

AWS(Amazon Web Services)

A.Devi Krishna

20A31A05D1

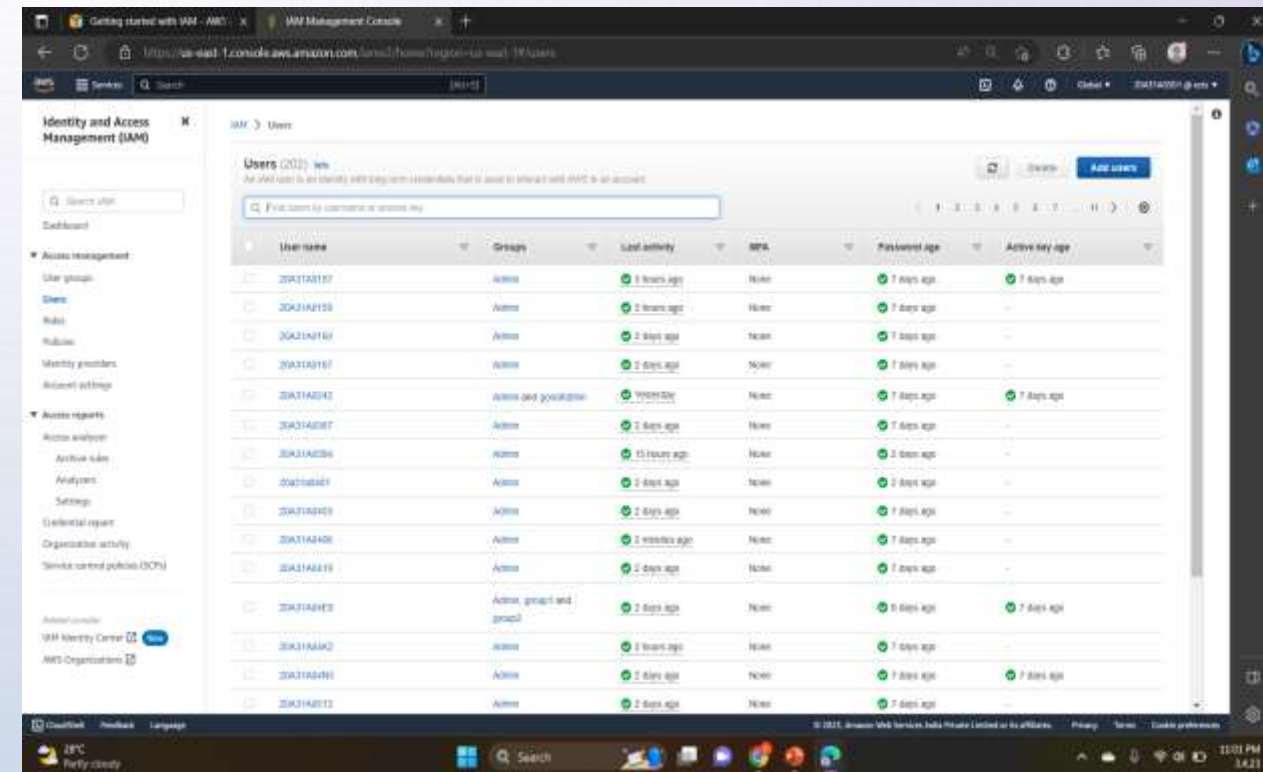
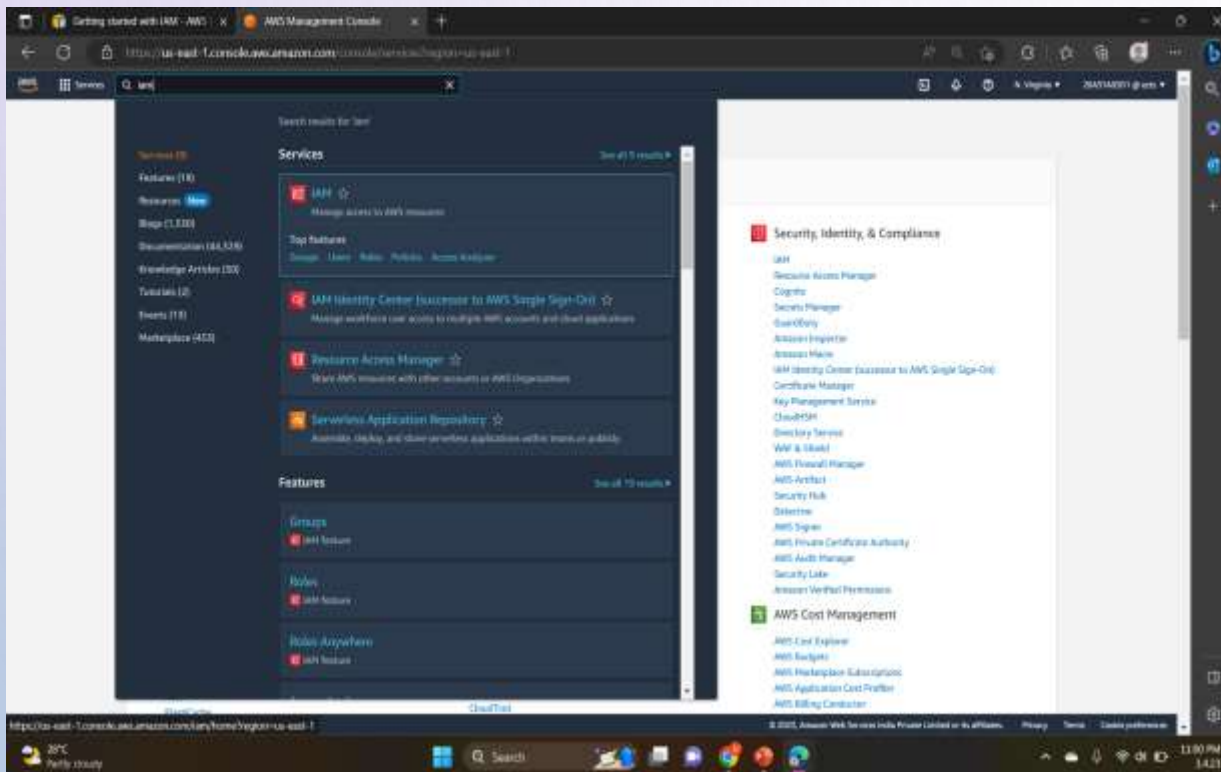
AWS Identity and Access Management (IAM)

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

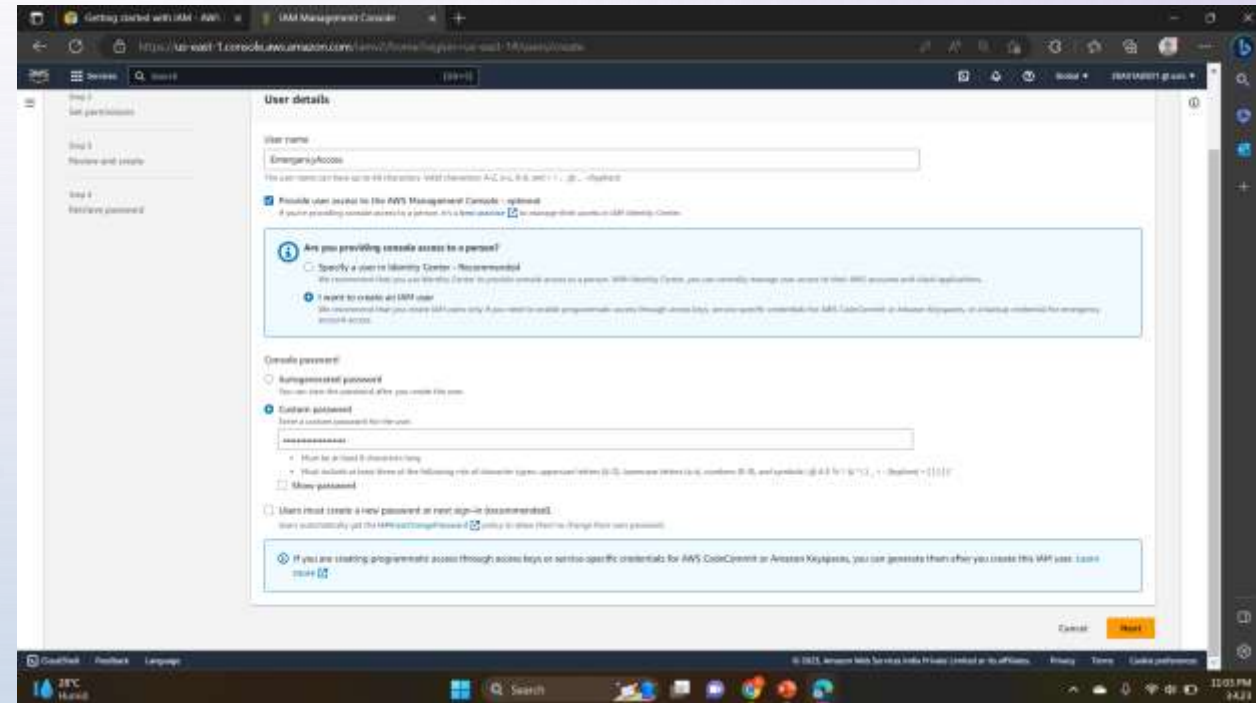
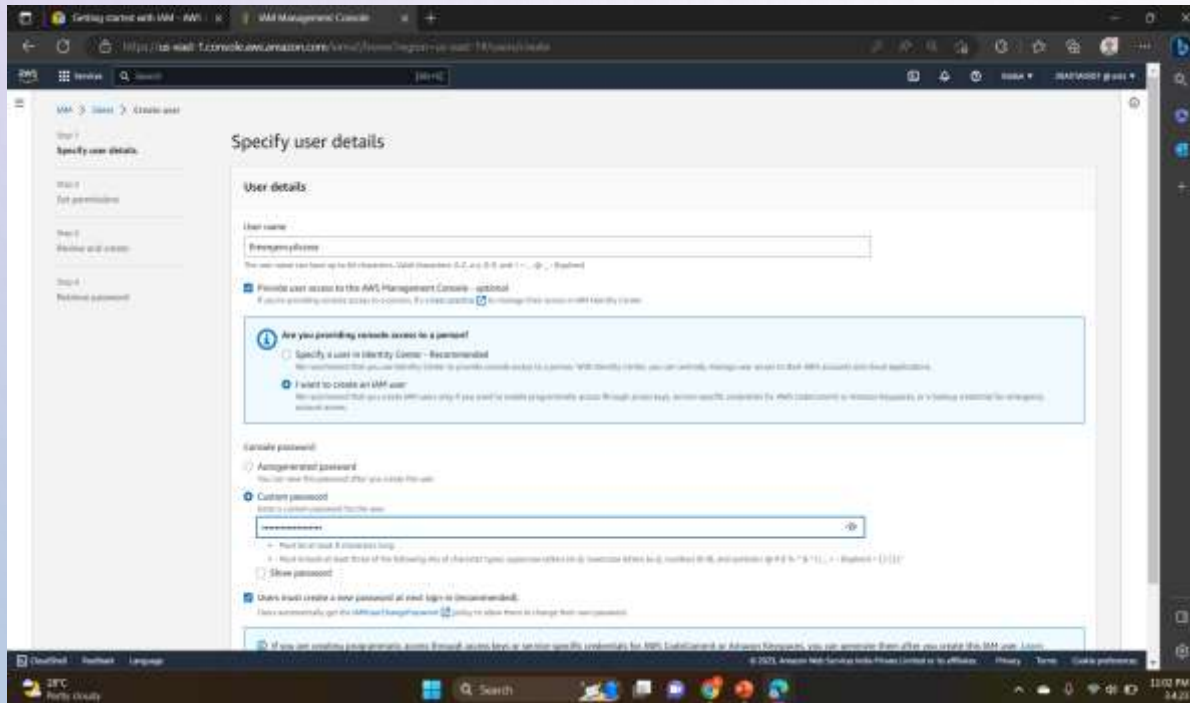
1. On the **Console Home** page, select the IAM service. 2. In the navigation pane, select **Users** and then select **Add users**.



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 **Next.**



Getting started with IAM - AWS: IAM Management Console

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

Set permissions

Add user to an existing group or create a new one. Using groups is a best practice way to manage user permissions by job functions. [Learn more](#)

Permissions options

- ☒ Add user to group
Add user to an existing group or create a new group. We recommend using groups to manage user permissions by job function.
- ☐ Copy permissions
Use all group membership, attached managed policies, and other settings from an existing user.
- ☐ Attach policies directly
Attach a managed policy directly to a user. We recommend attaching policies to a group instead. Then, add the user to the appropriate group.

User groups (132)

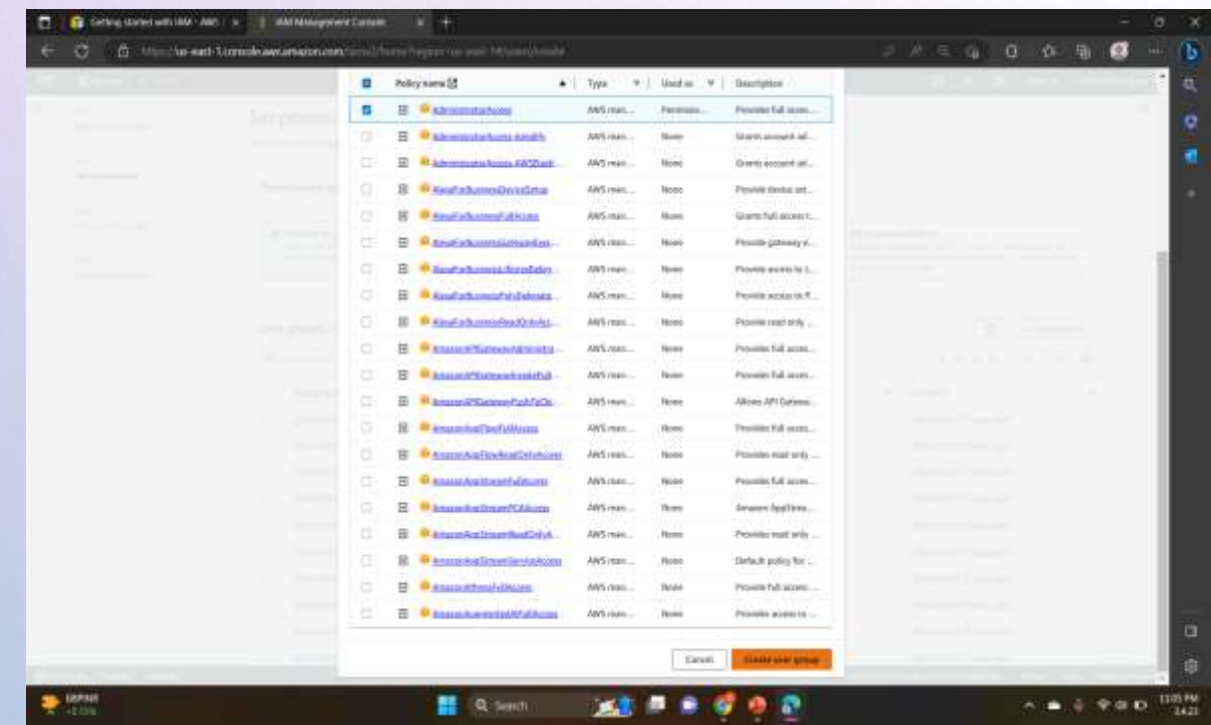
Search groups

Group name	Users	Attached policies	Created
glue2-readonly	0	AwsAccountUsageReadOnly	2023-03-27 (7 days ago)
20x31A314Group	1	AwsAccountUsageReadOnly	2023-03-27 (7 days ago)
20x31A314ReadOnly	1	AwsAccountUsageReadOnly	2023-03-27 (7 days ago)
20x31A314Group	0	AwsAccountUsageReadOnly	2023-03-27 (7 days ago)
20x31A314G1	1	AwsAccountUsageReadOnly	2023-03-27 (7 days ago)
20x31A314G2	1	AwsAccountUsageReadOnly	2023-03-27 (7 days ago)
20x31A314G3	0	AwsAccountUsageReadOnly	2023-03-27 (7 days ago)
20x31A314G4	0	AwsAccountUsageReadOnly	2023-03-27 (7 days ago)
20x31A314G5	1	AwsAccountUsageReadOnly	2023-03-27 (7 days ago)
20x31A314G6	0	AwsAccountUsageReadOnly	2023-03-27 (7 days ago)

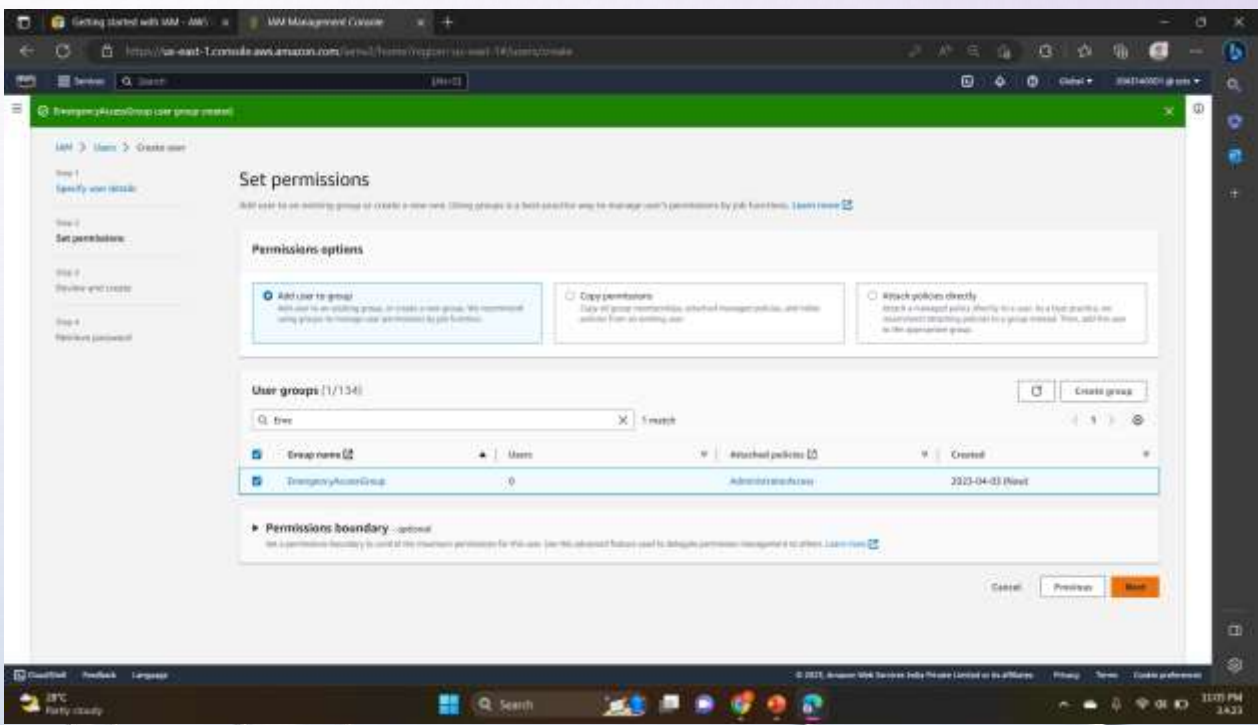
© 2023 Amazon Web Services, Inc. All rights reserved. Privacy Terms Account preferences

[illegible]

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



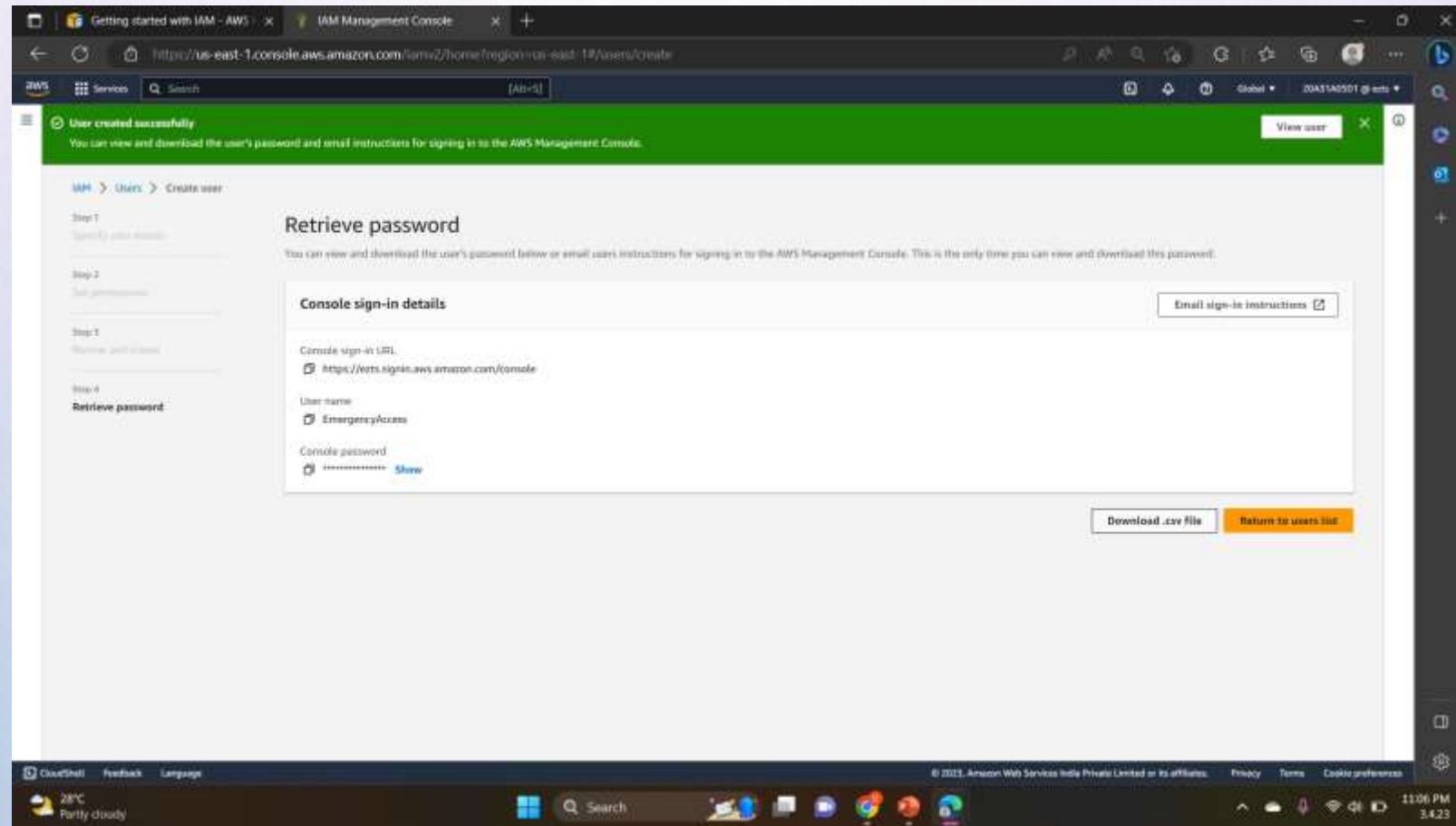
9. Select **Next** to proceed to the **Review and create** page.



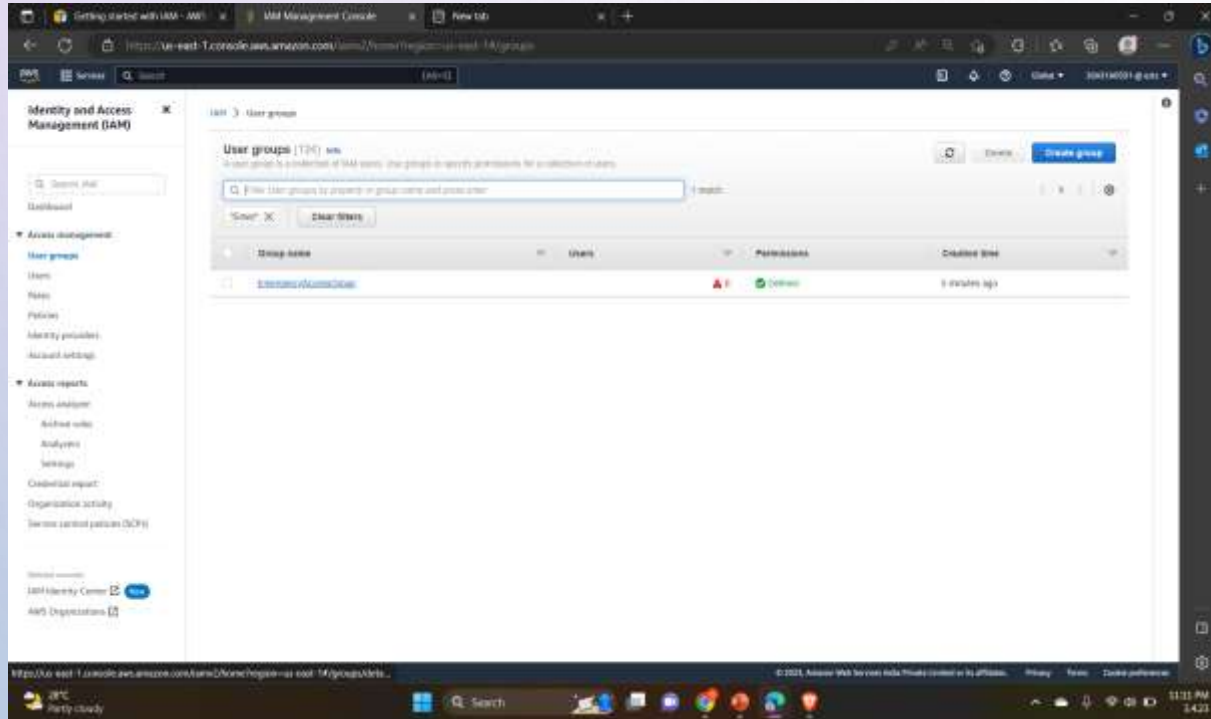
10. On the **Review and create** page, review the list of user group memberships to be added to the new user. When you are ready to proceed, select **Create user**.

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).

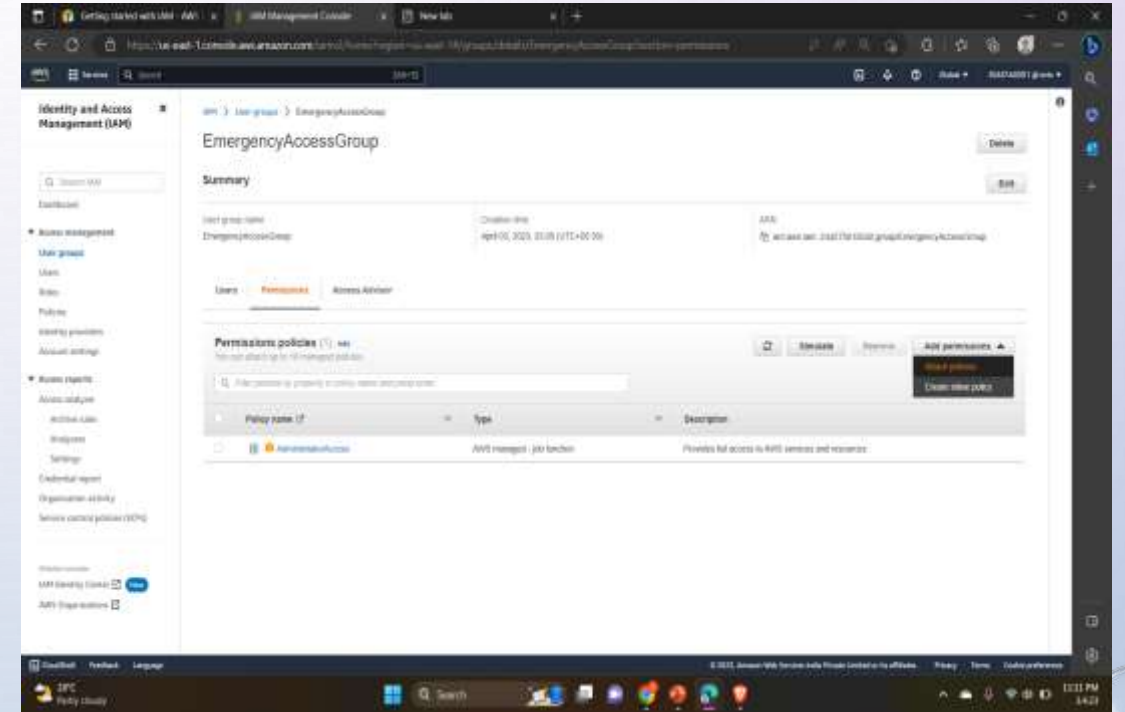
12. Save this file to use if you need to sign-in to IAM and do not have access to your federated identity provider.



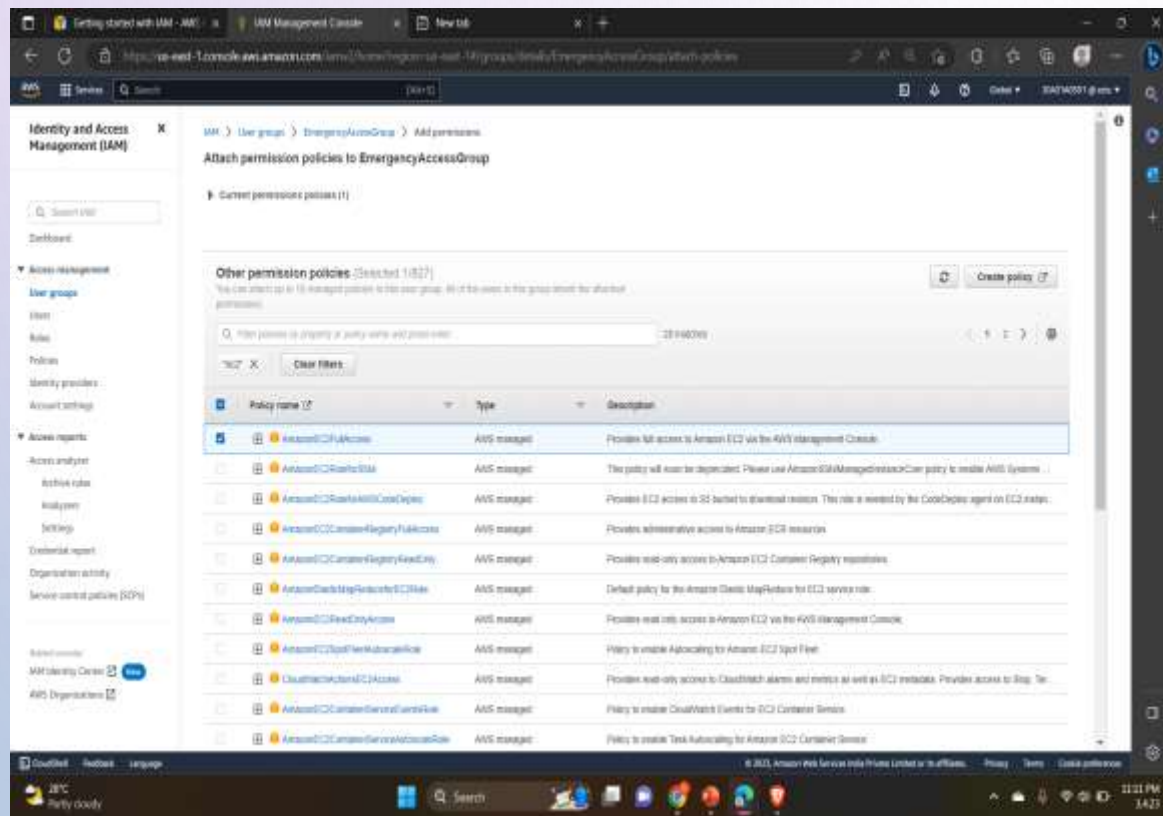
13. If you want to add permissions to the user group, then go to **User groups** and click on the respective **User group**.



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

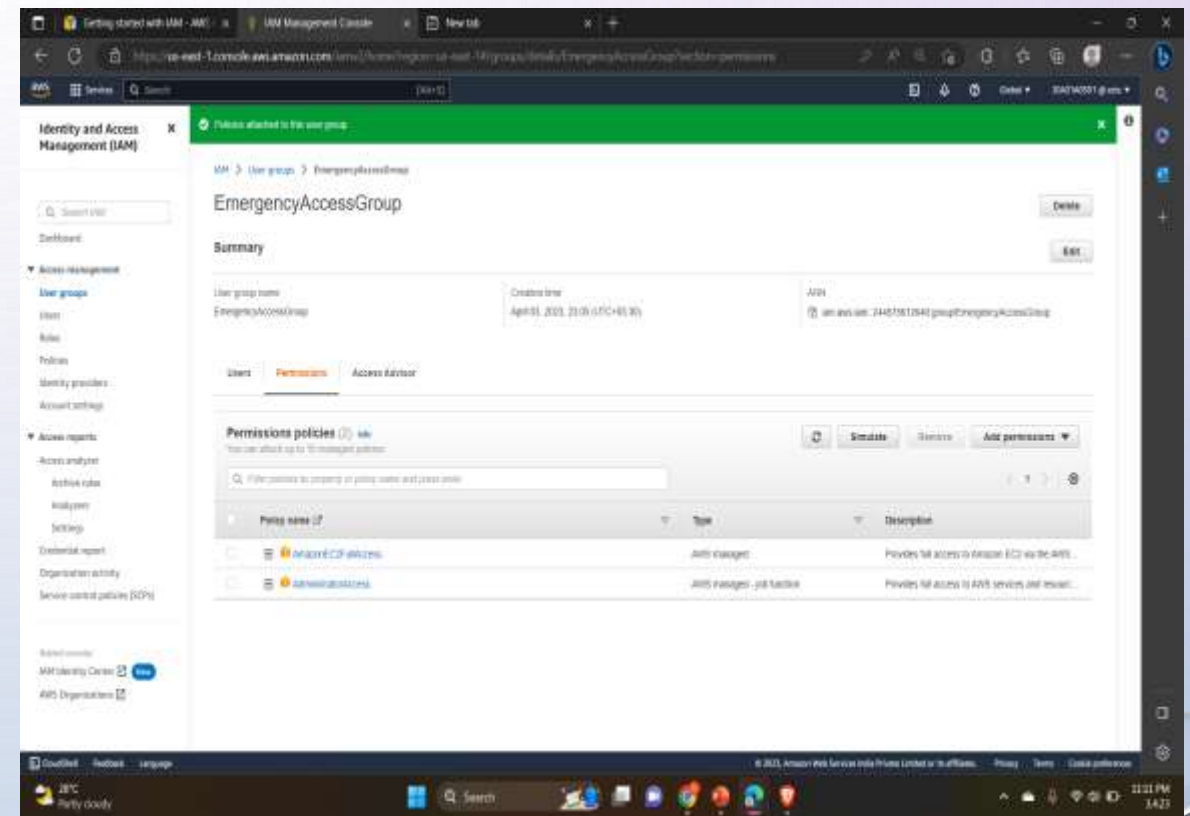


15. Add the permission policy and the policy is attached to the **User group**.



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, there's a section for 'Current permission policies (1)' which is empty. The main area is titled 'Other permission policies (Selected: 1/827)' and contains a search bar and a table of policies.

Policy name	Type	Description
<input checked="" type="checkbox"/> AmazonEC2FullAccess	AWS managed	Provides full access to Amazon EC2 via the AWS Management Console.
<input type="checkbox"/> AmazonEC2ReadOnlyAccess	AWS managed	The policy will never be dependent. Please use AmazonSSMManagedInstanceCore policy to enable AWS Systems Manager.
<input type="checkbox"/> AmazonEC2ReadOnlyAccessDelegator	AWS managed	Provides EC2 access to S3 bucket to download images. This role is needed by the CodeDeploy agent on EC2 instances.
<input type="checkbox"/> AmazonEC2ContainerRegistryFullAccess	AWS managed	Provides administrative access to Amazon ECR resources.
<input type="checkbox"/> AmazonEC2ContainerRegistryReadOnly	AWS managed	Provides read-only access to Amazon ECR Container Registry resources.
<input type="checkbox"/> AmazonElasticMapReduceEC2Role	AWS managed	Default policy for the Amazon Elastic MapReduce for EC2 service role.
<input type="checkbox"/> AmazonEC2ReadOnlyAccess	AWS managed	Provides read-only access to Amazon EC2 via the AWS Management Console.
<input type="checkbox"/> AmazonEC2SpotFleetAccess	AWS managed	Policy to enable AutoScaling for Amazon EC2 Spot Fleet.
<input type="checkbox"/> CloudWatchEventsRole	AWS managed	Provides read-only access to CloudWatch alarms and metrics as well as EC2 metadata. Provides access to Stop. To.
<input type="checkbox"/> AmazonEC2ContainerServiceReadOnlyAccess	AWS managed	Policy to enable CloudWatch Events for EC2 Container Service.
<input type="checkbox"/> AmazonEC2ContainerServiceReadOnlyAccessRole	AWS managed	Policy to enable Task Automating for Amazon EC2 Container Service.



The screenshot shows the AWS IAM console interface for the 'EmergencyAccessGroup' user group. The breadcrumb navigation is 'IAM > User groups > EmergencyAccessGroup'. The main heading is 'EmergencyAccessGroup'. Below this, there's a 'Summary' section with details about the user group. The 'Permissions' tab is selected, showing a list of attached permission policies.

Summary

User group name	Created time	ARN
EmergencyAccessGroup	April 8, 2023, 11:06 (UTC+05:30)	arn:aws:iam::244518128401:group/EmergencyAccessGroup

Permissions policies (1)

Policy name	Type	Description
<input checked="" type="checkbox"/> AmazonEC2FullAccess	AWS managed	Provides full access to Amazon EC2 via the AWS...
<input checked="" type="checkbox"/> AmazonElasticMapReduceEC2Role	AWS managed - job function	Provides full access to AWS services and resour...

EC2 INSTANCE

CREATING AN 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.

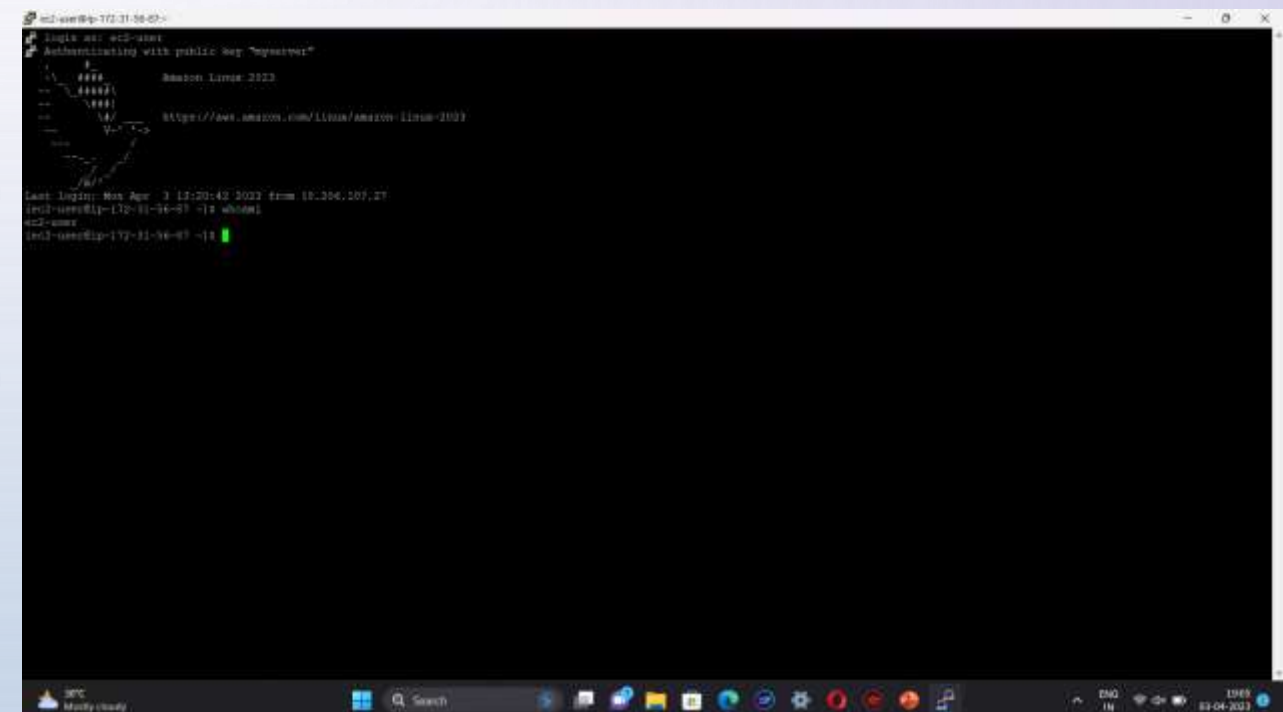
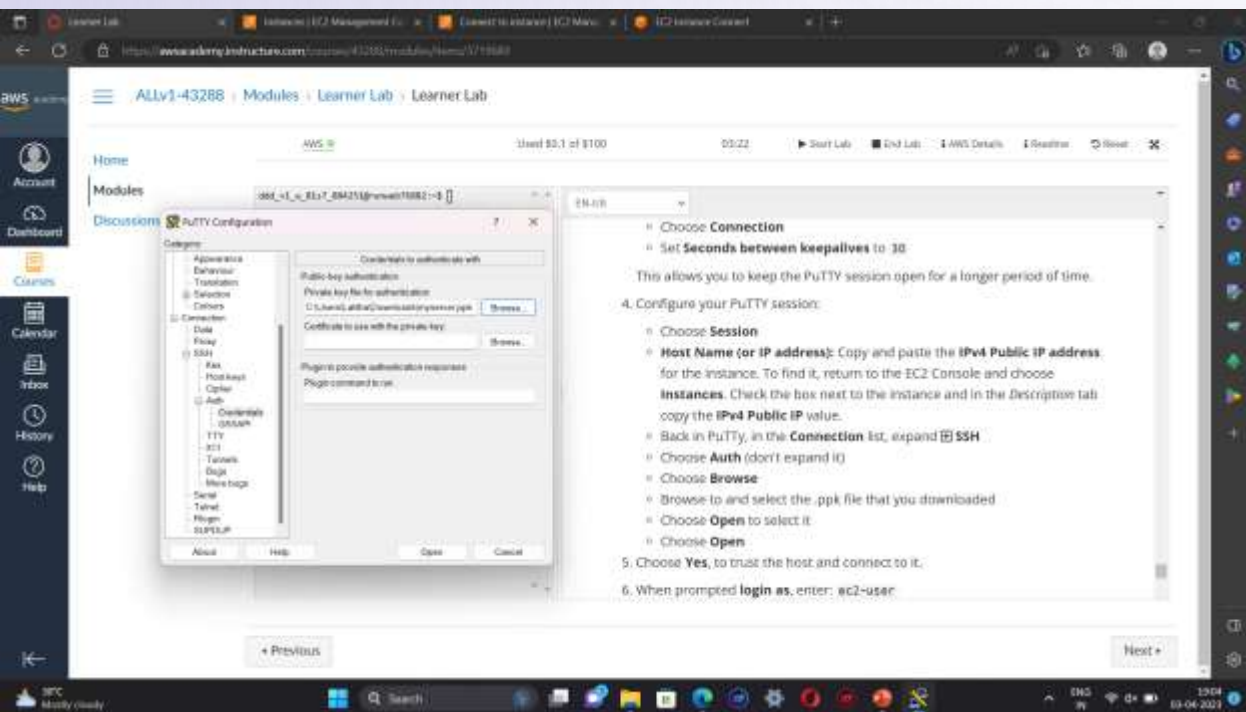
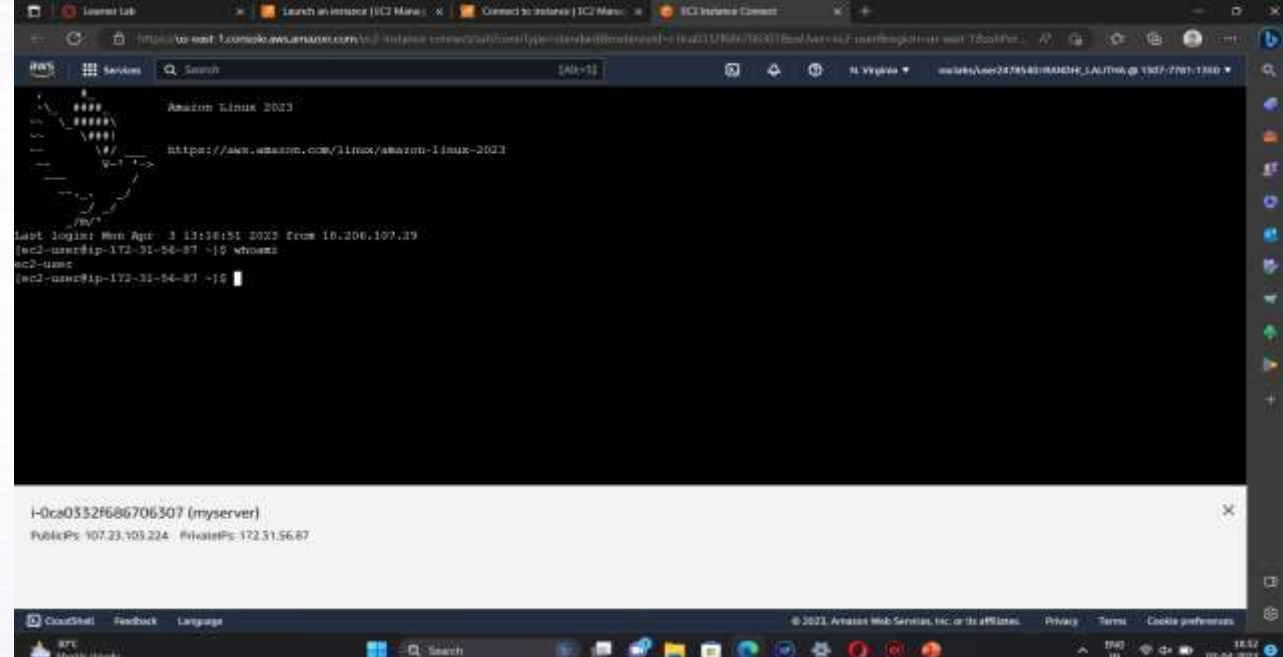
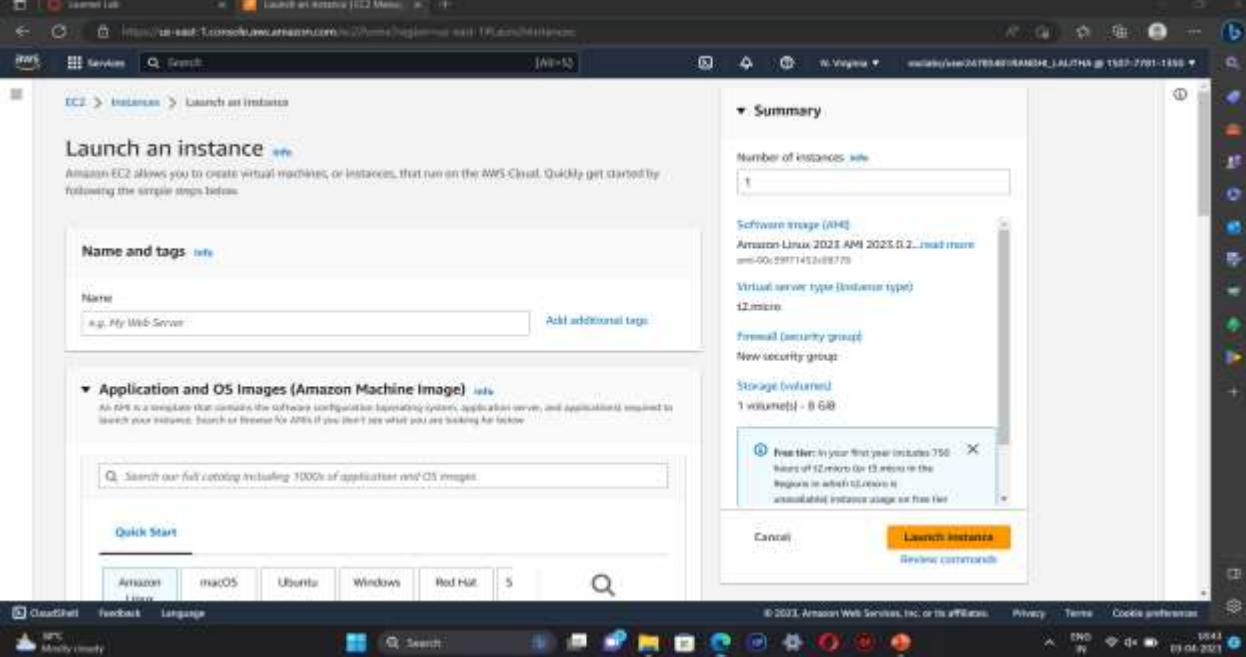
Step-3: For linux-select ppk key and for windows server-select pem key.

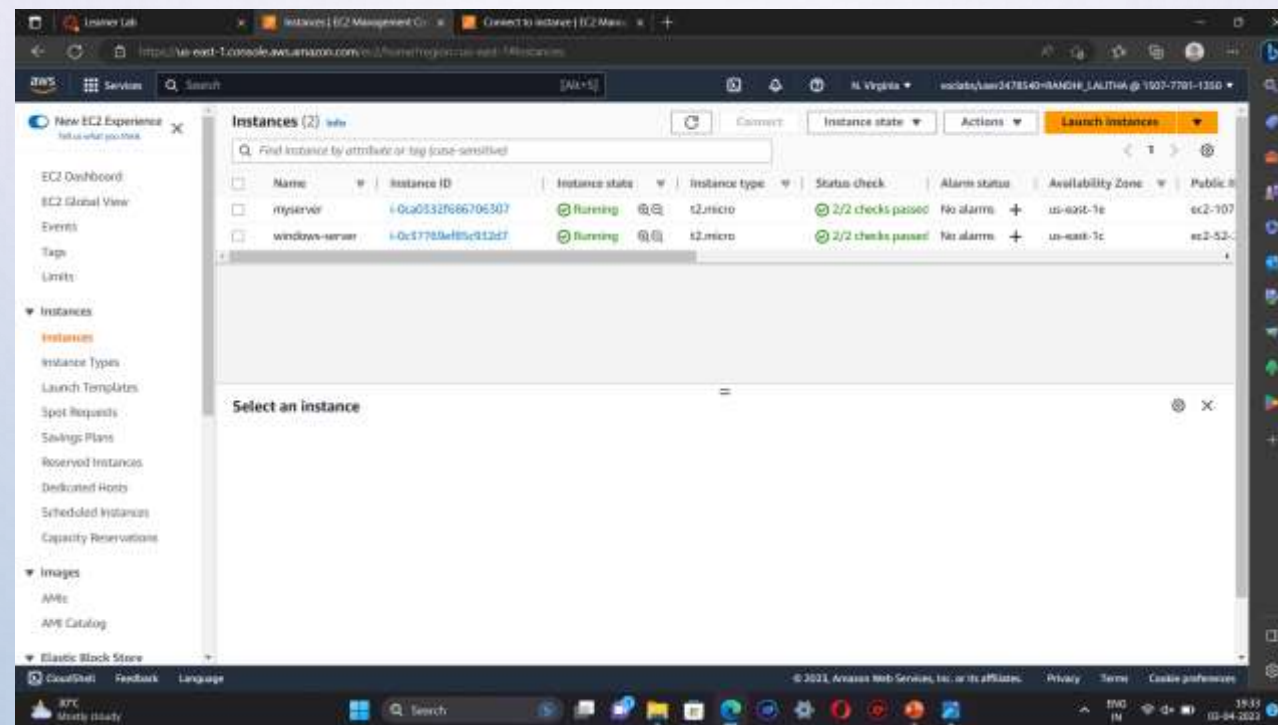
Step-4: If a key pair is not available create a new key.

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 .





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 the text "Customer 1". At the bottom left, there is a small instruction: "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.

8. 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.



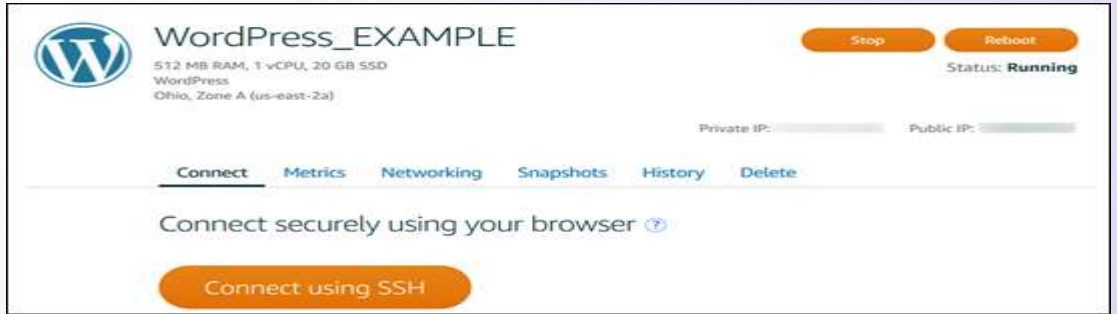

A dialog box titled "Key-value tags". It contains two text input fields. The first field is labeled "Key" and contains the text "Project". The second field is labeled "Value" and contains the text "Earth". A right-pointing arrow is positioned between the two fields. To the right of the fields are two buttons: "Cancel" with a red X icon and "Save" with a green checkmark icon and a mouse cursor icon pointing at it.

9. 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.



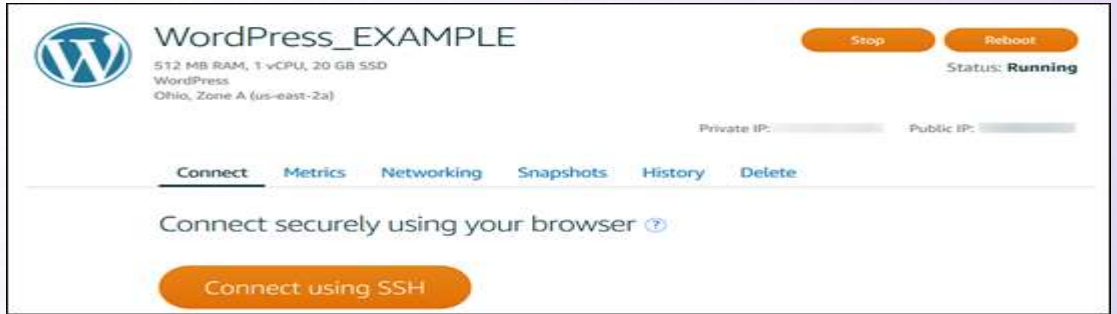

Alternately, you can open your instance management page and choose the Connect tab.

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



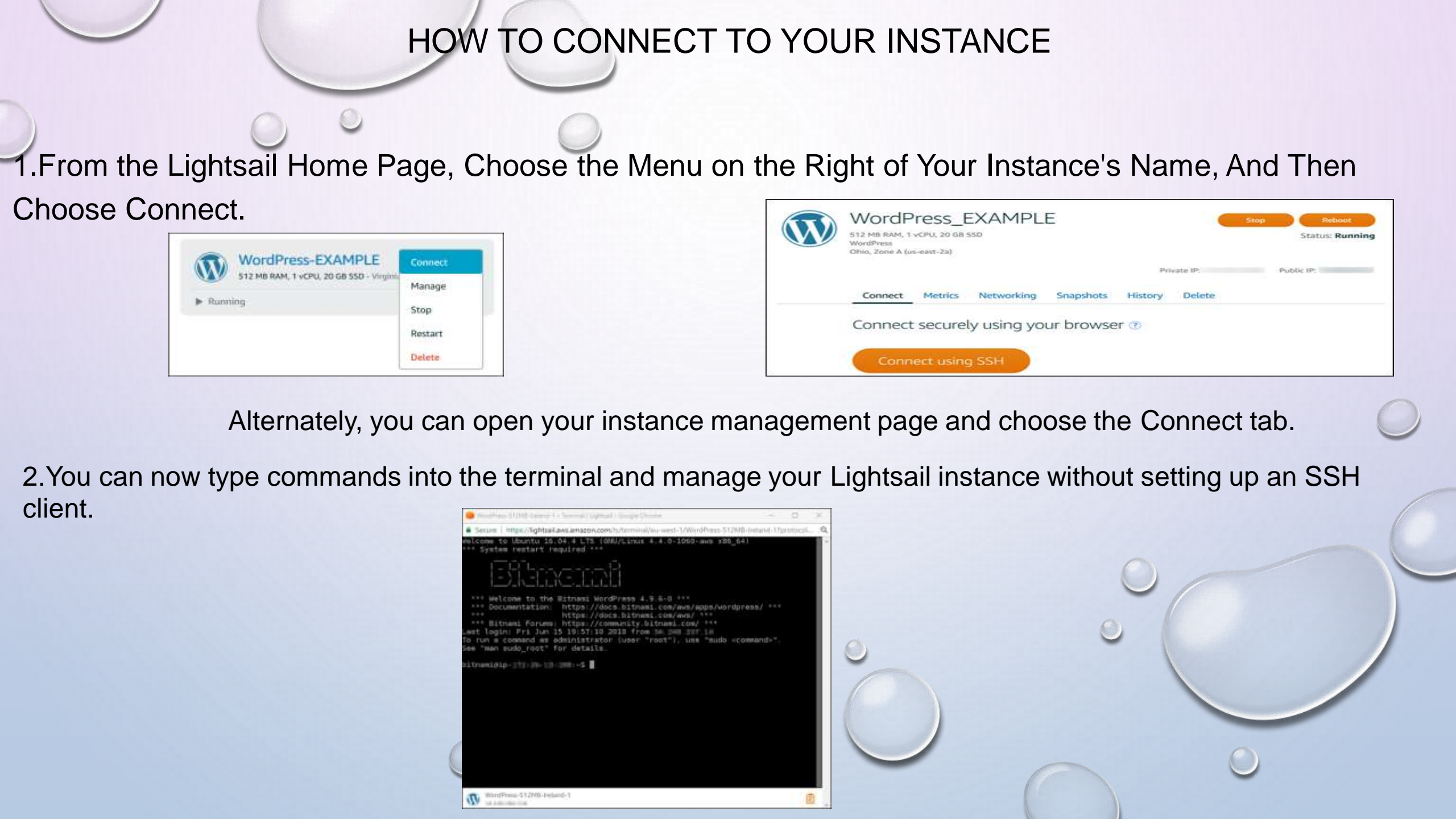
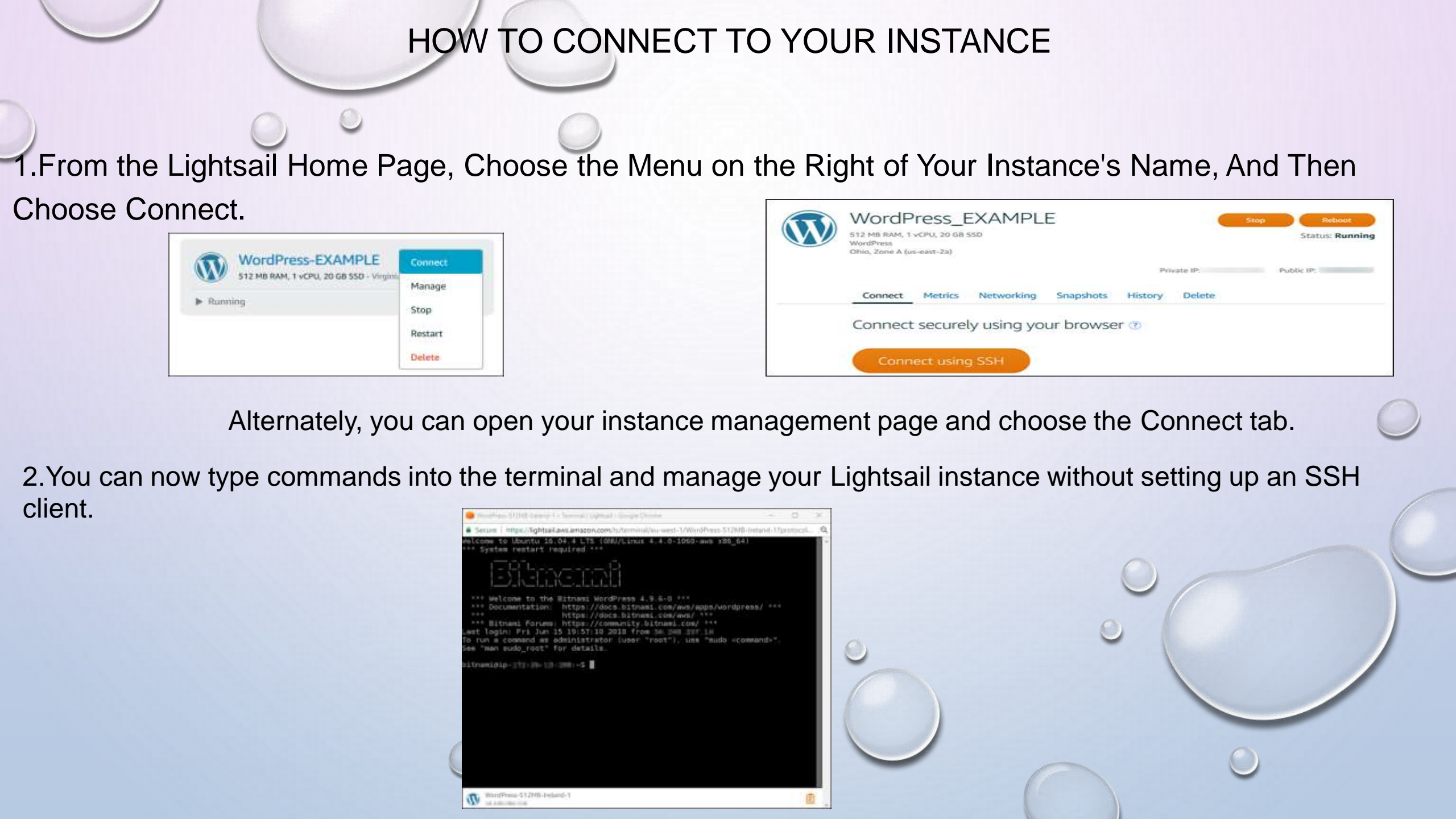

HOW TO CONNECT TO YOUR INSTANCE

1. From the Lightsail Home Page, Choose the Menu on the Right of Your Instance's Name, And Then Choose Connect.



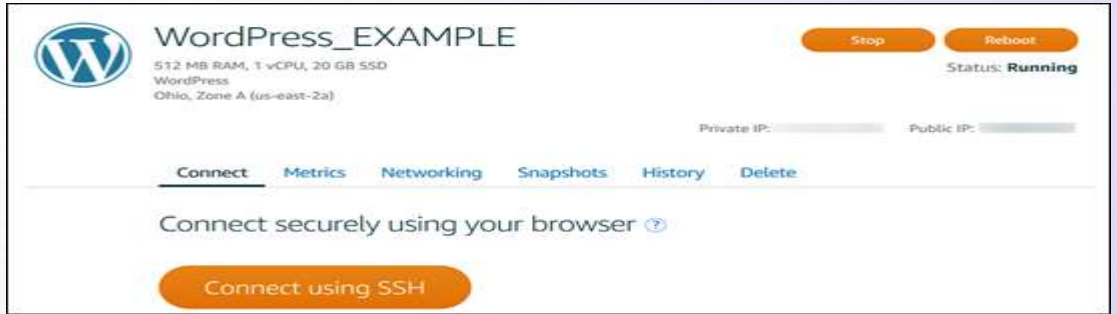

Alternately, you can open your instance management page and choose the Connect tab.

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




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.



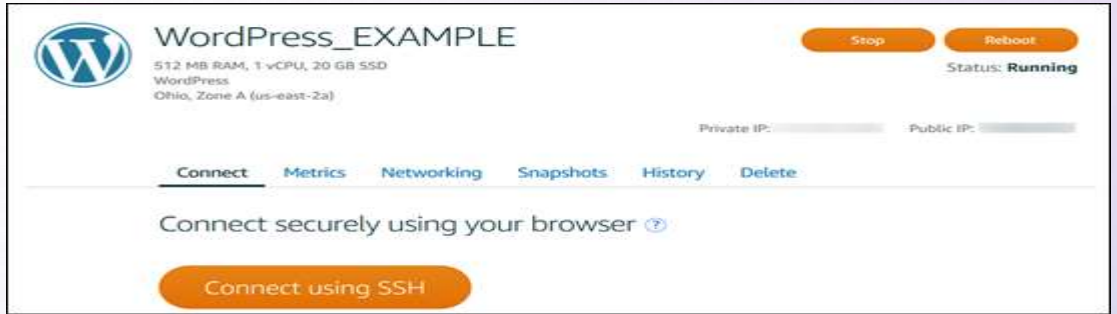

Alternately, you can open your instance management page and choose the Connect tab.

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



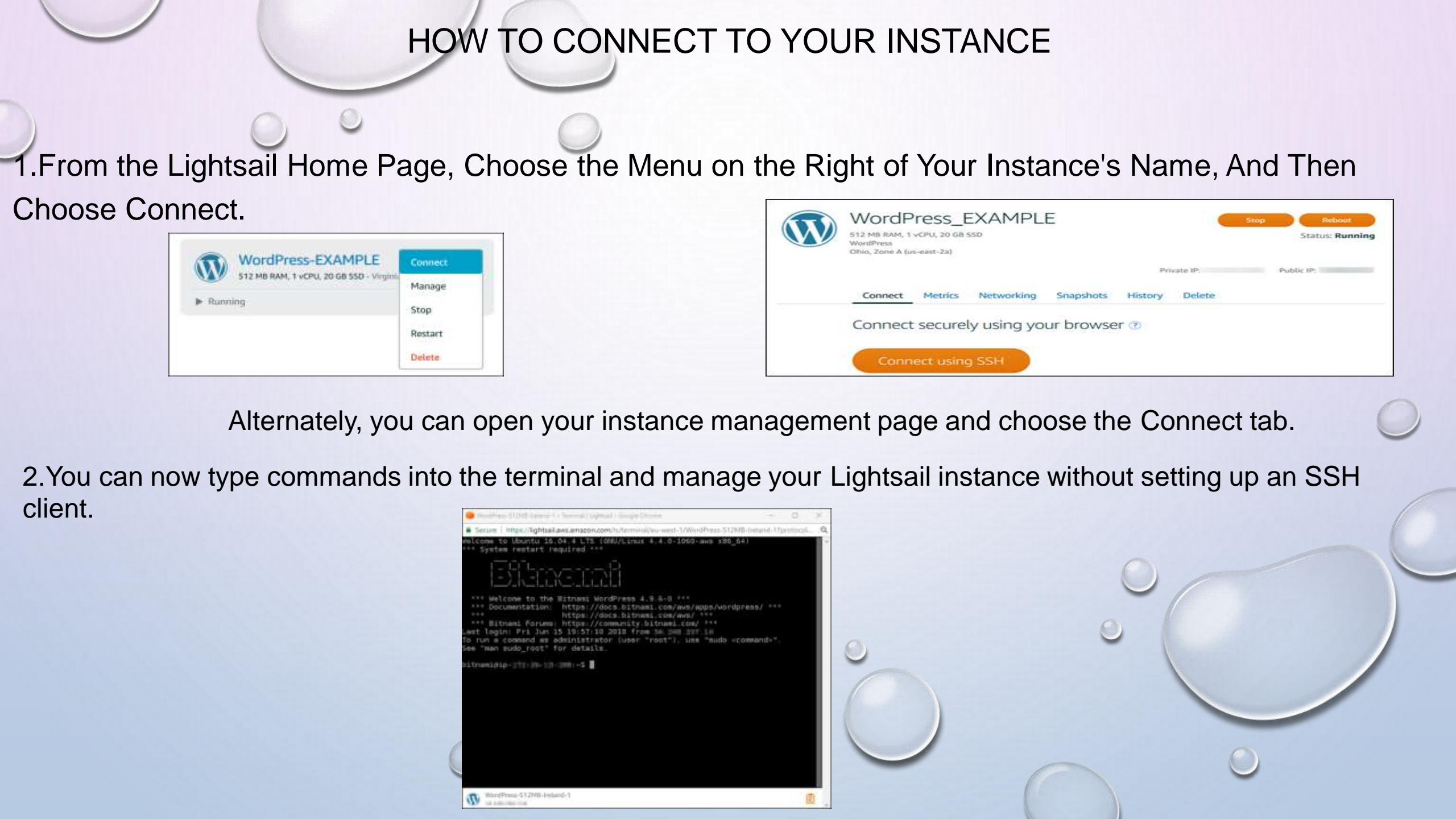

HOW TO CONNECT TO YOUR INSTANCE

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.

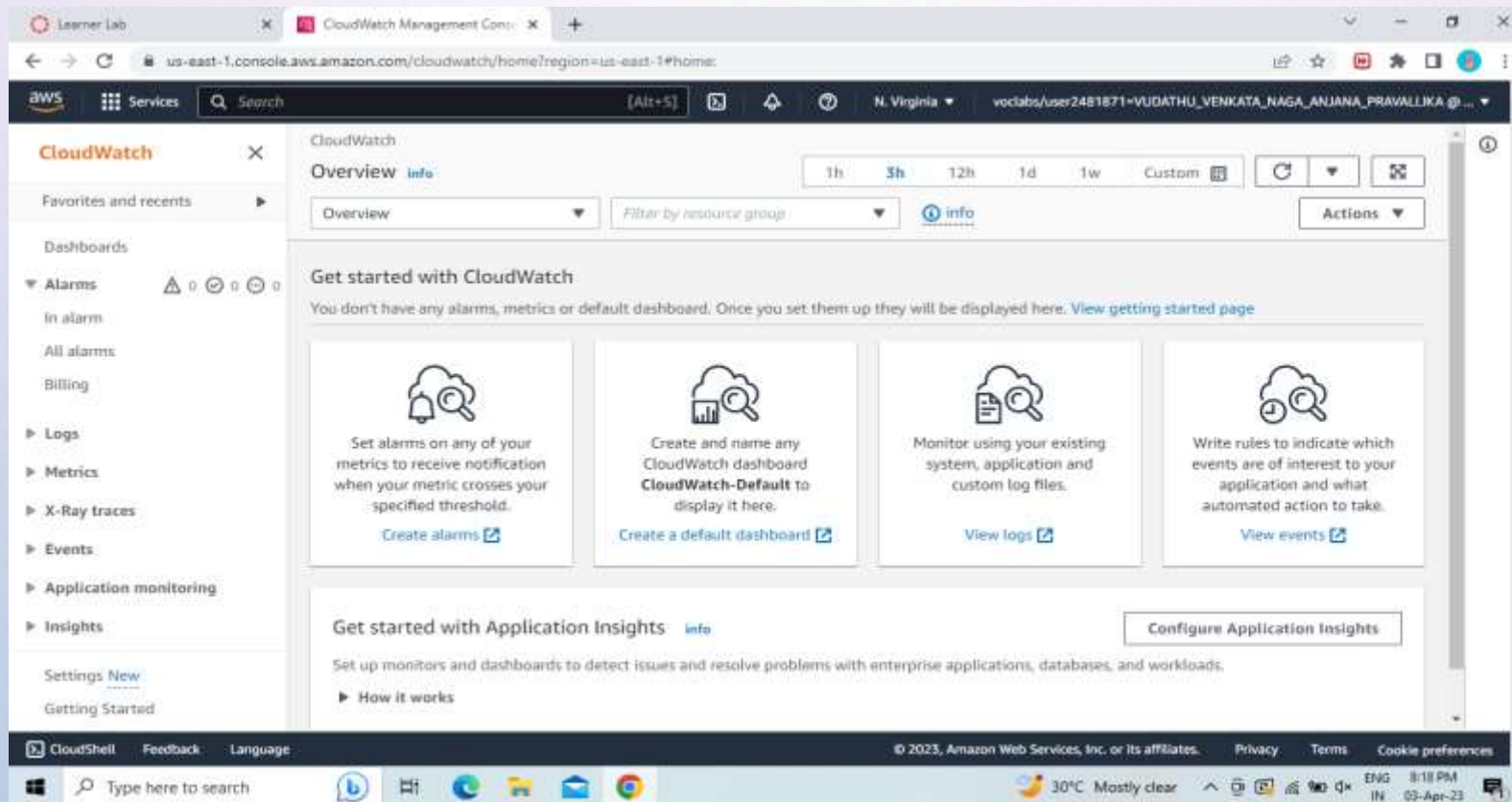
2. You can now type commands into the terminal and manage your Lightsail instance without setting up an SSH client.



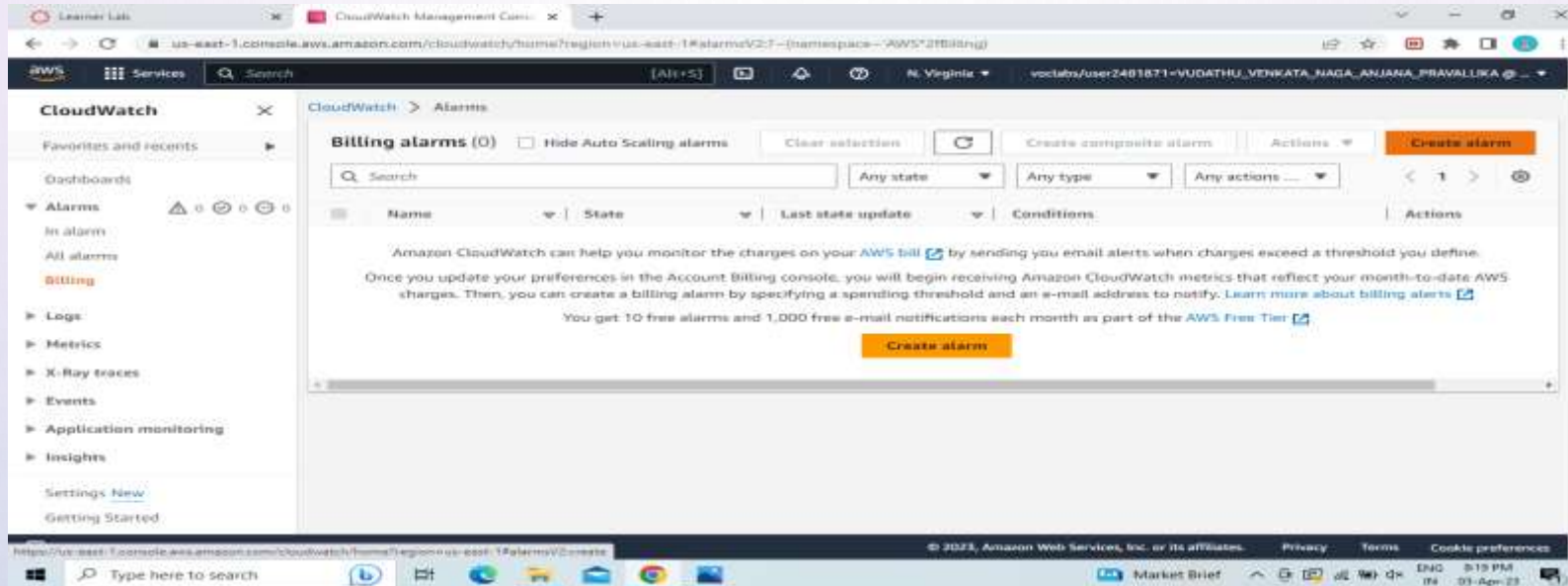
AWS CLOUDWATCH

PROCEDURE

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.



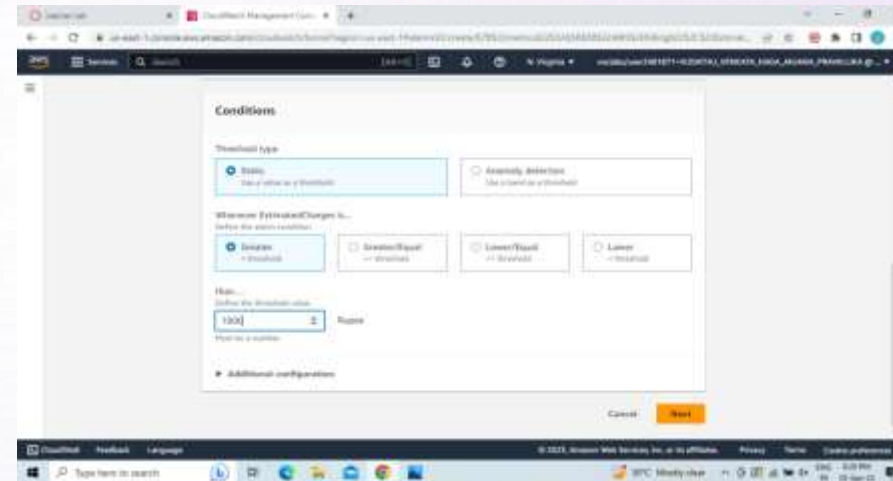
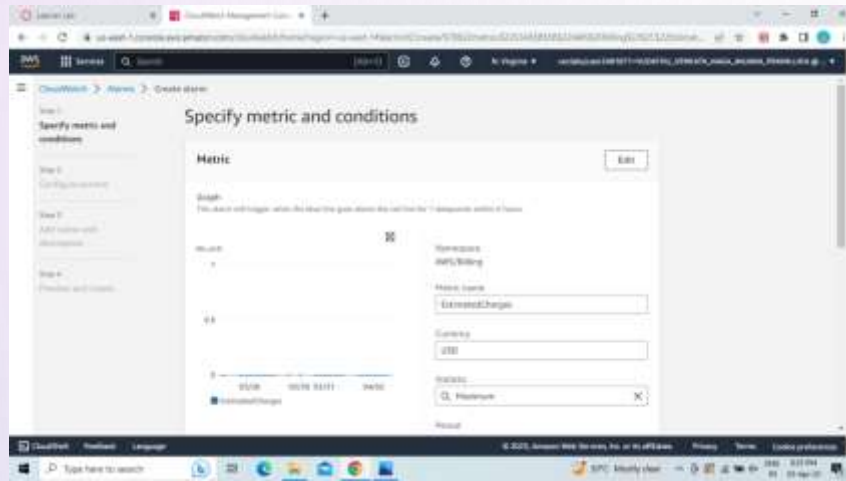
3.Then follow the steps.

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

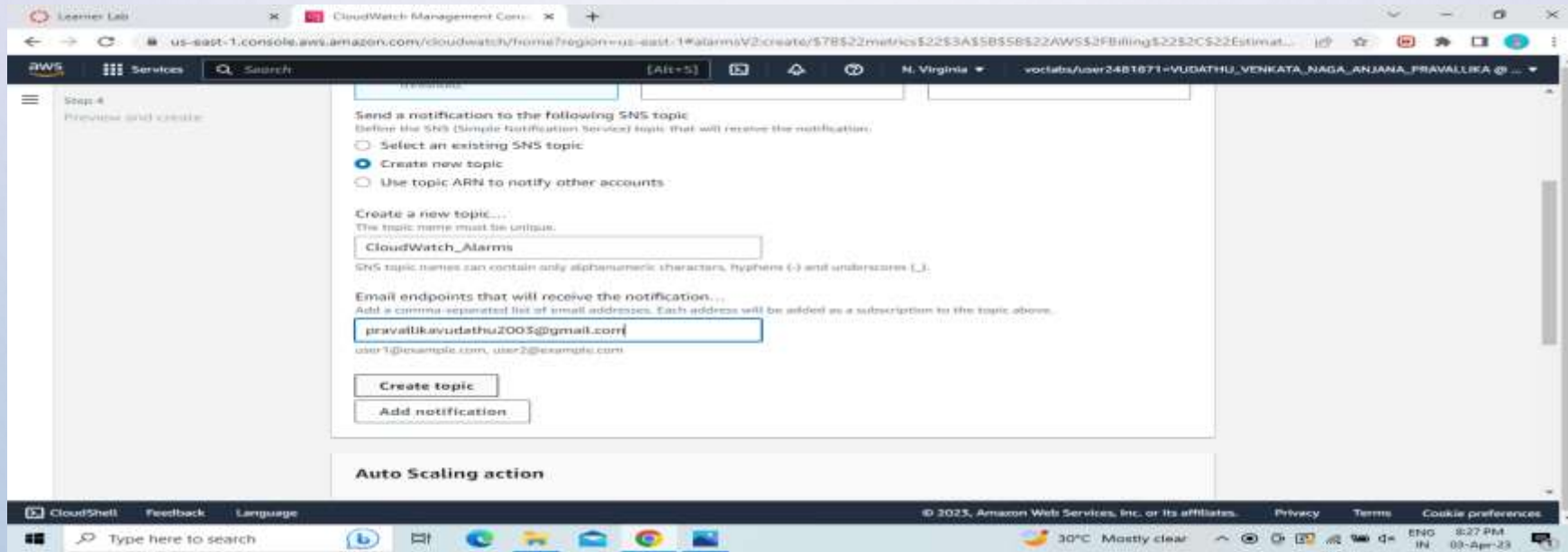
Change the Currency to Rupee.

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

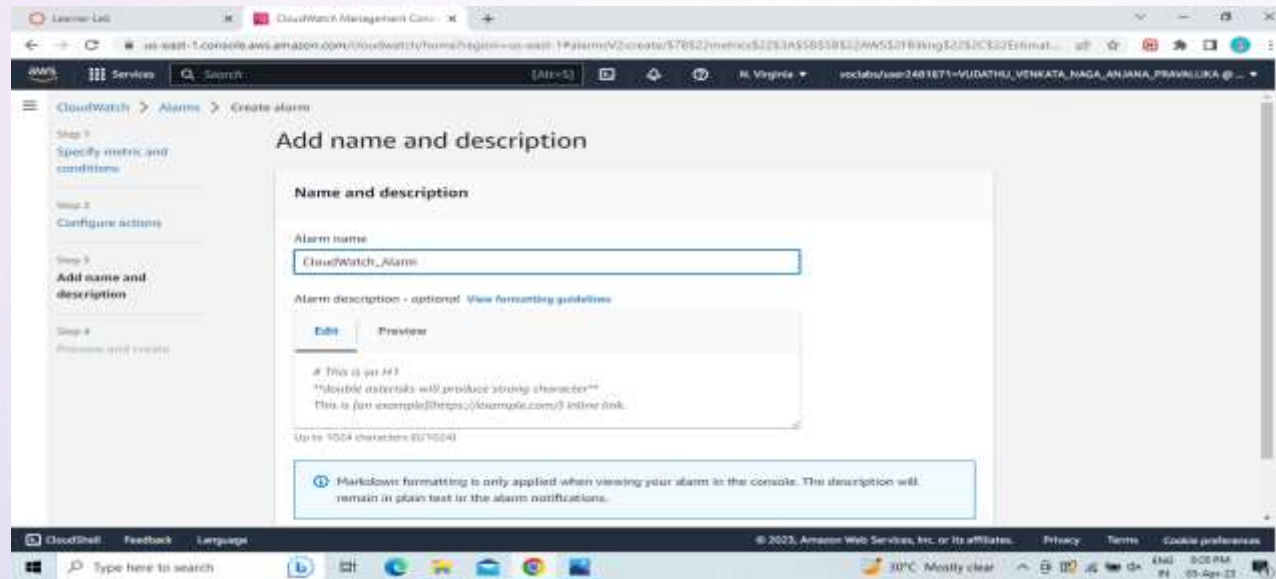
4.Click on Next.



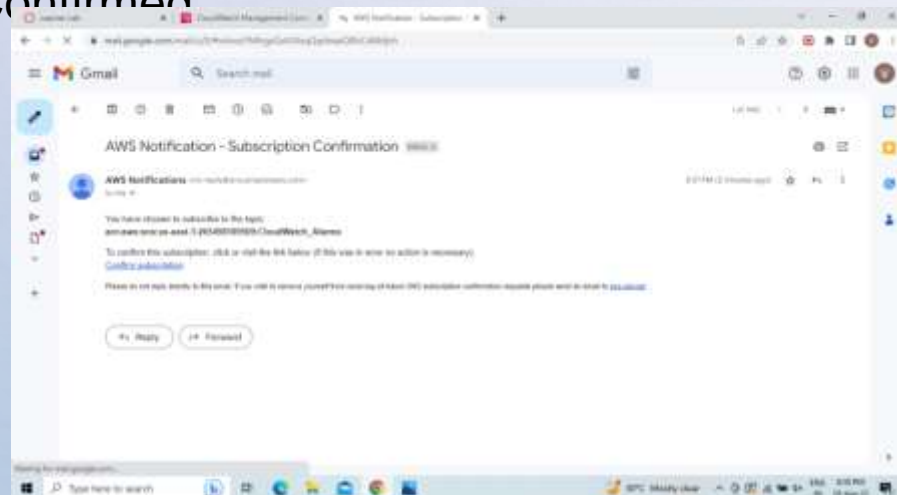
5. Now for Configure Actions choose Create new topic. Give a name to the topic and enter your email to receive a notification. Click on Create Topic, then Next.



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.

The screenshot displays the AWS CloudWatch console interface. At the top, a green banner indicates "Successfully created alarm CloudWatch_Alarm." with a "View alarm" button. The left sidebar shows the navigation menu with "Alarms" selected. The main content area shows "Billing alarms (1)" with a table listing the alarm. The table has columns for Name, State, Last state update, Conditions, and Actions. The alarm "CloudWatch_Alarm" is in the "Insufficient data" state, with a last state update of "2023-04-03 20:30:53" and a condition of "EstimatedCharges > 1000 for 1 datapoints within 6 hours". The "Actions" column shows "Actions enabled".

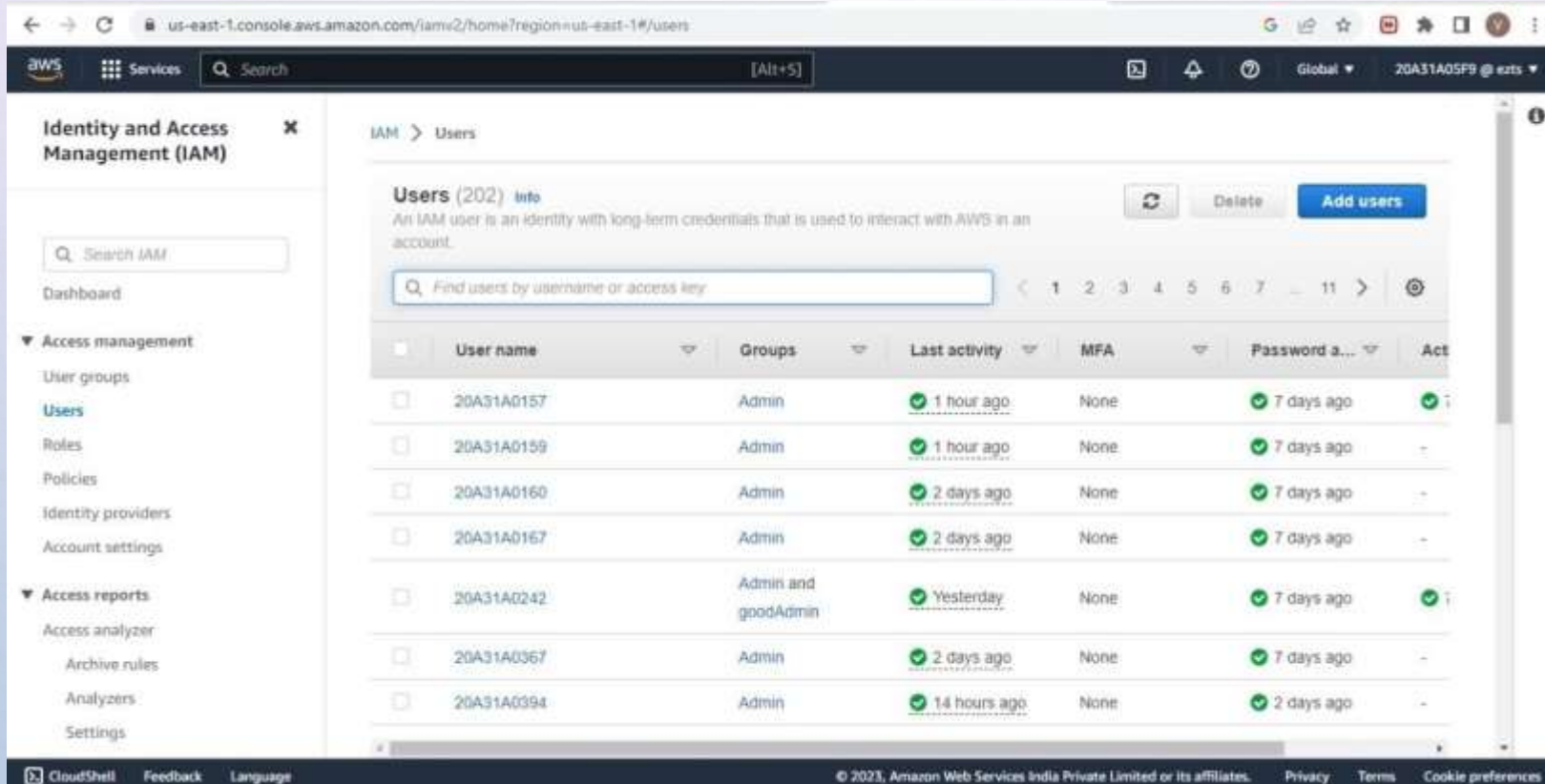
Name	State	Last state update	Conditions	Actions
CloudWatch_Alarm	Insufficient data	2023-04-03 20:30:53	EstimatedCharges > 1000 for 1 datapoints within 6 hours	Actions enabled

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

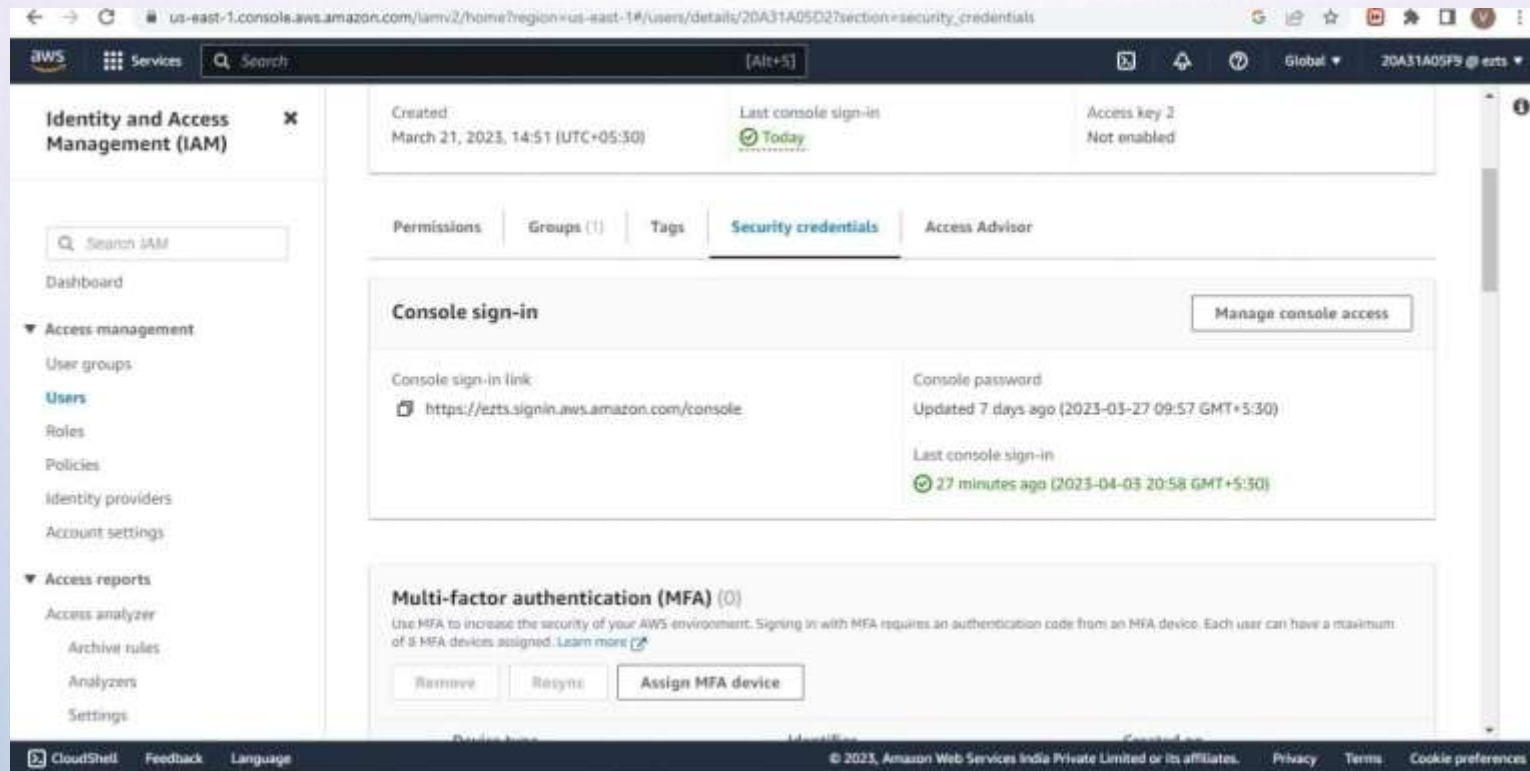


The screenshot displays the AWS IAM console interface. The left-hand navigation pane is titled "Identity and Access Management (IAM)" and includes sections for "Access management" (with links to User groups, Users, Roles, Policies, Identity providers, and Account settings) and "Access reports" (with links to Access analyzer, Archive rules, Analyzers, and Settings). The main content area is titled "IAM > Users" and shows a list of 202 users. A search bar is present with the placeholder text "Find users by username or access key". The user list table has columns for checkboxes, User name, Groups, Last activity, MFA, Password a..., and Act. The table lists several users, including those with names like 20A31A0157, 20A31A0159, 20A31A0160, 20A31A0167, 20A31A0242, 20A31A0367, and 20A31A0394, with their respective groups and last activity timestamps.

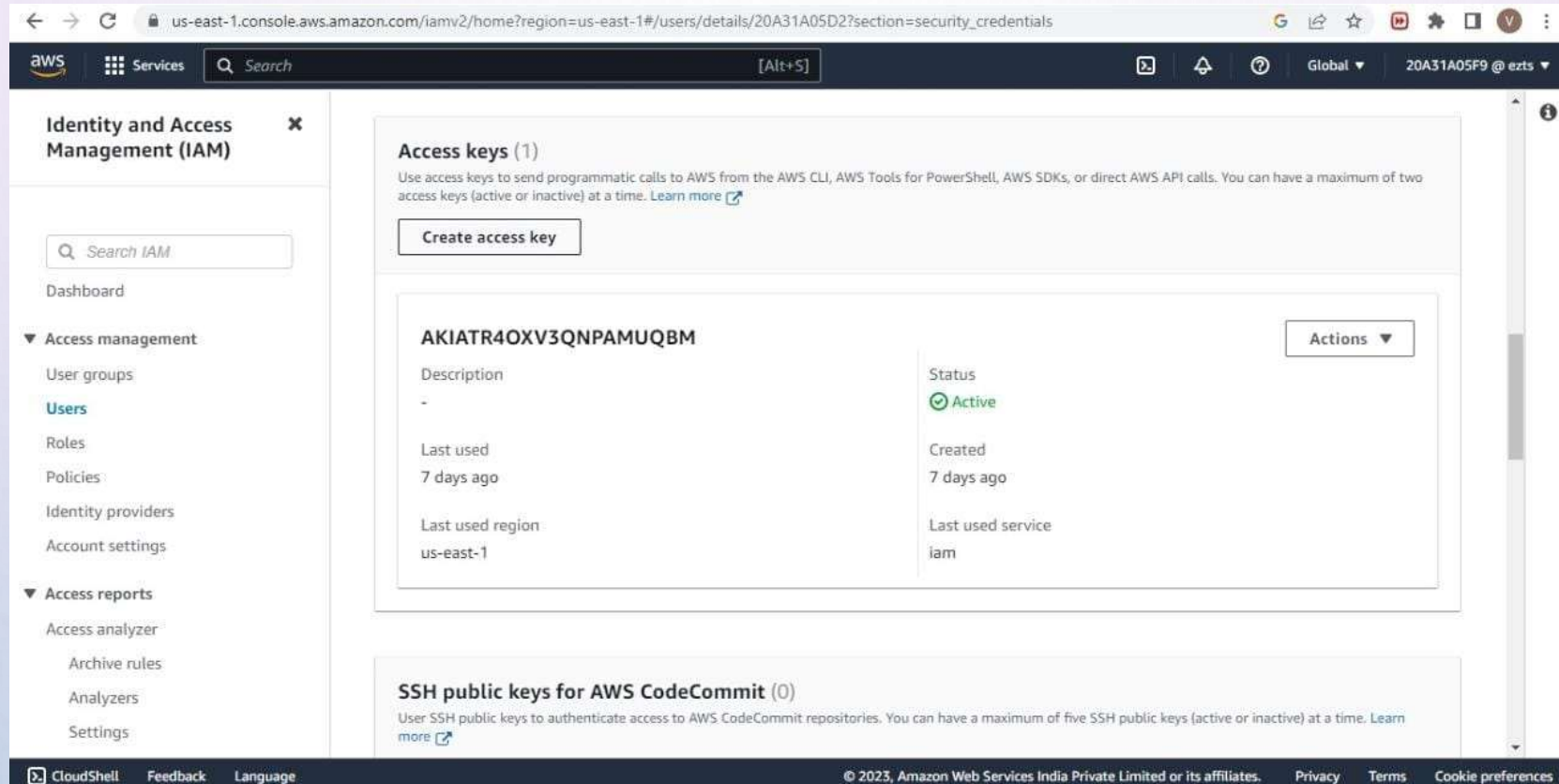
	User name	Groups	Last activity	MFA	Password a...	Act
<input type="checkbox"/>	20A31A0157	Admin	1 hour ago	None	7 days ago	✓
<input type="checkbox"/>	20A31A0159	Admin	1 hour ago	None	7 days ago	-
<input type="checkbox"/>	20A31A0160	Admin	2 days ago	None	7 days ago	-
<input type="checkbox"/>	20A31A0167	Admin	2 days ago	None	7 days ago	-
<input type="checkbox"/>	20A31A0242	Admin and goodAdmin	Yesterday	None	7 days ago	✓
<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.



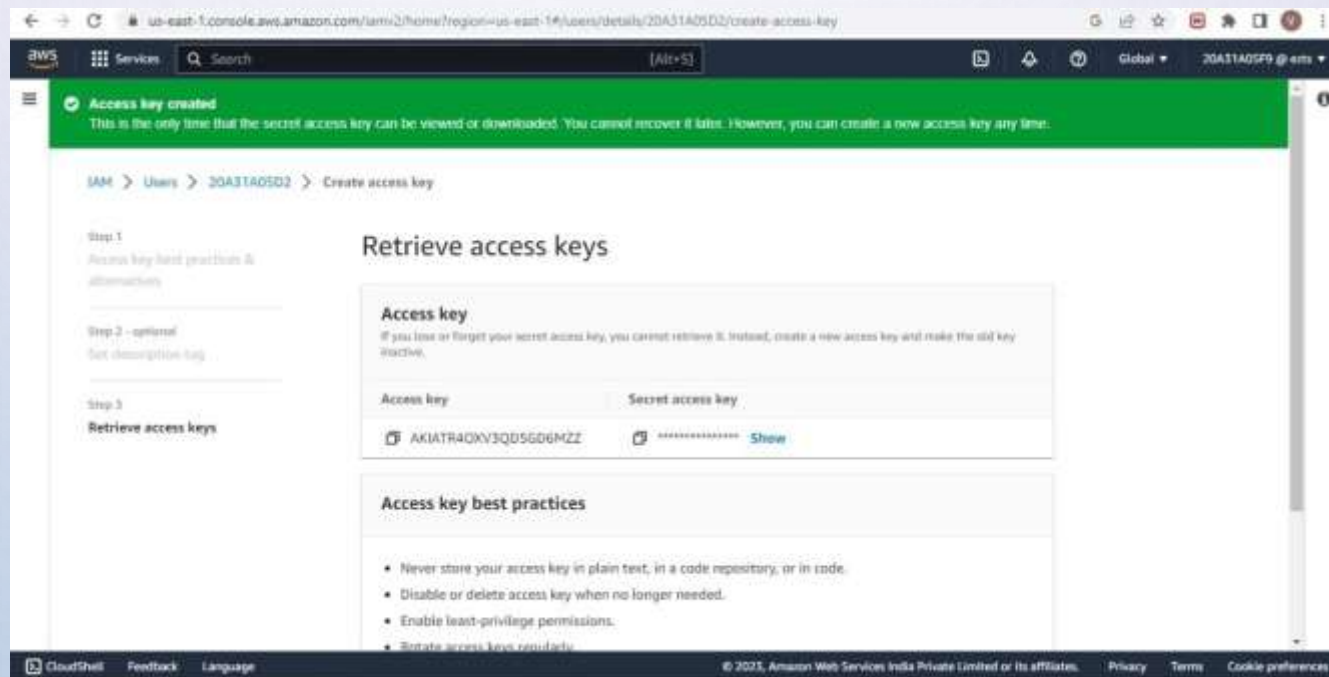
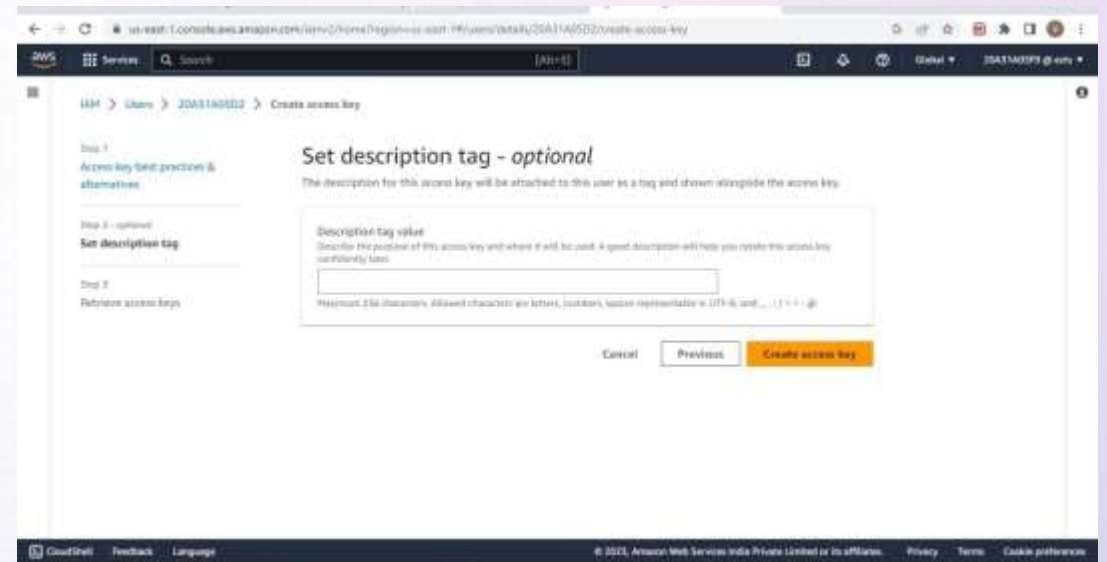
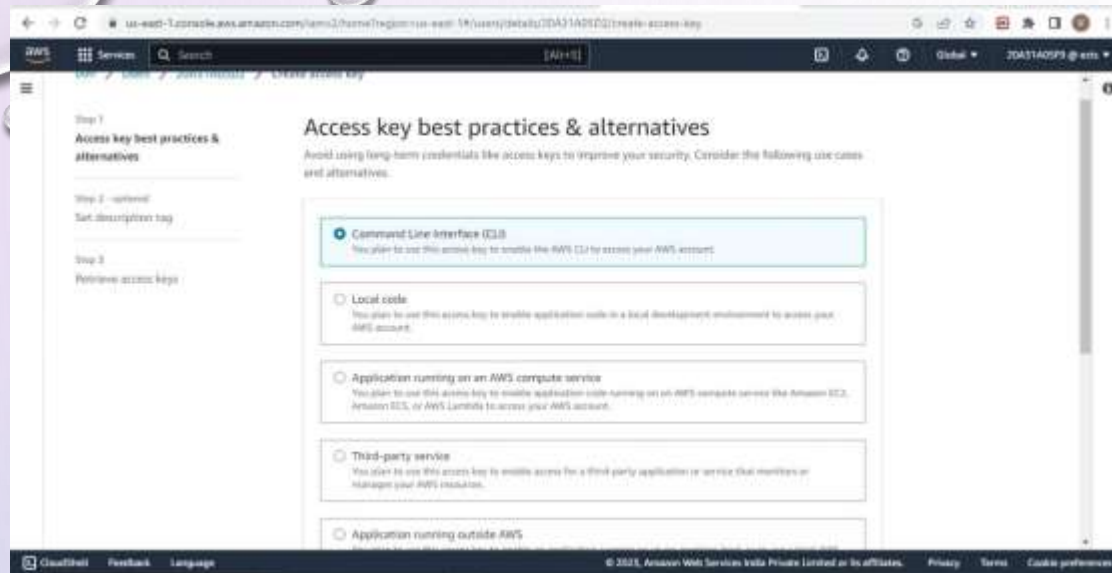
STEP 6 - In the access Keys section , choose Create access key.



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 following details:

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

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.



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.

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

Resources

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

- Instance Profiles: 1
- Auto Scaling Groups: 1
- Elastic IPs: 0
- Load Balancers: 1
- Snapshots: 0

Launch instance

Get started, launch on-demand EC2 instances, which are virtual servers in the cloud.

Service health

Region: US East (N. Virginia)

Status: This service is operating normally.

Instances (3/3)

Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone	Public IP
Backend Host	i-0f62ba0551719d9d	Pending	t2.micro	2/2 checks passed	No alarms	us-east-1a	ec2-54-210-99-1
Lab1	i-0e6b754941509d7	Running	t2.micro	2/2 checks passed	No alarms	us-east-1a	ec2-54-238-176-

Select an instance

Create volume

Only on Amazon EBS volume to attach to an EC2 instance in the same Availability Zone.

Volume settings

Volume type: **General Purpose SSD**

Size (GB): **1**

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

EBS

100 / 3000

Available on Amazon EBS are a maximum of 1000 volumes per Availability Zone.

Throughput (MB/s): **100**

IOPS: **100**

Snapshot ID: **us-east-1a**

Snapshot ID: **us-east-1a**

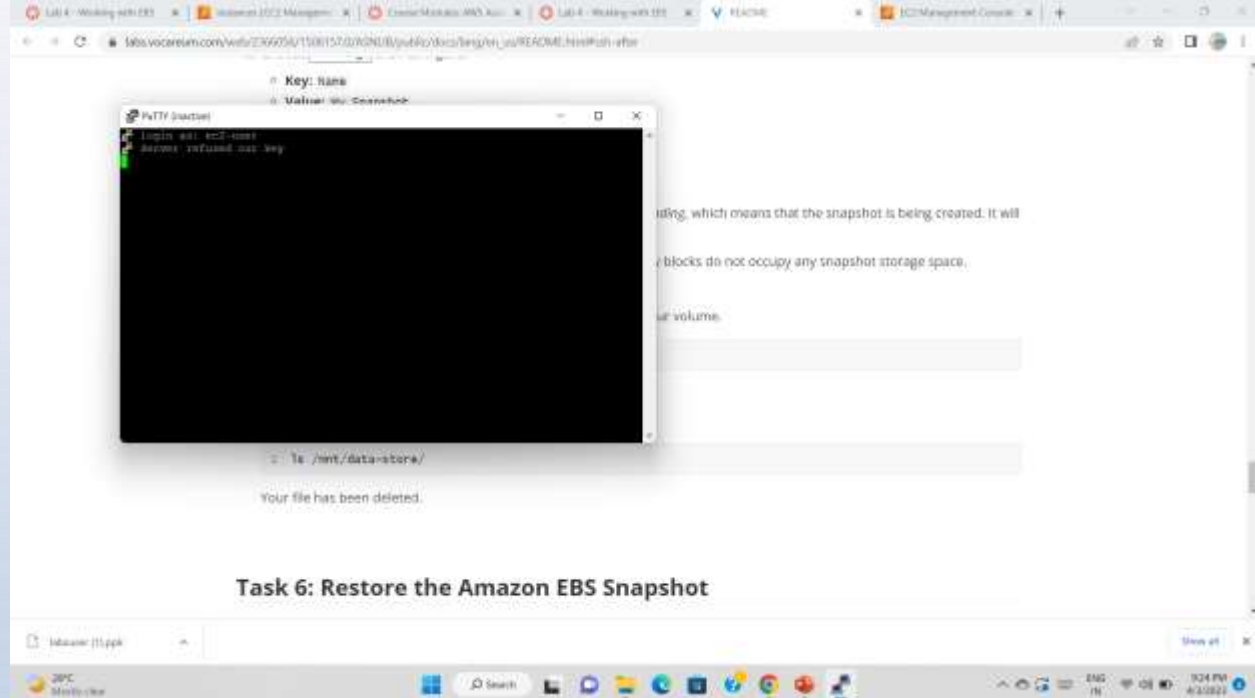
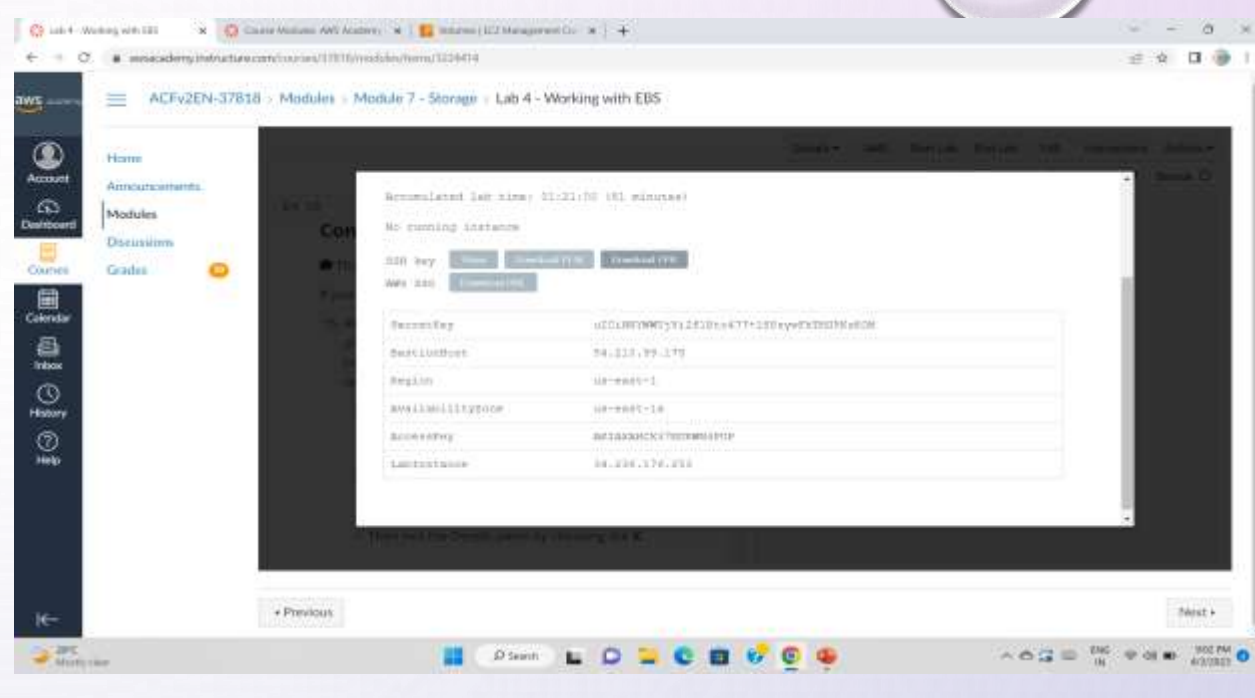
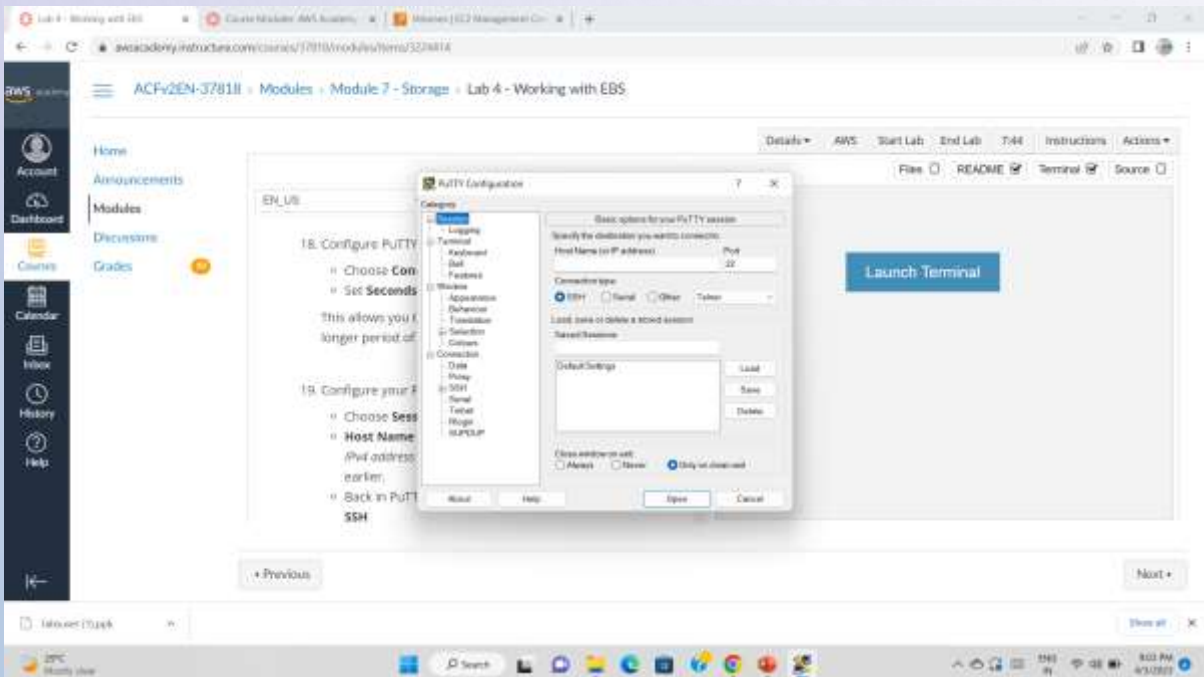
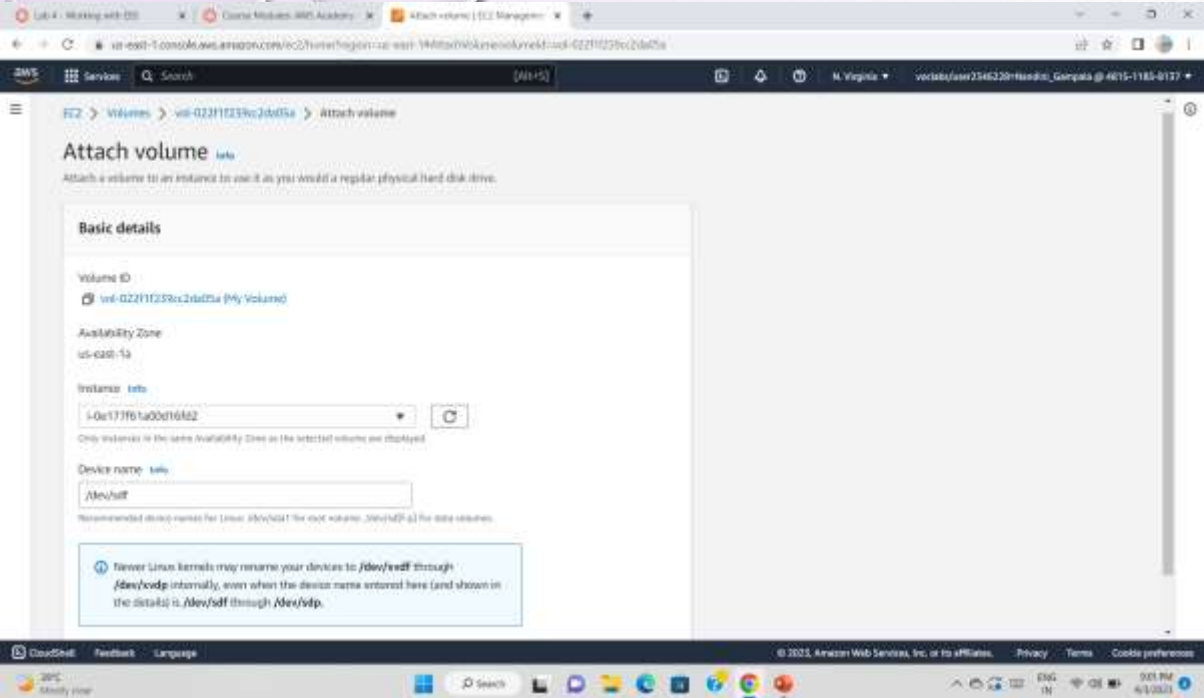
Encryption: **us-east-1a**

Volumes (3/2)

Name	Volume ID	Type	Size	IOPS	Throughput
My Volume	vol-022f1f239cc2da05a	gp2	1 GB	100	-
	vol-088a097038670d18	gp2	8 GB	3000	125

Attach volume

Volume ID: **vol-022f1f239cc2da05a (My Volume)**



Amazon EC2 console - Volumes (1/5)

Search

Name	Volume ID	Type	Size	IOPS	Throughput	Availability
-	vol-05d7811e986771c3	gp2	8 GB	100	-	us-east
-	vol-0c318f478584914f1	gp2	8 GB	100	-	us-east
My Volume	vol-0e10d525f2f83a0c5	gp2	1 GB	100	-	us-east

Actions: Modify volume, Create snapshot, Create snapshot lifecycle policy, Delete volume, Attach volume, Detach volume, Force detach volume, Manage auto-enabled i/o, Manage tags, Fault injection

Volume ID: vol-0e10d525f2f83a0c5 (My Volume)

Details Status checks Monitoring Tags

Amazon EC2 console - Snapshots (1/1)

Owned by me Search

Name	Snapshot ID	Size	Description	Storage...	Snapshot status
My Snapshot	snap-013c8ef099b54ee35	1 GB	-	Standard	Completed

Actions: Create volume from snapshot, Create image from snapshot, Copy snapshot, Modify permissions, Manage fast snapshot restore, Archive snapshot, Restore snapshot from archive, Change restore journal, Delete snapshot, Manage tags

Snapshot ID: snap-013c8ef099b54ee35 (My Snapshot)

Details Permissions Storage tier Tags

Amazon EC2 console - Create volume

Availability Zone: us-east-1a

Fast snapshot restore: Not enabled for selected snapshot

Encryption: Encrypt this volume

Tags - optional

Key: Name Value - optional: Restored Volume

Create volume

Amazon EC2 console - Attach volume

Volume ID: vol-0132dc6ef21347fb26 (Restored Volume)

Availability Zone: us-east-1a

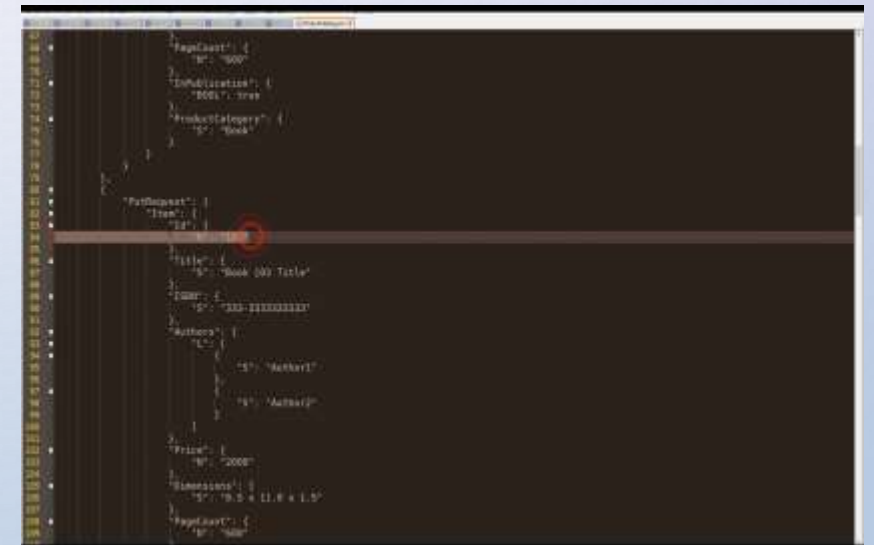
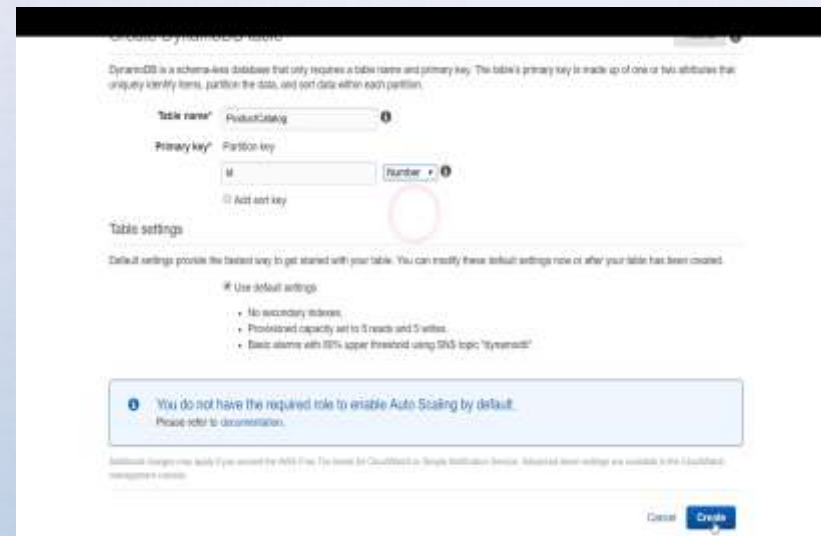
Instance: i-0229db07ae6522a7b

Device name: /dev/sdy

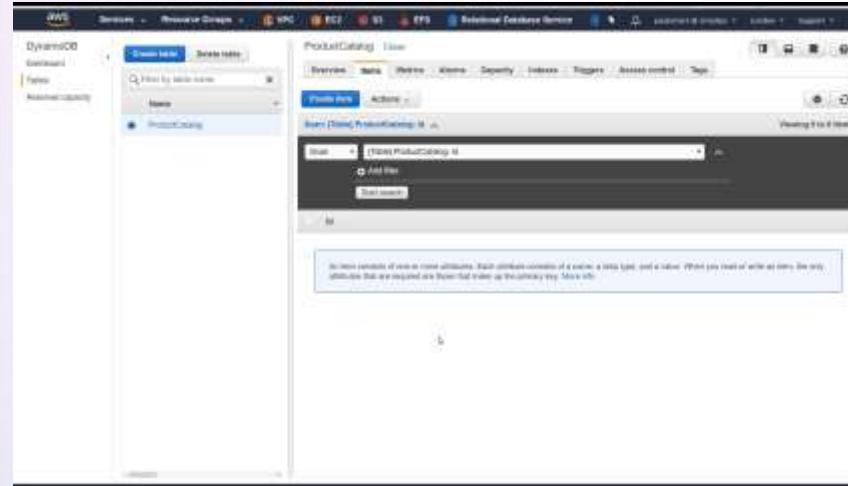
Attach volume

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:

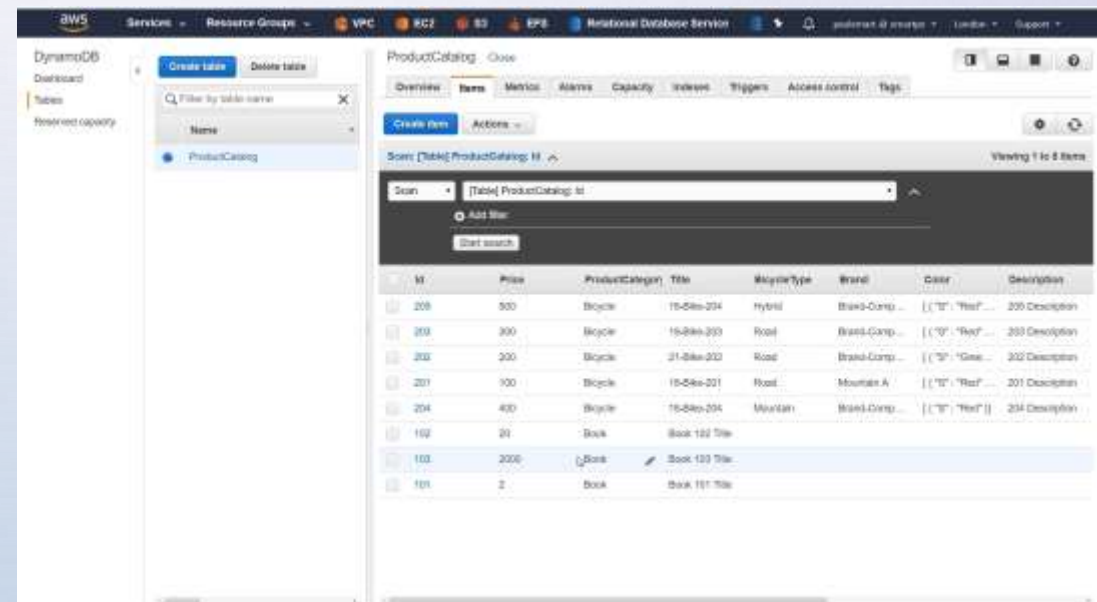


- AFTER CREATING THE TABLE , WE CAN SEE THAT THERE ARE NO ITEMS PRESENT.



- 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": "arn:aws:dynamodb:eu-west-2:407281224315:table/ProductCatalog",
    "AttributeDefinitions": [
      {
        "AttributeName": "id",
        "AttributeType": "N"
      }
    ],
    "ProvisionedThroughput": {
      "NumberOfDecreasesToday": 0,
      "WriteCapacityUnits": 5,
      "ReadCapacityUnits": 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 Relational Database Service

DynamoDB Dashboard Tables Reserved capacity

Create table **Delete table**

Filter by table name X

Name

ProductCatalog

ProductCatalog Close

Overview Items Metrics Alarms Capacity Indexes Triggers Access control Tags

Create item **Actions**

Query [Table] ProductCatalog: Id

Partition key Number 204

Add filter

Sort Ascending Descending

Attributes All Projected

Start search Cancel changes

	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": "Gree...	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				

AWS Services Resource Groups VPC EC2 S3 EFS Relational Database Service

DynamoDB Dashboard Tables Reserved capacity

Create table **Delete table**

Filter by table name X

Name

ProductCatalog

ProductCatalog Close

Overview Items Metrics Alarms Capacity Indexes Triggers Access control Tags

Create item **Actions**

Query [Table] ProductCatalog: Id

Partition key Number 204

Add filter

Sort Ascending Descending

Attributes All Projected

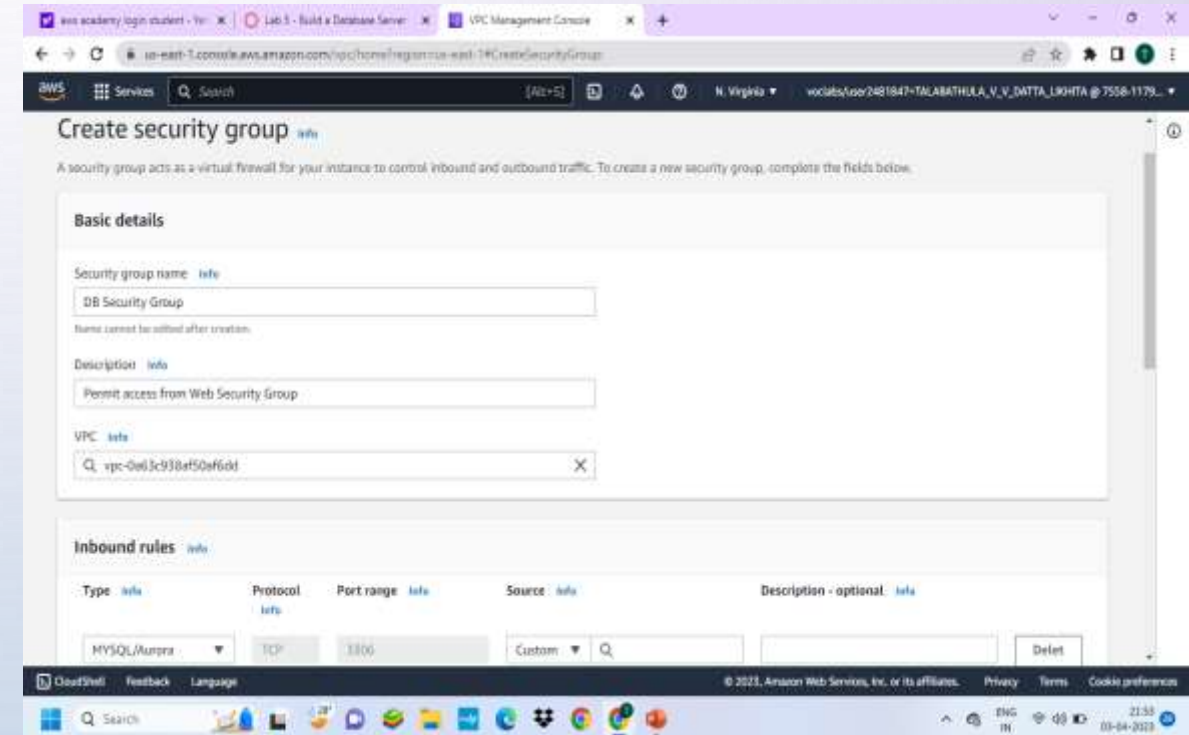
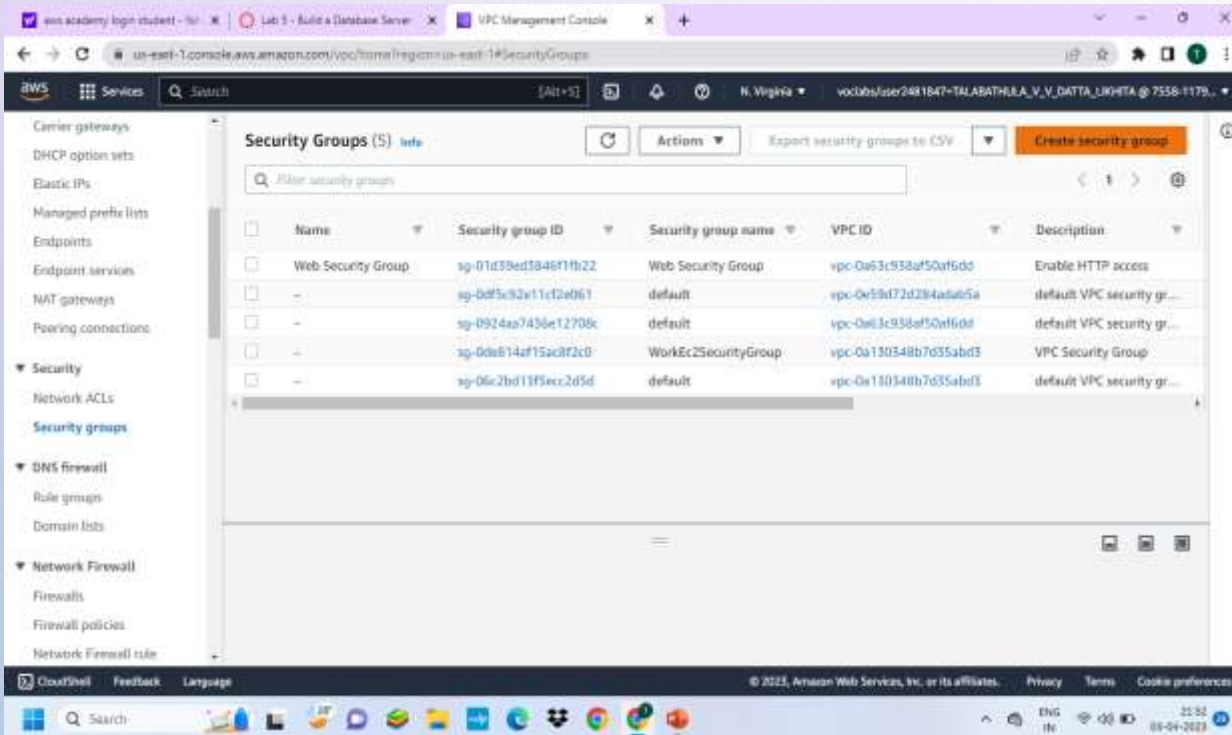
Start search

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

AWS RDS

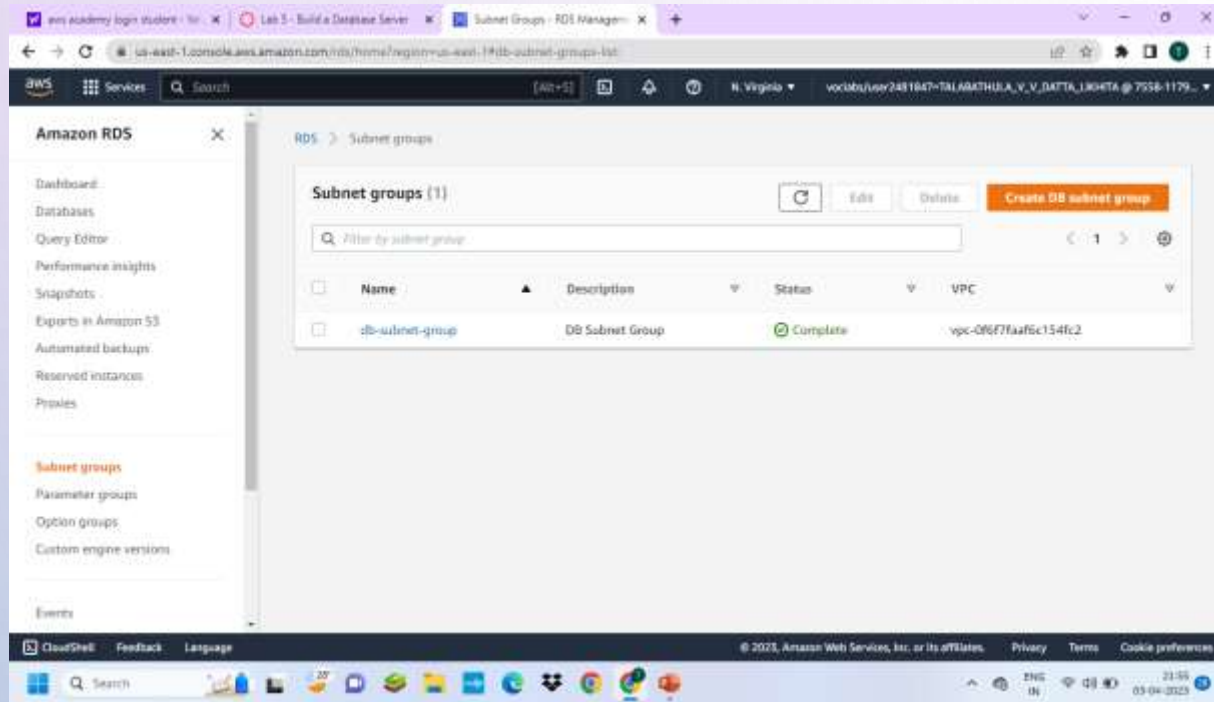
Step 1: Create a Security Group for the RDS DB Instance.

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



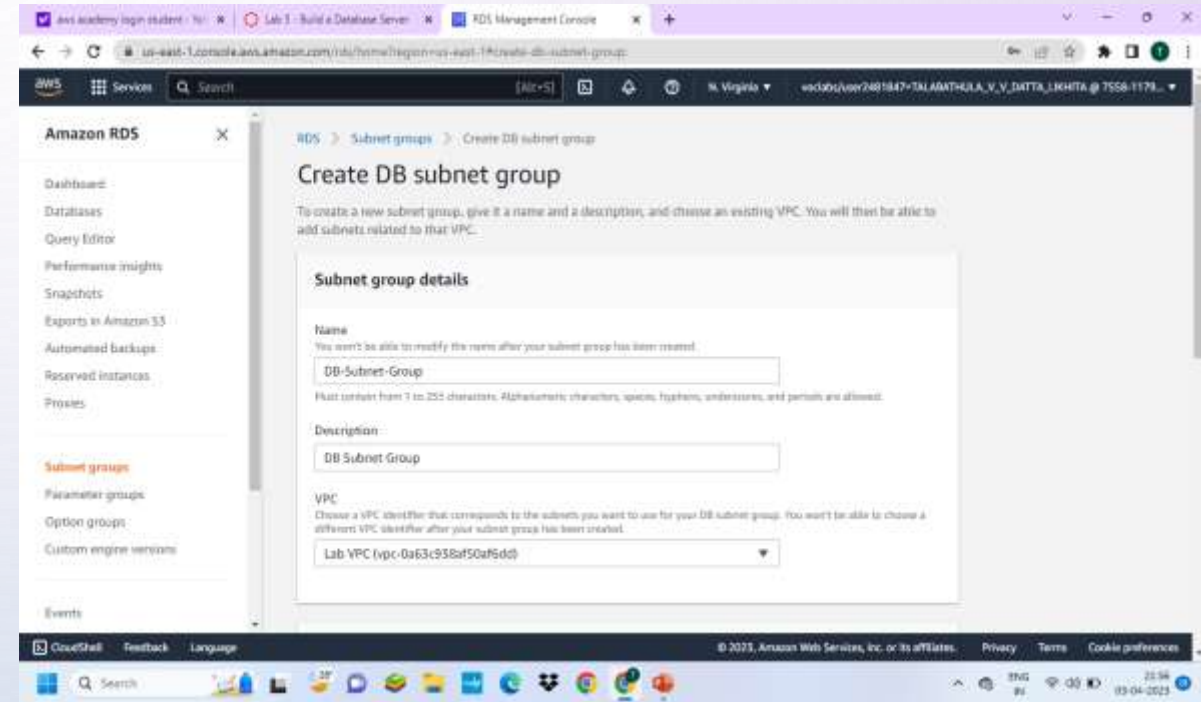
Step 2 : Create a DB Subnet Group.

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



The screenshot shows the Amazon RDS console's 'Subnet groups' page. The left sidebar contains navigation links for Dashboard, Databases, Query Editor, Performance insights, Snapshots, Exports in Amazon S3, Automated backups, Reserved instances, and Proxies. The main content area displays a table of subnet groups. One group is listed: 'db-subnet-group' with a description of 'DB Subnet Group', a status of 'Complete', and associated VPC 'vpc-0f6f7faaf5c154fc2'. Above the table are buttons for 'Refresh', 'Edit', 'Delete', and 'Create DB subnet group'. A search bar is also present.

Name	Description	Status	VPC
db-subnet-group	DB Subnet Group	Complete	vpc-0f6f7faaf5c154fc2

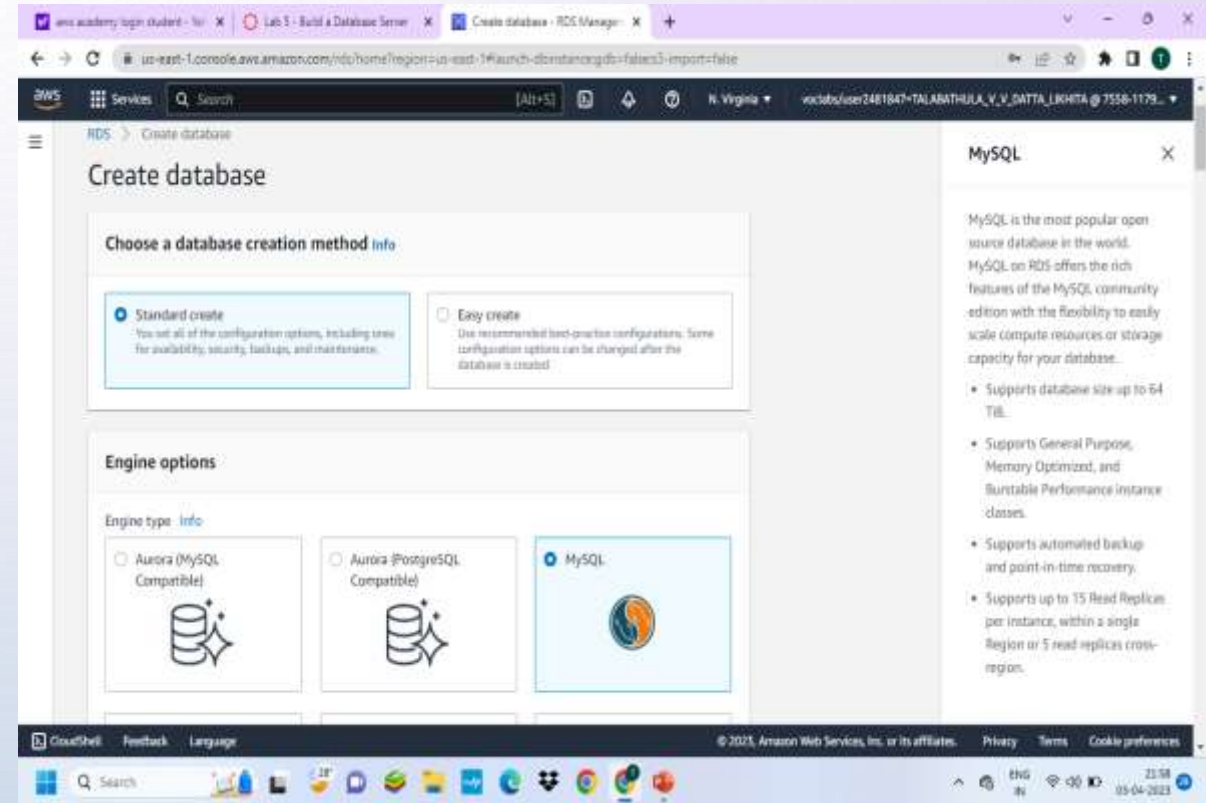
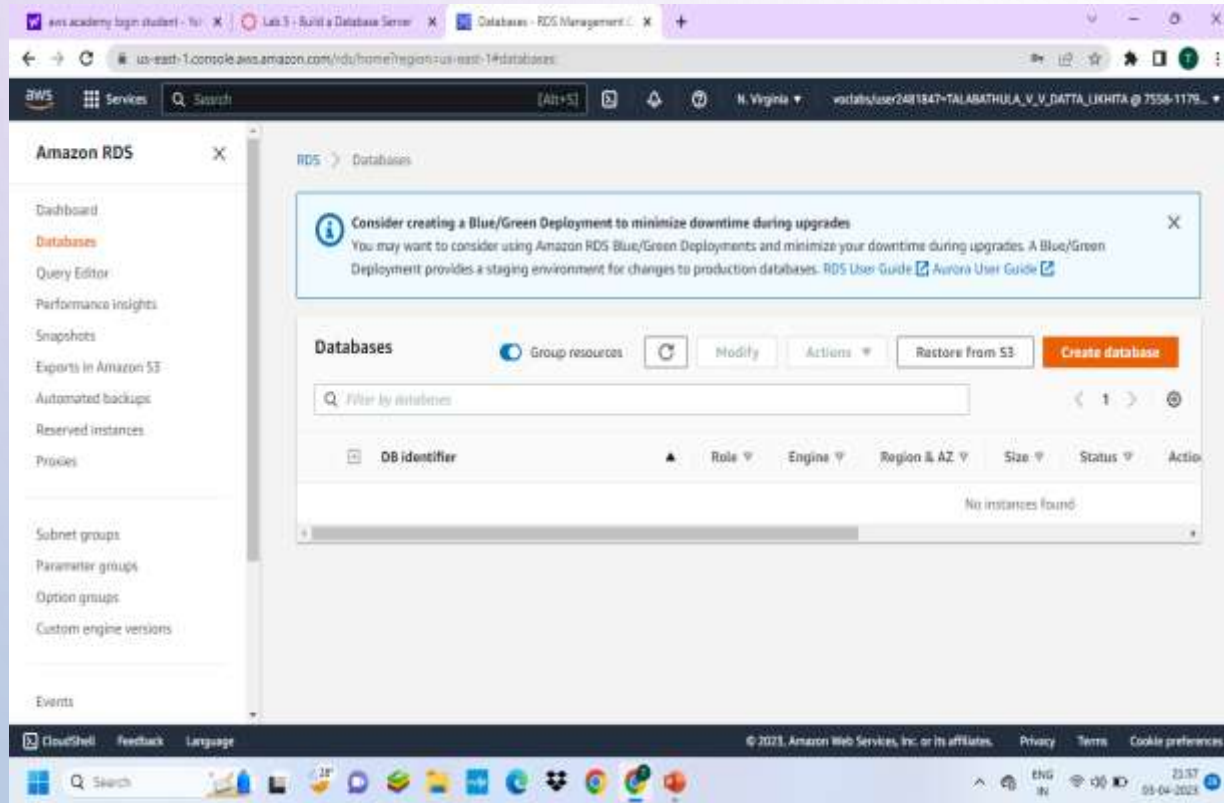


The screenshot shows the 'Create DB subnet group' form in the Amazon RDS console. The form includes the following fields:

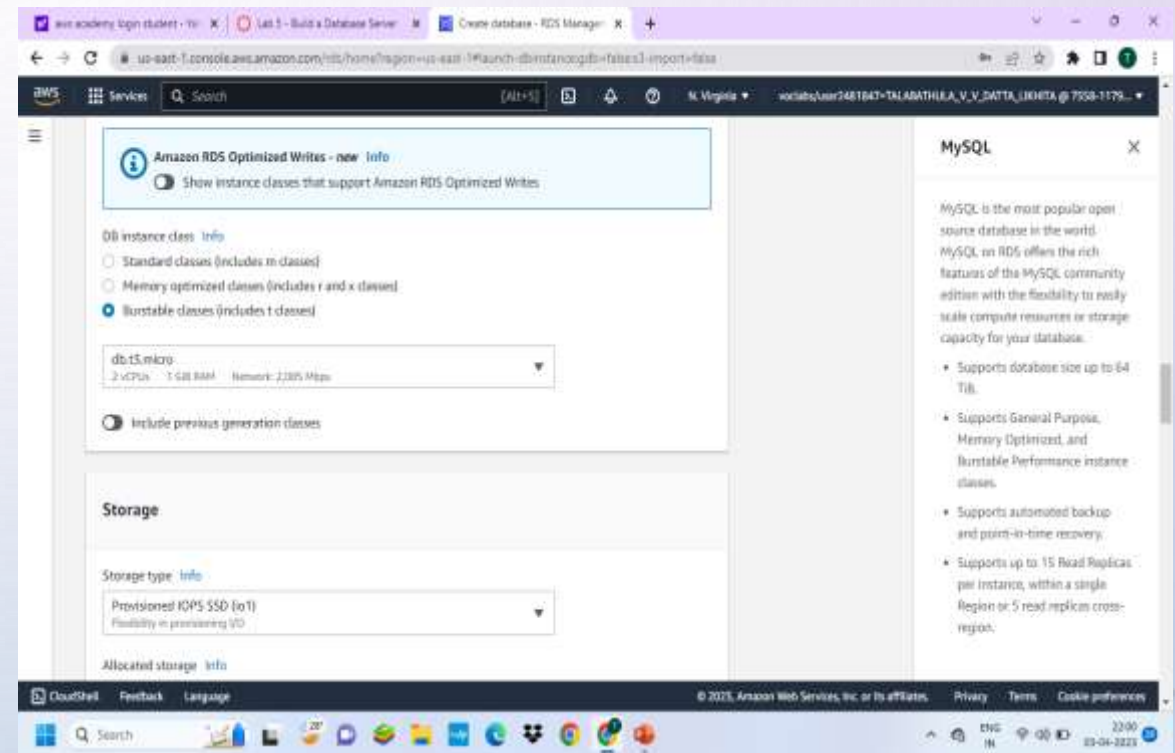
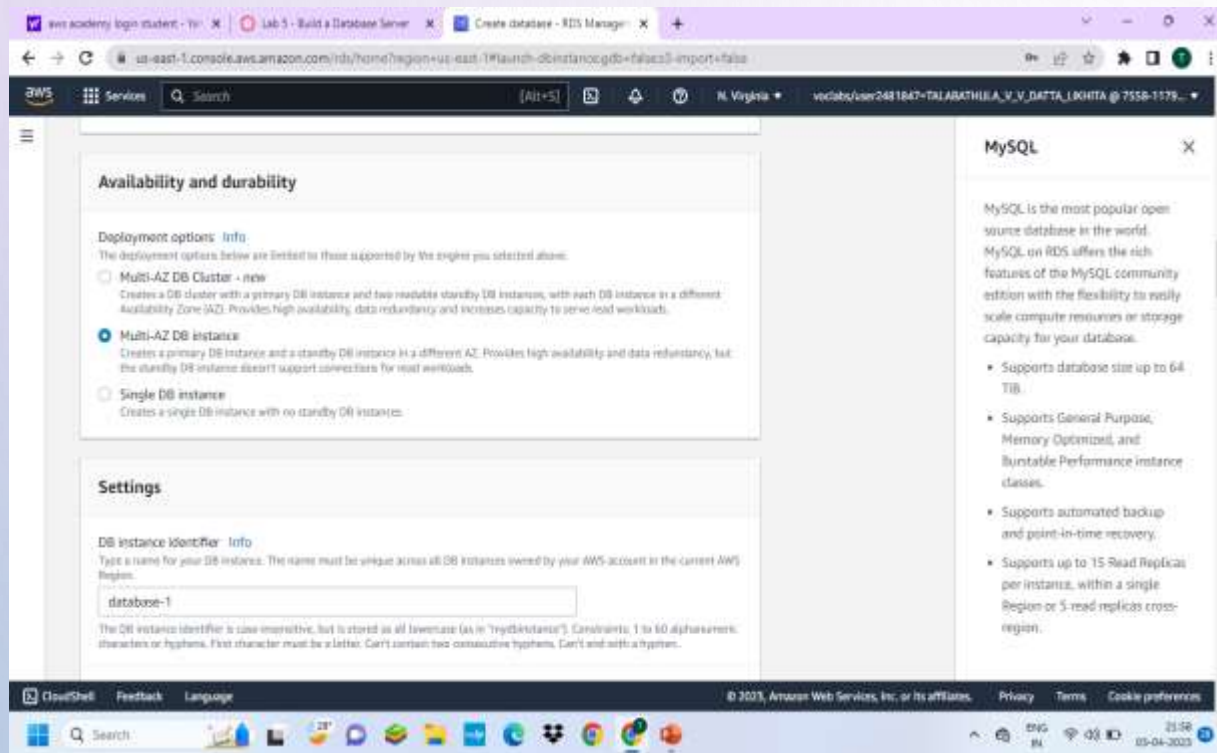
- Name:** DB-Subnet-Group
- Description:** DB Subnet Group
- VPC:** Lab VPC (vpc-0a63c956af50af5dd)

Instructions on the page state: 'To create a new subnet group, give it a name and a description, and choose an existing VPC. You will then be able to add subnets related to that VPC.'

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 displays the AWS Management Console interface for an Amazon RDS database instance. The browser tabs at the top include 'aws academy login student - Yah...', 'Lab 5 - Build a Database Server', and 'Database Details - RDS Manager'. The address bar shows the URL 'us-east-1.console.aws.amazon.com/rds/home?region=us-east-1#databaseid=lab-dbs-cluster=false'. The console header shows the AWS logo, 'Services', a search bar, and the current region 'N. Virginia'.

The left sidebar contains the 'Amazon RDS' navigation menu with options: Dashboard, Databases (selected), Query Editor, Performance insights, Snapshots, Exports in Amazon S3, Automated backups, Reserved instances, Proxies, Subnet groups, Parameter groups, Option groups, Custom engine versions, and Events.

The main content area shows the 'lab-db' instance details. At the top right are 'Modify' and 'Actions' buttons. Below is a 'Summary' section with a table of instance information:

Summary			
DB identifier lab-db	CPU 2.63%	Status Available	Class db.t3.micro
Role Instance	Current activity 0 Connections	Engine MySQL Community	Region & AZ us-east-1a

Below the summary is a horizontal tab bar with the following tabs: 'Connectivity & security' (selected), 'Monitoring', 'Logs & events', 'Configuration', 'Maintenance & backups', and 'Tags'.

The 'Connectivity & security' section contains three sub-sections:

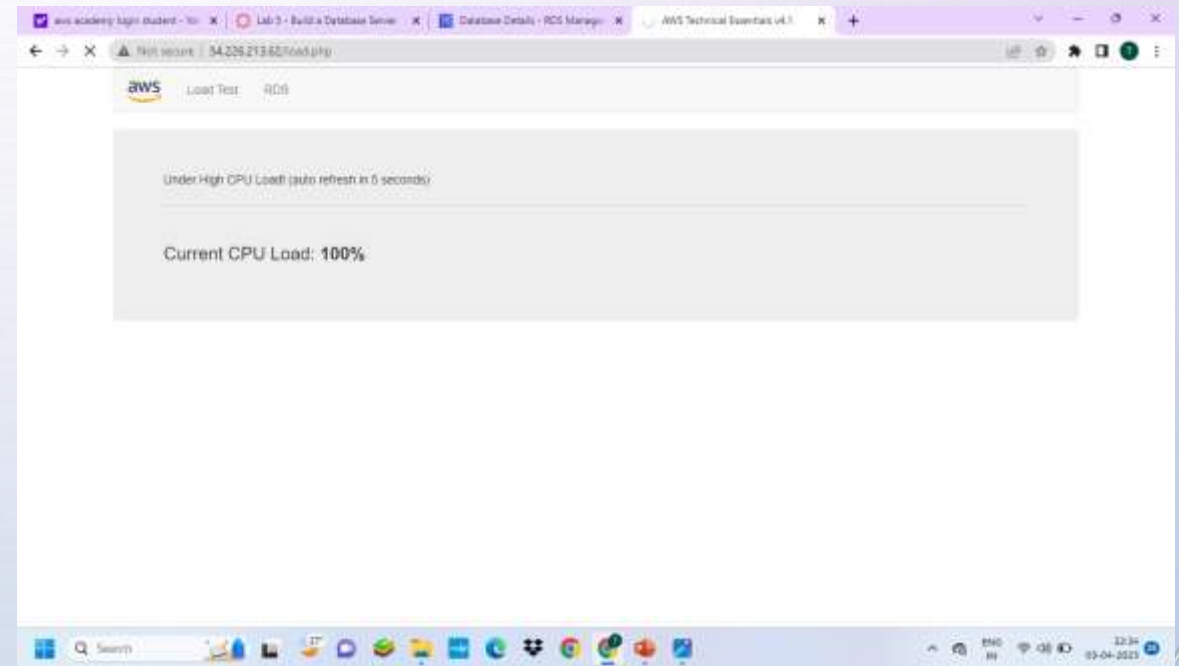
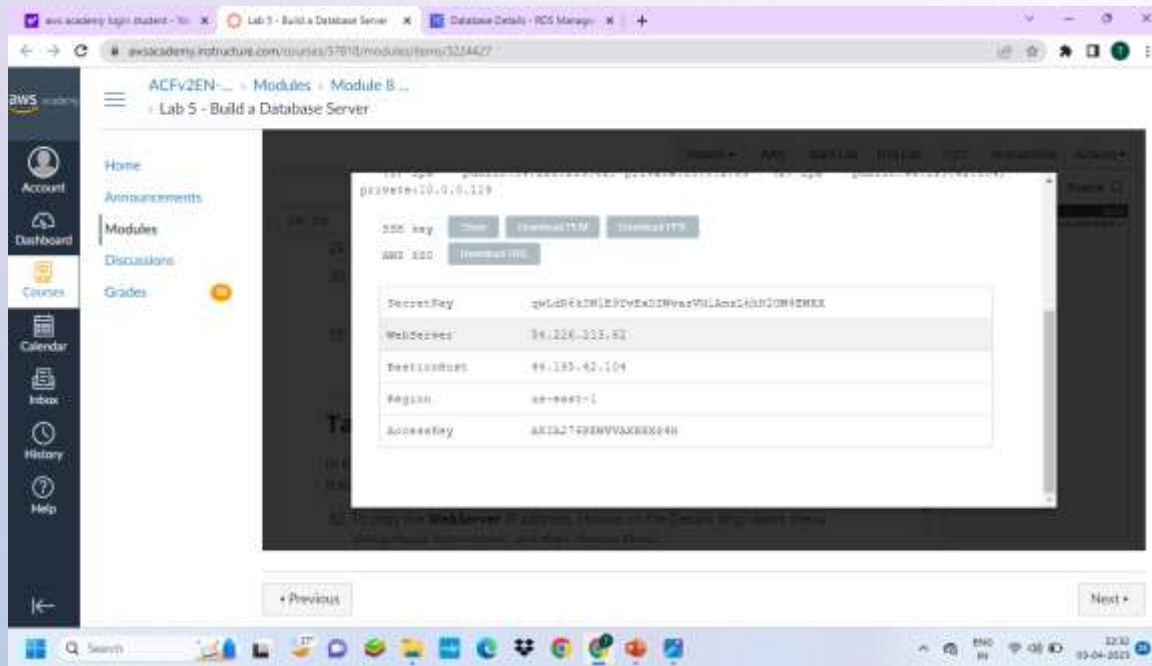
- Endpoint & port**: Endpoint
- Networking**: Availability Zone
- Security**: VPC security groups

The footer of the console shows 'CloudShell', 'Feedback', 'Language', and copyright information '© 2023, Amazon Web Services, Inc. or its affiliates.' along with links for 'Privacy', 'Terms', and 'Cookie preferences'. The Windows taskbar at the bottom shows the time as 22:30 on 03-04-2023.

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 - Yab X | Lab 5 - Build a Database Server X | Database Details - RDS Manager X | AWS Technical Essentials v4.1 X

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

aws Load Test RDS

Endpoint

Database

Username

Password

Submit

Windows Search | 27° | ENG IN | 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 - Y... Database Details - RDS Manager... Lab 5 - Build a Database Server... AWS Technical Essentials v4.1

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

aws Load Test RDS

Address Book

Last name	First name	Phone	Email	Admin
				Add Contact
Doe	Jane	010-110-1101	janed@someotheraddress.org	Edit Remove
Johnson	Roberto	123-456-7890	robertoj@someaddress.com	Edit Remove

27° 22:38 03-04-2023

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`.

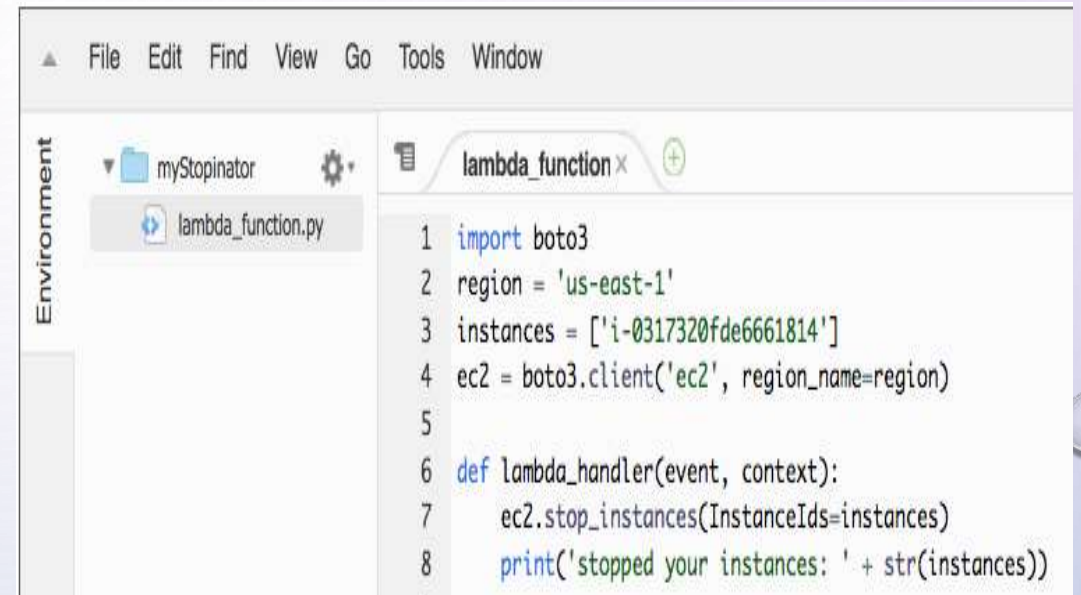
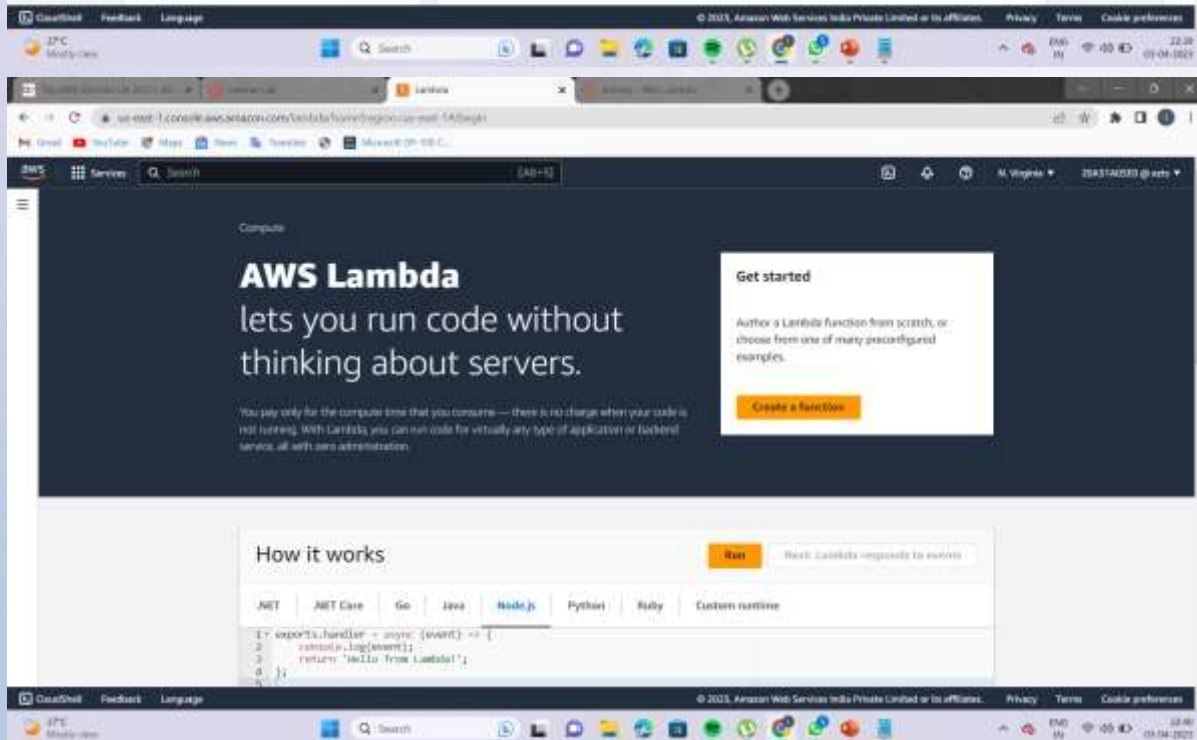
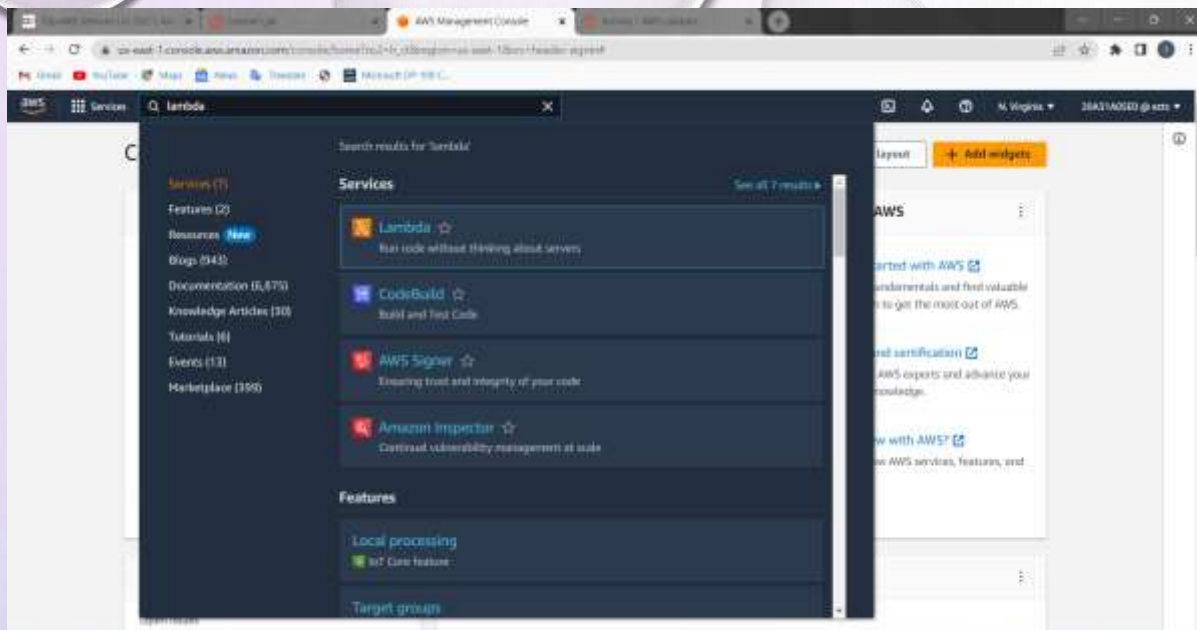
11) Verify that an EC2 instance named `instance1` is running in your account, and copy the `instance1` instance ID.

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.



The background features a light blue-to-white gradient. In the upper left, there are several realistic water droplets of varying sizes. A faint, large circular pattern, resembling a ripple or a stylized sun, is centered in the upper half of the image. The lower half of the image contains more water droplets, including a large, prominent one on the right side.

ELASTIC LOAD BALANCER(ELB)

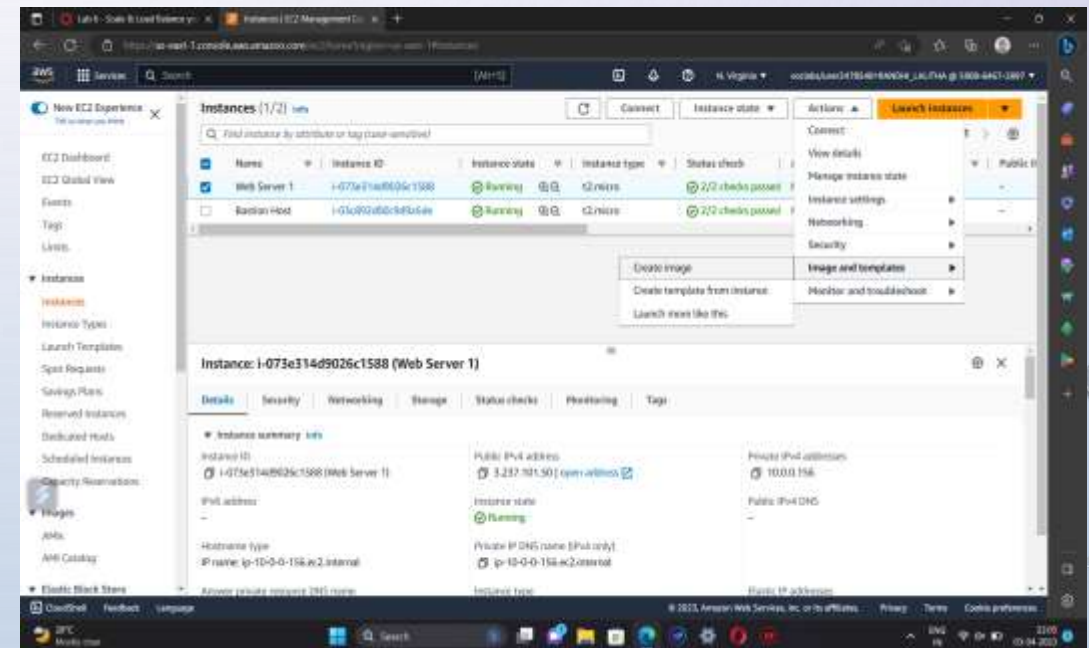
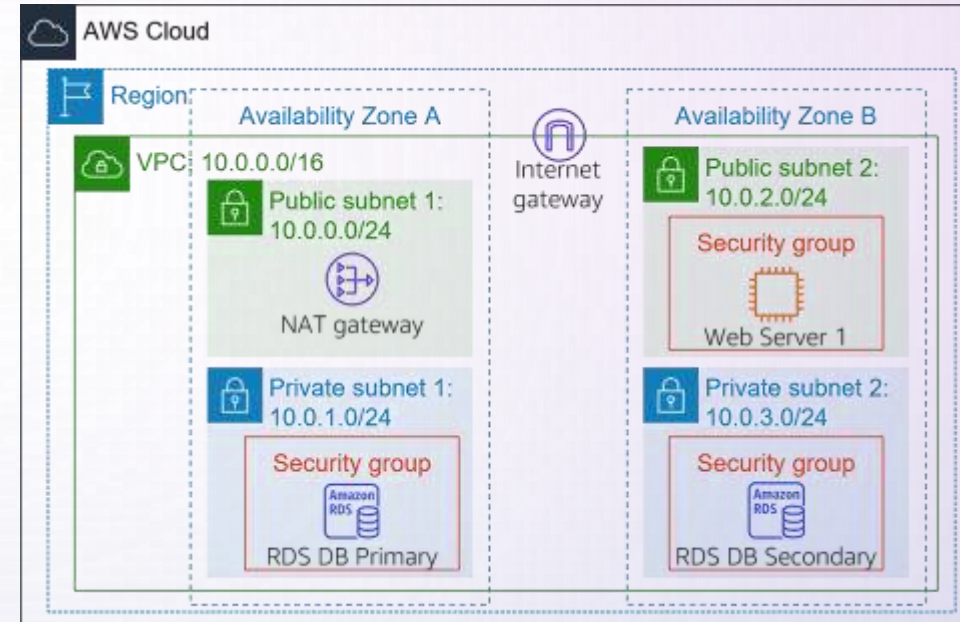
Elastic Load Balancing automatically distributes incoming application traffic across multiple Amazon EC2 instances.

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

Procedure:

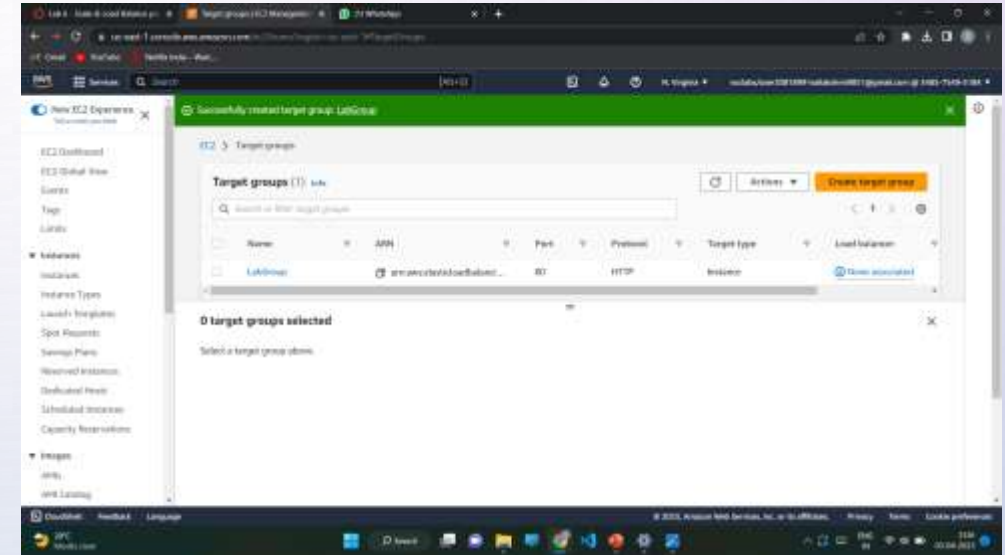
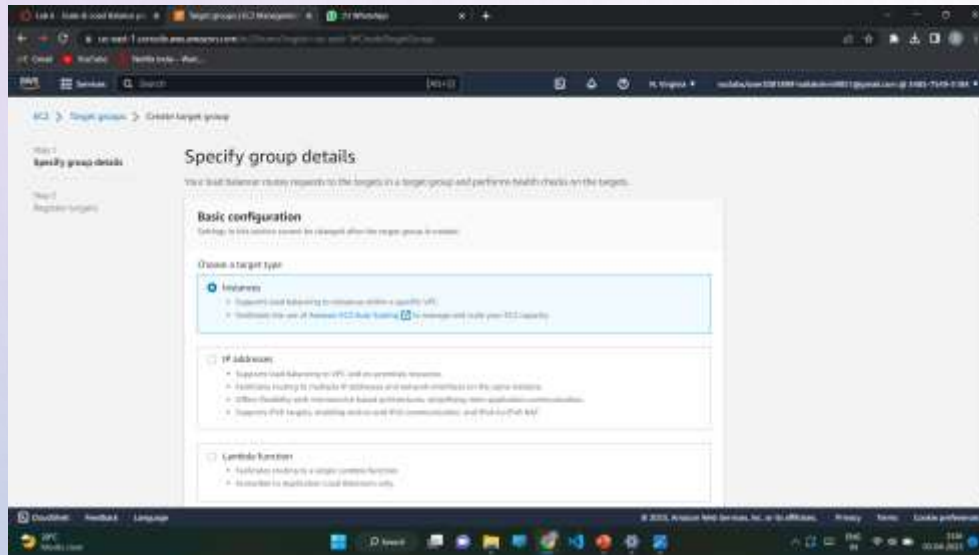
Task1: Creating an AMI for Auto Scaling

- ❖ 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.

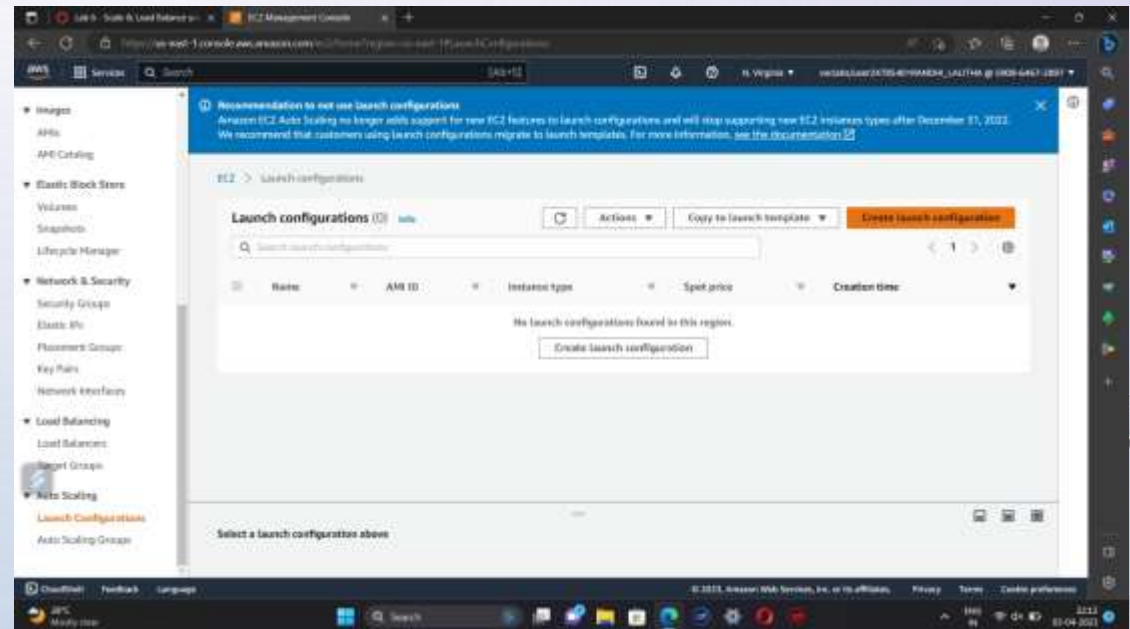
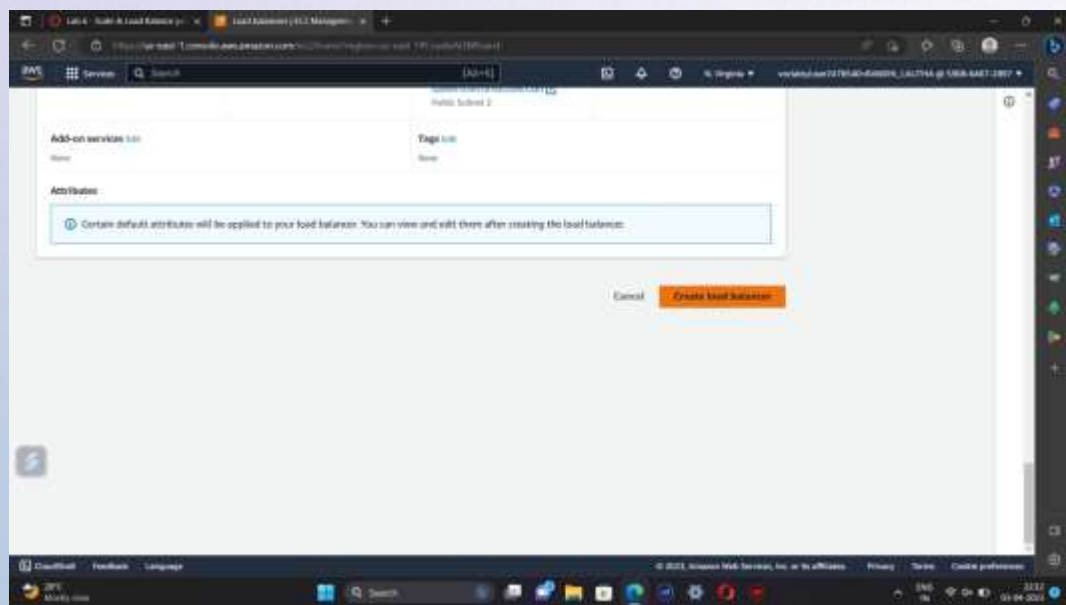
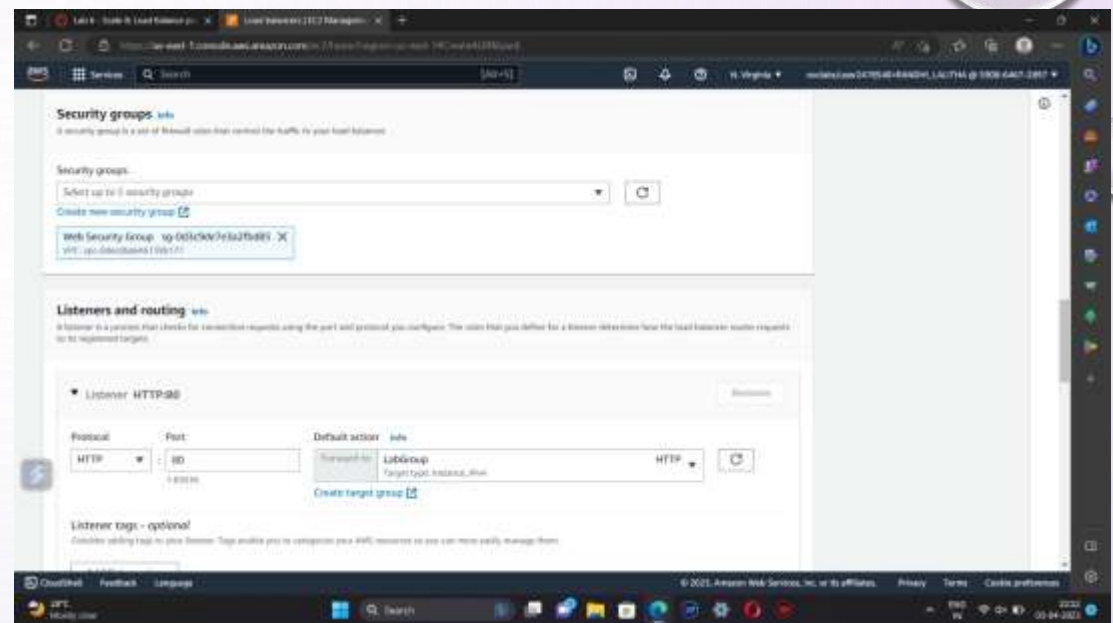
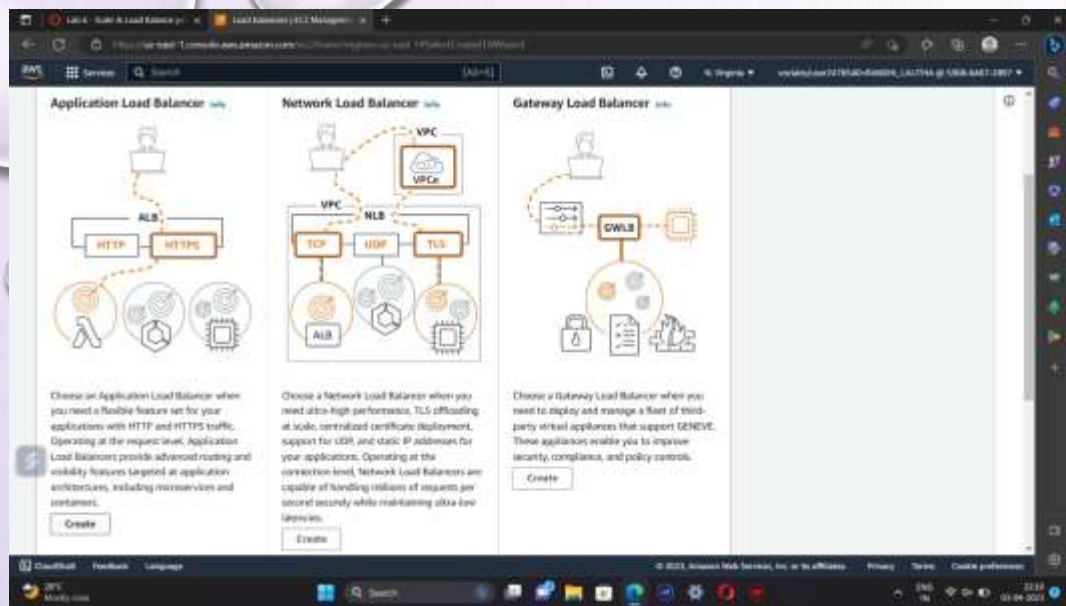


Task 2: Creating a load balancer

- ❖ 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.



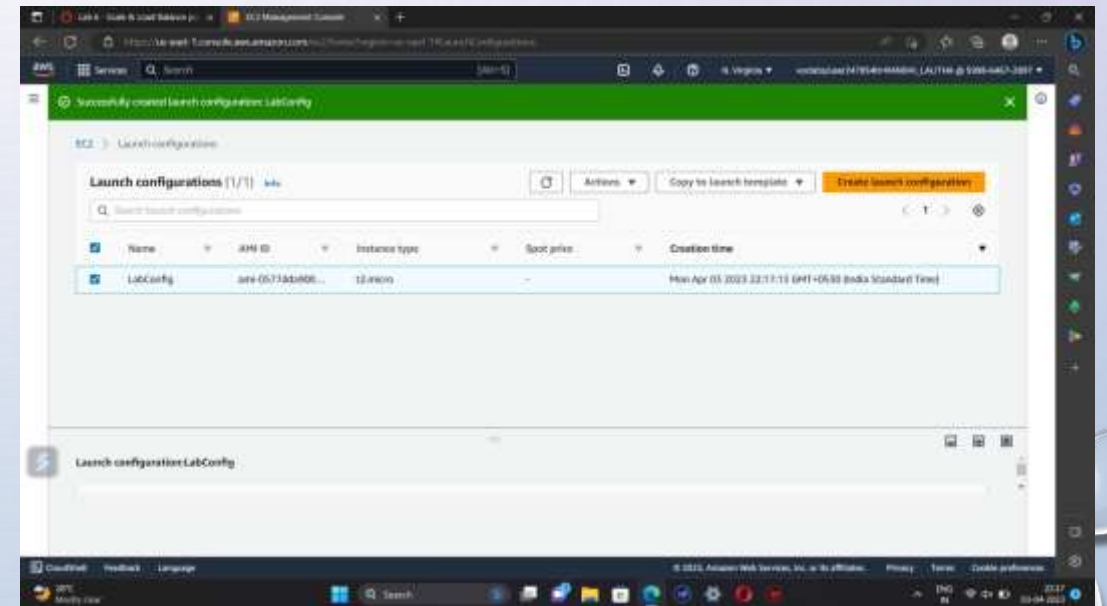
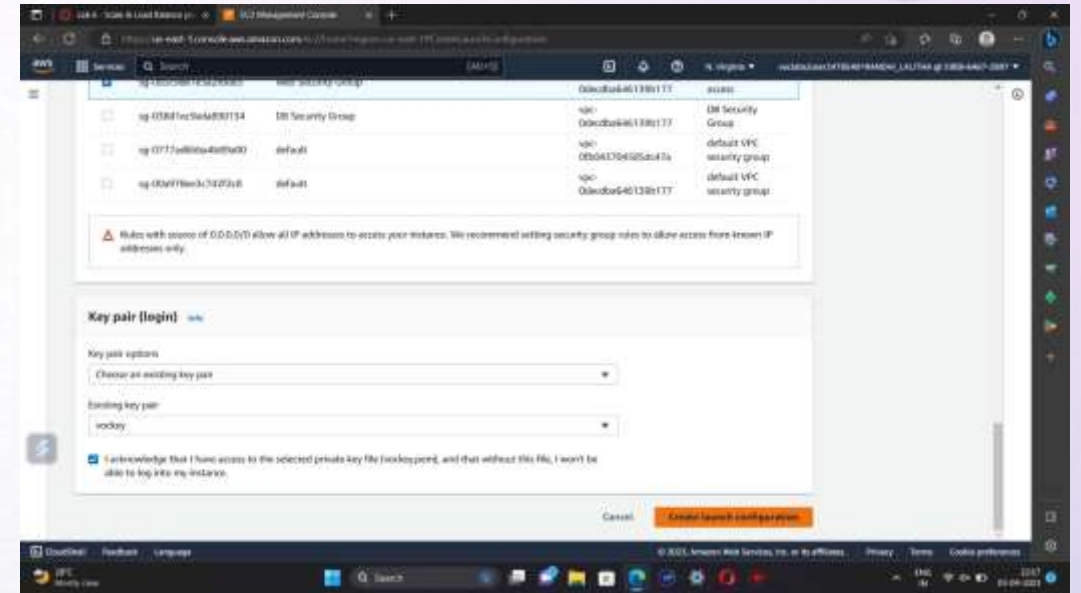
- ❖ From the left navigation pane , select Load Balancers. Click create load balancer.
- ❖ To create a application balancer, click create under Application Load Balancer and Name it.
- ❖ In Networking mapping, select Lab VPC and specify the subnets that the load balancer should use.
- ❖ In security groups,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



- ❖ 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 AWS Management Console interface for creating an Auto Scaling group. The browser address bar indicates the URL: <https://us-east-1.console.aws.amazon.com/ec2/home?region=us-east-1#directfrom-ec2>CreateAutoScalingGroupLaunchConfigurationName:LabConfig>. The console header shows the AWS logo, 'Services', a search bar, and the user's profile 'vsc:labs/owner2478540-RAMODH_LALITHA @ 5908-6467-2897' in the 'us-east-1' region.

The main content area displays the 'Create Auto Scaling group' wizard. The 'Instance scale-in protection' section is expanded, showing 'Instance scale-in protection' and a checkbox for 'Enable instance protection from scale-in'. Below this, 'Step 5: Add notifications' is shown with an 'Edit' button and a 'Notifications' section indicating 'No notifications'. 'Step 6: Add tags' is the current step, also with an 'Edit' button. It shows a table for 'Tags (1)' with columns 'Key', 'Value', and 'Tag new instances'.

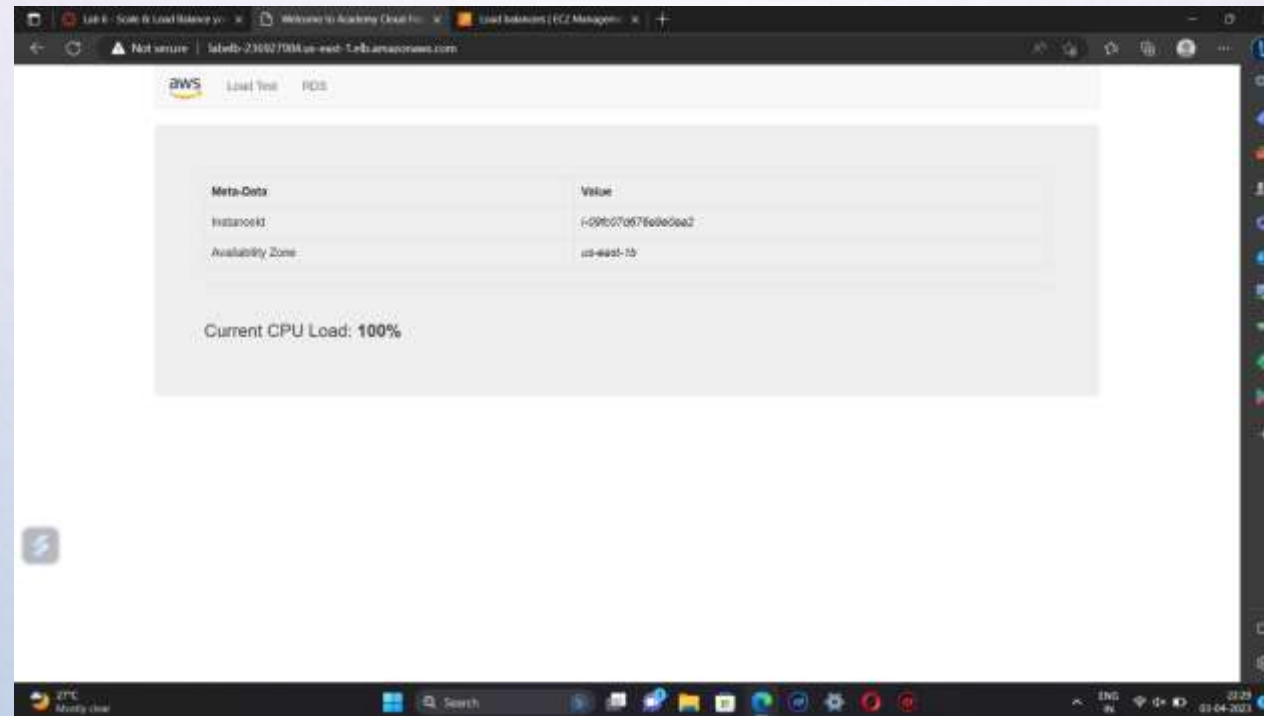
Key	Value	Tag new instances
Name	Lab Instance	Yes

At the bottom of the wizard, there are three buttons: 'Cancel', 'Previous', and 'Create Auto Scaling group' (highlighted in orange).

The footer of the console shows 'CloudShell', 'Feedback', 'Language', and copyright information: '© 2023, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences'. The system tray at the bottom of the screen shows the date '03-04-2023' and time '22:23'.

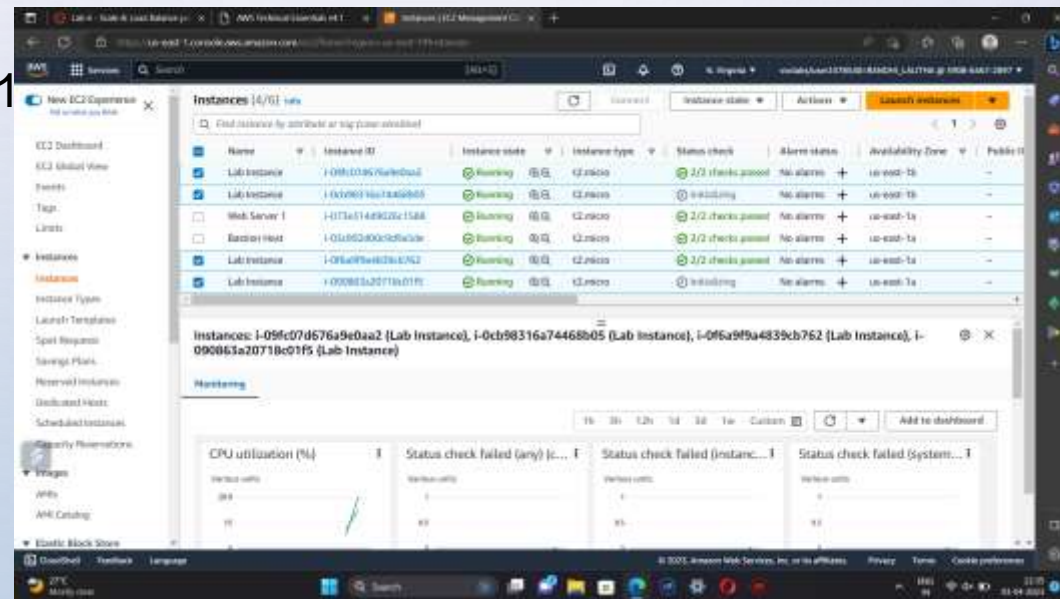
Task 4: Verify that Load Balancing is Working

- ❖ 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



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 names 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:

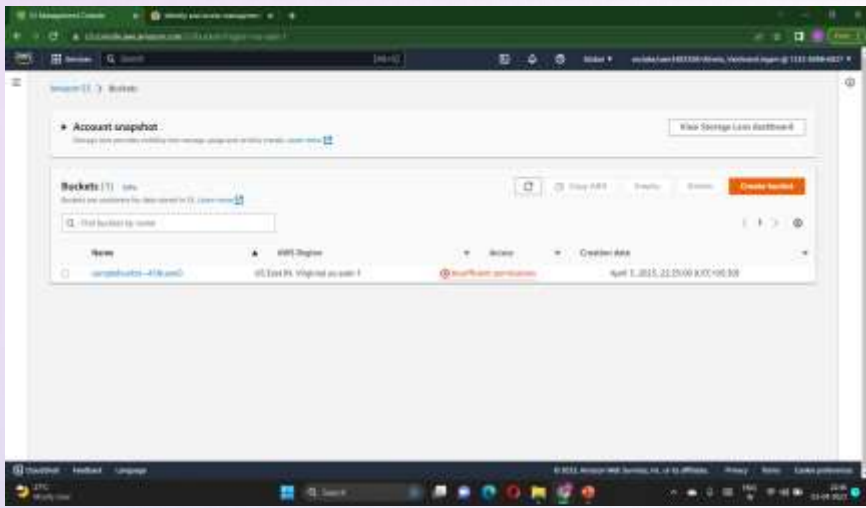
Step 10:Go back to your bucket and click on Permissions.

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.

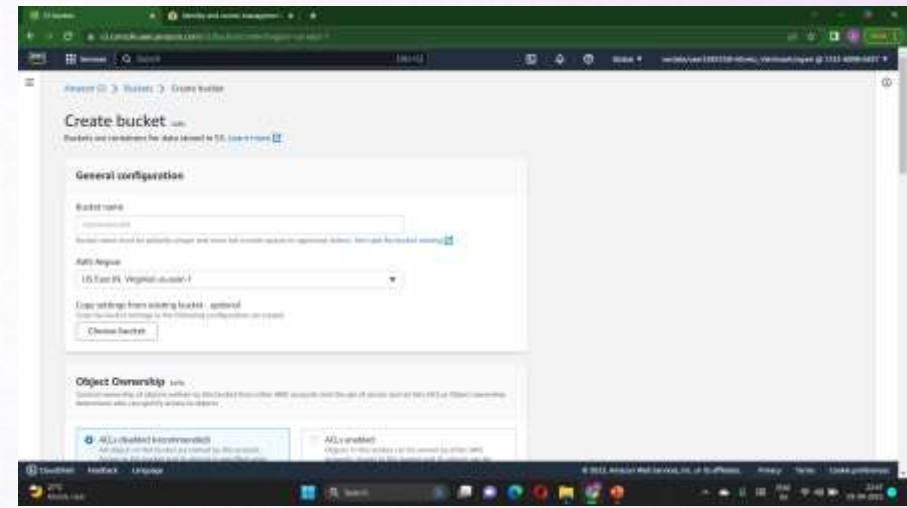
Step 12 :Now its state switches to Read Object - Yes

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

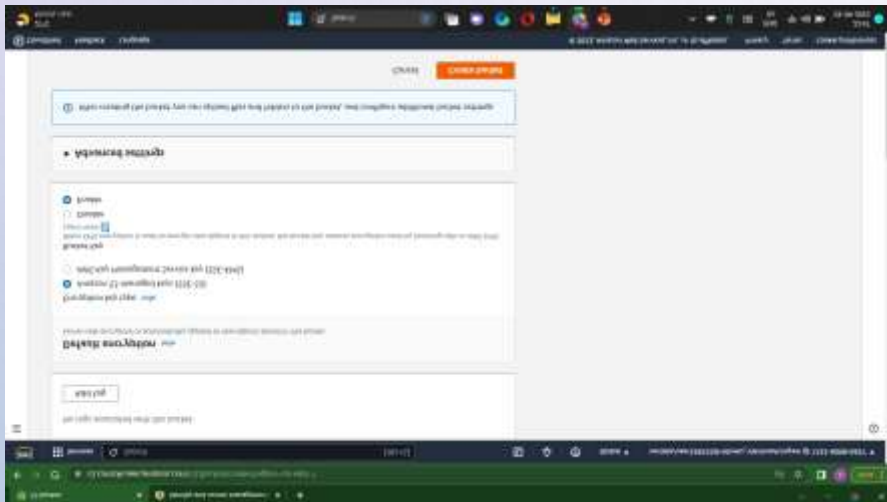
Step 14:Notice the URL on your browser



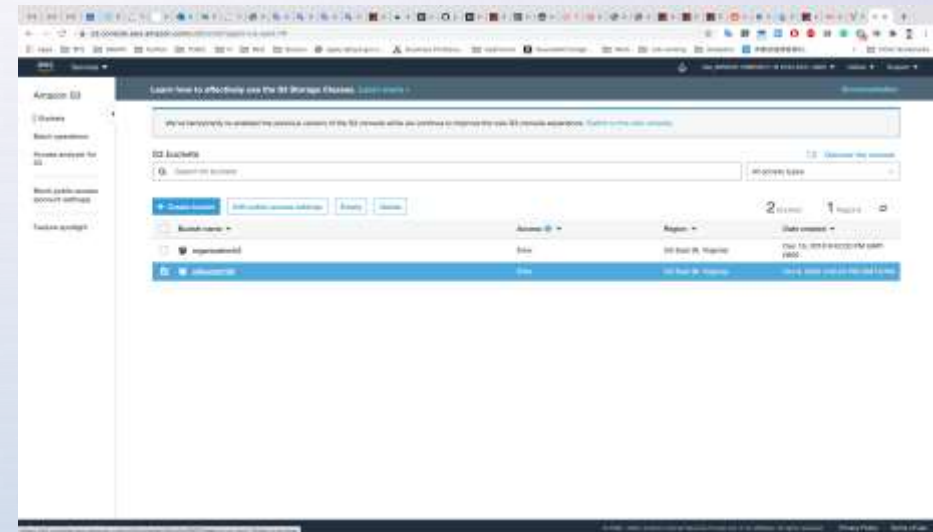
Step 1



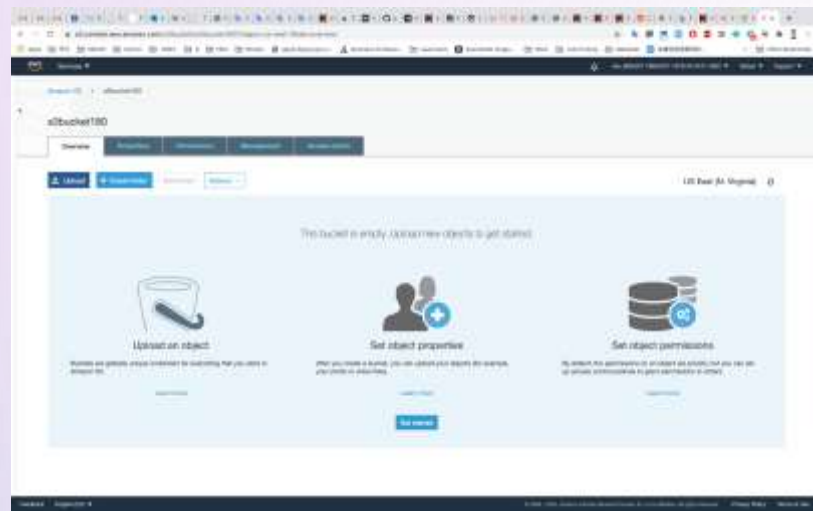
Step 2



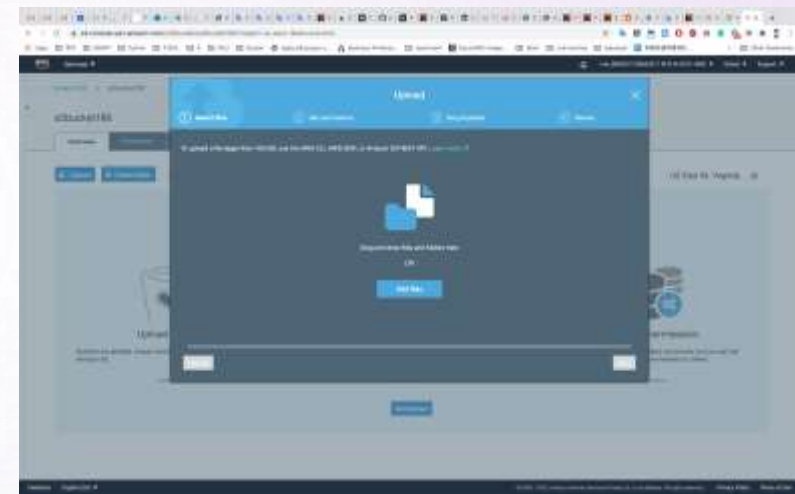
Step 2



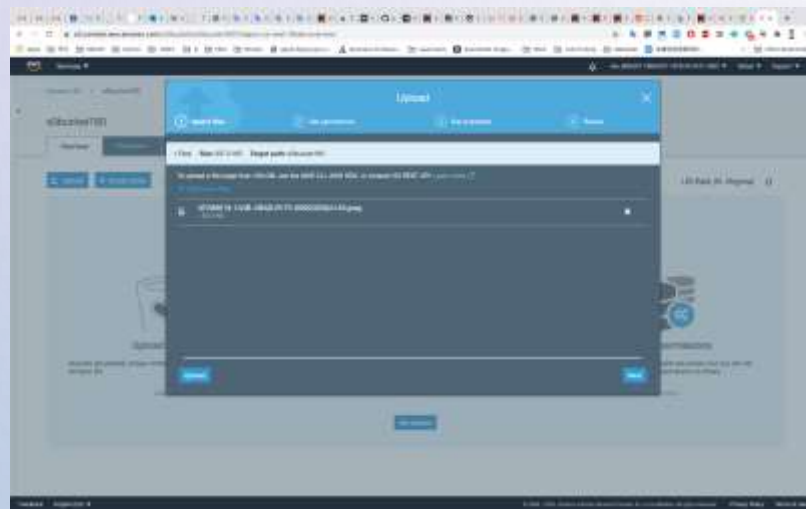
Step 3



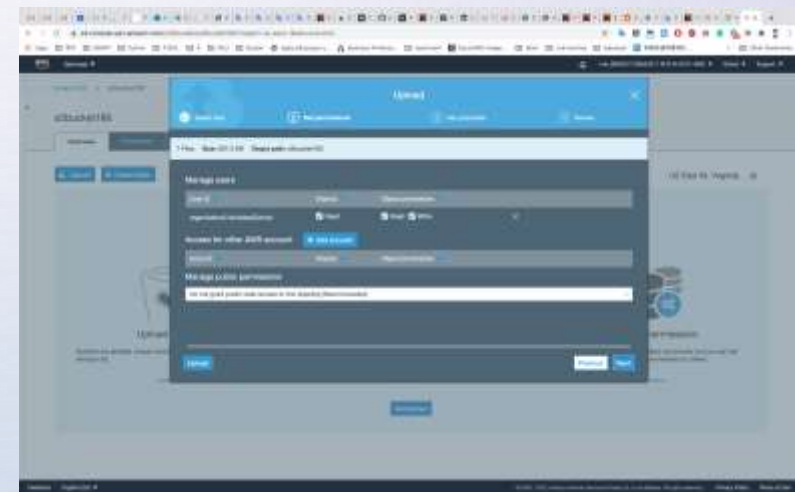
Step 4



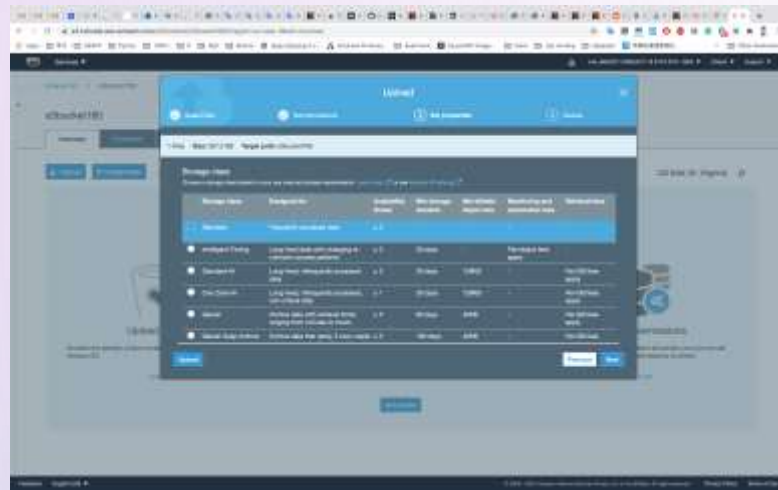
Step 5



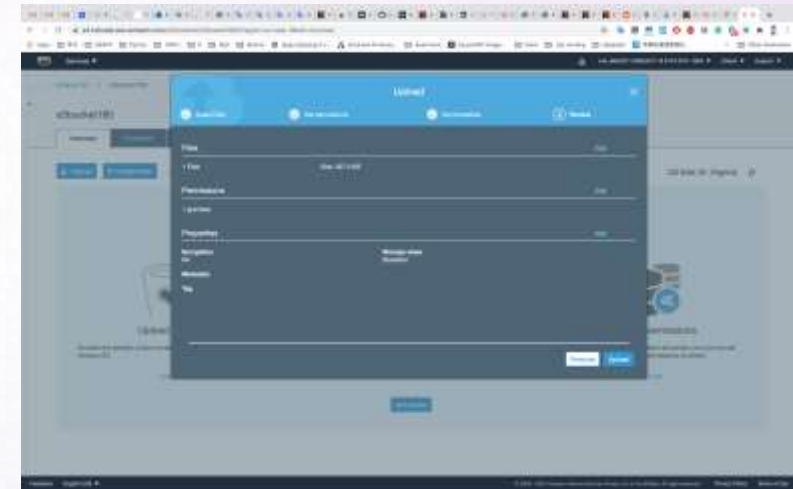
Step 6



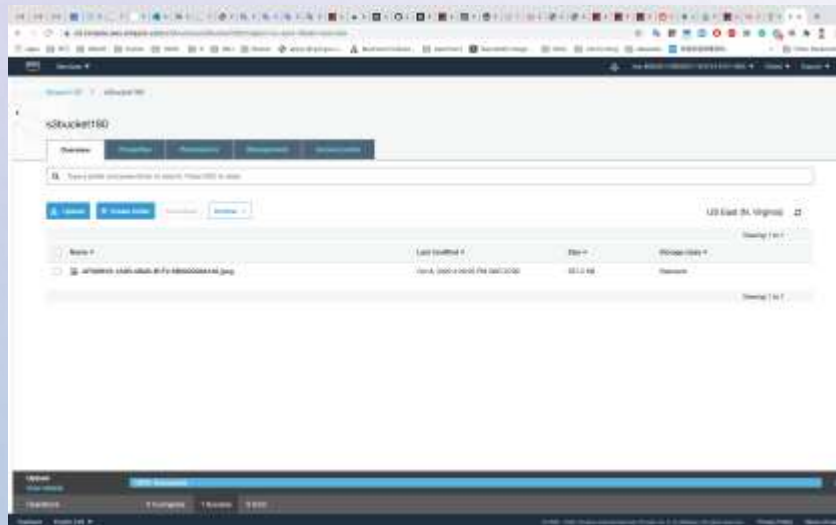
Step 7



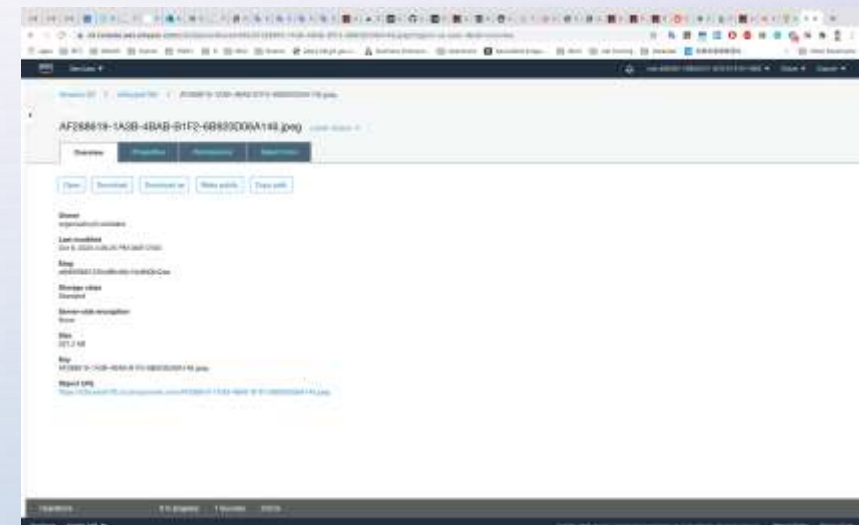
Step 8



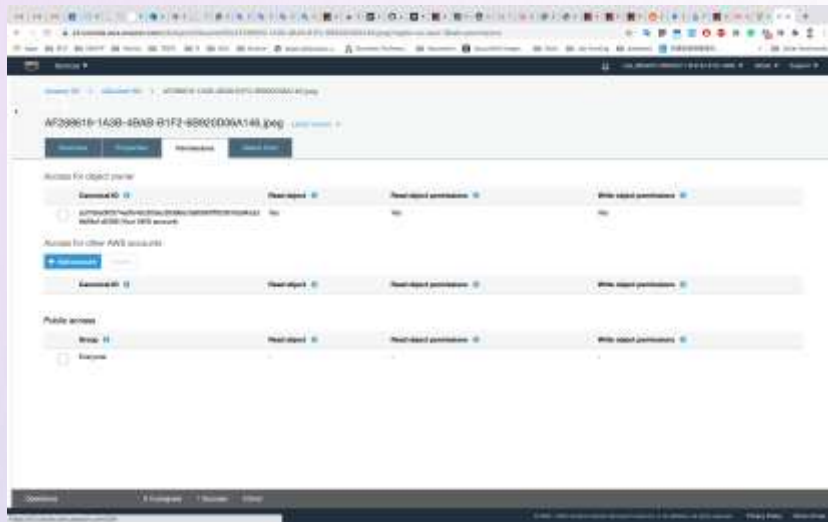
Step 9



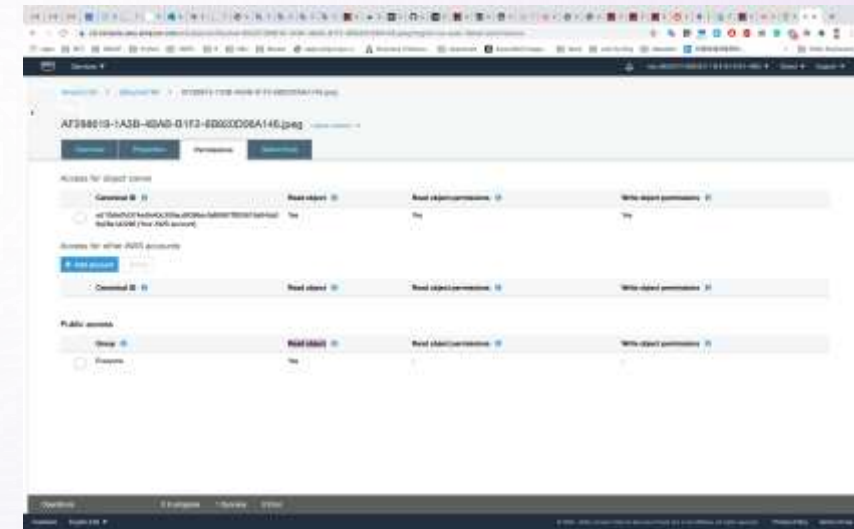
Step 10



Step 11



Step 12



Step 13



Step 14

BUILDING A VPC AND LAUNCHING A 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

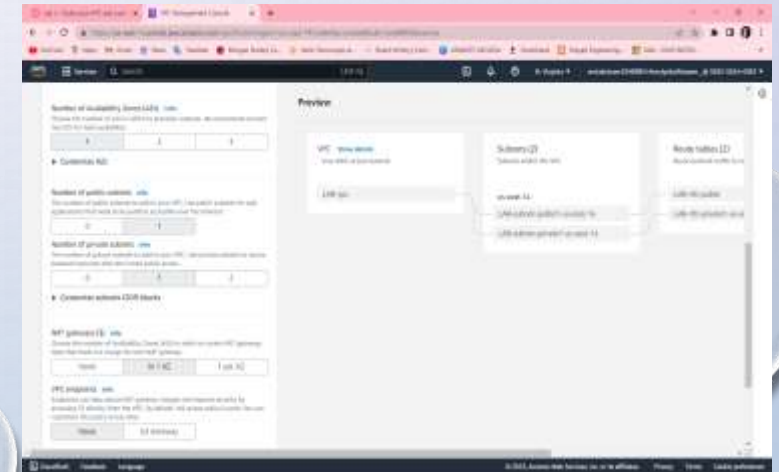
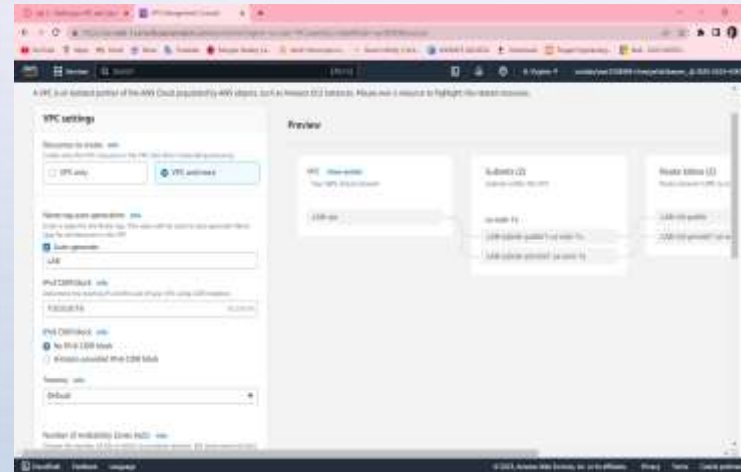
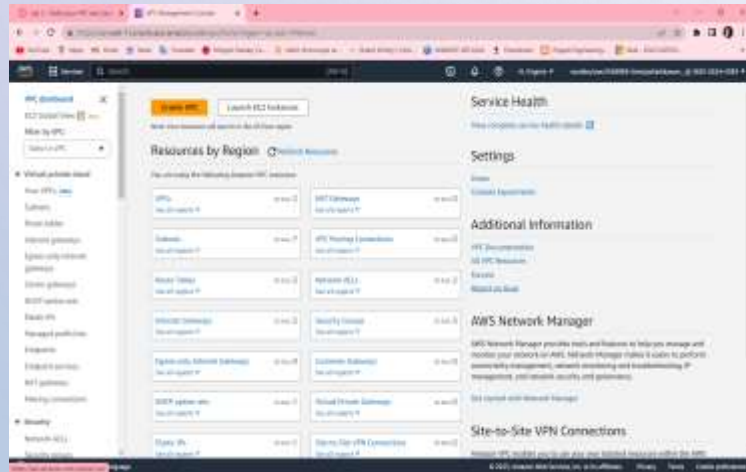
Step 4: Choose VPC and more, in name tag auto-generation, keep auto-generate select and change it to a lab.

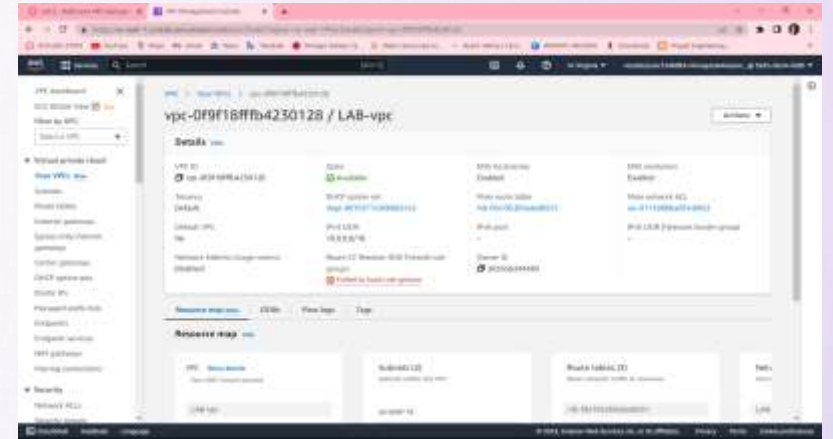
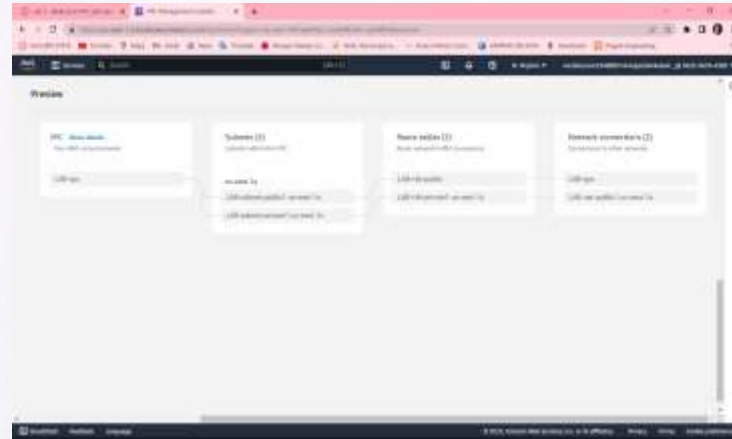
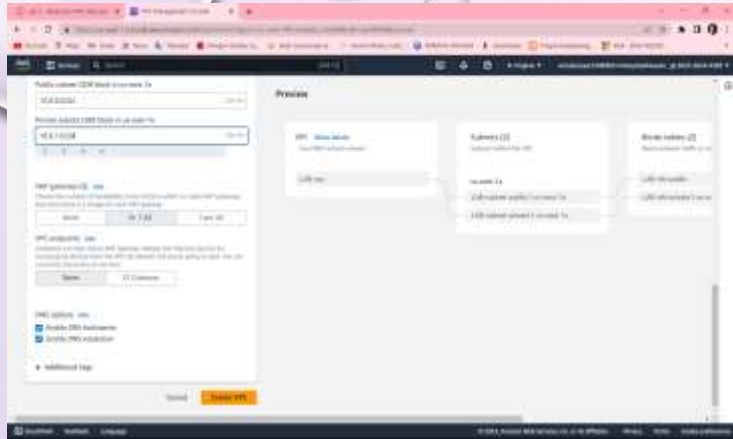
Step 5: Keep the IPv4 CIDR block to 10.10.0.0/16 and next for a number of availability zones select 1, number of public subnets select 1, number of private subnets select 1

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

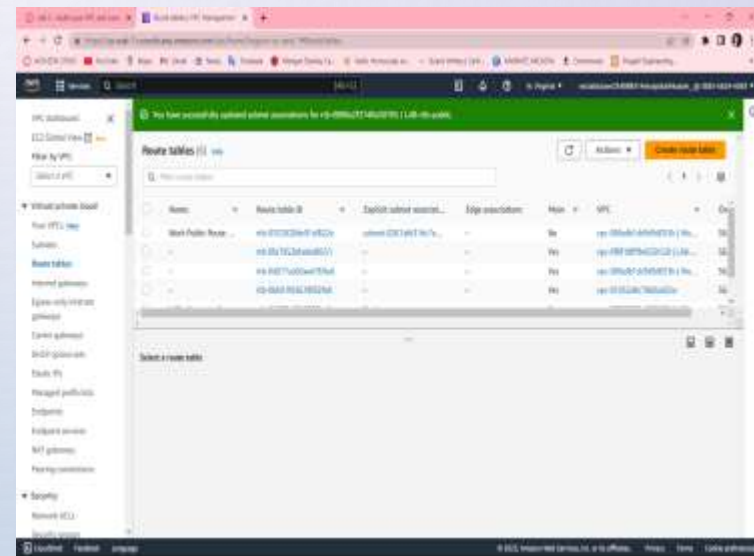
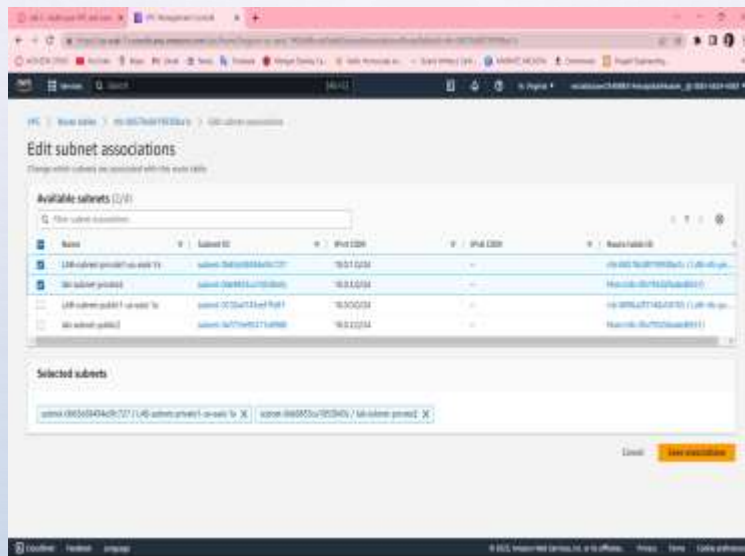
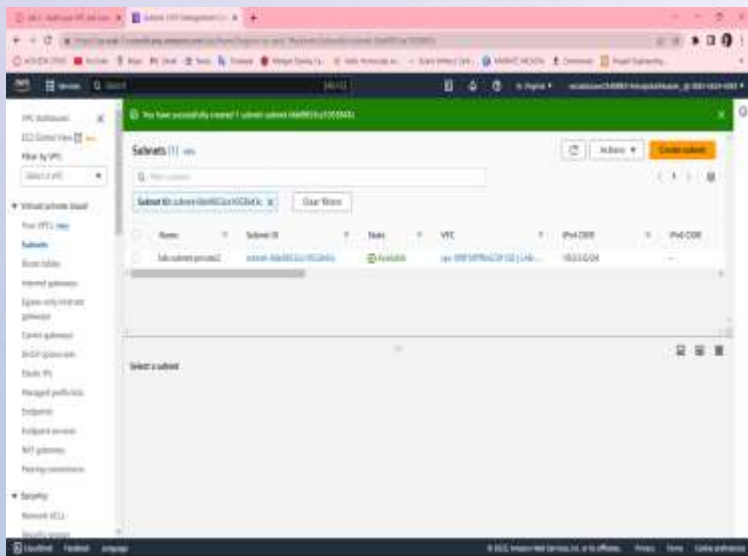
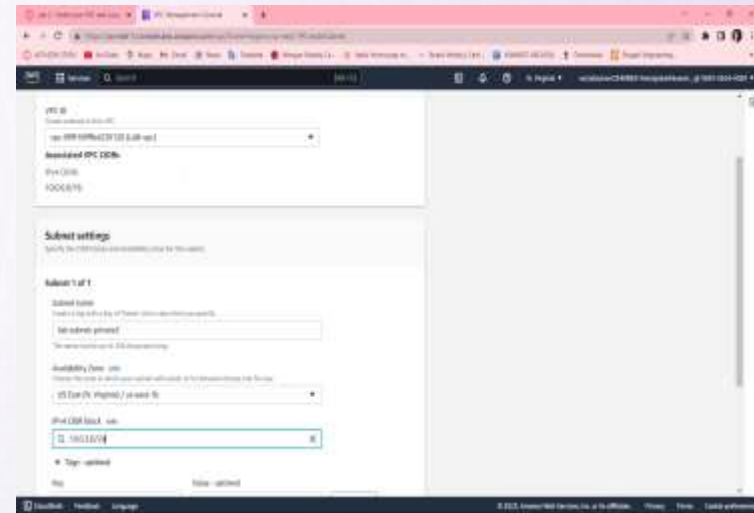
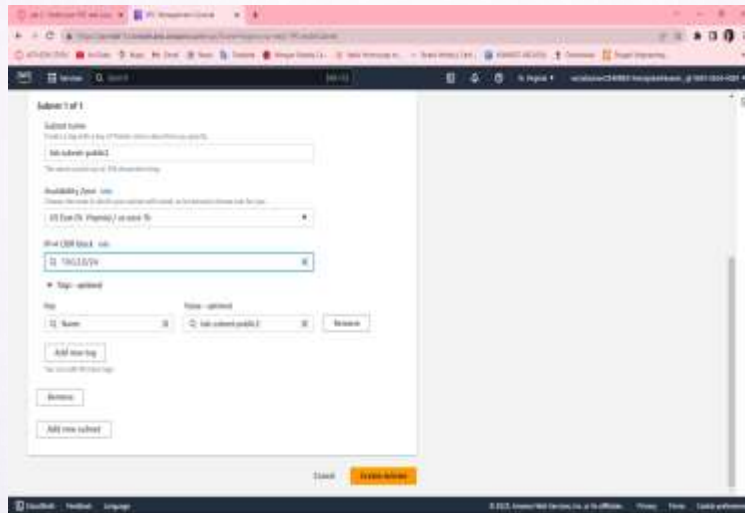
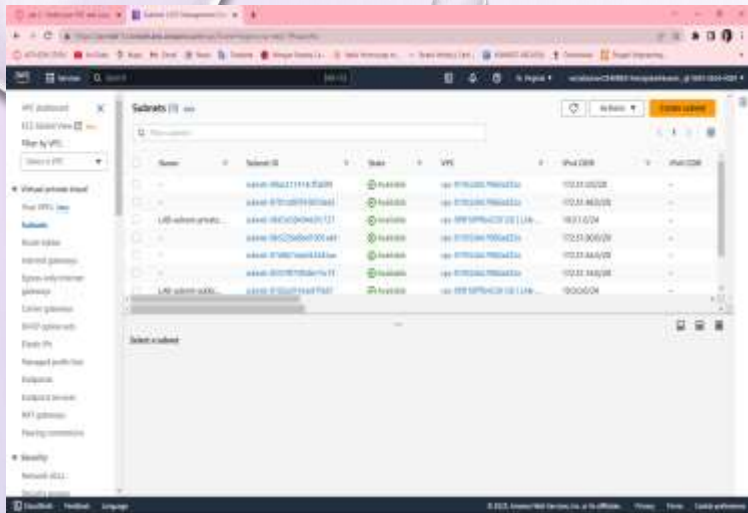
Step 5 : Leave lab-subnet-private1-us-east-1a and also select lab-subnet-private2

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



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

Create security group

A security group acts as a virtual firewall for your instance to control inbound and outbound traffic. To create a security group, complete the form below.

Basic details

Security group name:

Description:

VPC:

Inbound rules

Type: Protocol: Port range: Source: Description:

Outbound rules

Type: Protocol: Port range: Destination: Description:

Tags - optional

No tags associated with this resource.

Details

Security group name: Security group ID: Description: VPC ID:

Inbound rules (1/1)

Type	Protocol	Port range	Source	Description
HTTP	TCP	80	anywhere	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
```

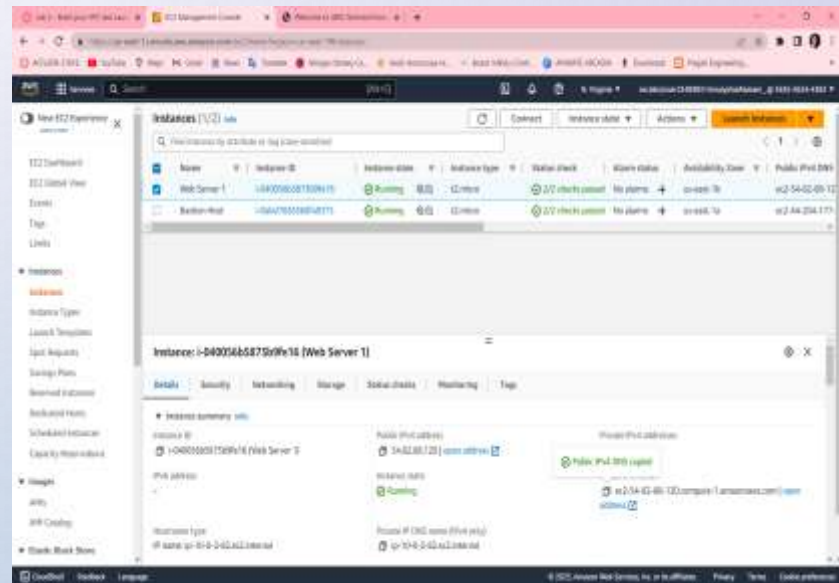
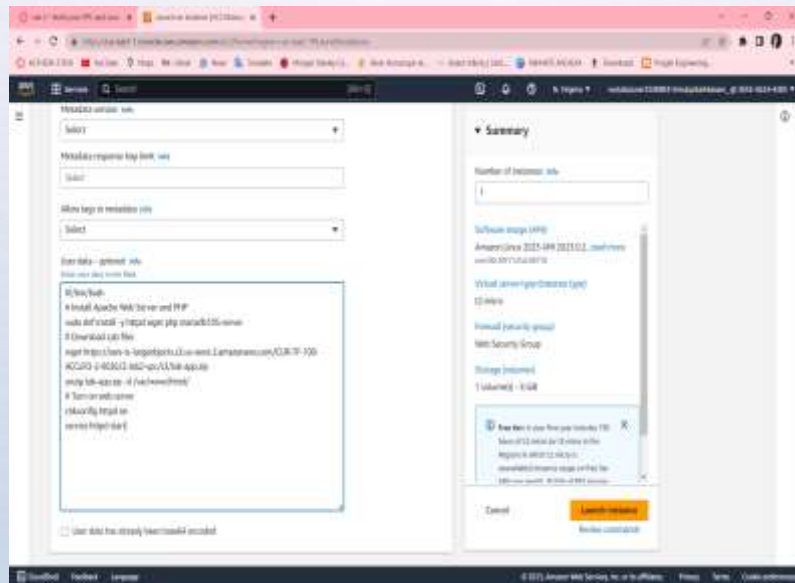
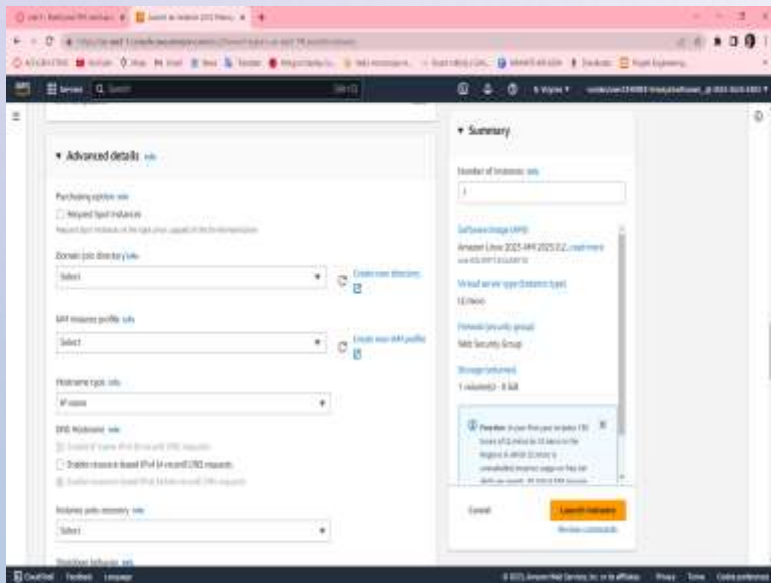
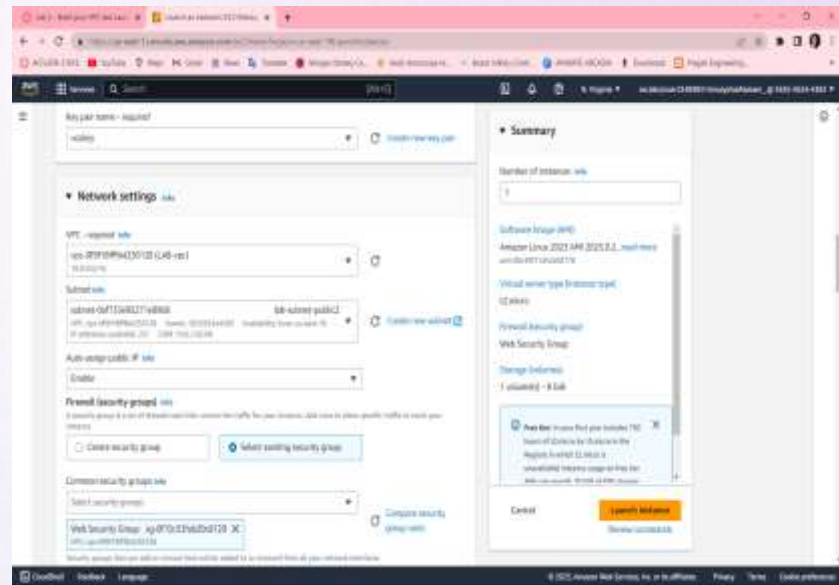
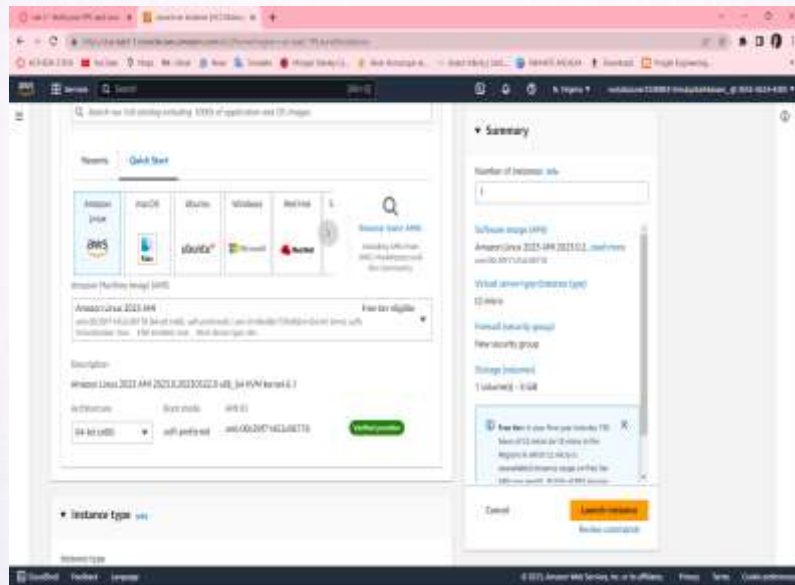
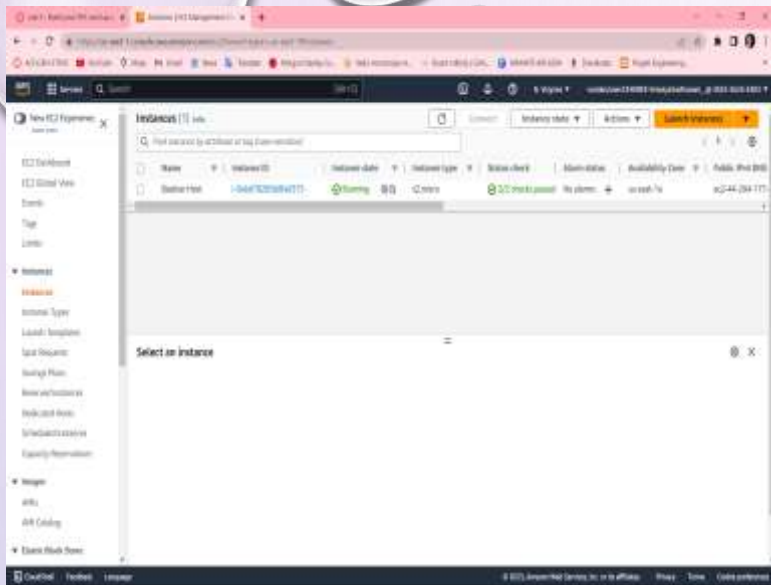
Step 6: At the bottom SUMMARY panel choose launch instance ,click on view instances

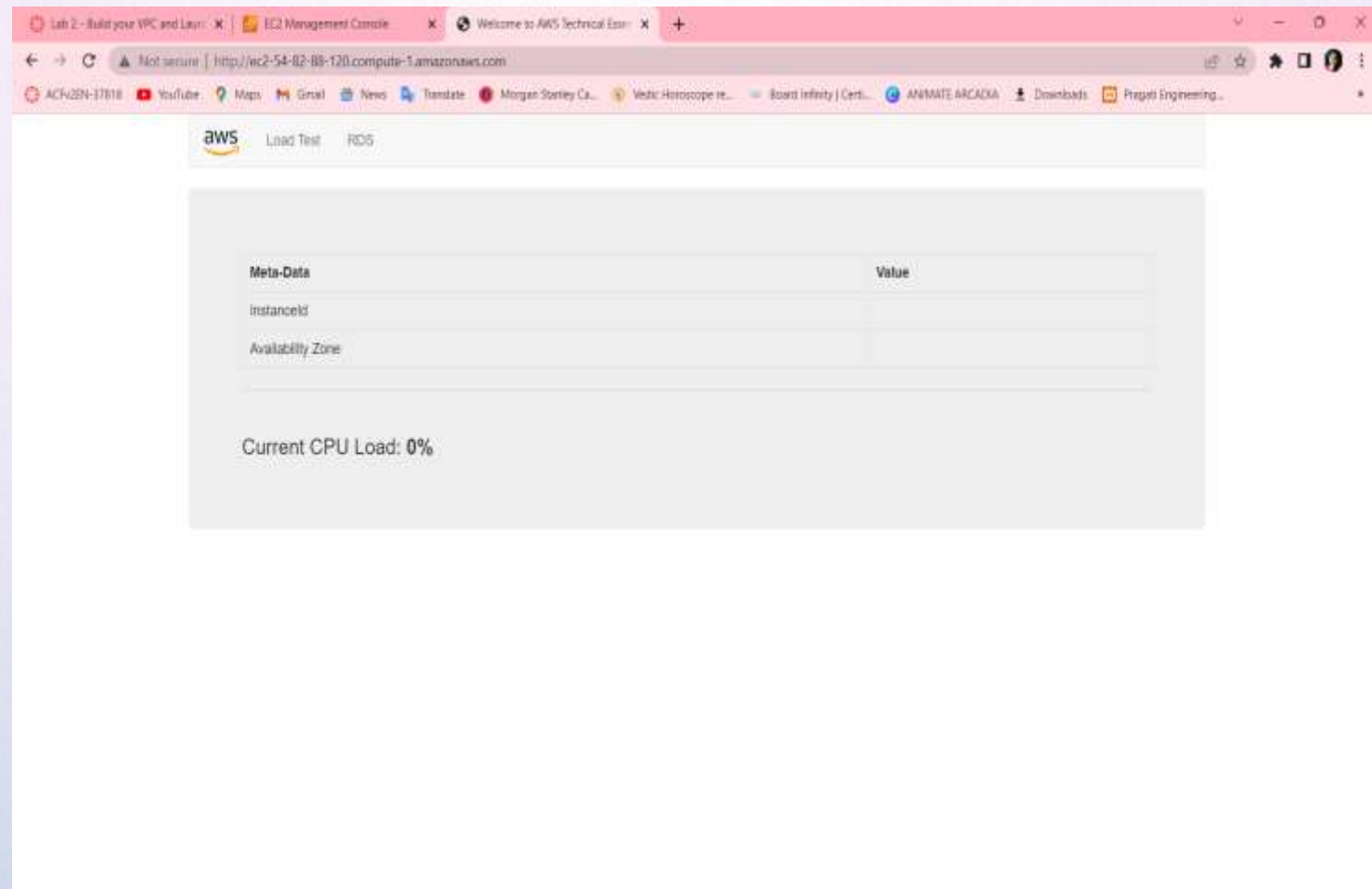
Step 7 : Wait until web server 1 shows 2/2 checks passed

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

The background is a light blue gradient. In the top left corner, there are several realistic water droplets of various sizes. A faint, circular logo is centered in the upper half of the image. The text "THANK YOU" is written in a large, bold, dark blue sans-serif font across the middle of the image. In the bottom right corner, there are more water droplets, including a large one and several smaller ones.

THANK YOU