

AWS creation of S3 bucket and usage.

What is S3?

Amazon S3 (Simple Storage Service) is **object storage**.

It stores:

- Files
- Backups
- Static websites
- Docker artifacts
- Logs
- Terraform state files
- CI/CD build outputs

It is:

- Highly scalable
- 99.99999999% durable
- Pay for what you use

I am creating an new private S3 bucket .

The screenshot shows the 'Create bucket' page in the AWS Management Console. The top navigation bar includes links for Home, Services, and AWS Marketplace, along with account information for HARIHARAN K (0896-6520-4192). The main content area is titled 'Create bucket' with a 'Info' link. It displays the following configuration options:

- General configuration**:
 - AWS Region**: Asia Pacific (Mumbai) ap-south-1
 - Bucket type**:
 - General purpose**: Recommended for most use cases and access patterns. General purpose buckets are the original S3 bucket type. They allow a mix of storage classes that redundantly store objects across multiple Availability Zones.
 - Directory**: Recommended for low-latency use cases. These buckets use only the S3 Express One Zone storage class, which provides faster processing of data within a single Availability Zone.
- Bucket name**: intergame211825 (highlighted in blue)
- Copy settings from existing bucket - optional**: Only the bucket settings in the following configuration are copied.
 - Choose bucket**: A button to select an existing bucket.
 - Format: s3://bucket/prefix
- 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.

Screenshot of the AWS S3 'Create bucket' configuration page.

Object Ownership

- 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.

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 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](#)

- Disable**
- Enable**

Tags - optional

You can use bucket tags to analyze, manage and specify permissions for a bucket. [Learn more](#)

- You can use s3>ListTagsForResource, s3:TagResource, and s3:UntagResource APIs to manage tags on S3 general purpose buckets for access control in addition to cost allocation and resource organization. To ensure a seamless transition, please provide permissions to s3>ListTagsForResource, s3:TagResource, and s3:UntagResource actions. [Learn more](#)**

No tags associated with this bucket.

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

CloudShell Feedback [Console Mobile App](#) © 2026, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

The screenshot shows the 'Create bucket' wizard on the Amazon S3 console. The 'Default encryption' section is open, showing the 'Info' tab. It states that server-side encryption is automatically applied to new objects stored in the bucket. Under 'Encryption type', the 'Server-side encryption with Amazon S3 managed keys (SSE-S3)' option is selected. Below it, there are three other options: 'Server-side encryption with AWS Key Management Service keys (SSE-KMS)', 'Dual-layer server-side encryption with AWS Key Management Service keys (DSSE-KMS)', and 'Bucket Key'. The 'Bucket Key' section notes that using an S3 Bucket Key for SSE-KMS reduces encryption costs by lowering calls to AWS KMS. It also mentions that S3 Bucket Keys aren't supported for DSSE-KMS. The 'Enable' option is selected. A note at the bottom says, 'After creating the bucket, you can upload files and folders to the bucket, and configure additional bucket settings.' At the bottom right are 'Cancel' and 'Create bucket' buttons.

And then I have uploaded the files.

When I want to access the file it says that the access denied.

The screenshot shows an XML error response from an S3 endpoint. The error message is: "This XML file does not appear to have any style information associated with it. The document tree is shown below." The XML content is as follows:

```
<Error>
  <Code>AccessDenied</Code>
  <Message>Access Denied</Message>
  <RequestId>04356CE7E85FD1X</RequestId>
  <HostId>StXyfWoC61T4k061zhsDfPyv66E1D2sMwJ8yM9Zd1leF8LdnJ6Rsoi0qienifC1e1XDsvqneb3ipFVCYohaDa0Zegjh6kk8</HostId>
</Error>
```

Then we have to give permission with all the public access to the file.

The screenshot shows another XML error response from an S3 endpoint. The error message is: "This XML file does not appear to have any style information associated with it. The document tree is shown below." The XML content is identical to the previous one:

```
<Error>
  <Code>AccessDenied</Code>
  <Message>Access Denied</Message>
  <RequestId>04356CE7E85FD1X</RequestId>
  <HostId>StXyfWoC61T4k061zhsDfPyv66E1D2sMwJ8yM9Zd1leF8LdnJ6Rsoi0qienifC1e1XDsvqneb3ipFVCYohaDa0Zegjh6kk8</HostId>
</Error>
```

We have to enable versioning for the reusability of older versions.

The screenshot shows the 'Edit Object Ownership' page in the AWS S3 console. Under 'Object Ownership', the 'ACLs enabled' option is selected, indicated by a blue outline around the radio button. A note below states: '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.' There are also sections for 'Bucket owner preferred' and 'Object writer' with their respective descriptions.

And we have to untick the all checkbox.

The screenshot shows the 'Edit Block public access (bucket settings)' page in the AWS S3 console. The 'Block all public access' checkbox is unchecked. A note above the checkbox states: 'Turning this setting on is the same as turning on all four settings below. Each of the following settings are independent of one another.' Below the main checkbox are four additional options, each with its own description:

- 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.

We have to give access to the user with ACL (Access Control Lists)

Edit access control list Info

Access control list (ACL)

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

Grantee

Object owner (your AWS account)

Canonical ID: [e242bcd19252dd2107ac6d6d96da31b42a](#)
6f0ace302df7e121ce8ed8eba7a0a

Objects

Read

Object ACL

Read

Write

Everyone (public access)

Group: [http://acs.amazonaws.com/groups/global/AllUsers](#)

⚠ Read

⚠ Read

Write

Authenticated users group (anyone with an AWS account)

Group: [http://acs.amazonaws.com/groups/global/AuthenticatedUsers](#)

Read

Read

Write

⚠ When you grant access to the Everyone or Authenticated users group grantees, anyone in the world can access this object.

[Learn more ↗](#)

I understand the effects of these changes on this object.

⌚ You must select the check box to continue.

Then we will have the access to the website . S3 has an Adv. Of independent service so it act as an webserver also.

