

Lesson-End Project

Deploying Static Website with S3 Buckets

Project agenda: To demonstrate the implementation of S3 buckets for hosting static website content

Description: As an organizational admin at a tech company, you are tasked with delivering HTML content through a static website. Your current project involves utilizing the capabilities of an S3 bucket for seamless content deployment. The goal is to set up and configure an S3 bucket to host a static website, ensuring your HTML content is easily accessible and efficiently delivered to users. This approach will leverage AWS's scalable infrastructure, providing a reliable and cost-effective solution for hosting static web content.

Tools required: AWS

Prerequisites: AWS free-tier account

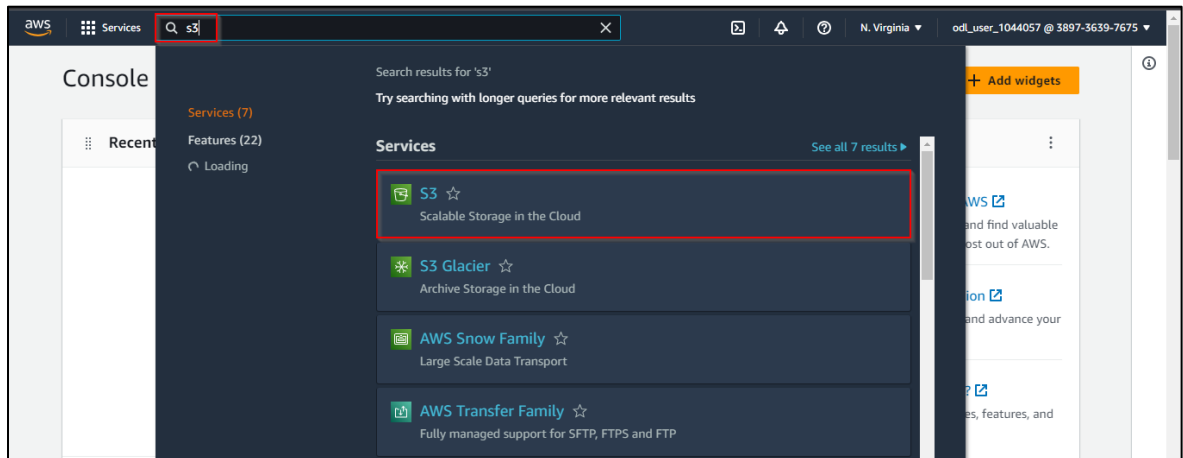
Expected deliverables: An S3 bucket configured to host the static website content.

Steps to be followed:

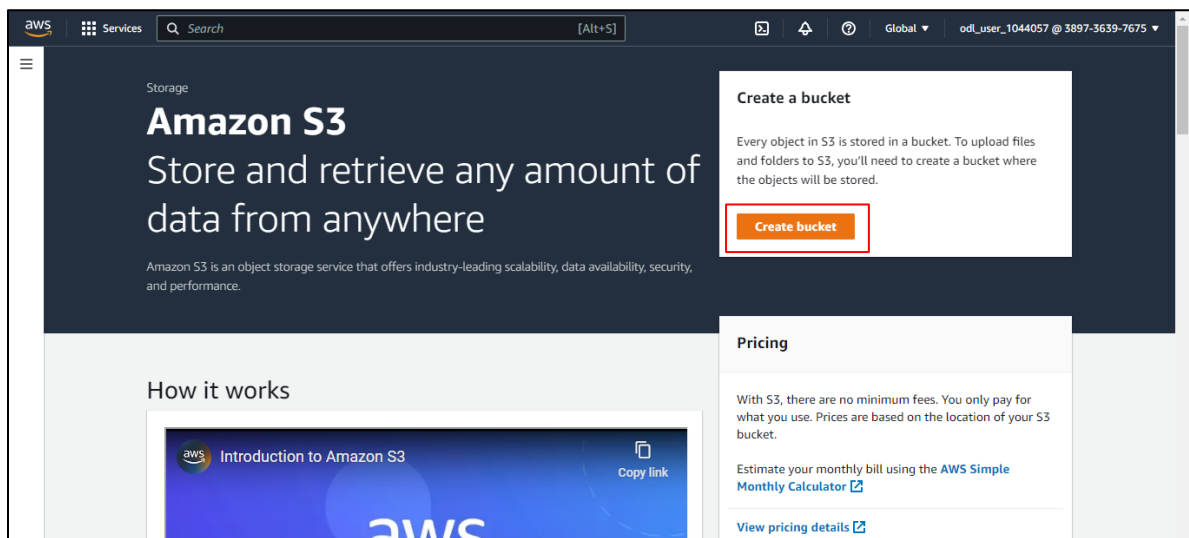
1. Create an S3 bucket
2. Generate a bucket policy
3. Enable static website hosting
4. Test and verify the hosted website content

Step 1: Create an S3 bucket

1.1 Navigate to the AWS Management Console and select the S3 service



1.2 Click Create bucket



1.3 Set the **Bucket name** to **my-webcontent-demo**

Create bucket Info

Buckets are containers for data stored in S3.

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
my-webcontent-demo
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.

Format: s3://bucket/prefix

1.4 Select the **ACLs enabled** and **Bucket owner preferred** options

Learn more'"/>

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.

☐ **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.

⚠️ 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.

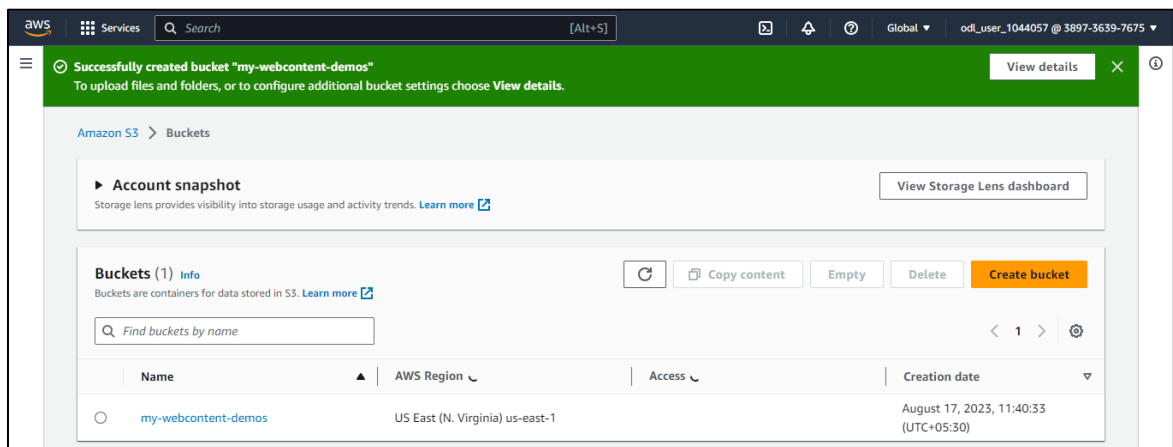
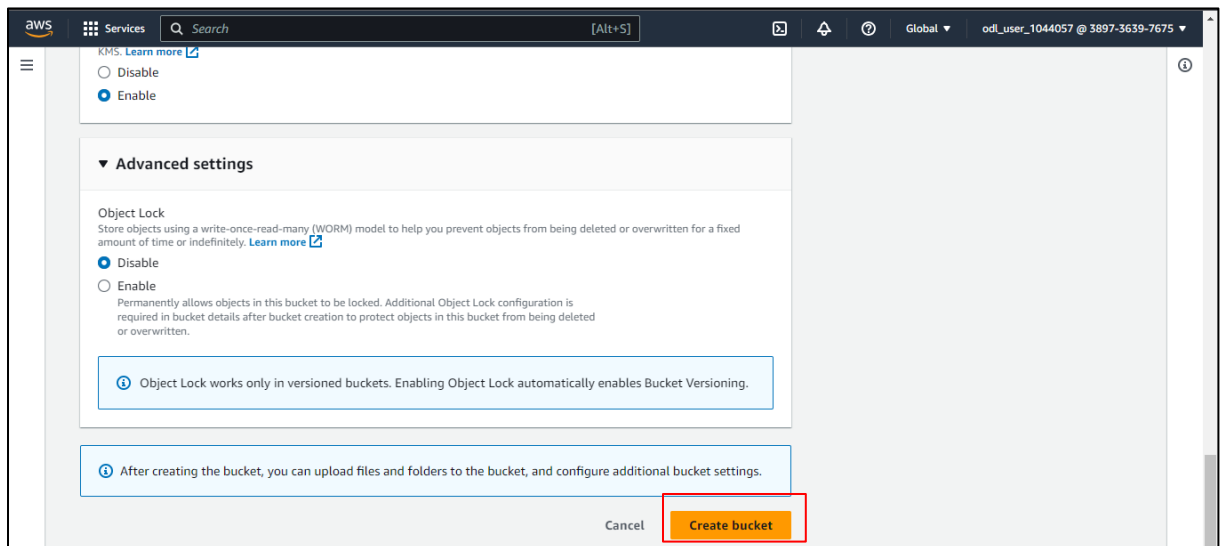
Object Ownership

☒ **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.

ℹ️ 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](#)

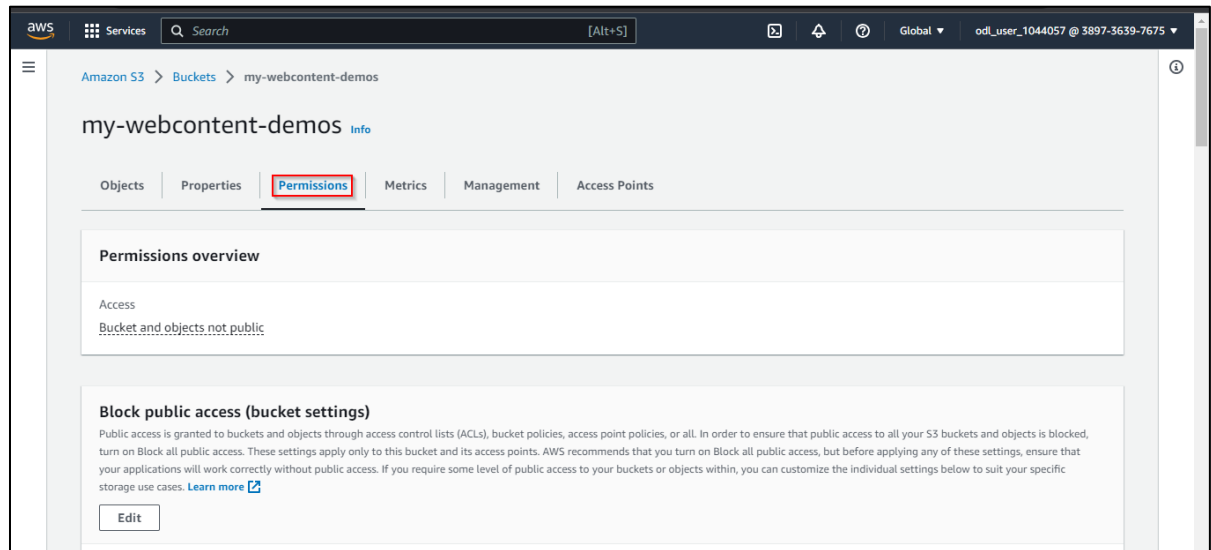
1.5 Click on **Create bucket**



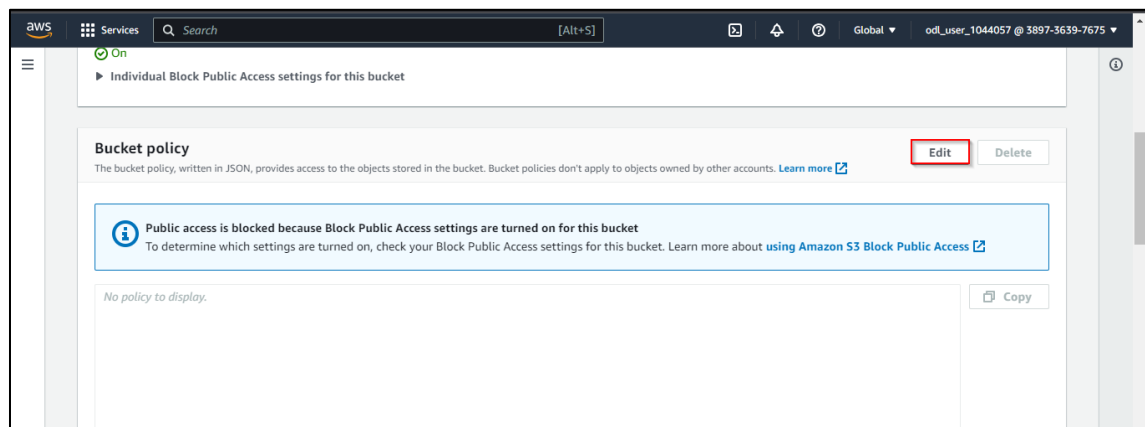
The S3 bucket **my-webcontent-demo** has been successfully created.

Step 2: Generate a bucket policy

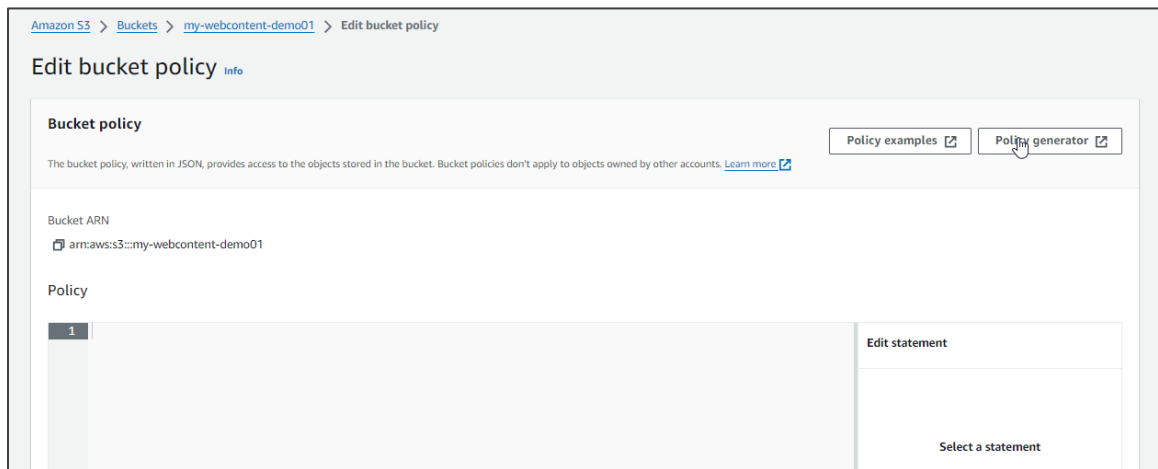
2.1 Open the newly created bucket and navigate to the **Permissions** tab



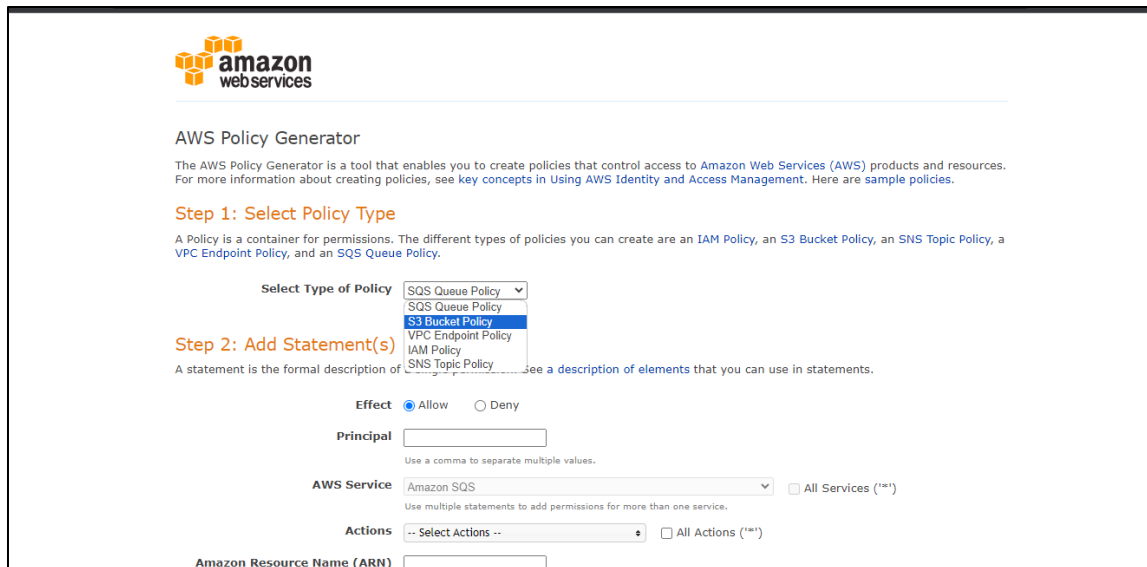
2.2 Scroll down and click **Edit** to modify permissions



2.3 Click on the **Policy generator**



2.4 Select **S3 Bucket Policy** as the policy type



Amazon S3 > Buckets > my-webcontent-demo01

my-webcontent-demo01 [Info](#)

Objects

Properties


Permissions

Metrics

Management

Access Points

Bucket overview

<div>AWS Region</div> <div>US East (N. Virginia) us-east-1</div>	<div>Amazon Resource Name (ARN)</div> <div> arn:aws:s3::my-webcontent-demo01</div>	<div>Creation date</div> <div>August 13, 2024, 14:29:23 (UTC+05:30)</div>
------------------------------------------------------------------	-----------------------------------------------------------------------------------------------------------------------------------------------------------------------	---------------------------------------------------------------------------

Bucket Versioning

Edit

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

Disabled

Multi-factor authentication (MFA) delete

2.7 Paste the **ARN** in the **Amazon Resource Name (ARN)** field and click **Add Statement**

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 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.

Add one or more statements above to generate a policy.

2.8 Click on the **Generate Policy** button

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](#)

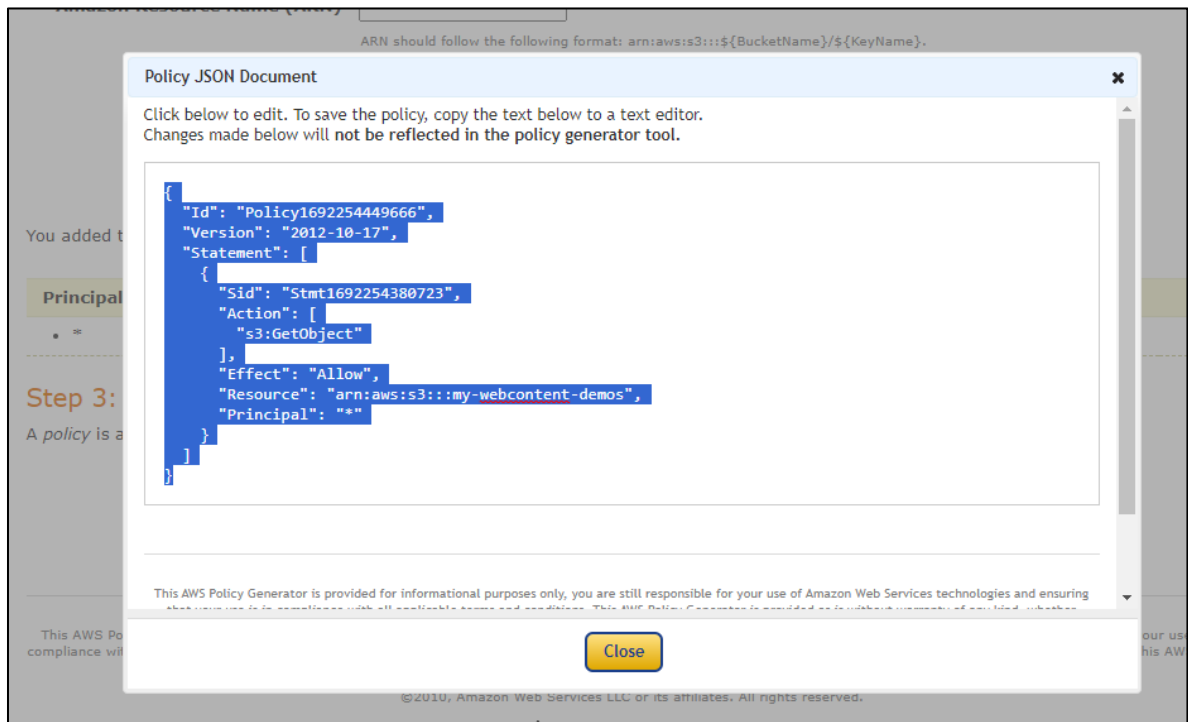
This AWS Policy Generator is provided for informational purposes only, you are still responsible for your use of Amazon Web Services technologies and ensuring that your use is in compliance with all applicable terms and conditions. This AWS Policy Generator is provided as is without warranty of any kind, whether express, implied, or statutory. This AWS Policy Generator does not modify the applicable terms and conditions governing your use of Amazon Web Services technologies.

©2010, Amazon Web Services LLC or its affiliates. All rights reserved.

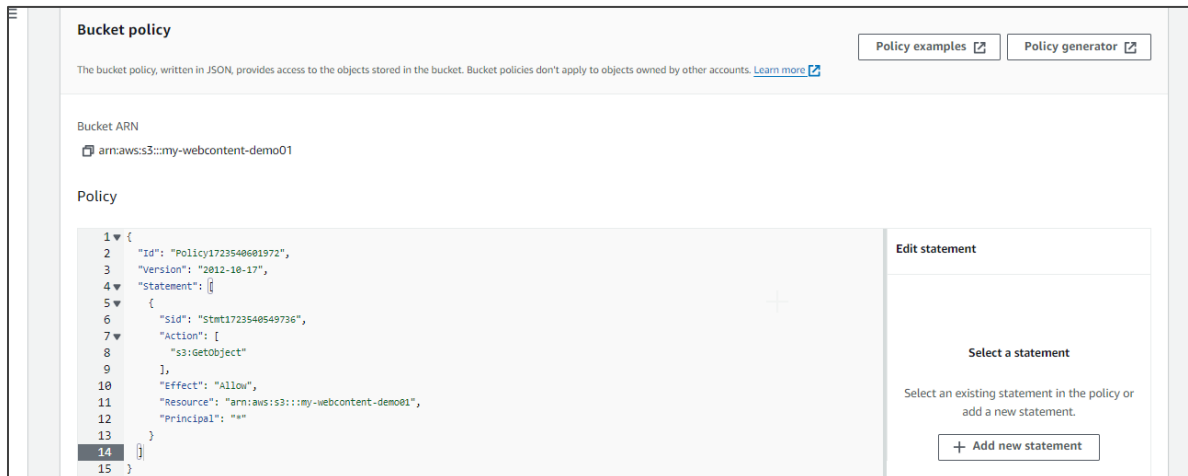
An **amazon.com** company

The bucket policy has been successfully generated.

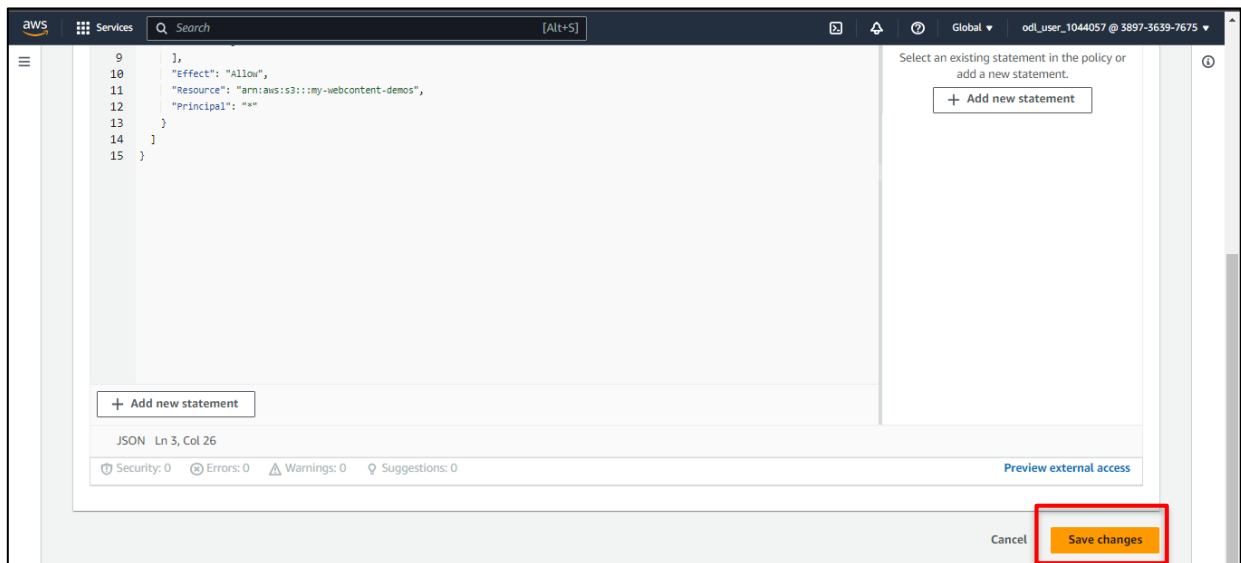
2.9 Copy the generated Policy JSON code

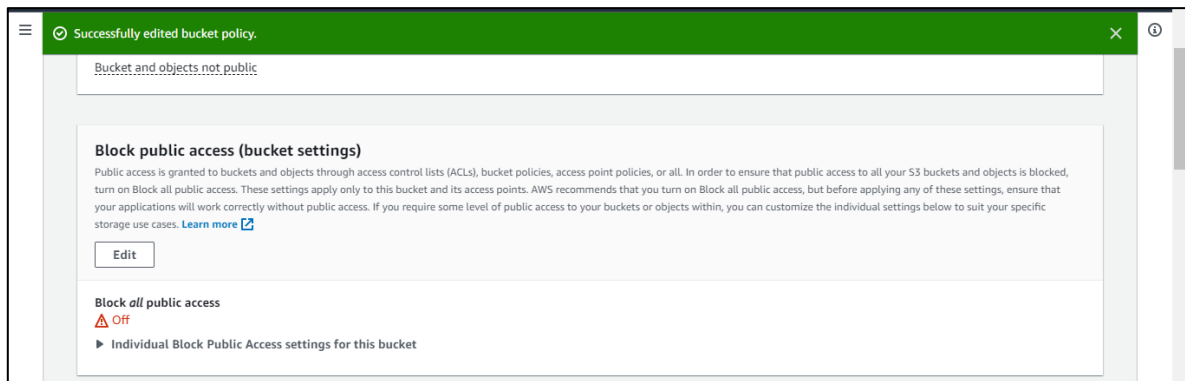


2.10 Paste the Policy JSON code in the Edit bucket policy section



2.11 Click on **Save changes**

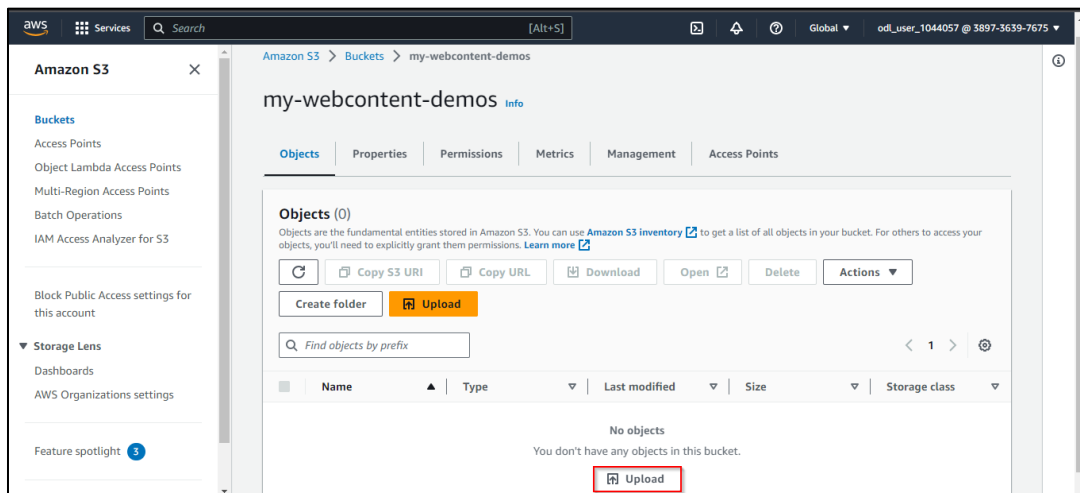




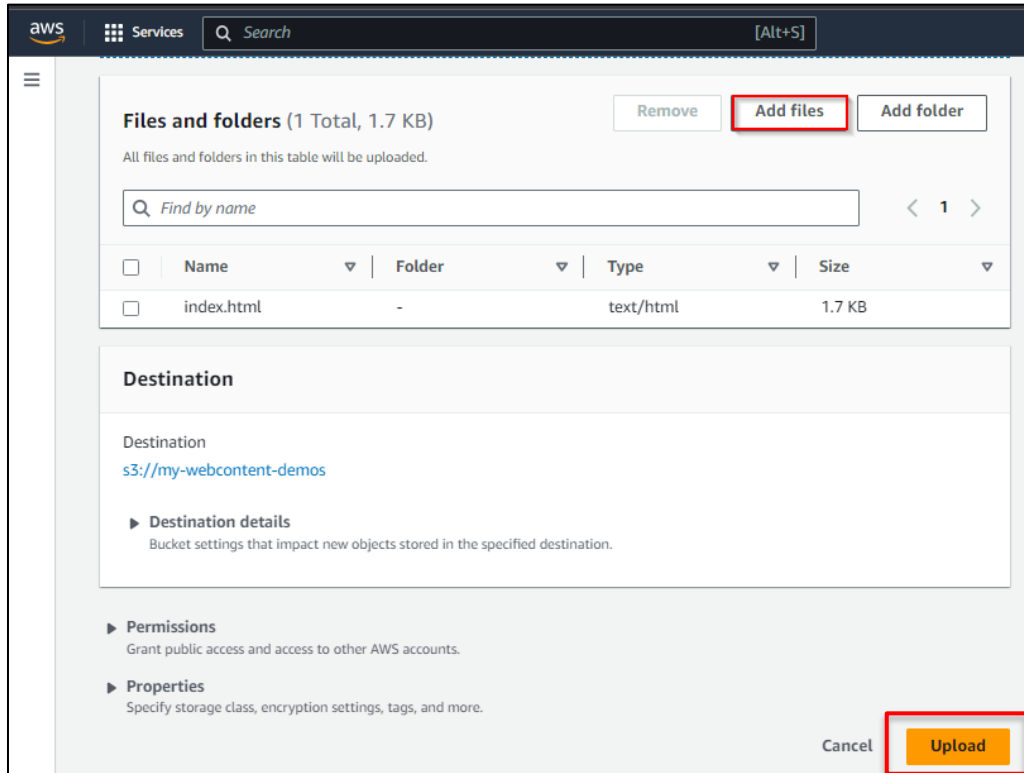
The bucket policy has been successfully added. If the bucket policy does not change, click on **Edit** in the **Block public access** section, and disable all public access.

Step 3: Enable static website hosting

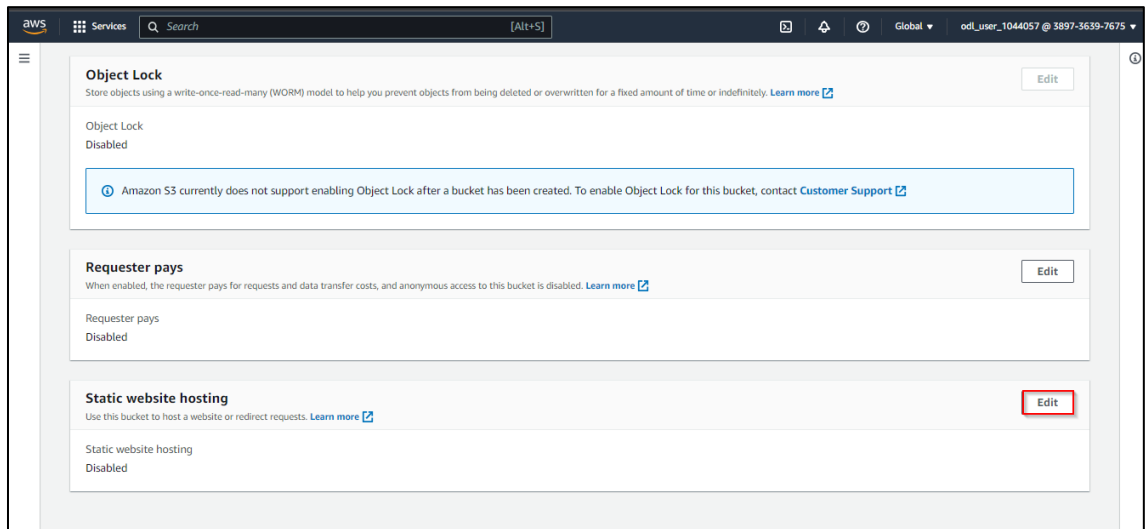
3.1 Navigate to **my-webcontent-demos**, click on the **Objects** tab, and then select **Upload**



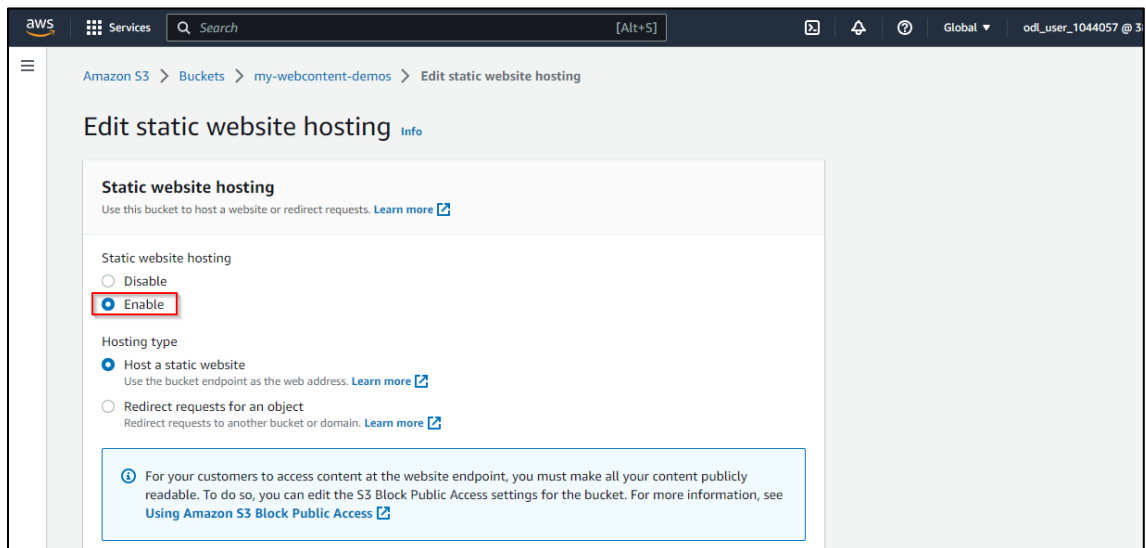
3.2 Click on **Add files**, upload any **index.html** file inside the S3 bucket **my-webcontent-demos**, and click on **Upload**



3.3 Navigate to the **Properties** tab and click on **Edit** in the **Static website hosting** section



3.4 Enable **Static website hosting**, specify the default page, and click **Save changes**



aws Services Search [Alt+S] Global od_user_1044057 @ 3

Amazon S3 > Buckets > my-webcontent-demos > Edit static website hosting

Edit static website hosting [Info](#)

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

Static website hosting

☐ Disable

☒ **Enable**

Hosting type

☒ **Host a static website**
Use the bucket endpoint as the web address. [Learn more](#)

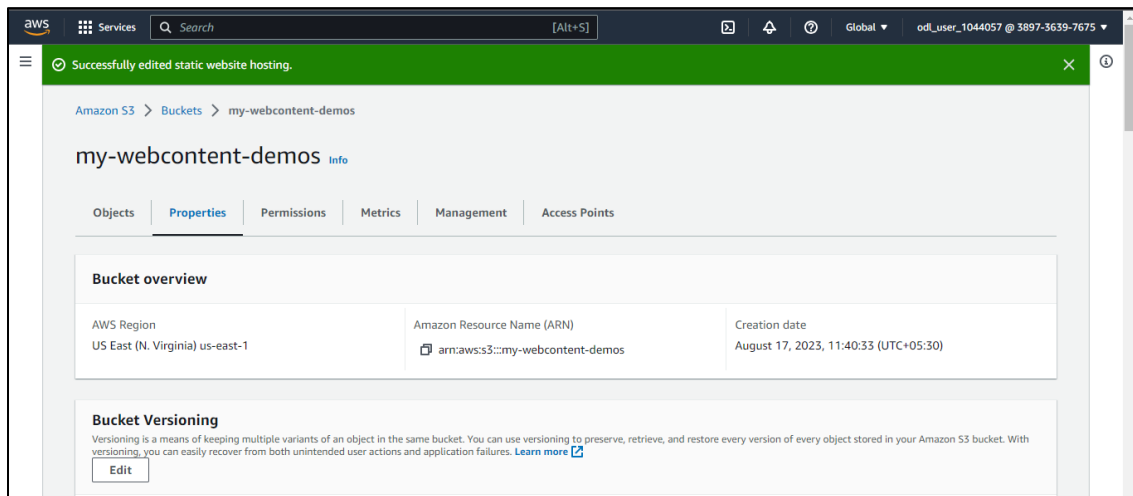
☐ Redirect requests for an object
Redirect requests to another bucket or domain. [Learn more](#)

Info For your customers to access content at the website endpoint, you must make all your content publicly readable. To do so, you can edit the S3 Block Public Access settings for the bucket. For more information, see [Using Amazon S3 Block Public Access](#)

Index document
Specify the home or default page of the website.

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

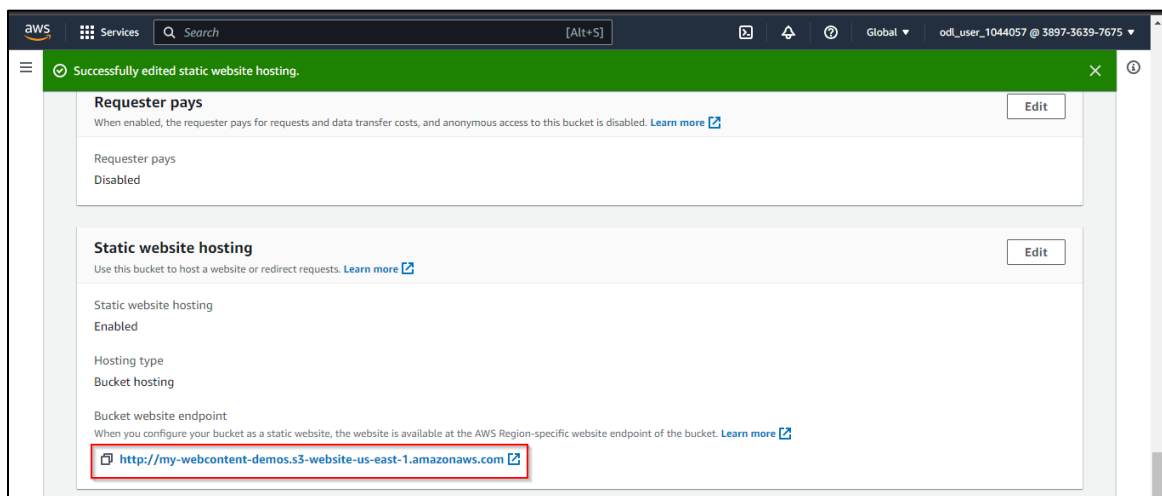
Redirection rules - optional
Redirection rules, written in JSON, automatically redirect webpage requests for specific content. [Learn more](#)

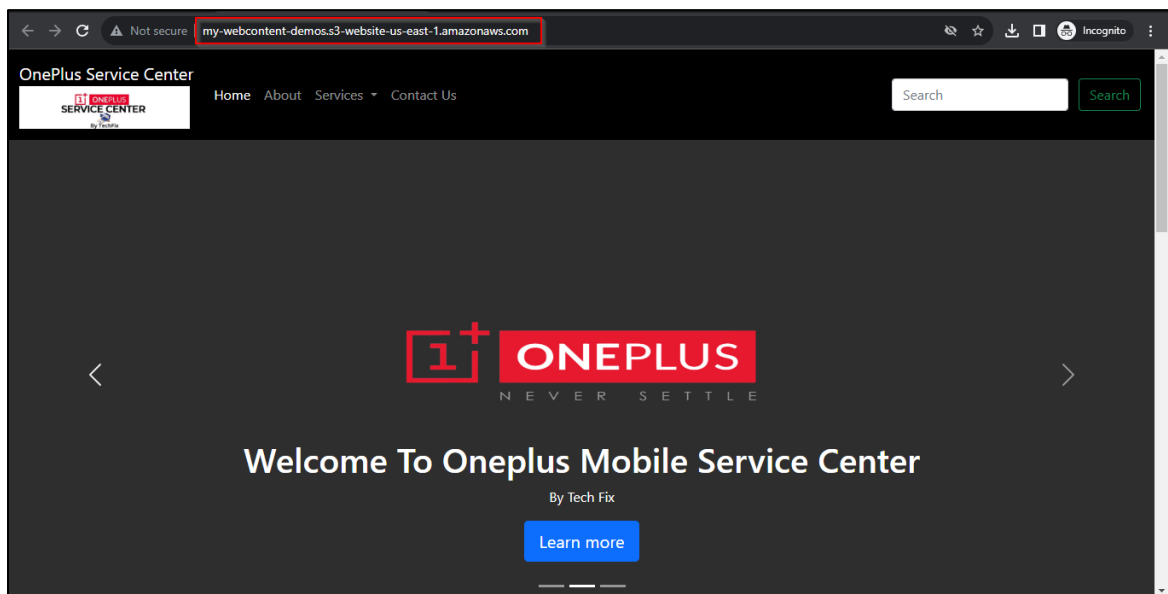


The static website hosting has been successfully edited.

Step 4: Test and verify the hosted website content

4.1 Navigate to the **Properties** tab, scroll to **Static website hosting**, and click the **Bucket website endpoint** link





By following these steps, you have effectively established a streamlined process for hosting static website content using an S3 bucket, ensuring secure access and efficient deployment.