

Step 1: Creating an S3 bucket in AWS Console.

- Go to Aws Console
- Search for S3
- Create New S3 Bucket
- Select the Bucket type As General purpose.
- Unmark the Block Public Access Settings for this Bucket so that Everyone can access from the URL.
- Now Click on Create Bucket.
- The new Bucket is Now Available.

- Step 1: Creating an S3 bucket in AWS Console.
- Go to Aws Console
 - Search for S3
 - Create New S3 Bucket
 - Select the Bucket type As General purpose.
 - Unmark the Block Public Access Settings for this Bucket so that Everyone can access from the URL.
 - Now Click on Create Bucket.
 - The new Bucket is Now Available.

Amazon S3

Buckets

Create bucket

Create bucket

Buckets are containers for data stored in S3.

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

codewarriorshackathon

Bucket names must be 3 to 63 characters and unique within the global namespace. Bucket names must also begin and end with a letter or number. Valid characters are a-z, 0-9, periods (.), and hyphens (-). [Learn More](#)

Copy settings from existing bucket - optional

Only the bucket settings in the following configuration are copied.

Choose bucket

Format: s3://bucket/prefix

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.

Object Ownership

Bucket owner enforced

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.

⚠ 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.

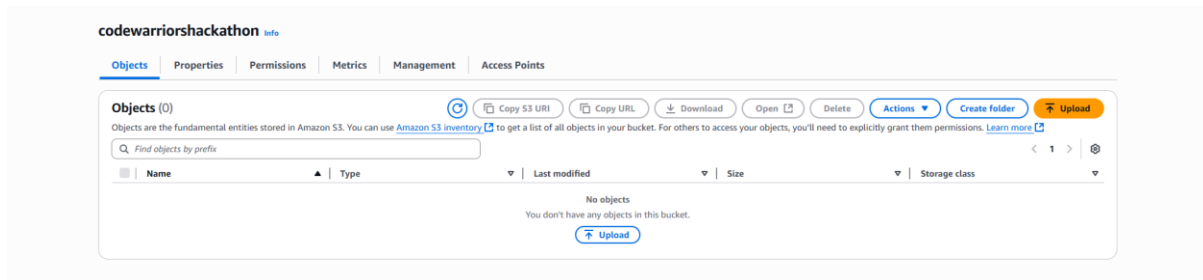
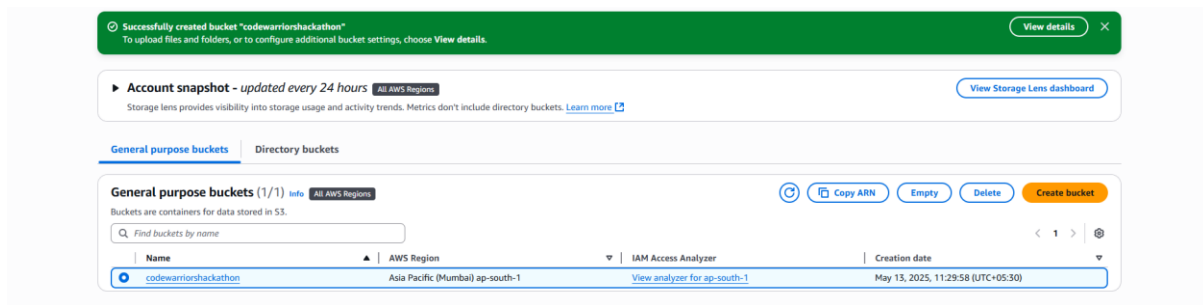
☐ I acknowledge that the current settings might result in this bucket and the objects within becoming public.

Bucket Versioning

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

Bucket Versioning

- ☒ **Disable**
- ☐ Enable



An S3 bucket policy in AWS is a resource-based policy that grants access permissions to your S3 bucket and the Object within it . it is the JSON document that defines permission for accessing a specific bucket.

- Click on Edit Bucket Policy
- Click on Policy Generator.
- Select the Type as S3 Bucket Policy.
- In Add Statement Allow the Effect and Enter * in principal
- Enter the ARN which is available in bucket details.

The policy will be generated Copy the policy and paste it.

If the Block Public Access bucket setting is ON By default, then turn it to OFF , so that it will Not Block Any Access Request.

Block public access (bucket settings)

Edit

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

EditDelete

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

Edit bucket policy [Info](#)

Bucket policy

Policy examplesPolicy generator

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:::codewarriorshackathon

Policy

1

Edit statement

Select a statement

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

+ Add new statement

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](#). Here are sample policies.

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.

Select 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.

AWS Service Amazon S3 ☐ All Services ("*")

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

Actions 1 Action(s) Selected ☐ All Actions ("*")

Amazon Resource Name (ARN) arn:aws:s3:::codewarriorshu

ARN should follow the following format: arn:aws:s3:::(BucketName)/S(KeyName).

Use a comma to separate multiple values.

Add Conditions (Optional)

Add Statement

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

Principal(s)	Effect	Action	Resource	Conditions
* *	Allow	s3:GetObject	arn:aws:s3:::codewarriorshackathon/*	None

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

Start Over

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.

AWS S3

Amazon Resource Name

You added the following statement

Principal(s)	Effect
* *	Allow

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.

```
{
  "Id": "Policy1747115575811",
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "Stmnt1747115567307",
      "Action": [
        "s3:GetObject"
      ],
      "Effect": "Allow",
      "Resource": "arn:aws:s3:::codewarriorshackathon/*",
      "Principal": "*"
    }
  ]
}
```

This AWS Policy Generator is provided for informational purposes only, you are still responsible for your use of Amazon Web Services technologies and ensuring that your use is in compliance with all applicable terms and conditions. This AWS Policy Generator is provided as a public service of Amazon Web Services.

Close

Successfully edited 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](#)

```
{
  "Version": "2012-10-17",
  "Id": "Policy1747116460517",
  "Statement": [
    {
      "Sid": "Stmnt1747116423793",
      "Effect": "Allow",
      "Principal": "*",
      "Action": "s3:GetObject",
      "Resource": "arn:aws:s3:::codewarriorshackathon/*"
    }
  ]
}
```

Edit

Delete

Copy