

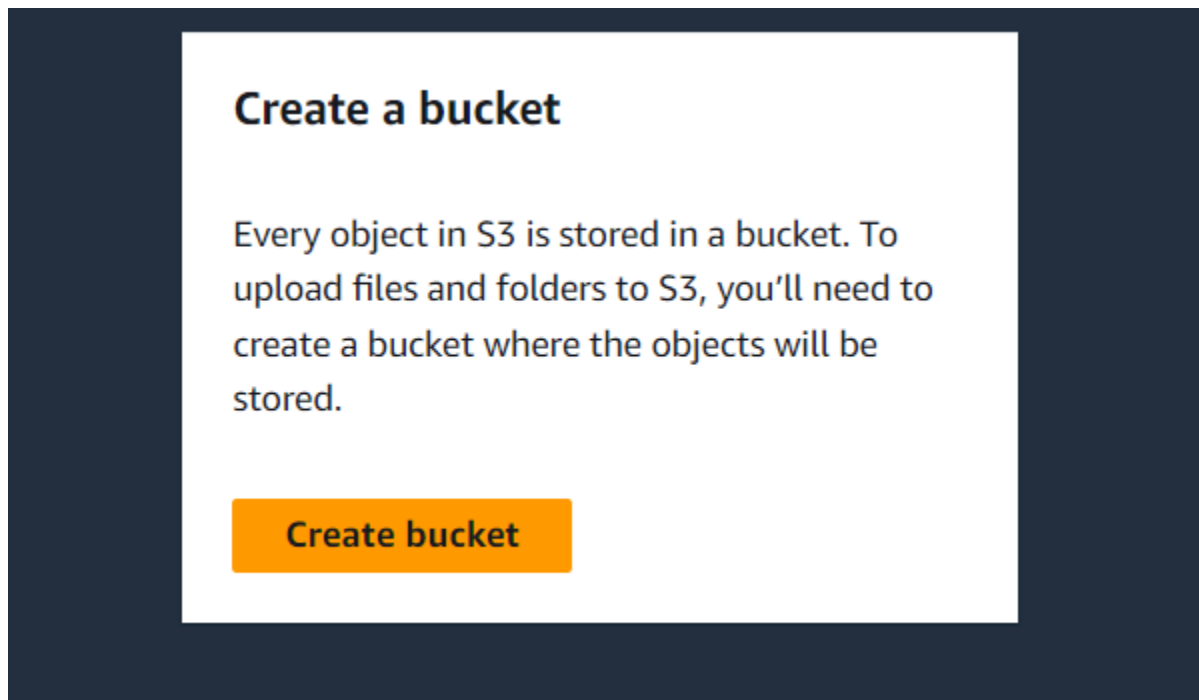
## Basic labs:

### 2. S3 Storage Fundamentals Lab

- **Objective:** To gain hands-on experience with Amazon S3 by performing basic storage operations.
- **Approach:** This lab involves creating an S3 bucket, uploading files to it, and setting up bucket policies for access control. Students will explore the S3 management console, learn about object storage, and understand the concepts of buckets and objects.
- **Goal:** Students will understand how to use S3 for storing and managing data, learn about S3 security and permissions, and become familiar with S3's user interface.

## Steps Involved

### 1) Create S3 bucket



### 2) Provide General Configuration

## General configuration

AWS Region

US East (N. Virginia) us-east-1 ▼

Bucket type [Info](#)

☒ **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 - New**

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 [Info](#)

first-bucket-sonu

Bucket name must be unique within the global namespace and follow the bucket naming rules. [See rules for bucket naming](#) 

Copy settings from existing bucket - *optional*

Only the bucket settings in the following configuration are copied.

**Choose bucket**

Format: s3://bucket/prefix

### 3) Block all public access

☒ **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](#) 

4) Click on Create Bucket

, and configure additional bucket settings.

Cancel

Create bucket

© 2024, Amazon V

5) The bucket is then created.

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

Buckets are containers for data stored in S3. [Learn more](#)


	Name	AWS Region	Access
<input type="radio"/>	<a href="#">first-bucket-sonu</a>	US East (N. Virginia) us-east-1	<a href="#">Bucket and objects not public</a>

6) Click on Upload button and upload your file.

▼	Last modified	▼	Size
---	---------------	---	------

No objects

You don't have any objects in this bucket.

 Upload


7) The file has been uploaded.

Files and folders

Configuration

Files and folders (1 Total, 311.0 B)

Find by name

Name	Folder	Type	Size	Status	Error
hello.html	-	text/html	311.0 B	 Succeeded	-

8) Click on Object URL. The link redirects to the new tab. The error is shown as below. When the file is viewed from object url link, the permission accessed denied is shown, as the “Block all public access” setting was checked during file upload.

hello.html [Info](#)

Copy S3 URI

Download

Open

PropertiesPermissionsVersions

Object overview

Owner

awslabsc0w6974788t1703159690

AWS Region

US East (N. Virginia) us-east-1

Last modified

February 23, 2024, 08:52:08 (UTC+05:45)


Size

311.0 B


Type

html


Key

 hello.html


S3 URI

 s3://first-bucket-sonu/hello.html


Amazon Resource Name (ARN)

 arn:aws:s3:::first-bucket-sonu/hello.html

Entity tag (Etag)

 00b3fc6dd2622b8de394b3e953f129da

Object URL

 <https://first-bucket-sonu.s3.amazonaws.com/hello.html>

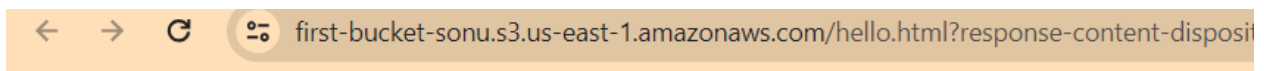
Feedback

© 2024 Amazon Web Services, Inc. or its affiliates

This XML file does not appear to have any style information associated with it. The document tree is shown below.

```
<?xml version="1.0" encoding="UTF-8" ?>
<Error>
  <Code>AccessDenied</Code>
  <Message>Access Denied</Message>
  <RequestId>EZEH1J1KPWFY3</RequestId>
  <HostId>HgiQp1PLwXldaJygpJl8nhaRoyLSd4JAvW5gUaCUco5gHMNjStlgHH5WIupoLgn7egK00IE8rb0=</HostId>
</Error>
```

But if we click on Open button, it shows no error.



# Hello ,This is Amazon Web services

Lets get started with AWS.

## Setting up bucket policies for access control

- 9) Select “permissions” tab and “edit” button of “Bucket policy” section to edit the policies of the bucket, which will take to new screen of bucket policy.

first-bucket-sonu

Info

Objects

Properties

Permissions

Metrics

Management

Access Points

Permissions overview

Access

Bucket and objects not public

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

On

► Individual Block Public Access settings for this bucket

## 10) Select Policy generator

Edit bucket policy

Info

Bucket policy

Policy examples

Policy 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](#)

11) Select policy type as “S3 Bucket Policy”. Fill the form as required. In effect “deny” and in action “PutPbject” is selected.

## Step 1: Select Policy Type

A Policy is a container for permissions. The different types of policies you can create are an [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](#) t

Effect ☐ Allow ☒ Deny

Principal

Use a comma to separate multiple values.

AWS Service Amazon S3

Use multiple statements to add permissions for more than one s

Actions 1 Action(s) Selected ☐ A

Amazon Resource Name (ARN)

- ☐ PutMetricsConfiguration
- ☐ PutMultiRegionAccessPointPolicy
- ☒ PutObject

(Bucket)

12) Copy the ARN value of s3 bucket from properties section.

first-bucket-sonu [Info](#)

Objects

Properties

Permissions

Metrics

Management


Access Point

Bucket overview

AWS Region

US East (N. Virginia) us-east-1

Amazon Resource Name (ARN)

 arn:aws:s3:::first-bucket-sonu

**13 Add /\* after bucket ARN value. Then, add conditions for denying specific object.**

**Here, we are denying any objects with Key s3:x-amz-server-side-encryption set to Null.**

## 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**  ☐ All Services  
Use multiple statements to add permissions for more than one service.

**Actions**  ☐ All Actions ('\*')

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

[Add Conditions \(Optional\)](#)

### Add Conditions (Optional)

Hide

Conditions are any restrictions or details about the statement. ([More Details](#)).

<b>Condition</b>	<input type="text" value="Null"/>
<b>Key</b>	<input type="text" value="s3:x-amz-server-side-encryption"/>
<b>Value</b>	<input type="text"/>
<input type="button" value="Add Condition"/>	

Condition	Keys
Null	<ul style="list-style-type: none"><li>s3:x-amz-server-side-encryption: "true"</li></ul>



14) Click on Generate Policy and copy the JSON policy document.

```
sonu
    "s3:x-amz-server-side-e
    "true"
```

### 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](#)

Amazon Resource Name (ARN)

**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": "Policy1708658680719",
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "Stmnt1708658676338",
      "Action": [
        "s3:PutObject"
      ],
      "Effect": "Deny",
      "Resource": "arn:aws:s3:::first-bucket-sonu",
      "Condition": {
        "Null": {
          "s3:x-amz-server-side-encryption": "true"
        }
      },
      "Principal": "*"
    }
  ]
}
```


15) Add the copied json document into the bucket policy. And click on “Save changes” button.

# Edit bucket policy [Info](#)

## Bucket policy

The bucket policy, written in JSON, provides access to the objects stored in the bucket. Bu

Bucket ARN

 arn:aws:s3:::first-bucket-sonu

## Policy


```
1 ▼ {  
2   "Id": "Policy1708658680719",  
3   "Version": "2012-10-17",  
4 ▼   "Statement": [  
5 ▼     {  
6       "Sid": "Stmt1708658676338",  
7 ▼     "Action": [  
8       "s3:PutObject"  
9     ],
```

[Preview external access](#)

Cancel


Save changes

**The bucket policy has been successfully edited.**

 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](#)

**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](#)

```
{
  "Version": "2012-10-17",
  "Id": "Policy1708658680719",
  "Statement": [
```

**For testing the policy, we can upload the same html file without specifying any encryption key. The access is denied in this condition. The file can be uploaded successfully only after adding encryption key otherwise it throws an error.**


### Server-side encryption [Info](#)

Server-side encryption protects data at rest.

#### Server-side encryption

☒ **Do not specify an encryption key**  
The bucket settings for default encryption are used to encrypt objects when storing them in Amazon S3.

☐ **Specify an encryption key**  
The specified encryption key is used to encrypt objects before storing them in Amazon S3.

 **If your bucket policy requires objects to be encrypted with a specific encryption key, you must specify the same encryption key when you upload objects. Otherwise, uploads will fail.**