

LABORATORY REPORT

AWS SOLUTION ARCHITECT

CSE3016

BL2025260100772

Submitted by

**NAME: Himanshu
REG. NO.: 22BCE10118**

BTech – BACHELOR OF TECHNOLOGY



Submitted to

**Mr. Satyabrata Nath
Teaching Fellow**

**SCHOOL OF COMPUTER SCIENCE AND ENGINEERING
(SCOPE)
VIT BHOPAL UNIVERSITY**

July-August 2025

Table of Contents			
S. No.	List of Experiments	Experiment Date	Page No.
01	Creating iam users and defining custom policies in aws identity and access management (iam)	09-07-2025	1
02	How to create iam groups	11-07-2025	10
03	How to assume iam role	14-07-2025	14
04	How to launch an ec2 instance with template	17-07-2025	22
05	Amazon s3 (bucket creation, creating url and s3 life cycle management)	24-07-2025	29
06	How to create an ec2 instance	25-07-2025	39
07	How to create a static website in s3	25-07-2025	48
08	How to setup ec2 instance in vpc	28-07-2025	53
09	How to implement load balancer, target group & auto- scaling group with ec2 instance	08-08-2025	78
10	How to create ebs and attach to ec2 instance, modify size and create a snapshot	12-08-2025	103

Date: 09-07-2025	Title
Exp. No: 01	Creating IAM Users and Defining Custom Policies in AWS Identity and Access Management (IAM)

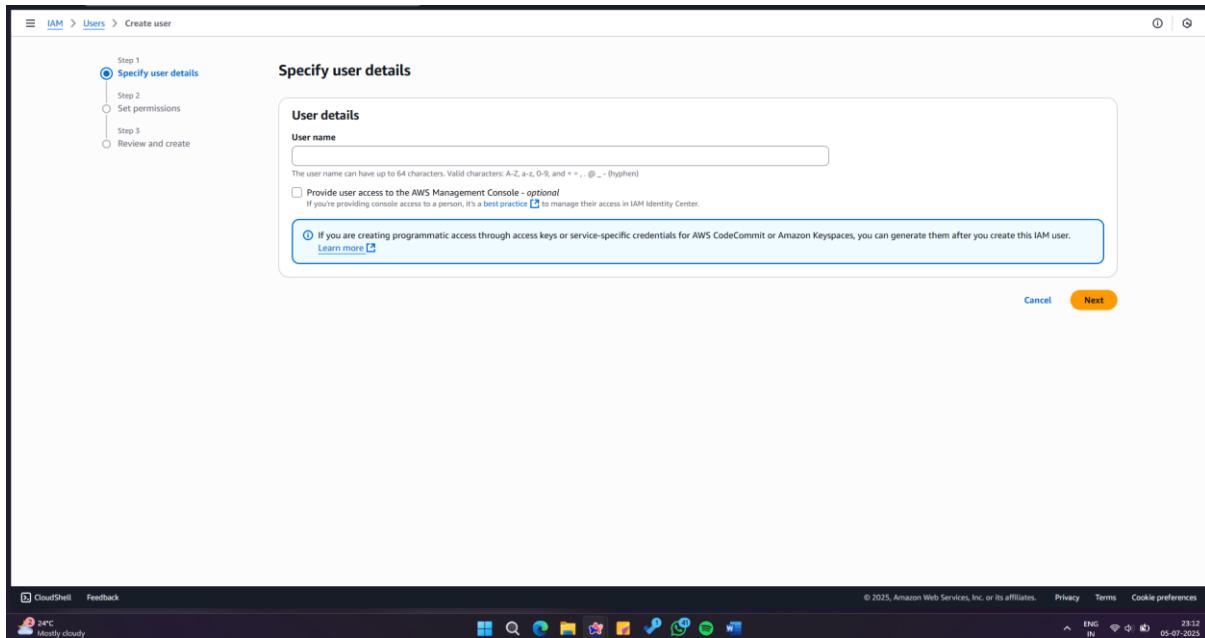
AIM OF THE EXPERIMENT: Creating IAM Users and Defining Custom Policies in AWS Identity and Access Management (IAM)

PROCEDURE:

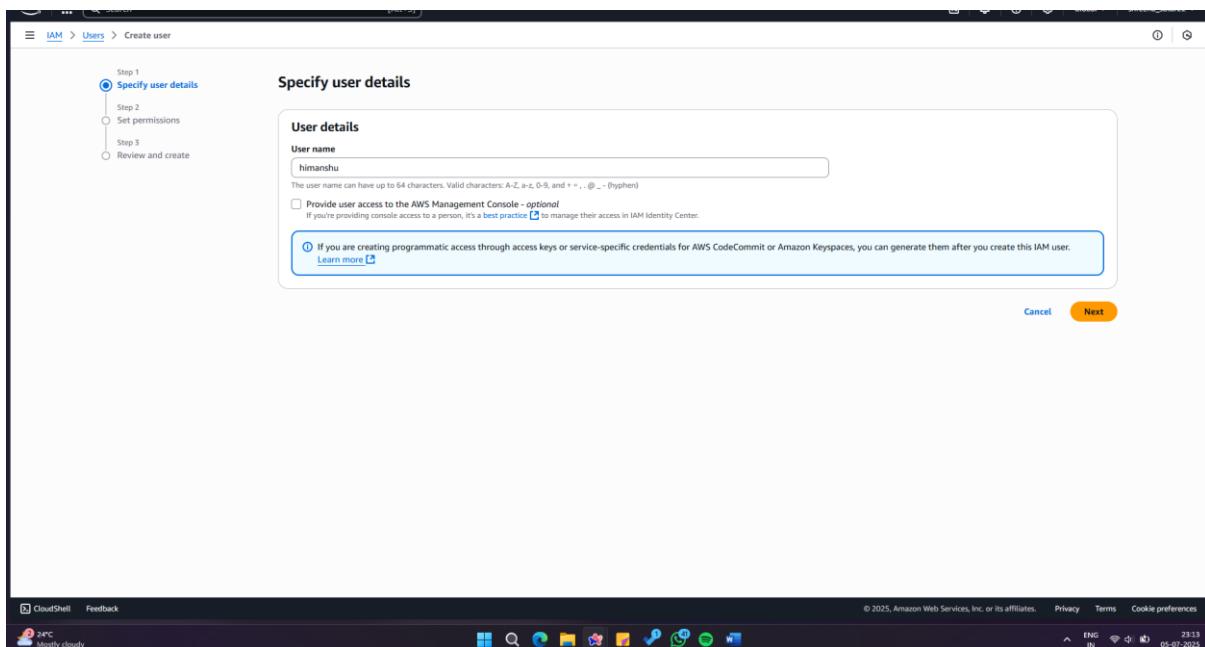
1. After logging in , Open the IAM (Identity and Access Management) service from the AWS Console.

The screenshot shows the AWS IAM Dashboard. On the left, there is a navigation sidebar with sections like 'Access management', 'Access reports', and 'AWS Organizations'. The main dashboard has several cards: 'Security recommendations' (warning about root user MFA), 'AWS Account' (account ID: 116555269880, account alias: Create), 'IAM resources' (0 User groups, 0 Users, 2 Roles, 0 Policies, 0 Identity providers), 'What's new' (list of recent announcements), 'Quick Links' (My security credentials), 'Tools' (Policy simulator), and 'Additional information' (Security best practices in IAM). At the bottom, there are links for CloudShell, Feedback, Trending videos, and a footer with copyright information and cookie preferences.

2. In the IAM dashboard, select “Users” and click “Add users”.



3. Enter the username in the required format and select the type of access required

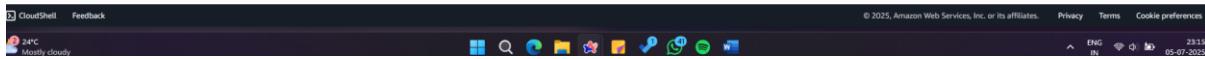


4. Set permission to add user to group .

The screenshot shows the 'Set permissions' step of the 'Create user' wizard. It includes a sidebar with steps 1-3: 'Specify user details' (selected), 'Set permissions' (current), and 'Review and create'. The main area shows 'Permissions options' with three radio button choices: 'Add user to group' (selected), 'Copy permissions', and 'Attach policies directly'. Below this is a 'Get started with groups' section with a 'Create group' button. A note says: 'Create a group and select policies to attach to the group. We recommend using groups to manage user permissions by job function, AWS service access, or custom permissions.' At the bottom are 'Cancel', 'Previous', and 'Next' buttons.

5. After proceeding , review all the details and click on create user .

The screenshot shows the 'Review and create' step of the 'Create user' wizard. It includes a sidebar with steps 1-3: 'Specify user details' (selected), 'Set permissions' (selected), and 'Review and create' (current). The main area shows 'User details' (Name: himanshu, Console password type: None, Require password reset: No) and a 'Permissions summary' table with one row (Name: himanshu, Type: User, Used as: No resources). Below is a 'Tags - optional' section with an 'Add new tag' button and a note: 'Tags are key-value pairs you can add to AWS resources to help identify, organize, or search for resources. Choose any tags you want to associate with this user.' At the bottom are 'Cancel', 'Previous', and 'Create user' (highlighted).



6. User has been successfully created

The screenshot shows the AWS IAM Users page. A green success message at the top states "User created successfully" and provides instructions for viewing and downloading the user's password and email instructions. Below this, the "Users (1) Info" section shows a single user named "himanshu". The user details include: ARN: arn:aws:iam::11655526980:user/himanshu, Path: /, Groups: 0, Last activity: N/A, MFA: N/A, Password age: N/A, Console last sign-in: N/A, Access key ID: N/A, Active key age: N/A, and Access key status: N/A. On the right side of the user card are "View user", "Delete", and "Create user" buttons. The left sidebar contains navigation links for IAM, Access management, Access reports, and other AWS services like CloudShell and IAM Identity Center.

7. Go to the permissions section of the user created , by clicking over it .

The screenshot shows the "himanshu" user details page. The "Summary" section displays basic information: ARN (arn:aws:iam::11655526980:user/himanshu), Created (July 05, 2025, 23:16 (UTC+05:30)), Console access (Disabled), and Last console sign-in (N/A). It also shows one Access key (Access key 1) with a "Create access key" button. The "Permissions" tab is selected, showing a table with columns for Policy name, Type, and Attached via. A search bar and a "Filter by Type" dropdown are present. The table currently shows "No resources to display". Below the table, there are sections for "Permissions policies (0)", "Permissions boundary (not set)", and "Generate policy based on CloudTrail events". The "Generate policy" button is highlighted with a blue border. The left sidebar is identical to the previous screenshot, showing the IAM navigation menu and other service links.

8. Now go on security credentials and click on enable console access.

The screenshot shows the AWS IAM User Details page for a user named 'himanshu'. In the 'Permissions' tab, a modal dialog titled 'Enable console access' is open. The dialog contains fields for 'Console password' (set to 'Autogenerated password') and 'Multi-factor authentication (MFA)' (disabled). A checkbox for 'User must create new password at next sign-in' is unchecked. At the bottom right of the dialog are 'Cancel' and 'Enable console access' buttons. The main user details page shows the ARN as 'arn:aws:iam::116555269880:user/himanshu', created on July 05, 2025, and has 'Console access Disabled'.

9. Console password successfully created .

The screenshot shows the same AWS IAM User Details page for 'himanshu'. The 'Console access' status is now 'Enabled without MFA'. A green success message box displays the text: 'Console access enabled.' and 'You have successfully enabled the user's new password. This is the only time you can view this password. After you close this window, if the password is lost, you must create a new one.' Below this, the 'Console password' field shows a masked password with a 'Show' link. The main user details page also shows the ARN and creation date.

10. With the help of credentials created log into your user account .

The screenshot shows the AWS Console Home page. On the left, under 'Recently visited', there is a link to 'IAM'. In the center, under 'Applications (0)', there is a message: 'Access denied to servicelogicatalog:ListApplications'. On the right, under 'Cost and usage', there are three sections: 'Current month' (Access denied), 'Forecasted month end' (Access denied), and 'Savings opportunities' (Access denied). At the bottom, there are links for 'CloudShell' and 'Feedback'.

11. You can use any service now with the help of user account , if you have permission . Now will provide permission for amazon s3

The screenshot shows the Amazon S3 service page. It features a large 'Create a bucket' button and a 'How it works' section with a video player. To the right, there are sections for 'Pricing' (with a note about no minimum fees) and 'Resources' (links to User guide, API reference, FAQs, and Discussion forums). At the bottom, there are links for 'CloudShell' and 'Feedback'.

12. Go on IAM dashboard then policies and click on create policies (Fill in the details).

The screenshot shows the 'Create policy' wizard in the AWS IAM console. The first step, 'Specify permissions', is completed. The policy name is set to 'himanshu-user-s3'. The 'Description - optional' field is empty. Under 'Permissions defined in this policy', it shows an 'Allow (1 of 444 services)' entry for the 'S3' service with 'Full access' at the 'Resource' level. There are no tags added yet.

13. Policy successfully created.

The screenshot shows the 'Policies' page in the AWS IAM console. A green banner at the top indicates that the policy 'himanshu-user-s3-access' has been created. The main table lists 1370 policies. The 'himanshu-user-s3-access' policy is visible in the list, categorized under 'AWS managed' policies. Other policies listed include various AWS services like Access Analyzer, AdministratorAccess, Amplify, AI Operations, AI Ops, AlexaForBusiness, and Amazon API Gateway.

14. Now click on your user and add permission and attach policies .

Permissions options

- Add user to group
- Copy permissions
- Attach policies directly

Permissions policies (1321)

Policy name	Type	Attached entities
AccessAnalyzerServiceRolePolicy	AWS managed	0
AdministratorAccess	AWS managed - job function	0
AdministratorAccess-Amplify	AWS managed	0

15. Policy successfully added .

Identity and Access Management (IAM)

1 policy added

arn:aws:iam::767828733348:user/munsifa	Console access Enabled without MFA	Access key 1 Create access key
Created January 27, 2025, 22:38 (UTC+05:30)	Last console sign-in Never	

Permissions | Groups | Tags | Security credentials | Last Accessed

Permissions policies (1)

Permissions are defined by policies attached to the user directly or through groups.

Policy name	Type	Attached via
munsifa-user-s3-access	Customer managed	Directly

16. Now we are able to use amazon s3 service in our user and successfully added a custom policy .

The screenshot shows the AWS S3 Buckets page. On the left, there's a sidebar with navigation links like 'Amazon S3', 'General purpose buckets', 'Directory buckets', etc. The main area has a heading 'Account snapshot - updated every 24 hours' with a link to 'View Storage Lens dashboard'. Below it, a message says 'Storage Lens provides visibility into storage usage and activity trends. Metrics don't include directory buckets.' A 'Create bucket' button is prominently displayed. The 'General purpose buckets' tab is selected, showing a table with columns 'Name', 'AWS Region', 'IAM Access Analyzer', and 'Creation date'. A message at the bottom states 'No buckets' and 'You don't have any buckets.' with a 'Create bucket' button.

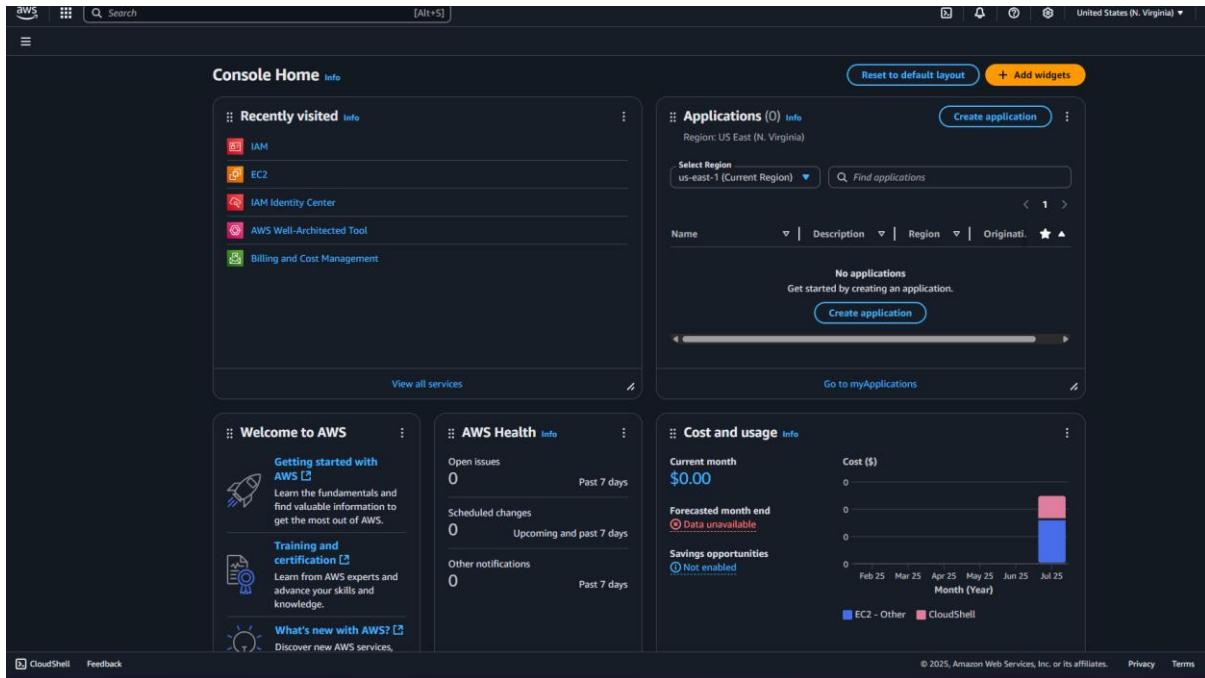
Date: 11-07-2025	Title
Exp. No: 02	How to create IAM Groups

AIM OF THE EXPERIMENT: How to create IAM Groups

PROCEDURE:

Below are the steps to create iam groups with screenshots :

- Sign in to the aws management console



ii) Navigate to the iam services .

The screenshot shows the AWS IAM Dashboard. On the left, there is a navigation pane with sections like Identity and Access Management (IAM), Access management, Access reports, IAM Identity Center, and AWS Organizations. The main area displays security recommendations (Add MFA for root user, Root user has no active access keys), IAM resources (User groups: 0, Users: 4, Roles: 4, Policies: 1, Identity providers: 0), and What's new (AWS IAM announces support for encrypted SAML assertions, AWS CodeBuild announces support for project ARN and build ARN IAM condition keys, IAM Roles Anywhere credential helper now supports TPM 2.0, Announcing AWS STS support for ECDSA-based signatures of OIDC tokens). To the right, there are boxes for AWS Account (Account ID: 116555269880, Account Alias: Create, Sign-In URL: https://116555269880signin.aws.amazon.com/console), Quick Links (My security credentials, Manage your access keys, multi-factor authentication (MFA) and other credentials), Tools (Policy simulator, The simulator evaluates the policies that you choose and determines the effective permissions for each of the actions that you specify), and Additional information (Security best practices in IAM, IAM documentation, Videos, blog posts, and additional resources).

iii) Access the group section on the left navigation pane .

The screenshot shows the User groups page under the IAM service. The left navigation pane is identical to the one in the previous screenshot. The main content area is titled "User groups (0) Info" and contains a table with columns for Group name, Users, Permissions, and Creation time. A note states "No resources to display". At the top right, there are buttons for Delete and Create group. At the bottom right, there are links for © 2025, Amazon Web Services, Inc. or its affiliates., Privacy, Terms, and Cookie preferences.

iv) Click on create group .

The screenshot shows the 'Create user group' interface. In the 'User group name' field, the value '22BCE11534_Himanshu' is entered. Under 'Add users to the group - Optional (4)', the user 'himanshu' is selected. In the 'Attach permissions policies - Optional (1059)' section, the policy 'AdministratorAccess' is selected.

v) Fill in all the required information and click on create group .

The screenshot shows the 'Create user group' interface. In the 'User group name' field, the value '22BCE11534_Himanshu' is entered. Under 'Add users to the group - Optional (1/4)', the user 'himanshu' is selected. In the 'Attach permissions policies - Optional (1/1059)' section, the policy 'AdministratorAccess' is selected and highlighted in blue.

vi) Group successfully created .

The screenshot shows the AWS IAM User Groups page. At the top, a green banner displays the message "22BCE10118_Himanshu user group created." Below the banner, the title "User groups (1)" is followed by a link "Info". A descriptive text states: "A user group is a collection of IAM users. Use groups to specify permissions for a collection of users." On the left, a sidebar menu includes sections for Dashboard, Access management (User groups, Roles, Policies, Identity providers, Account settings, Root access management), Access reports (Access Analyzer, Resource analysis, Unused access, Analyze settings, Credential report, Organization activity, Service control policies, Resource control policies), and IAM Identity Center and AWS Organizations. The main content area shows a table with one row for the newly created group:

Group name	Users	Permissions	Creation time
22BCE10118_Himanshu	0	0	Now

At the bottom right of the page, there are links for "View group", "Delete", and "Create group". The footer contains copyright information and links for CloudShell, Feedback, Privacy, Terms, and Cookie preferences.

vii) Now we can edit group permissions (revoke and grant permissions anytime) according to the need .

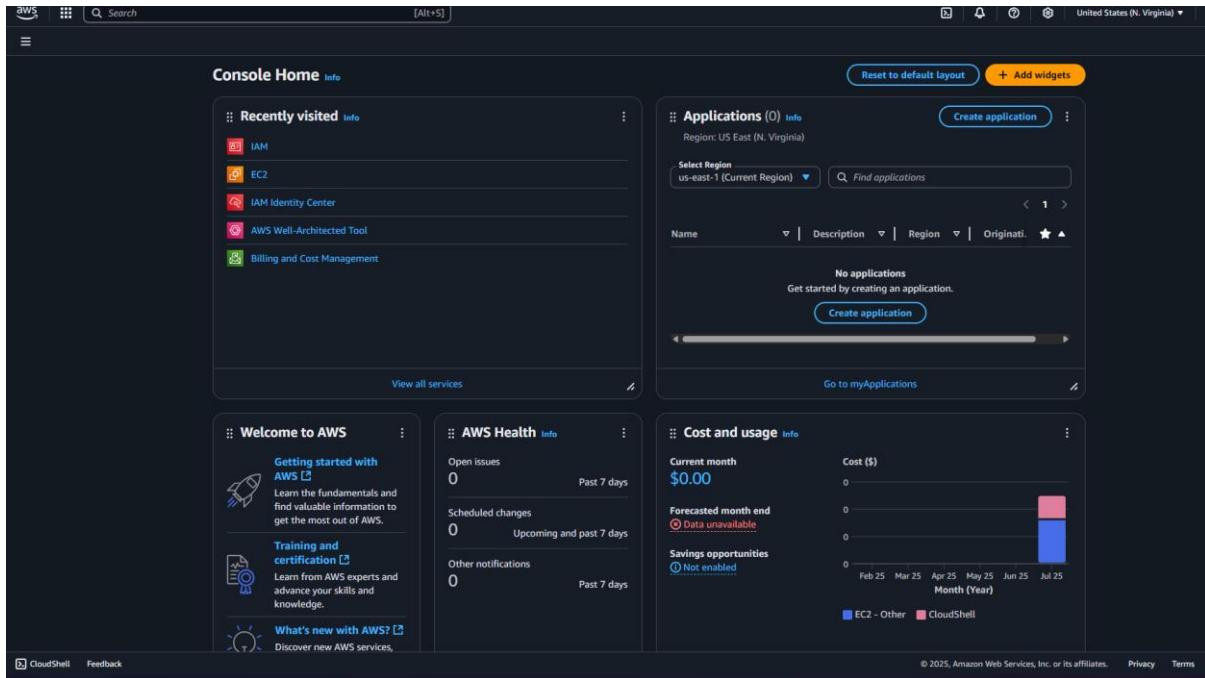
Date: 14-07-2025	Title
Exp. No: 03	How to assume IAM Roles

AIM OF THE EXPERIMENT: How to assume IAM Roles

PROCEDURE:

Below are the steps to create iam groups with screenshots :

- Sign in to the aws management console .



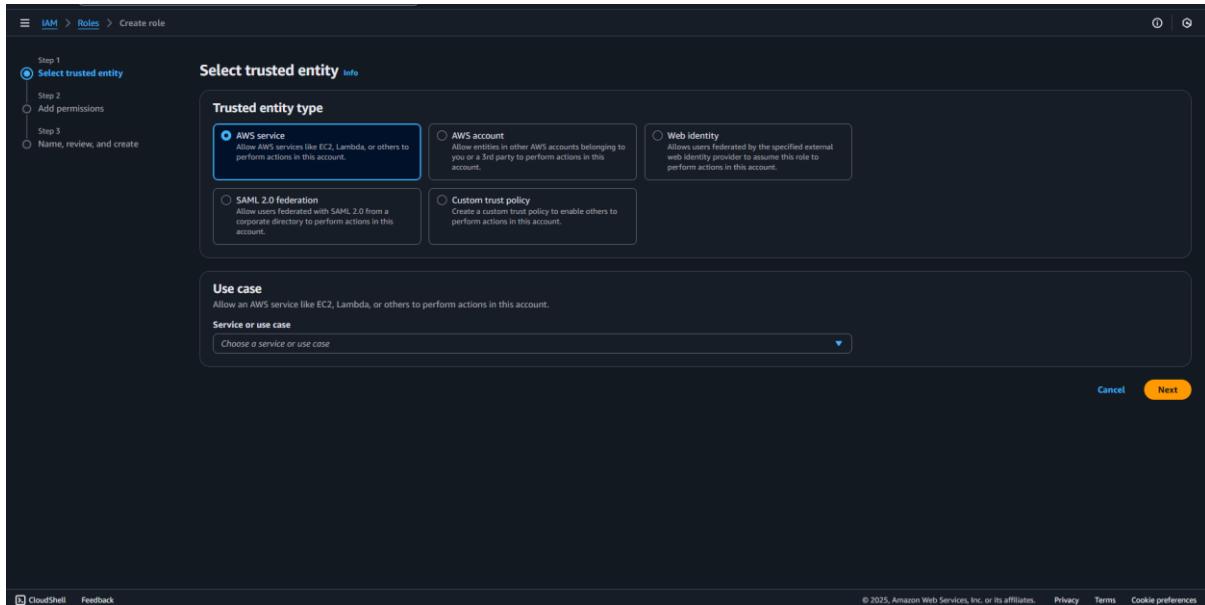
ii) Open iam .

The screenshot shows the AWS IAM Dashboard. On the left, there is a navigation pane with sections like Identity and Access Management (IAM), Access management, Access reports, and Tools. The main area displays security recommendations (Add MFA for root user, Root user has no active access keys), IAM resources (User groups: 0, Users: 4, Roles: 4, Policies: 1, Identity providers: 0), and a 'What's new' section with recent announcements about IAM support for encrypted SAML assertions, AWS CodeBuild support for project ARN and build ARN IAM condition keys, IAM Roles Anywhere credential helper, and AWS STS support for ECDSA-based signatures of OIDC tokens.

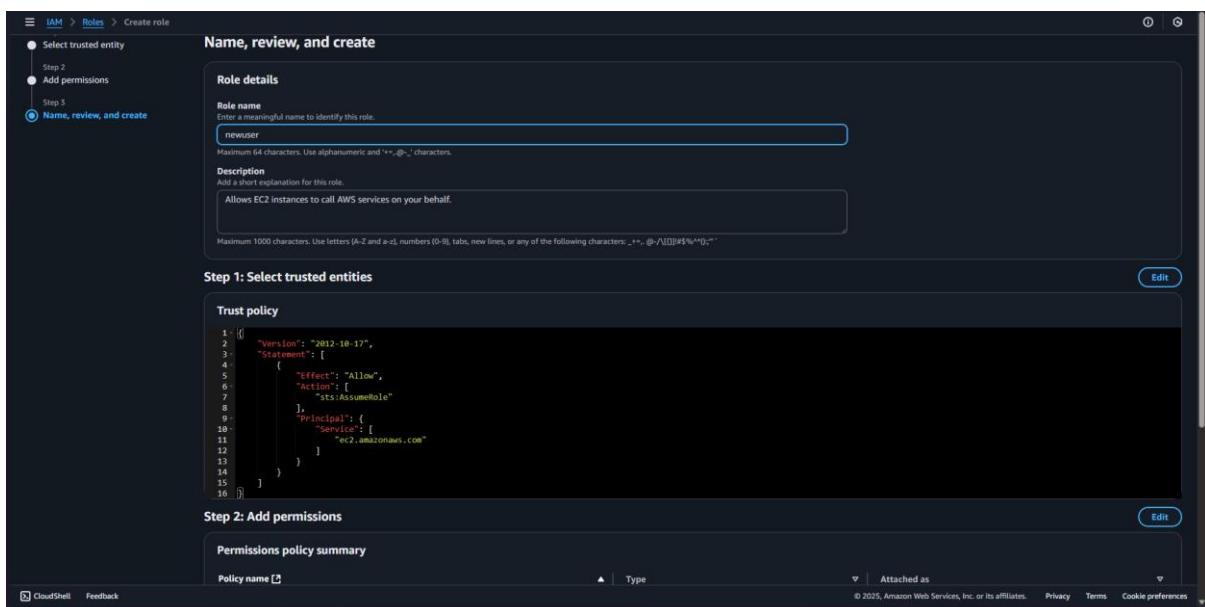
iii) Now click on roles on the left hand navigation pane .

The screenshot shows the 'Roles' page under the IAM service. The left navigation pane includes sections for Identity and Access Management (IAM), Access management, Access reports, and Tools. The main content area displays a table of existing roles, each with a checkbox, role name, trusted entity, and last activity. Below the table, there are sections for 'Roles Anywhere' (Authenticate non-AWS workloads), 'Access AWS from your non AWS workloads' (using X.509 Standard or AWS Certificate Manager), and 'Temporary credentials' (use temporary credentials with ease and benefit from enhanced security).

iv) Now click on create role .



v) Fill in the all necessary information . (add use case , provide permission and give it a name)



vi) New role successfully created .

The screenshot shows the AWS IAM Roles page. A green banner at the top indicates that the role 'newuser' has been created. Below this, a table lists five roles, including the newly created 'newuser'. The 'newuser' role is associated with the EC2 service. On the right side of the page, there are sections for 'Access AWS from your non AWS workloads' (using X.509 Standard) and 'Temporary credentials'.

vii) Click on role and copy arn .

The screenshot shows the detailed view of the 'newuser' role. It displays the ARN 'arn:aws:iam::116555269880:role/newuser' being copied. The 'Permissions' tab is selected, showing one managed policy named 'AdministratorAccess-Amplify'. There are also sections for 'Permissions boundary' and 'Generate policy based on CloudTrail events'.

viii) Now in the users section , click on the user whom you want to assume role .

The screenshot shows the AWS IAM User Details page for a user named 'himanshu'. The 'Permissions' tab is active. In the 'Permissions policies' section, there is a message stating 'No resources to display'. There are buttons for 'Add permissions' and 'Create inline policy'. Other tabs like 'Groups', 'Tags', and 'Security credentials' are also visible.

ix) In permissions section click on add permission .

The screenshot shows the AWS IAM User Details page for a user named 'himanshu'. The 'Permissions' tab is active. In the 'Permissions policies' section, there is a message stating 'No resources to display'. A button labeled 'Create inline policy' is highlighted. Other tabs like 'Groups', 'Tags', and 'Security credentials' are also visible.

x) Click on create inline policy .

The screenshot shows the 'Specify permissions' step of the IAM policy creation wizard. The JSON editor contains the following code:

```
1 { "Version": "2012-10-17", "Statement": [ { "Effect": "Allow", "Action": [], "Resource": [] } ] }
```

The sidebar on the right lists various AWS services under 'Available'.

xi) Change the policy editor lines and click on next and create .

Successfully created policy .

The screenshot shows the IAM user summary for 'himanshu'. A green banner at the top indicates 'Policy policy_newuser created.' The 'Permissions' tab is selected, showing one policy named 'policy_newuser' attached via 'Customer inline' and 'Inline'. Other tabs include 'Groups', 'Tags', and 'Security credentials'.

xii) Go back to roles and select the target role .

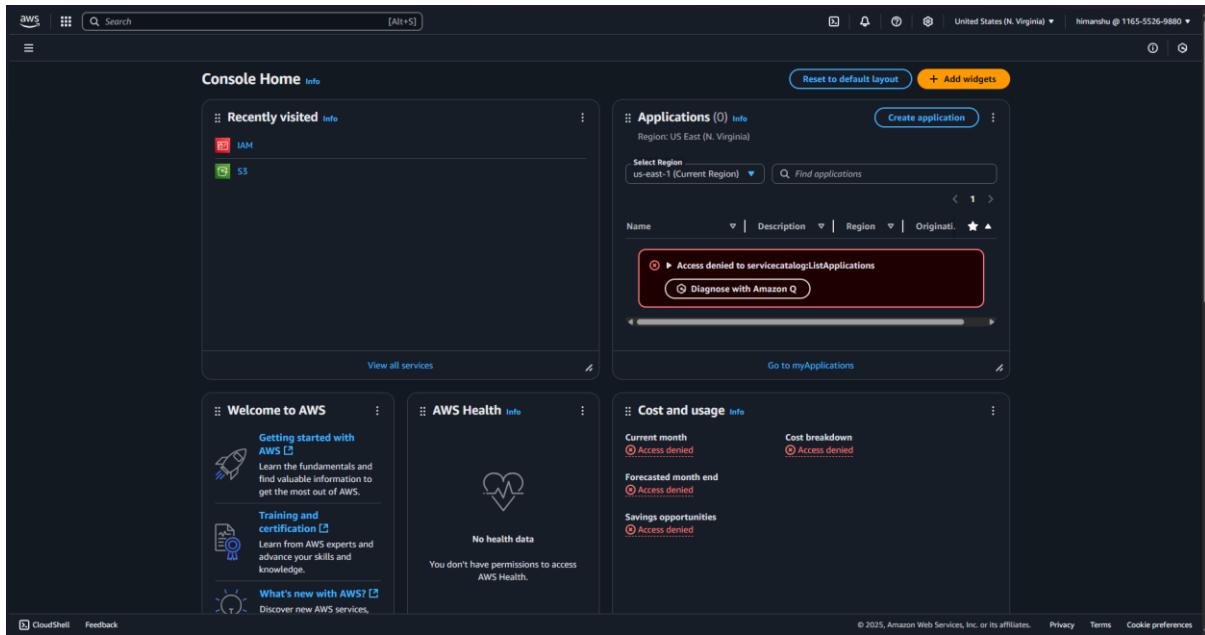
The screenshot shows the AWS IAM Roles page for the 'newuser' role. The 'Summary' section displays the ARN (arn:aws:iam::116555269880:role/newuser), creation date (July 09, 2025, 22:09 UTC+05:30), and maximum session duration (1 hour). The 'Permissions' tab is selected, showing one managed policy named 'AdministratorAccess-Amplify'. A 'Permissions boundary' section indicates '(not set)'. A 'Generate policy based on CloudTrail events' section shows no requests in the past 7 days.

xiii) Click on trust relationship tab then edit the trust policy .

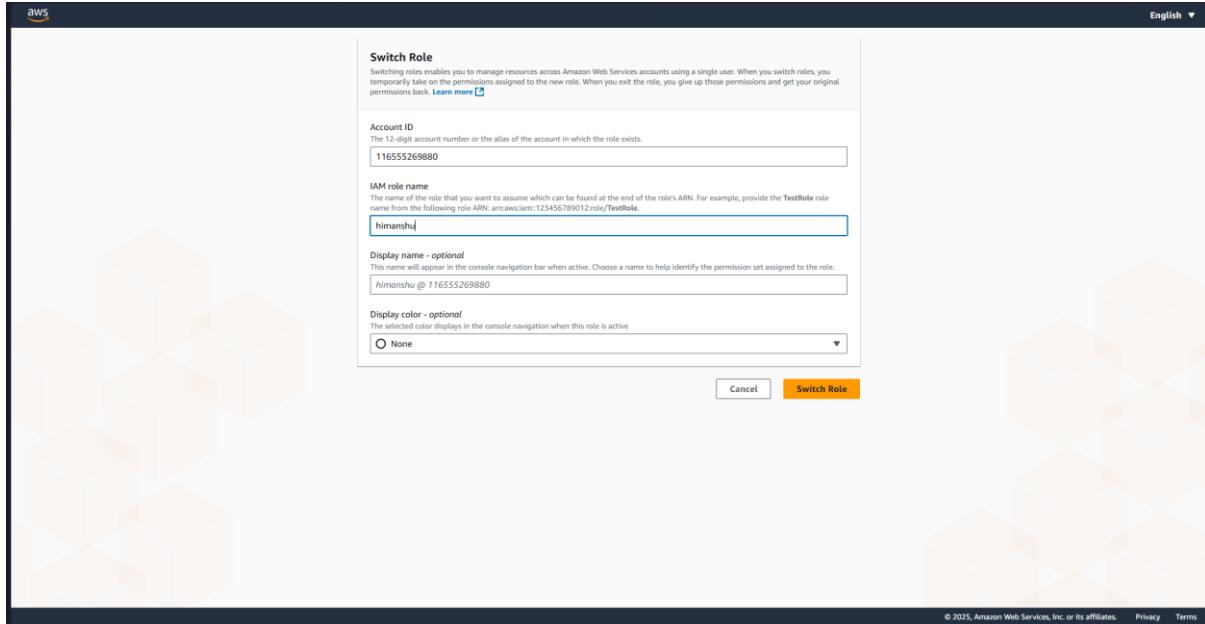
The screenshot shows the AWS IAM Roles page for the 'newuser' role. A green success message at the top states 'Trust policy updated.' The 'Summary' section shows the ARN (arn:aws:iam::116555269880:role/newuser), creation date (July 09, 2025, 22:09 UTC+05:30), and maximum session duration (1 hour). The 'Permissions' tab is selected, and the 'Trusted entities' section displays the following JSON trust policy:

```
1 - [ { 2 - "version": "2012-10-17", 3 - "statement": [ 4 - { 5 - "effect": "Allow", 6 - "principal": { 7 - "service": "ec2.amazonaws.com" 8 - }, 9 - "action": "sts:AssumeRole" 10 - }, 11 - { 12 - "effect": "Allow", 13 - "principal": { 14 - "arn": "arn:aws:iam::116555269880:role/newuser" 15 - }, 16 - "action": "sts:AssumeRole" 17 - } 18 - ] 19 - ]
```

xiv) Login to your user now .



xv) One the topleft account section click on switch and fill in the details .



xvi) You are now operating under the permissions of the assumed role. The console will indicate the role name and color at the top.

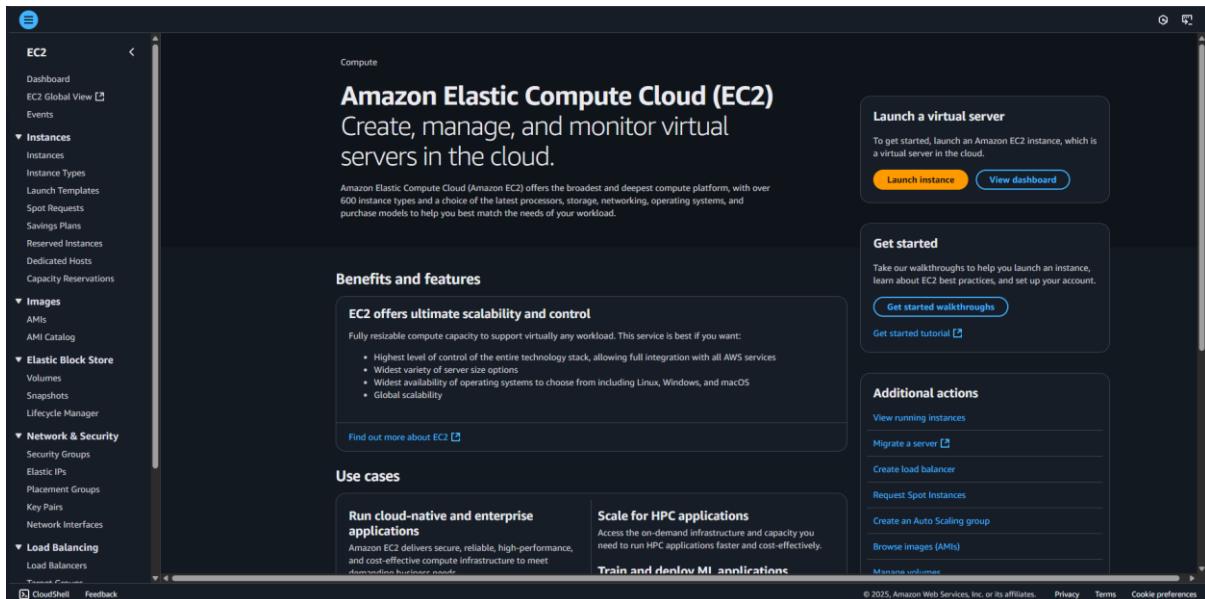
Date: 17-07-2025	Title
Exp. No: 04	How To Launch An EC2 Instance With Template

AIM OF THE EXPERIMENT: How To Launch An EC2 Instance With Template

PROCEDURE:

Follow the below steps to complete the requirements :

- open the ec2 dashboard and click on launch templates>create launch template .



- ii) give a suitable name and description to the template .

The screenshot shows the 'Launch an instance' wizard in the AWS Management Console. The current step is 'Name and tags'. A single tag named 'newec2' is listed under the 'Tags' section. The 'Summary' section shows 1 instance selected. The 'Software Image (AMI)' section shows 'Amazon Linux 2023 AMI 2023.7.2...' as the chosen AMI. The 'Virtual server type (instance type)' is set to 't2.micro'. The 'Storage (volumes)' section indicates 1 volume(s) - 8 GiB. A note about the free tier is visible. The 'Launch instance' button is at the bottom right.

- iii) click on template tags>add tags>info:name>value:any name

This screenshot shows the same 'Launch an instance' wizard as the previous one, but with a new tag added. Under the 'Name and tags' section, there is a table with two rows: 'Key' (Info) and 'Value' (Info). The 'Value' row contains the tag 'newec2'. The rest of the interface is identical to the first screenshot, including the summary, AMI selection, instance type, storage, and launch button.

iv) click on browse more ami

Search results

Add new tag

You can add up to 49 more tags.

▼ Application and OS Images (Amazon Machine Image) [Info](#)

An AMI is a template that contains the software configuration (operating system, application server, and applications) required to launch your instance. Search or Browse for AMIs if you don't see what you are looking for below

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

Quick Start

Amazon Linux macOS Ubuntu Windows Red Hat SUSE Linux Debian

Browse more AMIs

Amazon Machine Image (AMI)

Amazon Linux 2023 kernel-6.1 AMI
ami-05ffe3c48a9991133 (64-bit (x86), uefi-preferred) / ami-022bb032cf2f169f (64-bit (Arm), uefi)
Virtualization: hvm ENA enabled: true Root device type: ebs

Description

Amazon Linux 2023 (kernel-6.1) is a modern, general purpose Linux-based OS that comes with 5 years of long term support. It is optimized for AWS and designed to provide a secure, stable and high-performance execution environment to develop and run your cloud applications.

Amazon Linux 2023 AMI 2023.7.20250623.1 x86_64 HVM kernel-6.1

Architecture	Boot mode	AMI ID	Publish Date	Username
64-bit (x86)	uefi-preferred	ami-05ffe3c48a9991133	2025-06-20	ec2-user

Verified provider

▼ Instance type [Info](#) | [Get advice](#)

CloudShell Feedback

© 2025, Amazon Web Services, Inc. or its affiliates. [Privacy](#) [Terms](#) [Cookie preferences](#)

v) select ubuntu from the list

Search results

Search for an AMI by entering a search term e.g. "Windows"

Quick Start AMIs (47) My AMIs (0) AWS Marketplace AMIs (6607) Community AMIs (500)

SUSE Linux Enterprise Server 15 SP7 (HVM), SSD Volume Type
ami-0652811af66cef7a8 (64-bit (x86)) / ami-004f44e8ced71d35 (64-bit (Arm))
Platform: suse Root device type: ebs Virtualization: hvm ENA enabled: Yes
Select
64-bit (x86) 64-bit (Arm)

Ubuntu Server 24.04 LTS (HVM), SSD Volume Type
ami-0a20ca7e5df1f615 (64-bit (x86)) / ami-07041441b708cb0f6 (64-bit (Arm))
Platform: ubuntu Root device type: ebs Virtualization: hvm ENA enabled: Yes
Select
64-bit (x86) 64-bit (Arm)

Ubuntu Server 24.04 LTS (HVM), SSD Volume Type
ami-0a7db0731ae1a2435 (64-bit (x86)) / ami-050a99786ebf55a6a (64-bit (Arm))
Platform: ubuntu Root device type: ebs Virtualization: hvm ENA enabled: Yes
Select
64-bit (x86) 64-bit (Arm)

Ubuntu Server 22.04 LTS (HVM), SSD Volume Type
ami-02650b5095d1e5227 (64-bit (x86))
Platform: windows Root device type: ebs Virtualization: hvm ENA enabled: Yes
Select
64-bit (x86) 64-bit (Arm)

Ubuntu Server 22.04 LTS (HVM) with SQL Server 2022 Standard
ami-07b7f66b629de9364 (64-bit (x86))
Platform: windows Root device type: ebs Virtualization: hvm ENA enabled: Yes
Select
64-bit (x86) 64-bit (Arm)

CloudShell Feedback

© 2025, Amazon Web Services, Inc. or its affiliates. [Privacy](#) [Terms](#) [Cookie preferences](#)

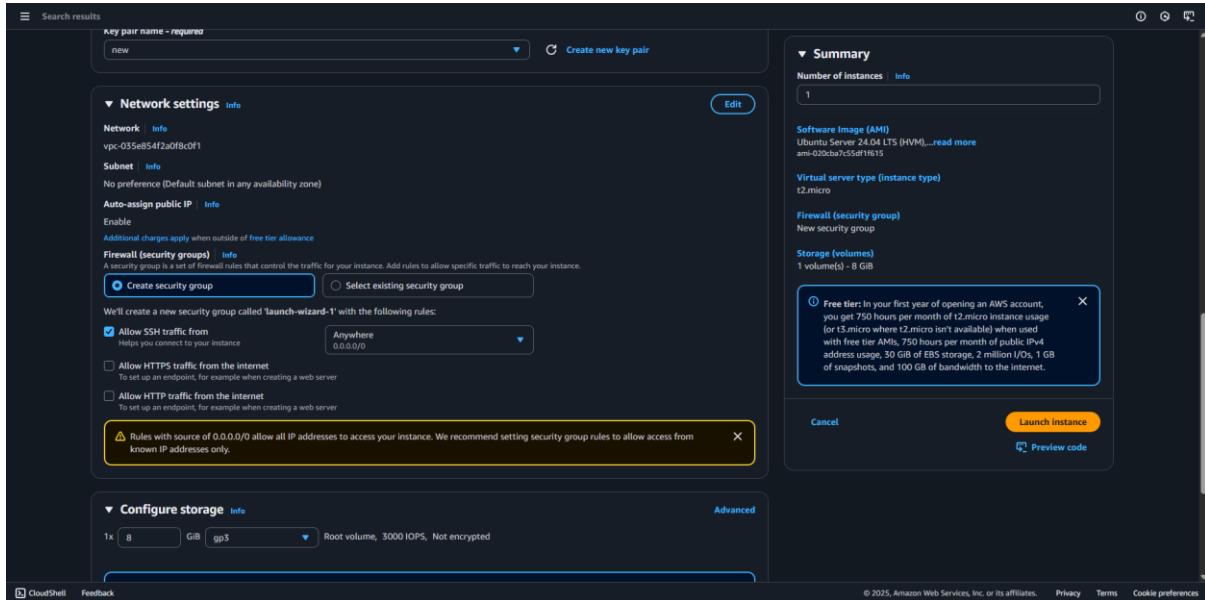
vi) select the instance type:t2 micro (free tier)

The screenshot shows the AWS Lambda console interface. On the left, there's a sidebar with 'Search results' and a list of Lambda functions. The main area is titled 'Create new function'. It has sections for 'Function name' (set to 'my-first-lambda'), 'Runtime' (set to 'Node.js 18.x'), and 'Handler' (set to 'index.handler'). Below these are 'Code provider' (set to 'GitHub'), 'GitHub repository' (set to 'https://github.com/...'), and 'Branch' (set to 'main'). A large 'Create function' button is at the bottom.

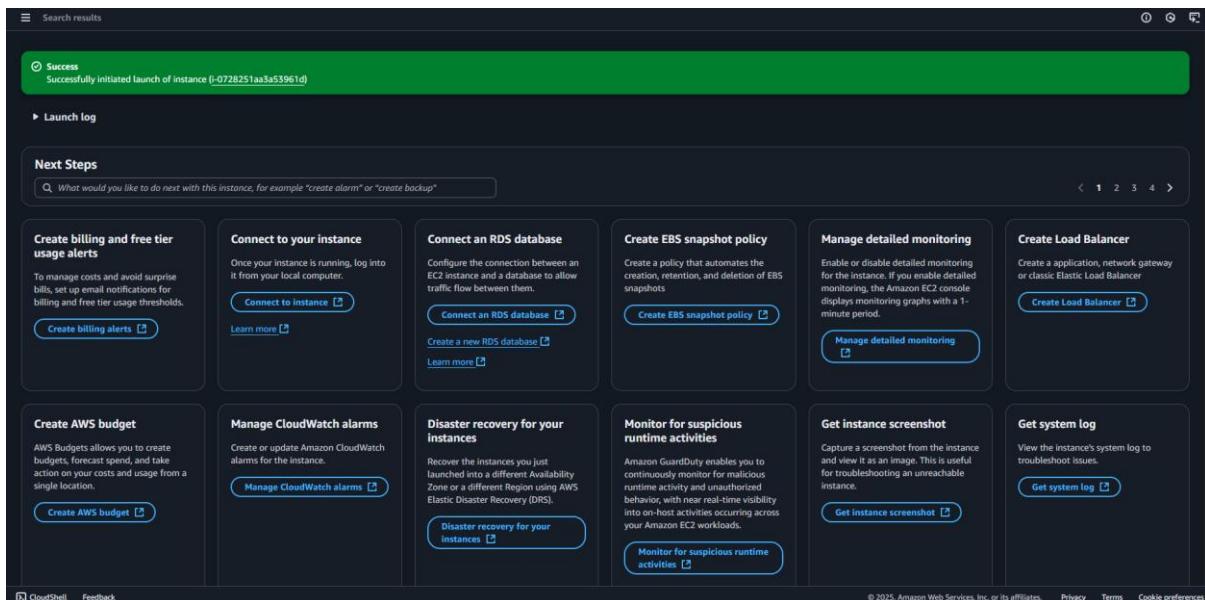
vii) create key pair

The screenshot shows the AWS Lambda console interface. On the left, there's a sidebar with 'Search results' and a list of Lambda functions. The main area is titled 'Create new function'. It has sections for 'Function name' (set to 'my-first-lambda'), 'Runtime' (set to 'Node.js 18.x'), and 'Handler' (set to 'index.handler'). Below these are 'Code provider' (set to 'GitHub'), 'GitHub repository' (set to 'https://github.com/...'), and 'Branch' (set to 'main'). A large 'Create function' button is at the bottom.

viii) select create security group and required things. choose type:ssh> source type: anywhere



ix) click on launch instance >launch template is created>click on view template .

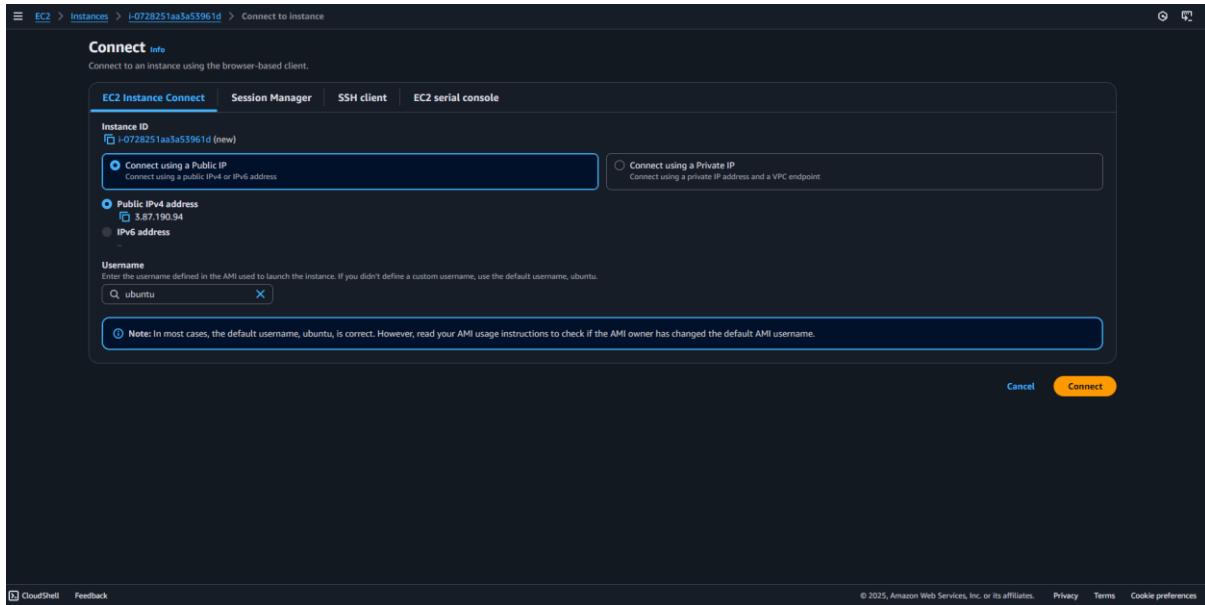


The screenshot shows the AWS EC2 Instances page. On the left, there's a navigation sidebar with sections like Dashboard, EC2 Global View, Events, Instances (selected), Instance Types, Launch Templates, Spot Requests, Savings Plans, Reserved Instances, Dedicated Hosts, Capacity Reservations, Images (AMIs, AMI Catalog), Elastic Block Store (Volumes, Snapshots, Lifecycle Manager), Network & Security (Security Groups, Elastic IPs, Placement Groups, Key Pairs, Network Interfaces), and Load Balancing (Load Balancers). The main area displays a table titled 'Instances (1) info' with one row. The row details are: Name: new, Instance ID: i-0728251aa3a53961d, Instance state: Running, Instance type: t2.micro, Status check: Initializing, Alarm status: View alarms, Availability Zone: us-east-1a, Public IPv4 DNS: ec2-3-87-190-94.compute-1.amazonaws.com, Public IPv4 IP: 3.87.190.94, and Elastic IP: none. Below the table, a message says 'Select an instance'. At the bottom right, there are links for 'CloudShell', 'Feedback', and copyright information: '© 2025, Amazon Web Services, Inc. or its affiliates.' followed by 'Privacy', 'Terms', and 'Cookie preferences'.

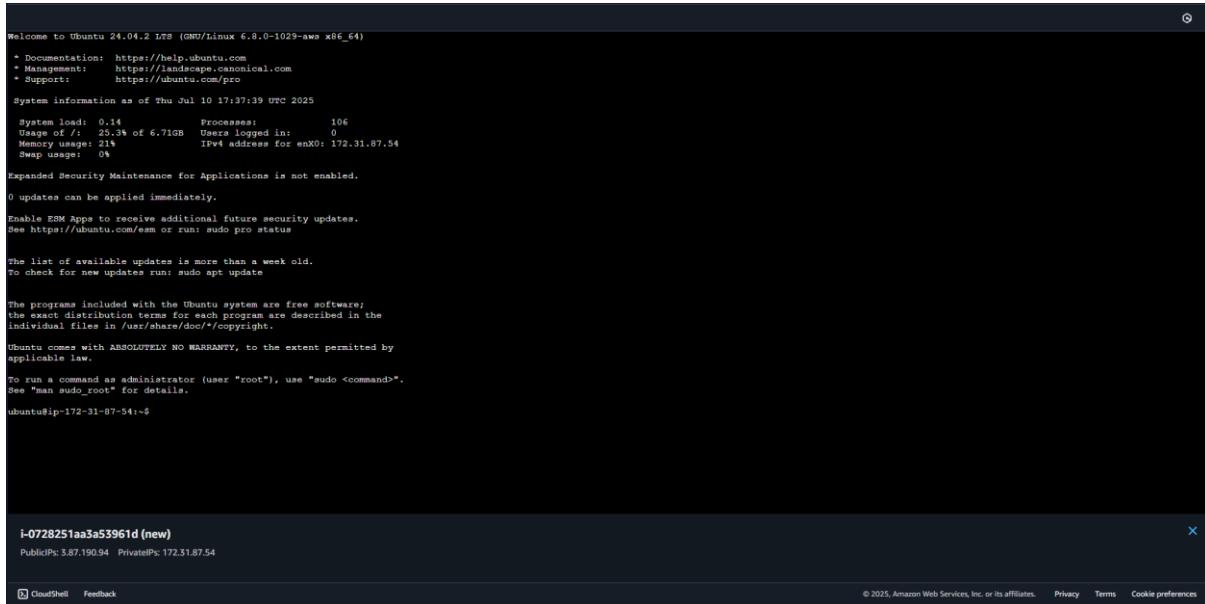
x) open instance and click on connect

The screenshot shows the 'Instance summary for i-0728251aa3a53961d (new)' page. The left sidebar is identical to the previous screenshot. The main content area has tabs at the top: Details (selected), Status and alarms, Monitoring, Security, Networking, Storage, and Tags. Under the Details tab, there are several sections: Instance ID (i-0728251aa3a53961d), IPv6 address (none), Hostname type (IP name: ip-172-31-87-54.ec2.internal), Answer private resource DNS name (IPv4 (A)), Auto-assigned IP address (3.87.190.94 [Public IP]), IAM Role (none), IMDSv2 (Required), Operator (none), and a large 'Instance details' section. This 'Instance details' section contains sub-sections for AMI ID (ami-020cba7c55df1f615), AMI name (ubuntu/images/hvm-ssd/gp3/ubuntu-noble-24.04-amd64-server-20250610), Stop protection (Disabled), Monitoring (disabled), Allowed image (none), Launch time (Thu Jul 10 2025 23:03:31 GMT+0530 (India Standard Time) (2 minutes)), Platform details (Linux/UNIX), Termination protection (Disabled), and AMI location (amazon/ubuntu/images/hvm-ssd/gp3/ubuntu-noble-24.04-amd64-server-20250610). At the bottom right, there are links for 'CloudShell', 'Feedback', and copyright information: '© 2025, Amazon Web Services, Inc. or its affiliates.' followed by 'Privacy', 'Terms', and 'Cookie preferences'.

xi) click on connect to instance



xii) now its successfully connected



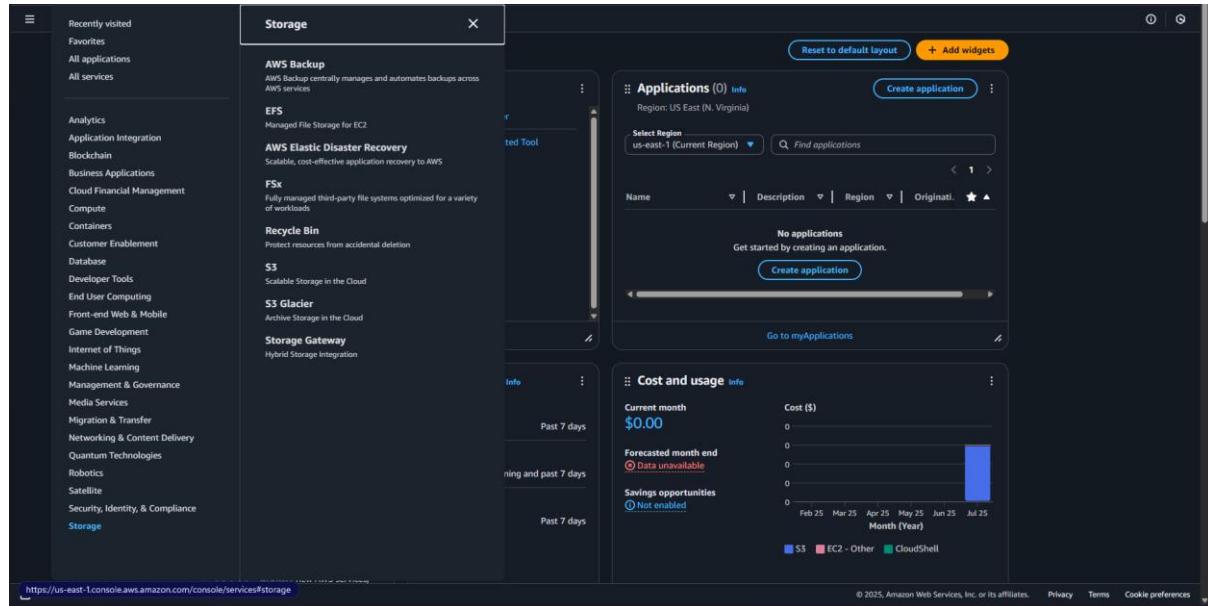
Date: 24-07-2025	Title
Exp. No: 05	Amazon S3 (Bucket creation, creating URL and S3 Life cycle Management)

AIM OF THE EXPERIMENT: Amazon S3 (Bucket creation, creating URL and S3 Life cycle Management)

PROCEDURE:

Follow the below steps to complete the requirements :

- Get in storage and then in storage dashboard.



- ii) Since no bucket is created so click on create bucket.

The screenshot shows the Amazon S3 console under the 'General purpose buckets' tab. A single bucket, 'utshaw007s', is listed. The bucket details include its name, AWS Region (Asia Pacific (Mumbai) ap-south-1), and creation date (July 10, 2025, 10:54:55 (UTC+05:30)). Action buttons for Copy ARN, Empty, Delete, and Create Bucket are visible. The left sidebar includes links for General purpose buckets, Directory buckets, Access Grants, and Storage Lens.

- iii) Fill in the general configuration and other details as required (also select the region.)

The screenshot shows the 'Create bucket' wizard on the 'General configuration' step. It includes fields for AWS Region (set to US East (N. Virginia) us-east-1), Bucket type (set to General purpose), Bucket name (set to 'myowebucket'), and Object Ownership (set to ACLs disabled). The 'Block Public Access settings for this bucket' section is also visible at the bottom.

iv) New bucket himanshuchitoria successfully created .

The screenshot shows the 'Amazon S3 > Buckets' page. A green success banner at the top states: 'Successfully created bucket "himanshuchitoria". To upload files and folders, or to configure additional bucket settings, choose View details.' Below the banner, there's an 'Account snapshot - updated every 24 hours' section with a link to 'View Storage Lens dashboard'. The main area shows two 'General purpose buckets': 'himanshuchitoria' (created July 11, 2025) and 'utsav007s3' (created July 10, 2025). There are tabs for 'General purpose buckets' and 'Directory buckets'. A 'Create bucket' button is visible in the top right of the table header.

v) Now we click on our bucket and upload file by clicking upload.

The screenshot shows the 'Amazon S3 > Buckets > himanshuchitoria' page. The 'himanshuchitoria' bucket is selected. The 'Objects' tab is active, showing 'Objects (0)'. It includes a search bar, filter options, and actions like 'Copy S3 URI', 'Copy URL', 'Download', 'Open', 'Delete', 'Actions', 'Create folder', and 'Upload'. A message indicates 'No objects' and 'You don't have any objects in this bucket.' A prominent blue 'Upload' button is located at the bottom of the table.

vi) Now under upload section we can upload the file as well as folder.

The screenshot shows the 'Upload' interface in the Amazon S3 console. At the top, there's a breadcrumb navigation: Amazon S3 > Buckets > himanshuchitoria > Upload. Below this is a large text input field with the placeholder 'Drag and drop files and folders you want to upload here, or choose Add files or Add folder.' To the right of the input field are three buttons: 'Remove', 'Add files', and 'Add folder'. Below the input field is a table titled 'Files and folders (0)' with a single row showing 'No files or folders'. Underneath the table is a message: 'You have not chosen any files or folders to upload.' Further down, there's a 'Destination' section with a dropdown menu set to 's3://himanshuchitoria'. Below it is a 'Destination details' section with a note about bucket settings. On the left, there are collapsed sections for 'Permissions' and 'Properties'. At the bottom right are 'Cancel' and 'Upload' buttons. The footer includes links for CloudShell, Feedback, Privacy, Terms, and Cookie preferences.

vii) In storage class there are different types so choose any one as per use.

The screenshot shows the 'Properties' interface in the Amazon S3 console. At the top, there's a breadcrumb navigation: Amazon S3 > Buckets > himanshuchitoria > Upload. Below this is a section titled 'Properties' with a note: 'Specify storage class, encryption settings, tags, and more.' The main focus is the 'Storage class' section, which has a table comparing nine different classes. The 'Standard' class is selected and highlighted with a blue border. Other classes listed include Intelligent-Tiering, Standard-IA, One Zone-IA, Glacier Instant Retrieval, Glacier Flexible Retrieval (formerly Glacier), Glacier Deep Archive, and Reduced redundancy. Each class has a brief description, designed-for scenario, bucket type, availability zones, min storage duration, min billable object size, monitoring and auto-tiering fees, and retrieval fees. At the bottom, there's a 'Server-side encryption' section with a note: 'Server-side encryption encrypts data at rest.' The footer includes links for CloudShell, Feedback, Privacy, Terms, and Cookie preferences.

viii) Now click on upload it show success.

The screenshot shows the AWS S3 'Upload: status' page. At the top, a green banner indicates 'Upload succeeded' with the message 'For more information, see the Files and folders table.' Below this, a summary table shows one file uploaded ('Succeeded') and zero files failed ('Failed'). The 'Files and folders' tab is selected, displaying a table with one row for 'successful.txt'. The table columns include Name, Folder, Type, Size, Status, and Error. The file 'successful.txt' is listed with a size of 10.0 B and a status of 'Succeeded'. At the bottom of the page, there are links for CloudShell, Feedback, and copyright information.

ix) Now open the file and we can see everything as shown in fig.

The screenshot shows the AWS S3 'Object details' page for the file 'successful.txt'. The left sidebar includes navigation links for Amazon S3, General purpose buckets, Storage Lens, and AWS Marketplace for S3. The main content area displays the object's properties: Owner (shreenu.sutar22), AWS Region (US East (N. Virginia)), Last modified (July 11, 2025, 22:55:07 (UTC+05:30)), Size (10.0 B), Type (txt), and Key (successful.txt). On the right, there are sections for 'Object overview' (containing S3 URI, ARN, Etag, and Object URL), 'Management configurations' (with Replication status and View replication rules), and 'Expiration rule' (with a note about lifecycle configuration). A warning message at the bottom left encourages enabling Bucket Versioning to prevent unintentional overwriting. The bottom of the page includes CloudShell, Feedback, and copyright information.

x) Under permission section you can see all required things like public url .

The screenshot shows the AWS S3 console interface. On the left, there's a sidebar with various navigation links like 'Amazon S3', 'General purpose buckets', 'Storage Lens', and 'Feature spotlight'. The main area shows a file named 'successful.txt' in the 'himanshuchitoria' bucket. The 'Permissions' tab is active. A note says: 'This bucket has the bucket owner enforced setting applied for Object Ownership. When bucket owner enforced is applied, use bucket policies to control access.' Below this, it lists grants: 'Object owner (your AWS account)' (Read, Read, Write), 'Everyone (public access)' (Group: http://acs.amazonaws.com/groups/global/AllUsers), and 'Authenticated users group (anyone with an AWS account)' (Group: http://acs.amazonaws.com/groups/global/AuthenticatedUsers). At the bottom right, there are links for 'CloudShell', 'Feedback', and copyright information.

xi) Now for lifecycle rules click on configure lifecycle rules .

The screenshot shows the AWS S3 console interface. The 'Versions' tab is selected for the 'successful.txt' object. A green banner at the top says 'Successfully edited Bucket Versioning for "himanshuchitoria"'. Below it, a note says 'To transition, archive, or delete older object versions, configure lifecycle rules for this bucket.' The main area shows a table titled 'Versions (0)' with columns: Version ID, Type, Last modified, Size, and Storage class. A message at the bottom says 'This object has no versions to display because Bucket Versioning has not been enabled for this bucket.' At the bottom right, there are links for 'CloudShell', 'Feedback', and copyright information.

xii) Click on create lifecycle rules .

The screenshot shows the 'Lifecycle configuration' page in the Amazon S3 console. The left sidebar includes sections for General purpose buckets, Storage Lens, and AWS Marketplace for S3. The main content area is titled 'Lifecycle configuration' and contains a sub-section 'Lifecycle rules'. It displays a search bar, filter options (Lifecycle rule name, Status, Scope), and a table header for Current version actions, Noncurrent versions a..., Expired object delete ..., and Incomplete multipart A message at the bottom states 'There are no lifecycle rules for this bucket.' and includes a 'Create lifecycle rule' button.

xiii) Enter all required configurations as per your need . For example here we are providing 30 days of expiration time .

The screenshot shows the 'Create lifecycle rule' dialog. It has several sections:

- Prefix:** An input field labeled 'Enter prefix' with placeholder text 'You can filter objects by prefix, object tags, object size, or whatever combination suits your usecase.'
- Object tags:** A section with an 'Add tag' button and a note about key/value pairs.
- Object size:** A section with checkboxes for 'Specify minimum object size' and 'Specify maximum object size'.
- Lifecycle rule actions:** A section where users choose actions. The 'Expire current versions of objects' checkbox is checked, while others like 'Transition current versions of objects between storage classes' and 'Delete expired object delete markers or incomplete multipart uploads' are unchecked.
- Days after object creation:** A section with an 'Enter number of days' input field and a note: 'Expiration is required for the selected action. Enter a value or deselect the action.'

xiv) Rule successfully created .

The screenshot shows the 'Lifecycle configuration' page for a bucket named 'himanshuchitoria'. A green success message at the top states: 'The rule "30days" has been successfully added and the lifecycle configuration has been updated. It may take some time for the configuration to be updated. Refresh the lifecycle rules list if changes to the configuration aren't displayed.' Below this, the 'Lifecycle rules (1)' section displays a single rule named '30days'. The rule is set to 'Enabled' and has a status of 'Filtered'. The 'Expires' field is set to 'Never'. The table header includes columns for 'Lifecycle rule name', 'Status', 'Scope', 'Current version actions', 'Noncurrent versions ac...', 'Expired object delete ...', and 'Incomplete multipart up...'. The 'Actions' button is highlighted in orange.

xv) Now in this we will see how to delete the object in bucket. Clicking on the object which we have to delete.

The screenshot shows the 'Delete objects' page for the same bucket. The 'Specified objects' section lists a single file named 'successful.txt' with a size of 10.0 B. The 'Delete objects?' confirmation box contains the word 'delete' in the input field. The 'Delete objects' button is highlighted in orange.

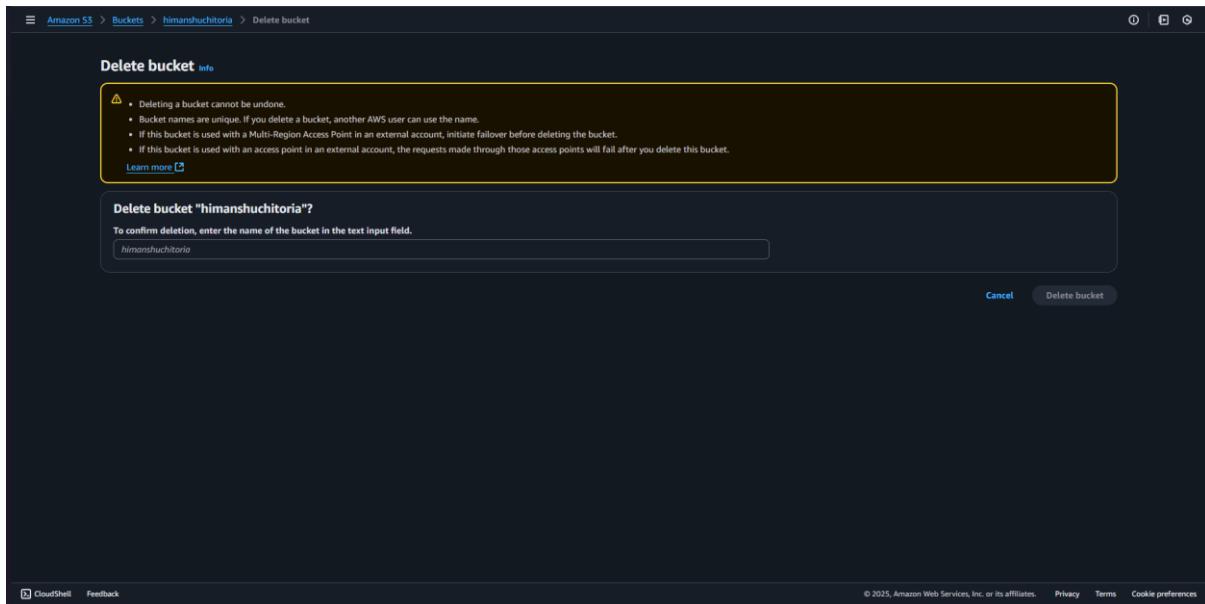
xvi) Successfully delete the object .

The screenshot shows the 'Delete objects: status' page. At the top, a green banner indicates 'Successfully deleted objects' with a link to 'View details below.' Below the banner, the title 'Delete objects: status' is displayed with a 'Close' button. A note states: 'After you navigate away from this page, the following information is no longer available.' The main area is titled 'Summary' and includes tabs for 'Failed to delete' (selected) and 'Configuration'. Under 'Failed to delete', it shows '0' failed objects. A search bar 'Find objects by name' is present. A table header row includes columns for Name, Type, Last modified, Size, and Error. A message at the bottom of the table says 'No objects failed to delete.'

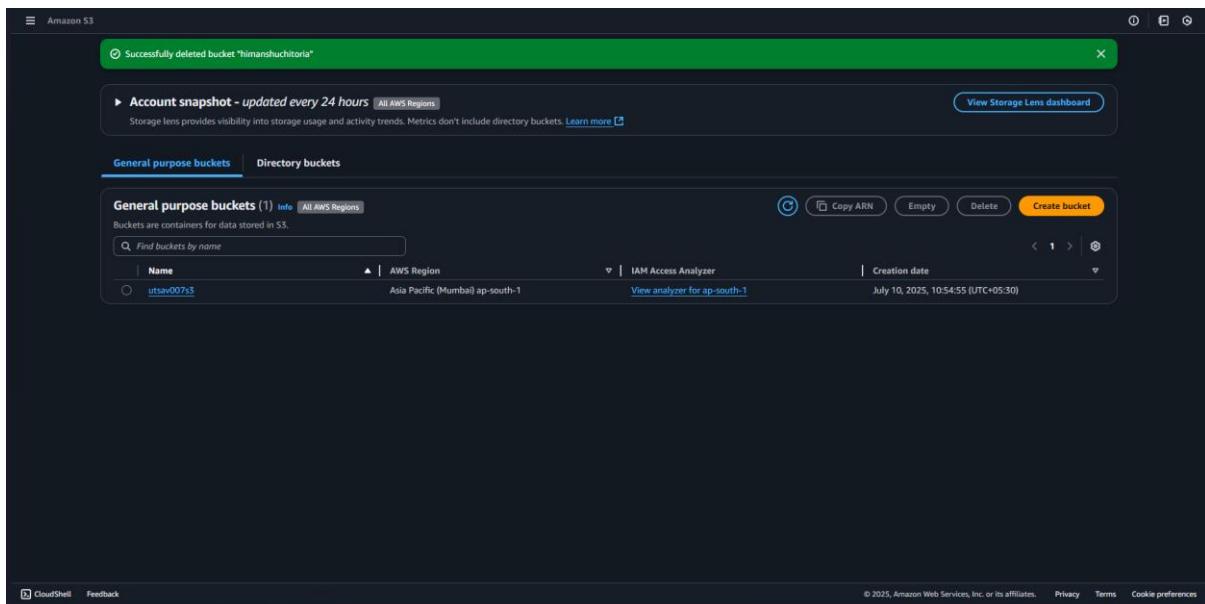
xvii) Now in this we will delete the bucket which we have created .For this the most important part is the buket must be empty .

The screenshot shows the 'Empty bucket' page for the 'himanshuchitoria' bucket. The top navigation bar shows 'Amazon S3 > Buckets > himanshuchitoria > Empty bucket'. A yellow warning box contains the following text: '⚠ Empting the bucket deletes all objects in the bucket and cannot be undone. • Objects added to the bucket while the empty bucket action is in progress might be deleted. • To prevent new objects from being added to this bucket while the empty bucket action is in progress, you might need to update your bucket policy to stop objects from being added to the bucket.' A 'Learn more' link is also present. Below the warning, a note says: 'If your bucket contains a large number of objects, creating a lifecycle rule to delete all objects in the bucket might be a more efficient way of emptying your bucket. Learn more' with a 'Go to lifecycle rule configuration' button. A section titled 'Permanently delete all objects in bucket "himanshuchitoria"' asks to 'confirm deletion' by typing 'permanently delete' into a text input field. At the bottom right are 'Cancel' and 'Empty' buttons.

xviii) Now again tick the bucket and click on delete and you will see this .



xix) Bucket successfully deleted .



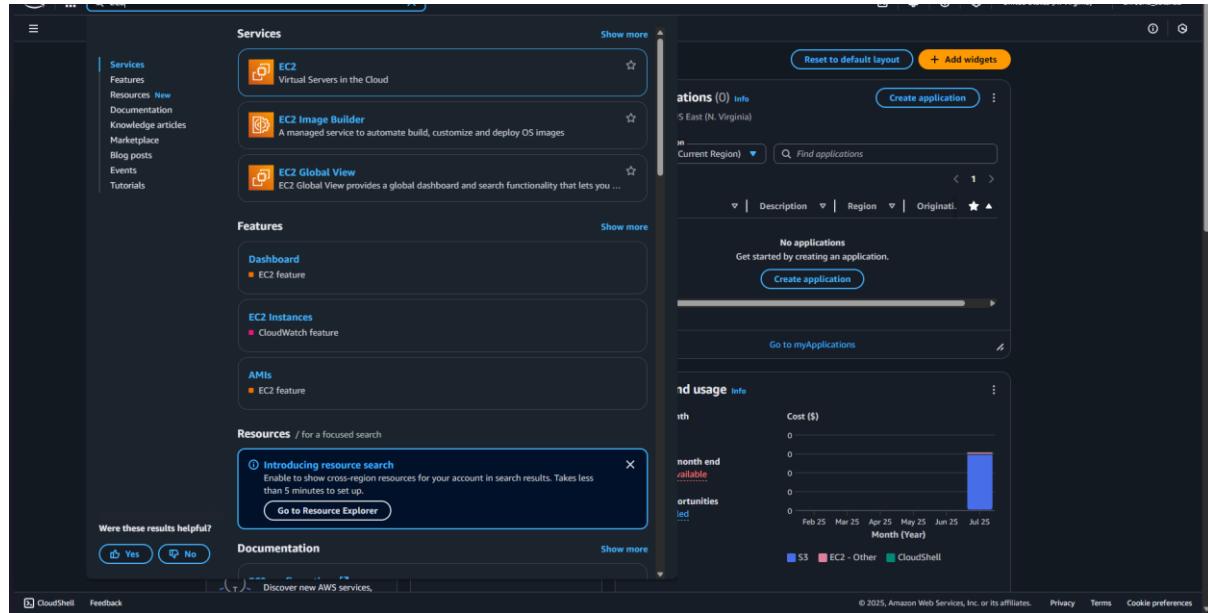
Date: 25-07-2025	Title
Exp. No: 06	HOW TO CREATE AN EC2 INSTANCE

AIM OF THE EXPERIMENT: HOW TO CREATE AN EC2 INSTANCE

PROCEDURE:

Follow the below steps to complete the requirements :

- OPEN THE AWS ROOT ACCOUNT AND SEARCH FOR EC2



ii) CLICK ON EC2, EC2 DASHBOARD WILL APPEAR.

The screenshot shows the AWS EC2 Dashboard. On the left, a sidebar menu includes options like Dashboard, Instances, Images, Elastic Block Store, Network & Security, and Load Balancing. The main area displays 'Resources' for the United States (N. Virginia) Region, showing 0 instances running, 0 dedicated hosts, 2 key pairs, and 5 security groups. It also shows 0 auto scaling groups, 0 elastic IPs, 0 load balancers, 0 capacity reservations, 0 instances, 0 placement groups, 0 snapshots, and 0 volumes. A 'Launch instance' button is present. To the right, there's a 'Service health' section indicating the service is operating normally, and a 'Zones' table listing availability zones (us-east-1a through us-east-1f) with their respective Zone IDs. The 'EC2 Free Tier' section shows 2 EC2 free tier offers in use. The 'Offer usage (monthly)' section provides details on Linux EC2 Instances and storage space on EBS. The 'Account attributes' section lists the Default VPC (vpc-035e854f2a0f8c0f1), Settings (Data protection and security, Allowed AMIs, Zones, EC2 Serial Console, Default credit specification, EC2 console preferences), and Account ID (14%).

iii) SELECT THE REGION>ASIA PACIFIC>MUMBAI

This screenshot is identical to the one above, showing the AWS EC2 Dashboard for the United States (N. Virginia) Region. However, the sidebar shows the user has selected the 'Asia Pacific' region, specifically 'Mumbai'. The 'Regions' dropdown on the top right also shows 'United States (N. Virginia)' and 'Asia Pacific (Mumbai)'. The rest of the interface remains the same, displaying resource counts, service health, zones, and account attributes for the Mumbai region.

iv) SELECT LAUNCH INSTANCE

v) TYPE THE NAME OF THE INSTANCE

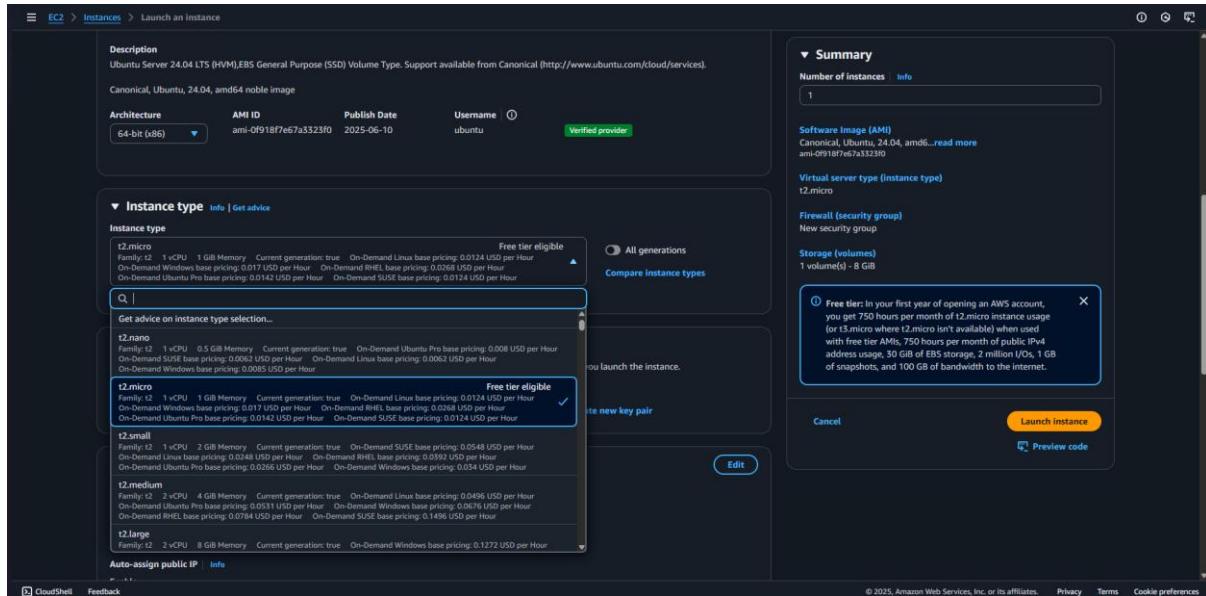
vi) CHOOSE THE OPERATING SYSTEM>UBUNTU

The screenshot shows the AWS EC2 Instances Launch an instance page. In the 'Name and tags' section, an AMI named 'Himanshu_22bee10118' is selected. Under 'Application and OS Images (Amazon Machine Image)', the 'Ubuntu' icon is highlighted. The 'Amazon Machine Image (AMI)' section shows 'Ubuntu Server 24.04 LTS (HVM), SSD Volume Type'. On the right, a summary box indicates 1 instance, software image (Canonical, Ubuntu, 24.04, amd64), and a virtual server type (t2.micro). A tooltip for t2.micro states: 'Free tier: In your first year of opening an AWS account, you get 750 hours per month of t2.micro instance usage (or t3.micro where t2.micro isn't available) when used with free tier AMIs, 750 hours per month of public IPv4 address usage, 30 GiB of EBS storage, 2 million I/Os, 1 GB of snapshots, and 100 GB of bandwidth to the internet.' A 'Launch instance' button is visible.

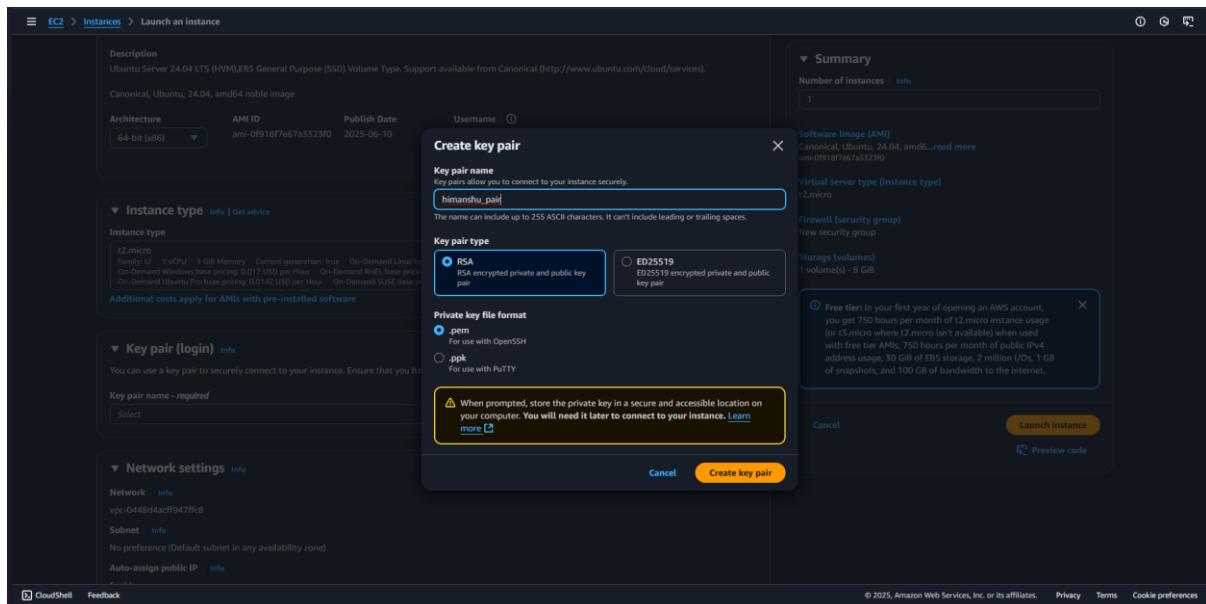
vii) CHOOSE THE ARCHITECTURE>64-bit(x86)

The screenshot shows the AWS EC2 Instances Launch an instance page. In the 'Architecture' section, '64-bit (x86)' is selected. The 'Amazon Machine Image (AMI)' section shows 'Ubuntu Server 24.04 LTS (HVM), SSD Volume Type'. Under 'Instance type', the 't2.micro' option is selected. A tooltip for t2.micro states: 'Free tier: In your first year of opening an AWS account, you get 750 hours per month of t2.micro instance usage (or t3.micro where t2.micro isn't available) when used with free tier AMIs, 750 hours per month of public IPv4 address usage, 30 GiB of EBS storage, 2 million I/Os, 1 GB of snapshots, and 100 GB of bandwidth to the internet.' A 'Launch instance' button is visible.

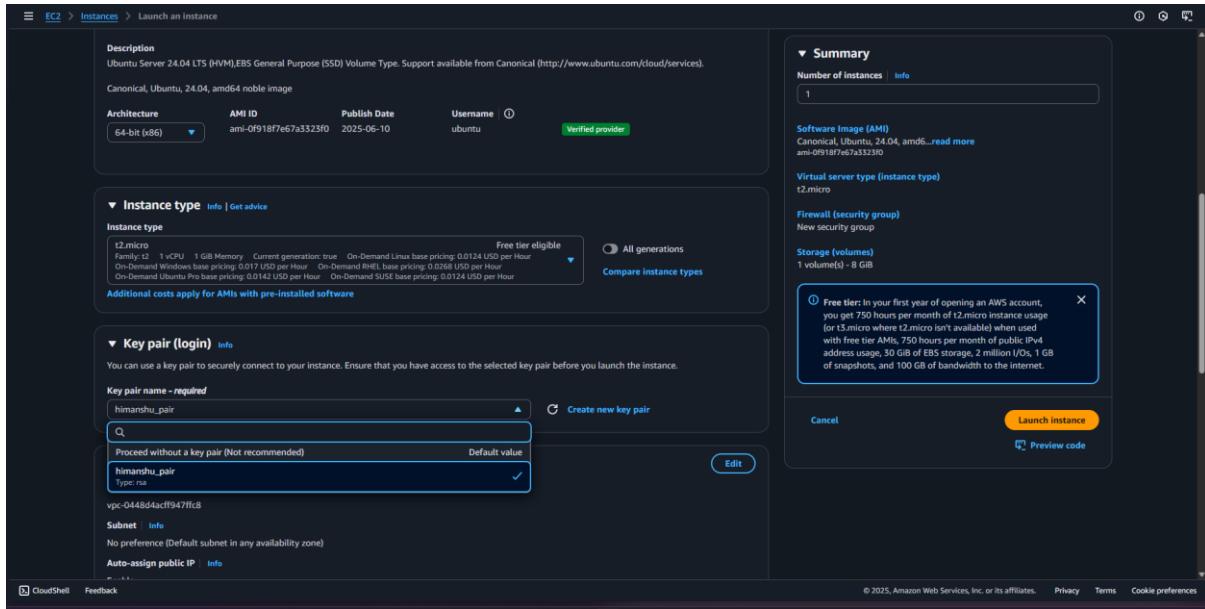
viii) CHOOSE INSTANCE TYPE: t2 micro (Free tier eligible)



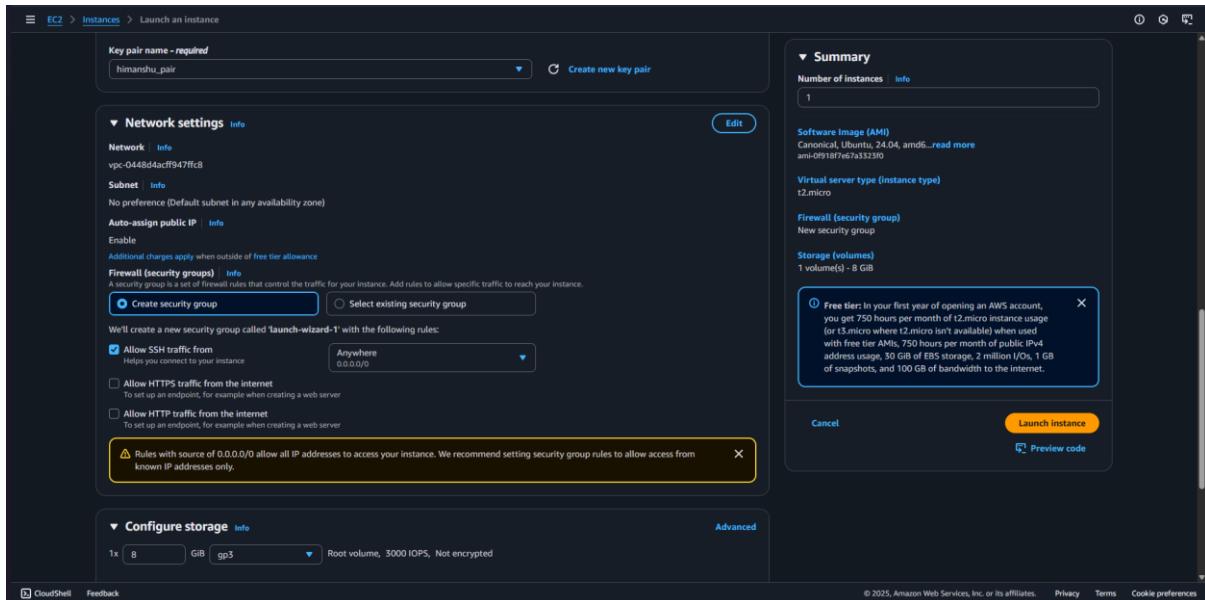
- ix) CREATE A NEW KEY PAIR: There are two keys involved in this step. One is private key for user and another is public key for the EC2 instance. Once we create a pair, both the keys will be generated. Public key need to saved separately for future use. Both keys will have same name as given.



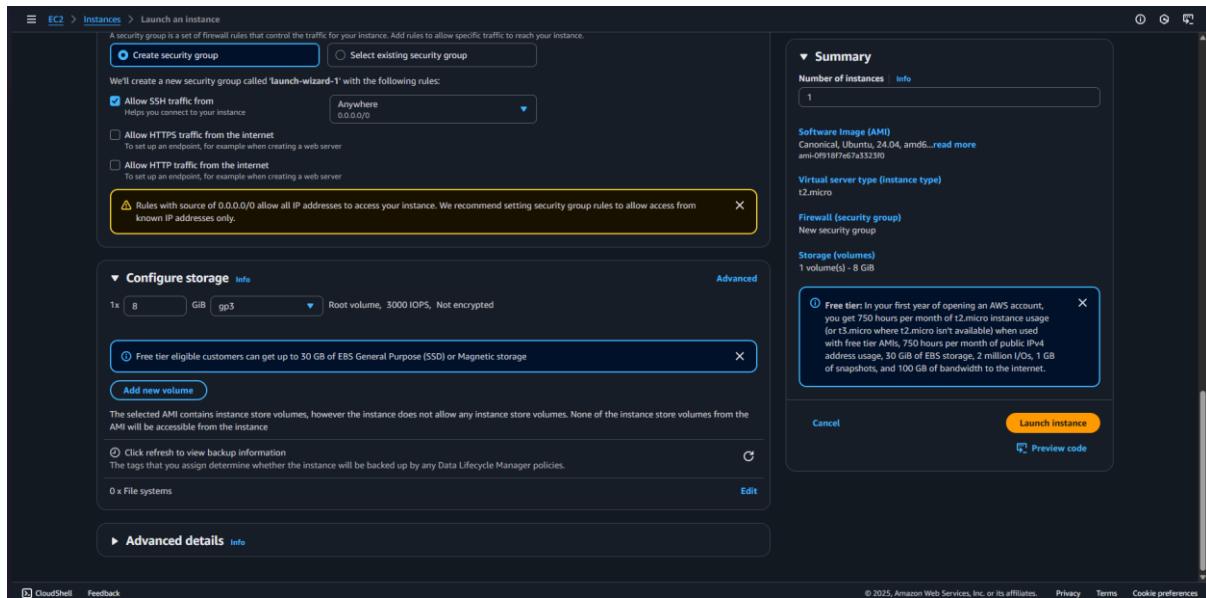
x) PUBLIC KEY IS AUTOMATICALLY ENABLED IN EC2 INSTANCE



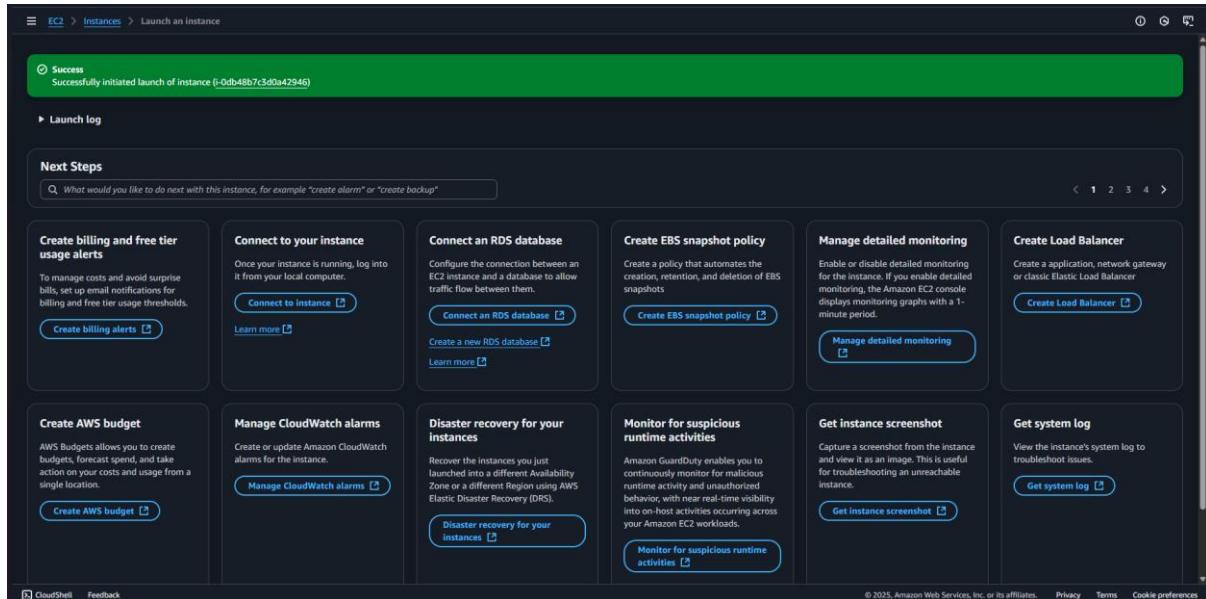
xi) CHOOSE THE DEFAULT NETWORK SETTINGS (NOTE: Auto-assign public IP should be enabled and source:0.0.0.0/0 allows all the IP addresses to access the EC2 instance)



xii) CHOOSE THE DEFAULT CONFIGURE STORAGE AND CLICK ON LAUNCH INSTANCE



xiii) EC2 INSTANCE IS CREATED, CLICK ON THE INSTANCE.



xiv) NOW CLICK ON THE EC2 INSTANCE

The screenshot shows the AWS EC2 Instances page. On the left, there's a navigation sidebar with various options like Dashboard, EC2 Global View, Events, Instances, Images, Elastic Block Store, Network & Security, Load Balancing, and CloudShell. The main area displays a table titled 'Instances (1) Info' with one row. The row contains the following information: Name (Himanshu_22...), Instance ID (i-0db48b7c3d0a42946), Instance state (Running), Instance type (t2.micro), Status check (Initializing), Alarm status (None), Availability Zone (ap-south-1b), Public IPv4 DNS (ec2-3-111-58-139.ap-s...), Public IPv4 IP (3.111.58.139), and Elastic IP (None). Below the table, a modal window titled 'Select an instance' is open, showing the same instance details. At the bottom right of the page, there are links for '© 2025, Amazon Web Services, Inc. or its affiliates.', 'Privacy', 'Terms', and 'Cookie preferences'.

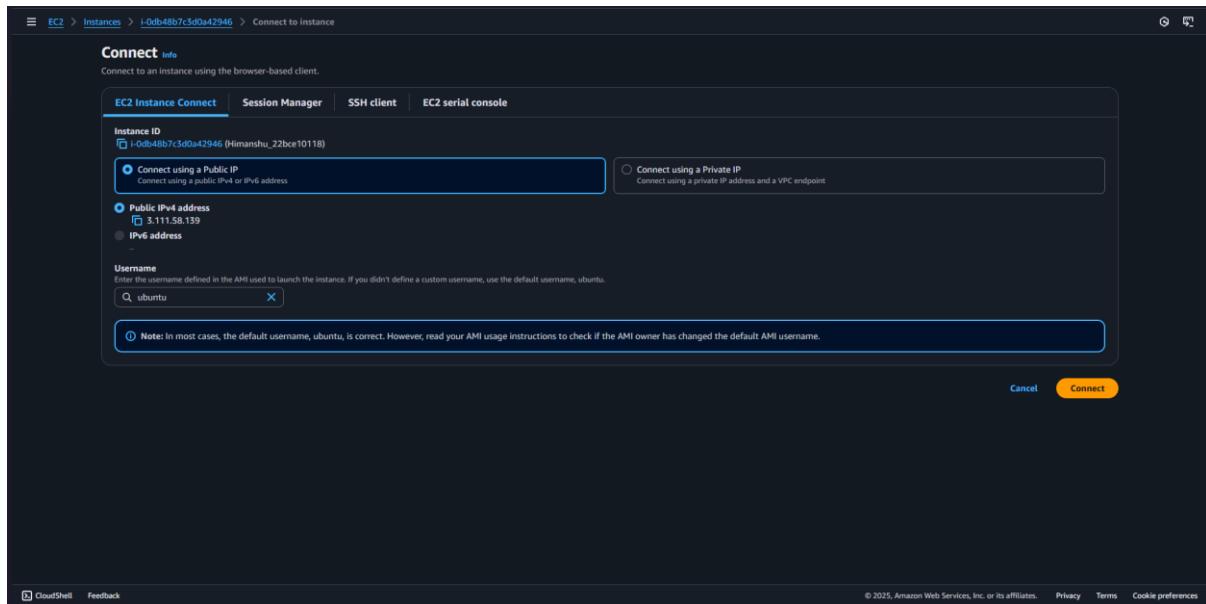
xv) DETAILS OF THE EC2 INSTANCE IS SHOWN, CLICK ON CONNECT

The screenshot shows the AWS EC2 Instances page with the same interface as the previous one, but the 'Details' tab is selected in the modal window. This tab provides more detailed information about the instance. Key details shown include:

- Instance summary:** Instance ID (i-0db48b7c3d0a42946), Public IPv4 address (3.111.58.139), Private IP address (172.31.8.71), Hostname type (IP name: ip-172-31-8-71.ap-south-1.compute.internal), Instance type (t2.micro), Auto-assigned IP address (3.111.58.139 [Public IP]), IAM Role (None), IMDSv2 Required, Operator (None).
- Networking:** VPC ID (vpc-044bd4acf947ffcb), Subnet ID (subnet-0e36df7fffc1220b), Instance ARN (arn:aws:ec2:ap-south-1:116555269880:instance/i-0db48b7c3d0a42946).
- Private IP addresses:** 172.31.8.71.
- Public DNS:** ec2-3-111-58-139.ap-south-1.compute.amazonaws.com.
- Elastic IP addresses:** None.
- AWS Compute Optimizer finding:** Opt-in to AWS Compute Optimizer for recommendations.
- Auto Scaling Group name:** None.
- Managed:** false.

At the bottom right of the page, there are links for '© 2025, Amazon Web Services, Inc. or its affiliates.', 'Privacy', 'Terms', and 'Cookie preferences'.

xvi) CLICK ON EC2 INSTANCE CONNECT>CONNECT



xvii) IT WILL LAND YOU TO THE TERMINAL PAGE

```
Welcome to Ubuntu 24.04.2 LTS (GNU/Linux 6.8.0-1029-aws x86_64)

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

System information as of Mon Jul 14 11:49:02 UTC 2025
System load: 0.24      Processes:          106
Usage of /: 25.3% of 6.71GB  Users logged in: 0
Memory usage: 21%
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-172-31-0-71:~$
```

i-0db48b7c5d0842946 (Himanshu_22bce10118)
PublicIPs: 3.111.58.139 PrivateIPs: 172.31.8.71

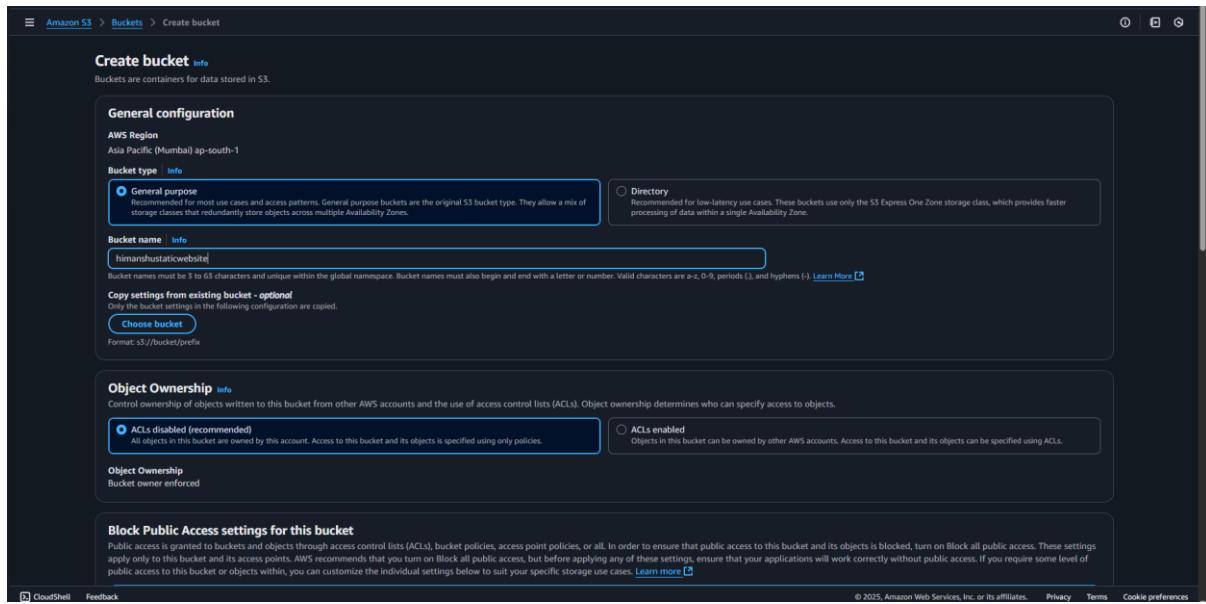
Date: 25-07-2025	Title
Exp. No: 07	HOW TO CREATE A STATIC WEBSITE IN S3

AIM OF THE EXPERIMENT: HOW TO CREATE A STATIC WEBSITE IN S3

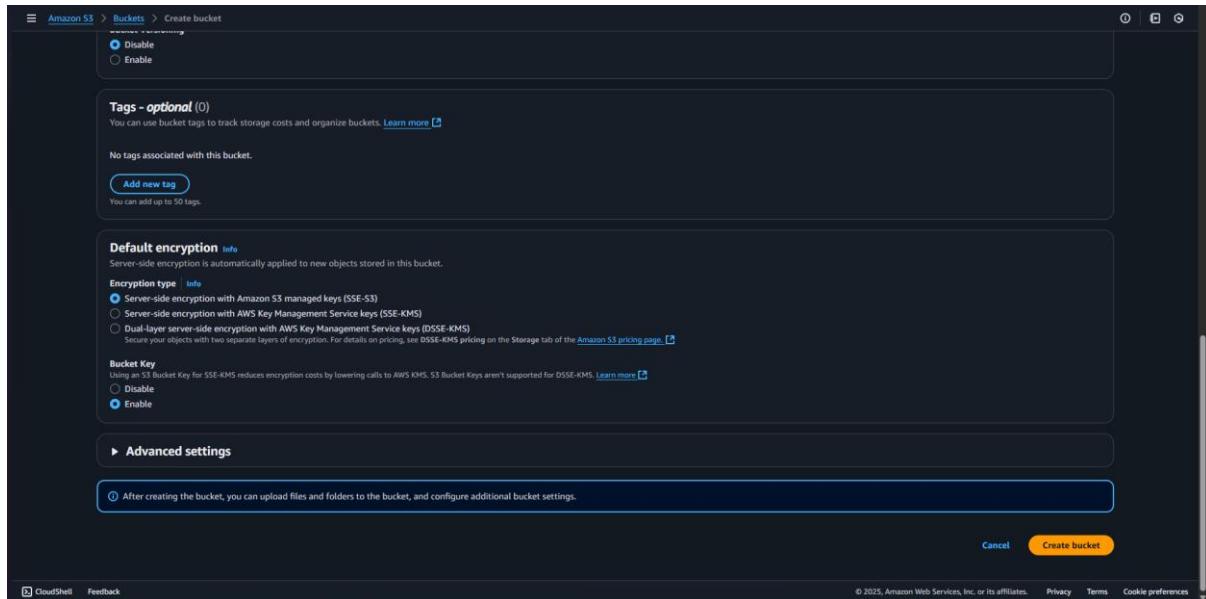
PROCEDURE:

Follow the below steps to complete the requirements :

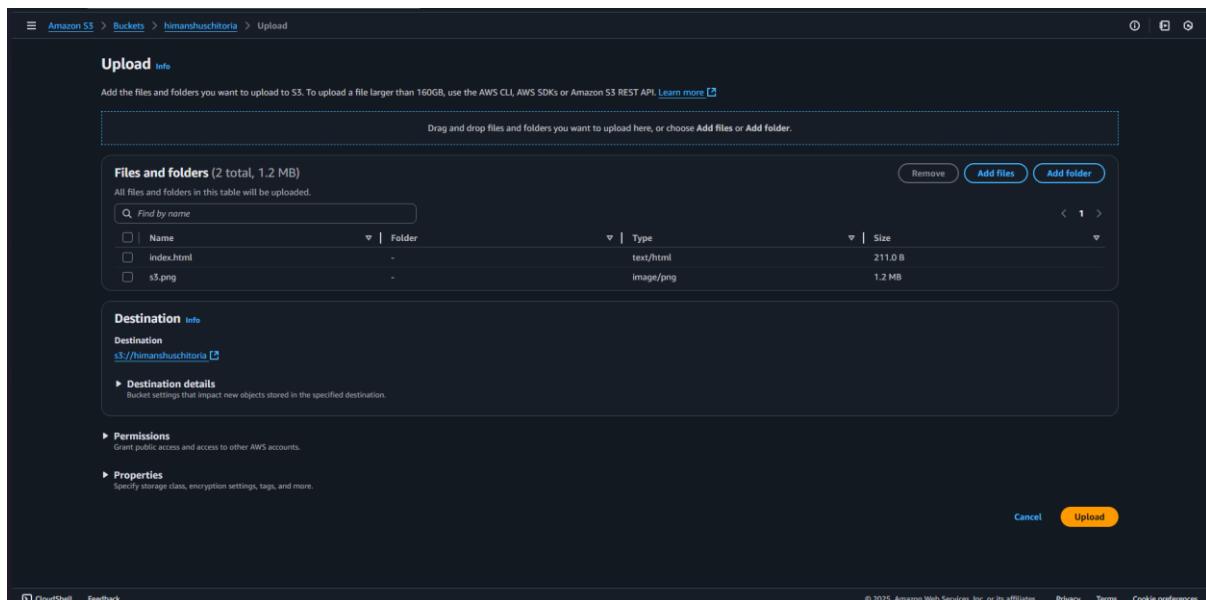
- i) GO TO AWS CONSOLE AND SEARCH FOR S3 AND CLICK ON CREATE A BUCKET.



- ii) GIVE THE BUCKET NAME AND KEEP THE REMAINING DEFAULT AND CLICK ON CREATE BUCKET .



- iii) ONCE THE BUCKET IS CREATED CLICK ON THE BUCKET TO UPLOAD FILES. Upload html file and image file.

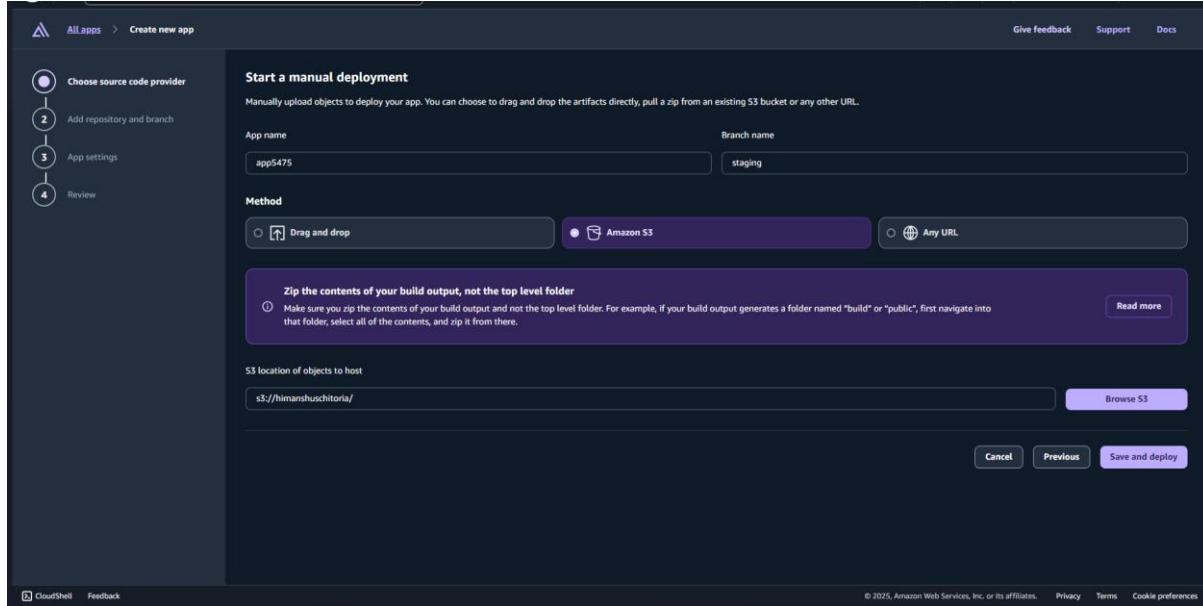


iv) ONCE THE FILES ARE UPLOADED. CLICK ON PROPERTIES AND CREATE AMPLIFY APP

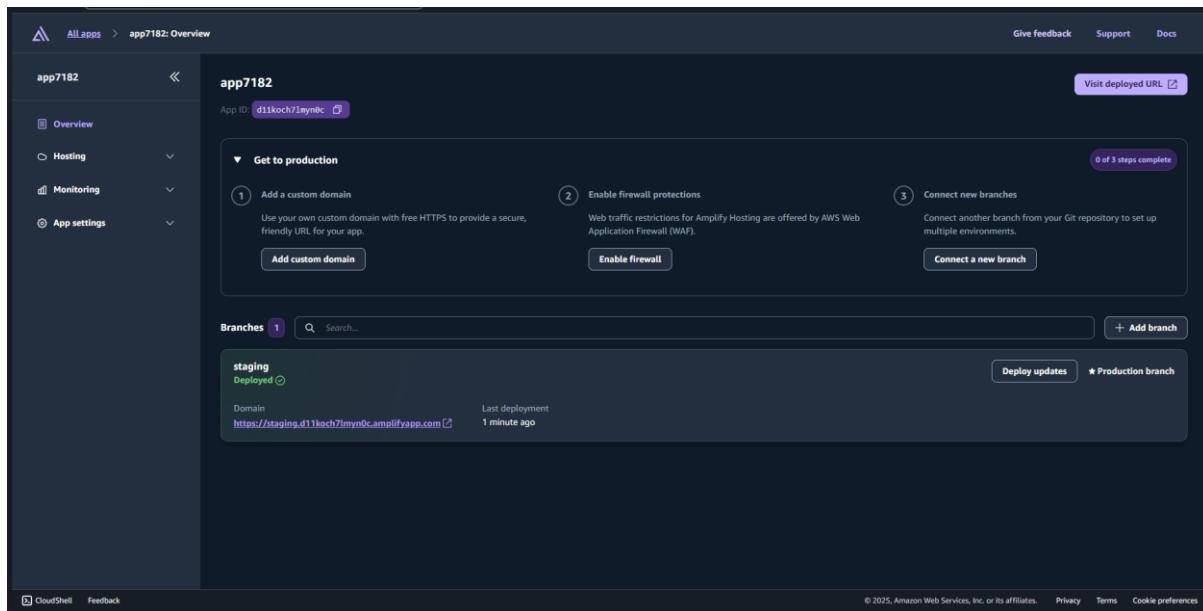
This screenshot shows the 'Properties' tab of the AWS S3 Bucket configuration for 'himanshuschitoria'. The 'Bucket overview' section displays the AWS Region (Asia Pacific (Mumbai) ap-south-1), ARN (arn:aws:s3:::himanshuschitoria), and Creation date (July 15, 2025, 21:53:36 (UTC+05:30)). The 'Bucket Versioning' section is set to 'Disabled'. The 'Multi-factor authentication (MFA) delete' section is also disabled. The 'Tags (0)' section shows no tags associated with the resource. The 'Default encryption' section indicates server-side encryption with Amazon S3 managed keys (SSE-S3). Navigation links at the bottom include CloudShell, Feedback, Privacy, Terms, and Cookie preferences.

This screenshot shows the 'Properties' tab of the AWS S3 Bucket configuration for 'himanshuschitoria'. It includes sections for notifications, transfer acceleration, object lock, requester pays, and static website hosting. The static website hosting section features a callout for AWS Amplify Hosting, with a 'Create Amplify app' button. Navigation links at the bottom include CloudShell, Feedback, Privacy, Terms, and Cookie preferences.

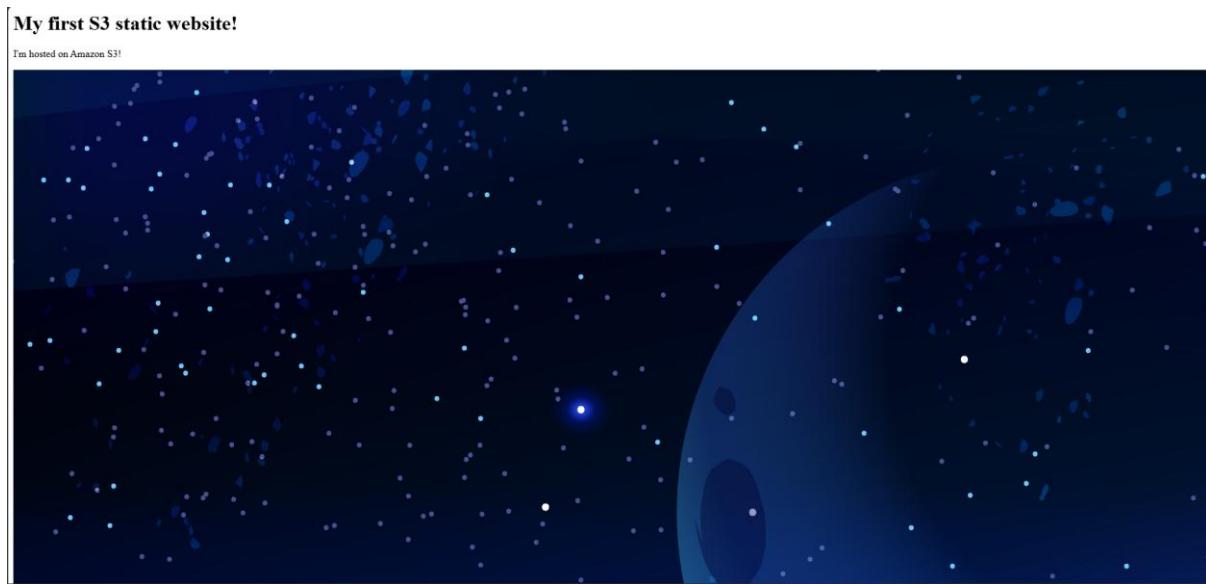
v) IT WILL LAND YOU TO AMPLIFY WINDOW. CLICK ON SAVE AND DEPLOY



vi) CLICK ON THE LINK BELOW.



vii) IT WILL LAND YOU TO YOUR STATIC WEBSITE



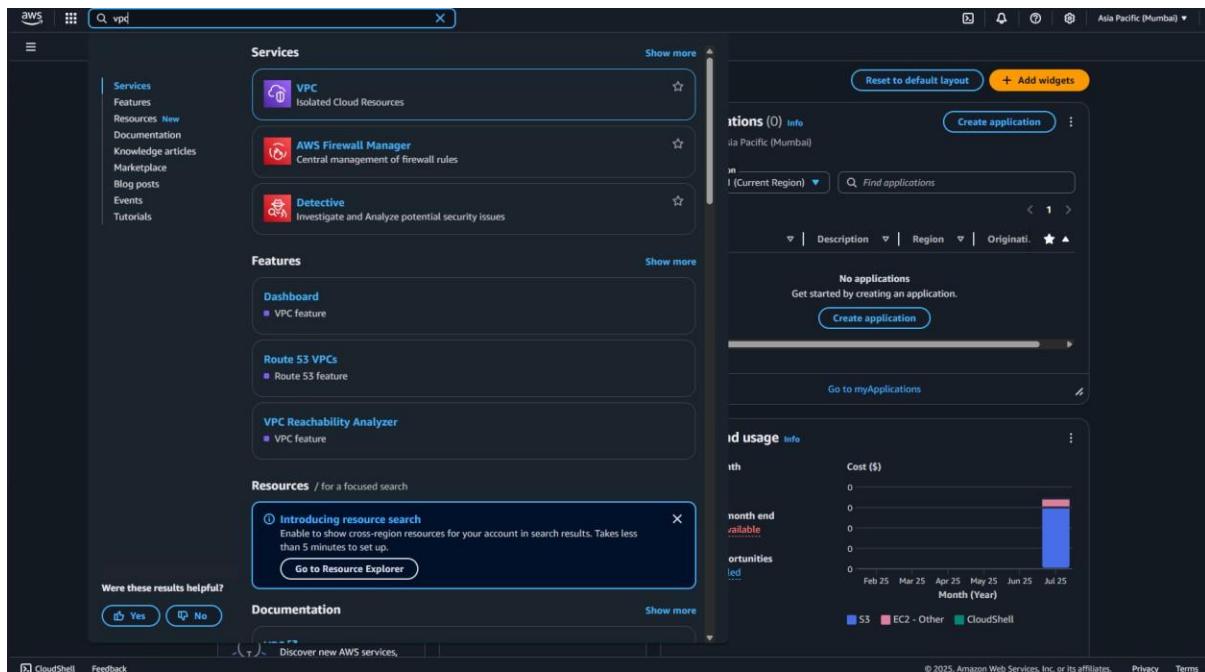
Date: 28-07-2025	Title
Exp. No: 08	HOW TO SETUP EC2 INSTANCE IN VPC

AIM OF THE EXPERIMENT: HOW TO SETUP EC2 INSTANCE IN VPC

PROCEDURE:

Follow the below steps to complete the requirements :

- LOGIN AS A ROOT USER AND SEARCH FOR VPC IN THE CONSOLE .



ii) CLICK ON CREATE VPC

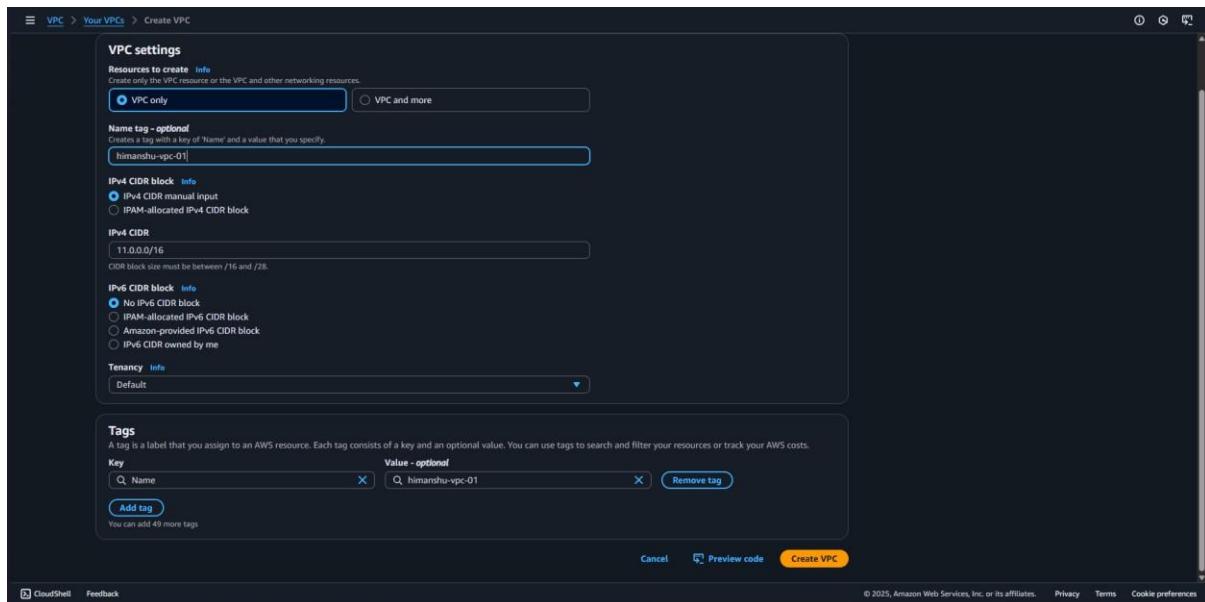
The screenshot shows the AWS VPC dashboard with the 'Create VPC' button highlighted. The dashboard displays various Amazon VPC resources across the Mumbai region, including VPCs (1), Subnets (5), Route Tables (1), Internet Gateways (0), and Security Groups (2). Other sections like NAT Gateways, VPC Peering Connections, Network ACLs, Customer Gateways, Virtual Private Gateways, Site-to-Site VPN Connections, and Running Instances are also visible.

iii) SELECT VPC ONLY> TYPE THE VPC NAME> IPv4CIDR-11.0.0.0/16
 NOTE: In AWS a VPC spans a specific IP address range using CIDR (Classless

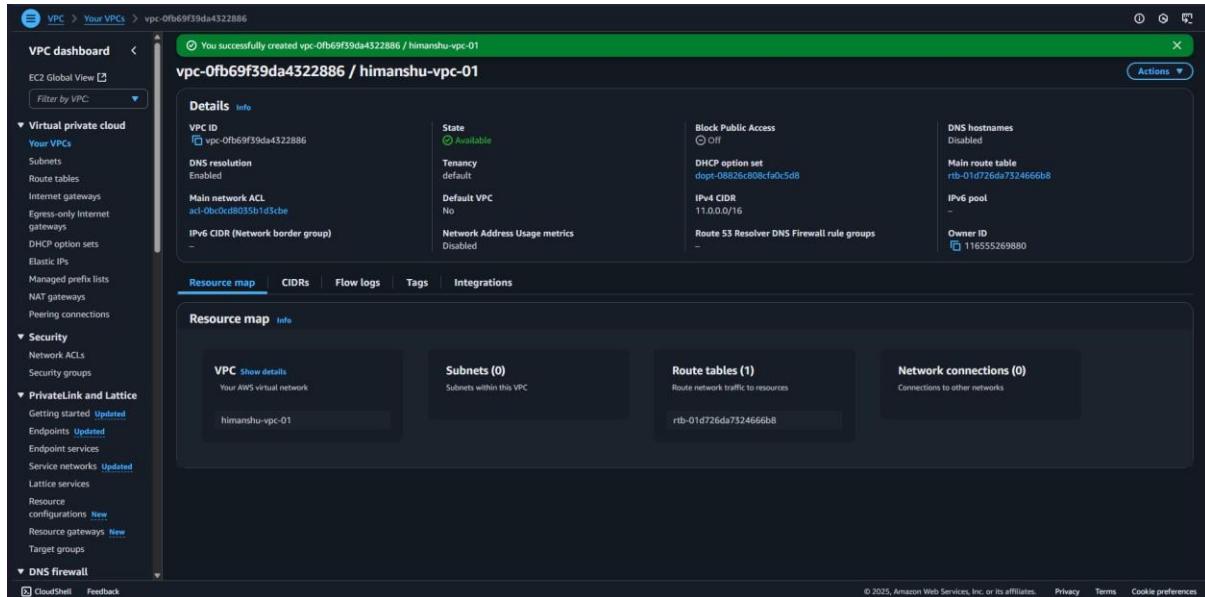
Inter-Domain Routing) blocks. The CIDR block defines the range of IP addresses that can be assigned to resources within the VPC

The screenshot shows the 'Create VPC' configuration page. Under 'VPC settings', the 'Resources to create' dropdown is set to 'VPC only'. The 'Name tag - optional' field contains 'my-vpc-01'. The 'IPv4 CIDR block' dropdown is set to 'IPv4 CIDR manual input' and the value '11.0.0.0/16' is entered. The 'Tenancy' dropdown is set to 'Default'. The 'Tags' section indicates 'No tags associated with the resource' and has an 'Add tag' button.

iv) CLICK ON CREATE VPC



v) VPC CREATED



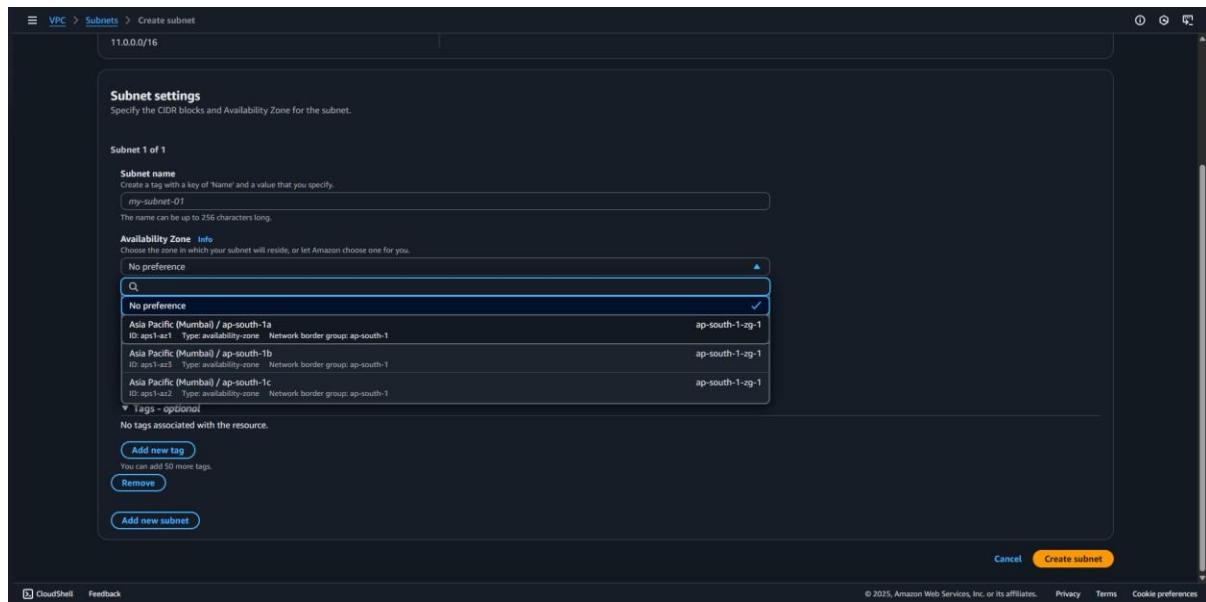
vi) CLICK ON SUBNET>CREATE SUBNET

The screenshot shows the AWS VPC Subnets page. On the left, there's a navigation sidebar with sections like EC2 Global View, Virtual private cloud, Security, Privatelink and Lattice, and DNS firewall. The main area displays a table titled 'Subnets (3) Info' with columns: Name, Subnet ID, State, VPC, Block Public..., IPv4 CIDR, IPv6 CIDR, and IPv6 I. The subnets listed are: subnet-0196030ffab11b0f5 (Available, vpc-0448d4acf947ffc8, Off, 172.31.16.0/20), subnet-0e56df7fffc11220b (Available, vpc-0448d4acf947ffc8, Off, 172.31.0.0/20), and subnet-0b7c8cc4b44cd8aa1 (Available, vpc-0448d4acf947ffc8, Off, 172.31.32.0/20). A 'Create subnet' button is located at the top right of the table.

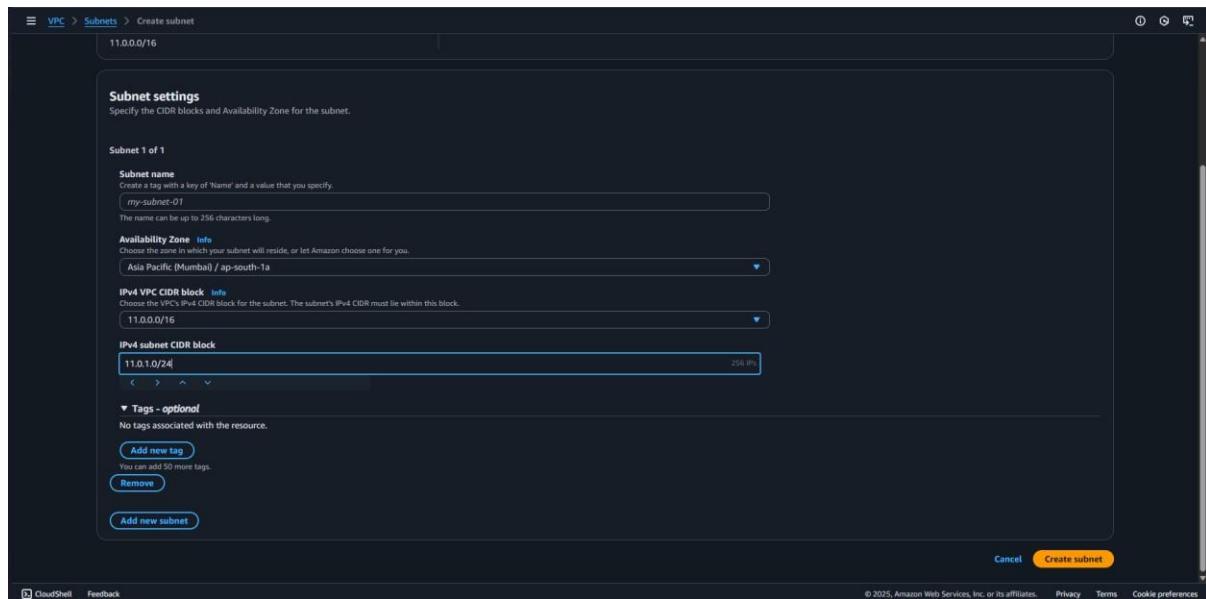
vii) SELECT THE VPC THAT YOU HAVE CREATED EARLIER

The screenshot shows the 'Create subnet' dialog box. It has a 'VPC' section where a dropdown menu is open, showing two options: 'vpc-0448d4acf947ffc8 (172.31.0.0/16)' and 'vpc-0fb69f39da4322886 (himanshu-vpc-01 11.0.0/16)'. Below the dropdown is a note: 'Select a VPC first to create new subnets.' At the bottom right are 'Cancel' and 'Create subnet' buttons.

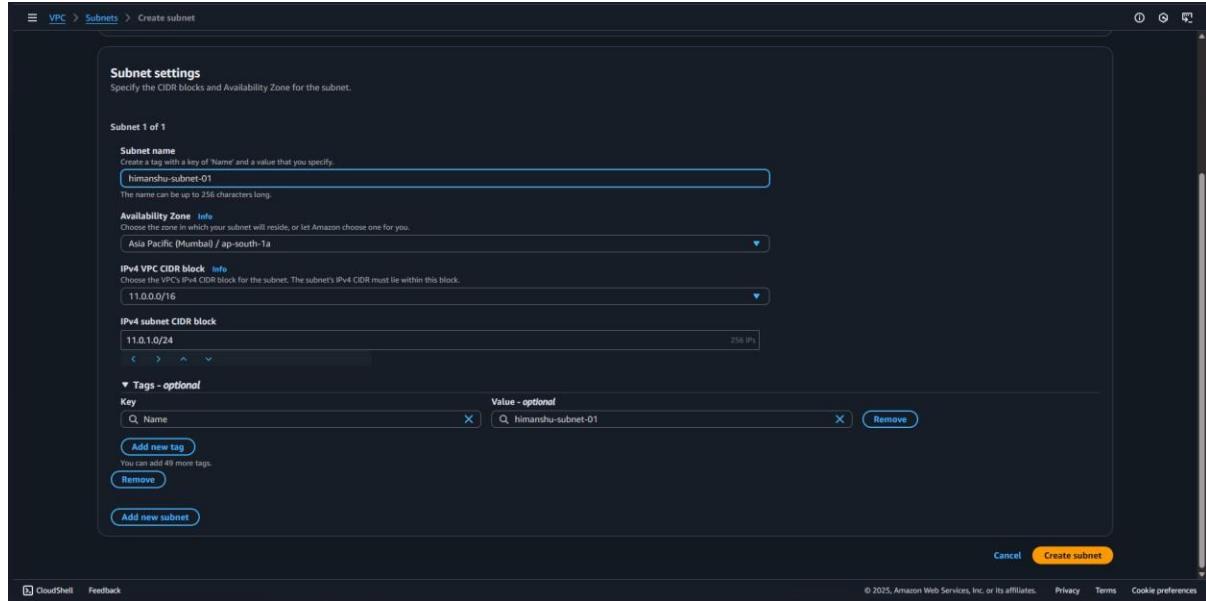
viii) SELECT ap-south-1a in the Availability Zone



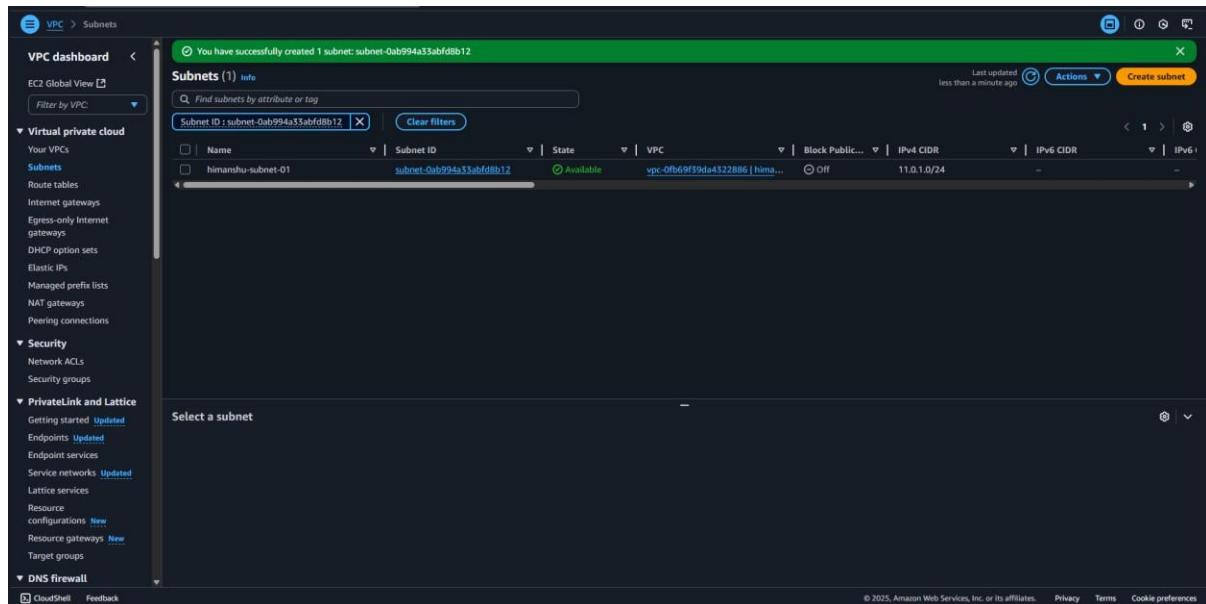
ix) ENTER IPv4 SUBNET CIDR BLOCK-11.0.1.0/24> CLICK ON ADD NEW SUBNET



- x) ENTER THE NAME OF THE PRIVATE SUBNET> AVAILABILITY ZONE:ap-south-1b> IPv4 subnet CIDR Block-11.0.2.0/24> CLICK ON CREATE SUBNET



- xi) BOTH THE PUBLIC AND PRIVATE SUBNET IS CREATED



- xii) NOW CREATE AN INTERNET GATEWAY FOR PUBLIC SUBNET. CLICK ON INTERNET GATEWAY FROM THE DASHBOARD> CLICK ON CREATE INTERNET GATEWAY

The screenshot shows the AWS VPC dashboard with the 'Internet gateways' section selected. A table lists one internet gateway:

Name	Internet gateway ID	State	VPC ID	Owner
-	igw-0b0fd369599a4f974	Attached	vpc-0448d4a-ff947ff-d	116555269880

A yellow button labeled 'Create internet gateway' is visible at the top right of the table.

- xiii) TYPE THE NAME OF THE GATEWAY

The screenshot shows the 'Create internet gateway' wizard. In the 'Internet gateway settings' step, a 'Name tag' is specified as 'himanshu-internet-gateway'. Below this, under 'Tags - optional', a single tag 'Name: himanshu-internet-gateway' is listed. At the bottom right, there are 'Cancel' and 'Create internet gateway' buttons.

xiv) INTERNET GATEWAY IS CREATED

The screenshot shows the AWS VPC dashboard with the 'Internet gateways' section selected. A success message at the top states: 'The following internet gateway was created: igw-0d608e79342ba1ce6 - himanshu-internet-gateway. You can now attach to a VPC to enable the VPC to communicate with the internet.' Below this, the 'igw-0d608e79342ba1ce6 / himanshu-internet-gateway' card displays the following details:

- Internet gateway ID:** igw-0d608e79342ba1ce6
- State:** Detached
- VPC ID:** -
- Owner:** 116555269880

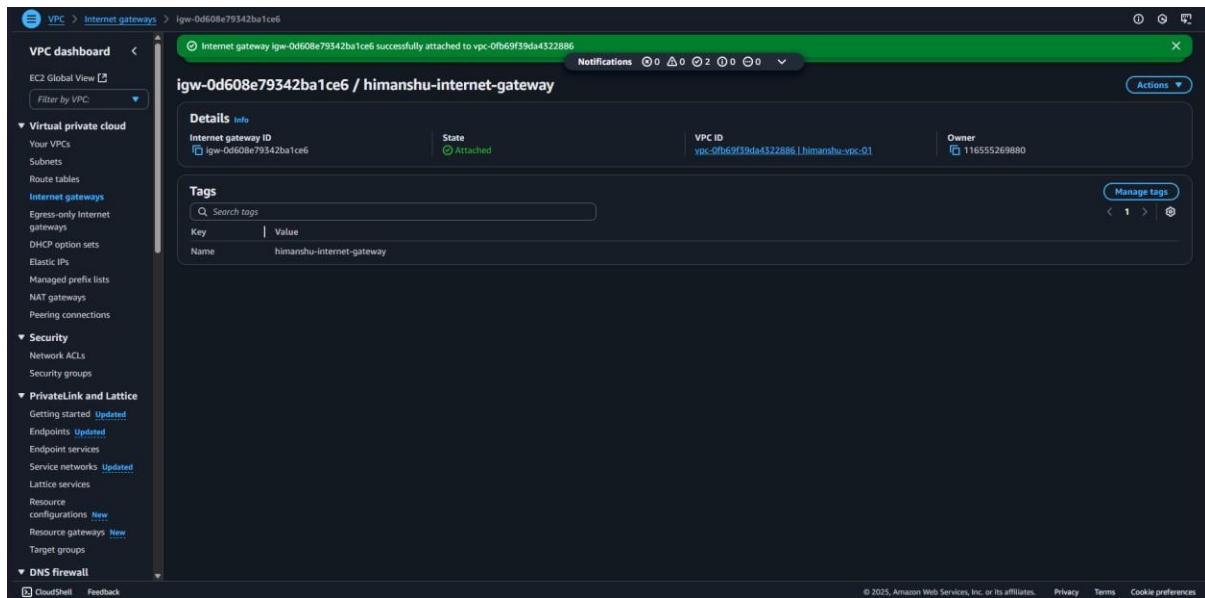
The 'Tags' section shows one tag: Name = himanshu-internet-gateway. The left sidebar lists various VPC management options like Virtual private cloud, Security, and PrivateLink and Lattice.

xv) CLICK ON ATTACH TO VPC> SELECT THE VPC CREATED EARLIER>
CLICK ON ATTACH INTERNET GATEWAY

The screenshot shows the 'Attach to VPC (igw-0d608e79342ba1ce6)' dialog box. It contains the following information:

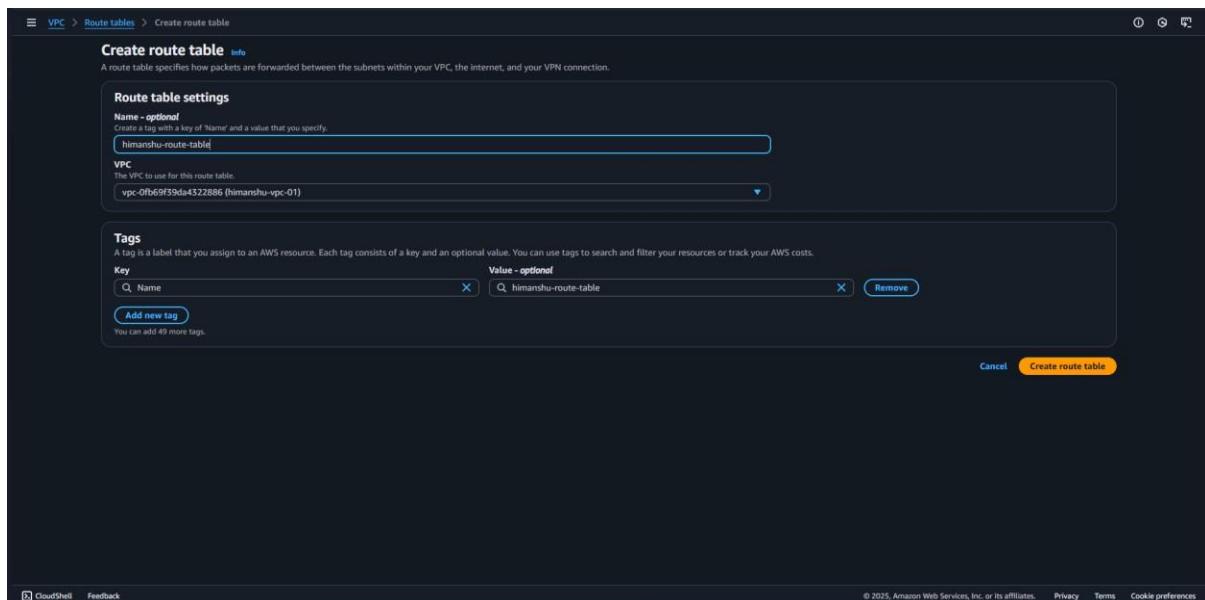
- A success message: 'The following internet gateway was created: igw-0d608e79342ba1ce6 - himanshu-internet-gateway. You can now attach to a VPC to enable the VPC to communicate with the internet.'
- A 'Available VPCs' section with a dropdown menu titled 'Select a VPC'. The dropdown shows one option: 'vpc-0f69599a4322886 - himanshu-vpc-01'.
- Buttons at the bottom: 'Cancel' and 'Attach internet gateway' (which is highlighted in yellow).

xvi) INTERNET GATEWAY IS ATTACHED TO THE VPC



xvii) NEXT CREATE TWO ROUTE TABLES (PRIVATE AND PUBLIC) FOR THE SUBNETS.

xviii) TO CREATE A PUBLIC ROUTE TABLE: CLICK ON ROUTE TABLES>CREATE A ROUTE TABLE> WRITE A SUITABLE NAME FOR THE ROUTE TABLE>CHOOSE THE VPC>CLICK ON CREATE ROUTE TABLE



- xix) BOTH THE PUBLIC AND PRIVATE ROUTE TABLES ARE CREATED AS SHOWN BELOW NOW WE NEED TO CONNECT BOTH THE ROUTE TABLES WITH THEIR CORRESPONDING SUBNETS.

The screenshot shows the AWS VPC dashboard with the 'Route tables' section selected. A success message at the top indicates 'Route table rtb-06bb9d6379b3f1d9c | himanshu-route-table was created successfully.' The 'Route tables (3) Info' table lists the following details:

Name	Route table ID	Explicit subnet associations	Main	VPC	Owner ID
-	rtb-096d8c140d110bf6	-	-	vpc-0448d4acf947ff8	116555269880
-	rtb-01d726da7324666b8	-	Yes	vpc-0fb69f39da4322886 him...	116555269880
himanshu-route-table	rtb-06bb9d6379b3f1d9c	-	No	vpc-0fb69f39da4322886 him...	116555269880

- xx) CLICK ON THE PUBLIC ROUTE TABLE>CLICK ON SUBNET ASSOCIATIONS

The screenshot shows the 'rtb-06bb9d6379b3f1d9c / himanshu-route-table' details page. The 'Subnet associations' tab is selected. A message at the top says 'Route table rtb-06bb9d6379b3f1d9c | himanshu-route-table was created successfully.' Below it, a table titled 'Explicit subnet associations (0)' shows no entries. A note below the table states 'No subnet associations' and 'You do not have any subnet associations.' At the bottom, a table titled 'Subnets without explicit associations (1)' lists a single subnet: 'himanshu-subnet-01' with 'subnet-0fb994a33abfd8b12' and '11.0.0/24'. An 'Edit subnet associations' button is located at the bottom right of this section.

- xxi) CLICK ON EDIT SUBNET ASSOCIATIONS > CHOOSE PUBLIC SUBNET FROM THE OPTIONS> CLICK ON SAVE ASSOCIATIONS

Name	Subnet ID	IPv4 CIDR	IPv6 CIDR	Route table ID
himanshu-subnet-01	subnet-0ab994a35abfd8b12	11.0.1.0/24	-	Main (rtb-01d726da7324666b8)

Selected subnets

subnet-0ab994a35abfd8b12 / himanshu-subnet-01

Save associations

- xxii) SUBNET ASSOCIATION IS DONE. REPEAT THE SAME STEP FOR PRIVATE SUBNET ASSOCIATION.

Name	Route table ID	Explicit subnet assoc...	Edge associations	Main	VPC	Owner ID
rtb-09dc8c140d110baf6	rtb-09dc8c140d110baf6	-	-	Yes	vpc-0448d4acf947ffcb	116555269880
rtb-01d726da7324666b8	rtb-01d726da7324666b8	-	-	Yes	vpc-0fb69f39da4322886 hima...	116555269880
himanshu-route-table	rtb-06bb9d6379b3f1d9c	subnet-0ab994a35abfd8b12	-	No	vpc-0fb69f39da4322886 hima...	116555269880

rtb-06bb9d6379b3f1d9c / himanshu-route-table

Details Routes Subnet associations Edge associations Route propagation Tags

Explicit subnet associations (1)

Name	Subnet ID	IPv4 CIDR	IPv6 CIDR
himanshu-subnet-01	subnet-0ab994a35abfd8b12	11.0.1.0/24	-

Subnets without explicit associations (0)

No subnets without explicit associations

All your subnets are associated with a route table.

- xxiii) NEXT WE NEED TO CREATE THE ROUTE SO THAT INTERNET CAN BE ACCESSED WITH THE HELP OF INTERNET GATEWAY THROUGH THESE ROUTE TABLES.
- xxiv) GO TO PUBLIC ROUTE TABLE FROM THE AWS CONSOLE> CLICK ON ROUTES>CLICK ON EDIT ROUTES

Name	Route table ID	Explicit subnet associations	Edge associations	Main	VPC	Owner ID
-	rtb-09d8c140d110bf6	-	-	Yes	vpc-0448d4acf947ff8	116555269880
-	rtb-01d726da7324666bb	-	-	Yes	vpc-0fb69f39da4322886 hima...	116555269880
himanshu-route-table	rtb-06bb9d6379b3f1d9c	-	-	No	vpc-0fb69f39da4522886 hima...	116555269880
himanshu-private - subnet	rtb-0124f9660dce455d7	subnet-0ab994a35abfd0...	-	No	vpc-0fb69f39da4522886 hima...	116555269880

- xxv) CLICK ON ADD ROUTE>SELECT THE IP-0.0.0.0/0>CHOOSE INTERNET GATEWAY> SELECT THE INTERNET GATEWAY THAT YOU HAVE CREATED> CLICK ON SAVE CHANGES (NOTE:0.0.0.0/0 means it allows all the IP addresses to access the resources present in the public subnet).

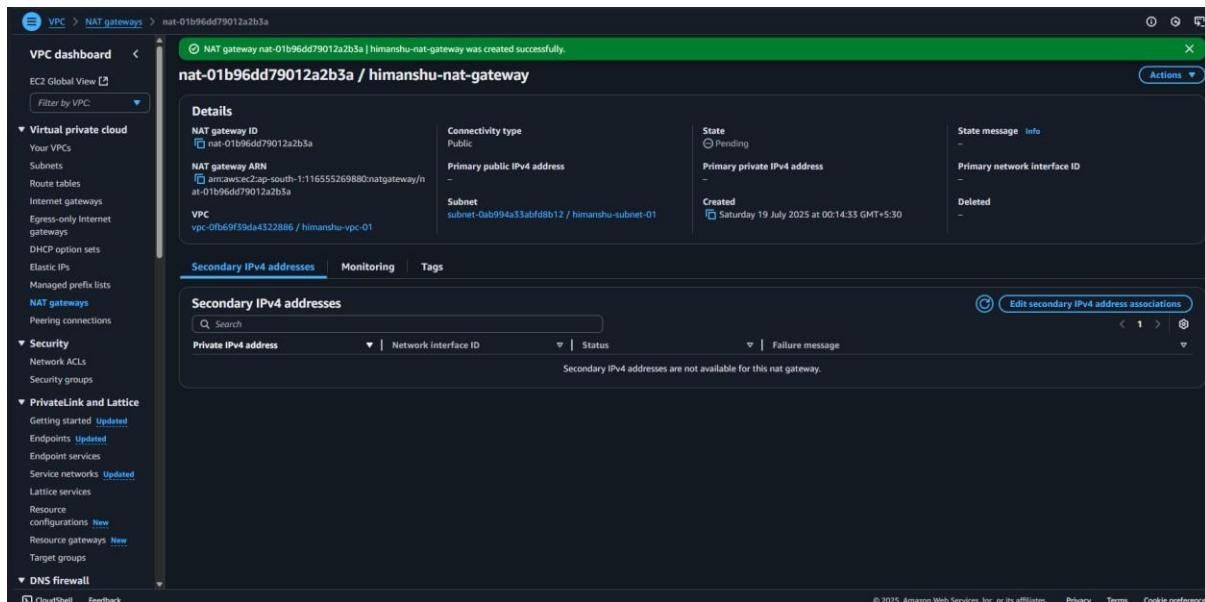
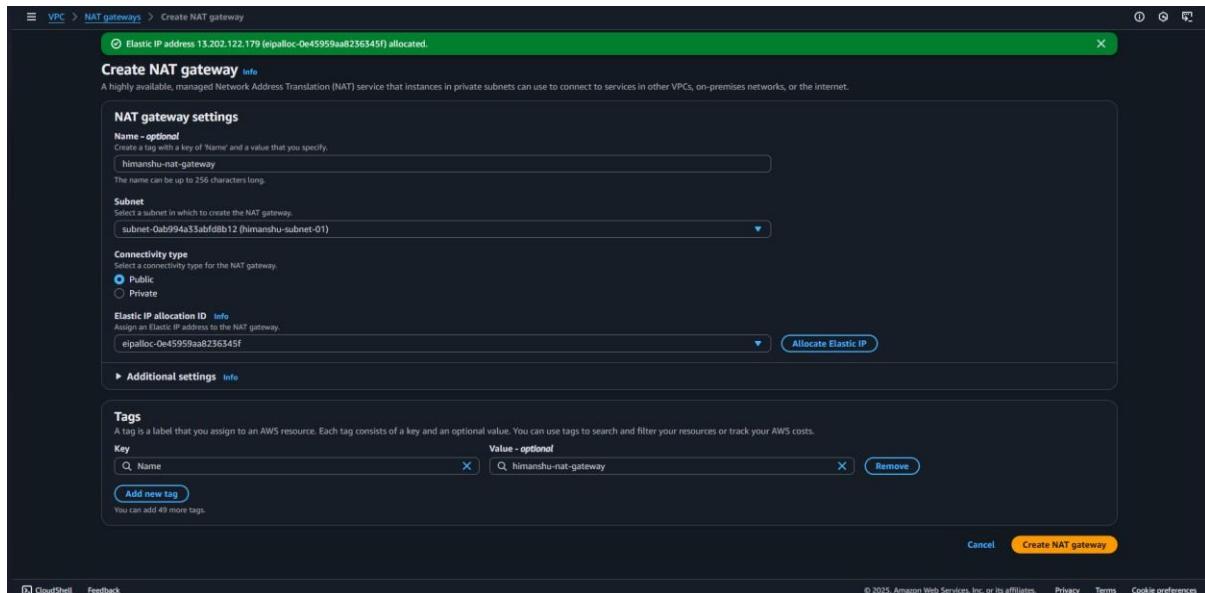
Destination	Target	Status	Propagated
11.0.0.0/16	local	Active	No

The screenshot shows the AWS VPC Route Tables page. At the top, a green banner displays the message "Updated routes for rtb-06bb9d6379b3f1d9c / himanshu-route-table successfully". Below this, the title "rtb-06bb9d6379b3f1d9c / himanshu-route-table" is shown. The left sidebar contains navigation links for VPC dashboard, Virtual private cloud (Your VPCs, Subnets, Route tables, Internet gateways, Egress-only Internet gateways, DHCP option sets, Elastic IPs, Managed prefix lists, NAT gateways, Peering connections), Security (Network ACLs, Security groups), PrivateLink and Lattice (Getting started, Endpoints, Endpoint services, Service networks, Lattice services, Resource configurations, Resource gateways, Target groups), and DNS firewall (CloudShell, Feedback). The main content area shows "Details" for the route table, including its ID (rtb-06bb9d6379b3f1d9c), Main status (No), Owner ID (vpc-0fb69f39da4322886 | himanshu-vpc-011655269880), and Edge associations. A "Routes" tab is selected, displaying two routes: one to igw-0d608e79342ba1ce6 (Status: Active, Propagated: No) and another local route (Status: Active, Propagated: No). The bottom right corner includes copyright information: "© 2025, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences".

- xxvi) WE NEED TO CREATE THE NAT GATEWAY FOR THE PRIVATE SUBNET SO THAT RESOURCES PRESENT INSIDE THE PRIVATE SUBNET CAN ACCESS THE INTERNET WITH THE HELP OF INTERNET GATEWAY.
- xxvii) CLICK ON NAT GATEWAYS FROM THE DASHBOARD > CLICK ON CREATE NAT GATEWAY.

The screenshot shows the AWS VPC NAT Gateways page. The left sidebar is identical to the previous VPC dashboard screenshot. The main content area shows a table titled "NAT gateways" with columns for Name, NAT gateway ID, Connectivity..., State, State message, Primary public IP..., Primary private IP..., Primary network..., and VPC. A message at the top states "No NAT gateways found". Below the table, a section titled "Select a NAT gateway" is displayed. The bottom right corner includes copyright information: "© 2025, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences".

xxviii) GIVE A NAME TO THE NAT GATEWAY>CHOOSE THE PUBLIC SUBNET>ALLOCATE ELASTIC IP> CLICK ON CREATE NAT GATEWAY.



xxix) NOW UPDATE THE PRIVATE ROUTE TABLE: CLICK ON THE ROUTE TABLES>CLICK ON THE PRIVATE ROUTE TABLE>CLICK ON ROUTES>CLICK ON EDIT ROUTES.

Name	Route table ID	Explicit subnet associ...	Edge associations	Main	VPC	Owner ID
rtb-09dc8c1404110bbf6	-	-	-	Yes	vpc-0448d4acff947ff8	116555269880
rtb-01d726da7324666b8	-	-	-	Yes	vpc-0fb69f39da4322886 hima...	116555269880
himanshu-route-table	rtb-056bd9d6379b3f1e9c	-	-	No	vpc-0fb69f39da4322886 hima...	116555269880
himanshu-private - subnet	rtb-0123f9660dce433d7	<u>subnet-0ab994a35abfd8...</u>	-	No	vpc-0fb69f39da4322886 hima...	116555269880

Routes (1)

Destination	Target	Status	Propagated
11.0.0.0/16	local	Active	No

xxx) CLICK ON ADD ROUTE>SELECT IP ADDRESS :0.0.0.0/0>SELECT NAT GATEWAY>CHOOSE THE NAT GATEWAY THAT YOU HAVE CREATED>CLICK ON SAVE CHANGES.

Destination	Target	Status	Propagated
11.0.0.0/16	local	Active	No
0.0.0.0/0	NAT Gateway		No
	nat-01b96dd79012a2b3a		

Add route

Edit routes

Cancel **Preview** **Save changes**

xxxii) PRIVATE SUBNET IS UPDATED WITH NAT GATEWAY

The screenshot shows the AWS VPC dashboard with the 'Route tables' section selected. A green banner at the top indicates that routes have been updated successfully. The main pane displays the details for the route table 'rtb-0123f9660dce433d7 / himanshu-private - subnet'. It shows the route table ID, owner, and explicit subnet associations. Below this, the 'Routes' tab is active, showing two routes: one to 'nat-01b96dd79012a2b5a' (Status: Active, Propagated: No) and one to 'local' (Status: Active, Propagated: No). The left sidebar contains various navigation links for VPC management.

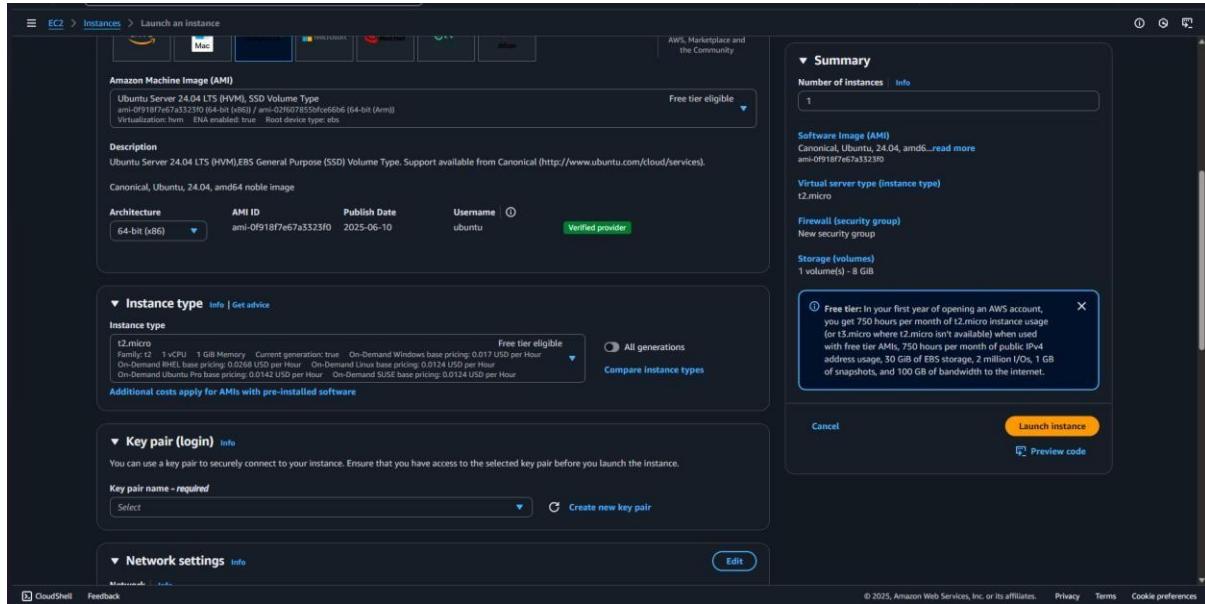
xxxii) WHOLE NETWORK SET UP IS READY, NOW WE HAVE TO CREATE EC2 INSTANCES FOR BOTH PUBLIC AND PRIVATE SUBNET. SEARCH FOR EC2>CLICK ON EC2

The screenshot shows the AWS VPC dashboard with the 'EC2' search term in the search bar. The main pane displays the 'Services' section, specifically the 'EC2' card, which describes it as 'Virtual Servers in the Cloud'. Below this, there are sections for 'Features' (Dashboard, EC2 Instances, AMIs), 'Resources' (Introducing resource search), and 'Documentation'. The left sidebar contains various navigation links for EC2 management.

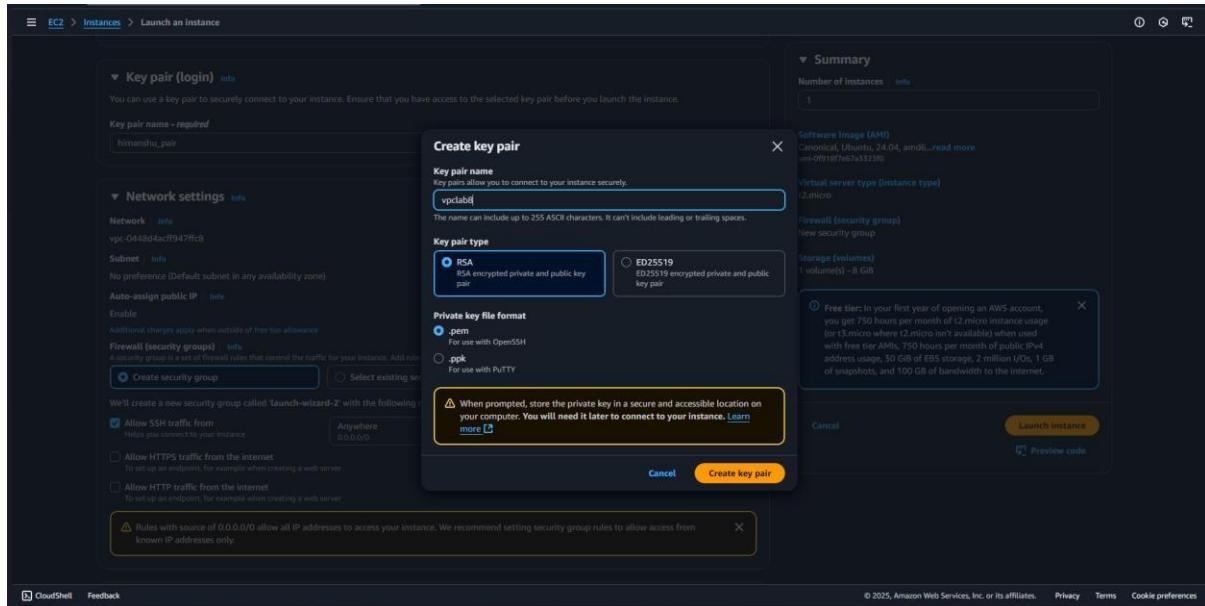
xxxiii) CLICK ON LAUNCH INSTANCE

xxxiv) GIVE A SUITABLE INSTANCE NAME>CHOOSE OS:UBUNTU

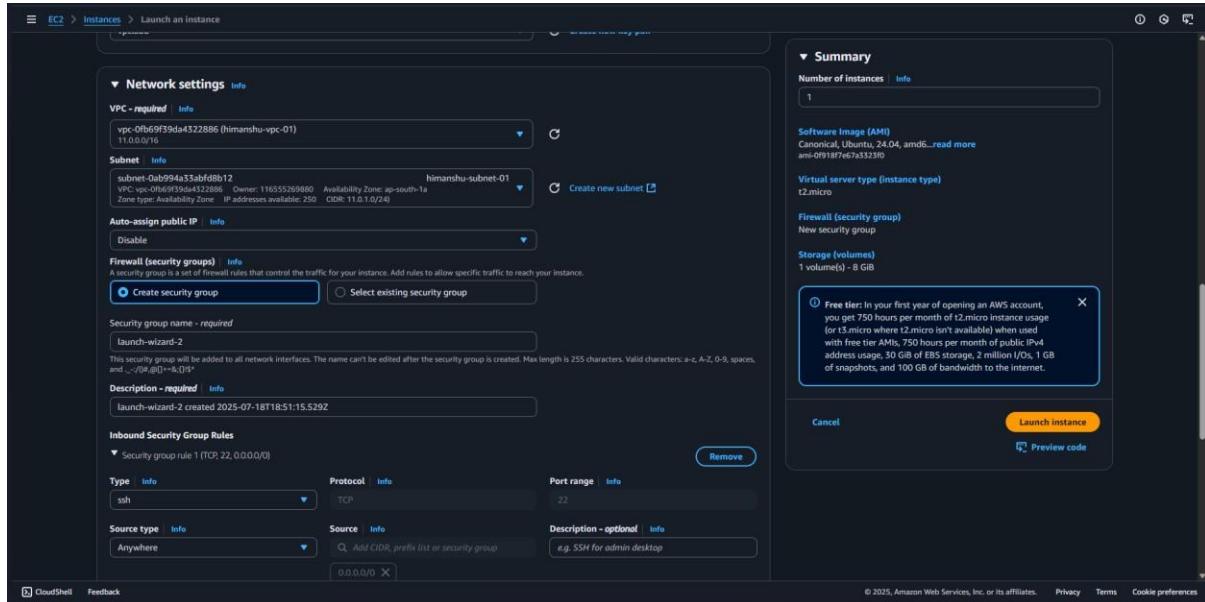
xxxv) CHOOSE THE DEFAULT ARCHITECTURE> FREE TIER INSTANCE TYPE



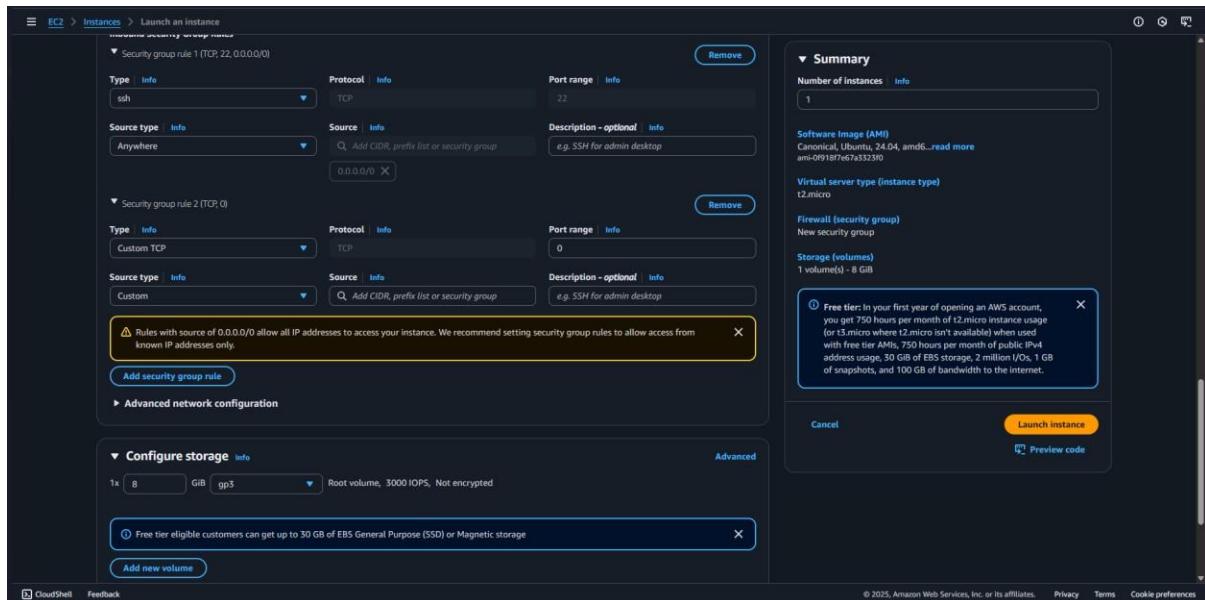
xxxvi) CREATE KEY PAIR



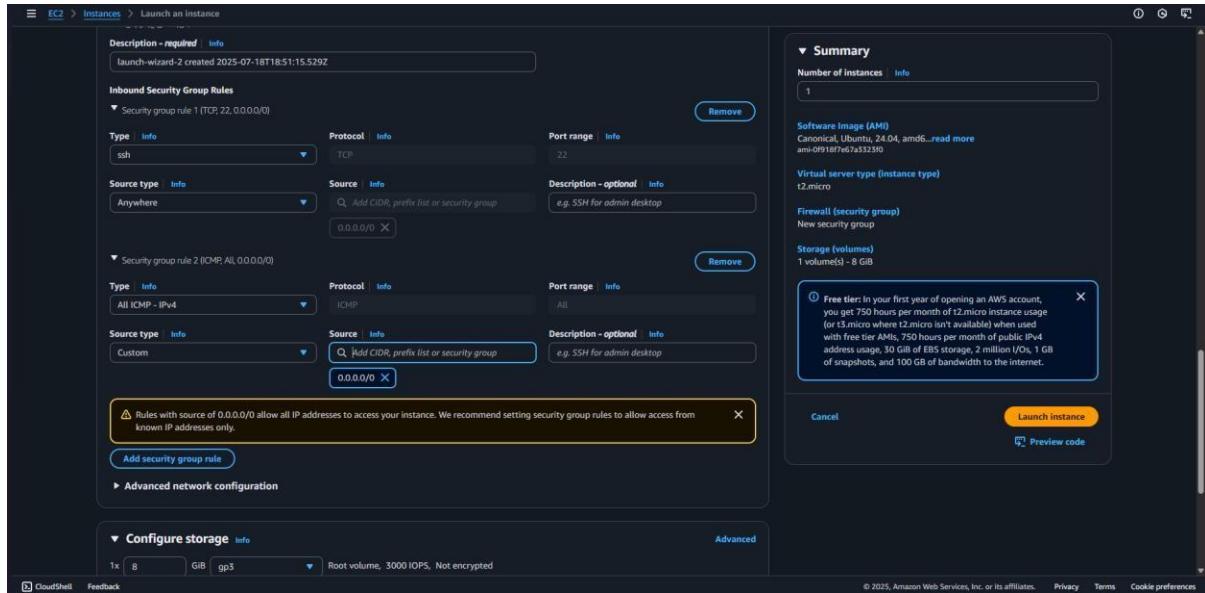
xxxvii) EDIT THE NETWORK SETTING>CHOOSE THE VPC CREATED EARLIER>SELECT THE PUBLIC SUBNET> ENABLE THE AUTO-ASSIGN PUBLIC IP>CHOOSE CREATE SECURITY GROUP



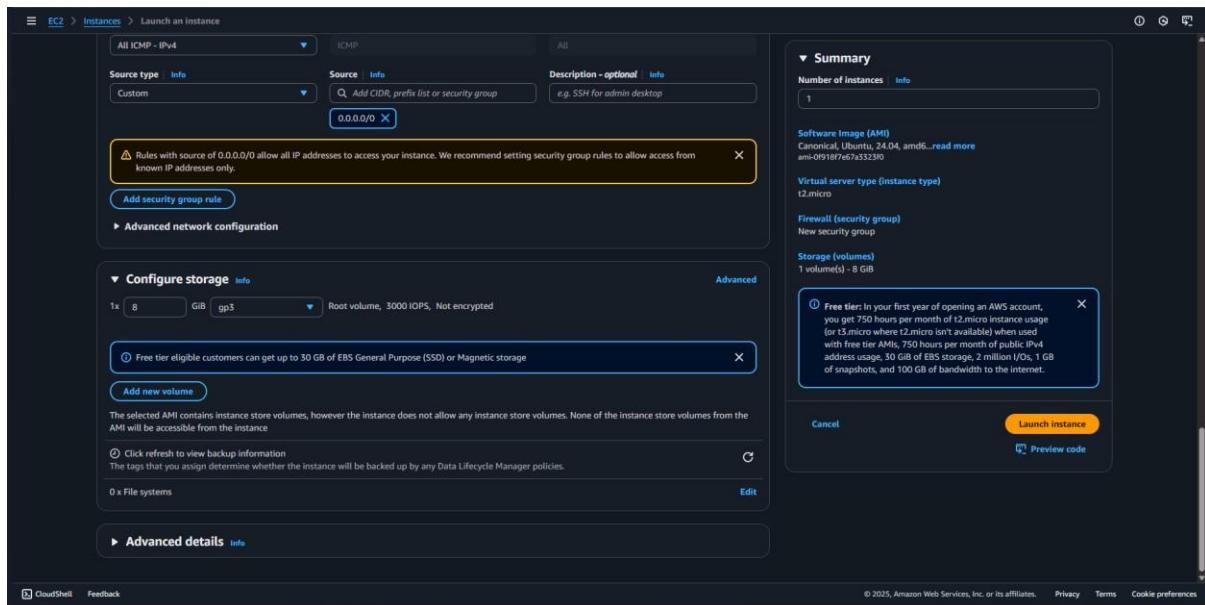
xxxviii) SECURITY GROUP RULE-1 IS DEFAULT> CLICK ON ADD SECURITY GROUP RULE



xxxix) CHOOSE ALL ICMP-IPV4> SOURCE:0.0.0.0/0



xl) CHOOSE DEFAULT CONFIGURE STORAGE: 8GB>CLICK ON LAUNCH INSTANCE



xli) PUBLIC INSTANCE CREATED

The screenshot shows the AWS EC2 Instances page. The left sidebar is collapsed. The main area displays a table titled "Instances (2) Info". The table has columns for Name, Instance ID, Instance state, Instance type, Status check, Alarm status, Availability Zone, Public IPv4 DNS, Public IPv4 IP, and Elastic IP. Two instances are listed:

Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone	Public IPv4 DNS	Public IPv4 IP	Elastic IP
Himanshu_22...	i-0db48b7c3d0a42946	Running	t2.micro	2/2 checks passed	View alarms +	ap-south-1b	ec2-3-111-58-139.ap-s...	3.111.58.139	-
vpc himanshu...	i-02cdc87e7b6bfa704	Running	t2.micro	Initializing	View alarms +	ap-south-1a	-	-	-

Below the table, a message says "Select an instance". The bottom right corner of the page includes copyright information: "© 2025, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences".

xlii) CREATE EC2 INSTANCE FOR PRIVATE SUBNET WITH THE SAME STEPS

This screenshot is identical to the one above, showing the AWS EC2 Instances page with two running t2.micro instances. The layout, table structure, and instance details are the same.

xliii) PRIVATE EC2 INSTANCE IS CREATED

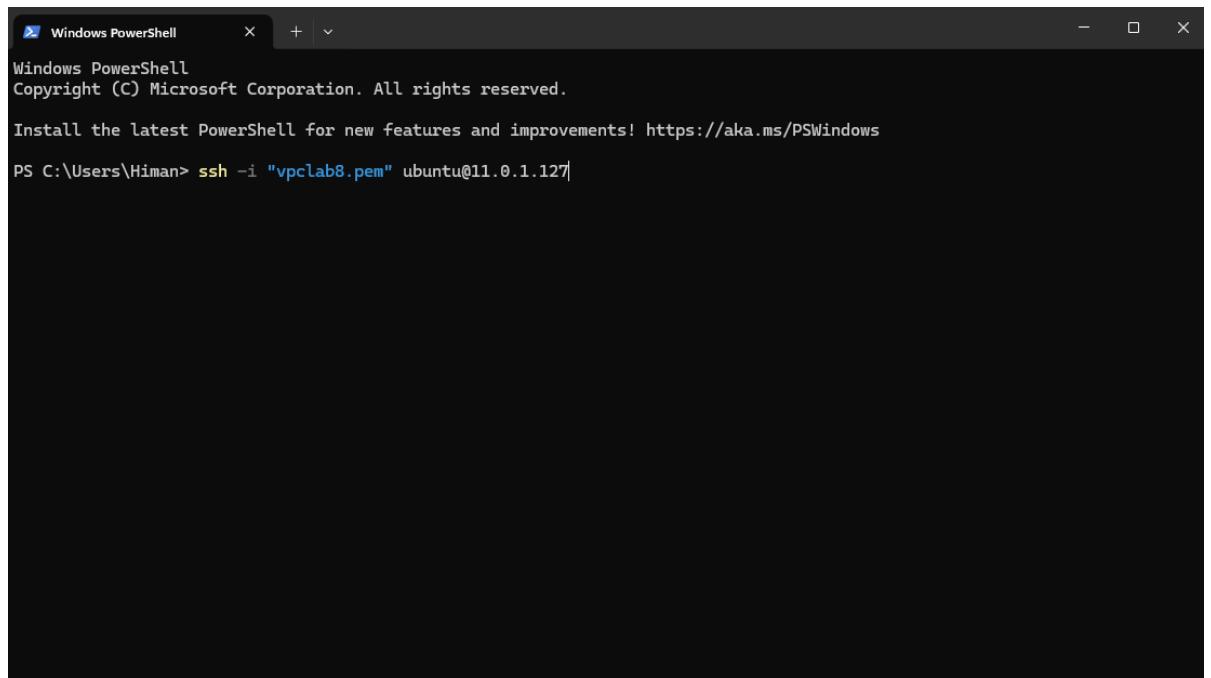
xliv) NOW CONNECT THE PUBLIC EC2 INSTANCE.CLICK ON THE PUBLIC INSTANCE> CLICK ON CONNECT

The screenshot shows the AWS EC2 Instances page. On the left, there's a sidebar with various navigation options like Dashboard, EC2 Global View, Events, Instances, Images, Elastic Block Store, Network & Security, Load Balancing, and more. The main area displays two instances: 'Himanshu_22...' and 'vpchimanshu...'. The 'vpchimanshu...' instance is selected. The center pane shows detailed information for this instance, including its ID, state, network settings, and VPC details. The right pane provides summary information for the selected instance.

xlv) CLICK ON SSH CLIENT> COPY THE EXAMPLE AND PASTE IN TERMINAL TO CONNECT

The screenshot shows the 'Connect' page for the instance i-02cdc87e7b6bfa704. The 'SSH client' tab is selected. It provides instructions for connecting via SSH, including steps to open an SSH client, locate the private key file (vpclab8.pem), run chmod 400 on it, and connect to the instance's private IP (11.0.1.127). An example command is shown: ssh -i <vpclab8.pem> ubuntu@11.0.1.127. A note at the bottom states: 'Note: In most cases, the guessed username is correct. However, read your AMI usage instructions to check if the AMI owner has changed the default AMI username.'

- xlvi) OPEN THE TERMINAL IN YOUR LAPTOP AND TYPE THE FOLLOWING COMMAND> NOW PASTE THE COMMAND HERE FROM THE SSH CLIENT

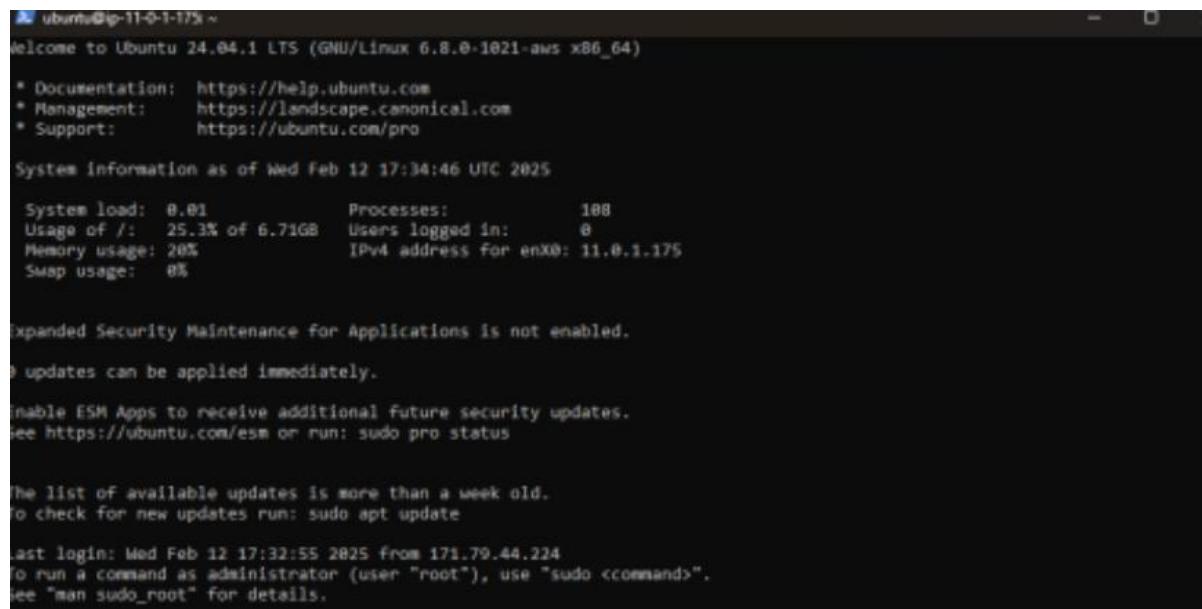


```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Install the latest PowerShell for new features and improvements! https://aka.ms/PSWindows

PS C:\Users\Himan> ssh -i "vpclab8.pem" ubuntu@11.0.1.127
```

- xlvii) PUBLIC EC2 INSTANCE IS CONNECTED



```
ubuntu@ip-11-0-1-17: ~
Welcome to Ubuntu 24.04.1 LTS (GNU/Linux 6.8.0-1021-aws x86_64)

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

System information as of Wed Feb 12 17:34:46 UTC 2025

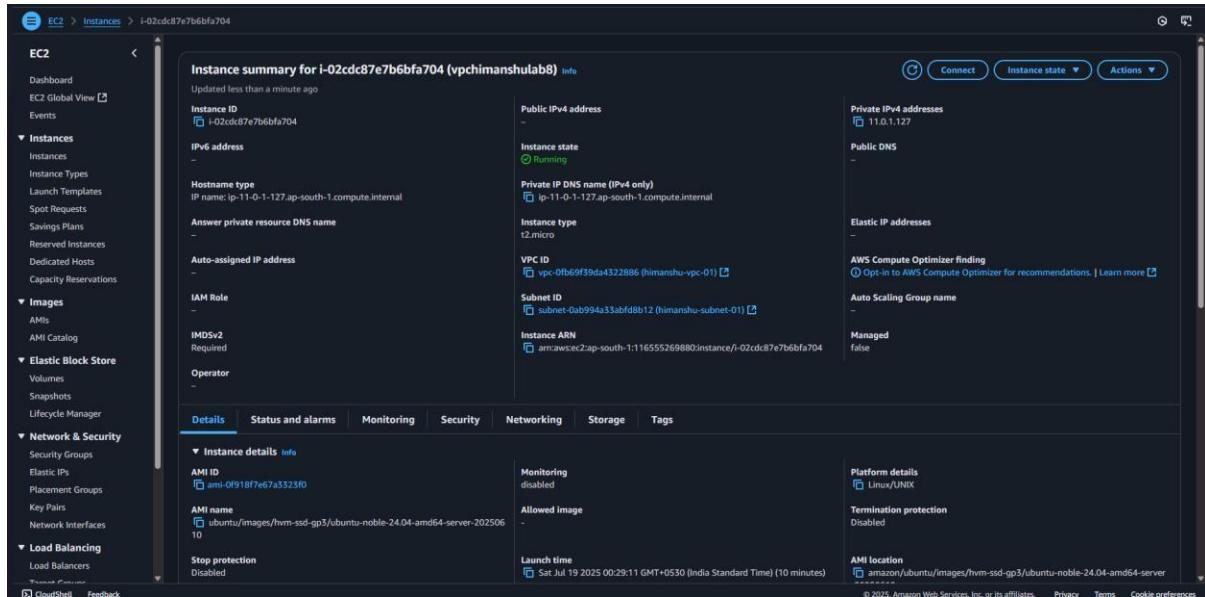
System load: 0.01      Processes:          188
Usage of /: 25.3% of 6.71GB  Users logged in:   8
Memory usage: 28%          IPv4 address for enx0: 11.0.1.125
Swap usage:  0%
```

Expanded Security Maintenance for Applications is not enabled.
9 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

```
Last login: Wed Feb 12 17:32:55 2025 from 171.79.44.224
To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.
```

xlviii) NOW PING THE PUBLIC EC2 INSTANCE WITH THE HELP OF YOUR LOCAL TERMINAL. GO TO INSTANCE AND COPY ITS IP ADDRESS AND TYPE THE FOLLOWING COMMAND. (IT MEANS FROM OUTSIDE AWS, WE ARE ABLE TO CONNECT TO THE PUBLIC EC2 INSTANCE)



xlix) NOW NEXT FROM PUBLIC EC2 INSTANCE TERMINAL, TYPE THE FOLLOWING COMMAND TO ACCESS RESOURCE FROM OUTSIDE THE AWS

```
ubuntu@ip-11-0-1-175:~$ curl ipinfo.io
{
  "ip": "13.235.241.171",
  "hostname": "ec2-13-235-241-171.ap-south-1.compute.amazonaws.com",
  "city": "Mumbai",
  "region": "Maharashtra",
  "country": "IN",
  "loc": "19.0728,72.8826",
  "org": "AS16509 Amazon.com, Inc.",
  "postal": "400017",
  "timezone": "Asia/Kolkata",
  "readme": "https://ipinfo.io/missingauth"
}ubuntu@ip-11-0-1-175:~$
```

- l) PING PRIVATE EC2 INSTANCE FROM THE LOCAL TERMINAL. COPY THE PRIVATE IP ADDRESS OF THE INSTANCE AND TYPE (PING 11.0.2.160) IN THE LOCAL TERMINAL.

```
buntu@ip-11-0-1-175:~$ curl ipinfo.io
{
  "ip": "13.235.241.171",
  "hostname": "ec2-13-235-241-171.ap-south-1.compute.amazonaws.com",
  "city": "Mumbai",
  "region": "Maharashtra",
  "country": "IN",
  "loc": "19.0728,72.8826",
  "org": "AS16589 Amazon.com, Inc.",
  "postal": "400017",
  "timezone": "Asia/Kolkata",
  "readme": "https://ipinfo.io/missingauth"
}
ubuntu@ip-11-0-1-175:~$ ping 11.0.2.160
PING 11.0.2.160 (11.0.2.160) 56(84) bytes of data.
4 bytes from 11.0.2.160: icmp_seq=1 ttl=64 time=1.85 ms
4 bytes from 11.0.2.160: icmp_seq=2 ttl=64 time=0.955 ms
4 bytes from 11.0.2.160: icmp_seq=3 ttl=64 time=0.987 ms
4 bytes from 11.0.2.160: icmp_seq=4 ttl=64 time=1.11 ms
4 bytes from 11.0.2.160: icmp_seq=5 ttl=64 time=1.11 ms
4 bytes from 11.0.2.160: icmp_seq=6 ttl=64 time=0.840 ms
4 bytes from 11.0.2.160: icmp_seq=7 ttl=64 time=0.987 ms
4 bytes from 11.0.2.160: icmp_seq=8 ttl=64 time=1.02 ms
4 bytes from 11.0.2.160: icmp_seq=9 ttl=64 time=1.20 ms
4 bytes from 11.0.2.160: icmp_seq=10 ttl=64 time=1.09 ms
4 bytes from 11.0.2.160: icmp_seq=11 ttl=64 time=0.748 ms
4 bytes from 11.0.2.160: icmp_seq=12 ttl=64 time=1.07 ms
4 bytes from 11.0.2.160: icmp_seq=13 ttl=64 time=1.23 ms
4 bytes from 11.0.2.160: icmp_seq=14 ttl=64 time=0.984 ms
4 bytes from 11.0.2.160: icmp_seq=15 ttl=64 time=0.927 ms
```

Date: 08-08-2025	Title
Exp. No: 09	HOW TO IMPLEMENT LOAD BALANCER, TARGET GROUP & AUTO-SCALING GROUP WITH EC2 INSTANCE

AIM OF THE EXPERIMENT: HOW TO IMPLEMENT LOAD BALANCER, TARGET GROUP & AUTO- SCALING GROUP WITH EC2 INSTANCE

PROCEDURE:

STEP1: CREATE A VPC>WRITE VPC NAME>IPv4 CIDR:12.0.0.0/16>CREATE VPC

The screenshot shows the 'Create VPC' wizard in the AWS Management Console. The first step, 'VPC settings', is displayed. Key configuration parameters shown include:

- Resources to create:** VPC only (selected).
- Name tag - optional:** divyanshi-aws-munsifa.
- IPv4 CIDR block:** IPv4 CIDR manual input (selected). Value: 12.0.0.0/16.
- IPv6 CIDR block:** No IPv6 CIDR block selected.
- Tenancy:** Default.

The screenshot shows the 'Details' page for the newly created VPC. The VPC ID is vpc-07baef0b41a7ac5a3. Other details include:

Setting	Value
VPC ID	vpc-07baef0b41a7ac5a3
State	Available
DNS resolution	Enabled
Main network ACL	acl-093a35b77346c5631
IPv6 CIDR (Network border group)	-
Tenancy	default
Default VPC	No
Network Address Usage metrics	Disabled
Block Public Access	Off
DHCP option set	dopt-095ceab98e60ffd2d
IPv4 CIDR	12.0.0.0/16
Route 53 Resolver DNS Firewall rule groups	-
DNS hostnames	Disabled
Main route table	rtb-0700dc1551f1c9495
IPv6 pool	-
Owner ID	138264596579

STEP2: NEXT CLICK ON INTERNET GATEWAY> CREATE INTERNET GATEWAY>TYPE NAME> CLICK ON CREATE

STEP3: NEXT CLICK ON ATTACH TO VPC> CHOOSE THE INTERNET GATEWAY>CLICK ON

The screenshot shows the 'Create internet gateway' wizard. In the 'Internet gateway settings' section, a 'Name tag' is added with the value 'himanshu_22BCE10118'. In the 'Tags - optional' section, a single tag 'Name' is added with the value 'himanshu_22BCE10118'. The 'Create internet gateway' button is highlighted in orange at the bottom right.

The screenshot shows the 'Attach to VPC' wizard. It displays a success message: 'The following internet gateway was created: igw-00b3b89352fe4788f - divyanshi-munsifa-22bce10700. You can now attach to a VPC to enable the VPC to communicate with the internet.' Below this, it lists an available VPC with ID 'vpc-07baef0b41a7ac5a3'. The 'Attach internet gateway' button is highlighted in orange at the bottom right.

STEP4: CREATE SUBNET> SELECT THE VPC>TYPE THE NAME OF SUBNET_1>AVAILABILITY ZONE:ap south 1a>IPv4 CIDR:12.0.1.0/24

STEP5: CLICK ON ADD SUBNET>TYPE THE NAME ODF SUBNET_2>AVAILABILITY ZONE:ap-south-1b>IPv4 CIDR:12.0.3.0/24

Subnet settings
Specify the CIDR blocks and Availability Zone for the subnet.

Subnet 1 of 1

Subnet name
Create a tag with a key of 'Name' and a value that you specify.

The name can be up to 256 characters long.

Availability Zone Info
Choose the zone in which your subnet will reside, or let Amazon choose one for you.

IPv4 VPC CIDR block Info
Choose the VPC's IPv4 CIDR block for the subnet. The subnet's IPv4 CIDR must lie within this block.

IPv4 subnet CIDR block
 256 IPs
< > ^ v

Tags - optional

CloudShell Feedback © 2025, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

south 1b>IPv4 CIDR:12.0.3.0/24

Subnet 2 of 2

Subnet name
Create a tag with a key of 'Name' and a value that you specify.

The name can be up to 256 characters long.

Availability Zone Info
Choose the zone in which your subnet will reside, or let Amazon choose one for you.

IPv4 VPC CIDR block Info
Choose the VPC's IPv4 CIDR block for the subnet. The subnet's IPv4 CIDR must lie within this block.

IPv4 subnet CIDR block
 256 IPs
< > ^ v

Tags - optional

Key	Value - optional	Remove
<input type="text" value="Name"/>	<input type="text" value="public-subnet-2"/>	<input type="button" value="Remove"/>

CloudShell Feedback © 2025, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

The screenshot shows the AWS VPC Subnets page. On the left, there's a navigation sidebar with options like VPC dashboard, EC2 Global View, Filter by VPC, Virtual private cloud (Your VPCs, Subnets, Route tables, Internet gateways, Egress-only internet gateways, DHCP option sets, Elastic IPs, Managed prefix lists, NAT gateways, Peering connections), Security (Network ACLs, Security groups), and PrivateLink and Lambda. The main area has a green banner at the top stating "You have successfully created 2 subnets: subnet-03964d10f6bfce187, subnet-044b4ee44ed9ef154". Below this is a table titled "Subnets (2) Info" with the following data:

Name	Subnet ID	State	VPC	Block Public...	IPv4 CIDR
public-subnet-1	subnet-03964d10f6bfce187	Available	vpc-07baef0b41a7ac5a3 divya...	Off	12.0.0.0/24
public-subnet-2	subnet-044b4ee44ed9ef154	Available	vpc-07baef0b41a7ac5a3 divya...	Off	12.0.3.0/24

Below the table, there's a section titled "Select a subnet" with a dropdown menu.

STEP6: NOW CREATE ROUTE TABLE: CLICK ON ROUTE TABLES>CREATE ROUTE TABLE>ROUTE TABLE NAME> CHOOSE VPC>CREATE ROUTE TABLE

STEP7: NOW ASSOCIATE ROUTE TABLE WITH THE SUBNETS: CLICK ON SUBNET ASSOCIATIONS>EDIT SUBNET ASSOCIATION

The screenshot shows the AWS VPC Route Tables page. At the top, a green success message states: "Route table rtb-069a02d0fc1de05d0 | divyanshi-munsifa-22bce10700 was created successfully." Below this, the route table ID is displayed as "rtb-069a02d0fc1de05d0 /Himanshu_22bce10118".

The left sidebar includes sections for Virtual private cloud (Your VPCs, Subnets, Route tables, Internet gateways, Egress-only internet gateways, DHCP option sets, Elastic IPs, Managed prefix lists, NAT gateways, Peering connections) and Security (Network ACLs, Security groups).

The main content area has a "Details" section with "Route table ID" (rtb-069a02d0fc1de05d0), "Main" (No), "Owner ID" (vpc-07baef0b41a7ac5a3 | divyanshi-aws-munsifa), and "Explicit subnet associations" and "Edge associations" both listed as "-".

The navigation tabs at the bottom are: Routes, Subnet associations (which is selected), Edge associations, Route propagation, and Tags.

The "Subnet associations" tab displays a table with columns: Name, Subnet ID, IPv4 CIDR, and IPv6 CIDR. A search bar at the top of this table says "Find subnet association". A message below the table states: "No subnet associations" and "You do not have any subnet associations." There is a "Edit subnet associations" button in the top right corner of the table area.

STEP8: SELECT BOTH THE SUBNETS>SAVE ASSOCIATIONS

STEP9: CLICK ON ROUTE>EDIT ROUTE>ADD ROUTE> SELECT THE DATA AS SHOWN>SAVE CHANGES

The screenshot shows the 'Edit subnet associations' page in the AWS VPC console. At the top, the navigation path is VPC > Route tables > rtb-069a02d0fc1de05d0 > Edit subnet associations. The main section is titled 'Edit subnet associations' with the sub-instruction 'Change which subnets are associated with this route table.' Below this is a table titled 'Available subnets (2/2)'.

Name	Subnet ID	IPv4 CIDR	IPv6 CIDR	Route table ID
public-subnet-1	subnet-03964d10f6bfce187	12.0.0.0/24	-	Main (rtb-0700dc1551f1c9495)
public-subnet-2	subnet-044b4ee44ed9ef154	12.0.3.0/24	-	Main (rtb-0700dc1551f1c9495)

Below the table, a section titled 'Selected subnets' lists the subnets currently associated with the route table:

- subnet-03964d10f6bfce187 / public-subnet-1
- subnet-044b4ee44ed9ef154 / public-subnet-2

At the bottom right are 'Cancel' and 'Save associations' buttons. The 'Save associations' button is highlighted with a yellow background.

VPC > Route tables > rtb-069a02d0fc1de05d0 > Edit routes

Edit routes

Destination	Target	Status	Propagated
12.0.0.0/16	local	Active	No
Q 0.0.0.0/0	Internet Gateway	-	No
	Q igw-00b3b89552fe4788f	X	

Add route Remove Cancel Preview Save changes

CloudShell Feedback © 2025, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

STEP10: GO TO EC2 DASHBOARD>CLICK ON TARGET GROUPS

STEP11: CHOOSE INSTANCES

EC2 > Target groups

Elastic Block Store
Volumes
Snapshots
Lifecycle Manager

Network & Security
Security Groups
Elastic IPs
Placement Groups
Key Pairs
Network Interfaces

Load Balancing
Load Balancers
Target Groups
Trust Stores

Auto Scaling
Auto Scaling Groups

Settings

Target groups Info

Actions Create target group

No target groups
You don't have any target groups in ap-south-1

Create target group

0 target groups selected
Select a target group above.

The screenshot shows the 'Specify group details' step of creating a target group. The left sidebar shows 'Step 1 Specify group details' (selected) and 'Step 2 Register targets'. The main area is titled 'Specify group details' with the sub-section 'Basic configuration'. It states: 'Your load balancer routes requests to the targets in a target group and performs health checks on the targets.' Below this is 'Choose a target type' with three options: 'Instances' (selected), 'IP addresses', and 'Lambda function'. The 'Instances' section includes a note: 'Supports load balancing to instances within a specific VPC. Facilitates the use of Amazon EC2 Auto Scaling [?] to manage and scale your EC2 capacity.' The 'IP addresses' section includes a note: 'Supports load balancing to VPC and on-premises resources. Facilitates routing to multiple IP addresses and network interfaces on the same instance. Offers flexibility with microservice based architectures, simplifying inter-application communication. Supports IPv6 targets, enabling end-to-end IPv6 communication, and IPv4-to-IPv6 NAT.' The 'Lambda function' section includes a note: 'Facilitates routing to a single Lambda function. Accessible to Application Load Balancers only.' At the bottom of the page are links for CloudShell, Feedback, Privacy, Terms, and Cookie preferences.

STEP12: WRITE A NAME TO THE TARGET GROUP STEP13: SELECT THE VPC> CLICK ON NEXT

The screenshot shows the 'Create target group' step. The left sidebar shows 'Step 1 Specify group details' (selected) and 'Step 2 Register targets'. The main area has a heading 'Application Load Balancer' (selected). It includes a note: 'Offers the flexibility for a Network Load Balancer to accept and route TCP requests within a specific VPC. Facilitates using static IP addresses and PrivateLink with an Application Load Balancer.' Below this is 'Target group name' with the value 'himanshu_22BC10118'. A note says: 'A maximum of 32 alphanumeric characters including hyphens are allowed, but the name must not begin or end with a hyphen.' Under 'Protocol' (selected), it says 'HTTP'. Under 'Port', the value '80' is selected. A note says: 'Port number where targets receive traffic. Can be overridden for individual targets during registration.' Under 'IP address type', 'IPv4' is selected. A note says: 'Each instance has a default network interface (eth0) that is assigned the primary private IPv4 address. The instance's primary private IPv4 address is the one that will be applied to the target.' Under 'IPv6', a note says: 'Each instance you register must have an assigned primary IPv6 address. This is configured on the instance's default network interface (eth0). Learn more [?]' Under 'VPC', it says: 'Select the VPC with the instances that you want to include in the target group. Only VPCs that support the IP address type selected above are available in this list.' At the bottom of the page are links for CloudShell, Feedback, Privacy, Terms, and Cookie preferences, along with system status icons like weather (24°C Haze), search, and date/time (22:11 30-07-2025).

VPC
Select the VPC with the instances that you want to include in the target group. Only VPCs that support the IP address type selected above are available in this list.
vpc-07baef0b41a7ac5a3 (divyanshi-aws-munsifa)
12.0.0.0/16 Create VPC

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

Health checks
The associated load balancer periodically sends requests, per the settings below, to the registered targets to test their status.

Health check protocol
HTTP

Health check path
Use the default path of "/" to perform health checks on the root, or specify a custom path if preferred.
/

CloudShell Feedback © 2025, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

STEP14: CLICK ON CREATE TARGET GROUP

STEP15: CLICK ON APPLICATION LOAD BALANCER

Health check protocol
HTTP

Health check path
Use the default path of "/" to perform health checks on the root, or specify a custom path if preferred.
/

Up to 1024 characters allowed.

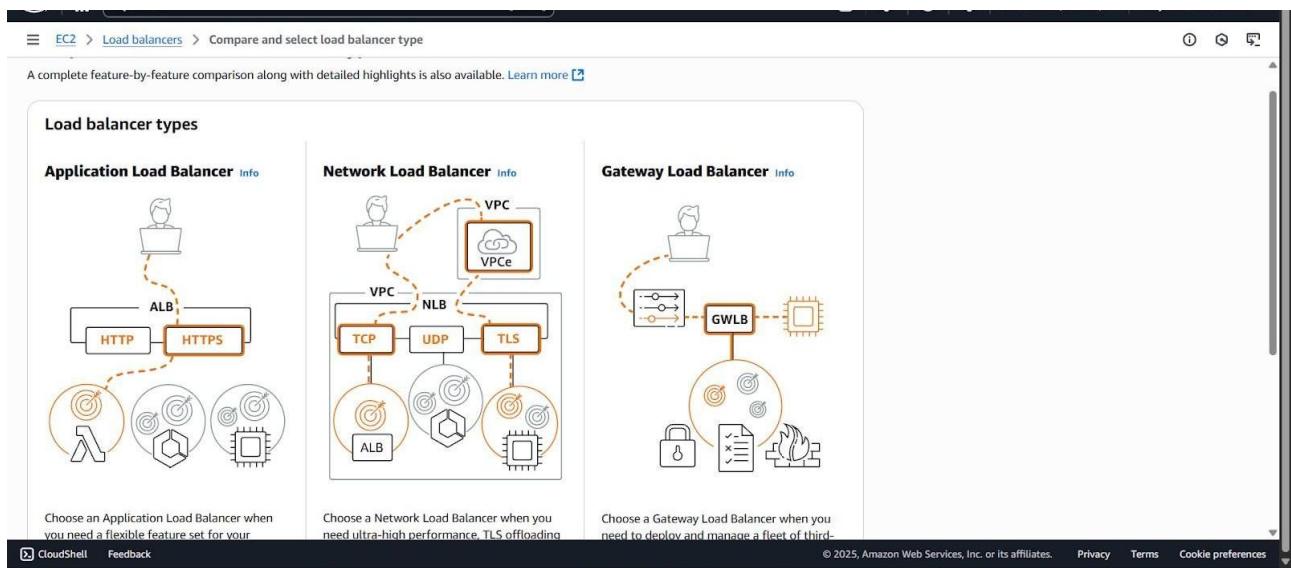
► Advanced health check settings

Attributes
Certain default attributes will be applied to your target group. You can view and edit them after creating the target group.

► Tags - optional
Consider adding tags to your target group. Tags enable you to categorize your AWS resources so you can more easily manage them.

Cancel Next

CloudShell Feedback © 2025, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences



STEP16: WRITE THE NAME OF THE LOAD BALANCER

The screenshot shows the "Create Application Load Balancer" configuration page. It includes sections for:

- How Application Load Balancers work**
- Basic configuration**:
 - Load balancer name**: A text input field for the load balancer name.
 - Scheme**: A dropdown menu showing "Internet-facing" (selected) and "Internal".
 - Load balancer IP address type**: A dropdown menu showing "IPv4" (selected).

STEP17: SELECT THE VPC CREATED

Network mapping [Info](#)

The load balancer routes traffic to targets in the selected subnets, and in accordance with your IP address settings.

VPC [Info](#)

The load balancer will exist and scale within the selected VPC. The selected VPC is also where the load balancer targets must be hosted unless routing to Lambda or on-premises targets, or if using VPC peering. To confirm the VPC for your targets, view [target groups](#).

vpc-07baef0b41a7ac5a3 (12.0.0.0/16) [Create VPC](#)

IP pools - new [Info](#)

You can optionally choose to configure an IPAM pool as the preferred source for your load balancers IP addresses. Create or view [Pools](#) in the [Amazon VPC IP Address Manager console](#).

Use IPAM pool for public IPv4 addresses

The IPAM pool you choose will be the preferred source of public IPv4 addresses. If the pool is depleted IPv4 addresses will be assigned by AWS.

Availability Zones and subnets [Info](#)

Select at least two Availability Zones and a subnet for each zone. A load balancer node will be placed in each selected zone and will automatically scale in response to traffic. The load balancer routes traffic to targets in the selected Availability Zones only.

ap-south-1a (aps1-az1)

ap-south-1b (aps1-az3)

Security groups [Info](#)

A security group is a set of firewall rules that control the traffic to your load balancer. Select an existing security group, or you can [create a new security group](#).

STEP18: SELECT BOTH THE ZONE(SUBNETS)

IP pools - new [Info](#)

You can optionally choose to configure an IPAM pool as the preferred source for your load balancers IP addresses. Create or view [Pools](#) in the [Amazon VPC IP Address Manager console](#).

Use IPAM pool for public IPv4 addresses

The IPAM pool you choose will be the preferred source of public IPv4 addresses. If the pool is depleted IPv4 addresses will be assigned by AWS.

Availability Zones and subnets [Info](#)

Select at least two Availability Zones and a subnet for each zone. A load balancer node will be placed in each selected zone and will automatically scale in response to traffic. The load balancer routes traffic to targets in the selected Availability Zones only.

ap-south-1a (aps1-az1)

Subnet
Only CIDR blocks corresponding to the load balancer IP address type are used. At least 8 available IP addresses are required for your load balancer to scale efficiently.

subnet-03964d10f6bfc187
IPv4 subnet CIDR: 12.0.0.0/24 [public-subnet-1](#)

ap-south-1b (aps1-az3)

Subnet
Only CIDR blocks corresponding to the load balancer IP address type are used. At least 8 available IP addresses are required for your load balancer to scale efficiently.

subnet-044b4ee44ed9ef15a
IPv4 subnet CIDR: 12.0.3.0/24 [public-subnet-2](#)

Security groups [Info](#)

STEP19: CLICK ON CREATE A NEW SECURITY GROUP> TYPE THE NAME AND DESCRIPTION OF THE SECURITY GROUP>SELECT THE VPC

Security groups [Info](#)
A security group is a set of firewall rules that control the traffic to your load balancer. Select an existing security group, or you can [create a new security group](#).

Security groups

Select up to 5 security groups

default sg-0e87b5bff7c1abd15 VPC: vpc-07baef0b41a7ac5a3

Listeners and routing [Info](#)
A listener is a process that checks for connection requests using the port and protocol you configure. The rules that you define for a listener determine how the load balancer routes requests to its registered targets.

Listener HTTP:80

Protocol	Port	Default action
HTTP	80	Forward to: Select a target group Create target group

Listener tags - optional
Consider adding tags to your listener. Tags enable you to categorize your AWS resources so you can more easily manage them.

Add listener tags

CloudShell Feedback 24°C Haze Search © 2025, Amazon Web Services, Inc. or its affiliates Privacy Terms Cookie preferences ENG IN 22:14 30-07-2025

Create application load balancer EC2 | ap-south-1

STEP20: SET THE IN BOUND RULE: CLICK ON ADD RULES> SET HTTP>SOURCE:0.0.0.0/0>
CLICK ON CREATE SECURITY GROUP.

The screenshot shows the AWS CloudFront Rule Editor interface. It includes sections for Inbound rules and Outbound rules, each with dropdown menus for Type, Protocol, Port range, and Source/Destination, along with a search bar and a Delete button. An Add rule button is also present. Below these sections is a Tags - optional input field.

STEP21: NOW SELECT THE SECURITY GROUP THAT YOU HAVE CREATED

STEP22: LISTENERS & ROUTING SECTION: SELECT TARGET GROUP THAT YOU HAVE
CREATED

Listeners and routing Info

A listener is a process that checks for connection requests using the port and protocol you configure. The rules that you define for a listener determine how the load balancer routes requests to its registered targets.

▼ Listener **HTTP:80**

Protocol	Port
HTTP	80 1-65535

Default action Info

Forward to **Himanshu_22bce101180** Target type: Instance, IPv4

HTTP ▼

[Create target group](#)

Listener tags - optional
Consider adding tags to your listener. Tags enable you to categorize your AWS resources so you can more easily manage them.

[Add listener tag](#) You can add up to 50 more tags.

[Add listener](#) You can add up to 49 more listeners.

CloudShell Feedback © 2025, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

STEP23: VERIFY THE DETAILS IN THE SUMMARY>CLICK ON CREATE LOAD BALANCER

STEP24: LOAD BALANCER IS CREATED

Review
Review the load balancer configurations and make changes if needed. After you finish reviewing the configurations, choose **Create load balancer**.

Summary
Review and confirm your configurations. [Estimate cost](#)

Basic configuration Edit Name: divyanshi-munsifa-22bce10700 Scheme: Internet-facing IP address type: IPv4	Network mapping Edit VPC: vpc-07baef0b41a7ac5a3 Public IPv4 IPAM pool: - Availability Zones and subnets: <ul style="list-style-type: none">ap-south-1a subnet-03964d10f6bfce187 public-subnet-1ap-south-1b subnet-044b4ee44ed9ef154 public-subnet-2	Security groups Edit divyanshi-munsifa-22bce10700 sg-0773793aff10472b3	Listeners and routing Edit HTTP:80 Target group: divyanshi-munsifa-22bce10700
Service integrations Edit Amazon CloudFront + AWS Web Application Firewall (WAF): - AWS WAF: - AWS Global Accelerator: -	Tags Edit -		
Attributes			

CloudShell Feedback © 2025, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

Himanshu_22bce10118

Details

Load balancer type	Status	VPC	Load balancer IP address type
Application	Provisioning	vpc-07baef0b41a7ac5a3	IPv4
Scheme	Hosted zone	Availability Zones	Date created
Internet-facing	ZP97RAFLXTNZK	subnet-03964d10f6bfce187 ap-south-1a (aps1-az1) subnet-044bdee44ed9ef154 ap-south-1b (aps1-az3)	July 30, 2025, 22:20 (UTC+05:30)
Load balancer ARN	DNS name		
arn:aws:elasticloadbalancing:ap-south-1:138264596579:loadbalancer/app/divyanshi-munsifa-22bce10700/b9235e0faaafb5c2	Info divyanshi-munsifa-22bce10700-248463820.ap-south-1.elb.amazonaws.com (A Record)		

3 | <https://ap-south-1.console.aws.amazon.com/home?region=ap-south-1&tab=SubnetDetails#/subnets/03964d10f6bfce187> © 2025, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

STEP25: CLICK ON AUTO-SCALING GROUP> CREATE AUTO-SCALING GROUP

Amazon EC2 Auto Scaling
helps maintain the availability of your applications

Auto Scaling groups are collections of Amazon EC2 instances that enable automatic scaling and fleet management features. These features help you maintain the health and availability of your applications.

Create Auto Scaling group

Get started with EC2 Auto Scaling by creating an Auto Scaling group.

Create Auto Scaling group

How it works

Pricing

Amazon EC2 Auto Scaling features have no additional fees beyond the service fees for Amazon EC2, CloudWatch (for scaling policies), and the other AWS resources that you use. Visit the pricing page of each service to learn more.

Getting started

STEP26: GIVE A NAME TO AUTO-SCALING >CLICK ON CREATE A LAUNCH TEMPLATE

EC2 > Auto Scaling groups > Create Auto Scaling group

Step 1

Choose launch template

Step 2

Choose instance launch options

Step 3 - optional

Integrate with other services

Step 4 - optional

Configure group size and scaling

Step 5 - optional

Add notifications

Step 6 - optional

Add tags

Step 7

Review

Choose launch template Info

Specify a launch template that contains settings common to all EC2 instances that are launched by this Auto Scaling group.

Name

Auto Scaling group name
Enter a name to identify the group.
himanshu_22fce10118

Must be unique to this account in the current Region and no more than 255 characters.

Launch template Info

Choose a launch template that contains the instance-level settings, such as the Amazon Machine Image (AMI), instance type, key pair, and security groups.

Select a launch template

Create a launch template (P)

For accounts created after May 31, 2023, the EC2 console only supports creating Auto Scaling groups with launch templates. Creating Auto Scaling groups with launch configurations is not recommended but still available via the CLI and API until December 31, 2023.

CloudShell Feedback © 2025, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

STEP27: GIVE A TEMPLATE NAME

STEP28: SELECT UBUNTU

EC2 > Launch templates > Create launch template

Create launch template

Creating a launch template allows you to create a saved instance configuration that can be reused, shared and launched at a later time. Templates can have multiple versions.

Launch template name and description

Launch template name - **required**
divyanshi-loadbalance

Must be unique to this account. Max 128 chars. No spaces or special characters like '/\;`~`^`@`.

Template version description
A prod webserver for MyApp

Max 255 chars

Auto Scaling guidance (P)

Select this if you intend to use this template with EC2 Auto Scaling

Provide guidance to help me set up a template that I can use with EC2 Auto Scaling

► Template tags
► Source template

Launch template contents

Specify the details of your launch template below. Leaving a field blank will result in the field not being included in the launch template.

CloudShell Feedback © 2025, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

Amazon Machine Image (AMI)

Ubuntu Server 24.04 LTS (HVM), SSD Volume Type
Free tier eligible

Description
Ubuntu Server 24.04 LTS (HVM), EBS General Purpose (SSD) Volume Type. Support available from Canonical (<http://www.ubuntu.com/cloud/services>).

Architecture: 64-bit (x86)
AMI ID: ami-0f918f7e67a3323f0
Publish Date: 2025-06-10
Username: ubuntu (Verified provider)

Summary

Software Image (AMI)
Canonical, Ubuntu, 24.04, amd6... [read more](#)
ami-0f918f7e67a3323f0

Virtual server type (instance type)

Firewall (security group)

Storage (volumes)
1 volume(s) - 8 GiB

Create launch template

STEP29: SELECT INSTANCE TYPE

Canonical, Ubuntu, 24.04, amd64 noble image

Architecture: 64-bit (x86)
AMI ID: ami-0f918f7e67a3323f0
Publish Date: 2025-06-10
Username: ubuntu (Verified provider)

Instance type [Info](#) | [Get advice](#)

Advanced

Instance type: Don't include in launch template

All generations

[Compare instance types](#)

Key pair (login) [Info](#)

You can use a key pair to securely connect to your instance. Ensure that you have access to the selected key pair before you launch the instance.

Key pair name: Don't include in launch template

[Create new key pair](#)

Network settings [Info](#)

Summary

Software Image (AMI)
Canonical, Ubuntu, 24.04, amd6... [read more](#)
ami-0f918f7e67a3323f0

Virtual server type (instance type)

Firewall (security group)

Storage (volumes)
1 volume(s) - 8 GiB

Create launch template

STEP30: CREATE A KEY PAIR

STEP31: NEXT WE HAVE TO CREATE A SECURITY GROUP TO BE ADDED IN THE LAUNCH TEMPLATE

- a. SEARCH VPC>OPEN VPC IN A NEW TAB>CLICK ON SECURITY GROUP>CREATE SECURITY GROUP
- b. WRITE A NAME & DESCRIPTION TO THE SECURITY GROUP> CHOOSE THE VPC THAT YOU HAVE CREATED

The screenshot shows the 'Create security group' page in the AWS Management Console. The URL in the address bar is 'VPC > Security Groups > Create security group'. The main title is 'Create security group Info'. Below it, a sub-instruction says: '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.' The 'Basic details' section contains two fields: 'Security group name Info' with the value 'himanshu_@2bcc10118' and 'Description Info' with the value 'Allows SSH access to developers'. Under 'VPC Info', the selected VPC is 'vpc-0448d4acff947ffc8'. The 'Inbound rules' section is empty, showing the message 'This security group has no inbound rules.' with a 'Add rule' button. The 'Outbound rules' section shows a single rule: 'Type' set to 'All traffic', 'Protocol' set to 'All', 'Port range' set to 'All', 'Destination' set to 'Custom' with '0.0.0.0/0' entered in the search field, and 'Description - optional' left empty. A note at the bottom of this section says: '⚠ Rules with destination of 0.0.0.0/0 or ::/0 allow your instances to send traffic to any IPv4 or IPv6 address. We recommend setting security group rules to be more restrictive and to only allow traffic to specific known IP addresses.' The 'Tags - optional' section is also empty. At the bottom of the page, there are links for CloudShell, Feedback, © 2025, Amazon Web Services, Inc. or its affiliates., Privacy, Terms, and Cookie preferences.

STEP32: SET IN BOUND RULE:

- a. CLICK ON ADD RULE> SELECT HTTP & SOURCE: ANYWHERE (0.0.0.0/0).
- b. CLICK ON ADD RULE> SELECT SSH & SOURCE: ANYWHERE (0.0.0.0/0). THEN CLICK ON ADD SECURITY GROUP

Inbound rules

Type	Protocol	Port range	Source	Description - optional
HTTP	TCP	80	Custom	(empty)
SSH	TCP	22	Custom	(empty)

Add rule

Outbound rules

Type	Protocol	Port range	Destination	Description - optional
All traffic	All	All	Custom	(empty)

Tags - optional
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 new tag

© 2025, Amazon Web Services, Inc. or its affiliates. Privacy Terms

STEP33: NOW SELECT THE SECURITY GROUP THAT YOU HAVE CREATED IN THE LAUNCH TEMPLATE> AUTO ASSIGN PUBLIC IP: ENABLE> KEEP DEFAULT EBS VOLUME>CLICK ON CREATE LAUNCH TEMPLATE

Select security groups

launch-template-divyanshi-22bce10700 sg-059d05037ac5a18cd X

VPC: vpc-07baef0d41a7ac5a5

Security groups that you add or remove here will be added to or removed from all your network interfaces.

Advanced network configuration

Network interface 1

Network interface

Subnet: Don't include in launch template
Not applicable for EC2 Auto Scaling

Primary IP: Not applicable for EC2 Auto Scaling

IPv4 Prefixes: Don't include in launch template

Security groups: Select security groups
Show all selected (1)

Auto-assign public IP: Enable (selected)

Secondary IP: Not applicable for EC2 Auto Scaling

IPv6 Prefixes: Not applicable for EC2 Auto Scaling

Assign Primary IPv6 IP: Don't include in launch template

Virtual server type (instance type)

Summary

Software Image (AMI)
Canonical, Ubuntu, 24.04, amd6...read more
ami-0f918f7e67a5323f0

Firewall (security group)
launch-template-divyanshi-22bce10700

Storage (volumes)
1 volume(s) - 8 GiB

Create launch template

© 2025, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

STEP34: NOW SELECT THE LAUNCH TEMPLATE FOR AUTO-SCALING GROUP> CLICK ON NEXT

STEP35: SELECT VPC THAT YOU HAVE CREATED>SELECT BOTH THE AVAILABILITY ZONES>CLICK ON NEXT.

The screenshot shows the 'Launch template' step of the 'Create Auto Scaling group' wizard. The 'Launch template' dropdown is set to 'divyanshi-loadbalance'. Other settings include:

- Version:** Default (1)
- Description:** -
- AMI ID:** ami-0f918f7e67a5323f0
- Key pair name:** divyanshi-munsifa-aws
- Security groups:** -
- Security group IDs:** sg-059d05037ac5a18cd
- Instance type:** -
- Request Spot Instances:** No

STEP36: SELECT ATTACH TO AN EXISTING LOAD BALANCER>CHOOSE FROM YOUR LOAD BALANCER TARGET GROUPS>CHOOSE THE TARGET GROUP THAT YOU HAVE CREATED

The screenshot shows the 'Network' step of the 'Create Auto Scaling group' wizard. The 'VPC' dropdown is set to 'vpc-07baef0b41a7ac5a3 (divyanshi-aws-munsifa)'. Other settings include:

- Availability Zones and subnets:** 'aps1-az1 (ap-south-1a)' and 'aps1-az3 (ap-south-1b)' are selected.
- Availability Zone distribution - new:** 'Balanced best effort' is selected.

The screenshot shows the AWS Auto Scaling 'Create Auto Scaling group' wizard at Step 3: Integrate with other services. The 'Attach to an existing load balancer' option is selected. The interface includes a sidebar with steps 2 through 7, and a main panel for configuring load balancing.

Load balancing Info

Use the options below to attach your Auto Scaling group to an existing load balancer, or to a new load balancer that you define.

No load balancer
Traffic to your Auto Scaling group will not be fronted by a load balancer.

Attach to an existing load balancer
Choose from your existing load balancers.

Attach to a new load balancer
Quickly create a basic load balancer to attach to your Auto Scaling group.

Attach to an existing load balancer

Select the load balancers that you want to attach to your Auto Scaling group.

Choose from your load balancer target groups
This option allows you to attach Application, Network, or Gateway Load Balancers.

Choose from Classic Load Balancers

Existing load balancer target groups

Only instance target groups that belong to the same VPC as your Auto Scaling group are available for selection.

Select target groups

divyanshi-munsifa-22bce10700 | HTTP X

Application Load Balancer: divyanshi-munsifa-22bce10700

STEP37: SELECT NO VPC LATTICE SERVICE

The screenshot shows the 'Create Auto Scaling group' page in the AWS Management Console. Under 'VPC Lattice integration options', the 'No VPC Lattice service' option is selected. It includes a note that VPC Lattice will not manage the Auto Scaling group's network access and connectivity with other services. There is also an option to 'Attach to VPC Lattice service' which routes requests to specified target groups. Below this, there is a section for 'Application Recovery Controller (ARC) zonal shift' with a checkbox for enabling it. The 'Health checks' section is expanded, showing 'EC2 health checks' is always enabled. A note states that health checks increase availability by replacing unhealthy instances. At the bottom, there are links for CloudShell and Feedback, and a copyright notice for 2025.

STEP38: SELECT TURN ON ELASTIC LOAD BALANCING>SET 20 SECONDS>CLICK ON NEXT

The screenshot shows the 'Create Auto Scaling group' page. In the 'Health checks' section, the 'Turn on Elastic Load Balancing health checks' option is selected and marked as recommended. It explains that Elastic Load Balancing monitors instances available to handle requests. Below this, there are two other optional health check types: 'Turn on VPC Lattice health checks' and 'Turn on Amazon EBS health checks'. The 'Health check grace period' is set to 300 seconds. The bottom of the screen shows standard AWS navigation links for CloudShell, Feedback, Privacy, Terms, and Cookie preferences.

STEP39: SET DESIRED CAPACITY:2, MIN CAPACITY:1 & MAXIMUM CAPACITY:3

STEP40: CLICK ON NEXT

EC2 > Auto Scaling groups > Create Auto Scaling group

Configure group size and scaling

Desired capacity type
Choose the unit of measurement for the desired capacity value. vCPUs and Memory(GiB) are only supported for mixed instances groups configured with a set of instance attributes.

Desired capacity
Specify your group size.
2

Scaling info
You can resize your Auto Scaling group manually or automatically to meet changes in demand.

Scaling limits
Set limits on how much your desired capacity can be increased or decreased.

Min desired capacity 1 **Max desired capacity** 3

Automatic scaling - optional
Choose whether to use a target tracking policy [Info](#)
You can set up other metric-based scaling policies and scheduled scaling after creating your Auto Scaling group.

No scaling policies
Your Auto Scaling group will remain at its initial size and will not dynamically resize to meet demand.

Target tracking scaling policy
Choose a CloudWatch metric and target value and let the scaling policy adjust the desired capacity in proportion to the metric's value.

STEP41: CLICK ON AUTO-SCALING GROUP

EC2 > Auto Scaling groups > Create Auto Scaling group

Instance maintenance policy [Info](#)
Control your Auto Scaling group's availability during instance replacement events. This includes health checks, instance refreshes, maximum instance lifetime features and events that happen automatically to keep your group balanced, called rebalancing events.

Choose a replacement behavior depending on your availability requirements

Mixed behavior
 No policy
For rebalancing events, new instances will launch before terminating others. For all other events, instances terminate and launch at the same time.

Prioritize availability
Launch before terminating

Control costs
 Terminate and launch
Terminate and launch instances at the same time. This allows you to go below your desired capacity by a given percentage and may temporarily reduce availability.

Flexible
 Custom behavior
Set custom values for the minimum and maximum amount of available capacity. This gives you greater flexibility in setting how far below and over your desired capacity EC2 Auto Scaling goes when replacing instances.

Additional capacity settings

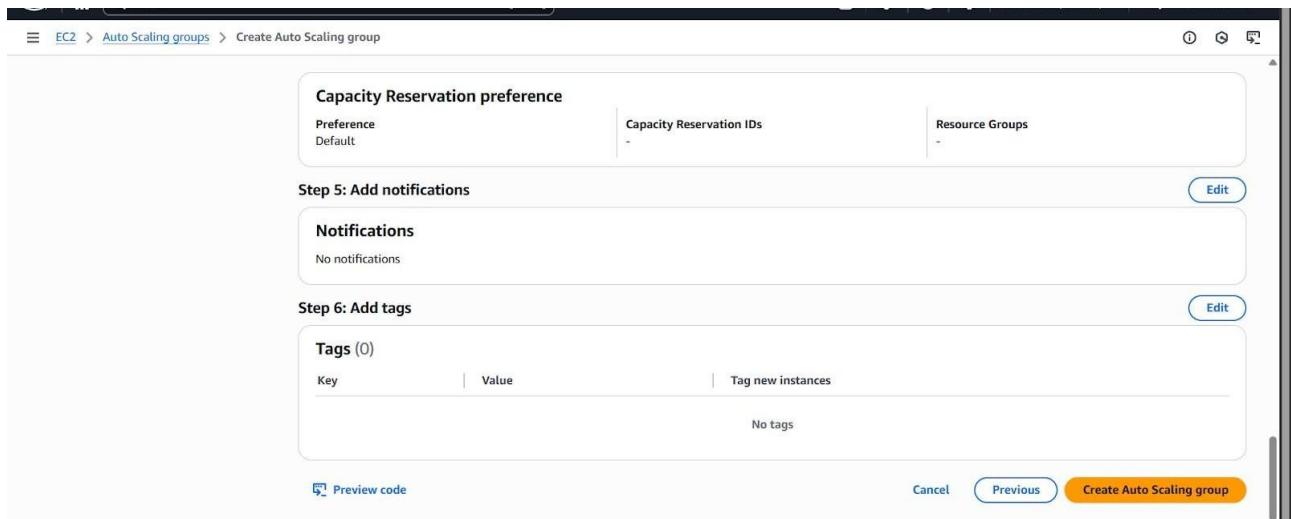
Capacity Reservation preference [Info](#)
Select whether you want Auto Scaling to launch instances into an existing Capacity Reservation or Capacity Reservation resource group.

Default
Auto Scaling uses the Capacity Reservation preference from your launch template.

None
Instances will not be launched into a Capacity Reservation.

Capacity Reservations only
Instances will only be launched into a Capacity Reservation. If capacity isn't available, the instances fail to launch.

Capacity Reservations first



STEP42: NOW CLICK ON EC2>INSTANCES TO CHECK THE NUMBER OF INSTANCES CREATED.

Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone	Public IPv4 DNS	Public IPv4 IP	Elastic IP
Himanshu_22...	i-0db48b7c3d0a42946	Stopped	t2.micro	-	View alarms +	ap-south-1b	-	-	-
vpchimanshul...	i-02cdc87e7b6bfa704	Stopped	t2.micro	-	View alarms +	ap-south-1a	-	-	-
himanshu_22b...	i-099a443da453e49bb	Running	t2.micro	2/2 checks passed	View alarms +	ap-south-1a	-	13.201.13.101	-

STEP43: NOW TERMINATE ONE OF THE INSTANCES FROM EC2 INSTANCES

The screenshot shows the AWS EC2 Instances page. On the left, there's a navigation sidebar with sections like EC2, Dashboard, EC2 Global View, Events, Instances (selected), 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), Network & Security (Security Groups, Elastic IPs, Placement Groups, Key Pairs, Network Interfaces), and Load Balancing (Load Balancers). The main area displays a table titled "Instances (3) Info" with columns: Name, Instance ID, Instance state, Instance type, Status check, Alarm status, Availability Zone, Public IPv4 DNS, and Public IPv4 IP. The table lists three instances: "Himanshu_22..." (Stopped, t2.micro, ap-south-1b, -), "vpchimanshu..." (Stopped, t2.micro, ap-south-1a, -), and "himanshu_22b..." (Running, t2.micro, ap-south-1a, 13.201.13.101). Below the table is a section titled "Select an instance".

STEP44: NOW GO TO AUTO-SCALING GROUPS>INSTANCE MANAGEMENT>HEALTH STATES: UNHEALTHY MEANS DELETED INSTANCE (IT WILL AUTOMATICALLY CREATE ANOTHER INSTANCE AFTER DELETION)

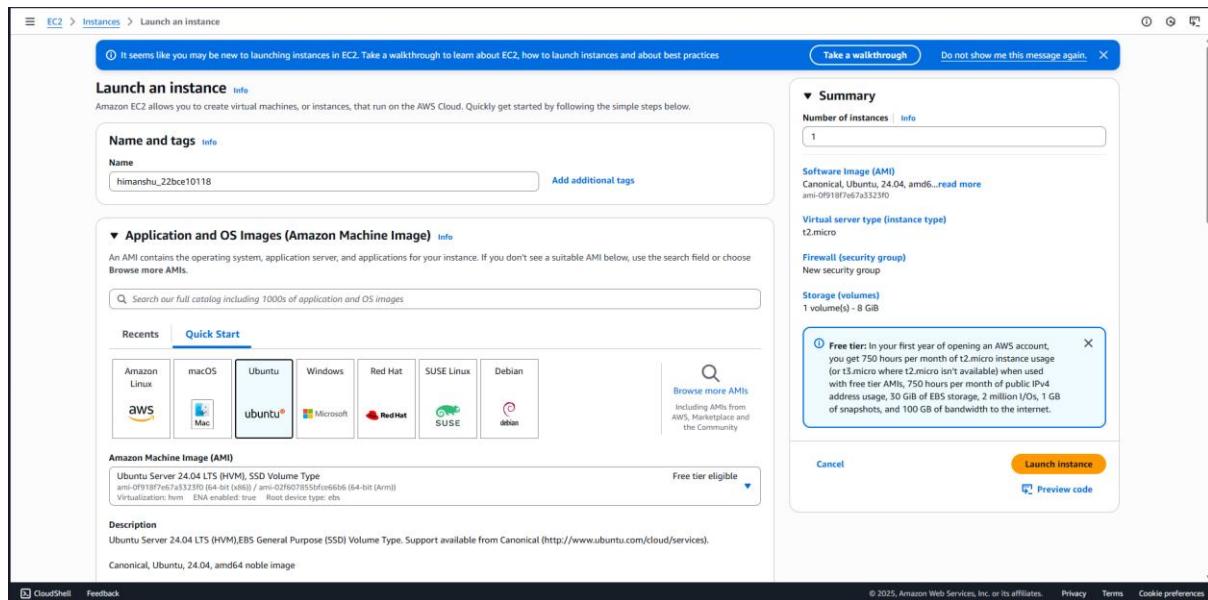
The screenshot shows the AWS Auto Scaling Groups page. The left sidebar includes Network & Security (Security Groups, Elastic IPs, Placement Groups, Key Pairs, Network Interfaces), Load Balancing (Load Balancers, Target Groups, Trust Stores), and Auto Scaling (Auto Scaling Groups, Settings). The main content area shows a summary card for an auto scaling group: Desired capacity 2, Scaling limits (Min - Max) 1 - 3, Desired capacity type Units (number of instances), and Status Updating capacity. Below this is a "Date created" field showing Wed Jul 30 2025 22:39:50 GMT+0530 (India Standard Time). A tab navigation bar at the top of the main content area includes Details, Integrations - new, Automatic scaling, Instance management (selected), Instance refresh, Activity, and Monitoring. The "Instance management" section shows a table titled "Instances (2)" with columns: Instance ID, Lifecycle, Instance..., Weight..., Launch..., Availability..., Health..., and Protect... . It lists two instances: "i-02049f36329c8989c" (InService, c6a.large, -, divyanshi-loadb, aps1-az1 ..., Healthy) and "i-0d36c0cf84ecd63fc" (InService, c6a.large, -, divyanshi-loadb, aps1-az3 ..., Healthy). At the bottom of the page are links for CloudShell, Feedback, and Copyright information: © 2025, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences.

Date: 12-08-2025	Title
Exp. No: 10	HOW TO CREATE EBS AND ATTACH TO EC2 INSTANCE, MODIFY SIZE AND CREATE A SNAPSHOT

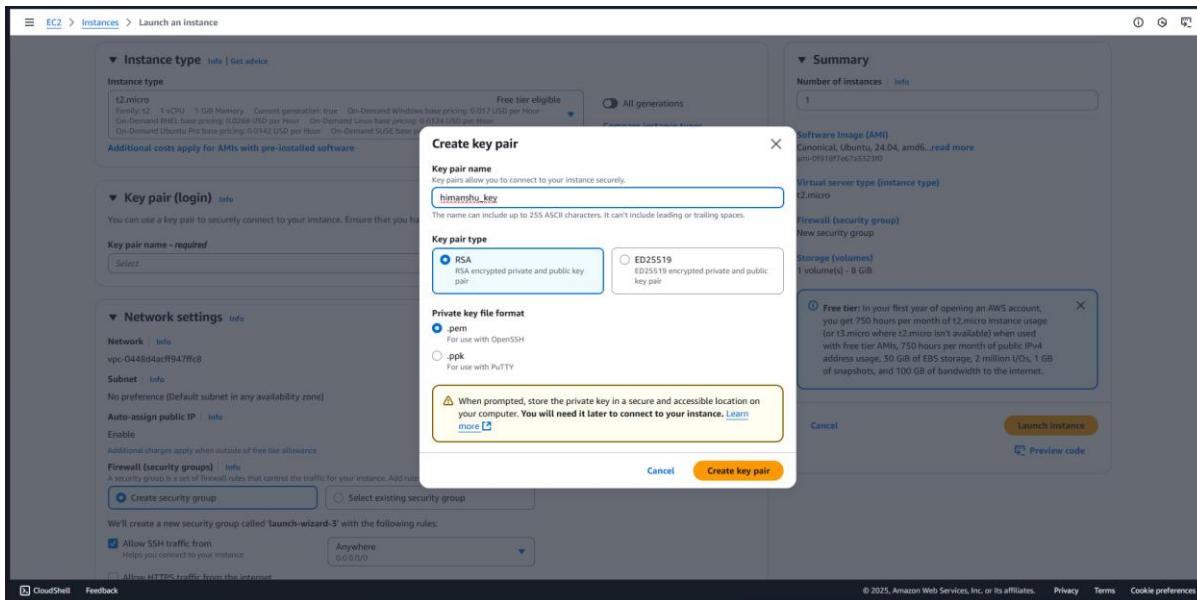
AIM OF THE EXPERIMENT: HOW TO CREATE EBS AND ATTACH TO EC2 INSTANCE, MODIFY SIZE AND CREATE A SNAPSHOT

PROCEDURE:

- GO TO EC2 DASHBOARD>CLICK ON INSTANCES>CLICK ON LAUNCH INSTANCE>TYPE THE NAME OF THE INSTANCE>CHOOSE THE UBUNTU

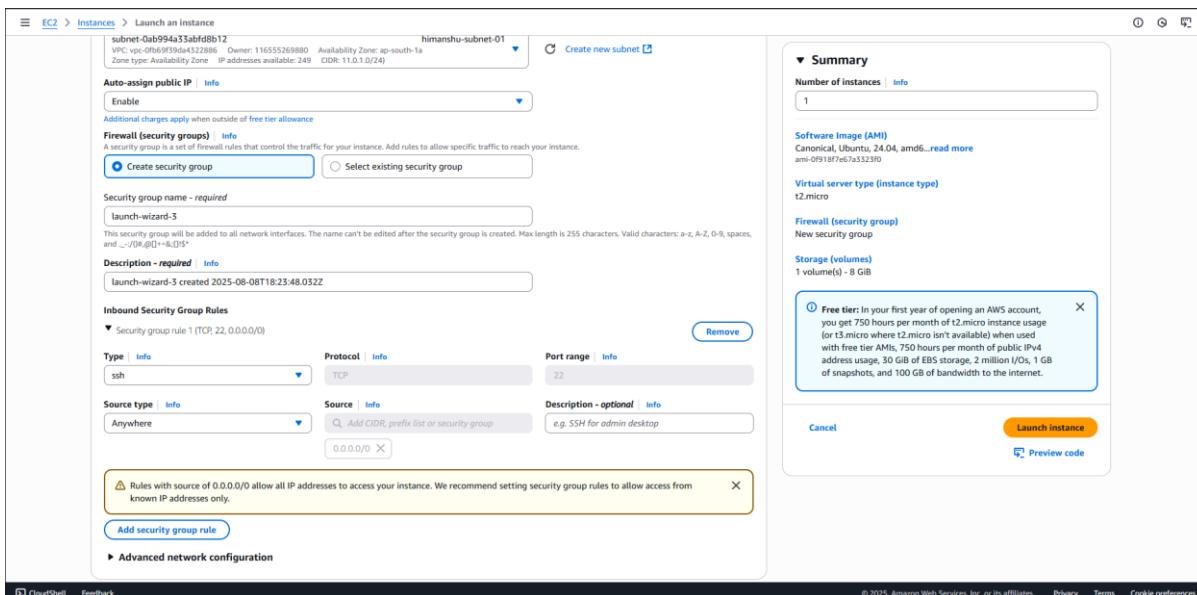


ii) CREATE A KEY PAIR



iii) EDIT THE NETWORK SETTING> SELECT THE VPC CREATED>CHOOSE THE PUBLIC SUBNET>ENABLE AUTO-ASSIGN PUBLIC IP>CREATE SECURITY GROUP

iv) SET TYPE: SSH IN THE SECURITY GROUP>CLICK ON LAUNCH INSTANCE



v) CLICK ON THE EC2 INSTANCE CREATED>CLICK ON CONNECT

The screenshot shows the AWS EC2 Instances page. On the left, there's a sidebar with navigation links like Dashboard, EC2 Global View, Events, 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, Network & Security, Security Groups, Elastic IPs, Placement Groups, Key Pairs, Network Interfaces, and Load Balancing. The main area displays the 'Instance summary for i-099a443da453e49bb (himanshu_22bce10118)'. It includes fields for Instance ID (i-099a443da453e49bb), IPv6 address (-), Hostname type (IP name: ip-11-0-1-66.ap-south-1.compute.internal), Answer private resource DNS name (-), Auto-assigned IP address (13.201.13.101 (Public IP)), IAM Role (Required), IMDSv2 (Required), Operator (-), Public IPv4 address (13.201.13.101), Instance state (Pending), Private IP DNS name (IPv4 only) (ip-11-0-1-66.ap-south-1.compute.internal), Instance type (t2.micro), VPC ID (vpc-0fb69f39da4322886 (himanshu-vpc-01)), Subnet ID (subnet-0ab994a33abfd8b12 (himanshu-subnet-01)), Instance ARN (arn:aws:ec2:ap-south-1:116555269880:instance/i-099a443da453e49bb), Private IPv4 addresses (11.0.1.66), Public DNS (-), Elastic IP addresses (-), AWS Compute Optimizer finding (Opt-in to AWS Compute Optimizer for recommendations.), Auto Scaling Group name (-), Managed (false). Below this, there are tabs for Details, Status and alarms, Monitoring, Security, Networking, Storage, and Tags. The 'Details' tab is selected. At the bottom, there are links for CloudShell and Feedback.

vi) CLICK ON EC2 INSTANCE CONNECT

The screenshot shows the 'Connect to instance' dialog box. At the top, it says 'Connect info' and 'Connect to an instance using the browser-based client.' Below that, there are tabs for EC2 Instance Connect, Session Manager, SSH client, and EC2 serial console. The 'EC2 Instance Connect' tab is selected. A note at the top states: 'Instance is not in public subnet. Associated subnet subnet-0ab994a33abfd8b12 (himanshu-subnet-01) is not a public subnet. To use EC2 Instance Connect, your instance must be in a public subnet. To make the subnet a public subnet, add a route in the subnet route table to an internet gateway.' There are two radio buttons: 'Connect using a Public IP' (selected) and 'Connect using a Private IP'. Under 'Public IPv4 address', the value is 13.201.13.101. Under 'Username', the value is ubuntu. A note at the bottom says: 'Note: In most cases, the default username, ubuntu, is correct. However, read your AMI usage instructions to check if the AMI owner has changed the default AMI username.' At the bottom right, there are 'Cancel' and 'Connect' buttons.

vii) EC2 Instance is connected

```
deep usage...  
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-12-0-1-109:~$  
i-0546548b85ee  
Public IPs: 43.205.120.50 Private IPs: 12.0.1.109
```

viii) TYPE “lsblk” COMMAND IN THE TERMINAL. IT WILL SHOW YOU HOW MANY VOLUMES ARE ATTACHED TO THE EC2 INSTANCE. IT SHOWS THE DEFAULT 8G VOLUME WHICH WE SET WHILE CREATING EC2 INSTANCE.

```
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-12-0-1-109:~$ lsblk  
NAME   MAJ:MIN RM  SIZE RO TYPE MOUNTPOINTS  
loop0    7:0    0  26.3M  1 loop /snap/amazon-ssm-agent/9881  
loop1    7:1    0  73.9M  1 loop /snap/core22/1722  
loop2    7:2    0  44.4M  1 loop /snap/snapsd/23545  
vda     202:0   0   8G  0 disk  
└─xvda1  202:1   0   7G  0 part /  
└─xvda14 202:14   0   4M  0 part  
└─xvda15 202:15   0 106M  0 part /boot/efi  
└─xvda16 259:0   0  913M  0 part /boot  
ubuntu@ip-12-0-1-109:~$  
i-0546548b85  
_1_ec2)
```

EBS Volume created

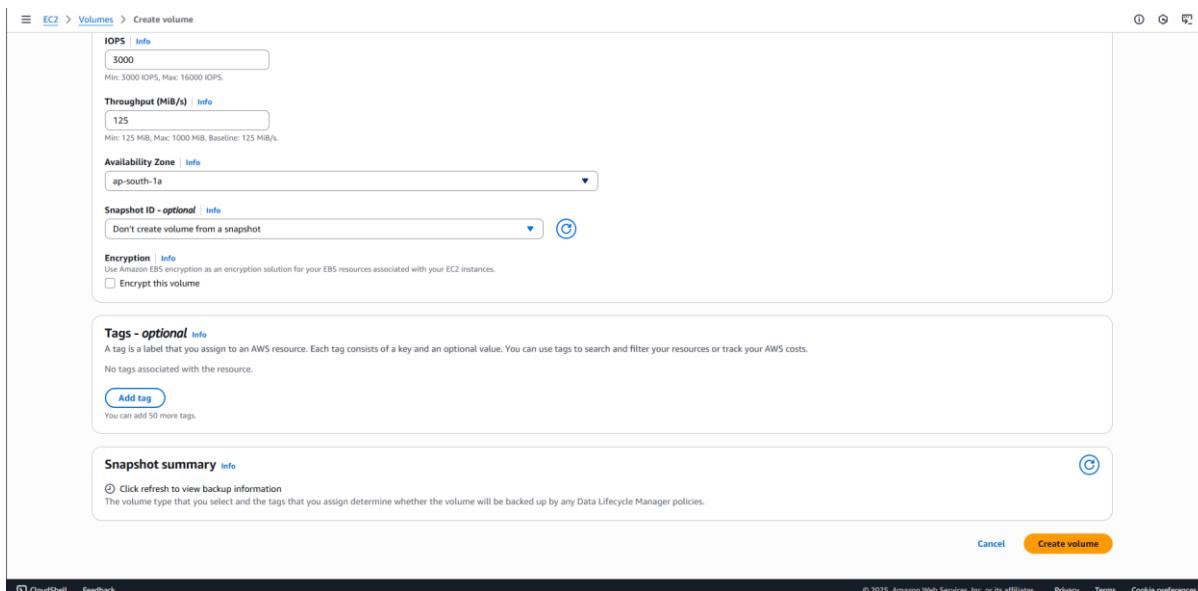
ix) NOW CREATE EBS VOLUME FROM EC2 DASHBOARD: ELASTIC BLOCK STORE>VOLUMES>CREATE VOLUME

Name	Volume ID	Type	Size	IOPS	Throughput	Snapshot ID	Source volume ID	Created	Availability Zone
vol-04e5b6aab09f79775	gp3	8 GiB	3000	125	snap-0b1af51...	-	2025/07/14 17:16 GMT+5:...	ap-south-1a	
vol-0ae2dd1c4df3001f6	gp3	8 GiB	3000	125	snap-0b1af51...	-	2025/08/08 23:59 GMT+5:...	ap-south-1a	
vol-09babfbbea4d2962fb	gp3	8 GiB	3000	125	snap-0b1af51...	-	2025/07/19 00:29 GMT+5:...	ap-south-1a	

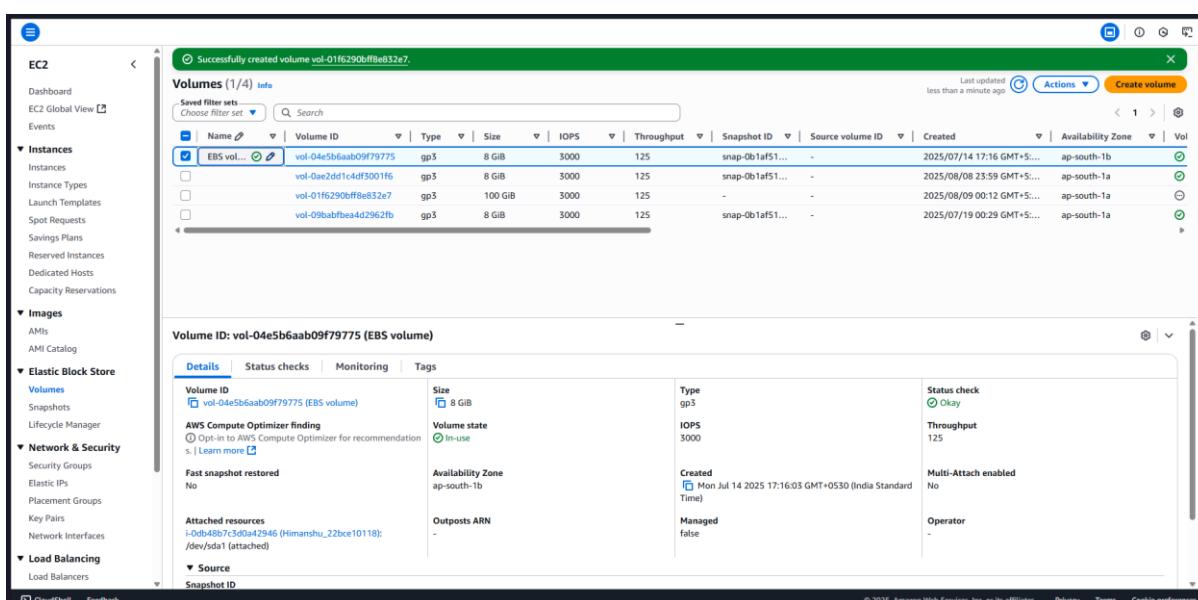
x) YOU CAN CHOOSE ANY OF THE VOLUME TYPES FROM THE DROP-DOWN >SELECT gp3

xi) KEEP THE DATA AS SHOWN

xii) CLICK ON CREATE VOLUME.



xiii) EDIT THE VOLUME NAME BY CLICKING ON IT>CLICK ON THE VOLUME THAT YOU HAVE CREATED



xiv) CLICK ON ACTIONS>ATTACH VOLUME

The screenshot shows the AWS EC2 Volumes page for an EBS volume named 'vol-04e5b6aab09f79775'. The 'Actions' menu is open, highlighting the 'Attach volume' option. Other visible actions include 'Create snapshot', 'Create snapshot lifecycle policy', 'Detach volume', 'Force detach volume', 'Manage auto-enabled I/O', and 'Fault injection'.

xv) SELECT INSTANCE THAT YOU HAVE CREATED>CHOOSE THE DEVICE:/dev/sdk>CLICK ON ATTACH VOLUME

The screenshot shows the 'Attach volume' dialog box. It includes fields for 'Basic details' (Volume ID: vol-0f813db80abfc9414, Availability Zone: ap-south-1), 'Instance' (selected instance: i-0546548b85ee7e08a), and 'Device name' (selected as /dev/sdk). A note at the bottom states: 'Newer Linux kernels may rename your devices to /dev/xvdf through /dev/xvdः internally, even when the device name entered here (and shown in the details) is /dev/sdf through /dev/sdp.'

- xvi) NOW GO TO EC2 TERMINAL AND TYPE:lsblk>IT WILL LIST ALL THE VOLUME(100G IS SHOWN BELOW)

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

ubuntu@ip-12-0-1-109:~$ lsblk
NAME   MAJ:MIN RM  SIZE RO TYPE MOUNTPOINTS
loop0    7:0    0 26.3M  1 loop /snap/amazon-ssm-agent/9881
loop1    7:1    0 73.9M  1 loop /snap/core22/1722
loop2    7:2    0 44.4M  1 loop /snap/snappyd/23545
xvda   202:0    0   8G  0 disk 
|__xvda1 202:1    0   7G  0 part /
|__xvda14 202:14   0   4M  0 part
|__xvda15 202:15   0 106M 0 part /boot/efi
|__xvda16 259:0    0 913M 0 part /boot
xvdk   202:16   0 100G 0 disk
ubuntu@ip-12-0-1-109:~$ lsblk
NAME   MAJ:MIN RM  SIZE RO TYPE MOUNTPOINTS
loop0    7:0    0 26.3M  1 loop /snap/amazon-ssm-agent/9881
loop1    7:1    0 73.9M  1 loop /snap/core22/1722
loop2    7:2    0 44.4M  1 loop /snap/snappyd/23545
xvda   202:0    0   8G  0 disk 
|__xvda1 202:1    0   7G  0 part /
|__xvda14 202:14   0   4M  0 part
|__xvda15 202:15   0 106M 0 part /boot/efi
|__xvda16 259:0    0 913M 0 part /boot
xvdk   202:16   0 100G 0 disk
ubuntu@ip-12-0-1-109:~$
```

- xvii) TYPE sudo fdisk -l (IT WILL LIST OUT ALL THE DISK PARTITION)

```
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes

Disk /dev/xvda: 8 GiB, 8589934592 bytes, 16777216 sectors
Units: sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disklabel type: gpt
Disk identifier: D7B2CFD6-F96A-42FB-B8E1-13FP6555EB07

Device        Start      End  Sectors  Size Type
/dev/xvda1  2099200 16777182 14677983   7G linux filesystem
/dev/xvda14  2048  10239   8192   4M BIOS boot
/dev/xvda15  10240 227327 217088 106M EFI System
/dev/xvda16  227328 2097152 1869825 913M linux extended boot

Partition table entries are not in disk order.

Disk /dev/xvdk: 100 GiB, 107374182400 bytes, 209715200 sectors
Units: sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
ubuntu@ip-12-0-1-109:~$
```

- xviii) TYPE sudo file -s /dev/xvdk (IT WILL SHOW “DATA” WHICH MEANS THERE IS NO FILE SYSTEM CREATED FOR THIS EBS VOLUME)

```
ubuntu@ip-12-0-1-109:~$ sudo file -s /dev/xvdk
/dev/xvdk: data
ubuntu@ip-12-0-1-109:~$
```

- xix) WE NEED TO CREATE FILE SYSTEM FOR EBS VOLUME: TYPE sudo mkfs -t xfs /dev/xvdk
(FILE SYSTEM CREATED)

```
ubuntu@ip-12-0-1-109:~$ sudo file -s /dev/xvdk
/dev/xvdk: data
ubuntu@ip-12-0-1-109:~$ sudo mkfs -t xfs /dev/xvdk
meta-data=/dev/xvdk isize=512 agcount=4, agsize=6553600 blks
          =           sectorsz=512 attr=2, projid32bit=1
          =           crc=1 finobt=1, sparse=1, rmapbt=1
          =           reflink=1 bigtime=1 inobtcount=1 nrext64=0
          =           bsize=4096 blocks=26214400, imaxpct=25
          =           sunit=0 swidth=0 blks
          naming=version 2 bsize=4096 ascii-ci=0, ftype=1
          log=internal log bsize=4096 blocks=16384, version=2
          =           sectsz=512 sunit=0 blks, lazy_count=1
          realtime=none extsz=4096 blocks=0, rtextents=0
ubuntu@ip-12-0-1-109:~$ i-0546548b85e
Public IPs: 43.205.120.58 Private IPs: 12.0.1.109
```

- xx) NOW AGAIN TYPE sudo file -s /dev/xvdk TO CHECK THE FILE SYSTEM (ITS SHIWS EBS VOLUME HAS xfs FILESYSTEM)

```
ubuntu@ip-12-0-1-109:~$ sudo file -s /dev/xvdk
/dev/xvdk: SGI XFS filesystem data (blksize 4096, inosz 512, v2 dirs)
ubuntu@ip-12-0-1-109:~$
```

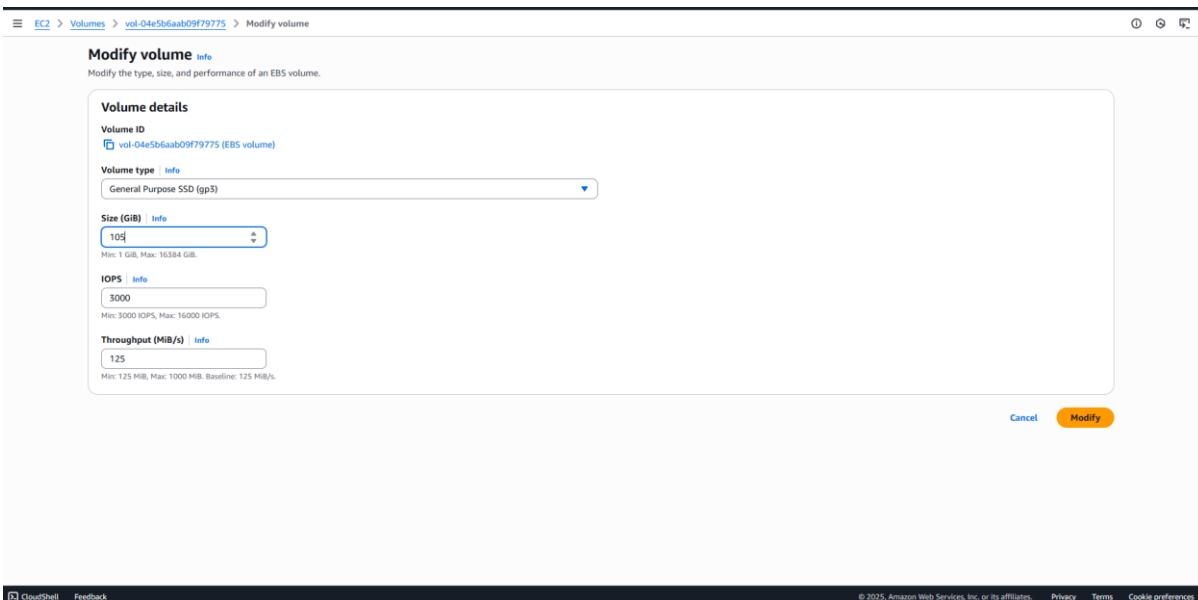
- xxi) CREATE A DIRECTORY: a. TYPE sudo mkdir /munsifaebsvol b. NEXT TYPE sudo mount /dev/xvdk / munsifaebsvol c. TYPE ls -lart /munsifaebsvol

```
ubuntu@ip-12-0-1-109:~$ sudo mkdir /munsifaebsvol
ubuntu@ip-12-0-1-109:~$ sudo mount /dev/xvdk /munsifaebsvol
mount: bad usage
try 'mount --help' for more information.
ubuntu@ip-12-0-1-109:~$ sudo mount /dev/xvdk /munsifaebsvol
ubuntu@ip-12-0-1-109:~$ ls -lart /munsifaebsvol
ls: cannot access '/munsifaebsvol': No such file or directory
ubuntu@ip-12-0-1-109:~$ ls -lart /munsifaebsvol
total 4
drwxr-xr-x 2 root root 6 Feb 23 13:44 .
drwxr-xr-x 23 root root 4096 Feb 23 13:51 ..
ubuntu@ip-12-0-1-109:~$
```

- xxii) NOW TYPE df -h (IT WILL SHOW THAT EBS VOLUME HAS BEEN MOUNTED TO DIRECTORY “munsifaebsvol”)

```
ubuntu@ip-12-0-1-109:~$ sudo mkdir /munsifaebsvol
ubuntu@ip-12-0-1-109:~$ sudo mount /dev/xvdk /munsifaebsvol
mount: bad usage
try 'mount --help' for more information.
ubuntu@ip-12-0-1-109:~$ sudo mount /dev/xvdk /munsifaebsvol
ubuntu@ip-12-0-1-109:~$ ls -lart /munsifaebsvol
ls: cannot access '/munsifaebsvol': No such file or directory
ubuntu@ip-12-0-1-109:~$ ls -lart /munsifaebsvol
total 4
drwxr-xr-x 2 root root 6 Feb 23 13:44 .
drwxr-xr-x 23 root root 4096 Feb 23 13:51 ..
ubuntu@ip-12-0-1-109:~$
```

- xxiii) NOW NEXT GO TO EBS VOLUME TO INCREASE THE VOLUME(NOTE THAT EBS VOLUME CAN BE INCREASED BUT YOU CANNOT REDUCE THE VOLUME SIZE ONCE AN EBS VOLUME IS CREATED BECAUSE THERE IS A PROBABILITY OF DATA LOSS) a. CLICK ON EBS VOLUME>SELECT THE VOLUME THAT YOU HAVE CREATED>CLICK ON MODIFY b. INCREASE THE VOLUME SIZE FROM 100 TO 105>CLICK MODIFY



- xxiv) NOW GO TO THE EC2 TERMINAL AND VERIFY WHETHER THE DISK SIZE HAS CHANGED OR NOT. (TYPE sudo fdisk -l)

```
sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes

Disk /dev/xvda: 8 GiB, 8589934592 bytes, 16777216 sectors
Units: sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disklabel type: gpt
Disk identifier: D7B2CFD6-F96A-42FB-B8E1-13FF6555EB07

Device      Start    End  Sectors  Size Type
/dev/xvda1  2099200 16777182 14677983   7G Linux filesystem
/dev/xvda4    2048    10239    8192   4M BIOS boot
/dev/xvda5   10240   227327  217088 100M EFI System
/dev/xvda6  227328  2097152 1869825 913M Linux extended boot

Partition table entries are not in disk order.

Disk /dev/xvdk: 105 GiB, 112742891520 bytes, 220200960 sectors
Units: sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
ubuntu@ip-12-0-1-109:~$
```

- xxv) NOW IN THE EC2 TERMINAL GO TO EBS VOLUME DIRECTORY AND CREATE FILES. a. TYPE cd /munsifaebsvol (GO TO EBS VOLUME DIRECTORY) b. TYPE sudo touch 1.txt (CREATE FILE1) c. TYPE sudo touch 2.txt (CREATE FILE2) d. TYPE ls -lart (TO VERIFY WHETHER FILES ARE THERE OR NOT)

```
ubuntu@ip-12-0-1-109:/mnt/munsifaebsvol$ sudo touch 1.txt
ubuntu@ip-12-0-1-109:/mnt/munsifaebsvol$ sudo touch 2.txt
ubuntu@ip-12-0-1-109:/mnt/munsifaebsvol$ ls -lart
total 4
drwxr-xr-x 23 root root 4096 Feb 23 13:51 ..
-rw-r--r-- 1 root root 0 Feb 24 08:22 1.txt
drwxr-xr-x 2 root root 32 Feb 24 08:22 .
-rw-r--r-- 1 root root 0 Feb 24 08:22 2.txt
ubuntu@ip-12-0-1-109:/mnt/munsifaebsvol$
```

- xxvi) CREATE SECOND EC2 INSTANCE (CREATE IN A SIMILAR MANNER LIKE YOU HAVE CREATED FOR EC1)>CONNECT EC2 INSTANCE. THEN CHECK THE DISK SIZE OF EC2 INSTANCE (TYPE sudo fdisk -l) IT SHOWS THE DEFAULT 8G

```
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes

Disk /dev/loop2: 44.44 MiB, 46596096 bytes, 91008 sectors
Units: sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes

Disk /dev/xvda: 8 GiB, 8589934592 bytes, 16777216 sectors
Units: sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disklabel type: gpt
Disk identifier: D7B2CFD6-F96A-42FB-B8E1-13FF6555EB07

Device Start End Sectors Size Type
/dev/xvda1 2099200 16777182 14677983 7G Linux filesystem
/dev/xvda14 2048 10239 8192 4M BIOS boot
/dev/xvda15 10240 227327 217088 106M EFI System
/dev/xvda16 227328 2097152 1869825 913M Linux extended boot

Partition table entries are not in disk order.
ubuntu@ip-12-0-1-169:~$
```

- xxvii) NOW TO CREATE A SNAPSHOT GO TO EC2 DASHBOARD: a. EBS VOLUME>CLICK ON THE VOLUME THAT YOU HAVE CREATED>CLICK ON ACTIONS>CLICK ON CREATE SNAPSHOT b. TYPE THE DESCRIPTION>CLICK ON CREATE A SNAPSHOT

xxviii) NOW GO TO SNAPSHOT>CLICK ON THE SNAPSHOT THAT YOU HAVE CREATED>CLICK ON ACTIONS>CREATE VOLUME FROM SNAPSHOT

xxix) KEEP THE DATA SAME>CLICK ON TAG>GIVE A NAME>CLICK ON CREATE SNAPSHOT.

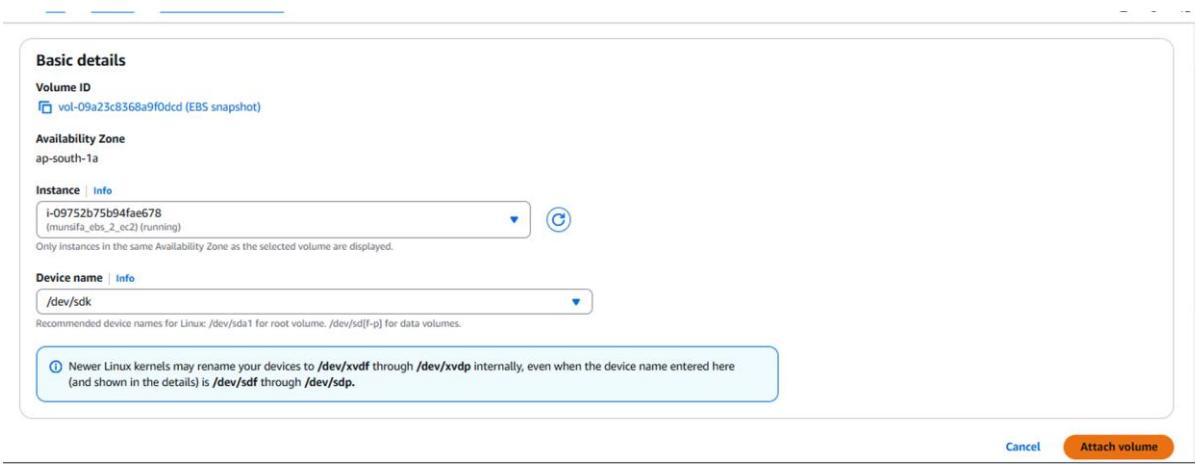
xxx) NOW GO TO VOLUME>MODIFY THE VOLUME NAME

The screenshot shows the AWS EC2 Volumes page. The left sidebar includes sections for Dashboard, EC2 Global View, Events, 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), Network & Security (Security Groups, Elastic IPs, Placement Groups, Key Pairs, Network Interfaces), and Load Balancing (Load Balancers). The main content area displays a table titled "Volumes (1/4) info" with columns: Name, Volume ID, Type, Size, IOPS, Throughput, Snapshot ID, Source volume ID, Created, Availability Zone, and Actions. One row is selected, labeled "snapshot". Below this, a detailed view for "Volume ID: vol-09babfbbea4d2962fb" is shown with tabs for Details, Status checks, Monitoring, and Tags. The Details tab displays information such as Volume ID (vol-09babfbbea4d2962fb), Size (8 GiB), Type (gp3), Status check (Okay), and Attached resources (i-02cd87e7b6bfa704). The Status checks tab shows a single entry: Status check (Okay).

xxxi) CLICK ON THE VOLUME>CLICK ON ACTION>CLICK ON ATTACH VOLUME

The screenshot shows the AWS EC2 Volume details page for "vol-09babfbbea4d2962fb (EBS snapshot)". The left sidebar is identical to the previous screenshot. The main content area shows the volume's details, including Volume ID, Size, Type, Status check, and Attached resources. Below these, there are sections for Source (Snapshot ID: snap-0b1af51ad250df5e) and Encryption (Encryption: Not encrypted). At the bottom, there are tabs for Status checks, Monitoring, and Tags. The Status checks tab contains entries for Status check (Okay), Initialization state (Completed), and Auto-enabled I/O (Enabled). The Monitoring tab shows I/O status (Enabled) and I/O status updated on (Sat Jul 19 2025 00:29:11 GMT+0530). The Tags tab is currently empty. On the right side of the page, there are buttons for Actions (Delete, Modify), Status check (Okay), Throughput (125), Multi-Attach enabled (No), Operator (-), and a note about Multi-Attach support.

xxxii) SELECT EC2 INSTANCE>SELECT sdk IN DEVICE>CLICK ON ATTACH VOLUME



xxxiii) GO TO EC2 TERMINAL>TYPE sudo fdisk -l TO CHECK WHETHER THE NEW VOLUME IS ADDED OR NOT. 105G IS ADDED AS SHOWN BELOW

```
sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes

Disk /dev/xvda: 8 GiB, 8589934592 bytes, 16777216 sectors
Units: sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disklabel type: gpt
Disk identifier: D7B2CFD6-F96A-42FB-B8E1-13FP6555EB07

Device      Start    End Sectors Size Type
/dev/xvda1  2099200 16777182 14677983   7G Linux filesystem
/dev/xvda14    2048   10239    8192   4M BIOS boot
/dev/xvda15  10240  227327  217088 106M EFI System
/dev/xvda16  227328 2097152 1869825 913M Linux extended boot

Partition table entries are not in disk order.

Disk /dev/xvdk: 105 GiB, 112742891520 bytes, 220200960 sectors
Units: sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
ubuntu@ip-12-0-1-169:~$
```

xxxiv) NOW CHECK WHETHER FILE SYSTEM IS ATTACHED OR NOT. TYPE sudo file -s /dev/xvdk

xxxv) NOW CREATE A DIRECTORY: a. TYPE sudo mkdir /munsifaebsvol2 b. MOUNT THE FILE, TYPE sudo mount /dev/xvdk /munsifaebsvol2 c. TYPE ls -lart /munsifaebsvol2

```
Last login: Mon Feb 24 08:57:59 2025 from 13.233.177.4
ubuntu@ip-12-0-1-169:~$ sudo file -s /dev/xvdk
/dev/xvdk: SGI XFS filesystem data (blksz 4096, inosz 512, v2 dirs)
ubuntu@ip-12-0-1-169:~$ sudo mkdir /munsifaebsvol2
ubuntu@ip-12-0-1-169:~$ ^C
ubuntu@ip-12-0-1-169:~$ sudo mount /dev/xvdk / munsifaebsvol2
mount: bad usage
Try 'mount --help' for more information.
ubuntu@ip-12-0-1-169:~$ sudo mount /dev/xvdk /munsifaebsvol2
ubuntu@ip-12-0-1-169:~$ ls -lart /munsifaebsvol2
total 4
-rw-r--r-- 1 root root 0 Feb 24 08:22 1.txt
drwxr-xr-x 2 root root 32 Feb 24 08:22 .
-rw-r--r-- 1 root root 0 Feb 24 08:22 2.txt
drwxr-xr-x 23 root root 4096 Feb 24 10:09 ..
ubuntu@ip-12-0-1-169:~$
```

- xxxvi) NOW YOU CAN CHECK IN BOTH EC2 INSTANCES, FILE1 AND FILE2 IS PRESENT a. TYPE ls (EC2 1) b. TYPE cd \munsifaebsvol2 > ls (EC2 2)

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

Last login: Mon Feb 24 08:57:59 2025 from 13.233.177.4
ubuntu@ip-12-0-1-169:~$ sudo file -s /dev/xvdk
/dev/xvdk: SGI XFS filesystem data (blksz 4096, inosz 512, v2 dirs)
ubuntu@ip-12-0-1-169:~$ sudo mkdir /munsifaebsvol2
ubuntu@ip-12-0-1-169:~$ ^C
ubuntu@ip-12-0-1-169:~$ sudo mount /dev/xvdk / munsifaebsvol2
mount: bad usage
Try 'mount --help' for more information.
ubuntu@ip-12-0-1-169:~$ sudo mount /dev/xvdk /munsifaebsvol2
ubuntu@ip-12-0-1-169:~$ ls -lart /munsifaebsvol2
total 4
-rw-r--r-- 1 root root 0 Feb 24 08:22 1.txt
drwxr-xr-x 2 root root 32 Feb 24 08:22 .
-rw-r--r-- 1 root root 0 Feb 24 08:22 2.txt
drwxr-xr-x 23 root root 4096 Feb 24 10:09 ..
ubuntu@ip-12-0-1-169:~$ cd /munsifaebsvol2
ubuntu@ip-12-0-1-169:/munsifaebsvol2$ ls
1.txt 2.txt
ubuntu@ip-12-0-1-169:/munsifaebsvol2$
```

- xxxvii) IF YOU CREATE ANOTHER FILE IN FIRST EC2 INSTANCE, IT WILL NOT REFLECT IN THE SECOND EC2 INSTANCE. a. TYPE sudo touch 3.txt in FIRST EC2 INSTANCE b. CHECK WITH ls (FIRST EC2 INSTANCE-IT WILL DISPLAY ALL THE THREE TEXT TILES.) c. TYPE ls in SECOND EC2 INSTANCE (IT WILL ONLY DISPLAY TWO TEXT FILES)