

# aws



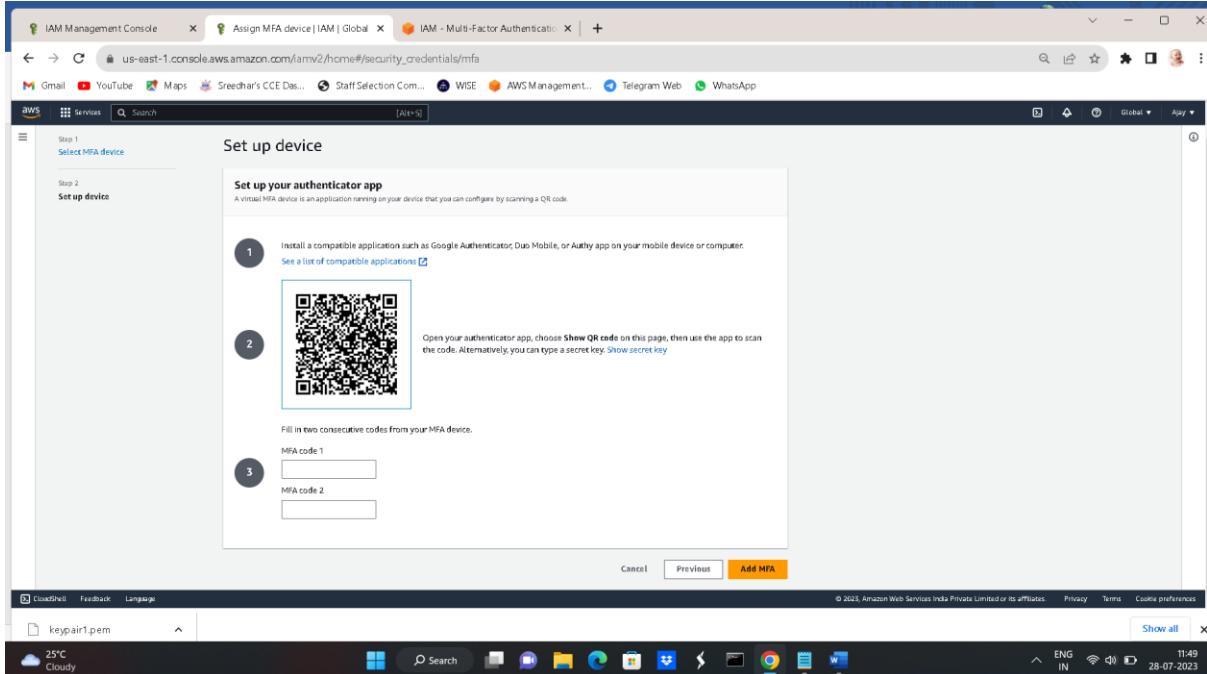
T.Ajay

6301925313

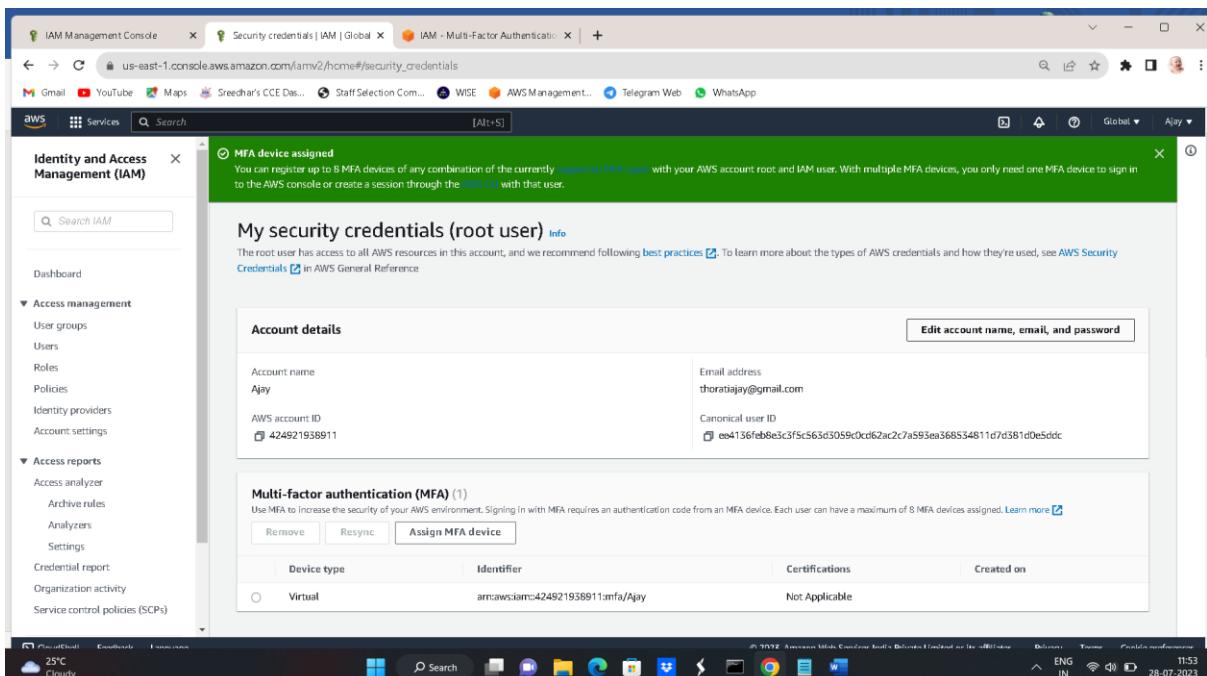
# LAB-1

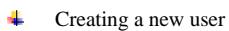
## IAM Hands on

- Creating mfa for root user
- For the creation of mfa you need to install one authenticator app from play store and scan the QR through the app .in that app mfa codes are generated.enter the codes below and click on add mfa.



Mfa is assigned to the user successfully.





- Creating a new user  
For creating new user go to IAM and goto users and provide name and attach policies to user and create user.

Specify user details

User details

User name: dhoni

Provide user access to the AWS Management Console - optional

Are you providing console access to a person?

User type:

Specify a user in Identity Center - Recommended

We recommend that you use Identity Center to provide console access to a person. With Identity Center, you can centrally manage user access to their AWS accounts and cloud applications.

I want to create an IAM user

We recommend that you create IAM users only if you need to enable programmatic access through access keys, service-specific credentials for AWS CodeCommit or Amazon Keyspaces, or a backup credential for emergency account access.

If you are creating programmatic access through access keys or service-specific credentials for AWS CodeCommit or Amazon Keyspaces, you can generate them after you create this IAM user. Learn more

Cancel Next Step

- By default there is no permissions for user you have to attach it. First assign EC2full access and try to access another resource.

IAM > Users > Create user

Review and create

User details

User name: dhoni

Console password type: Custom password

Require password reset: Yes

Permissions summary

Name	Type	Used as
AmazonEC2FullAccess	AWS managed	Permissions policy
IAMUserChangePassword	AWS managed	Permissions policy

Tags - optional

No tags associated with the resource.

Add new tag

Create user

- ↳ Iam trying to create an s3 bucket it will throw an error as permissions are required.

The screenshot shows the AWS IAM Management Console with the URL [s3.console.aws.amazon.com/s3/bucket/create?region=us-east-1](https://s3.console.aws.amazon.com/s3/bucket/create?region=us-east-1). The 'Create bucket' button is highlighted in yellow. A red error message box is displayed, stating: "Failed to create bucket" and "To create a bucket, the s3:CreateBucket permission is required." It also links to "View your permissions in the IAM console" and "Identity and Access Management in Amazon S3". Below the error message, there's a link to "API response".

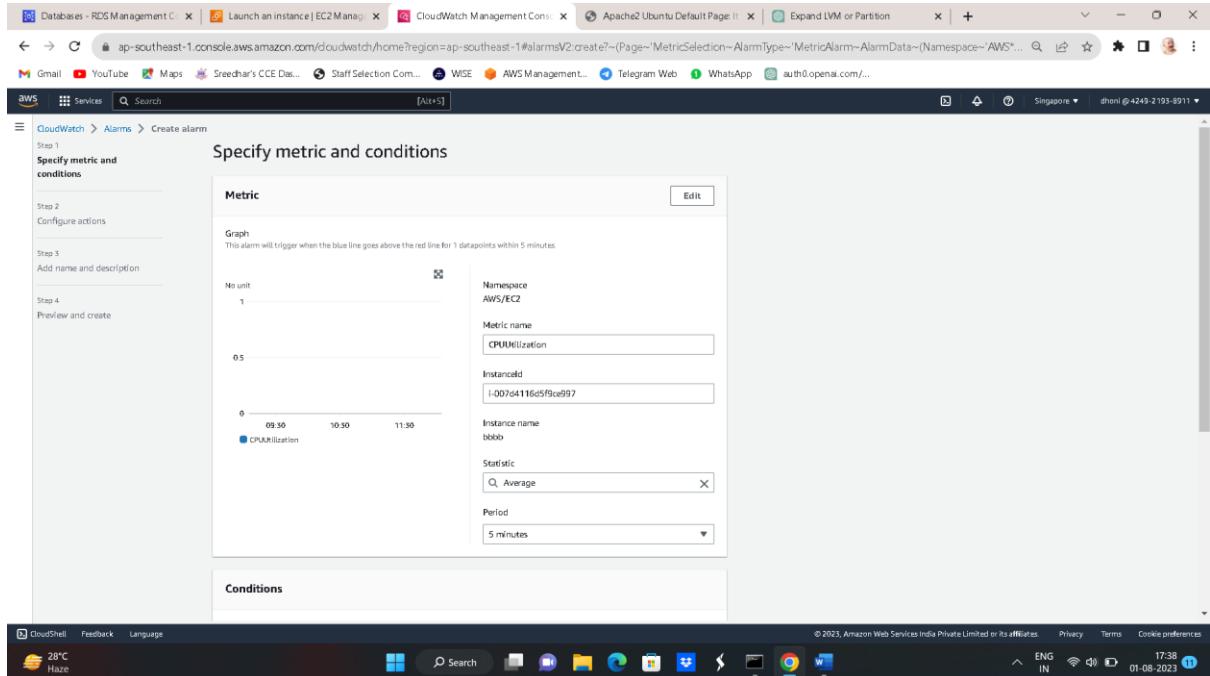
- ↳ Adding administration access to the user then you have to access all the all services.

The screenshot shows the AWS IAM Management Console with the URL [us-east-1.console.aws.amazon.com/iamv2/home?region=ap-south-1#/users/details/dhoni?section=permissions](https://us-east-1.console.aws.amazon.com/iamv2/home?region=ap-south-1#/users/details/dhoni?section=permissions). The 'Permissions' tab is selected. Under 'Permissions policies (2)', the 'AdministrationAccess' policy is listed under 'AWS managed - job function'. The 'AmazonEC2FullAccess' policy is also listed under 'AWS managed'. The 'Attached via' column shows 'Directly' for both policies.

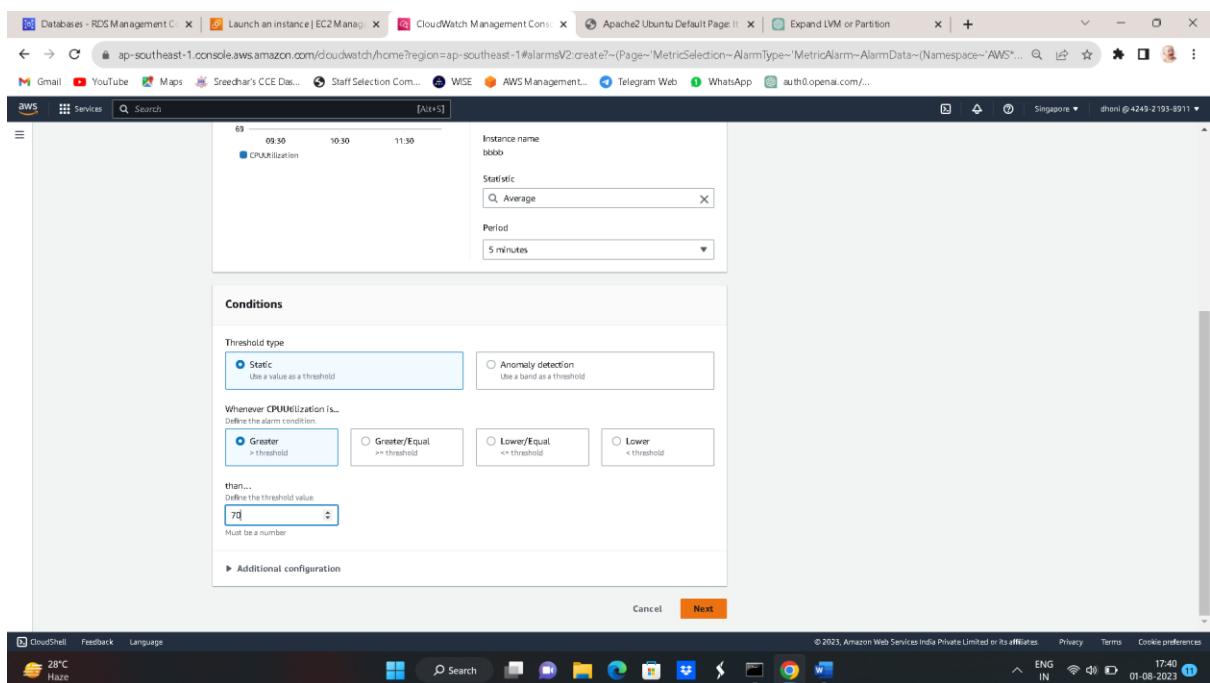
# LAB-2

## Billing alarm

- Creating billing alarm for your account to get a notification whenever you cross the billing threshold.
- For the creation of alarm go to cloud watch and click on create alarm and select metric



- Setup your conditions and threshold values.



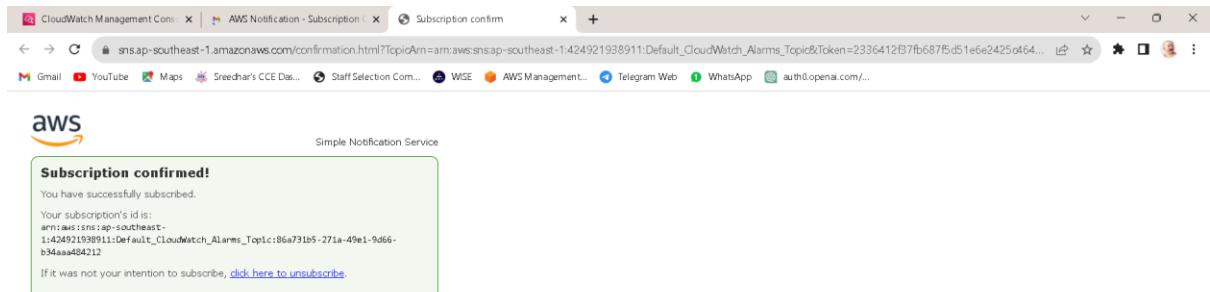
- ❖ Create an SNS topic with your email.

The screenshot shows the AWS CloudWatch Metrics Alarm creation wizard at Step 2: Configure actions. In the 'Notification' section, under 'Alarm state trigger', the 'In alarm' option is selected. Under 'Send a notification to the following SNS topic', the 'Create new topic' option is selected, and the topic name is 'aws'. Below this, an email endpoint 'thoratjay@gmail.com' is listed. In the 'Auto Scaling action' section, there is a 'Create topic' button and an 'Add notification' button.

- ❖ In the next step add name and configuration and click review and create.
- ❖ Alarm is created but we need to confirm the subscription via email.

The screenshot shows the AWS CloudWatch Metrics Alarm creation wizard at Step 3: Add name and configuration. A green banner at the top says 'Successfully created alarm ec2alarm.' Below it, a message states 'Some subscriptions are pending confirmation' with a link to 'View SNS Subscriptions'. The main table shows one alarm entry: 'ec2alarm' with the condition 'CPUUtilization > 70 for 1 datapoints within 6 hours'. The status is 'Actions enabled' with a 'Warning' icon.

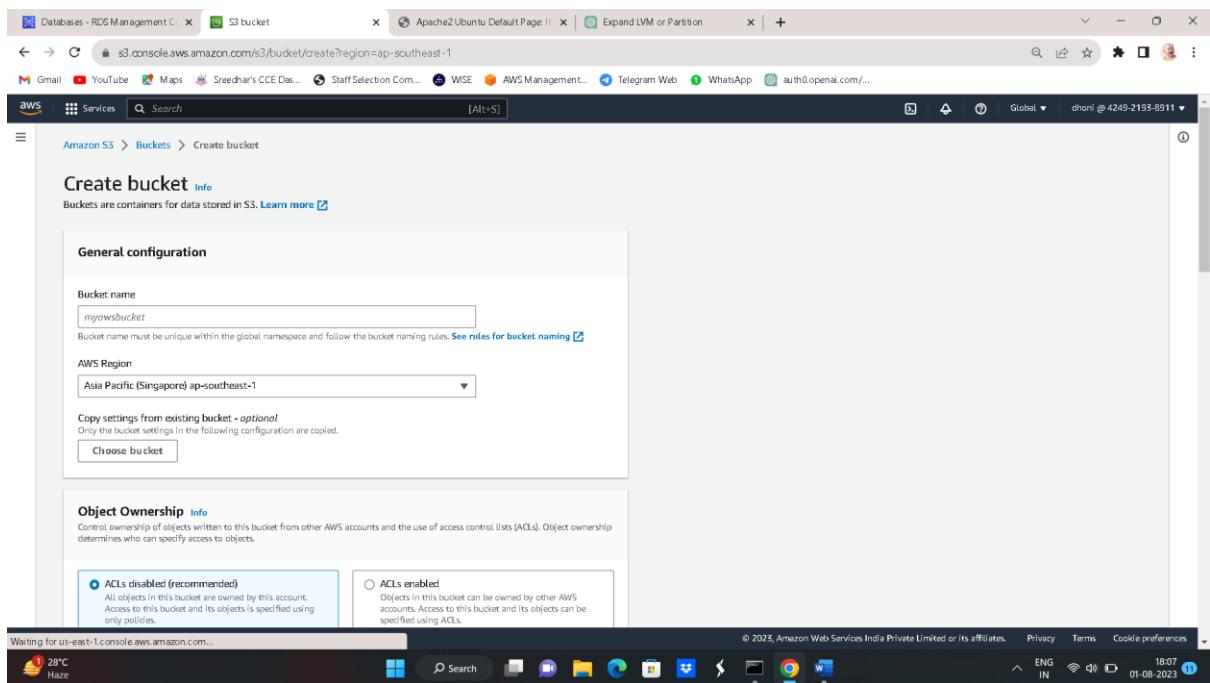
- ❖ Open your email and confirm the subscription then you will get alarm notifications to your mail.



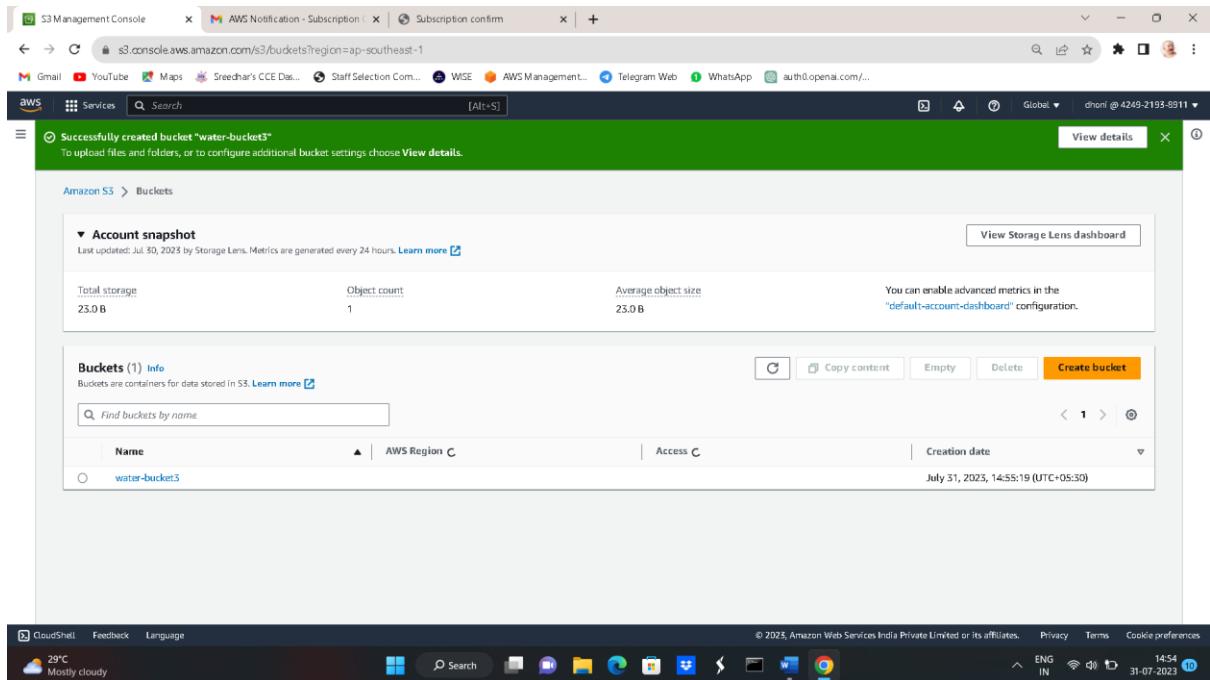
## LAB-3

### S3 bucket

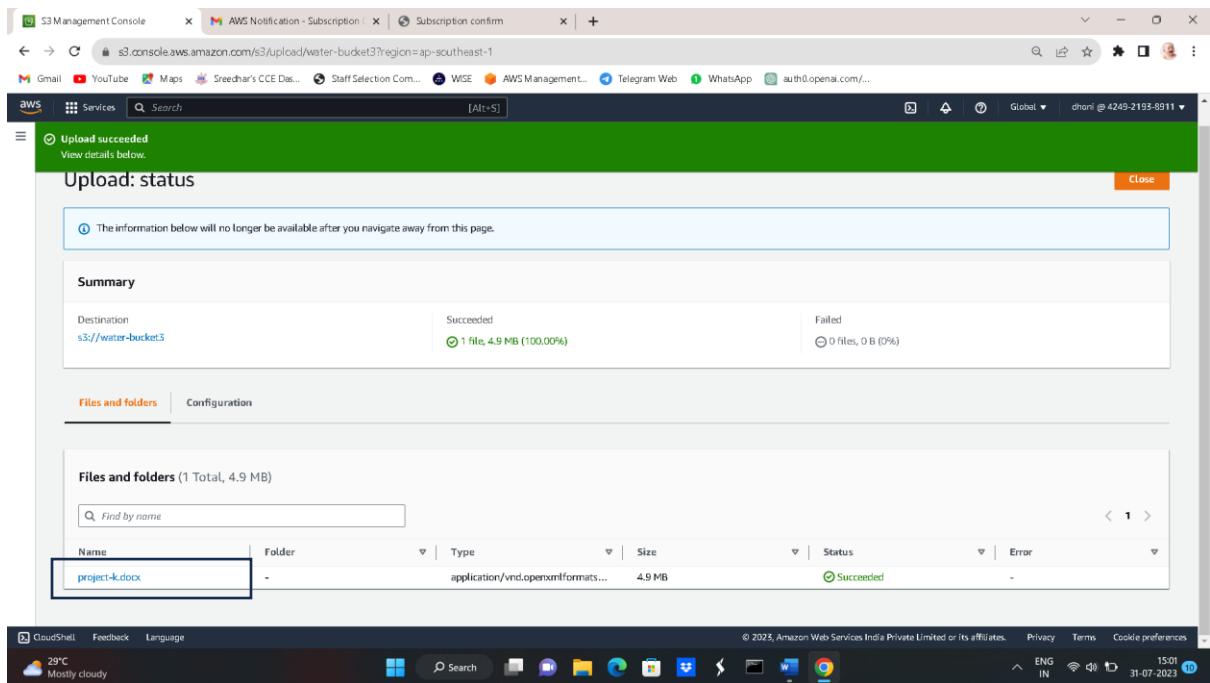
- ➊ Creating an s3 bucket with unique name
- ➋ For the creation of s3 bucket goto s3 bucket click on create bucket and give bucket name and ACL's disable and don't give any public access.



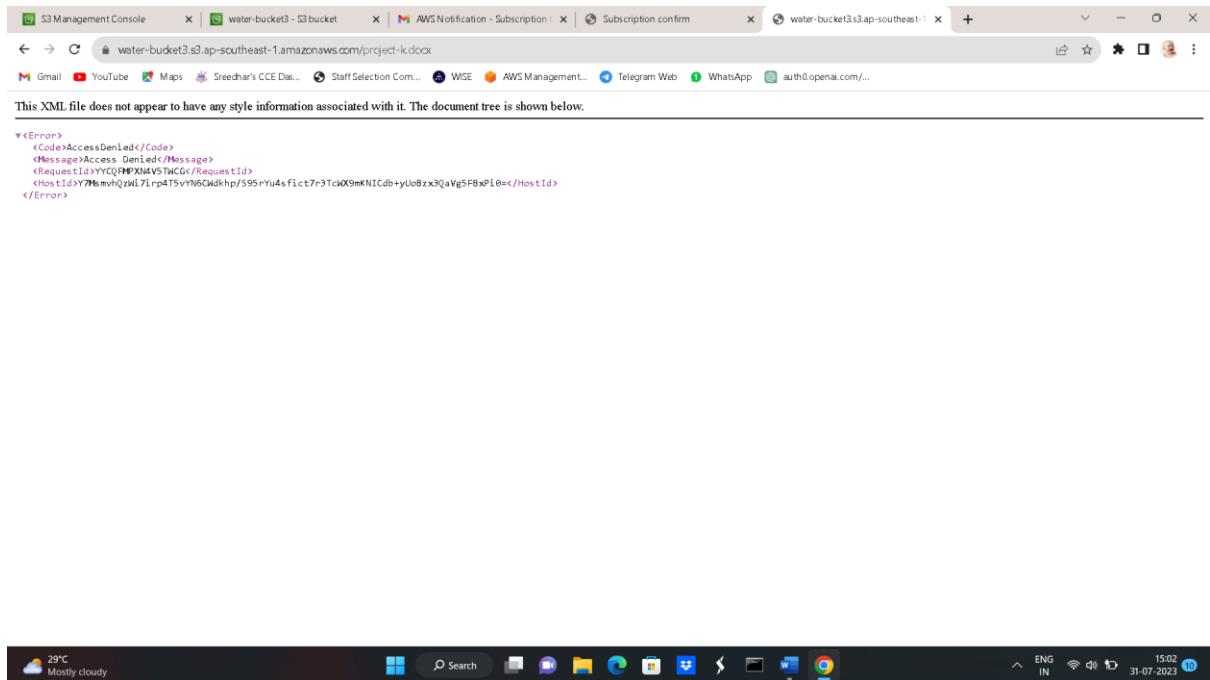
- ➌ Bucket created successfully.



✍ Enter into the bucket and Add some file into that bucket by using upload file icon.



✍ Try to access the file by copying the url it throws an error because we are not give public access to that bucket.



Modify the permissions of the bucket and enable ACL's in the permissions.

water-bucket3

Permissions

Block public access (bucket settings)

Block all public access

Off

Individual Block Public Access settings for this bucket

Bucket policy

Edit Delete

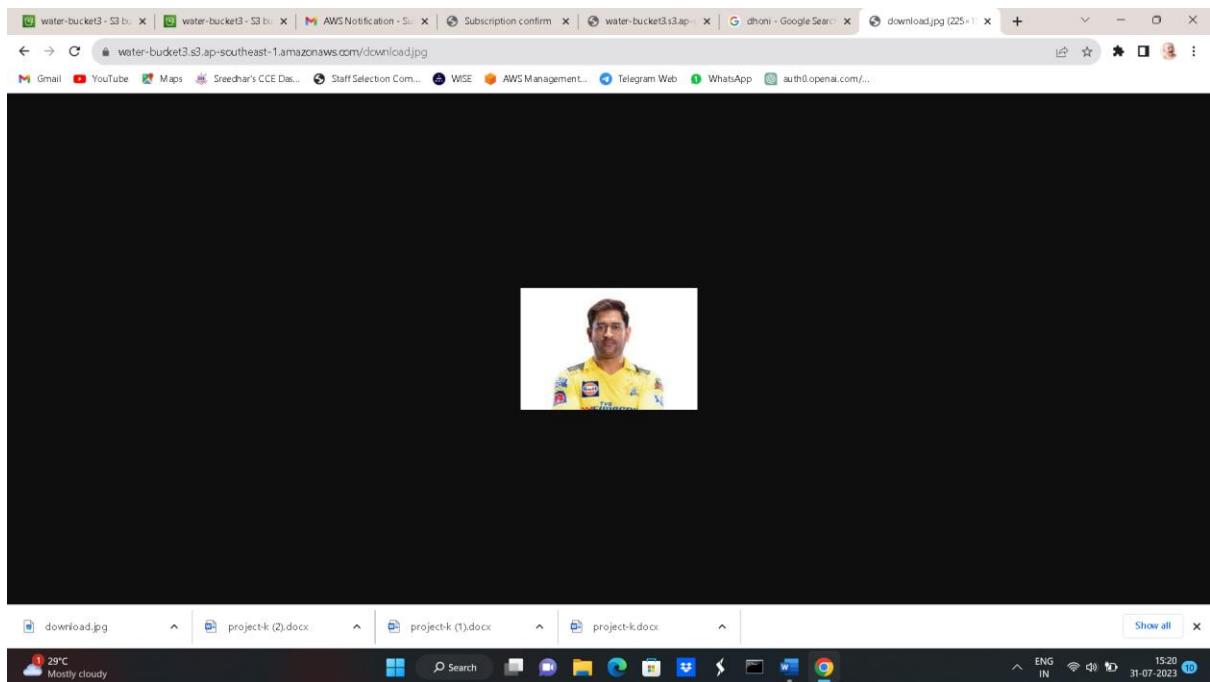
- Successfully added the public access.

The screenshot shows the AWS S3 console with a green success banner at the top stating "Successfully edited public access". Below it, a summary table shows "Source: s3://water-bucket3" with "Successfully edited public access" and "1 object, 4.9 MB". A "Failed to edit public access" section shows "0 objects". The status bar at the bottom indicates "29°C Mostly cloudy" and the date "31-07-2023".

- Upload the file and in the go to actions and select make the object public.

The screenshot shows the AWS S3 console with a red "Publicly accessible" button. The "Objects" tab is selected, showing one item: "download.jpg" (Type: jpg). The "Actions" dropdown menu is highlighted. The status bar at the bottom indicates "29°C Mostly cloudy" and the date "31-07-2023".

- Copy the URL of that file and paste in browser now you can access file publicly.



Now enable the versioning of the bucket so that you can retrieve your file after deletion.

A screenshot of the AWS Management Console for an S3 bucket named 'water-bucket3'. The top navigation bar shows the URL 's3.console.aws.amazon.com/s3/buckets/water-bucket3?region=ap-southeast-1&amp;tab=properties'. A green banner at the top says 'Successfully edited Bucket Versioning'. The 'Bucket overview' section shows the AWS Region as 'Asia Pacific (Singapore) ap-southeast-1', the ARN as 'arn:aws:s3:::water-bucket3', and the Creation date as 'July 31, 2023, 14:55:19 (UTC+05:30)'. The 'Bucket Versioning' section has a status of 'Enabled'. The 'Tags (0)' section indicates no tags are present. The bottom of the page includes standard AWS footer links like CloudShell, Feedback, Language, and a copyright notice for 2023. The taskbar and system tray are visible at the bottom, showing the same information as the previous screenshot.

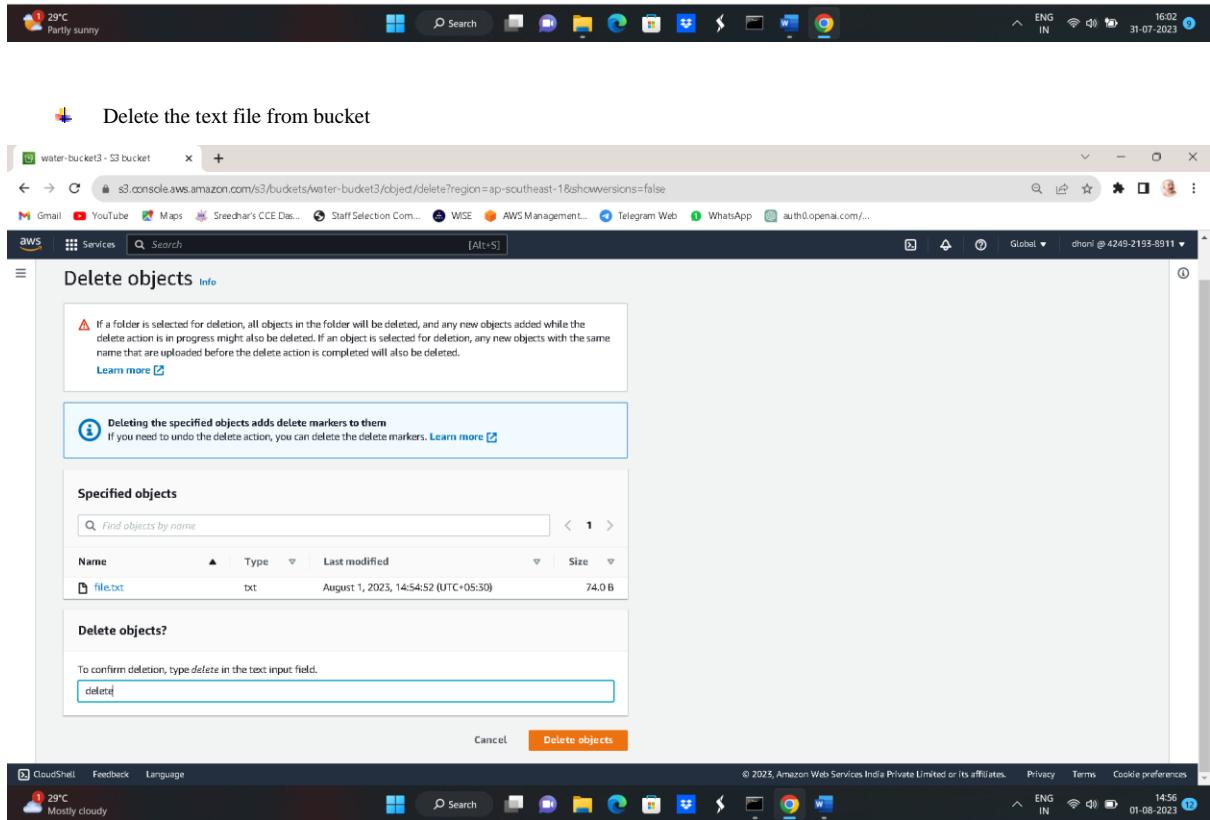
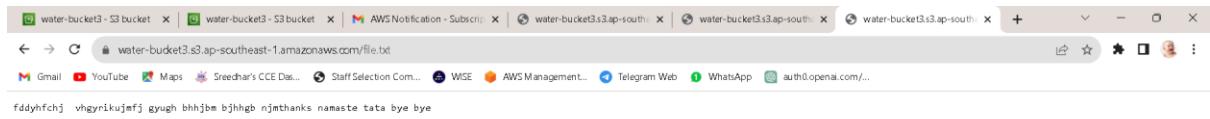
Created a text file and uploaded in the bucket

The screenshot shows the AWS S3 console interface. At the top, there are several tabs and links. Below the header, the navigation bar shows 'Amazon S3 > Buckets > water-bucket3'. The main content area is titled 'water-bucket3 info' and has a 'Publicly accessible' button. Below this are tabs for 'Objects', 'Properties', 'Permissions', 'Metrics', 'Management', and 'Access Points'. The 'Objects' tab is selected, displaying a table with two rows. The first row is for 'download.jpg' (jpg type, 5.0 KB, last modified July 31, 2023, 15:18:56 UTC+05:30). The second row is for 'file.txt' (txt type, 14.0 B, last modified July 31, 2023, 15:31:07 UTC+05:30). The 'file.txt' row is highlighted with a blue selection box.

☛ Check the content of the file

The screenshot shows a web browser window with multiple tabs open. The active tab displays the content of the 'file.txt' file from the 'water-bucket3' S3 bucket. The content of the file is: 'thanks namaste tata bye bye'. The browser's address bar shows the URL: 'water-bucket3.s3.ap-southeast-1.amazonaws.com/file.txt'. The browser's toolbar includes icons for back, forward, search, and other functions. The status bar at the bottom right shows the date and time: '31-07-2023 15:55'.

☛ Update the text file content and upload into the bucket. After uploading the old text file was replaced with new file automatically.



- After deleting the file the versions are present . now click on show versions there you have your deleted file now delete the marker file then the file is retrieved back automatically.

The screenshot shows the AWS S3 console interface. At the top, there's a navigation bar with tabs like 'Services', 'Search', and 'AWS Management...'. Below it, a breadcrumb trail shows 'Amazon S3 > Buckets > water-bucket3'. The main area is titled 'water-bucket3 info' and has tabs for 'Objects', 'Properties', 'Permissions', 'Metrics', 'Management', and 'Access Points'. Under the 'Objects' tab, there's a table with two rows. The first row is for a 'Delete marker' object named 'file.txt', which was last modified on August 1, 2023, at 14:57:49 UTC+05:30. The second row is for a 'txt' object named 'file.txt', which was last modified on August 1, 2023, at 14:54:52 UTC+05:30. Both objects have a size of 0 B and are in the 'Standard' storage class.

## LAB-4

### EC2 Instance

Creating one ec2 instance of type t2.micro with ubuntu OS .

The screenshot shows the AWS EC2 Instances page. On the left, there's a sidebar with options like 'New EC2 Experience', 'EC2 Dashboard', 'EC2 Global View', 'Events', 'Instances' (selected), 'Instance Types', 'Launch Templates', 'Spot Requests', 'Savings Plans', 'Reserved Instances', 'Dedicated Hosts', 'Capacity Reservations', 'Images', 'AMIs', and 'AMI Catalog'. The main area shows a table with one instance listed: 'ec2' (Instance ID: i-067807647ab4ec262). The instance is 'Running' (Status check: Initializing) and is of type 't2.micro'. It's located in the 'ap-southeast-1b' availability zone with a public IPv4 DNS of 'ec2-13-229-69-'. The instance details pane shows the AMI ID as 'ami-0df7a207adb9748c7', the AMI name as 'ubuntu/images/hvm-ssd/ubuntu-jammy-22.04-amd64-server-20230516', and the launch time as 'Mon Jul 31 2023 16:22:14 GMT+0530 (India Standard Time)'. The AMI location is 'amazon/ubuntu/images/hvm-ssd/ubuntu-jammy-22.04-amd64-server-20230516'.

Allowed the required port in the security groups so that you can access it from outside.

**Details**

Security group name	sg-0ceca4c4ba982f307	Description	VPC ID
Owner	424921938911	Inbound rules count	2 Permission entries
		Outbound rules count	1 Permission entry

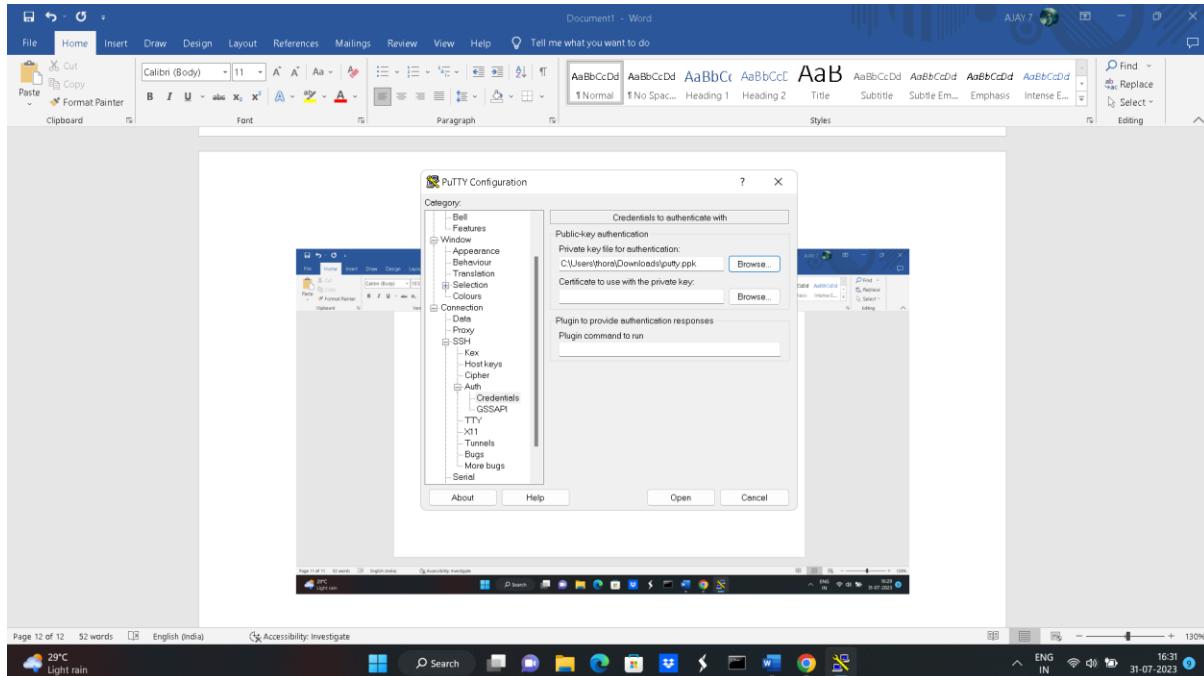
**Inbound rules (2)**

Name	Security group rule...	IP version	Type	Protocol	Port range	Source
-	sgr-02462ff7d5d1042c9	IPv4	SSH	TCP	22	0.0.0.0/0
-	sgr-091caa35c8a850f63	IPv4	All TCP	TCP	0 - 65535	0.0.0.0/0

Copy the public ip of instance and give to the putty.

The screenshot shows a Microsoft Word document titled "Document1 - Word". A "Putty Configuration" dialog box is open over the document. The "Host Name (or IP address)" field in the dialog box is highlighted with a red box, containing the value "13.223.69.108". The dialog box also shows "Port" set to 22, "Protocol" set to SSH, and "Save" and "Cancel" buttons at the bottom. The background of the Word document shows a sidebar with various AWS services like CloudWatch, Lambda, and Step Functions.

- Now go to SSH → Auth → credentials → Browse and Provide private key file with .ppk extension click on open.



- Enter Login as ubuntu now you can access your ubuntu machine.

```
ubuntu@ip-172-31-21-181:~$ login as: ubuntu
[warn] No matching host key fingerprint found. You might be connecting to a different host.
Welcome to Ubuntu 22.04.2 LTS (GNU/Linux 5.19.0-1025-aws x86_64)

 * Documentation: https://help.ubuntu.com
 * Management: https://landscape.canonical.com
 * Support:   https://ubuntu.com/advantage

System information as of Mon Jul 31 11:04:18 UTC 2023

System load:  0.0          Processes:           96
Usage of /:  20.6% of 7.57GB   Users logged in:    0
Memory usage: 24%           IPV4 address for eth0: 172.31.21.181
Swap usage:  0B

Expanded Security Maintenance for Applications is not enabled.

0 updates can be applied immediately.

Enable ESM Apps to receive additional future security updates.
See https://ubuntu.com/esm or run: sudo pro status

The list of available updates is more than a week old.
To check for new updates run: sudo apt update

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/*copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.

ubuntu@ip-172-31-21-181:~$
```

# Lab-5

## Security group

- Creating new security group by default there is no inbound rules assigned to the security group.

The screenshot shows the AWS VPC Management Console. On the left, a sidebar lists various VPC-related services like EC2 Global View, Subnets, Route tables, and Security groups. The main area displays the details of a security group named 'sg-0ceca4c4ba982f307 - mynewSG'. The 'Details' section shows the security group name, ID, owner, and counts for inbound and outbound rules. Below this, the 'Inbound rules' tab is selected, showing a table with columns for Name, Security group rule..., IP version, Type, Protocol, Port range, and Source. A note at the top of this section says, 'You can now check network connectivity with Reachability Analyzer' and includes a 'Run Reachability Analyzer' button. The status bar at the bottom indicates it's 29°C, Light rain, and the date is 31-07-2023.

- Add port 22,80 to the security group.

This screenshot shows the same security group 'mynewSG' after adding two inbound rules. The 'Inbound rules' table now contains two entries:

Name	Security group rule...	IP version	Type	Protocol	Port range	Source
-	sgr-02462fffd5d1042c9	IPv4	SSH	TCP	22	0.0.0.0/0
-	sgr-0f50ab9b34dab10c3	IPv4	HTTP	TCP	80	0.0.0.0/0

The rest of the interface and status bar are identical to the previous screenshot.

Attaching this new security group to existing ec2 instance.

Instance details

Associated security groups

No security groups attached to this network interface

Cancel Save

Connect the instance through ssh using port number 22.

```
ec2-user@ip-172-31-31-207: ~ % ssh -i mykeypair.pem ec2-user@ec2-18-142-186-66.ap-southeast-1.compute.amazonaws.com
The authenticity of host 'ec2-18-142-186-66.ap-southeast-1.compute.amazonaws.com (18.142.186.66)' can't be established.
ECDSA key fingerprint is SHA256:8dG78Exh6njpBswk5lYIVzvxi5MFnels5BAE1hs.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added 'ec2-18-142-186-66.ap-southeast-1.compute.amazonaws.com,18.142.186.66' (ECDSA) to the list of known hosts.

Amazon Linux 2023
https://aws.amazon.com/linux/amazon-linux-2023
```

# Lab-6

## Volumes and Snapshots

- Creating 5GB EBS volume.

The screenshot shows the AWS Management Console with the EC2 service selected. In the main pane, a success message states "Successfully created volume vol-0cae94ff2f4e3d2ef." Below this, the "Volumes (1/2) Info" table lists the newly created volume. The volume details are shown in a modal window titled "Volume ID: vol-0cae94ff2f4e3d2ef (myvolume)".

Name	Volume ID	Type	Size	IOPS	Throughput	Snapshot	Created	Availability Zone
myvolume	vol-0cae94ff2f4e3d2ef	gp2	5 GiB	100	-	-	2023/07/31 18:08 GMT+5:30	ap-southeast-1a
	vol-0b69b5b6fd0c5a60b	gp3	8 GiB	3000	125	snap-0131791...	2023/07/31 17:57 GMT+5:30	ap-southeast-1b

Volume ID: vol-0cae94ff2f4e3d2ef (myvolume)

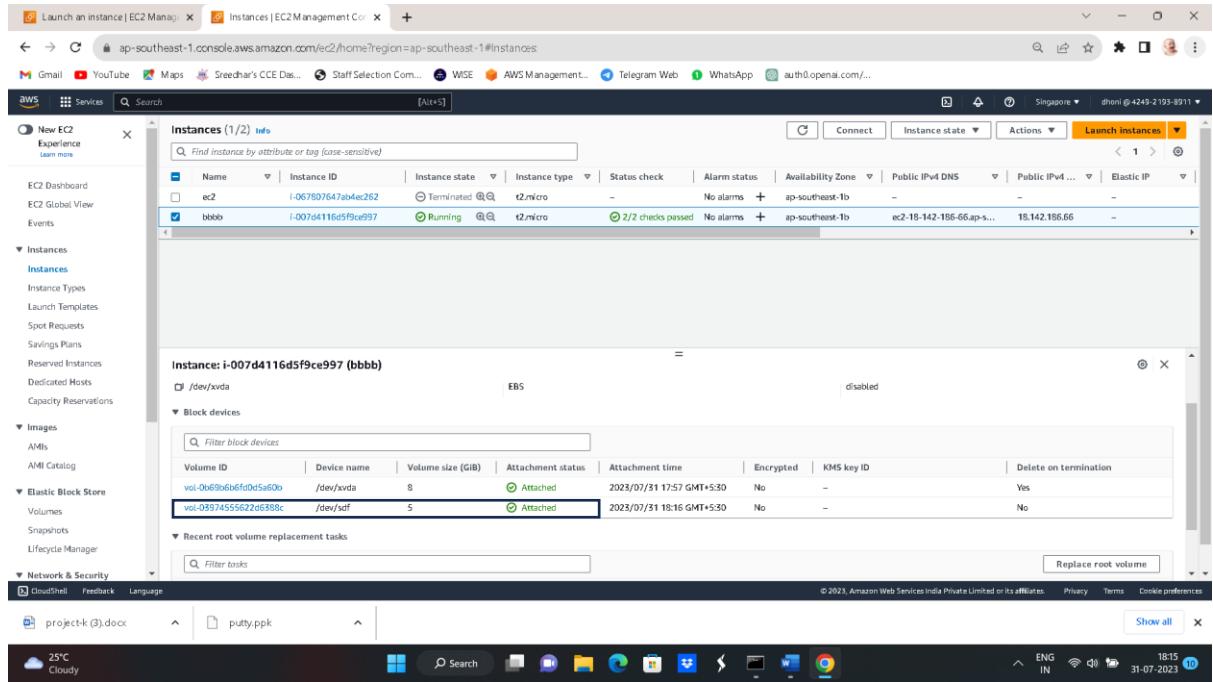
Details	Status checks	Monitoring	Tags
Volume ID vol-0cae94ff2f4e3d2ef (myvolume)	Size 5 GiB	Type gp2	Volume status OK
AWS Compute Optimizer finding Opt-in to AWS Compute Optimizer for recommendations, <a href="#">Learn more</a>	Volume state Creating	IOPS 100	Throughput
Encryption Not encrypted	KMS key ID -	KMS key alias -	KMS key ARN
Fast snapshot restored	Snapshot	Availability Zone	Created

- Attaching this volume to my instance

For the attachment select volume and go to actions and click on attach volume and select instance and click attach volume.

The screenshot shows the AWS Management Console with the EC2 service selected. A dialog box titled "Attach volume" is open, showing the "Basic details" section. The volume ID is set to "vol-03974555622d6388c (myvolume)" and the availability zone is "ap-southeast-1b". An instance is selected with the ID "i-00744116d5f9ce997". The device name is set to "/dev/sdf". A note at the bottom of the dialog box states: "Newer Linux kernels may rename your devices to /dev/rdisk through /dev/rwdb internally, even when the device name entered here (and shown in the details) is /dev/sdf through /dev/sdp." At the bottom right of the dialog box is a yellow "Attach volume" button.

 Successfully volume attached to instance.



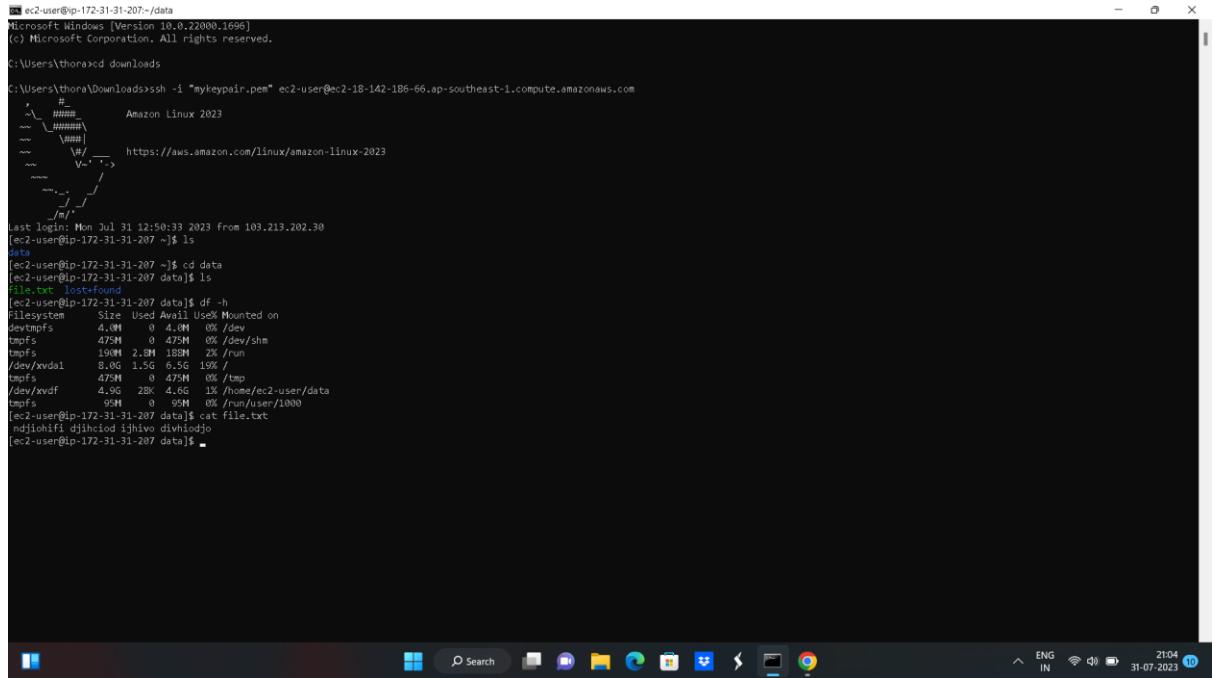
The screenshot shows the AWS EC2 Instances page. It lists two instances: 'ec2' (terminated) and 'bbbb' (running). The 'bbbb' instance is selected. In the 'Block devices' section, there are two entries:

Volume ID	Device name	Volume size (GiB)	Attachment status	Attachment time	Encrypted	KMS key ID	Delete on termination
vol-0b69a616fd0d5a60b	/dev/xvda	8	Attached	2023/07/31 17:57 GMT+5:30	No	-	Yes
vol-097455622d6390c	/dev/sdf	5	Attached	2023/07/31 18:16 GMT+5:30	No	-	No

 Mount the volume and add some text file.

 By default volume is not mounted you have to mount by using fallowing commands

- Sudo mkfs -t ext4 /dev/xvdf
- Sudo mkdir data
- Sudo mount /dev/xvdf data
- echo "This is a sample user data script." >> data/sample\_file.txt



```
ec2-user@ip-172-31-31-207:/data
Microsoft Windows [Version 10.0.22000.1696]
(c) Microsoft Corporation. All rights reserved.

C:\Users\thora>cd downloads

C:\Users\thora\Downloads>ssh -i "mykeypair.pem" ec2-user@ec2-18-142-186-66.ap-southeast-1.compute.amazonaws.com
Last Login: Mon Jul 31 12:50:33 2023 From 109.213.202.30
[ec2-user@ip-172-31-31-207 ~]$ ls
data
[ec2-user@ip-172-31-31-207 data]$ cd data
[ec2-user@ip-172-31-31-207 data]$ ls
file.txt lost+found
[ec2-user@ip-172-31-31-207 data]$ df -h
Filesystem      Size  Used Avail Use% Mounted on
udev            4.0M   4.0M    0  100% /dev
tmpfs           475M   475M    0  100% /dev/shm
tmpfs           190M   188M    2K   100% /run
/dev/xvda1      8.0G  6.5G  1.5G  19% /
tmpfs           473M   473M    0  100% /tmp
/dev/xvdf      4.9G  4.6G  300M  98% /home/ec2-user/data
[ec2-user@ip-172-31-31-207 data]$ cat file.txt
ndjihifj djihciod ijhiwo dihividjo
[ec2-user@ip-172-31-31-207 data]$
```

- now modify the volume size to 8 gb.

The screenshot shows two consecutive screenshots of the AWS EC2 Management Console. The top screenshot displays the 'Modify volume' dialog for volume `vol-03974555622d6388c`. In the 'Volume details' section, the 'Size (GiB)' field is set to 8, which is highlighted with a red box. The bottom screenshot shows the 'Volumes' list after the modification. The volume `myvolume` is listed with a size of 8 GiB and IOPS of 100, also highlighted with a red box. Both screenshots are taken from a Windows desktop environment.

Name	Volume ID	Type	Size	IOPS
-	<code>vol-0b69b6b6fd0d5a6...</code>	gp3	8 GiB	3000
<code>myvolume</code>	<code>vol-03974555622d63...</code>	gp2	8 GiB	100

- Bi defaultly modifying volume size in aws console not reflected in the linux machine so Extend the size of this volume inside the linux machine. By using resize2fs command.

```

ec2-user@ip-172-31-16-129: ~
/dev/xvda1 8.0G 1.6G 6.5G 20% /
tmpfs 475M 0 475M 0% /tmp
tmpfs 95M 0 95M 0% /run/user/1000
/dev/xvdf 4.9G 24K 4.6G 1% /home/ec2-user/data
[ec2-user@ip-172-31-16-129 ~]$ lsblk
NAME   MAJ MIN SIZE RO MOUNTPOINT
xvda   202 0 8G 0 disk
└─xvda1 202 1 0 8G 0 part /
└─xvda12 259 0 1M 0 part
└─xvda128 259 1 0 10M 0 part
xvdf   202 8 0 8G 0 disk /home/ec2-user/data
[ec2-user@ip-172-31-16-129 ~]$ df -h
Filesystem Size Used Avail Use% Mounted on
devtmpfs 4.0M 0 4.0M 0% /dev
tmpfs 475M 0 475M 0% /dev/shm
tmpfs 190M 2.8M 188M 2% /run
/dev/xvda1 8.0G 1.6G 6.5G 20%
tmpfs 95M 0 95M 0% /run/user/1000
/dev/xvdf 4.9G 24K 4.6G 1% /home/ec2-user/data
[ec2-user@ip-172-31-16-129 ~]$ sudo resize2fs /dev/xvdf data
resize2fs 1.46.5 (30-Dec-2011)
resize2fs: Invalid new size: data

[ec2-user@ip-172-31-16-129 ~]$ df -h
Filesystem Size Used Avail Use% Mounted on
devtmpfs 4.0M 0 4.0M 0% /dev
tmpfs 475M 0 475M 0% /dev/shm
tmpfs 190M 2.8M 188M 2% /run
/dev/xvda1 8.0G 1.6G 6.5G 20%
tmpfs 95M 0 95M 0% /run/user/1000
/dev/xvdf 4.9G 24K 4.6G 1% /home/ec2-user/data
[ec2-user@ip-172-31-16-129 ~]$ sudo resize2fs /dev/xvdf
[ec2-user@ip-172-31-16-129 ~]$ resize2fs 1.46.5 (30-Dec-2011)
Filesystem at /dev/xvdf is mounted on /home/ec2-user/data; on-line resizing required
old_desc_blocks = 1, new_desc_blocks = 1
The filesystem on /dev/xvdf is now 2097152 (4k) blocks long.

[ec2-user@ip-172-31-16-129 ~]$ df -h
Filesystem Size Used Avail Use% Mounted on
devtmpfs 4.0M 0 4.0M 0% /dev
tmpfs 475M 0 475M 0% /dev/shm
tmpfs 190M 2.8M 188M 2% /run
/dev/xvda1 8.0G 1.6G 6.5G 20%
tmpfs 95M 0 95M 0% /run/user/1000
/dev/xvdf 7.8G 24K 7.4G 1% /home/ec2-user/data
[ec2-user@ip-172-31-16-129 ~]$

```

28°C Mostly cloudy

ENG IN 16:10 01-08-2023

- Creating snapshot from the volume

Create snapshot | EC2 Management > Create 5GB EBS Volume.

Create snapshot [Info](#)

Create a point-in-time snapshot to back up the data on an Amazon EBS volume to Amazon S3.

**Details**

Volume ID: [vol-03974555622d638bc](#) (myvolume)

Description: Add a description for your snapshot.  
snap  
255 characters maximum.

Encryption [Info](#): Not encrypted

**Tags** [Info](#)

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

Key	Value - optional
<input type="text" value="Name"/>	<input type="text" value="snap"/> Use "snap"
<a href="#">Add tag</a>	You can add 49 more tags.

[Cancel](#) [Create snapshot](#)

Feedback Language 24°C Heavy storms

ENG IN 21:28 31-07-2023

Now Detach the volume and delete it. you can retrieve this volume by using snapshot.

The screenshot shows the AWS EC2 Management Console with the 'Volumes' section selected. A success message at the top states: "Successfully created snapshot snap-0d57788b16a09ecba from volume vol-03974555622d6388c. If you need your snapshot to be immediately available consider using Fast Snapshot Restore." Below this, a table lists a single volume named 'myvolume' with Volume ID 'vol-03974555622d6388c'. The volume is 8 GiB, Type gp2, IOPS 100, and was created on 2023/07/31 18:14 GMT+5:50. The Actions menu on the right includes options like 'Modify volume', 'Create snapshot', and 'Delete volume'.

Creating volume from the snapshot.

The screenshot shows the AWS EC2 Management Console with the 'Schemas' section selected. A success message at the top states: "Successfully deleted snapshot snap-07e9e203c930f85ab." Below this, a table lists a single snapshot named 'snap' with Snapshot ID 'snap-0d57788b16a09ecba'. The snapshot is 8 GiB, Volume size 8 GiB, and was created by 'CreateImage@0...'. The Actions menu on the right includes options like 'Create volume from snapshot', 'Create image from snapshot', and 'Copy snapshot'.

- Volume created successfully from the snapshot.

The screenshot shows the AWS EC2 Management Console with the URL [ap-southeast-1.console.aws.amazon.com/ec2/home?region=ap-southeast-1#VolumeDetails:volumId=vol-0505a384e4c8198c3](https://ap-southeast-1.console.aws.amazon.com/ec2/home?region=ap-southeast-1#VolumeDetails:volumId=vol-0505a384e4c8198c3). The page displays detailed information about a volume named **vol-0505a384e4c8198c3**. Key details include:

- Volume ID:** vol-0505a384e4c8198c3
- Size:** 8 GiB
- Type:** gp2
- AWS Compute Optimizer finding:** Opt-in to AWS Compute Optimizer for recommendations. [Learn more]
- Volume state:** Available
- IOPS:** 100
- Encryption:** Not encrypted
- KMS key ID:**
- KMS key alias:**
- Fast snapshot restored:** No
- Snapshot:** snap-0d57788b16a09ecba
- Availability Zone:** ap-southeast-1a
- Multi-Attach enabled:** No
- Attached Instances:** -
- Outposts ARN:**
- Volume status:** Okay
- Throughput:** -
- KMS key ARN:**
- Created:** Mon Jul 31 2023 21:37:08 GMT+0530 (India Standard Time)

The interface includes tabs for Status checks, Monitoring, and Tags. The bottom right corner shows the date and time as 31-07-2023 21:36.

## LAB7

### Amazon machine image(AMI's)

- Creating AMI of running instance
- Goto instance → actions → image from templates → create image.

The screenshot shows the AWS EC2 Management Console with the URL [ap-southeast-1.console.aws.amazon.com/ec2/home?region=ap-southeast-1#Instancesvisibility=owned-by-me](https://ap-southeast-1.console.aws.amazon.com/ec2/home?region=ap-southeast-1#Instancesvisibility=owned-by-me). The page displays a list of instances under the **Instances** section. One instance, **bbbb** (Instance ID: i-007d4116d5f9ce997), is selected. The Actions menu is open, showing options like Connect, View details, Manage instance state, Instance settings, Networking, Security, Image and templates, and Monitor and troubleshoot. The **Image and templates** option is highlighted. A tooltip for this option shows the sub-options: Create image, Create template from instance, and Launch more like this.

The bottom right corner shows the date and time as 31-07-2023 22:04.

Created image successfully.

The screenshot shows the AWS EC2 Management Console interface. On the left, there's a navigation sidebar with options like Instances, Images, and Elastic Block Store. The main area displays the 'Amazon Machine Images (AMIs) (1/1) Info' page. It lists a single AMI entry:

- Name:** ami-0d8cbc09cf5fe9e2b
- AMI name:** myimage
- Source:** 424921938911/myimage
- Owner:** 424921938911
- Visibility:** Private
- Status:** Pending

Below this, the 'AMI ID: ami-0d8cbc09cf5fe9e2b' details page is open, showing more specific information such as Platform details (Linux/UNIX), Root device type (EBS), and various status metrics.

## LAB-8

### Load balancers

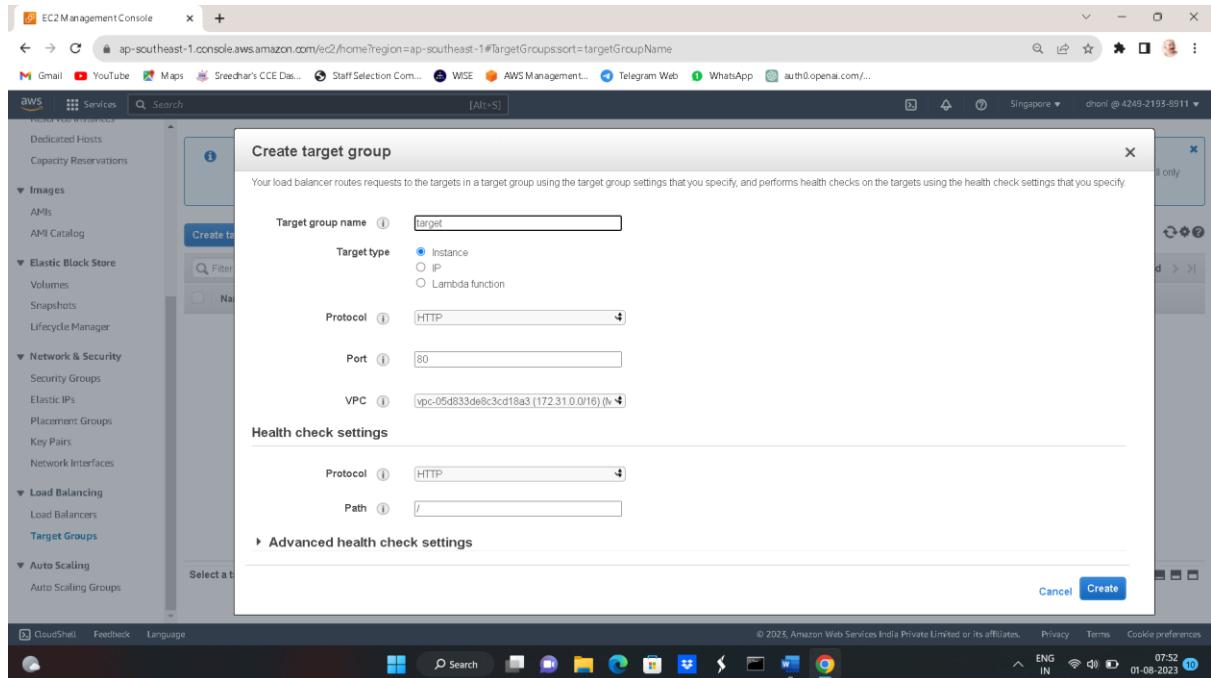
- For the creation of load balancer we need two or more instances.
- In the 1<sup>st</sup> instance install nginx and in the 2<sup>nd</sup> instance we have to install apache .

The screenshot shows the AWS EC2 Management Console interface. The left sidebar includes options for Instances, Images, and Elastic Block Store. The main area displays the 'Instances (2/4) Info' page, listing the following instances:

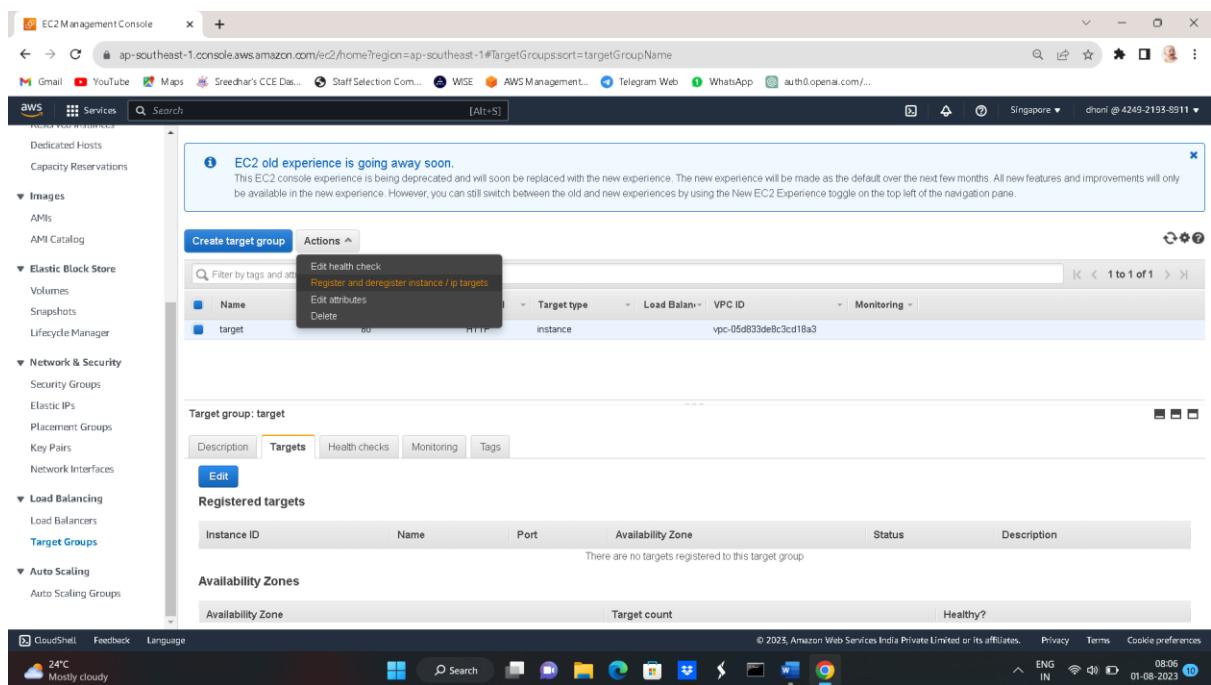
Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone	Public IPv4 DNS	Public IPv4
bbbд	i-007d4116d59ce997	Running	t2.micro	2/2 checks passed	No alarms	ap-southeast-1b	ec2-18-142-186-66.ap-s...	18.142.186.66
httpd	i-0f76dcf4dabf84e5b	Terminated	t2.micro	-	No alarms	ap-southeast-1b	-	13.229.201.3
<b>nginx</b>	i-0b1d9700a37f27ff7	Running	t2.micro	2/2 checks passed	No alarms	ap-southeast-1b	ec2-54-255-0-113.ap-so...	54.255.0.113
<b>apache</b>	i-06a306e2e68014bac	Running	t2.micro	2/2 checks passed	No alarms	ap-southeast-1b	ec2-13-229-65-204.ap-s...	13.229.65.204

Below the instance list, a monitoring dashboard is shown for the selected instances (nginx and apache). It displays four graphs: CPU utilization (%), Status check failed (any) (count), Status check failed (instance) (count), and Status check failed (system) (count). The CPU utilization graph shows a sharp drop at approximately 18:15.

- Before going to create the load balancer you need to create the target group first .



- After creating target group you have to register the targets so go to actions click on register instances.



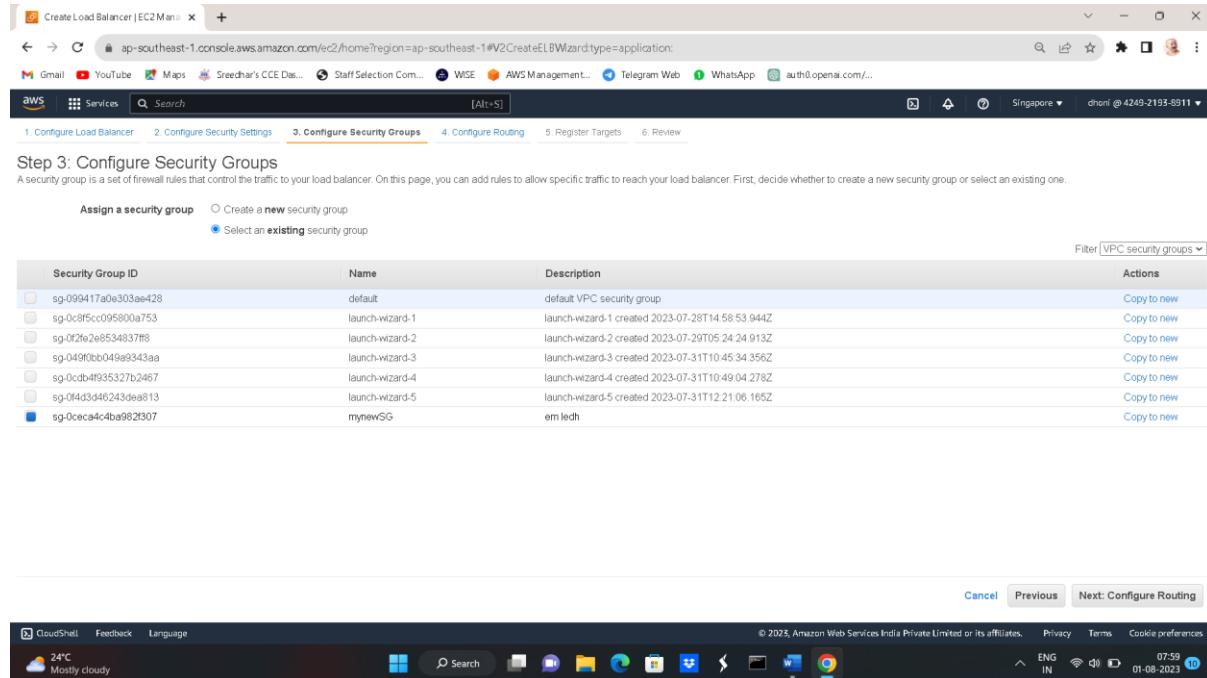
- Select your instances and click on add to register and then save it.

The screenshot shows the AWS EC2 Management Console with the 'Register and deregister targets' dialog open. The 'Registered targets' section lists two instances: 'nginx' and 'apache2', both running on port 80. The 'Instances' section shows two more instances: 'nginx' and 'apache2', both running on port 80. A search bar is present above the instance list. The AWS navigation menu on the left includes options like Images, Elastic Block Store, Network & Security, Load Balancing, and Auto Scaling.

- Create load balancer
- While creating load balancer You need to give name and you must specify two availability zones.

The screenshot shows the 'Step 1: Configure Load Balancer Listeners' dialog. It is configured for an 'HTTP' protocol on port 80. Under 'Availability Zones', three zones are selected: 'ap-southeast-1a', 'ap-southeast-1b', and 'ap-southeast-1c'. The 'Next: Configure Security Settings' button is visible at the bottom right.

 In the next step select existing security group or create new security group.



Step 3: Configure Security Groups

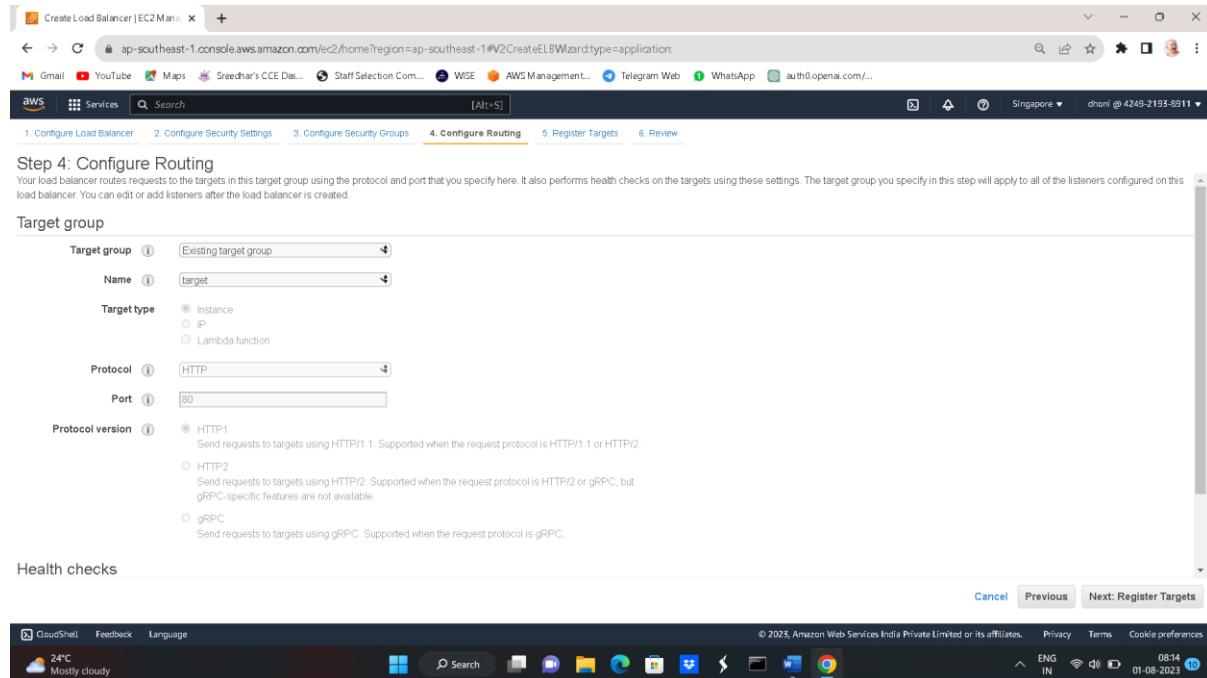
A security group is a set of firewall rules that control the traffic to your load balancer. On this page, you can add rules to allow specific traffic to reach your load balancer. First, decide whether to create a new security group or select an existing one.

Assign a security group:

- Create a new security group
- Select an existing security group

Security Group ID	Name	Description	Actions
sg-099417a0a303ae428	default	default VPC security group	<a href="#">Copy to new</a>
sg-08f5c095800a753	launch-wizard-1	launch-wizard-1 created 2023-07-28T14:58:53.944Z	<a href="#">Copy to new</a>
sg-0f2e2e8534937f8	launch-wizard-2	launch-wizard-2 created 2023-07-29T05:24:34.913Z	<a href="#">Copy to new</a>
sg-049fb0b049a9343aa	launch-wizard-3	launch-wizard-3 created 2023-07-31T10:45:34.356Z	<a href="#">Copy to new</a>
sg-0cd493327b2467	launch-wizard-4	launch-wizard-4 created 2023-07-31T10:49:04.276Z	<a href="#">Copy to new</a>
sg-0fd3d46243dea813	launch-wizard-5	launch-wizard-5 created 2023-07-31T12:21:06.165Z	<a href="#">Copy to new</a>
sg-0ceca4c4ba982307	mynewSG	em ledh	<a href="#">Copy to new</a>

 in the configure routing you need to select an existing target group.



Step 4: Configure Routing

Your load balancer routes requests to the targets in this target group using the protocol and port that you specify here. It also performs health checks on the targets using these settings. The target group you specify in this step will apply to all of the listeners configured on this load balancer. You can edit or add listeners after the load balancer is created.

**Target group**

Target group: Existing target group

Name: target

Target type:

- Instance
- IP
- Lambda function

Protocol: HTTP

Port: 80

Protocol version:

- HTTP1.1 Send requests to targets using HTTP/1.1. Supported when the request protocol is HTTP/1.1 or HTTP/2.
- HTTP2 Send requests to targets using HTTP/2. Supported when the request protocol is HTTP/2 or gRPC, but gRPC-specific features are not available.
- gRPC Send requests to targets using gRPC. Supported when the request protocol is gRPC.

**Health checks**

- In nextstep select your registered targets and review it and then create load balancer.

**Create Load Balancer**

Name	DNS name	State	VPC ID	Availability Zones	Type	Created At
mylb	mylb-1350098300.ap-southeast-1.elb.amazonaws.com	Active	vpc-05d833de8c3cd1ba3	ap-southeast-1a, ap-southeast-1b	application	August 1, 2023 at 8:16:55 A...

- Copy the DNS end point address and browse it.

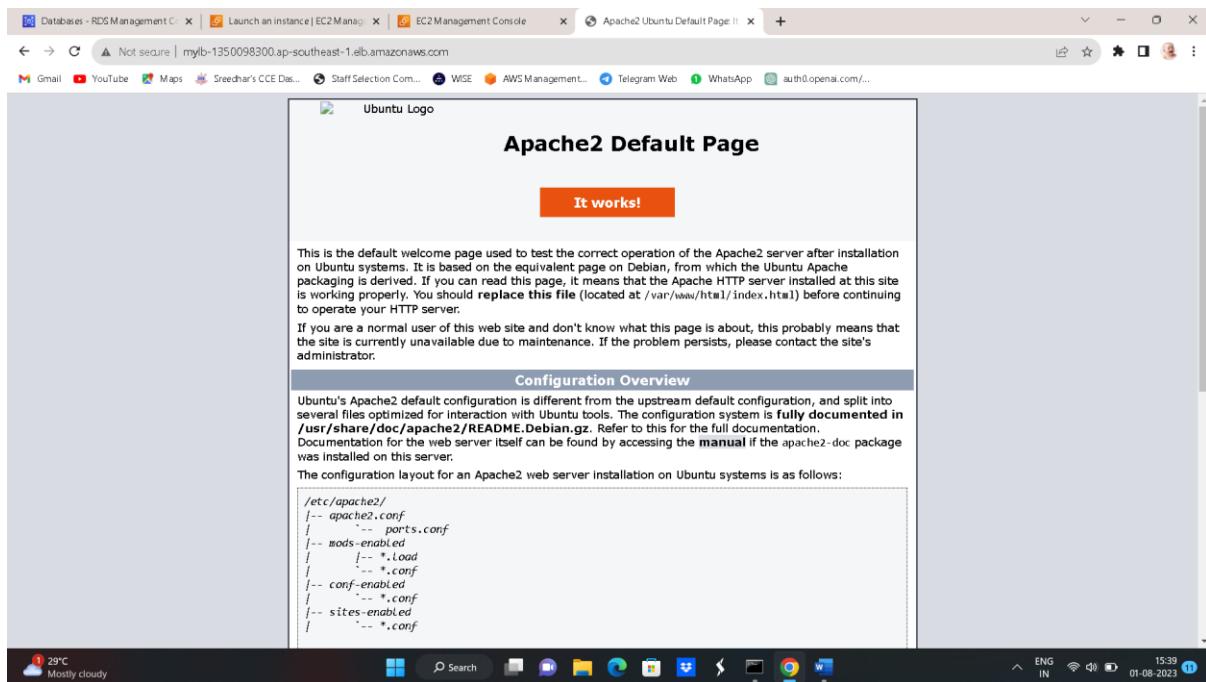
Welcome to nginx!

If you see this page, the nginx web server is successfully installed and working. Further configuration is required.

For online documentation and support please refer to [nginx.org](http://nginx.org). Commercial support is available at [nginx.com](http://nginx.com).

Thank you for using nginx.

- Click on refresh it will change another server.



## Lab-9

### Auto scaling group

Create one ubuntu instance

Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone	Public IPv4 DNS	Public IPv4
ubuntu	i-0f97f3558d87bcc8	Running	t2.micro	Initializing	No alarms	ap-southeast-1b	ec2-3-0-61-70.ap-south...	3.0.61.70

- Go to Auto Scaling group, give name and click on Create a launch configuration.

The screenshot shows the 'Create Auto Scaling group' wizard on the AWS Management Console. The current step is 'Step 1: Choose launch template or configuration'. On the left, there's a sidebar with steps 1-7. Step 1 is expanded, showing 'Auto Scaling group name' with the value 'myasg'. A note below says: 'Must be unique to this account in the current Region and no more than 255 characters.' Step 2 shows 'Choose instance launch options', Step 3 shows 'Configure advanced options', Step 4 shows 'Configure group size and scaling policies', Step 5 shows 'Add notifications', Step 6 shows 'Add tags', and Step 7 shows 'Review'. At the bottom right of the main form, there's a button labeled 'Switch to launch template'.

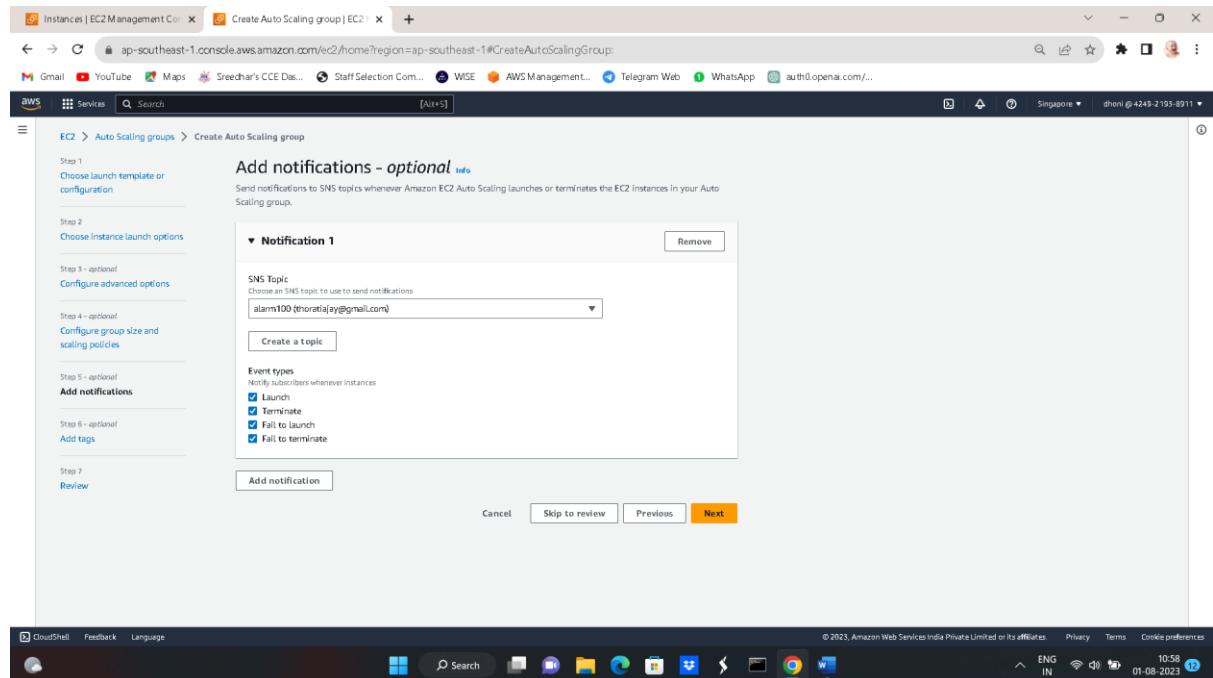
- Choose AMI ID and instance type, security group, keypair and create launch configuration.

The screenshot shows the 'EC2 Management Console' interface. The top navigation bar includes links for Instances, EC2 Management Console, and EC2 Home. The main content area displays a message about migrating launch configurations to launch templates, followed by a success message: 'Successfully created launch configuration: mylaunch'. Below this, the 'Launch configurations (1)' section is shown, listing the newly created configuration. The table has columns for Name, AMI ID, Instance type, Spot price, and Creation time. The single entry is 'mylaunch' with AMI ID 'ami-0df7a207adb...', Instance type 't2.micro', and Creation time 'Tue Aug 01 2023 10:54:32 GMT+0530 (India Standard Time)'. At the bottom, there's a note: 'Select a launch configuration above'.

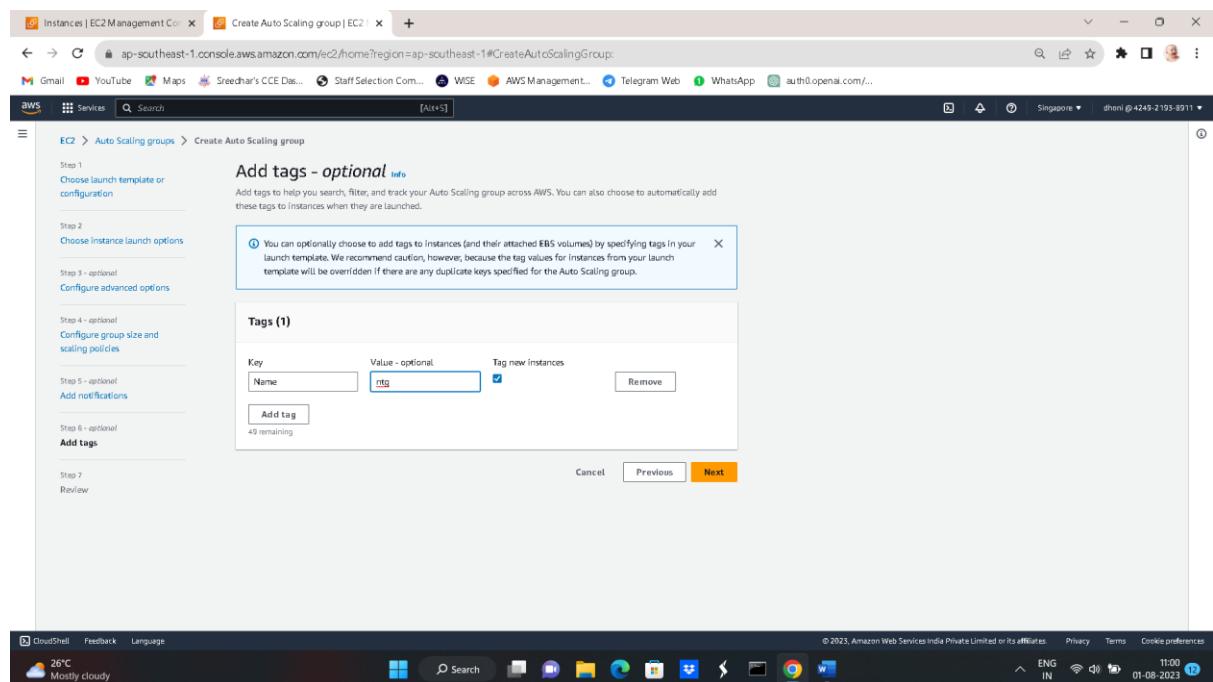
Choose instance launch options.

Select the minimum capacity=1,max capacity=3.

- >Add notifications by selecting SNS topic.



- Add name tag for ASG.



Now goto review and click on create auto scaling group.

The screenshot shows the AWS CloudShell interface. The terminal window displays the command:

```
aws autoscaling create-auto-scaling-group
```

Below the terminal, the AWS Management Console shows the 'Create Auto Scaling group' wizard. Step 5: Add notifications shows a notification configuration for an SNS Topic named 'alarm100'. Step 6: Add tags shows a tag named 'ntg' with the value 'Yes'. At the bottom right of the CloudShell interface, there is a 'Create Auto Scaling group' button.

Now iam going to terminate the instances .the ASG will create new instances.

The screenshot shows the AWS CloudShell interface. The terminal window displays the command:

```
aws ec2 terminate-instances
```

Below the terminal, the AWS Management Console shows the 'Instances' page. It lists several EC2 instances, including 'ntg' (Running), 'bbb' (Stopped), 'nginx' (Stopped), 'apache' (Stopped), and 'ubuntu' (Running). The 'Actions' dropdown for the 'ubuntu' instance includes the option 'Terminate instance'. The monitoring section shows various metrics for these instances.

- The instances are created again successfully by using autoscaling group.

The screenshot shows the AWS EC2 Instances page. A list of instances is displayed, with one instance named 'ntg' selected. The instance details show it is running, has a Public IPv4 address of 15.212.257.73, a Private IPv4 address of 172.31.13.125, and a Public DNS name of ec2-15-212-257-73.ap-southeast-1.compute.amazonaws.com. The interface includes a sidebar with various AWS services like CloudWatch Metrics, Lambda, and CloudWatch Logs.

## LAB-10

### RDS

- Goto Rds and create database.

The screenshot shows the AWS RDS Create database page. It displays the 'Create database' section with two creation methods: 'Standard create' (selected) and 'Easy create'. Under 'Engine options', 'PostgreSQL' is selected. Other engine options shown include Aurora (MySQL Compatible), Aurora (PostgreSQL Compatible), MySQL, MariaDB, and Oracle. The interface includes a sidebar with CloudWatch Metrics, Lambda, and CloudWatch Logs.

Give instance name and Create password for the database.

The screenshot shows the 'Create database - MySQL' configuration page. In the 'DB instance identifier' field, 'database-2' is entered. Under 'Master username', 'admin' is specified. A note indicates that master user credentials can be managed in AWS Secrets Manager. There are options to auto-generate or manually enter a master password ('\*\*\*\*\*'). A note states that if master user credentials are managed in Secrets Manager, some RDS features won't be supported. The right panel provides information about MySQL, mentioning its popularity and various features like support for up to 64 TiB, General Purpose, Memory Optimized, and Burstable Performance Instance classes, automated backup, point-in-time recovery, and up to 15 Read Replicas per instance.

Give the instance configuration based on your requirement.

This screenshot is identical to the one above, showing the 'Create database - MySQL' configuration page. It displays the same input fields for 'DB instance identifier' ('database-2'), 'Master username' ('admin'), and password options. The note about Secrets Manager and the MySQL feature summary on the right panel are also present.

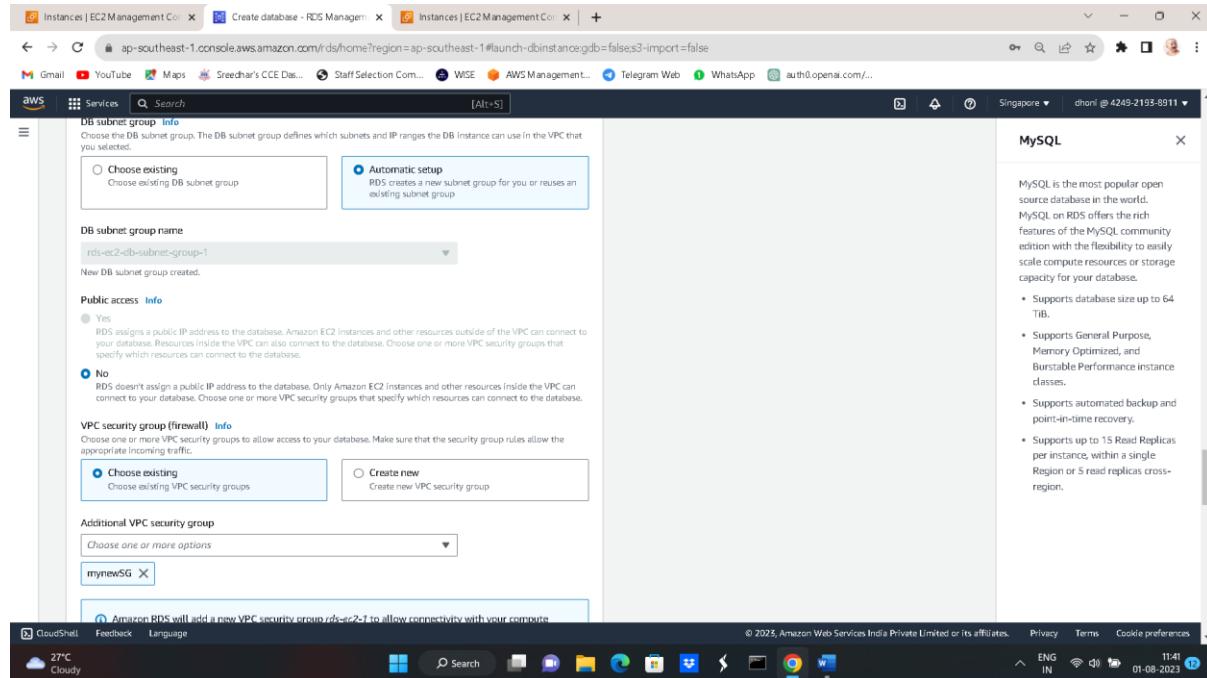
## Set your storage limit

The screenshot shows the AWS RDS MySQL storage configuration page. On the left, there are sections for Storage type (General Purpose SSD gp2), Allocated storage (10 GiB), and Maximum storage threshold (22 GiB). A note states: "After you modify the storage for a DB instance, the status of the DB instance will be in storage-optimization. Your instance will remain available as the storage-optimization operation completes." On the right, a sidebar titled "MySQL" provides information about MySQL's popularity and features, including support for database sizes up to 64 TiB, various instance classes, automated backups, and up to 15 read replicas per instance.

## Set up your ec2 machine

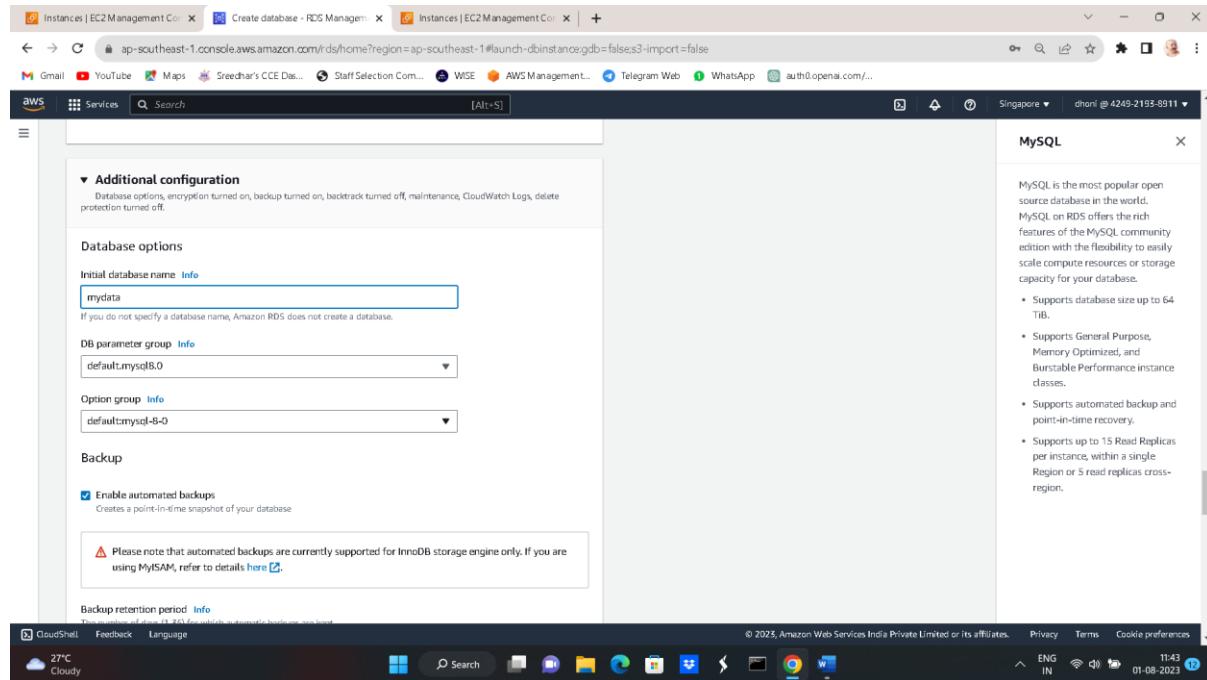
The screenshot shows the AWS RDS MySQL connectivity setup page. It includes sections for Compute resource (choosing to connect to an EC2 compute resource), EC2 instance (selecting an EC2 instance), VPC settings (noting that some cannot be changed), Network type (choosing IPv4 or Dual-stack mode), and Virtual private cloud (choosing a VPC). A note in the VPC section explains that an EC2 compute resource automatically selects the VPC, DB subnet group, and public access settings. On the right, a sidebar titled "MySQL" reiterates MySQL's features and cross-region replication capabilities.

 Assign security group.

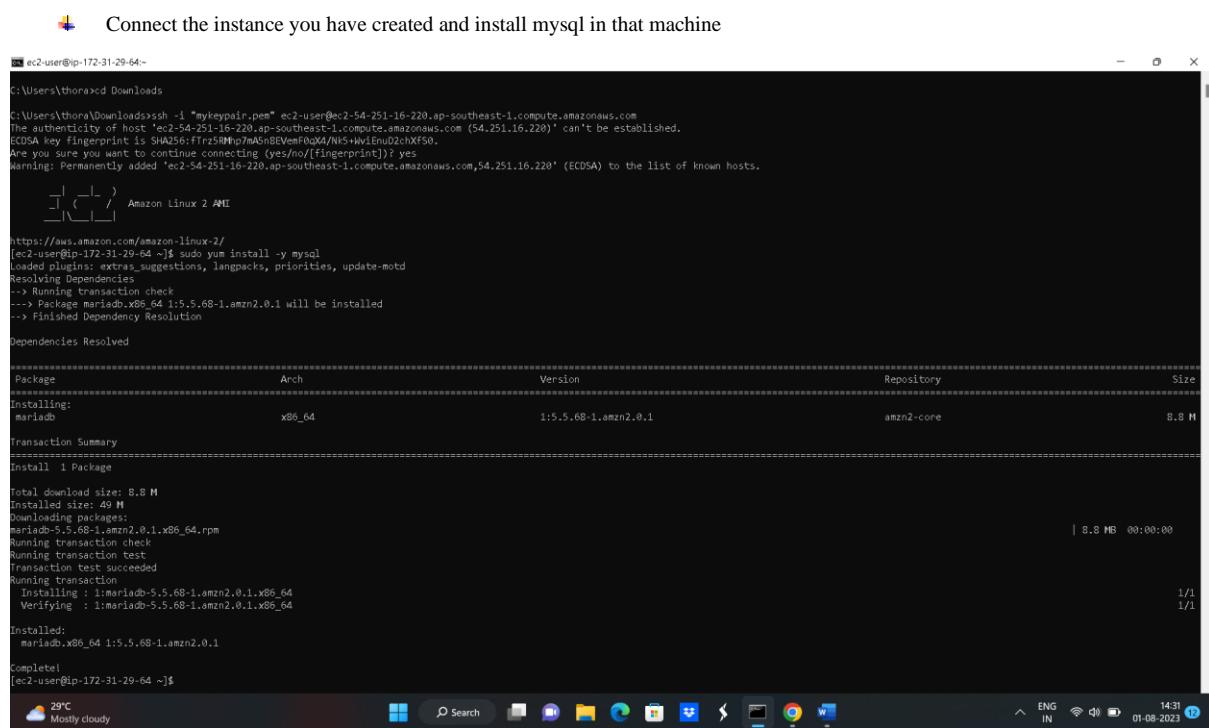
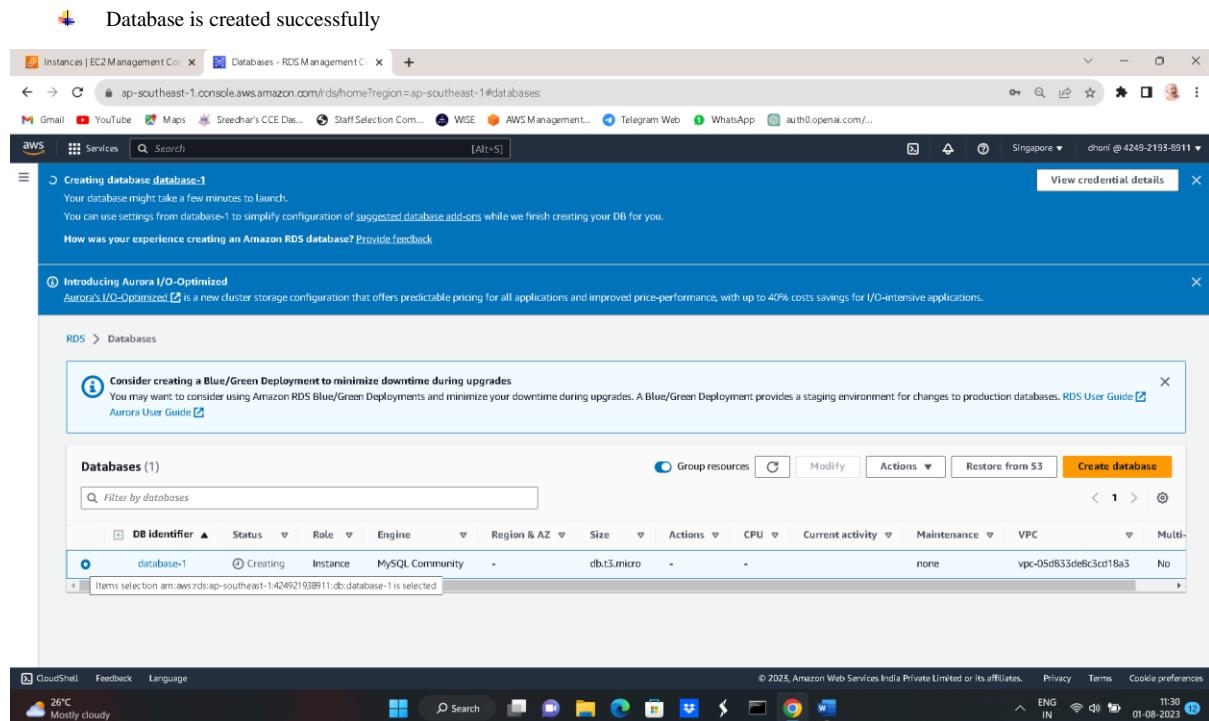


The screenshot shows the AWS RDS MySQL setup page. Under 'DB subnet group', 'Automatic setup' is selected, creating a new subnet group. A new DB subnet group has been created. Under 'VPC security group (firewall)', 'Choose existing' is selected, and 'mynewSG' is chosen. A note indicates that Amazon RDS will add a new VPC security group. The right sidebar provides information about MySQL, including its popularity and features like automated backup and up to 15 read replicas.

 In additional configurations you have to give the name for database.



The screenshot shows the 'Additional configuration' section of the AWS RDS MySQL setup page. It includes fields for 'Initial database name' (set to 'mydata'), 'DB parameter group' (set to 'default.mysql8.0'), 'Option group' (set to 'defaultmysql8-0'), and 'Backup' (with 'Enable automated backups' checked). A note states that automated backups are currently supported for InnoDB storage engine only. The right sidebar continues to provide MySQL information.



- Connect the mysql database by using the below command
  - mysql -h database-1.c8yeqqdlhyxj.ap-southeast-1.rds.amazonaws.com -u admin -P 3306 -p
- in the next step you have to provide password.

```

[ec2-user@ip-172-31-29-64: ~] Transaction test succeeded
[ec2-user@ip-172-31-29-64: ~] Running transaction
[ec2-user@ip-172-31-29-64: ~] Installing : mariadb-5.5.60-1.amzn2.0.1.x86_64
[ec2-user@ip-172-31-29-64: ~] Verifying : mariadb-5.5.60-1.amzn2.0.1.x86_64
[ec2-user@ip-172-31-29-64: ~] Installed:
[ec2-user@ip-172-31-29-64: ~] mariadb.x86_64 1:5.5.60-1.amzn2.0.1
[ec2-user@ip-172-31-29-64: ~] Complete!
[ec2-user@ip-172-31-29-64: ~]$ mysql -h database-1.c8yeqqdlhyxj.ap-southeast-1.rds.amazonaws.com -u admin -P 3306 -p
ERROR 1049 (42000): Unknown database "3306"
[ec2-user@ip-172-31-29-64: ~]$ mysql -h database-1.c8yeqqdlhyxj.ap-southeast-1.rds.amazonaws.com -u admin -P 3306 -p
Enter password:
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MySQL connection id is 47
Server version: 8.0.33 Source distribution

Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

MySQL [(none)]> show databases;
+-----+
| Database |
+-----+
| information_schema |
| mysql |
| performance_schema |
| sys |
+-----+
5 rows in set (0.01 sec)

MySQL [(none)]> 
```