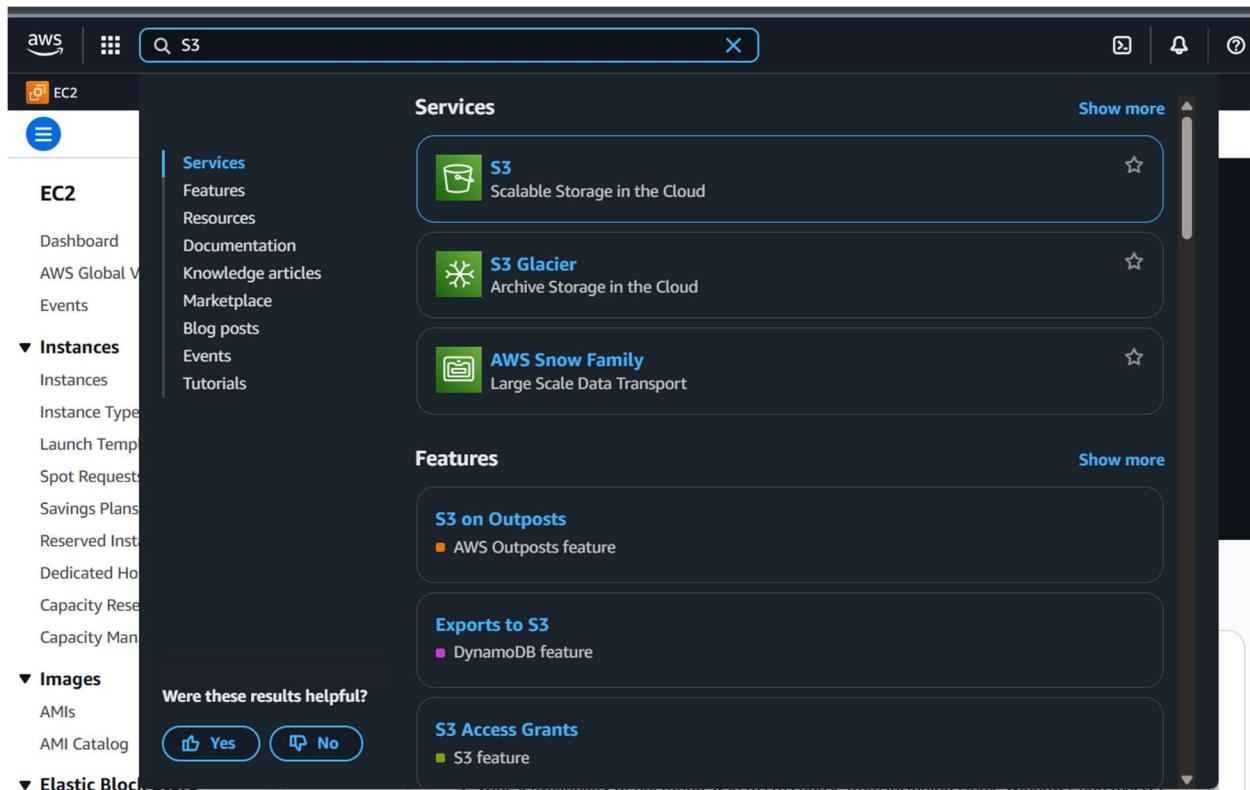


S3(Simple Storage Service)

Steps to Create Buckets and Upload Objects

1) Sign in to AWS Management Console

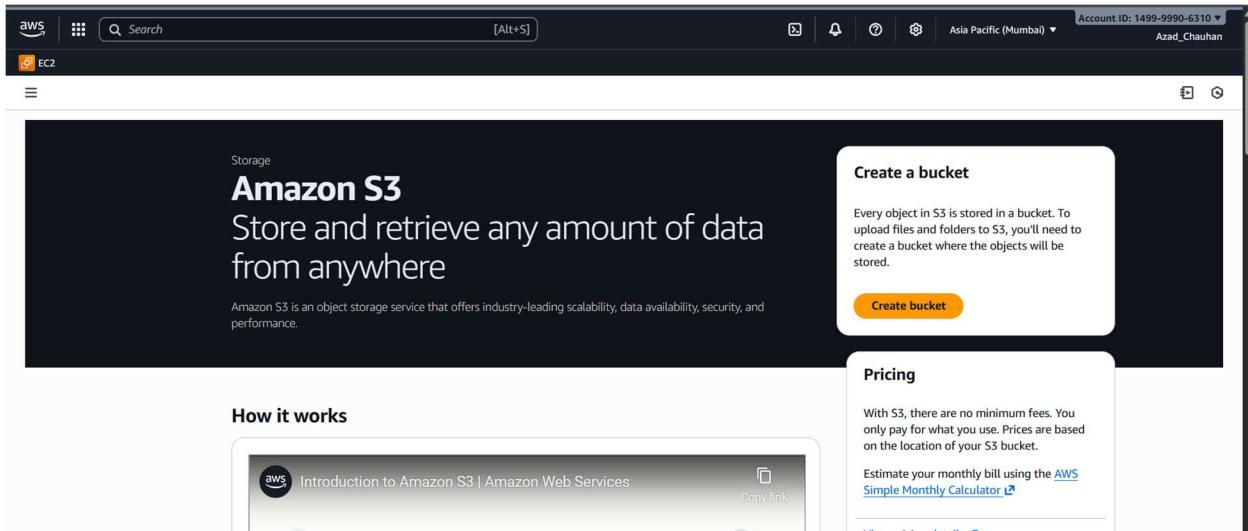
- Go to  AWS Console.
- Login with your AWS credentials.
- In the **Search bar**, type **S3** and open it.



2) Create a New S3 Bucket

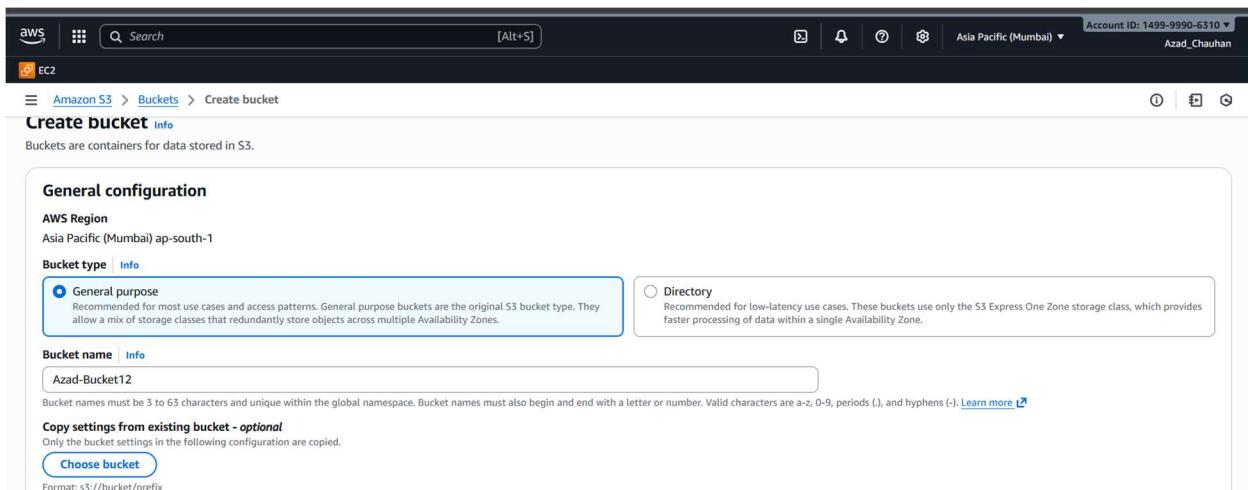
- Click **Create bucket**.

Azad Chauhan



3) Enter a unique **Bucket name** (must be globally unique, e.g. azad-bucket12).

- Choose **AWS Region** (select nearest region for better performance).



4) **Bucket settings:**

- Uncheck **Block all public access** if you want files to be publicly accessible.
- Confirm warning for public access if needed.

The screenshot shows the AWS S3 'Create bucket' interface. At the top, there's a navigation bar with the AWS logo, search bar, and account information (Account ID: 1499-9990-6310, Asia Pacific (Mumbai), Azad_Chauhan). Below the navigation is a breadcrumb trail: Amazon S3 > Buckets > Create bucket. The main content area is titled 'Block Public Access settings for this bucket'. It contains a note about public access being granted through ACLs, bucket policies, and access point policies. A checkbox for 'Block all public access' is checked, with a sub-note explaining it applies to all four settings. Below this are five other checkboxes for different access control options. A warning message in a yellow box states: 'Turning off block all public access might result in this bucket and the objects within becoming public. AWS recommends that you turn on block all public access, unless public access is required for specific and verified use cases such as static website hosting.' A checkbox below the warning is checked, acknowledging the risk. The bottom right corner of the main content area has a vertical scroll bar.

5) Click Create bucket.

- Leave other settings as default (versioning, encryption can be enabled later).

The screenshot shows the 'Create bucket' interface. The top navigation and breadcrumb trail are identical to the previous screenshot. The main content area includes a 'Default encryption' section with a note that server-side encryption is automatically applied to new objects. It shows the 'Encryption type' section where 'Server-side encryption with Amazon S3 managed keys (SSE-S3)' is selected. Below this is the 'Bucket Key' section, which notes that using an S3 Bucket Key for SSE-KMS reduces costs but that S3 Bucket Keys aren't supported for DSSE-KMS. The 'Enable' option is selected. A 'Advanced settings' button is visible at the bottom of this section. A note at the bottom of the page says: 'After creating the bucket, you can upload files and folders to the bucket, and configure additional bucket settings.'

Here We See Buckets (azad-bucket12) Are Successfully Created

The screenshot shows the AWS S3 console interface. At the top, there's a navigation bar with the AWS logo, a search bar, and account information (Account ID: 1499-9990-6310, Region: Asia Pacific (Mumbai), User: Azad_Chauhan). Below the navigation bar, the main header says "Amazon S3 > Buckets". A green success message box displays: "Successfully created bucket 'azad-bucket12'. To upload files and folders, or to configure additional bucket settings, choose View details." There are two tabs: "General purpose buckets" (selected) and "Directory buckets". Under "General purpose buckets", there's a table with one row: "azad-bucket12" (Name), "Asia Pacific (Mumbai)" (AWS Region), and "November 15, 2025, 09:36:49 (UTC+05:30)" (Creation date). To the right of the table are two boxes: "Account snapshot" (updated daily) and "External access summary - new" (updated daily).

6) Upload an Objects (File)

- Open the Buckets.
- Click Upload → Click Add files → (Choose your image/Object from laptop).

Click on Upload.

Here We See Photo is Successfully Upload

The screenshot shows the AWS S3 console after a file upload. At the top, there's a navigation bar with the AWS logo, a search bar, and account information (Account ID: 1499-9990-6310, Region: Asia Pacific (Mumbai), User: Azad_Chauhan). Below the navigation bar, a green success message box displays: "Upload succeeded. For more information, see the Files and folders table." It also includes a note: "After you navigate away from this page, the following information is no longer available." Below the message, there are two sections: "Summary" and "Files and folders". The "Summary" section shows a table with two rows: "Succeeded" (1 file, 121.9 KB (100.00%)) and "Failed" (0 files, 0 B (0%)). The "Files and folders" section shows a table with one row: "1 file" (Name: 1.jpg, Type: Folder, Size: 121.9 KB, Status: Succeeded).

7) Click on Open , Here We See The Uploaded image Succesfully Show But When We Click On Object URL Then We Got Error.

The screenshot shows the AWS S3 console interface. On the left, there's a sidebar titled 'Amazon S3' with sections for 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 area displays an object named '1' in the 'azad-bucket12' bucket. The 'info' tab is selected. The 'Properties' tab is active. The 'Object overview' section contains the following details:

- Owner: 2055eaafdf2f1e04bd499c647e453665aa5eea8b7be596bca399b7ed146398586
- AWS Region: Asia Pacific (Mumbai) ap-south-1
- Last modified: November 15, 2025, 09:48:33 (UTC+05:30)
- Size: 121.9 KB
- Type: (not specified)

Action buttons at the top right include 'Copy S3 URI', 'Download', 'Open', and 'Object actions'.

Error Show Like That

This screenshot shows a browser window with the URL `azad-bucket12.s3.ap-south-1.amazonaws.com/1`. The page content is an XML error response:

```
<Error>
<Code>AccessDenied</Code>
<Message>Access Denied</Message>
<RequestId>C9MSHG0H8SFQTN</RequestId>
<HostId>Sn2Mxsilunq8A50u2B44ph9sNzGo/kLvpincj582zT/lBAtSf1bYwtkndDOMeCQ15gMOPqtHCT6UIZBFvfxCCUdjmw7mk0</HostId>
</Error>
```

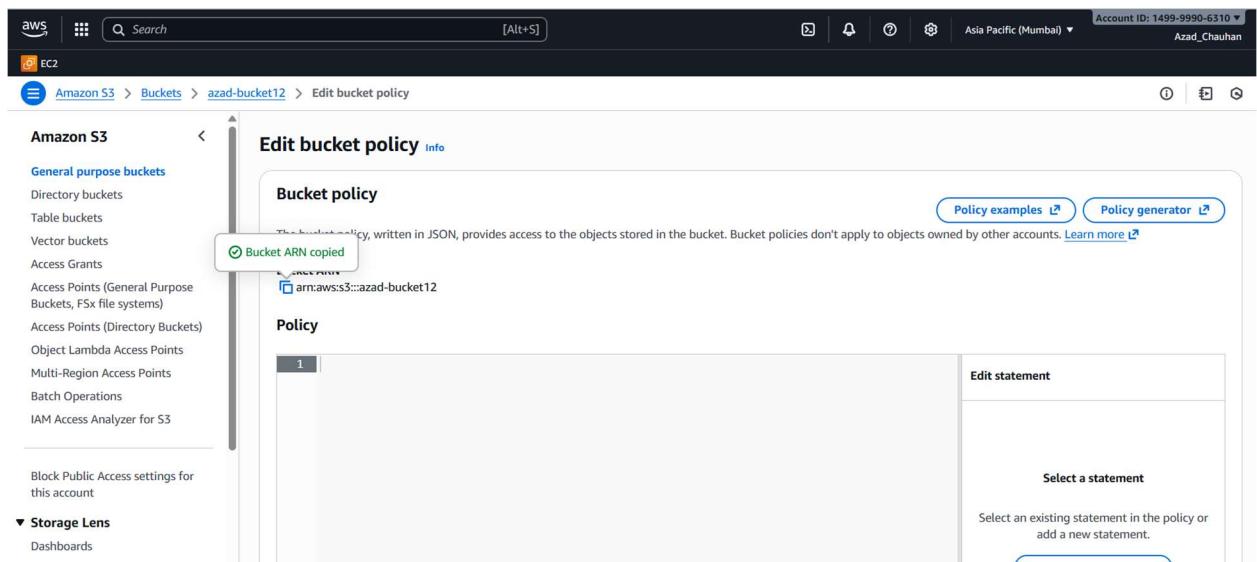
• To Solve The Error We Follow The Following Steps :

8) Here We Again Go To Buckets & Open It

- Click On **Permissions**
- Go to **Bucket Policy** Section & Click On **Edit**
- Paste this **JSON**

9) Here The Question Rays How we create Bucket Policy , Here The Steps For Create Bucket Policy.

- Click On Policy Generator



10) Here The AnotherTab Is Open Automatically

- Like This Here We Perform Following Steps
 - a) Here We Select Policy Type S3 Bucket Policy
 - b) Add Principal as (*), Here * Means All.
 - c) Go to Actions and Select GetObject
 - d) Go to Amazon Resource Name (ARN) Here we Paste BucketARN.
(Ex:- arn:aws:s3:::azad-bucket12) and Add /*)
 - e) Click On AddStatement

Azad Chauhan

aws policymaker.s3.amazonaws.com/policygen.html

AWS Policy Generator

The AWS Policy Generator is a tool that enables you to create policies that control access to Amazon Web Services (AWS) products and resources. For more information about creating policies, see [key concepts in Using AWS Identity and Access Management](#).

Step 1: Select policy type

A Policy is a container for permissions. The different types of policies you can create are an [IAM Policy](#), an [S3 Bucket Policy](#), an [SNS Topic Policy](#), a [VPC Endpoint Policy](#), and an [SQS Queue Policy](#).

Type of Policy

S3 Bucket Policy

Step 2: Add statement(s)

A statement is the formal description of a single permission. See [a description of elements](#) that you can use in statements.

Effect

Allow

Deny

Principal

*

Use a comma to separate multiple values.

Actions

All Actions ("*")

–Select Actions–

GetObject X

Amazon Resource Name (ARN)

All Resources ("*")

arn:aws:s3:::azad-bucket12

ARN should follow the following format: arn:aws:s3:::\${BucketName}/\${KeyName}. Use a comma to separate multiple values.

► Add conditions (optional)

Add Statement

Step 3: Generate policy

A policy is a document (written in the [Access Policy Language](#)) that acts as a container for one or more statements.

Generate Policy

• Click On GeneratePolicy

Statements added (1)

You added the following statements. Click the button below to Generate a policy.

Principal(s)	Effect	Action	Resource(s)	Condition(s)	Remove
*	Allow	s3:GetObject	arn:aws:s3:::azad-bucket12	None	Remove

Step 3: Generate policy

A policy is a document (written in the [Access Policy Language](#)) that acts as a container for one or more statements.

Generate Policy

11) The Policy JSON Document is Generated , Copy this file

The screenshot shows the AWS Policy Generator interface. On the left, there are sections for 'Actions' (checkboxes for 'All Actions' and 'Select Actions'), 'Amazon Resource Name (ARN)' (checkbox for 'All Resources'), and 'Add conditions (optional)'. In the center, a modal window titled 'Policy JSON Document' displays the following JSON code:

```

1  [
2    "Version": "2012-10-17",
3    "Statement": [
4      {
5        "Sid": "Statement1",
6        "Effect": "Allow",
7        "Principal": "*",
8        "Action": [
9          "s3:GetObject"
10        ],
11        "Resource": "arn:aws:s3:::azad-bucket12"
12      }
13    ]
14 ]

```

Below the code, it says 'Statements added (1)'. To the right of the code, there are buttons for 'JSON' (selected), 'Remove', and 'Copy Policy'. A green 'Copied' button is visible above the 'Copy Policy' button. At the bottom, there's a 'Close' button and a note about the generator being for informational purposes only.

12) Then we Copy Policy & Paste in Bucket Polic ,Click On Save Changes

The screenshot shows the 'Edit bucket policy' page in the AWS S3 console. The left sidebar shows 'Amazon S3' with options like 'General purpose buckets', 'Access Grants', and 'Storage Lens'. The main area has a 'Bucket policy' section with a 'Policy' tab. The policy text is:

```

1  [
2    "Version": "2012-10-17",
3    "Statement": [
4      {
5        "Sid": "Statement1",
6        "Effect": "Allow",
7        "Principal": "*",
8        "Action": [
9          "s3:GetObject"
10        ],
11        "Resource": "arn:aws:s3:::azad-bucket12"
12      }
13    ]
14 ]

```

To the right of the policy text, there are several buttons: 'Edit statement' (with 'Statement1' selected), 'Add actions', 'Choose a service' (with 'Search services' input), 'Included' (with 'S3' selected), 'Available' (with 'AI Operations' and 'AMP' listed), and 'Available' (with 'AI Operations' and 'AMP' listed again).

Azad Chauhan

Go To S3 > Your Bucket > Objects > Click your image/file. (**Scroll down > You will see > Object URL >Copy your url > Open in browser**)

If You follow the same step your file will open.