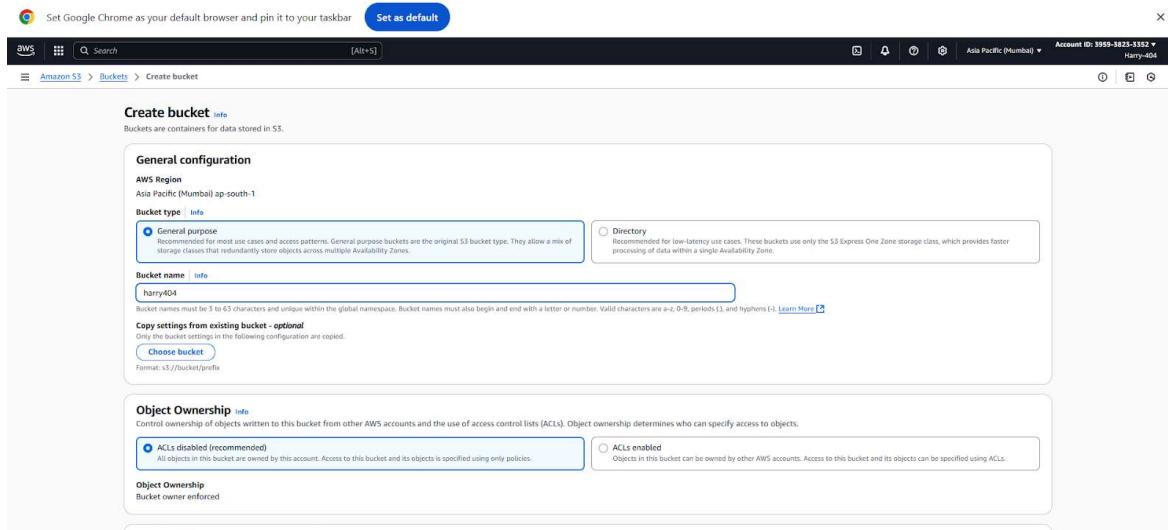


# AWS S3 Static Website Hosting with Public Image Access

## 1. Create an S3 Bucket

1. Go to Amazon S3 in AWS console.
2. Click Create bucket.
3. Choose:
  - Name: `harry404`
  - Region: Asia Pacific (Mumbai) `ap-south-1`
  - Bucket type: General purpose
4. Keep Copy settings disabled.
5. Under Object Ownership: Keep ACLs disabled (recommended).
6. Block all public access → ON for now (default).
7. Leave versioning Disabled.
8. No tags.
9. Default encryption: SSE-S3 (default).
10. Click Create bucket.



Set Google Chrome as your default browser and pin it to your taskbar [Set as default](#)

aws Search [Alt+5] Asia Pacific (Mumbai) Account ID: 3959-3823-3352 Harry-404

Amazon S3 > Buckets > Create bucket

**Block Public Access settings for this bucket**

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 this bucket and its 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 this bucket 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 block public access permissions applied to any existing 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 new public bucket or access point policies**  
S3 will block public access permissions applied to any new public bucket or access point policies. 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 prevent 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](#)

**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.

© 2015, Amazon Web Services, Inc. or its affiliates. [Privacy](#) [Terms](#) [Cookie preferences](#)

aws Search [Alt+5] Asia Pacific (Mumbai) Account ID: 3959-3823-3352 Harry-404

Amazon S3 > Buckets > Create bucket

**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](#)  
 **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 (DSS-E-KMS)**  
 Secure your objects with two separate layers of encryption. For details on pricing, see [DSS-E-KMS pricing](#) on the Storage tab of the [Amazon S3 pricing page](#).

**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 DSS-E-KMS. [Learn more](#)

**Disable**  
 **Enable**

**Advanced settings**

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

[Cancel](#) [Create bucket](#)

aws Search [Alt+5] Asia Pacific (Mumbai) Account ID: 3959-3823-3352 Harry-404

Amazon S3 > Buckets

**General purpose buckets** [All AWS Regions](#) **Directory buckets**

**General purpose buckets (1) [Info](#)**  
Buckets are containers for data stored in S3.

**Find buckets by name**

Name	AWS Region	Creation date
harry404	Asia Pacific (Mumbai) ap-south-1	August 11, 2025, 11:17:38 (UTC+05:30)

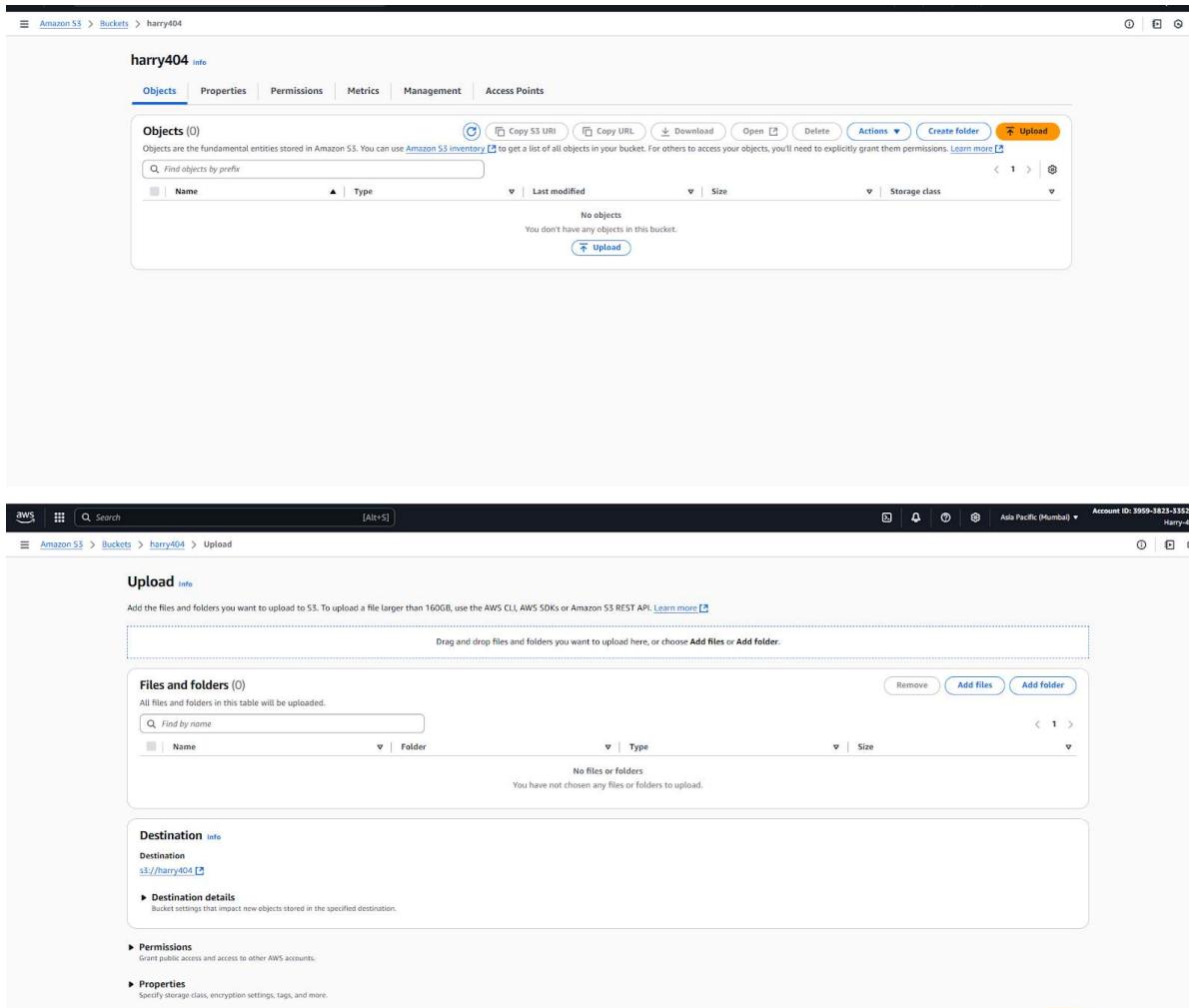
[Copy ARN](#) [Empty](#) [Delete](#) [Create bucket](#)

**Account snapshot** [Info](#) [View dashboard](#)  
Uploaded daily  
Storage Lens provides visibility into storage usage and activity trends.

**External access summary - new [Info](#)**  
Updated daily  
External access findings help you identify bucket permissions that allow public access or access from other AWS accounts.

## 2. Upload an Image to the Bucket

1. Open the bucket `harry404`.
2. Click Upload → Add files.
3. Select: `Screenshot 2025-08-04 114432.png` (151.1 KB).
4. Keep default permissions & properties.
5. Click Upload → Status: Succeeded.



The screenshot shows the AWS S3 console interface. At the top, the navigation bar includes 'Amazon S3 > Buckets > harry404'. The main content area has a header 'harry404 info' with tabs for 'Objects', 'Properties', 'Permissions', 'Metrics', 'Management', and 'Access Points'. The 'Objects' tab is selected, showing a table with one row: 'No objects'. Below the table is a message: 'You don't have any objects in this bucket.' At the bottom of this section is a blue 'Upload' button. The second part of the screenshot shows the 'Upload' tab selected. It has a large text input field with the placeholder 'Drag and drop files and folders you want to upload here, or choose Add files or Add folder.' Below this is a table with one row: 'Files and folders (0)'. The table has columns for 'Name', 'Type', and 'Size'. A message below the table says 'No files or folders' and 'You have not chosen any files or folders to upload.' At the bottom of this section are three buttons: 'Remove', 'Add files', and 'Add folder'. The third part of the screenshot shows the 'Destination' tab selected. It displays the URL `s3://harry404`. Below this are sections for 'Destination details' (with a note: 'Bucket settings that impact new objects stored in the specified destination.') and 'Permissions' (with a note: 'Grant public access and access to other AWS accounts.'). At the bottom of this section are three buttons: 'Remove', 'Add files', and 'Add folder'.

aws | Search [Alt+S] | Account ID: 3959-3413-3352 | Harry-404 | Asia Pacific (Mumbai) |

Amazon S3 > Buckets > harry404 > Upload

**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 (1 total, 151.1 KB)**  
All files and folders in this table will be uploaded.

Find by name		Folder	Type	Size
<input type="checkbox"/>	Name	-	image/png	151.1 KB
<input type="checkbox"/>	Screenshot 2025-08-04 114432.png	-		

**Destination** Info  
Destination  
[s3://harry404](#)

**Destination details**  
Bucket settings that impact how objects stored in the specified destination.

**Permissions**  
Grant public access and access to other AWS accounts.

**Properties**  
Specify storage class, encryption settings, tags, and more.

[Cancel](#) [Upload](#)

Set Google Chrome as your default browser and pin it to your taskbar [Set as default](#)

aws | Search [Alt+S] | Account ID: 3959-3413-3352 | Harry-404 | Asia Pacific (Mumbai) |

**Upload: status**

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

**Close**

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

**Summary**

Destination	Succeeded	Failed
<a href="#">s3://harry404</a>	1 file, 151.1 KB (100.00%)	0 files, 0 B (0%)

**Files and folders** [Configuration](#)

**Files and folders (1 total, 151.1 KB)**

Find by name		Folder	Type	Size	Status	Error
<input type="checkbox"/>	Name	-	image/png	151.1 KB	<a href="#">Succeeded</a>	-
<input type="checkbox"/>	Screenshot 2025-08-04 114432.png	-				

CloudShell Feedback

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

aws | Search [Alt+S] | Account ID: 3959-3413-3352 | Harry-404 | Asia Pacific (Mumbai) |

Amazon S3 > Buckets > harry404 > Screenshot 2025-08-04 114432.png

**Screenshot 2025-08-04 114432.png** Info

[Copy S3 URI](#) [Download](#) [Open](#) [Object actions](#)

**Properties** [Permissions](#) [Versions](#)

**Object overview**

**Owner**  
r0ddu92f951d8ca5481a462b17c6d1c525c7a028fd9537f57a84e007105460158

**AWS Region**  
Asia Pacific (Mumbai) ap-south-1

**Last modified**  
August 11, 2025, 20:21 (UTC+05:30)

**Size**  
151.1 KB

**Type**  
png

**Key**  
[Screenshot 2025-08-04 114432.png](#)

**Object management overview**  
The following bucket properties and object management configurations impact the behavior of this object.

**Bucket properties**

**Bucket Versioning**  
When enabled, multiple variants of an object can be stored in the bucket to easily recover from unintended user actions and application failures.  
 Enabled

**Object management**

**Object tags**

**Object URL**  
<https://harry404.s3.ap-south-1.amazonaws.com/Screenshot+2025-08-04+114432.png>

**Management configurations**

**Replication status**  
When a replication rule is applied to an object the replication status indicates the progress of the operation.

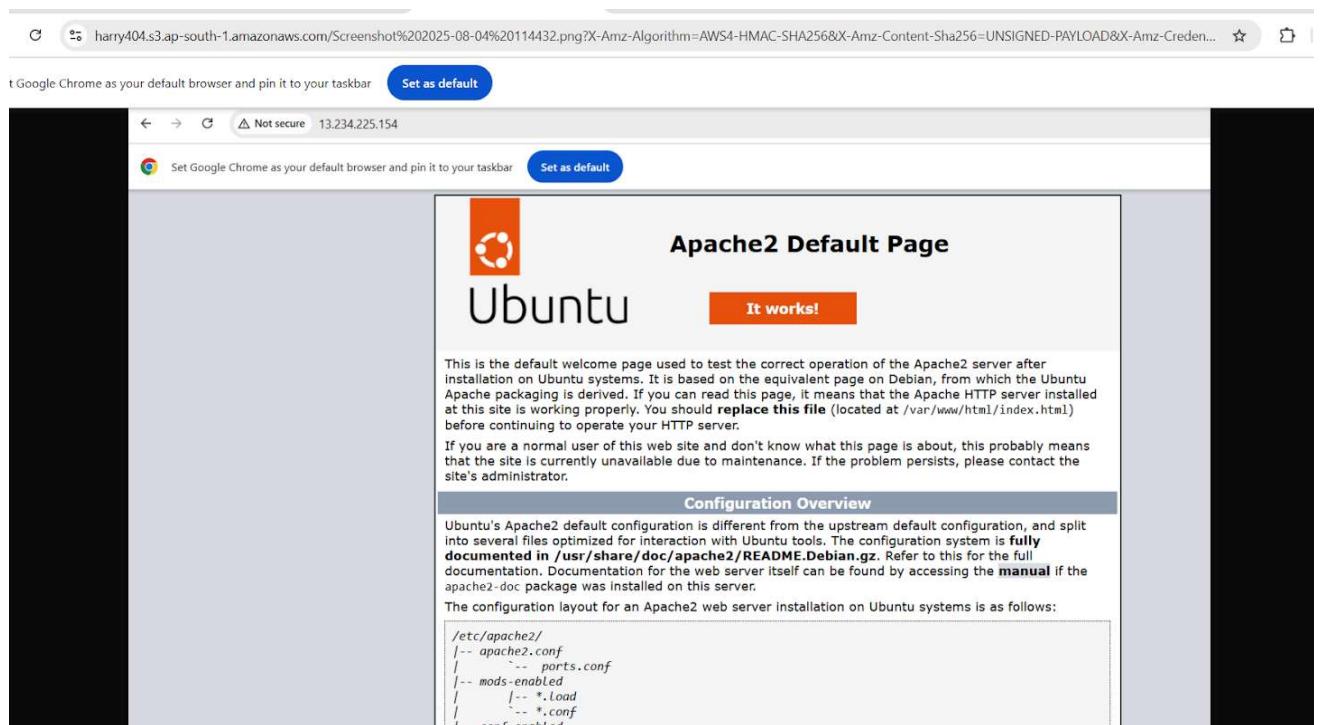
[View replication rules](#)

CloudShell Feedback

### 3. After Upload: Attempt to View the Image

- If you try to open the private S3 object URL (the one with temporary credentials and a long query string, available if you're logged in as the AWS owner), the image will be visible.
- If you visit the public S3 link (like <https://harry404.s3.ap-south-1.amazonaws.com/Screenshot+2025-08-04+14432.png>) from a browser where you are NOT logged into your AWS account, you will get an Access Denied error.

*This happens because, by default, S3 blocks public access to all content.*



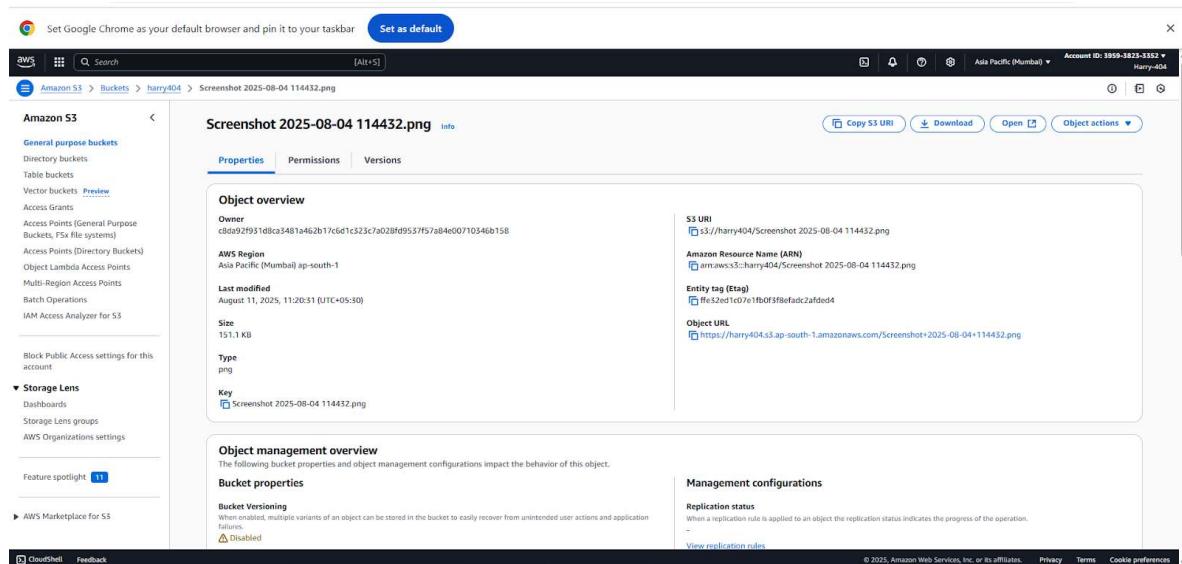
## 4. Fix “Access Denied” for Image

Initially, when trying the object URL, you get **AccessDenied**.

To make the image public:

1. Go to the bucket Permissions tab.
2. Edit Block Public Access → Turn OFF “Block all public access” (uncheck).
3. Save changes & confirm by typing confirm.
4. In Bucket Policy:
  - Click Edit.
  - Use JSON policy:

```
{  
  "Version": "2012-10-17",  
  "Statement": [  
    {  
      "Sid": "PublicReadGetObject",  
      "Effect": "Allow",  
      "Principal": "*",  
      "Action": "s3:GetObject",  
      "Resource": "arn:aws:s3:::harry404/*"  
    }  
  ]  
}
```



The screenshot shows the AWS S3 Object Details page for the file 'Screenshot 2025-08-04 114432.png'. The object was uploaded by 'harry404' on August 11, 2025, at 11:20:31 (UTC+05:30). The file is 151.1 KB in size and has a type of 'png'. The 'Properties' tab is selected, showing the S3 URI (s3://harry404/Screenshot 2025-08-04 114432.png), ARN (arn:aws:s3:::harry404/Screenshot 2025-08-04 114432.png), Entity tag (f6e22e1c07e1fb0f3fbfad2afed4), and Object URL (https://harry404.s3.ap-south-1.amazonaws.com/Screenshot+2025-08-04+114432.png). The 'Permissions' tab is also visible. The left sidebar shows the bucket structure and various AWS services like CloudWatch Metrics and CloudWatch Metrics Insights.

Set Google Chrome as your default browser and pin it to your taskbar [Set as default](#)

aws [Alt+S] Search Account ID: 3959-3823-3352 Harry-404

Amazon S3 Buckets

**Amazon S3**

**General purpose buckets**

- Directory buckets
- Table buckets
- Vector buckets [Preview](#)
- Access Grants
- Access Points (General Purpose Buckets, FSx file systems)
- Access Points (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**

- Dashboards
- Storage Lens groups
- AWS Organizations settings

Feature spotlight [11](#)

AWS Marketplace for S3

**General purpose buckets (1) [info](#)**

Buckets are containers for data stored in S3.

**Find buckets by name**

Name	AWS Region	Creation date
harry404	Asia Pacific (Mumbai) ap-south-1	August 11, 2025, 11:17:38 (UTC+05:30)

**Account snapshot [info](#)** [View dashboard](#)

Updated daily Storage Lens provides visibility into storage usage and activity trends.

**External access summary - new [info](#)**

Updated daily External access findings help you identify bucket permissions that allow public access or access from other AWS accounts.

aws [Alt+S] Search Account ID: 3959-3823-3352 Harry-404

Amazon S3 Buckets [harry404](#)

**Amazon S3**

**General purpose buckets**

- Directory buckets
- Table buckets
- Vector buckets [Preview](#)
- Access Grants
- Access Points (General Purpose Buckets, FSx file systems)
- Access Points (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**

- Dashboards
- Storage Lens groups
- AWS Organizations settings

Feature spotlight [11](#)

AWS Marketplace for S3

**harry404 [info](#)**

**Objects (1)**

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, you'll need to explicitly grant them permissions. [Learn more](#)

**Find objects by prefix**

Name	Type	Last modified	Size	Storage class
Screenshot 2025-08-04 114452.png	png	August 11, 2025, 11:20:31 (UTC+05:30)	151.1 KB	Standard

aws [Alt+S] Search Account ID: 3959-3823-3352 Harry-404

Amazon S3 Buckets [harry404](#)

**Amazon S3**

**General purpose buckets**

- Directory buckets
- Table buckets
- Vector buckets [Preview](#)
- Access Grants
- Access Points (General Purpose Buckets, FSx file systems)
- Access Points (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**

- Dashboards
- Storage Lens groups
- AWS Organizations settings

Feature spotlight [11](#)

AWS Marketplace for S3

**harry404 [info](#)**

**Permissions**

**Permissions overview**

**Access findings**

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

**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. If you're receiving public access to your buckets or objects, but haven't applied 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](#)

**Public access is blocked because Block Public Access settings are turned on for this bucket**

To determine which settings are turned on, check your Block Public Access settings for this bucket. Learn more about [Using Amazon S3 Block Public Access](#)

No policy to display. [Copy](#)

aws Search [Alt+S] Account ID: 3959-1823-1152 Harry-404

Amazon S3 > Buckets > harry404 > Edit Block public access (bucket settings)

### 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.

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

General purpose buckets

- Directory buckets
- Table buckets
- Vector buckets [Preview](#)

Access Grants

Access Points (General Purpose Buckets, FSx file systems)

Access Points (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

Dashboards

Storage Lens groups

AWS Organizations settings

Feature spotlight [11](#)

AWS Marketplace for S3

aws Search [Alt+S] Account ID: 3959-1823-1152 Harry-404

Amazon S3 > Buckets > harry404 > Edit Block public access (bucket settings)

### 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.

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

General purpose buckets

- Directory buckets
- Table buckets
- Vector buckets [Preview](#)

Access Grants

Access Points (General Purpose Buckets, FSx file systems)

Access Points (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

Dashboards

Storage Lens groups

AWS Organizations settings

Feature spotlight [11](#)

AWS Marketplace for S3

aws Search [Alt+S] Account ID: 3959-1823-1152 Harry-404

Amazon S3 > Buckets > harry404 > Edit Block public access (bucket settings)

### 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.

**Updating the Block Public Access settings for this bucket will affect this bucket and all objects within. This may result in some objects becoming public.**

**To confirm the settings, enter confirm in the field.**

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

General purpose buckets

- Directory buckets
- Table buckets
- Vector buckets [Preview](#)

Access Grants

Access Points (General Purpose Buckets, FSx file systems)

Access Points (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

Dashboards

Storage Lens groups

AWS Organizations settings

Feature spotlight [11](#)

AWS Marketplace for S3

Amazon S3 > Buckets > harry404

Successfully edited Block Public Access settings for this bucket.

**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**

Off

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](#)

No policy to display.

Copy

aws Search [All+S]

Amazon S3 > Buckets > harry404 > Edit bucket policy

Amazon S3

General purpose buckets

Bucket ARN: [arn:aws:s3:::harry404](#)

**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](#)

**Policy**

1

Edit statement

Select a statement

Select an existing statement in the policy or add a new statement.

+ Add new statement

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, [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**

IAM 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

**AWS**

All Services (\*\*)

--Select Service--

Use multiple statements to add permissions for more than one service.

## 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, 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.

#### 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:::harry404/\*

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](#)

#### Actions

All Actions (\*\*\*)

--Select Actions--

#### Amazon Resource Name (ARN)

All Resources (\*\*\*)

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

#### ► Add conditions (optional)

[Add Statement](#)

#### 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:::harry404/*	None	<a href="#">Remove</a>

### 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](#)

**Policy JSON Document**

Click below to edit. To save the policy, copy the text below to a text editor. Changes made below will **not be reflected in the policy generator tool**.

```

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

```

1.1 JSON

Principal(s) | Effect

Allow

**Step 3: Generate policy**  
A policy is a document (written in the Access Policy Generator) that defines the permissions for your AWS resources.

Generate Policy

Close | Copy Policy

**Edit bucket policy**

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](#)

Bucket ARN: [arn:aws:s3:::harry404](#)

Policy examples | Policy generator

```

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

```

Edit statement

Select a statement

Select an existing statement in the policy or add a new statement.

+ Add new statement

**Edit bucket policy**

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](#)

Bucket ARN: [arn:aws:s3:::harry404](#)

Policy examples | Policy generator

```

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

```

Add new statement

JSON | Line 14, Col. 1

Security: 0 Errors: 0 Warnings: 0 Suggestions: 0

Preview external access

Cancel | Save changes

Save Changes.

Amazon S3 > Buckets

**General purpose buckets** All AWS Regions

**General purpose buckets (1) Info**

Buckets are containers for data stored in S3.

**Find buckets by name**

Name	AWS Region	Creation date
harry404	Asia Pacific (Mumbai) ap-south-1	August 11, 2025, 11:17:58 (UTC+05:30)

**Create bucket**

**Account snapshot** Info View dashboard

Updated daily

Storage Lens provides visibility into storage usage and activity trends.

**External access summary - new** Info

Updated daily

External access findings help you identify bucket permissions that allow public access or access from other AWS accounts.

Block Public Access settings for this account.

**Storage Lens**

- Dashboards
- Storage Lens groups
- AWS Organizations settings

Feature spotlight 11

AWS Marketplace for S3

Amazon S3 > Buckets > harry404

**harry404** Info

**Objects** (1)

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, you'll need to explicitly grant them permissions. Learn more

**Find objects by prefix**

Name	Type	Last modified	Size	Storage class
Screenshot 2025-08-04 114432.png	png	August 11, 2025, 11:20:31 (UTC+05:30)	151.1 KB	Standard

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

Block Public Access settings for this account.

**Storage Lens**

- Dashboards
- Storage Lens groups
- AWS Organizations settings

Feature spotlight 11

AWS Marketplace for S3

Amazon S3 > Buckets > harry404 > Screenshot 2025-08-04 114432.png

**Screenshot 2025-08-04 114432.png** Info

**Properties** Permissions Versions

**Object overview**

**Owner** cb0a92f931d8ca3481a462b17c6d1c323c7a028fe9537f57a84e00710346b158

**AWS Region** Asia Pacific (Mumbai) ap-south-1

**Last modified** August 11, 2025, 11:20:31 (UTC+05:30)

**Size** 151.1 KB

**Type** png

**Key** Screenshot 2025-08-04 114432.png

**S3 URI** <https://s3.ap-south-1.amazonaws.com/harry404/Screenshot 2025-08-04 114432.png>

**Amazon Resource Name (ARN)** arn:aws:s3:::harry404/Screenshot 2025-08-04 114432.png

**Entity tag (Etag)** ffc32ed1d07e1fb0f38befa0c2afde4

**Object URL** <https://harry404.s3.ap-south-1.amazonaws.com/Screenshot+2025-08-04+114432.png>

**Object management overview**

The following bucket properties and object management configurations impact the behavior of this object.

**Bucket properties**

**Bucket Versioning** When enabled, multiple variants of an object can be stored in the bucket to easily recover from unintended user actions and application failures.

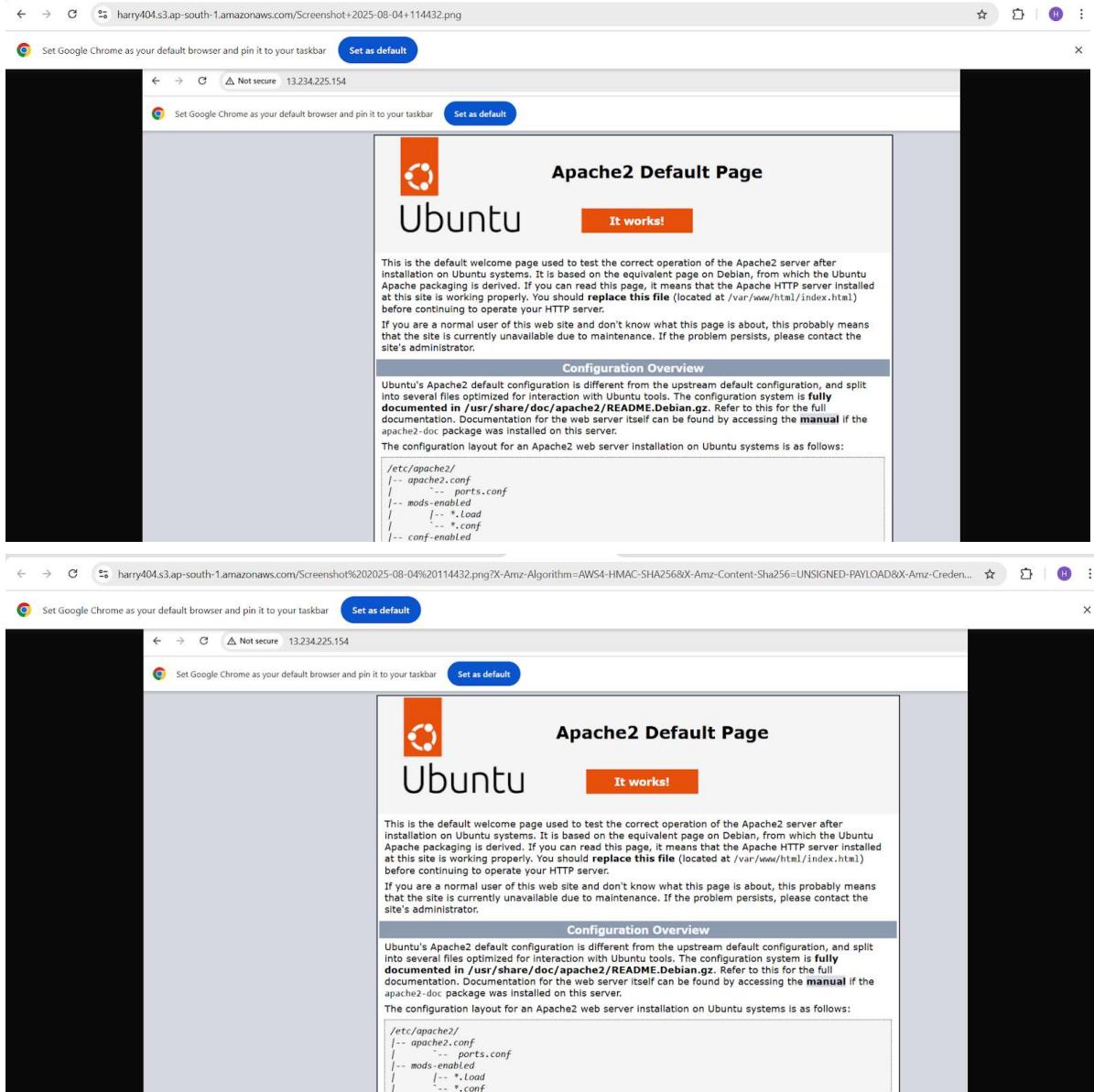
**Management configurations**

**Replication status**

When a replication rule is applied to an object the replication status indicates the progress of the operation.

Minor modifications made

Now the image URL will open publicly.



## 5. Enable Static Website Hosting

1. Open bucket → Properties tab.
2. Scroll to Static website hosting → Click Edit.
3. Select Enable, and Hosting type → Host a static website.
4. Index document: `index.html`
5. Error document: `error.html` (optional).
6. Save changes.

Amazon S3 > Buckets > harry404

**Bucket overview**

**Properties**

**Bucket Versioning**

**Tags (0)**

**Default encryption**

Amazon S3 > Buckets > harry404

**Transfer acceleration**

**Object Lock**

**Requester pays**

**Static website hosting**

Amazon S3 > Buckets > harry404 > Edit static website hosting

**Static website hosting**

**Hosting type**

**Index document**

**Error document - optional**

**Redirection rules - optional**

Amazon S3 > Buckets > harry404 > Edit static website hosting

**Amazon S3**

**General purpose buckets**

- Directory buckets
- Table buckets
- Vector buckets [Preview](#)
- Access Grants
- Access Points (General Purpose Buckets, FSx file systems)
- Access Points (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

- Dashboards
- Storage Lens groups
- AWS Organizations settings

Feature spotlight [11](#)

► AWS Marketplace for S3

**Error document - optional**  
This is returned when an error occurs.

**Redirection rules - optional**  
Redirection rules; written in JSON, automatically redirect webpage requests for specific content. [Learn more](#)

1

JSON Ln 1, Col 1 Errors: 0 Warnings: 0

Cancel Save changes

aws Search [Alt+S]

Amazon S3 > Buckets > harry404

**Amazon S3**

**General purpose buckets**

- Directory buckets
- Table buckets
- Vector buckets [Preview](#)
- Access Grants
- Access Points (General Purpose Buckets, FSx file systems)
- Access Points (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

- Dashboards
- Storage Lens groups
- AWS Organizations settings

Feature spotlight [11](#)

► AWS Marketplace for S3

Successfully edited static website hosting.

**Object lock**  
Store objects using a write-once-read-many (WORM) model to help you prevent objects from being deleted or overwritten for a fixed amount of time or indefinitely. Object Lock works only in versioned buckets. [Learn more](#)

**Object Lock**  
Disabled

**Requester pays**  
When enabled, the requester pays for requests and data transfer costs, and anonymous access to this bucket is disabled. [Learn more](#)

**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](#)

[Create Amplify app](#)

**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://harry404.s3-website.ap-south-1.amazonaws.com>

The image shows two screenshots of the AWS S3 console for the 'harry404' bucket.

**Upload Page:** This page is for uploading files and folders. It shows a table with one item: 'index.html' (text/html, 566.0 B). Below the table, the 'Destination' section shows the path 's3://harry404'. The 'Upload' button is highlighted in orange.

Name	Type	Size
index.html	text/html	566.0 B

**Objects Page:** This page lists the objects in the 'harry404' bucket. It shows one item: 'Screenshot 2025-08-04 114452.png' (png, 151.1 KB, Standard storage class). The 'Actions' dropdown menu is open, showing options like Copy S3 URI, Copy URL, Download, Open, Delete, and Upload.

Name	Type	Last modified	Size	Storage class
Screenshot 2025-08-04 114452.png	png	August 11, 2025, 11:20:51 (UTC+05:30)	151.1 KB	Standard

## 6. Create and Upload First `index.html` (Only Text Shown)

- Locally create `index.html` with just the text content:

```

<html>
  <head>
    <title>My Simple Website</title>
    <style>
      body { font-family: Arial, sans-serif; text-align: center;
margin-top: 100px; background-color: #fefefe; color: #333; }
      h1 { color: #0073e6; }
    </style>
  </head>
  <body>

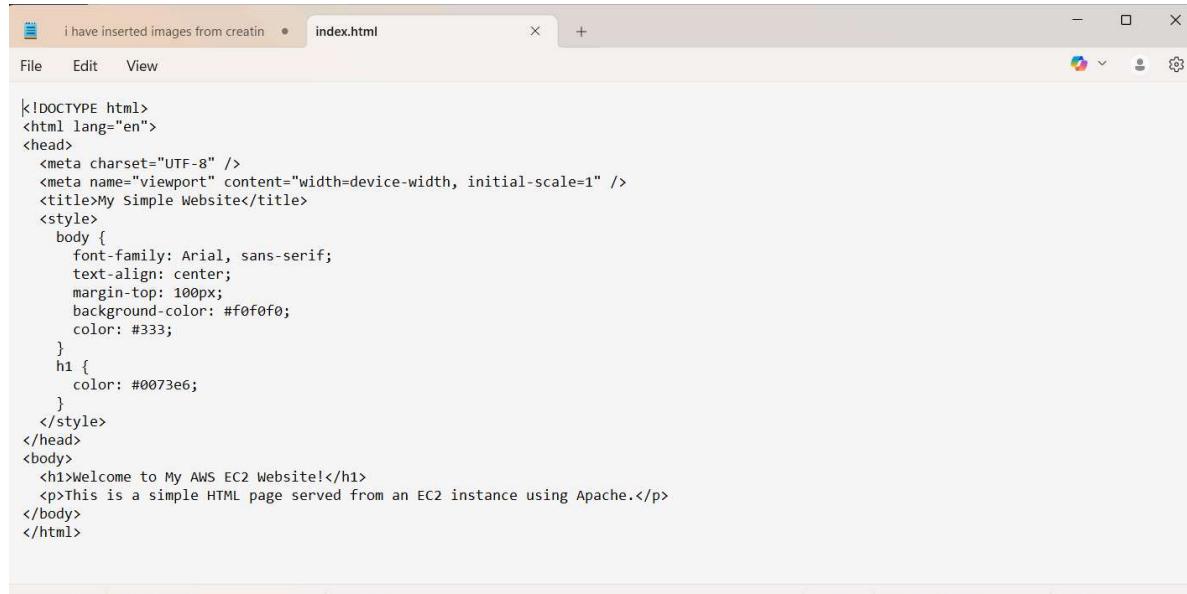
```

```

<h1>Welcome to My AWS EC2 Website!</h1>
<p>This is a simple HTML page served from an EC2 instance
using Apache.</p>
</body>
</html>

```

- Upload `index.html` to the bucket via Upload → Add files → Upload.

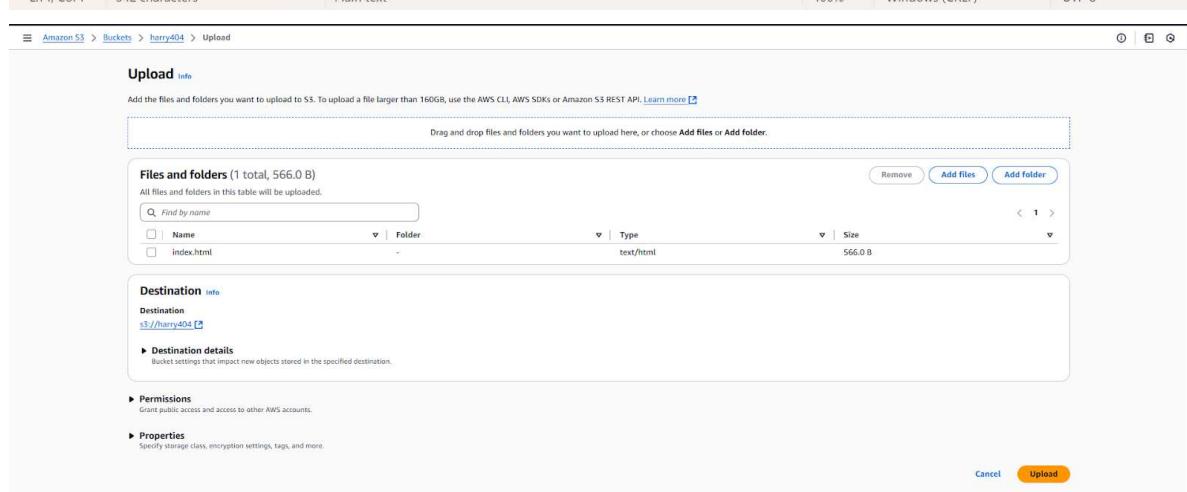


```

<!DOCTYPE html>
<html lang="en">
<head>
<meta charset="UTF-8" />
<meta name="viewport" content="width=device-width, initial-scale=1" />
<title>My Simple Website</title>
<style>
body {
    font-family: Arial, sans-serif;
    text-align: center;
    margin-top: 100px;
    background-color: #f0f0f0;
    color: #333;
}
h1 {
    color: #0073e6;
}
</style>
</head>
<body>
<h1>Welcome to My AWS EC2 Website!</h1>
<p>This is a simple HTML page served from an EC2 instance using Apache.</p>
</body>
</html>

```

Ln 1, Col 1 542 characters Plain text 100% Windows (CRLF) UTF-8



Amazon S3 > Buckets > harry404 > Upload

**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** (1 total, 566.0 B)

Find by name	Remove	Add files	Add folder
<input type="text"/>	<a href="#">Remove</a>	<a href="#">Add files</a>	<a href="#">Add folder</a>
<input type="checkbox"/> Name	<a href="#">▼</a>	<a href="#">▼</a>	<a href="#">▼</a>
<input type="checkbox"/> index.html	-	text/html	566.0 B

**Destination** info

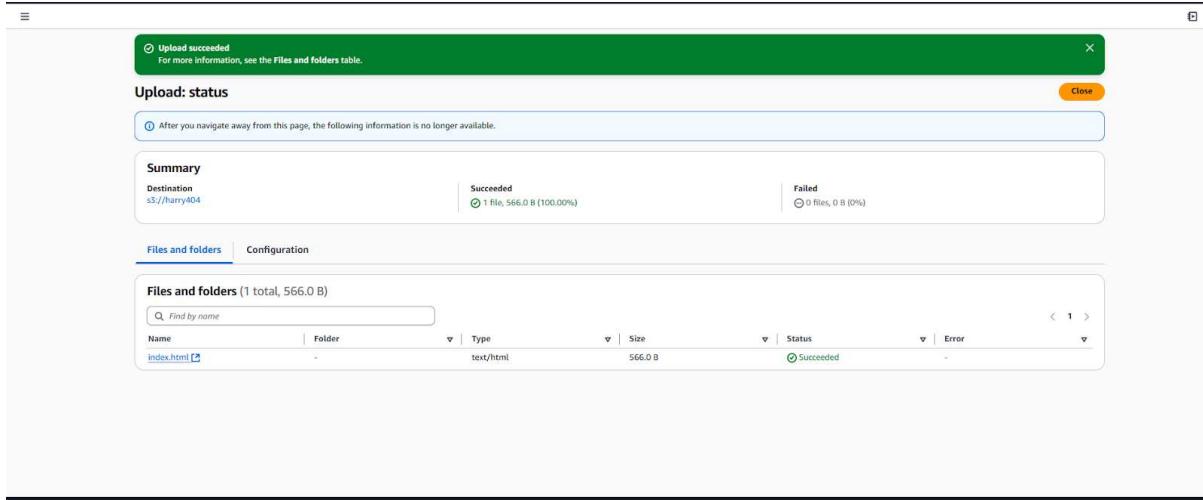
Destination [s3://harry404/](#)

▶ **Destination details** Bucket settings that impact new objects stored in the specified destination.

▶ **Permissions** Grant public access and access to other AWS accounts.

▶ **Properties** Specify storage class, encryption settings, tags, and more.

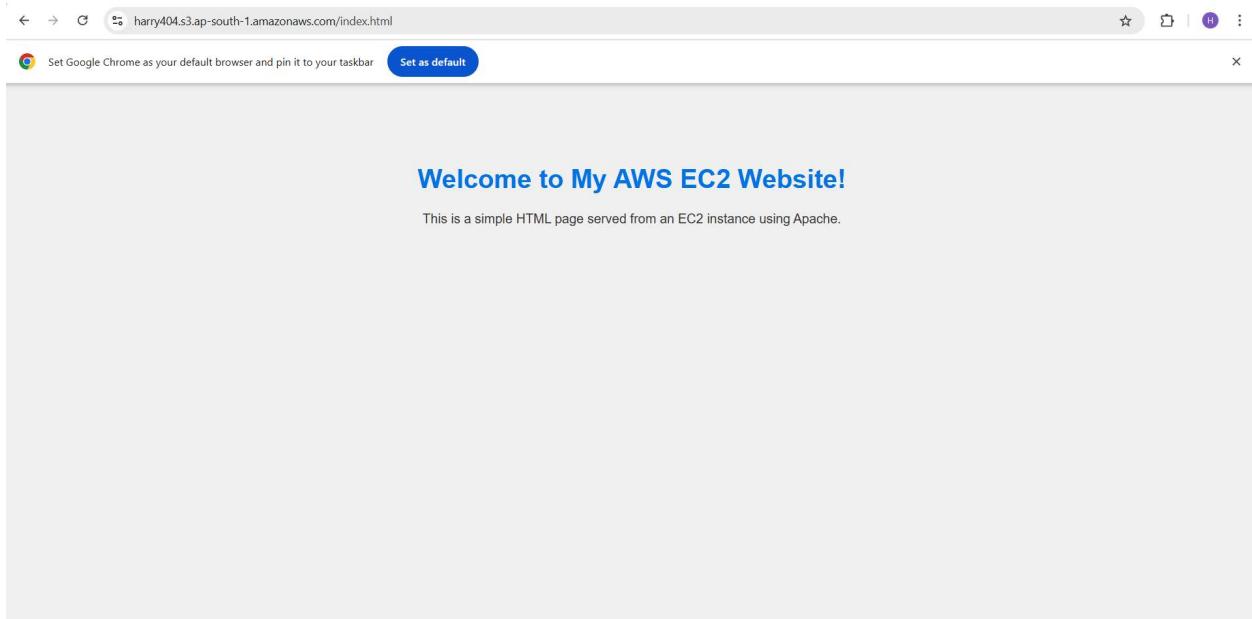
[Cancel](#) [Upload](#)



The screenshot shows the AWS S3 console. At the top, a green banner displays the message "Upload succeeded" with a link to the "Files and folders table". Below this, a "Upload: status" section shows a note that the information is no longer available. The main area is titled "Summary" and shows the destination as "s3://harry404". It includes two tabs: "Files and folders" (selected) and "Configuration". The "Files and folders" tab displays a table with one item: "index.html" (1 file, 566.0 B (100.00%)) with a status of "Succeeded".

## 7. Access Your Website

- Website URL:  
<http://harry404.s3-website.ap-south-1.amazonaws.com>
- Result: Website shows the title & text.



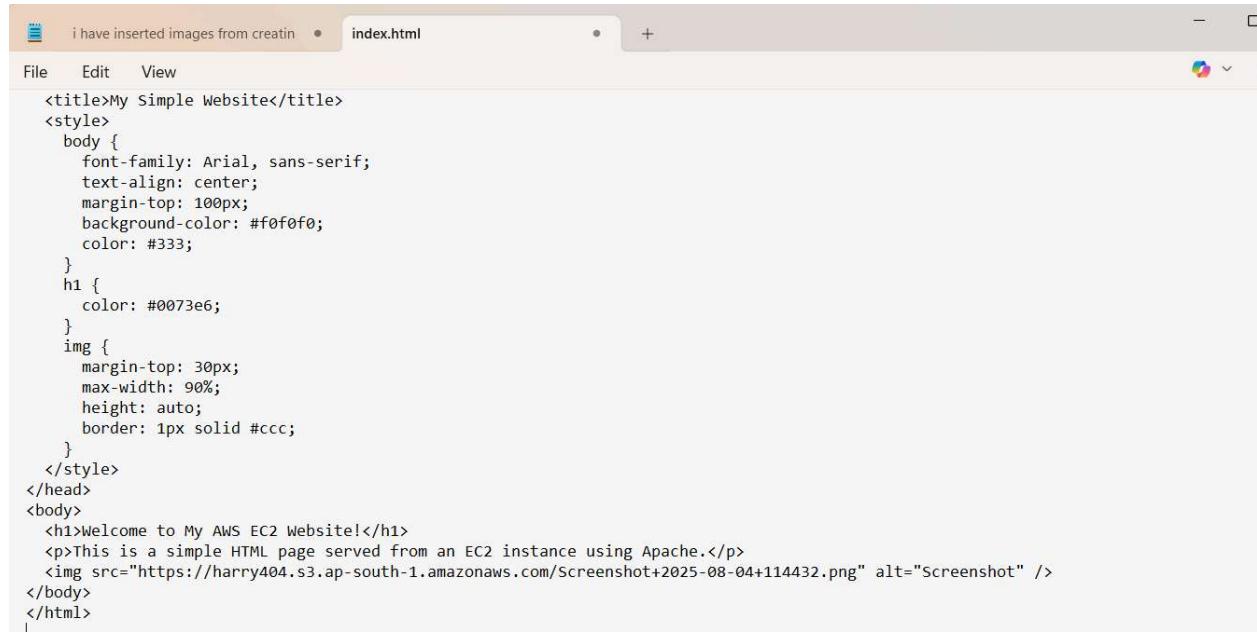
The screenshot shows a web browser window with the URL "harry404.s3-website.ap-south-1.amazonaws.com/index.html" in the address bar. A "Set as default" button is visible. The main content of the page is a simple HTML page titled "Welcome to My AWS EC2 Website!". Below the title, a small note states: "This is a simple HTML page served from an EC2 instance using Apache."

## 8. Update `index.html` to Include Public Image

- After public access is enabled for the image, edit `index.html` to include the image tag:

```
<html>
  <head>
    <title>My Simple Website</title>
    <style>
      body { font-family: Arial, sans-serif; text-align: center;
margin-top: 100px; background-color: #fefefe; color: #333; }
      h1 { color: #0073e6; }
      img { margin-top: 30px; max-width: 90%; height: auto;
border: 1px solid #ccc; }
    </style>
  </head>
  <body>
    <h1>Welcome to My AWS EC2 Website!</h1>
    <p>This is a simple HTML page served from an EC2 instance
using Apache.</p>
    
  </body>
</html>
```

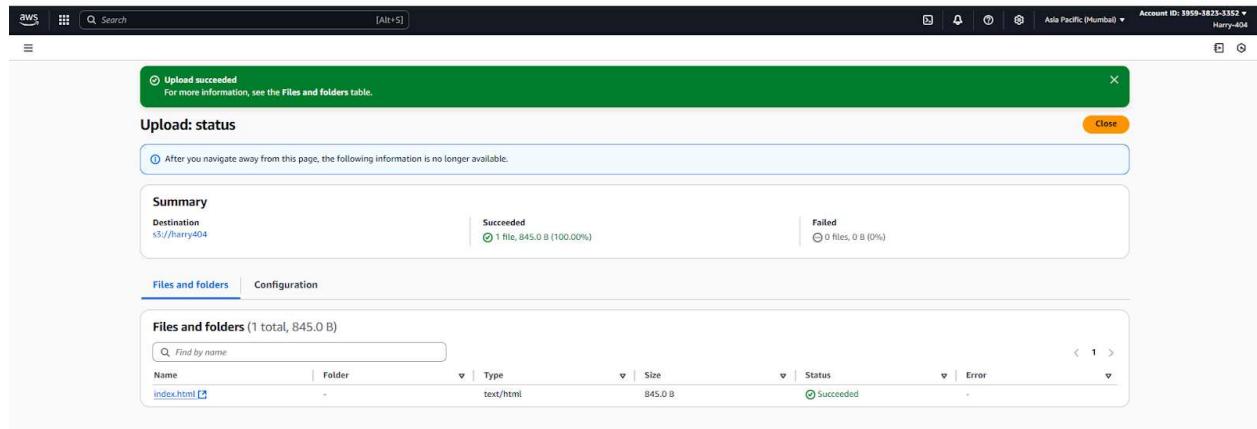
- Re-upload this new version of `index.html` to the bucket (overwrite the previous file).



```

i have inserted images from creatin  • index.html
File Edit View
<title>My Simple Website</title>
<style>
body {
  font-family: Arial, sans-serif;
  text-align: center;
  margin-top: 100px;
  background-color: #f0f0f0;
  color: #333;
}
h1 {
  color: #0073e6;
}
img {
  margin-top: 30px;
  max-width: 90%;
  height: auto;
  border: 1px solid #ccc;
}
</style>
</head>
<body>
  <h1>Welcome to My AWS EC2 Website!</h1>
  <p>This is a simple HTML page served from an EC2 instance using Apache.</p>
  
</body>
</html>

```



Upload succeeded

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

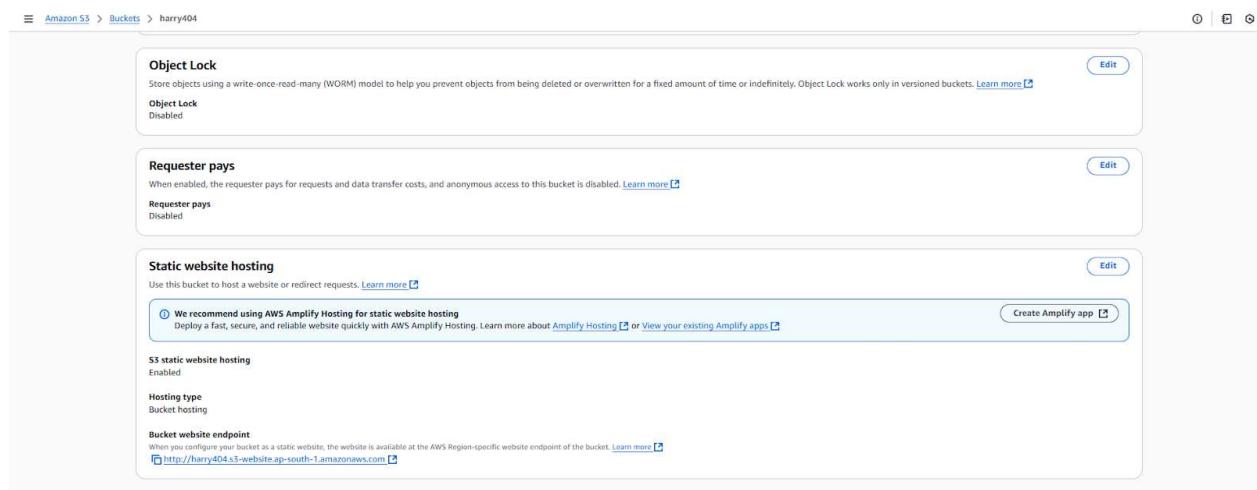
**Upload: status**

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

Summary	
Destination	
s3://harry404	<b>Succeeded</b> <span style="color: green;">(1 file, 845.0 B (100.00%))</span>
	<b>Failed</b> <span style="color: red;">(0 files, 0 B (0%))</span>

**Files and folders** (1 total, 845.0 B)

Files and folders (1 total, 845.0 B)						
<span style="float: left;">Find by name</span> <span style="float: right;">1</span>						
Name	Folder	Type	Size	Status	Error	
index.html	-	text/html	845.0 B	<span style="color: green;">Succeeded</span>	-	<span style="color: green;">Edit</span>



**Object Lock**

Store objects using a write-once-read-many (WORM) model to help you prevent objects from being deleted or overwritten for a fixed amount of time or indefinitely. Object Lock works only in versioned buckets. [Learn more](#)

**Object Lock**  
Disabled

**Requester pays**

When enabled, the requester pays for requests and data transfer costs, and anonymous access to this bucket is disabled. [Learn more](#)

**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://harry404.s3-website.ap-south-1.amazonaws.com>

## 9. Access Your Website

- Refresh your website URL:  
<http://harry404.s3-website.ap-south-1.amazonaws.com>
- Result: Website shows the title, text, and the image.

The screenshot shows a web browser with two tabs open. The top tab displays the AWS EC2 website at <http://harry404.s3-website.ap-south-1.amazonaws.com>. The page content is as follows:

**Welcome to My AWS EC2 Website!**  
This is a simple HTML page served from an EC2 instance using Apache.

The bottom tab shows the AWS S3 console. The 'General purpose buckets' section lists one bucket:

Name	AWS Region	Creation date
harry404	Asia Pacific (Mumbai) ap-south-1	August 11, 2025, 11:17:38 (UTC+05:30)

On the right side of the S3 console, there are two informational boxes:

- Account snapshot** (info) Updated daily  
Storage Lens provides visibility into storage usage and activity trends.
- External access summary - new** (info) Updated daily  
External access findings help you identify bucket permissions that allow public access or access from other AWS accounts.

## 10. Delete Everything

- Empty bucket → type `permanently delete` → confirm.
- Delete bucket → type `harry404` → confirm.

The image consists of three vertically stacked screenshots of the AWS S3 console, illustrating the steps to delete a bucket.

**Screenshot 1: Delete bucket**  
The first screenshot shows the "Delete bucket" page for the bucket "harry404". A red box highlights the error message: "This bucket is not empty. Buckets must be empty before they can be deleted." Below the message, a text input field contains "harry404". At the bottom are "Cancel" and "Delete bucket" buttons.

**Screenshot 2: Empty bucket**  
The second screenshot shows the "Empty bucket" page for the same bucket. A red box highlights the note: "Emptying the bucket deletes all objects in the bucket and cannot be undone." Below the note, a text input field contains "permanently delete". At the bottom are "Cancel" and "Empty" buttons.

**Screenshot 3: Success**  
The third screenshot shows a green success message: "Successfully emptied bucket 'harry404'". It includes a link to "View details below" and "Delete bucket configuration". Below the message is the "Empty bucket: status" section, which shows a summary table with "Successfully deleted" (2 objects, 152.0 KB) and "Failed to delete" (0 objects). The "Failed to delete" table is empty.

Amazon S3 > Buckets

General purpose buckets (1/1) [Info](#)

Buckets are containers for data stored in S3.

Name: [harry404](#) AWS Region: Asia Pacific (Mumbai) ap-south-1 Creation date: August 11, 2025, 11:17:38 (UTC+05:30)

[Copy ARN](#) [Empty](#) [Delete](#) [Create bucket](#)

Find buckets by name:

General purpose buckets (1/1) [Info](#)

Account snapshot [Info](#) [View dashboard](#)

Updated daily. Storage Lens provides visibility into storage usage and activity trends.

External access summary - new [Info](#)

Updated daily. External access findings help you identify bucket permissions that allow public access or access from other AWS accounts.

Amazon S3 > Buckets > [harry404](#) > Delete bucket

Delete bucket [Info](#)

⚠ Deleting a bucket cannot be undone.

- Bucket names are unique. If you delete a bucket, another AWS user can use the name.
- If this bucket is used with a Multi-Region Access Point in an external account, initiate failover before deleting the bucket.
- If this bucket is used with an access point in an external account, the requests made through those access points will fail after you delete this bucket.
- This bucket is configured to host a static website. We recommend that you clean up the Route 53 hosted zone settings that are related to the bucket.

[Learn more](#)

Delete bucket "harry404"?

To confirm deletion, enter the name of the bucket in the text input field.

[Cancel](#) [Delete bucket](#)

Successfully deleted bucket "harry404"

Storage

## Amazon S3

Store and retrieve any amount of data from anywhere

Amazon S3 is an object storage service that offers industry-leading scalability, data availability, security, and performance.

[Create a bucket](#)

**Pricing**

With S3, there are no minimum fees. You only pay for what you use. Prices are based on the location of your S3 bucket. Estimate your monthly bill using the [AWS Simple Monthly Calculator](#).

[View pricing details](#)

**Resources**

[User guide](#) [API reference](#) [FAQs](#)

How it works

Introduction to Amazon S3 | Amazon Web Services

Copy link

Create a bucket

Every object in S3 is stored in a bucket. To upload files and folders to S3, you'll need to create a bucket where the objects will be stored.

Create bucket