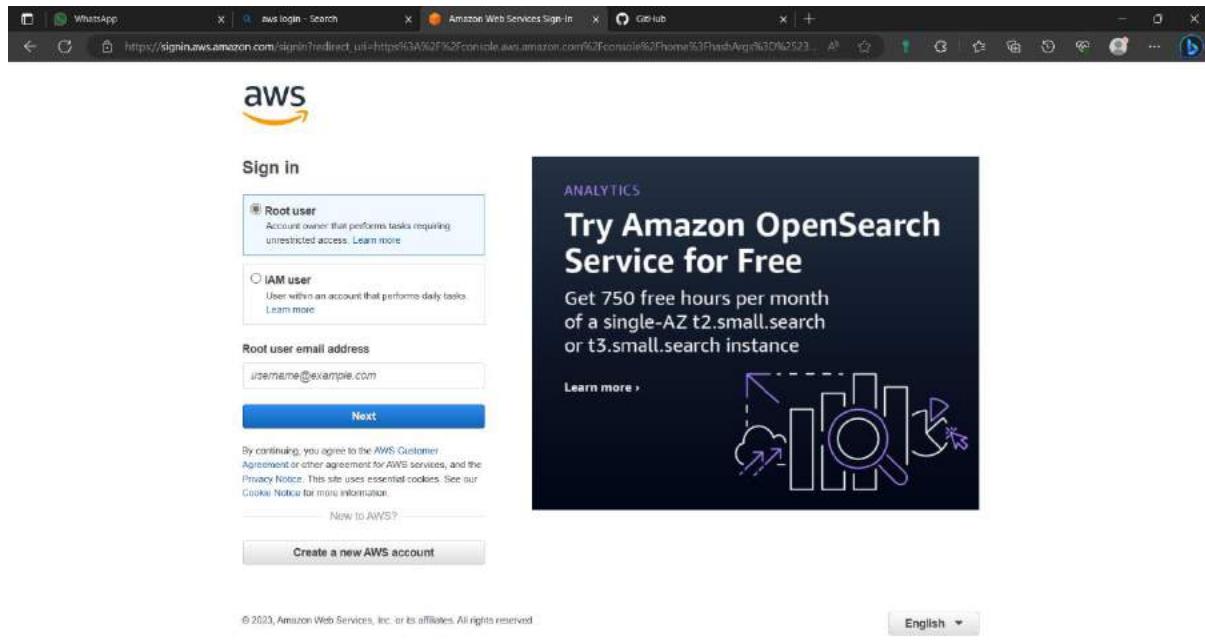


MINI PROJECT ON AWS(AMAZON WEB SERVICES)

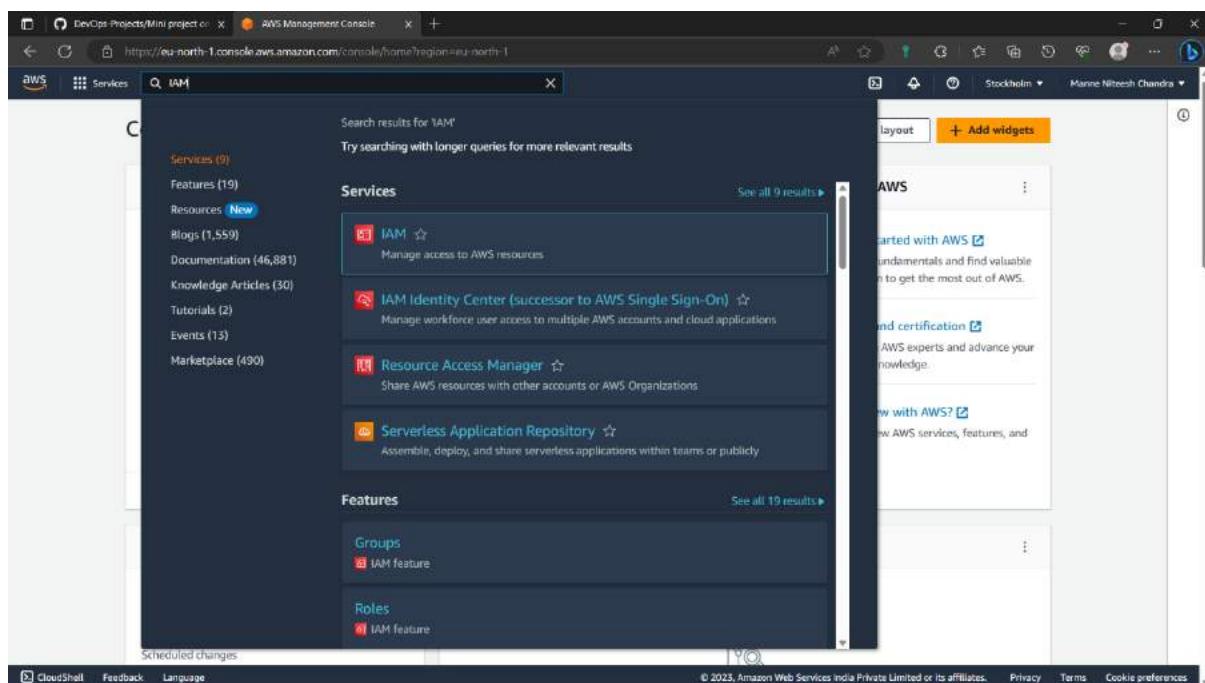
IAM Hands-On:

Github link:<https://github.com/NiteeshManne?tab=repositories>

1)Login to the AWS console as a root user.



2)Type IAM in search bar and select the IAM option.



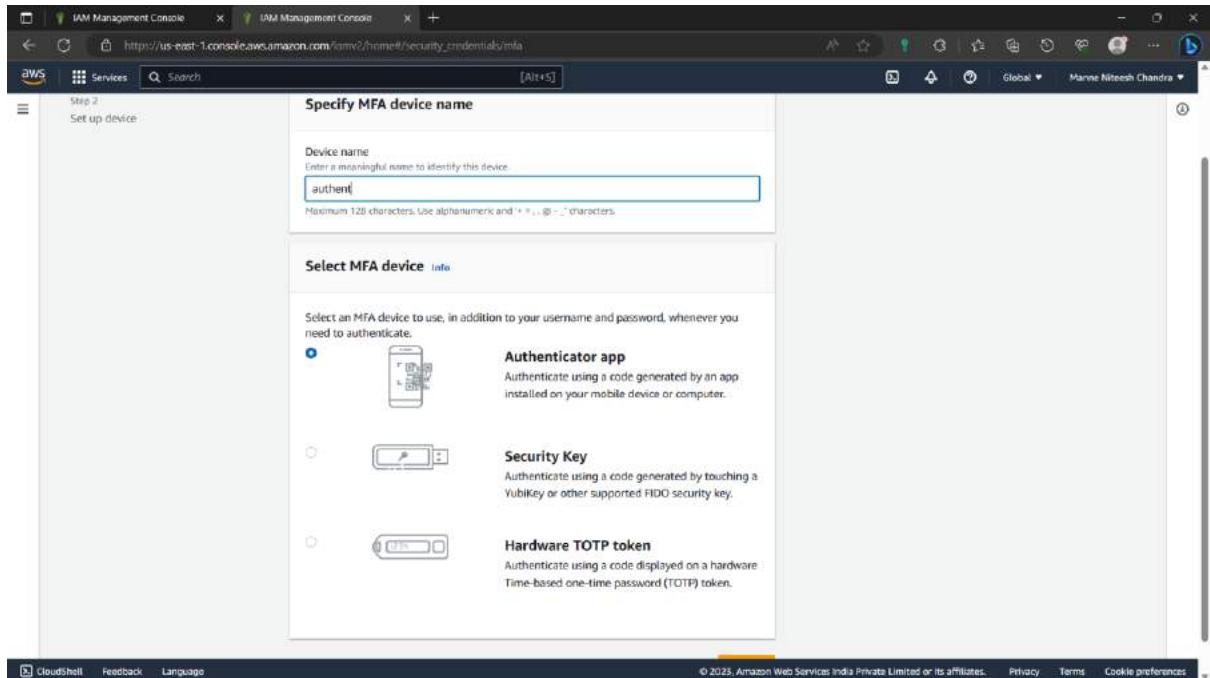
3) Click on add MFA

The screenshot shows the AWS IAM Management Console. The left sidebar includes sections for Dashboard, Access management, and Access reports. The main area is the IAM dashboard, which features a 'Security recommendations' section with a red warning icon for 'Add MFA for root user'. Below this is an 'IAM resources' summary with counts for User groups, Users, Roles, Policies, and Identity providers. A 'What's new' section lists recent updates. To the right, there's an 'AWS Account' sidebar with account details such as Account ID (851943206657) and a prominent 'Add MFA' button.

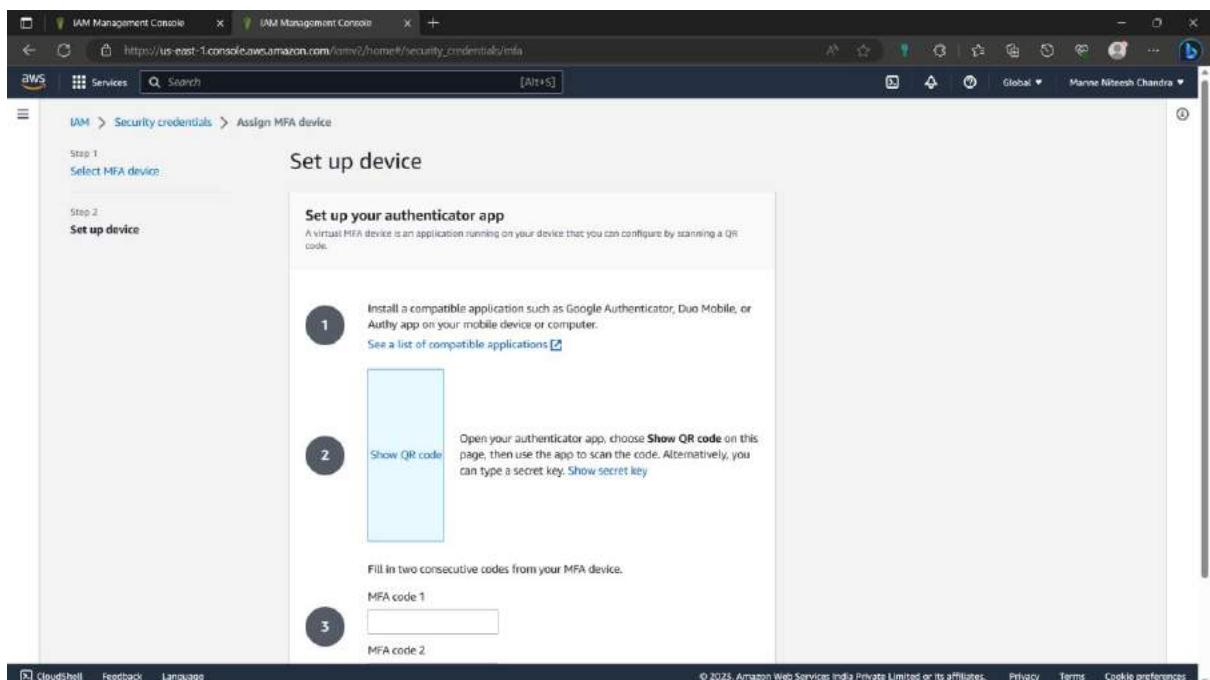
4) It will open My security credentials in a new tab, Click on "Assign MFA" option.

The screenshot shows the 'My security credentials (root user)' page in the AWS IAM Management Console. The left sidebar is identical to the previous screenshot. The main content area shows account details for the root user, including the account name (Manne Niteesh Chandra), AWS account ID (851943206657), email address (19pa1a04a1@gvishnu.edu.in), and canonical user ID (386d157135e6adc17866ccdb2bad67692493bc1e86d6c022eff95462a383d7). Below this is a 'Multi-factor authentication (MFA)' section with a note about best practices and an 'Assign MFA device' button.

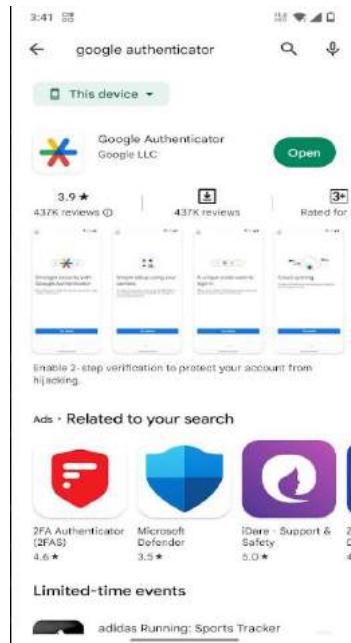
5) Now specify MFA details-Give a name, and select MFA device – authenticator app(if you want to choose mobile for authentication) and click on next.



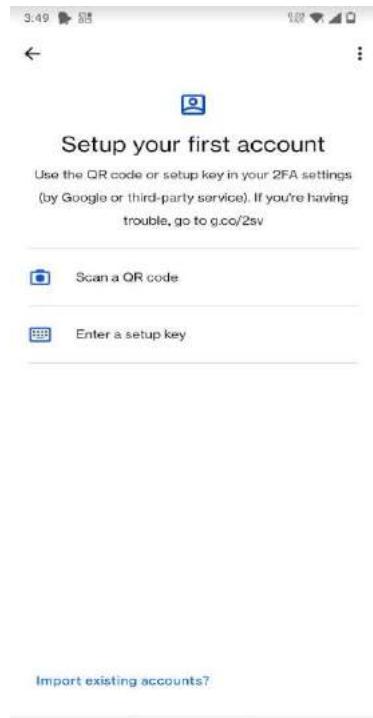
6) Next setup up your device by following the steps given below.



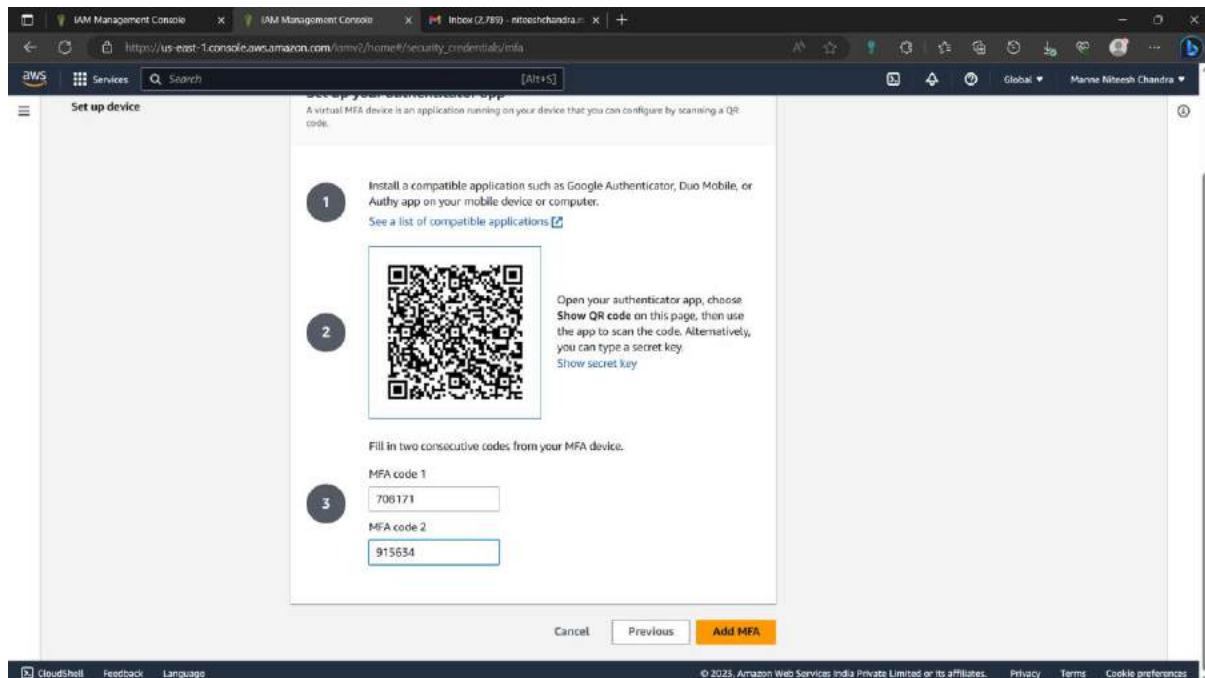
7)Now install Google Authenticator from play store to your device.



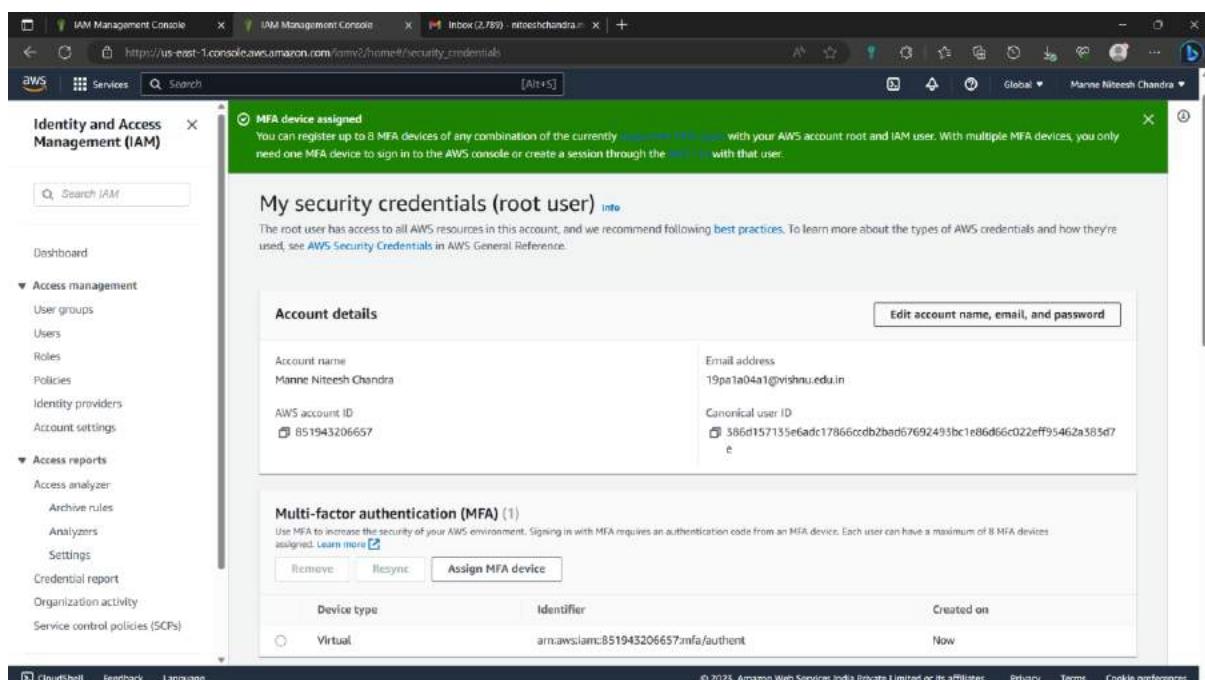
8)After logging in click on “Scan a QR code” scan the QR code which will showed at (point-2) by clicking “show QR code”.



9) After scanning the QR codes you will get OTP in 6 digits, type that OTP in MFA code 1 after a few seconds you will get to another OTP type it in MFA code 2, click on “Add MFA”.



10) Now the MFA is created.



11)Now log out of your AWS console.

MFA device assigned

You can register up to 8 MFA devices of any combination of the currently supported methods with your AWS account root and IAM user. You need one MFA device to sign in to the AWS console or create a session through the AWS CLI with that user.

My security credentials (root user)

The root user has access to all AWS resources in this account, and we recommend following best practices. To learn more about the types of users, see [AWS Security Credentials in AWS General Reference](#).

Account details

Account name: Manne Niteesh Chandra

AWS account ID: 851943206657

Email address: 19pa1a04a1@vishnu.edu.in

Canonical user ID: 386d157135e6adc17866c6db2bad67692493bc1e06d66c022eff95462a383d7

Sign-out

12)Now Login again. This time it will ask for MFA code, type the six digit code that will appear in google authenticator to login to your console.

aws

Multi-factor authentication

Your account is secured using multi-factor authentication (MFA). To finish signing in, turn on or view your MFA device and type the authentication code below.

Email address: 19pa1a04a1@vishnu.edu.in

MFA code:

Submit

Troubleshoot MFA

Cancel

ANALYTICS

Try Amazon OpenSearch Service for Free

Get 750 free hours per month of a single-AZ t2.small.search or t3.small.search instance

Learn more

English

https://aws.amazon.com/products/security/resource/tic/campaign-awacs_200_console_signin_security_content_hub_2023_q2_june_wizy2Macx_icchannel=heBoc_iccontent=awsum-2071_awacs_iplace=igw_rndlink=789132ee-0405-4979-ab25-7da117bf0f3-hx_awsum-2071...

13) Go to IAM in AWS console.

The screenshot shows the AWS Management Console search results for 'IAM'. The search bar at the top contains the query 'IAM'. Below the search bar, there are two main sections: 'Services' and 'Features'.

Services (9 results):

- IAM** (Manage access to AWS resources)
- IAM Identity Center (successor to AWS Single Sign-On)** (Manage workforce user access to multiple AWS accounts and cloud applications)
- Resource Access Manager** (Share AWS resources with other accounts or AWS Organizations)
- Serverless Application Repository** (Assemble, deploy, and share serverless applications within teams or publicly)

Features (19 results):

- Groups** (IAM feature)
- Roles** (IAM feature)

On the right side of the search results, there is a sidebar titled 'AWS' with several links:

- Started with AWS
- Find certification
- Learn with AWS?

At the bottom of the page, there are links for CloudShell, Feedback, Language, and a copyright notice: © 2023, Amazon Web Services India Private Limited or its affiliates.

14) Click on users.

The screenshot shows the IAM dashboard. On the left, there is a navigation menu with the following sections:

- Identity and Access Management (IAM)
- Dashboard
- Access management
 - User groups
 - Users
 - Roles
 - Policies
 - Identity providers
 - Account settings
- Access reports
 - Access analyzer
 - Archive rules
 - Analyzers
 - Settings
- Credential report
- Organization activity
- Service control policies (SCPs)

The main content area displays the following information:

- IAM dashboard**
- Security recommendations**:
 - Root user has MFA
 - Root user has no active access keys
- IAM resources**:

User groups	Users	Roles	Policies	Identity providers
0	0	2	0	0
- What's new**:
 - Advanced Notice: Amazon S3 will automatically enable S3 Block Public Access and disable access control lists for all new buckets starting in April 2023. (6 months ago)
 - AWS IAM Identity Center now supports session management capabilities for AWS Command Line Interface (AWS CLI) and SDKs. (7 months ago)
 - AWS Lambda announces support for Attribute-Based Access Control (ABAC) in AWS GovCloud (US) Regions. (7 months ago)
 - Amazon ElastiCache simplifies password rotations with Secrets Manager. (7 months ago)
- AWS Account**:
 - Account ID: 851943206657
 - Account Alias: 851943206657 - Create
 - Sign-in URL for IAM users in this account: https://851943206657.signin.amazonaws.com/console
- Quick Links**:
 - My security credentials
 - Manage your access keys, multi-factor authentication (MFA) and other credentials.
- Tools**:
 - Policy simulator
 - Web identity federation playground
 - Authenticate yourself to any of the

At the bottom of the page, there is a footer with links for https://eu-north-1.console.aws.amazon.com/iamv2/home?region=eu-north-1#users, © 2023, Amazon Web Services India Private Limited or its affiliates., Privacy, Terms, and Cookie preferences.

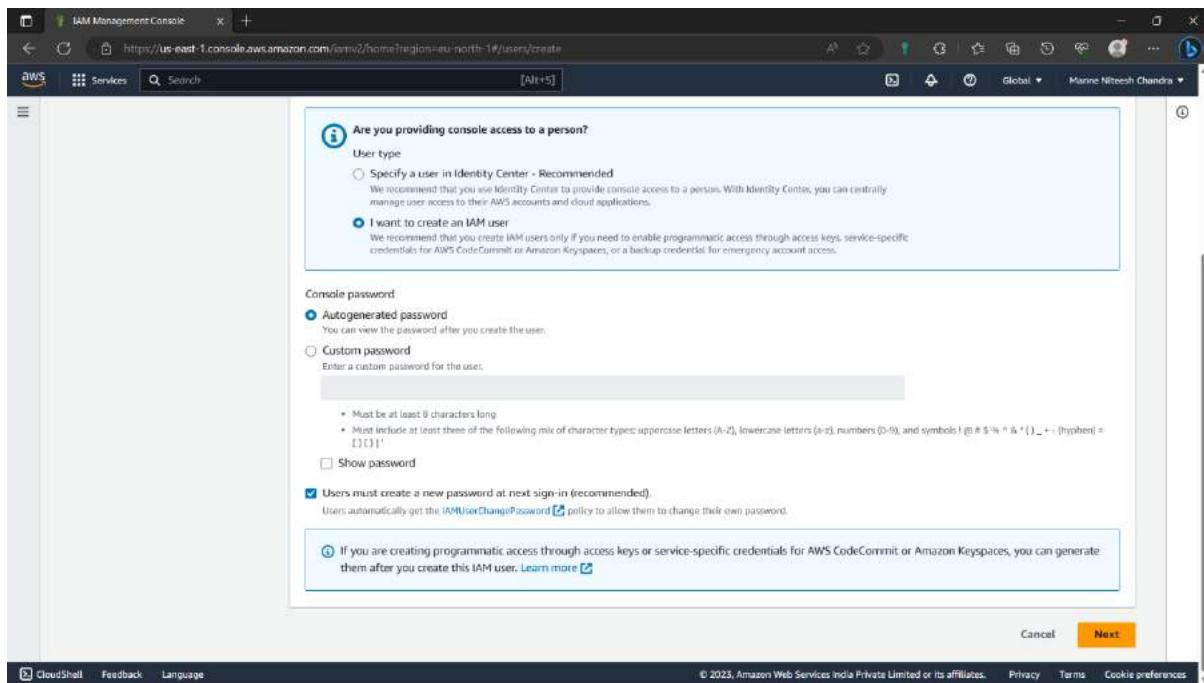
15)Click on Add user.

Screenshot of the AWS IAM Management Console - Users page. The sidebar shows 'Access management' with 'Users' selected. The main area displays a table with no resources found. A search bar at the top allows finding users by username or access key. A blue 'Add users' button is located in the top right corner.

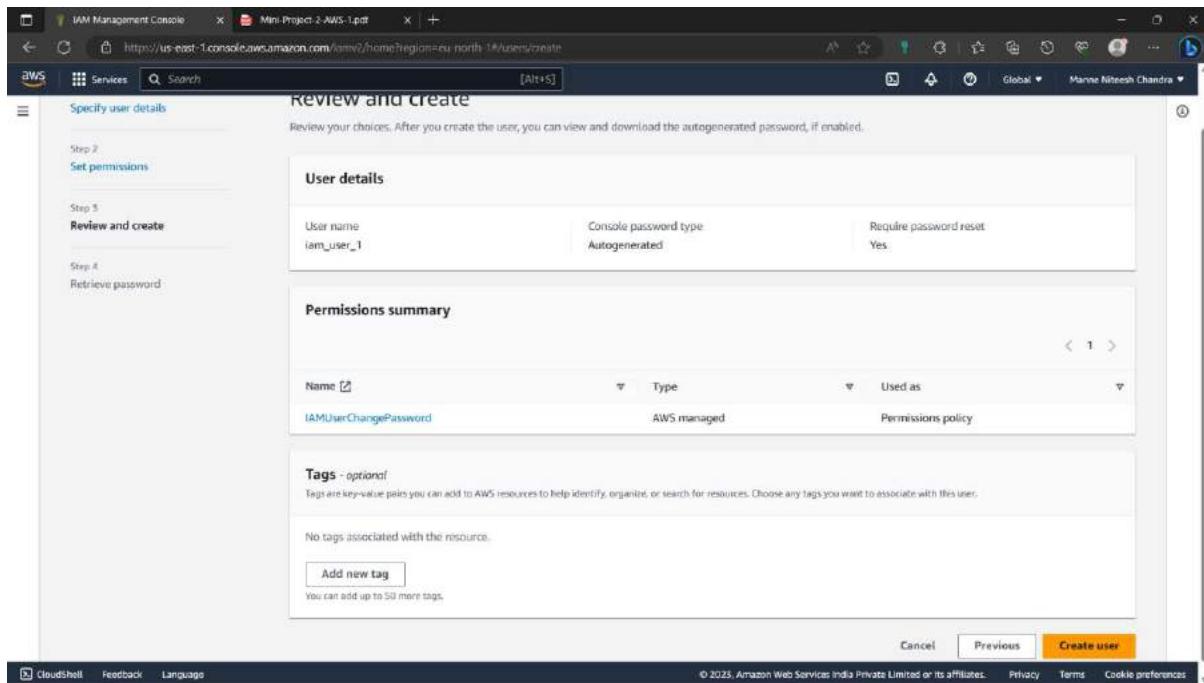
16)Give the name of your choice, enable user access, enable I want to create an IAM user, enable Autogenerated password.

Screenshot of the AWS IAM Management Console - Create user wizard, Step 1: Specify user details. The 'User name' field is set to 'iam_user_1'. The 'Provide user access to the AWS Management Console - optional' checkbox is checked. The 'I want to create an IAM user' radio button is selected. The 'Console password' section shows 'Auto-generated password' is selected. The bottom of the screen shows the AWS footer with links like CloudShell, Feedback, Language, Privacy, Terms, and Cookie preferences.

17)Enable “User must create for the next sign-in” and click on next.



18)Review all the details and click next.



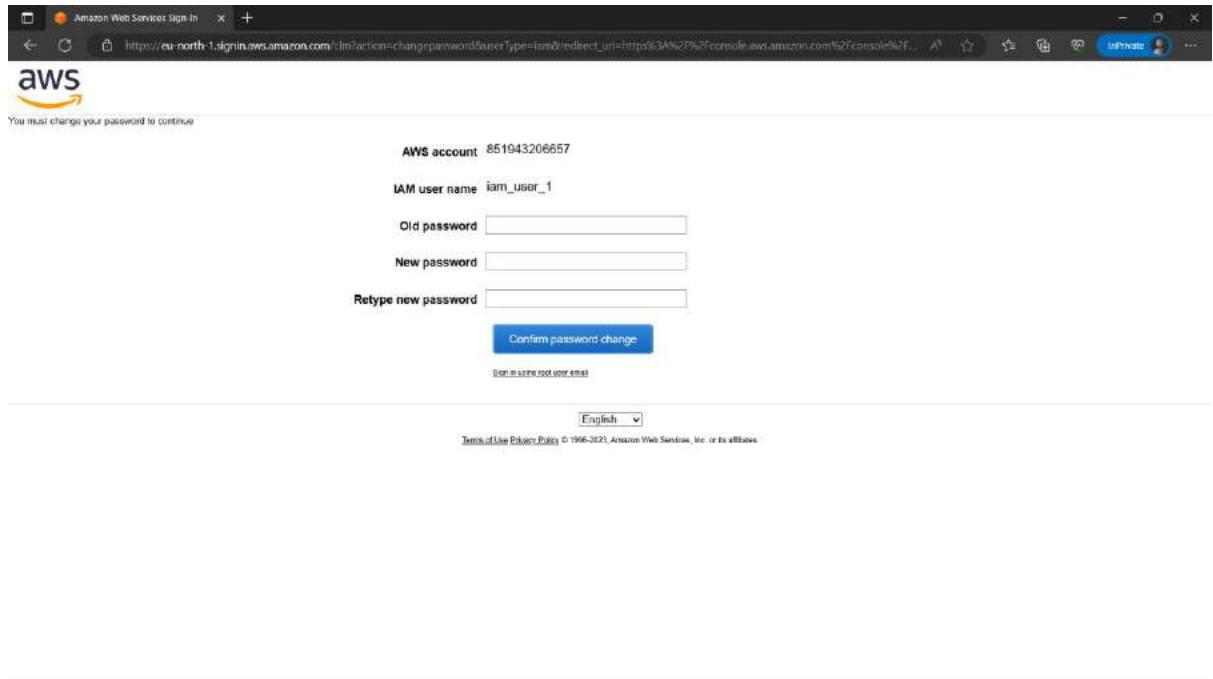
19)Now the IAM user is created. Copy the details save it file(Excel, word, notepad).

The screenshot shows the AWS IAM Management Console. A green banner at the top indicates "User created successfully". Below it, the "Create user" page is displayed. On the left, a sidebar lists steps: Step 1 (Specify user details), Step 2 (Set permissions), Step 3 (Review and create), and Step 4 (Retrieve password). The "Retrieve password" section is active. It contains "Console sign-in details" with fields for "Console sign-in URL" (redacted), "User name" (iam_user_1), and "Console password" (redacted). There are "Email sign-in instructions" and "Show" buttons. At the bottom are "Download .csv file" and "Return to users list" buttons.

20)After saving copy the sign-in url and paste it in a incognito tab(ctrl+shift+n). By default there will be account id, type the username and password and click sign in.

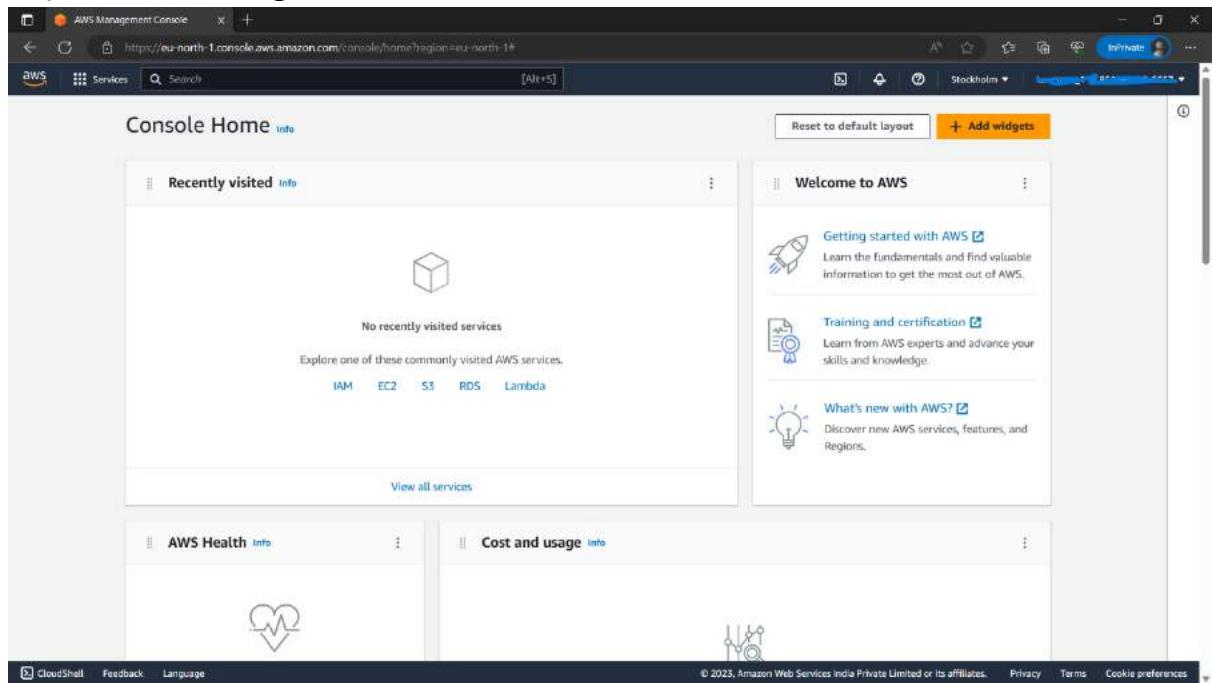
The screenshot shows the AWS Sign-in page. The left side has a "Sign in as IAM user" form with fields for "Account ID (12 digits) or account alias" (redacted), "IAM user name" (iam_user_1), "Password" (redacted), and a "Remember this account" checkbox. Below the form are links for "Sign in using root user email" and "Forgot password?". The right side features an advertisement for "Amazon Lightsail" with the tagline "Lightsail is the easiest way to get started on AWS" and a "Learn more »" button. A cartoon robot character is shown pointing upwards.

21) Now it will ask to change the password, let IAM user change the password so that they can remember it easily. After typing the password click on “confirm password change.”



The screenshot shows the AWS IAM password change form. It includes fields for the AWS account (851943206657), IAM user name (iam_user_1), Old password, New password, and Retype new password. A blue "Confirm password change" button is at the bottom. Below the form, there is a link to "Forgot my password? Get help via email". The page also features language selection ("English") and links to "Terms of Use" and "Privacy Policy".

22) Now we are signed in as a IAM user.



The screenshot shows the AWS Management Console home page. It features a "Welcome to AWS" section with links to "Getting started with AWS", "Training and certification", and "What's new with AWS?". Below this, there are sections for "Recently visited" services (with a note that none have been visited) and "AWS Health" and "Cost and usage". The footer includes links for CloudShell, Feedback, Language, and various legal and policy documents.

23)Now open ec2 by searching in the search bar click on ec2 instance option.

Search results for 'ec2'
Try searching with longer queries for more relevant results

See all 12 results ▾

Services

- EC2 ☆ Virtual Servers in the Cloud
- EC2 Image Builder ☆ A managed service to automate build, customize and deploy OS images
- Amazon Inspector ☆ Continual vulnerability management at scale
- AWS Firewall Manager ☆ Central management of firewall rules

See all 53 results ▾

Features

- Dashboard
- EC2 feature
- Limits
- EC2 feature

24)We see that it shows API error because we don't have ec2 permission to create an instance.

Dashboard | EC2 Management

New EC2 Experience Tell us what you think

EC2 Dashboard

- EC2 Global View
- Events
- Limits
- Instances
- Instances
- Instance Types
- Launch Templates
- Spot Requests
- Savings Plans
- Reserved Instances
- Dedicated Hosts
- Capacity Reservations
- Images
- AMIs
- AMI Catalog
- Elastic Block Store
- Volumes
- Snapshots
- Lifecycle Manager

Resources

You are using the following Amazon EC2 resources in the Europe (Stockholm) Region:

Instances (running)	0	Auto Scaling Groups	API Error	Dedicated Hosts	API Error
Elastic IPs	API Error	Instances	API Error	Key pairs	API Error
Load balancers	API Error	Placement groups	API Error	Security groups	API Error
Snapshots	API Error	Volumes	API Error		

Learn more about the latest in AWS Compute from AWS re:Invent by viewing the [EC2 Videos](#).

Launch instance

Note: Your instances will launch in the Europe (Stockholm) Region

Service health

Region: Europe (Stockholm)

Status: This service is operating normally

Zones

Account attributes

Supported platforms

- An error occurred An error occurred retrieving supported platforms
- An error occurred An error occurred checking for a default VPC

Settings

EBS encryption

Zones

EC2 Serial Console

Default credit specification

Console experiments

Explore AWS

10 Things You Can Do Today to Reduce AWS Costs

Explore how to effectively manage your AWS costs without compromising on performance or capacity.

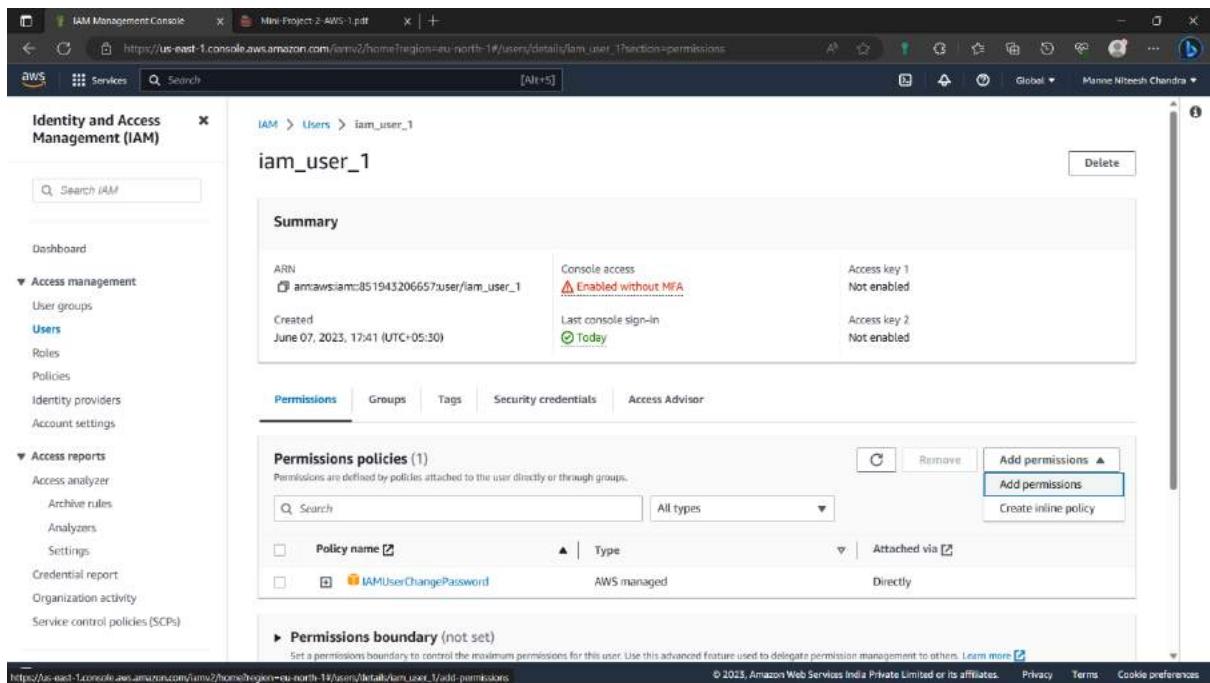
25) Now go to IAM user in root account which created the IAM user.

A screenshot of the AWS IAM Management Console. The left sidebar shows navigation options under 'Identity and Access Management (IAM)' such as Dashboard, Access management (User groups, Users, Roles, Policies, Identity providers, Account settings), and Access reports (Access analyzer, Archive rules, Analyzers, Settings, Credential report, Organization activity, Service control policies (SCPs)). The main content area is titled 'Users (1) Info' and contains a table with one row for 'iam_user_1'. The table columns include User name, Groups, Last activity, MFA, Password age, and Active key age. The 'Last activity' column shows '36 minutes ago' with a green checkmark. The 'Password age' column shows '32 minutes ago' with a green checkmark. The 'Active key age' column shows '-'.

26) Click on the created IAM user.

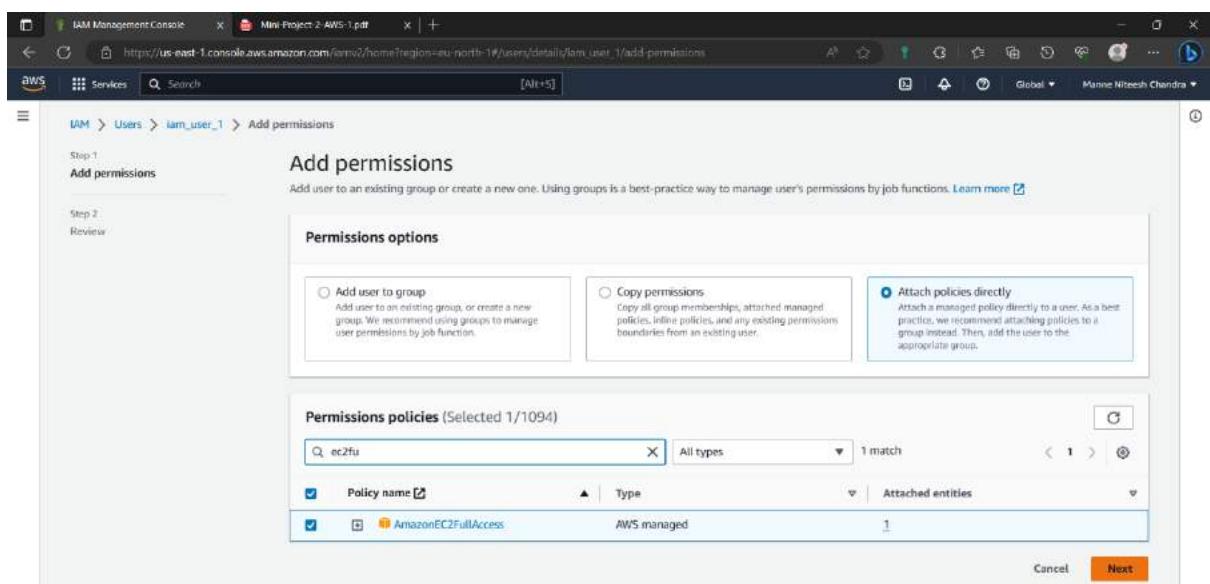
A screenshot of the AWS IAM Management Console showing the details for the 'iam_user_1' user. The left sidebar is identical to the previous screenshot. The main content area has a title 'iam_user_1'. Under the 'Summary' section, it shows ARN (arn:aws:iam:851943206657:user/iam_user_1), Created (June 07, 2023, 17:41 (UTC+05:30)), and Console access (Enabled without MFA). It also lists Access key 1 (Not enabled) and Access key 2 (Not enabled). Below the summary are tabs for 'Permissions', 'Groups', 'Tags', 'Security credentials', and 'Access Advisor'. The 'Permissions' tab is selected, showing a table for 'Permissions policies (1)'. The table has columns for Policy name, Type, and Attached via. It lists one policy: 'IAMUserChangePassword' (AWS managed, Directly attached). There is also a 'Permissions boundary (not set)' section with a note about delegating permission management.

27) Click on add permission option.



The screenshot shows the AWS IAM Management Console. On the left, there's a sidebar with navigation links like Dashboard, Access management, and Access reports. The main area is titled 'Summary' for the user 'iam_user_1'. It displays basic information such as ARN, creation date, and access keys. The 'Permissions' tab is active, showing a table with one row for the policy 'IAMUserChangePassword'. A large orange 'Add permissions' button is located at the top right of this section. Below the table, there's a section for 'Permissions boundary (not set)'.

28)Select “Attach policies directly” option and select “AmazonEC2FullAccess” permission and click on next.



This screenshot shows the 'Add permissions' wizard, Step 1: Add permissions. It has two tabs: Step 1 (Add permissions) and Step 2 (Review). Under Step 1, there are three options: 'Add user to group', 'Copy permissions', and 'Attach policies directly'. The 'Attach policies directly' option is selected. Below these options, there's a search bar with 'ec2fu' typed in, and a list of 'Permissions policies' showing one result: 'AmazonEC2FullAccess'.

29) Review the assigned data and click on Add permission.

The screenshot shows the AWS IAM Management Console. The URL is https://us-east-1.console.aws.amazon.com/iamv2/home?region=eu-north-1#/users/details/iam_user_1/add-permissions. The page title is "Review". It shows the following details:

- User details:** User name: iam_user_1
- Permissions summary (1):**

Name	Type	Used as
AmazonEC2FullAccess	AWS managed	Permissions policy

At the bottom right, there are buttons for "Cancel", "Previous", and "Add permissions" (which is highlighted).

30) Now open incognito tab and sign in as IAM user.

The screenshot shows the AWS Sign-In page for IAM users. The URL is https://eu-north-1.signin.aws.amazon.com/console?client_id=amzn%3Aaws%3Agl%3A%2Fconsole%2Fnav%2Fcode_challenge-1bW5y09jwefItpT9fC-oY.... The page has the following elements:

- Sign in as IAM user:**
 - Account ID (12 digits) or account alias: 851943206657
 - IAM user name: iam_user_1
 - Password: [REDACTED]
 - Remember this account
 - Sign in** button
- Sign in using root user email** and **Forgot password?** links
- Amazon Lightsail** promotional banner:

Lightsail is the easiest way to get started on AWS

[Learn more »](#)


- Language selection: English
- Footer links: Terms of Use, Privacy Policy, © 1996-2023, Amazon Web Services, Inc. or its affiliates.

31) Now open ec2 by searching in the search bar click on ec2 instance option.

The screenshot shows the AWS Management Console search results for the query 'ec2'. The search bar at the top contains 'ec2'. Below it, there are two main sections: 'Services' and 'Features'. The 'Services' section is expanded, showing 12 results. The first result is 'EC2' with the description 'Virtual Servers in the Cloud'. To the right of the search results, there is a sidebar titled 'AWS' with several cards: 'Getting started with AWS', 'Find certification', and 'New with AWS?'. At the bottom of the page, there are links for 'CloudShell', 'Feedback', 'Language', and copyright information: '© 2023, Amazon Web Services India Private Limited or its affiliates.' and 'Privacy Terms Cookie preferences'.

32)Now we don't see any api error because we added "amazonec2fullacces" permission.

33) Now create an instance by clicking on launching instance.

34) Give a name to the instance and let everything be default.

The screenshot shows the 'Launch an instance | EC2 Manager' wizard on the AWS console. The current step is 'Name and tags'. A 'Name' field contains 'web'. On the right, a summary panel shows: 'Number of instances: 1', 'Software Image (AMI): Amazon Linux 2023 AMI 2023.0.2...', 'Virtual server type (instance type): t3.micro', and a note about free tier benefits. At the bottom right is a 'Launch instance' button.

35) click on “create a keypair” and give a random name,type,file format and click “create key pair”.

The screenshot shows the 'Launch an instance | EC2 Manager' wizard on the AWS console. The current step is 'Create key pair'. It shows a 'Key pair name' field with 'key1' and a note about key pairs for secure connection. Below it, 'Key pair type' is set to 'RSA' and 'Private key file format' is set to '.pem'. A warning message at the bottom says: 'When prompted, store the private key in a secure and accessible location on your computer. You will need it later to connect to your instance.' At the bottom right are 'Cancel' and 'Create key pair' buttons.

36) Review everything at Summary and click on launch instance.

The screenshot shows the AWS EC2 Launch an Instance wizard. In the 'Configure storage' section, a single gp3 volume of 8 GiB is selected as the root volume. The 'Advanced' tab is open. In the 'Summary' section, it shows 1 instance being launched with an Amazon Linux 2023 AMI and a t3.micro instance type. The 'Launch instance' button is highlighted in orange.

37) Now the instance is created.

The screenshot shows the AWS EC2 Instances page after the instance has been successfully launched. A success message indicates the launch was initiated for instance [i-0a494adb9c3dddb7a0]. Below the message, there are several 'Next Steps' options: 'Create billing and free tier usage alerts', 'Connect to your instance', 'Connect an RDS database', 'Create EBS snapshot policy', 'Manage detailed monitoring', 'Create Load Balancer', 'Create AWS budget', and 'Manage CloudWatch alarms'.

38) We created ec2 instance because we assigned “ec2fullaccess” permission to the “IAM” user we cannot create any other tool with this permission. Now let's try to create a S3 bucket. In search bar type S3 and click on S3 option.

The screenshot shows the AWS Management Console search results for 'S3'. The search bar at the top contains 's3'. The results are categorized under 'Services' and 'Features'. Under 'Services', there are four items: 'S3' (Scalable Storage in the Cloud), 'S3 Glacier' (Archive Storage in the Cloud), 'AWS Snow Family' (Large Scale Data Transport), and 'AWS Transfer Family' (Fully managed support for SFTP, FTPS and FTP). Under 'Features', there are two items: 'Amazon S3 File Gateway' (Storage Gateway feature) and 'Batch Operations' (S3 feature). On the right side of the console, there is a sidebar with various links related to AWS, such as 'Getting started with AWS', 'AWS certification', and 'Learn with AWS?'. The bottom of the screen includes standard AWS navigation links like CloudShell, Feedback, Language, and cookie preferences.

39) Click on create bucket option.

The screenshot shows the AWS S3 Management Console. The main heading is 'Amazon S3' with the subtext 'Store and retrieve any amount of data from anywhere'. Below this, there is a brief description of Amazon S3 and a link to the 'Introduction to Amazon S3' video. To the right, there is a 'Create a bucket' dialog box with the subtext 'Every object in S3 is stored in a bucket. To upload files and folders to S3, you'll need to create a bucket where the objects will be stored.' A prominent orange 'Create bucket' button is at the bottom of this dialog. Below the dialog, there are sections for 'Pricing' (with a note about no minimum fees and a link to the Simple Monthly Calculator) and 'Resources' (with a link to the User guide). The bottom of the screen includes standard AWS navigation links like Feedback, Language, and cookie preferences.

40) Now give a name to the bucket it has to be unique.

The screenshot shows the 'Create bucket' page in the AWS S3 console. In the 'General configuration' section, the 'Bucket name' is set to 'bucket' and the 'AWS Region' is set to 'EU (Stockholm) eu-north-1'. Under 'Object Ownership', the 'ACLs disabled (recommended)' option is selected. The page also includes sections for 'Tags (U) - optional' and 'Default encryption'.

41) Let everything be default and click on “create bucket”.

The screenshot shows the 'Create bucket' page with all settings left at their defaults. The 'Create bucket' button is highlighted in orange at the bottom right of the form.

42) It will show that you do not have permission to create a S3 bucket. Now let's try adding administrator permission to the user. with administrator we can create anything.

The screenshot shows the AWS S3 console at <https://s3.console.aws.amazon.com/s3/bucket/create?region=eu-north-1>. The 'Default encryption' section is visible, showing 'Amazon S3 managed keys (SSE-S3)' selected. Under 'Bucket Key', 'Enable' is selected. A note says 'After creating the bucket you can upload files and folders to the bucket, and configure additional bucket settings.' A prominent red error box displays the message 'Failed to create bucket' with the subtext 'To create a bucket, s3:CreateBucket permissions are required.' It also links to 'View your permissions in the IAM console' and 'Identity and Access Management in Amazon S3'. At the bottom right is a 'Create bucket' button.

43) Now go to IAM user in root account which created the IAM user.

The screenshot shows the AWS IAM Management Console at <https://us-east-1.console.aws.amazon.com/iamv2/home?region=eu-north-1#/users>. The left sidebar shows 'Identity and Access Management (IAM)' with 'Users' selected. The main pane displays a table titled 'Users (1)'. The table has one row for 'iam_user_1', which is highlighted. The table includes columns for User name, Groups, Last activity, MFA, Password age, and Active key age. The 'Last activity' column shows '36 minutes ago'. The 'Active key age' column shows '32 minutes ago'. At the top right of the table are 'Delete' and 'Add users' buttons.

44) Click on the created IAM user.

The screenshot shows the AWS IAM Management Console. On the left, there's a navigation sidebar with options like Dashboard, Access management (User groups, Users, Roles, Policies, Identity providers, Account settings), Access reports (Access analyzer, Archive rules, Analyzers, Settings, Credential report, Organization activity, Service control policies (SCPs)), CloudShell, Feedback, Language, and a footer with CloudShell, Feedback, Language, © 2023, Amazon Web Services India Private Limited or its affiliates., Privacy, Terms, and Cookie preferences.

The main area is titled 'Users (1) Info' and contains a table with one row for 'iam_user_1'. The columns are User name, Groups, Last activity, MFA, Password age, and Active key age. The user 'iam_user_1' has None in all these fields.

45) Click on add permission option.

This screenshot shows the detailed view of the 'iam_user_1' user. The left sidebar is identical to the previous screenshot. The main area shows the 'Summary' section with ARN (arn:aws:iam::1943206657:user/iam_user_1), Console access (Enabled without MFA), and two Access keys (Not enabled). Below this is the 'Permissions' tab, which lists three attached policies: 'AdministratorAccess', 'AmazonEC2FullAccess', and 'IAMUserChangePassword'. There are buttons for 'Add permissions' and 'Create inline policy'.

46) Type “administratoraccess” and select it.

The screenshot shows the AWS IAM Management Console. The URL is https://us-east-1.console.aws.amazon.com/iamv2/home?region=eu-north-1#/users/details/iam_user_1/add-permissions. The page title is "Add permissions".
Step 1: Add permissions
Step 2: Review
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 functions.
 Copy permissions
Copy all group memberships, attached managed policies, inline policies, and any existing permissions boundaries from an existing user.
 Attach policies directly
Attach a managed policy directly to a user. As a best practice, we recommend attaching policies to a group instead. Then, add the user to the appropriate group.
Permissions policies (Selected 1/1093)

Policy name	Type	Attached entities
AccessAnalyzerServiceRolePolicy	AWS managed	0
<input checked="" type="checkbox"/> AdministratorAccess	AWS managed - job function	0
AdministratorAccess-Amplify	AWS managed	0
AdministratorAccess-AWSElasticBea...	AWS managed	0
AlexaForBusinessDeviceSetup	AWS managed	0

47) Click Next.

The screenshot shows the AWS IAM Management Console. The URL is https://us-east-1.console.aws.amazon.com/iamv2/home?region=eu-north-1#/users/details/iam_user_1/add-permissions. The page title is "Add permissions".
Step 1: Add permissions
Step 2: Review
Permissions policies

Policy name	Type	Attached entities
AlexaForBusinessDeviceSetup	AWS managed	0
AlexaForBusinessFullAccess	AWS managed	0
AlexaForBusinessGatewayExecution	AWS managed	0
AlexaForBusinessLifesizeDelegated...	AWS managed	0
AlexaForBusinessNetworkProfileSer...	AWS managed	0
AlexaForBusinessPolyDelegatedAcc...	AWS managed	0
AlexaForBusinessReadOnlyAccess	AWS managed	0
AmazonAPIGatewayAdministrator	AWS managed	0
AmazonAPIGatewayInvokeFullAccess	AWS managed	0
AmazonAPIGatewayPushToCloudW...	AWS managed	0
AmazonAppFlowFullAccess	AWS managed	0
AmazonAppFlowReadOnlyAccess	AWS managed	0
AmazonAppStreamFullAccess	AWS managed	0
AmazonAppStreamPCAAccess	AWS managed	0
AmazonAppStreamReadOnlyAccess	AWS managed	0
AmazonAppStreamServiceAccess	AWS managed	0

Next Step

48) Now go to IAM user account and repeat the steps from 24-27. Now the bucket is created because we give administrator access in permissions which will let you create the tool use it, remove it.

The screenshot shows the AWS S3 Management Console interface. A green success message at the top states "Successfully created bucket 'bucket878'. To upload files and folders, or to configure additional bucket settings choose View details." On the left, a sidebar menu includes options like Buckets, Access Points, Object Lambda Access Points, Multi-Region Access Points, Batch Operations, IAM Access Analyzer for S3, Block Public Access settings for this account, Storage Lens, Dashboards, and AWS Organizations settings. The main content area displays an "Account snapshot" with a "Storage lens provides visibility into storage usage and activity trends. Learn more" link and a "View Storage Lens dashboard" button. Below this is a "Buckets (1)" section with a table. The table has columns for Name, AWS Region, Access, and Creation date. It lists a single bucket named "bucket878" located in "EU (Stockholm) eu-north-1" with "Bucket and objects not public" access and created on "June 7, 2023, 17:23:30 (UTC+05:30)". Action buttons for Copy ARN, Empty, Delete, and Create bucket are visible above the table. At the bottom of the page, there are links for CloudShell, Feedback, Language, and a footer with copyright information and links for Privacy, Terms, and Cookie preferences.

Billing Alarm:

49) Type “CloudWatch” in search bar and select the “CloudWatch” service below.

The screenshot shows the AWS CloudWatch search results page. The search bar at the top contains the query "Cloudwatch". The results are categorized into "Services" and "Features". Under "Services", "CloudWatch" is selected and highlighted, described as a "Monitor Resources and Applications" service. Other services listed include "Amazon EventBridge" (a serverless event-driven application service) and "Athena" (a serverless interactive analytics service). Under "Features", sections include "Servers" (listing "AWS Transfer Family feature"), "CloudWatch Synthetics" (a CloudWatch feature), and "CloudWatch Evidently" (another CloudWatch feature). A sidebar on the right provides information about getting started with AWS, learning and certification, and viewing AWS services, features, and products. The footer of the page includes links for CloudShell, Feedback, Language, and standard AWS footer links for Privacy, Terms, and Cookie preferences.

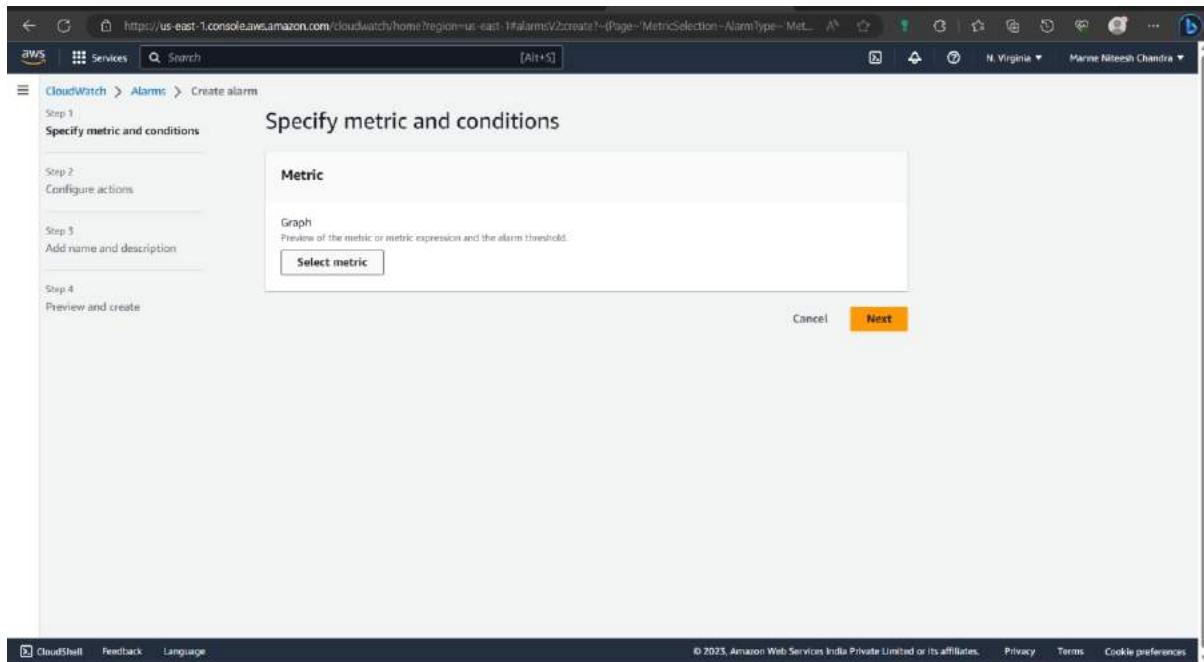
50)Select “All alarms” options in the navigation bar.

The screenshot shows the AWS CloudWatch Home page. The navigation bar on the left has 'All alarms' selected under the 'Alarms' category. The main content area displays a 'Get started with CloudWatch' section with four cards: 'Create alarms', 'Create a default dashboard', 'View logs', and 'View events'. Below this is a 'Get started with Application Insights' section with a 'Configure Application Insights' button. At the bottom, there is a 'CloudWatch Logs' section and a note that 'No alarms configured'.

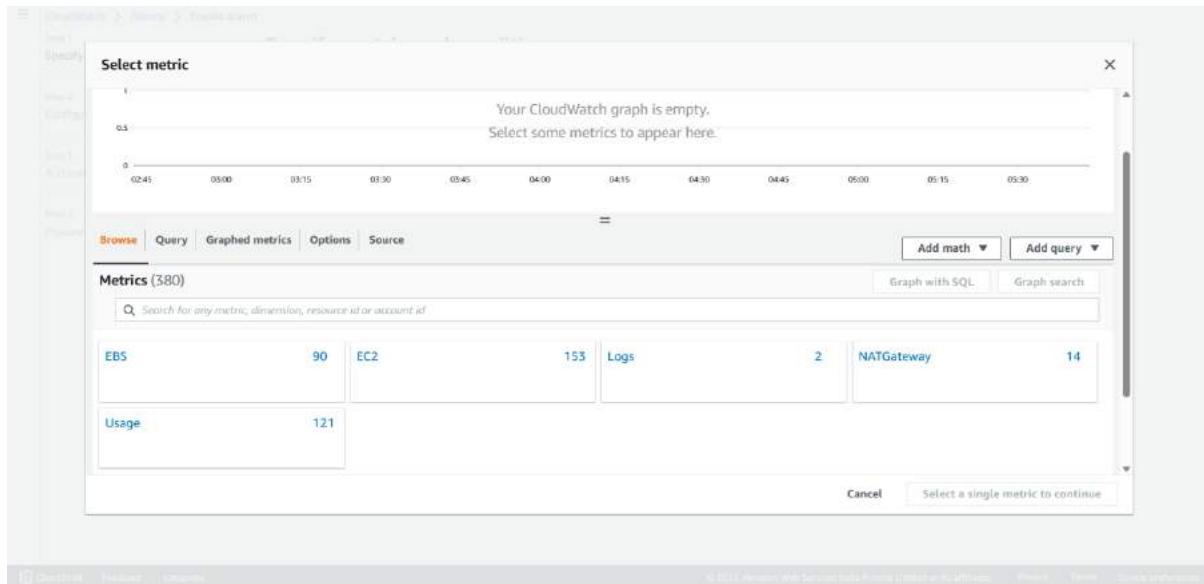
51)Click on “create alarm” option at top right side in yellow colour.

The screenshot shows the AWS CloudWatch Alarms page. The navigation bar on the left has 'All alarms' selected under the 'Alarms' category. The main content area shows a table titled 'Alarms (0)' with columns for Name, State, Last state update, and Conditions. A large orange 'Create alarm' button is located at the top right of the table area. The URL in the address bar is https://us-east-1.console.aws.amazon.com/cloudwatch/home?region=us-east-1#alarmsV2:create.

52) Click on “Select metric” option.



53) In “browse” we cannot find billing option. If you find the billing option click the billing option, else follow the below steps to enable the billing option.



54) Now go to search bar type “Billing” and select the “Billing” option.

The screenshot shows the AWS search interface with the query "billing" entered in the search bar. The results are categorized under "Services" and "Features". The "Billing" service is highlighted in the "Services" section, showing its description: "Access, analyze, and control your AWS costs and usage." Below it are three related services: "AWS Billing Conductor", "AWS Wicks", and "IoT TwinMaker". In the "Features" section, there is one item: "Billing groups". On the right side of the search results, there is a sidebar titled "AWS" with sections for "Getting started with AWS", "AWS certification", and "Learn with AWS".

55) Select the “Billing Preference” in navigation panel i.e., at bottom of the navigation panel.

The screenshot shows the AWS Billing Dashboard. The left navigation panel is expanded, showing various options like Bills, Payments, Credits, Purchase orders, etc., with "Billing preferences" highlighted in yellow. The main dashboard area displays the "AWS Billing Dashboard" with a summary of current month's total forecast, MTD balance, and active services/accounts/regions. Below this, there are sections for "Highest cost" (Data Transfer) and "Cost trend by top five services". The status bar at the bottom indicates the URL as https://us-east-1.console.aws.amazon.com/billing/home?region=us-east-1#preferences.

56) Click on edit option for “Alert preferences”.

The screenshot shows the AWS Billing preferences page. On the left sidebar, under the 'Billing' section, the 'Billing preferences' link is highlighted. The main content area displays three sections: 'Invoice delivery preferences', 'Alert preferences', and 'Detailed billing reports (legacy)'. The 'Alert preferences' section contains two options: 'AWS Free Tier alerts' (selected) and 'CloudWatch billing alerts' (not selected). Below these options is a note about legacy reports and a 'Legacy report delivery to S3' section. At the bottom right of the 'Alert preferences' section is an 'Edit' button.

57) Enable the “CloudWatch billing alerts” option (Note: Once it is enabled it cannot be disabled) click update.

This screenshot shows the same AWS Billing preferences page as the previous one, but with a key difference: the 'CloudWatch billing alerts' checkbox in the 'Alert preferences' section is now checked. The other alert preference, 'AWS Free Tier alerts', remains checked. Below the checkboxes is a note about additional email addresses for alerts. At the bottom right of the 'Alert preferences' section, there is an 'Update' button.

58)Now it is enabled.

The screenshot shows the AWS Billing preferences page. A green success message at the top right says "Your alert preferences were updated successfully." On the left sidebar, under "Billing preferences", "Payment preferences" is selected. The main content area has two sections: "Invoice delivery preferences" and "Alert preferences". Under "Invoice delivery preferences", there is a note about PDF invoices being delivered by email, which is currently deactivated. Under "Alert preferences", there are entries for AWS Free Tier alerts and CloudWatch billing alerts, both of which are set to "Delivered". At the bottom, there is a section for "Detailed billing reports (legacy)" with a note about the AWS Cost & Usage report.

59)Now repeat the steps 49-52 and in browse option we can see the billing option, Click the “Billing” option.

The screenshot shows the "Select metric" dialog box from the AWS CloudWatch Metrics interface. The "Metrics (103)" section is visible, and the "Billing" metric is selected, indicated by a blue border. Other metrics shown include EBS, EC2, and Logs. Below the metrics, there is a search bar and buttons for "Graph with SQL" and "Graph search". At the bottom right of the dialog, there is a button labeled "Select a single metric to continue".

60) Click the “Total Estimated Charge”.

The screenshot shows the 'Select metric' dialog box from the AWS CloudWatch Management Console. The 'Metrics' tab is selected, showing a list of metrics. One metric, 'Total Estimated Charge', is highlighted with a blue border. At the bottom right of the dialog, there is a button labeled 'Select metric to continue'.

61) Select the “EstimatedCharges” and click on select metric.

The screenshot shows the 'Select metric' dialog box from the AWS CloudWatch Management Console. The 'Metrics' tab is selected, showing a list of metrics under the 'Billing' category. One metric, 'EstimatedCharges', is highlighted with a blue border. At the bottom right of the dialog, there is a button labeled 'Select metric'.

62) Now we can see the graph give an name to metric, Static-maximum, period.

The screenshot shows the 'Specify metric and conditions' step of creating a new alarm. On the left, a sidebar lists steps: Step 1 (Specify metric and conditions), Step 2 (Configure actions), Step 3 (Add name and description), and Step 4 (Preview and create). The main area is titled 'Metric' and contains a graph showing 'EstimatedCharges' over time. The graph has a red line at the top and a blue line below it, with a shaded area between them. The Y-axis is labeled 'No unit' with values 0, 0.5, and 1. The X-axis shows dates: 06/06, 06/08, and 06/10. A legend indicates the blue line represents 'EstimatedCharges'. To the right of the graph, fields are filled out: Namespace 'AWS/Billing', Metric name 'EstimatedCharges', Currency 'USD', Statistic 'Maximum', and Period '6 hours'. Below the graph, a 'Conditions' section is visible.

63) In conditions Threshold type-Static, EstimatedCharges-Greater, than-10(value your choice i.e., bill should not exceed this value) and click on “Next”.

The screenshot shows the 'Conditions' step of creating a new alarm. It displays the configuration for the previously selected metric. Under 'Threshold type', the 'Static' option is selected. Under 'Whenever EstimatedCharges is...', the 'Greater' option is selected with the threshold value set to '10'. The currency is listed as 'USD'. At the bottom, there is an 'Additional configuration' link and a 'Next' button.

64)Notification- In alarm, Notification to following SNS topic- Create new topic, Name, Email ID(which email id you want receive the notification about billing).

CloudWatch Management Console

Notification

Alarm state trigger

In alarm The metric or expression is outside of the defined threshold.

OK The metric or expression is within the defined threshold.

Insufficient data The alarm has just started or not enough data is available.

Add name and description

Select an existing SNS topic

Create new topic (selected)

Use topic ARN to notify other accounts

Default_CloudWatch_Alarms_Topic

Email endpoints that will receive the notification...

Add a comma-separated list of email addresses. Each address will be added as a subscription to the topic above.

user1@example.com, user2@example.com

Create topic

Add notification

65)Click on “Next”.

CloudWatch Management Console

Auto Scaling action

Add Auto Scaling action

EC2 action

This action is only available for EC2 Per-Instance Metrics.

Add EC2 action

Systems Manager action [Info](#)

This action will create an Incident or OpItem in Systems Manager when the alarm is **In alarm** state.

Add Systems Manager action

Cancel Previous Next

66) Give a name, description of your choice and click on next.

The screenshot shows the AWS CloudWatch Management Console with the URL <https://us-east-1.console.aws.amazon.com/cloudwatch/home?region=us-east-1#alarm:V2:create?{Page=Preview&AlarmType=MetricAlarm...}>. The page title is "CloudWatch Management Console". The left sidebar shows steps: Step 1: Specify metric and conditions, Step 2: Configure actions, Step 3: Add name and description (which is selected), and Step 4: Preview and create. The main content area is titled "Add name and description". It has a "Name and description" section with a "Name" input field containing "Billing" and a "Description" input field with the placeholder "# This is an H1\n**double asterisks will produce strong character**\nThis is [an example](https://example.com/) inline link.". Below these fields is a note: "Up to 1024 characters (0/1024)". At the bottom are "Cancel", "Previous", and a yellow "Next" button.

67) Review all the data and click on “Create alarm” option.

The screenshot shows the AWS CloudWatch Management Console with the same URL as the previous screenshot. The left sidebar shows steps: Step 1: Specify metric and conditions, Step 2: Configure actions, Step 3: Add name and description, and Step 4: Preview and create. The main content area shows the configuration from the previous step: "Greater than..." with "10" selected, and an "Additional configuration" section. Below this is "Step 2: Configure actions" with an "Actions" section containing a "Notification" entry: "When in alarm, send a notification to 'Default_CloudWatch_Alarms_Topic'". Below this is "Step 3: Add name and description" with a "Name and description" section showing "Name: Billing" and "Description: -". At the bottom are "Cancel", "Previous", and a yellow "Create alarm" button.

68)Now the billing alarm is created.

The screenshot shows the AWS CloudWatch Management Console. On the left, the navigation pane includes sections like Favorites and recent, Dashboards, Alarms (with a sub-section for All alarms), Logs, Metrics, X-Ray traces, and Events. The main content area displays a success message: "Successfully created alarm Billing." Below this, a notification says "Some subscriptions are pending confirmation" and "Amazon SNS doesn't send messages to an endpoint until the subscription is confirmed". The main table lists one alarm named "Billing" with the following details:

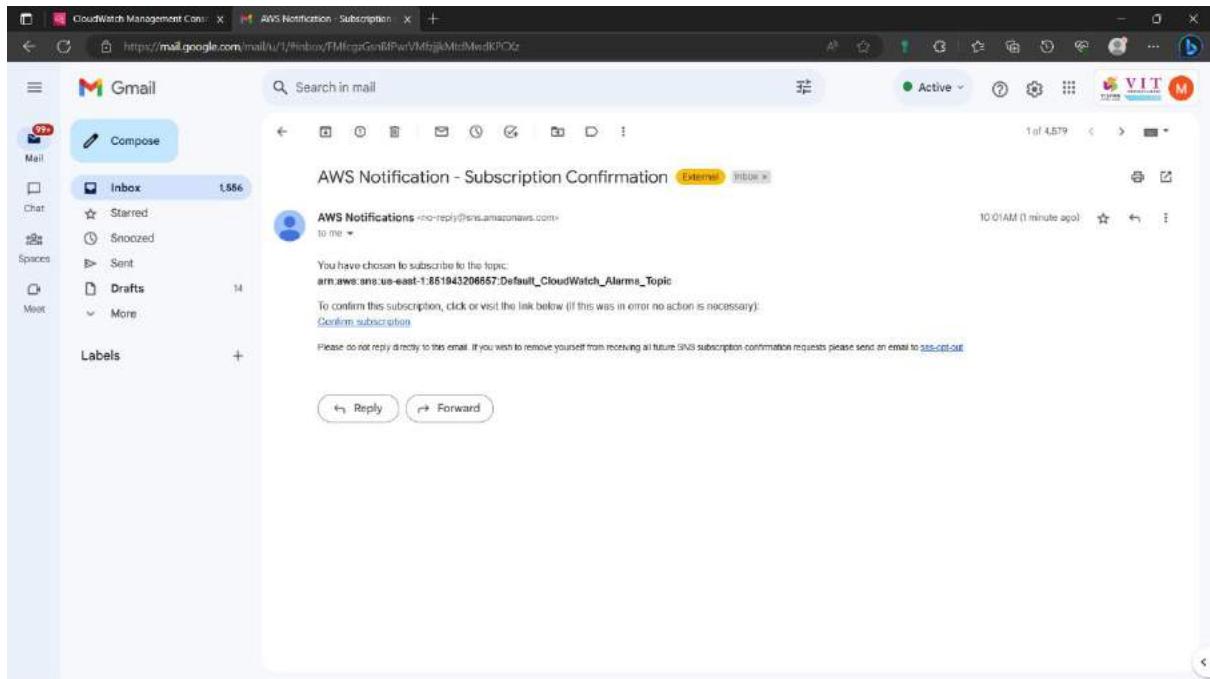
Name	State	Last state update	Conditions	Actions
Billing	Insufficient data	2023-06-12 04:32:15	EstimatedCharges > 10 for 1 datapoints within 6 hours	Actions enabled Warning

69)Open the Gmail of the email id you provided in the billing for notification. you can see there is AWS notification open it.

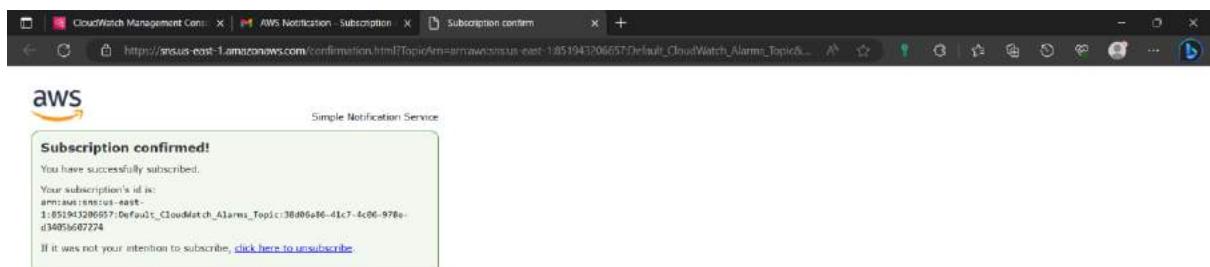
The screenshot shows a Gmail inbox with 1,587 messages. The inbox list includes several AWS-related notifications:

- AWS Notifications: AWS Notification - Subscription Confirmation
- Coding Ninjas: Manne, crack top tech jobs with up to 100% scholarship
- Career Camp: From foodie to Full Stack Developer in 9 months
- ISP Team from Inter.: Manne, you're a 99% - here's the 1% you need!
- ZEPP Student Purcha.: The Scent of Confidence! #studentpurchaseprogram
- Amazon Web Services: New associate-level cloud training—free on Twitch - Expand your career opportunities Amazon Web Services AWS Power H...
- LinkedIn: Ankur Warikoo and others just posted
- Career Camp: Enter IoT Industry with full stack development
- ZEPP Student Purcha.: Powerful HP Laptops: Perfect for Students! #studentpurchaseprogram
- ISP Team from Inter.: Manne, you're a catch - here's your perfect match!
- GeeksforGeeks: Weekly Coding Contest Time!
- AWS India: Welcome to your Getting Started series
- Infosys Springboard: Top 10 Learners of May 2023 are..!
- Amazon Web Services: Watch on-demand | AWSome Day Online Conference
- InterviewBit: [Invite] Multi-threading and Java Concurrency
- Coding Ninjas Studio: Get placed in top tech companies offering up to 25 LPA
- Get up to 100% scholarship like a boss

70) Click the “confirm subscription” option.



71) Now you will receive the notification if the bill value exceeds the given value.



S3 Bucket:

72) Type “S3” in search bar and select the “S3” option below.

The screenshot shows the AWS Management Console search results for 'S3'. The search bar at the top contains 'S3'. Below it, the 'Services' section lists several options, with 'S3' being the first and highlighted with a green box. Other listed services include S3 Glacier, AWS Snow Family, and AWS Transfer Family. The 'Features' section also lists Amazon S3 File Gateway and Batch Operations. On the right side of the screen, there is a sidebar with various links related to AWS, such as 'Getting started with AWS', 'AWS certification', and 'AWS白皮书'.

73) Click “create bucket” option.

The screenshot shows the AWS S3 Management Console. The main header says 'Amazon S3' and 'Store and retrieve any amount of data from anywhere'. Below this, there is a 'How it works' section with a video thumbnail titled 'Introduction to Amazon S3'. To the right, there is a 'Create a bucket' dialog box with the text: 'Every object in S3 is stored in a bucket. To upload files and folders to S3, you'll need to create a bucket where the objects will be stored.' Below this is a large orange 'Create bucket' button. Further down, there are sections for 'Pricing' (with a note about no minimum fees) and 'Resources' (with a link to 'User guide').

74) Give a unique name to the bucket.

The screenshot shows the 'Create bucket' page in the AWS S3 console. In the 'General configuration' section, the 'Bucket name' field contains 'engrocloudarl'. The 'AWS Region' dropdown is set to 'US East (N. Virginia) us-east-1'. Below these fields is a 'Copy settings from existing bucket - optional' section with a 'Choose bucket' button. In the 'Object Ownership' section, the 'ACLs disabled (recommended)' option is selected. At the bottom of the page, there are links for CloudShell, Feedback, Language, and cookie preferences, along with a note about copyright and terms.

75) Click on “create bucket”

The screenshot shows the 'Create bucket' page in the AWS S3 console, continuing from the previous step. It includes sections for 'Tags (0) - optional' (with a note about tracking costs and organization), 'Default encryption' (with a note about server-side encryption), and 'Bucket Key' (with options to enable or disable KMS encryption). At the bottom of the page, there is an 'Advanced settings' link and a callout box containing the text: 'After creating the bucket, you can upload files and folders to the bucket, and configure additional bucket settings.' The 'Create bucket' button is prominently displayed at the bottom right.

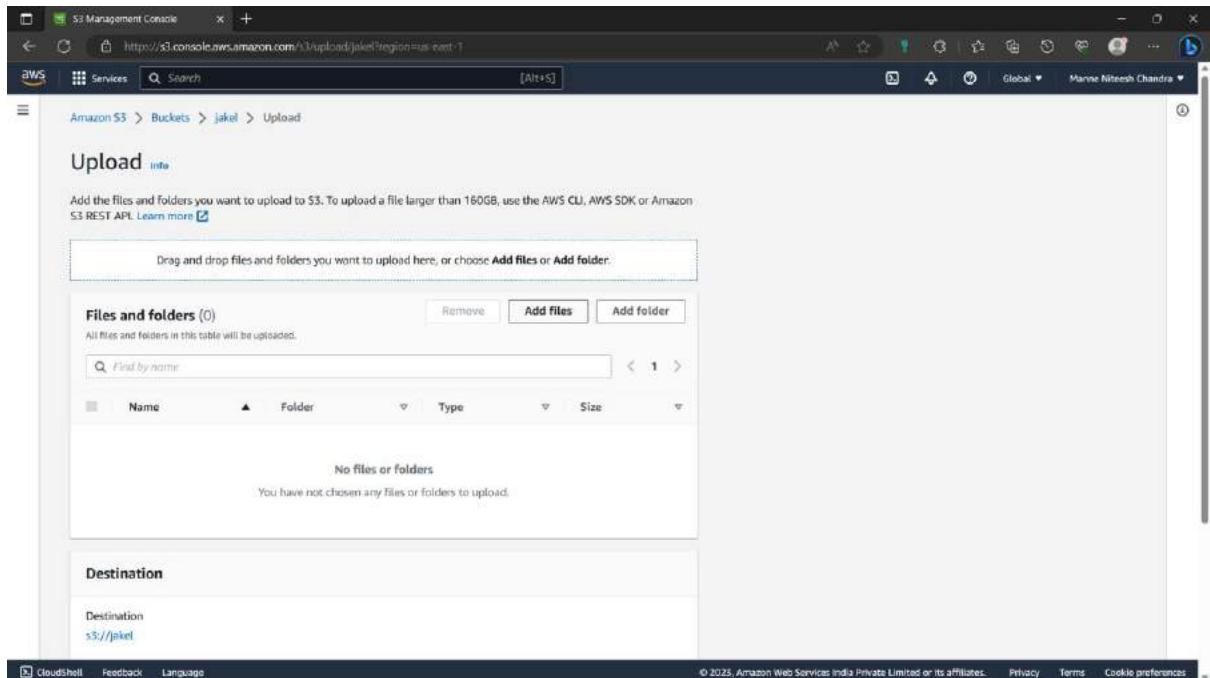
76)Now a “S3” bucket is created.

The screenshot shows the AWS S3 Management Console. A green success message at the top states "Successfully created bucket 'jakel'". Below it, the "Buckets" section displays an "Account snapshot" and a table of buckets. The table has one row for the newly created bucket "jakel", which is located in the "US East (N. Virginia) us-east-1" region and has "Bucket and objects not public" access. The table includes columns for Name, AWS Region, Access, and Creation date.

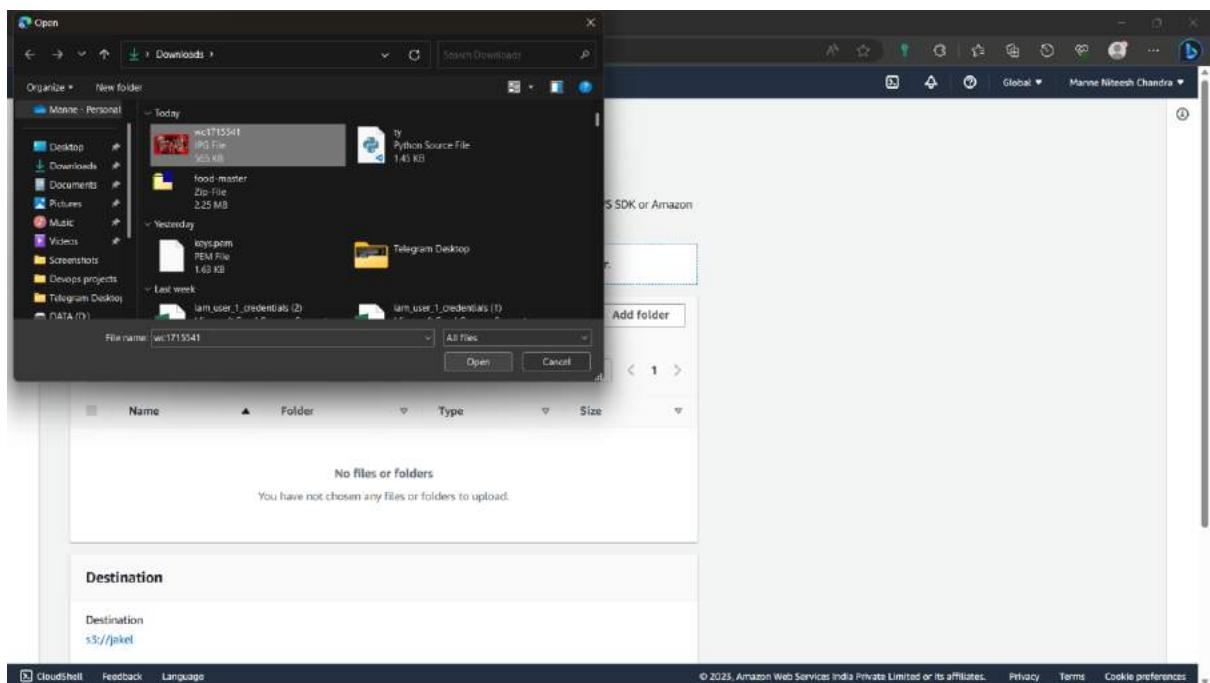
77)Now open the S3 bucket you created and click on “upload”.

The screenshot shows the AWS S3 bucket "jakel" in the "Objects" tab. At the top, there are tabs for Objects, Properties, Permissions, Metrics, Management, and Access Points. The Objects tab is selected. Below the tabs, there is a search bar and a toolbar with actions like Copy S3 URI, Copy URL, Download, Open, Delete, Actions, Create folder, and Upload. The main area shows a table with a single row labeled "No objects". Below the table, a message says "You don't have any objects in this bucket." A prominent "Upload" button is located at the bottom of the table area.

78) Click on “Add file” option.



79) A new window of local computer open to choose which file to be upload, click on the file or folder you want to upload.



80)Click on upload.

The screenshot shows the AWS S3 Management Console interface. At the top, the URL is https://s3.console.aws.amazon.com/s3/upload?bucket=jake1®ion=us-east-1. The main area has a large input field for dragging files or choosing them. Below it, a table lists one file: wc1715541.jpg, which is an image/jpeg type file of 565.1 KB. Under the heading 'Destination', the bucket s3://jake1 is selected. On the right, there are sections for 'Destination details' and 'Permissions'. At the bottom right, there are 'Cancel' and 'Upload' buttons, with 'Upload' being highlighted in orange.

81)The file has been uploaded. Click on close option at the top right.

The screenshot shows the AWS S3 Management Console after the upload was successful. A green banner at the top says 'Upload succeeded' with a link to 'View details below.' Below this, the 'Upload: status' section shows a summary table with one row: Destination s3://jake1, Status Succeeded, and Details 1 file, 565.1 KB (100.00%). The 'Files and folders' section shows the same file wc1715541.jpg with its details: Name wc1715541.jpg, Type image/jpeg, Size 565.1 KB, Status Succeeded. At the bottom right of the main content area, there is a 'Close' button.

82)Now you returned to the buckets page.

The screenshot shows the AWS S3 Management Console. The left sidebar has 'Buckets' selected. The main area shows an 'Account snapshot' with a link to 'View Storage Lens dashboard'. Below it is a table titled 'Buckets (1)'. The table has columns for Name, AWS Region, Access, and Creation date. One row is shown: 'jake1' (US East (N. Virginia) us-east-1), 'Bucket and objects not public', and 'June 12, 2023, 12:53:28 (UTC+05:30)'. There are buttons for 'Create bucket' and other actions like Copy ARN, Empty, and Delete.

83)Open the bucket you created, click on the file you uploaded.

The screenshot shows the AWS S3 Management Console for the 'jake1' bucket. The left sidebar is identical to the previous screenshot. The main area is titled 'jake1' and has tabs for Objects, Properties, Permissions, Metrics, Management, and Access Points. The 'Objects' tab is selected. A table titled 'Objects (1)' shows one item: 'scr1715541.jpg' (Type: jpg, Last modified: June 12, 2023, 12:54:17 (UTC+05:30), Size: 565.1 KB, Storage class: Standard). There are buttons for Actions (Copy S3 URI, Copy URL, Download, Open, Delete, Create folder, Upload), a search bar for 'Find objects by prefix', and a link to 'Metrics'.

84)Now copy the “Object URL” and paste it in a new window.

The screenshot shows the AWS S3 console interface. On the left, there's a sidebar with navigation links like 'Amazon S3', 'Buckets', 'Access Points', etc. The main area displays the 'wc1715541.jpg' object from the 'jakel' bucket. The 'Properties' tab is selected. Key details shown include:

- Owner:** 19pa1a04a1
- AWS Region:** US East (N. Virginia) us-east-1
- Last modified:** June 12, 2023, 12:54:17 (UTC+05:30)
- Size:** 565.1 KB
- Type:** jpg
- Key:** wc1715541.jpg
- S3 URI:** s3://jakel/wc1715541.jpg
- Amazon Resource Name (ARN):** arn:aws:s3:::jakel/wc1715541.jpg
- Entity tag (Etag):** 7915cce0c28bd157824d010b45b6058f
- Object URL:** https://jakel.s3.amazonaws.com/wc1715541.jpg

85)It shows error because we didn't assign any permissions to the file. Now we assign permission to this file.

The screenshot shows a browser window displaying an XML error response. The URL is <https://jakel.s3.amazonaws.com/wc1715541.jpg>. The error message is as follows:

```
<Error>
<Code>AccessDenied</Code>
<Message>Access Denied</Message>
<RequestId>F94MD204Q4M3HWW</RequestId>
<HostId>U0yVAA3/v1Lfp687Efmr11G98EqqDw/KrczHBLPUKCdcvXicrxTNEOrive/8h4cr9mb51s=Q/hn1Lid</HostId>
</Error>
```

86) Navigate to the permission option in the file. Click on “bucket owner enforced” option show in blue colour.

This bucket has the bucket owner enforced setting applied for Object Ownership.
When bucket owner enforced is applied, use bucket policies to control access.

Grantee	Object	Object ACL
Object owner (your AWS account) Canonical ID: 586d157155efadcc17856c0fb2bad676f2493bc1e86c6fc22ef95402a583d7e	Read	Read, Write
Everyone (public access) Group: http://acs.amazonaws.com/groups/global/AllUsers	-	-
Authenticated users group (anyone with an AWS account) Group: http://acs.amazonaws.com/groups/global/AuthenticatedUsers	-	-

87) It will navigate to Object ownership. Enable “ACLs enabled”.

Object Ownership
Control ownership of objects written to this bucket from other AWS accounts and the use of access control lists (ACLs). Object ownership determines who can specify access to objects.

ACLs disabled (recommended)
All objects in this bucket are owned by this account. Access to this bucket and its objects is specified using only policies.

ACLs enabled
Objects in this bucket can be owned by other AWS accounts. Access to this bucket and its objects can be specified using ACLs.

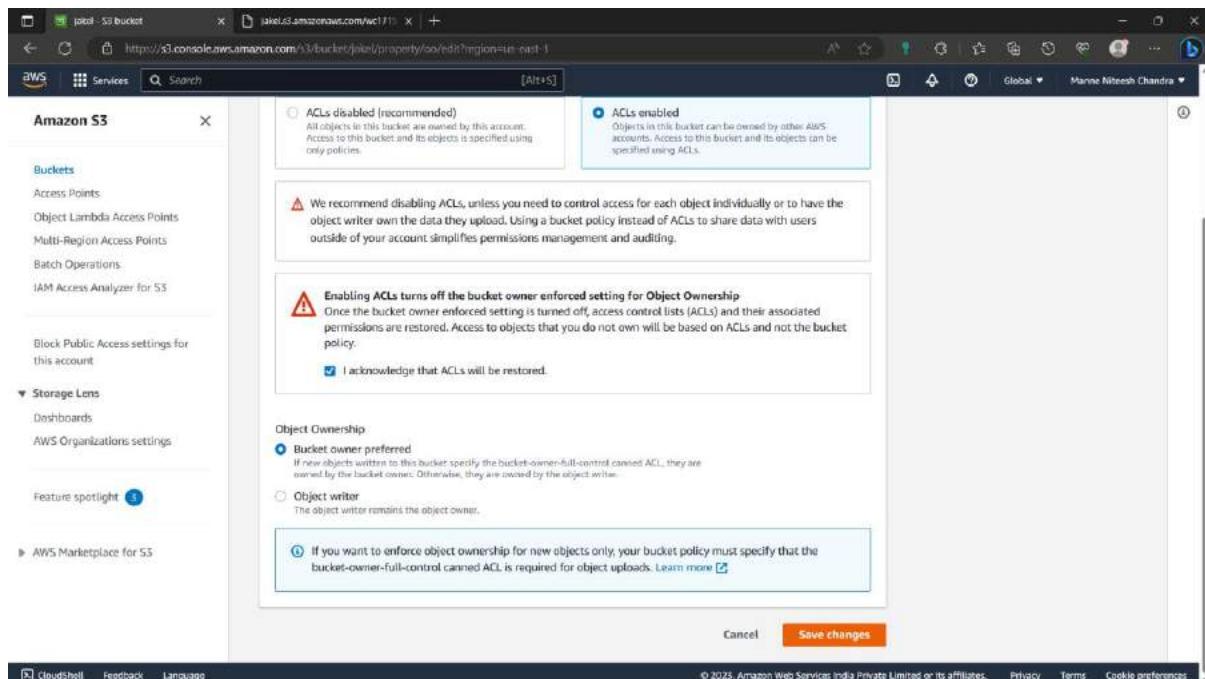
⚠ We recommend disabling ACLs, unless you need to control access for each object individually or to have the object writer own the data they upload. Using a bucket policy instead of ACLs to share data with users outside of your account simplifies permissions management and auditing.

⚠ Enabling ACLs turns off the bucket owner enforced setting for Object Ownership
Once the bucket owner enforced setting is turned off, access control lists (ACLs) and their associated permissions are restored. Access to objects that you do not own will be based on ACLs and not the bucket policy.

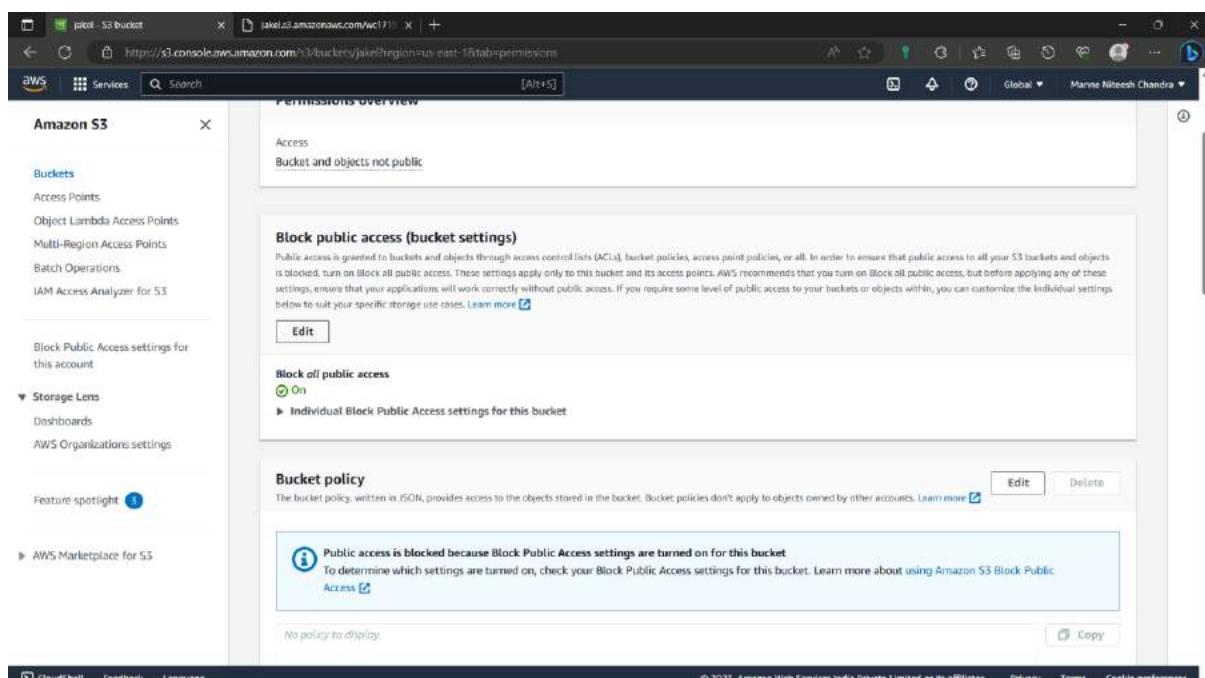
I acknowledge that ACLs will be restored.

Object Ownership
 Bucket owner preferred
If new objects written to this bucket specify the bucket-owner-full-control canned ACL, they are

88)Enable the “I acknowledge that ACLs will be restored” and click on “save changes” option.



89)Now the bucket became public. Click on edit option for “Block public access”.



90)Uncheck the “Block all public access” option and click on “save changes”.

The screenshot shows the AWS S3 console with the URL <https://s3.console.aws.amazon.com/s3/bucket/jakel/property?region=us-east-1>. The left sidebar is titled 'Amazon S3' and includes sections for Buckets, Access Points, Object Lambda Access Points, Multi-Region Access Points, Batch Operations, IAM Access Analyzer for S3, Storage Lens, Dashboards, AWS Organizations settings, Feature spotlight, and AWS Marketplace for S3. The main content area is titled 'Edit Block public access (bucket settings)' and contains a section titled 'Block public access (bucket settings)'. It explains that public access is granted through access control lists (ACLs), bucket policies, access point policies, or all. It notes that turning on 'Block all public access' will turn off all other settings. Below this, there are four checkboxes under 'Block all public access': 'Block public access to buckets and objects granted through new access control lists (ACLs)', 'Block public access to buckets and objects granted through new public bucket or access point policies', and 'Block public and cross-account access to buckets and objects through any public bucket or access point policies'. The fourth checkbox is 'Block public access to buckets and objects granted through any access control lists (ACLS)', which is currently selected. At the bottom right of the main content area are 'Cancel' and 'Save changes' buttons. A modal dialog box is overlaid on the page, containing a warning message: 'Updating the Block Public Access settings for this bucket will affect this bucket and all objects within. This may result in some objects becoming public.' It also has a 'Confirm' button and 'Cancel' buttons for both the dialog and the main page.

91)Type “confirm” and click the confirm button.

The screenshot shows the same AWS S3 console and URL as the previous image. The left sidebar and main content area are identical. The modal dialog box is still present, displaying the confirmation message: 'Updating the Block Public Access settings for this bucket will affect this bucket and all objects within. This may result in some objects becoming public.' Below this message is a text input field with the word 'Confirm' typed into it. At the bottom of the dialog are 'Cancel' and 'Confirm' buttons. The 'Confirm' button is highlighted with a blue border.

92)Now the data can be accessed by public.

The screenshot shows the AWS S3 Bucket Permissions page for the 'jake' bucket. A green success message at the top states 'Successfully edited Block Public Access settings for this bucket.' Below this, the 'Access control list (ACL)' section is displayed. It includes a note: 'The console displays combined access grants for duplicate grantees. To see the full list of ACLs, use the Amazon S3 REST API, AWS CLI, or AWS SDKs.' The ACL table lists four entries:

Grantee	Objects	Bucket ACL
Bucket owner (your AWS account) Canonical ID: 360d157135e5ad17806cd2b2bd17602493bc1e86d6c022eff95462a585d7e	List, Write	Read, Write
Everyone (public access) Group: http://acs.amazonaws.com/groups/global/AllUsers	-	-
Authenticated users group (anyone with an AWS account) Group: http://acs.amazonaws.com/groups/global/AuthenticatedUsers	-	-
S3 log delivery group Group: http://acs.amazonaws.com/groups/LogDelivery	-	-

Below the ACL section, there is a 'Cross-origin resource sharing (CORS)' configuration table with one entry:

CORS rule	Edit
Origin: *	Edit

At the bottom of the page, there are links for CloudShell, Feedback, Language, and a copyright notice: © 2023, Amazon Web Services India Private Limited or its affiliates.

93)Now go back and open the created S3 bucket.

The screenshot shows the AWS S3 Management Console. The left sidebar shows the navigation menu with 'Buckets' selected. The main content area displays an 'Account snapshot' with a note: 'Storage Lens provides visibility into storage usage and activity trends. Learn more.' Below this, a table titled 'Buckets (1)' shows the details of the 'jake' bucket:

Name	AWS Region	Access	Creation date
jake	US East (N. Virginia) us-east-1	Objects can be public	June 12, 2023, 14:33:01 (UTC+05:30)

At the bottom of the page, there are links for CloudShell, Feedback, Language, and a copyright notice: © 2023, Amazon Web Services India Private Limited or its affiliates.

94)Select the file i.e., uploaded and click on actions.

The screenshot shows the AWS S3 console interface. The top navigation bar includes tabs for 'jake - S3 bucket', '(199) AWS Service - Bucket', and 'WhatsApp'. The main title is 'Amazon S3 > Buckets > jake'. Below the title, there's a sub-header 'jake' with an 'Info' link. A horizontal menu bar contains 'Objects', 'Properties', 'Permissions', 'Metrics', 'Management', and 'Access Points'. The 'Objects' tab is selected. A sub-menu titled 'Objects (1)' is displayed, showing a table with one item: 'wc1715541.jpg' (Type: jpg, Last modified: June 12, 2023, 16:22:57 (UTC+05:30), Size: 565.1 KB, Storage class: Standard). Below the table are buttons for 'Actions', 'Create folder', and 'Upload'. A search bar labeled 'Find objects by prefix' is also present. At the bottom of the page, there are links for 'CloudShell', 'Feedback', 'Language', and copyright information: '© 2023, Amazon Web Services India Private Limited or its affiliates.' followed by 'Privacy', 'Terms', and 'Cookie preferences'.

95)Select the "Make public using ACL" option in the bottom.

This screenshot is similar to the previous one, showing the AWS S3 console for the 'jake' bucket. The 'Actions' dropdown menu is now open, revealing a list of options: 'Calculate total size', 'Copy', 'Move', 'Institute restore', 'Query with S3 Select', 'Edit actions', 'Rename object', 'Edit storage class', 'Edit server-side encryption', 'Edit metadata', 'Edit tags', and 'Make public using ACL'. The 'Make public using ACL' option is highlighted with a blue selection bar. The rest of the interface, including the table of objects and the bottom navigation links, remains the same as in the previous screenshot.

96) Click on “make public”.

The screenshot shows the 'Amazon S3 > Buckets > jakel > Make public' interface. A warning message states: 'When public read access is enabled and not blocked by Block Public Access settings, anyone in the world can access the specified objects.' Below this is a table titled 'Specified objects' showing one item: 'wc1715541.jpg' (Type: jpg, Last modified: June 12, 2023, 16:22:57 (UTC+05:30), Size: 565.1 KB). At the bottom right of the dialog is a red 'Make public' button.

97) Now the file also became public.

The screenshot shows the 'Amazon S3 > Buckets > jakel > Make public: status' page. A green success message at the top says: 'Successfully edited public access' and 'View details below.' Below this is a summary table:

Source	Successfully edited public access	Failed to edit public access
s3://jakel	1 object, 565.1 KB	0 objects

Below the summary is a tabbed section: 'Failed to edit public access' (selected) and 'Configuration'. The 'Failed to edit public access' tab shows a table with no data: 'No objects failed to edit'.

98) Now refresh the “Object URL” page we can see the image i.e., uploaded in S3 bucket.



99) Now go to the properties of your created S3 bucket. Click on edit option of “Bucket Versioning”.

Amazon S3

Buckets

Access Points

Object Lambda Access Points

Multi-Region Access Points

Batch Operations

IAM Access Analyzer for S3

Block Public Access settings for this account

Storage Lens

Dashboards

AWS Organizations settings

Feature spotlight

AWS Marketplace for S3

CloudShell Feedback Language

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

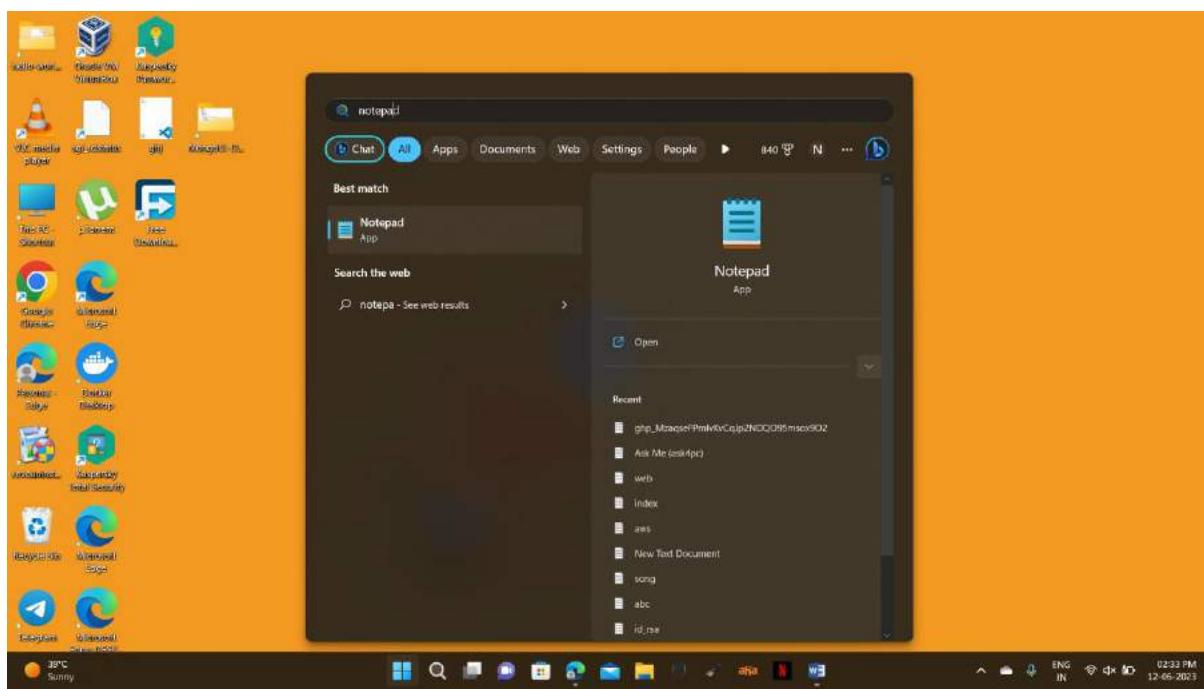
100)Select the “Enable” option and click on save changes.

The screenshot shows the 'Edit Bucket Versioning' page for the 'jakel' bucket. The 'Bucket Versioning' section has the 'Enable' radio button selected. A note below it says: 'After enabling Bucket Versioning, you might need to update your lifecycle rules to manage previous versions of objects.' At the bottom right, there are 'Cancel' and 'Save changes' buttons. The status bar at the bottom indicates '© 2023, Amazon Web Services India Private Limited or its affiliates.'

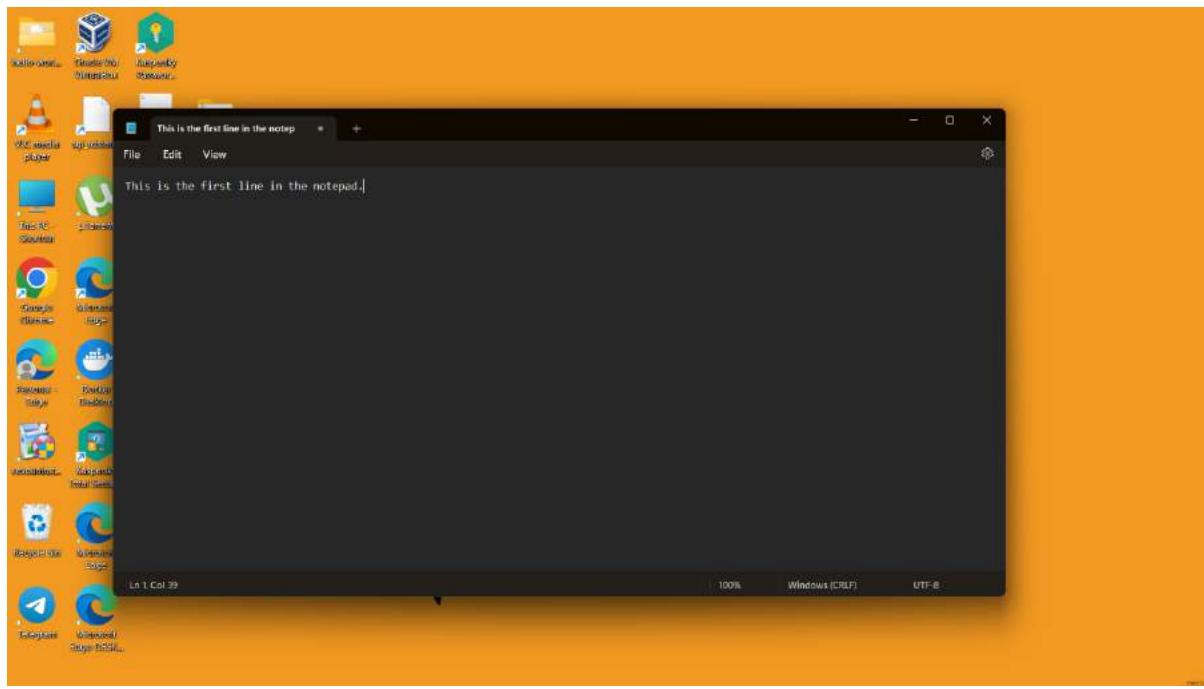
101)Now the bucket versioning is successfully edited.

The screenshot shows the 'Properties' tab of the 'jakel' bucket's properties. A green success message at the top says: 'Successfully edited Bucket Versioning. To transition, archive, or delete older object versions, configure lifecycle rules for this bucket.' Below it, the 'Bucket overview' section shows the AWS Region as 'US East (N. Virginia) us-east-1'. The 'Bucket Versioning' section shows 'Enabled'. At the bottom right, there are 'Cancel' and 'Save changes' buttons. The status bar at the bottom indicates '© 2023, Amazon Web Services India Private Limited or its affiliates.'

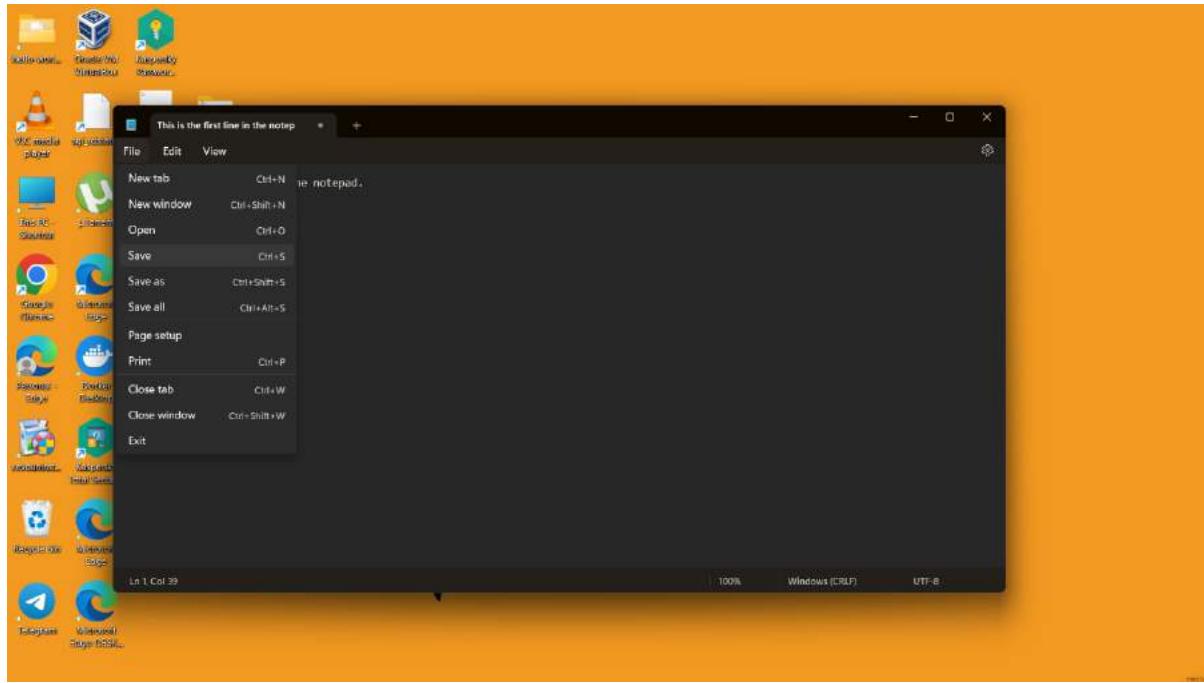
102)Now go to your local windows and open notepad.



103)Type some content(random) in the notepad.



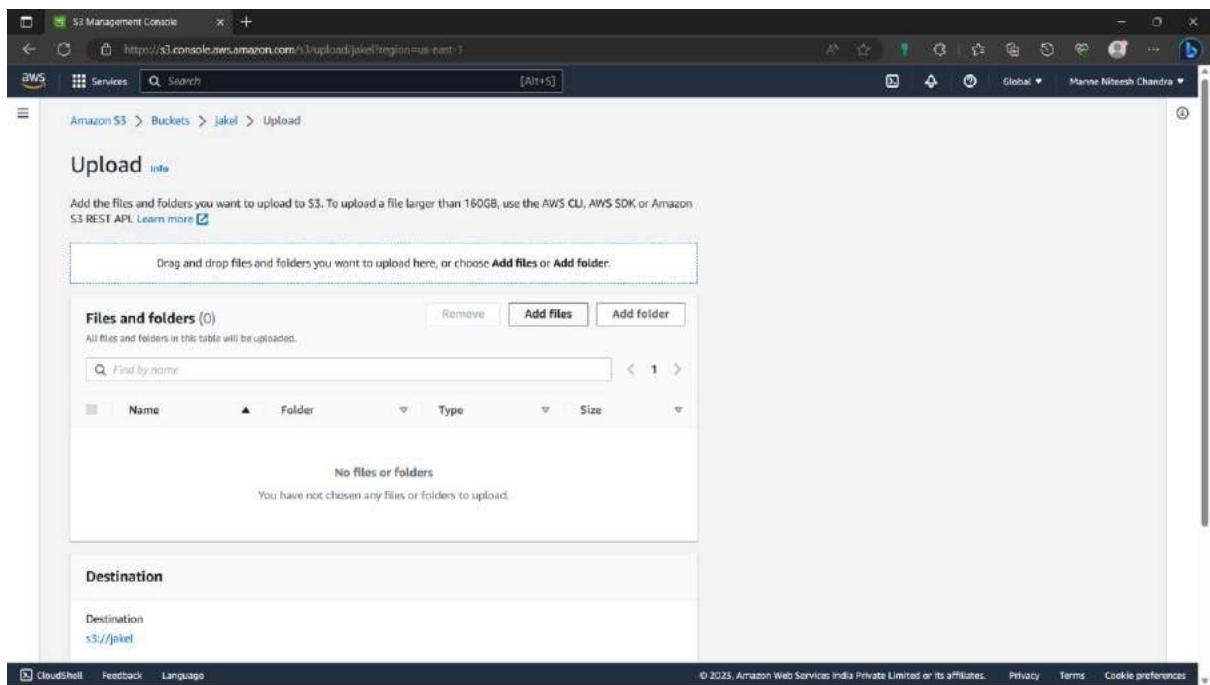
104) Save it as a text file in the windows.



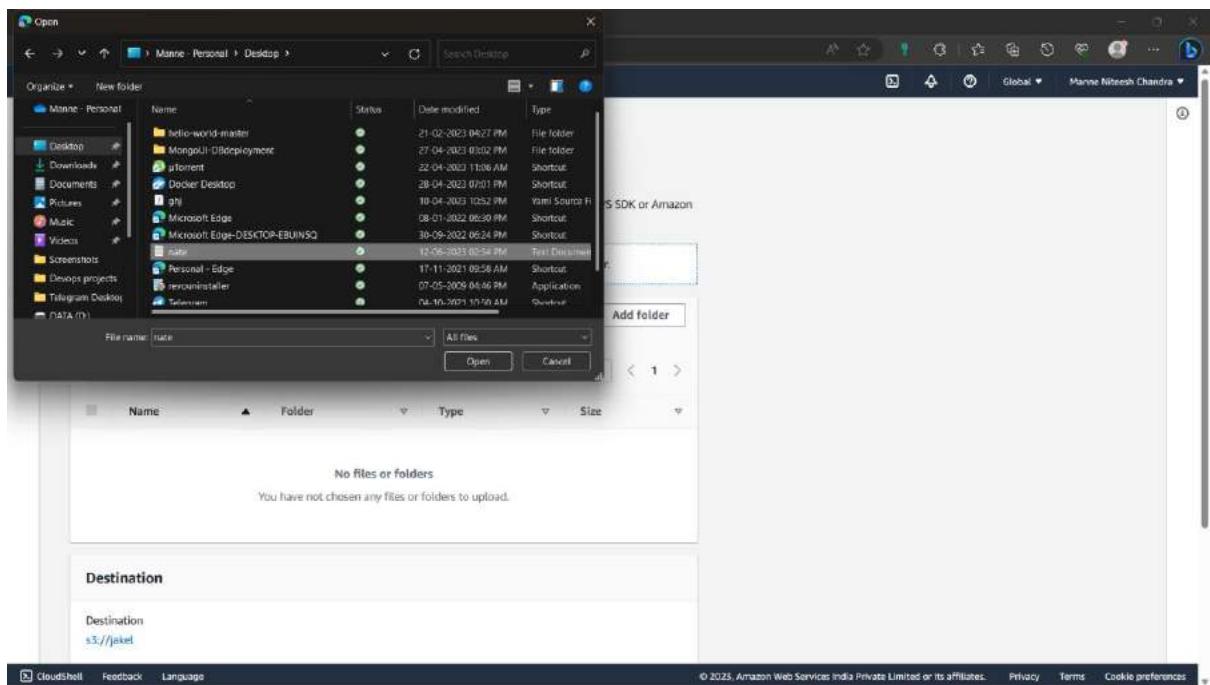
105) Go to S3 bucket you created in AWS account and click on upload.

A screenshot of the AWS S3 console. The URL in the browser is https://s3.console.aws.amazon.com/v1/buckets/jaket?region=us-east-1&tab=objects. The page shows the 'jaket' bucket under the 'Buckets' section. On the left, there's a sidebar with options like Buckets, Access Points, Object Lambda Access Points, Multi-Region Access Points, Batch Operations, IAM Access Analyzer for S3, Block Public Access settings for this account, Storage Lens, Dashboards, AWS Organizations settings, Feature spotlight, and AWS Marketplace for S3. The main content area is titled 'jaket' and shows the 'Objects' tab selected. It displays a message stating 'Objects (0)' and 'No objects'. Below this, there's a large 'Upload' button. At the bottom of the page, there are links for CloudShell, Feedback, Language, and a footer with copyright information and links for Privacy, Terms, and Cookie preferences.

106)Click on add file.



107)A new window is appeared with local files, Select the text file you created.



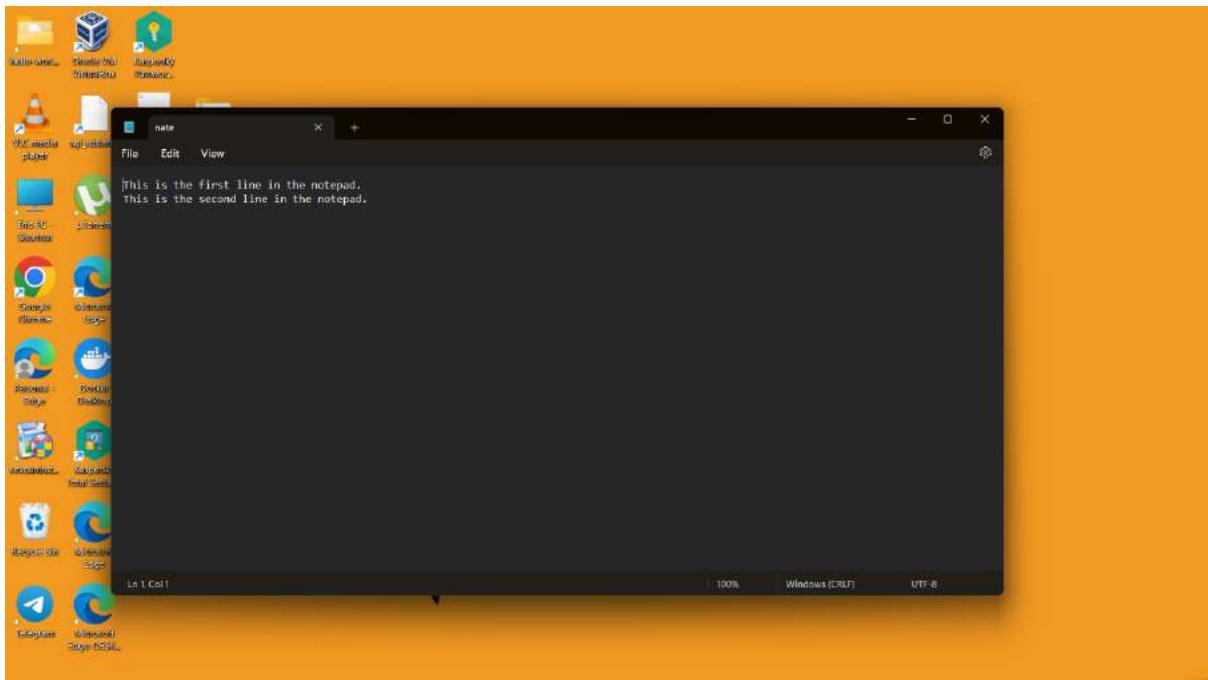
108)The text file is uploaded.

The screenshot shows the AWS S3 Management Console interface. At the top, there's a green header bar with the message "Upload succeeded". Below it, a summary table shows the destination as "s3://joket" with one succeeded file ("note.txt") and zero failed files. Under the "Files and folders" tab, a table lists the uploaded file "note.txt" with details: Name (note.txt), Folder (-), Type (text/plain), Size (38.0 B), Status (Succeeded), and Error (-). The status column includes a green checkmark icon.

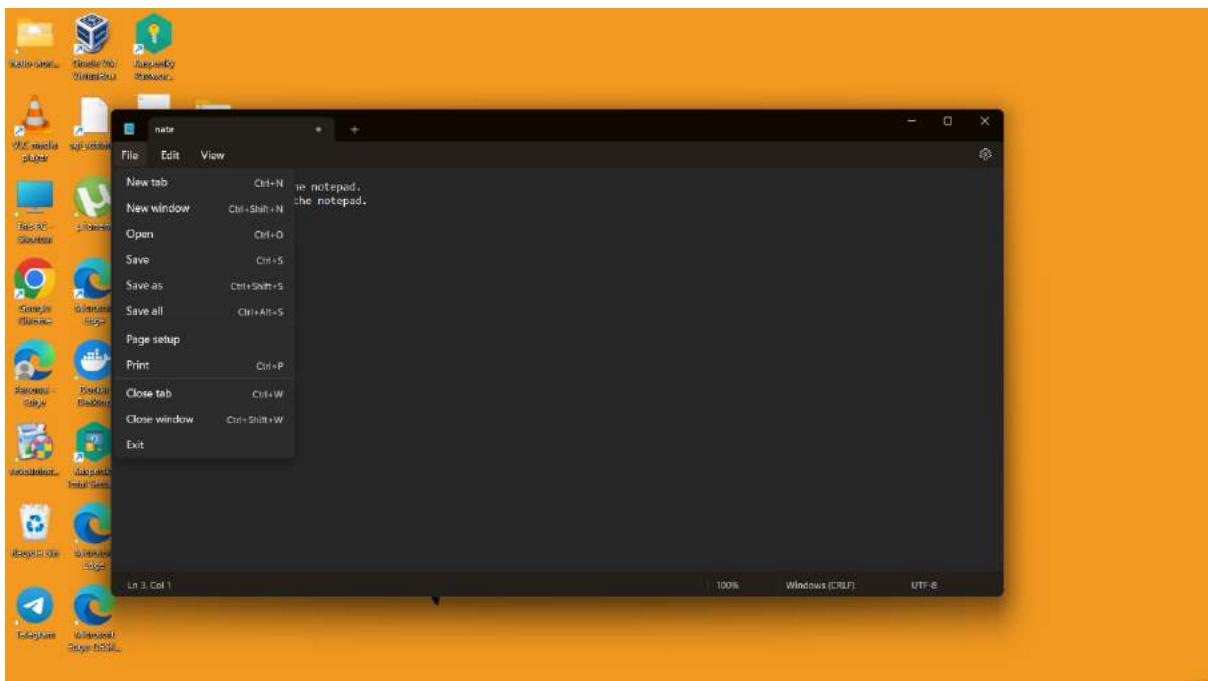
109)Now open the same text file again in the local host.



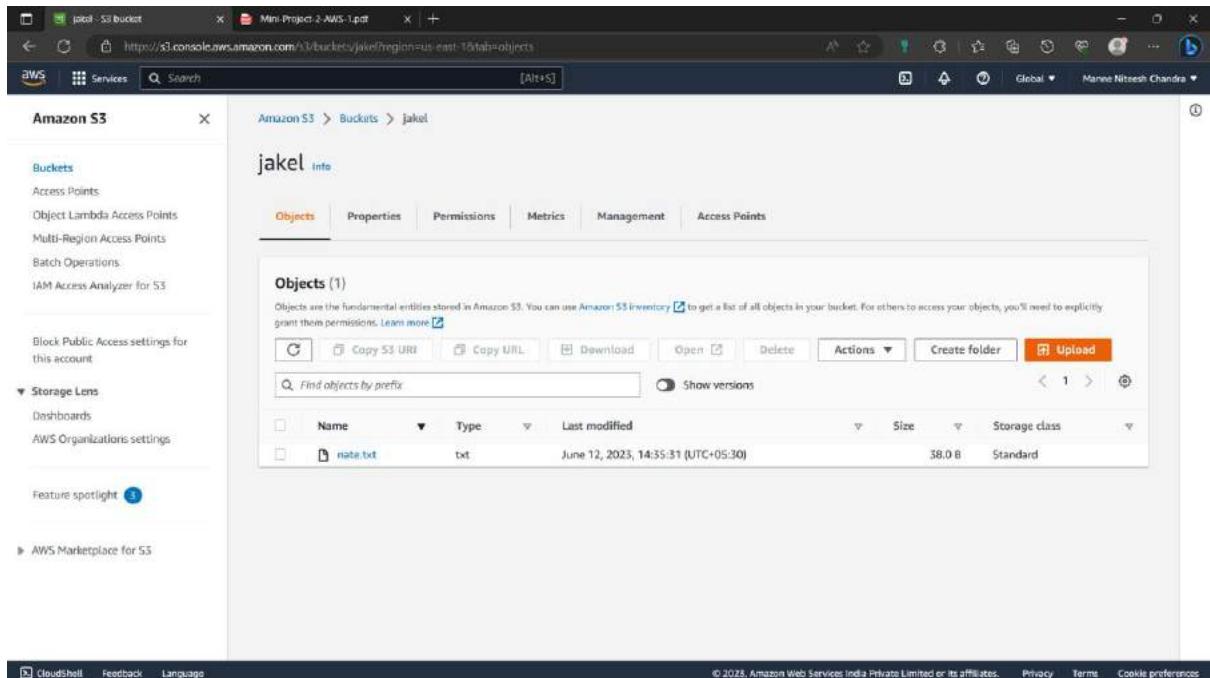
110) Before adding extra content save a copy of the current file in another path for checking purpose. Now add extra content to the file.



111) Don't change the text file name and save it.

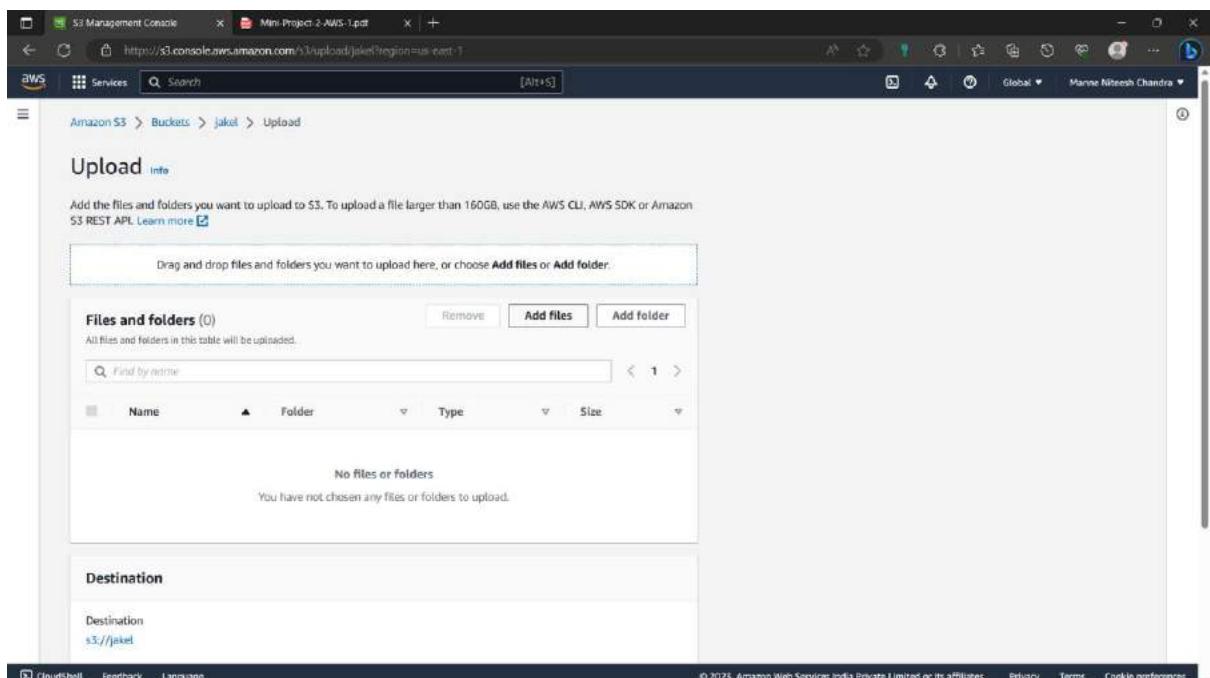


112) Now upload the file in the S3 bucket. Go to the S3 bucket you created and click on upload option.



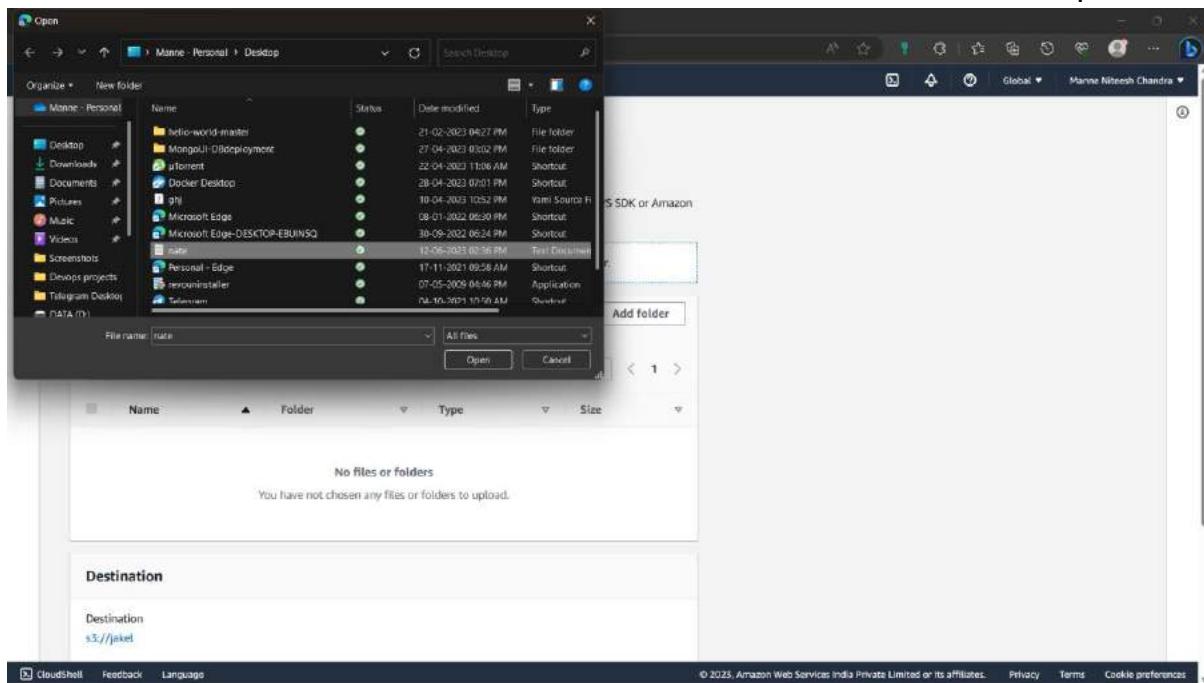
The screenshot shows the AWS S3 console interface. On the left, there's a sidebar with options like 'Buckets', 'Access Points', 'Object Lambda Access Points', 'Multi-Region Access Points', 'Batch Operations', 'IAM Access Analyzer for S3', 'Block Public Access settings for this account', 'Storage Lens', 'Dashboards', 'AWS Organizations settings', 'Feature spotlight', and 'AWS Marketplace for S3'. The main area shows the 'jakel' bucket under 'Amazon S3 > Buckets > jakel'. At the top of this area, there are tabs for 'Objects' (which is selected), 'Properties', 'Permissions', 'Metrics', 'Management', and 'Access Points'. Below the tabs, there's a search bar with placeholder text 'Find objects by prefix' and a 'Show versions' checkbox. A toolbar below the search bar includes icons for 'Copy S3 URI', 'Copy URL', 'Download', 'Open', 'Delete', 'Actions', 'Create folder', and 'Upload'. A table lists one object: 'note.txt' (Type: txt, Last modified: June 12, 2023, 14:35:31 (UTC+05:30), Size: 38.0 B, Storage class: Standard).

113) Click “Add file” option.

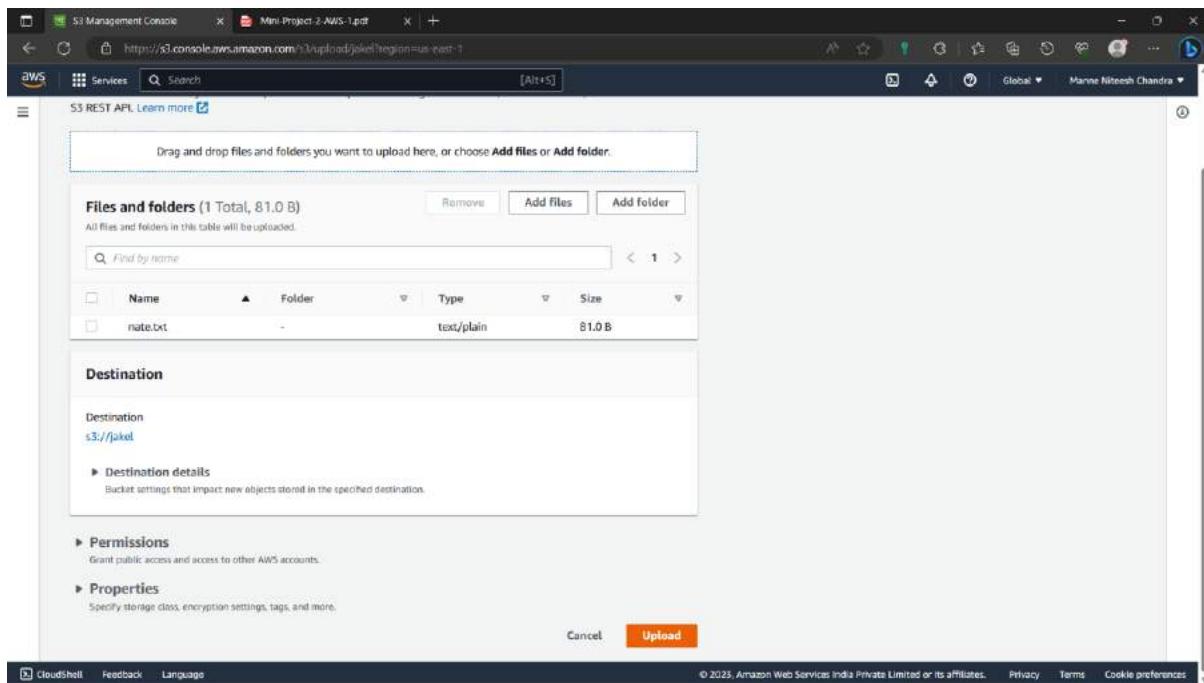


The screenshot shows the AWS S3 Management Console 'Upload' interface for the 'jakel' bucket. The top navigation bar shows 'Amazon S3 > Buckets > jakel > Upload'. The main area has a title 'Upload' with a 'info' link. Below it, a message says 'Add the files and folders you want to upload to S3. To upload a file larger than 160GB, use the AWS CLI, AWS SDK or Amazon S3 REST API.' with a 'Learn more' link. There's a large input field with placeholder text 'Drag and drop files and folders you want to upload here, or choose Add files or Add folder.' Below this is a section titled 'Files and folders (0)' with a note 'All files and folders in this table will be uploaded.' It includes a search bar 'Find by name' and a table with columns 'Name', 'Folder', 'Type', and 'Size'. The table displays the message 'No files or folders' and 'You have not chosen any files or folders to upload.' At the bottom, there's a 'Destination' section with a dropdown menu set to 's3://jakel'.

114)Now a new window with local files will be opened select the file i.e., content is upadated.



115)Click on “upload” option.



116)Now the files has been uploaded successfully.

The screenshot shows the AWS S3 Management Console with a green header bar indicating 'Upload succeeded'. Below it, a summary table shows one file uploaded to the 'jakes' bucket. A table below lists the uploaded file 'note.txt' with its details: Name, Folder, Type, Size, Status, and Error. The status is marked as 'Succeeded'.

Files and folders (1 Total, 81.0 B)						
Name	Folder	Type	Size	Status	Error	
note.txt	-	text/plain	81.0 B	Succeeded	-	

117)Rather than the files showing separately it shows only the current updated file.

The screenshot shows the AWS S3 Management Console with the 'Objects' tab selected. It displays a single object named 'note.txt' with its details: Name, Type, Last modified, Size, and Storage class. The file was last modified on June 12, 2023, at 14:35:31 (UTC+05:30) and is 38.0 B in size, stored in the Standard storage class.

Name	Type	Last modified	Size	Storage class
note.txt	txt	June 12, 2023, 14:35:31 (UTC+05:30)	38.0 B	Standard

118)Now click on the “show older version”. It will show the older file i.e., first updated file. the files are arranged like this because of bucket versioning option. The current version means the file which is currently is updated and using.

A screenshot of a web browser displaying the AWS S3 console. The URL in the address bar is <https://s3.console.aws.amazon.com/s3/object/jake1?region=us-east-1&prefix=nate.txt&tab=versions>. The page shows the 'nate.txt' file in the 'jake1' bucket. The 'Versions' tab is selected. A table lists two versions of the file:

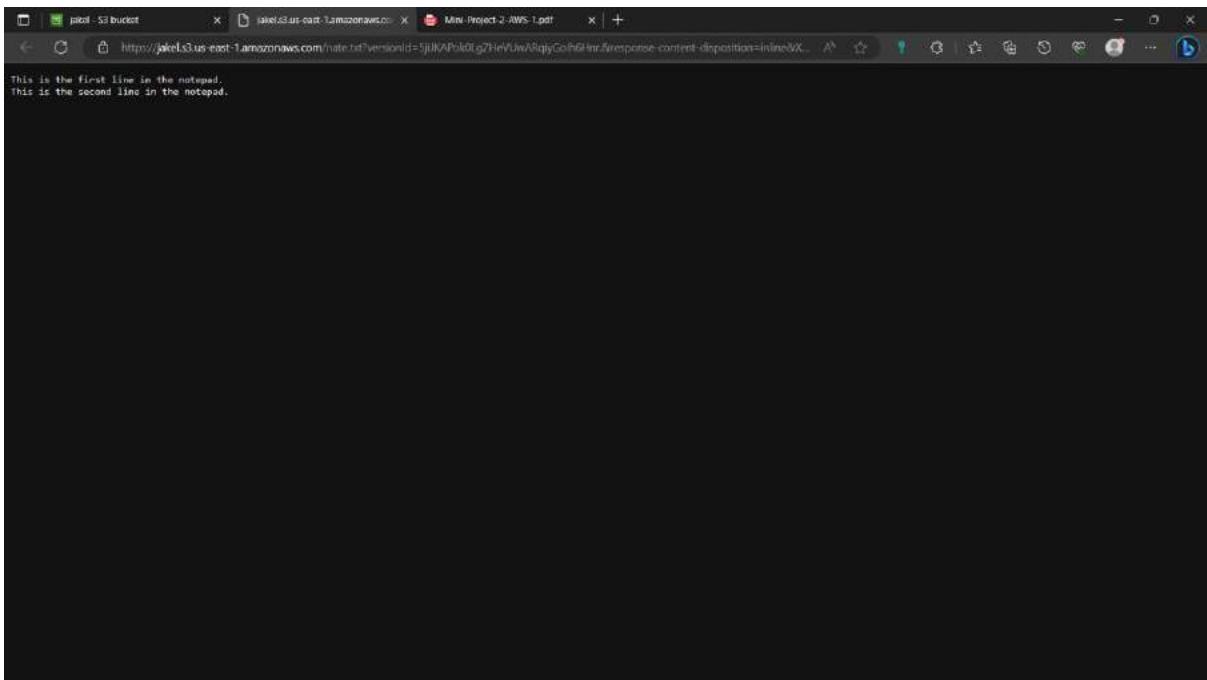
Version ID	Type	Last modified	Size	Storage class
5jUkAPokOLgZHeVUwARqiyGolh6Hn (Current version)	txt	June 12, 2023, 14:57:58 (UTC+05:30)	81.0 B	Standard
Nb8qUPK04Nh6AjOPVcqv6R3nfhZchaf	txt	June 12, 2023, 14:35:31 (UTC+05:30)	38.0 B	Standard

119)Now check the contents of both the files. Using the object URL. The first uploaded file content is shown below. Check it with your local text file where you save the copy in a different path. If you get error while openinh this file in new window repeat the steps (86-98).

A screenshot of a web browser showing the content of the 'nate.txt' file. The URL in the address bar is <https://jake1.s3.us-east-1.amazonaws.com/nate.txt?versionId=Nb8qUPK04Nh6AjOPVcqv6R3nfhZchaf&response-content-disposition=inline&response-content-type=text/plain>. The page displays the text 'This is the first line in the notepad.'

120) Now check the contents of the second uploaded file.

Now

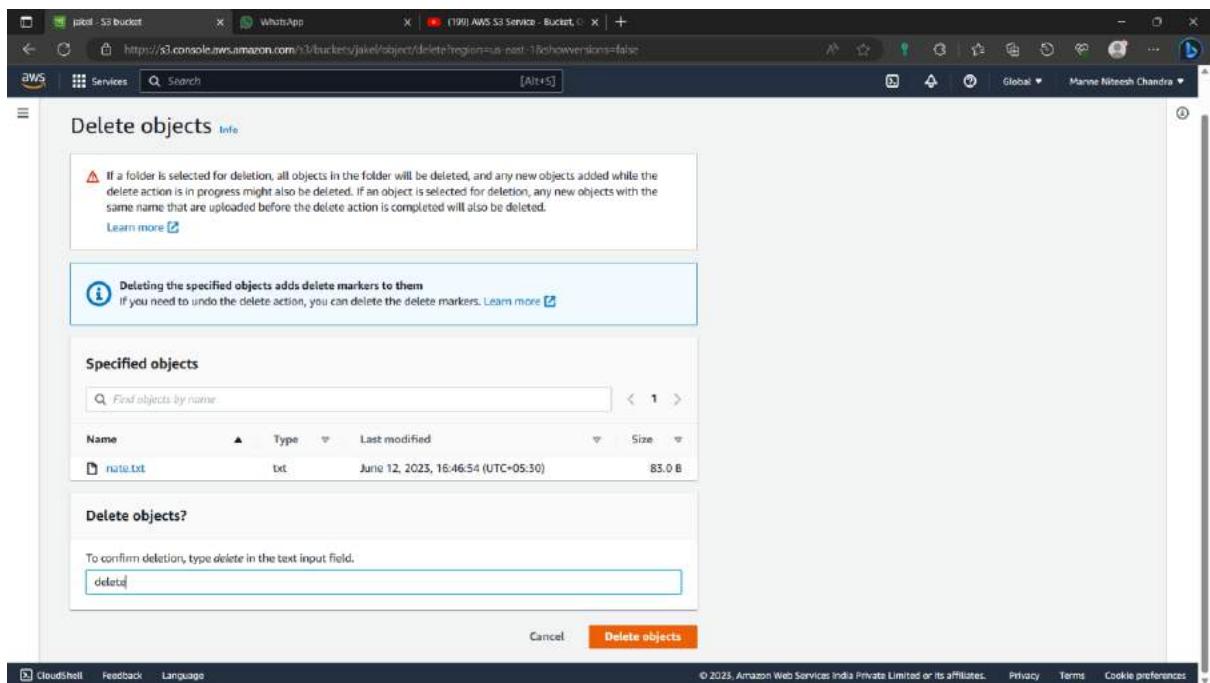


121) Now go to object of file in the S3 bucket. Select the file created and click on delete option.

The screenshot shows the AWS S3 console interface. The top navigation bar includes tabs for 'CloudShell', 'Feedback', 'Language', 'AWS S3 Service', 'Bucket', and 'Objects'. The main area displays the 'Objects' tab for the 'jake1' bucket. A single object, 'nate.txt', is listed in the table below. The 'Delete' button is visible in the toolbar above the table, indicating it can be used to remove the selected file.

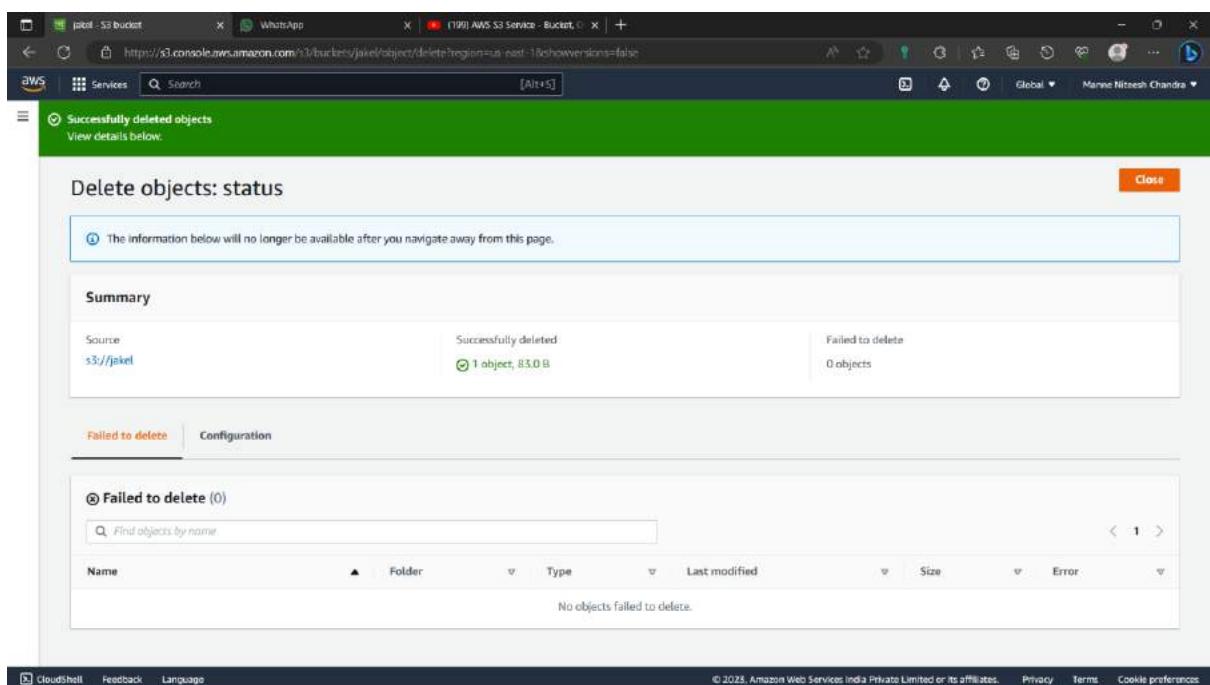
Name	Type	Last modified	Size	Storage class
nate.txt	txt	June 12, 2023, 16:46:54 (UTC+05:30)	83.0 B	Standard

122) Type “delete” and click on “delete object” option.



The screenshot shows the AWS S3 console with a single file named 'nate.txt' selected for deletion. The 'Delete objects?' step is active, and the word 'delete' is typed into the confirmation input field. The 'Delete objects' button is visible at the bottom right.

123) Now the files are deleted.



The screenshot shows the AWS S3 console after a successful delete operation. A green header bar indicates 'Successfully deleted objects'. The 'Delete objects: status' section shows a summary table with one successfully deleted object and zero failed deletions. The 'Failed to delete' tab is selected, showing an empty table with a note: 'No objects failed to delete.'

124) Even though the files are deleted because of bucket versioning they won't be deleted permanently. Go to objects in the S3 bucket you created. Click on "Show versions".

The screenshot shows the AWS S3 console interface. On the left, there's a sidebar with options like Buckets, Access Points, Storage Lens, and Feature spotlight. The main area is titled 'jakel' and shows the 'Objects' tab selected. A message at the top says 'Objects (0)' and 'No objects'. Below it is a search bar labeled 'Find objects by prefix' and a 'Show versions' button. At the bottom, there's a table header with columns: Name, Type, Last modified, Size, and Storage class. A note below the table says 'You don't have any objects in this bucket.' There are also 'Upload' and 'Actions' buttons.

125) Now we can see a marker file(Copy of the original file) and the two text files.

This screenshot shows the same AWS S3 console as the previous one, but with the 'show versions' option selected. The main area now displays 'Objects (3)'. The table shows three entries:

Name	Type	Version ID	Last modified	Size	Storage class
note.txt	Delete marker	Y2RmNNQSRMVkpyV5FM4FmjS8Et6roF7n	June 12, 2023, 16:47:53 (UTC+05:30)	0 B	-
note.txt	txt	7wa2OfeM3CnD2.suMloYbm56udV5xs	June 12, 2023, 16:46:54 (UTC+05:30)	83.0 B	Standard
note.txt	txt	null	June 12, 2023, 16:45:00 (UTC+05:30)	42.0 B	Standard

126)By deleting the marker file we can restore both the files. Select the marker file and click on delete option.

The screenshot shows the AWS S3 console interface. On the left, there's a sidebar with options like 'Buckets', 'Access Points', 'Object Lambda Access Points', etc. The main area shows the 'Objects' tab for the 'jakel' bucket. There are three objects listed:

Name	Type	Version ID	Last modified	Size	Storage class
nate.txt	Delete marker	Y2RnNNQSRMVKpyV5FM4FmjS8Et6roF7n	June 12, 2023, 16:47:53 (UTC+05:30)	0 B	-
nate.txt	txt	7wa2OfeM3CnD2.suMoYbmS6udV5xs	June 12, 2023, 16:46:54 (UTC+05:30)	83.0 B	Standard
nate.txt	null		June 12, 2023, 16:45:00 (UTC+05:30)	42.0 B	Standard

127)Type “permanently delete” and click on “delete object” option.

The screenshot shows the 'Delete objects' dialog. It includes a warning message about deleting a folder, a table of specified objects, and a confirmation step.

Warning:

- If a folder is selected for deletion, all objects in the folder will be deleted, and any new objects added while the delete action is in progress might also be deleted. If an object is selected for deletion, any new objects with the same name that are uploaded before the delete action is completed will also be deleted.
- Deleting the specified objects can't be undone.

Specified objects:

Name	Version ID	Type	Last modified	Size
nate.txt	Y2RnNNQSRMVKpyV5FM4FmjS8Et6roF7n	Delete marker	June 12, 2023, 16:47:53 (UTC+05:30)	0 B

Permanently delete objects?

To confirm deletion, type **permanently delete** in the text input field.

Delete objects

128) Now can see that both the deleted files are restored after deleting the marked file.

The screenshot shows the AWS S3 console interface. The top navigation bar includes tabs for 'jaked - S3 Bucket', 'WhatsApp', and '(199) AWS S3 Service - Bucket'. The main content area is titled 'jakel' and shows the 'Objects' tab selected. A table lists two objects:

Name	Type	Version ID	Last modified	Size	Storage class
nate.txt	txt	7wg2OfeM3CnD2suMloYb.mS6udVSxs	June 12, 2023, 16:46:54 (UTC+05:30)	83.0 B	Standard
nate.txt	txt	null	June 12, 2023, 16:45:00 (UTC+05:30)	42.0 B	Standard

EC2 Instance:

129) Type “EC2” in the search bar and select the “EC2” option below.

The screenshot shows the AWS Management Console search results for 'EC2'. The search bar at the top contains 'EC2'. The left sidebar shows various AWS services and features. The 'Services' section is expanded, and 'EC2' is selected, showing its details: 'Virtual Servers in the Cloud'. Other listed services include EC2 Image Builder, Amazon Inspector, and AWS Firewall Manager. The right sidebar displays a 'Started with AWS' section with links to fundamental concepts and certification information.

130) Click on “Launch instance” option to create an EC2 instance.

The screenshot shows the AWS EC2 Management Console Dashboard. On the left, there's a sidebar with various navigation options like EC2 Dashboard, Instances, Images, and Elastic Block Store. The main area has sections for Resources (Instances running: 0, Auto Scaling Groups: 0, Dedicated Hosts: 0; Elastic IPs: 0, Instances: 0, Key pairs: 1; Load balancers: 0, Placement groups: 0, Security groups: 2; Snapshots: 0, Volumes: 0), Service health (Region: US East (N. Virginia), Status: This service is operating normally), and Account attributes (Supported platforms: VPC, Default VPC: vpc-0b7c25909d5dbfae). A central box titled "Launch instance" contains buttons for "Launch instance" and "Launch instance From template". Below it is a "Scheduled events" section for "US East (N. Virginia)". On the right, there's an "Explore AWS" sidebar with links for "Save up to 90% on EC2 with Spot Instances", "Enable Best Price-Performance with AWS Graviton2", and "Get Up to 40% Better Price Performance".

131) Give a name to the instance.

The screenshot shows the "Launch an instance" wizard. It starts with a "Launch an instance" summary step, followed by the "Name and tags" step where "Ubuntu Server" is entered. Then it moves to the "Application and OS Images (Amazon Machine Image)" step, which lists "Amazon Linux 2023 AMI 2023.0.2...read more" and "ami-0badae173da580765". The next step is "Quick Start", showing a grid of OS options: Amazon Linux, macOS, Ubuntu, Windows, Red Hat, and SUSE. A search bar at the top says "Search our full catalog including 1000s of application and OS images". Finally, the "Summary" step shows a "Free tier" message: "In your first year includes 750 hours of t2.micro (or t3.micro in the Regions in which t2.micro is unavailable) instance usage on free tier AMIs per month, 30 GiB of EBS storage, 2 million IOPS, 1 GiB of snapshots, and 100 GiB of bandwidth to the internet." It includes "Cancel", "Launch instance", and "Review commands" buttons.

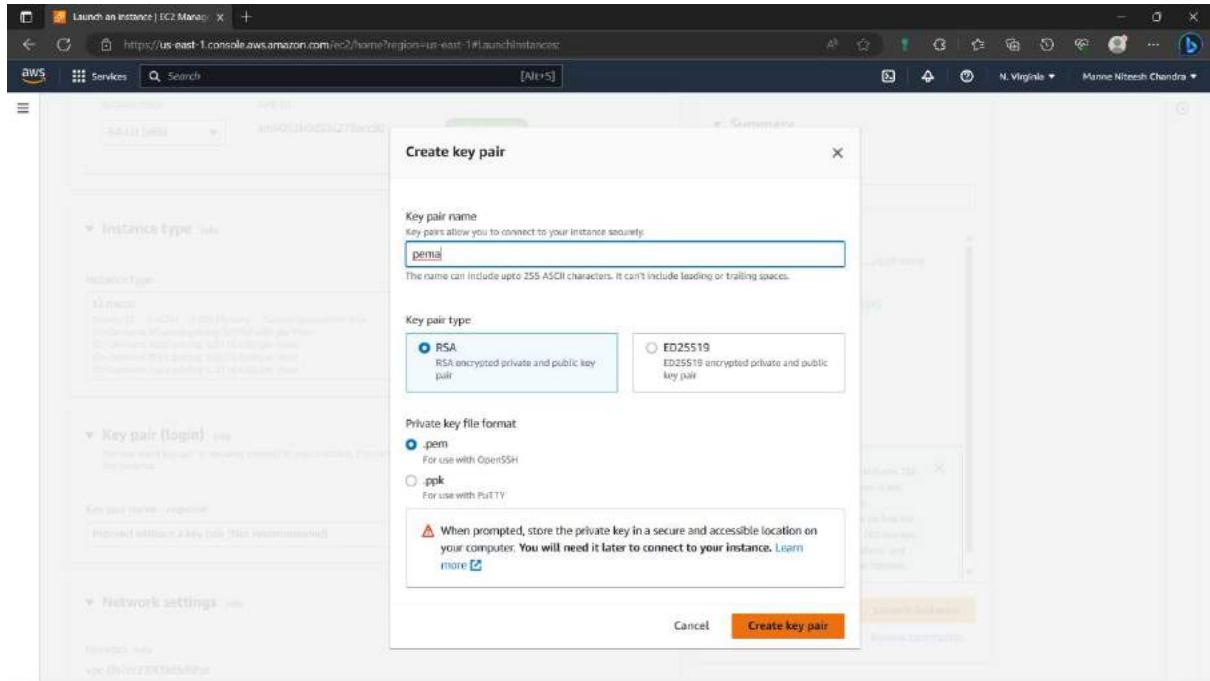
132)Select the AMI- Ubuntu OS, Description(default), Architecture(default), Am ID(default).

The screenshot shows the AWS EC2 Launch Instance wizard. In the left sidebar, under 'Application and OS Images (Amazon Machine Image)', the 'ubuntu' image is selected. The main panel displays the 'Ubuntu Server 22.04 LTS (HVM, SSD Volume Type)' AMI details. The 'Architecture' dropdown is set to '64-bit (x86)'. The 'AMI ID' is 'ami-053b0d53c279acc90'. A 'Verified provider' badge is present. On the right, the 'Summary' section shows 'Number of instances' set to 1. The 'Software Image (AMI)' is 'Canonical, Ubuntu, 22.04 LTS, ...'. The 'Virtual server type (instance type)' is 't2.micro'. A tooltip for 'Free tier' indicates it includes 750 hours of t2.micro usage in specific regions. At the bottom right are 'Launch instance' and 'Review commands' buttons.

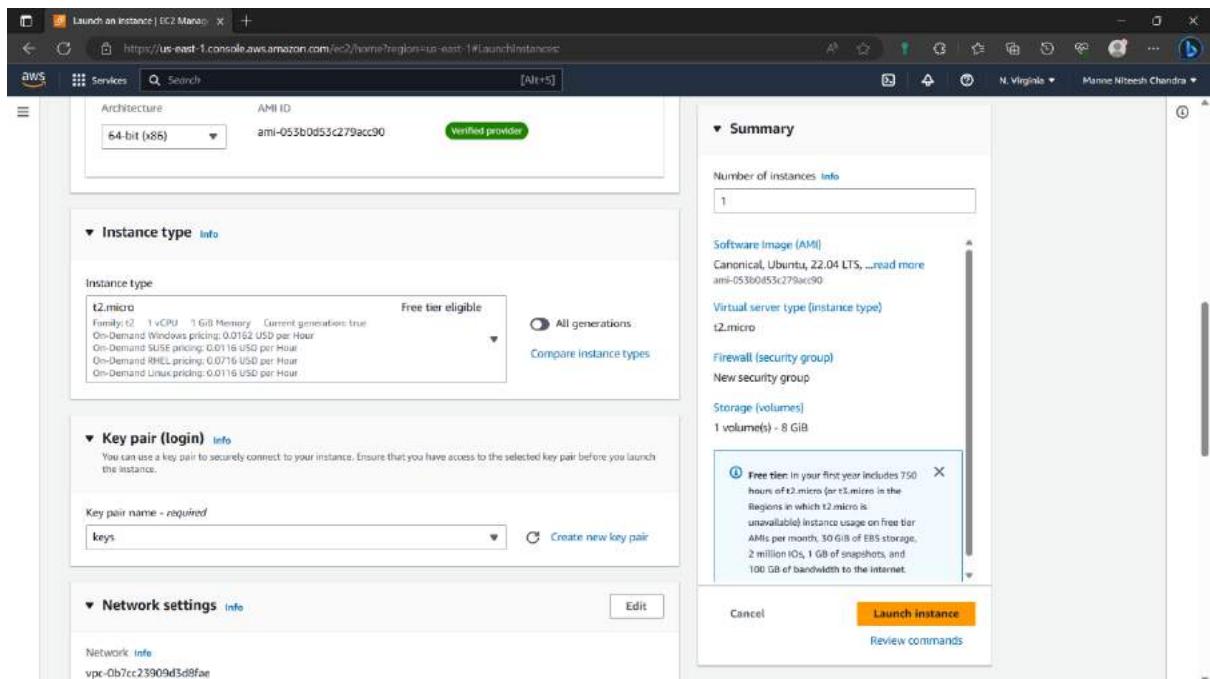
133)Select the instance type-t2.micro.

The screenshot shows the AWS EC2 Launch Instance wizard. The 'Instance type' section is open, showing the 't2.micro' option selected. The 'AMI ID' is 'ami-053b0d53c279acc90'. A 'Verified provider' badge is present. The 'Key pair (login)' section is expanded, showing the 't2.micro' key pair. A tooltip for 'Free tier' indicates it includes 750 hours of t2.micro usage in specific regions. At the bottom right are 'Launch instance' and 'Review commands' buttons.

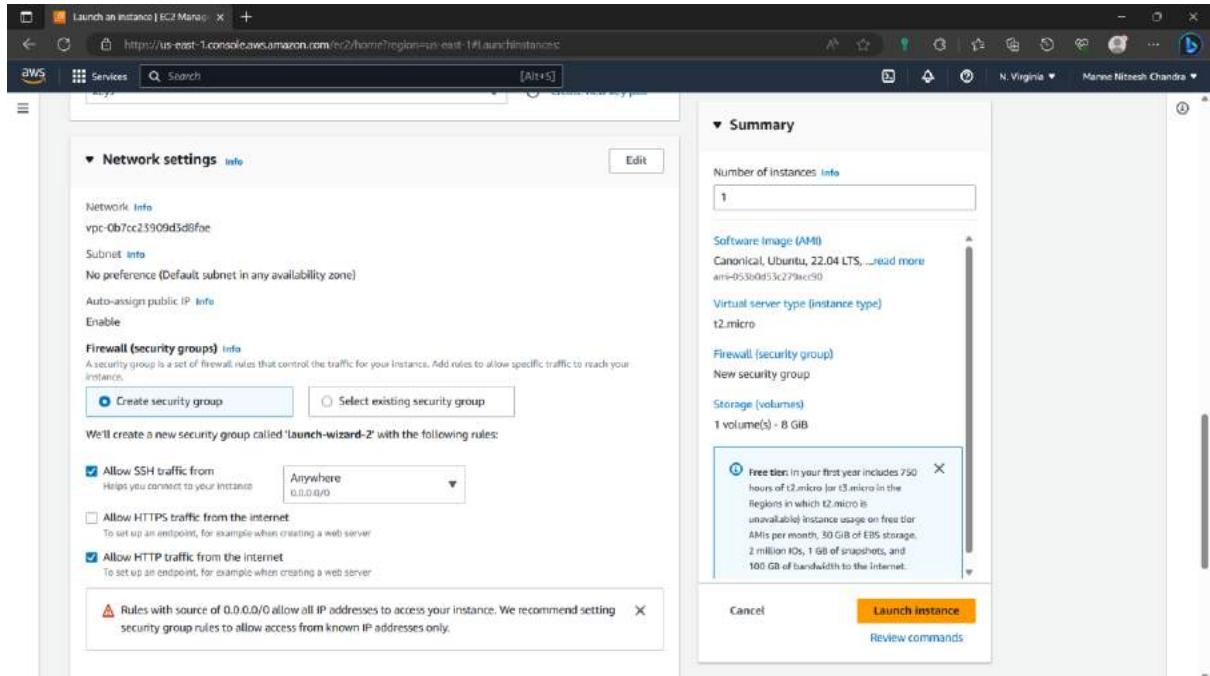
134) If you have the key pair select the key pair you have. Else click on “Create a new key pair” option. Give a name of your choice and click on “create key pair”.



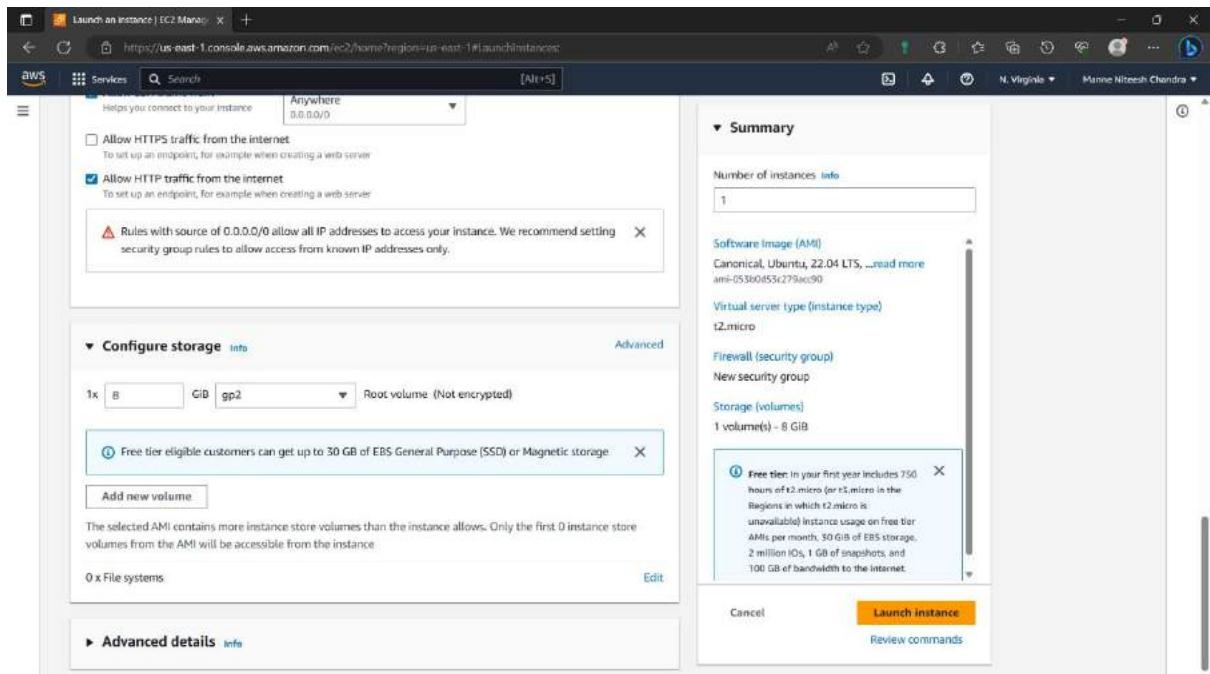
135) Now a copy of key pair is downloaded to the local system. And select the key pair you created in the system.



136)Enable the “HTTP Traffic” option in the network settings. So that it can be accessed through the URL.



137)Review all the details you given in the summary and click on “Launch instance” option to create the instance.



138)Now the instance is created.

The screenshot shows the AWS EC2 "Launch an Instance" page. At the top, there is a success message: "Successfully initiated launch of instance [i-09f22d6ef9c90dafe]". Below this, there is a "Launch log" link. Under the "Next Steps" section, there are several options:

- Create billing and free tier usage alerts
- Connect to your instance
- Connect an RDS database
- Create EBS snapshot policy
- Manage detailed monitoring
- Create Load Balancer
- Create AWS budget
- Manage CloudWatch alarms

139)Now go to the instances. We can see the created instance. Wait till the Instance state- Running, Status type -2/2 checks passed.

The screenshot shows the AWS EC2 "Instances" management interface. On the left, there is a sidebar with navigation links like EC2 Dashboard, EC2 Global View, Events, Limits, Instances, Images, and Elastic Block Store. The main area displays a table of instances:

Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone	Public IPv4 DNS
Ubuntu Server	i-09f22d6ef9c90dafe	Running	t2.micro	initializing	No alarms	us-east-1c	ec2-54-239-122-

A modal window titled "Select an instance" is open at the bottom, listing the instance "Ubuntu Server".

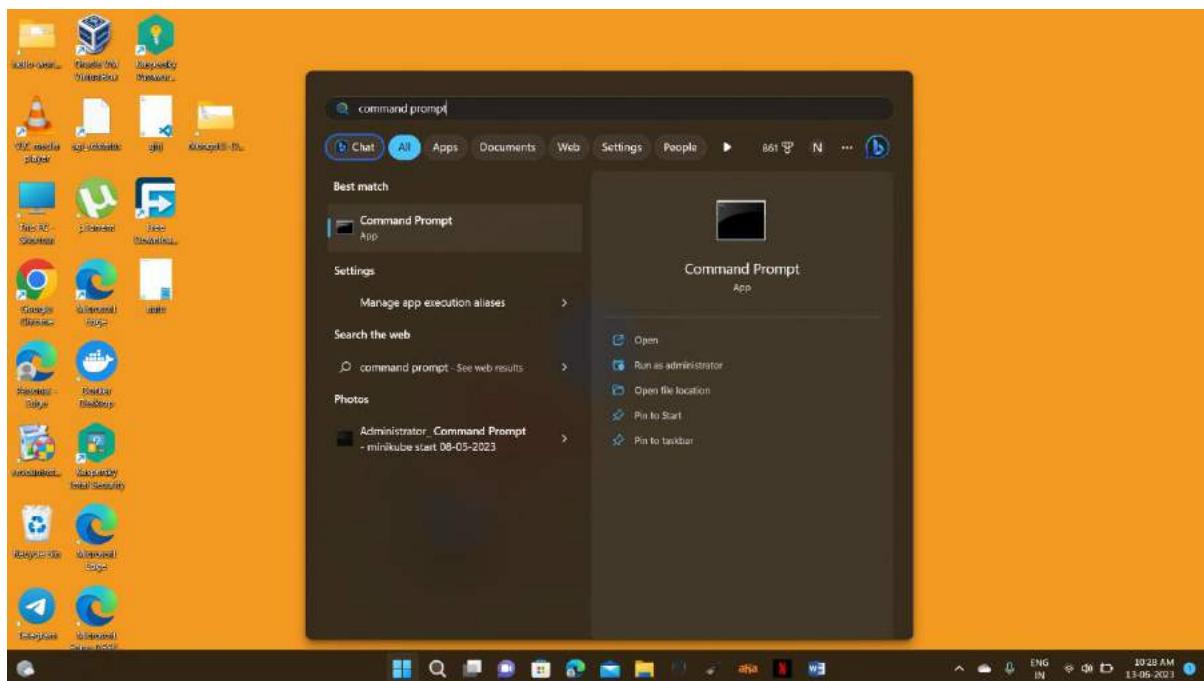
140) Refresh the instance, now the instance is ready. Select the created instance click on “connect”.

The screenshot shows the AWS EC2 Management Console. The left sidebar is collapsed. The main area displays a table of instances. One instance is selected: "Ubuntu Server" (Instance ID: i-09f22d6ef9c90date). The instance is listed as "Running" with the status check "2/2 checks passed". Below the table, a detailed view for the selected instance is shown. The "Details" tab is selected, displaying information such as Instance ID (i-09f22d6ef9c90date), Public IPv4 address (34.239.122.241), Instance state (Running), and Hostname type (IP name: ip-172-31-82-125.ec2.internal). The "SSH client" tab is also visible in the navigation bar at the bottom of the detailed view.

141) We are going to access the instance through local machine. Browse to “SSH client” option and copy the command below the “Example”.

The screenshot shows the "Connect to instance" dialog box. The "SSH client" tab is selected. It displays instructions for connecting to the instance using an SSH client. It includes steps like opening an SSH client, locating the private key file (keys.pem), running chmod 400 keys.pem, and connecting using the Public DNS (ec2-34-239-122-241.compute-1.amazonaws.com). An "Example" section shows the command: ssh -i "keys.pem" ubuntu@ec2-34-239-122-241.compute-1.amazonaws.com. A note at the bottom states: "Note: In most cases, the guessed user name is correct. However, read your AMI usage instructions to check if the AMI owner has changed the default AMI user name." A "Cancel" button is at the bottom right.

142)Open the command prompt in your local machine.



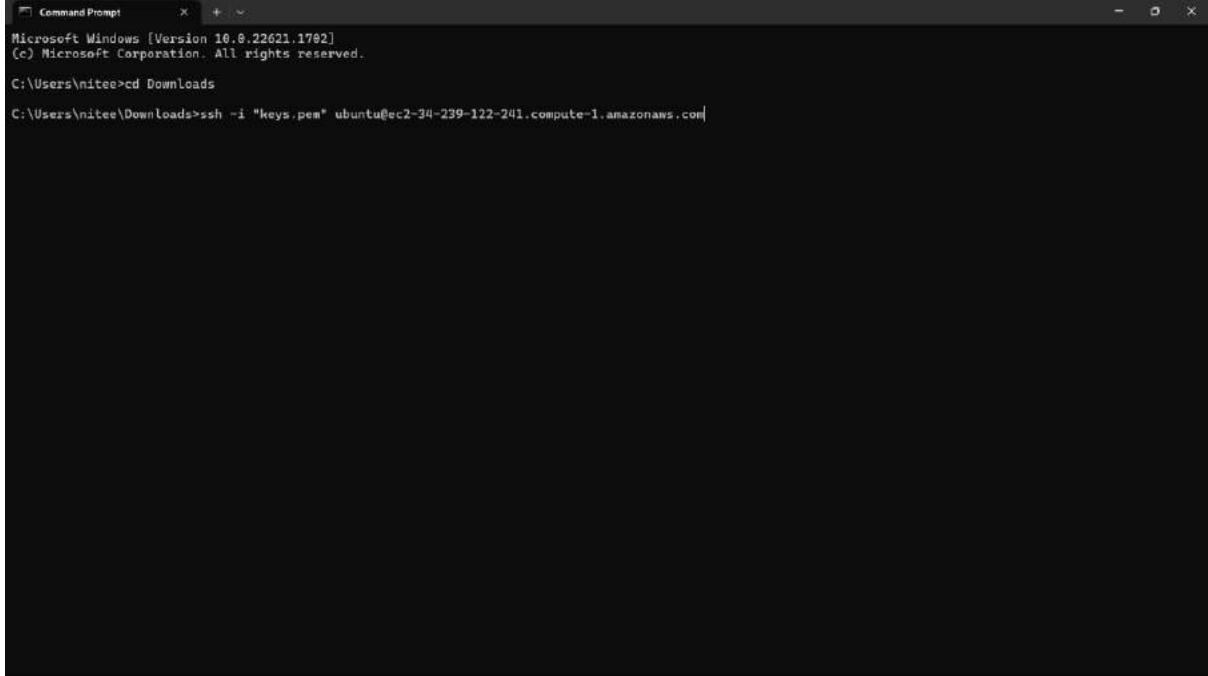
143)Type the command – “cd path” path-Where the key pair is located in my local system the key pair is in downloads so my command- “cd downloads”.

```
Microsoft Windows [Version 10.0.22621.1702]
(c) Microsoft Corporation. All rights reserved.

C:\Users\nitee>cd Downloads
C:\Users\nitee\Downloads>
```

A screenshot of a Command Prompt window titled 'Command Prompt'. The window shows the command 'cd Downloads' being entered and the resulting directory change to 'C:\Users\nitee\Downloads>'. The background of the window is dark, and the text is white.

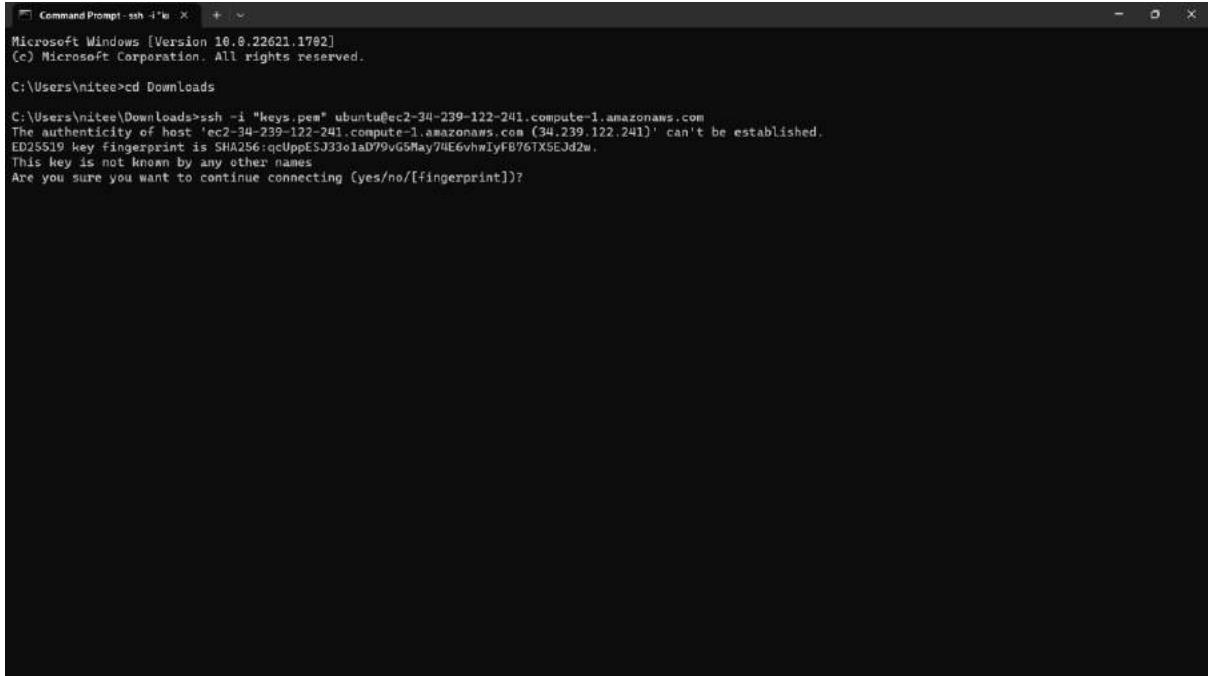
144)Now paste the command you copied in “step-141”(because it is the command which is used to connect with the instance locally and key pair is the middleman between the ec2 at AWS and ec2 in the command prompt) and click on enter.



```
Command Prompt
Microsoft Windows [Version 10.0.22621.1702]
(c) Microsoft Corporation. All rights reserved.

C:\Users\nitee>cd Downloads
C:\Users\nitee\Downloads>ssh -i "keys.pem" ubuntu@ec2-34-239-122-241.compute-1.amazonaws.com
```

145)type “yes” click enter button in the keyboard.



```
Command Prompt - ssh -i "keys.pem"
Microsoft Windows [Version 10.0.22621.1702]
(c) Microsoft Corporation. All rights reserved.

C:\Users\nitee>cd Downloads
C:\Users\nitee\Downloads>ssh -i "keys.pem" ubuntu@ec2-34-239-122-241.compute-1.amazonaws.com
The authenticity of host 'ec2-34-239-122-241.compute-1.amazonaws.com (34.239.122.241)' can't be established.
ED25519 key fingerprint is SHA256:qcUppESJ33olaD79vG5May74E6vhvIyFB76TXSEJd2w.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])?
```

146)Now the instance is created in your local system.

```
ubuntu@ip-172-31-82-125:~ % 
C:\Users\nitee\Downloads>ssh -i "keys.pem" ubuntu@ec2-34-239-122-241.compute-1.amazonaws.com
The authenticity of host 'ec2-34-239-122-241.compute-1.amazonaws.com (34.239.122.241)' can't be established.
ED25519 key fingerprint is SHA256:qcUppE5J33olaD79vG5May74E6vhwIyFB76TX5EJd2w.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added 'ec2-34-239-122-241.compute-1.amazonaws.com' (ED25519) to the list of known hosts.

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

System information as of Tue Jun 13 05:06:05 UTC 2023

System load: 0.8      Processes:         95
Usage of /: 20.6% of 7.59GB  Users logged in:   0
Memory usage: 25%          IPv4 address for eth0: 172.31.82.125
Swap usage:  0%

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-172-31-82-125:~ |
```

Security Group:

147)Go to the search bar in AWS and type “VPC”, Click the “VPC” option.

The screenshot shows the AWS Management Console search results for 'VPC'. The search bar at the top contains 'vpd'. The results are categorized into 'Services' and 'Features'.

- Services** (12):
 - VPC (Isolated Cloud Resources)
 - AWS Firewall Manager (Central management of firewall rules)
 - Detective (Investigate and analyze potential security issues)
 - Managed Services (IT operations management for AWS)
- Features** (48):
 - Dashboard (VPC feature)
 - VPC Reachability Analyzer (VPC feature)

A sidebar on the right displays a 'AWS' widget with links to 'Getting started with AWS', 'Fundamentals', 'AWS certification', and 'AWS News'.

148) In the navigation panel below on the left side in “security” there is “security group” option, click on the “security group” option.

The screenshot shows the AWS VPC Management Console. On the left, a navigation sidebar lists various VPC resources under 'Virtual private cloud' and 'Security'. The 'Security groups' link is highlighted with a yellow box. The main content area displays a grid of resource cards for VPCs, NAT Gateways, Subnets, Route Tables, Internet Gateways, Egress-only Internet Gateways, DHCP option sets, Elastic IPs, Managed prefix lists, Endpoints, Endpoint services, NAT gateways, Peering connections, and Security Groups. The 'Security Groups' card is also highlighted with a yellow box. On the right, there are sections for 'Service Health', 'Settings', 'Additional Information', and 'AWS Network Manager'.

149) Click on “create security group” option at top right corner in yellow colour.

The screenshot shows the AWS VPC Management Console with the 'Security Groups' page open. The left sidebar shows the 'Security groups' link is selected. The main area displays a table of existing security groups with columns for Name, Security group ID, Security group name, VPC ID, Description, and Owner. A new row is being added, indicated by a dashed border. At the top right of the table, a yellow-highlighted 'Create security group' button is visible.

150) Give name to the security group (you can identify it easily among all the security groups) let the VPC be default. Click add rule in inbound rule add 2 rules

- i) Type- SSH, port-20, IP range-0.0.0.0/28, Description(your choice).
- ii) Type-HTTP, port-80, IP range-0.0.0.0/28, Description(your choice).

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

Basic details

Security group name: mynewSG
Description: Security Group
VPC: vpc-0b7cc25909d3d8fse

Inbound rules

Type	Protocol	Port range	Source	Description - optional
SSH	TCP	22	Custom	0.0.0.0/28
HTTP	TCP	80	Custom	0.0.0.0/28

Add rule

151) Click on “create security group”.

HTTP inbound rule
0.0.0.0/28

HTTP inbound rule
0.0.0.0/28

Outbound rules

Type	Protocol	Port range	Destination	Description - optional
All traffic	All	All	Custom	0.0.0.0/0

Add rule

Tags - optional

No tags associated with the resource.

Add new tag

Create security group

152)The security group is created.

The screenshot shows the AWS VPC Management Console. A green banner at the top indicates that a security group was created successfully. The main page displays the details of the security group 'sg-0976be0e482c6ef37 - mynewSG'. The 'Details' section shows the security group name, ID, owner, and rule counts. Below this, there are tabs for 'Inbound rules' (selected), 'Outbound rules', and 'Tags'. A note suggests checking network connectivity with the Reachability Analyzer, with a 'Run Reachability Analyzer' button. The left sidebar lists various VPC management options like Subnets, Route tables, and Security groups. The bottom of the screen includes standard AWS navigation links like CloudShell, Feedback, and Language.

153)Go to search bar type “EC2” and select the “EC2” instance option.

The screenshot shows the AWS Management Console search results for 'EC2'. The search bar at the top has 'EC2' typed into it. The results are categorized into 'Services' and 'Features'. Under 'Services', 'EC2' is listed as 'Virtual Servers in the Cloud'. Other services like EC2 Image Builder, Amazon Inspector, and AWS Firewall Manager are also shown. Under 'Features', 'Dashboard' and 'Limits' are listed, both containing an 'EC2 feature'. On the right side of the screen, there is a sidebar with links related to AWS fundamentals, certification, and getting started.

154)Click on “Instance(running)” option.

The screenshot shows the AWS EC2 Management Console. On the left, there's a navigation sidebar with options like EC2 Dashboard, Instances, Images, and Elastic Block Store. The main area is titled "Resources" and displays a summary of Amazon EC2 resources in the US East (N. Virginia) Region. It shows 1 instance running, 0 Auto Scaling Groups, 0 Dedicated Hosts, 0 Elastic IPs, 1 instance, 1 Key pair, 0 Load balancers, 0 Placement groups, 4 Security groups, 0 Snapshots, and 1 Volumes. Below this, there's a "Launch instance" section with a "Launch instance" button and a "Migrate a server" link. To the right, there's a "Service health" section showing "Region: US East (N. Virginia)" and "Status: This service is operating normally". Further down, there's a "Scheduled events" section for the "US East (N. Virginia)" region. On the far right, there's an "Account attributes" panel with sections for Supported platforms (VPC), Default VPC (vpc-0b7c23909d5d8fae), Settings, EBS encryption, Zones, EC2 Serial Console, Default credit specification, and Console experiments. At the bottom, there's an "Explore AWS" section with links for EC2 instances and AWS Graviton2.

155)Select the instance you created in steps(131-138) and click “Actions”→“Security”→“change security group”.

The screenshot shows the AWS EC2 Management Console on the "Instances" page. The left sidebar has the same navigation as before. The main area shows a table of instances with one entry: "Ubuntu Server" (i-09f22d6ef9c90daf). The "Actions" dropdown menu for this instance is open, and the "Change security groups" option is highlighted. Below the table, there's a detailed view for the selected instance, showing its security group (sg-0976be0e482c6ef37) and inbound rules. The bottom of the screen shows standard AWS footer links.

156) Remove the security group i.e., assigned default.

The screenshot shows the 'Change security groups' interface for an EC2 instance. In the 'Associated security groups' section, the 'default' security group is listed with its ID 'sg-07140d8125bd3eedf'. A 'Remove' button is visible next to it. Below the table, there are 'Cancel' and 'Save' buttons. The search bar at the top contains the placeholder 'Select security groups'.

157) In search bar of “Associated security group” select the security group we created (Steps:149-152).

The screenshot shows the 'Change security groups' interface for an EC2 instance. The search bar at the top contains the text 'mynewSG'. Below the search bar, a list of security groups is displayed, including 'mynewSG (sg-09f76be0e482c6ef57)', 'mynewSG (sg-09f76be0e482c6ef57)', 'default (sg-01bb7d320a46b5be)', 'default', 'Launch-wizard-1 (sg-0ddf074ee8b1f25174)', 'Launch-wizard-1', 'Launch-wizard-2 (sg-07140d8125bd3eedf)', and 'Launch-wizard-2'. The 'Save' button is visible at the bottom right.

158) Click on “Add security group”.

The screenshot shows the AWS EC2 console with the URL [https://us-east-1.console.aws.amazon.com/ec2/home?region=us-east-1#ChangeSecurityGroup\\$instanceId=i-09f22d6ef9c90date](https://us-east-1.console.aws.amazon.com/ec2/home?region=us-east-1#ChangeSecurityGroup$instanceId=i-09f22d6ef9c90date). The page title is "Change security groups". The "Associated security groups" section contains a search bar with the value "sg-0976be0e482c6ef57" and an "Add security group" button. Below the search bar, it says "Security groups associated with the network interface (eni-09dc0be4ab980d33c)". A table lists one security group: "mynewSG" with "sg-0976be0e482c6ef57". There are "Cancel" and "Save" buttons at the bottom.

159) Click on “save” option.

The screenshot shows the same AWS EC2 console and URL as the previous screenshot. The "Associated security groups" section now shows the "mynewSG" security group that was added. The "Save" button is highlighted in orange at the bottom of the page.

160)Now the security group is added to the instance.

The screenshot shows the AWS EC2 Management Console. On the left, there's a navigation sidebar with options like EC2 Dashboard, EC2 Global View, Events, Limits, Instances (selected), Images, and Elastic Block Store. The main area displays a table of instances. One instance, "Ubuntu Server" (i-09f22d6ef9c90daf), is selected and shown in more detail. The "Security" tab is active in the instance details panel. Under "Security details", it shows the IAM Role and Owner ID. Under "Security groups", it lists "sg-0976be0e482c6ef37 (inynewSG)". Below that, the "Inbound rules" section is visible, showing a table with columns for Name, Security group rule ID, Port range, Protocol, Source, and Security groups.

161)You can check it by selecting the security group assigned ec2 instance and navigate to the “security” option of the instance. In security we can see the assigned security group in “security group” option.

This screenshot is identical to the one above, showing the AWS EC2 Management Console. The "Instances" tab is selected in the sidebar. A single instance, "Ubuntu Server" (i-09f22d6ef9c90daf), is selected. The "Security" tab is active in the instance details panel. It shows the IAM Role, Owner ID, and the assigned security group "sg-0976be0e482c6ef37 (inynewSG)". The "Inbound rules" section is also visible.

Volume and Snapshot:

162) Type “EC2” in the search bar and select the “EC2” option below.

The screenshot shows the AWS Management Console search results for 'EC2'. The search bar at the top contains the query 'EC2'. Below it, the 'Services' section lists several items, with 'EC2' being the first and highlighted in orange. Other listed items include EC2 Image Builder, Amazon Inspector, and AWS Firewall Manager. The 'Features' section also lists EC2 under 'EC2 feature'. To the right of the search results, there is a sidebar with various AWS-related links such as 'Getting started with AWS', 'AWS Fundamentals', 'AWS certification', and 'AWS白皮书'.

163) Select volumes in “Elastic block store” i.e., bottom of the navigation panel of the EC2 instance.

The screenshot shows the AWS EC2 Management console. The left sidebar has a tree view with 'Instances' expanded, showing 'Volumes' as a child node. The main 'Resources' section displays various EC2 metrics like Instances (running), Auto Scaling Groups, Dedicated Hosts, etc. The 'Volumes' section shows 1 volume. The 'Service health' section indicates that the service is operating normally. The 'Explore AWS' section includes links to GuardDuty Malware Protection and 10 Things You Can Do Today to Reduce AWS Costs.

163) Click on “create volume”.

The screenshot shows the AWS EC2 Management Console with the URL <https://us-east-1.console.aws.amazon.com/ec2/home?region=us-east-1#Volumes>. The left sidebar is collapsed. The main area displays a table titled "Volumes (1) Info" with one row. The row contains the following information:

Name	Volume ID	Type	Size	IOPS	Throughput	Snapshot	Created
-	vol-0a2ae54b18469205a	gp2	8 GiB	100	-	-	2023/06/13 13:59 GMT+5:30

Below the table, there is a message: "Select a volume above". At the top right of the main area, there is a "Create volume" button. The bottom of the screen shows standard AWS navigation links: CloudShell, Feedback, Language, Privacy, Terms, and Cookie preferences.

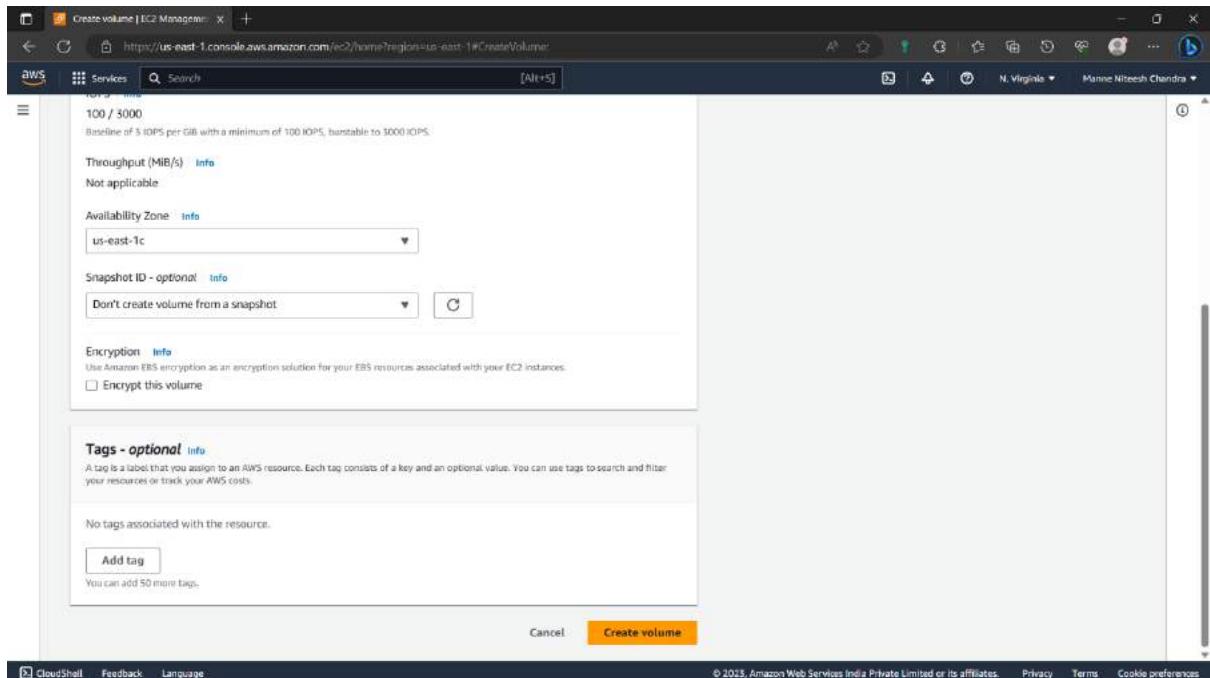
164) Size-5GB, the availability zone of the volume should be in the same zone as instance.

The screenshot shows the AWS EC2 Management Console with the URL <https://us-east-1.console.aws.amazon.com/ec2/home?region=us-east-1#CreateVolume>. The left sidebar shows "EC2 > Volumes > Create volume". The main area is titled "Create volume" with a "Volume settings" section. The settings are as follows:

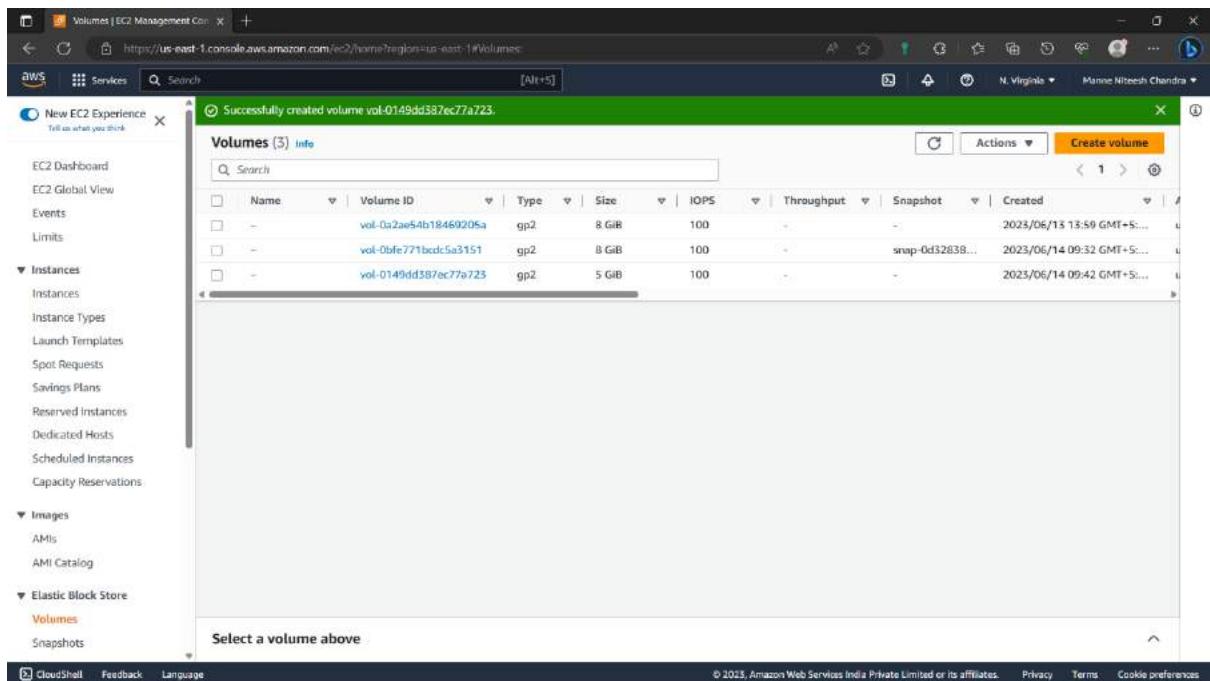
- Volume type: General Purpose SSD (gp2)
- Size (GiB): 5
- IOPS: 100 / 3000
- Throughput (MiB/s): Not applicable
- Availability Zone: us-east-1c
- Snapshot ID - optional: Don't create volume from a snapshot

At the bottom of the page, there are standard AWS navigation links: CloudShell, Feedback, Language, Privacy, Terms, and Cookie preferences.

165) you can give tag to this volume i.e., can identify it easily among all the volumes. click on “click volume”.



166) If you didn't give any tag then it would be better to remember the volume Id. The volume is created.



167)Attach this volume to the instance. Refresh the Page and select the volume you created and click on “actions”→“Attach volume”.

The screenshot shows the AWS EC2 Management Console with the 'Volumes' page open. On the left, there's a navigation sidebar with various EC2-related options like EC2 Dashboard, Instances, and Images. The main area displays a table of volumes with columns for Name, Volume ID, Type, Size, IOPS, Throughput, and Snapshot. One volume, 'vol-0149dd387ec77a723', is selected and highlighted in blue. A context menu is open to the right of this volume, listing actions such as 'Modify volume', 'Create snapshot', 'Delete volume', and 'Attach volume'. The 'Attach volume' option is currently selected and highlighted in blue. Below the table, a detailed view for the selected volume is shown, including its Volume ID (vol-0149dd387ec77a723), Size (5 GiB), Type (gp2), Volume status (Okay), and other metadata like AWS Compute Optimizer finding and KMS key ARN.

168)Select the instance you want to attach, Click on “Attach volume”.

This screenshot shows the 'Attach volume' wizard in the AWS EC2 Management Console. The first step, 'Basic details', is displayed. It requires selecting a 'Volume ID' (which is already set to 'vol-0149dd387ec77a723') and an 'Instance' (which is set to 'i-064dbb1f68aaa029'). There's also a note about selecting instances in the same Availability Zone. Below these fields, a 'Device name' field is set to '/dev/sdf'. A warning message in a callout box states: 'Newer Linux kernels may rename your devices to /dev/xvdf through /dev/vxpd internally, even when the device name entered here (and shown in the details) is /dev/sdf through /dev/sdp.' At the bottom of the form are 'Cancel' and 'Attach volume' buttons, with 'Attach volume' being the active button.

169)The volume is attached to the instance.

The screenshot shows the AWS EC2 Management Console with the URL <https://us-east-1.console.aws.amazon.com/ec2/home?region=us-east-1#Volumes>. The left sidebar is collapsed, and the main area displays a table titled "Volumes [3] Info". The table has columns: Name, Volume ID, Type, Size, IOPS, Throughput, Snapshot, and Created. Three volumes are listed:

Name	Volume ID	Type	Size	IOPS	Throughput	Snapshot	Created
-	vol-0a2ae54b18469205a	gp2	8 GiB	100	-	-	2023/06/13 13:59 GMT+5...
-	vol-0bfe771bcd5a3151	gp2	8 GiB	100	-	snap-0d32838...	2023/06/14 09:32 GMT+5...
-	vol-0149dd387ec77a723	gp2	5 GiB	100	-	-	2023/06/14 09:42 GMT+5...

A message at the bottom of the table says "Select a volume above". The status bar at the bottom right shows "© 2023, Amazon Web Services India Private Limited or its affiliates. Privacy Terms Cookie preferences".

170)Access the instance by following the previous steps: (140-146).

```
C:\Users\Nitee\Downloads>ssh -i "keys.pem" ubuntu@ec2-3-88-34-94.compute-1.amazonaws.com
The authenticity of host 'ec2-3-88-34-94.compute-1.amazonaws.com (3.88.34.94)' can't be established.
ED25519 key fingerprint is SHA256:x/DNB4Vvk10Phkqz2GSMVlznqjD8H9EJjh18mSVwPQ.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added 'ec2-3-88-34-94.compute-1.amazonaws.com' (ED25519) to the list of known hosts.
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 Wed Jun 14 04:26:38 UTC 2023

System load: 0.2265625   Processes:          99
Usage of /: 26.6% of 7.57GB  Users logged in:     0
Memory usage: 24%           IPv4 address for eth0: 172.31.89.31
Swap usage:  0%

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/ess 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-172-31-89-31:~$ |
```

171)Type the command “lsblk”:it will all the volumes attached to this instance. “xvdf” is the additional volume we attached.

```
ubuntu@ip-172-31-89-31:~$ System information as of Wed Jun 14 04:26:38 UTC 2023
System load: 0.2265625 Processes: 99
Usage of /: 26.6% of 7.57GB Users logged in: 0
Memory usage: 24% IPv4 address for eth0: 172.31.89.31
Swap usage: 0%
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/esa 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-172-31-89-31:~$ lsblk
NAME MAJ:MIN RM SIZE RO TYPE MOUNTPOINTS
loop0 7:0 0 24.4M 1 loop /snap/amazon-ssm-agent/6312
loop1 7:1 0 55.6M 1 loop /snap/core18/2745
loop2 7:2 0 63.3M 1 loop /snap/core20/1879
loop3 7:3 0 111.9M 1 loop /snap/lxd/24322
loop4 7:4 0 53.2M 1 loop /snap/snappyd/39122
xvda 202:0 0 8G 0 disk
└─xvda1 202:1 0 7.9G 0 part /
└─xvda14 202:14 0 4M 0 part
└─xvda15 202:15 0 106M 0 part /boot/efi
xvdf 202:80 0 5G 0 disk
ubuntu@ip-172-31-89-31:~$ |
```

172)Type the command “mkfs -t ext4 /dev/xvdf” if it doesn’t work try using sudo before i.e., “sudo mkfs -t ext4 /dev/xvdf”. It is used to create files in additional volumes.

```
ubuntu@ip-172-31-89-31:~$ See https://ubuntu.com/esa 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-172-31-89-31:~$ lsblk
NAME MAJ:MIN RM SIZE RO TYPE MOUNTPOINTS
loop0 7:0 0 24.4M 1 loop /snap/amazon-ssm-agent/6312
loop1 7:1 0 55.6M 1 loop /snap/core18/2745
loop2 7:2 0 63.3M 1 loop /snap/core20/1879
loop3 7:3 0 111.9M 1 loop /snap/lxd/24322
loop4 7:4 0 53.2M 1 loop /snap/snappyd/39122
xvda 202:0 0 8G 0 disk
└─xvda1 202:1 0 7.9G 0 part /
└─xvda14 202:14 0 4M 0 part
└─xvda15 202:15 0 106M 0 part /boot/efi
xvdf 202:80 0 5G 0 disk
ubuntu@ip-172-31-89-31:~$ sudo mkfs -t ext4 /dev/xvdf
mkfs.ext4 1.46.5 (30-Dec-2021)
Creating filesystem with 1310720 4K blocks and 329680 inodes
Filesystem UUID: d08f3263-1473-4b46-a2ef-6b5eb22875ff
Superblock backups stored on blocks:
    32768, 98304, 163840, 229376, 294912, 819200, 884736
Allocating group tables: done
Writing inode tables: done
Creating journal (16384 blocks): done
Writing superblocks and filesystem accounting information: done
ubuntu@ip-172-31-89-31:~$ |
```

Sudo-super user

Mkfs-make format.

/dev/xvdf- dev: device, xvdf- additional volume.

173)Create a repository using the command- “sudo mkdir /reponame” :- “sudo mkdir /app”.

```
ubuntu@ip-172-31-89-31:~$ + | ~
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-172-31-89-31:~$ lsblk
NAME   MAJ:MIN RM  SIZE RO TYPE MOUNTPOINTS
loop0    7:0     0  24.4M  1 loop /snap/amazon-ssm-agent/6312
loop1    7:1     0  55.6M  1 loop /snap/core18/2745
loop2    7:2     0  63.3M  1 loop /snap/core20/1879
loop3    7:3     0 111.9M  1 loop /snap/lxd/24322
loop4    7:4     0  53.2M  1 loop /snap/snapd/39122
xvda   202:0     0    8G  0 disk 
└─xvda1 202:1     0   7.9G  0 part /
  ├─xvda14 202:14    0   4H  0 part
  └─xvda15 202:15    0 106M  0 part /boot/efi
xvdf   202:8     0    5G  0 disk 
ubuntu@ip-172-31-89-31:~$ sudo mkfs -t ext4 /dev/xvdf
mke2fs 1.46.5 (30-Dec-2021)
Creating filesystem with 1310720 4k blocks and 327680 inodes
Filesystem UUID: d08f3263-1473-4b46-a2ef-6b5eb22875ff
Superblock backups stored on blocks:
        32768, 98304, 163840, 229376, 294912, 819200, 884736

Allocating group tables: done
Writing inode tables: done
Creating journal (16384 blocks): done
Writing superblocks and filesystem accounting information: done

ubuntu@ip-172-31-89-31:~$ sudo mkdir /app
ubuntu@ip-172-31-89-31:~$ |
```

174)Attach the volume to this folder by using the command : “sudo mount /dev/xvdf /app”.

```
ubuntu@ip-172-31-89-31:~$ + | ~
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-172-31-89-31:~$ lsblk
NAME   MAJ:MIN RM  SIZE RO TYPE MOUNTPOINTS
loop0    7:0     0  24.4M  1 loop /snap/amazon-ssm-agent/6312
loop1    7:1     0  55.6M  1 loop /snap/core18/2745
loop2    7:2     0  63.3M  1 loop /snap/core20/1879
loop3    7:3     0 111.9M  1 loop /snap/lxd/24322
loop4    7:4     0  53.2M  1 loop /snap/snapd/39122
xvda   202:0     0    8G  0 disk 
└─xvda1 202:1     0   7.9G  0 part /
  ├─xvda14 202:14    0   4H  0 part
  └─xvda15 202:15    0 106M  0 part /boot/efi
xvdf   202:8     0    5G  0 disk 
ubuntu@ip-172-31-89-31:~$ sudo mkfs -t ext4 /dev/xvdf
mke2fs 1.46.5 (30-Dec-2021)
Creating filesystem with 1310720 4k blocks and 327680 inodes
Filesystem UUID: d08f3263-1473-4b46-a2ef-6b5eb22875ff
Superblock backups stored on blocks:
        32768, 98304, 163840, 229376, 294912, 819200, 884736

Allocating group tables: done
Writing inode tables: done
Creating journal (16384 blocks): done
Writing superblocks and filesystem accounting information: done

ubuntu@ip-172-31-89-31:~$ sudo mkdir /app
ubuntu@ip-172-31-89-31:~$ sudo mount /dev/xvdf /app
ubuntu@ip-172-31-89-31:~$ |
```

175) Navigate to that folder by using the command – “cd dirname” :- “cd /app”.

```
ubuntu@ip-172-31-89-31:~$ + .. 
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-172-31-89-31:~$ lsblk
NAME   MAJ:MIN RM  SIZE RO TYPE MOUNTPOINTS
loop0    7:0    0 24.4M  1 loop /snap/amazon-ssm-agent/6312
loop1    7:1    0 55.6M  1 loop /snap/core18/2745
loop2    7:2    0 63.3M  1 loop /snap/core20/1879
loop3    7:3    0 111.9M 1 loop /snap/lxd/24322
loop4    7:4    0 53.2M  1 loop /snap/snappyd/39122
xvda   202:0    0   8G  0 disk
└─xvda1 202:1    0   7.9G 0 part /
└─xvda14 202:14   0   4M  0 part
└─xvda15 202:15   0  166M 0 part /boot/efi
xvdf   202:8    0   5G  0 disk
ubuntu@ip-172-31-89-31:~$ sudo mkfs -t ext4 /dev/xvdf
mkfs.ext4 1.46.5 (30-Dec-2021)
Creating filesystem with 1310720 4k blocks and 327680 inodes
Filesystem UUID: d08f3263-1473-4b46-a2ef-6b5eb22875ff
Superblock backups stored on blocks:
      32768, 98304, 163840, 229376, 294912, 819200, 884736

Allocating group tables: done
Writing inode tables: done
Creating journal (16384 blocks): done
Writing superblocks and filesystem accounting information: done

ubuntu@ip-172-31-89-31:~$ sudo mkdir /app
ubuntu@ip-172-31-89-31:~$ sudo mount /dev/xvdf /app
ubuntu@ip-172-31-89-31:~$ cd /app
ubuntu@ip-172-31-89-31:/app$
```

176) Create two files inside the colder using the command- “sudo touch filename” :- “sudo touch file1.txt file2.txt”. you can check the files created or not using the command “ls”.

```
ubuntu@ip-172-31-89-31:~$ + .. 
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-172-31-89-31:~$ lsblk
NAME   MAJ:MIN RM  SIZE RO TYPE MOUNTPOINTS
loop0    7:0    0 24.4M  1 loop /snap/amazon-ssm-agent/6312
loop1    7:1    0 55.6M  1 loop /snap/core18/2745
loop2    7:2    0 63.3M  1 loop /snap/core20/1879
loop3    7:3    0 111.9M 1 loop /snap/lxd/24322
loop4    7:4    0 53.2M  1 loop /snap/snappyd/39122
xvda   202:0    0   8G  0 disk
└─xvda1 202:1    0   7.9G 0 part /
└─xvda14 202:14   0   4M  0 part
└─xvda15 202:15   0  166M 0 part /boot/efi
xvdf   202:8    0   5G  0 disk
ubuntu@ip-172-31-89-31:~$ sudo mkfs -t ext4 /dev/xvdf
mkfs.ext4 1.46.5 (30-Dec-2021)
Creating filesystem with 1310720 4k blocks and 327680 inodes
Filesystem UUID: d08f3263-1473-4b46-a2ef-6b5eb22875ff
Superblock backups stored on blocks:
      32768, 98304, 163840, 229376, 294912, 819200, 884736

Allocating group tables: done
Writing inode tables: done
Creating journal (16384 blocks): done
Writing superblocks and filesystem accounting information: done

ubuntu@ip-172-31-89-31:~$ sudo mkdir /app
ubuntu@ip-172-31-89-31:~$ sudo mount /dev/xvdf /app
ubuntu@ip-172-31-89-31:~$ cd /app
ubuntu@ip-172-31-89-31:/app$ sudo touch file1.txt file2.txt
ubuntu@ip-172-31-89-31:/app$ ls
file1.txt  file2.txt  lost+found
ubuntu@ip-172-31-89-31:/app$
```

177)Now go to the volumes in the ec2.

The screenshot shows the AWS EC2 Volumes Management console. On the left, there is a navigation sidebar with various services like Dedicated Hosts, Scheduled Instances, Capacity Reservations, Images, AMIs, AMI Catalog, Elastic Block Store (with Volumes selected), Snapshots, Lifecycle Manager, Network & Security, Security Groups, Elastic IPs, Placement Groups, Key Pairs, Network interfaces, Load Balancing, and Auto Scaling. The main content area is titled "Volumes (3) Info". It displays a table with columns: Name, Volume ID, Type, Size, IOPS, Throughput, Snapshot, and Created. The table contains three rows, each representing a volume attached to an instance. A message at the bottom says "Select a volume above".

178)Select the additional volume and click on “actions”→“modify volume”.

The screenshot shows the same AWS EC2 Volumes Management console as before, but with a different view. A specific volume (vol-01959415116f6961b) is selected in the list. The "Actions" dropdown menu is open, and the "Modify volume" option is highlighted. The main content area shows detailed information for the selected volume, including its Volume ID, Size, Type, Volume status, and various configuration details like AWS Compute Optimizer finding, Encryption, and Snapshot.

179) Increase the size to 8GB and click on “Modify”.

The screenshot shows the 'Modify volume' page in the AWS EC2 Management console. The URL is <https://us-east-1.console.aws.amazon.com/ec2/home?region=us-east-1#ModifyVolume?volumeId=vol-01959415116f6961b>. The page title is 'Modify volume'. The main section is 'Volume details' with the following fields:

- Volume ID: vol-01959415116f6961b
- Volume type: General Purpose SSD (gp2)
- Size (GiB): 8
- IOPS: 100/3000

At the bottom right are 'Cancel' and 'Modify' buttons, with 'Modify' being highlighted.

180) Click on modify again.

The screenshot shows the 'Modify volume' page with a confirmation dialog overlay. The dialog title is 'Modify vol-01959415116f6961b?' and contains the following text:

If you are increasing the size of the volume, you must extend the file system to the new size of the volume. You can only do this when the volume enters the optimizing state. For more information see extending the file system for Linux and Windows.

The modification might take a few minutes to complete.

You are charged for the new volume configuration after volume modification starts. For pricing information, see [Amazon EBS Pricing](#).

Are you sure that you want to modify vol-01959415116f6961b?

At the bottom right of the dialog are 'Cancel' and 'Modify' buttons, with 'Modify' being highlighted.

181)Now the request in made.

Requested volume modification for volume vol-01959415116f6961b.
The volume is being modified.

Name	Volume ID	Type	Size	IOPS	Throughput	Snapshot	Created	Actions
-	vol-0a2ae54b18469205a	gp2	8 GiB	100	-	-	2023/06/13 13:59 GMT+5:30	
-	vol-01959415116f6961b	gp2	5 GiB	100	-	-	2023/06/14 09:55 GMT+5:30	
-	vol-0638628f381437d6a	gp2	8 GiB	100	-	snap-0d32838...	2023/06/14 09:54 GMT+5:30	

Select a volume above

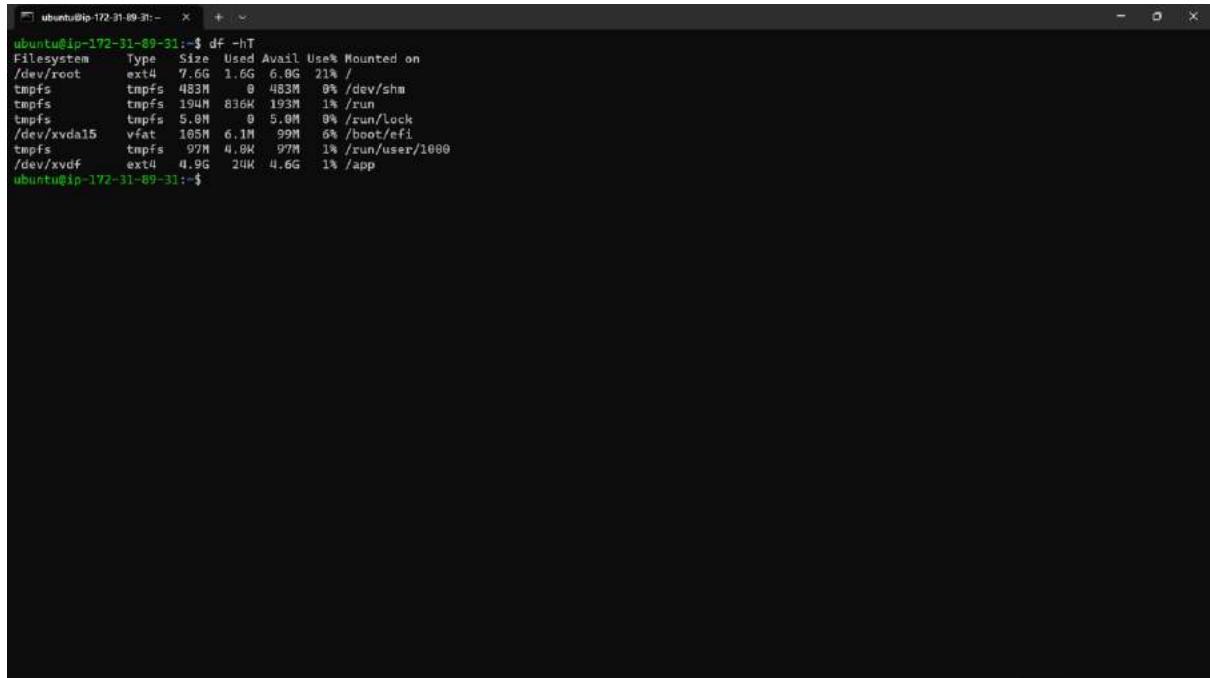
182)Go to your instance type the command “cd”:-will bring back to the previous path.

```
ubuntu@ip-172-31-89-31:~$ lsblk
NAME   MAJ:MIN SIZE RO TYPE MOUNTPOINTS
loop0    7:0    24.4M  1 loop /snap/amazon-ssm-agent/6312
loop1    7:1    55.6M  1 loop /snap/core18/2745
loop2    7:2    63.3M  1 loop /snap/core20/1879
loop3    7:3    111.9M 1 loop /snap/lxd/24322
loop4    7:4    53.2M  1 loop /snap/snappy/39122
xvda   202:0     8G  0 disk
└─xvda1 202:1     7.9G 0 part /
  └─xvda14 202:14    4K 0 part
  └─xvda15 202:15    16M 0 part /boot/efi
xvdf   202:80     5G  0 disk
ubuntu@ip-172-31-89-31:~$ sudo mkfs -t ext4 /dev/xvdf
mke2fs 1.46.5 (30-Dec-2021)
Creating filesystem with 1310728 4k blocks and 327680 inodes
Filesystem UUID: d08f3263-1d73-4b46-a2ef-6b5eb22875ff
Superblock backups stored on blocks:
        32768, 98304, 163840, 229376, 294912, 361920, 4284736

Allocating group tables: done
Writing inode tables: done
Creating journal (16384 blocks): done
Writing superblocks and filesystem accounting information: done

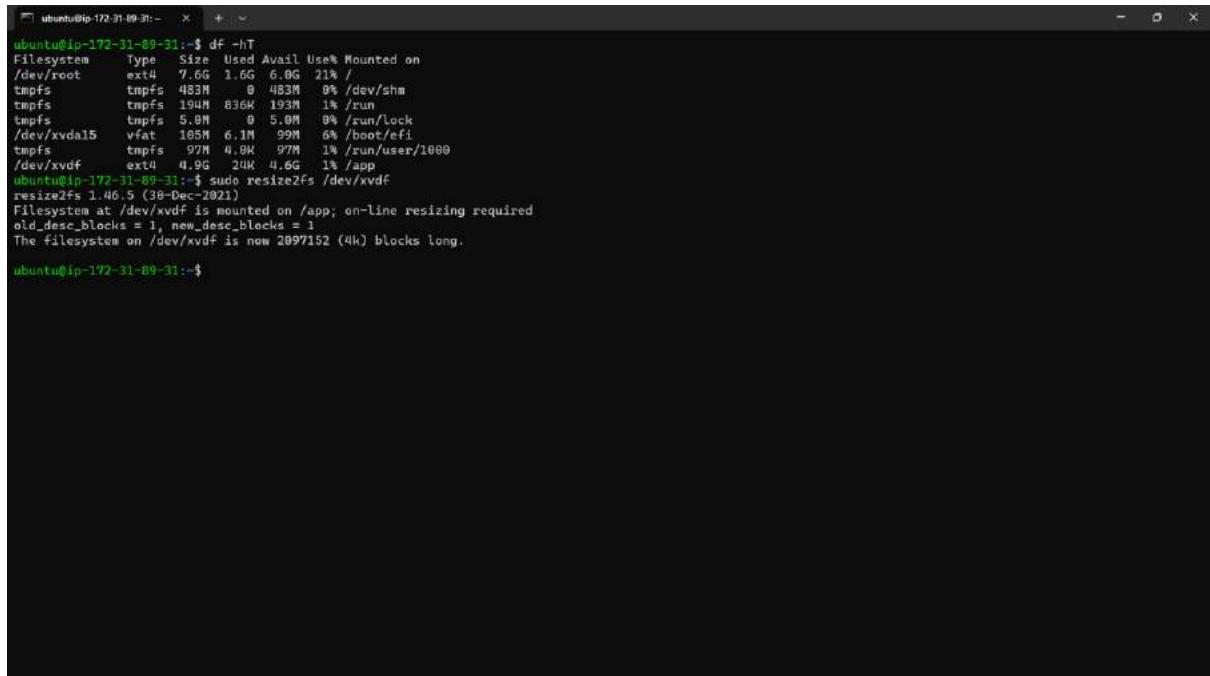
ubuntu@ip-172-31-89-31:~$ sudo mkdir /app
ubuntu@ip-172-31-89-31:~$ sudo mount /dev/xvdf /app
ubuntu@ip-172-31-89-31:~$ cd /app
ubuntu@ip-172-31-89-31:/app$ sudo touch file1.txt file2.txt
ubuntu@ip-172-31-89-31:/app$ ls
file1.txt  file2.txt
ubuntu@ip-172-31-89-31:/app$ cd ..
ubuntu@ip-172-31-89-31:~$
```

183) Type the command “df -hT”: shows name, size, type, and mount point for the file system that you need to extend.



```
ubuntu@ip-172-31-89-31:~$ df -hT
Filesystem      Type  Size  Used  Avail Use% Mounted on
/dev/root      ext4  7.6G  1.6G  6.0G  21% /
tmpfs         tmpfs  483M    8  483M   0% /dev/shm
tmpfs         tmpfs  194M  836K  193M   1% /run
tmpfs         tmpfs  5.8M    0  5.8M   0% /run/lock
/dev/xvda15    vfat  185M  6.1M  99M   6% /boot/efi
tmpfs         tmpfs  97M  4.8K  97M   1% /run/user/1000
/dev/xvdf      ext4  4.9G  24K  4.6G   1% /app
ubuntu@ip-172-31-89-31:~$
```

184) File system type is “Ext4” then the command is “sudo resize2fs /dev/filesystem” :- “sudo resize2fs /dev/xvdf”.



```
ubuntu@ip-172-31-89-31:~$ df -hT
Filesystem      Type  Size  Used  Avail Use% Mounted on
/dev/root      ext4  7.6G  1.6G  6.0G  21% /
tmpfs         tmpfs  483M    8  483M   0% /dev/shm
tmpfs         tmpfs  194M  836K  193M   1% /run
tmpfs         tmpfs  5.8M    0  5.8M   0% /run/lock
/dev/xvda15    vfat  185M  6.1M  99M   6% /boot/efi
tmpfs         tmpfs  97M  4.8K  97M   1% /run/user/1000
/dev/xvdf      ext4  4.9G  24K  4.6G   1% /app
ubuntu@ip-172-31-89-31:~$ sudo resize2fs /dev/xvdf
resize2fs 1.46.5 (30-Dec-2021)
Filesystem at /dev/xvdf is mounted on /app; on-line resizing required
old_desc_blocks = 1, new_desc_blocks = 1
The filesystem on /dev/xvdf is now 2097152 (4k) blocks long.
ubuntu@ip-172-31-89-31:~$
```

185) Type the command: “df -hT” to check the updated storage, we can see that the additional volume xvdf changes from 5gb→8gb.

```
ubuntu@ip-172-31-89-31:~$ df -hT
Filesystem      Type  Size  Used  Avail  Use%  Mounted on
/dev/root      ext4   7.6G  1.6G  6.0G  21%  /
tmpfs         tmpfs   483M   0    483M  0%   /dev/shm
tmpfs         tmpfs  194M  836K  193M  1%   /run
tmpfs         tmpfs   5.0M   0    5.0M  0%   /run/lock
/dev/xvda15     vfat   105M  6.1M  99M  6%   /boot/efi
tmpfs         tmpfs   97M   4.8K  97M  1%   /run/user/1000
/dev/xvdf      ext4   4.9G  24K   4.8G  1%   /app
ubuntu@ip-172-31-89-31:~$ sudo resize2fs /dev/xvdf
resize2fs 1.46.5 (30-Dec-2021)
Filesystem at /dev/xvdf is mounted on /app; on-line resizing required
old_desc_blocks = 1, new_desc_blocks = 1
The filesystem on /dev/xvdf is now 2097152 (4k) blocks long.

ubuntu@ip-172-31-89-31:~$ df -hT
Filesystem      Type  Size  Used  Avail  Use%  Mounted on
/dev/root      ext4   7.6G  1.6G  6.0G  21%  /
tmpfs         tmpfs   483M   0    483M  0%   /dev/shm
tmpfs         tmpfs  194M  836K  193M  1%   /run
tmpfs         tmpfs   5.0M   0    5.0M  0%   /run/lock
/dev/xvda15     vfat   105M  6.1M  99M  6%   /boot/efi
tmpfs         tmpfs   97M   4.8K  97M  1%   /run/user/1000
/dev/xvdf      ext4   7.8G  24K   7.4G  1%   /app
ubuntu@ip-172-31-89-31:~$
```

186) Now detach the volume from this instance by using the command : “sudo umount /dev/devicename” -; “sudo umount /dev/xvdf”. We can check it by using the command “df -hT”.

```
ubuntu@ip-172-31-89-31:~$ df -hT
Filesystem      Type  Size  Used  Avail  Use%  Mounted on
/dev/root      ext4   7.6G  1.6G  6.0G  21%  /
tmpfs         tmpfs   483M   0    483M  0%   /dev/shm
tmpfs         tmpfs  194M  836K  193M  1%   /run
tmpfs         tmpfs   5.0M   0    5.0M  0%   /run/lock
/dev/xvda15     vfat   105M  6.1M  99M  6%   /boot/efi
tmpfs         tmpfs   97M   4.8K  97M  1%   /run/user/1000
/dev/xvdf      ext4   4.9G  24K   4.8G  1%   /app
ubuntu@ip-172-31-89-31:~$ sudo resize2fs /dev/xvdf
resize2fs 1.46.5 (30-Dec-2021)
Filesystem at /dev/xvdf is mounted on /app; on-line resizing required
old_desc_blocks = 1, new_desc_blocks = 1
The filesystem on /dev/xvdf is now 2097152 (4k) blocks long.

ubuntu@ip-172-31-89-31:~$ df -hT
Filesystem      Type  Size  Used  Avail  Use%  Mounted on
/dev/root      ext4   7.6G  1.6G  6.0G  21%  /
tmpfs         tmpfs   483M   0    483M  0%   /dev/shm
tmpfs         tmpfs  194M  836K  193M  1%   /run
tmpfs         tmpfs   5.0M   0    5.0M  0%   /run/lock
/dev/xvda15     vfat   105M  6.1M  99M  6%   /boot/efi
tmpfs         tmpfs   97M   4.8K  97M  1%   /run/user/1000
/dev/xvdf      ext4   7.8G  24K   7.4G  1%   /app
ubuntu@ip-172-31-89-31:~$ sudo umount /dev/xvdf
ubuntu@ip-172-31-89-31:~$ df -hT
Filesystem      Type  Size  Used  Avail  Use%  Mounted on
/dev/root      ext4   7.6G  1.6G  6.0G  21%  /
tmpfs         tmpfs   483M   0    483M  0%   /dev/shm
tmpfs         tmpfs  194M  836K  193M  1%   /run
tmpfs         tmpfs   5.0M   0    5.0M  0%   /run/lock
/dev/xvda15     vfat   105M  6.1M  99M  6%   /boot/efi
tmpfs         tmpfs   97M   4.8K  97M  1%   /run/user/1000
ubuntu@ip-172-31-89-31:~$
```

We cannot see the “/dev/xvdf” because it is detached from the instance.

187)Select the instance i.e., you created(Additional volume attached)and click “instance state”→“Stop instance”.

The screenshot shows the AWS EC2 Management Console. In the left sidebar, under 'Instances', 'Instances' is selected. The main area displays three instances:

- Ubuntu Server**: Instance ID i-06bc94c17e49c70c8, Instance state Running, Instance type t2.micro, Status Initial.
- terse**: Instance ID i-06f55a24a25b3fec, Instance state Terminated, Instance type t2.micro.
- hug/hbjhv**: Instance ID i-0512ba9cc0a044cf, Instance state Terminated, Instance type t2.micro.

A context menu is open over the **Ubuntu Server** instance, with the 'Stop instance' option highlighted. The menu also includes options like Start instance, Reboot instance, Hibernate instance, and Terminate instance.

188)Click on “stop”.

The screenshot shows the AWS EC2 Management Console with the same interface as the previous screenshot. A confirmation dialog box titled 'Stop instance?' is overlaid on the page. The dialog contains the following text:

Stop instance?

To confirm that you want to stop the instance, choose the Stop button below.

Cancel Stop

The background shows the list of instances, with the **Ubuntu Server** instance still listed as **Running**.

189) Navigate to “volumes” in the Elastic block storage at the bottom of the navigation panel.

The screenshot shows the AWS EC2 Management Console with the URL <https://us-east-1.console.aws.amazon.com/ec2/home?region=us-east-1#Volumes>. The left sidebar is collapsed. The main content area displays a table titled "Volumes [3] Info" with columns: Name, Volume ID, Type, Size, IOPS, Throughput, Snapshot, and Created. Three volumes are listed:

Name	Volume ID	Type	Size	IOPS	Throughput	Snapshot	Created
-	vol-0a2ae54b18469205a	gp2	8 GiB	100	-	-	2023/06/13 13:59 GMT+5:30
-	vol-01959415116f6961b	gp2	8 GiB	100	-	-	2023/06/14 09:55 GMT+5:30
-	vol-0638628f381437d6a	gp2	8 GiB	100	-	snap-0d3285...	2023/06/14 09:54 GMT+5:30

A modal window titled "Select a volume above" is open below the table. The bottom right corner of the screen shows the copyright notice: © 2023, Amazon Web Services India Private Limited or its affiliates.

190) Select the additional volume by volume id or by the tag(if you given). Click on “Actions”→“Force detach volume”. Because normal detach take so much time so we use force detach.

The screenshot shows the same AWS EC2 Management Console interface as the previous one, but with a different view. A volume with Volume ID "vol-01959415116f6961b" is selected in the list. The "Actions" dropdown menu is open, and the option "Force detach volume" is highlighted. The main content area shows detailed information for the selected volume, including its ID, size, type, and status.

Volume ID: vol-01959415116f6961b

Details	Status checks	Monitoring	Tags
Volume ID vol-01959415116f6961b	Size 8 GiB	Type gp2	Volume status OK
AWS Compute Optimizer finding Opt-in to AWS Compute Optimizer for recommendations. Learn more	Volume state In-use	IOPS 100	Throughput -
Encryption Not encrypted	KMS key ID -	KMS key alias -	KMS key ARN -
Fast snapshot restored No	Snapshot -	Availability Zone us-east-1c	Created Wed Jun 14 2023 09:55:09 GMT+0530

191) Type “detach” and click on “force detach” option.

The screenshot shows the AWS EC2 Management Console with the 'Volumes' section selected. A modal dialog box titled 'Force detach vol-0fb56908f588a720a?' is open. The dialog contains a warning message about forced detachment and a confirmation field with the word 'detach'. At the bottom right of the dialog are 'Cancel' and 'Force detach' buttons. The background shows a list of volumes with their details like Name, Volume ID, Type, Size, IOPS, Throughput, Snapshot, and Created date.

192) Now the volume is detached successfully.

The screenshot shows the AWS EC2 Management Console with the 'Volumes' section selected. A green success message box at the top says 'Successfully force detached volume.' Below it, the 'Volumes' table shows three detached volumes. A message 'Select a volume above' is displayed below the table. The bottom of the screen includes standard AWS footer links for CloudShell, Feedback, Language, Privacy, Terms, and Cookie preferences.

193)Select the additional volume click on “actions”→“create snapshot”

The screenshot shows the AWS EC2 Management Console with the 'Volumes' section selected. A context menu is open over a selected volume (vol-01959415116f6961b). The 'Actions' menu is expanded, and the 'Create snapshot' option is highlighted.

Volumes (1/3) Info

Name	Volume ID	Type	Size	IOPS	Throughput	Snapshot
-	vol-0a2ae54b18469205a	gp2	8 GiB	100	-	-
<input checked="" type="checkbox"/>	vol-01959415116f6961b	gp2	8 GiB	100	-	-
-	vol-0658628f38143706a	gp2	8 GiB	100	-	snap-0d32

Volume ID: vol-01959415116f6961b

Details | Status checks | Monitoring | Tags

Volume ID vol-01959415116f6961b	Size 8 GiB	Type gp2	Volume status Okay
AWS Compute Optimizer finding Opt-in to AWS Compute Optimizer for recommendations. Learn more	Volume state Available	IOPS 100	Throughput
Encryption Not encrypted	KMS key ID -	KMS key alias -	KMS key ARN
Fast snapshot restored No	Snapshot	Availability Zone us-east-1c	Created Wed Jun 14 2023 09:55:09 GMT+0530

194)Give a name if you want by clicking on “add tag”. Click on “Create snapshot”.

The screenshot shows the 'Create snapshot' wizard. The 'Details' step is active, showing the selected volume (vol-01959415116f6961b), a description ('snapshot of the additional volume'), and encryption settings ('Not encrypted'). The 'Tags' step is shown below, indicating no tags are associated with the resource.

Create snapshot

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

Details

Volume ID
vol-01959415116f6961b

Description
Add a description for your snapshot
snapshot of the additional volume

Encryption info
Not encrypted

Tags

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.

No tags associated with the resource.

Add tag

You can add 50 more tags.

Create snapshot

195)Now the snapshot is created you can check it by going to “snapshot” below the “volumes” in “Elastic block storage” on the navigation panel.

The screenshot shows the AWS EC2 Management Console with the "Snapshots" section selected in the navigation pane. The main area displays a table titled "Snapshots (1) Info" with one item listed:

Name	Snapshot ID	Volume...	Description	Storage...	Snapshot status	Started
-	snap-0b40c810161028ebd	8 GiB	snapshot of the additional ...	Standard	Completed	2023/06/14 10:46 GMT+5...

A message at the bottom of the table says "Select a snapshot above." The top right corner of the table has a yellow "Create snapshot" button. The left sidebar contains various EC2 management options like Instances, Images, and Elastic Block Store.

196)Select the snapshot click on “actions”→“create volume from snapshot”.

The screenshot shows the same AWS EC2 Management Console interface as the previous one, but with a context menu open over the selected snapshot row. The menu is titled "Actions" and includes the following options:

- Create volume from snapshot
- Create image from snapshot
- Copy snapshot
- Modify permissions
- Manage fast snapshot restore
- Archive snapshot
- Restore snapshot from archive
- Change restore period
- Delete snapshot
- Manage tags

The "Create volume from snapshot" option is highlighted with a yellow background. The rest of the interface remains the same, showing the snapshot details and the left sidebar.

197)The availability zone should be same as instance availability zone.

The screenshot shows the 'Create volume' page in the AWS EC2 Management console. The 'Volume settings' section is visible, containing the following fields:

- Snapshot ID:** snap-0b40c810161028ebd
- Volume type:** General Purpose SSD (gp2)
- Size (GiB):** 8
- IOPS:** 100 / 3000
- Throughput (MiB/s):** Not applicable
- Availability Zone:** us-east-1c
- Fast snapshot restore:** Not enabled for selected snapshot
- Encryption:** Info

At the bottom right of the form, there is a 'Create volume' button.

198)Click on “create volume”.

The screenshot shows the 'Create volume' page in the AWS EC2 Management console, similar to the previous one but with a different view of the form fields. The 'Create volume' button is now highlighted in orange at the bottom right of the page.

199)Now the volume is created from the snapshot.

The screenshot shows the AWS EC2 Management Console with the 'Solutions' tab selected. A success message at the top says 'Successfully created volume vol-02d3542e93fb64953.' Below it, the 'Snapshots' section displays one item:

Name	Snapshot ID	Volume...	Description	Storage...	Snapshot status	Started
-	snap-0b40c810161028ebd	8 GiB	snapshot of the additional ...	Standard	Completed	2023/06/14 10:46 GMT+5:30

A note below the table says 'Select a snapshot above.'

200)Give a name to the additional volume so that you can identify it easily by clicking on the additional volume at “name” column. after typing the name click on save now the name is saved for the additional volume, identify it easily

The screenshot shows the AWS EC2 Management Console with the 'Volumes' section selected. It lists three volumes, with the third one being the 'additional vol...' which has been renamed:

Name	Volume ID	Type	Size	IOPS	Throughput	Snapshot	Created
-	vol-0a2ae54b18469205a	gp2	8 GiB	100	-	-	2023/06/13 13:59 GMT+5:30
-	vol-0638628f3814576fa	gp2	8 GiB	100	-	snap-0d32838...	2023/06/14 09:54 GMT+5:30
<input checked="" type="checkbox"/>	additional vol...	gp2	8 GiB	100	-	snap-0b40c81...	2023/06/14 10:48 GMT+5:30

Below the table, a detailed view for the 'additional vol...' volume is shown:

Volume ID: vol-02d3542e93fb64953 (additional volume)			
Details	Status checks	Monitoring	Tags
Volume ID vol-02d3542e93fb64953 (additional volume)	Size 8 GiB	Type gp2	Volume status Okay
AWS Compute Optimizer finding Opt-in to AWS Compute Optimizer for recommendations. Learn more	Volume state Available	IOPS 100	Throughput -
Encryption Not encrypted	KMS key ID -	KMS key alias -	KMS key ARN -
Fast snapshot restored	Snapshot	Availability Zone	Created

201)Create a new instance by following the steps:129-139.

The screenshot shows the AWS EC2 Management Console interface. In the top navigation bar, the URL is https://us-east-1.console.aws.amazon.com/ec2/home?region=us-east-1#Instances:. The main content area displays a table titled 'Instances (1/3)'. The table has columns for Name, Instance ID, Instance state, Instance type, Status check, Alarm status, Availability Zone, and Public IPv4 DNS. One row is visible, showing 'Ubuntu Server 2' with Instance ID i-0bcc7cfdb94dcf00, Instance state as Running, Instance type t2.micro, 2/2 checks passed, No alarms, Availability Zone us-east-1c, and Public IPv4 DNS ec2-18-233-101-128. There are buttons for Connect, Instance state, Actions, and Launch instances.

202)Access the instance by following the steps:(140-146).

```
C:\Users\Nitee\Downloads>ssh -i "keys.pem" ubuntu@ec2-18-233-101-181.compute-1.amazonaws.com
The authenticity of host 'ec2-18-233-101-181.compute-1.amazonaws.com (18.233.101.181)' can't be established.
ED25519 key fingerprint is SHA256:b0TESSsLySWY94zbFBzOsjHjgmQX1KtDLyzzC3Sjos.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added 'ec2-18-233-101-181.compute-1.amazonaws.com' (ED25519) to the list of known hosts.
Welcome to Ubuntu 22.04.2 LTS (GNU/Linux 5.19.0-1625-nwa x86_64)

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

 System information as of Wed Jun 14 05:24:52 UTC 2023

 System load: 0.11328125 Processes:          101
 Usage of /:  20.6% of 7.59GB Users logged in:      0
 Memory usage: 25%           IPv4 address for eth0: 172.31.92.85
 Swap usage:  0%

 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-172-31-92-85:~$
```

203)Type the command “lsblk” to see the attached voulmes we can see the additional attached volume .

```
ubuntu@ip-172-31-92-85:~$ lsblk
NAME   MAJ:MIN RM  SIZE RO TYPE MOUNTPOINTS
loop0    7:0     0 24.4M  1 loop /snap/amazon-ssm-agent/6312
loop1    7:1     0 55.6M  1 loop /snap/core18/2745
loop2    7:2     0 63.3M  1 loop /snap/core20/1879
loop3    7:3     0 111.9M 1 loop /snap/lxd/24322
loop4    7:4     0 53.2M  1 loop /snap/snapd/39122
xvda   202:0     0   8G  0 disk
└─xvda1 202:1     0  7.9G 0 part /
└─xvda4 202:14    0   4M 0 part
└─xvda5 202:15    0 106M 0 part /boot/efi
xvdf   202:8     0   8G  0 disk
ubuntu@ip-172-31-92-85:~$
```

204)Create a repository using the command “sudo mkdir reponame” – “sudo mkdir /jug”.

```
ubuntu@ip-172-31-92-85:~$ sudo mkdir /jug
ubuntu@ip-172-31-92-85:~$ df -hT
Filesystem  Type  Size  Used  Avail Use% Mounted on
/dev/root   ext4  7.6G  1.6G  6.0G  21% /
tmpfs       tmpfs  483M   0  483M  0% /dev/shm
tmpfs       tmpfs  194M  836K  193M  1% /run
tmpfs       tmpfs  5.0M   0  5.0M  0% /run/lock
/dev/xvda5  vfat   165M  6.1M  99M  6% /boot/efi
tmpfs       tmpfs  97M  4.0K  97M  1% /run/user/1000
ubuntu@ip-172-31-92-85:~$ sudo mkdir /jug
ubuntu@ip-172-31-92-85:~$
```

205)Now attach the volume to these repository – “sudo mount /dev/xvdf /jug”.

```
ubuntu@ip-172-31-92-85:~$ apt update
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.

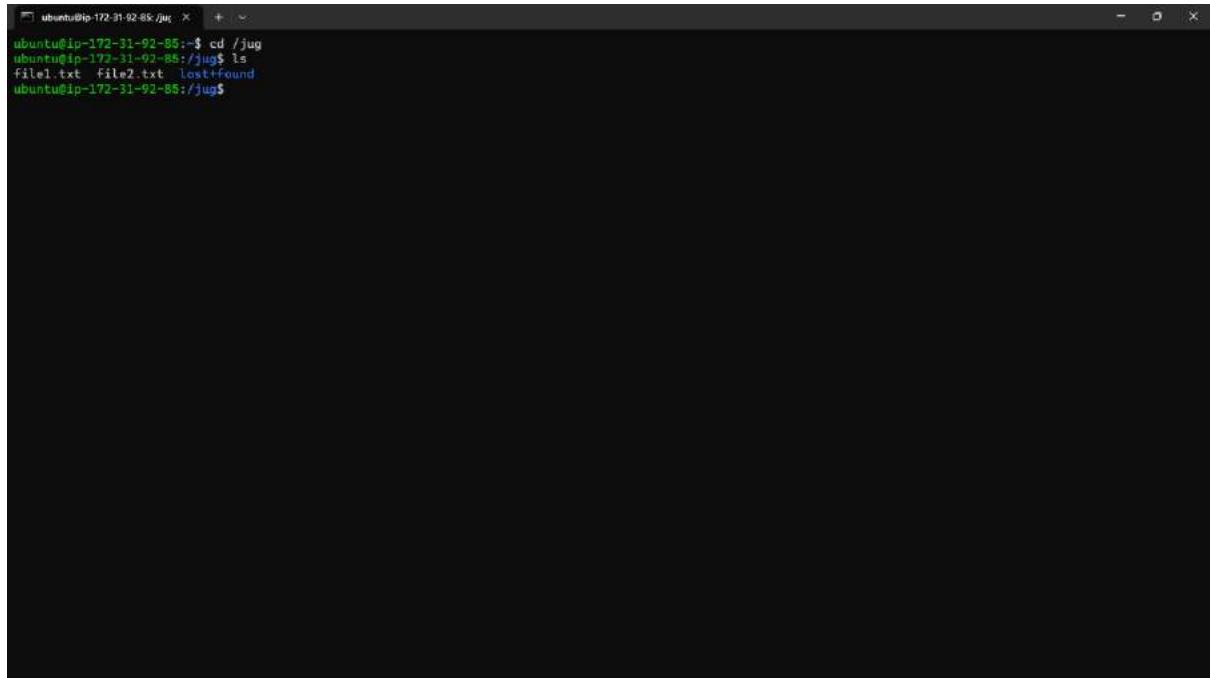
To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.

ubuntu@ip-172-31-92-85:~$ lsblk
NAME   MAJ:MIN RM  SIZE RO TYPE MOUNTPOINTS
loop0    7:0    0 24.4M  1 loop /snap/amazon-ssm-agent/6312
loop1    7:1    0 55.6M  1 loop /snap/core18/2745
loop2    7:2    0 63.3M  1 loop /snap/core20/1879
loop3    7:3    0 111.9M 1 loop /snap/lxd/24322
loop4    7:4    0 53.2M  1 loop /snap/snapd/39122
xvda   202:0    0   8G  0 disk 
└─xvda1 202:1    0   7.9G 0 part /
  ├─xvda14 202:14   0   4M 0 part 
  └─xvda15 202:15   0  186M 0 part /boot/efi
xvdf   202:80   0   8G  0 disk 
ubuntu@ip-172-31-92-85:~$ df -hT
Filesystem  Type  Size  Used  Avail Use% Mounted on
/dev/root   ext4  7.6G  6.0G  21% /
tmpfs       tmpfs  483M   8M  483M  0% /dev/shm
tmpfs       tmpfs  194M  836K 193M  1% /run
tmpfs       tmpfs  5.8M   0  5.8M  0% /run/lock
/dev/xvda15 vfat   185M  6.1M  99M  6% /boot/efi
tmpfs       tmpfs  97M  4.8K  97M  1% /run/user/1000
ubuntu@ip-172-31-92-85:~$ sudo mkdir /jug
ubuntu@ip-172-31-92-85:~$ sudo mount /dev/xvdf /jug
ubuntu@ip-172-31-92-85:~$
```

206)Go to the repository using the command “ cd reponame ” :- “cd /jug”.

```
ubuntu@ip-172-31-92-85:/jug$ cd /jug
ubuntu@ip-172-31-92-85:/jug$
```

207) Type the “ls” command, we can see the list of files we created in the first mount.



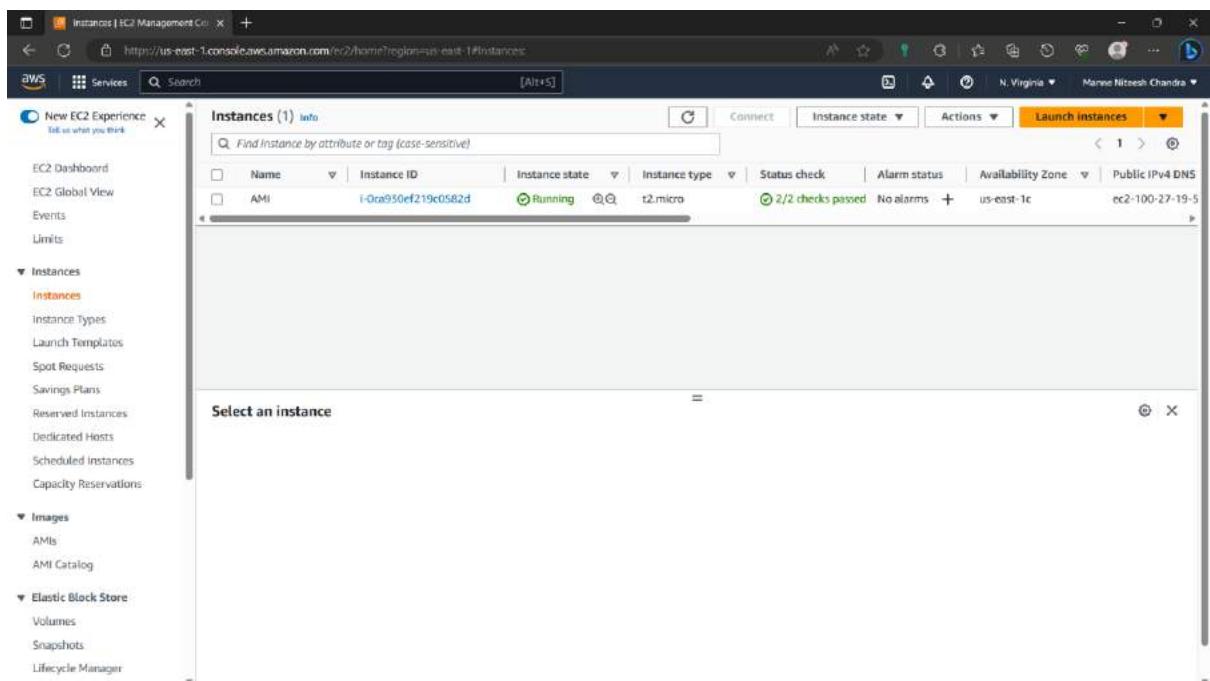
```
ubuntu@ip-172-31-92-85:~$ cd /jug
ubuntu@ip-172-31-92-85:/jug$ ls
file1.txt file2.txt lost+Found
ubuntu@ip-172-31-92-85:/jug$
```

EBS-It is used to share the data in same availability zones

EBS Snapshot-It is used to share the data in different availability zones.

AMI:

208) Create an EC2 instance by following the steps:-(129-139).



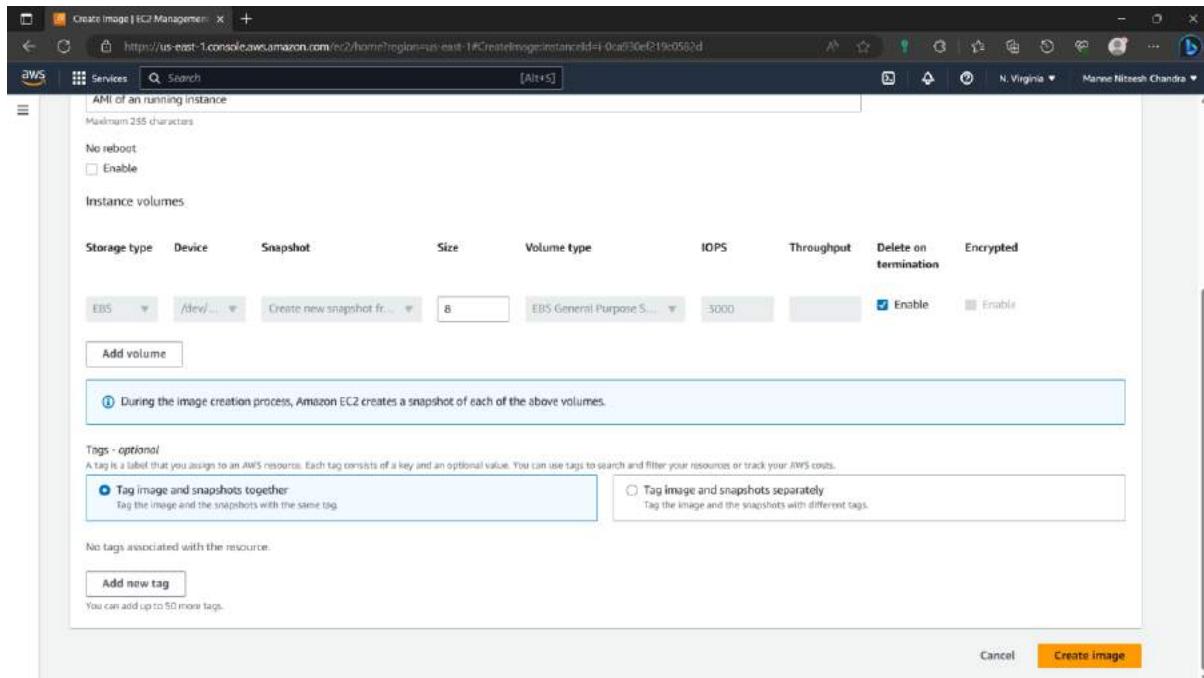
209)Select the instance and click on “actions”→“Images and Templates”→“Create image”.

The screenshot shows the AWS EC2 Management Console. On the left, there's a navigation sidebar with sections like EC2 Dashboard, Instances, Images, and Elastic Block Store. The main area displays a table of instances. One instance, named 'AMI' with the ID 'i-0ca930ef219c0582d', is selected. A context menu is open for this instance, with the 'Actions' dropdown expanded. Under 'Image and templates', the 'Create image' option is highlighted. Below the table, there's a detailed view for the selected instance, showing its public and private IP addresses, instance state (Running), and other configuration details.

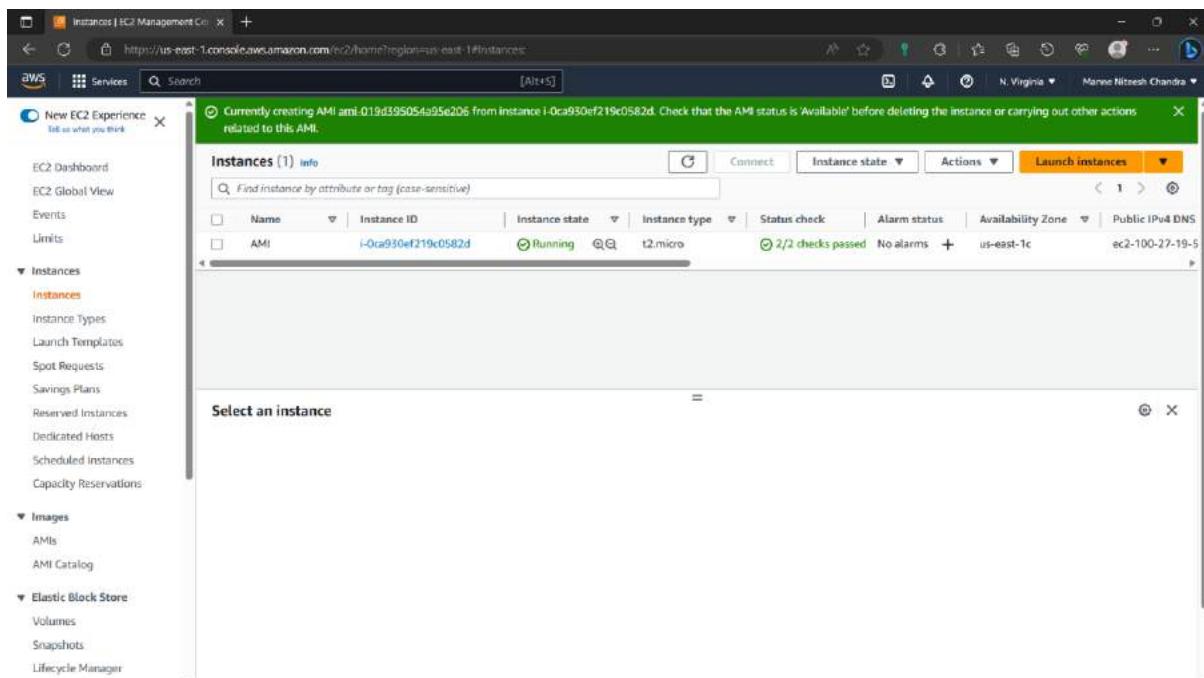
210)Give name, description of your choice.

The screenshot shows the 'Create image' wizard. Step 1: 'Create image'. It asks for an 'Image name' (set to 'AMI') and an 'Image description - optional' (set to 'AMI of an running instance'). Below these, there's a section for 'Instance volumes'. A table lists one volume: '/dev/sda1' (Storage type: EBS, Size: 8, Volume type: EBS General Purpose 5...). There are checkboxes for 'No reboot' (unchecked) and 'Enable' (unchecked). At the bottom, a note says: 'During the image creation process, Amazon EC2 creates a snapshot of each of the above volumes.'

211) Click on “Create image”.



212) The image has been created.



213) You can see the created image in “AMIs” of Images at the navigation panel.

The screenshot shows the AWS EC2 Management Console with the 'Images' section selected in the navigation bar. Under 'Images', 'AMIs' is also selected. The main area displays a table titled 'Amazon Machine Images (AMIs) (1) Info'. The table has columns: Name, AMI ID, AMI name, Source, Owner, and Visibility. One entry is listed: 'ami-019d59504a95e206' with 'AMI' in the Name column, 'ami-019d59504a95e206/AMI' in the AMI ID column, and '651943206657/AMI' in the Source column. The Owner is '651943206657' and the Visibility is 'Private'. Below the table, a modal window titled 'Select an AMI' is open, showing the same single entry.

214) Wait till the “status” in AMI shows “Available”, then we can use these image.

This screenshot shows the same EC2 Management Console interface as the previous one, but the table now includes a 'Status' column. The entry for the AMI 'ami-019d59504a95e206' now shows 'Available' in the Status column instead of 'Pending'. The other columns remain the same: Visibility (Private), Creation date (2023/06/14 15:07 GMT+5:30), Platform (Linux/UNIX), Root device type (ebs), and Block devices (/dev/xvda=snap-052154c5cb74).

Load Balancers:

215) Type “EC2” in search bar and select the “EC2” option from below.

The screenshot shows the AWS Management Console search results for 'EC2'. The search bar at the top contains 'EC2'. Below it, there are two main sections: 'Services' and 'Features'. In the 'Services' section, 'EC2' is listed under 'Virtual Servers in the Cloud'. Other services listed include EC2 Image Builder, Amazon Inspector, and AWS Firewall Manager. In the 'Features' section, 'Dashboard' and 'Limits' are listed under 'EC2 feature'. A sidebar on the right provides information about getting started with AWS, finding certification, and viewing AWS services, features, and limits.

216) Select “launch instance” option to create a new instance.

The screenshot shows the EC2 Management Dashboard. On the left, a navigation menu includes 'New EC2 Experience', 'EC2 Dashboard', 'Events', 'Limits', 'Instances', 'Instance Types', 'Launch Templates', 'Spot Requests', 'Savings Plans', 'Reserved Instances', 'Dedicated Hosts', 'Scheduled Instances', 'Capacity Reservations', 'Images', 'AMIs', 'AMI Catalog', and 'Elastic Block Store' with 'Volumes' and 'Snapshots'. The main area has sections for 'Resources' (listing Instances (running), Auto Scaling Groups, Dedicated Hosts, Elastic IPs, Instances, Key pairs, Load balancers, Placement groups, Security groups, Snapshots, and Volumes), 'Launch instance' (with 'Launch instance' and 'Launch instance from template' buttons), 'Service health' (showing Region: US East (N. Virginia) and Status: This service is operating normally), 'Zones' (listing Zone name: us-east-1a and Zone ID: use1-az6), and 'Explore AWS' (promoting AWS Graviton2 and GuardDuty). A sidebar on the right shows 'Account attributes' like Supported platforms (VPC selected), Default VPC (vpc-0b7cc25909d5dbfae), and Settings for EBS encryption, Zones, EC2 Serial Console, Default credit specification, and Console experiments.

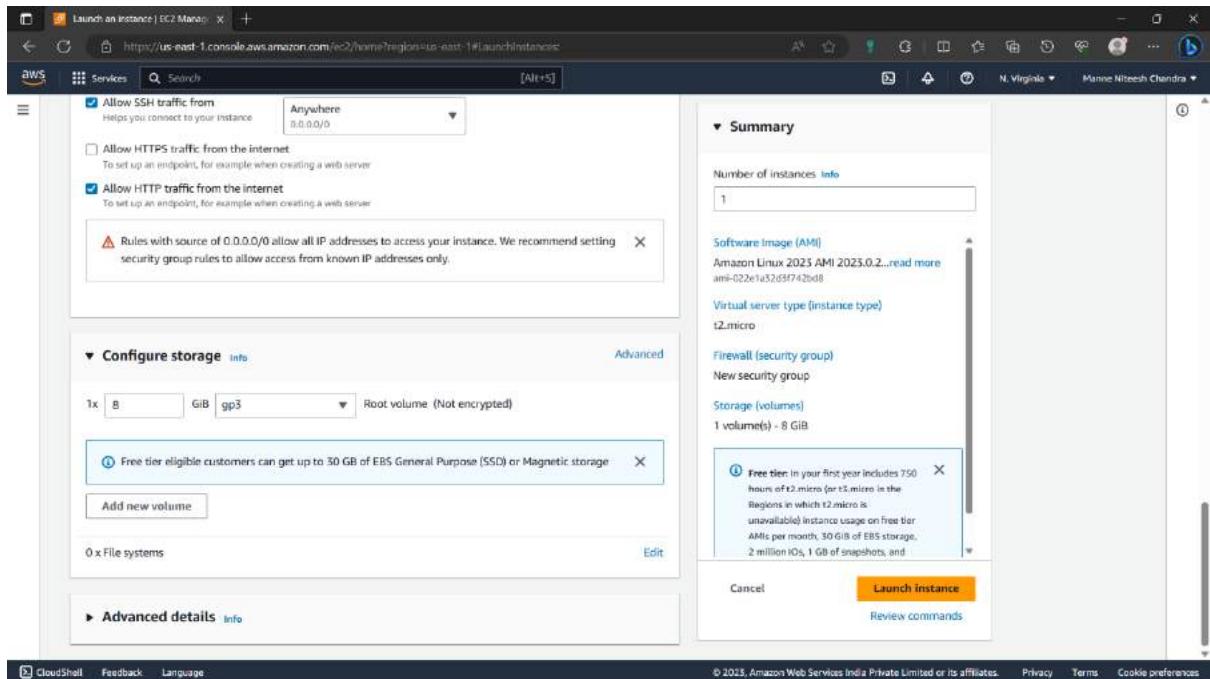
217) Give name “nginx” let the AMI be default.

The screenshot shows the 'Launch an instance' wizard on the AWS EC2 console. In the 'Name and tags' section, the name 'Nginx' is entered. The 'Application and OS Images (Amazon Machine Image)' section shows a search bar and a grid of AMI icons, with 'Ubuntu' selected. On the right, the 'Summary' panel shows 1 instance, using the 'Amazon Linux 2023 AMI 2023.0.2...' AMI, t2.micro instance type, and 1 volume(s) - 8 GB storage. A tooltip indicates a free tier of 750 hours of t2.micro usage. At the bottom are 'Launch instance' and 'Review commands' buttons.

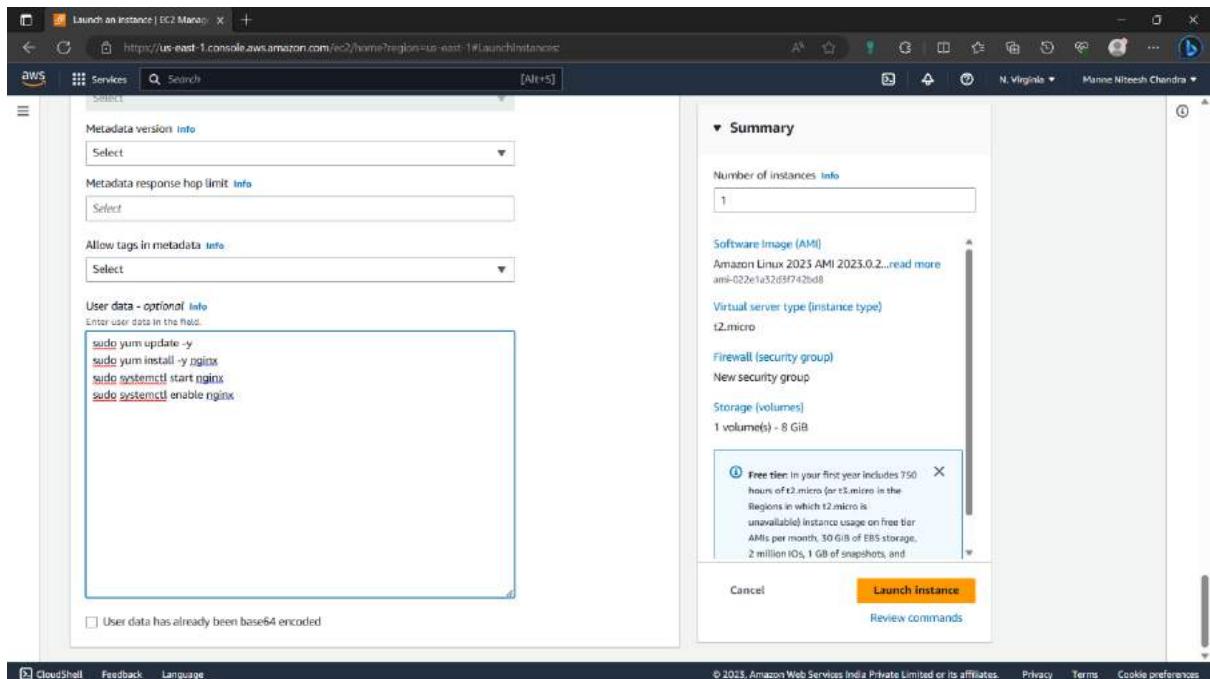
218) Enable the “HTTPS Traffic” in “network settings”.

The screenshot shows the 'Network settings' step of the EC2 launch wizard. Under 'Firewall (security groups)', the 'Create security group' button is selected. Below it, under 'We'll create a new security group called "launch-wizard-22" with the following rules:', three checkboxes are shown: 'Allow SSH traffic from Anywhere (0.0.0.0/0)', 'Allow HTTPS traffic from the internet To let up an endpoint, for example when creating a web server', and 'Allow HTTP traffic from the internet To set up an endpoint, for example when creating a web server'. A note at the bottom says 'Rules with source of 0.0.0.0/0 allow all IP addresses to access your instance. We recommend setting security group rules to allow access from known IP addresses only.' The right side of the screen shows the same summary and instance configuration as the previous screenshot.

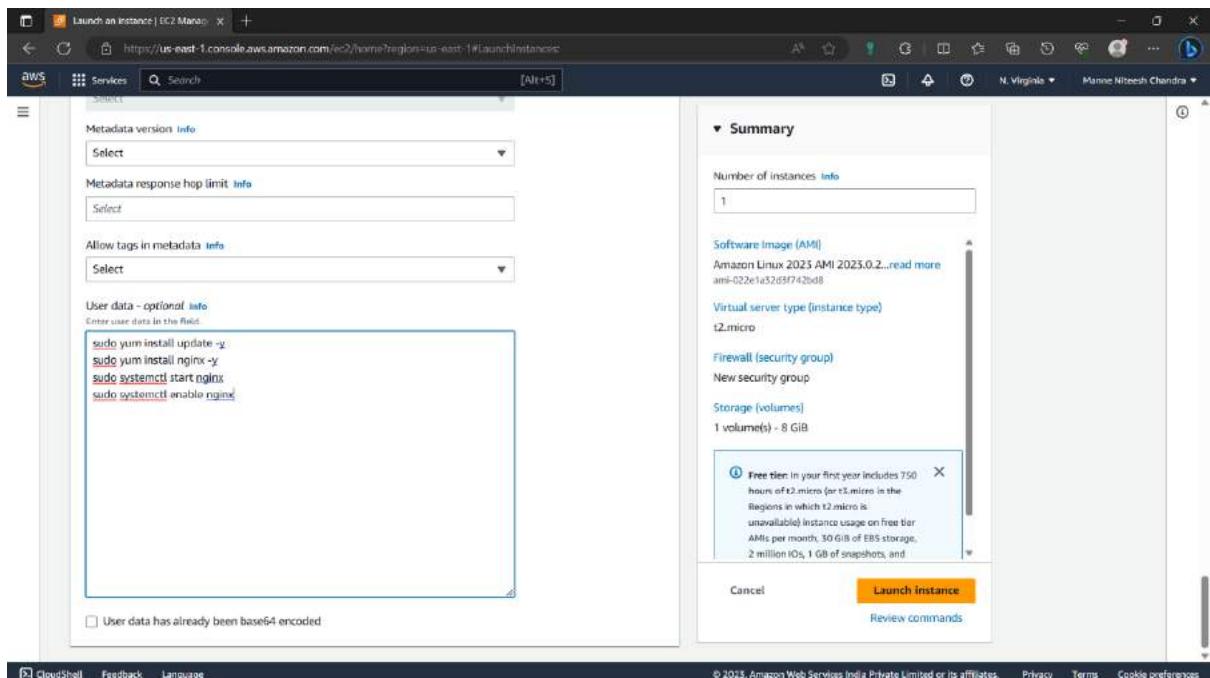
219) Click on “Advanced details” option.



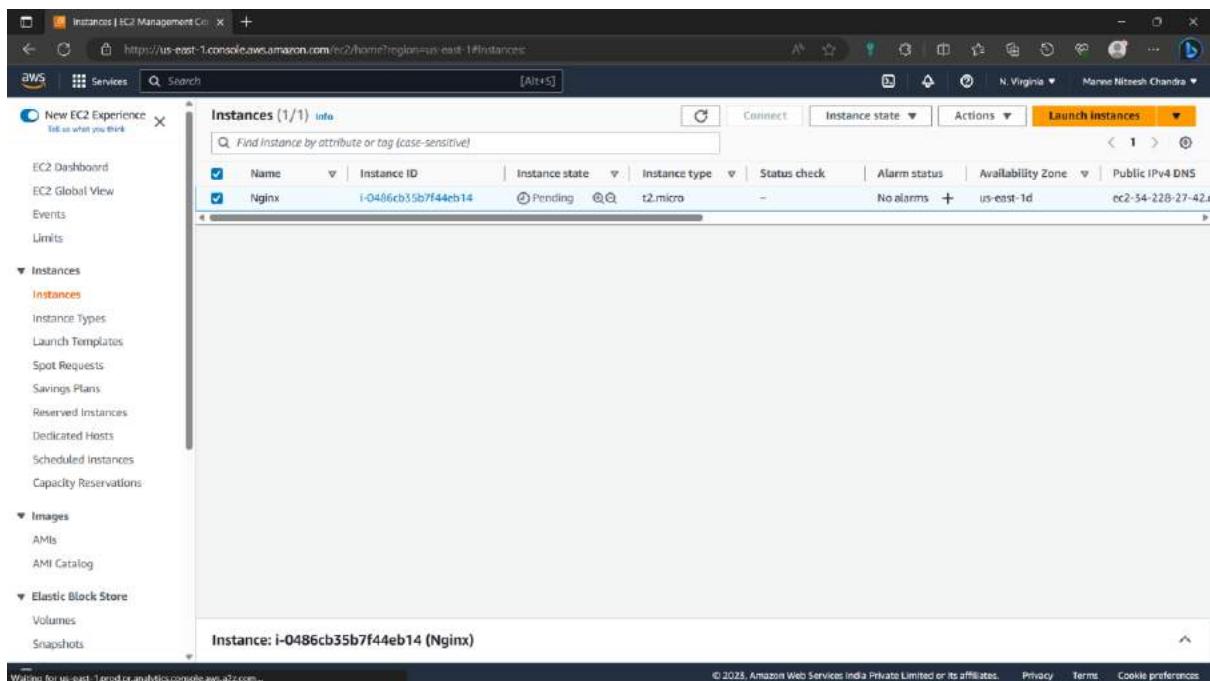
220) Type below commands in image in “user data” box at bottom of the page.



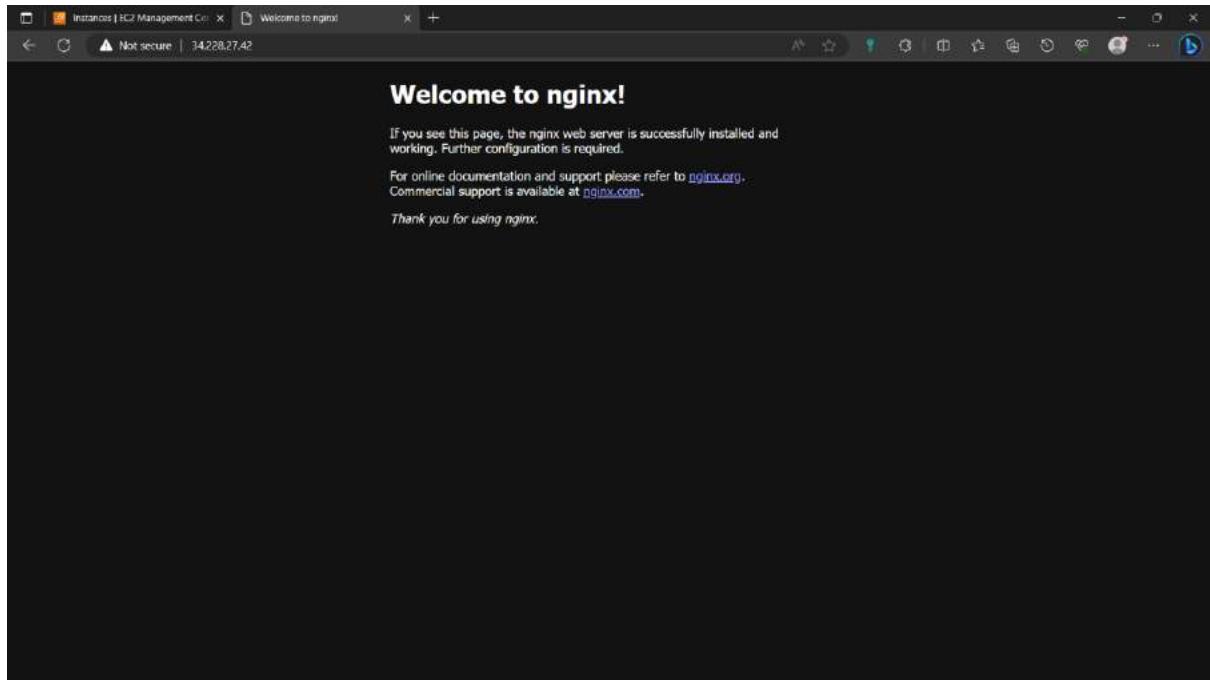
221)Click on “Launch instance” to create the instance.



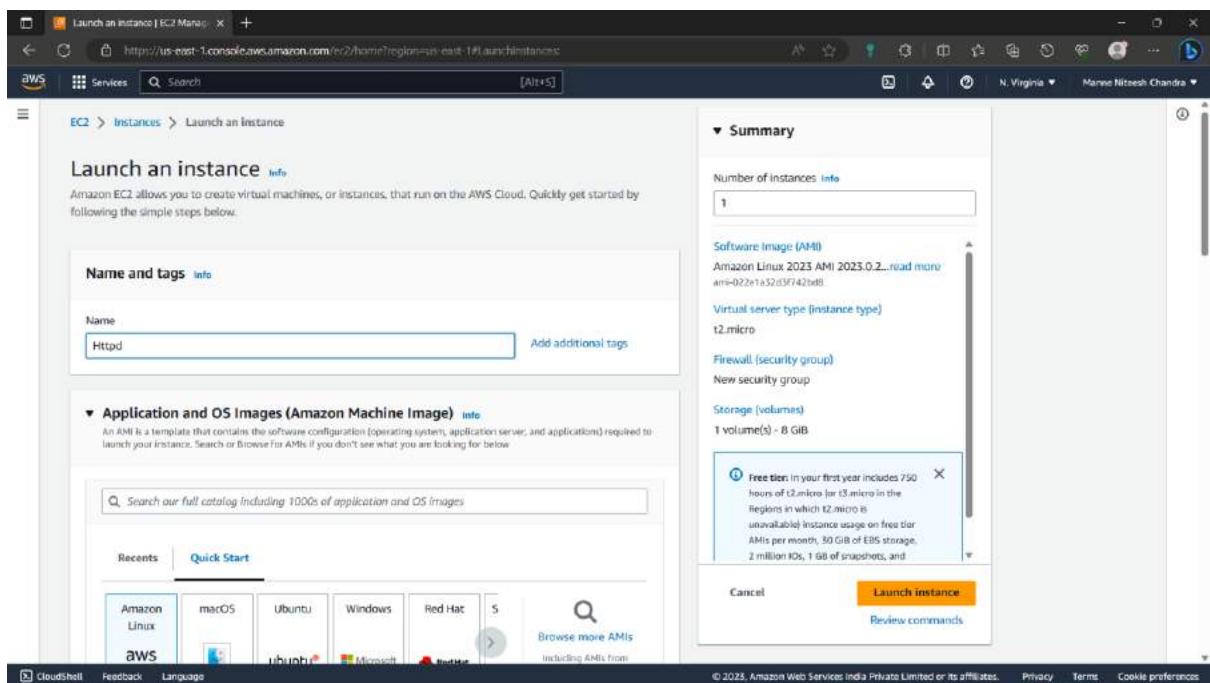
222)Now instance is created.



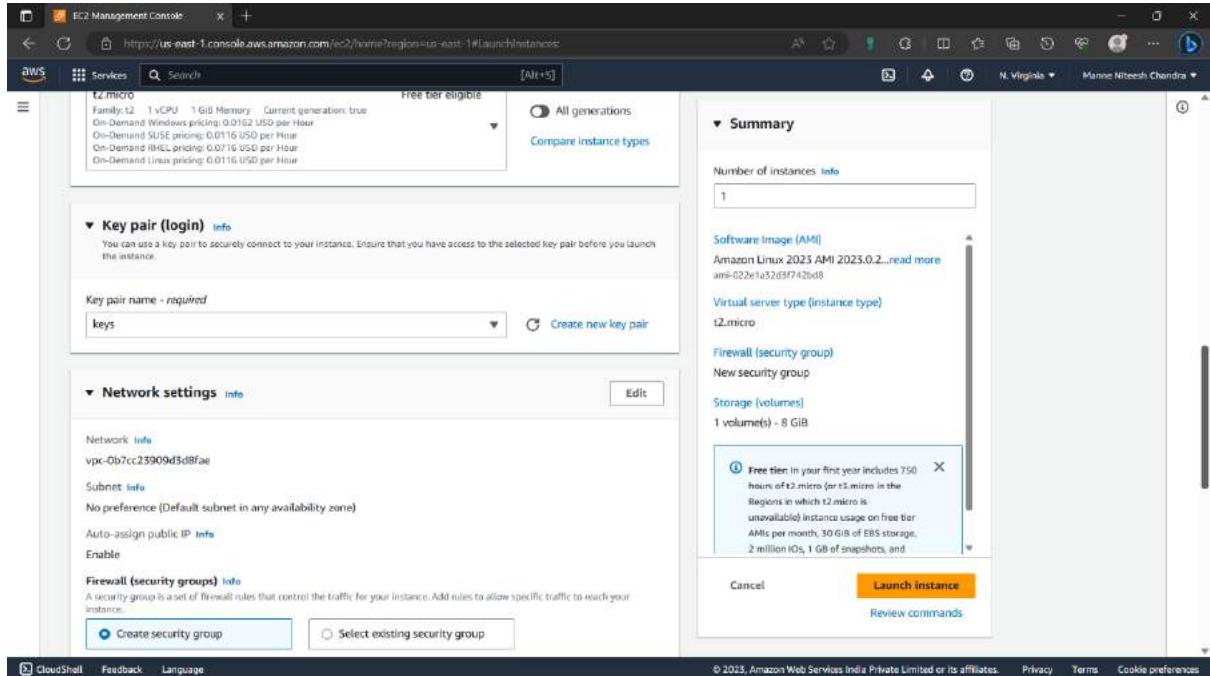
223)Select the instance you can see the details below, copy the Ipv4 address of the instance and past it in a new browser.



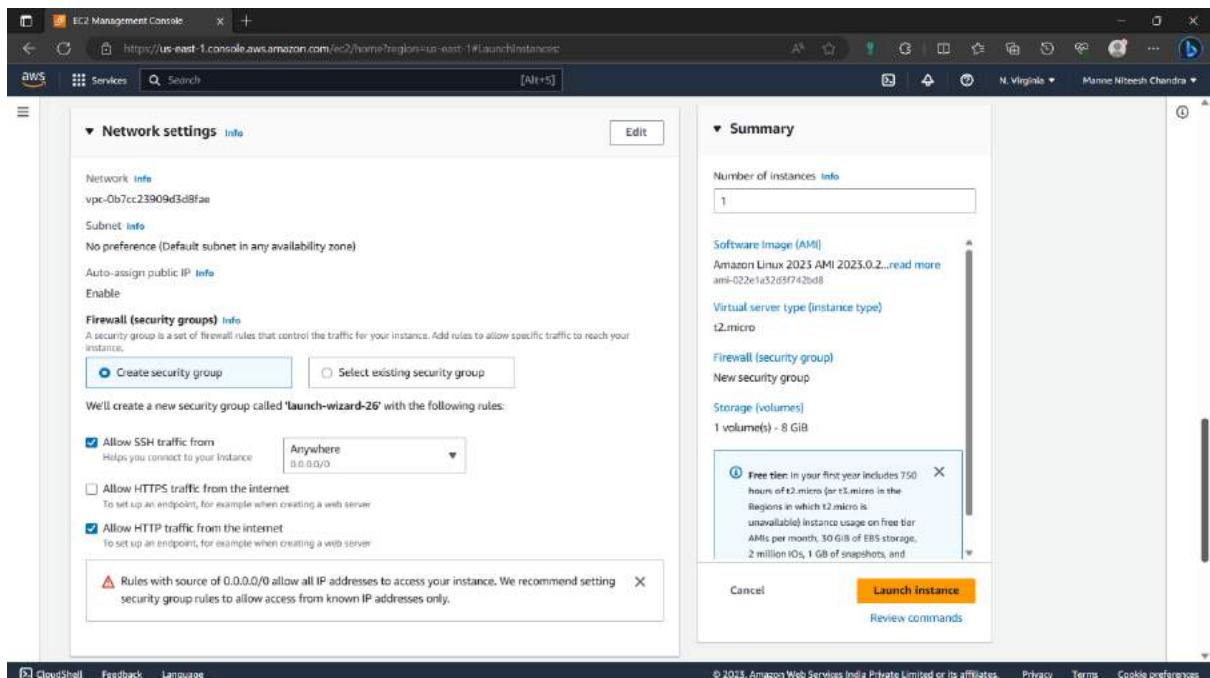
224)Now create a new instance for “Apache Httpd” , Click on “Launch instance” option. Give “Httpd” as name and let the AMI be default.



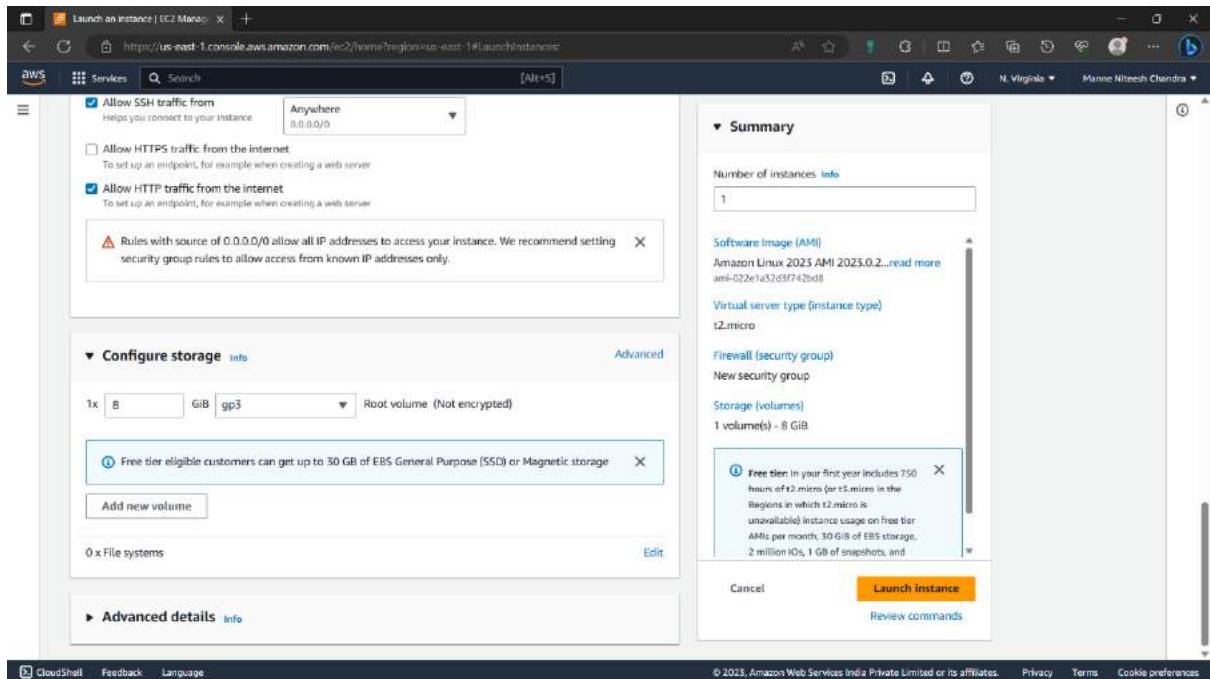
225)Select the key pair you have create new a pair key pair by clicking on “create a new key pair option”.



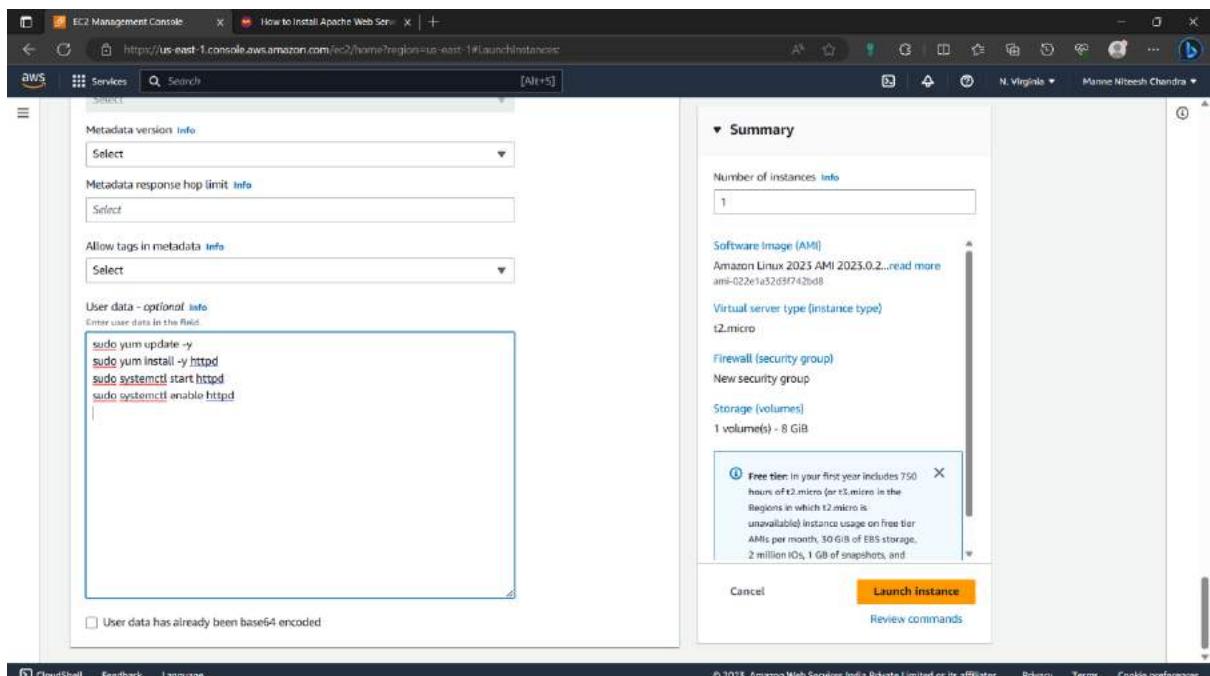
226)Enable the “Https traffic” option form “network settings”.



227) Click on “Advanced details” option below.



228) Type below commands in image in “user data” box at bottom of the page.



229) Now the instance is created.

The screenshot shows the AWS EC2 Management Console. At the top, there's a success message: "Successfully initiated launch of instance [i-0e998a934f1d37c4f]". Below it is a "Launch log" link. A "Next Steps" section follows, containing several options: "Create billing and free tier usage alerts", "Connect to your instance", "Connect an RDS database", "Create EBS snapshot policy", "Manage detailed monitoring", "Create Load Balancer", "Create AWS budget", and "Manage CloudWatch alarms". The URL in the browser is <https://us-east-1.console.aws.amazon.com/ec2/home?region=us-east-1#launchinstances>.

230) Select the instance you can see the details below, copy the Ipv4 address of the instance and past it in a new browser.

The screenshot shows a browser window with the title "Instances | EC2 Management Con... 13.233.49.156". The address bar shows "Not secure | 13.233.49.156". Below the address bar, the text "It works!" is displayed. The URL in the browser is <http://13.233.49.156>.

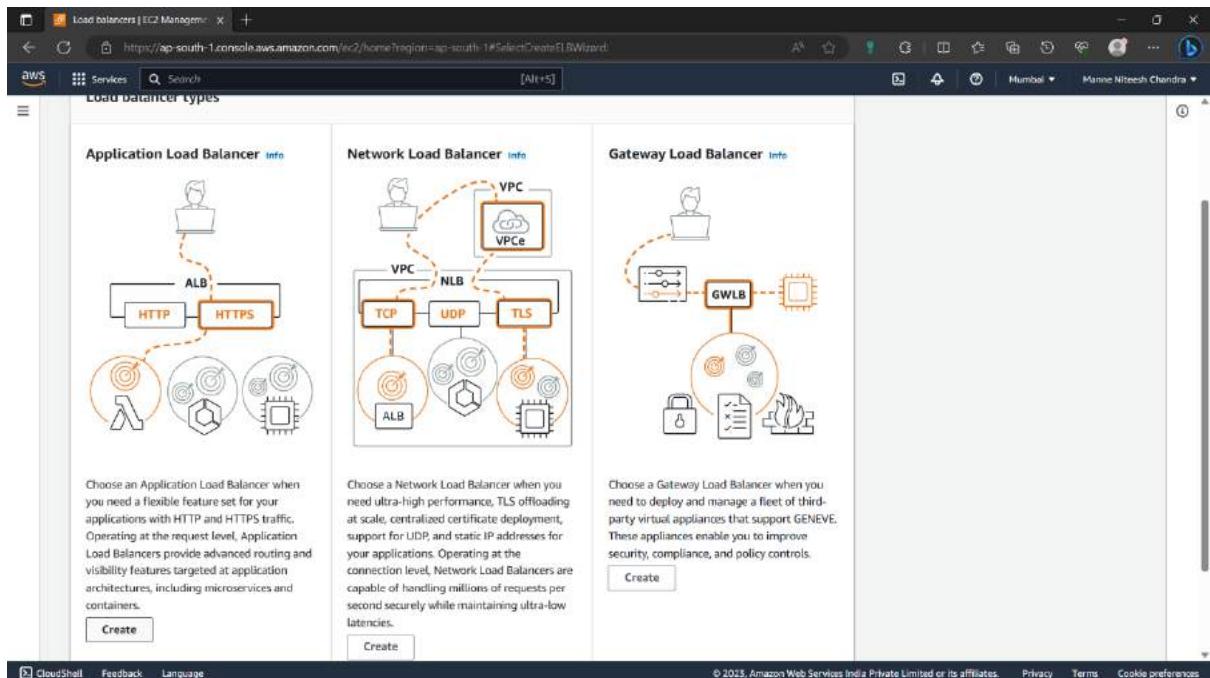
231) Click on “load balancer” in “load balancing” in below the left navigation pane.

The screenshot shows the AWS EC2 Management Console. The left navigation pane is open, showing the 'Load Balancing' section under 'Load Balancers'. The main content area displays the 'Instances (2/2)' page. It lists two instances: 'Nginx' (Instance ID: i-052a1ccb4bb4d5d16, Status: Running, Type: t2.micro) and 'Apache Httpd' (Instance ID: i-0958f1d81015bbf23, Status: Running, Type: t2.micro). Below the instance table, there is a monitoring dashboard with four graphs: CPU utilization (%), Status check failed (any), Status check failed (instance), and Status check failed (system). The status check graphs show no data available for the selected time range.

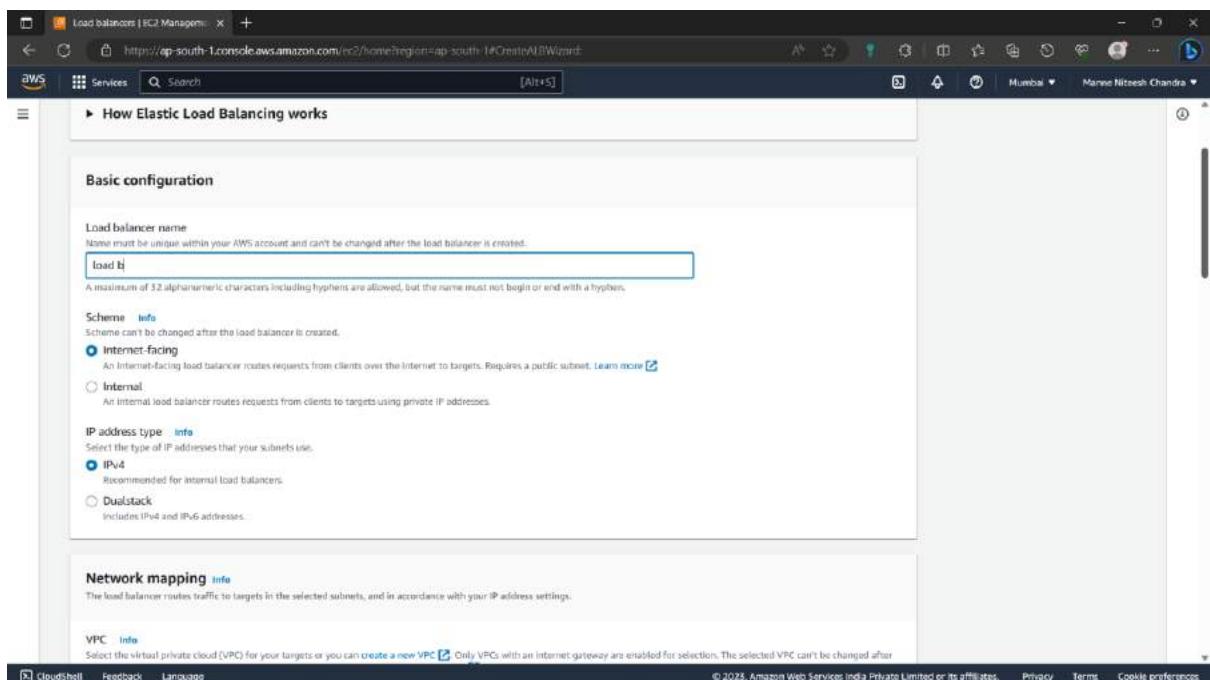
232) Click on “create load balancer” option to create load balancer.

The screenshot shows the AWS Load Balancers page. The left navigation pane is open, showing the 'Load Balancers' section under 'Load Balancing'. The main content area displays the 'Load balancers' section. It includes a search bar, a table header with columns for Name, DNS name, State, VPC ID, Availability Zones, Type, and Data, and a message stating 'No load balancers'. At the bottom of the table, there is a large orange 'Create load balancer' button. A modal window titled '0 load balancers selected' is open, with the instruction 'Select a load balancer above.'.

233)Select “Application Load Balancer” because we are creating both the EC2's under same VPC.



234)Give a name to the load balancer and let everything be default.



235)Select VPC, 2 Availability zones for subnets.

The screenshot shows the 'Create ALB Wizard' step 2 of 3. In the 'Mappings' section, two subnets are selected: 'subnet-0651a548a6e0eda7' (IPv4 address 172.31.0.0/16) under 'ap-south-1a (aps1-az1)' and 'subnet-0ba94cd0666609d9' under 'ap-south-1b (aps1-az3)'. Both subnets are assigned by AWS.

236)Port number “80” click on “create target group” below the bar in blue color.

The screenshot shows the 'Listeners and routing' section. A new listener 'HTTP:80' is being configured. The 'Protocol' is set to 'HTTP' and the 'Port' is '80'. The 'Default action' dropdown is set to 'Forward to' with the value 'Select a target group'. Below this, a blue button labeled 'Create target group' is visible. At the bottom of the page, there is an 'Add listener' button.

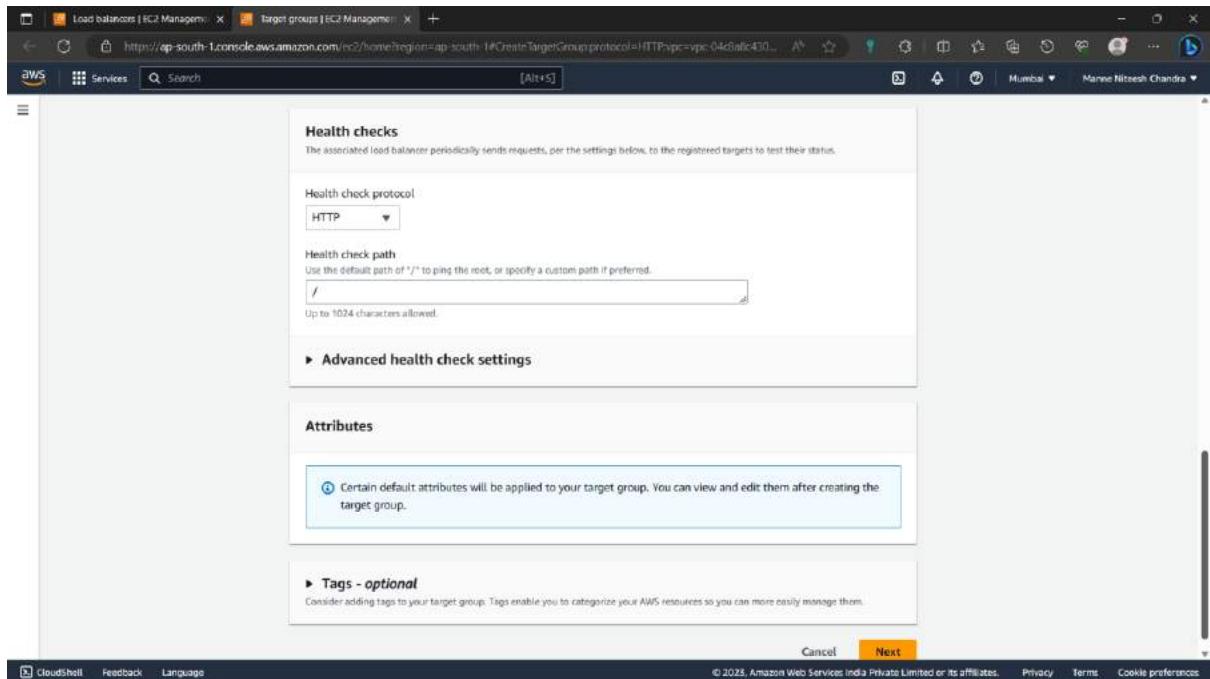
237) Now the target group is opened in new tab and select the “instance” option.

The screenshot shows the 'Specify group details' step of creating a target group. Under 'Basic configuration', the 'Instances' option is selected. It includes a note: 'Supports load balancing to instances within a specific VPC' and 'Facilitates the use of Amazon EC2 Auto Scaling to manage and scale your EC2 capacity'. Other options like 'IP addresses', 'Lambda function', and 'Application Load Balancer' are also listed with their respective descriptions.

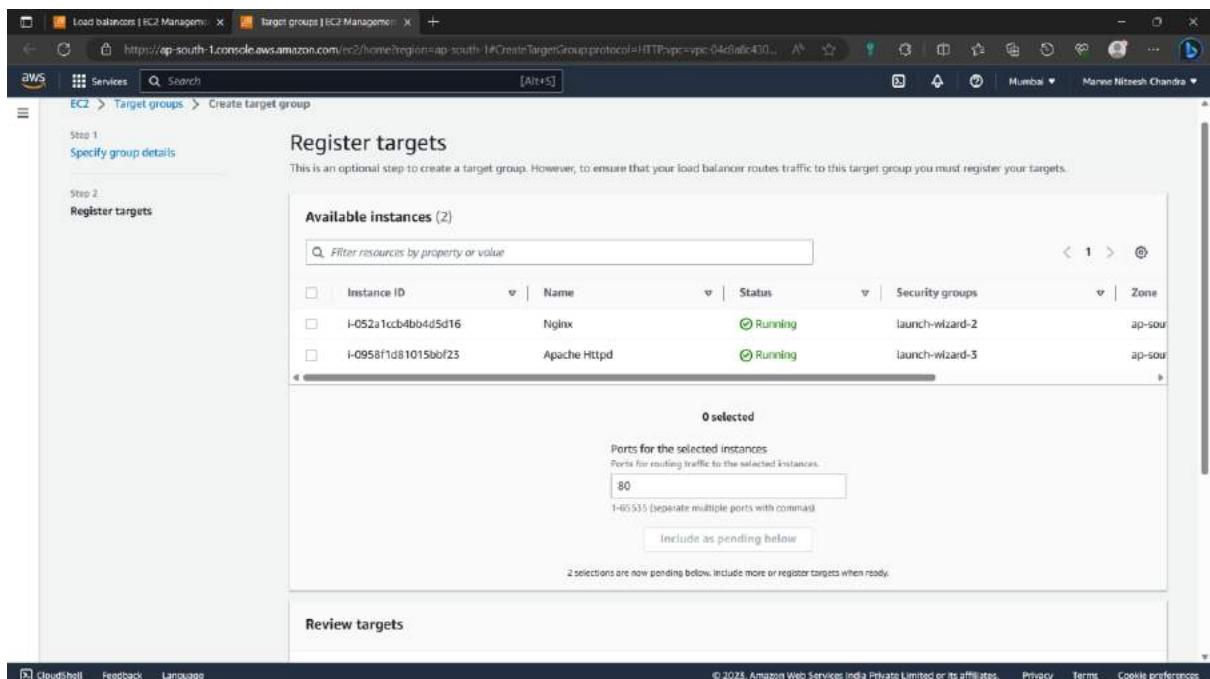
238) Give a name to the target group and let everything be default.

The screenshot shows the continuation of the target group creation process. The 'Target group name' field is filled with 'load b'. The 'Protocol' section shows 'HTTP' selected with port '80'. The 'VPC' section lists a single VPC entry: 'vpc-0dcb8c4041e013d IPv4: 172.31.0.0/16'. The 'Protocol version' section has 'HTTP1' selected. At the bottom, there is a 'Health checks' section which is currently empty.

239)Click on “next”.



240)Select both the instances and click on “Including pending as below”.



241)Click on “Create target group”.

The screenshot shows the 'Target groups' creation page in the AWS EC2 Management console. At the top, there's a section for 'Ports for the selected instances' with a dropdown set to '80'. Below it, a note says '2 selections are now pending below. Include more or register targets when ready.' A 'Review targets' section lists two pending targets:

Remove	Health status	Instance ID	Name	Port	State	Security groups	Zone	Subnet
X	Pending	i-052a1ccb4bb4d5d16	Nginx	80	Running	launch-wizard-2	ap-south-1b	subnet-00000000
X	Pending	i-0958f1d81015b723	Apache Httpd	80	Running	launch-wizard-3	ap-south-1b	subnet-00000000

At the bottom right, there are 'Cancel', 'Previous', and 'Create target group' buttons. The 'Create target group' button is highlighted in orange.

242)Now the target group is created.

The screenshot shows the 'Target groups' page in the AWS EC2 Management console. A green success message at the top says 'Successfully created target group: loadb'. The main table displays one target group:

Name	ARN	Port	Protocol	Target type	Load balancer
loadb	arnawselasticloadbalanc...	80	HTTP	Instance	(None associated)

Below the table, a message says '0 target groups selected' and 'Select a target group above.'

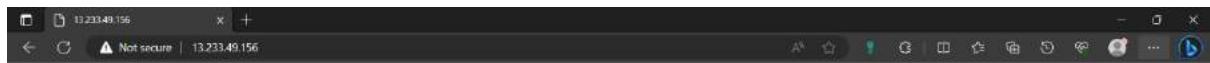
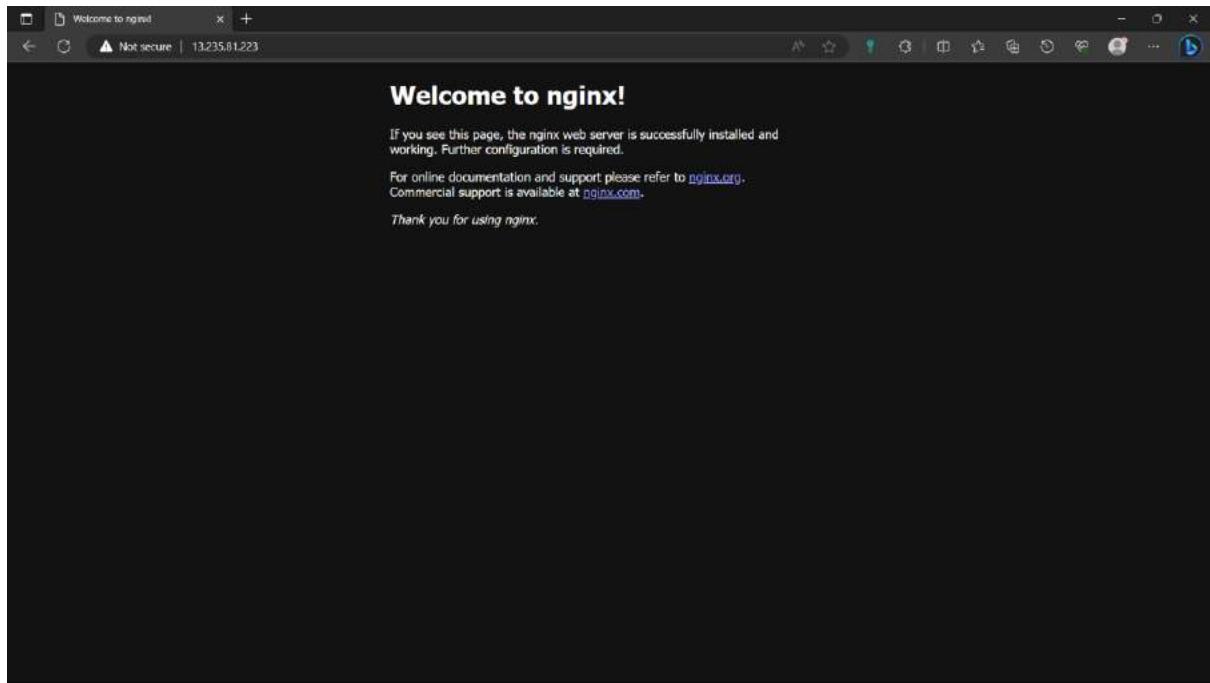
243) Go to the load balancer page and click on the refresh below which is beside the bar and select the created target group.

The screenshot shows the 'Listeners and routing' section of the AWS Load Balancers | EC2 Management console. It displays a single listener configuration for port 80, set to forward traffic to a target group named 'loadb'. Below the listener, there's a section for 'Listener tags - optional' and a link to 'Add-on services - optional'. At the bottom of the page, there's a note about AWS Global Accelerator and standard footer links for CloudShell, Feedback, Language, Privacy, Terms, and Cookie preferences.

244) Click on “create load balancer”, The load balancer is created and assigned to the instances once refresh the load balancer and open the web pages of the instances by copying their Ipv4 addresses.

The screenshot shows the 'Create Application Load Balancer' page after successful creation. A green banner at the top indicates 'Successfully created load balancer: loadb'. Below the banner, a note states that it might take a few minutes for the load balancer to be fully set up and ready to route traffic. The main content area shows the 'Create Application Load Balancer' form with a 'Suggested next steps' box containing two bullet points: 'Review, customize, or configure attributes for your load balancer and listeners using the Description and Listeners tabs within loadb.' and 'Discover other services that you can integrate with your load balancer. Visit the Integrated services tab within loadb.'. A 'View load balancer' button is located at the bottom right of the form. The page includes standard footer links for CloudShell, Feedback, Language, Privacy, Terms, and Cookie preferences.

245)Now the webpages are opened.



ASL and LG:

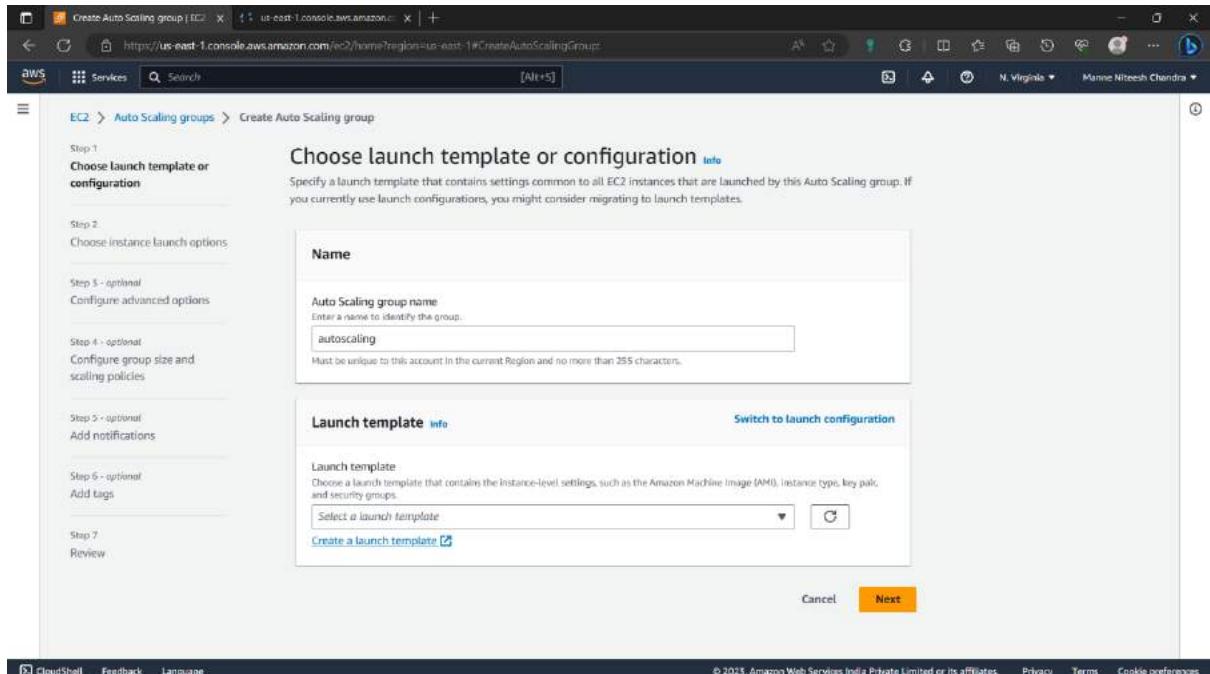
246)Click on “Auto Scaling Group” option “Auto Scaling” which is below the navigation panel of EC2.\

The screenshot shows the AWS EC2 Management Dashboard. On the left, there's a navigation pane with various options like Dedicated Hosts, Scheduled Instances, Capacity Reservations, Images, AMIs, Elastic Block Store, Volumes, Snapshots, Lifecycle Manager, Network & Security, Load Balancing, Auto Scaling, and Auto Scaling Groups. The 'Auto Scaling Groups' option is highlighted. The main content area has sections for Resources (listing Instances (running), Auto Scaling Groups, Dedicated Hosts, etc.), Launch instance (with 'Launch instance' and 'Migrate a server' buttons), Service health (showing the service is operating normally), and Scheduled events (listing US East (N. Virginia)). On the right, there are boxes for Account attributes (Supported platforms: VPC, Default VPC: vpc-0b7cc25909d3d8fae, Settings, EBS encryption, Zones, EC2 Serial Console, Default credit specification, Console experiments), Explore AWS (10 Things You Can Do Today to Reduce AWS Costs, Get Up to 40% Better Price Performance), and a footer with copyright information.

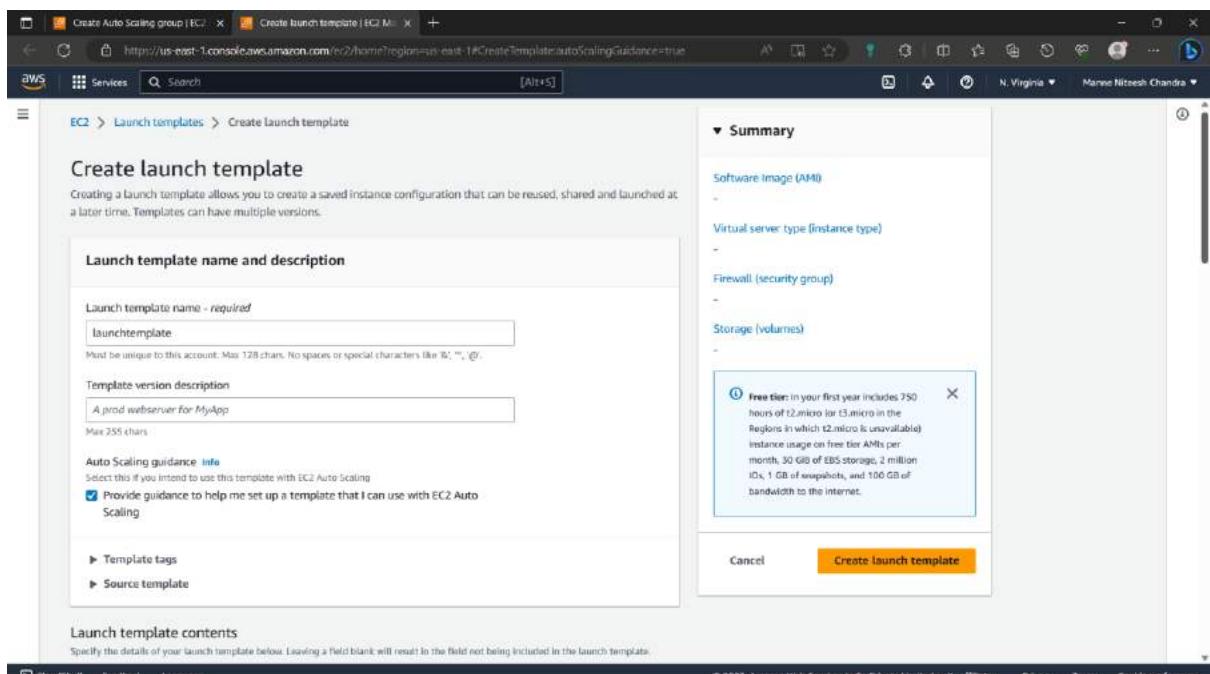
247)Click on “create auto scaling group” option.

The screenshot shows the AWS Auto Scaling Groups page. The left sidebar includes the same navigation options as the previous dashboard, with 'Auto Scaling Groups' selected. The main content features a large banner with the text "Amazon EC2 Auto Scaling helps maintain the availability of your applications". Below it, a diagram illustrates how an Auto Scaling group works: it shows four squares representing EC2 instances, with one dashed square labeled "Scale out as needed". Labels indicate "Auto Scaling group", "Minimum size", "Desired capacity", and "Scale out as needed". To the right, there are sections for "Pricing" (describing no additional fees beyond service fees for Amazon EC2, CloudWatch, and other AWS resources) and "Getting started" (with a link to "What is Amazon EC2 Auto Scaling?"). A prominent orange "Create Auto Scaling group" button is located in the center-right area.

248) Give a name to the auto scaling and click on “create a launch template” in “Launch template” option.



249) The launch template creation is opened in a new tab. Give a name to the launch template.



250)Select the AMI “Ubuntu” let everything be default.

The screenshot shows the 'Create launch template' wizard on the AWS EBS console. The current step is 'Software Image (AMI)'. A tooltip for the 'Free tier' is displayed, stating: 'In your first year includes 750 hours of t2.micro (or t3.micro in the Regions in which t2.micro is unavailable) instance usage on free tier AMIs per month, 50 GB of EBS storage, 2 million I/Os, 1 GB of snapshots, and 100 GB of bandwidth to the internet.' The 'Create launch template' button is highlighted in orange at the bottom right.

251)Instance type-“t2.micro”,key pair-keys(you have in your machine i.e., you created).

The screenshot shows the 'Create launch template' wizard on the AWS EBS console. The current step is 'Summary'. It shows the selected instance type as 't2.micro' and the key pair as 'keys'. A tooltip for the 'Free tier' is displayed, stating: 'In your first year includes 750 hours of t2.micro (or t3.micro in the Regions in which t2.micro is unavailable) instance usage on free tier AMIs per month, 50 GB of EBS storage, 2 million I/Os, 1 GB of snapshots, and 100 GB of bandwidth to the internet.' The 'Create launch template' button is highlighted in orange at the bottom right.

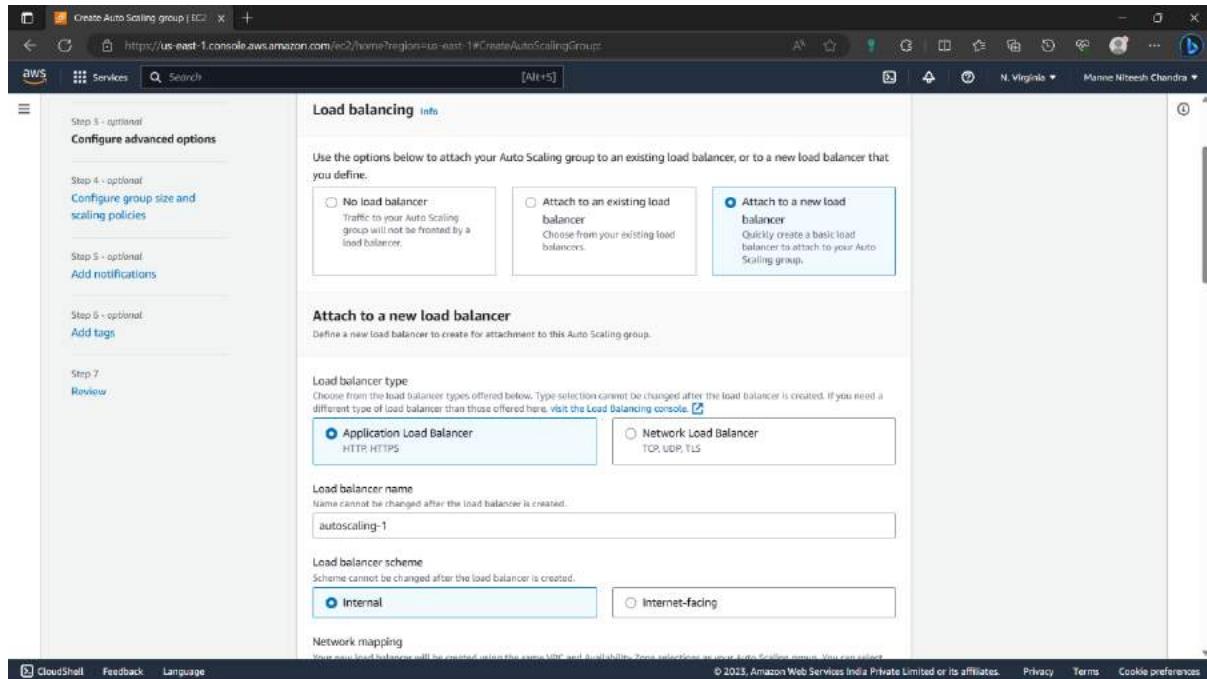
252) In network settings no need to select the subnet let everything be default and click on “Create launch template”.

The screenshot shows the 'Network settings' step of the 'Create launch template' wizard. It includes sections for Subnet info, Firewall (security groups), Common security groups, Advanced network configuration, and Subnet info. A summary panel on the right lists the software image (AMIs), virtual server type (instance type), firewall, storage, and a note about free tier benefits. At the bottom right is a 'Create launch template' button.

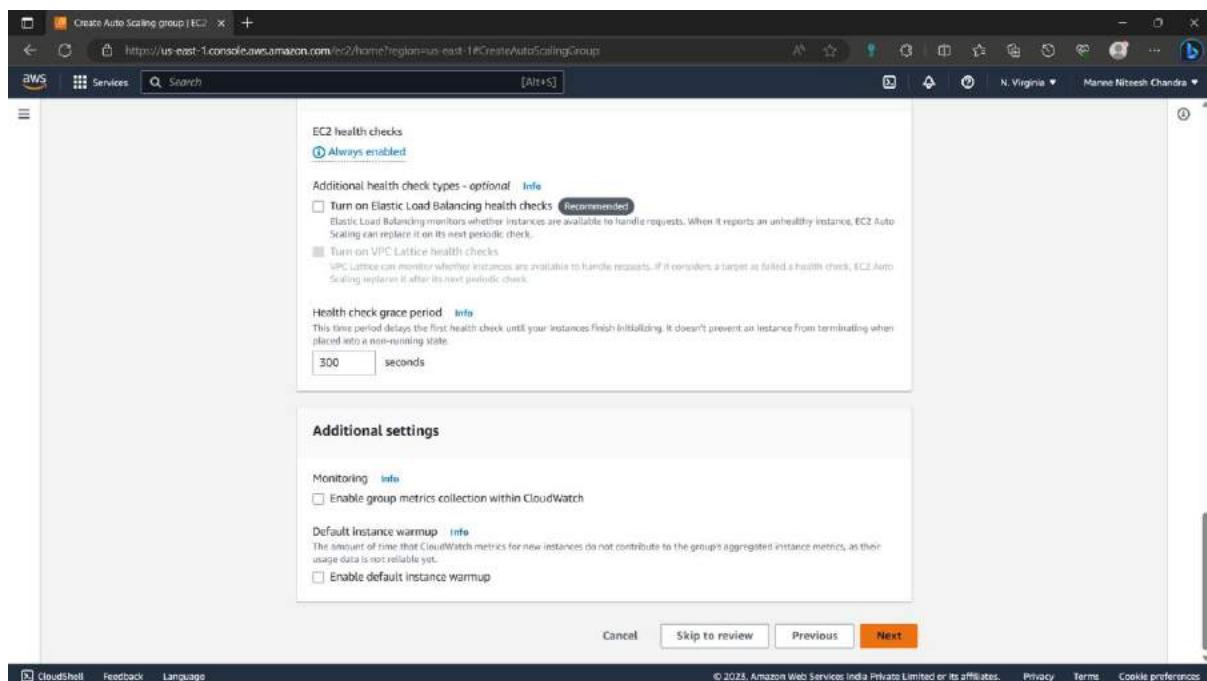
253) Launch template is created.

The screenshot shows the 'Success' message for creating the launch template 'launchtemplate (lt-0f52732e7622aa4b)'. It includes a 'Actions log' section, a 'Next steps' section with links for 'Launch an instance', 'Create an Auto Scaling group from your template', 'Create a Spot Fleet', and a 'View launch templates' button at the bottom right.

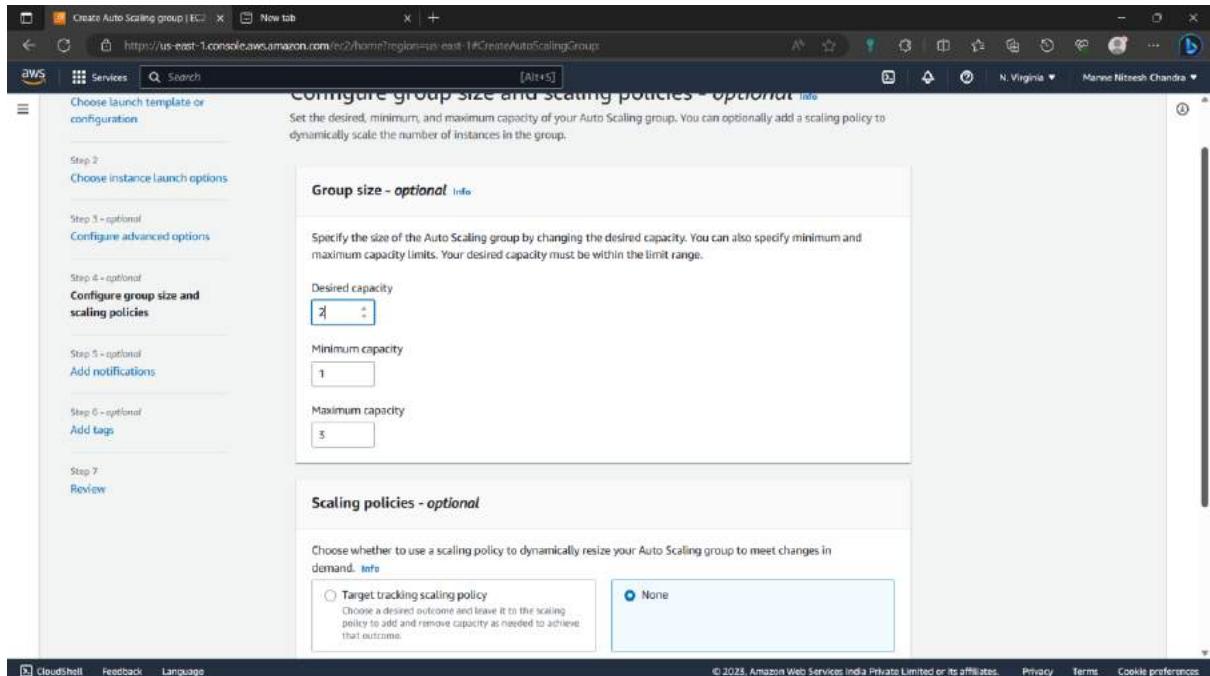
254) Go back to the auto scaling tab and select the created launch template and click on “next”. Select “Attach to a new load balancer” because I didn’t have a load balancer. If you have a load balancer attach it.



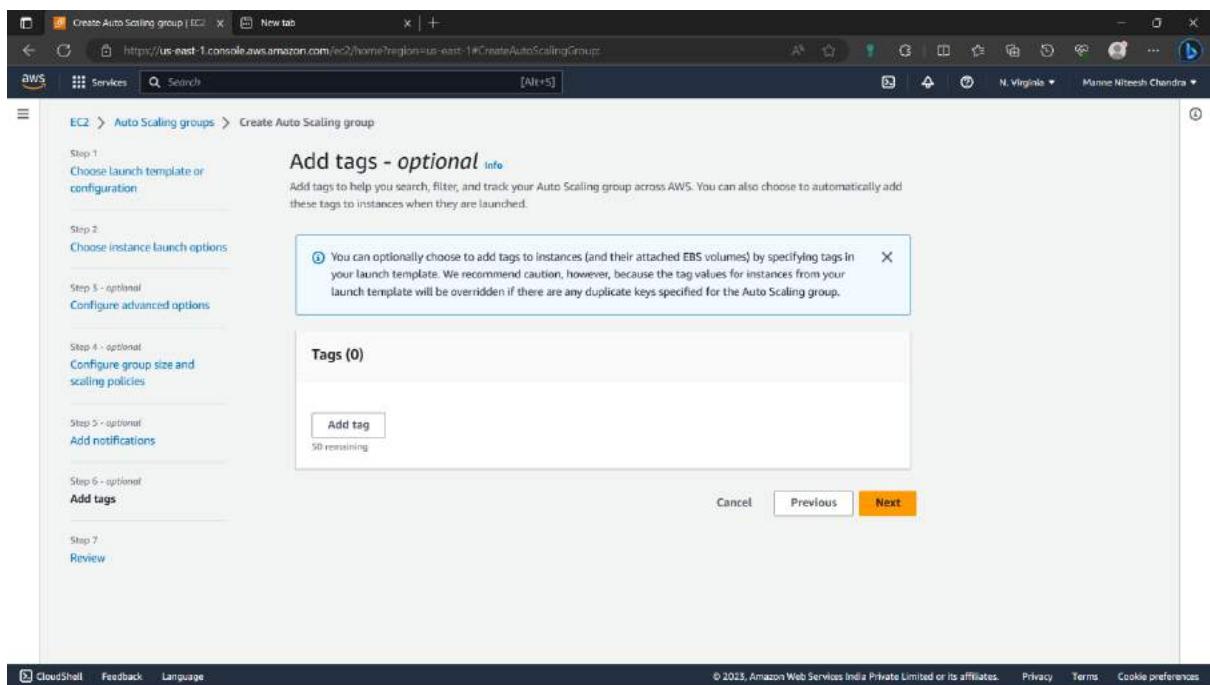
255) Click on “Next”.



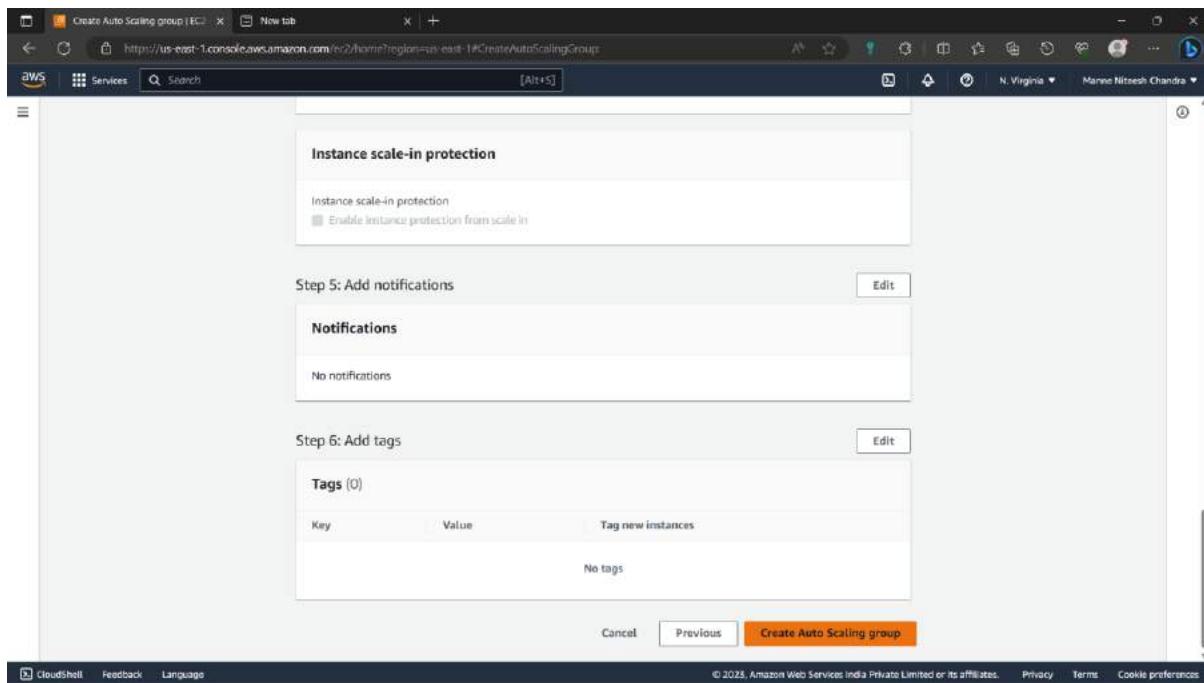
256) Give Desired, Maximum, Minimum capacity values (your choice) and click on “Next”.



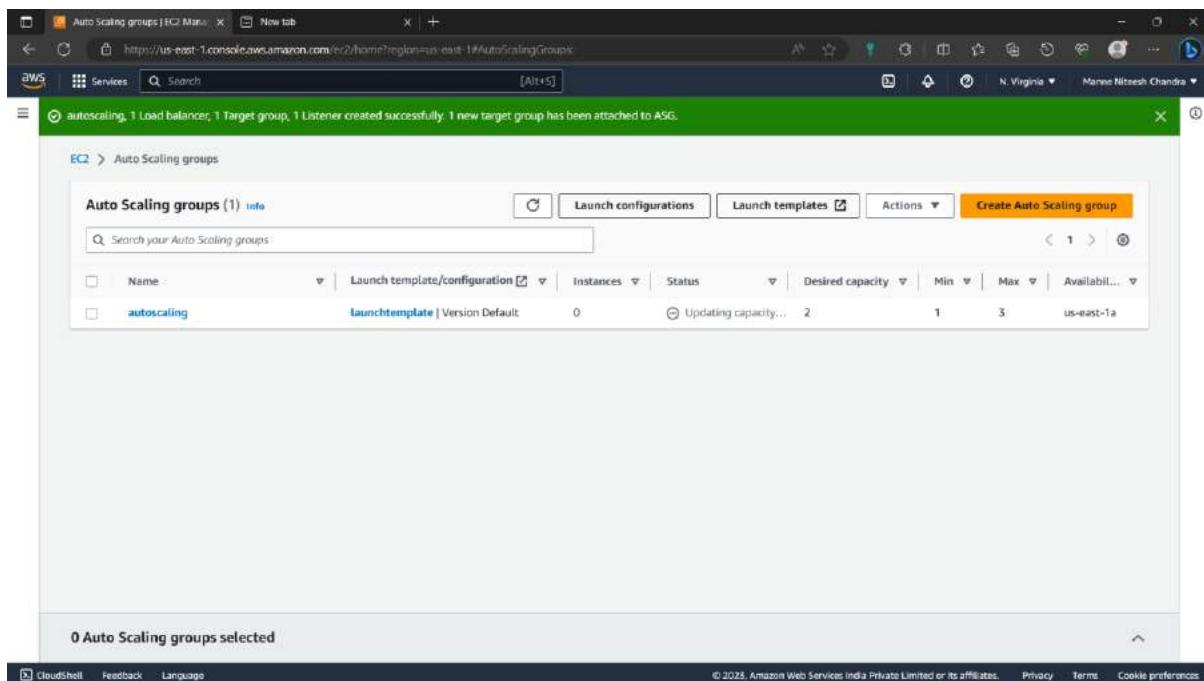
257) Click on “next” for step-5,6.



258) Review all the details and click on “Create Auto Scaling Group”.



259) The Auto Scaling Group is created.



260) Go to “Instances” you can see the instances running(Instances without names) according to the capacity of users.

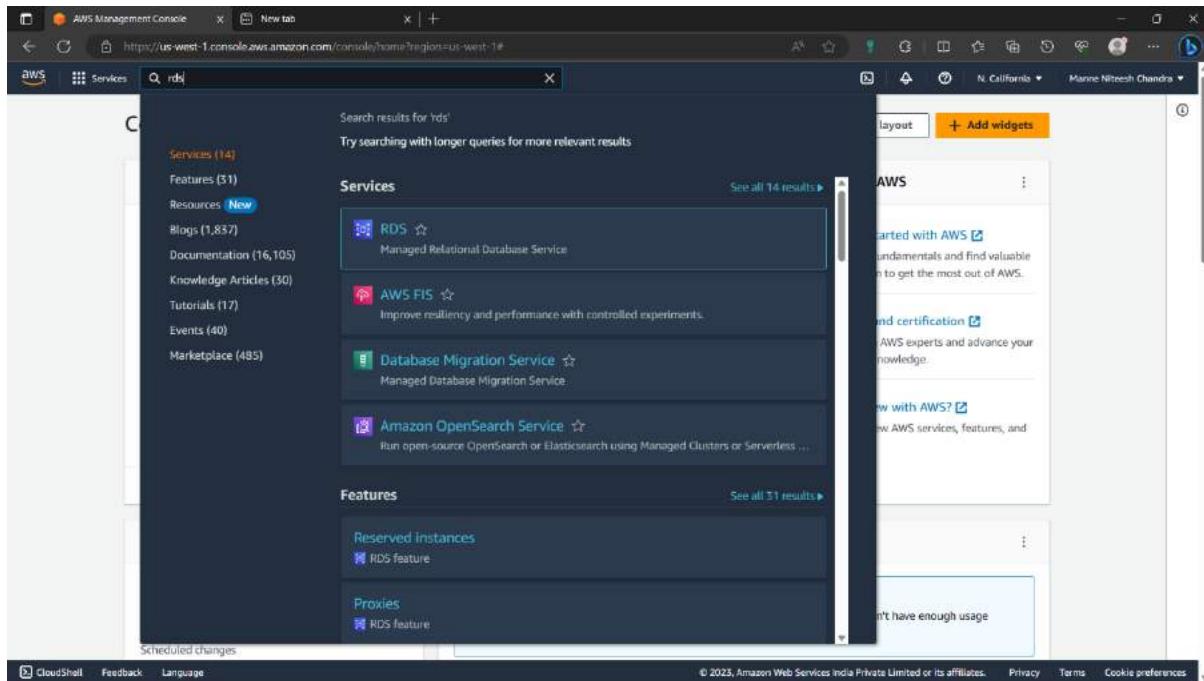
The screenshot shows the AWS EC2 Instances page. The left sidebar navigation includes: EC2 Dashboard, EC2 Global View, Events, Limits, Instances (selected), Instances, Instance Types, Launch Templates, Spot Requests, Savings Plans, Reserved Instances, Dedicated Hosts, Scheduled Instances, Capacity Reservations, Images (AMIs, AMI Catalog), and Elastic Block Store (Volumes, Snapshots). The main content area displays a table titled "Instances (7) info" with the following data:

Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone	Public IPv4 DNS
Apache	i-025c8bcd00cc057e9b	Terminated	t2.micro	-	No alarms	us-east-1d	-
Nginx	i-0486cc35b7f44eb14	Terminated	t2.micro	-	No alarms	us-east-1d	-
Httpd	i-0e998a934f1d37c4f	Terminated	t2.micro	-	No alarms	us-east-1d	-
Apache Tomcat	i-0a821ab58995acf1e	Terminated	t2.micro	-	No alarms	us-east-1d	-
-	i-0f1bd3f01dea01b2	Running	t2.micro	Initializing	No alarms	us-east-1a	ec2-34-220-252-
-	i-08bc4ff2d47d6fb62	Running	t2.micro	Initializing	No alarms	us-east-1a	ec2-54-162-254-
Nginx1	i-07fe587e7789d5aea	Terminated	t2.micro	-	No alarms	us-east-1c	-

A modal window titled "Select an instance" is open at the bottom, showing the same list of instances.

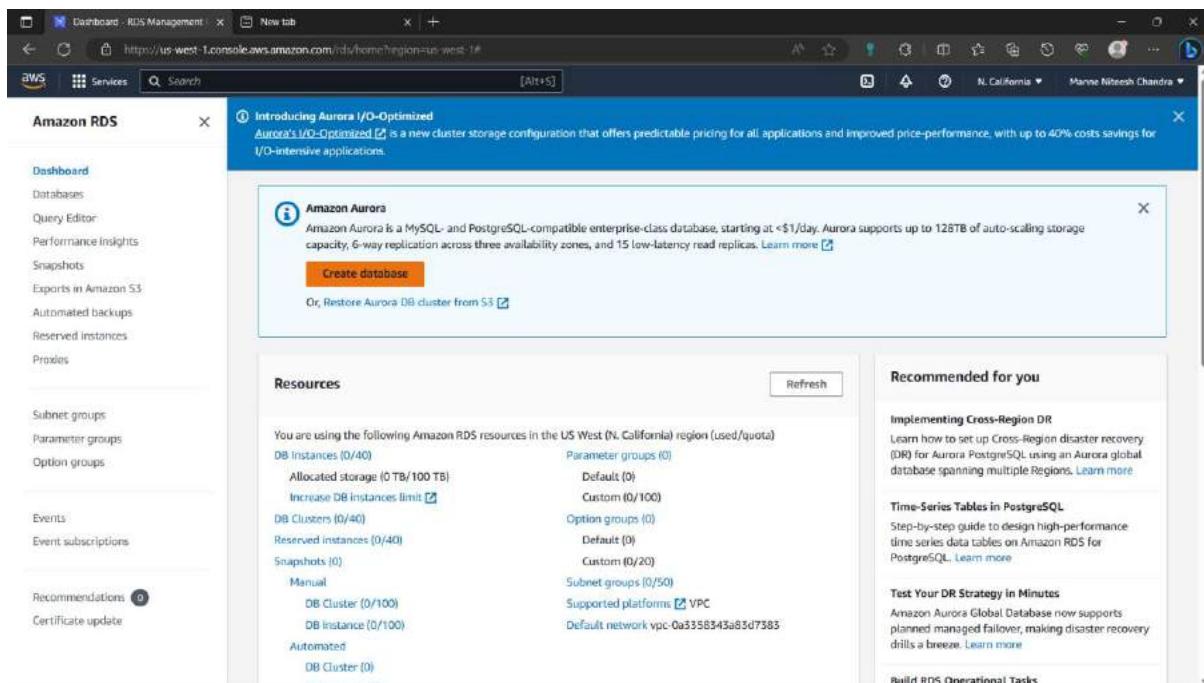
RDS:

261) Type “RDS” in search bar and select the “RDS” option from below.



The screenshot shows the AWS Management Console search results for 'rds'. The 'RDS' service card is highlighted, showing it's a Managed Relational Database Service. Other services listed include AWS FIS, Database Migration Service, and Amazon OpenSearch Service.

262) Click on “Create database” option.



The screenshot shows the Amazon RDS Management Dashboard. The 'Create database' button is visible on the main page under the 'Amazon Aurora' section. The dashboard also displays various RDS resources and recommendations.

263)database creation method-“standard method”, Engine option- “MySql”.

The screenshot shows the 'Create database' page in the AWS RDS Management console. At the top, there are two options: 'Standard create' (selected) and 'Easy create'. Below this, the 'Engine options' section is shown, with 'MySQL' selected from a list that also includes Aurora (MySQL Compatible), Aurora (PostgreSQL Compatible), MariaDB, PostgreSQL, Oracle, and Microsoft SQL Server.

264)Template-“Free tier”.

The screenshot shows the 'Create database' page in the AWS RDS Management console, specifically for the 'Free tier' template. It includes a note about known issues, a dropdown for 'Engine Version' (set to MySQL 8.0.32), and a 'Templates' section where 'Free tier' is selected. The 'Settings' section at the bottom shows the 'DB instance identifier' is set to 'database-1'.

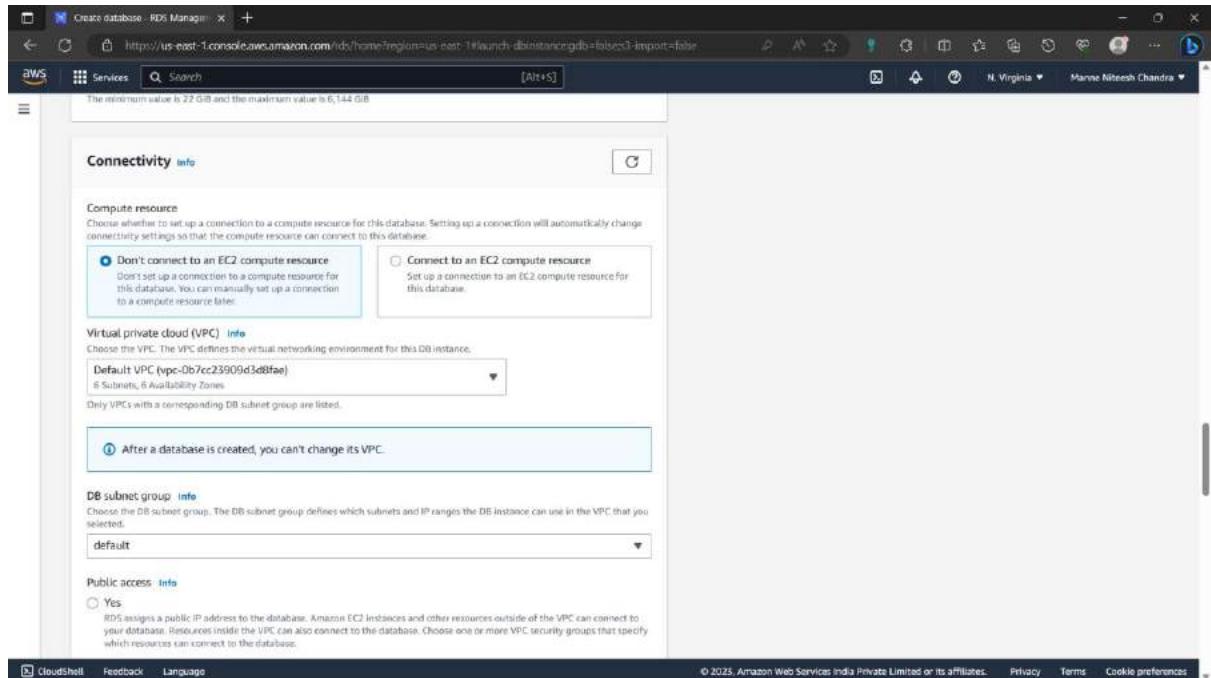
265) Give a name to the database and give a password to the admin in “credential settings”.

The screenshot shows the AWS RDS Create Database - RDS Manager interface. In the 'Database identifier' field, 'database-1' is entered. Under 'Master username', 'admin' is typed. A note states: 'If you manage the master user credentials in Secrets Manager, some RDS features aren't supported.' Below this, there are fields for 'Master password' and 'Confirm master password', both containing '*****'. At the bottom, the 'Instance configuration' section is visible.

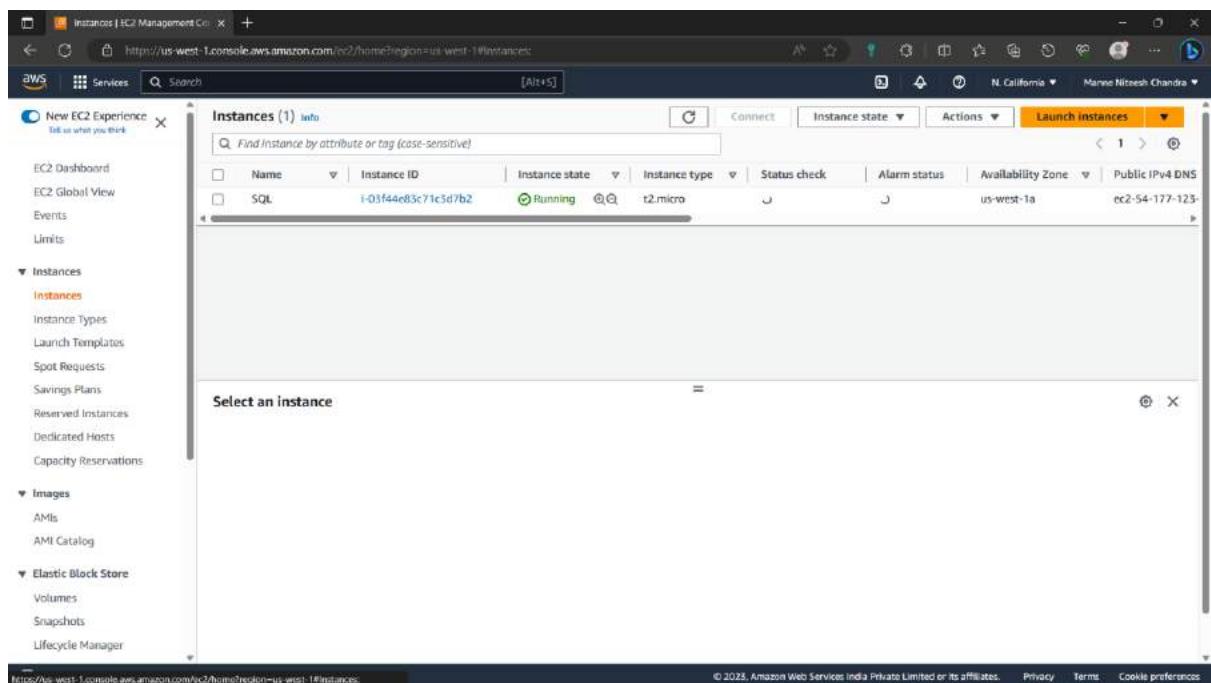
257) Instance configuration-“Burstable class”, Storage type- “General purpose”.

The screenshot shows the 'Instance configuration' section of the AWS RDS Create Database - RDS Manager interface. Under 'Amazon RDS Optimized Writes - new', it says 'Show instance classes that support Amazon RDS Optimized Writes'. Under 'DB instance class', 'Burstable classes (includes t classes)' is selected. The dropdown shows 'db.t3.micro' (2 vCPUs, 1 GB RAM, Network: 2,085 Mbps). The 'Storage' section shows 'General Purpose SSD (gp2)' selected. At the bottom, 'Allocated storage' is listed as 'Info'.

258)Connectivity-Don't connect to EC2(you're choice), Select VPC and let everything be default and click on “Create database”.

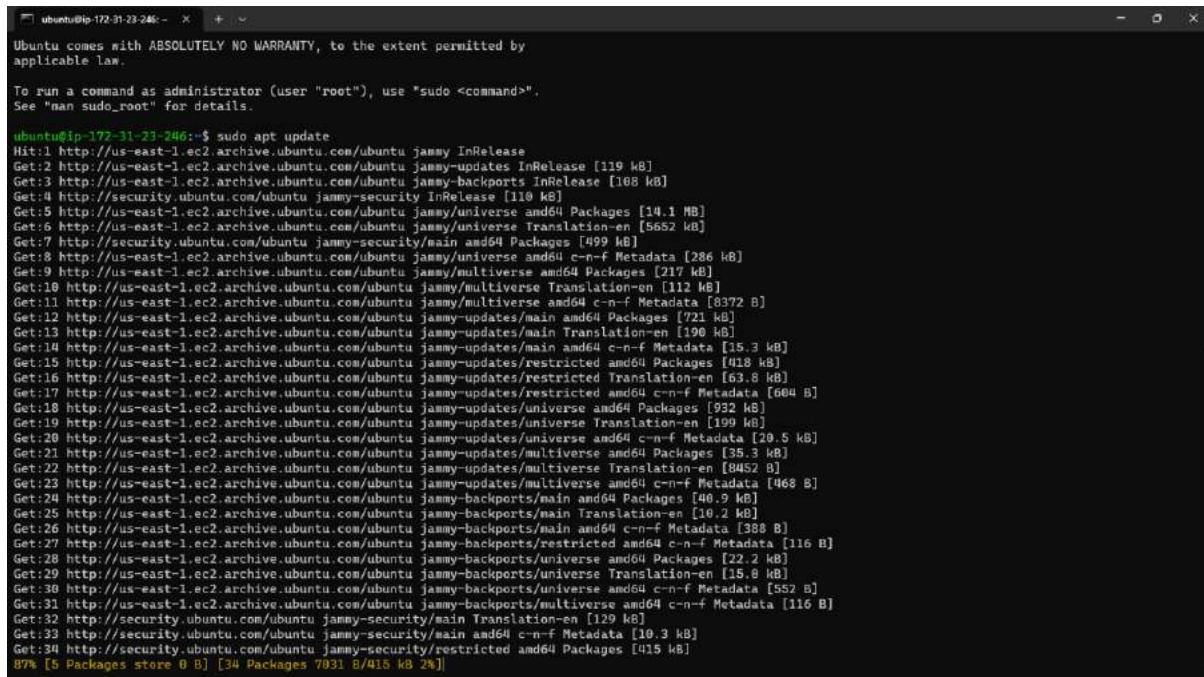


259)Now open the EC2 instance in the vpc (given in database) if you don't have the VPC, Create the vpc by following the steps-(129-140).



260) Access the instance by following the instructions from steps:(141-146). And type the command

“sudo apt update”: To install the terminal to latest version.

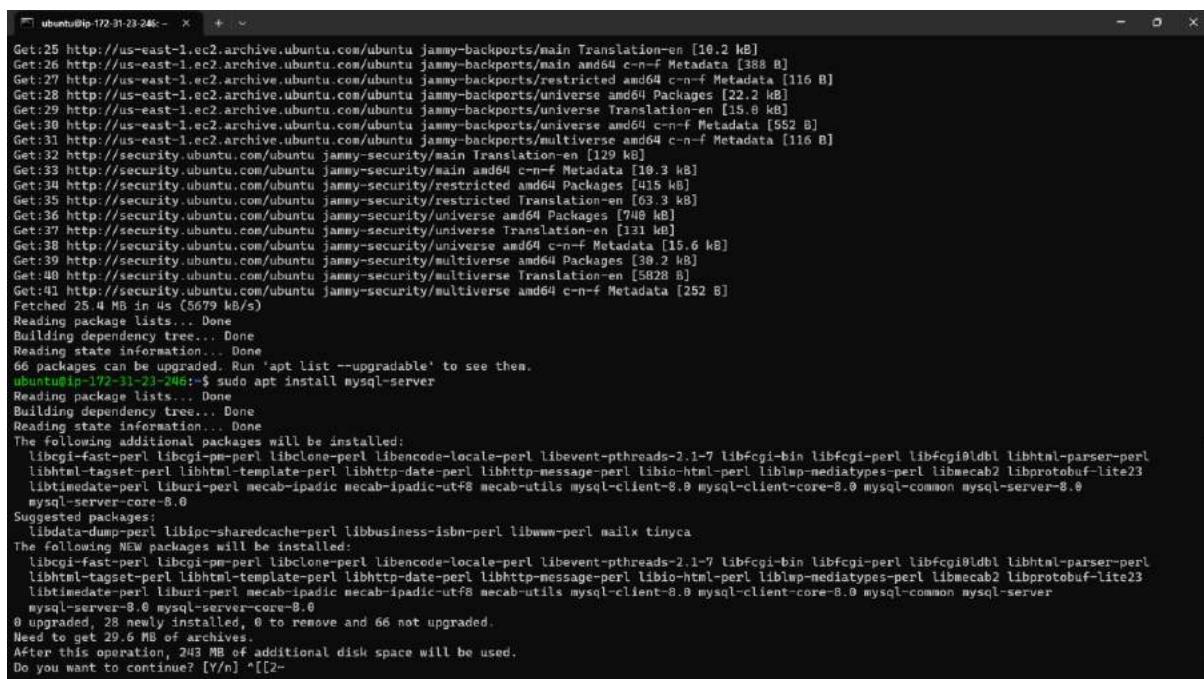


```
ubuntu@ip-172-31-23-246:~$ sudo apt update
Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

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

ubuntu@ip-172-31-23-246:~$ sudo apt update
Hit:1 http://us-east-1.ec2.archive.ubuntu.com/ubuntu jammy InRelease
Get:2 http://us-east-1.ec2.archive.ubuntu.com/ubuntu jammy-updates InRelease [119 kB]
Get:3 http://us-east-1.ec2.archive.ubuntu.com/ubuntu jammy-backports InRelease [108 kB]
Get:4 http://security.ubuntu.com/ubuntu jammy-security InRelease [110 kB]
Get:5 http://us-east-1.ec2.archive.ubuntu.com/ubuntu jammy/universe amd64 Packages [14.1 MB]
Get:6 http://us-east-1.ec2.archive.ubuntu.com/ubuntu jammy/universe Translation-en [5652 kB]
Get:7 http://security.ubuntu.com/ubuntu jammy-security/main amd64 Packages [499 kB]
Get:8 http://us-east-1.ec2.archive.ubuntu.com/ubuntu jammy/universe amd64 c-n-f Metadata [286 kB]
Get:9 http://us-east-1.ec2.archive.ubuntu.com/ubuntu jammy/multiverse amd64 Packages [217 kB]
Get:10 http://us-east-1.ec2.archive.ubuntu.com/ubuntu jammy/multiverse Translation-en [112 kB]
Get:11 http://us-east-1.ec2.archive.ubuntu.com/ubuntu jammy/multiverse amd64 c-n-f Metadata [8372 B]
Get:12 http://us-east-1.ec2.archive.ubuntu.com/ubuntu jammy-updates/main amd64 Packages [721 kB]
Get:13 http://us-east-1.ec2.archive.ubuntu.com/ubuntu jammy-updates/main Translation-en [190 kB]
Get:14 http://us-east-1.ec2.archive.ubuntu.com/ubuntu jammy-updates/main amd64 c-n-f Metadata [15.3 kB]
Get:15 http://us-east-1.ec2.archive.ubuntu.com/ubuntu jammy-updates/restricted amd64 Packages [418 kB]
Get:16 http://us-east-1.ec2.archive.ubuntu.com/ubuntu jammy-updates/restricted Translation-en [63.8 kB]
Get:17 http://us-east-1.ec2.archive.ubuntu.com/ubuntu jammy-updates/restricted amd64 c-n-f Metadata [604 kB]
Get:18 http://us-east-1.ec2.archive.ubuntu.com/ubuntu jammy-updates/universe amd64 Packages [932 kB]
Get:19 http://us-east-1.ec2.archive.ubuntu.com/ubuntu jammy-updates/universe Translation-en [199 kB]
Get:20 http://us-east-1.ec2.archive.ubuntu.com/ubuntu jammy-updates/universe amd64 c-n-f Metadata [20.5 kB]
Get:21 http://us-east-1.ec2.archive.ubuntu.com/ubuntu jammy-updates/multiverse amd64 Packages [35.3 kB]
Get:22 http://us-east-1.ec2.archive.ubuntu.com/ubuntu jammy-updates/multiverse Translation-en [8452 kB]
Get:23 http://us-east-1.ec2.archive.ubuntu.com/ubuntu jammy-updates/multiverse amd64 c-n-f Metadata [468 kB]
Get:24 http://us-east-1.ec2.archive.ubuntu.com/ubuntu jammy-backports/main amd64 Packages [46.9 kB]
Get:25 http://us-east-1.ec2.archive.ubuntu.com/ubuntu jammy-backports/main Translation-en [10.2 kB]
Get:26 http://us-east-1.ec2.archive.ubuntu.com/ubuntu jammy-backports/main amd64 c-n-f Metadata [388 kB]
Get:27 http://us-east-1.ec2.archive.ubuntu.com/ubuntu jammy-backports/restricted amd64 c-n-f Metadata [116 kB]
Get:28 http://us-east-1.ec2.archive.ubuntu.com/ubuntu jammy-backports/restricted amd64 c-n-f Metadata [116 kB]
Get:29 http://us-east-1.ec2.archive.ubuntu.com/ubuntu jammy-backports/universe amd64 c-n-f Metadata [116 kB]
Get:30 http://us-east-1.ec2.archive.ubuntu.com/ubuntu jammy-backports/universe Translation-en [129 kB]
Get:31 http://security.ubuntu.com/ubuntu jammy-security/main amd64 c-n-f Metadata [10.3 kB]
Get:32 http://security.ubuntu.com/ubuntu jammy-security/main Translation-en [129 kB]
Get:33 http://security.ubuntu.com/ubuntu jammy-security/restricted amd64 Packages [415 kB]
Get:34 http://security.ubuntu.com/ubuntu jammy-security/restricted amd64 c-n-f Metadata [208 kB]
87% [5 Packages store 0 B] [34 Packages 7031 B/415 kB 2%]
```

261) “sudo apt install mysql-server”: To install mysql in this instance.

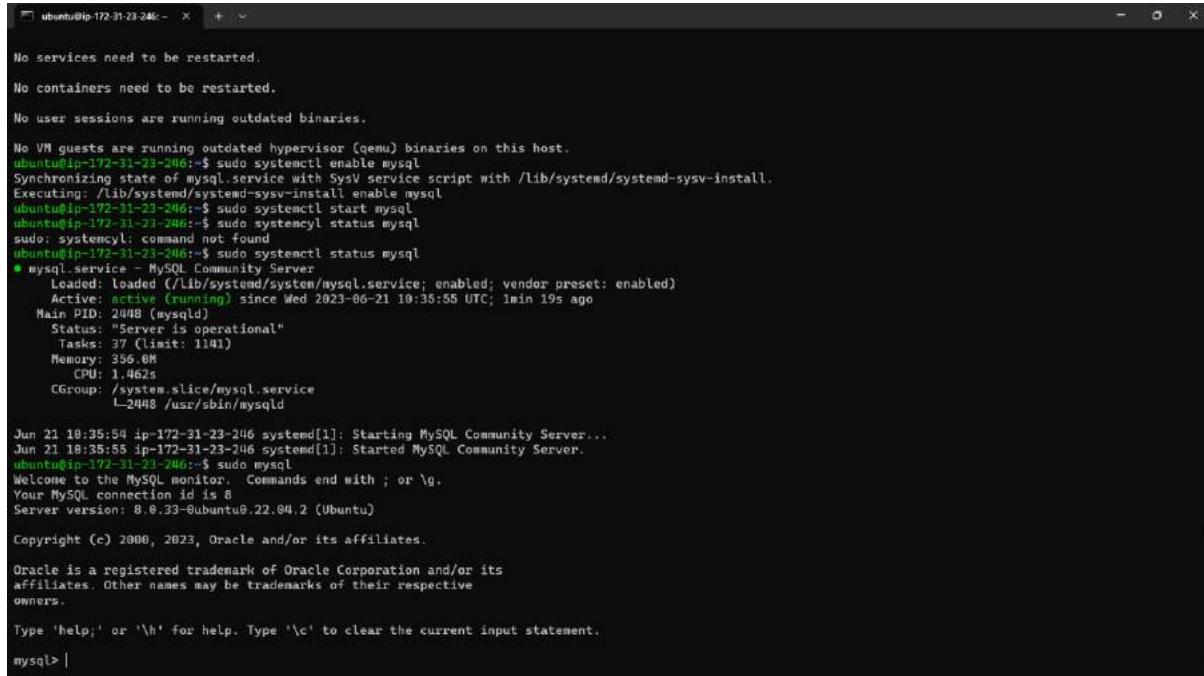


```
ubuntu@ip-172-31-23-246:~$ sudo apt install mysql-server
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
66 packages can be upgraded. Run 'apt list --upgradable' to see them.
ubuntu@ip-172-31-23-246:~$ sudo apt install mysql-server
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
  libcgid-perl libcgipm-perl libclone-perl libencode-locale-perl libevent-pthreads-2.1-7 libfcgi-bin libfcgi-perl libfcgi0ldbl libhtml-parser-perl
  libhtml-tagset-perl liblhttp-template-perl liblhttp-date-perl liblhttp-message-perl libio-html-perl liblwp-mediatypes-perl libmecab2 libprotobuf-lite23
  libtimedate-perl liburi-perl mecab-ipadic mecab-ipadic-utf8 mecab-utils mysql-client-8.0 mysql-client-core-8.0 mysql-common mysql-server-8.0
  mysql-server-core-8.0
Suggested packages:
  libdata-dump-perl libipc-sharedcache-perl libbusiness-isbn-perl libwww-perl mailx tinyca
The following NEW packages will be installed:
  libcgifast-perl libcgipm-perl libclone-perl libencode-locale-perl libevent-pthreads-2.1-7 libfcgi-bin libfcgi-perl libfcgi0ldbl libhtml-parser-perl
  libhtml-tagset-perl liblhttp-template-perl liblhttp-date-perl liblhttp-message-perl libio-html-perl liblwp-mediatypes-perl libmecab2 libprotobuf-lite23
  libtimedate-perl liburi-perl mecab-ipadic mecab-ipadic-utf8 mecab-utils mysql-client-8.0 mysql-client-core-8.0 mysql-common mysql-server
  mysql-server-8.0 mysql-server-core-8.0
0 upgraded, 28 newly installed, 0 to remove and 66 not upgraded.
Need to get 29.6 MB of archives.
After this operation, 243 MB of additional disk space will be used.
Do you want to continue? [Y/n] [2]
```

262) "sudo systemctl start mysql": To start mysql

"sudo systemctl enable mysql": To enable mysql

"sudo mysql": To perform mysql programming in the instance.



```
No services need to be restarted.
No containers need to be restarted.
No user sessions are running outdated binaries.

No VM guests are running outdated hypervisor (qemu) binaries on this host.
ubuntu@ip-172-31-23-246:~$ sudo systemctl enable mysql
Synchronizing state of mysql.service with SysV service script with /lib/systemd/systemd-sysv-install.
Executing: /lib/systemd/systemd-sysv-install enable mysql
ubuntu@ip-172-31-23-246:~$ sudo systemctl start mysql
ubuntu@ip-172-31-23-246:~$ sudo systemctl status mysql
sudo: systemctl: command not found
ubuntu@ip-172-31-23-246:~$ sudo systemctl status mysql
● mysql.service - MySQL Community Server
   Loaded: loaded (/lib/systemd/system/mysql.service; enabled; vendor preset: enabled)
     Active: active (running) since Wed 2023-06-21 10:35:55 UTC; 1min 19s ago
       Main PID: 2048 (mysqld)
          Status: "Server is operational"
             Tasks: 37 (limit: 1141)
            Memory: 356.0M
              CPU: 1.462s
            CGroup: /system.slice/mysql.service
                      └─2448 /usr/sbin/mysqld

Jun 21 10:35:54 ip-172-31-23-246 systemd[1]: Starting MySQL Community Server...
Jun 21 10:35:55 ip-172-31-23-246 systemd[1]: Started MySQL Community Server.
ubuntu@ip-172-31-23-246:~$ sudo mysql
Welcome to the MySQL monitor. Commands end with ; or \g.
Your MySQL connection id is 8
Server version: 8.0.33-0ubuntu0.22.04.2 (Ubuntu)

Copyright (c) 2000, 2023, Oracle and/or its affiliates.

Oracle is a registered trademark of Oracle Corporation and/or its
affiliates. Other names may be trademarks of their respective
owners.

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

mysql> |
```