

# PRACTICAL IMPLEMENTATION ON AWS

20A31A05E0

## DEPLOYMENT OF EC2 INSTANCE

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

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

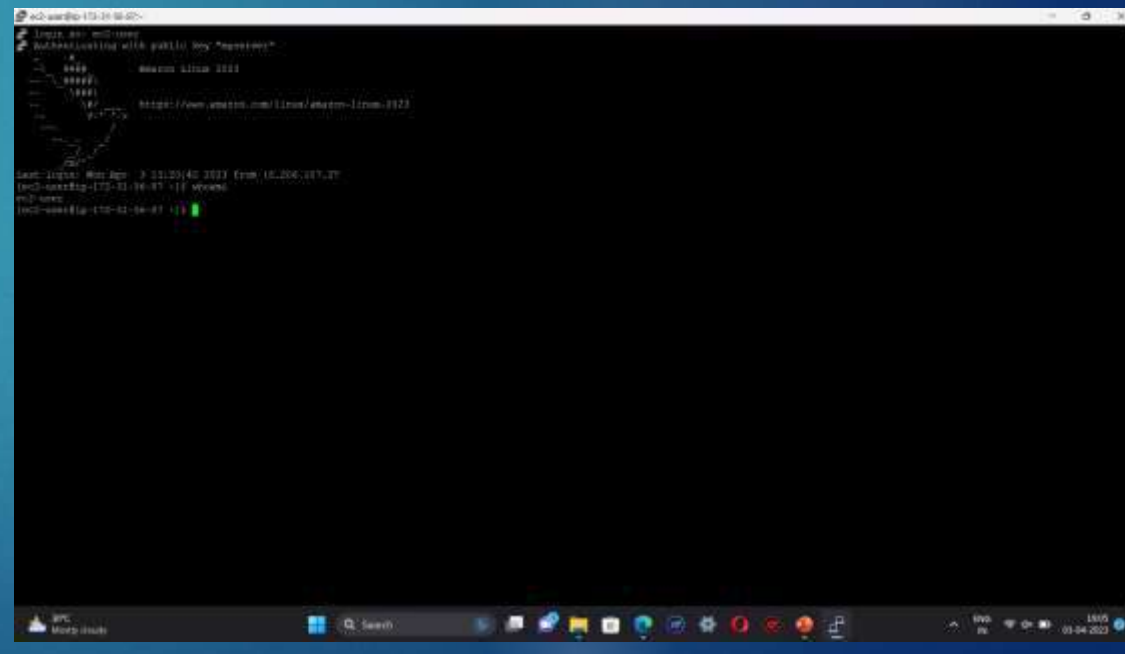
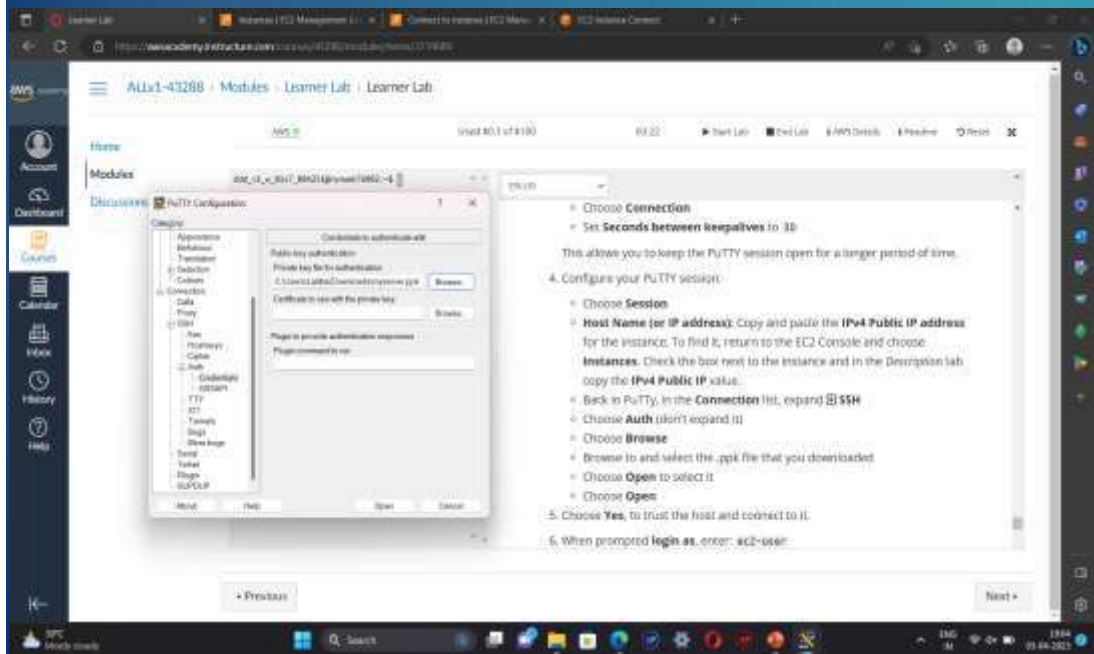
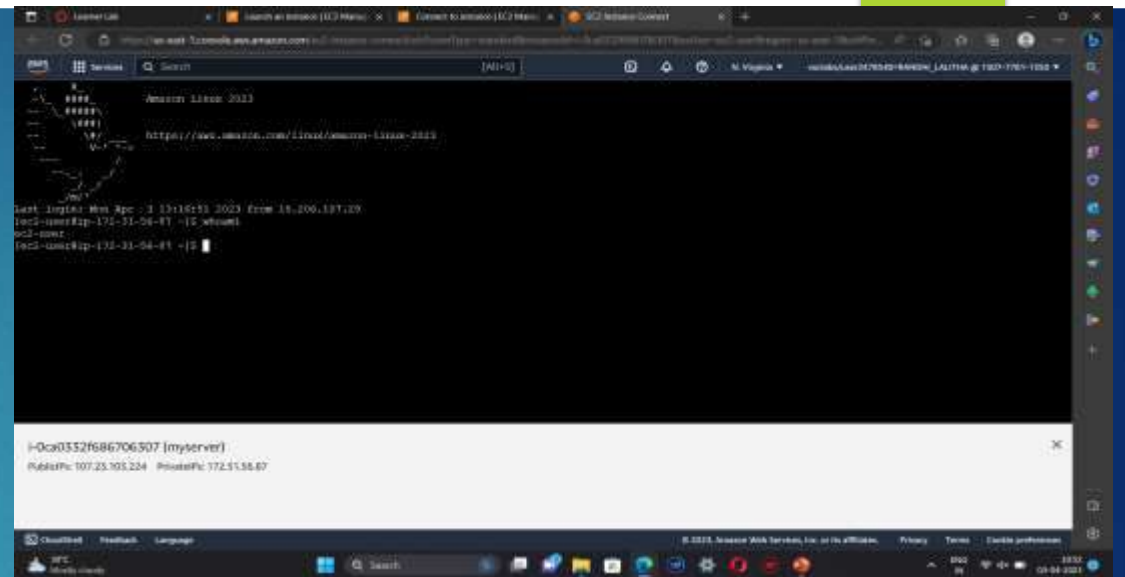
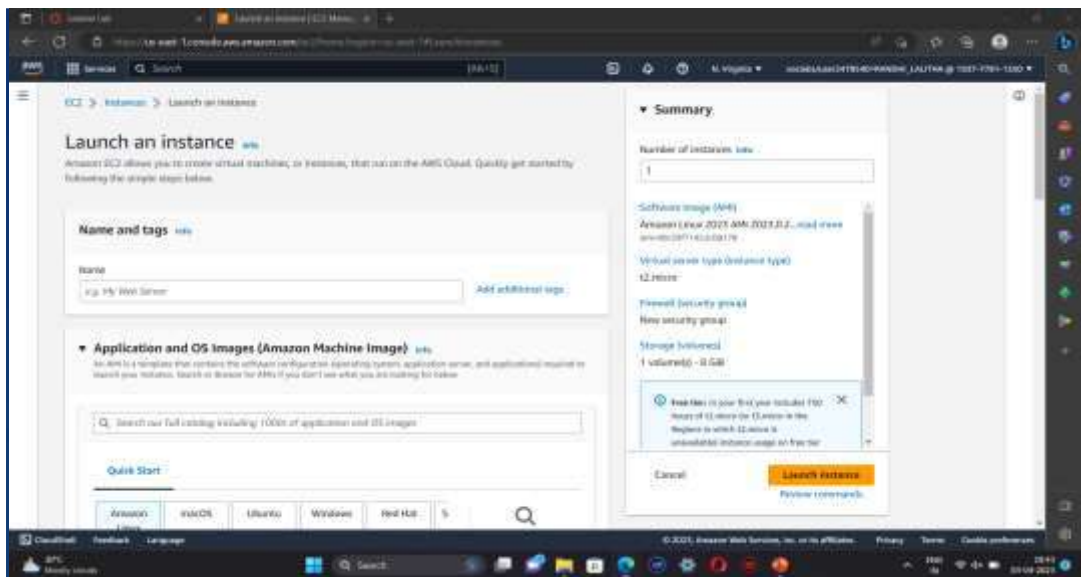
Step-3: For linux-select ppk key and for windows server-select pem key.

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

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. This will redirects you to the windows server.

Step-6: Terminate the instances



## DEPLOYMENT OF AMAZON LIGHTSAIL

- 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:

Must be unique within each AWS Region in your Lightsail account.

Must contain 2 to 255 characters.

Must start and end with an alphanumeric character or number.

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.



Key-only tags

Version 1 x Customer 1

Add a tag key and press Enter.

Save Cancel

- 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.



The image shows a 'Key-value tags' interface. It has two input fields: 'Key' with the value 'Project' and 'Value' with the value 'Earth'. An arrow points from the Key field to the Value field. To the right of the fields are two circular icons: a red one with a diagonal line (cancel) and a green one with a checkmark (save). A mouse cursor is hovering over the green save icon.

## 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





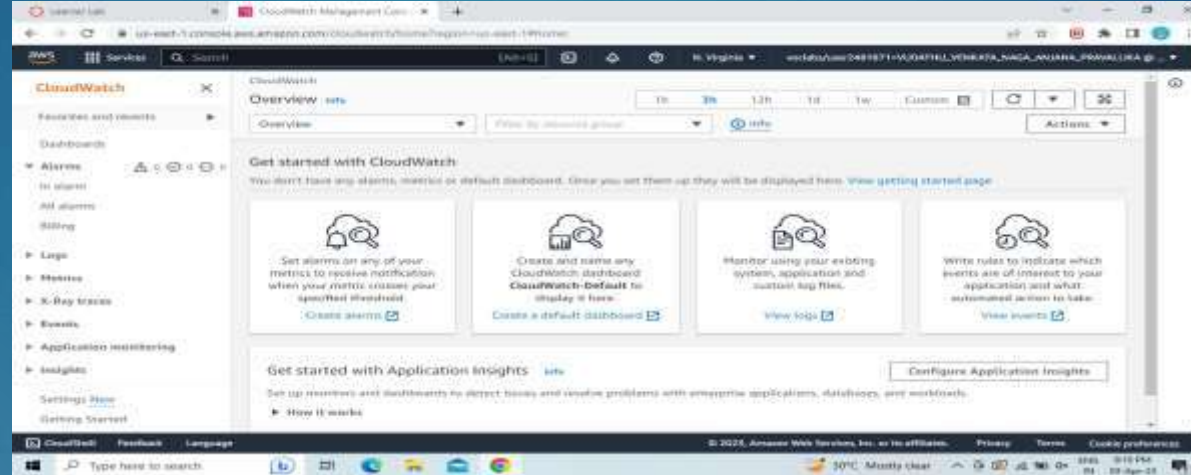
100

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

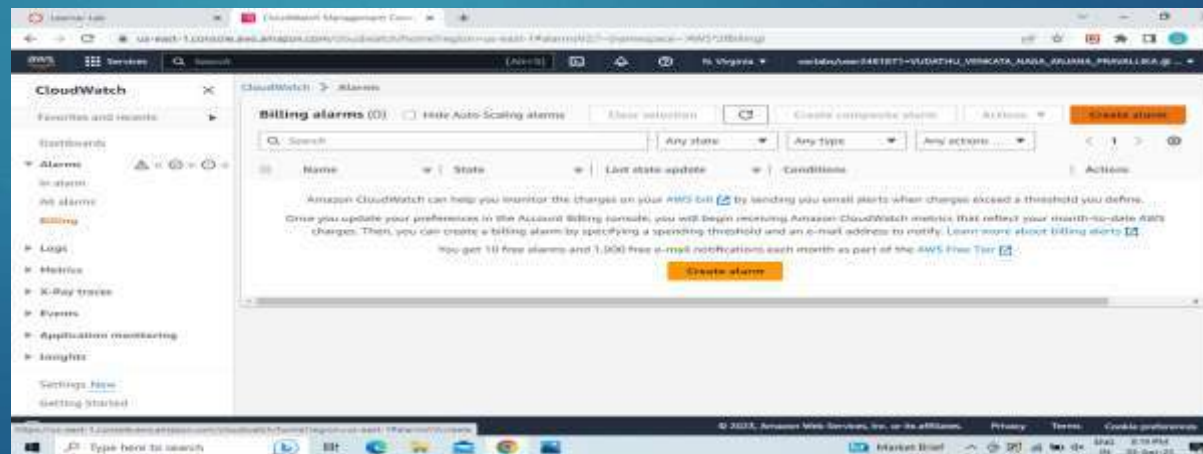
A screenshot of a terminal window titled "WordPress-512MB-Ireland-1 - Terminal | Lightsail - Google Chrome". The browser's address bar shows a secure connection to "https://lightsail.aws.amazon.com/ls/terminal/eu-west-1/WordPress-512MB-Ireland-1?protocol...". The terminal output displays the Ubuntu 16.04.4 LTS login banner, followed by a system restart requirement message and the Bitnami logo. Below the logo, it says "Welcome to the Bitnami WordPress 4.9.6-0 \*\*\*", provides documentation links at "https://docs.bitnami.com/aws/apps/wordpress/" and "https://docs.bitnami.com/aws/", and forum links at "https://community.bitnami.com/". It also shows the last login time as "Fri Jun 15 19:57:10 2018 from [redacted]" and instructions to run commands as administrator using "sudo". The prompt "bitnami@ip-[redacted]:~\$" is visible at the bottom. The terminal window has a dark background with light green text. The browser interface includes standard Windows taskbar icons and a status bar at the bottom with the WordPress icon and title "WordPress-512MB-Ireland-1".

# DEPLOYEMENT OF AMAZON CLOUDWATCH

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



2.Then Click on CREATE ALARM.



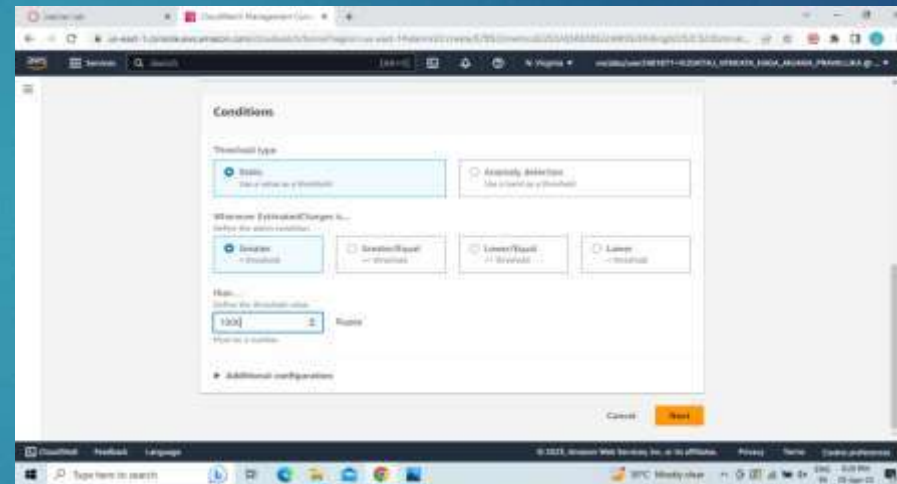
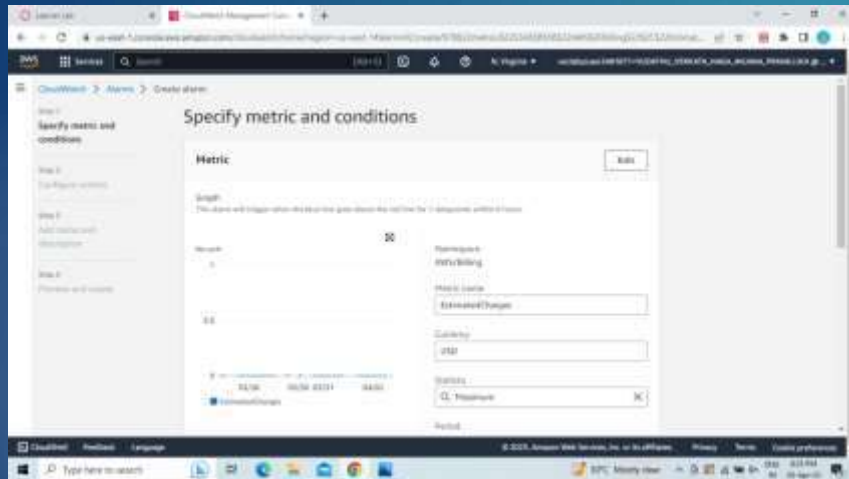
3. Then follow the steps.

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

Change the Currency to Rupee.

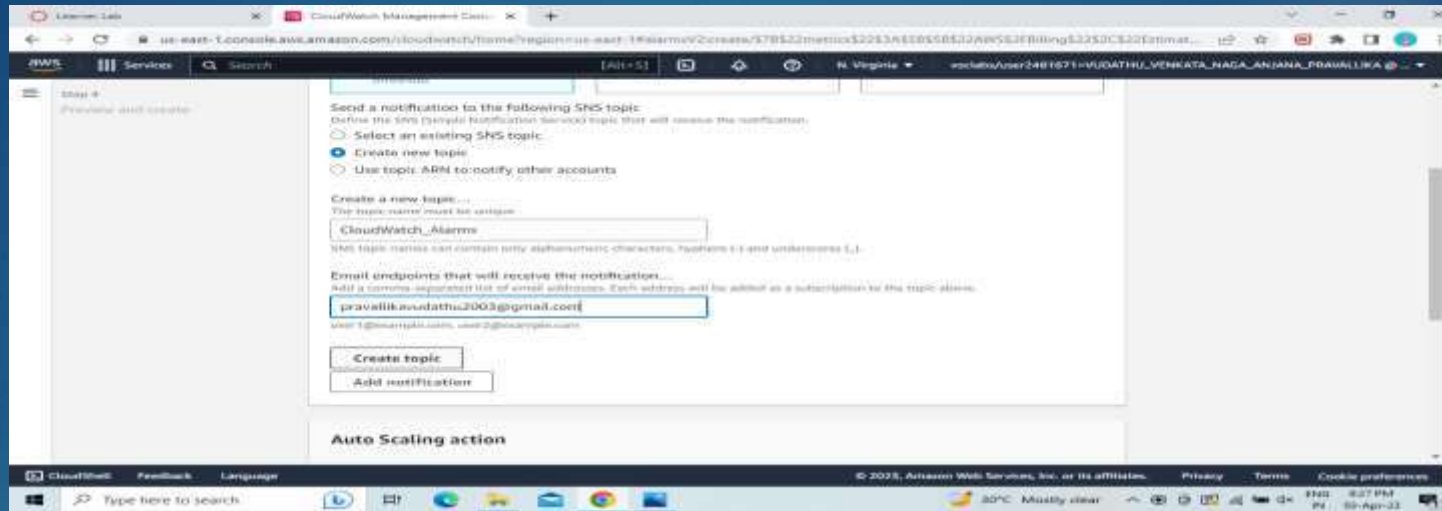
In the Conditions section choose the EstimatedCharges like Greater/GreaterEqual/Lowerequal/Lower and also define the threshold value.

4. Click on Next.

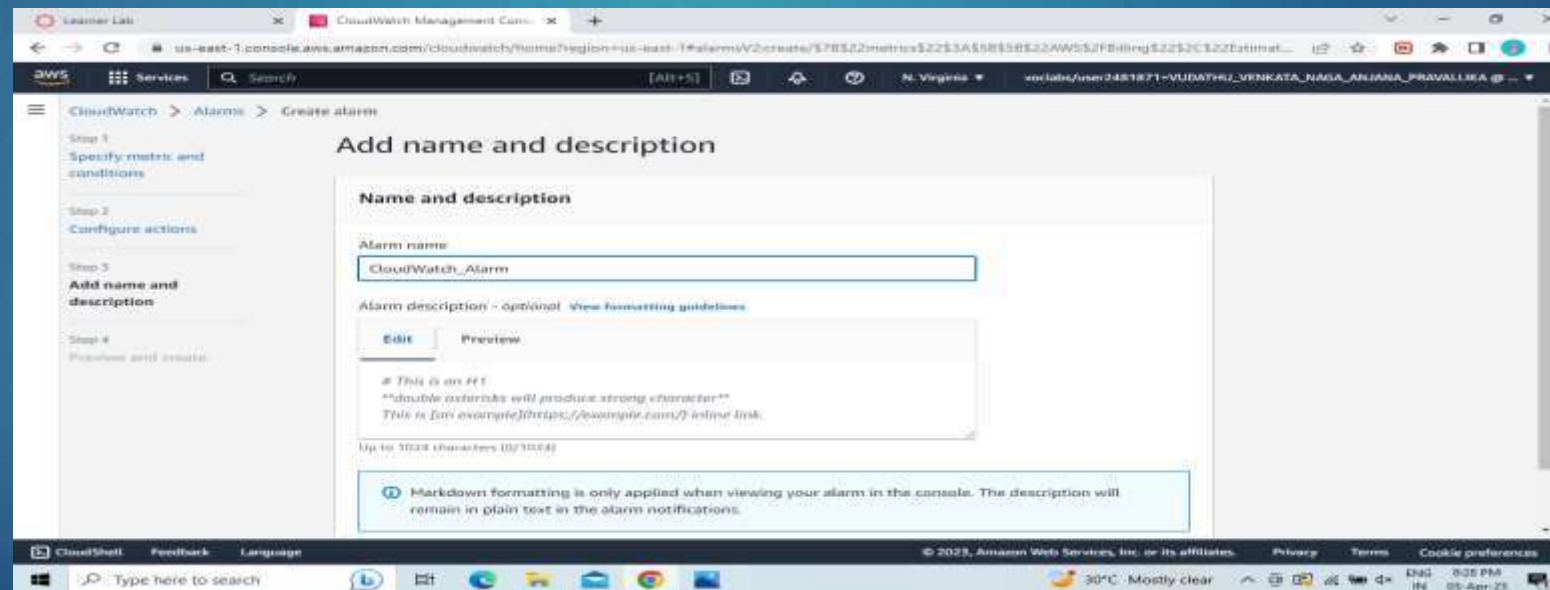


5. Now for Configure Actions choose Create new topic. Give a name to the topic and enter your email to receive a notification. Click on

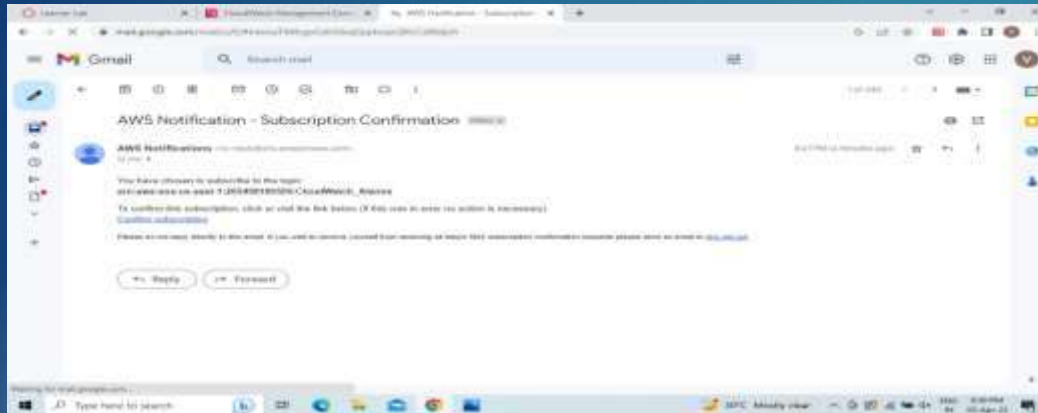




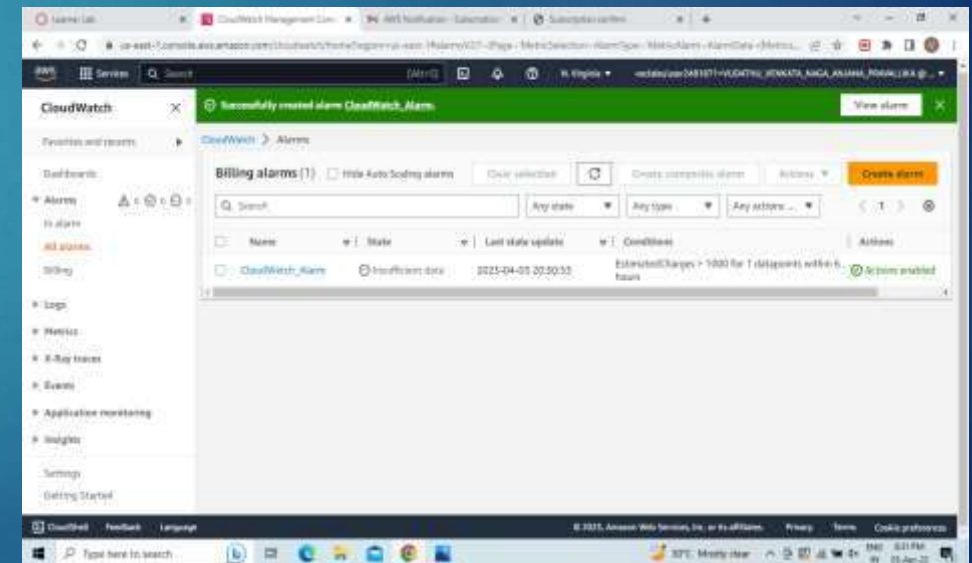
6. Give a name to your Alarm and Click on next



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



8.Preview the details you have entered .  
9.Click on Create alarm. This will Create your Alarm.

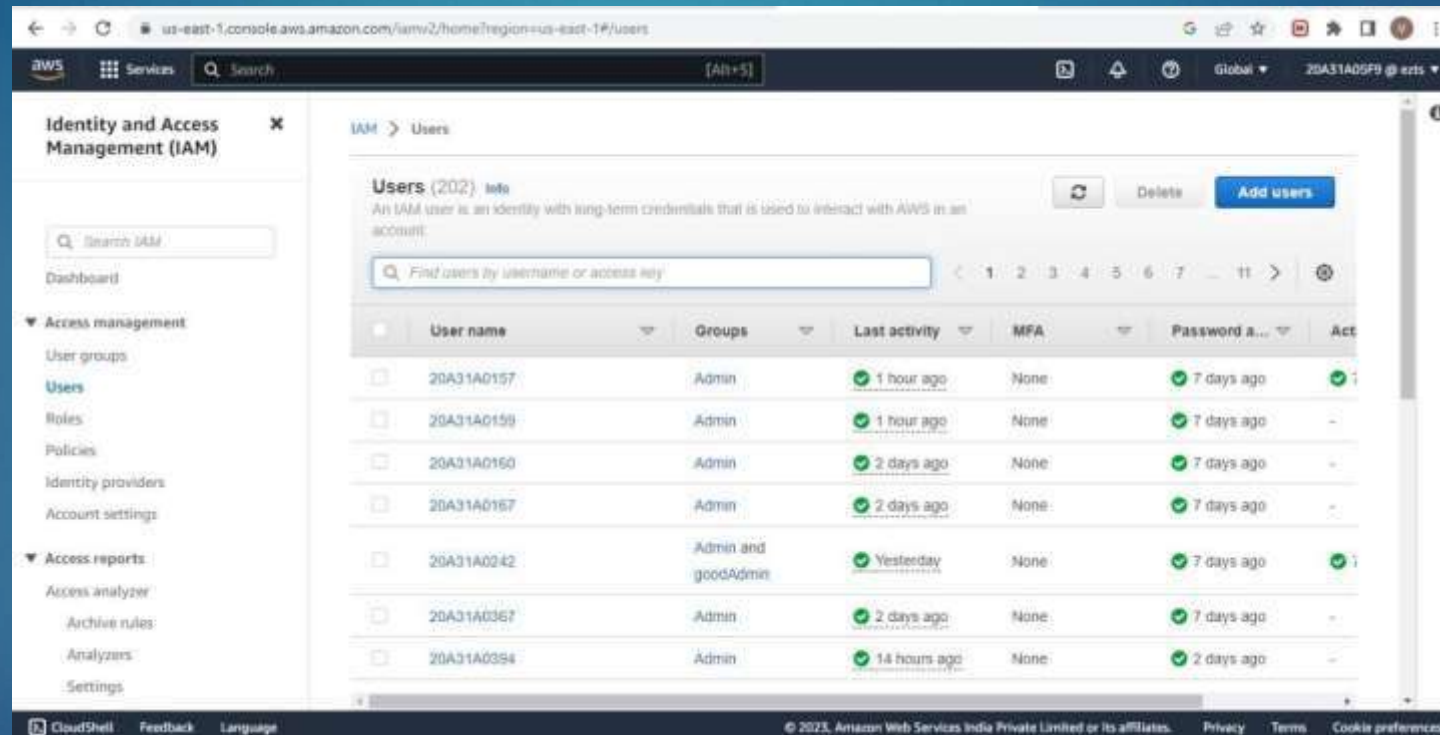


## DEPLOYMENT OF AWS COMMAND LINE INTERFACE

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

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

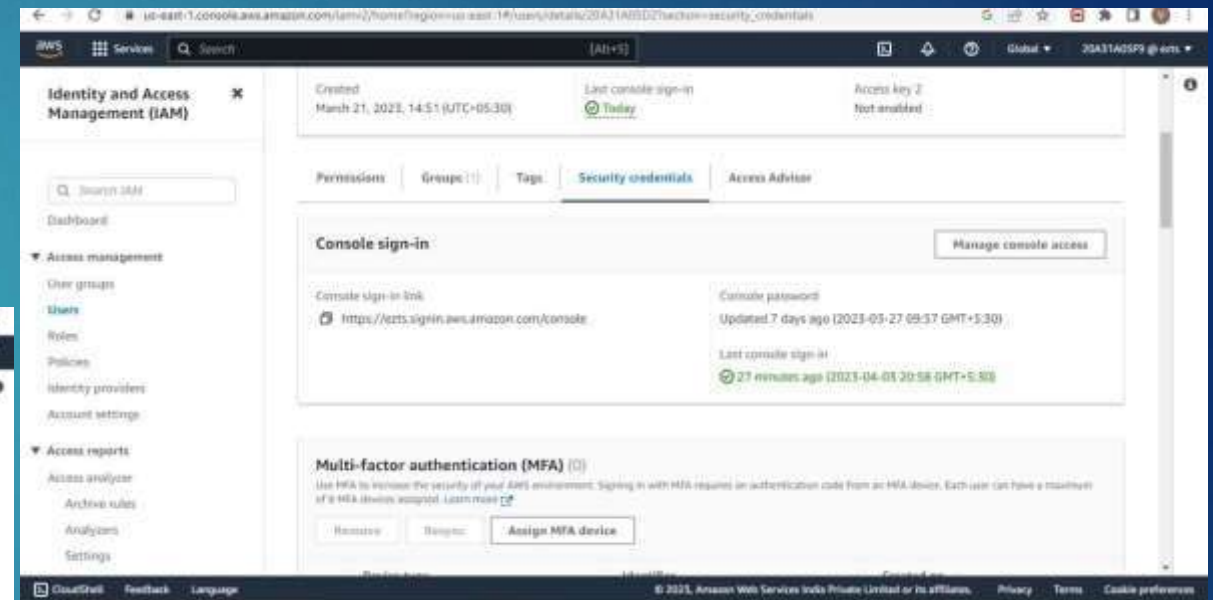
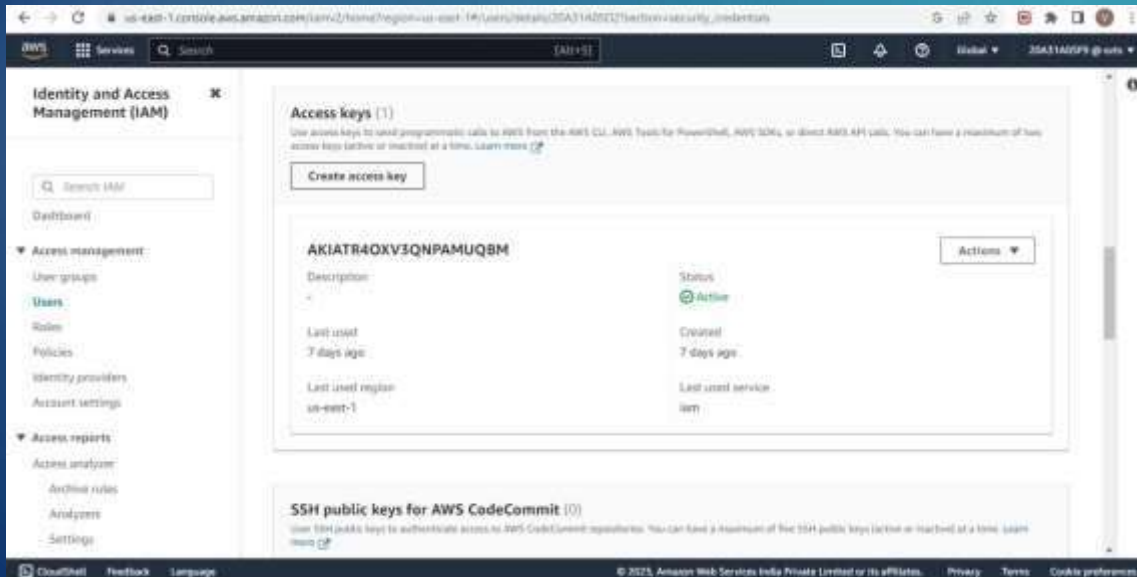
STEP 3 - In the navigation pane ,select Users

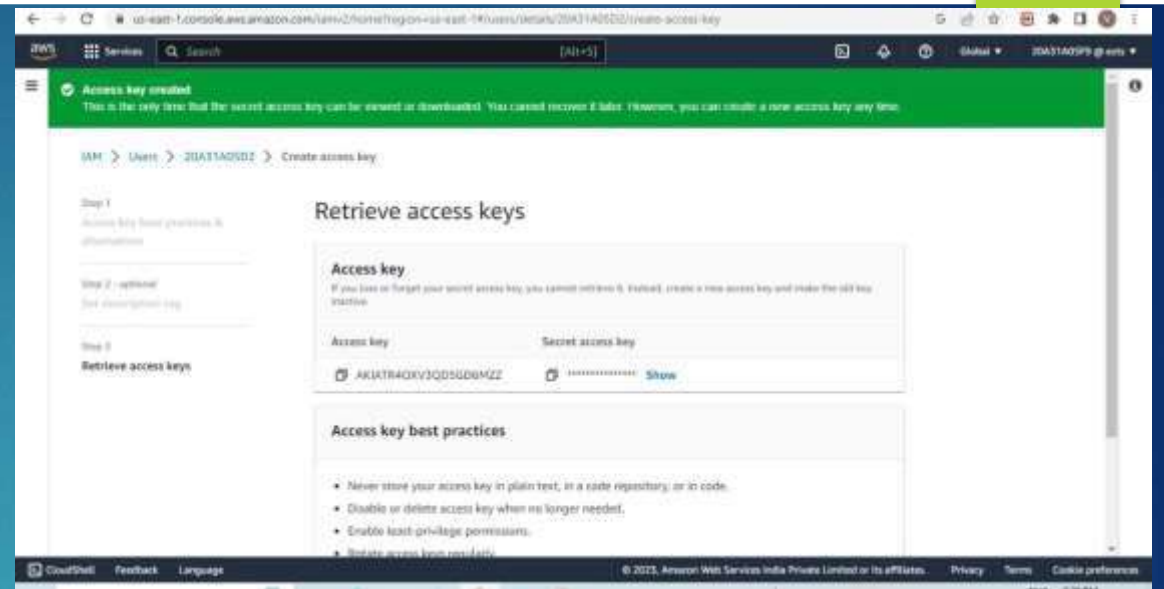
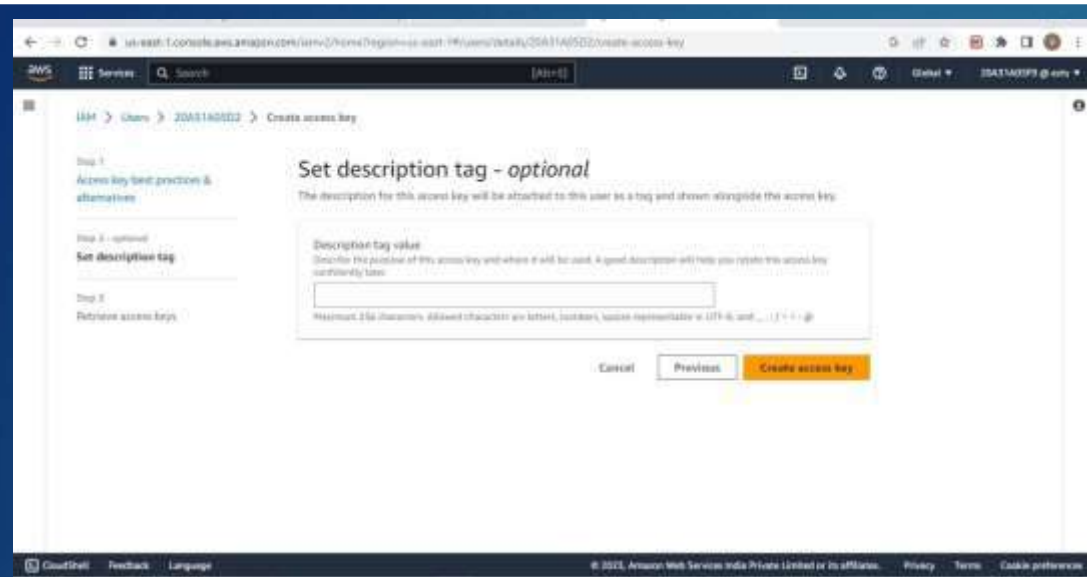


STEP 4 - In the users select the name of the user whose access keys you want to create.

STEP 5 - Click on Security Credentials tab.

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





STEP 6 – Now you can use this access key to configure CLI

STEP 7 - 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.

100

- 100

Lab 4 - Working with EBS

Dashboard | EC2 Management | us-east-1.console.aws.amazon.com/ec2/home?region=us-east-1#Home

Resources

You are using the following Amazon EC2 resources in the US East (N. Virginia) Region:

Resource	Count	Details
Instances (running)	2	Auto Scaling Groups, API Error, Dedicated Hosts
Elastic IPs	0	Instances, Key pairs
Load Balancers	0	API Error, Placement groups
Snapshots	0	Volumes

Launch instance

Launch Instance

Service health

Region: US East (N. Virginia)

Status: This service is operating normally

Account attributes

Supported platforms

- VPC
- Default VPC
- vpc-d033b060743f36e5

Settings

- EB encryption
- Zones
- EC2 Serial Console
- Default credit specification
- Console experience

Explore AWS

Amazon GuardDuty Malware Protection

GuardDuty now provides agentless malware detection in Amazon EC2 & EC2 container workloads. Learn more

Save up to 90% on EC2 with Spot Instances

Optimize price performance by combining EC2 Spot Instances with Amazon S3 and Amazon ElastiCache.

Lab 4 - Working with EBS

Instances | EC2 Management | us-east-1.console.aws.amazon.com/ec2/home?region=us-east-1#Instances

Instances (2)

Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone	Public IPv4 DNS
Badion Host	i-0f2baad5517156b0	Running	t2.micro	2/2 checks passed	No alarms	us-east-1a	ec2-54-210-99-1
Lab	i-0a0e734541153f0f	Running	t2.micro	2/2 checks passed	No alarms	us-east-1a	ec2-54-238-176

Select an instance

Lab 4 - Working with EBS

Create volume

Create an EBS volume to attach to any EC2 instance in the same Availability Zone.

Volume settings

Volume type: **General Purpose SSD (gp3)**

Size (GB): **1**

IOPS: **100**

Throughput (MB/s): **Not applicable**

Availability Zone: **us-east-1a**

Snapshot ID: **optional**

Encryption: **Not applicable**

Lab 4 - Working with EBS

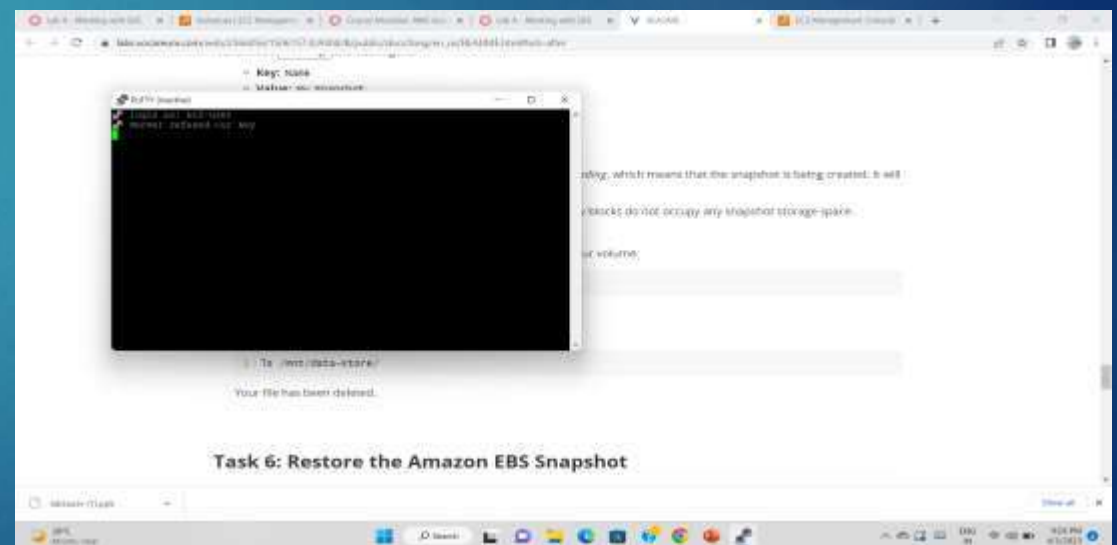
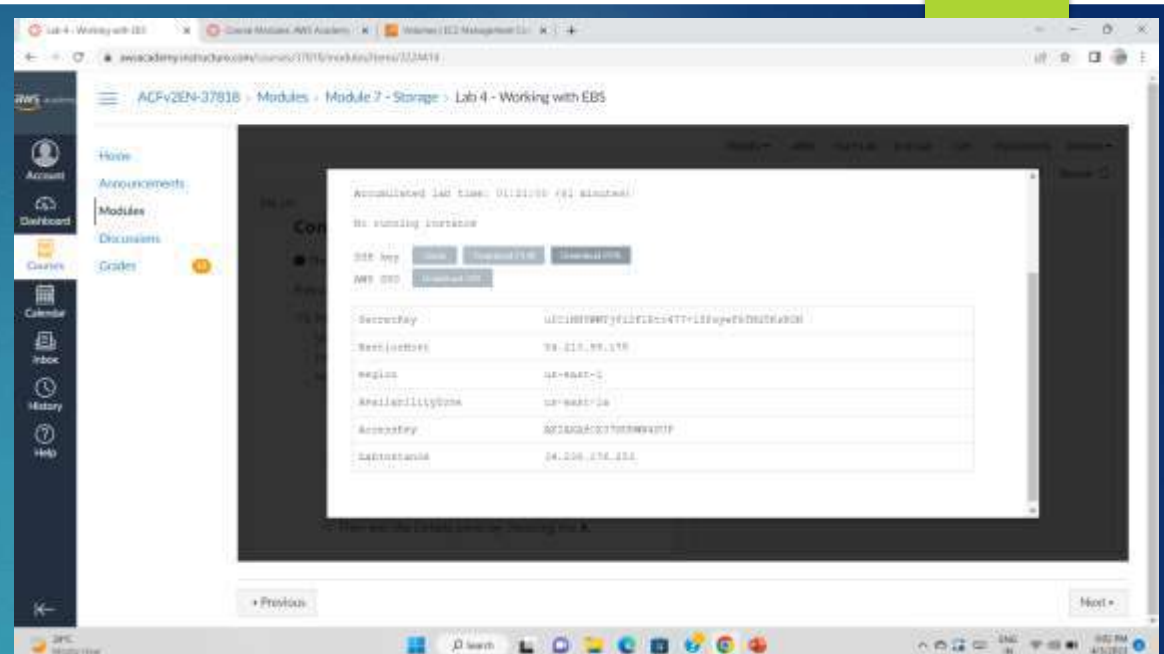
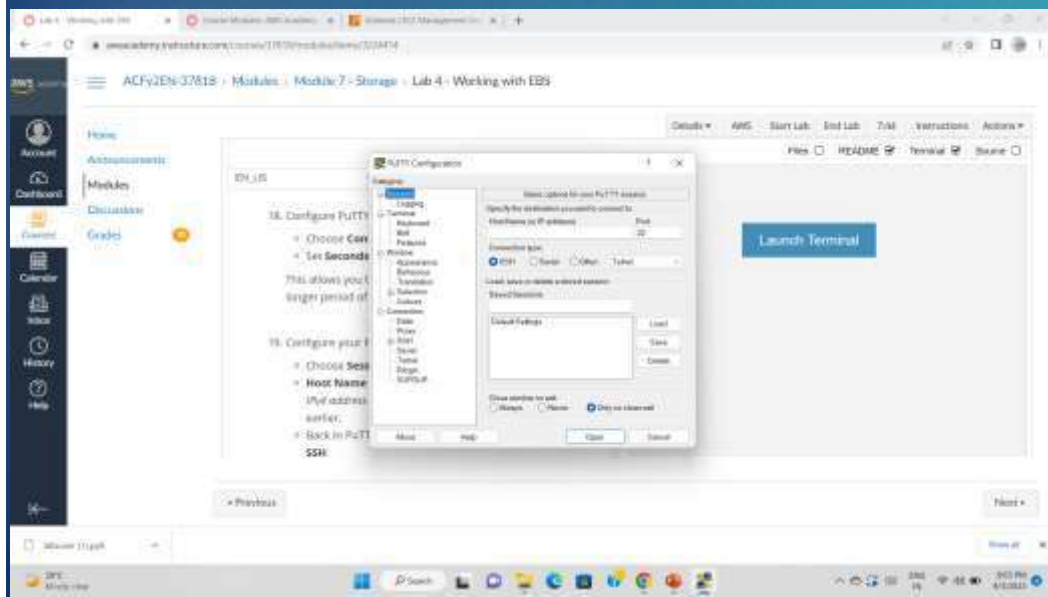
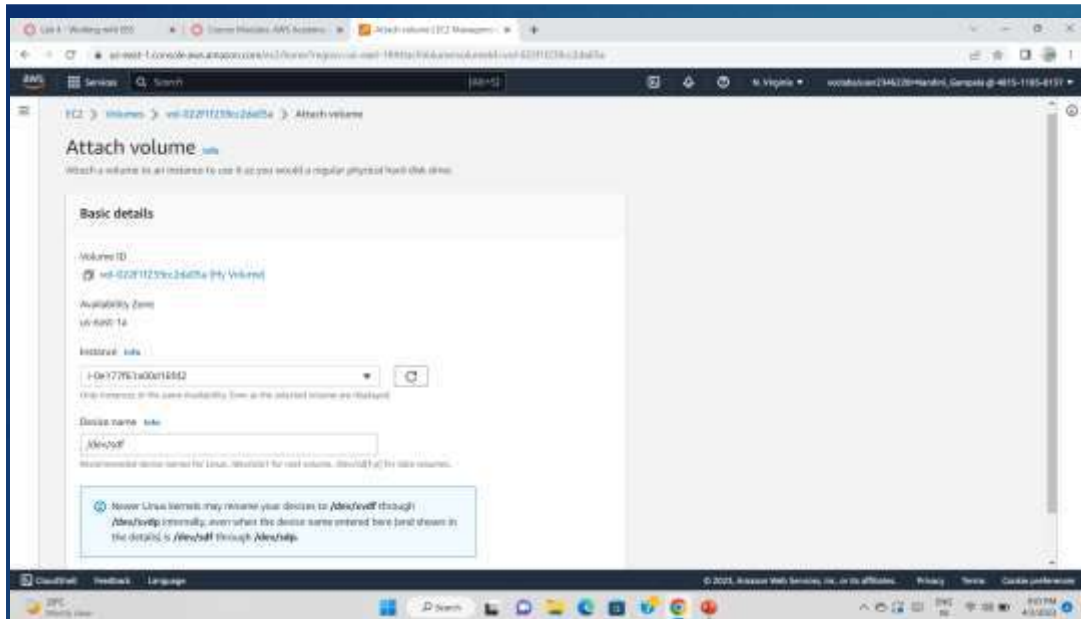
Volumes | EC2 Management | us-east-1.console.aws.amazon.com/ec2/home?region=us-east-1#Volumes

Volumes (1/2)

Name	Volume ID	Type	Size	IOPS	Throughput
My Volume	vol-022f1f239cc2da05a	gp2	1 GB	100	-
	vol-00b0f07818675a38	gp3	8 GB	3000	125

Volume ID: vol-022f1f239cc2da05a (My Volume)

Details | Status checks | Monitoring | Tags





Amazon EC2 Management Console - Volumes (1/1)

Search

Name	Volume ID	Type	Size	IOPS	Throughput	Availability
My Volume	vol-0d10452f2085ab5	gp2	1 GB	100		Available

Actions: **Create volume**

Volume ID: vol-0d10452f2085ab5 (My Volume)

Details | Status checks | Monitoring | Tags

Availability Zone: us-east-1a

Fast snapshot restore: [info](#)

Not enabled for selected snapshot

Encryption: [info](#)

Tags - optional: [info](#)

Key:  Value: optional:

Amazon EC2 Management Console - Snapshots (1/1)

Search

Name	Snapshot ID	Size	Description	Storage	Snapshot status
My Snapshot	snap-013c8ef009b54ee35	1 GB		Standard	Completed

Actions: **Create snapshot**

Snapshot ID: snap-013c8ef009b54ee35 (My Snapshot)

Details | Permissions | Storage tier | Tags

Basic details

Volume ID: [vol-0d10452f2085ab5 \(Attached Volume\)](#)

Availability Zone: us-east-1a

Instance: [i-00298bc30e6522a7b](#)

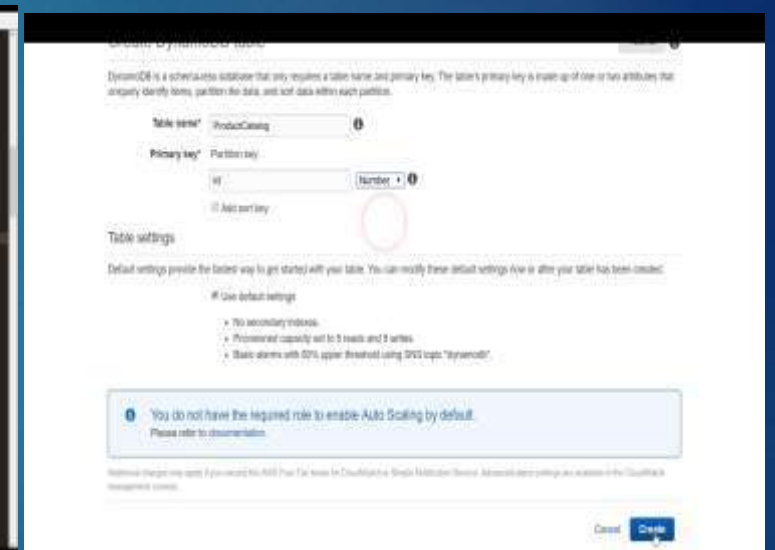
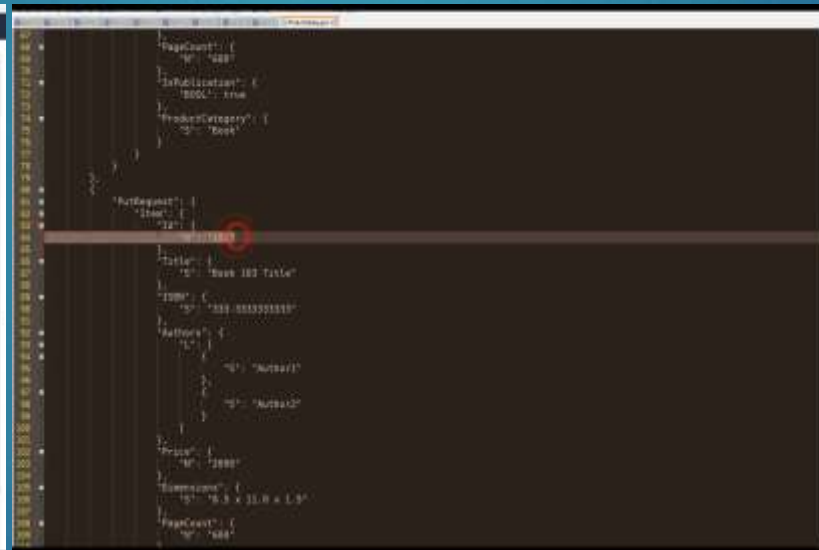
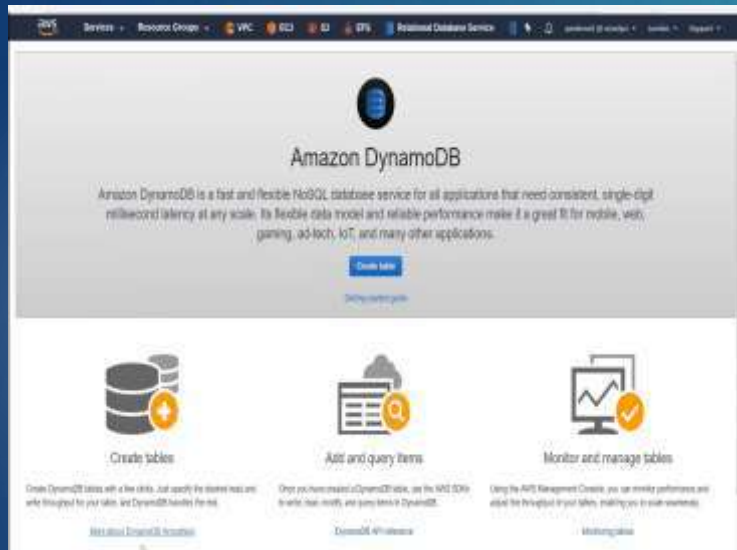
Device name: [info](#)



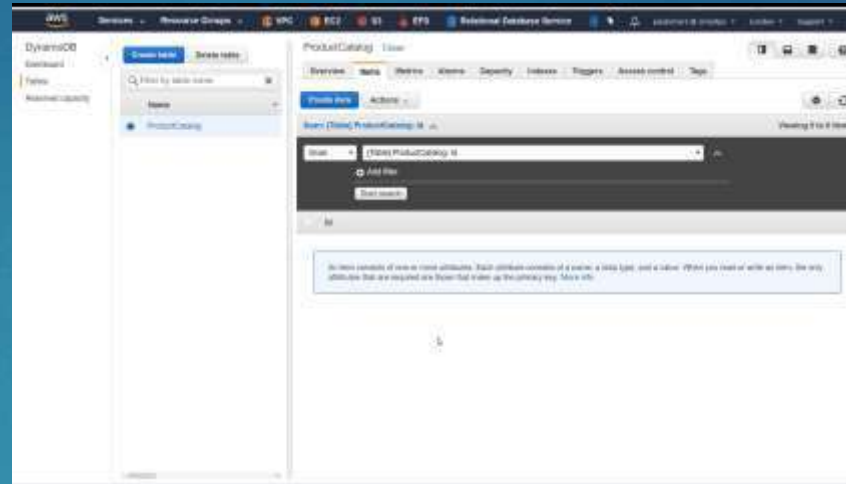
# DEPLOYEMENT OF AMAZON DYNAMO DB

## 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
PS C:\> aws dynamodb list-tables --region us-west-2
{
  "TableNames": [
    "ProductCatalog"
  ]
}
PS C:\> aws dynamodb describe-table --table-name ProductCatalog --region us-west-2
{
  "Table": {
    "TableName": "aws:iam::635561993154:dynamodb-us-west-2:489281224315: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": 2024-12-26T12:32:43.724Z
  }
}
PS C:\> aws dynamodb batch-write-item --request-items file://ProductCatalog.json --region us-west-2
```

ProductCatalog

Overview Items Metrics Alarms Capacity Indexes Triggers Access control Tags

Create table Delete table

Filter by table name

Name

ProductCatalog

Scan [Table] ProductCatalog: id

Viewing 1 to 9 items

ID	Price	ProductCategory	Title	BicycleType	Brand	Color	Description
205	300	Bicycle	15-Bike-204	Hybrid	Brand-Comp...	[{"S": "Red"}]	205 Description
203	300	Bicycle	15-Bike-203	Road	Brand-Comp...	[{"S": "Red"}]	203 Description
202	200	Bicycle	21-Bike-202	Road	Brand-Comp...	[{"S": "Green"}]	202 Description
201	100	Bicycle	15-Bike-201	Road	Mountain A	[{"S": "Red"}]	201 Description
204	400	Bicycle	15-Bike-204	Mountain	Brand-Comp...	[{"S": "Red"}]	204 Description
102	20	Book	Book 102 Title				
103	2000	Book	Book 103 Title				
101	2	Book	Book 101 Title				

ProductCatalog

Overview Items Metrics Alarms Capacity Indexes Triggers Access control Tags

Create table Delete table

Filter by table name

Name

ProductCatalog

Query [Table] ProductCatalog: id

Viewing 1 to 9 items

Partition key

Sort

Attributes

ID	Price	ProductCategory	Title	BicycleType	Brand	Color	Description
205	300	Bicycle	15-Bike-204	Hybrid	Brand-Comp...	[{"S": "Red"}]	205 Description
203	300	Bicycle	15-Bike-203	Road	Brand-Comp...	[{"S": "Red"}]	203 Description
202	200	Bicycle	21-Bike-202	Road	Brand-Comp...	[{"S": "Green"}]	202 Description
201	100	Bicycle	15-Bike-201	Road	Mountain A	[{"S": "Red"}]	201 Description
204	400	Bicycle	15-Bike-204	Mountain	Brand-Comp...	[{"S": "Red"}]	204 Description
102	20	Book	Book 102 Title				
103	2000	Book	Book 103 Title				
101	2	Book	Book 101 Title				

ProductCatalog

Overview Items Metrics Alarms Capacity Indexes Triggers Access control Tags

Create table Delete table

Filter by table name

Name

ProductCatalog

Query [Table] ProductCatalog: id

Viewing 1 to 1 items

Partition key

Sort

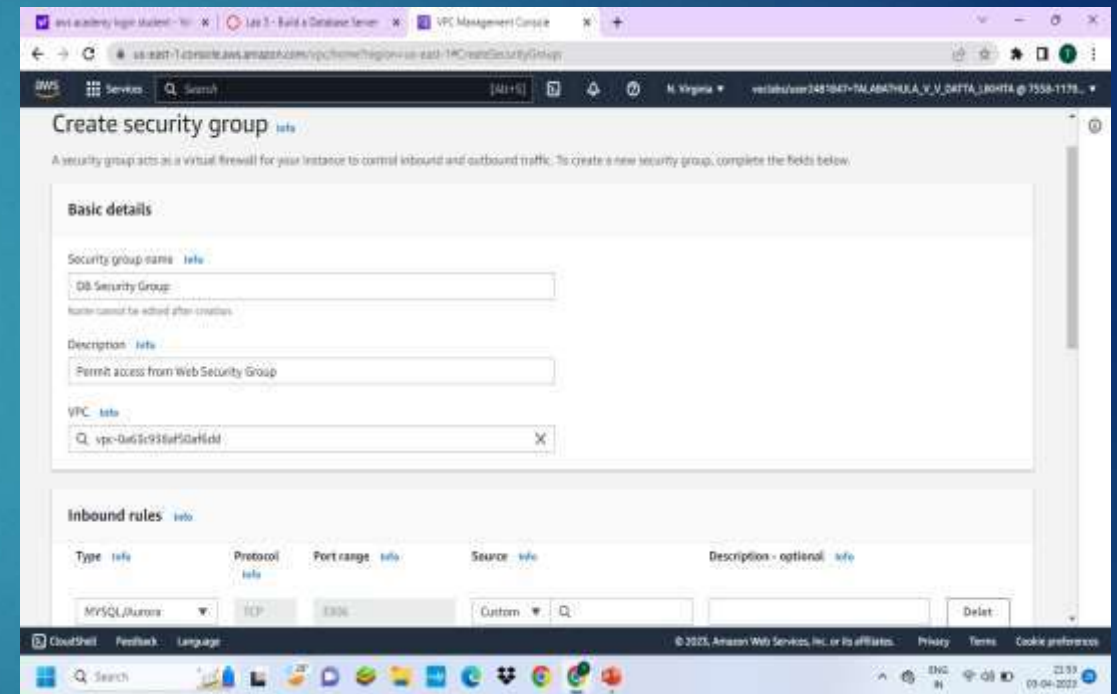
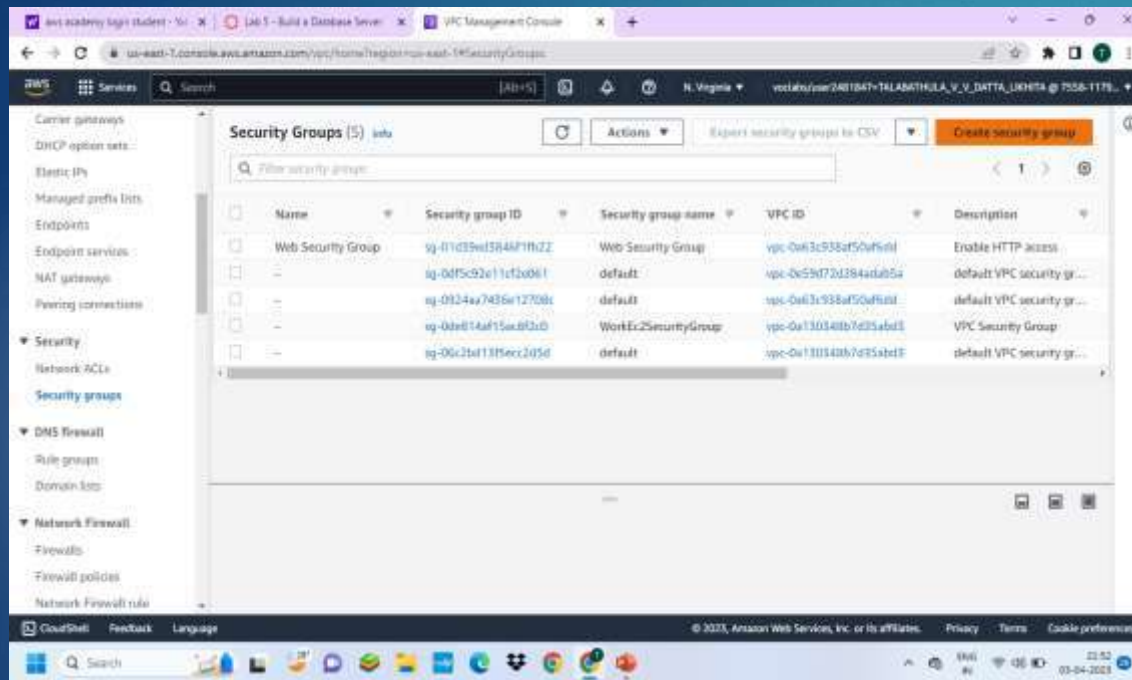
Attributes

ID	Price	ProductCategory	Title	BicycleType	Brand	Color	Description
204	400	Bicycle	15-Bike-204	Mountain	Brand-Comp...	[{"S": "Red"}]	204 Description

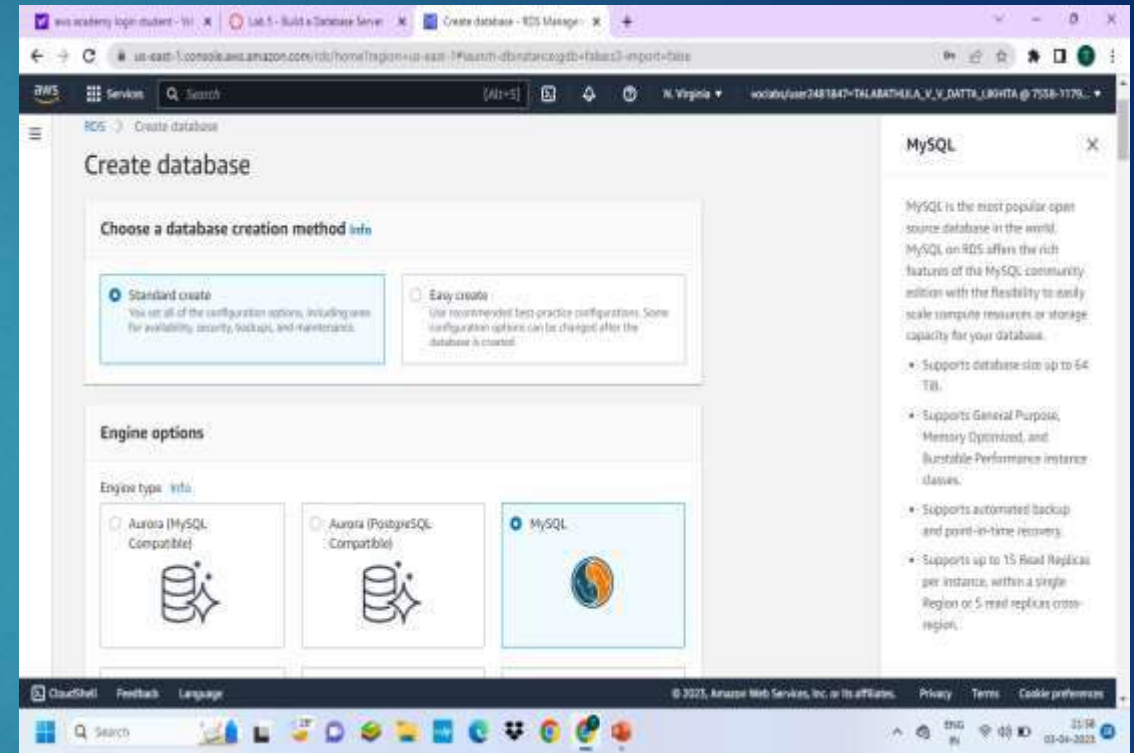
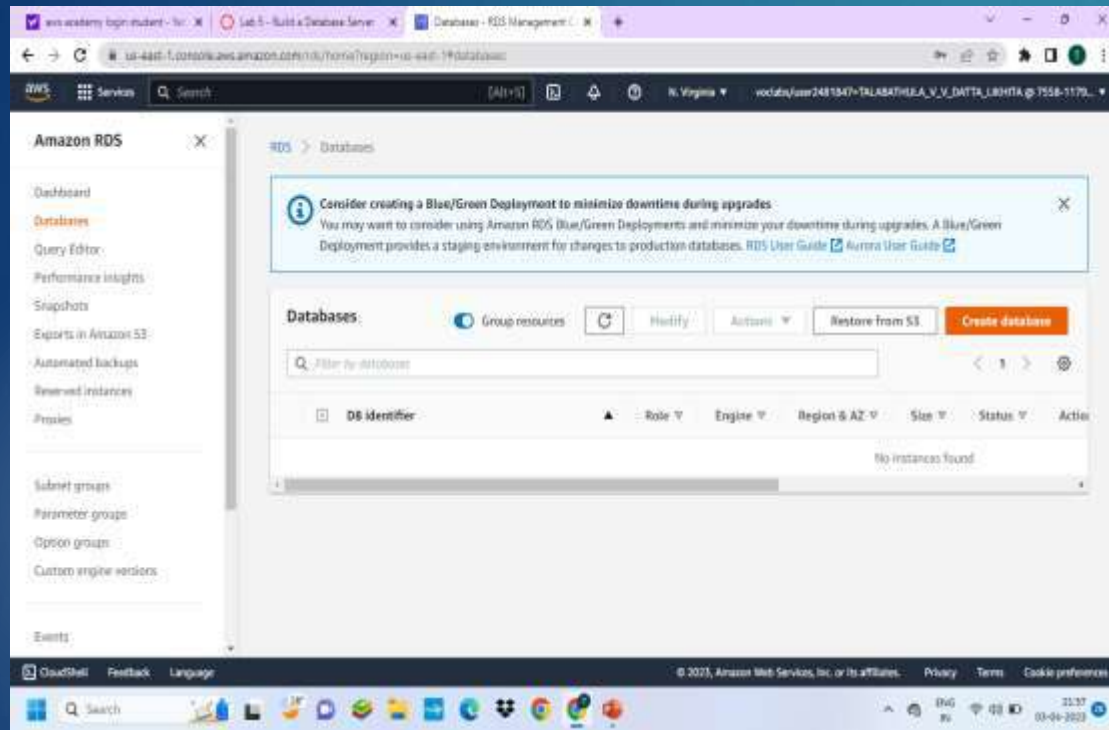
# DEPLOYMENT OF AMAZON RDS

## 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.

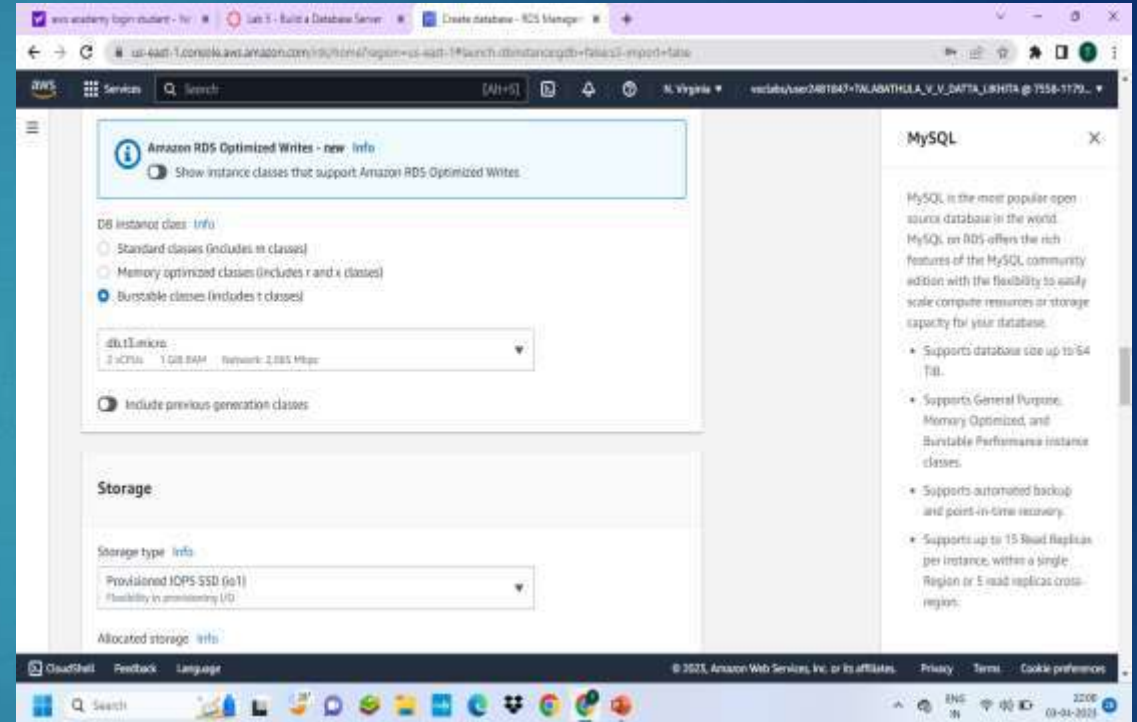
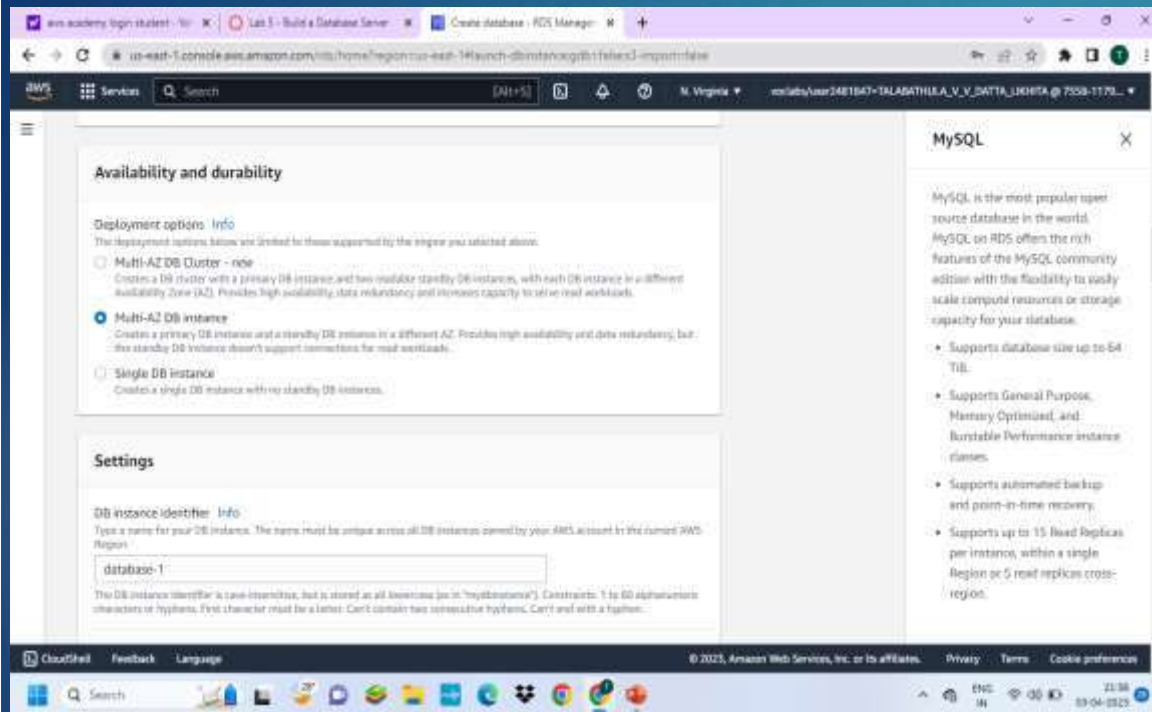


**Step 3: In the left navigation pane, choose Databases → choose create database → MYSQL**

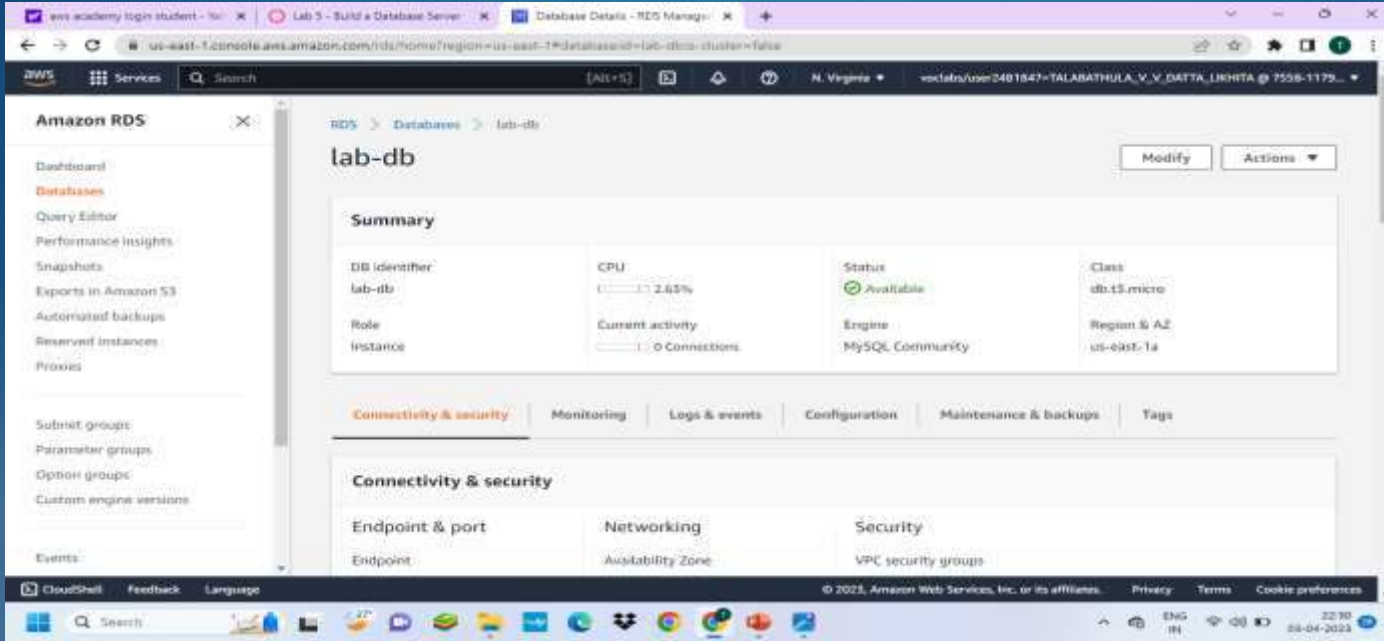




**Step 4: In Availability and durability, choose Multi -AZ DB instance then configure settings , DB instance class, Storage, connectivity, choose existing vpc security group and setup additional configuration.**

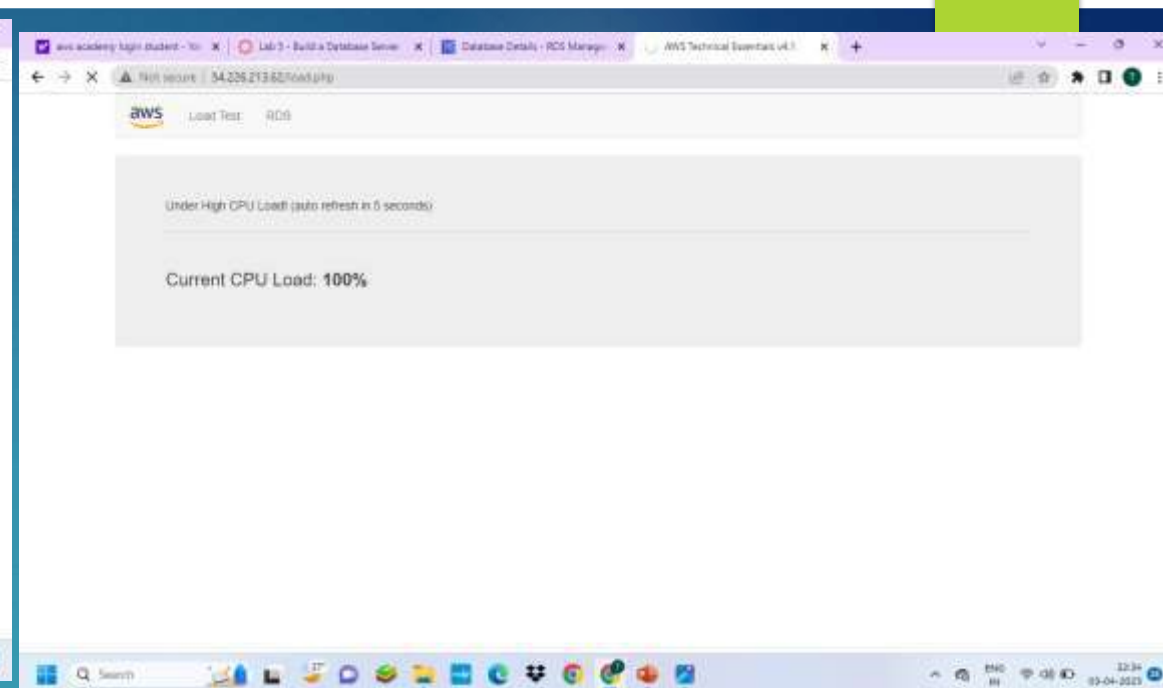
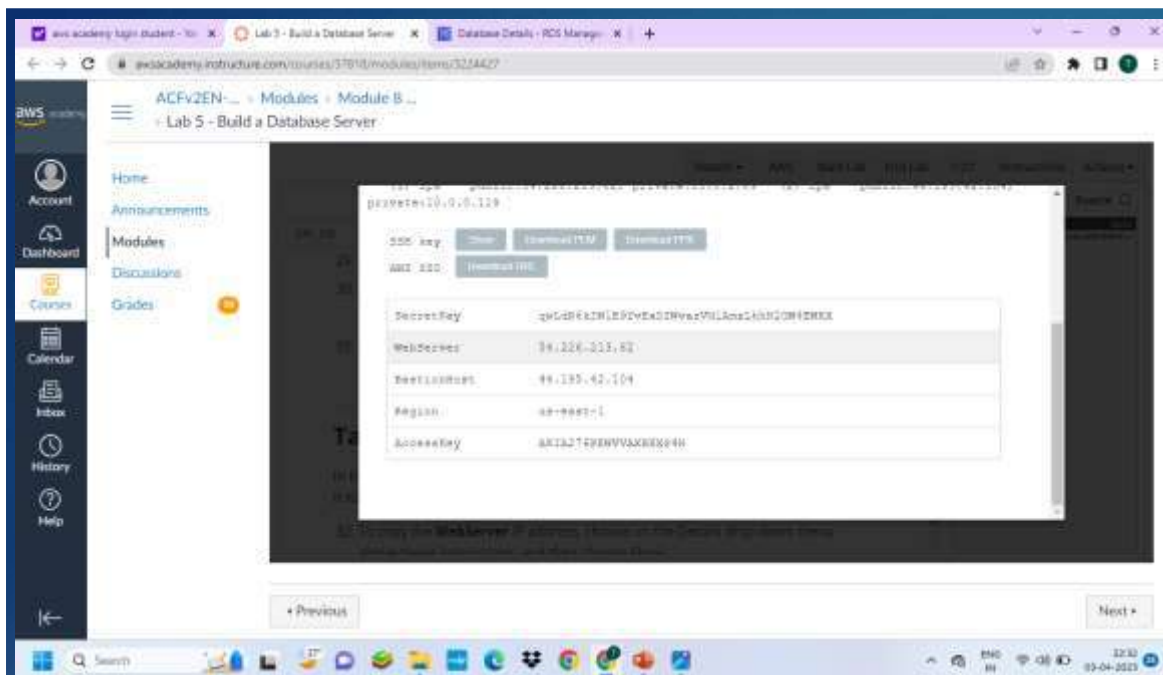


100

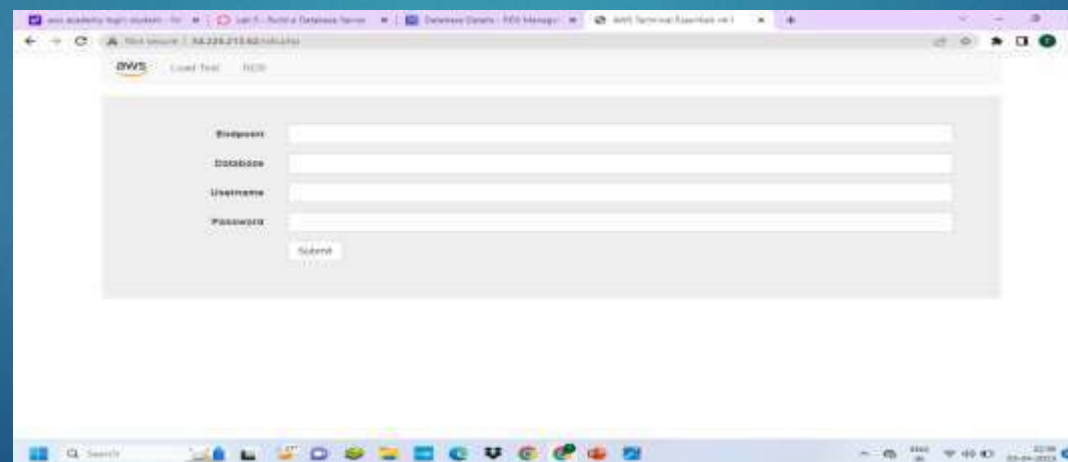


## Step 6 : Interact with Your Database.

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.**



**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 - Yab 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

## DEPLOYEMENT OF AMAZON 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`.

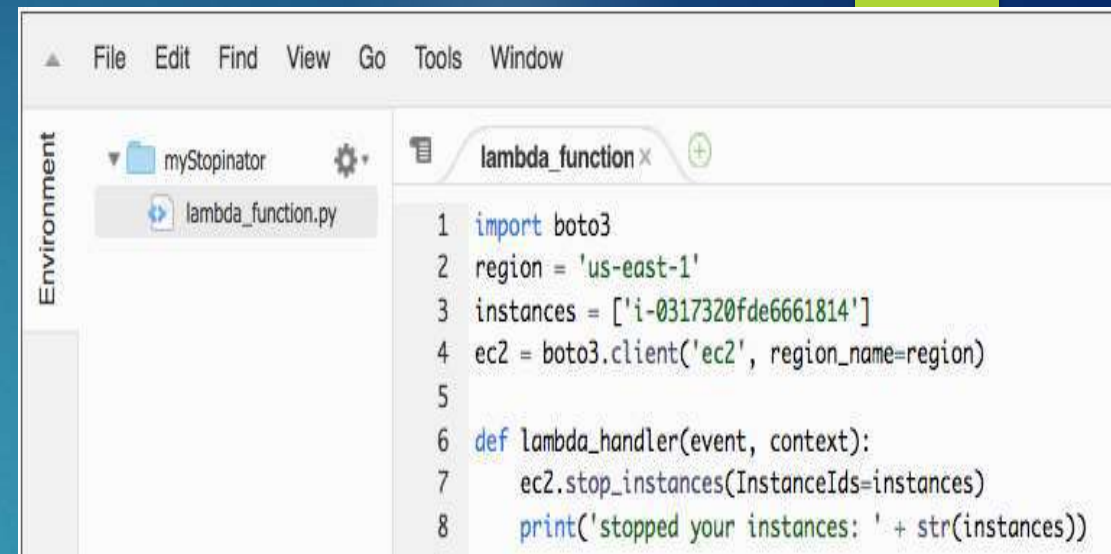
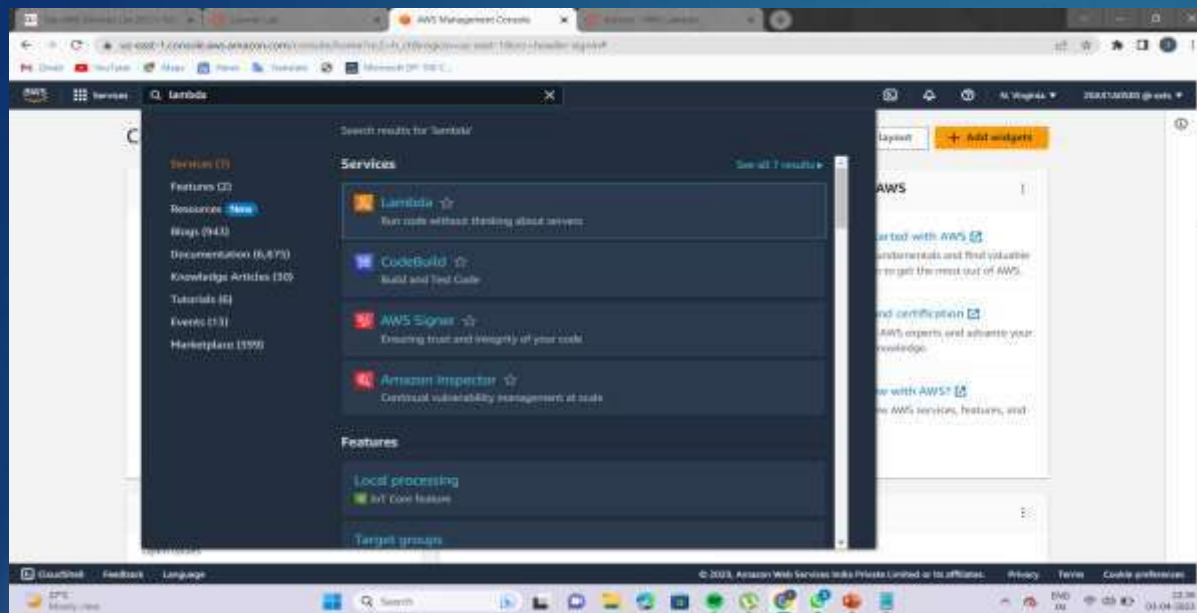
11) Verify that an EC2 instance named `instance1` is running in your account, and copy the instance ID.

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

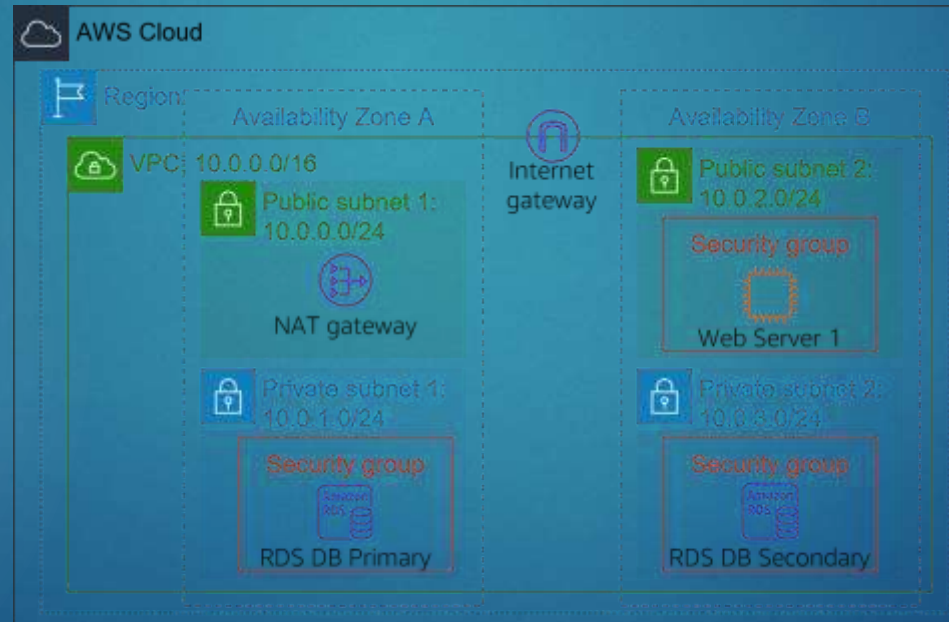
15) Return to the Amazon EC2 console browser tab and see if your instance was stopped.



## AMAZON ELASTIC LOAD BALANCING(ELB)

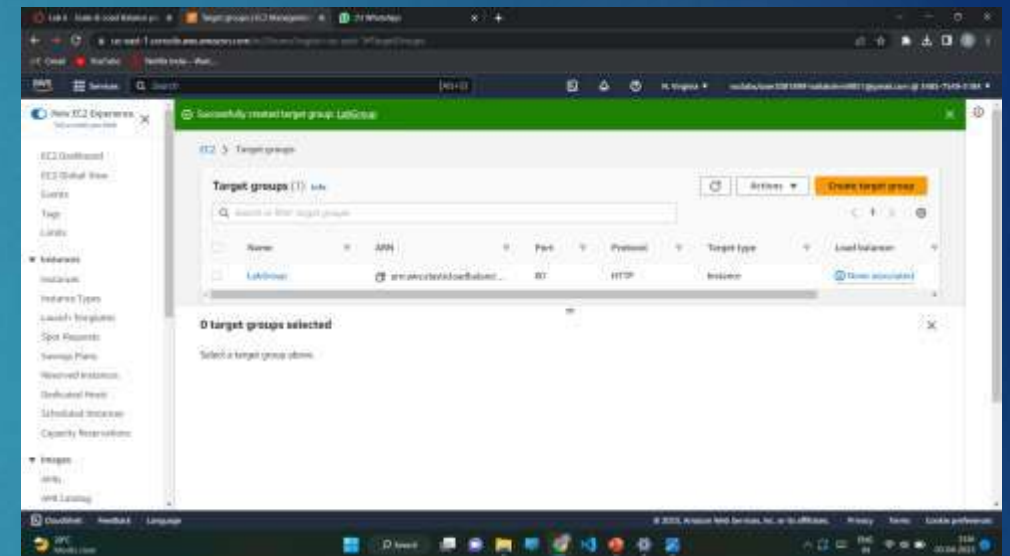
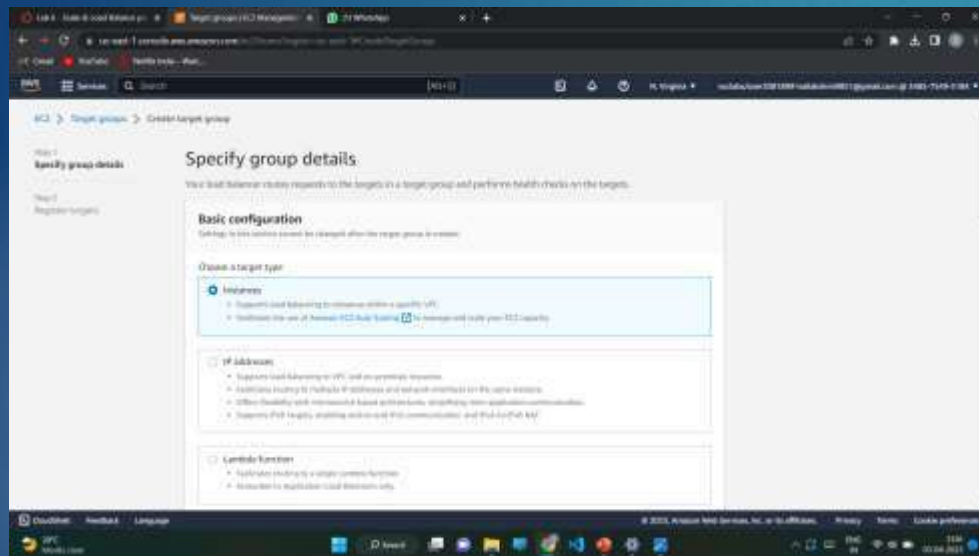
### Task1: Creating an AMI for Auto Scaling

- ❖ 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



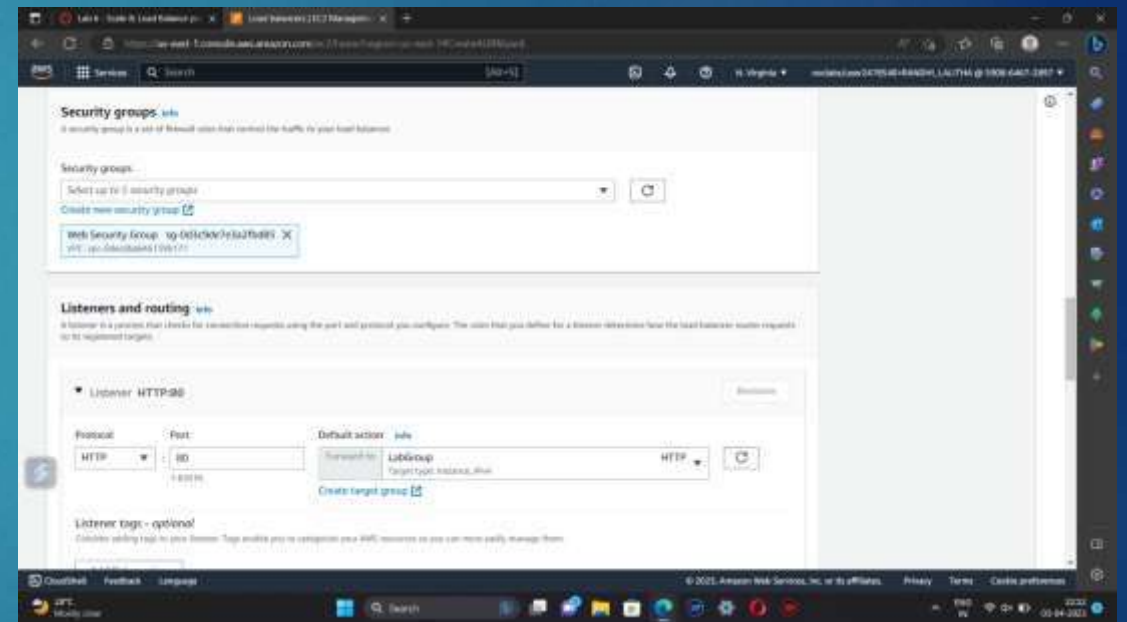
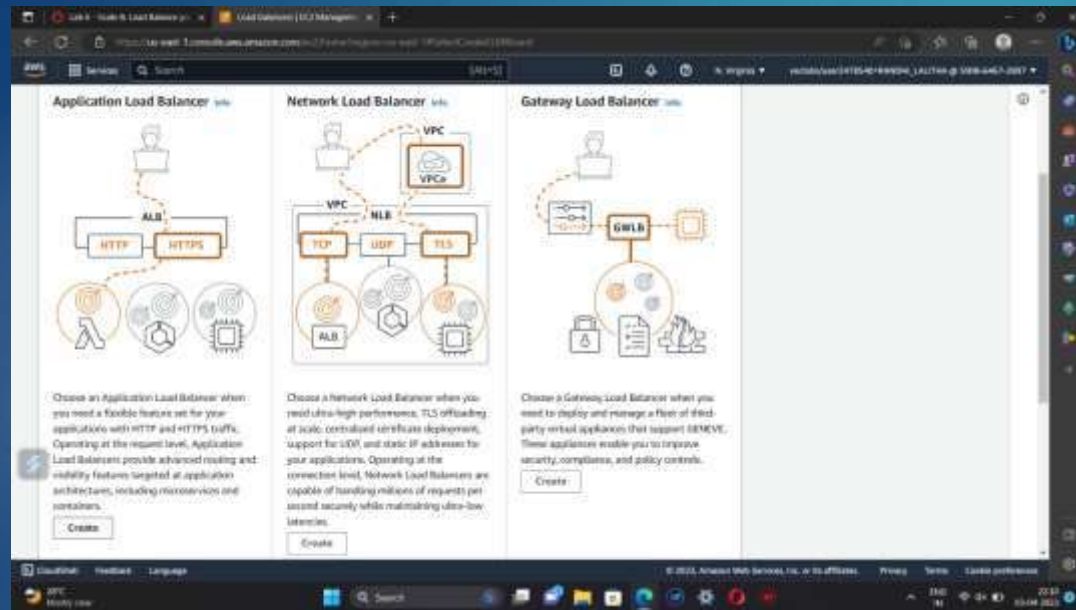
## Task 2: Creating a load balancer

- ❖ 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.

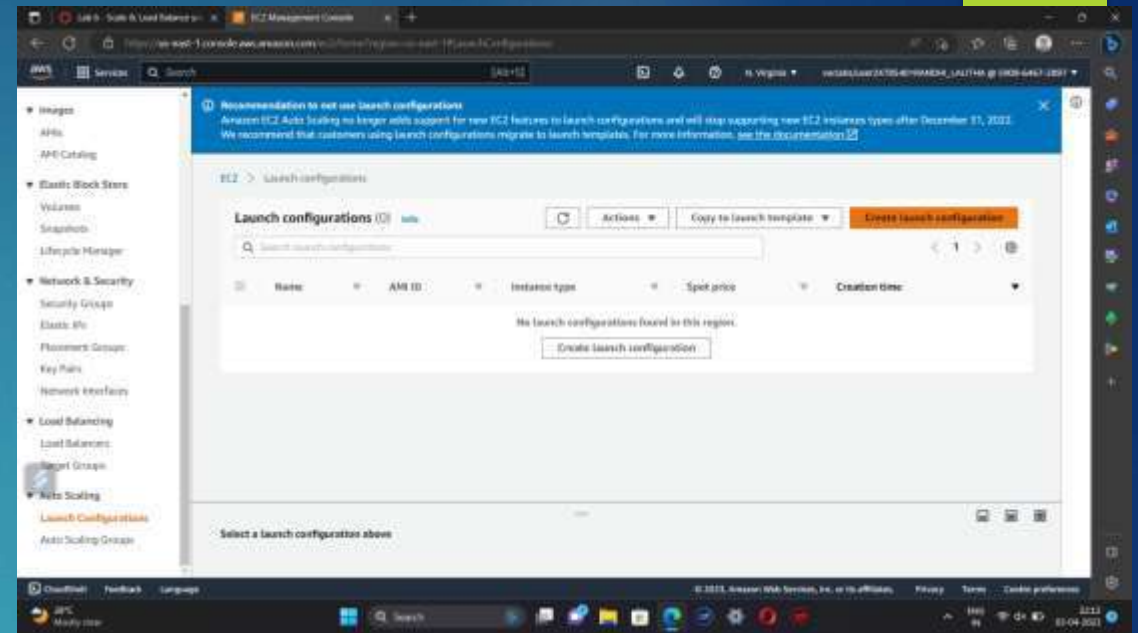
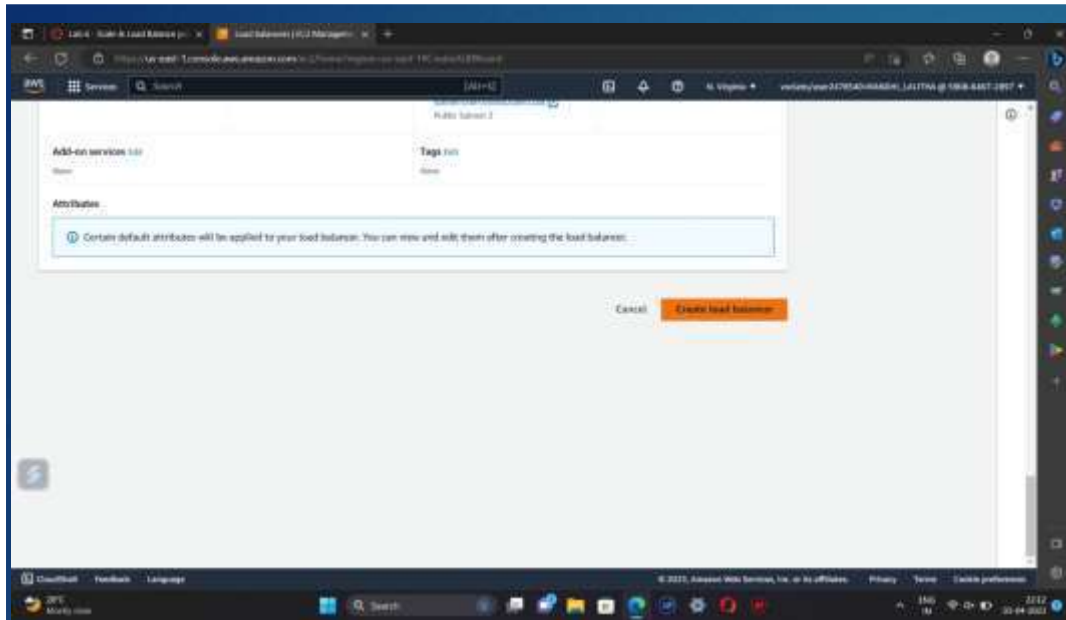




- ❖ From the left navigation pane , select Load Balancers. Click create load balancer.
- ❖ To create a application balancer, click create under Application Load Balancer and Name it.
- ❖ In Networking mapping, select Lab VPC and specify the subnets that the load balancer should use.
- ❖ In security groups, 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**.



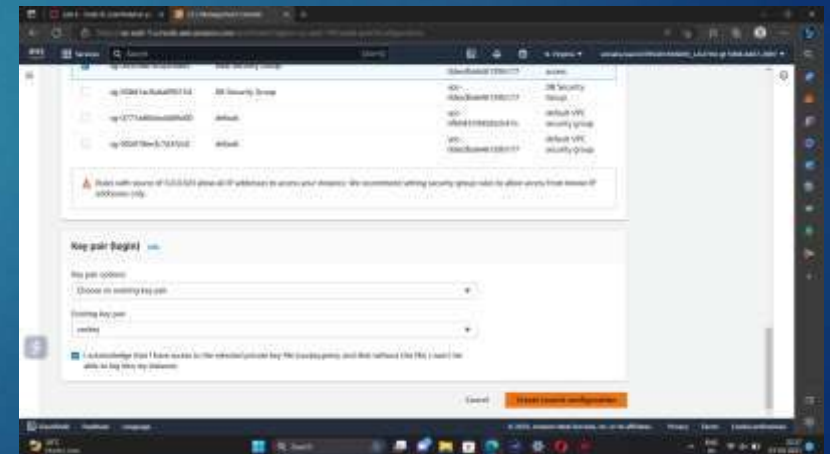




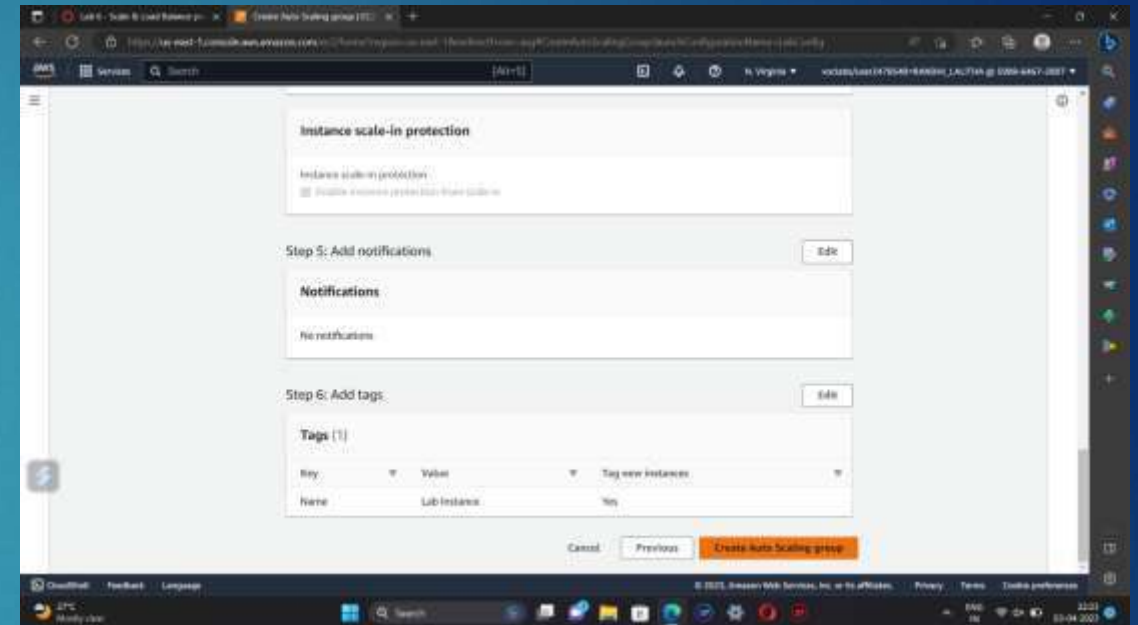
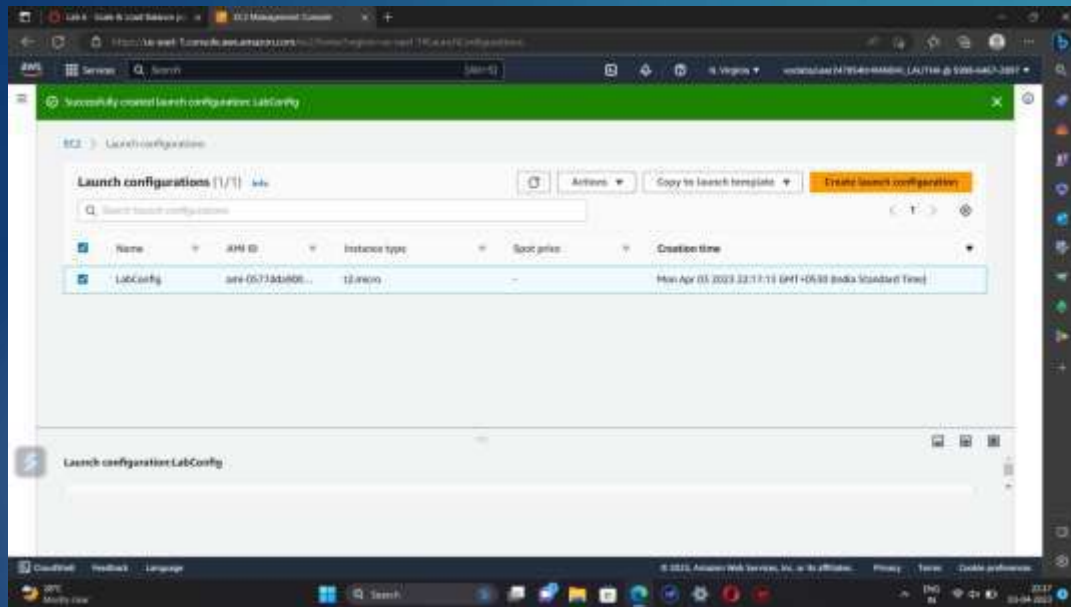
- ❖ Click create load balancer.

### 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 within CloudWatch**

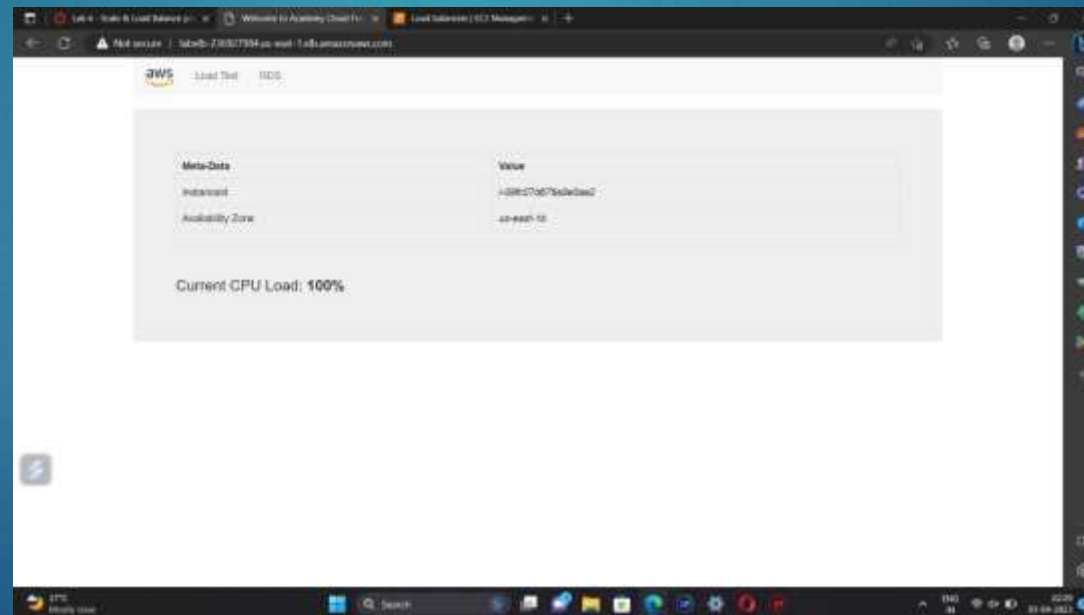


- ❖ Specify the values under Group size.
- ❖ Under **Scaling policies**, choose *Target tracking scaling policy* and name the policy. Specify metric type and target value. Then add a tag and click create auto scaling group.



#### 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



Lab 6 - Scale & Load Balance you

AWS Technical Essentials v4.1

Instances | EC2 Management Co

https://us-east-1.console.aws.amazon.com/ec2/home?region=us-east-1#Instances:

aws Services Search [Alt+S]

N. Virginia voclabs/user2478540=RANDHI\_LALITHA @ 5908-6467-2897

New EC2 Experience Tell us what you think

EC2 Dashboard

EC2 Global View

Events

Tags

Limits

Instances

Instances

Instance Types

Launch Templates

Spot Requests

Savings Plans

Reserved Instances

Dedicated Hosts

Scheduled Instances

Capacity Reservations

Images

AMIs

AMI Catalog

Elastic Block Store

Instances (4/6) Info

Find instance by attribute or tag (case-sensitive)

	Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone	Public IP
<input checked="" type="checkbox"/>	Lab Instance	i-09fc07d676a9e0aa2	Running	t2.micro	2/2 checks passed	No alarms	us-east-1b	-
<input checked="" type="checkbox"/>	Lab Instance	i-0cb98316a74468b05	Running	t2.micro	Initializing	No alarms	us-east-1b	-
<input type="checkbox"/>	Web Server 1	i-073e314d9026c1588	Running	t2.micro	2/2 checks passed	No alarms	us-east-1a	-
<input type="checkbox"/>	Bastion Host	i-03c892d00c9d9a5de	Running	t2.micro	2/2 checks passed	No alarms	us-east-1a	-
<input checked="" type="checkbox"/>	Lab Instance	i-0f6a9f9a4839cb762	Running	t2.micro	2/2 checks passed	No alarms	us-east-1a	-
<input checked="" type="checkbox"/>	Lab Instance	i-090863a20718c01f5	Running	t2.micro	Initializing	No alarms	us-east-1a	-

Instances: i-09fc07d676a9e0aa2 (Lab Instance), i-0cb98316a74468b05 (Lab Instance), i-0f6a9f9a4839cb762 (Lab Instance), i-090863a20718c01f5 (Lab Instance)

Monitoring

1h 3h 12h 1d 3d 1w Custom

CPU utilization (%) Various units 29.9 15 0

Status check failed (any) (c... Various units 1 0.5 0

Status check failed (instanc... Various units 1 0.5 0

Status check failed (system... Various units 1 0.5 0

CloudShell Feedback Language

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

27°C Mostly clear

Search

22:35 03-04-2023

## DEPLOYEMENT OF AMAZON 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:

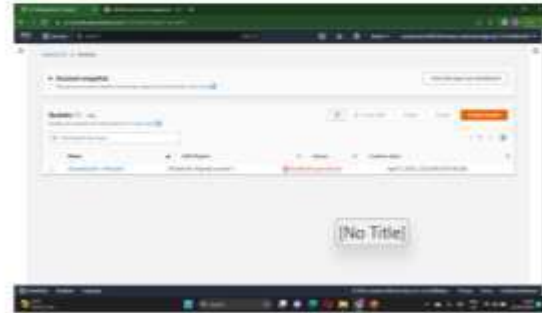
**Step 10:**Go back to your bucket and click on Permissions.

**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.

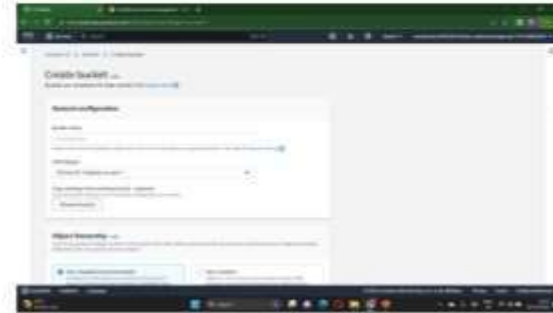
**Step 12 :**Now its state switches to Read Object - Yes

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

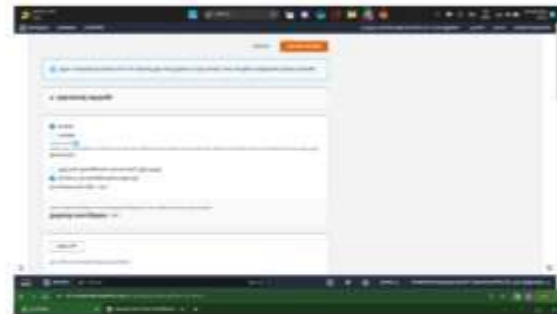
**Step 14:**Notice the URL on your browser



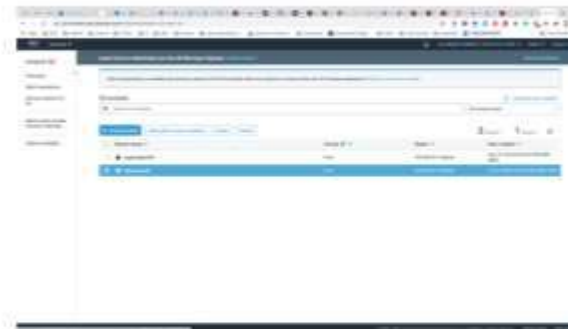
Step 1



Step 2



Step 2



Step 3

3\_PPT[1] - Protected View • Saved to this PC

Design Transitions Animations Slide Show Record Review View Help


from the Internet can contain viruses. Unless you need to edit, it's safer to stay in Protected View. [Enable Editing](#)

**Step 4**

**Step 5**

**Step 6**

**Step 7**



The image displays a Microsoft PowerPoint presentation in Protected View. The slide content is organized into four quadrants, each showing a different step of a process. Step 4 shows a login page with 'Username' and 'Password' fields and a 'Log In' button. Step 5 shows a dashboard with a 'Welcome' message and a 'Get Started' button. Step 6 shows a 'New Project' dialog box with 'Project Name' and 'Description' fields. Step 7 shows a 'New Project' dialog box with 'Project Name', 'Description', and a 'Create Project' button. The presentation interface includes a title bar, a ribbon with tabs like Design, Transitions, Animations, Slide Show, Record, Review, View, and Help, and a status bar at the bottom.



Protected View • Saved to this PC


Search

Lalitha Sri Sai Manasa


Transitions Animations Slide Show Record Review View Help

Present in Teams

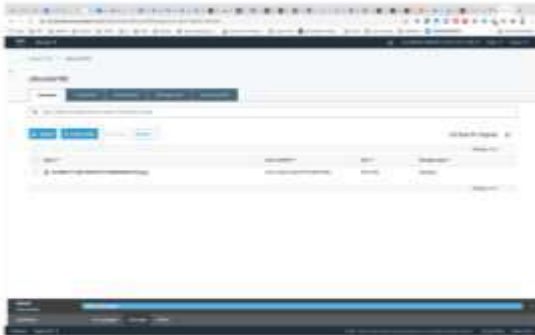
Internet can contain viruses. Unless you need to edit, it's safer to stay in Protected View. [Enable Editing](#)




**Step 8**



**Step 9**



**Step 10**



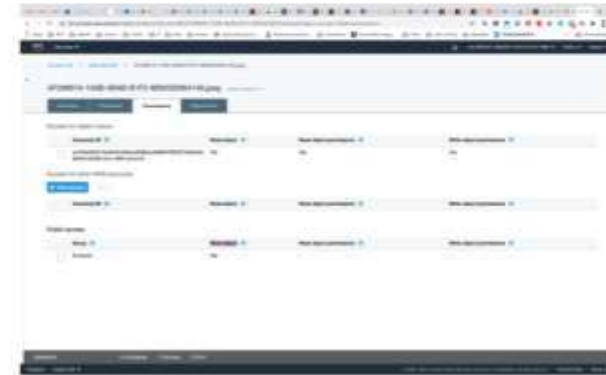
**Step 11**

Files from the Internet can contain viruses. Unless you need to edit, it's safer to stay in Protected View.

Enable Editing



Step 12



Step 13



Step 14

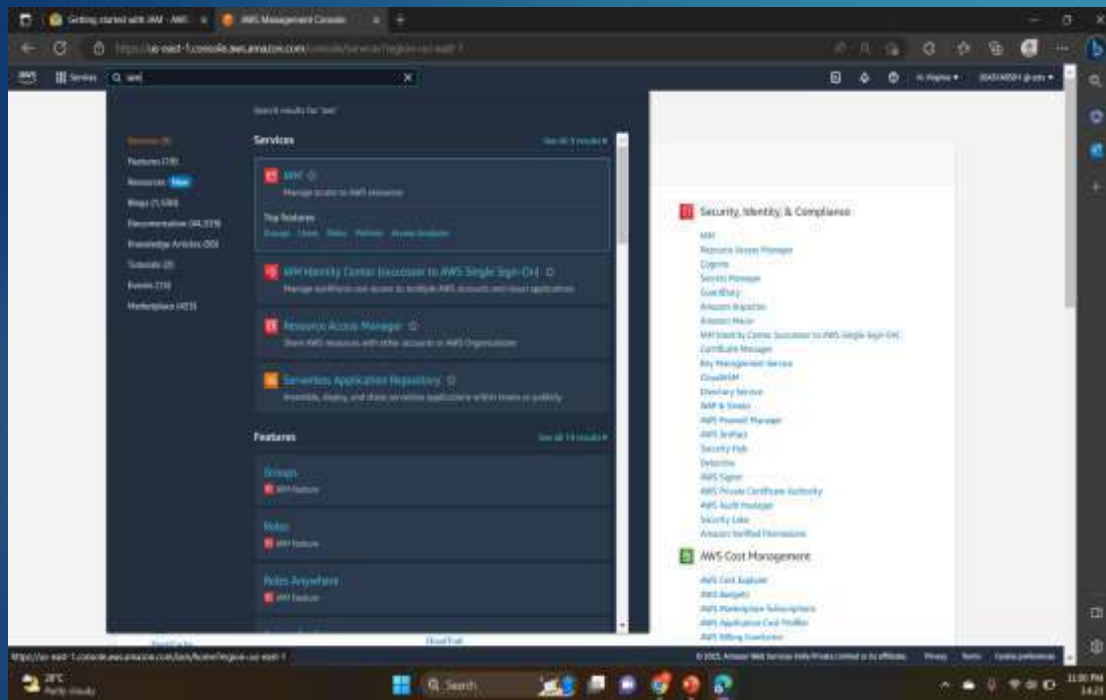
## DEPLOYEMENT OF AMAZON IAM(IDENTIFY AND ACCESS MANAGEMENT)

**AWS Identity and Access Management (IAM)** is a web service that enables Amazon Web Services (AWS) customers to manage users and user permissions in AWS. With IAM, you can centrally manage **users**, **security credentials** such as access keys, and **permissions** that control which AWS resources users can access.

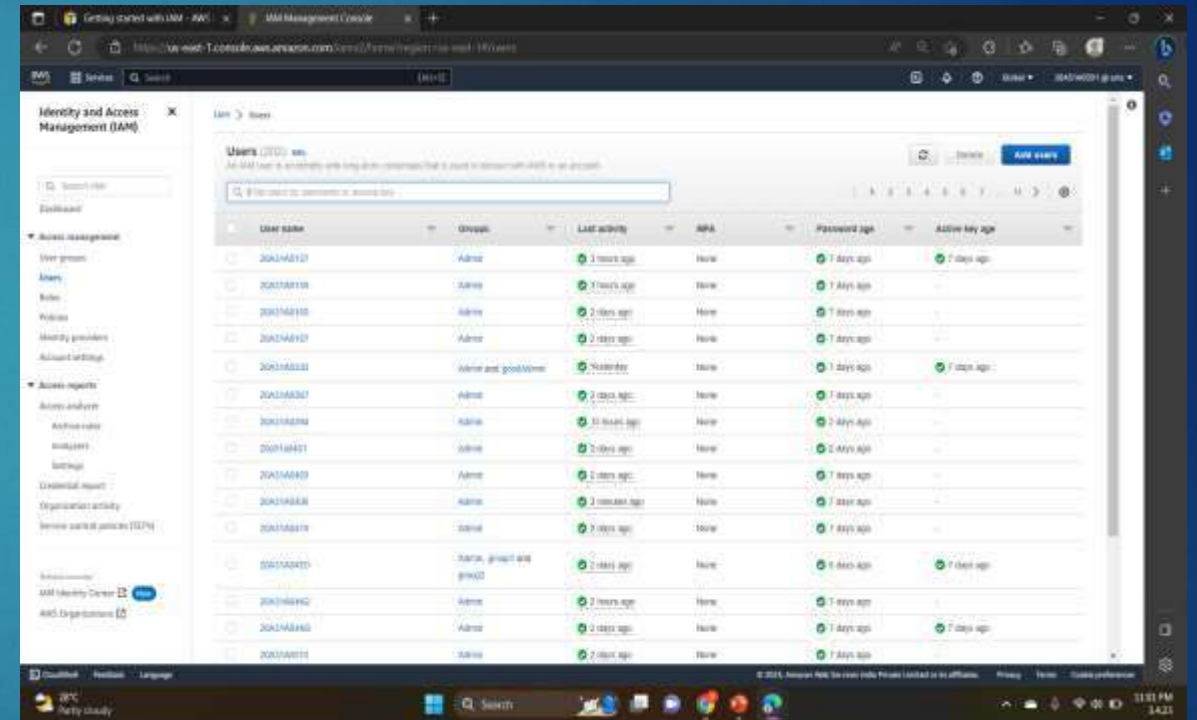


# Steps to create IAM User and User Groups

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



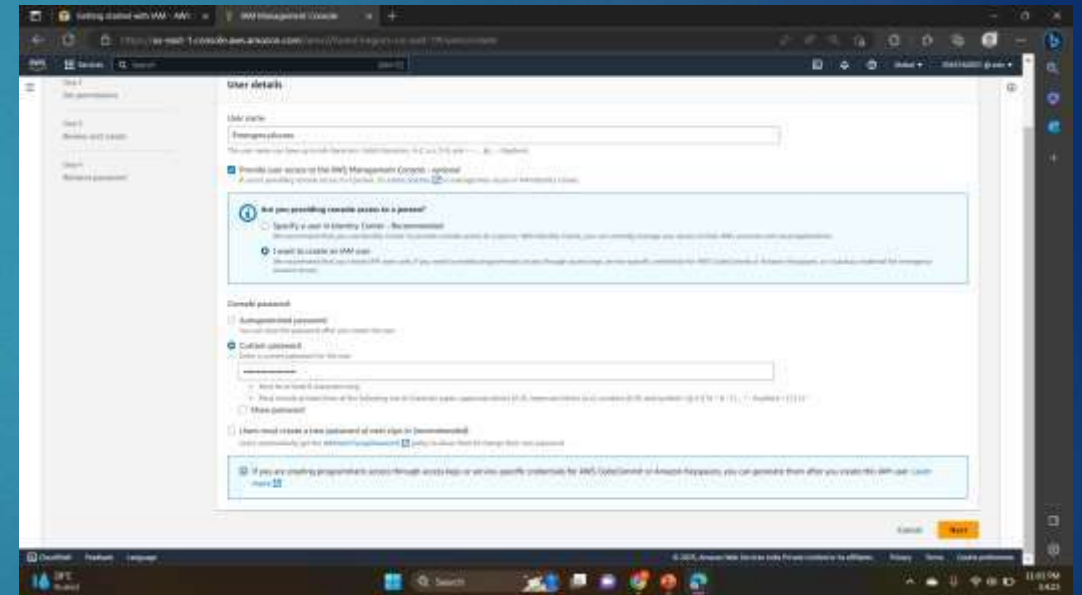
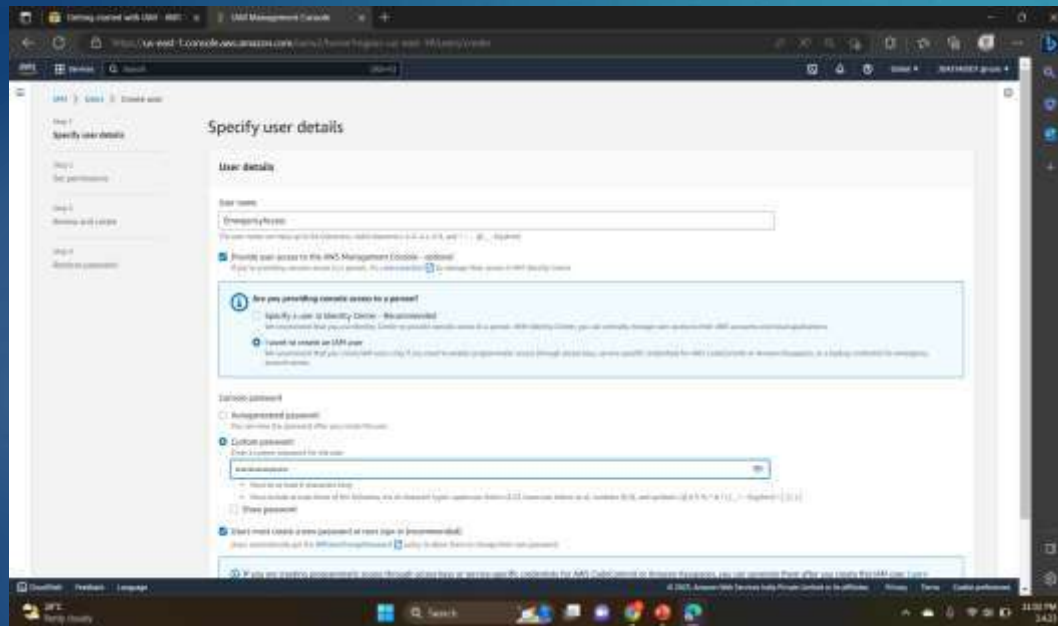
In the navigation pane, select **Users** and then select **Add users**.



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.**

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

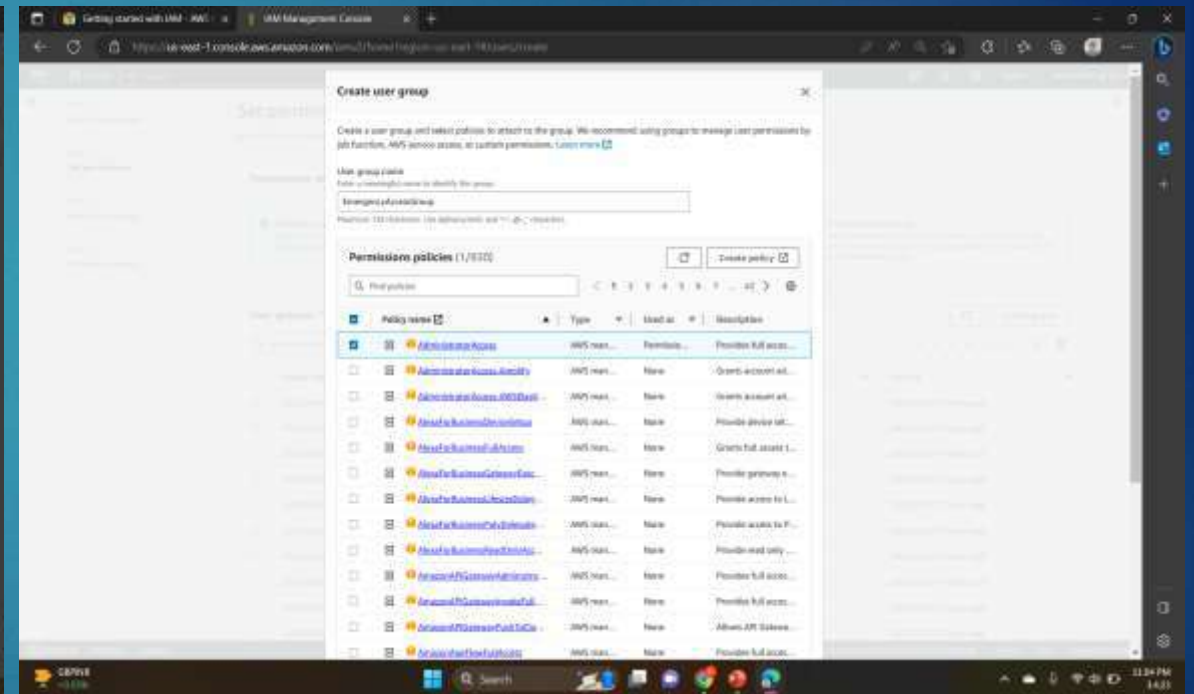
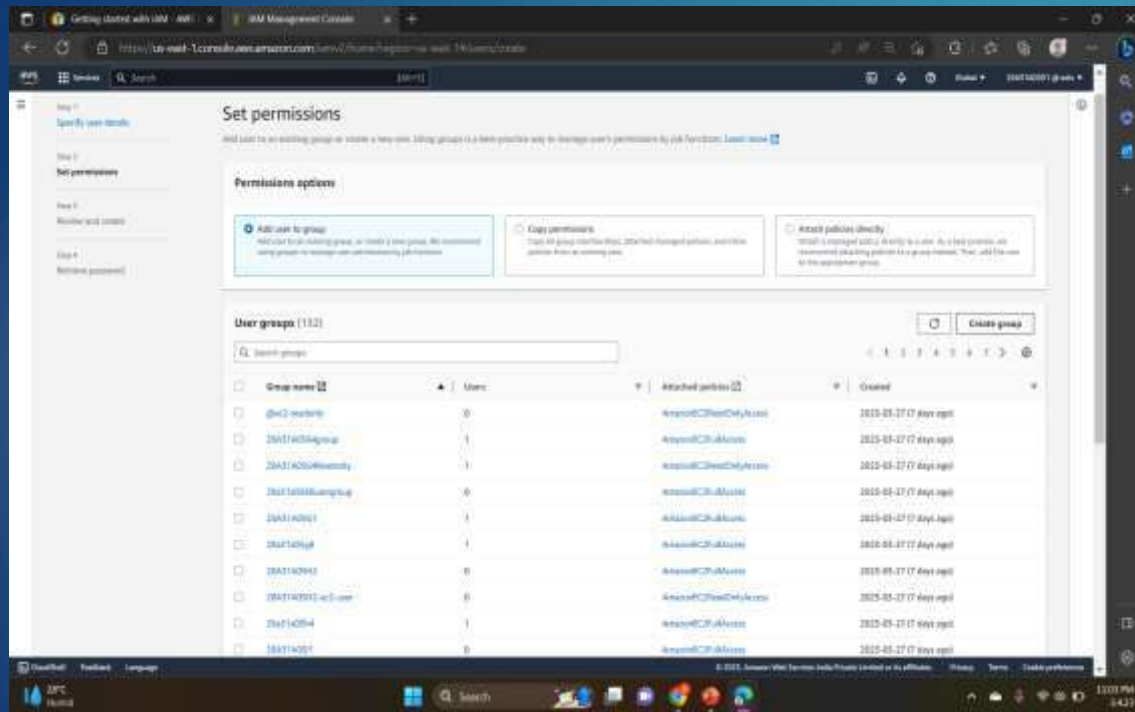
5. Clear the check box next to **User must create a new password at next sign-in (recommended)**. Then click on





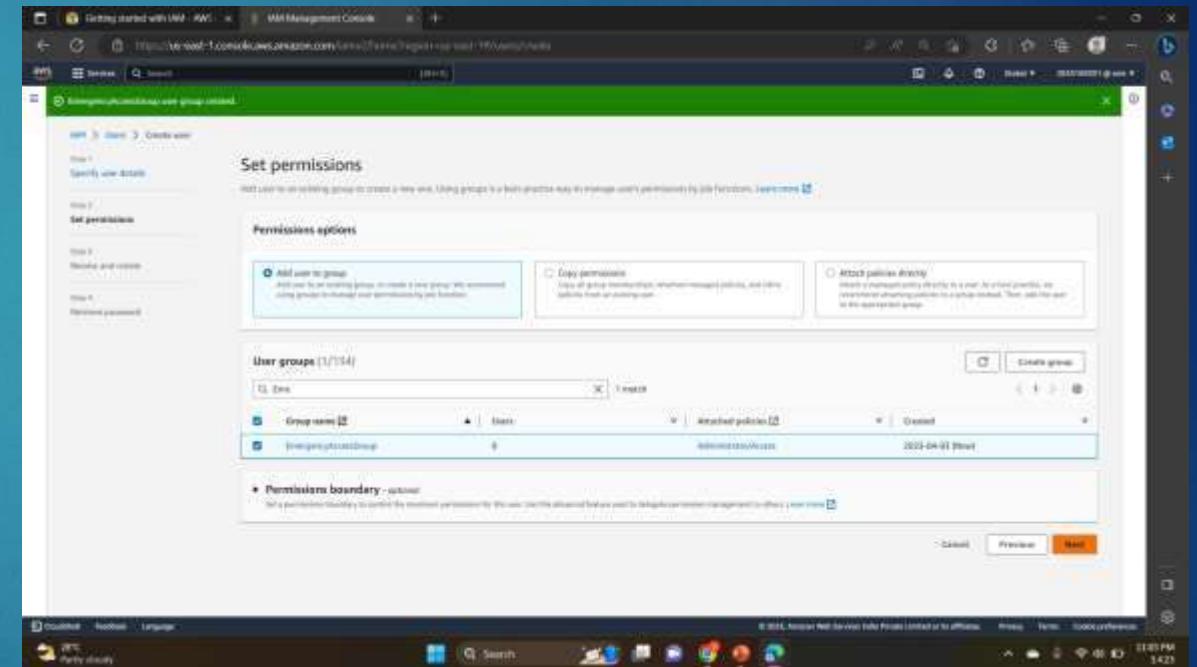
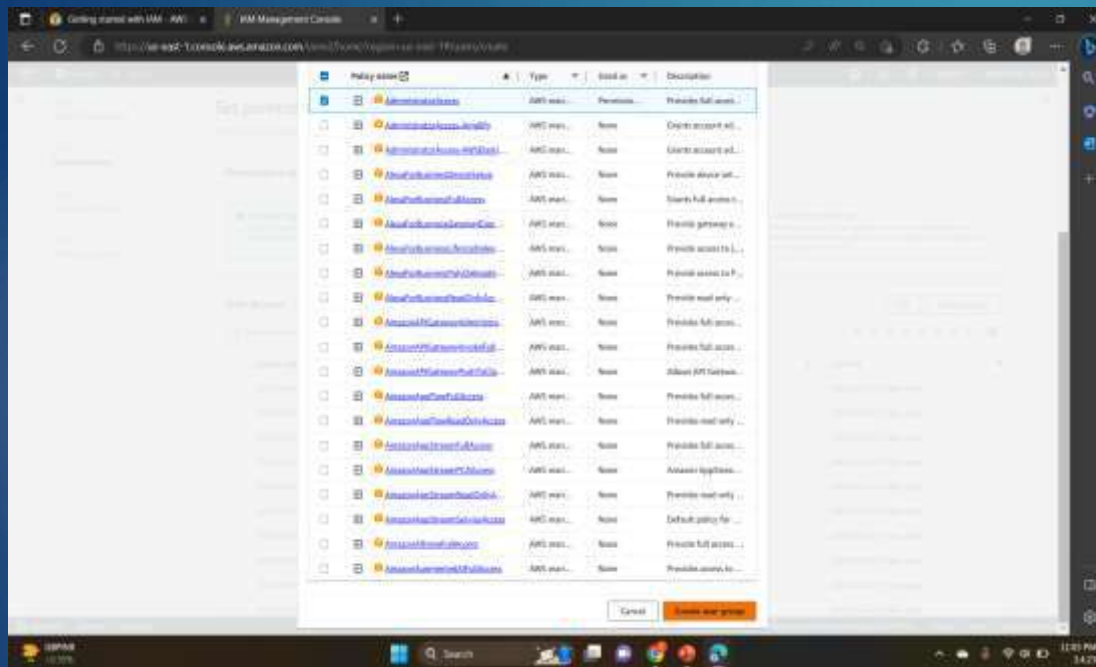
6. On the **Set permissions** page, under **Permissions options**, select **Add user to group**. Then, under **User groups**, select **Create group**.

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



8. Select **Create user group** to return to the **Set permissions** page.

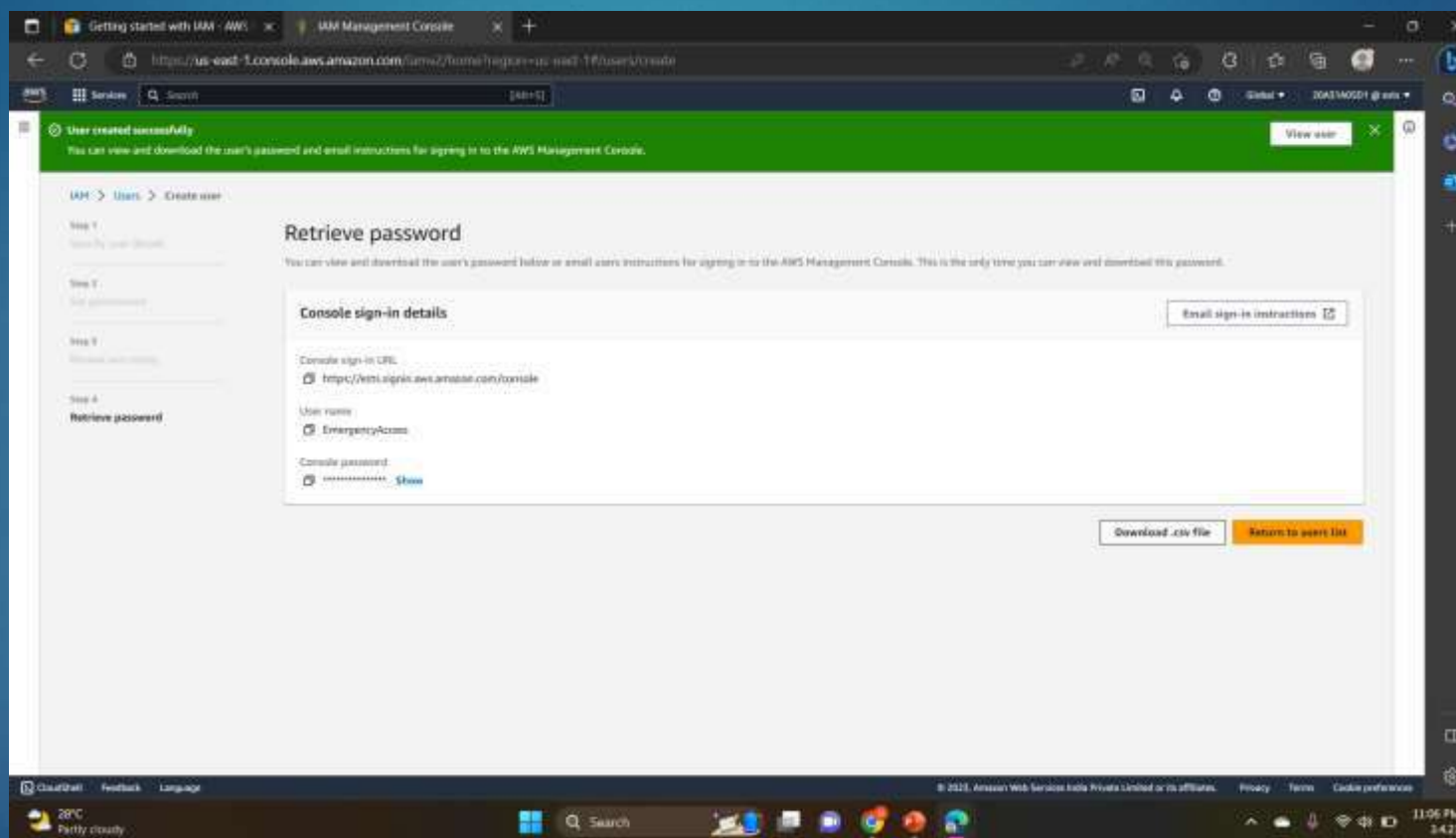
9.. Select **Next** to proceed to the **Review and create** page.



the new u

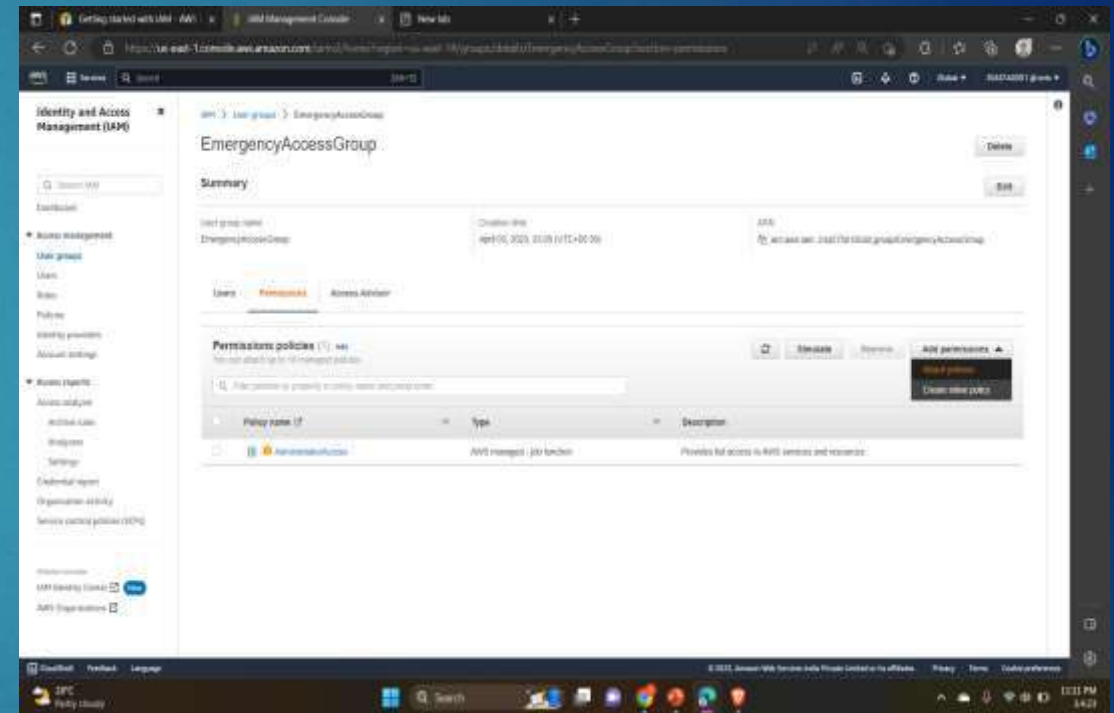
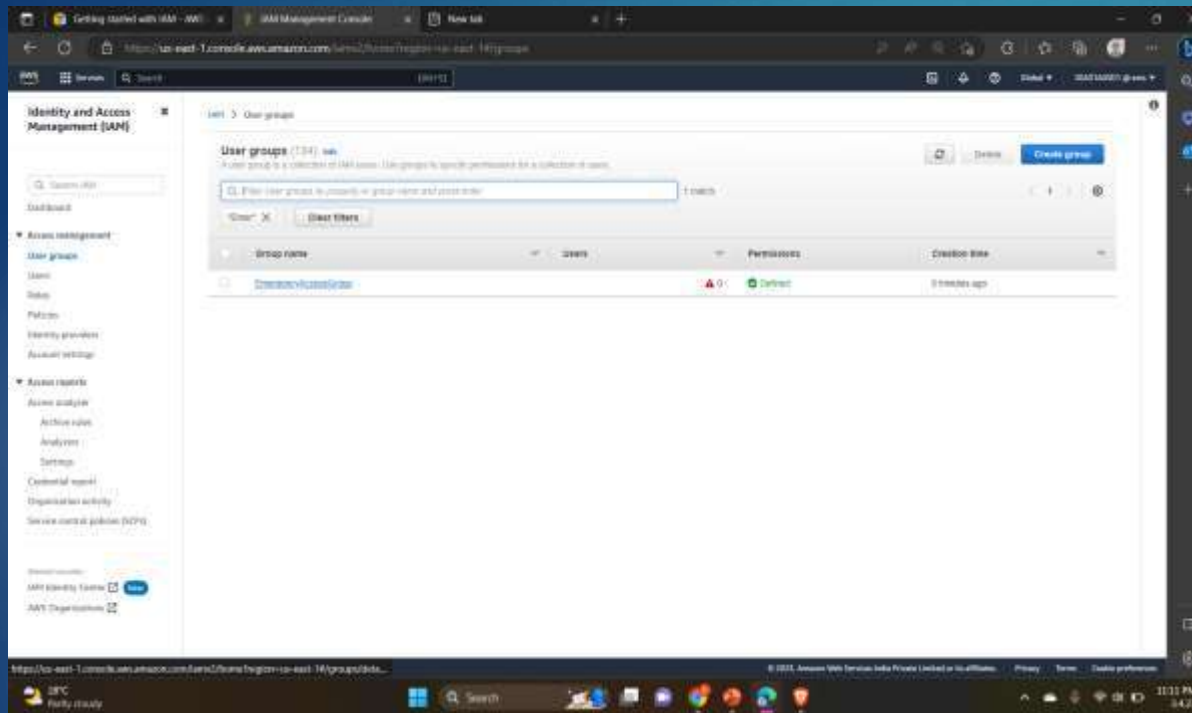
11. On the **Retrieve password** page, select **Download .csv file** to save a .csv file with the user credential information (Connection URL, user name, and password).

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

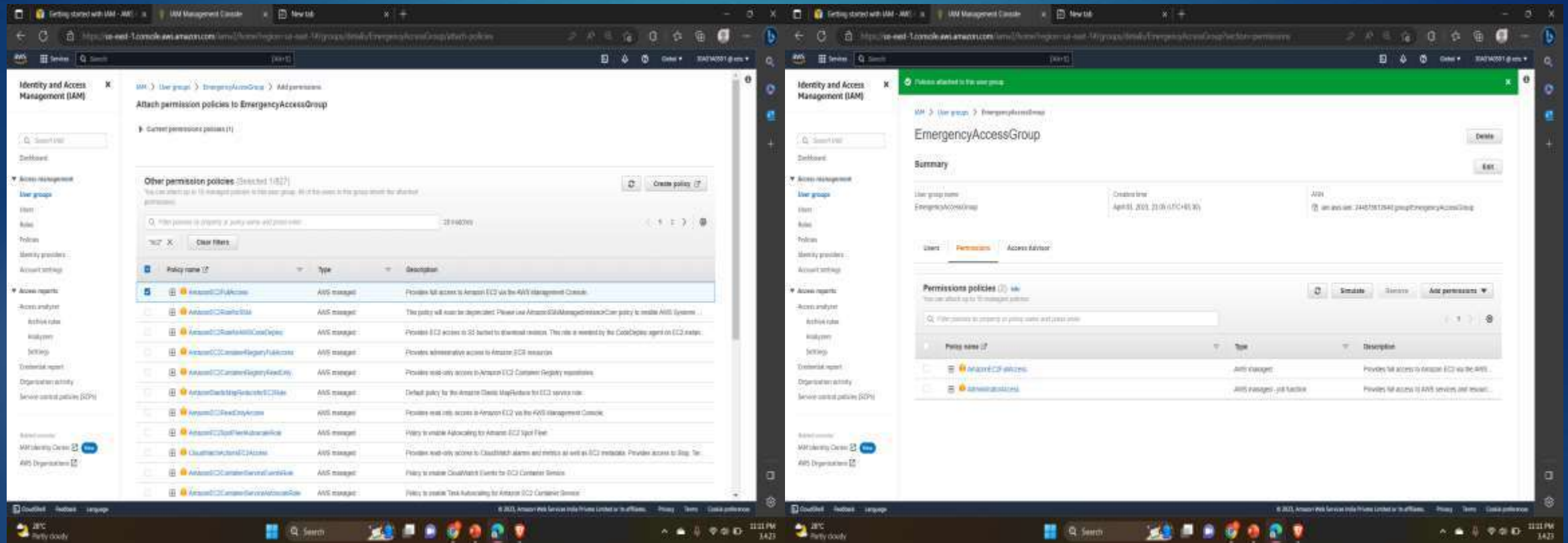


13. If you want to add permissions to the user group, then go to **User groups** and click on the respective **User group**.

14. Go to **Permissions** → **All permissions** → **Attach policies**



100





## DEPLOYEMENT OF VPC AND LAUNCHING WEB SERVER

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

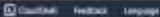
Step 4: Choose VPC and more, in name tag auto-generation, keep auto-generate select and change it to a lab.

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

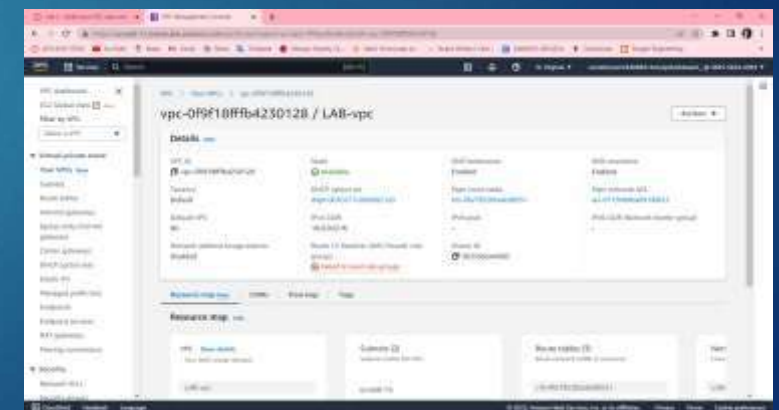
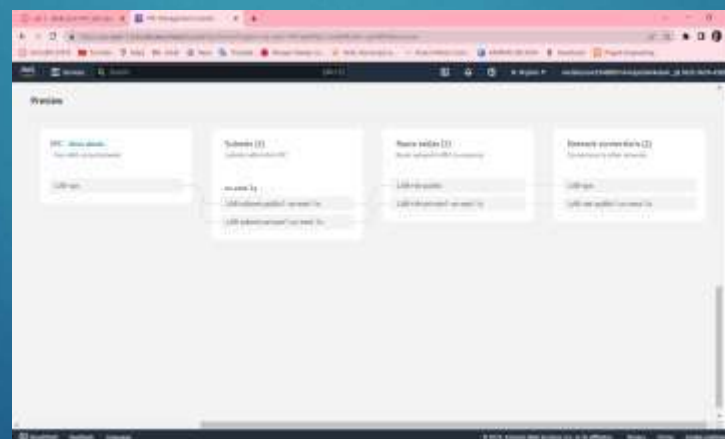
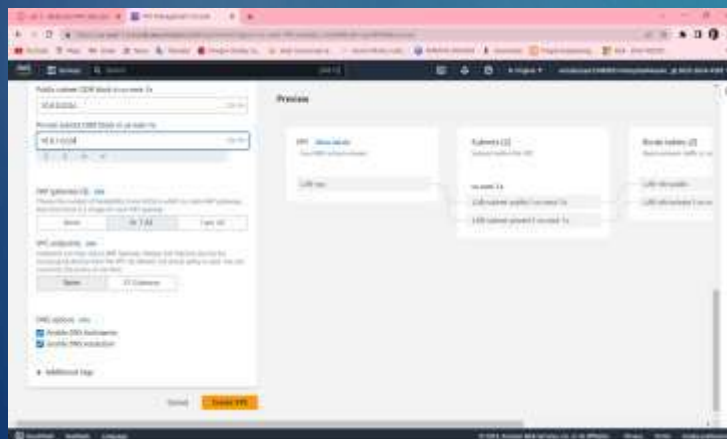
Step 5 : Leave lab-subnet-private1-us-east-1a and also select lab-subnet-private2

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



ected View • Saved to this PC

Search

Lalitha Sri Sai Manasa

LS

-

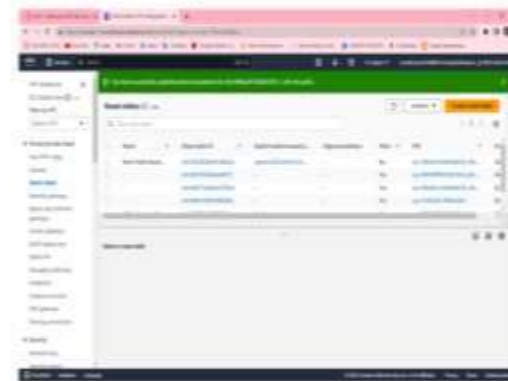
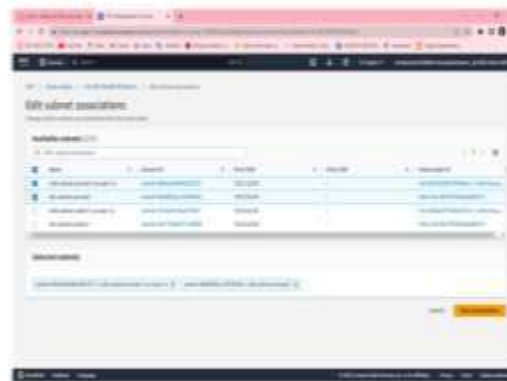
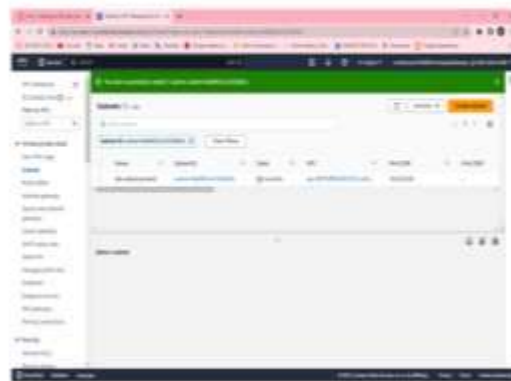
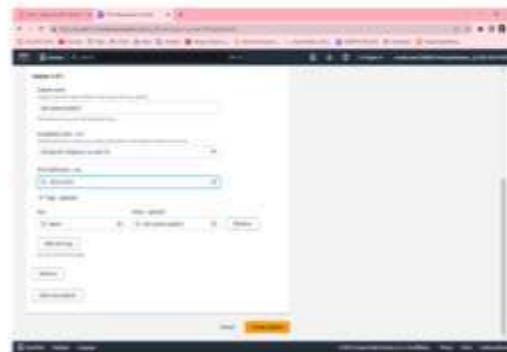
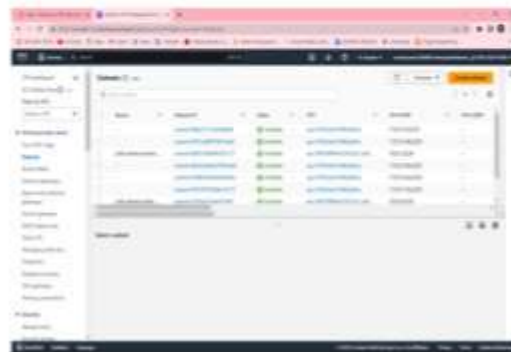
Transitions Animations Slide Show Record Review View Help

Present in Teams

Share

he Internet can contain viruses. Unless you need to edit, it's safer to stay in Protected View.

Enable Editing

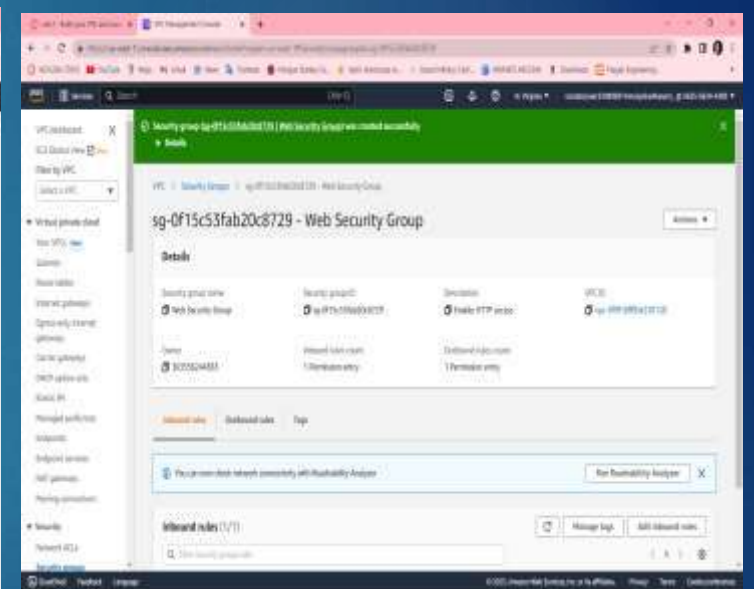
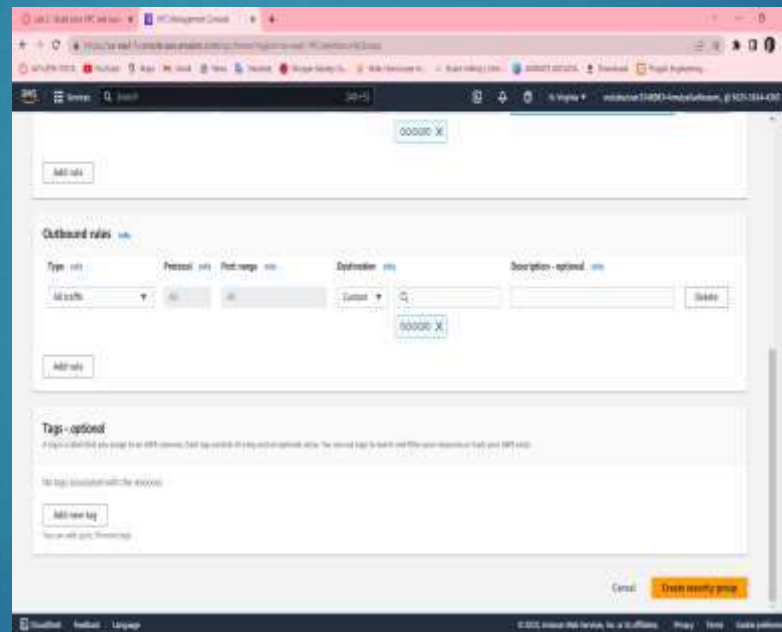
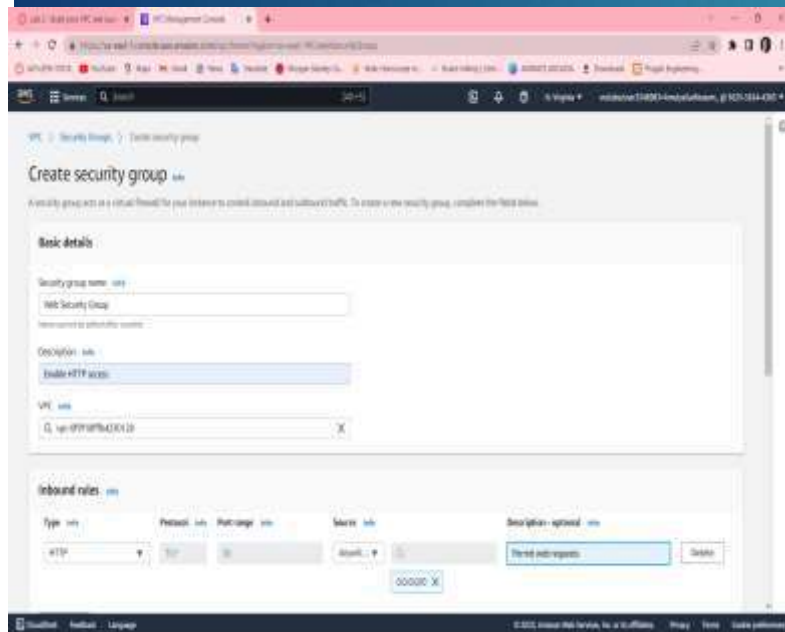




# CREATING A VPC SECURITY GROUP

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 auto 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
```

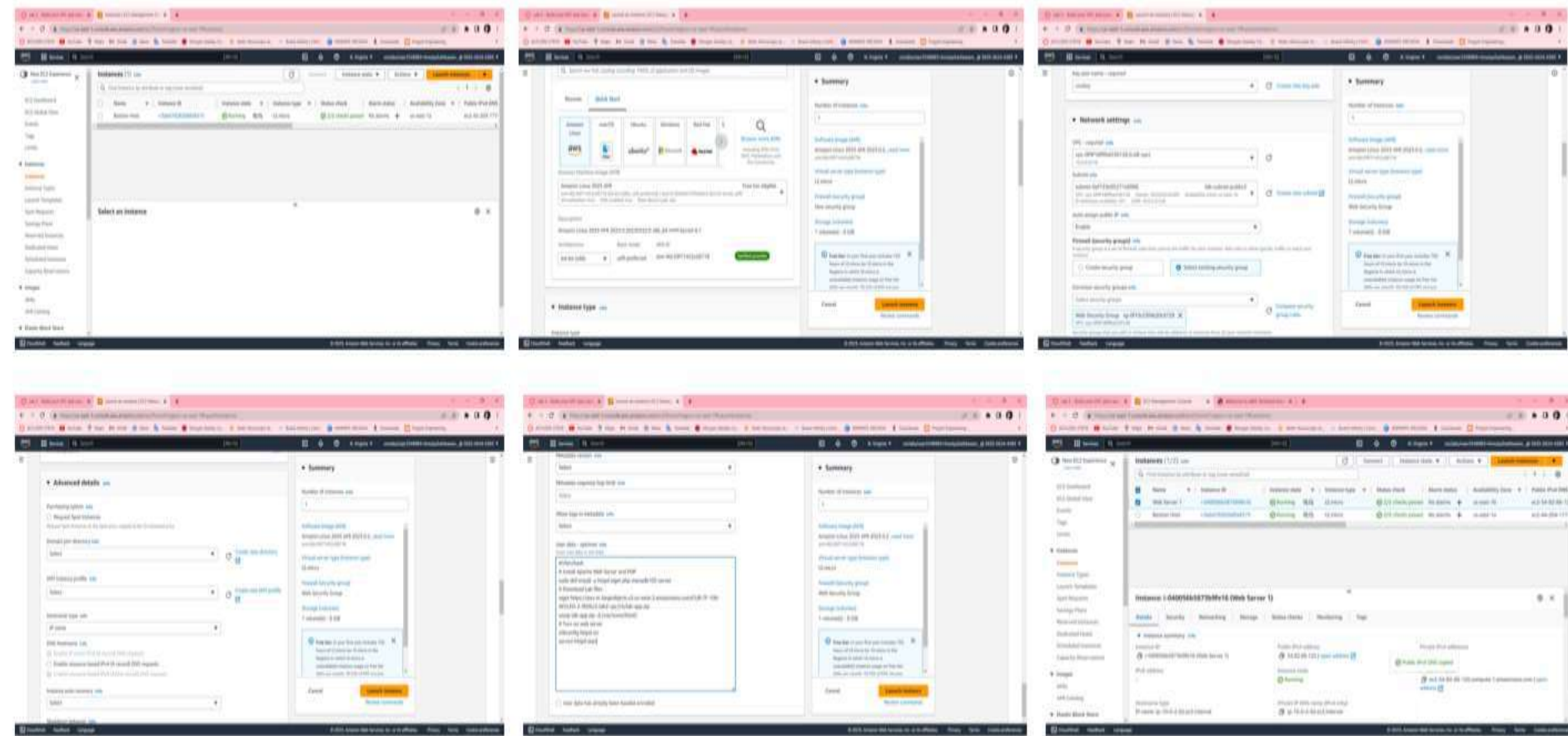
Step 6: At the bottom SUMMARY panel choose launch instance ,click on view instances

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