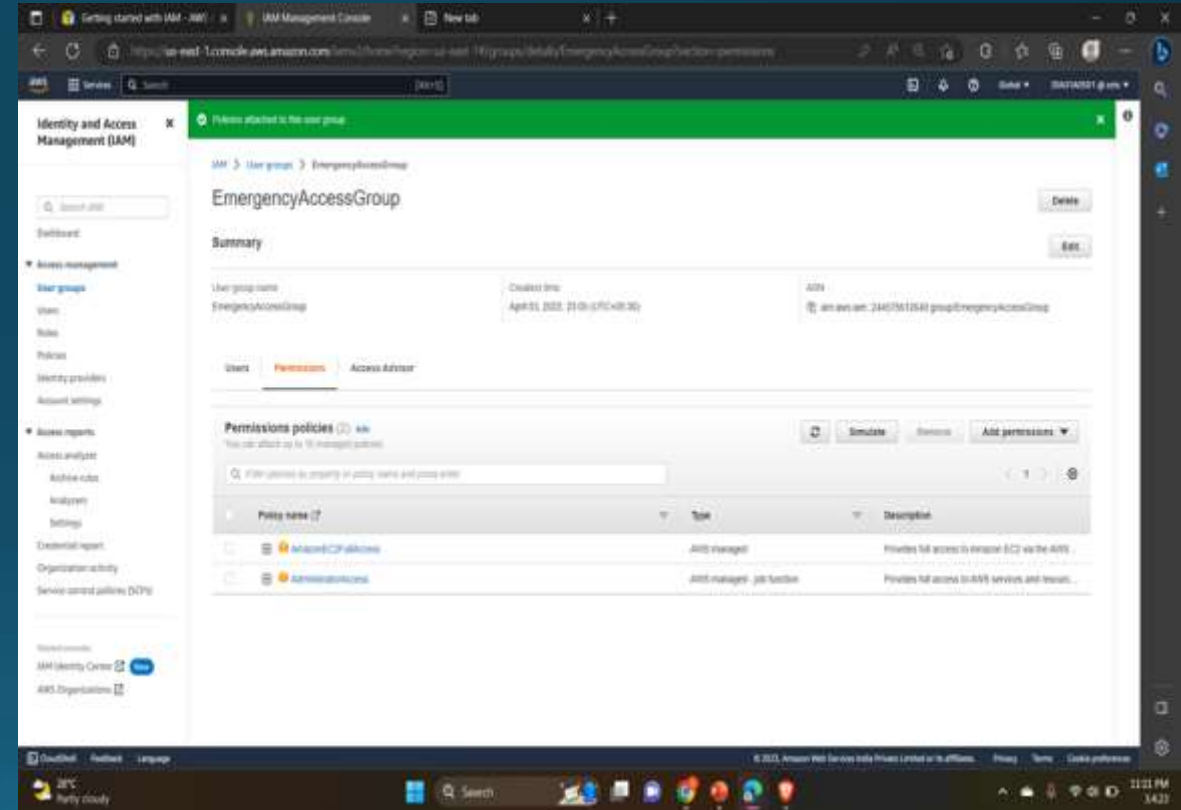


## Step 15. Add the permission policy and the policy is attached to the User group.



The screenshot shows the AWS IAM console interface. The breadcrumb navigation is 'IAM > User groups > EmergencyAccessGroup > Add permissions'. The main heading is 'Attach permission policies to EmergencyAccessGroup'. Below this, it says 'Current permission policies (1)'. A section titled 'Other permission policies (Selected: 1/18)' contains a list of policies. The first policy, 'AmazonEC2FullAccess', is selected and highlighted in blue. The table lists the following policies:

Policy name	Type	Description
AmazonEC2FullAccess	AWS managed	Provides full access to Amazon EC2 via the AWS Management Console.
AmazonEC2ReadOnlyAccess	AWS managed	This policy will soon be deprecated. Please use AmazonEC2ReadOnlyAccess policy to replace AWS Systems...
AmazonEC2ReadOnlyAccess	AWS managed	Provides EC2 access to S3 bucket to download images. This role is needed by the CodeDeploy agent on EC2 inst...
AmazonEC2ContainerRegistryFullAccess	AWS managed	Provides administration access to Amazon ECR resources.
AmazonEC2ContainerRegistryReadOnly	AWS managed	Provides read-only access to Amazon ECR Container Registry repositories.
AmazonElasticMapReduceReadOnlyAccess	AWS managed	Default policy for the Amazon Elastic MapReduce for EC2 service role.
AmazonElasticMapReduceReadOnlyAccess	AWS managed	Provides read-only access to Amazon EC2 via the AWS Management Console.
AmazonEC2SpotFleetAccess	AWS managed	Policy to enable AutoScaling for Amazon EC2 Spot Fleet.
CloudWatchReadOnlyAccess	AWS managed	Provides read-only access to CloudWatch alarms and metrics as well as EC2 metadata. Provides access to logs, Te...
AmazonEC2ContainerServiceReadOnlyRole	AWS managed	Policy to enable CloudWatch Events for EC2 Container Service.
AmazonEC2ContainerServiceReadOnlyRole	AWS managed	Policy to enable Task AutoScaling for Amazon EC2 Container Service.



The screenshot shows the AWS IAM console interface. The breadcrumb navigation is 'IAM > User groups > EmergencyAccessGroup'. The main heading is 'Permissions attached to the user group'. Below this, it says 'Permissions policies (2)'. A section titled 'Permissions policies (2)' contains a list of policies. The first policy, 'AmazonEC2FullAccess', is selected and highlighted in blue. The table lists the following policies:

Policy name	Type	Description
AmazonEC2FullAccess	AWS managed	Provides full access to Amazon EC2 via the AWS...
AmazonEC2ReadOnlyAccess	AWS managed	Provides full access to AWS services and resour...

# AMAZON VPC



Step 1: First start the lab, when the lab status gets ready, it redirects to the AWS management console.

Step 2: Go to AWS services, search, and choose VPC to open the VPC console.

Step 3: Verify that your regions remain in the N-Virginia(us-east-1). Choose to create VPC in the VPC dashboard

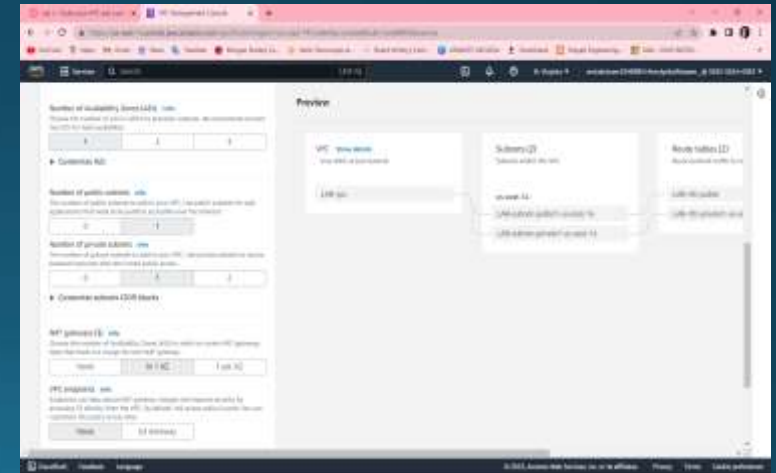
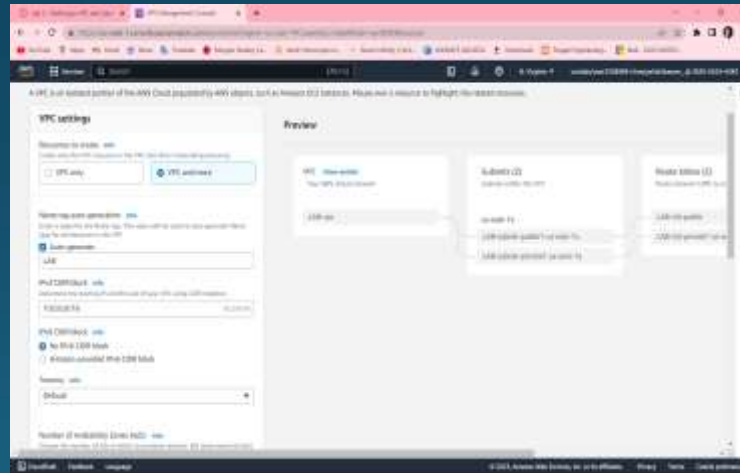
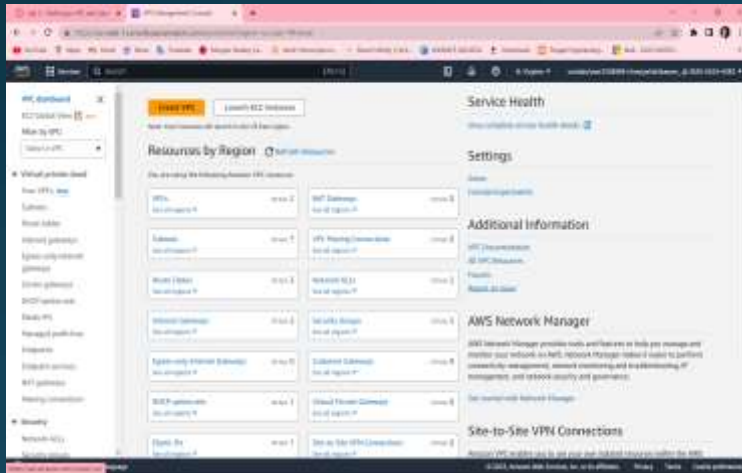
Step 4: Choose VPC and more, in name tag auto-generation, keep auto-generate select and change it to a lab.

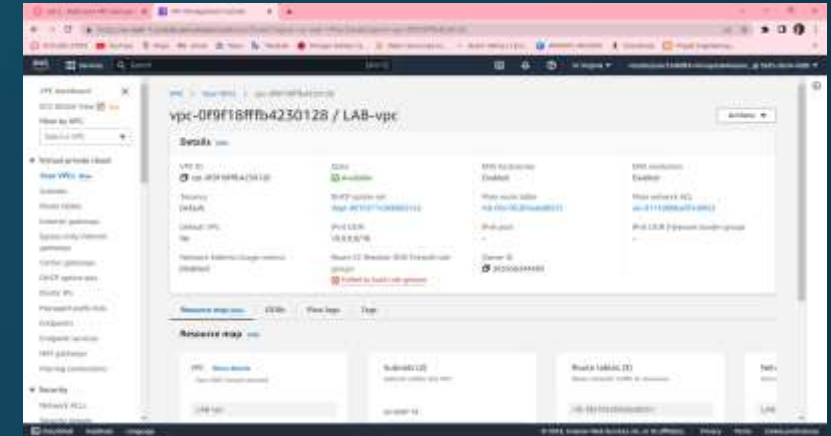
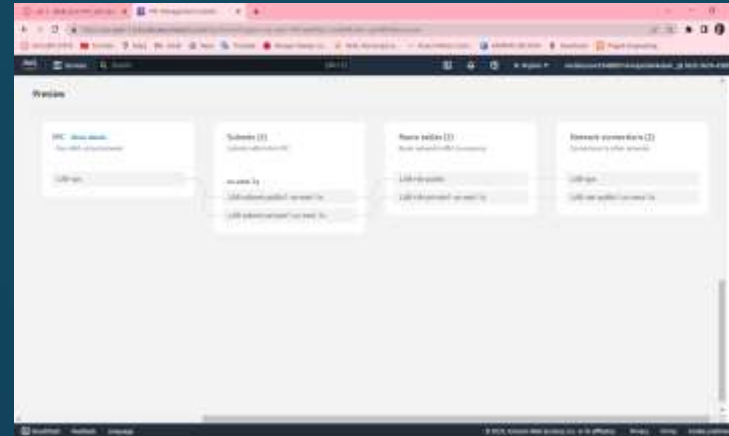
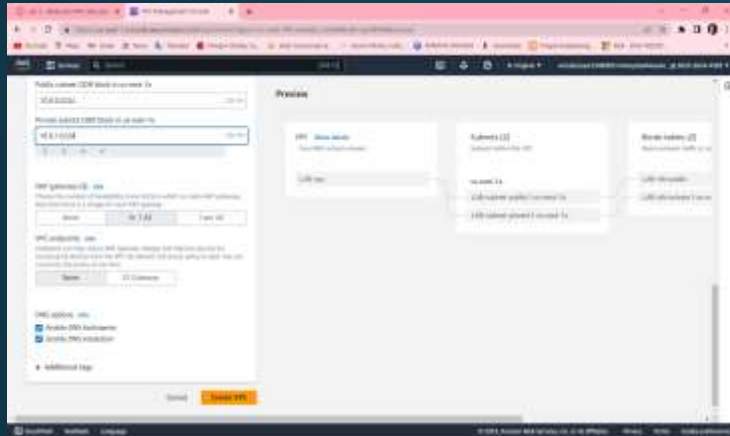
Step 5: Keep the IPv4 CIDR block to 10.10.0.0/16 and next for a number of availability zones select 1, number of public subnets select 1 , number of private subnets select 1

Step 6: Now customize subnets CIDR blocks, change public subnet(us-east-1a) to 10.10.0.0/24, and change private subnet (us-east-1a) to 10.0.1.0/24

Step 7: Set the NAT gateways to 1AZ and set VPC endpoints to none and keep both DNS hostnames and DNS resolutions enabled

Step 8: Check on the preview panel on the right side whether they match with the given regions or not





## CREATING ADDITIONAL SUBNETS :

Step 1: Choose subnets in the left panel, choose to CREATE SUBNET

Step 2: in this, choose VPC ID: LAB-vpc and choose subnet name to lab-subnet-public2, choose availability zone to us-east-1b and choose IPv4 block to 10.0.2.0/24

Step 3: choose to create a subnet and again create the same subnet with lab-subnet-private2, change the IPv4 block to 10.0.2.0/24, and then create a subnet

Step 4: Choose the routing table in the left panel, select lab-rtb-private1-us-east-1a, in the lower panel, choose routes note destination, choose the subnet association tab, in the explicit subnet associations panel choose EDIT SUBNET ASSOCIATIONS

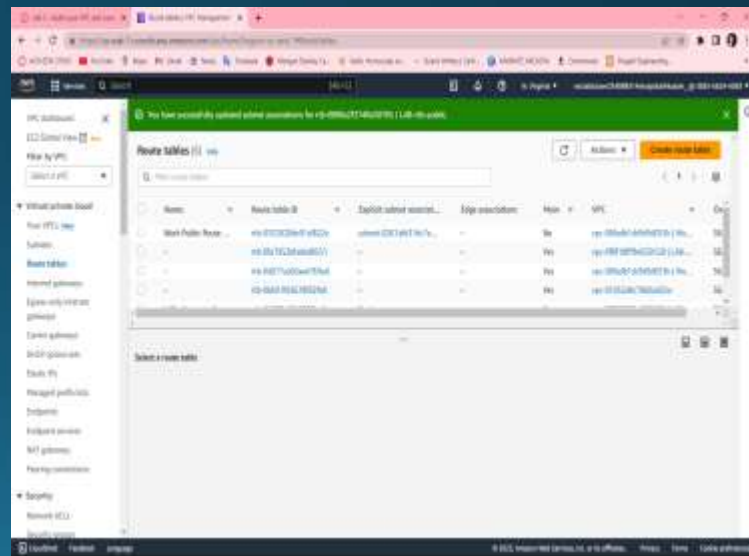
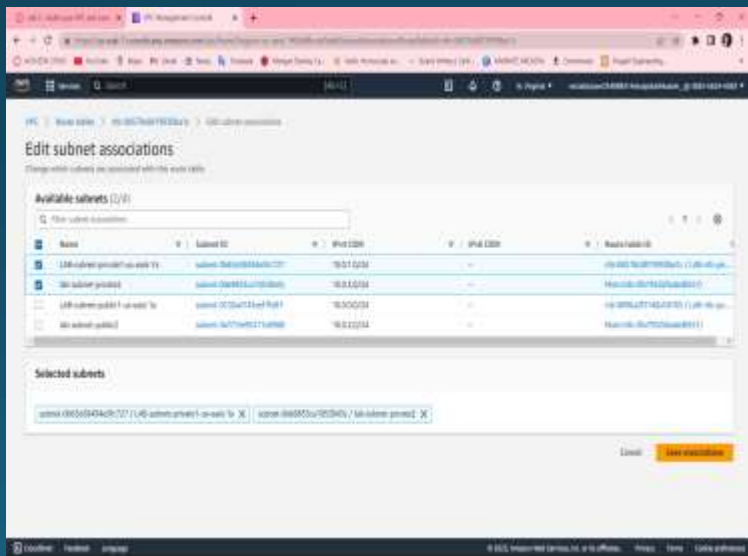
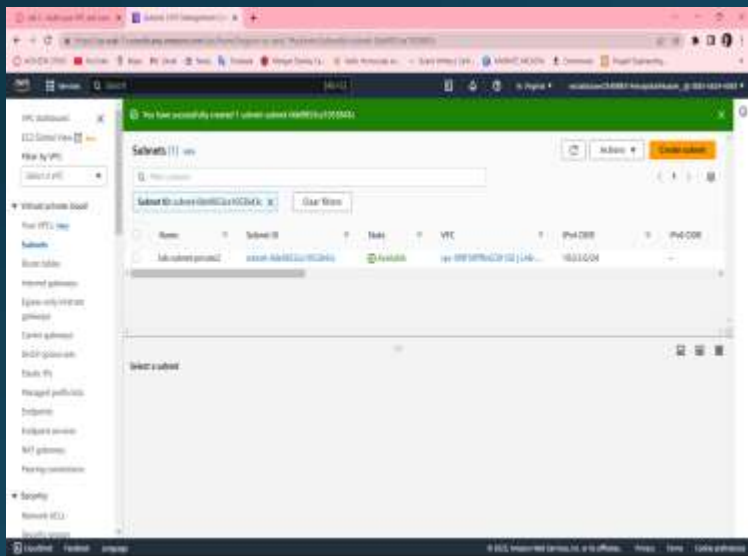
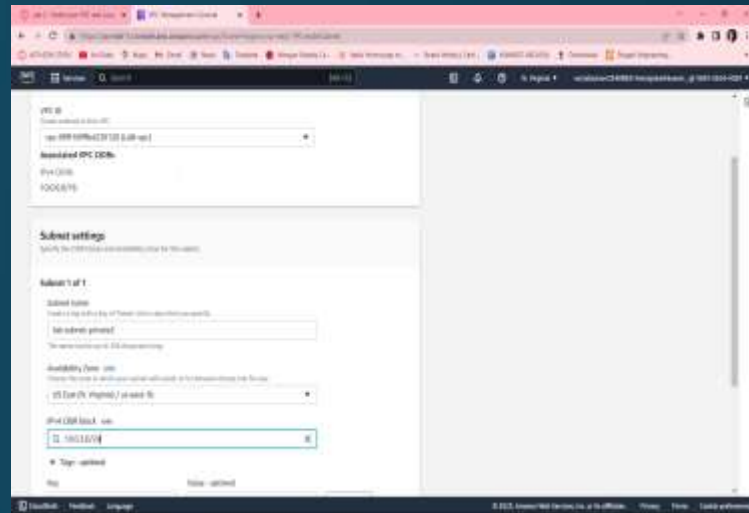
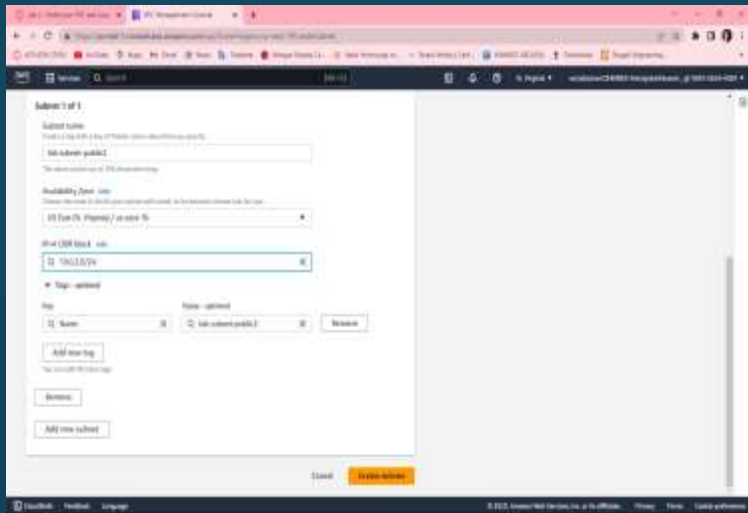
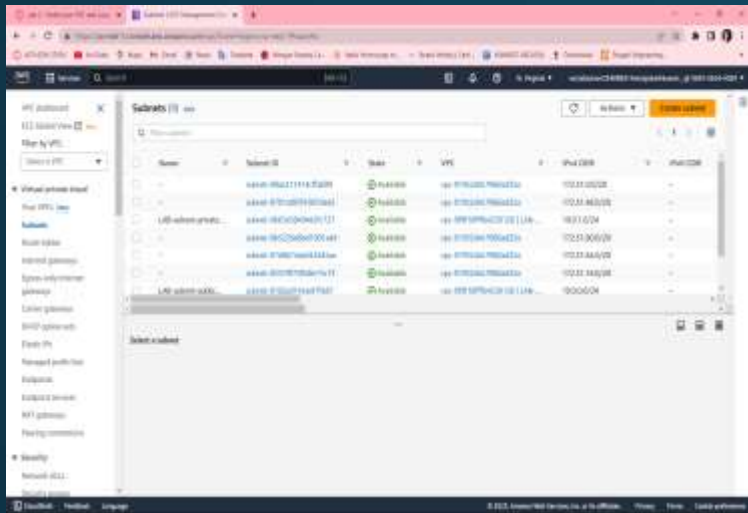
Step 5 : Leave lab-subnet-private1-us-east-1a and also select lab-subnet-private2

Step 6: Choose SAVE ASSOCIATIONS

Step 7: Select lab-rtb-public route table and deselect any other subnet

Step 8: In the lower panel, again repeat from step 4 but here we select lab-subnet-public2 also

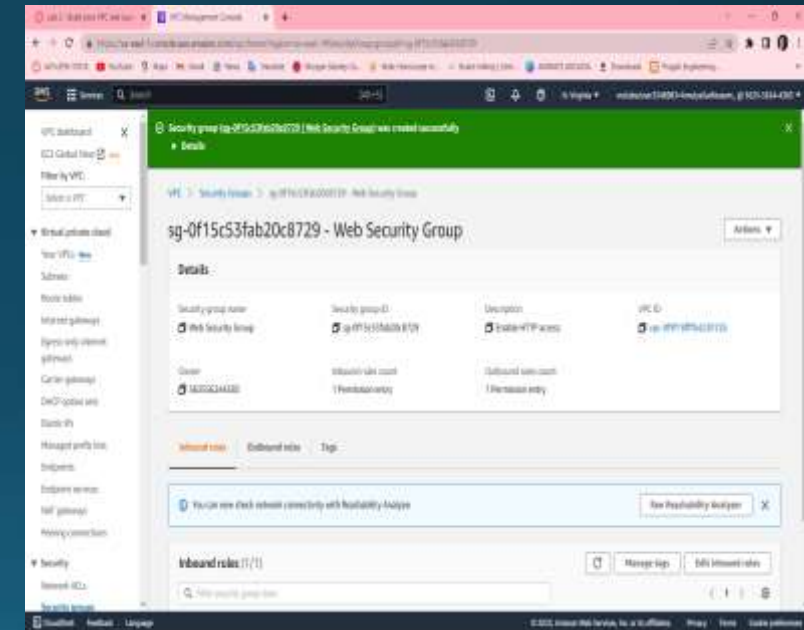
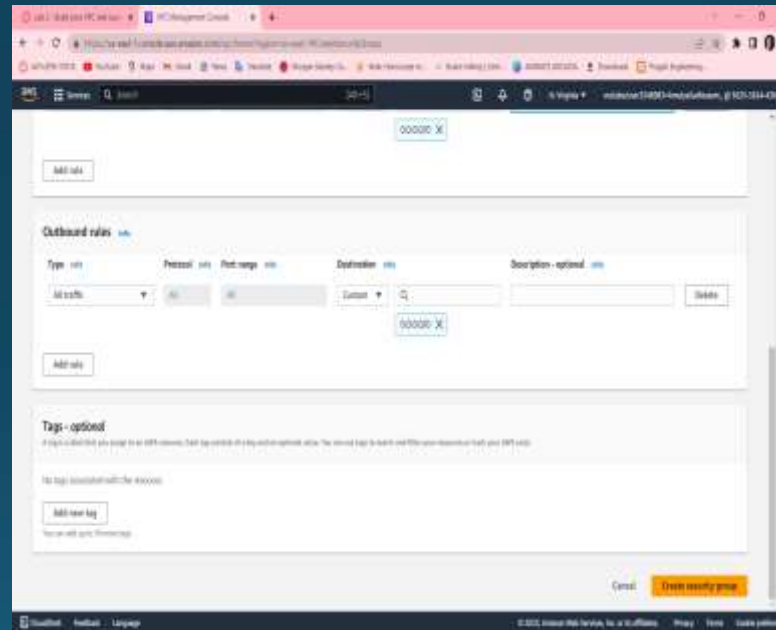
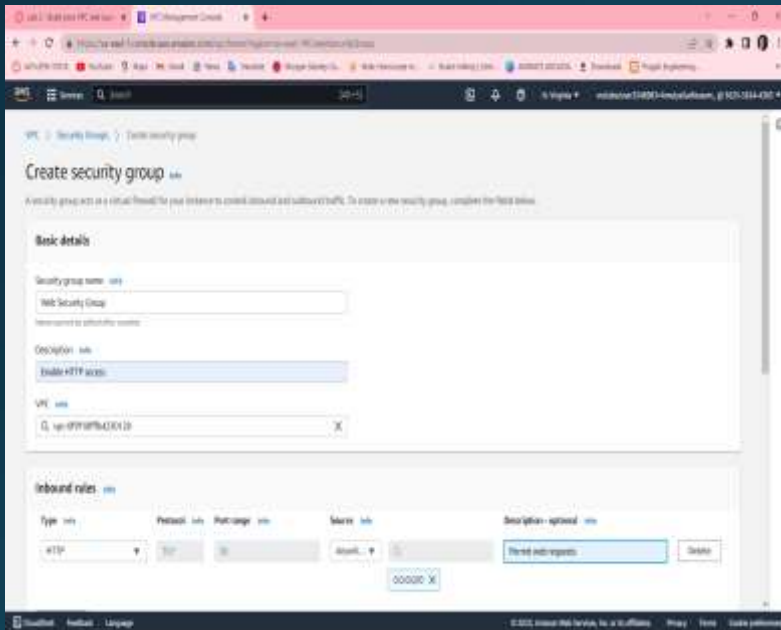
Step 9: Choose SAVE ASSOCIATIONS



# CREATING A VPC SECURITY GROUP

Step 1: Choose to create a security group and in this choose the security group name to a web security group, have a description as enable HTTP access and choose vpc to lab-vpc

Step 2: In inbound rules choose to add rule and then in this chosen type to HTTP, source to Anywhere ipv4 and description to permit web requests



## LAUNCH A WEB SERVER INSTANCE

Step 1 : Choose EC2 to open EC2 console , from instances click launch instance and give name as web server 1

Step 2 : Keep Amazon Linux select and select amazon linux 2023 AMI , Choose t2.micro

Step 3 : Choose key pair name to vockey , in network settings choose edit select network to lab-vpc ,subnet to lab-subnet-public2 and auton assign to enable

Step 4 : Under firewall choose select existing security group , for common security groups select web security group

Step 5 : Expand the advanced details panel , scroll down upto the user data box appear

```
#!/bin/bash
# Install Apache Web Server and PHP
sudo dnf install -y httpd wget php mariadb105-server
# Download Lab files get https://aws-tc-largeobjects.s3.us-west-2.amazonaws.com/CUR-TF-100-ACCLFO-2-9026/2-lab2-vpc/s3/lab-app.zip
unzip lab-app.zip -d /var/www/html/
# Turn on web server
chkconfig httpd on
service httpd start
```

Step 6: At the bottom SUMMARY panel choose launch instance ,click on view instances

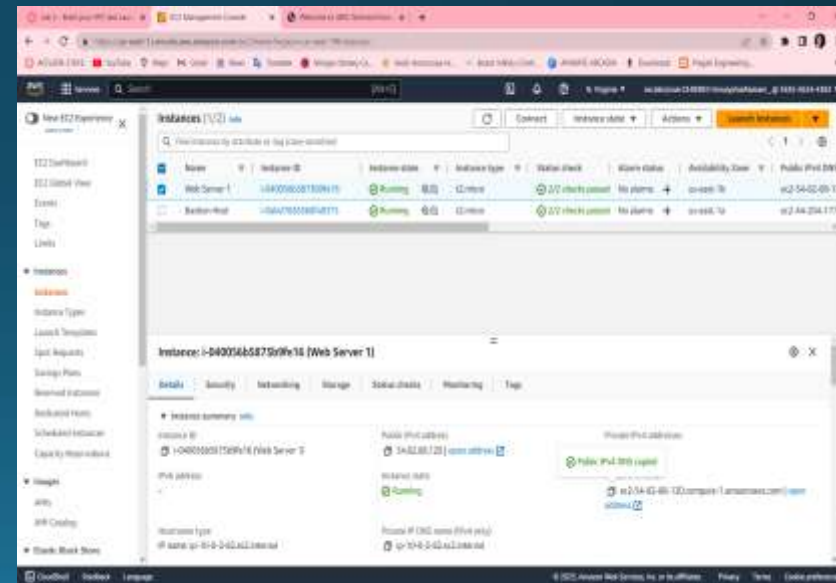
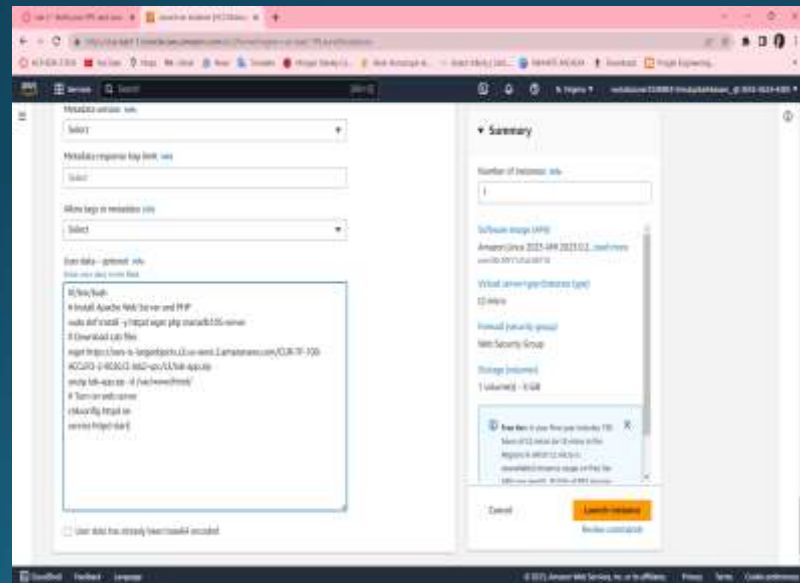
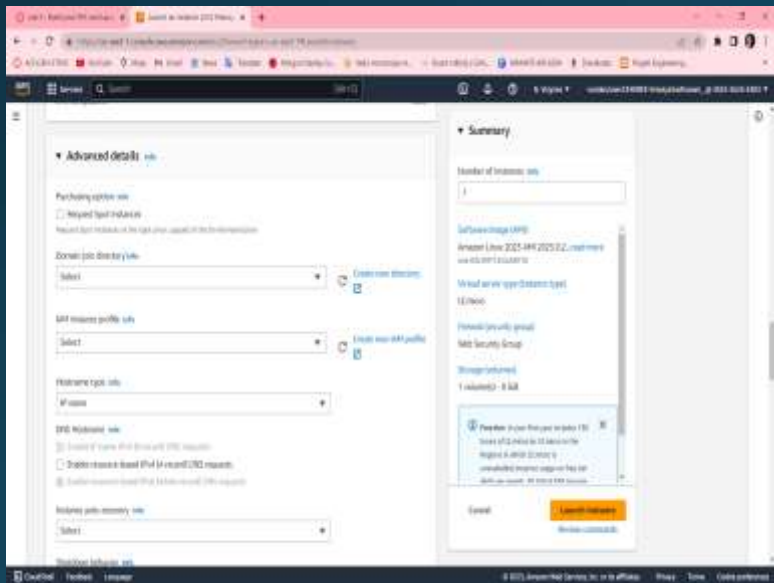
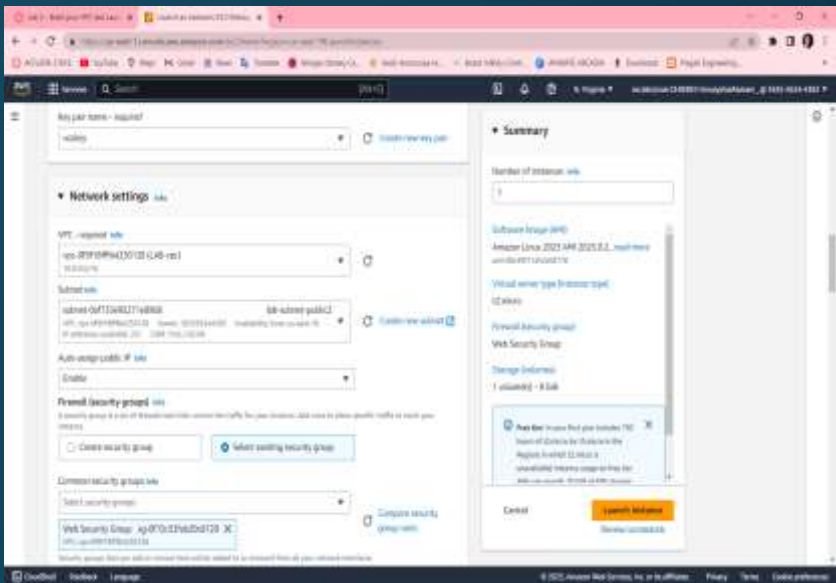
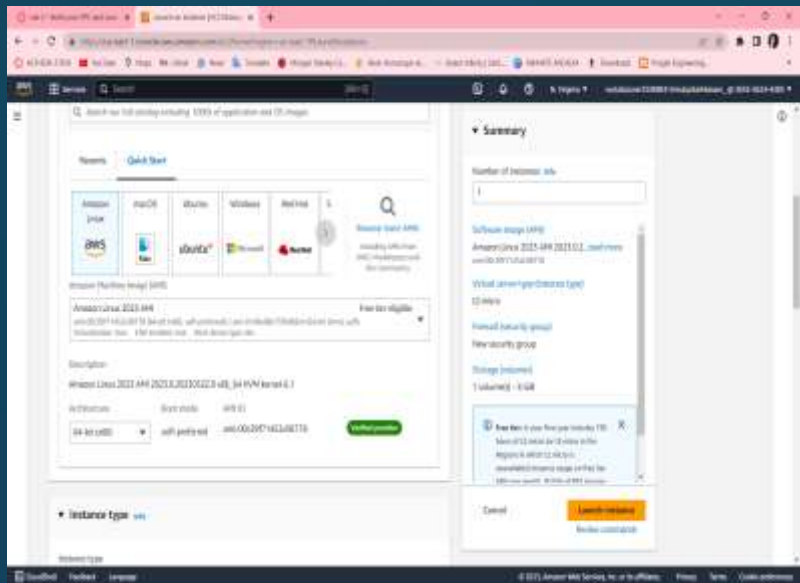
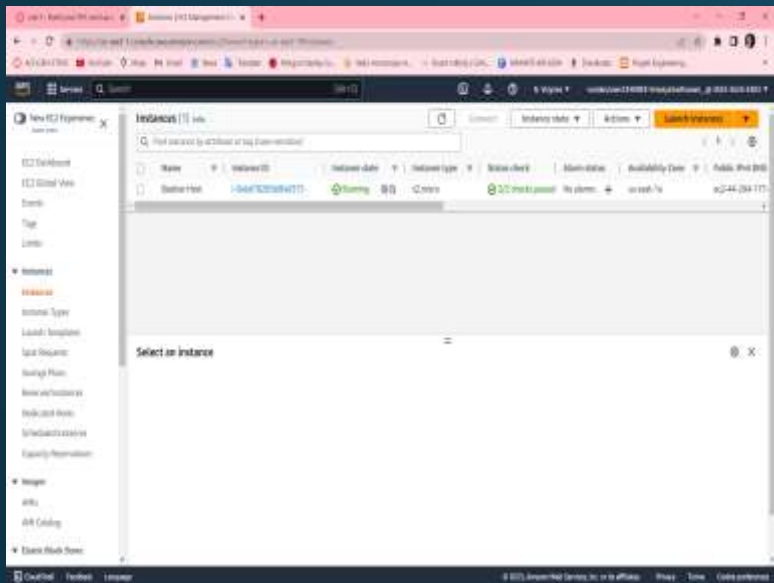
Step 7 : Wait until web server 1 shows 2/2 checks passed

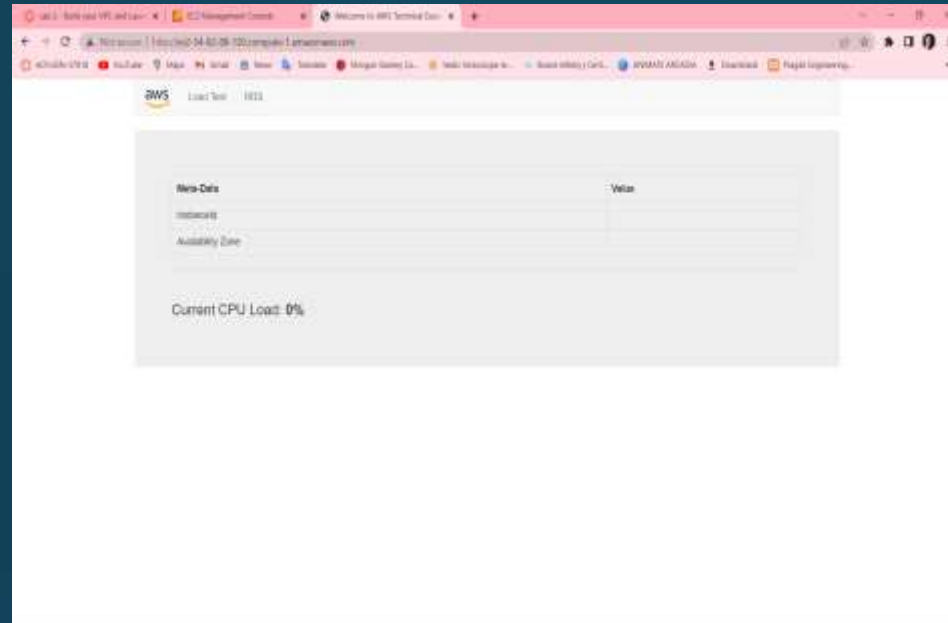
Step 8 : Copy the public ipv4 dns value present in details tab

Step 9 : Open a new browser , copy the public dns

Step 10 : Finally we see a web page displaying AWS logo and instances meta-data values





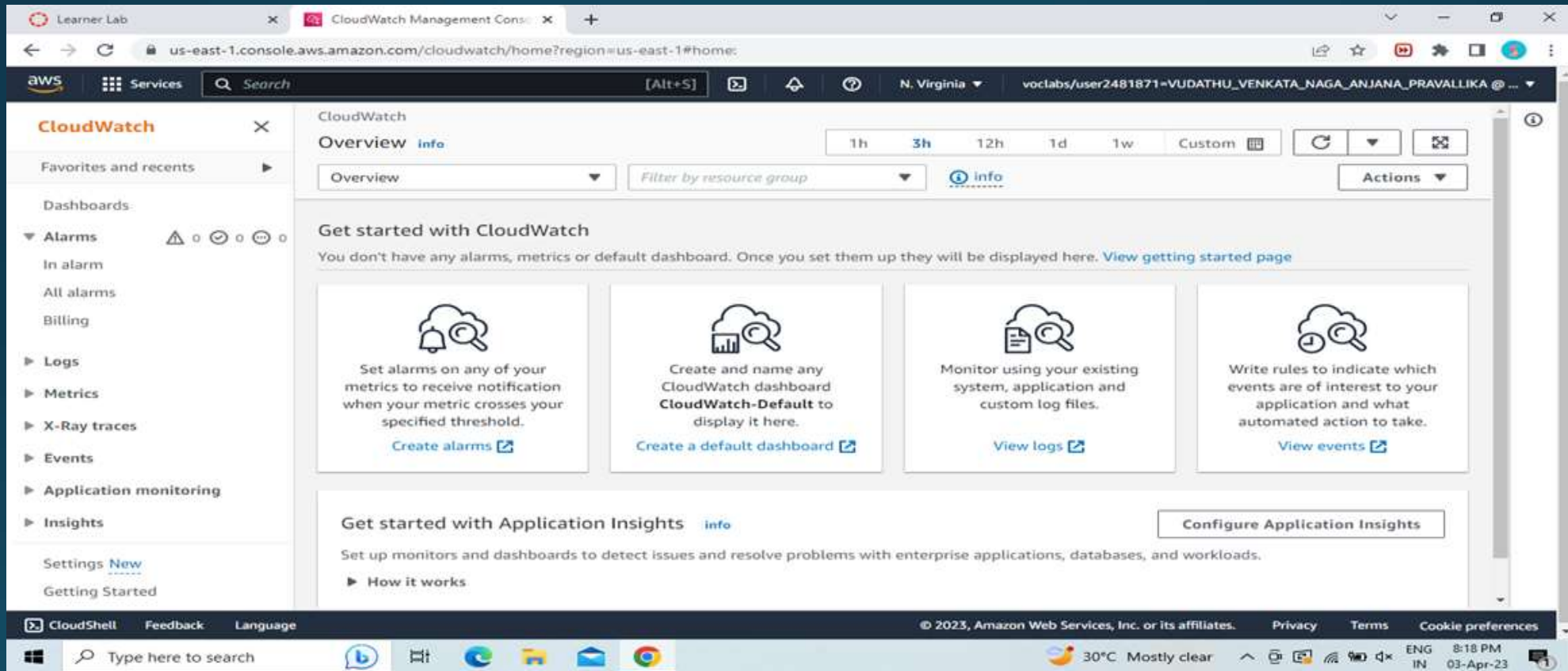


Finally, a web page opens displaying the AWS logo and instances of metadata values

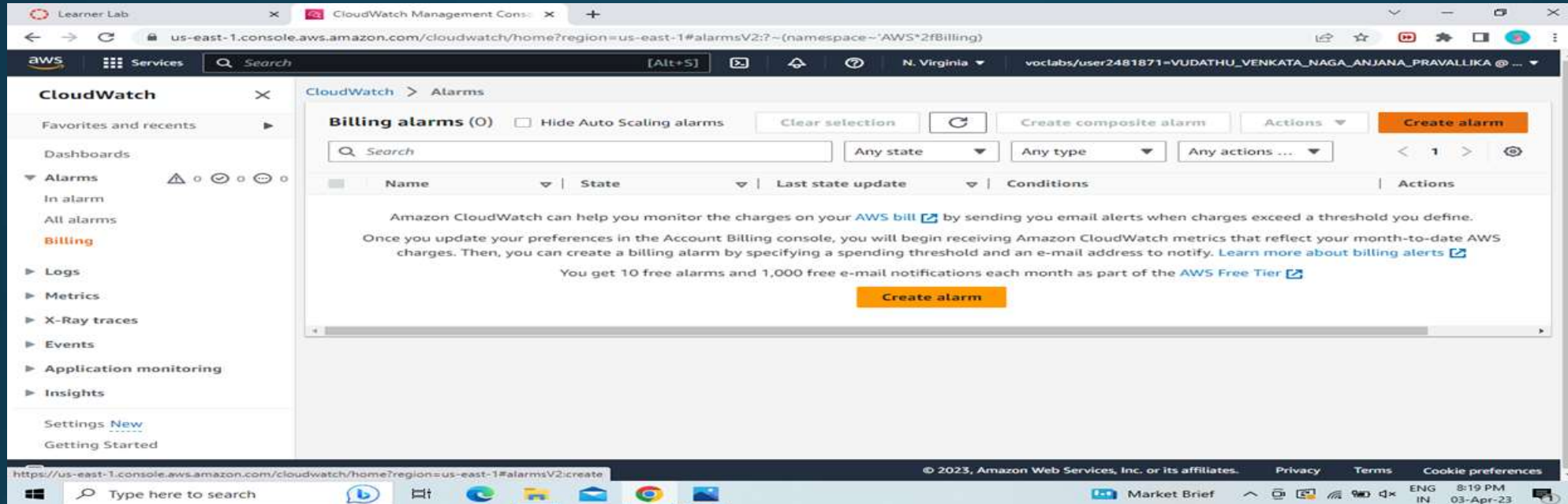
# AWS CLOUD WATCH



Step 1. Go to AWS Services, Click on CloudWatch and then in the Dashboard go to Alarms section and select Billings.



## Step 2: Then Click on CREATE ALARM



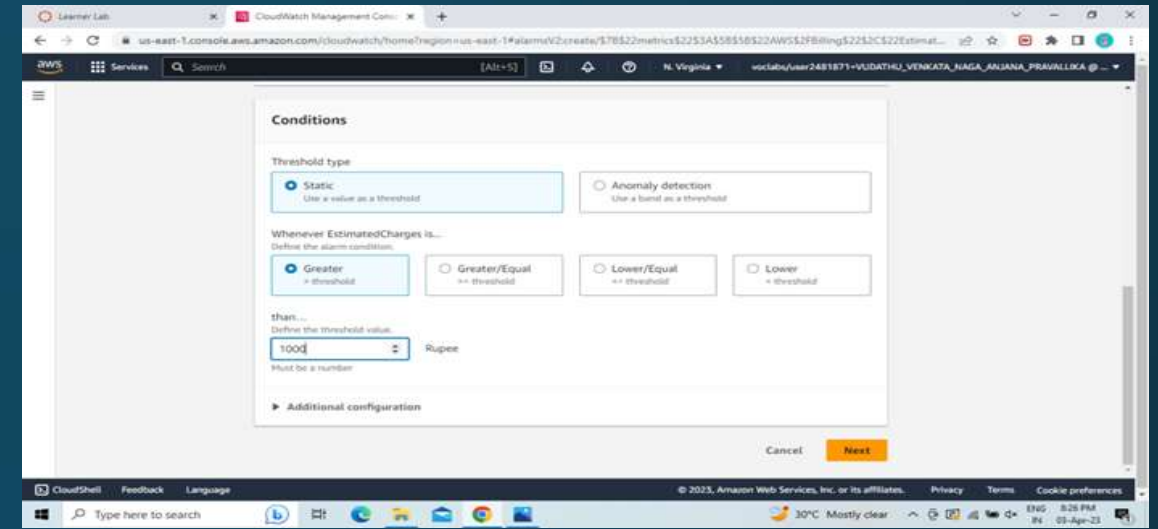
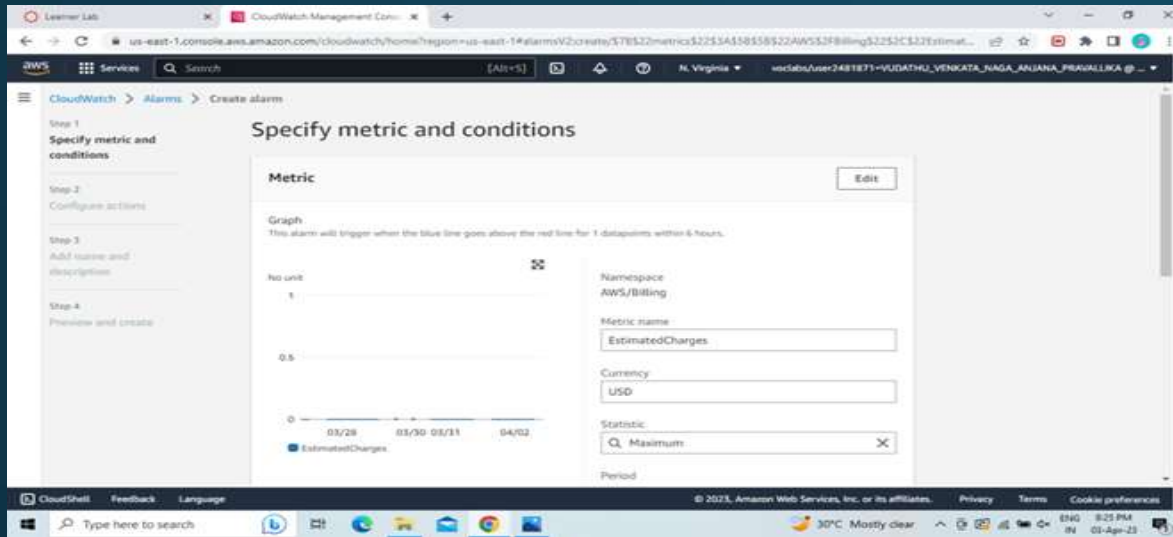
Step 3: Then follow the steps.

In the first step it will ask us to Specify metric and conditions. Click on Select Metric.

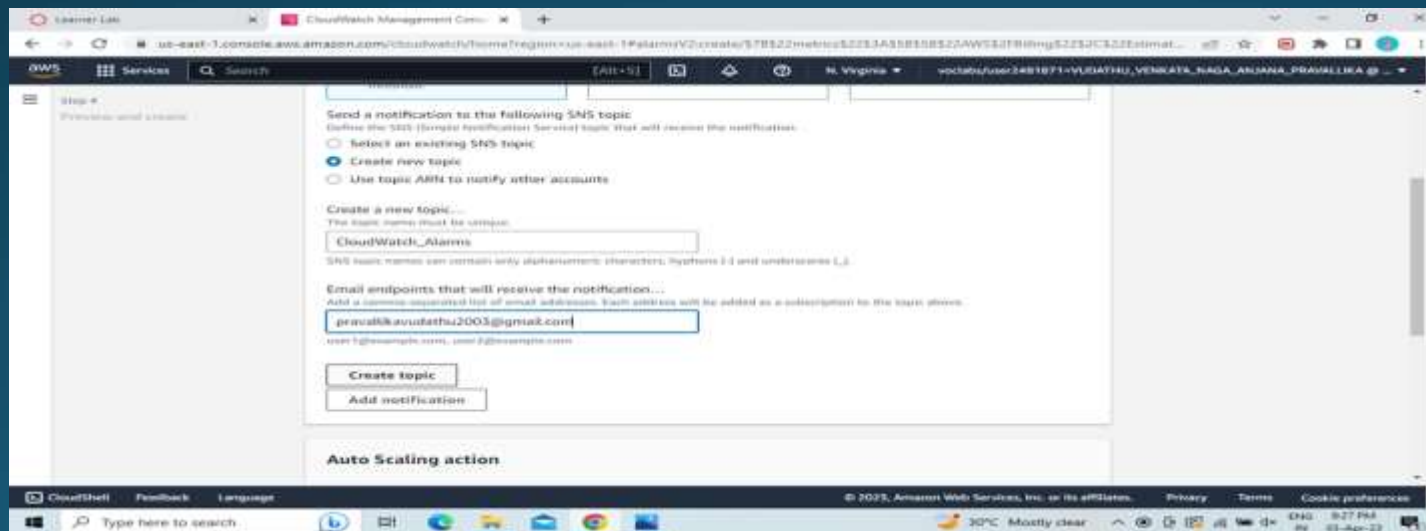
Change the Currency to Rupee.

In the Conditions section choose the EstimatedCharges like Greater/GreaterEqual/Lowerequal/Lower and also define the threshold value.

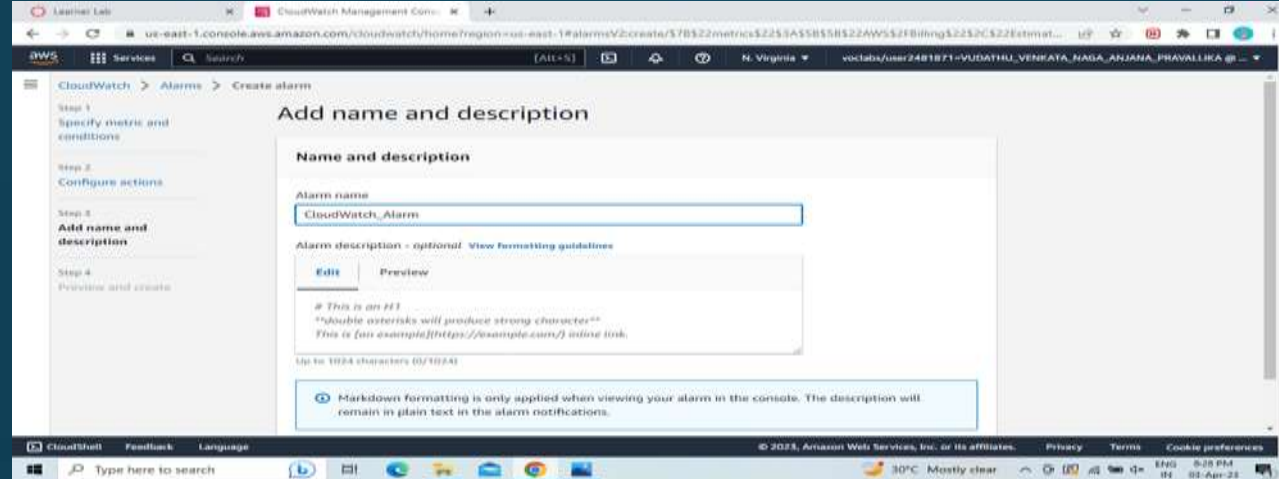
Step 4 : Click on Next.



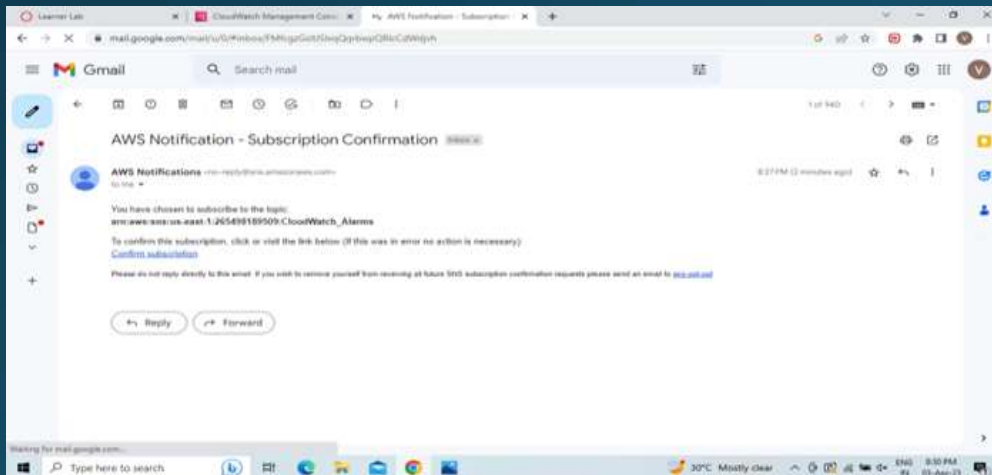
**Step 5 :** Now for Configure Actions choose Create new topic. Give a name to the topic and enter your email to receive a notification. Click on Create Topic, then Next.



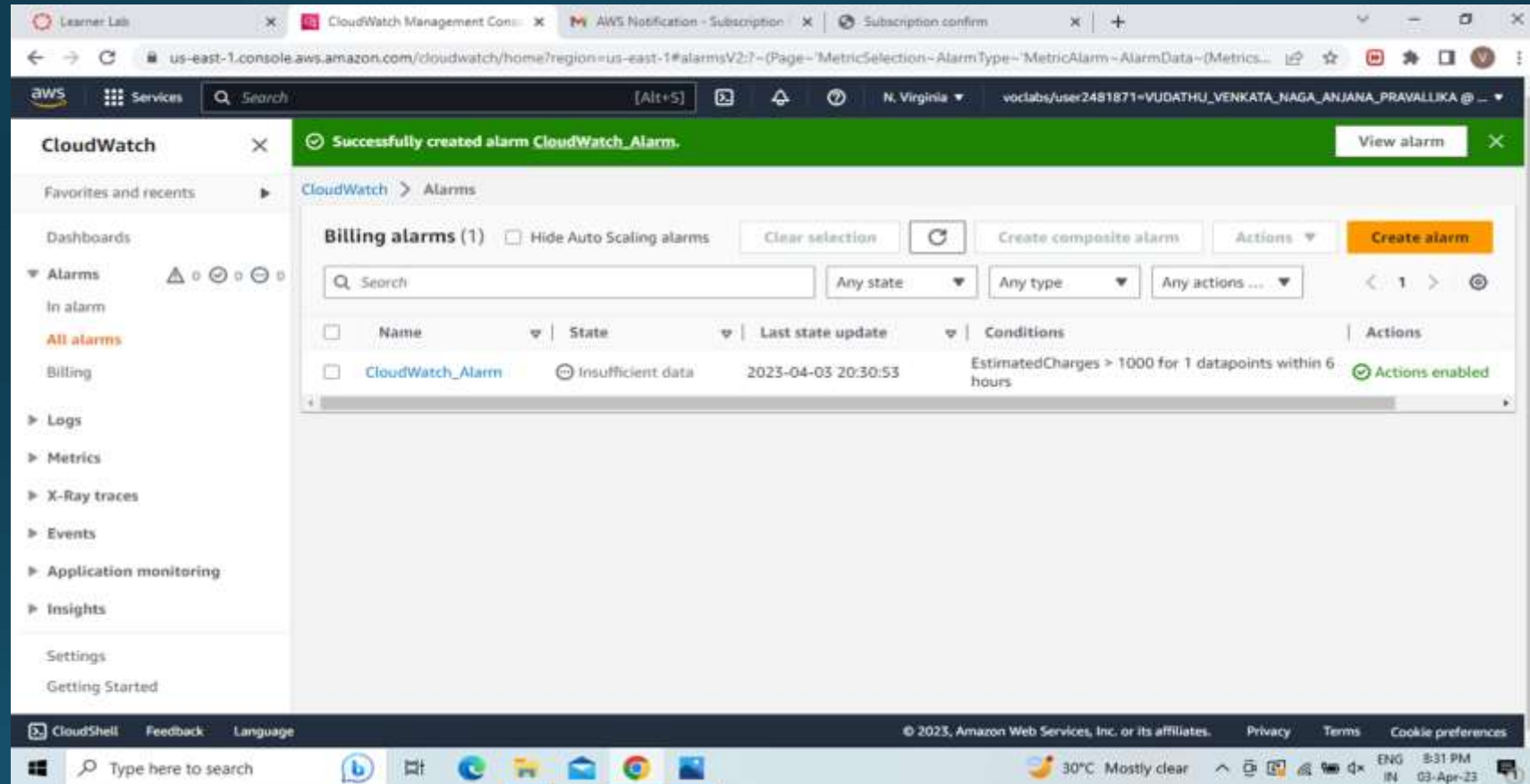
## Step 6: Give a name to your Alarm and Click on next



## Step 7: You will get a AWS Notification-Subscription Confirmation mail to the email which you have provided. Click on Confirm Subscription. Then it will open a window showing Subscription Confirmed.



Step 8. Preview the details you have entered .  
Step 9. Click on Create alarm. Alarm is successfully created.



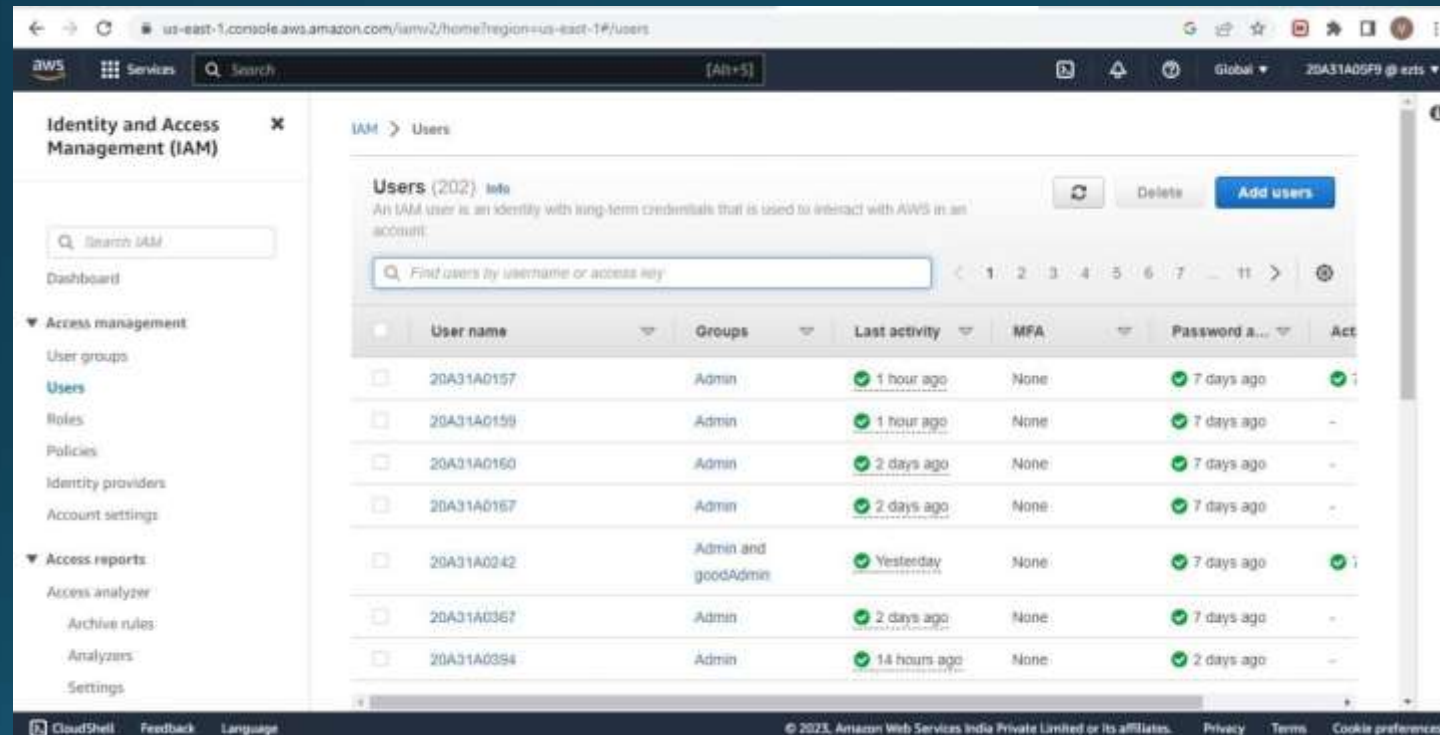
# AWS COMMAND LINE INTERFACE(CLI)



STEP 1 - Download and install AWS CLI and complete the installation steps.

STEP 2 - Login to AWS Management Console and search for IAM.

STEP 3 - In the navigation pane ,select Users

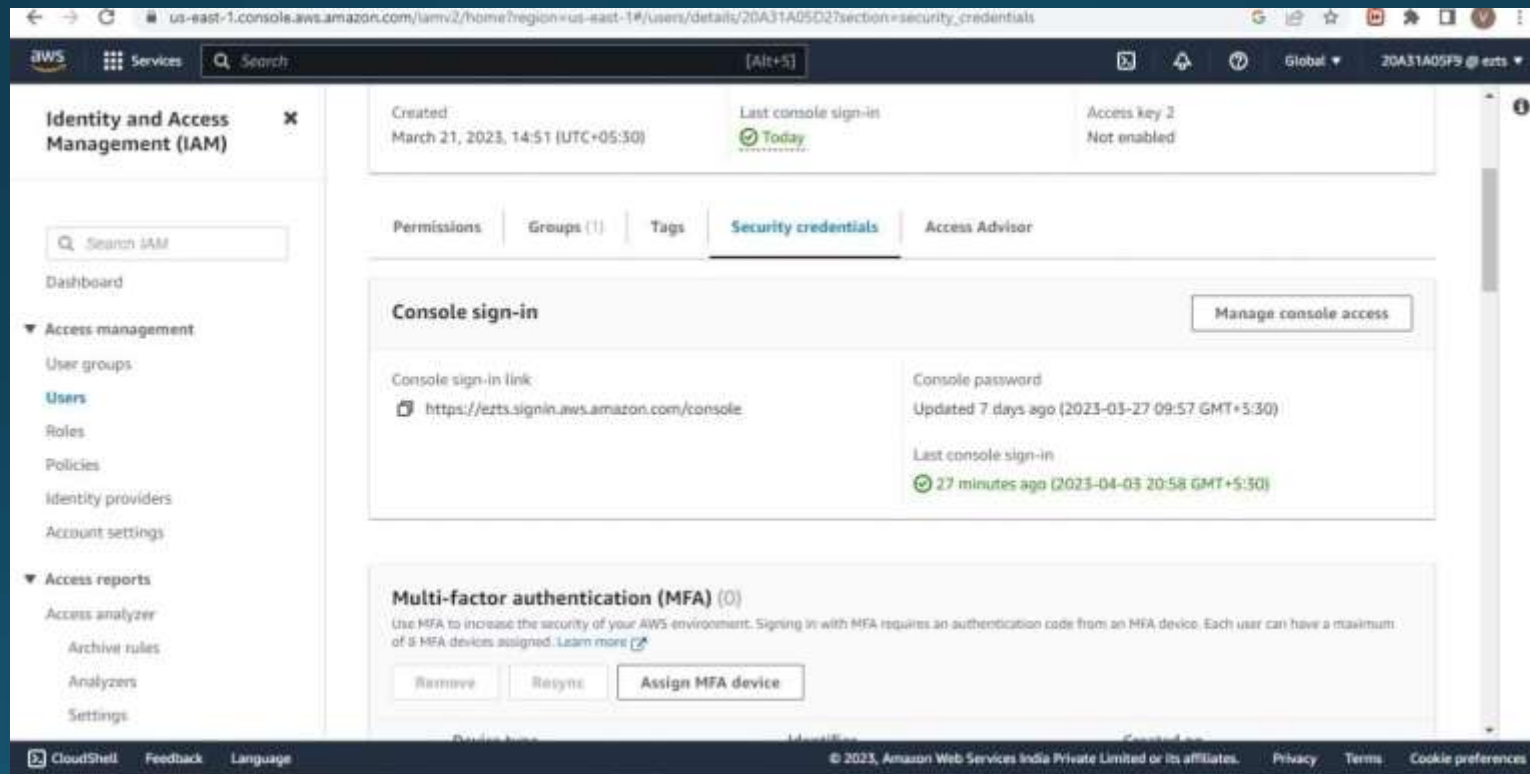


The screenshot displays the AWS IAM console interface. The left-hand navigation pane is titled "Identity and Access Management (IAM)" and includes sections for "Access management" (with links to User groups, Users, Roles, Policies, Identity providers, and Account settings) and "Access reports" (with links to Access analyzer, Archive rules, Analyzers, and Settings). The main content area is titled "IAM > Users" and features a "Users (202)" header with a description: "An IAM user is an identity with long-term credentials that is used to interact with AWS in an account." Below this is a search bar labeled "Find users by username or access key" and a table of users. The table has columns for checkboxes, User name, Groups, Last activity, MFA, Password a..., and Actions. The footer of the console shows "CloudShell", "Feedback", "Language", and copyright information for Amazon Web Services India Private Limited.

	User name	Groups	Last activity	MFA	Password a...	Act
<input type="checkbox"/>	20A31A0157	Admin	1 hour ago	None	7 days ago	1
<input type="checkbox"/>	20A31A0158	Admin	1 hour ago	None	7 days ago	-
<input type="checkbox"/>	20A31A0160	Admin	2 days ago	None	7 days ago	-
<input type="checkbox"/>	20A31A0167	Admin	2 days ago	None	7 days ago	-
<input type="checkbox"/>	20A31A0242	Admin and goodAdmin	Yesterday	None	7 days ago	1
<input type="checkbox"/>	20A31A0367	Admin	2 days ago	None	7 days ago	-
<input type="checkbox"/>	20A31A0394	Admin	14 hours ago	None	2 days ago	-

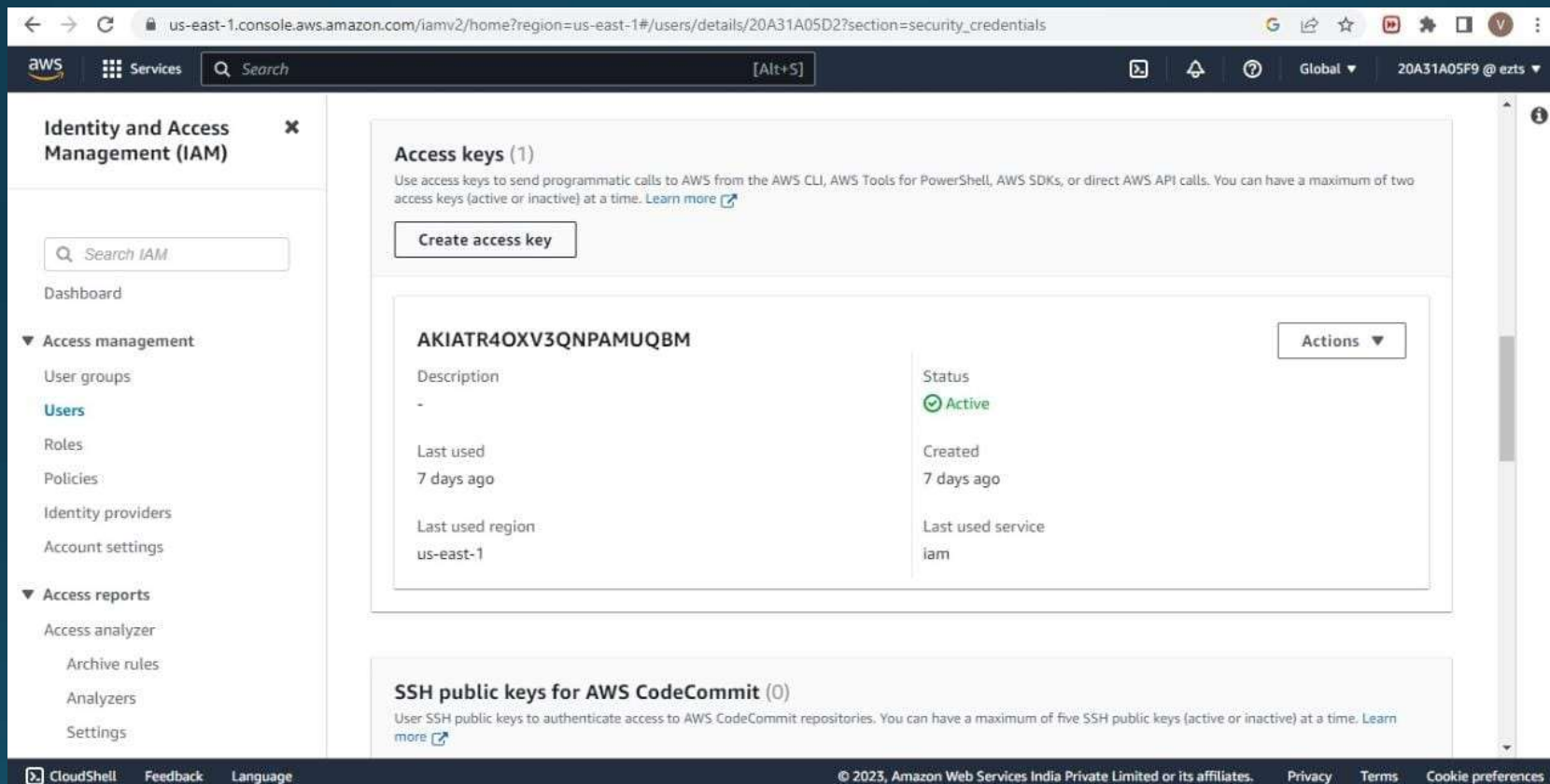
STEP 4 - In the users select the name of the user whose access keys you want to create.

STEP 5 - Click on Security Credentials tab.





STEP 6 - In the access Keys section , choose Create access key.



The screenshot shows the AWS IAM console interface. The left sidebar contains the 'Identity and Access Management (IAM)' menu with options like Dashboard, Access management, Users, Roles, Policies, Identity providers, Account settings, Access reports, Access analyzer, Archive rules, Analyzers, and Settings. The main content area is titled 'Access keys (1)' and includes a 'Create access key' button. Below this, a table lists the existing access key with the ID 'AKIATR40XV3QNPAMUQBM'. The table has columns for Description, Status, Last used, Created, Last used region, and Last used service. The status is 'Active' with a green checkmark. The last used date is '7 days ago'. The last used region is 'us-east-1' and the last used service is 'iam'. An 'Actions' dropdown menu is visible next to the key ID. Below the table, there is a section for 'SSH public keys for AWS CodeCommit (0)' with a brief description and a 'Learn more' link. The footer of the console shows 'CloudShell', 'Feedback', 'Language', and copyright information for Amazon Web Services India Private Limited.

us-east-1.console.aws.amazon.com/iamv2/home?region=us-east-1#/users/details/20A31A05D2?section=security\_credentials

**Identity and Access Management (IAM)**

Search IAM

Dashboard

Access management

- User groups
- Users**
- Roles
- Policies
- Identity providers
- Account settings

Access reports

- Access analyzer
- Archive rules
- Analyzers
- Settings

**Access keys (1)**

Use access keys to send programmatic calls to AWS from the AWS CLI, AWS 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. [Learn more](#)

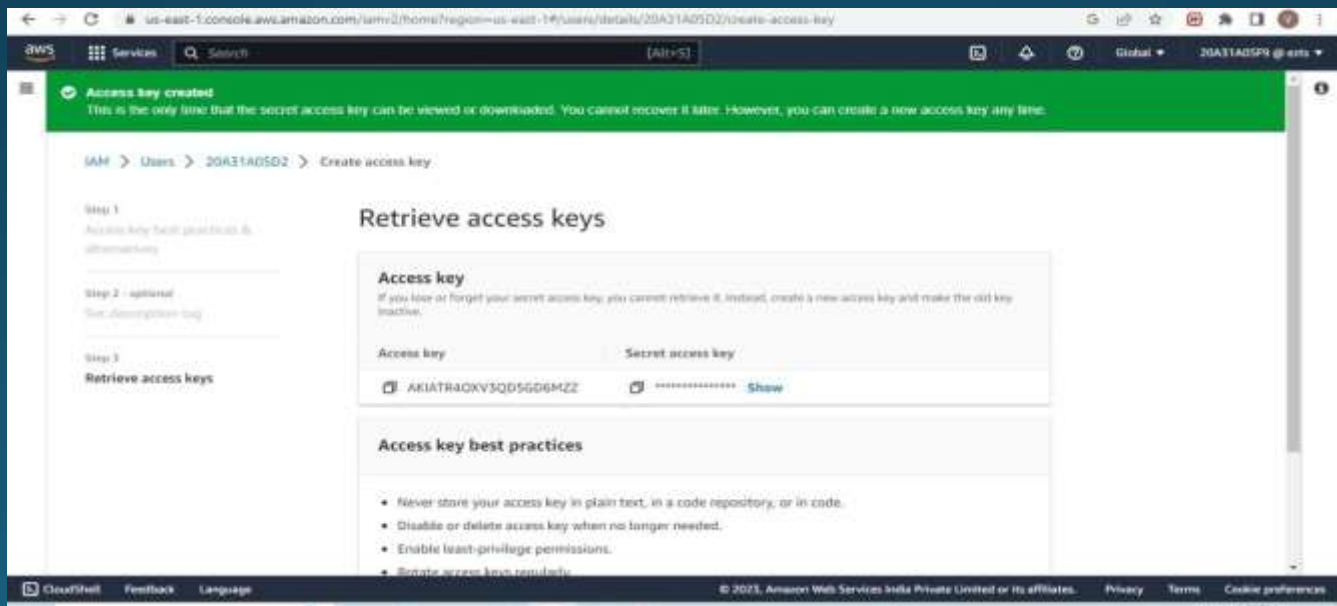
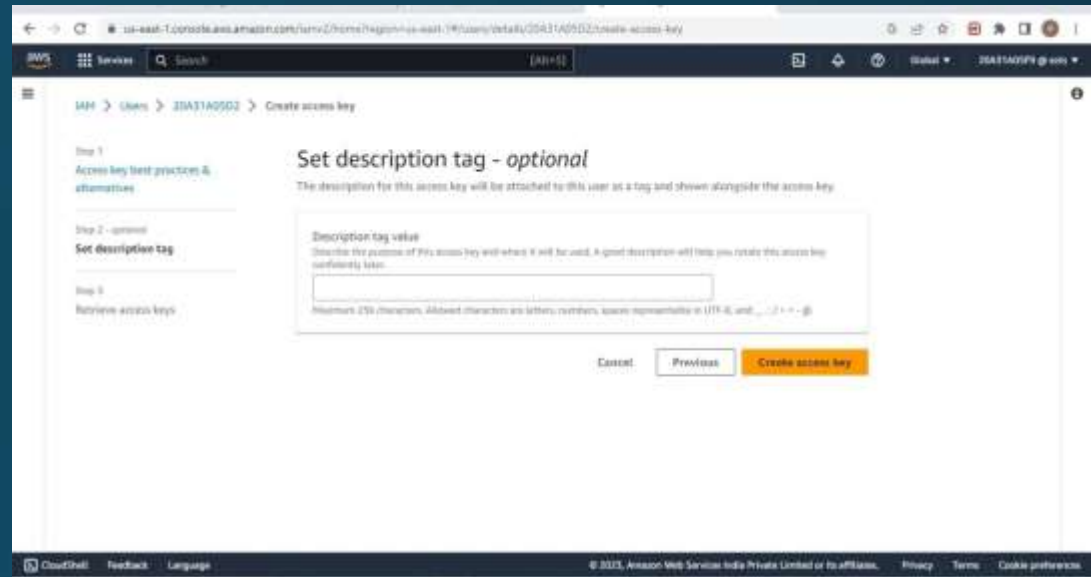
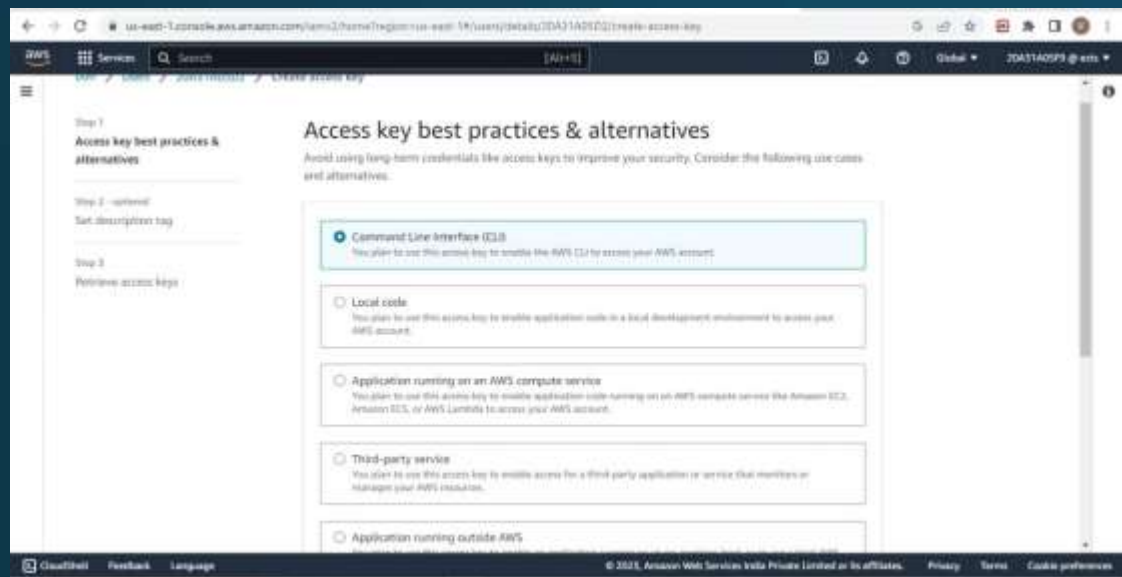
Create access key

AKIATR40XV3QNPAMUQBM		Actions
Description		Status
-		Active
Last used		Created
7 days ago		7 days ago
Last used region		Last used service
us-east-1		iam

**SSH public keys for AWS CodeCommit (0)**

User SSH public keys to authenticate access to AWS CodeCommit repositories. You can have a maximum of five SSH public keys (active or inactive) at a time. [Learn more](#)

CloudShell Feedback Language © 2023, Amazon Web Services India Private Limited or its affiliates. Privacy Terms Cookie preferences



STEP 7 – Now you can use this access key to configure CLI

STEP 8 - Open Command Line Interface and run the following command

>aws configure

After entering this command AWS CLI prompts us with four pieces of information

1. Access Key ID: (enter your ID)
2. Secret Access Key: ( enter your key)
3. AWS Region: (enter the desired region )
4. Output Format: (enter the desired output)

```
Microsoft Windows [Version 10.0.22621.1413]
(c) Microsoft Corporation. All rights reserved.

C:\Users\sivas>aws configure
AWS Access Key ID [None]: AKIATR40XV3QD5GD6MZZ
AWS Secret Access Key [None]: vMQP4GL99CbDSxsPWSgiTkkozMiRsUUZ0i+hDdNT
Default region name [None]: us-east-1
Default output format [None]: json
```

Finally we get Javascript Object Notation of all the users as output.

AWS LAMBDA

1) In the search box to the right of Services, search for and choose Lambda to open the AWS Lambda console.

2) Choose Create function.

3) In the Create function screen, configure these settings:

> Choose Author from scratch

> Function name: myStopinator

> Runtime: Python 3.8

> Choose Change default execution role

> Execution role: Use an existing role

> Existing role: From the dropdown list, choose myStopinatorRole

4) Choose Create function.

5) Choose Add trigger.

6) Choose the Select a trigger dropdown menu, and select EventBridge (CloudWatch Events).

7) For the rule, choose Create a new rule and configure these settings:

Rule name: everyMinute

Rule type: Schedule expression

Schedule expression: rate(1 minute)

8) Choose Add.

Below the Function overview pane, choose Code, and then choose `lambda_function.py` to display and edit the Lambda function code.

In the Code source pane, delete the existing code. Copy the following code, and paste it in the box:

```
import boto3
region = '<REPLACE_WITH_REGION>'
instances = ['<REPLACE_WITH_INSTANCE_ID>']
ec2 = boto3.client('ec2', region_name=region)

def lambda_handler(event, context):
    ec2.stop_instances(InstanceIds=instances)
    print('stopped your instances: ' + str(instances))
```

9) Replace the `<REPLACE_WITH_REGION>` placeholder with the actual Region that you are using. To do this:

10) Choose on the region on the top right corner and use the region code. For example, the region code for US East (N. Virginia) is `us-east-1`.

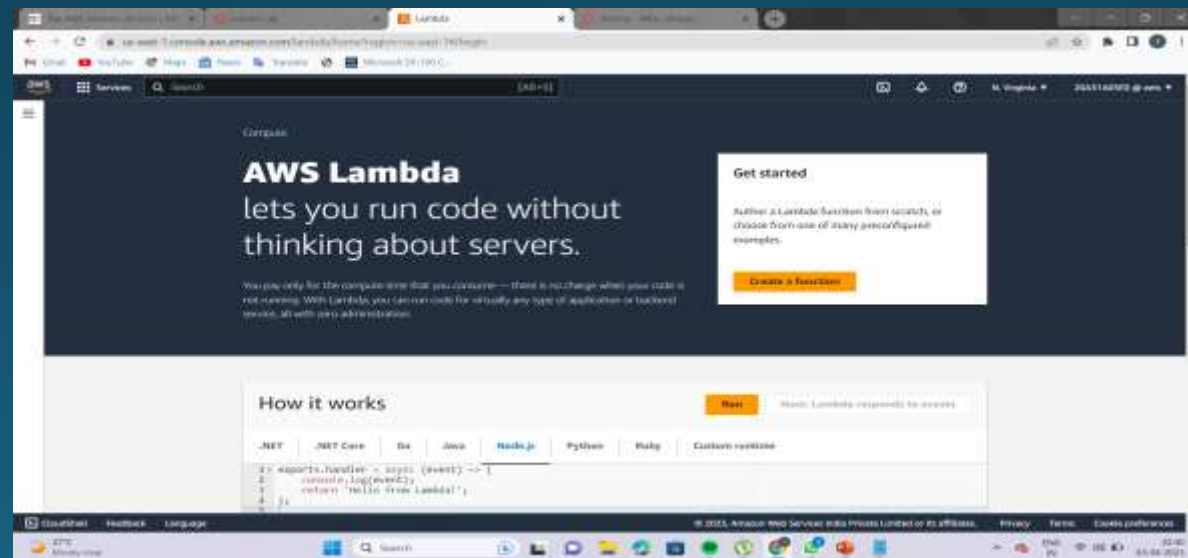
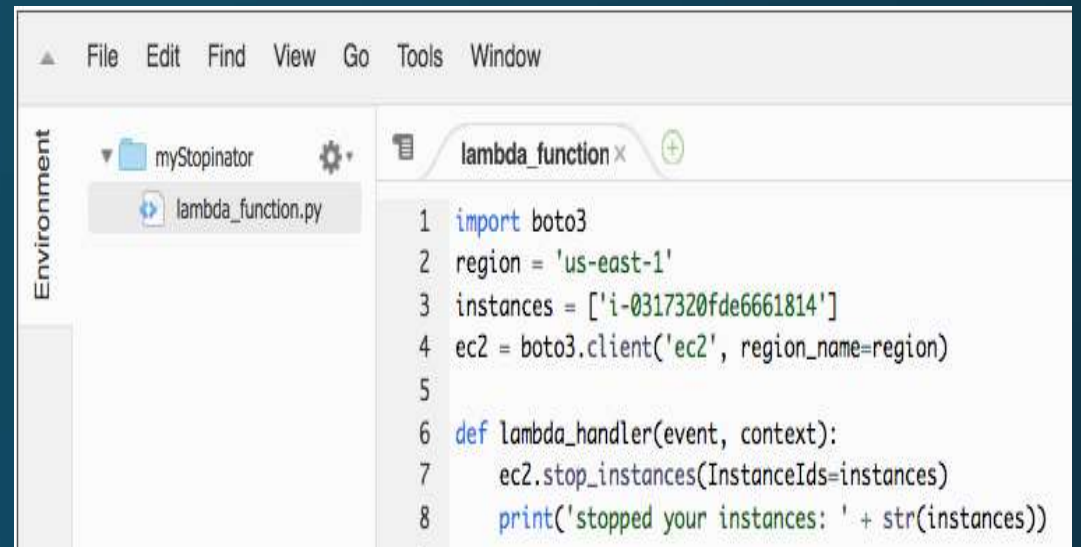
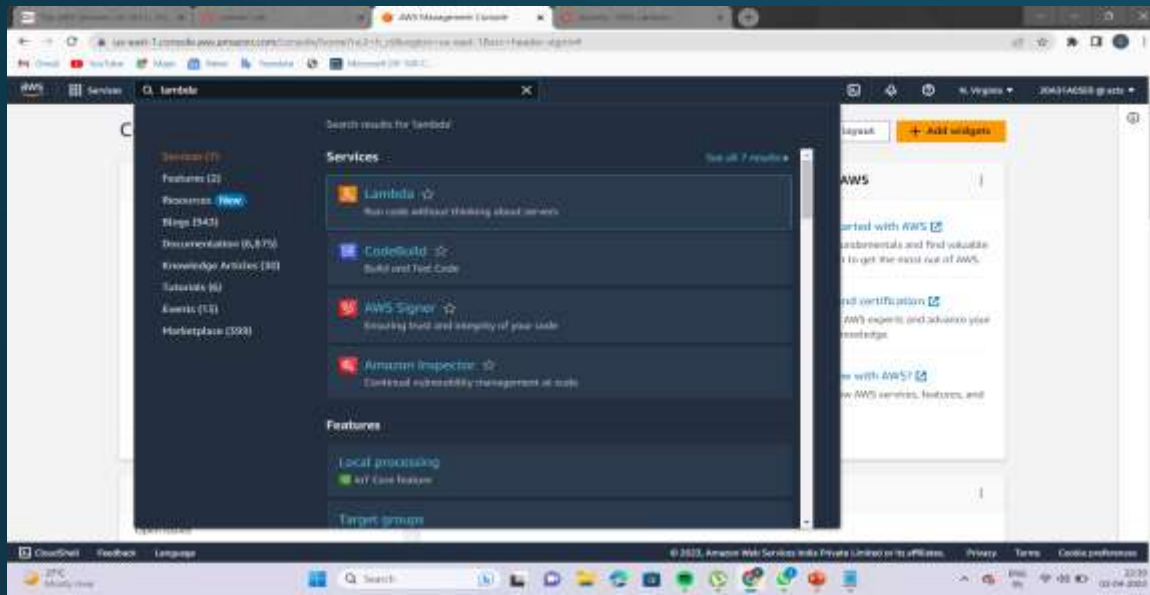
11) Verify that an EC2 instance named `instance1` is running in your account, and copy the `instance1` instance ID.

12) Return to the AWS Lambda console browser tab, and replace `<REPLACE_WITH_INSTANCE_ID>` with the actual instance ID that you just copied.

13) Choose the File menu and Save the changes. Then, in the top-right corner of the Code source box, choose Deploy.

14) Choose Monitor

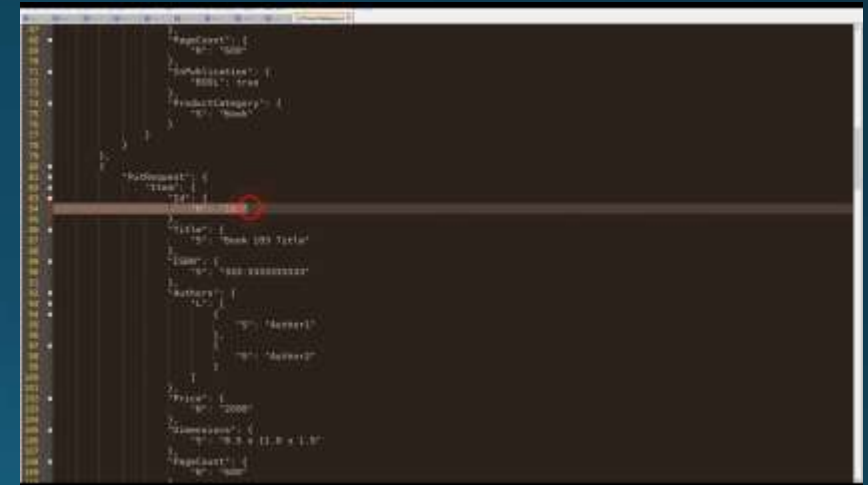
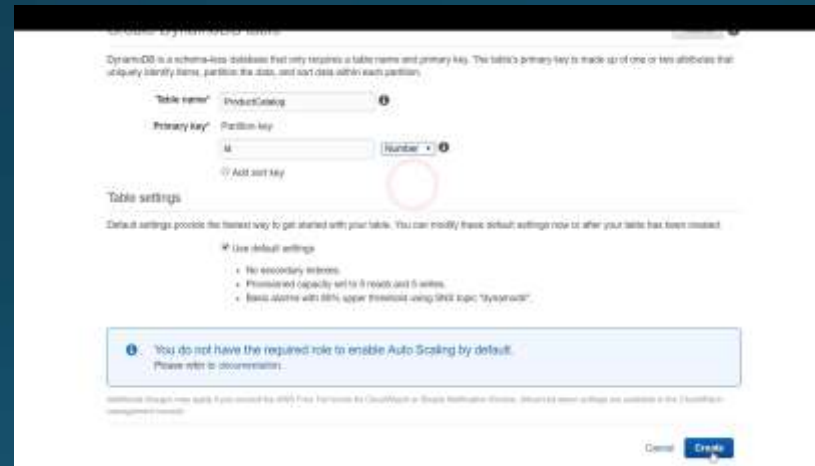
15) Return to the Amazon EC2 console browser tab and see if your instance was stopped.



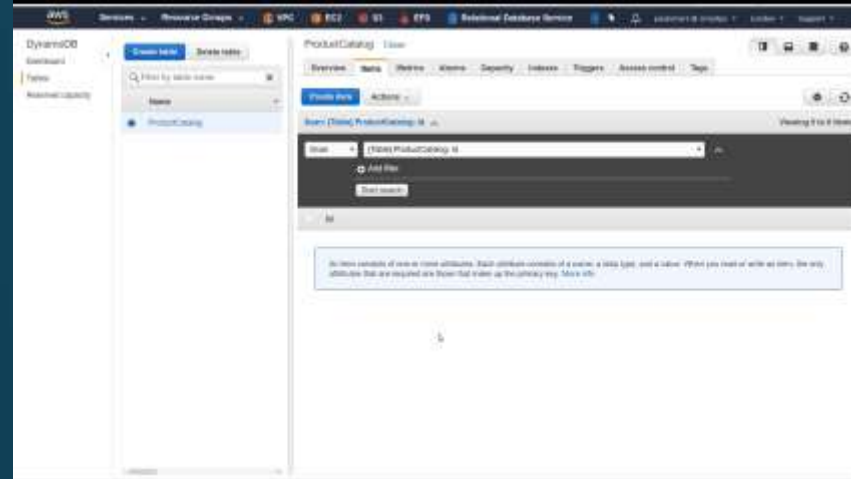
DYNAMO DB



- Setting up the Amazon DynamoDB
- here, we will be having an JSON file which is a product catalog
- the products have a lot of different attributes and **id** is only common.
- the interface looks like this:



- After creating the table, we can see that there are no items present.

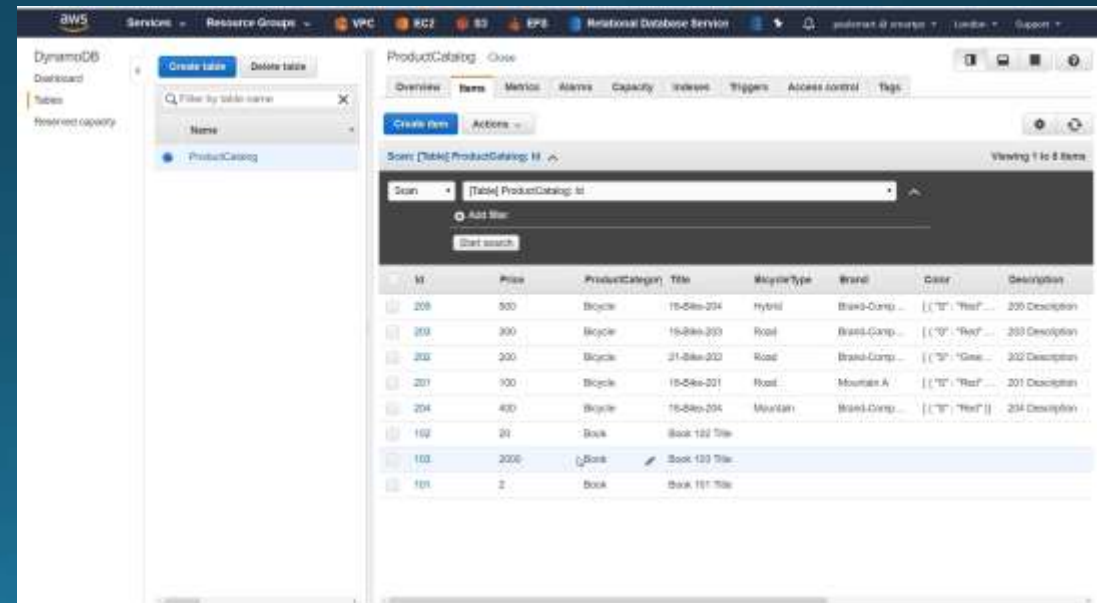


- So we will use the CLI to populate the table. Open powershell of AWS.

```
Windows PowerShell for AWS
C:\> aws dynamodb list-tables --region eu-west-2
{
  "TableNames": [
    "ProductCatalog"
  ]
}

C:\> aws dynamodb describe-table --table-name ProductCatalog --region eu-west-2
{
  "Table": {
    "TableName": "aws-iam-dynamodb:eu-west-2:409281224315:table/ProductCatalog",
    "AttributeDefinitions": [
      {
        "AttributeName": "id",
        "AttributeType": "N"
      }
    ],
    "ProvisionedThroughput": {
      "NumberOfDecreasesToday": 0,
      "ReadCapacityUnits": 5,
      "WriteCapacityUnits": 5
    },
    "TableSizeBytes": 0,
    "TableName": "ProductCatalog",
    "TableStatus": "ACTIVE",
    "KeySchema": [
      {
        "KeyType": "HASH",
        "AttributeName": "id"
      }
    ],
    "ItemCount": 0,
    "CreationDateTime": 1521726613.734
  }
}

C:\> aws dynamodb batch-write-item --request-items file://ProductCatalog.json --region eu-west-2
```



**AWS** Services Resource Groups VPC EC2 S3 EFS Amazon Database Service **product101-ec2-aws** Launch Support

**DynamoDB** Dashboard Tables Reserved capacity

**Create table** **Delete table**

Filter by table name

Name

ProductCatalog

**ProductCatalog** **Class**

Overview **Items** Metrics Alarms Capacity Indices Triggers Access control Tags

**Create table** **Actions**

Item (Table) ProductCatalog: Item Viewing 1 to 8 items

Query [Table] ProductCatalog: Item

Partition key

Number 204

Add filter

Sort ☐ Ascending ☒ Descending

Attributes ☐ All ☒ Projected

Start search Cancel changes

ID	Price	ProductCategory	Title	ItemType	Brand	Color	Description
<input type="checkbox"/> 208	550	Boysie	15-666-204	Hybrid	Brand-Corp.	[{"T": "Red"}]	208 Description
<input type="checkbox"/> 202	390	Boysie	15-666-203	Food	Brand-Corp.	[{"T": "Red"}]	202 Description
<input type="checkbox"/> 202	290	Boysie	21-666-202	Food	Brand-Corp.	[{"T": "Blue"}]	202 Description
<input type="checkbox"/> 201	190	Boysie	15-666-201	Food	Mountain	[{"T": "Red"}]	201 Description
<input type="checkbox"/> 204	480	Boysie	15-666-204	Mountain	Brand-Corp.	[{"T": "Red"}]	204 Description
<input type="checkbox"/> 102	25	Book	Book 102 Title				
<input type="checkbox"/> 103	2300	Book	Book 103 Title				
<input type="checkbox"/> 101	2	Book	Book 101 Title				

**AWS** Services Resource Groups VPC EC2 S3 EFS Amazon Database Service **product101-ec2-aws** Launch Support

**DynamoDB** Dashboard Tables Reserved capacity

**Create table** **Delete table**

Filter by table name

Name

ProductCatalog

**ProductCatalog** **Class**

Overview **Items** Metrics Alarms Capacity Indices Triggers Access control Tags

**Create table** **Actions**

Item (Table) ProductCatalog: Item Viewing 1 to 1 item

Query [Table] ProductCatalog: Item

Partition key

Number 204

Add filter

Sort ☐ Ascending ☒ Descending

Attributes ☐ All ☒ Projected

Start search

ID	Price	ProductCategory	Title	ItemType	Brand	Color	Description
<input type="checkbox"/> 204	400	Boysie	15-666-204	Mountain	Brand-Corp.	[{"T": "Red"}]	204 Description

AWS LIGHT SAIL

## PROCEDURE:

1. On the home page, choose Create instance.
2. Select a location for your instance (an AWS Region and Availability Zone). Choose Change Region and zone to create your instance in another location.
3. Optionally, you can change the Availability Zone. Choose an Availability Zone from the dropdown list.
4. Pick an application (Apps + OS) or an operating system (OS Only).
5. Choose your instance plan.
6. Enter a name for your instance.

### Resource names:

1. Must be unique within each AWS Region in your Lightsail account.
2. Must contain 2 to 255 characters.
3. Must start and end with an alphanumeric character or number.
4. Can include alphanumeric characters, numbers, periods, dashes, and underscores.

7. Choose one of the following options to add tags to your instance:

- Add key-only tags or Edit key-only tags (if tags have already been added). Enter your new tag into the tag key text box, and press Enter. Choose Save when you're done entering your tags to add them, or choose Cancel to not add them.



A dialog box titled "Key-only tags". It features a tab labeled "Version 1" with a close button (X). Below the tab is a text input field containing "Customer 1". At the bottom left, it says "Add a tag key and press Enter." At the bottom right, there are two buttons: "Save" with a green checkmark icon and "Cancel" with a red X icon.

- Create a key-value tag, then enter a key into the Key text box, and a value into the Value text box. Choose Save when you're done entering your tags, or choose Cancel to not add them. Key-value tags can only be added one at a time before saving. To add more than one key-value tag, repeat the previous steps.



A dialog box titled "Key-value tags". It contains two text input fields: "Key" with the value "Project" and "Value" with the value "Earth", separated by a right-pointing arrow. To the right of the input fields are two buttons: "Cancel" with a red X icon and "Save" with a green checkmark icon and a hand cursor pointing at it.

8. Choose Create instance.

Within minutes, your Lightsail instance is ready and you can connect to it via SSH, without leaving Lightsail!



# How to connect to your instance

1. From the Lightsail home page, choose the menu on the right of your instance's name, and then choose connect.



Alternately, you can open your instance management page and choose the Connect tab.

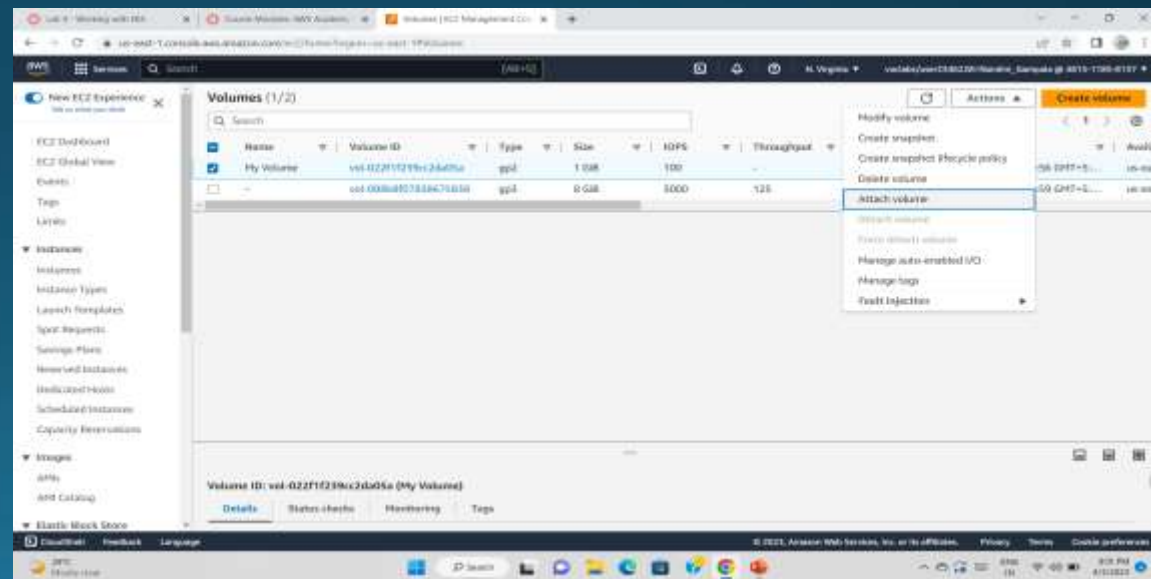
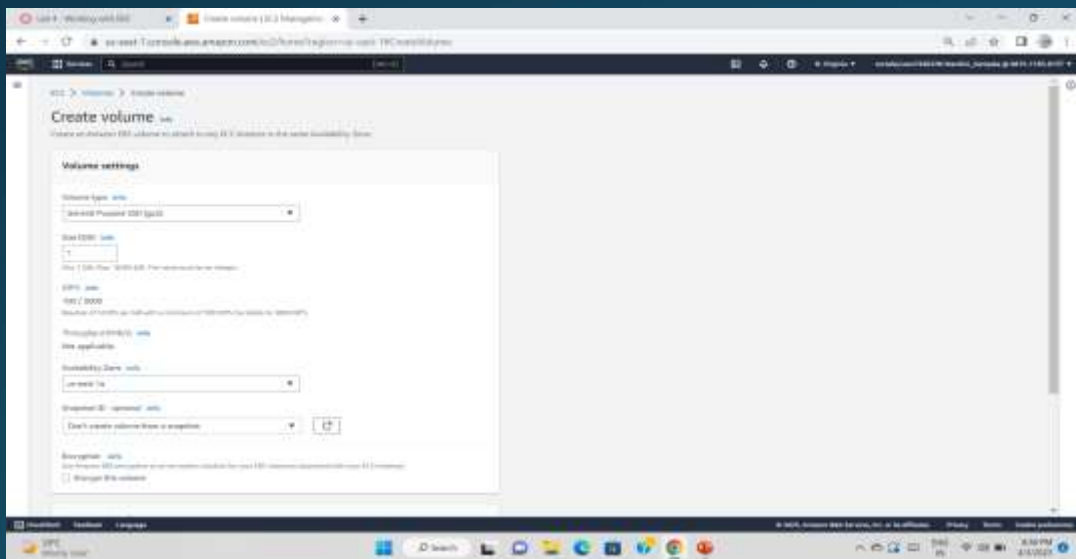
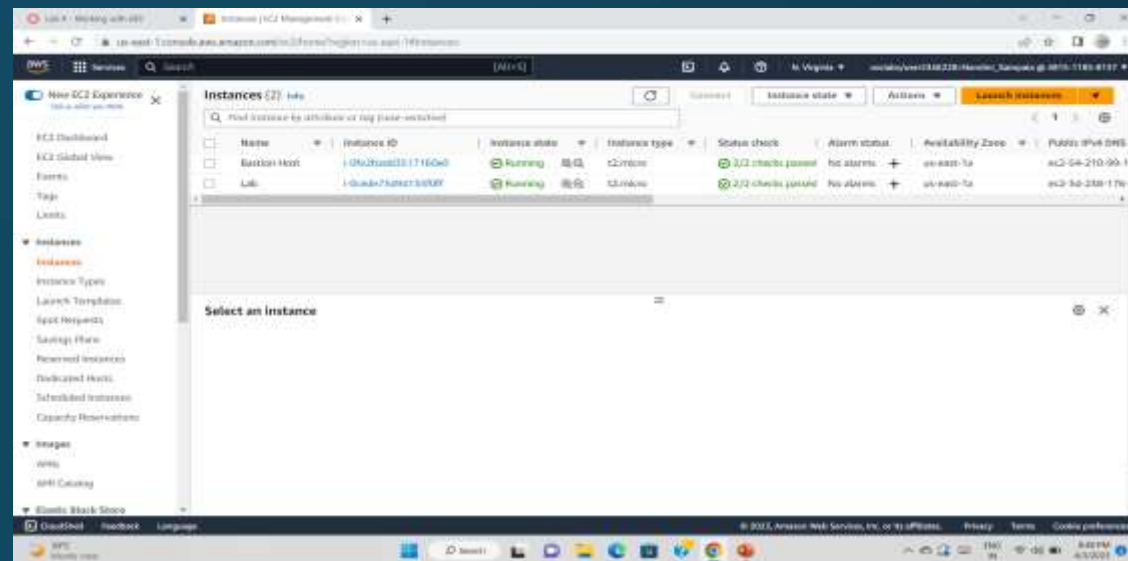
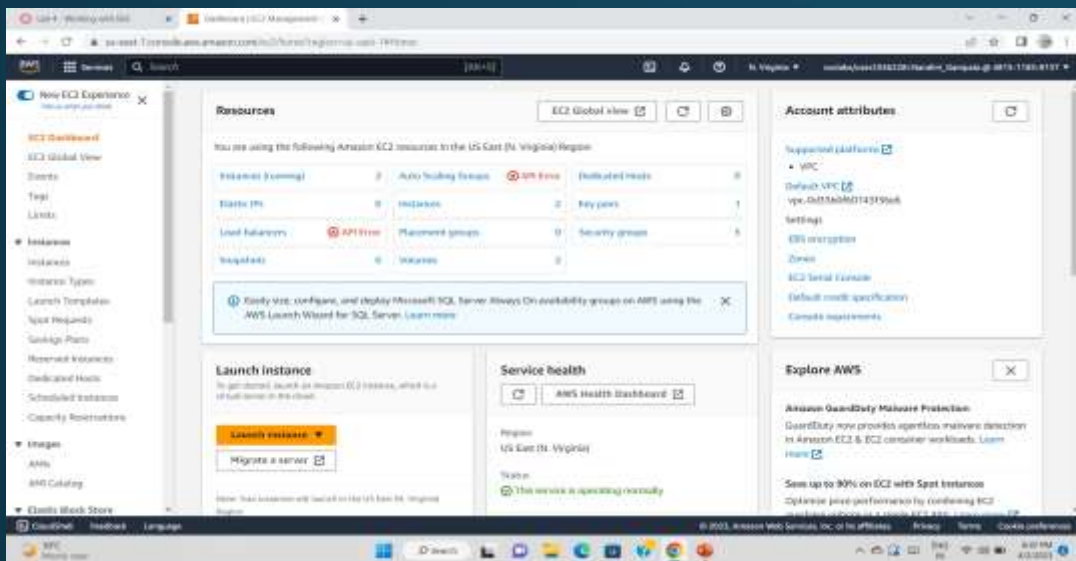
2. You can now type commands into the terminal and manage your Lightsail instance without setting up an SSH client.

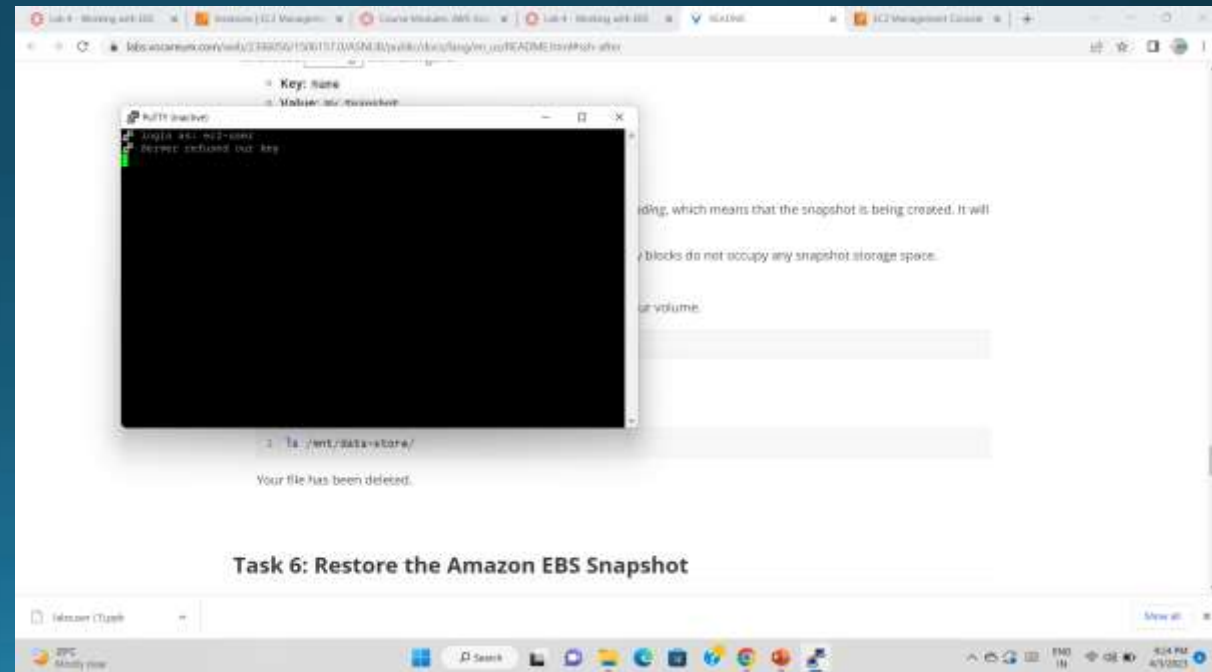
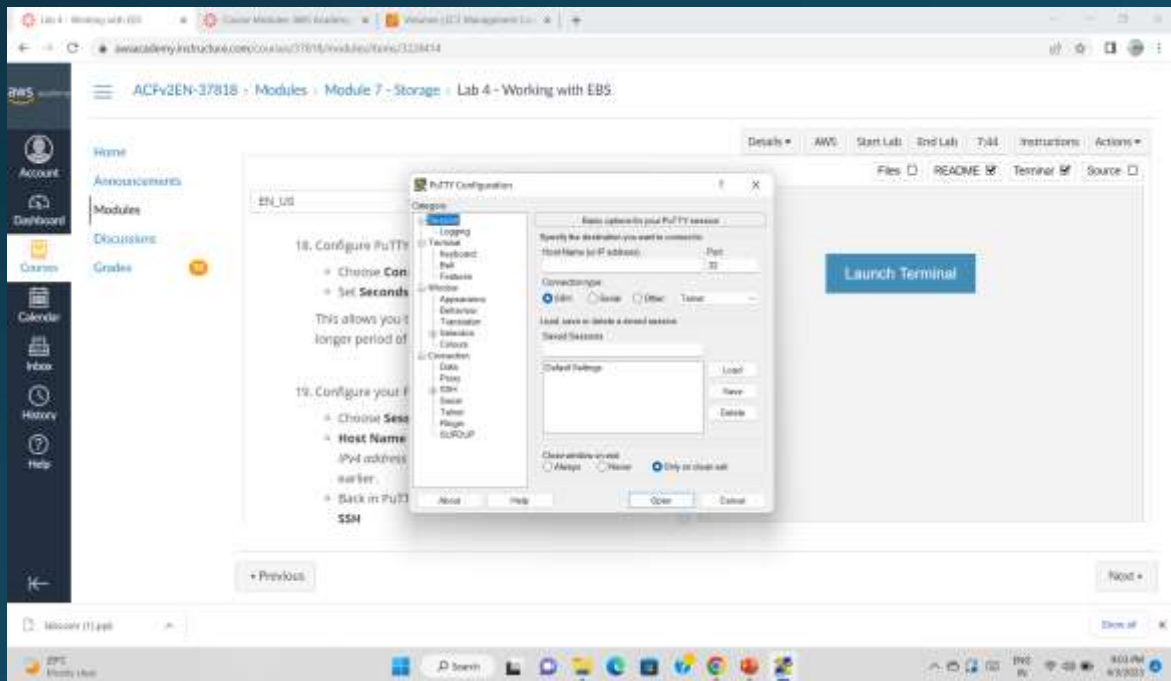
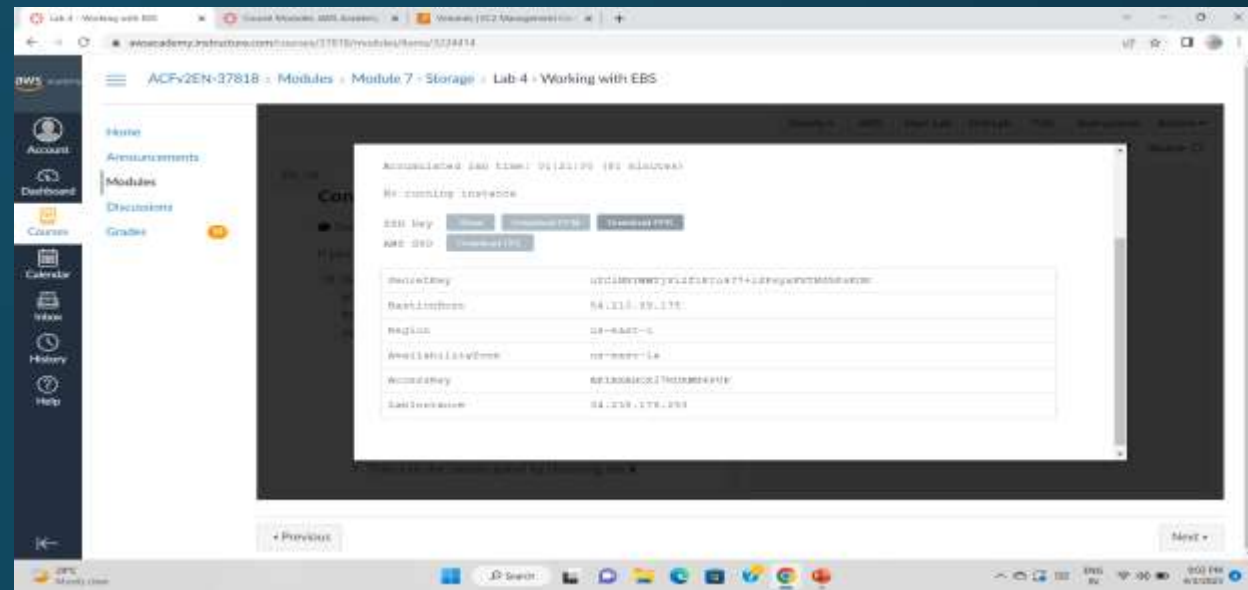
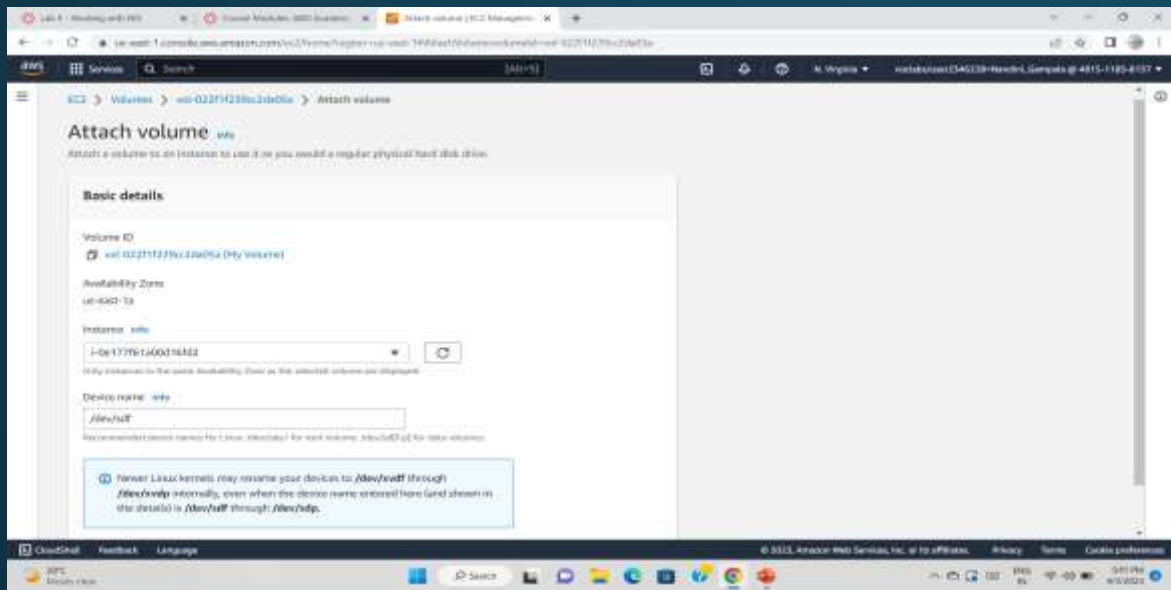


# AWS ELASTIC BLOCK STORE(EBS)

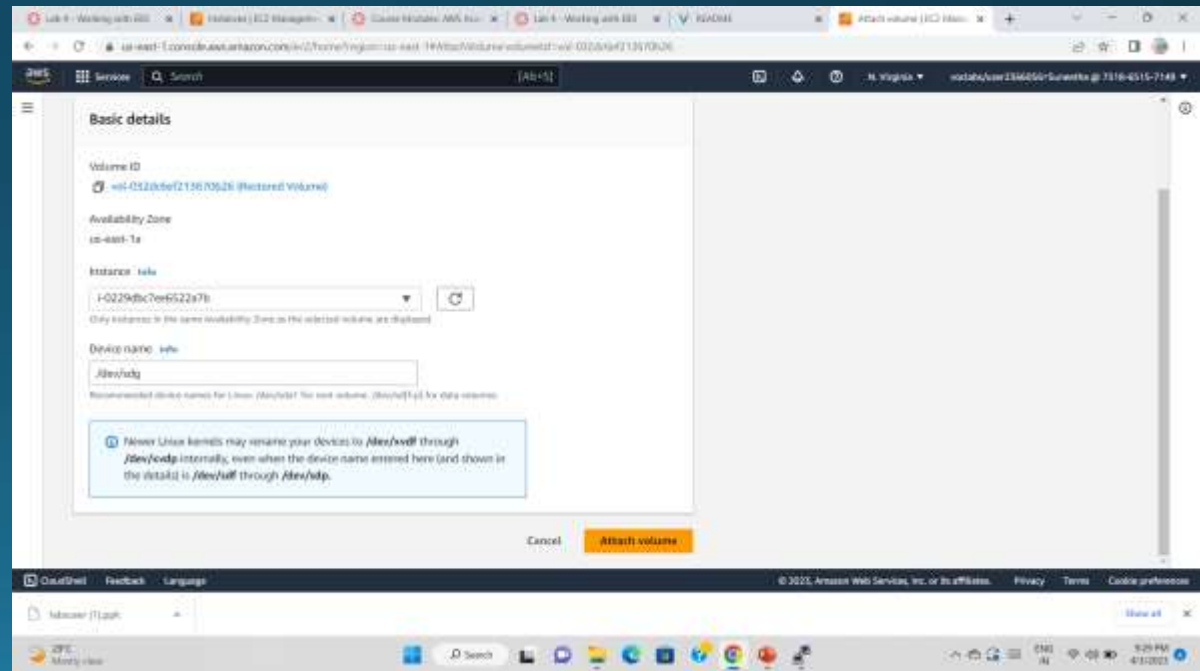
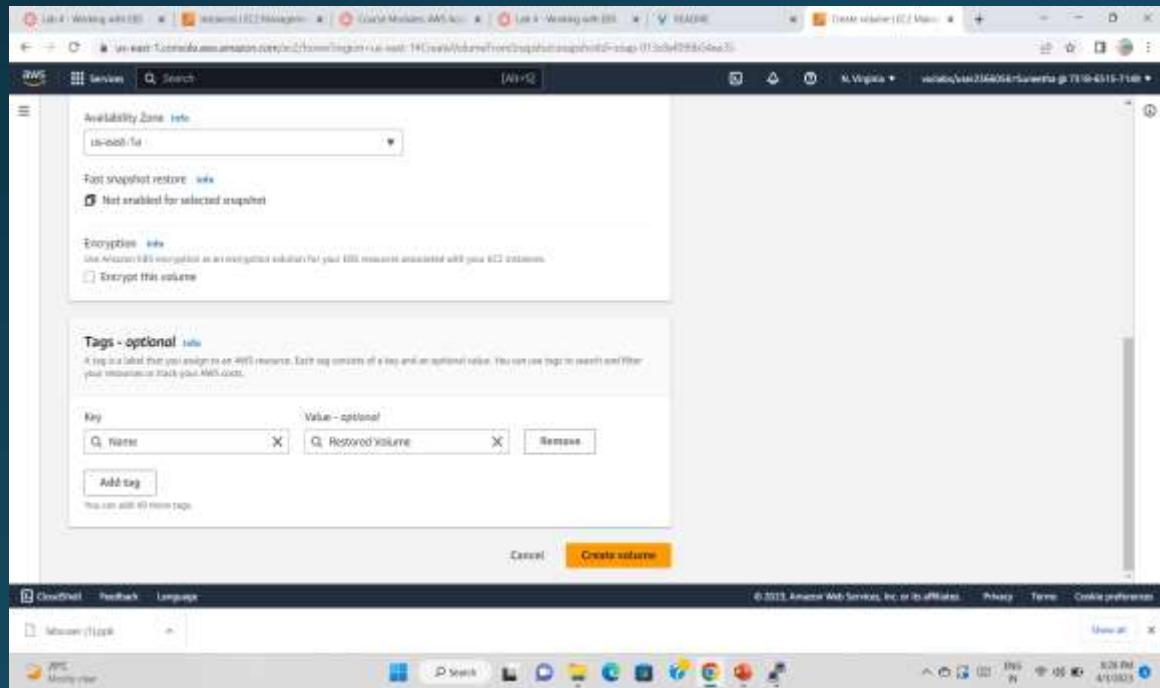
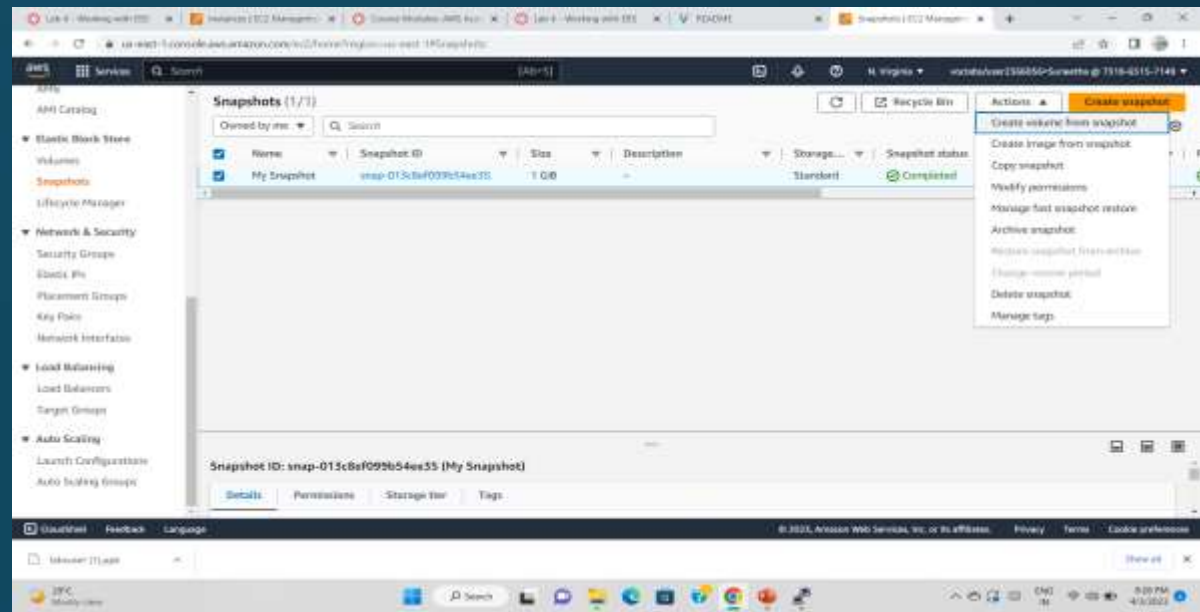
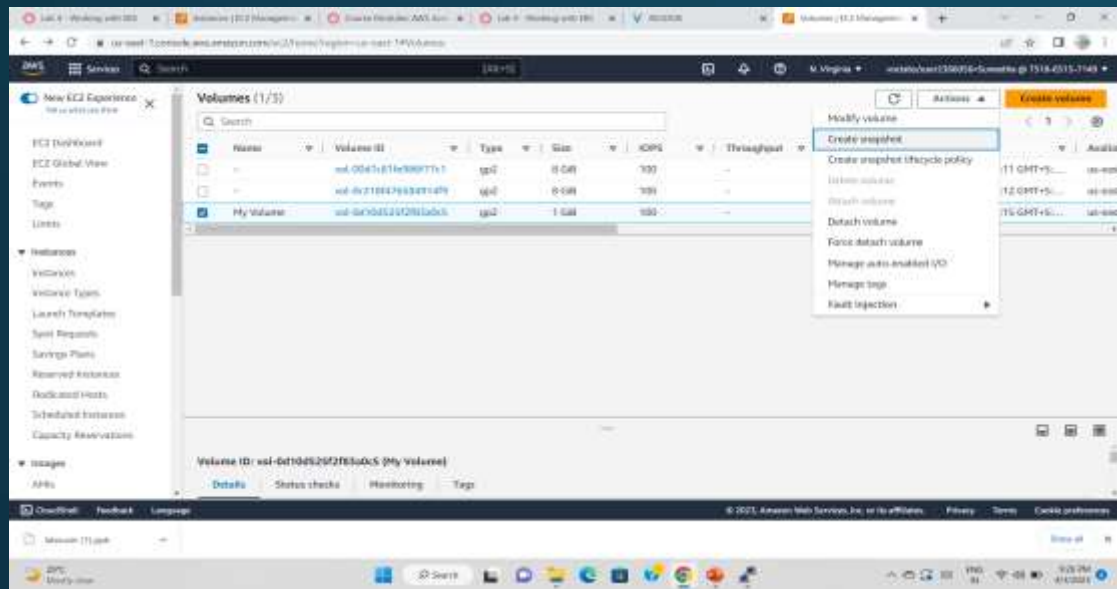
# CREATING A EBS VOLUME

1. Open Management Console, on the services menu open Ec2
2. In the left navigation pane choose instances and create a instance with a name
3. Next, In the left navigation pane choose Volumes
4. Click on Create Volume
5. Select volume type, size(Gib),Availability Zone and in Add tag section add key and value names.
6. Then click on create volume
7. Click on volumes on left navigation pane select the created volume and attach a previously created instance to it.
8. Then, go to “Details” drop down, choose “show”
9. Download the ppk file
10. Download putty
11. Open putty set the fields (such as Host name, public key, private key) as per the requirement.
12. The putty shell will open , then login into it and run the commands.
13. The commands looks like:  
df -h  
sudo mkfs -t ext3/dev/sdf                      etc.,
14. Create a EBS snapshot by giving the necessary fields.
15. Create a volume using snapshot.
16. Attach the volume to the created EC2 instance











# AWS S3 (SIMPLE STORAGE SERVICE)

## TASKS FOR CONFIGURING S3:

1. Log into the AWS Management Console.
2. Create an S3 bucket.
3. Upload an object to S3 Bucket.
4. Access the object on the browser.
5. Change S3 object permissions.
6. Setup the bucket policy and permission and test the object accessibility.

## STEPS :

**Step 1:** Click on **create group**.

**Step 2:** Set up the bucket name. S3 bucket name are globally unique, choose a name which is available. Leave other settings as default and click on **create group**.

**Step 3:** Click on your bucket name.

**Step 4:** Click Upload.

**Step 5:** Click on Add Files , and choose a file from your computer.

**Step 6:** After choosing your file, click on Next.

**Step 7:** Click on Upload.

**Step 8:**Now you have a private S3 bucket with a private object uploaded, which means you cannot visit it through Internet.

**Step 9:**Now you have a private S3 bucket with a private object uploaded, which means you cannot visit it through Internet.

## CHANGE BUCKET PERMISSIONS:

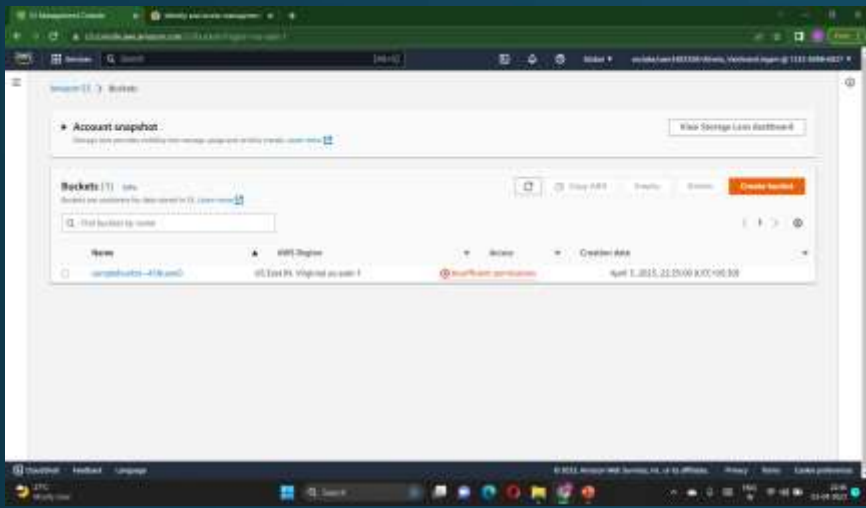
**Step 10:**Go back to your bucket and click on Permissions.

**Step 11:**Click on Everyone under the Public access, and click on Read object on the right of pop-up window. Then click on Save.

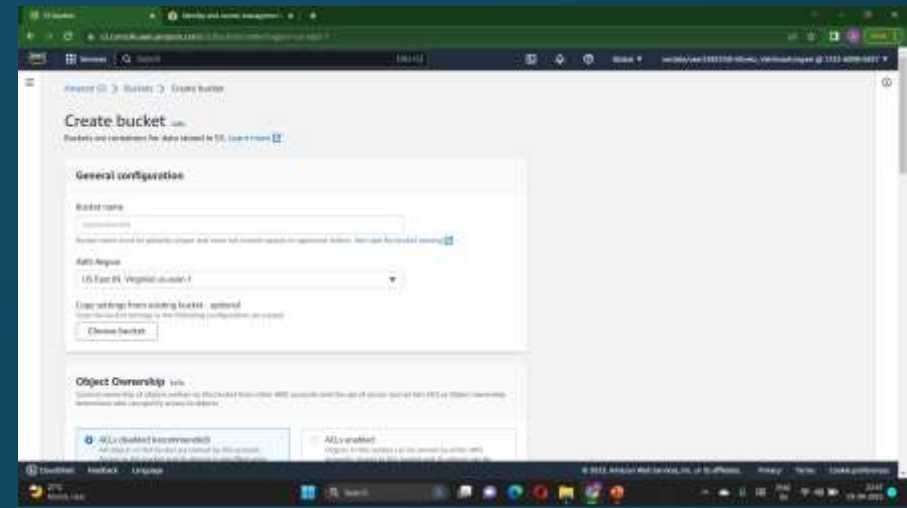
**Step 12 :**Now its state switches to Read Object - Yes

**Step 13:**Click on Overview, and click on your Object URL again .

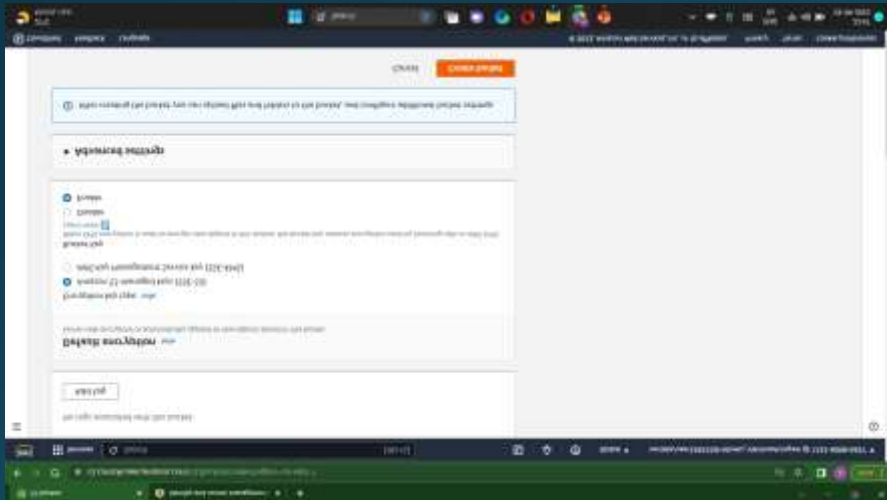
**Step 14:**Notice the URL on your browser



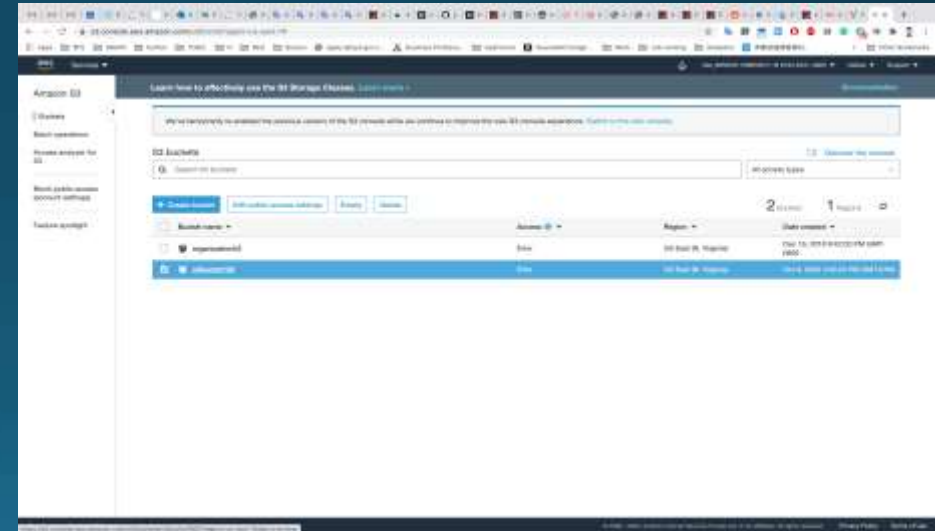
Step 1



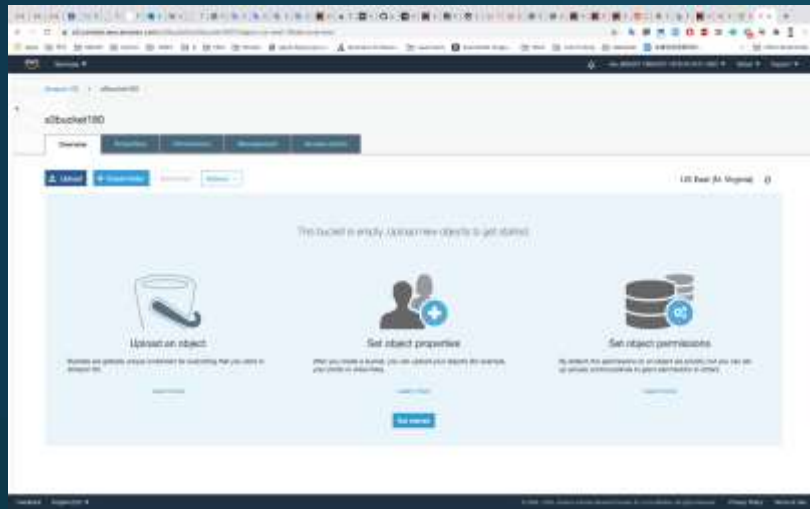
Step 2



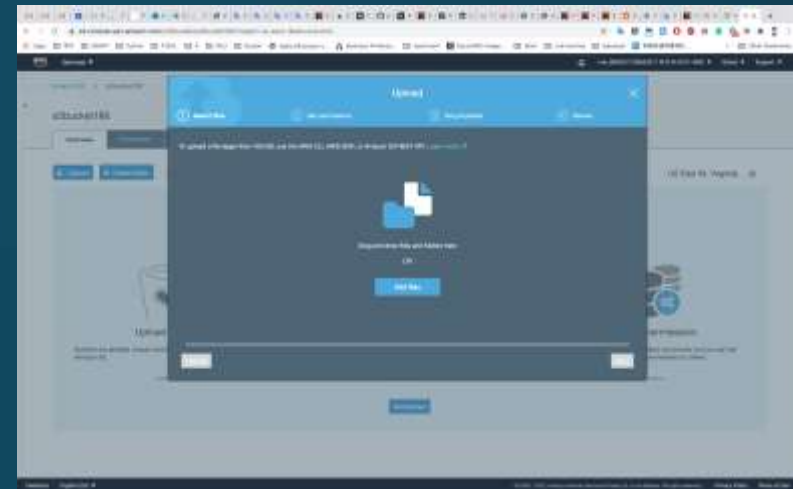
Step 2



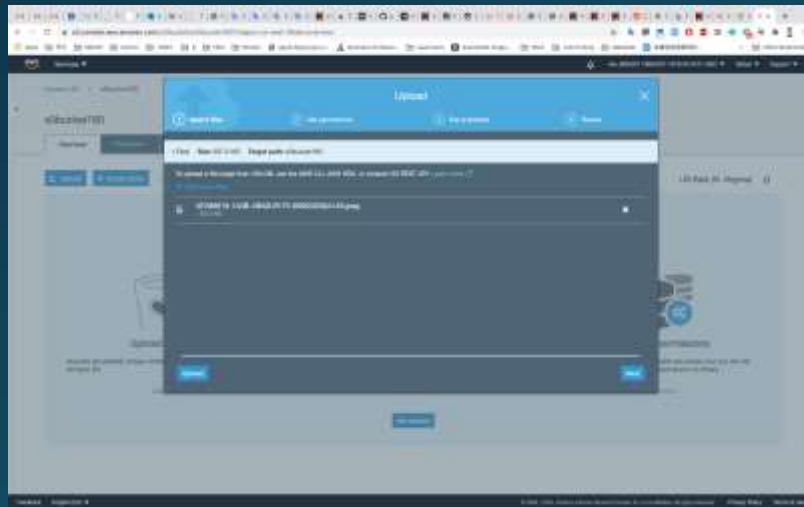
Step 3



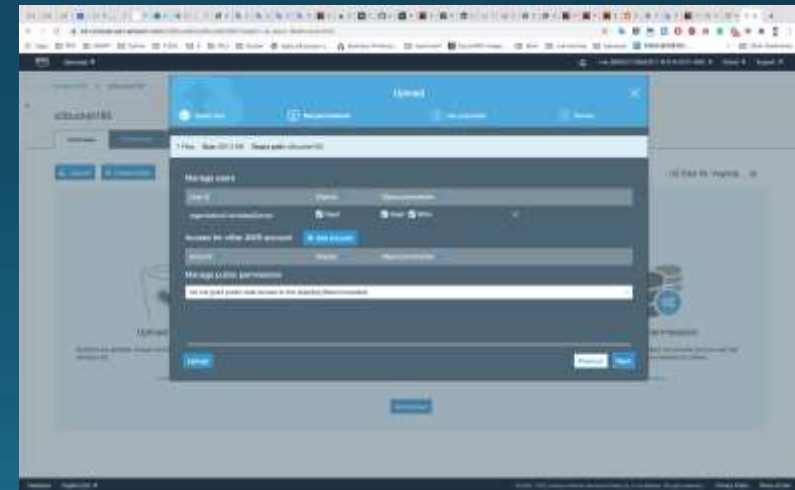
Step 4



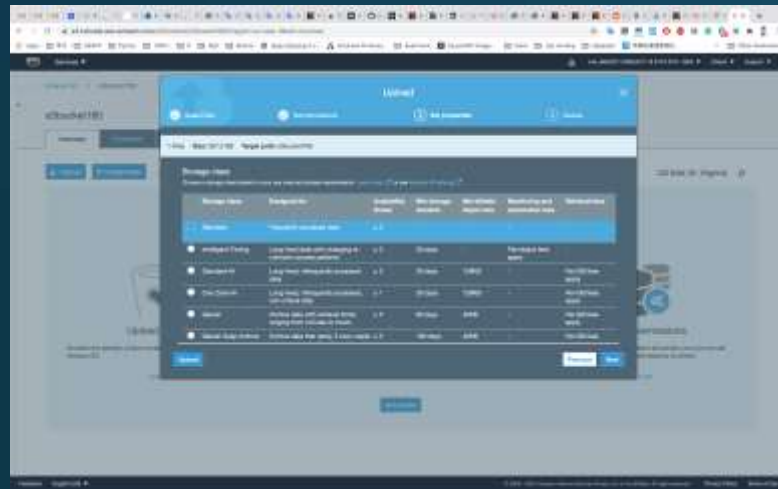
Step 5



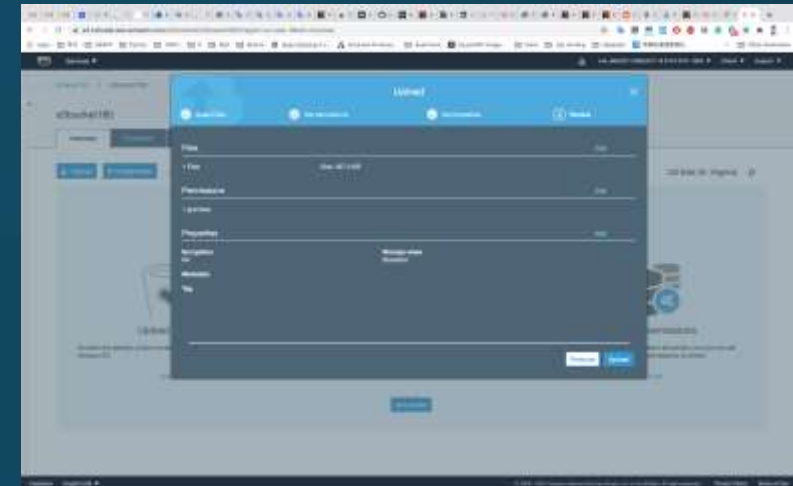
Step 6



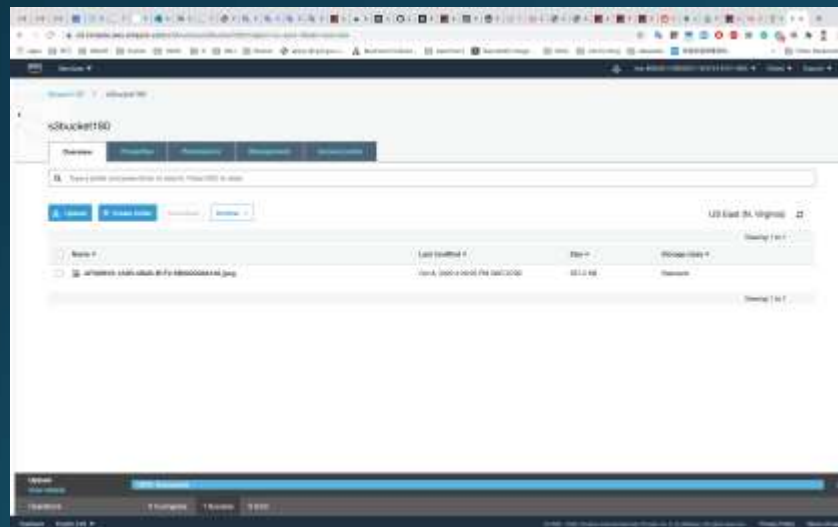
Step 7



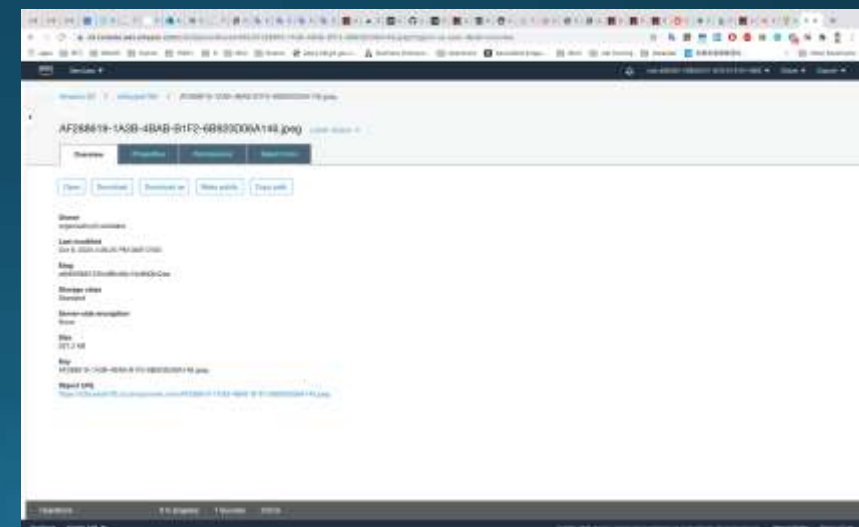
Step 8



Step 9

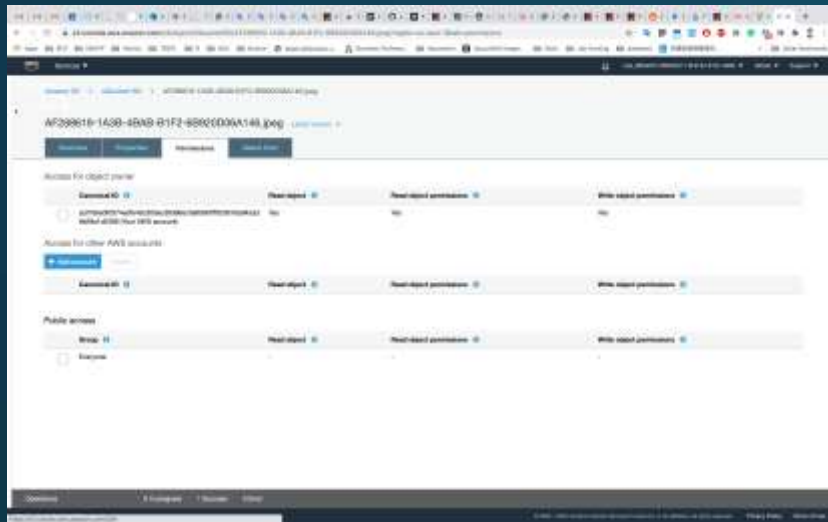


Step 10

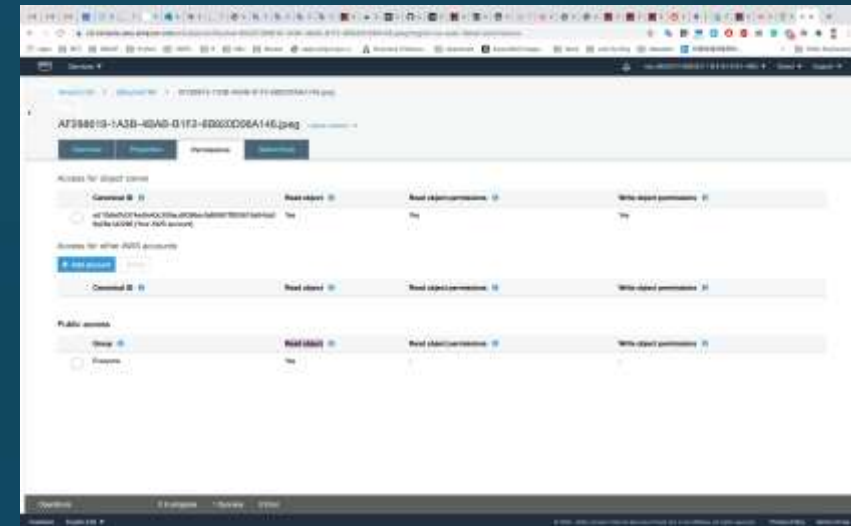


Step 11





Step 12



Step 13



Step 14

# ELASTIC LOAD BALANCER(ELB)

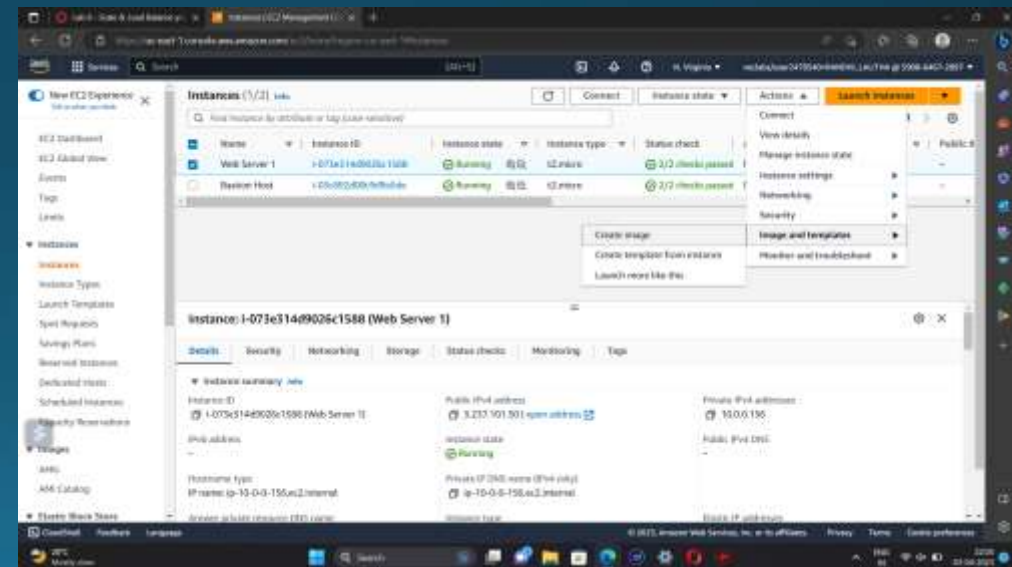
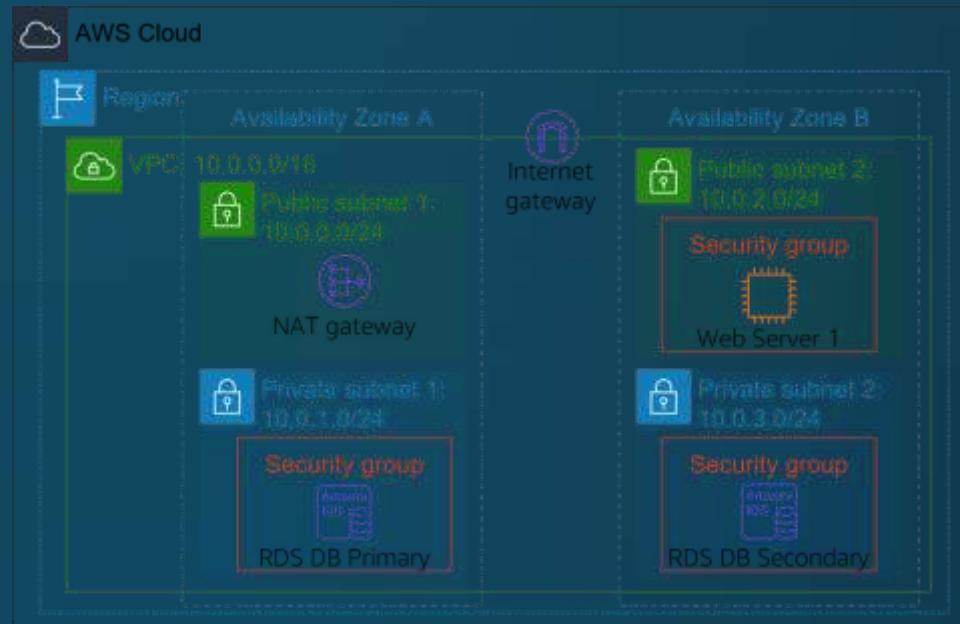
**Elastic Load Balancing** automatically distributes incoming application traffic across multiple Amazon EC2 instances

In this lab, We are provided with the given infrastructure.

Procedure:

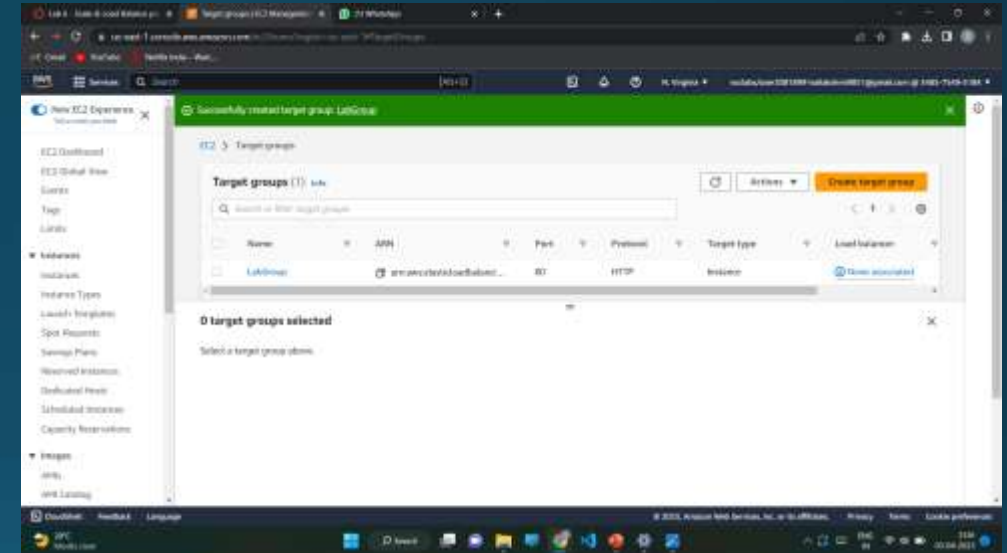
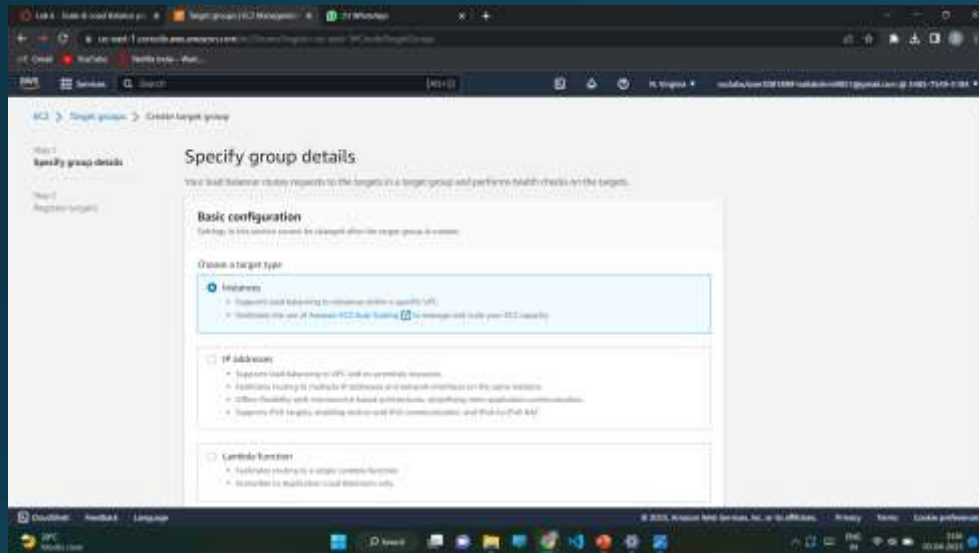
Task1: Creating an AMI for Auto Scaling

- ❖ Click start lab then click on AWS.
- ❖ You will navigate to AWS management console. Click on services and select EC2.
- ❖ Click instances. Make sure that **Status Checks** for **Web Server 1** displays 2/2 checks.
- ❖ Select Web Server 1 and in actions click images and templates > create image. Name the image and give the description.
- ❖ Click create image.

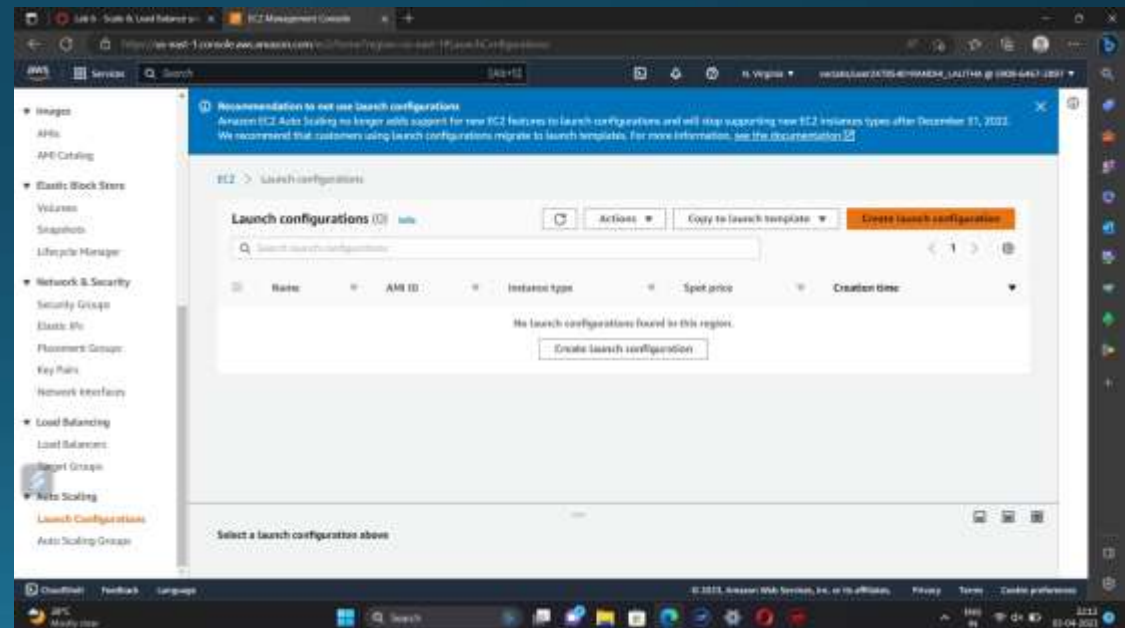
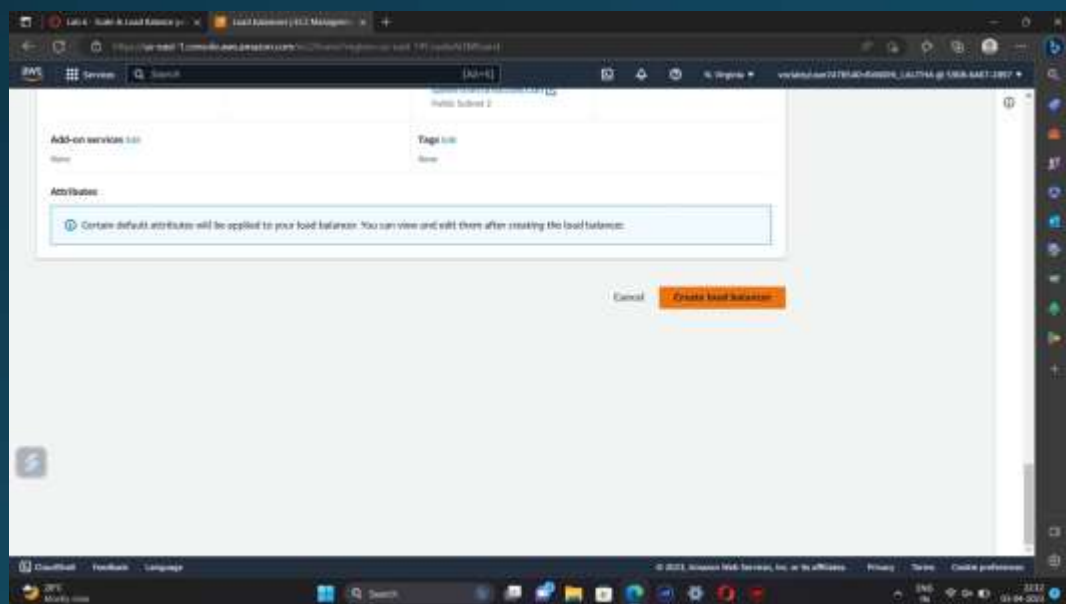
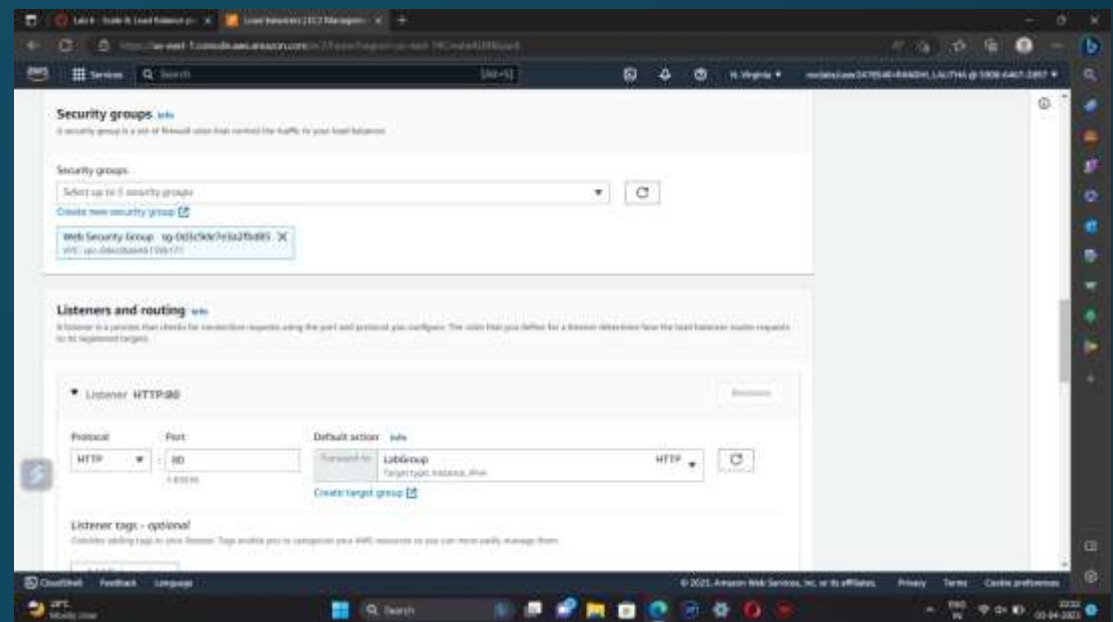
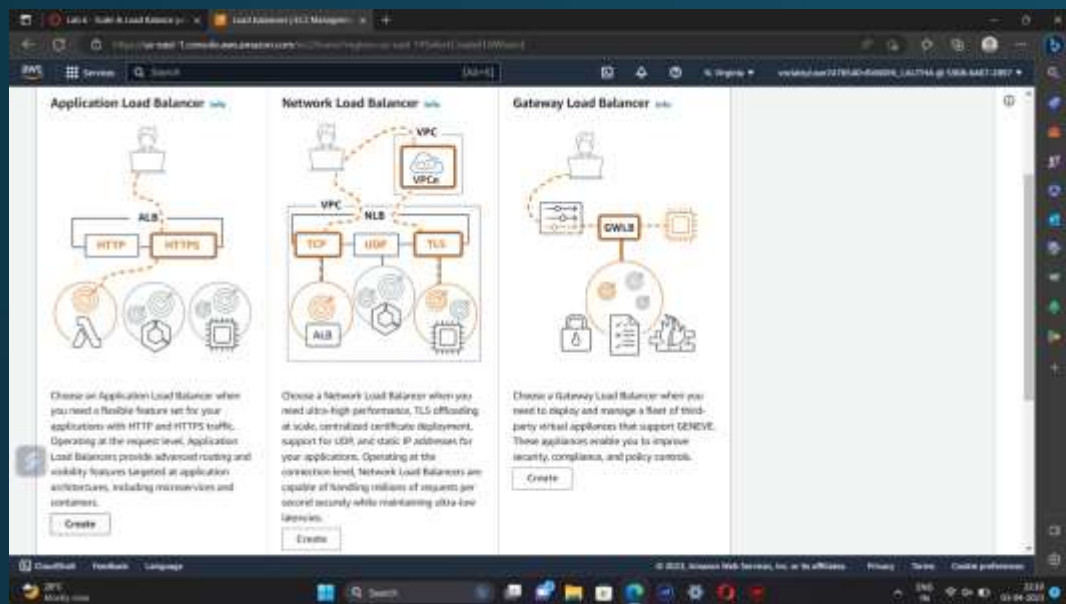


## Task 2: Creating a load balancer

- ❖ Choose Target Groups and then click on create target group.
- ❖ Select target type as instances. Name the target group. Select Lab VPC under VPC that is we are creating load balancer in Lab VPC .
- ❖ Choose next and then click on create target group.



- ❖ From the left navigation pane , select Load Balancers. Click create load balancer.
- ❖ To create a application balancer, click create under Application Load Balancer and Name it.
- ❖ In Networking mapping, select Lab VPC and specify the subnets that the load balancer should use.
- ❖ In security groups, select only Web Security Group and deselect all other than it .
- ❖ For the Listener HTTP:80 row, set the Default action to forward to **LabGroup**.

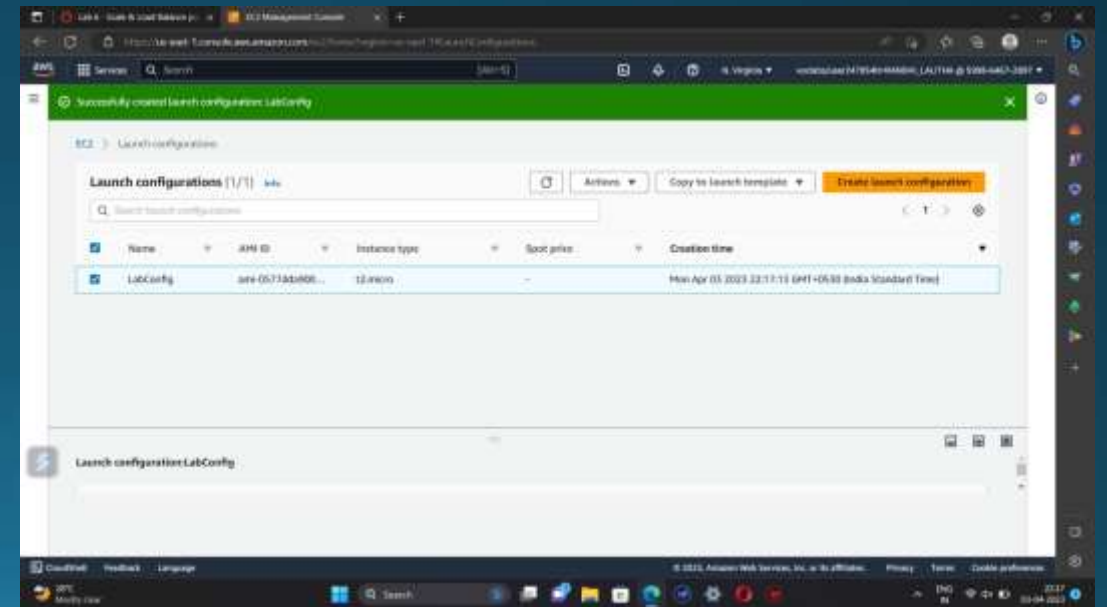
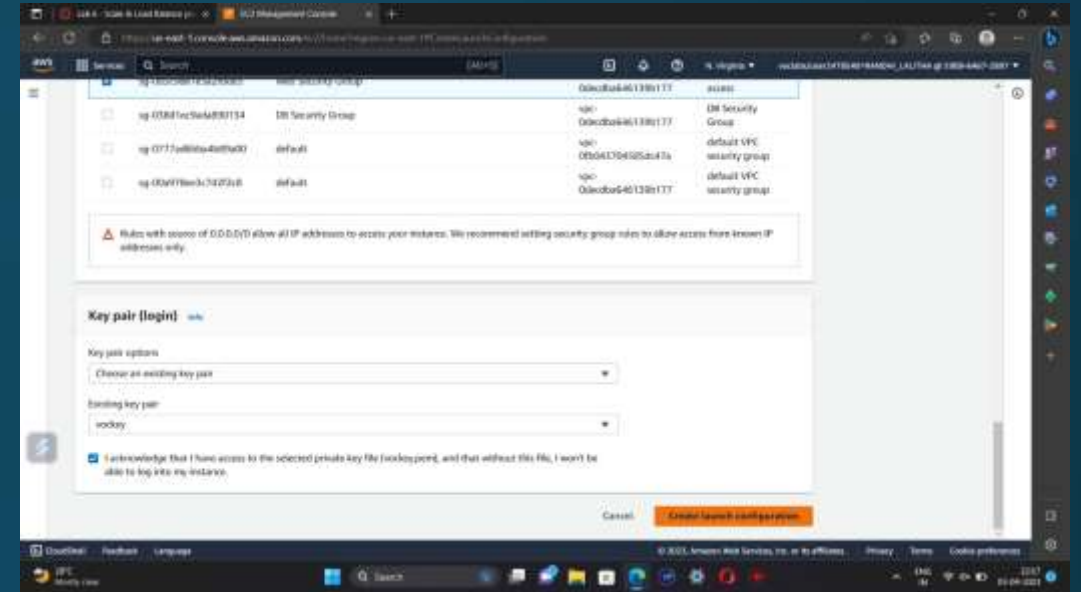




- ❖ Click create load balancer.

### Task 3: Create a Launch Configuration and an Auto Scaling Group

- ❖ In Launch Configurations, click create launch configuration.
- ❖ Name the configuration and for AMI choose web server AMI that you created in task 1.
- ❖ Select the instance type.
- ❖ Under Additional Configuration, for monitoring select Enable EC2 instance detailed monitoring within CloudWatch.
- ❖ Under security groups, choose an existing security group Web Security Group.
- ❖ Under key pair, choose an existing key pair vockey. Check I acknowledge...
- ❖ Click Create launch configuration.
- ❖ For created launch configuration, select create auto scaling group from actions.
- ❖ Name it and select Lab VPC under VPC, select the private subnets.
- ❖ Select an existing load balancer which was created earlier.
- ❖ In the **Additional settings - optional** pane, select **Enable group metrics collection within CloudWatch**





- ❖ Specify the values under Group size.
- ❖ Under **Scaling policies**, choose *Target tracking scaling policy* and name the policy. Specify metric type and target value. Then add a tag and click create auto scaling group.

The screenshot shows the 'Create Auto Scaling group' wizard in the AWS Management Console, specifically Step 6: Add tags. The browser address bar shows the URL: <https://us-east-1.console.aws.amazon.com/ec2/home?region=us-east-1#/directfrom-arg/CreateAutoScalingGroup?searchConfigurationName=LabConfig>. The AWS logo and 'Services' link are visible in the top left. The user's profile and account ID are in the top right.

**Instance scale-in protection**

Instance scale-in protection

☐ Enable instance protection from scale-in

**Step 5: Add notifications** [Edit](#)

**Notifications**

No notifications

**Step 6: Add tags** [Edit](#)

**Tags (1)**

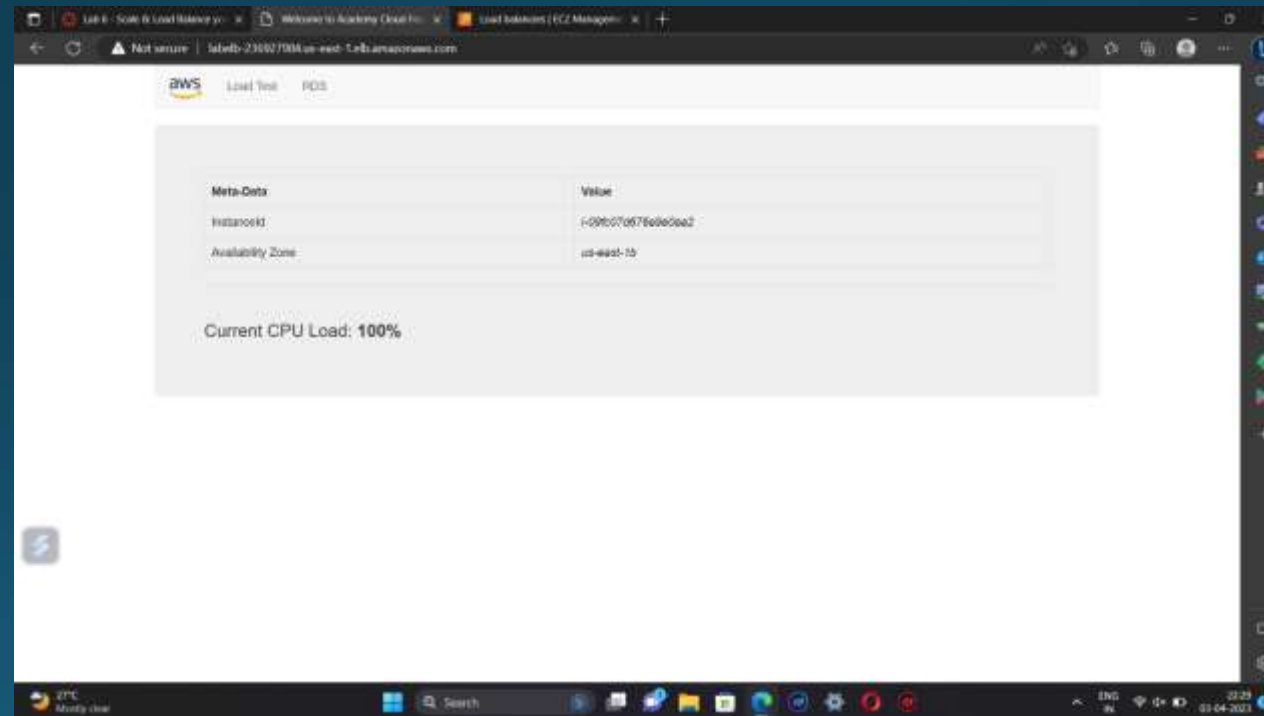
Key	Value	Tag new instances
Name	Lab Instance	Yes

[Cancel](#) [Previous](#) [Create Auto Scaling group](#)

CloudShell Feedback Language © 2023, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences 27°C Mostly clear 32.23 03-04-2023

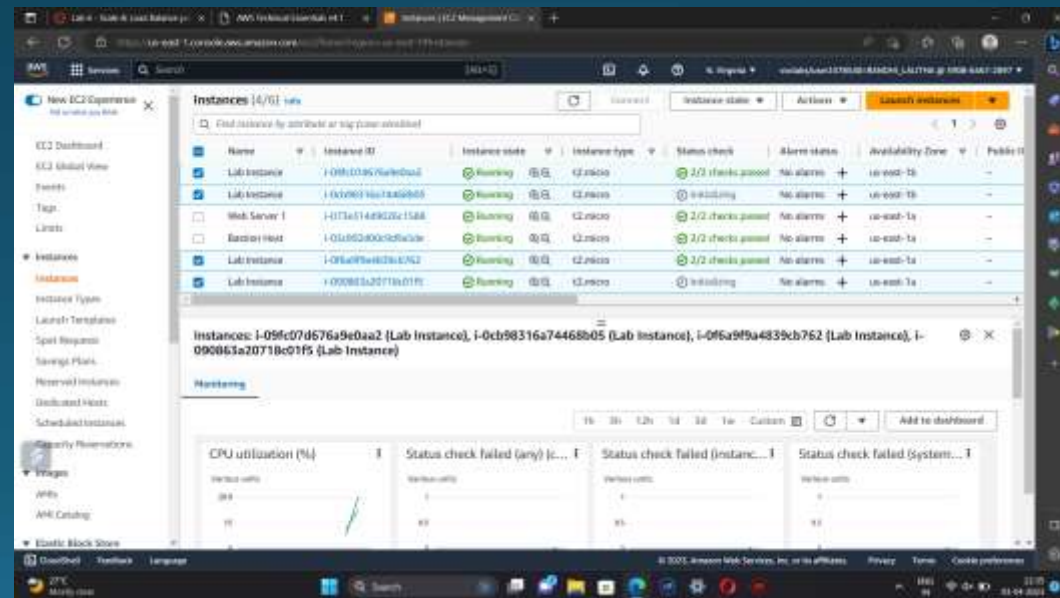
#### Task 4: Verify that Load Balancing is Working

- ❖ click **Instances**. You should see two new instances named **Lab Instance**. These were launched by Auto Scaling.
- ❖ In the labgroup target group, two **Lab Instance** targets should be listed for this target group. Wait until the **Status** of both instances transitions to *healthy*.
- ❖ Now copy the DNS name of the created load balancer making sure to omit "(A Record)". and paste it in a new browser
- ❖ The application should appear in your browser. This indicates that the Load Balancer received the request, sent it to one of the EC2 instances, then passed back the result.



## Task 5: Test Auto Scaling

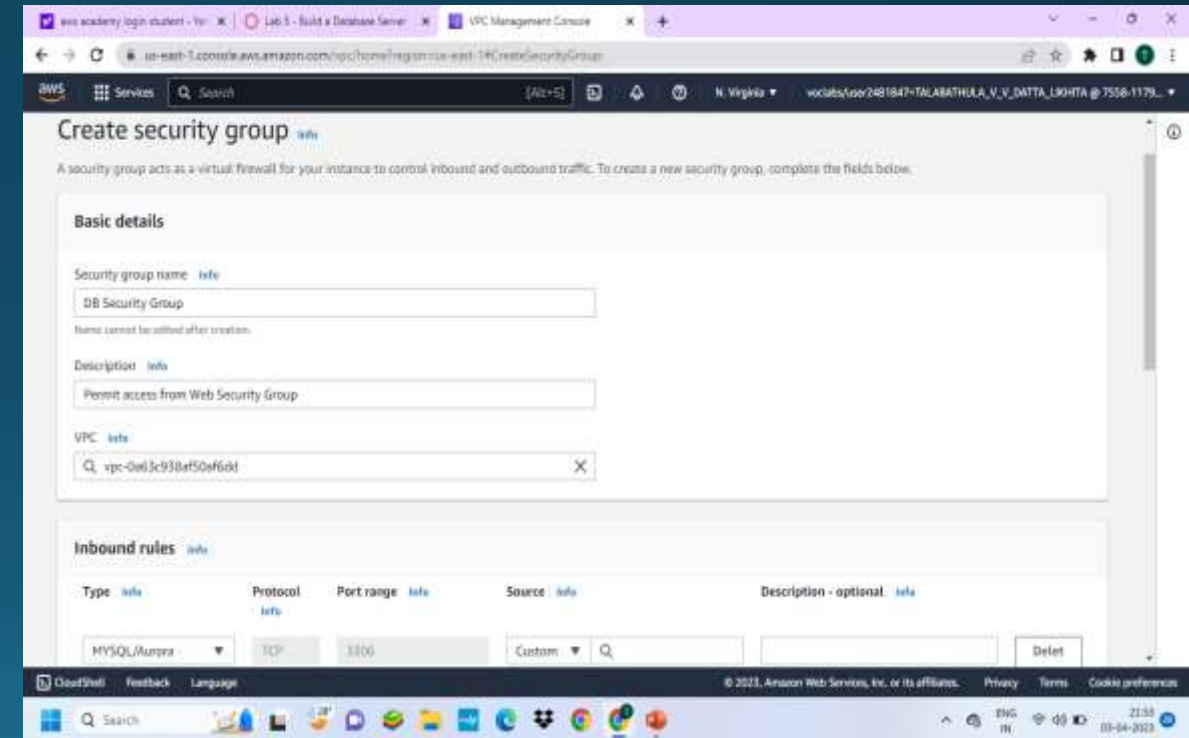
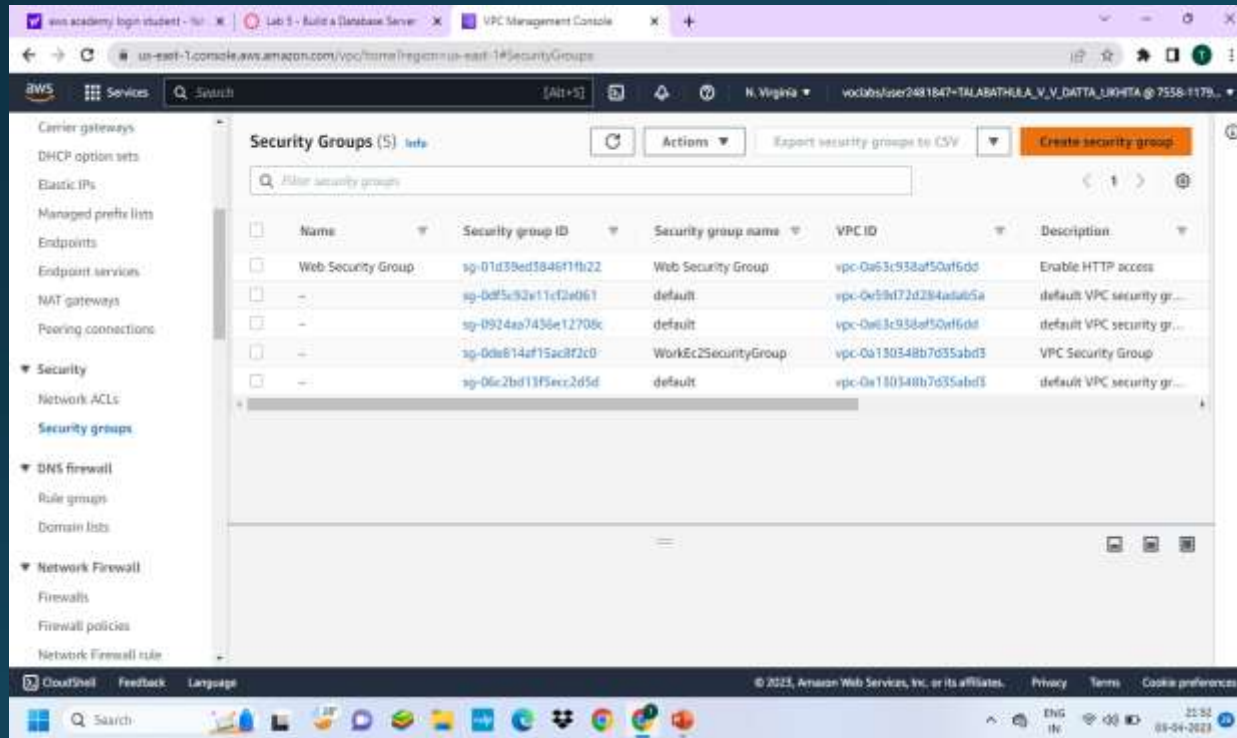
- ❖ On the **Services** menu, click **CloudWatch**. In the left navigation pane, choose **All alarms**. Two alarms will be displayed. These were created automatically by the Auto Scaling group.
- ❖ From services select EC2 and choose Auto Scaling Groups and select Lab Auto Scaling Group which you created.
- ❖ choose the **Automatic Scaling** tab. Select **LabScalingPolicy** and from actions change the target value to 50. click update.
- ❖ To go cloudwatch and click all alarms and verify.
- ❖ Click the **OK** alarm, which has *AlarmHigh* in its name. Return to the browser tab with the web application. Click **Load Test** beside the AWS logo. This will cause the application to generate high loads.
- ❖ You should see the **AlarmHigh** chart indicating an increasing CPU percentage. Once it crosses the 60% line for more than 3 minutes, it will trigger Auto Scaling to add additional instances.
- ❖ In EC2 instances, you notice that more than two instances labeled **Lab Instance** should now be running.
- ❖ Finally terminate the Web Server 1.



# RELATIONAL DATABASE SERVICE (RDS)

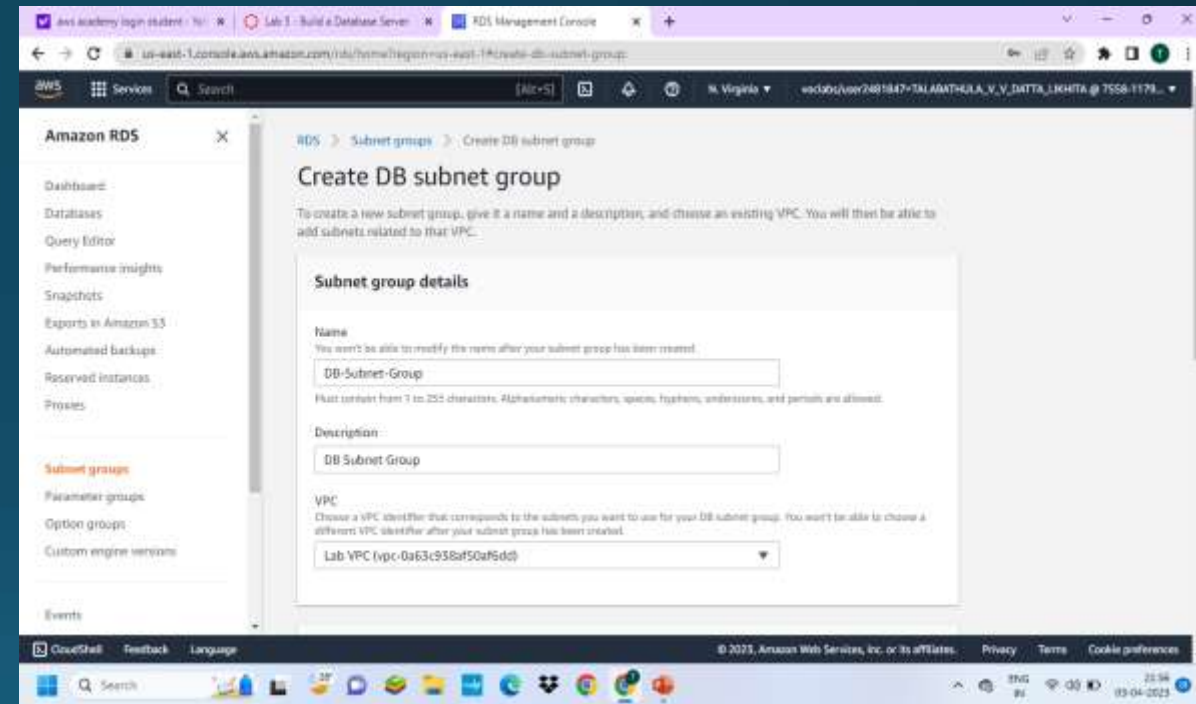
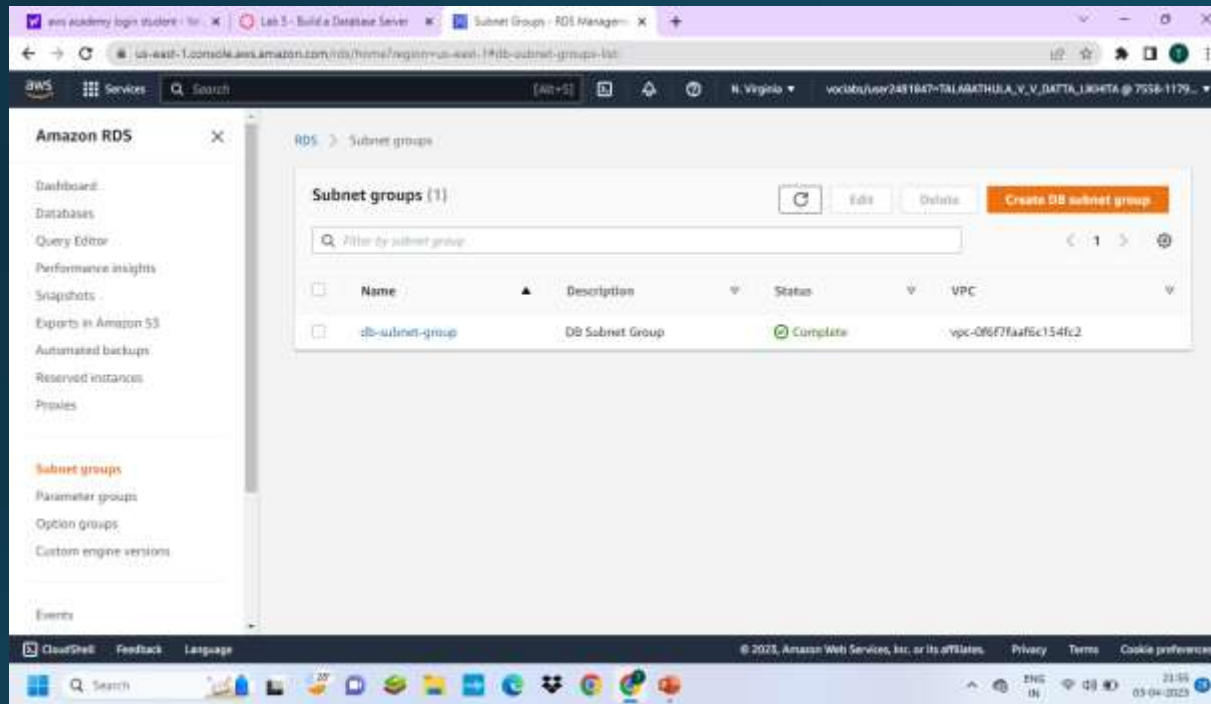
## Step 1: Create a Security Group for the RDS DB Instance.

aws management console → vpc → security groups → choose create security group → add inbound rule → create security group.



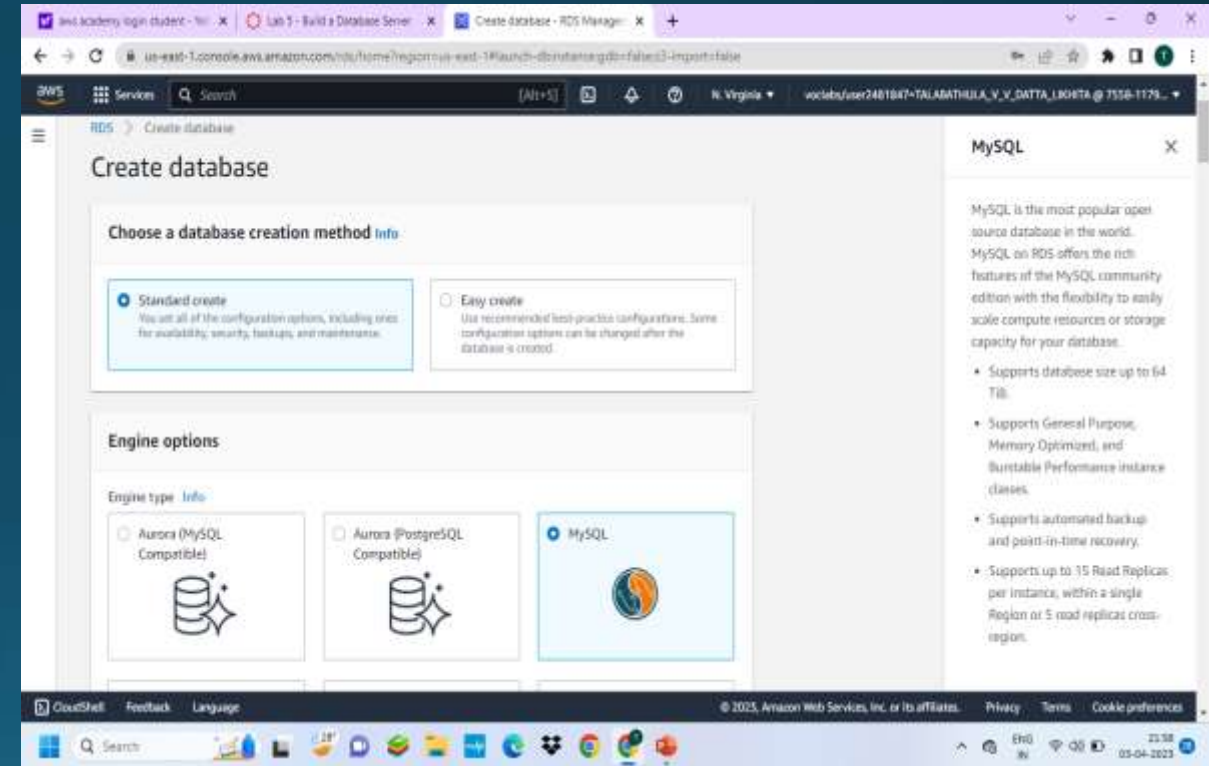
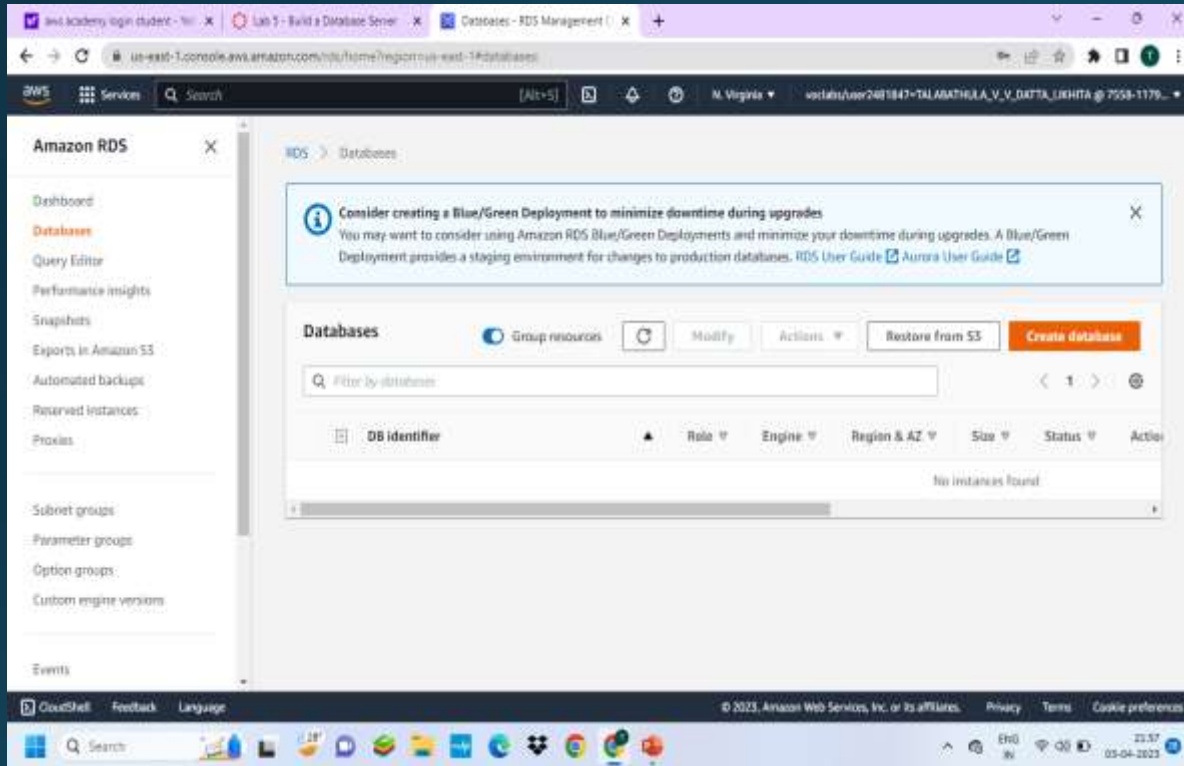
## Step 2 : Create a DB Subnet Group.

Rds → subnet groups → choose create DB subnet group → add subnets → create DB subnet group.



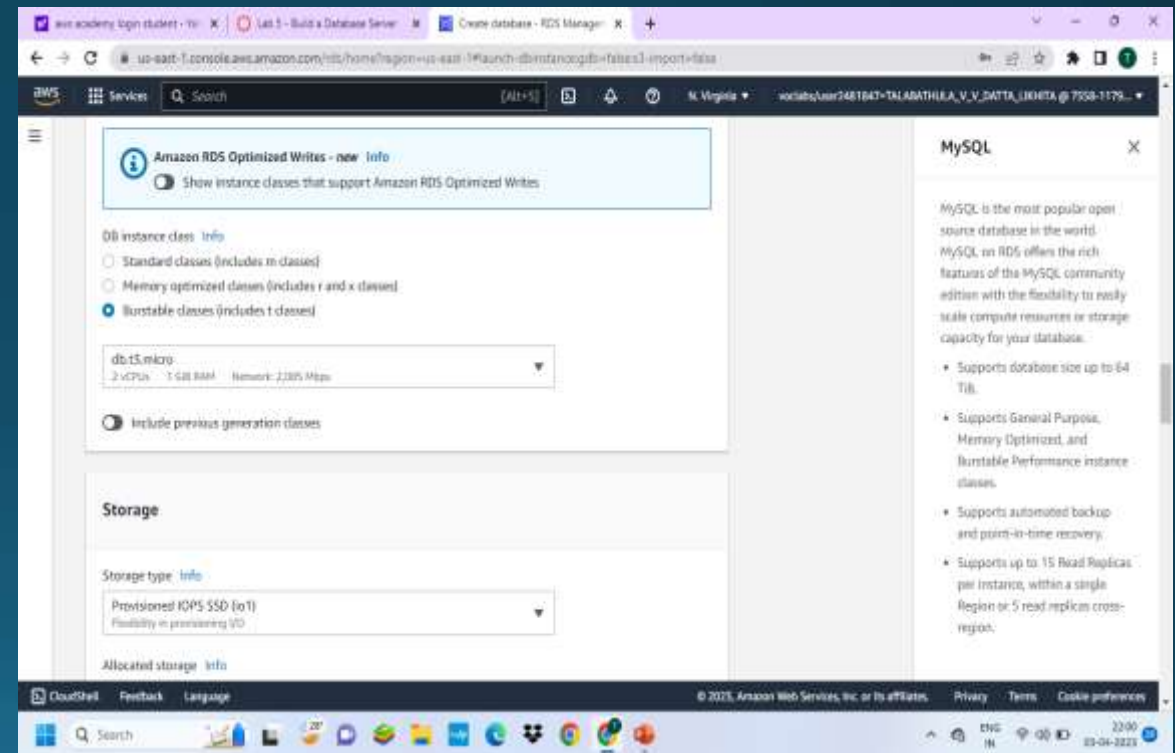
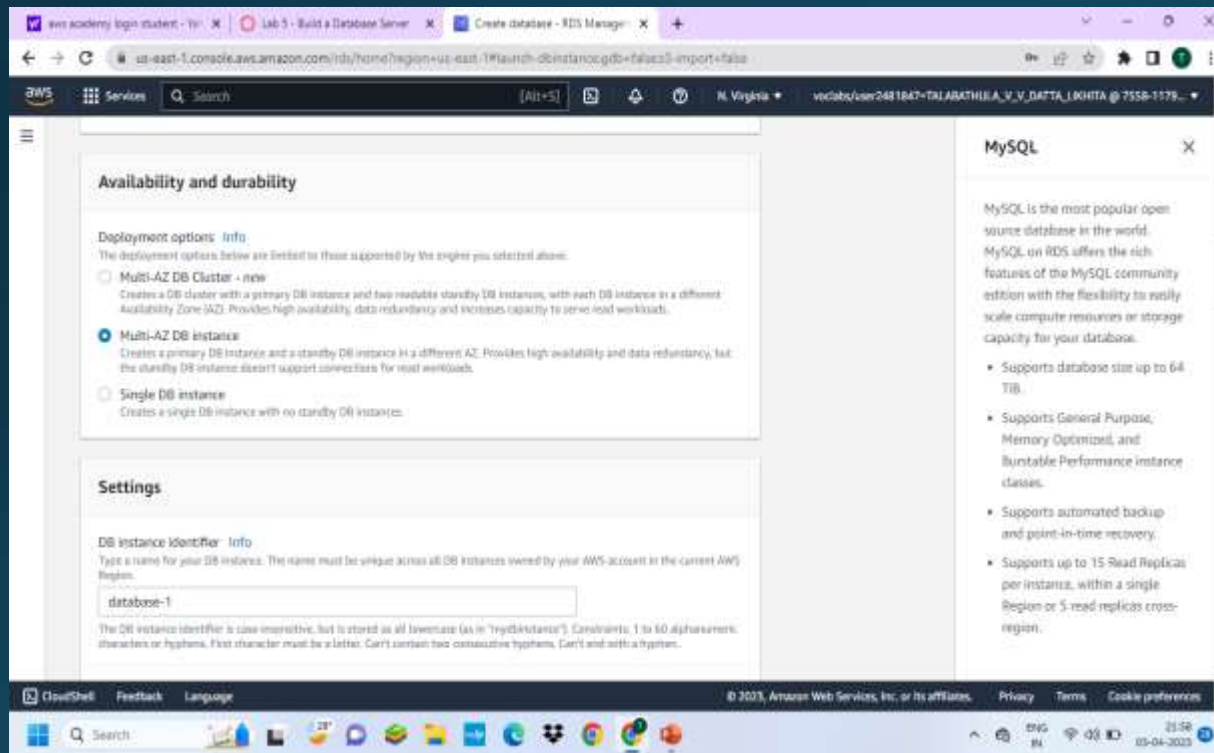


**Step 3: In the left navigation pane, choose Databases → choose create database → MYSQL**





**Step 4: In Availability and durability ,choose Multi –AZ DB instance then configure settings , DB instance class, Storage, connectivity, choose existing vpc security group and setup additional configuration.**



**Step 5: Wait until Info changes to Modifying or Available.**  
**Scroll down to the Connectivity & security section and copy the Endpoint field.**

The screenshot shows the AWS RDS console for a database instance named 'lab-db'. The instance is in the 'Available' status. The 'Connectivity & security' tab is selected, and the 'Endpoint & port' section is visible, showing the endpoint 'lab-db.us-east-1.rds.amazonaws.com' and port '3306'.

**Summary**

DB identifier	CPU	Status	Class
lab-db	2.63%	Available	db.t3.micro

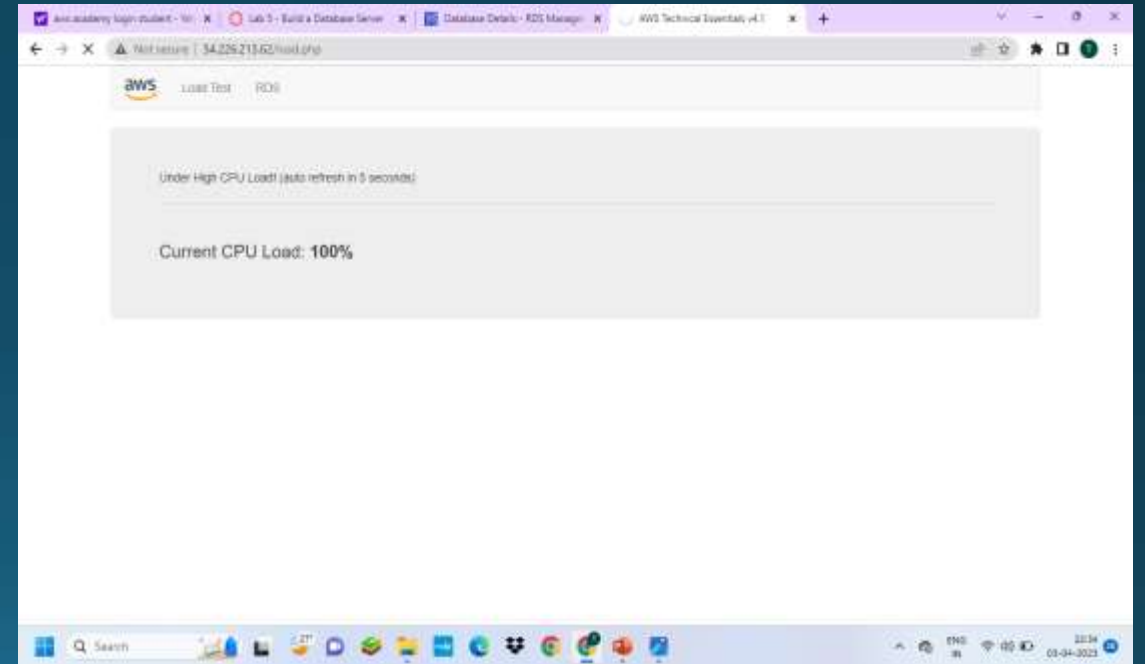
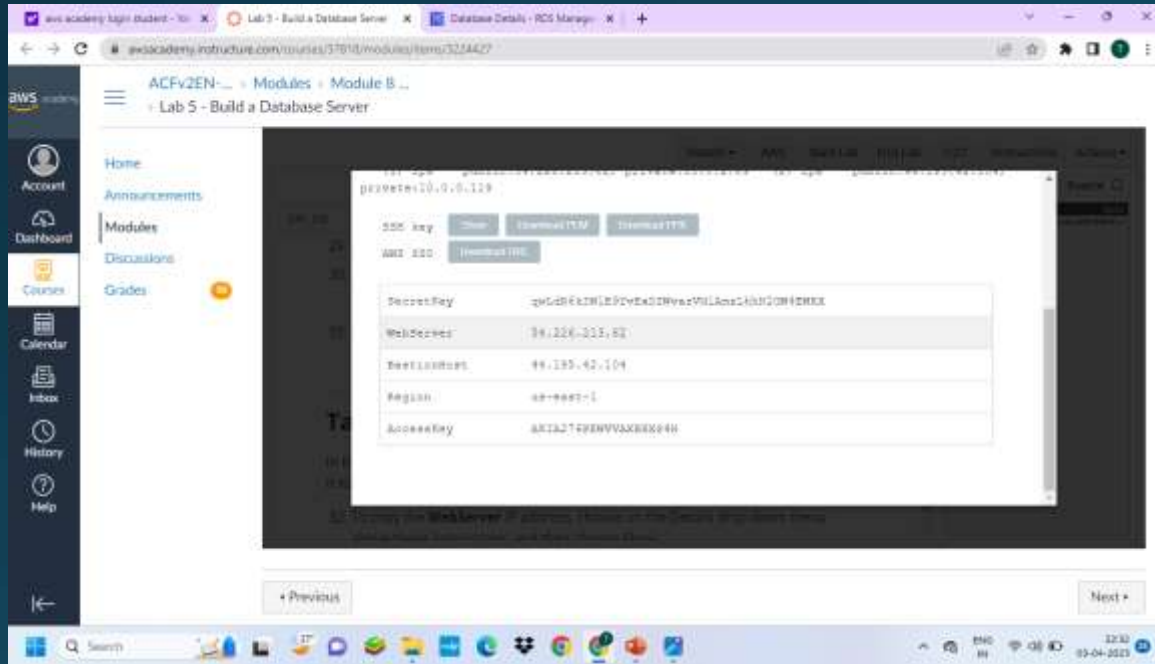
Role	Current activity	Engine	Region & AZ
Instance	0 Connections	MySQL Community	us-east-1a

**Connectivity & security**

Endpoint & port	Networking	Security
Endpoint lab-db.us-east-1.rds.amazonaws.com:3306	Availability Zone us-east-1a	VPC security groups sg-xxxxxx

## Step 6 : Interact with Your Database.

On Details , copy the **WebServer** IP address. Open a new web browser tab, paste the WebServer IP address and press Enter. The web application will be displayed, showing information about the EC2 instance.



**Step 7 : Choose the RDS link at the top of the page and configure the settings.**

aws academy login student - Yahoo! | Lab 5 - Build a Database Server | Database Details - RDS Manager | AWS Technical Essentials v4.1

← → ↻ ⚠ Not secure | 54.226.213.62/rds.php

aws Load Test RDS

Endpoint

Database

Username

Password

Submit

27°

Search

22:36 03-04-2023

**Step 8:** After a few seconds the application will display an **Address Book**.  
The Address Book application is using the RDS database to store information.

aws academy login student - Yeh x Database Details - RDS Manager x Lab 5 - Build a Database Server x AWS Technical Essentials v4.1 x

← → ↻ ⚠ Not secure | 54.226.213.62/rds.php

aws Load Test RDS

## Address Book

Last name	First name	Phone	Email	Admin	
				<a href="#">Add Contact</a>	
Doe	Jane	010-110-1101	<a href="mailto:janed@someotheraddress.org">janed@someotheraddress.org</a>	<a href="#">Edit</a>	<a href="#">Remove</a>
Johnson	Roberto	123-456-7890	<a href="mailto:robertoj@someaddress.com">robertoj@someaddress.com</a>	<a href="#">Edit</a>	<a href="#">Remove</a>

Windows taskbar: Search, 27°, ENG IN, 22:38, 03-04-2023

THANK YOU