Module 6: S3 Website Hosting Assignment

Assignment Submitted By:-Hitesh Chauhan
Course Offered: -Advanced Cloud Computing and Devops
Assignment By: -Intellipaat
Trainer: -Puneet Gavri
Date Of Submission: -24/10/2024

Problem Statement:

You work for XYZ Corporation. Their application requires a storage service that can store files and publicly share them if required. Implement S3 for the same.

Tasks To Be Performed:

1. Use the created bucket in the previous task to host static websites, upload an index.html file and error.html page.

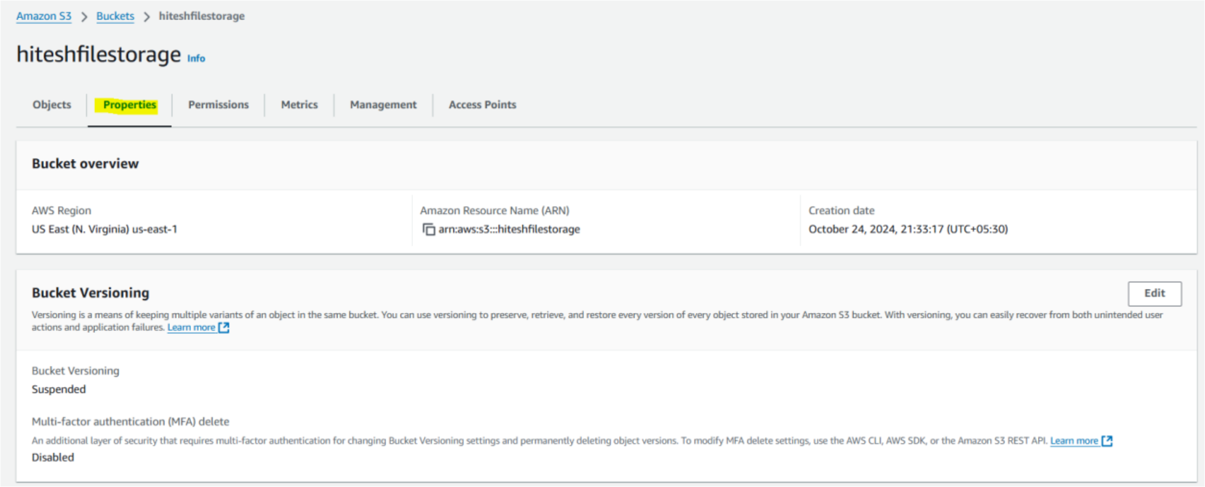
2. Add a lifecycle rule for the bucket:

a. Transition from Standard to Standard-IA in 60 days

b. Expiration in 200 days

S3 Website Hosting Assignment

Now select the bucket you want to use for creating a static website, Click on Properties



Bucket overview

AWS Region	Amazon Resource Name (ARN)	Creation date
US East (N. Virginia) us-east-1	arn:aws:s3:::hiteshfilestorage	October 24, 2024, 21:33:17 (UTC+05:30)

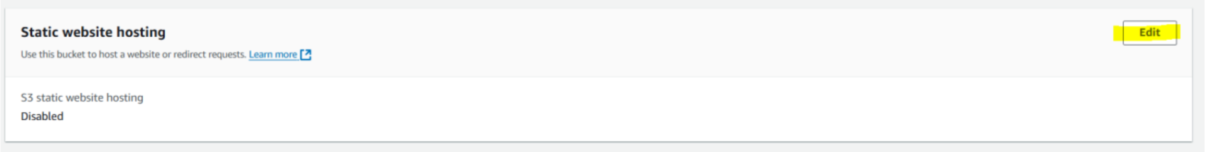
Bucket Versioning

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
Suspended

Multi-factor authentication (MFA) delete
An additional layer of security that requires multi-factor authentication for changing Bucket Versioning settings and permanently deleting object versions. To modify MFA delete settings, use the AWS CLI, AWS SDK, or the Amazon S3 REST API. Learn more
Disabled

Scroll Down The Page and you will see static web hosting option

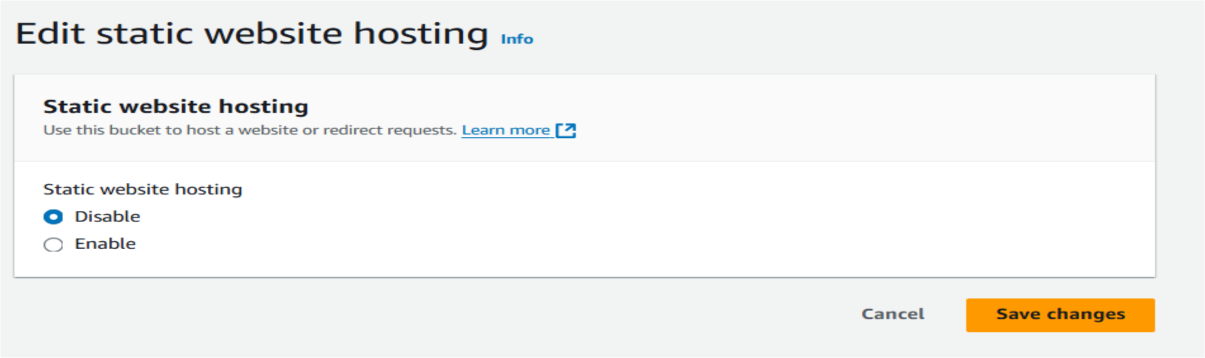


Static website hosting

Use this bucket to host a website or redirect requests. Learn more

S3 static website hosting
Disabled

Go To edit By default you will see the disable but you want to enable this option



Edit static website hosting Info

Static website hosting

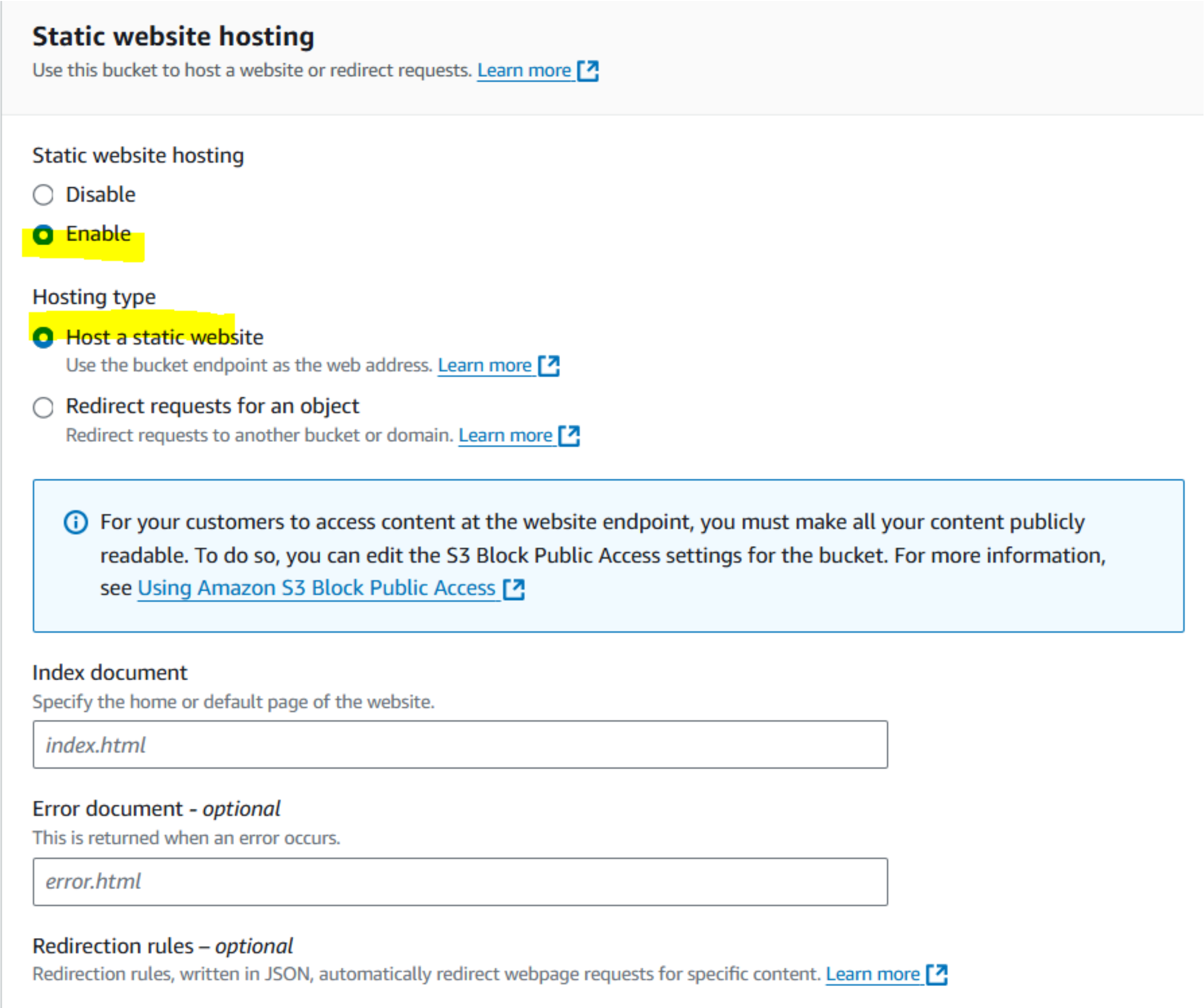
Use this bucket to host a website or redirect requests. Learn more

Static website hosting

● Disable

○ Enable

After enable this options.



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

ⓘ 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.

index.html

Error document - *optional*

This is returned when an error occurs.

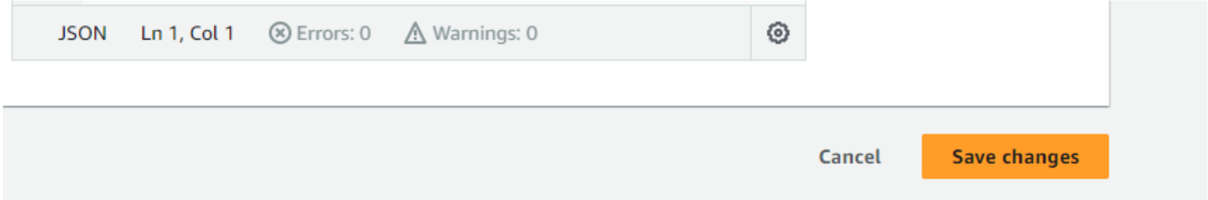
error.html

Redirection rules – *optional*

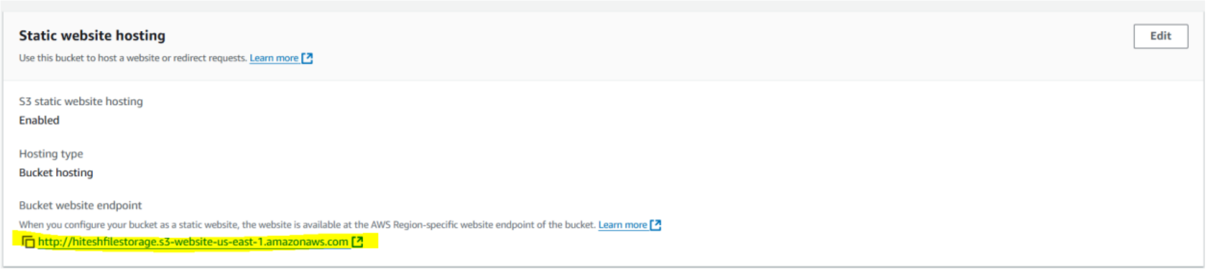
Redirection rules, written in JSON, automatically redirect webpage requests for specific content. Learn more

Select Enable

Provide the index.html and error.html file name they should be case sensitive and name should be matching as per the apache default configuration then click save changes.



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



Static website hosting

Use this bucket to host a website or redirect requests. Learn more

S3 static website hosting
Enabled

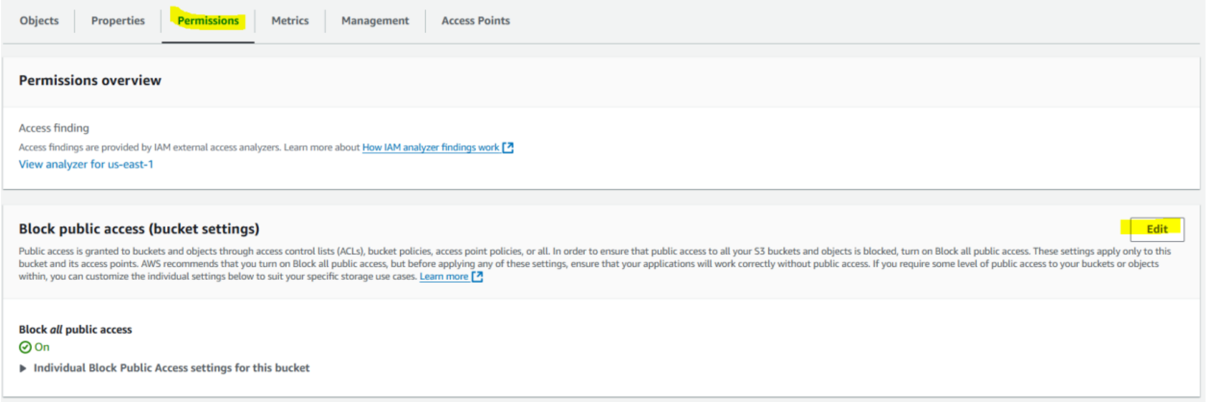
Hosting type
Bucket hosting

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://hiteshfilestorage.s3-website-us-east-1.amazonaws.com

Once the website is enable it will provide you the endpoint details, you have to copy the URL and then browse is using the browser.

Before that, you have to upload index.html and error.html to the S3 bucket.

Go to permission and click edit.



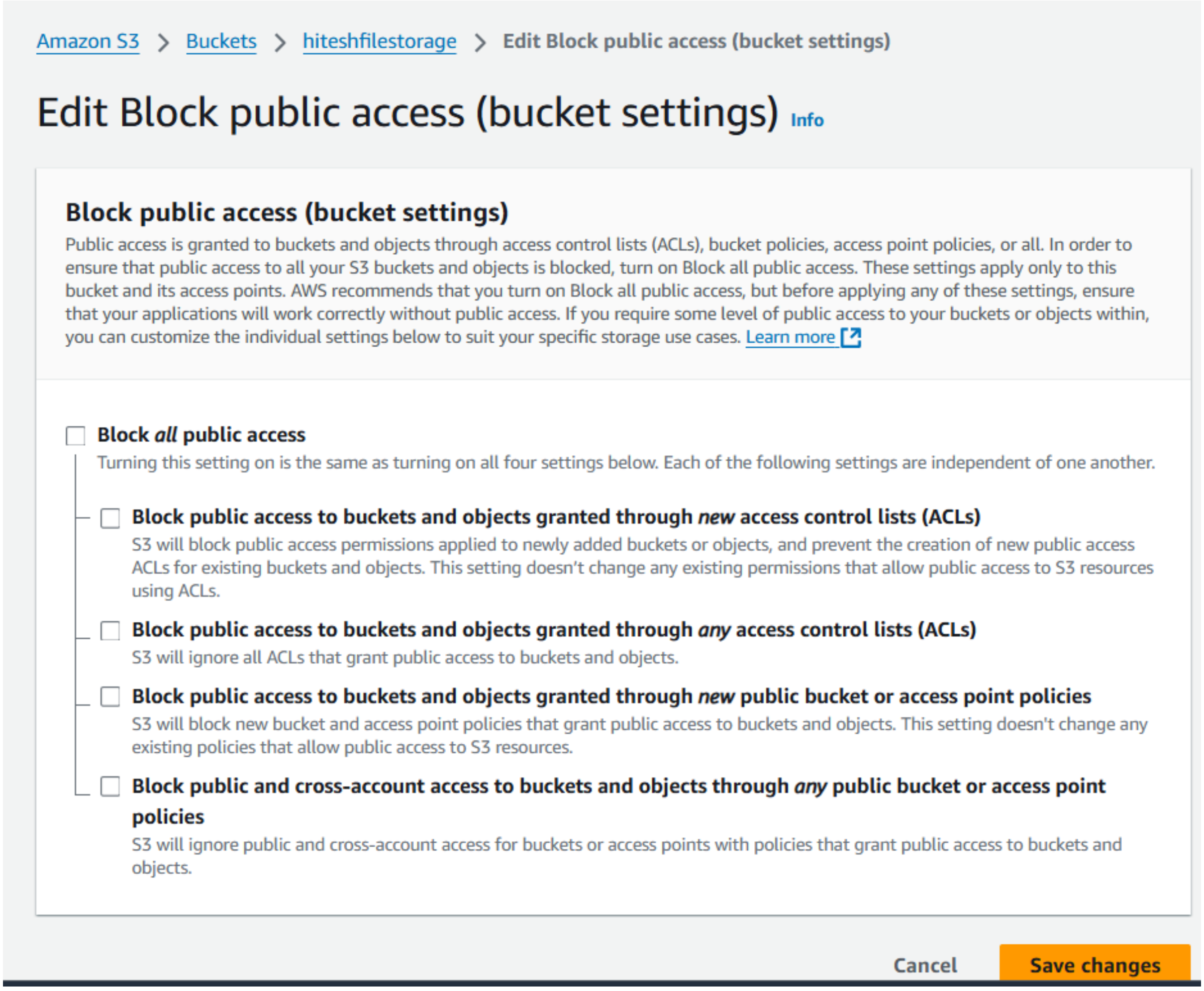
Permissions overview

Access finding
Access findings are provided by IAM external access analyzers. Learn more about How IAM analyzer findings work
View analyzer for us-east-1

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
✓ On
▶ Individual Block Public Access settings for this bucket



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

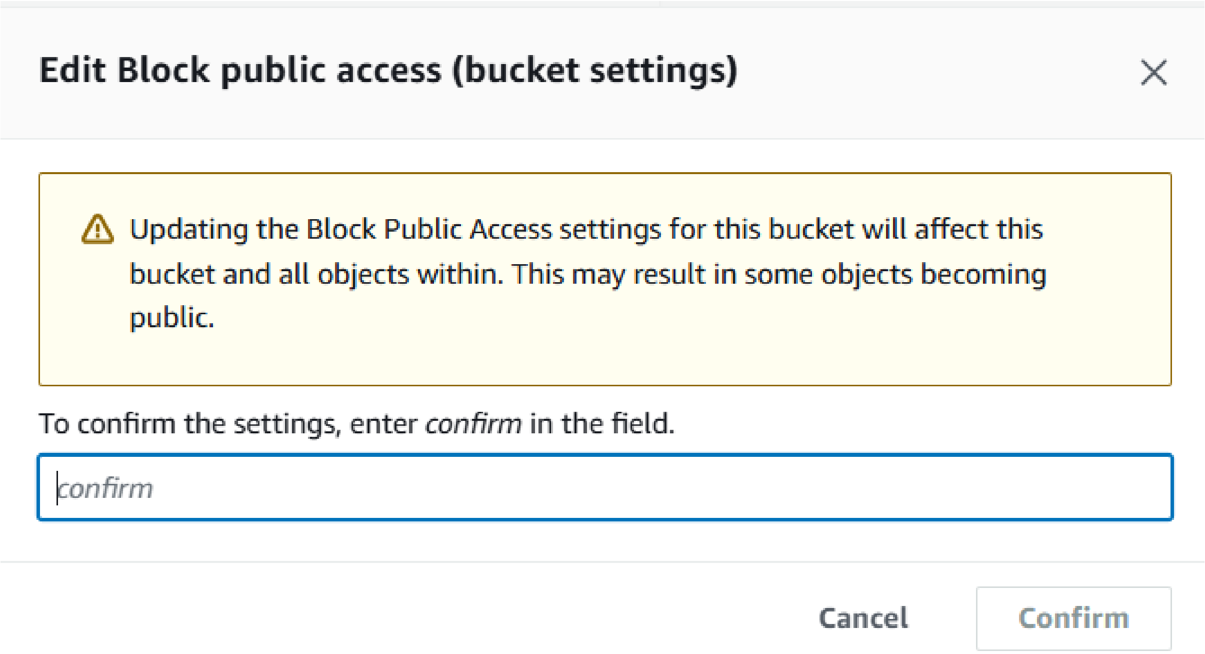
Edit Block public access (bucket settings) Info

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.



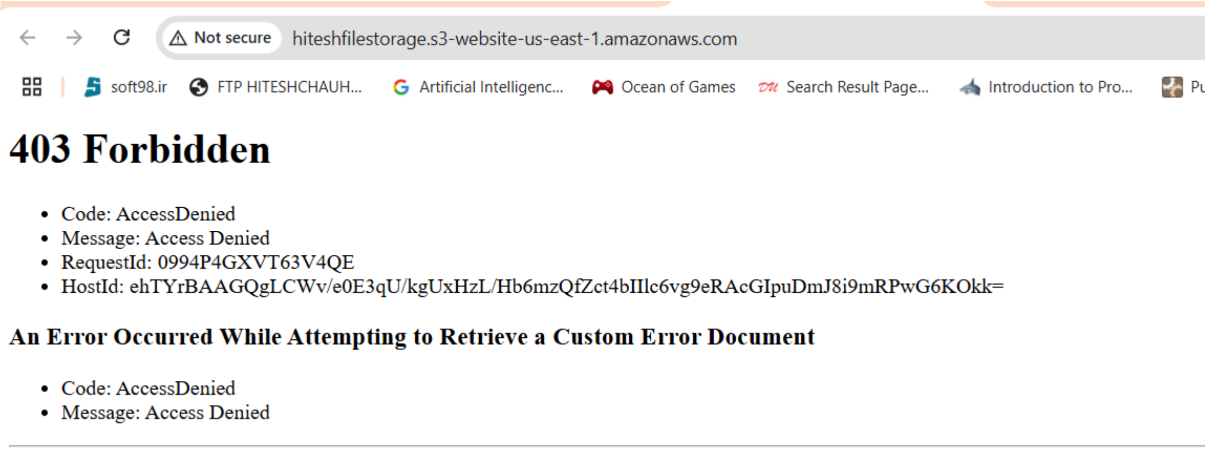
Edit Block public access (bucket settings)

⚠ 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.

confirm

Once your enable the public access on the S3 bucket, you need to write the bucket policy otherwise it will give the below error message.

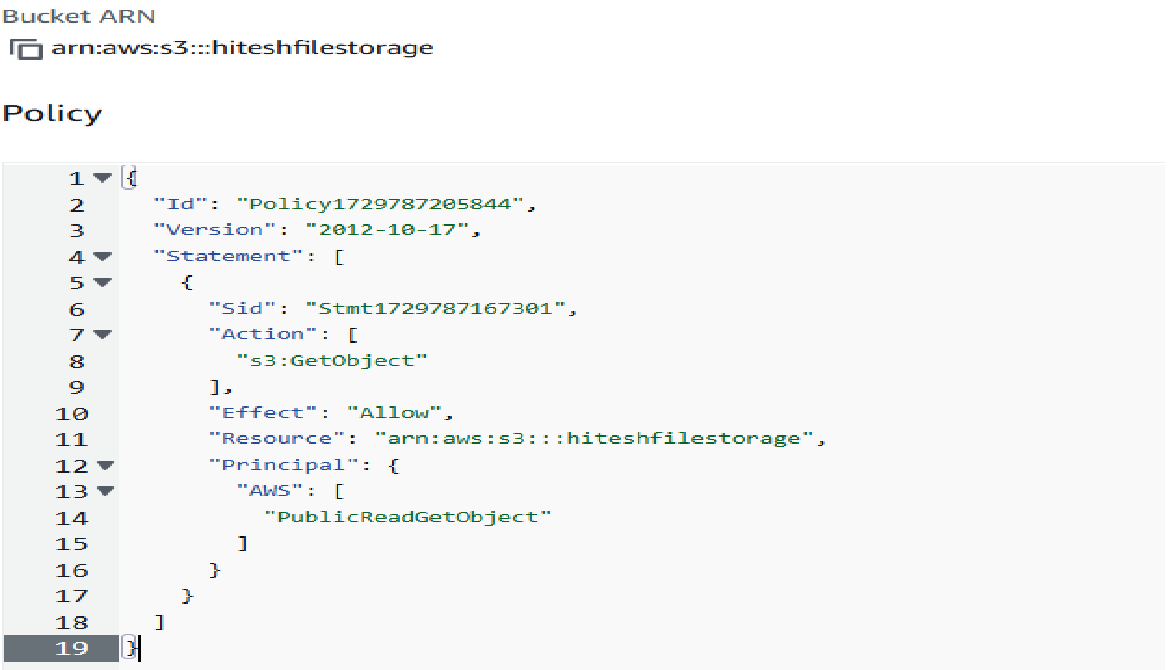


403 Forbidden

- Code: AccessDenied
- Message: Access Denied
- RequestId: 0994P4GXVT63V4QE
- HostId: ehTYrBAAGQgLCWv/e0E3qU/kgUxHzL/Hb6mzQfZct4bIIlc6vg9eRAcGIpuDmJ8i9mRPwG6KOkk=

An Error Occurred While Attempting to Retrieve a Custom Error Document

- Code: AccessDenied
- Message: Access Denied



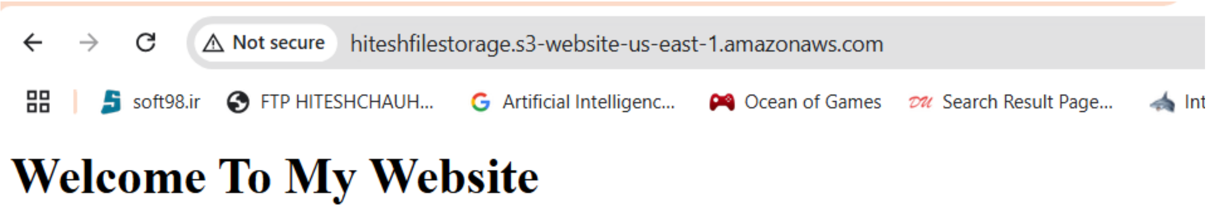
Bucket ARN
arn:aws:s3:::hiteshfilestorage

Policy

```
{
  "Id": "Policy1729787205844",
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "Stmt1729787167301",
      "Action": [
        "s3:GetObject"
      ],
      "Effect": "Allow",
      "Resource": "arn:aws:s3:::hiteshfilestorage",
      "Principal": {
        "AWS": [
          "PublicReadGetObject"
        ]
      }
    }
  ]
}
```

```
{
  "Version": "2012-10-17",
  "Id": "Policy1729787205844",
  "Statement": [
    {
      "Sid": "PublicReadGetObject",
      "Effect": "Allow",
      "Principal": "*",
      "Action": "s3:GetObject",
      "Resource": "arn:aws:s3:::hiteshfilestorage/*"
    }
  ]
}
```

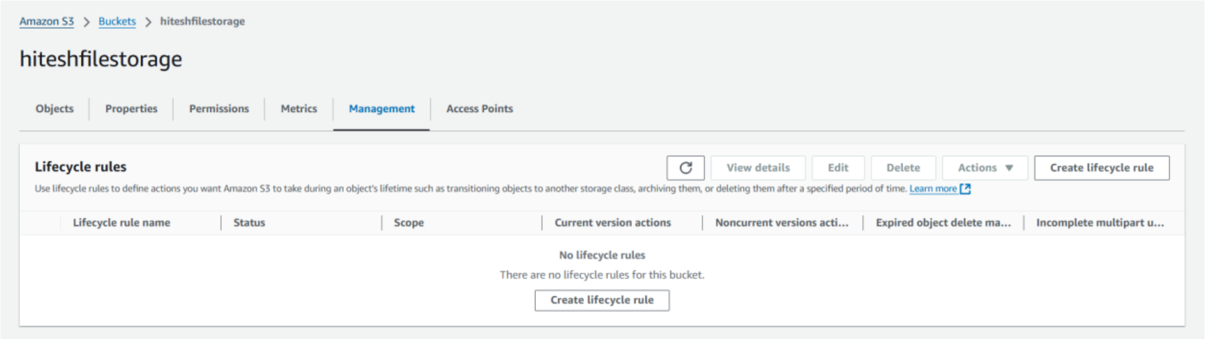
Add the bucket policy as shown above that’s it your static website is published successfully.


Not secure
hiteshfilestorage.s3-website-us-east-1.amazonaws.com
soft98.ir
FTP HITESHCHAUH...
Artificial Intelligenc...
Ocean of Games
Search Result Page...
Int

Welcome To My Website

Adding Life Cycle Policies

Select the S3 bucket you want to apply the Lifecycle rules, **S3 bucket Management Lifecycle rules Create lifecycle rule**



hiteshfilestorage

Lifecycle rules

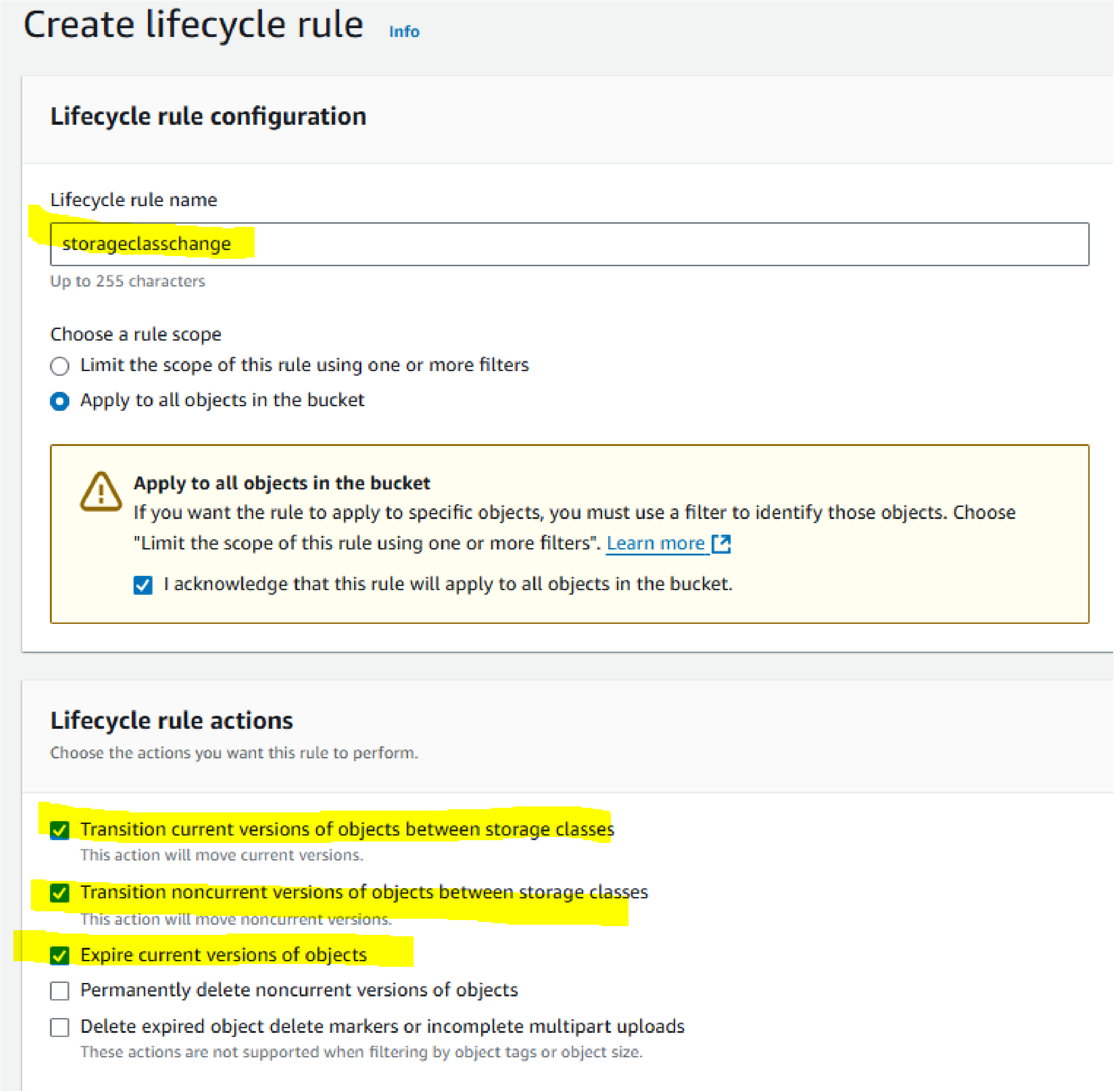
Use lifecycle rules to define actions you want Amazon S3 to take during an object's lifetime such as transitioning objects to another storage class, archiving them, or deleting them after a specified period of time.

Lifecycle rule name	Status	Scope	Current version actions	Noncurrent versions acti...	Expired object delete ma...	Incomplete multipart u...

No lifecycle rules

There are no lifecycle rules for this bucket.

Create lifecycle rule



Create lifecycle rule Info

Lifecycle rule configuration

Lifecycle rule name

storageclasschange

Up to 255 characters

Choose a rule scope

○ Limit the scope of this rule using one or more filters

● Apply to all objects in the bucket

Apply to all objects in the bucket
If you want the rule to apply to specific objects, you must use a filter to identify those objects. Choose "Limit the scope of this rule using one or more filters". Learn more

☑ I acknowledge that this rule will apply to all objects in the bucket.

Lifecycle rule actions

Choose the actions you want this rule to perform.

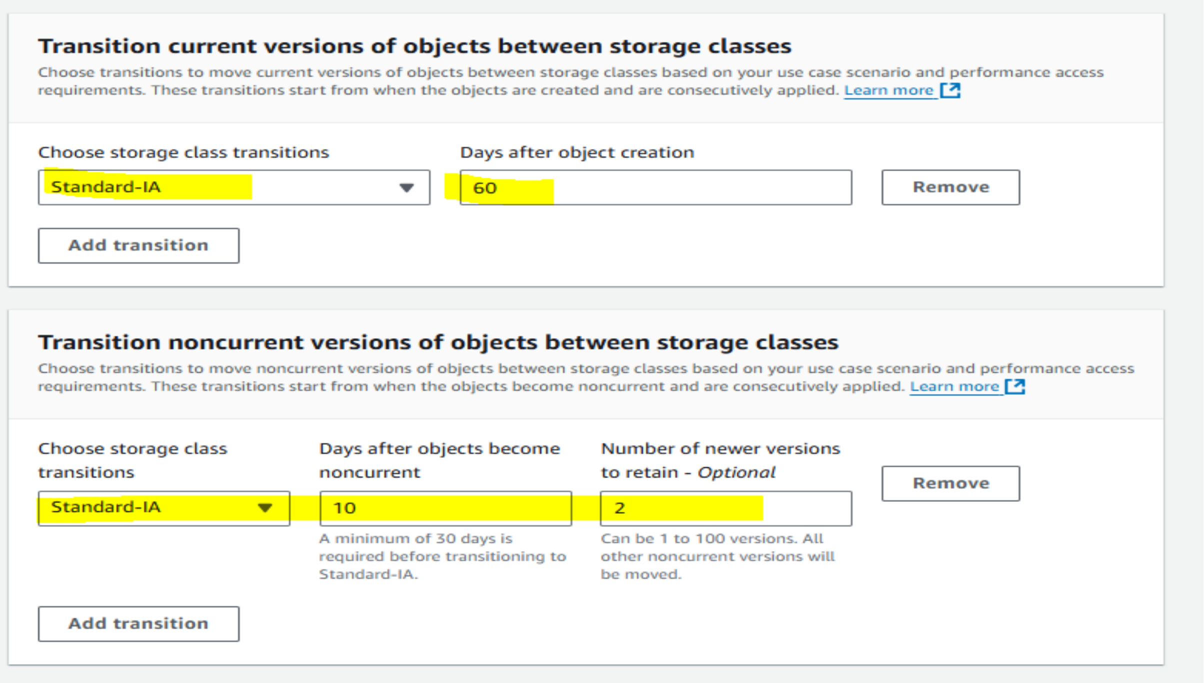
☑ Transition current versions of objects between storage classes
This action will move current versions.

☑ Transition noncurrent versions of objects between storage classes
This action will move noncurrent versions.

☑ Expire current versions of objects

□ Permanently delete noncurrent versions of objects

□ Delete expired object delete markers or incomplete multipart uploads
These actions are not supported when filtering by object tags or object size.



Transition current versions of objects between storage classes

Choose transitions to move current versions of objects between storage classes based on your use case scenario and performance access requirements. These transitions start from when the objects are created and are consecutively applied. Learn more

Choose storage class transitions: Standard-IA

Days after object creation: 60

Transition noncurrent versions of objects between storage classes

Choose transitions to move noncurrent versions of objects between storage classes based on your use case scenario and performance access requirements. These transitions start from when the objects become noncurrent and are consecutively applied. Learn more

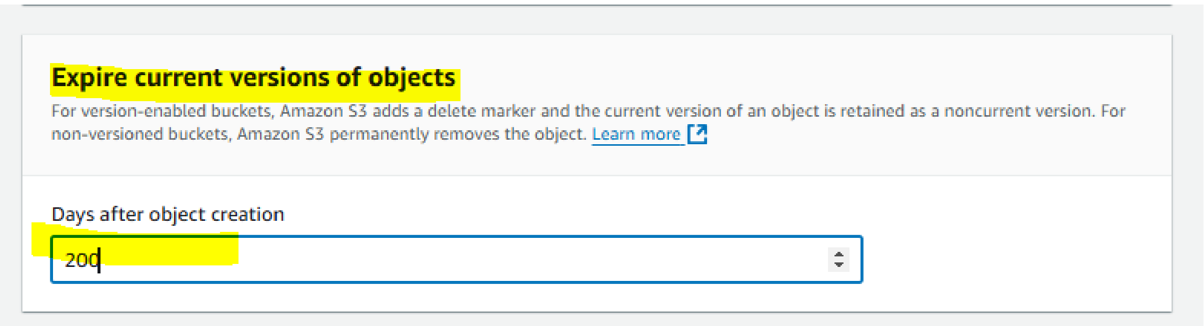
Choose storage class transitions: Standard-IA

Days after objects become noncurrent: 10

A minimum of 30 days is required before transitioning to Standard-IA.

Number of newer versions to retain - *Optional*: 2

Can be 1 to 100 versions. All other noncurrent versions will be moved.

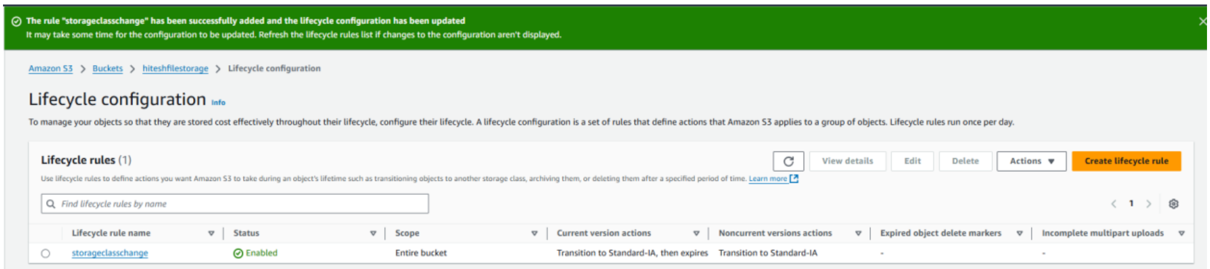


Expire current versions of objects

For version-enabled buckets, Amazon S3 adds a delete marker and the current version of an object is retained as a noncurrent version. For non-versioned buckets, Amazon S3 permanently removes the object. Learn more

Days after object creation: 200

Minimum 30Days is required to objects to become noncurrent



The rule "storageclasschange" has been successfully added and the lifecycle configuration has been updated
It may take some time for the configuration to be updated. Refresh the lifecycle rules list if changes to the configuration aren't displayed.

Amazon S3 > Buckets > hiteshfilestorage > Lifecycle configuration

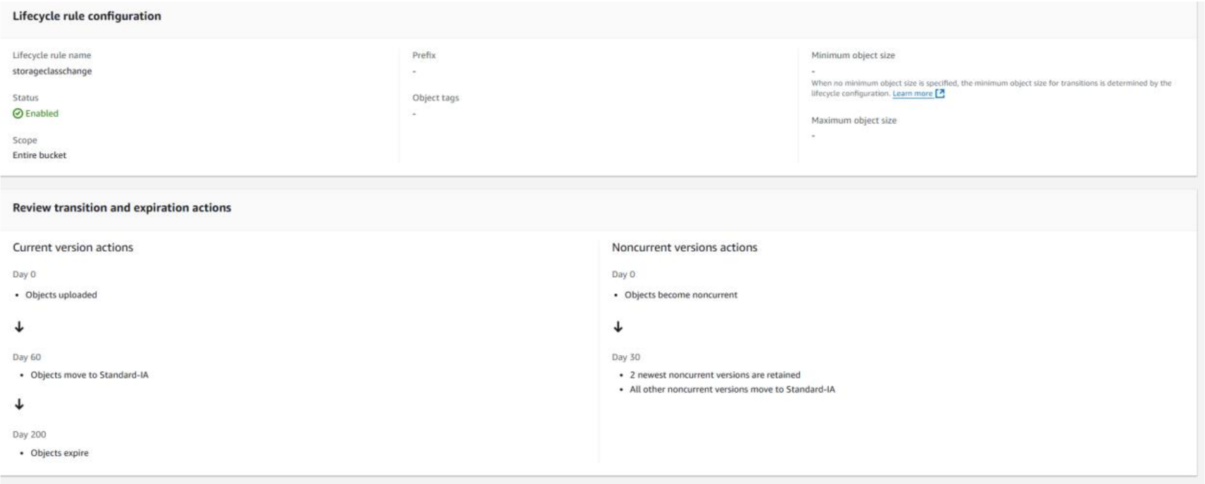
Lifecycle configuration

To manage your objects so that they are stored cost effectively throughout their lifecycle, configure their lifecycle. A lifecycle configuration is a set of rules that define actions that Amazon S3 applies to a group of objects. Lifecycle rules run once per day.

Lifecycle rules (1)

Use lifecycle rules to define actions you want Amazon S3 to take during an object's lifetime such as transitioning objects to another storage class, archiving them, or deleting them after a specified period of time. Learn more

	Lifecycle rule name	Status	Scope	Current version actions	Noncurrent versions actions	Expired object delete markers	Incomplete multipart uploads
○	storageclasschange	Enabled	Entire bucket	Transition to Standard-IA, then expires	Transition to Standard-IA	-	-



Lifecycle rule configuration

Lifecycle rule name
storageclasschange

Status
Enabled

Scope
Entire bucket

Prefix
-

Object tags
-

Minimum object size
-
When no minimum object size is specified, the minimum object size for transitions is determined by the lifecycle configuration. Learn more

Maximum object size
-

Review transition and expiration actions

Current version actions

Day 0
- Objects uploaded

↓

Day 60
- Objects move to Standard-IA

↓

Day 200
- Objects expire

Noncurrent versions actions

Day 0
- Objects become noncurrent

↓

Day 30
- 2 newest noncurrent versions are retained
- All other noncurrent versions move to Standard-IA

That’s All LifeCycle policies are configured successfully.