



K.R. MANGALAM UNIVERSITY
THE COMPLETE WORLD OF EDUCATION

11/28/2025

Fundamentals Of Cloud Computing & its Security lab

Practical File ENCS-353

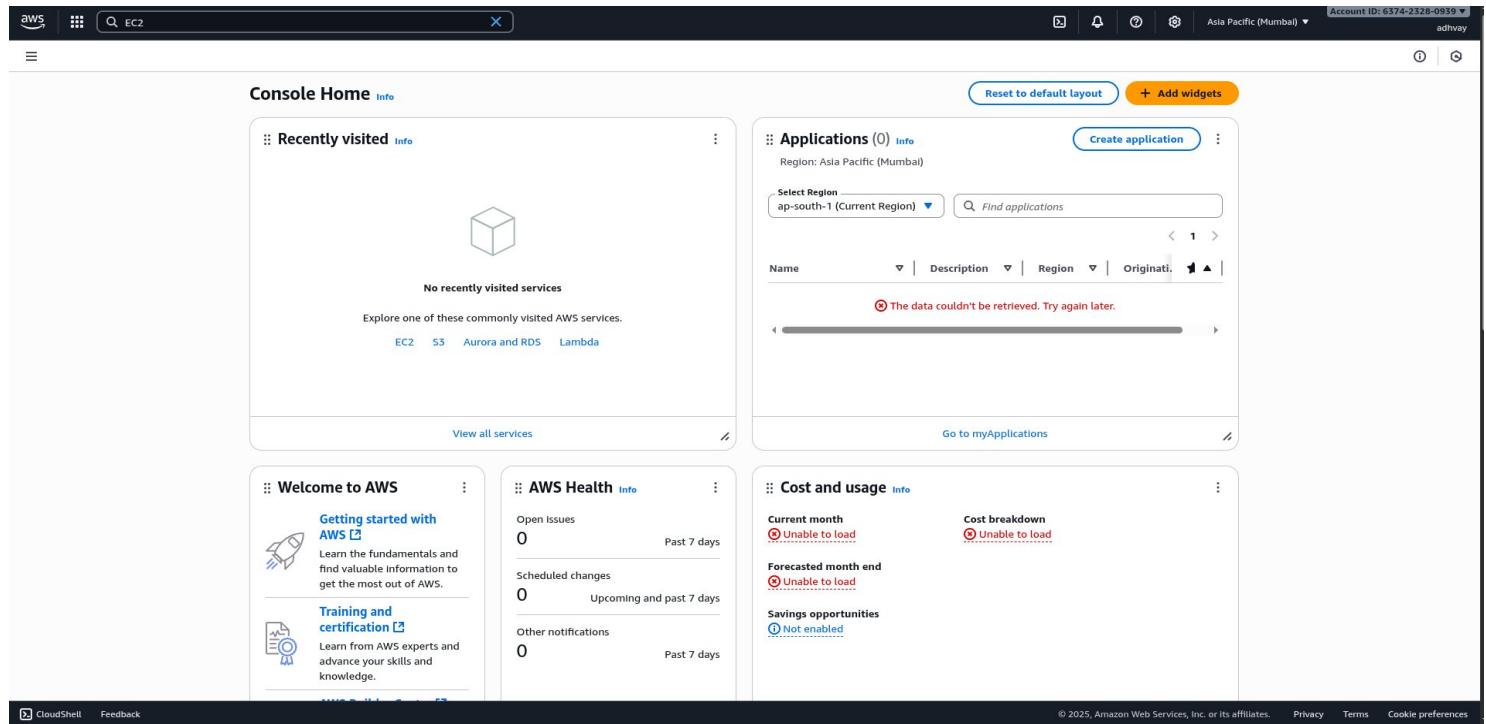
B. Tech CSE Cyber Security

Index

S. No.	Name of Practical	Sign
1	To launch an EC2 instance in AWS and connect to it using SSH.	
2	To create an Elastic Block Store (EBS) volume in AWS and attach it to an EC2 instance.	
3	To create and configure an Amazon S3 bucket in AWS Management Console.	
4	To create an AWS Lambda function and test its execution in AWS Management Console.	
5	To Create an IAM User in AWS	
6	To secure an AWS IAM user account by enabling Multi-Factor Authentication (MFA) .	
7	To create a user group in AWS IAM to manage permissions collectively for multiple users who share similar roles or responsibilities.	
8	To create a security role in AWS IAM for providing secure and temporary access to specific AWS resources.	
9	To Create a Virtual Private Cloud.	

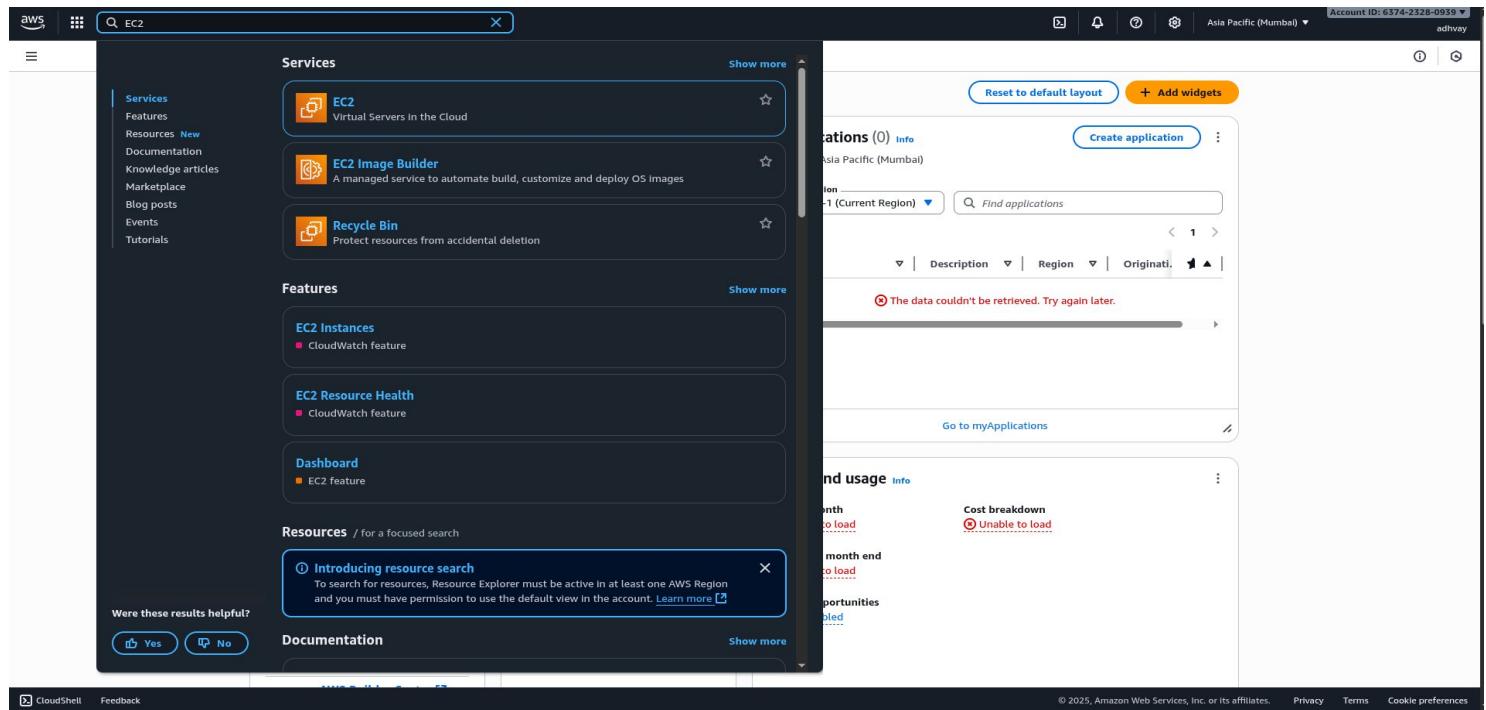
Practical 1: To launch an EC2 instance in AWS

Step -1 Navigate to the EC2 Dashboard



The screenshot shows the AWS Console Home page. At the top, there is a search bar with 'EC2' typed into it. Below the search bar, there are several cards: 'Recently visited' (empty), 'Applications (0)' (Region: Asia Pacific (Mumbai)), 'Welcome to AWS' (Getting started with AWS, Training and certification), 'AWS Health' (Open Issues: 0, Scheduled changes: 0, Other notifications: 0), and 'Cost and usage' (Current month: Unable to load, Forecasted month end: Unable to load, Savings opportunities: Not enabled). At the bottom left, there is a sidebar with 'Services' (EC2, EC2 Image Builder, Recycle Bin), 'Features' (EC2 Instances, EC2 Resource Health, Dashboard), and 'Resources' (Introducing resource search, Documentation). The status bar at the bottom right indicates the region is Asia Pacific (Mumbai) and the account ID is 6374-2328-0939.

Once signed in, use the search bar at the top to find and select EC2. This will take you to the EC2 dashboard, where you can manage your virtual servers.



The screenshot shows the AWS Services page. The search bar at the top has 'EC2' typed into it. On the left, there is a sidebar with 'Services' (Features, Resources New, Documentation, Knowledge articles, Marketplace, Blog posts, Events, Tutorials), 'Features' (EC2 Instances, EC2 Resource Health, Dashboard), and 'Resources' (Introducing resource search, Documentation). The main content area shows the 'Applications (0)' card from the previous screenshot. The status bar at the bottom right indicates the region is Asia Pacific (Mumbai) and the account ID is 6374-2328-0939.

Step -2 Launch an Instance

On the EC2 dashboard, click the "Launch instance" button. This will start the wizard for creating a new EC2 instance.



Step -3 Choose an Amazon Machine Image (AMI)

Select an AMI, which is a template for your instance's operating system and software. For a basic setup, I choose a free tier eligible AMI like Amazon Linux 2023 AMI or Ubuntu Server 22.04 LTS.

Step -4 Choose an Instance Type

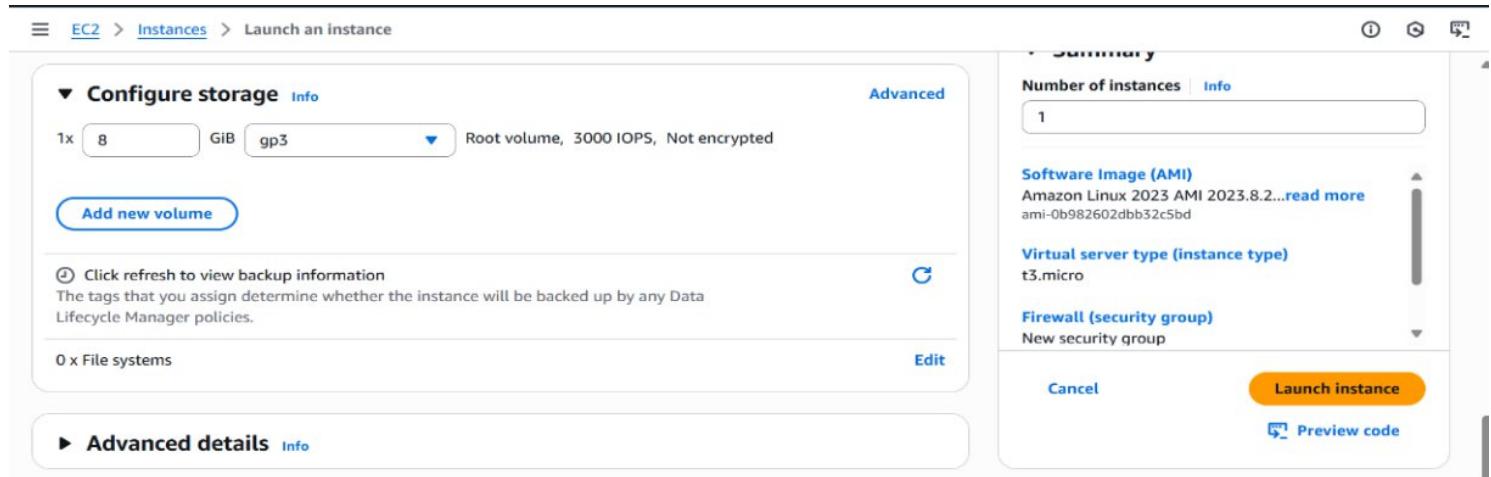
An instance type determines the CPU, memory, storage, and networking capacity of your instance. For most basic use cases, the t2.micro or t3.micro instance types are a great choice as they are free tier eligible.

Step-5 Configure Instance Details

On this page, you can configure network settings, assign an IAM role, and more. For a simple setup, you can often leave most of the settings at their defaults.

Step-6 Add Storage

Here you can specify the size and type of the root volume (the main disk) for your instance. The default is usually sufficient, but you can increase it if you need more space. Free tier includes up to 30 GB of EBS General Purpose SSD (gp2) or Magnetic storage.



Step-7 Configure Security Group

A security group acts as a virtual firewall for your instance, controlling inbound and outbound traffic. You can create a new security group or use an existing one. For a basic web server, you'll need to allow inbound traffic on port 80 (HTTP) and port 22 (SSH) to connect to the instance.

Step-8 Review and Launch

Review all the settings you've chosen. If everything looks correct, click the "Launch" button

Step-9 Create or Select a Key Pair

The screenshot shows the 'Key pair (login)' step of the EC2 instance launch wizard. It includes a note about using a key pair for secure connection, a dropdown for selecting a key pair name (with 'Key pair name - required' highlighted), and a 'Create new key pair' button. To the right, a summary panel shows 1 instance being launched with the Amazon Linux 2023 AMI 2 (ami-0b982602dbb32c5bd).

This is a crucial step. A **key pair** is used to securely connect to your instance via SSH. You must either **create a new key pair** or select an existing one. If you create a new one, you'll be prompted to download the **private key file (.pem)**. **Store this file securely**, as you will need it to connect to your instance and it cannot be re-downloaded later.

Step-10 Launch the Instance

After selecting or creating the key pair, click "**Launch instance**". AWS will now provision your new EC2 instance. You can monitor its status on the EC2 dashboard, where it will show up as "**Pending**" and then transition to "**Running**" when it's ready.

The screenshot shows the EC2 Instances dashboard with two instances listed: 'randomnonse...' (t3.micro, Running) and 'bannerEC2' (t3.micro, Running). The left sidebar includes sections for EC2, Dashboard, EC2 Global View, Events, Instances (selected), Instance Types, Launch Templates, Spot Requests, Savings Plans, Reserved Instances, Dedicated Hosts, Capacity Reservations, Capacity Manager, Images (AMIs, AMI Catalog), Elastic Block Store (Volumes, Snapshots, Lifecycle Manager), and Network & Security (Security Groups, Elastic IPs, Placement Groups). The bottom navigation bar includes CloudShell, Feedback, and links to 2025 AWS terms and cookie preferences.

```
Welcome to Ubuntu 24.04.3 LTS (GNU/Linux 6.14.0-1015-aws x86_64)
```

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

```
System information as of Sun Nov 9 17:48:38 UTC 2025
```

```
System load: 0.08 Temperature: -273.1 C
Usage of /: 25.8% of 6.71GB Processes: 108
Memory usage: 22% Users logged in: 0
Swap usage: 0% IPv4 address for ens5: 172.31.31.132
```

```
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-172-31-31-132:~$ ls
ubuntu@ip-172-31-31-132:~$ █
```

i-087e63f2c2da7c9fe (bannerEC2)

Public IPs: 3.90.0.226 Private IPs: 172.31.31.132

Practical 2 . Create Volume

Step-1: Search EC2 & scroll to volumes

The screenshot shows the 'Create volume' page in the AWS Management Console. The 'Volume type' is set to 'General Purpose SSD (gp3)'. The 'Size (GiB)' is set to 100. The 'IOPS' is set to 3000. The 'Throughput (MiB/s)' is set to 125. The 'Availability Zone' is set to 'use1-az4 (us-east-1c)'. The 'Encryption' section has a checked checkbox for 'Encrypt this volume'. The 'KMS key' dropdown is empty. At the bottom, there are links for 'CloudShell', 'Feedback', and copyright information: '© 2025, Amazon Web Services, Inc. or its affiliates.' and 'Privacy Terms Cookie preferences'.

**Click on create volume and choose the settings as per the requirements.
(here we have chosen gp3 -> size=5 and rest are default.)**

Step 2:- Keep the availability zone as the required zone in other activities

The screenshot shows the 'Create volume' page with the 'KMS key' dropdown expanded. It lists three options: 'Default key that protects my EBS volumes when no other key is defined', 'O18252911125 (This account)', and 'cda75099-a5a2-4d73-b52e-d2fafa2c5a8e'. A note at the bottom of this section states: 'Volumes that are created from encrypted snapshots are automatically encrypted using the same key as the snapshot, or using a different key that you specify. Volumes that are created from unencrypted snapshots are automatically unencrypted, but you can choose to encrypt them using a specific key. If no snapshot is selected, you can choose to encrypt the volume and specify your own key.' Below this is a 'Tags - optional' section with a note about tags being labels assigned to AWS resources. The 'Snapshot summary' section includes a note about Data Lifecycle Manager policies. At the bottom right are 'Cancel' and 'Create volume' buttons.

Step 3: Attach the volume

EC2 > Volumes > vol-0b30025ca51db9938 > Attach volume

Attach volume [Info](#)

Attach a volume to an instance to use it as you would a regular physical hard disk drive.

Basic details

Volume ID
 vol-0b30025ca51db9938

Availability Zone
use1-az4 (us-east-1c)

Instance [Info](#)
i-087e63f2c2da7c9fe (bannerEC2) (running)
Only instances in the same Availability Zone as the selected volume are displayed.

Device name [Info](#)
/dev/sdb
Recommended device names for Linux: /dev/sda1 for root volume. /dev/sd[f-p] for data volumes.

ⓘ Newer Linux kernels may rename your devices to `/dev/xvdf` through `/dev/xvdp` internally, even when the device name entered here (and shown in the details) is `/dev/sdf` through `/dev/sdp`.

[Cancel](#) Attach volume

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

```
Swap usage: 0%           IPv4 address for ens5: 172.31.31.132
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-172-31-31-132:~$ ls
ubuntu@ip-172-31-31-132:~$ lsblk
NAME      MAJ:MIN RM  SIZE RO TYPE MOUNTPOINTS
loop0       7:0    0 27.6M  1 loop /snap/amazon-ssm-agent/11797
loop1       7:1    0 50.8M  1 loop /snap/snapd/25202
loop2       7:2    0 73.9M  1 loop /snap/core22/2133
nvme0n1    259:0   0   8G  0 disk
└─nvme0n1p1 259:1   0   7G  0 part /
└─nvme0n1p14 259:2   0   4M  0 part
└─nvme0n1p15 259:3   0 106M 0 part /boot/efi
└─nvme0n1p16 259:4   0  913M 0 part /boot
nvme1n1    259:5   0 100G 0 disk
ubuntu@ip-172-31-31-132:~$
```

i-087e63f2c2da7c9fe (bannerEC2)

Public IPs: 3.90.0.226 Private IPs: 172.31.31.132

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

Finally the volume is attached

EC2 Global View ▾

Events

Instances

Instance Types

Launch Templates

Spot Requests

Savings Plans

Reserved Instances

Dedicated Hosts

Capacity Reservations

Capacity Manager [New](#)

Images

AMIs

AMI Catalog

Elastic Block Store

Volumes

Snapshots

Lifecycle Manager

Network & Security

Security Groups

Elastic IPs

Placement Groups

Key Pairs

Network Interfaces

Load Balancing

[CloudShell](#)

[Feedback](#)

Successfully attached volume vol-0b30025ca51db9938 to instance i-087e63f2c2da7c9fe.

Volumes (1/4) [Info](#)

Last updated less than a minute ago [Actions](#) [Create volume](#)

Name	Volume ID	Type	Size	IOPS	Throughput	Snapshot ID	Source volume ID	Created
vol-07e59d214b4495144	gp3	8 GiB	3000	125	-	snap-051ef35...	-	2025/11/09 22:08 GMT+5:...
vol-0b30025ca51db9938	gp3	100 GiB	3000	125	-	-	-	2025/11/09 23:21 GMT+5:...
vol-0e5601bd25b935470	gp3	100 GiB	3000	125	-	-	-	2025/11/09 22:22 GMT+5:...
vol-0aaaace21ca26b803	gp3	8 GiB	3000	125	-	snap-01e432c...	-	2025/11/09 22:57 GMT+5:...

Volume ID: vol-0b30025ca51db9938

Details	Status checks	Monitoring	Tags
Volume ID vol-0b30025ca51db9938	Size 100 GiB	Type gp3	Status check Insufficient data
AWS Compute Optimizer finding Opt-in to AWS Compute Optimizer for recommendations. Learn more	Volume state In-use	IOPS 3000	Throughput 125
Fast snapshot restored No	Availability Zone use1-az4 (us-east-1c)	Created Sun Nov 09 2025 23:21:36 GMT+0530 (India Standard Time)	Multi-Attach enabled No
Attached resources i-087e63f2c2da7c9fe (bannerEC2): /dev/sdd (attached)	Outposts ARN -	Managed false	Operator -

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

Practical 3 - CREATE AN S3 BUCKET IN AWS

2. Navigate to S3

- In the search bar at the top, type **S3**.
- Click on **S3 (Scalable Storage in the Cloud)**.

The screenshot shows the AWS Management Console homepage. The search bar at the top contains 's3'. The main content area is titled 'Services' and lists three items: 'S3 Scalable Storage in the Cloud', 'S3 Glacier Archive Storage in the Cloud', and 'AWS Snow Family Large Scale Data Transport'. Below this, under 'Features', there are two sections: 'S3 on Outposts' (with a note about AWS Outposts feature) and 'Exports to S3' (with a note about DynamoDB feature). On the left, a sidebar titled 'Console' has a 'Recent' section with links to Services, Features, Resources, Documentation, Knowledge articles, Marketplace, Blog posts, Events, and Tutorials.

3. Create a New Bucket

- Click on “Create bucket” button.

The screenshot shows the 'Amazon S3' service page. The left sidebar lists various bucket types: General purpose buckets, Directory buckets, Table buckets, Vector buckets, Access Grants, Access Points (General Purpose Buckets, FSx file systems), Access Points (Directory Buckets), Object Lambda Access Points, Multi-Region Access Points, Batch Operations, and IAM Access Analyzer for S3. The main content area is titled 'General purpose buckets' and shows '1' bucket. A table lists the bucket details: Name (my3bucket8292536), AWS Region (Asia Pacific (Mumbai) ap-south-1), and Creation date (September 8, 2025, 10:10:41 (UTC+05:30)). There are buttons for 'Copy ARN', 'Empty', 'Delete', and 'Create bucket'. Below the table, there are sections for 'Account snapshot' and 'External access summary - new'.

4. Configure Bucket Settings

- **Bucket name:** Enter a unique name (e.g., my-first-s3-bucket-2025).
⚠ Bucket names must be globally unique across AWS.
- **AWS Region:** Select a region (choose one closest to your users for better performance).

The screenshot shows the 'Create bucket' configuration page in the Amazon S3 console. At the top, there's a breadcrumb navigation: 'Amazon S3 > Buckets > Create bucket'. Below the header, the title 'Create bucket' has a 'Info' link. A note says 'Buckets are containers for data stored in S3.' Under 'General configuration', the 'AWS Region' is set to 'US East (N. Virginia) us-east-1'. The 'Bucket type' section shows 'General purpose' selected (with a note about redundancy across Availability Zones) and 'Directory' as an option (with a note about low-latency use cases). The 'Bucket name' field is filled with 'banner'. The 'Copy settings from existing bucket - optional' section includes a 'Choose bucket' button and a note about copied settings. In the 'Object Ownership' section, 'ACLs disabled (recommended)' is selected (noting ownership by the account), while 'ACLs enabled' is also available (noting ownership by other accounts). The footer includes links for 'CloudShell', 'Feedback', and copyright information: '© 2025, Amazon Web Services, Inc. or its affiliates.', 'Privacy', 'Terms', and 'Cookie preferences'.

5. Set Bucket Options

- **Object Ownership:**
- Choose **ACLs disabled (recommended)** for most use cases.
- **Block Public Access:**
- By default, all public access is blocked (recommended for private buckets).
- If you need a public bucket (for hosting static websites), uncheck the option and acknowledge the warning.

6. Configure Bucket Settings (Optional)

- **Versioning:** Enable if you want to keep multiple versions of an object.
- **Encryption:** Enable default encryption if required.
- **Tags:** Add key-value tags if you want to manage cost tracking or organization.

- Block all public access**
- Turning this setting on is the same as turning on all four settings below. Each of the following settings are independent of one another.
- Block public access to buckets and objects granted through new access control lists (ACLs)**
S3 will block public access permissions applied to newly added buckets or objects, and prevent the creation of new public access ACLs for existing buckets and objects. This setting doesn't change any existing permissions that allow public access to S3 resources using ACLs.
 - Block public access to buckets and objects granted through any access control lists (ACLs)**
S3 will ignore all ACLs that grant public access to buckets and objects.
 - Block public access to buckets and objects granted through new public bucket or access point policies**
S3 will block new bucket and access point policies that grant public access to buckets and objects. This setting doesn't change any existing policies that allow public access to S3 resources.
 - Block public and cross-account access to buckets and objects through any public bucket or access point policies**
S3 will ignore public and cross-account access for buckets or access points with policies that grant public access to buckets and objects.

Bucket Versioning

Versioning is a means of keeping multiple variants of an object in the same bucket. You can use versioning to preserve, retrieve, and restore every version of every object stored in your Amazon S3 bucket. With versioning, you can easily recover from both unintended user actions and application failures. [Learn more ↗](#)

Bucket Versioning

Disable
 Enable

Tags - optional (0)

You can use bucket tags to track storage costs and organize buckets. [Learn more ↗](#)

No tags associated with this bucket.

[Add new tag](#)

You can add up to 50 tags.

Default encryption [Info](#)

Server-side encryption is automatically applied to new objects stored in this bucket.

Encryption type [Info](#)
 Secure your objects with two separate layers of encryption. For details on pricing, see DSSE-KMS pricing on the Storage tab of the [Amazon S3 pricing page](#). [↗](#)

Server-side encryption with Amazon S3 managed keys (SSE-S3)
 Server-side encryption with AWS Key Management Service keys (SSE-KMS)

Enable

Tags - optional (0)

You can use bucket tags to track storage costs and organize buckets. [Learn more ↗](#)

No tags associated with this bucket.

[Add new tag](#)

You can add up to 50 tags.

Default encryption [Info](#)

Server-side encryption is automatically applied to new objects stored in this bucket.

Encryption type [Info](#)
 Secure your objects with two separate layers of encryption. For details on pricing, see DSSE-KMS pricing on the Storage tab of the [Amazon S3 pricing page](#). [↗](#)

Server-side encryption with Amazon S3 managed keys (SSE-S3)
 Server-side encryption with AWS Key Management Service keys (SSE-KMS)
 Dual-layer server-side encryption with AWS Key Management Service keys (DSSE-KMS)

Bucket Key
 Using an S3 Bucket Key for SSE-KMS reduces encryption costs by lowering calls to AWS KMS. S3 Bucket Keys aren't supported for DSSE-KMS. [Learn more ↗](#)

Disable
 Enable

► Advanced settings

i After creating the bucket, you can upload files and folders to the bucket, and configure additional bucket settings.

[Cancel](#)

[Create bucket](#)

7. Review and Create

- Review your settings.
- Click **Create bucket**.

The screenshot shows the Amazon S3 Buckets page. At the top, a green banner indicates "Successfully created bucket 'bannerbucket69'". Below this, there are two tabs: "General purpose buckets" (selected) and "Directory buckets". A search bar labeled "Find buckets by name" is present. The main table lists two buckets:

Name	AWS Region	Creation date
bannerbucket69	US East (N. Virginia) us-east-1	November 9, 2025, 23:28:57 (UTC+05:30)
randomnigga	US East (N. Virginia) us-east-1	November 9, 2025, 22:31:33 (UTC+05:30)

On the right side, there are three informational boxes: "Account snapshot" (updated daily), "External access summary - new" (updated daily), and "Storage Lens provides visibility into storage usage and activity trends".

8. Upload Objects (Optional)

- After creation, open the bucket.
- Click **Upload → Add files**.
- Select your file(s), then click **Upload**.

The screenshot shows the Amazon S3 bannerbucket69 Objects page. The top navigation bar includes "Amazon S3 > Buckets > bannerbucket69". The main content area has tabs for "Objects" (selected), "Metadata", "Properties", "Permissions", "Metrics", "Management", and "Access Points". A "Create folder" button is visible. The "Actions" dropdown menu includes "Upload". The table lists three objects:

Name	Type	Last modified	Size	Storage class
Fedora-KDE-Desktop-Live-43-1.6.x86_64.iso	Iso	November 9, 2025, 23:31:14 (UTC+05:30)	3.0 GB	Standard
image_2025-11-09_233007404.png	png	November 9, 2025, 23:31:16 (UTC+05:30)	170.1 KB	Standard
Vedic Maths.pptx	pptx	November 9, 2025, 23:31:15 (UTC+05:30)	440.4 KB	Standard

Upload succeeded
For more information, see the [Files and folders](#) table.

X

Upload: status

Close

ⓘ After you navigate away from this page, the following information is no longer available.

Summary

Destination
<s3://bannerbucket69>

Succeeded

3 files, 3.0 GB (100.00%)

Failed

0 files, 0 B (0%)

[Files and folders](#)

[Configuration](#)

Files and folders (3 total, 3.0 GB)

Files and folders (3 total, 3.0 GB)						
<input type="text"/> Find by name						
Name	Folder	Type	Size	Status	Error	
Vedic Maths.pptx ↗	-	application/vnd.openxmlformats-...	440.4 KB	Success Succeeded	-	
Fedora-KDE-Desktop-Live-43-1.6.x86_64.iso ↗	-	-	3.0 GB	Success Succeeded	-	
image_2025-11-09_233007404.png ↗	-	image/png	170.1 KB	Success Succeeded	-	

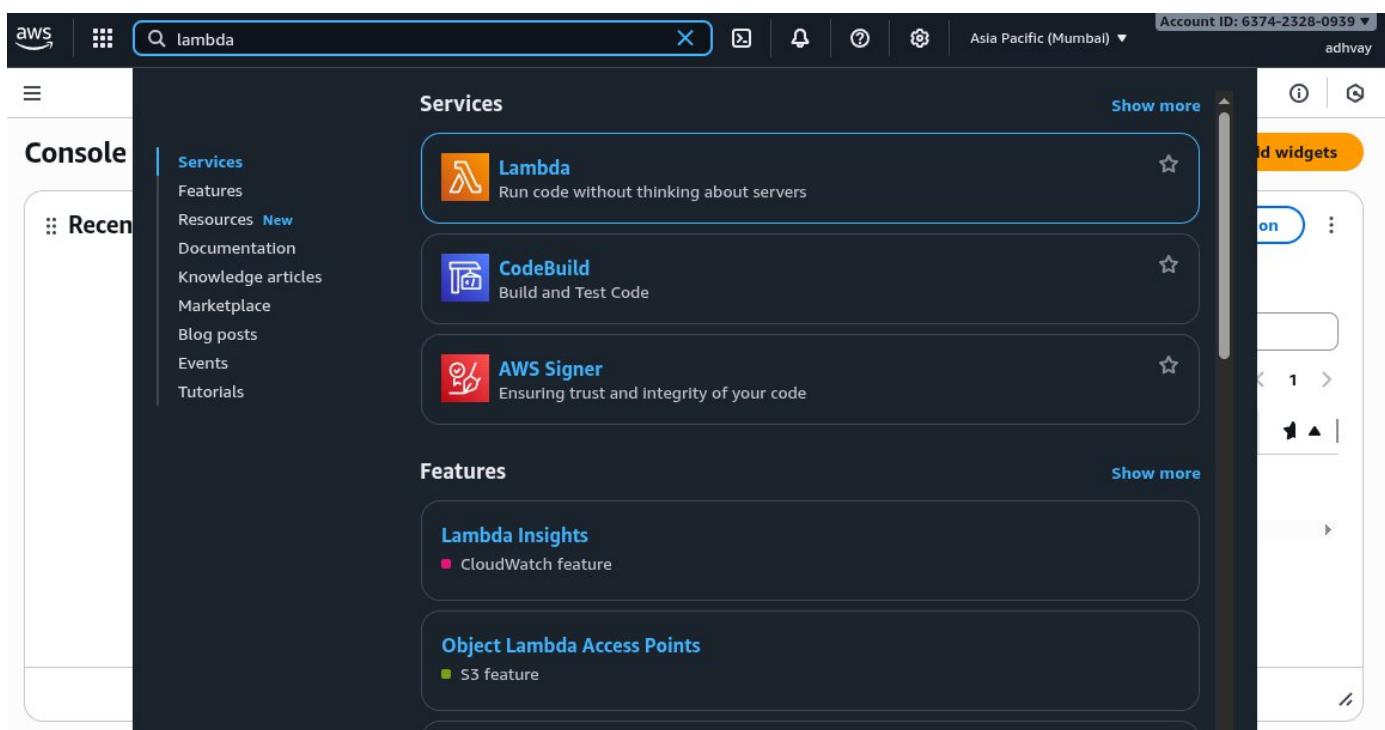
Practical 4 . Steps to Create an AWS Lambda Function

1. Log in to AWS Management Console

- Go to AWS Console.
 - Sign in with your credentials.
-

2. Navigate to AWS Lambda

- In the search bar, type **Lambda**.
- Click on **Lambda** service.



3. Create a New Lambda Function

- Click **Create function**.

4. Choose a Creation Method

You'll see 3 options:

1. **Author from scratch** → (most common, start fresh).
2. **Use a blueprint** → predefined templates.
3. **Container image** → deploy code as Docker container.

👉 Select **Author from scratch**.

The screenshot shows the 'Create function' wizard in the AWS Lambda console. The top navigation bar includes 'Lambda > Functions > Create function'. On the right, there's a 'Tutorials' section with a link to 'Create a simple web app'. The main form has three options: 'Author from scratch' (selected), 'Use a blueprint', and 'Container image'. The 'Author from scratch' section contains fields for 'Function name' (set to 'bannerfunction'), 'Runtime' (set to 'Python 3.13'), 'Architecture' (set to 'x86_64'), and 'Permissions' (with a note about default execution role creation). Below these are sections for 'Additional configurations' and 'Change default execution role'. At the bottom right are 'Cancel' and 'Create function' buttons.

5. Configure Basic Settings

- o **Function name:** Enter a unique name (e.g., SampleLambda).
- o **Runtime:** Choose a runtime (Python, Go, etc. → example: Python 3.12).
- o **Permissions (Execution Role):**

- o Create a new role with basic Lambda permissions (recommended if you're new).
- o Or choose an existing IAM role if you already have one.

6. Click Create Function

Connect your function to a VPC to access private resources during invocation.
 Enable

Security & governance

Code signing | [Info](#)
 Use code signing configurations to ensure that the code has been signed by an approved source and has not been altered since signing.
 Enable

Encryption with an AWS KMS customer managed key | [Info](#)
 By default, Lambda encrypts the .zip file archive using an AWS owned key.
 Enable

Tags | [Info](#)
 A tag is a label that you assign to an AWS resource. Each tag consists of a key and an optional value. You can use tags to search and filter your resources, track your AWS costs, and enforce attribute-based access control.
 Enable

[Cancel](#) [Create function](#)

Wait a few seconds while AWS provisions the function.

Successfully created the function **bannerfunction**. You can now change its code and configuration. To invoke your function with a test event, choose "Test".

bannerfunction

[Function overview](#) | [Info](#)

[Diagram](#) | [Template](#)

bannerfunction

[Layers \(0\)](#)

[+ Add trigger](#) [+ Add destination](#)

[Throttle](#) [Copy ARN](#) [Actions](#)

[Export to Infrastructure Composer](#) [Download](#)

Description

Last modified 10 seconds ago

Function ARN arn:aws:lambda:us-east-1:01825291125:function:bannerfunction

Function URL | [Info](#)

[Create a simple web app](#)

In this tutorial you will learn how to:

- Build a simple web app, consisting of a Lambda function with a function URL that outputs a webpage
- Invoke your function through its function URL

[Learn more](#) [Start tutorial](#)

[Code](#) | [Test](#) | [Monitor](#) | [Configuration](#) | [Aliases](#) | [Versions](#)

Code source | [Info](#)

[Open in Visual Studio Code](#) | [Upload from](#)

EXPLORER

BANNERFUNCTION

index.mjs

```
index.mjs
1 export const handler = async (event) => {
2   // TODO implement
3   const response = {
4     statusCode: 200,
5     body: JSON.stringify('Hello from Lambda!'),
6   };
7   return response;
}
```

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

7. Add Your Code

- In the **Function code** section, you can:
- Write inline code in the editor.
- Or upload a .zip file.
- Or use **Amazon S3** (if your code is stored there).

Example default code in Js:

The screenshot shows the AWS Lambda Functions console. In the left sidebar, under 'Functions', 'bannerfunction' is selected. The main area displays the function code in a code editor:

```
JS index.mjs
1 export const handler = async (event) => {
2   // TODO implement
3   const response = {
4     statusCode: 200,
5     body: JSON.stringify('Hello from Lambda!'),
6   };
7   return response;
8 };
```

Below the code editor are buttons for 'Deploy' and 'Test'. A message at the top says: "Successfully created the function bannerfunction. You can now change its code and configuration. To invoke your function with a test event, choose 'Test'." On the right side, there's a 'Tutorials' tab with a link to 'Create a simple web app'.

The screenshot shows the same AWS Lambda Functions console as above. The code editor for index.mjs remains the same. A 'Create new test event' dialog is open on the right side:

Create new test event

Event Name: testing_test
Maximum of 25 characters consisting of letters, numbers, dots, hyphens and underscores.

Event sharing settings:

- Private: This event is only available in the Lambda Console and to the event creator. You can configure a total of ten events. [Learn more](#)
- Shareable: This event is available to IAM users within the same account who have permissions to access and use shareable events. [Learn more](#)

Template - optional: Hello World

Event JSON:

```
1 { "key1": "value1",
2  "key2": "value2",
3  "key3": "value3"
4 }
```

On the right, the 'Tutorials' tab is still visible with the 'Create a simple web app' link.

8. Configure Test Event

- Click **Test** → **Configure test event**.

The screenshot shows the AWS Lambda console interface. On the left, there's a sidebar with navigation links like 'Lambda', 'Functions', and 'bannerfunction'. Below that is a code editor for 'index.mjs' containing a simple Node.js script. To the right of the code editor is a 'Create new test event' dialog box. The 'Event Name' field is set to 'testing_test'. Under 'Event sharing settings', the 'Private' radio button is selected. In the 'Event JSON' section, there's a text area with the following JSON:

```
1 {  
2   "key1": "value1",  
3   "key2": "value2",  
4   "key3": "value3"  
5 }
```

At the bottom of the dialog, a message says 'Test event is saved successfully.' On the far right, there's a 'Tutorials' sidebar with a link to 'Create a simple web app'.

- Give it a name (e.g., `TestEvent`).
- Keep the default event JSON or modify as needed.
- Save.

9. Run the Function

- Click **Test** again.
Check the execution results (output, logs, and status)

Lambda > Functions > bannerfunction

EXPLORER
BANNERFUNCTION
JS index.mjs

JS index.mjs > ...
9

Create new test event

Event Name: testing_test

Event sharing settings: Private

PROBLEMS OUTPUT CODE REFERENCE LOG TERMINAL

Status: Succeeded
Test Event Name: testing_test

DEPLOY

Deploy (Ctrl+Shift+U)
Test (Ctrl+Shift+I)

TEST EVENTS [SELECTED: TESTING_TEST] +
+ Create new test event
v Private saved events
testing_test >

ENVIRONMENT VARIABLES

Code properties [Info](#)

Package size: 295 byte

Encryption with AWS KMS customer managed KMS key [Info](#)

SHA256 hash: q8E7Nexf5xxhKT9/d4bGpAYOXJYFAUjJ0UDj8OivK8E=

Last modified: 4 minutes ago

Execution Results

Function Logs:

```
START RequestId: 266832b5-2bbc-4268-a330-e75f409bac4a Version: $LATEST
END RequestId: 266832b5-2bbc-4268-a330-e75f409bac4a
REPORT RequestId: 266832b5-2bbc-4268-a330-e75f409bac4a Duration: 17.61 ms Billed Duration: 159 ms Memory Size: 128 MB Max Memory Used: 72 MB
Init Duration: 141.37 ms
Request ID: 266832b5-2bbc-4268-a330-e75f409bac4a
```

Test event is saved successfully.

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

Info [Tutorials](#)

Learn how to implement common use cases in AWS Lambda.

Create a simple web app

In this tutorial you will learn how to:

- Build a simple web app, consisting of a Lambda function with a function URL that outputs a webpage
- Invoke your function through its function URL

[Learn more](#) [Start tutorial](#)

Practical 5: Creating an IAM (Identity and Access Management) user in AWS

1. Open the IAM dashboard

The screenshot shows the AWS IAM Dashboard. On the left sidebar, there are sections for Identity and Access Management (IAM), Dashboard, Access management (User groups, Users, Roles, Policies, Identity providers, Account settings, Root access management, Temporary delegation requests), Access reports (Access Analyzer, Resource analysis, Unused access, Analyzer settings, Credential report, Organization activity, Service control policies, Resource control policies), IAM Identity Center, and AWS Organizations.

The main content area includes:

- Security recommendations:** 2 items:
 - Root user has MFA: Having multi-factor authentication (MFA) for the root user improves security for this account.
 - Root user has no active access keys: Using access keys attached to an IAM user instead of the root user improves security.
- IAM resources:** Resources in this AWS Account:

User groups	Users	Roles	Policies	Identity providers
1	4	7	2	0
- What's new:** Updates for features in IAM:
 - Amazon Bedrock introduces API keys for streamlined development. 4 months ago
 - AWS Service Reference now supports annotations for service actions. 5 months ago
 - AWS expands resource control policies (RCPs) support to two additional services. 5 months ago
 - AWS IAM now enforces MFA for root users across all account types. 5 months ago[View all](#)
- AWS Account:** Account ID: 018252911125, Account Alias: Create, Sign-in URL for IAM users in this account: https://018252911125.signin.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.
- Additional information:** Security best practices in IAM, IAM documentation, Videos, blog posts, and additional resources.

2. Go to Users Section

In the left sidebar, click on Users. You will see a list of all existing users. Click “Create user”

The screenshot shows the "Specify user details" step of the IAM User creation wizard. The left sidebar shows the steps: Step 1 (Specify user details, selected), Step 2 (Set permissions), and Step 3 (Review and create).

The main form fields include:

- User details:**
 - User name:** A text input field with placeholder text: "The user name can have up to 64 characters. Valid characters: A-Z, a-z, 0-9, and + = , . @ _ - (hyphen)".
 - Provide user access to the AWS Management Console - optional**: A checkbox with a note: "In addition to console access, users with SigninLocalDevelopmentAccess permissions can use the same console credentials for programmatic access without the need for access keys."
 - If you are creating programmatic access through access keys or service-specific credentials for AWS CodeCommit or Amazon Keyspaces, you can generate them after you create this IAM user.**: A checkbox with a note: "Learn more".
- Cancel** and **Next** buttons at the bottom right.

- Step 1 Specify user details
- Step 2 Set permissions
- Step 3 Review and create
- Step 4 Retrieve password

Specify user details

User details

User name

The user name can have up to 64 characters. Valid characters: A-Z, a-z, 0-9, and + = , _ - (hyphen)

Provide user access to the AWS Management Console - optional

In addition to console access, users with SignInLocalDevelopmentAccess permissions can use the same console credentials for programmatic access without the need for access keys.

Console password

Autogenerated password

You can view the password after you create the user.

Custom password

Enter a custom password for the user.

- Must be at least 8 characters long
- Must include at least three of the following mix of character types: uppercase letters (A-Z), lowercase letters (a-z), numbers (0-9), and symbols ! @ # \$ % ^ & () _ + - (hyphen) = [] { } | ^

Show password

Users must create a new password at next sign-in - Recommended

Users automatically get the IAMUserChangePassword policy to allow them to change their own password.

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

[Cancel](#)
[Next](#)

3. Set Permissions

Choose Attach policies directly → assign permissions manually (e.g., AmazonS3FullAccess, AdministratorAccess, etc.)

- Step 1 Specify user details
- Step 2 Set permissions
- Step 3 Review and create
- Step 4 Retrieve password

Review and create

Review your choices. After you create the user, you can view and download the autogenerated password, if enabled.

User details

User name
Adhvay

Console password type
Autogenerated

Require password reset
Yes

Permissions summary

Name ↗

Type

Used as

AccessAnalyzerServiceRolePolicy	AWS managed	Permissions policy
IAMUserChangePassword	AWS managed	Permissions policy

IAMUserChangePassword

Tags - optional

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.

No tags associated with the resource.

Add new tag

You can add up to 50 more tags.

[Cancel](#)
[Previous](#)
[Create user](#)

Finally click “Create User”

User created successfully

You can view and download the user's password and email instructions for signing in to the AWS Management Console.

[View user](#)

X

- Step 1 Specify user details
- Step 2 Set permissions
- Step 3 Review and create
- Step 4 Retrieve password

Retrieve password

You can view and download the user's password below or email users instructions for signing in to the AWS Management Console. This is the only time you can view and download this password.

Console sign-in details

[Email sign-in instructions](#)

Console sign-in URL

User name

Console password

Show

[Cancel](#)
[Download .csv file](#)
[Return to users list](#)

Practical :-6

Objective:- To secure an AWS IAM user account by enabling Multi-Factor Authentication (MFA)

Step 1 :-Open “Users”

The screenshot shows the AWS IAM Users page. On the left, there's a navigation sidebar with options like Dashboard, Access management (User groups, Users, Roles, Policies, Identity providers, Account settings, Root access management, Temporary delegation requests), and Access reports (Access Analyzer, Resource analysis). The main area displays a table titled "Users (1) Info". The table has columns: User name, Path, Group, Last activity, MFA, Password age, Console last sign-in, Access key ID, Active key age, and Access key last used. One row is present, showing "Adhvay_Banerjee" under User name, with other fields like Last activity (0), MFA (Enabled without MFA), and Console last sign-in (2 minutes) filled.

The screenshot shows the AWS IAM User details page for "Adhvay_Banerjee". The left sidebar is identical to the previous screenshot. The main area is divided into sections: Summary, Permissions, Groups, Tags, Security credentials, and Last Accessed. The Summary section shows ARN (arn:aws:iam::018252911125:user/Adhvay_Banerjee), Created (November 29, 2025, 01:30 (UTC+05:30)), Console access (Enabled without MFA), and Last console sign-in (Never). The Permissions section shows two attached policies: "AmazonS3FullAccess" and "IAMUserChangePassword", both of which are AWS managed and attached directly. There are also sections for "Permissions boundary (not set)" and "Generate policy based on CloudTrail events". A note at the bottom states "No requests to generate a policy in the past 7 days."

Step 2. In the left navigation panel, select Users. Click the username for which you want to enable MFA.

- Go to the “Security Credentials” Tab
- After opening the user’s profile, click on Security credentials.
- Scroll down to the section Multi-Factor Authentication (MFA).

The screenshot shows the AWS IAM User Security Credentials page for a user named Adhvay_Banerjee. The 'Security credentials' tab is selected. The 'Multi-factor authentication (MFA)' section is visible, showing that no MFA devices are assigned. The 'Access keys' section shows two access keys have been created. The 'API keys for Amazon Bedrock' section shows zero API keys.

Step 3: Click “Assign MFA Device”

- A popup will open with 3 options:
 1. FIDO2 Security Key
 2. Authenticator App (Google Authenticator / Authy / Microsoft Authenticator)
 3. Hardware TOTP Device

For most labs, choose Authenticator App for simplicity.

Select MFA device Info

MFA device name

Device name

This name will be used within the identifying ARN for this device.

Phone

Maximum 64 characters. Valid characters: A-Z, a-z, 0-9, and + = , . @ _ - (hyphen)

MFA device

Device options

In addition to username and password, you will use this device to authenticate into your account.



Passkey or security key

Authenticate using your fingerprint, face, or screen lock. Create a passkey on this device or use another device, like a FIDO2 security key.



Authenticator app

Authenticate using a code generated by an app installed on your mobile device or computer.



Hardware TOTP token

Authenticate using a code generated by Hardware TOTP token or other hardware devices.

[Cancel](#)

[Next](#)

Step 4:-Select “Authenticator App” and Continue

- Click Continue.
- AWS will show a QR code for MFA enrollment.

Step 5:-Open your Authenticator App

You can use any app:

- Google Authenticator
- Authy
- Microsoft Authenticator
- LastPass Authenticator

Click Add Account → Scan QR Code.

The app will generate a 6-digit one-time password (OTP) that refreshes every 30 seconds.

- Step 1
Select MFA device
- Step 2
Set up device

Set up device Info

Authenticator app

A virtual MFA device is an application running on your device that you can configure by scanning a QR code.

1

Install a compatible application such as Google Authenticator, Duo Mobile, or Authy app on your mobile device or computer.

[See a list of compatible applications](#)

2



Open your authenticator app, choose **Show QR code** on this page, then use the app to scan the code. Alternatively, you can type a secret key. [Show secret key](#)

3

Type two consecutive MFA codes below

Enter a code from your virtual app below

MFA Code 1

Wait 30 seconds, and enter a second code entry.

MFA Code 2

[Cancel](#)

[Previous](#)

Add MFA



Identity and Access Management (IAM)

[Search IAM](#)

Dashboard

Access management

User groups

Users

Roles

Policies

Identity providers

Account settings

Root access management

Temporary delegation requests

New

Access reports

Access Analyzer

Resource analysis New

Unused access

Analyzer settings

Credential report

Organization activity

Service control policies

Resource control policies

IAM Identity Center

AWS Organizations

MFA device assigned

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

Adhvay_Banerjee Info

[Delete](#)

Summary

ARN

[arn:aws:iam::018252911125:user/Adhvay_Banerjee](#)

Created

November 29, 2025, 01:30 (UTC+05:30)

Console access

Enabled with MFA

Last console sign-in

Never

Access key 1

[Create access key](#)

Permissions

Groups

Tags

Security credentials

Last Accessed

Console sign-in

Console sign-in link

<https://018252911125.signin.aws.amazon.com/console>

[Manage console access](#)

Console password

Updated 8 minutes ago (2025-11-29 01:30 GMT+5:30)

Last console sign-in

Never

Multi-factor authentication (MFA) (1)

Use MFA to increase the security of your AWS environment. Signing in with MFA requires an authentication code from an MFA device. Each user can have a maximum of 8 MFA devices assigned. [Learn more](#)

[Remove](#)

[Resync](#)

Assign MFA device

Access keys (0)

Use access keys to send programmatic calls to AWS from the AWS CLI, AWS Tools for PowerShell, AWS SDKs, or direct AWS API calls. You can have a maximum of two access keys (active or inactive) at a time. [Learn more](#)

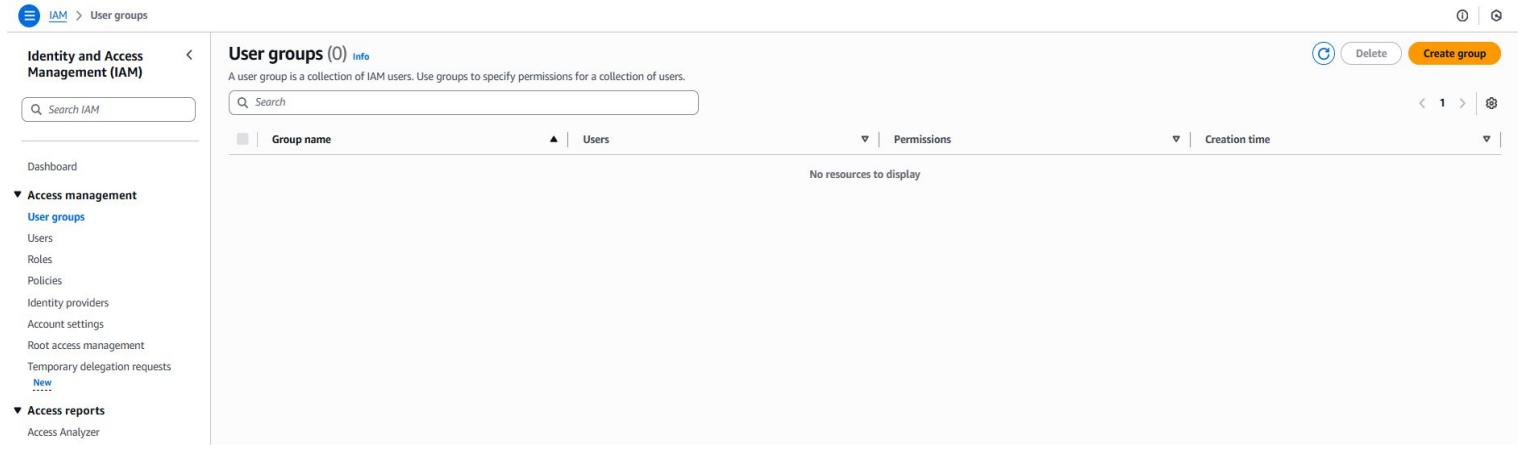
[Create access key](#)

No access keys. As a best practice, avoid using long-term credentials like access keys. Instead, use tools which provide short term credentials. [Learn more](#)

Practical:-7

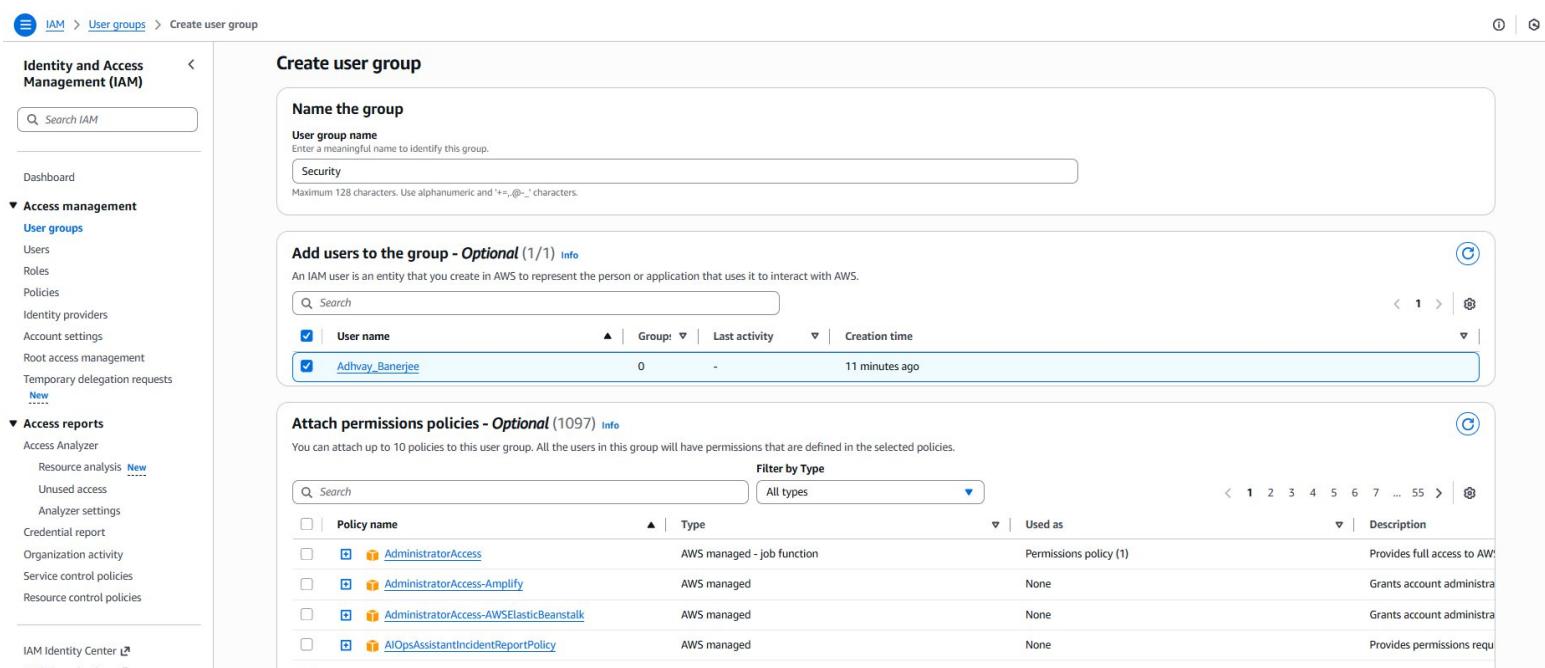
Objective: To create a user group in AWS IAM

**Step 1:- Go to User Groups Section:
In the left-hand sidebar, click on User groups.**



The screenshot shows the AWS IAM User Groups page. The left sidebar has sections for Identity and Access Management (IAM) like Dashboard, Access management (User groups, Users, Roles, Policies, Identity providers, Account settings, Root access management, Temporary delegation requests), and Access reports (Access Analyzer). The main area shows 'User groups (0)' with a note: 'A user group is a collection of IAM users. Use groups to specify permissions for a collection of users.' There's a search bar, a table header with columns 'Group name' (sorted by 'Users'), 'Permissions', and 'Creation time', and a message 'No resources to display'. Action buttons at the top right include 'Delete' and 'Create group'.

Step 3:- Click on “Create group”:
On the User Groups page, click the “Create group” button to start creating a new group



The screenshot shows the 'Create user group' page. The left sidebar includes sections for Identity and Access Management (IAM) (Dashboard, Access management, User groups, Users, Roles, Policies, Identity providers, Account settings, Root access management, Temporary delegation requests), Access reports (Access Analyzer, Resource analysis, Unused access, Analyzer settings, Credential report, Organization activity, Service control policies, Resource control policies), and IAM Identity Center. The main area has a 'Name the group' section with a 'User group name' input field containing 'Security'. Below it is an 'Add users to the group - Optional (1/1)' section showing 'Adhavy_Banerjee' as the added user. The final section is 'Attach permissions policies - Optional (1097)' which lists several AWS managed policies: 'AdministratorAccess' (AWS managed - job function, Permissions policy (1), Provides full access to AW), 'AdministratorAccess-Amplify' (AWS managed, None, Grants account administra), 'AdministratorAccess-AWSElasticBeanstalk' (AWS managed, None, Grants account administra), and 'AIOpsAssistantIncidentReportPolicy' (AWS managed, None, Provides permissions requ).

Step 4:- Enter Group Name:

Type a unique name for your group (for example, Developers, Admins, or ReadOnlyUsers).

For Example, here Administrators.

Step 5:- Attach Permissions Policies (Optional): You can choose policies to attach to this group, such as:

- AmazonS3FullAccess
- AmazonEC2ReadOnlyAccess
- AdministratorAccess

If you want to add permissions later, you can skip this step and click Next.

The screenshot shows the AWS IAM User groups page. The left sidebar includes options like Identity and Access Management (IAM), Dashboard, Access management (User groups, Users, Roles, Policies, Identity providers, Account settings, Root access management, Temporary delegation requests, New), and Access reports (Access Analyzer, Resource analysis, Unused access, Analyzer settings, Credential report, Organization activity). The main content area displays a table for User groups. A green banner at the top right says "Sec user group created." The table has columns for Group name (with a checkbox and "Sec" selected), Users (with an upward arrow icon), Permissions (with a downward arrow icon and "Defined" status), and Creation time (with a downward arrow icon and "Now" status). There are also "View group", "Delete", and "Create group" buttons at the top right of the table area.

Practical:-8

Objective:-To create a security role in AWS IAM

Step 1:- Go to Roles Section:

In the left-hand navigation pane, click on Roles.

The screenshot shows the AWS IAM Roles page. At the top, there is a green banner with the text "Sec user group created." Below this, the main title is "Roles (7) info". A sub-instruction says "An IAM role is an identity you can create that has specific permissions with credentials that are valid for short durations. Roles can be assumed by entities that you trust." There is a search bar labeled "Search". To the right, there are buttons for "View group", "Delete", and "Create role". The main area displays a table of roles with columns for "Role name", "Trusted entities", and "Last activity". The roles listed are: AWSServiceRoleForNATGateway, AWSServiceRoleForResourceExplorer, AWSserviceRoleForSupport, AWSServiceRoleForTrustedAdvisor, bannerfunction-role-sa0w2pl1, gfyrbvurelbvks-role-gmhideso, and QA. Below the table, there are three sections: "Roles Anywhere" (info), "Access AWS from your non AWS workloads" (info), and "X.509 Standard" (info). On the far right, there is a "Temporary credentials" section with a "Manage" button.

Step 2:- Click on “Create role”:

On the Roles page, click the “Create role” button to start the process.

Step 3:- Select Trusted Entity Type:

Choose who will use the role, such as:

- AWS Service (e.g., EC2, Lambda)
- Another AWS Account
- Web Identity or SAML 2.0 Federation

Click Next after selecting the appropriate option.

Step 1
 Select trusted entity

Step 2
 Add permissions

Step 3
 Name, review, and create

Select trusted entity Info

Trusted entity type

- AWS service Allow AWS services like EC2, Lambda, or others to perform actions in this account.
- AWS account Allow entities in other AWS accounts belonging to you or a 3rd party to perform actions in this account.
- Web identity Allows users federated by the specified external web identity provider to assume this role to perform actions in this account.
- SAML 2.0 federation Allow users federated with SAML 2.0 from a corporate directory to perform actions in this account.
- Custom trust policy Create a custom trust policy to enable others to perform actions in this account.

Use case
 Allow an AWS service like EC2, Lambda, or others to perform actions in this account.

Service or use case

EC2

Choose a use case for the specified service.

Use case

- EC2 Allows EC2 instances to call AWS services on your behalf.
- EC2 Role for AWS Systems Manager Allows EC2 instances to call AWS services like CloudWatch and Systems Manager on your behalf.
- EC2 Spot Fleet Role Allows EC2 Spot Fleet to request and terminate Spot Instances on your behalf.
- EC2 - Spot Fleet Auto Scaling Allows Auto Scaling to access and update EC2 spot fleets on your behalf.
- EC2 - Spot Fleet Tagging Allows EC2 to launch spot instances and attach tags to the launched instances on your behalf.
- EC2 - Spot Instances Allows EC2 Spot Instances to launch and manage spot instances on your behalf.
- EC2 - Spot Fleet Allows EC2 Spot Fleet to launch and manage spot fleet instances on your behalf.
- EC2 - Scheduled Instances Allows EC2 Scheduled Instances to manage instances on your behalf.

Step 4:-Attach Permissions Policies:

Select the permissions policies that define what actions the role can perform (for example, AmazonS3FullAccess or AmazonEC2FullAccess)

Step 1
 Select trusted entity

Step 2
 Add permissions

Step 3
 Name, review, and create

Add permissions Info

Permissions policies (1/1097) Info

Choose one or more policies to attach to your new role.

Policy name	Type	Description
<input type="checkbox"/> AdministratorAccess	AWS managed - job function	Provides full access to AWS services an...
<input type="checkbox"/> AdministratorAccess-Amplify	AWS managed	Grants account administrative permissi...
<input type="checkbox"/> AdministratorAccess-AWSElasticBeanstalk	AWS managed	Grants account administrative permissi...
<input type="checkbox"/> AIOpsAssistantIncidentReportPolicy	AWS managed	Provides permissions required by the A...
<input type="checkbox"/> AIOpsAssistantPolicy	AWS managed	Provides ReadOnly permissions require...
<input type="checkbox"/> AIOpsConsoleAdminPolicy	AWS managed	Grants full access to Amazon AI Opera...
<input type="checkbox"/> AIOpsOperatorAccess	AWS managed	Grants access to the Amazon AI Opera...
<input type="checkbox"/> AIOpsReadOnlyAccess	AWS managed	Grants ReadOnly permissions to the A...
<input type="checkbox"/> AlexaForBusinessDeviceSetup	AWS managed	Provide device setup access to AlexaFo...
<input type="checkbox"/> AlexaForBusinessFullAccess	AWS managed	Grants full access to AlexaForBusiness ...
<input type="checkbox"/> AlexaForBusinessGatewayExecution	AWS managed	Provide gateway execution access to Al...
<input type="checkbox"/> AlexaForBusinessLifesizeDelegatedAccessPolicy	AWS managed	Provide access to Lifesize AVS devices
<input type="checkbox"/> AlexaForBusinessPolyDelegatedAccessPolicy	AWS managed	Provide access to Poly AVS devices

Step 5:- Name and Review the Role:

Enter a role name (for example, EC2SecurityRole or LambdaAccessRole) and review all selected settings.

Step 1

Stage 2

Add permissions

○ Name, review, and create

Name, review, and create

Role details

Role name

Enter a meaningful name to identify this role.

Security|

Maximum 64 characters. Use alpha

Description

Description	Add a short explanation for this role.
Allows EC2 instances to call AWS services on your behalf.	
<p>Maximum 1000 characters. Use letters (A-Z and a-z), numbers (0-9), tabs, new lines, or any of the following characters: _+=-, @/\{()\}!#%\$^@`</p>	

Step 1: Select trusted entities

Trust policy

```
1 [ {  
2     "Version": "2012-10-17",  
3     "Statement": [  
4         {  
5             "Effect": "Allow",  
6             "Action": [  
7                 "sts:AssumeRole"  
8             ],  
9             "Principal": {  
10                 "Service": [  
11                     "ec2.amazonaws.c  
12                 ]  
13             }  
14         }  
15     ]  
16 }
```

Step 2: Add permissions

Permissions policy summary

Policy name (2)

Typo

v | Attached

Step 6:- Create the Role:
Click Create role to finish.

Identity and Access Management (IAM)

Role Security created.

Roles (8) Info

An IAM role is an identity you can create that has specific permissions with credentials that are valid for short durations. Roles can be assumed by entities that you trust.

<input type="checkbox"/>	Role name	Trusted entities	Last activity
<input type="checkbox"/>	AWSServiceRoleForNATGateway	AWS Service: ec2-nat-gateway (Service)	33 minutes ago
<input type="checkbox"/>	AWSServiceRoleForResourceExplorer	AWS Service: resource-explorer-2 (Service)	15 minutes ago
<input type="checkbox"/>	AWSServiceRoleForSupport	AWS Service: support (Service-Linker)	-
<input type="checkbox"/>	AWSServiceRoleForTrustedAdvisor	AWS Service: trustedadvisor (Service)	-
<input type="checkbox"/>	bannerfunction-role-sa0w2pl1	AWS Service: lambda	19 days ago
<input type="checkbox"/>	gfyerbvurelbvks-role-gmhideso	AWS Service: lambda	-
<input type="checkbox"/>	QA	AWS Service: ec2	-
<input type="checkbox"/>	Security	AWS Service: ec2	-

Roles Anywhere Info

Authenticate your non AWS workloads and securely provide access to AWS services.



Access AWS from your non AWS workloads

Operate your non AWS workloads using the same authentication and authorization strategy that you use within AWS.



X.509 Standard

Use your own existing PKI infrastructure or use [AWS Certificate Manager Private Certificate Authority](#) to authenticate identities.



Temporary credentials

Use temporary credentials with ease and benefit from the enhanced security they provide.

View role

Delete

Create role

Practical :- 9

Objective:- To understand how to design and create a Virtual Private Cloud (VPC) in AWS.

Step 1. Open VPC Dashboard

- Sign in to AWS Console.
- Search VPC in the services search bar.
- Click VPC Dashboard.

The screenshot shows the AWS VPC Dashboard. On the left, there's a navigation sidebar with sections like 'Virtual private cloud' (Your VPCs, Subnets, Route tables, Internet gateways, Egress-only internet gateways, Carrier gateways, DHCP option sets, Elastic IPs, Managed prefix lists, NAT gateways, Peering connections, Route servers), 'Security' (Network ACLs, Security groups), and 'PrivateLink and Lattice' (Getting started, Endpoints, Endpoint services, Service networks, Lattice services). The main area has tabs for 'Create VPC' and 'Launch EC2 Instances'. It displays 'Resources by Region' (N. Virginia) with counts for VPCs (1), Subnets (6), Route Tables (1), Internet Gateways (1), Egress-only Internet Gateways (0), DHCP option sets (1), and Endpoints (0). There are also sections for NAT Gateways (0), VPC Peering Connections (0), Network ACLs (1), Security Groups (3), Customer Gateways (0), Virtual Private Gateways (1), and Site-to-Site VPN Connections (0). On the right, there are boxes for 'Service Health' (refresh button), 'Settings' (Block Public Access, Zones, Console Experiments), 'Additional Information' (VPC Documentation, All VPC Resources, Forums, Report an Issue), and 'AWS Network Manager' (Get started with Network Manager, Site-to-Site VPN Connections).

Step 2. Start Creating a VPC

- On the left menu, select Your VPCs.
- Click Create VPC.

You will get two options:

1. VPC Only → Create VPC manually
2. VPC and more → Automatically create VPC with subnets, IGW, route tables, etc.

Choose VPC Only for full control

Create VPC Info

A VPC is an isolated portion of the AWS Cloud populated by AWS objects, such as Amazon EC2 instances.

VPC settings

Resources to create Info

Create only the VPC resource or the VPC and other networking resources.

 VPC only VPC and more

Name tag - optional

Creates a tag with a key of 'Name' and a value that you specify.

MYvpc

IPv4 CIDR block Info

- IPv4 CIDR manual input
- IPAM-allocated IPv4 CIDR block

IPv4 CIDR

10.0.0.0/16

CIDR block size must be between /16 and /28.

IPv6 CIDR block Info

- No IPv6 CIDR block
- IPAM-allocated IPv6 CIDR block
- Amazon-provided IPv6 CIDR block
- IPv6 CIDR owned by me

Tenancy Info

Default

VPC encryption control (\$ - new) Info

Monitor mode provides visibility into encryption status without blocking traffic. Enforce mode prevents unencrypted traffic. Additional charges apply

 None Monitor mode

See which resources in your VPC are unencrypted but allow the creation of unencrypted resources.

 Enforce mode

Requires all resources, except exclusions, in your VPC to be encryption-capable and blocks creation of unencrypted resources.

Tags

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

Key

 Name

Value - optional

 MYvpc[Remove tag](#)

⌚ You successfully created **vpc-0c3a476b1a18805a7 / MYvpc**

vpc-0c3a476b1a18805a7 / MYvpc

Actions ▾

Details Info

VPC ID
 vpc-0c3a476b1a18805a7

DNS resolution
Enabled

Main network ACL
acl-036e6dd8f5333de01

IPv6 CIDR (Network border group)
-

Encryption control ID
-

State
 Available

Tenancy
default

Default VPC
No

Network Address Usage metrics
Disabled

Encryption control mode
-

Block Public Access
 Off

DHCP option set
dopt-0844d923f3579dd97

IPv4 CIDR
10.0.0.0/16

Route 53 Resolver DNS Firewall rule groups
-

DNS hostnames
Disabled

Main route table
rtb-0d08dd78c975602e2

IPv6 pool
-

Owner ID
 018252911125

Resource map

CIDRs

Flow logs

Tags

Integrations

Resource map Info

Show all details

VPC

Your AWS virtual network

MYvpc

Subnets (0)

Subnets within this VPC

Route tables (1)

Route network traffic to resources

rtb-0d08dd78c975602e2

Network Connections (0)

Connections to other networks

VPC dashboard

Subnets (6) Info

Find subnets by attribute or tag

Name	Subnet ID	State	VPC	Block Public...	IPv4 CIDR	IPv6 CIDR	IPv6 CIDR association ID
-	subnet-07b82a2b-f038f96d	<input checked="" type="radio"/> Available	vpc-0505a753f6ca9600	<input type="radio"/> Off	172.31.32.0/20	-	-
-	subnet-0c4564fcfc6f77de0	<input checked="" type="radio"/> Available	vpc-0505a753f6ca9600	<input type="radio"/> Off	172.31.0.0/20	-	-
-	subnet-0dcab66f95b21f36f	<input checked="" type="radio"/> Available	vpc-0505a753f6ca9600	<input type="radio"/> Off	172.31.80.0/20	-	-
-	subnet-0cab952223f097fa6	<input checked="" type="radio"/> Available	vpc-0505a753f6ca9600	<input type="radio"/> Off	172.31.16.0/20	-	-
-	subnet-0f6049bf55706840	<input checked="" type="radio"/> Available	vpc-0505a753f6ca9600	<input type="radio"/> Off	172.31.48.0/20	-	-
-	subnet-04310741ab7640e80	<input checked="" type="radio"/> Available	vpc-0505a753f6ca9600	<input type="radio"/> Off	172.31.64.0/20	-	-

Last updated
4 minutes ago

Actions ▾

Create subnet

1

2

3

4

5

6

7

8

9

10

11

12

13

14

15

16

17

18

19

20

21

22

23

24

25

26

27

28

29

30

31

32

33

34

35

36

37

38

39

40

41

42

43

44

45

46

47

48

49

50

51

52

53

54

55

56

57

58

59

60

61

62

63

64

65

66

67

68

69

70

71

72

73

74

75

76

77

78

79

80

81

82

83

84

85

86

87

88

89

90

91

92

93

94

95

96

97

98

99

100

101

102

103

104

105

106

107

108

109

110

111

112

113

114

115

116

117

118

119

120

121

122

123

124

125

126

127

128

129

130

131

132

133

134

135

136

137

138

139

140

141

142

143

144

145

146

147

148

149

150

151

152

153

154

155

156

157

158

159

160

161

162

163

164

165

166

167

168

169

170

171

172

173

174

175

176

177

178

179

180

181

Step 3: Create Subnet

Create subnet Info

VPC

VPC ID

Create subnets in this VPC.

vpc-0c3a476b1a18805a7 (MYvpc)



Associated VPC CIDRs

IPv4 CIDRs

10.0.0.0/16

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.

my-subnet-01

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.

No preference



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.

10.0.0.0/16



IPv4 subnet CIDR block

10.0.0.0/20



▼ Tags - optional

No tags associated with the resource.

Add new tag

VPC dashboard < AWS Global View Subnets

You have successfully created 1 subnet: subnet-0fe9a532267bc41be

Subnets (1) Info Last updated less than a minute ago

Filter by VPC	Name	Subnet ID	State	VPC	Block Public...	IPv4 CIDR	IPv6 CIDR	IPv6 CIDR association ID
	-	subnet-0fe9a532267bc41be	Available	vpc-0c3a476b1a18805a7 MYvpc	Off	10.0.0.0/20	-	-

Step 4: Create Internet Gateways

Internet gateways (1) <small>Info</small>					
<input type="text"/> Find internet gateways by attribute or tag					
Name	Internet gateway ID	State	VPC ID	Owner	Actions ▾
-	igw-0d0c087b246f1d05f	Attached	vpc-05055a753f6ca9600	018252911125	Edit Actions ▾ Create internet gateway

Virtual private cloud

- Your VPCs
- Subnets
- Route tables
- Internet gateways**
- Egress-only internet gateways
- Carrier gateways
- DHCP option sets
- Elastic IPs
- Managed prefix lists
- NAT gateways
- Peering connections
- Route servers

Security

Create internet gateway Info

An internet gateway is a virtual router that connects a VPC to the internet. To create a new internet gateway specify the name for the gateway below.

Internet gateway settings

Name tag

Creates a tag with a key of 'Name' and a value that you specify.

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.

Key

Value - optional

[X](#)
[Remove](#)
[Add new tag](#)

You can add 49 more tags.

[Cancel](#)
[Create internet gateway](#)

The following internet gateway was created: igw-0a0e4d8252d99cf4e - my_gateway. You can now attach to a VPC to enable the VPC to communicate with the internet.

[Attach to a VPC](#)

igw-0a0e4d8252d99cf4e / my_gateway

[Actions ▾](#)

Details Info

Internet gateway ID

 igw-0a0e4d8252d99cf4e

State

 Detached

VPC ID

 -

Owner

 018252911125

Tags (1)

[Manage tags](#)
[<](#) [1](#) [>](#) [⚙️](#)

Key	Value
Name	my_gateway

The following internet gateway was created: igw-0a0e4d8252d99cf4e - my_gateway. You can now attach to a VPC to enable the VPC to communicate with the internet.

[Attach to a VPC](#)

Attach to VPC (igw-0a0e4d8252d99cf4e) Info

[Actions ▾](#)

VPC

Attach an internet gateway to a VPC to enable the VPC to communicate with the internet. Specify the VPC to attach below.

Available VPCs

Attach the internet gateway to this VPC.

▶ AWS Command Line Interface command

[Cancel](#) [Attach internet gateway](#)

Internet gateway igw-0a0e4d8252d99cf4e successfully attached to vpc-0c3a476b1a18805a7

igw-0a0e4d8252d99cf4e / my_gateway

Details [Info](#)

Internet gateway ID igw-0a0e4d8252d99cf4e	State Attached	VPC ID vpc-0c3a476b1a18805a7 MYvpc	Owner 018252911125
--	--	---	-----------------------

Tags (1)

Search tags	
Key	Value
Name	my_gateway

[Manage tags](#)

Route tables

Route tables (1) [Info](#)

Find route tables by attribute or tag						
Name	Route table ID	Explicit subnet associ...	Edge associations	Main	VPC	Owner ID
-	rtb-01c1f7effcb68f0e	-	-	Yes	vpc-05055a753f6ca9600	018252911125

Step 5: Create Route Table

Create route table [Info](#)

A route table specifies how packets are forwarded between the subnets within your VPC, the internet, and your VPN connection.

Route table settings

Name - optional

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

VPC

The VPC to use for this route table.

Tags

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

No tags associated with the resource.

[Add new tag](#)

You can add 50 more tags.

[Cancel](#) [Create route table](#)

Route table rtb-0b1de253ea2888692 was created successfully.

rtb-0b1de253ea2888692

[Actions](#)

Details		Main	Explicit subnet associations	Edge associations
Route table ID	rtb-0b1de253ea2888692	No	-	-
VPC	vpc-0c3a476b1a18805a7 MYvpc	Owner ID	018252911125	

[Routes](#) | [Subnet associations](#) | [Edge associations](#) | [Route propagation](#) | [Tags](#)

Routes (1)

Filter routes		Both		Edit routes	
Destination	Target	Status	Propagated	Route Origin	Create Route Table
10.0.0.0/16	local	Active	No	CreateRouteTable	

aws | Search [Alt+S] | United States (N. Virginia) | Account ID: 018252911125 | Amitabh@kmu

VPC > Route tables > rtb-0b1de253ea2888692 > Edit routes

Edit routes

Destination	Target	Status	Propagated	Route Origin
10.0.0.0/16	local	Active	No	CreateRouteTable
	<input type="text"/> local	<input type="button" value="X"/>		

[Add route](#)

[Cancel](#) [Preview](#) [Save changes](#)

VPC > Route tables > rtb-0b1de253ea2888692 > Edit routes

Edit routes

Destination	Target	Status	Propagated	Route Origin	
10.0.0.0/16	local	Active	No	CreateRouteTable	
<input type="text"/> 0.0.0.0/0	<input type="button" value="X"/>	-	No	CreateRoute	Remove
<input type="text"/> igw-0a0e4d8252d99cf4e	<input type="button" value="X"/>				

[Add route](#)

[Cancel](#) [Preview](#) [Save changes](#)

VPC > Route tables > rtb-0b1de253ea2888692

Updated routes for rtb-0b1de253ea2888692 successfully

rtb-0b1de253ea2888692

Details

Route table ID	Main	Explicit subnet associations	Edge associations
rtb-0b1de253ea2888692	<input checked="" type="checkbox"/> No	-	-
VPC	Owner ID	Actions	
vpc-0c3a476b1a18805a7 MyVpc	018252911125	Edit	

Routes

Destination	Target	Status	Propagated	Route Origin
0.0.0.0/0	igw-0a0e4d8252d99cf4e	Active	No	Create Route
10.0.0.16	local	Active	No	Create Route Table

Step 6: Create NAT Gateway

VPC > NAT gateways

NAT gateways

No NAT gateways found

Actions

[Create NAT gateway](#)

VPC > NAT gateways > Create NAT gateway

Create NAT gateway

A highly available, managed Network Address Translation (NAT) service that instances in private subnets can use to connect to services in other VPCs, on-premises networks, or the internet.

NAT gateway settings

Name - optional
Create a tag with a key of 'Name' and a value that you specify.

The name can be up to 256 characters long.

Availability mode Info
Choose whether to deploy across all zones in the region or restrict to a single availability zone.

Regional - new
Scales automatically across all regional AZs, simplifying management for multi AZ deployments.

Zonal
Provides granular control within a specific availability zone, adhering to subnet level settings.

VPC
Select a VPC in which to create the regional NAT gateway.

Connectivity type
Select a connectivity type for the NAT gateway.

Public

Private

Method of Elastic IP (EIP) allocation Info
Choose how IP addresses are associated with NAT gateways.

Automatic
AWS automatically manages EIPs and AZ coverage for NAT gateways. This ensures easy scaling—adding AZs automatically allocates EIPs, simplifying management.

Manual
Manually assigns specific IP addresses for compliance or whitelisting. Note: Requires manual scaling to new AZs as workloads expand.

Tags
A tag is a label that you assign to an AWS resource. Each tag consists of a key and an optional value. You can use tags to search and filter your resources or track your AWS costs.
No tags associated with the resource.

[Add new tag](#)

You can add 50 more tags.

[Cancel](#) [Create NAT gateway](#)

VPC > NAT gateways > nat-16a1555850760ed57

NAT gateway nat-16a1555850760ed57 was created successfully.

nat-16a1555850760ed57

[Actions ▾](#)

Virtual private cloud

- Your VPCs
- Subnets
- Route tables
- Internet gateways
- Egress-only internet gateways
- Carrier gateways
- DHCP option sets
- Elastic IPs
- Managed prefix lists
- NAT gateways**
- Peering connections
- Route servers

Security

- Network ACLs
- Security groups

PrivateLink and Lattice

- Getting started
- Endpoints
- Endpoint services
- Service networks

Details

NAT gateway ID nat-16a1555850760ed57	Availability mode Regional	State Pending	State message Info -
NAT gateway ARN arn:aws:ec2:us-east-1:018252911125:natgateway/nat-16a1555850760ed57	Connectivity type Public	Created Saturday, November 29, 2025 at 01:09:40 GMT+5:30	Deleted -
VPC vpc-0c3a476b1a18805a7 / MYvpc	Method of EIP allocation Automatic		

[IP addresses](#) | [Monitoring](#) | [Flow logs](#) | [Tags](#)

Associated IP addresses

IP address	Status	Availability Zone	Allocation ID	Association ID
No associated IP addresses found. If this NAT gateway was recently created with the automatic allocation method, your IP addresses are still being allocated. Click the refresh button to view them.				

[Edit IP address associations](#)