

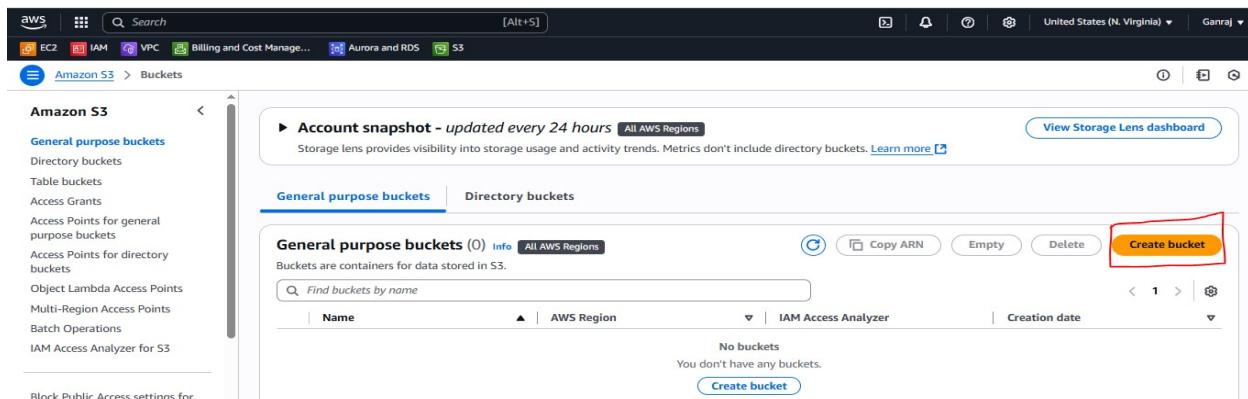
Creating S3 Bucket with adding object in it which will run a web page.

What Type of Data Can You Store in S3?

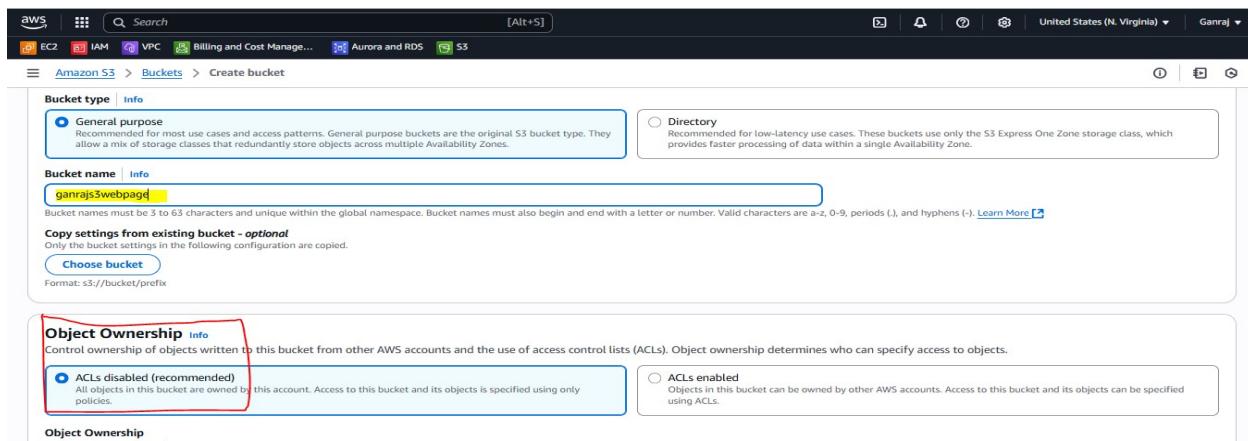
ANY KIND OF DIGITAL FILE.

- **Documents:** PDF, Word files, spreadsheets
 - **Images:** JPG, PNG, GIF
 - **Videos:** MP4, MOV
 - **Audio:** MP3, WAV
 - **Backups:** Database dumps, zip archives
 - **Logs:** Text files from apps
 - **Software packages:** .zip, .tar.gz
 - **Static website files:** HTML, CSS, JS
-
- **General bucket:** No slashes in the object keys.
 - **Directory-style bucket:** Uses slashes to organize keys visually.

Here we are using General bucket



The screenshot shows the AWS S3 Buckets page. On the left, there's a sidebar with options like EC2, IAM, VPC, Billing and Cost Management, Aurora and RDS, and S3. The main area has tabs for 'General purpose buckets' (selected) and 'Directory buckets'. Below the tabs, there's a heading 'General purpose buckets (0)' with a 'Create bucket' button. A red box highlights this 'Create bucket' button. Below the button, it says 'No buckets' and 'You don't have any buckets.' There's also a 'Create bucket' link.



The screenshot shows the 'Create bucket' wizard. It has several sections: 'Bucket type' (with 'General purpose' selected), 'Bucket name' (with 'ganraj3swebpage' entered), 'Copy settings from existing bucket - optional', 'Object Ownership' (with 'ACLS disabled (recommended)' selected), and 'Object Ownership' (with 'ACLS enabled' selected). A red box highlights the 'Object Ownership' section under 'ACLS disabled (recommended)'.

Always remember Bucket name should be unique not been used before.

Lets learn about ACL

ACL = Access Control List

Think of an ACL as a basic permission list you attach to:

- Buckets
- Objects (files)

It controls who can access them and what they can do

Grant or restrict access to your bucket or files at a very basic level.

What permissions can you set?

With ACLs, you can give permissions like:

- Read (download/list)
- Write (upload/delete)
- Read ACP (read ACL)
- Write ACP (write ACL)
- Full Control

You assign these to:

- The owner account
- Other AWS accounts
- Everyone (public access) (⚠ Be careful—makes your files public)

The screenshot shows the AWS S3 'Create bucket' page. At the top, there's a navigation bar with links for EC2, IAM, VPC, Billing and Cost Management, Aurora and RDS, and S3. Below the navigation is a breadcrumb trail: Amazon S3 > Buckets > Create bucket. A note states: 'S3 will ignore public and cross-account access for buckets or access points with policies that grant public access to buckets and objects.' The main section is titled 'Bucket Versioning'. It explains versioning and has a 'Bucket Versioning' dropdown where 'Disable' is selected. There's also a 'Learn more' link. The 'Tags - optional (0)' section indicates no tags are associated with this bucket and provides an 'Add new tag' button. The 'Default encryption' section includes an 'Info' link. The top right of the page shows 'United States (N. Virginia)' and 'Ganraj'.

For Versioning : - It depends that if we want maintain version(V1,V2 like GitHub) of our data. it best practice is for data corruption (failure) after updating new data but it will save different versions of same data

The screenshot shows the 'Create bucket' wizard on the AWS S3 service. The 'Encryption type' section is set to 'Server-side encryption with Amazon S3 managed keys (SSE-S3)'. The 'Bucket Key' section has 'Enable' selected. Under 'Advanced settings', there is a note about uploading files and configuring additional settings. A red box highlights the 'Create bucket' button at the bottom right.

The screenshot shows the 'Buckets' page on the AWS S3 service. A green success message states 'Successfully created bucket "ganrajs3webpage"'. Below it, there's an 'Account snapshot' section and a table of general purpose buckets. The 'ganrajs3webpage' bucket is listed with its details: Name (ganrajs3webpage), AWS Region (US East (N. Virginia) us-east-1), IAM Access Analyzer (View analyzer for us-east-1), and Creation date (July 9, 2025, 22:07:16 (UTC+05:30)). A red box highlights the 'Create bucket' button in the top right corner of the table header.

Click on your bucket **ganrajs3webpage** and upload you website data or you can simply drag and drop your data from system.

Objects (0)

No objects

You don't have any objects in this bucket.

[Upload](#)

Name	Date modified	Type	Size
404	4/10/2023 1:08 PM	Chrome HTML Do...	1 KB
image	7/9/2025 10:13 PM	JFIF File	21 KB
index	4/10/2023 1:08 PM	Chrome HTML Do...	2 KB
README	4/10/2023 1:08 PM	Markdown Source...	1 KB

Upload Info

Add the files and folders you want to upload to S3. To upload a file larger than 160GB, use the AWS CLI, AWS SDKs or Amazon S3 REST API. [Learn more](#)

Drag and drop files and folders you want to upload here, or choose [Add files](#) or [Add folder](#).

Files and folders (4 total, 22.3 KB)

Name	Folder	Type	Size
404.html	-	text/html	440.0 B
image.jpg	-	image/jpeg	20.2 KB
index.html	-	text/html	1.7 KB
README.md	-	-	25.0 B

Click on upload

The screenshot shows the AWS S3 console interface. At the top, the navigation bar includes links for EC2, IAM, VPC, Billing and Cost Management, Aurora and RDS, and S3. The current path is Amazon S3 > Buckets > ganrajs3webpage > Upload. The main area displays a table for uploading files, with a search bar and columns for Name, Folder, Type, and Size. Below the table, sections for Destination (info about s3://ganrajs3webpage) and Permissions (granting public access) are visible. A large orange 'Upload' button is highlighted with a red box. The status bar at the bottom indicates 'Upload succeeded'.

Now we need allow some properties of bucket for our static site (webpage) like hosting main page
Like enabling static hosting

The screenshot shows the AWS S3 console interface. The left sidebar lists 'Amazon S3' and 'General purpose buckets'. The main area shows the 'ganrajs3webpage' bucket's properties. The 'Properties' tab is selected, with other tabs for Objects, Metadata, Permissions, Metrics, Management, and Access Points. The 'Objects' tab is active, showing a list of four objects: 404.html, image.jfif, index.html, and README.md. Each object has a preview icon, name, type, last modified date, size, and storage class (Standard). An orange 'Upload' button is visible at the top of the objects table.

The screenshot shows the AWS S3 Bucket Properties page for the bucket 'ganrajs3webpage'. On the left, there's a sidebar with 'Amazon S3' and various options like 'General purpose buckets' and 'Storage Lens'. The main content area has a 'Disabled' status at the top. Under 'Static website hosting', it says 'Disabled' and has a red box around the 'Edit' button. A note recommends using AWS Amplify Hosting for static website hosting, with a 'Create Amplify app' button. There's also a note about S3 static website hosting.

Here you can see we have enabled the hosting also we need to mention our main **index page** and if any error occurs what need to see the **End User** also need to add in error document

The screenshot shows the 'Edit static website hosting' configuration for the same bucket. It has 'Enable' selected under 'Static website hosting'. Under 'Hosting type', 'Host a static website' is selected. In the 'Index document' section, 'index.html' is specified. In the 'Error document - optional' section, '404.html' is specified. A note about public access is present.

Click on save changes then.

Go to Permissions :-

Need to change permissions to see every one our site publicly accessible.

Amazon S3

General purpose buckets

- Directory buckets
- Table buckets
- Access Grants
- Access Points for general purpose buckets
- Access Points for directory buckets
- Object Lambda Access Points
- Multi-Region Access Points
- Batch Operations
- IAM Access Analyzer for S3

Block Public Access settings for this account

Storage Lens

Permissions overview

Access finding

Access findings are provided by IAM external access analyzers. Learn more about [How IAM analyzer findings work](#)

[View analyzer for us-east-1](#)

Edit

Block public access (bucket settings)

Public access is granted to buckets and objects through access control lists (ACLs), bucket policies, access point policies, or all. In order to ensure that public access to all your S3 buckets and objects is blocked, turn on Block all public access. These settings apply only to this bucket and its access points. AWS recommends that you turn on Block all public access, but before applying any of these settings, ensure that your applications will work correctly without public access. If you require some level of public access to your buckets or objects within, you can customize the individual settings below to suit your specific storage use cases. [Learn more](#)

Block all public access

On

► Individual Block Public Access settings for this bucket

Bucket policy

The bucket policy, written in JSON, provides access to the objects stored in the bucket. Bucket policies don't apply to objects owned by other accounts. [Learn more](#)

Edit **Delete**

Amazon S3

General purpose buckets

- Directory buckets
- Table buckets
- Access Grants
- Access Points for general purpose buckets
- Access Points for directory buckets
- Object Lambda Access Points
- Multi-Region Access Points
- Batch Operations
- IAM Access Analyzer for S3

Block Public Access settings for this account

Storage Lens

Edit Block public access (bucket settings) Info

Block public access (bucket settings)

Public access is granted to buckets and objects through access control lists (ACLs), bucket policies, access point policies, or all. In order to ensure that public access to all your S3 buckets and objects is blocked, turn on Block all public access. These settings apply only to this bucket and its access points. AWS recommends that you turn on Block all public access, but before applying any of these settings, ensure that your applications will work correctly without public access. If you require some level of public access to your buckets or objects within, you can customize the individual settings below to suit your specific storage use cases. [Learn more](#)

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.

Save changes

Also need to allow ACL for our website

Amazon S3

General purpose buckets

- Directory buckets
- Table buckets
- Access Grants
- Access Points for general purpose buckets
- Access Points for directory buckets
- Object Lambda Access Points
- Multi-Region Access Points
- Batch Operations
- IAM Access Analyzer for S3

Block Public Access settings for this account

Storage Lens

Successfully edited Block Public Access settings for this bucket.

Object Ownership Info

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

Object Ownership

Bucket owner enforced

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

Edit

Access control list (ACL)

Grant basic read/write permissions to other AWS accounts. [Learn more](#)

This bucket has the bucket owner enforced setting applied for Object Ownership

When [bucket owner enforced](#) is applied, use bucket policies to control access. [Learn more](#)

Grantee	Objects	Bucket ACL
Bucket owner (your AWS account)	List, Write	Read, Write

Edit Object Ownership

Object Ownership

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

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

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

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

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

I acknowledge that ACLs will be restored.

Object Ownership

Bucket owner preferred

Edit Object Ownership

Object Ownership

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

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

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

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

Object Ownership

Bucket owner preferred
If new objects written to this bucket specify the bucket-owner-full-control canned ACL, they are owned by the bucket owner. Otherwise, they are owned by the object writer.

Object writer
The object writer remains the object owner.

Information: If you want to enforce object ownership for new objects only, your bucket policy must specify that the bucket-owner-full-control canned ACL is required for object uploads. [Learn more](#)

Save changes

Just click on save changes then.
now edit some ACL permissions

Access control list (ACL)

Grant basic read/write permissions to other AWS accounts. [Learn more](#)

Information: The console displays combined access grants for duplicate grantees
To see the full list of ACLs, use the Amazon S3 REST API, AWS CLI, or AWS SDKs.

Grantee	Objects	Bucket ACL
Bucket owner (your AWS account) Canonical ID: 60f1ae7/bf8f6aa808bf1f75767d49dab628a1a074087f3761a63e0f9cc65767	List, Write	Read, Write
Everyone (public access) Group: http://acs.amazonaws.com/groups/global/AllUsers	-	-
Authenticated users group (anyone with an AWS account) Group: http://acs.amazonaws.com/groups/global/AuthenticatedUsers	-	-
S3 log delivery group Group: http://acs.amazonaws.com/groups/s3/LogDelivery	-	-

Cross-origin resource sharing (CORS)

Edit

Edit access control list (ACL) Info

Access control list (ACL)
Grant basic read/write permissions to other AWS accounts. [Learn more](#)

Grantee	Objects	Bucket ACL
Bucket owner (your AWS account) Canonical ID: 60f1ae7b7bf8faa808bf1f17576 7d49dab628a1a074087f3761a63e0f9ce65767	<input checked="" type="checkbox"/> List <input checked="" type="checkbox"/> Write	<input checked="" type="checkbox"/> Read <input checked="" type="checkbox"/> Write
Everyone (public access) Group: http://acs.amazonaws.com/groups/global/AllUsers	<input checked="" type="checkbox"/> List <input type="checkbox"/> Write	<input checked="" type="checkbox"/> Read <input type="checkbox"/> Write
Authenticated users group (anyone with an AWS account) Group: http://acs.amazonaws.com/groups/global/AuthenticatedUsers	<input type="checkbox"/> List <input type="checkbox"/> Write	<input type="checkbox"/> Read <input type="checkbox"/> Write
S3 log delivery group Group: http://acs.amazonaws.com/groups/s3/LogDelivery	<input type="checkbox"/> List <input type="checkbox"/> Write	<input type="checkbox"/> Read <input type="checkbox"/> Write

Edit access control list (ACL) Info

Access for other AWS accounts
No other AWS accounts associated with the resource.

Add grantee

Note: When you grant access to the Everyone or Authenticated users group grantees, anyone in the world can access the objects in this bucket.
[Learn more](#)

I understand the effects of these changes on my objects and buckets.

Actions **Create folder** **Upload** **Cancel** **Save changes**

Then go to objects and select all uploaded objects and click on action use option make public using ACL

ganrajs3webpage Info

Objects (4/4)
Objects are the fundamental entities stored in Amazon S3. You can use [Amazon S3 inventory](#) to get a list of all objects in your bucket. For others to access your objects, [more](#)

Name	Type	Last modified	Size	Storage class
404.html	html	July 9, 2025, 22:17:26 (UTC+05:30)	440.0 B	Standard
image.jfif	jfif	July 9, 2025, 22:17:27 (UTC+05:30)	20.2 KB	Standard
index.html	html	July 9, 2025, 22:17:27 (UTC+05:30)	1.7 KB	Standard
README.md	md	July 9, 2025, 22:17:28 (UTC+05:30)	25.0 B	Standard

Actions **Create folder** **Upload**

- Download as
- Share with a presigned URL
- Calculate total size
- Copy
- Move
- Initiate restore
- Query with S3 Select
- Edit actions**
- Rename object
- Edit storage class
- Edit server-side encryption
- Edit metadata
- Edit tags

Make public using ACL

And click on make public.

The make public action enables public read access in the object access control list (ACL) settings. Learn more [\[Info\]](#)

Specified objects

Name	Type	Last modified	Size
404.html	html	July 9, 2025, 22:17:26 (UTC+05:30)	440.0 B
image.jpg	jif	July 9, 2025, 22:17:27 (UTC+05:30)	20.2 KB
index.html	html	July 9, 2025, 22:17:27 (UTC+05:30)	1.7 KB
README.md	md	July 9, 2025, 22:17:28 (UTC+05:30)	25.0 B

Cancel **Make public**

See a scenario-- if I made some changes in my objects (data) and I have reuploaded files in that bucket always remember we need to **make them public using ACL then and then only we can see updated webpage or it will show error.**

△ Not secure ganrajs3webpage.s3-website-us-east-1.amazonaws.com/

Ubuntu | Docker Docs | aws | EduBlitz | Powered... | DigitalOcean linux | Server World | My Courses | Rohan... | Quora Question Pai... | https://chatgpt.com... | All Bookmarks

403 Forbidden

An Error Occurred While Attempting to Retrieve a Custom Error Document

- Code: AccessDenied
- Message: Access Denied

Amazon S3

ganrajs3webpage [Info](#)

Objects (4/4)

Name	Type	Last modified	Size
404.html	html	July 9, 2025, 23:09:52 (UTC+05:30)	
image.jpg	jif	July 9, 2025, 23:09:53 (UTC+05:30)	
index.html	html	July 9, 2025, 23:09:53 (UTC+05:30)	
README.md	md	July 9, 2025, 23:09:54 (UTC+05:30)	

Actions ▾

- Copy S3 URI
- Copy URL
- Download
- Open
- Delete
- Actions ▾**
- Create folder
- Upload

Download as

Share with a presigned URL

Calculate total size

Copy

Move

Initiate restore

Query with S3 Select

Edit actions

Rename object

Edit storage class

Edit server-side encryption

Edit metadata

Edit tags

Make public using ACL

And showing in snap that if you enabled versioning of bucket then if you reupload the same name files (data) it will show you two versions of it (V2,V2)

Name	Type	Version ID	Last modified	Size	Storage class
404.html	html	1MdNWzGe4bWDg8bR_s8nxuXkw5Mfy3eL	July 9, 2025, 23:09:52 (UTC+05:30)	440.0 B	Standard
404.html	html	null	July 9, 2025, 23:01:11 (UTC+05:30)	440.0 B	Standard
image.jfif	jfif	x1es46POy.mOwN9fzyY.PSN1VGHFfp7U	July 9, 2025, 23:09:53 (UTC+05:30)	20.2 KB	Standard
image.jfif	jfif	null	July 9, 2025, 23:01:13 (UTC+05:30)	20.2 KB	Standard
index.html	html	9_gf62kUTnT99ARTe8x.HKeoK7W258A5P	July 9, 2025, 23:09:53 (UTC+05:30)	1.5 KB	Standard
index.html	html	null	July 9, 2025, 23:01:13 (UTC+05:30)	1.5 KB	Standard

Go to properties tab and scroll it down you see our bucket DNS for our website .

requester pays
Disabled

Static website hosting
Use this bucket to host a website or redirect requests. [Learn more](#)

We recommend using AWS Amplify Hosting for static website hosting
Deploy a fast, secure, and reliable website quickly with AWS Amplify Hosting. Learn more about [Amplify Hosting](#) or [View your existing Amplify apps](#)

S3 static website hosting
Enabled

Hosting type
Bucket hosting

Bucket website endpoint
When you configure your bucket as a static website, the website is available at the AWS Region-specific website endpoint of the bucket. [Learn more](#)
<http://ganrajs3webpage.s3-website-us-east-1.amazonaws.com>

When you hit it to you browser you see our webpage.

Not secure ganrajs3webpage.s3-website-us-east-1.amazonaws.com

Ganraj Dol

Karad
Maharashtra

in Contact