

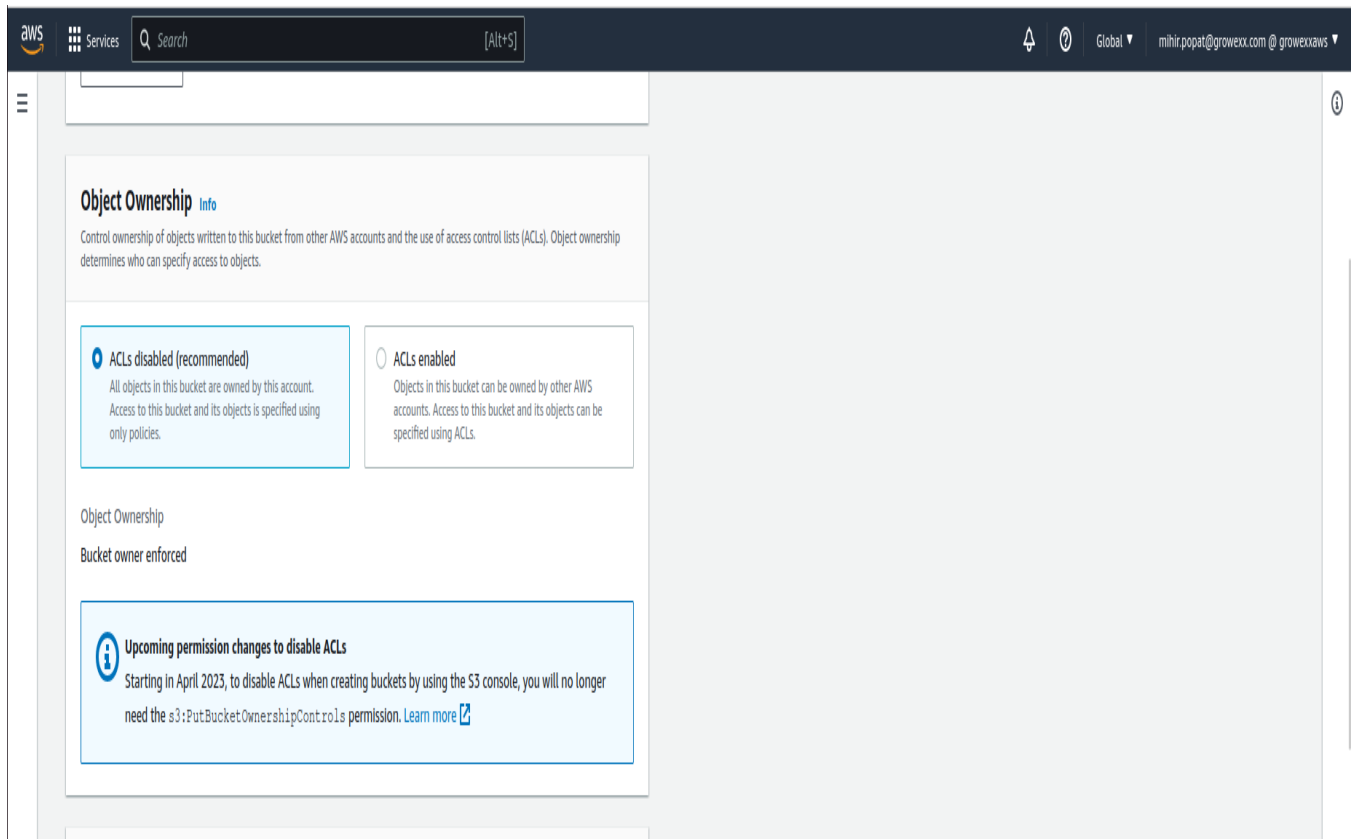
Hosting a static website with S3 & CloudFront

Steps :-

Inside of the S3 dashboard, click on “Create bucket”.

Give your bucket a unique name and select the options as shown below:

The screenshot displays the AWS Management Console's 'Create bucket' page. The top navigation bar includes the AWS logo, 'Services', a search bar, and user information. The breadcrumb trail indicates the path: Amazon S3 > Buckets > Create bucket. The main heading is 'Create bucket' with an 'Info' link. Below this, a note states: 'Buckets are containers for data stored in S3. [Learn more](#)'. The 'General configuration' section contains a 'Bucket name' input field with the text 'mihir_cloudfront_s3_task'. A note below the field states: 'Bucket name must be globally unique and must not contain spaces or uppercase letters. [See rules for bucket naming](#)'. The 'AWS Region' dropdown menu is set to 'US West (N. California) us-west-1'. At the bottom of the configuration section, there is a link for 'Copy settings from existing bucket - optional' with a note: 'Only the bucket settings in the following configuration are copied.' and a 'Choose bucket' button.



This is done to make the bucket accessible to the public because it is the host of your static website.

aws

Services

Search

[Alt+S]

Global

mihir.popat@growexx.com @ growexxaws

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.

Upcoming permission changes to disable any Block Public Access setting

Starting in April 2023, to disable any Block Public Access setting when creating buckets by using the S3 console, you must have the `s3:PutBucketPublicAccessBlock` permission. [Learn more](#)

Scroll to the bottom and click “Create bucket”.

Starting in April 2023, to disable any Block Public Access setting when creating buckets by using the S3 console, you must have the `s3:PutBucketPublicAccessBlock` permission. [Learn more](#)

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

Tags (0) - optional

You can use bucket tags to track storage costs and organize buckets. [Learn more](#)

No tags associated with this bucket.

Add tag

Default encryption [Info](#)

Server-side encryption is automatically applied to new objects stored in this bucket.

Encryption key type [Info](#)

- ☒ Amazon S3 managed keys (SSE-S3)
- ☐ AWS Key Management Service key (SSE-KMS)

Bucket Key

When KMS encryption is used to encrypt new objects in this bucket, the bucket key reduces encryption costs by lowering calls to AWS KMS. [Learn more](#)

- ☐ Disable
- ☒ Enable

Add tag

Default encryption [Info](#)

Server-side encryption is automatically applied to new objects stored in this bucket.

Encryption key type [Info](#)

☒ Amazon S3 managed keys (SSE-S3)

☐ AWS Key Management Service key (SSE-KMS)

Bucket Key

When KMS encryption is used to encrypt new objects in this bucket, the bucket key reduces encryption costs by lowering calls to AWS KMS. [Learn more](#)

☐ Disable

☒ Enable

▼ Advanced settings

Object Lock

Store objects using a write-once-read-many (WORM) model to help you prevent objects from being deleted or overwritten for a fixed amount of time or indefinitely. [Learn more](#)

☒ Disable

☐ Enable

Permanently allows objects in this bucket to be locked. Additional Object Lock configuration is required in bucket details after bucket creation to protect objects in this bucket from being deleted or overwritten.

Object Lock works only in versioned buckets. Enabling Object Lock automatically enables Bucket Versioning.

After creating the bucket you can upload files and folders to the bucket, and configure additional bucket settings.

Cancel

Create bucket

Feedback

Language

© 2023, Amazon Web Services India Private Limited or its affiliates. [Privacy](#) [Terms](#) [Cookie preferences](#)

aws

Services

Search

[Alt+S]

Global

mihir.popat@growwex.com @ growwexaws

Amazon S3

Successfully created bucket "mihir-cloudfront-s3-task"

To upload files and folders, or to configure additional bucket settings choose [View details](#).

Buckets

Access Points

Object Lambda Access Points

Multi-Region Access Points

Batch Operations

IAM Access Analyzer for S3

Block Public Access settings for this account

▼ Storage Lens

Dashboards

AWS Organizations settings

Feature spotlight

AWS Marketplace for S3

Amazon S3 > Buckets

▼ Account snapshot

Last updated: Mar 26, 2023 by Storage Lens. Metrics are generated every 24 hours. [Learn more](#)

Total storage

Object count

Average object size

You can enable advanced metrics in the "default-account-dashboard" configuration.

147.5 GB

35.6 k

4.2 MB

Buckets (82) [Info](#)

Copy ARN

Empty

Delete

Create bucket

mihr

1 match

Name

▲

AWS Region

▼

Access

▼

Creation date

▼

☐

mihir-cloudfront-s3-task

US West (N. California) us-west-1

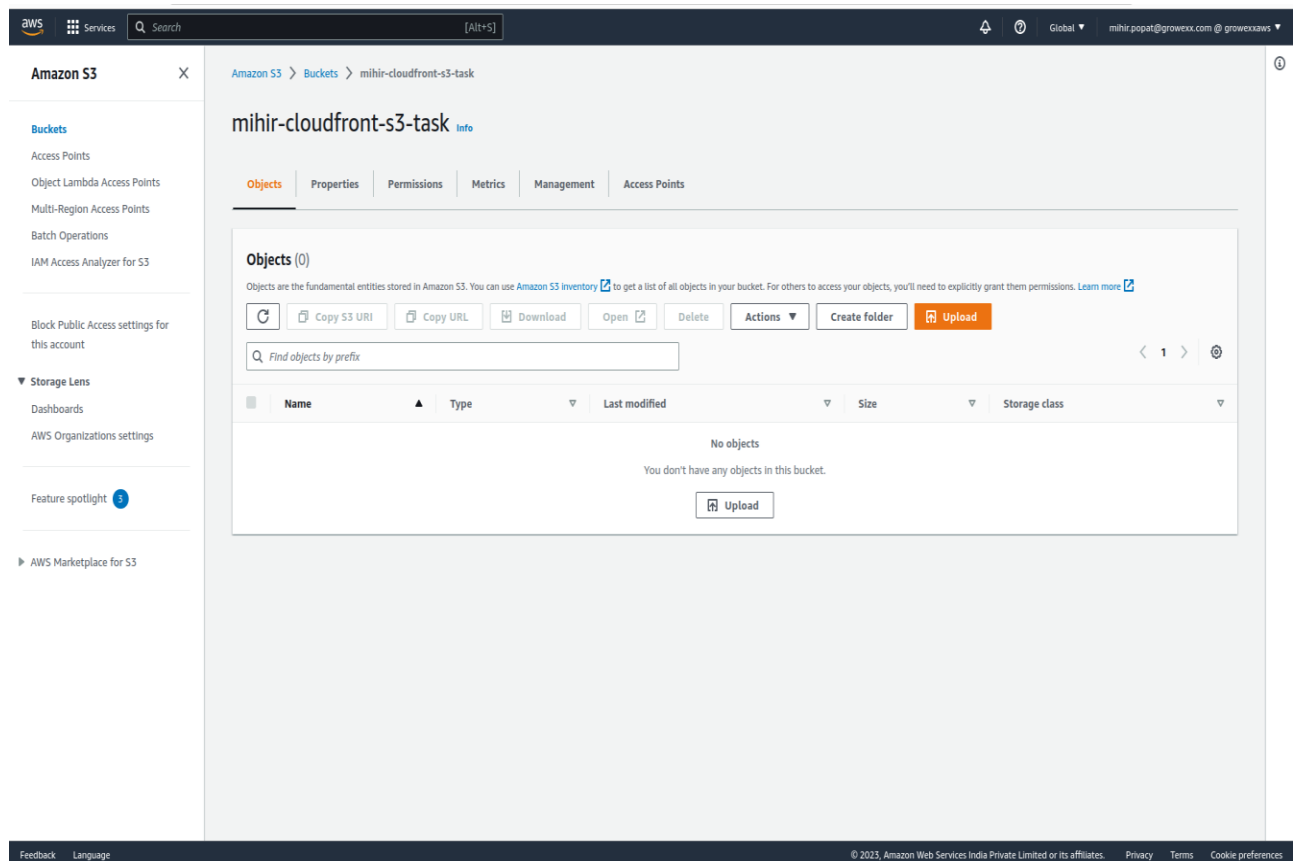
Objects can be public

March 28, 2023, 10:10:18 (UTC+05:30)

Feedback

Language

© 2023, Amazon Web Services India Private Limited or its affiliates. [Privacy](#) [Terms](#) [Cookie preferences](#)



After creating the bucket, upload your website to the bucket by clicking on the bucket name. Once inside of your bucket on the “Objects” tab, click on the “Upload” button.

Services

Search

[Alt+S]

Global

mihir.popat@growexx.com @ growexxaws

Amazon S3

Buckets

mihir-cloudfront-s3-task

Upload

Upload

Info

Add the files and folders you want to upload to S3. To upload a file larger than 160GB, use the AWS CLI, AWS SDK or Amazon S3 REST API. [Learn more](#)

Drag and drop files and folders you want to upload here, or choose **Add files**, or **Add folders**.

Files and folders (1 Total, 102.0 B)

Remove

Add files

Add folder

All files and folders in this table will be uploaded.

Find by name

< 1 >

<input type="checkbox"/>	Name	Folder	Type	Size
<input type="checkbox"/>	index.html	-	text/html	102.0 B

Destination

Destination

s3://mihir-cloudfront-s3-task

Destination details

Bucket settings that impact new objects stored in the specified destination.

Permissions

Grant public access and access to other AWS accounts.

Properties

Specify storage class, encryption settings, tags, and more.

Cancel

Upload

Feedback

Language

© 2023, Amazon Web Services India Private Limited or its affiliates.

Privacy

Terms

Cookie preferences

aws Services Search [Alt+S]

Upload succeeded
View details below.

Upload: status

The information below will no longer be available after you navigate away from this page.

Summary

Destination s3://mihir-cloudfront-s3-task	Succeeded 1 file, 102.0 B (100.00%)	Failed 0 files, 0 B (0%)
--	--	-----------------------------

Files and folders

Configuration

Files and folders (1 Total, 102.0 B)

Find by name

Name	Folder	Type	Size	Status	Error
index.html	-	text/html	102.0 B	Succeeded	-

Feedback Language © 2023, Amazon Web Services India Private Limited or its affiliates. Privacy Terms Cookie preferences

Now click on the “Properties” tab and scroll to the bottom to the “Static website hosting” section and click on the “Edit” button.

aws Services Search [Alt+S]

Amazon S3

Buckets

- Access Points
- Object Lambda Access Points
- Multi-Region Access Points
- Batch Operations
- IAM Access Analyzer for S3

Block Public Access settings for this account

Storage Lens

- Dashboards
- AWS Organizations settings

Feature spotlight

AWS Marketplace for S3

Send notifications to Amazon EventBridge for all events in this bucket
Off

Transfer acceleration

Use an accelerated endpoint for faster data transfers. [Learn more](#)

Transfer acceleration
Disabled

Object Lock

Store objects using a write-once-read-many (WORM) model to help you prevent objects from being deleted or overwritten for a fixed amount of time or indefinitely. [Learn more](#)

Object Lock
Disabled

Amazon S3 currently does not support enabling Object Lock after a bucket has been created. To enable Object Lock for this bucket, contact [Customer Support](#)

Requester pays

When enabled, the requester pays for requests and data transfer costs, and anonymous access to this bucket is disabled. [Learn more](#)

Requester pays
Disabled

Static website hosting

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

Static website hosting
Disabled

Feedback Language © 2023, Amazon Web Services India Private Limited or its affiliates. Privacy Terms Cookie preferences

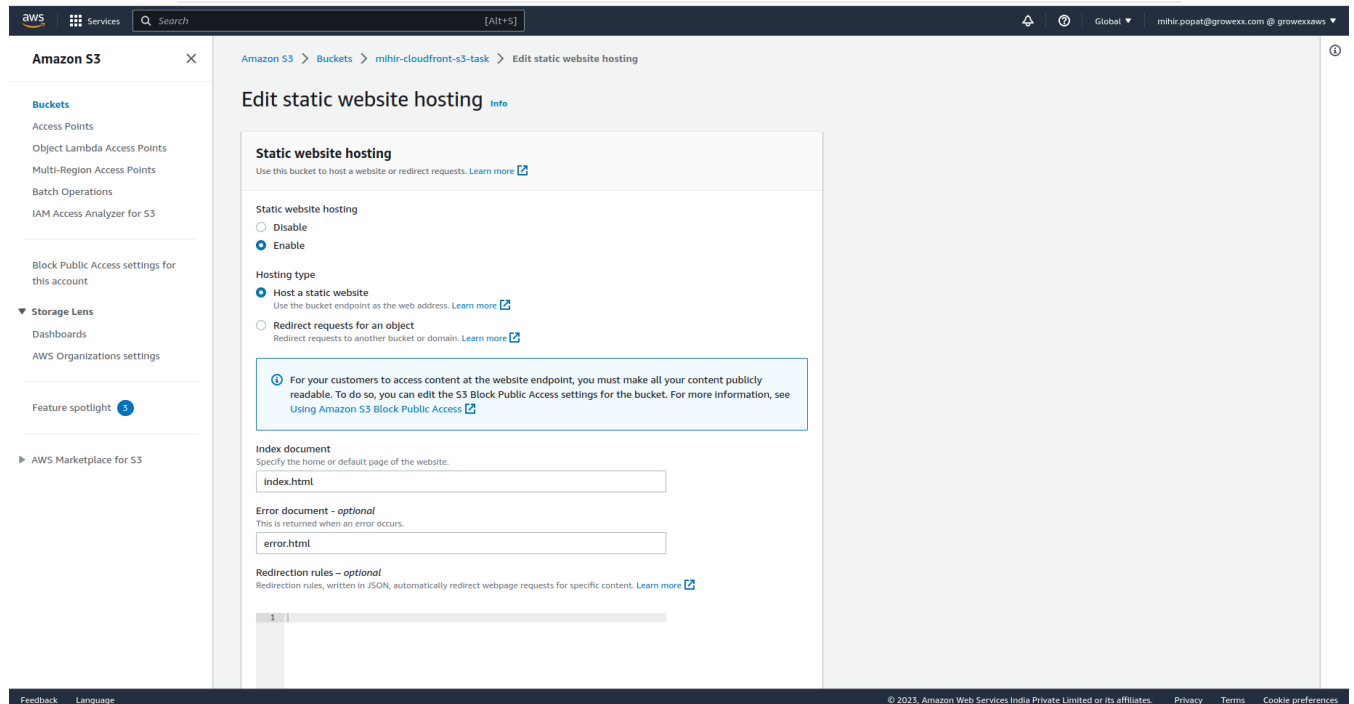
Select “Enable” for Static website hosting.

Also, select “Host a static website” for the Hosting type.

Enter the file for your “index” document. The error document is optional as this will load an error page if you try to access a file that isn’t available.

The screenshot displays the AWS Management Console interface for an Amazon S3 bucket named 'mihir-cloudfront-s3-task'. The left sidebar shows the 'Amazon S3' service with various options like Buckets, Access Points, and Storage Lens. The main content area shows the bucket's 'Objects' tab, which lists two files: 'error.html' (81.0 B) and 'index.html' (102.0 B), both in the 'Standard' storage class. The console header includes the AWS logo, a search bar, and user information. The footer contains links for Feedback, Language, and Copyright information.

Name	Type	Last modified	Size	Storage class
error.html	html	March 28, 2023, 10:17:45 (UTC+05:30)	81.0 B	Standard
index.html	html	March 28, 2023, 10:13:42 (UTC+05:30)	102.0 B	Standard



The next step is to grant permissions to your bucket so that this page is accessible by everyone.

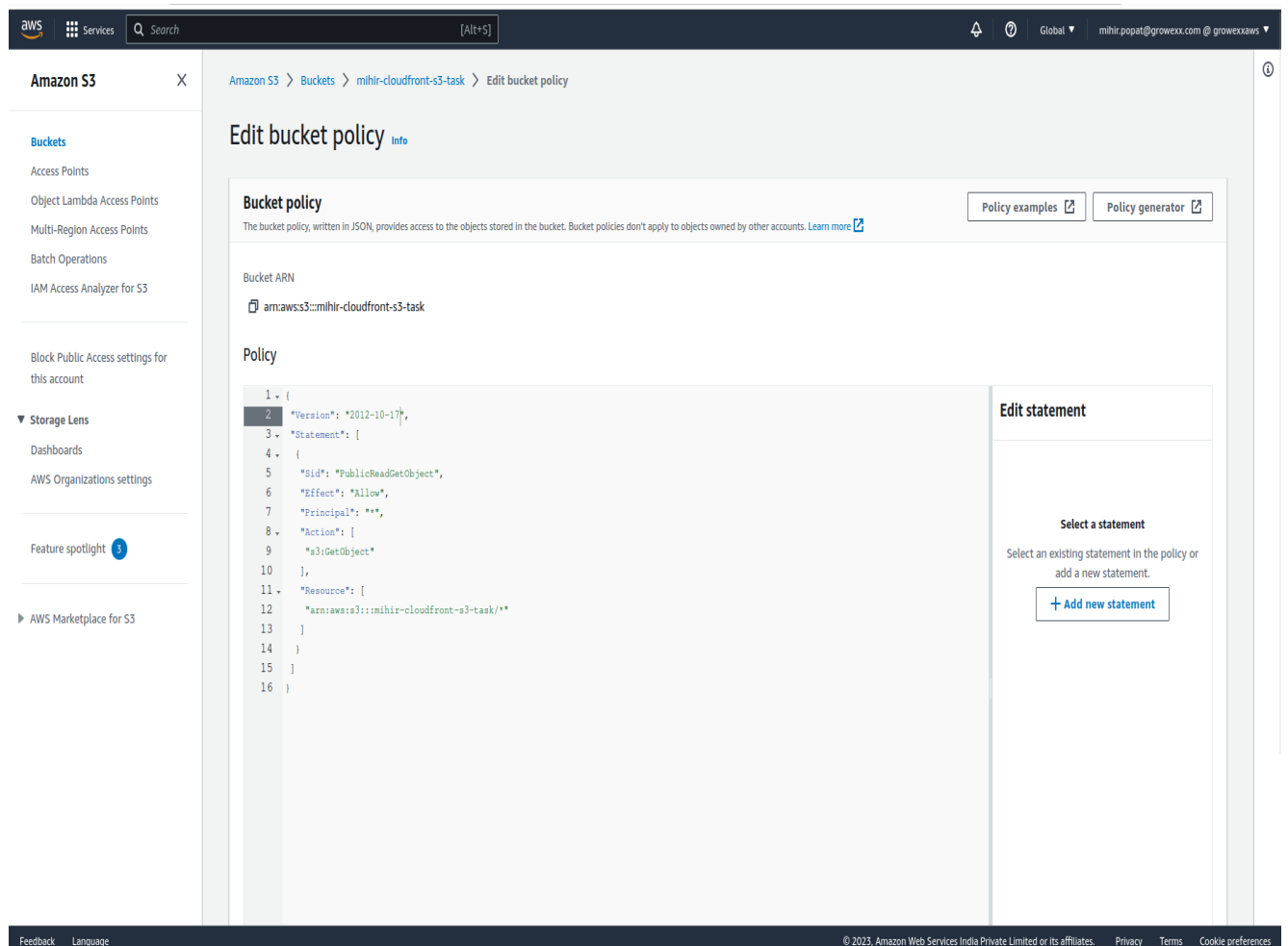
To do that, head over to the “Permissions” tab of your bucket. Scroll down to the “Bucket policy” section and click on the “Edit” button.

Paste the below code into the bucket policy:

```
{  
  "Version": "2012-10-17",  
  "Statement": [  
    {  
      "Sid": "PublicReadGetObject",  
      "Effect": "Allow",  
      "Principal": "*",  
      "Action": [  
        "s3:GetObject"  
      ],  
    },  
  ],  
}
```

```
"Resource": [  
  
  "arn:aws:s3:::<BUCKET_NAME>/*"  
  
]  
  
}  
  
]  
  
}
```

Then scroll down and click on “Save changes”.



Now the last step is to create a CloudFront Distribution.

Head over to the search bar and type in “CloudFront”. The CloudFront dashboard will now be displayed.

From the dashboard, on the right-hand side click on the orange button “Create a CloudFront distribution”.

This should take you to the Create Distribution page, click on the Origin Domain Name field and select the S3 bucket you created earlier.

Also notice that name is already pre-filled. For Under “S3 Bucket Access”, select “Yes Use OAI”. Click on “Create new OAI”. OAI or Origin Access ID grants CloudFront the permissions to call our S3 bucket.

The picture below sums up everything discussed above:

Select public in origin access

Create distribution

Origin

Origin domain
Choose an AWS origin, or enter your origin's domain name.

Warning: This S3 bucket has static web hosting enabled. If you plan to use this distribution as a website, we recommend using the S3 website endpoint rather than the bucket endpoint.
[Use website endpoint](#)

Origin path - optional [Info](#)
Enter a URL path to append to the origin domain name for origin requests.

Name
Enter a name for this origin.

Origin access [Info](#)

☒ **Public**
Bucket must allow public access.

☐ **Origin access control settings (recommended)**
Bucket can restrict access to only CloudFront.

☒ **Legacy access identities**
Use a CloudFront origin access identity (OAI) to access the S3 bucket.

Origin access identity
Select an existing origin access identity (recommended) or create a new identity.

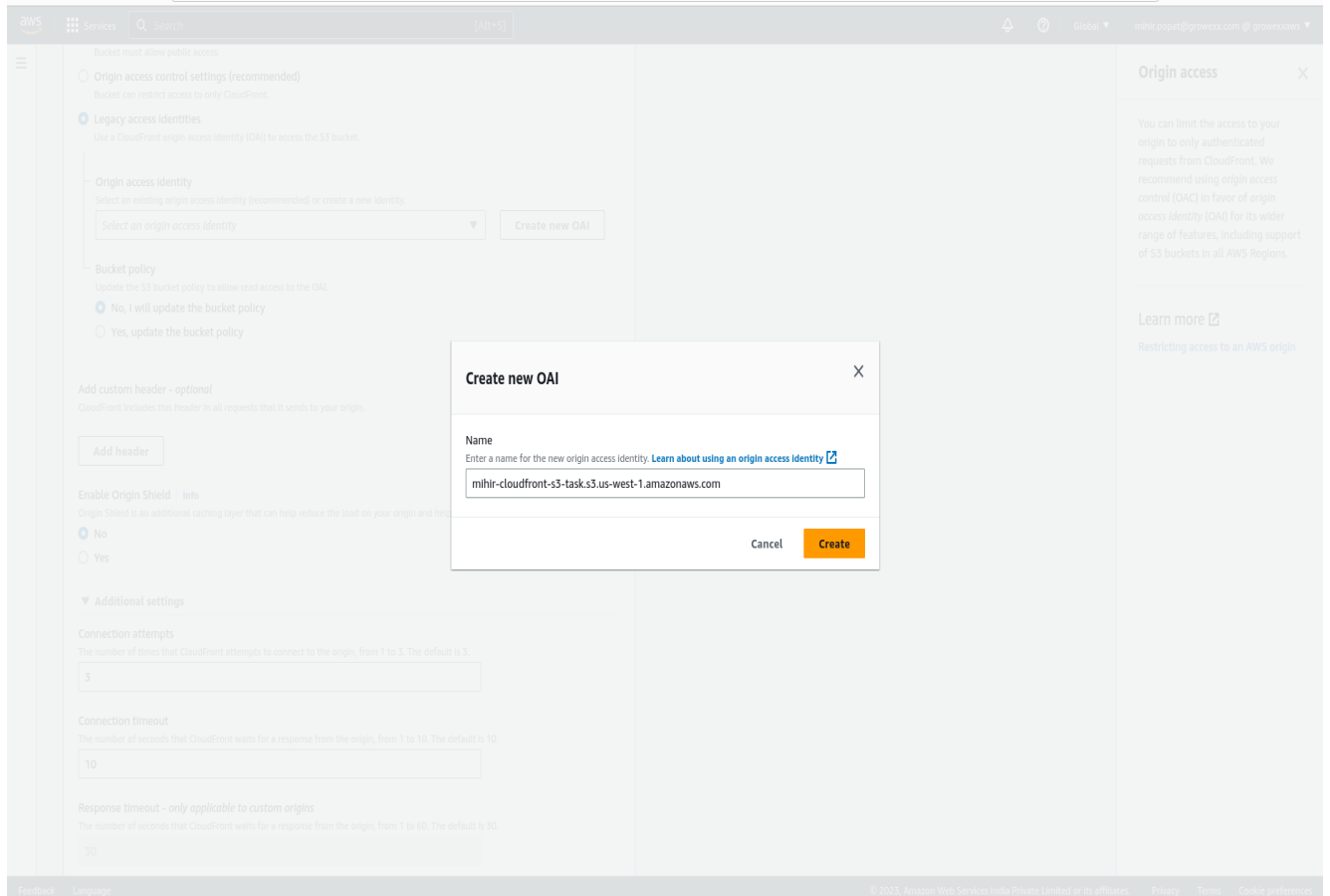
[Create new OAI](#)

Origin access

You can limit the access to your origin to only authenticated requests from CloudFront. We recommend using *origin access control* (OAC) in favor of *origin access identity* (OAI) for its wider range of features, including support of S3 buckets in all AWS Regions.

[Learn more](#)

[Restricting access to an AWS origin](#)



Scroll down to until you see “Viewer”, For “Viewer Protocol Policy”, select “Redirect HTTP to HTTPS”. And the reasons for this are mostly for security measures as HTTPS is more secure than HTTP.

aws

Services

Search

[Alt+S]

Global

mihir.popat@growexx.com @ growexxaws

Keep-alive timeout - only applicable to custom origins

The number of seconds that CloudFront maintains an idle connection with the origin, from 1 to 60. The default is 5.

5

Default cache behavior

Path pattern

Info

Default (*)

Compress objects automatically

Info

No

Yes

Viewer

Viewer protocol policy

HTTP and HTTPS

Redirect HTTP to HTTPS

HTTPS only

Allowed HTTP methods

GET, HEAD

GET, HEAD, OPTIONS

GET, HEAD, OPTIONS, PUT, POST, PATCH, DELETE

Restrict viewer access

If you restrict viewer access, viewers must use CloudFront signed URLs or signed cookies to access your content.

No

Yes

Cache key and origin requests

We recommend using a cache policy and origin request policy to control the cache key and origin requests.

Cache policy and origin request policy (recommended)

Legacy cache settings

Origin access

You can limit the access to your origin to only authenticated requests from CloudFront. We recommend using *origin access control* (OAC) in favor of *origin access identity* (OAI) for its wider range of features, including support of S3 buckets in all AWS Regions.

Learn more

Restricting access to an AWS origin

Feedback

Language

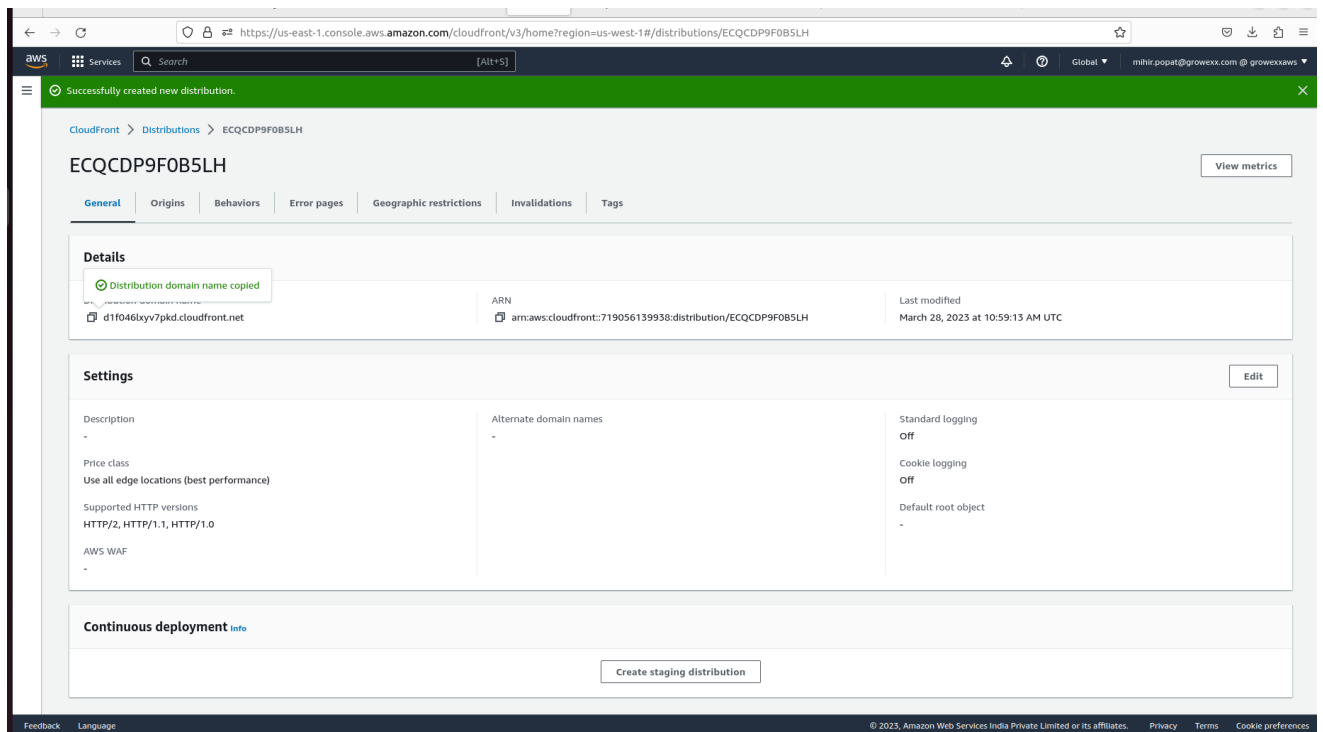
© 2023, Amazon Web Services India Private Limited or its affiliates.

Privacy

Terms

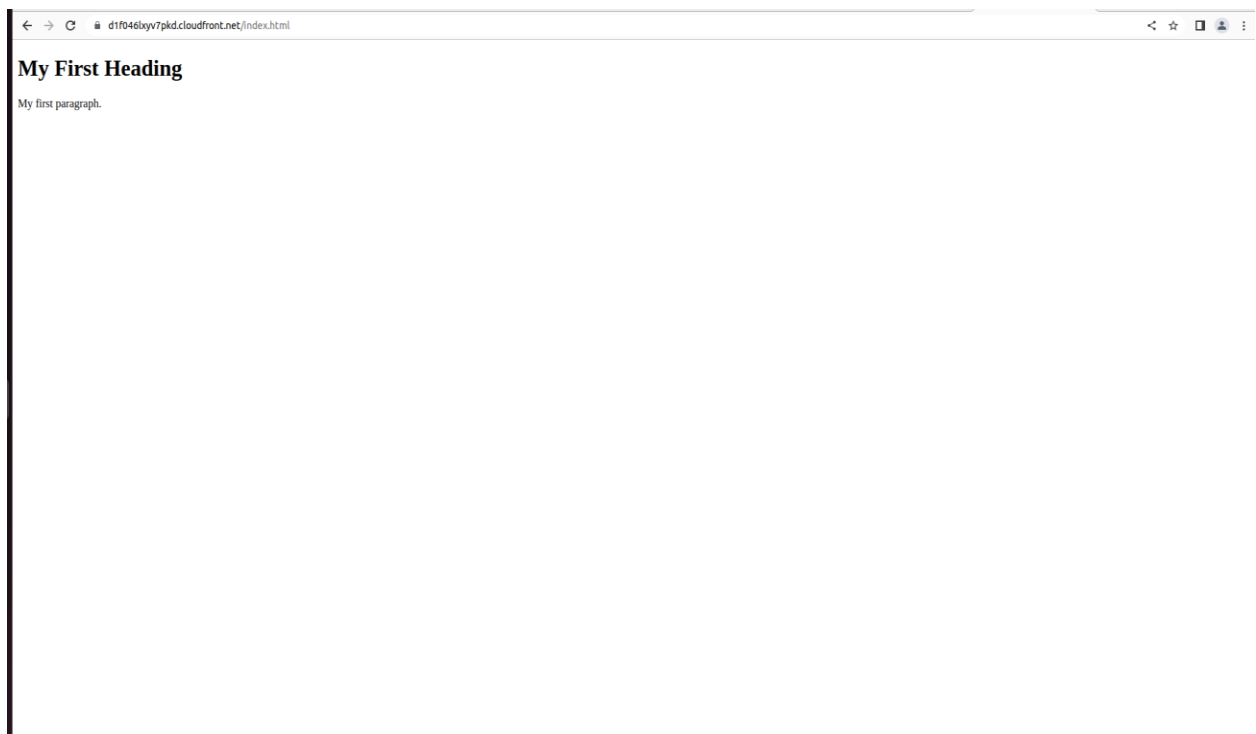
Cookie preferences

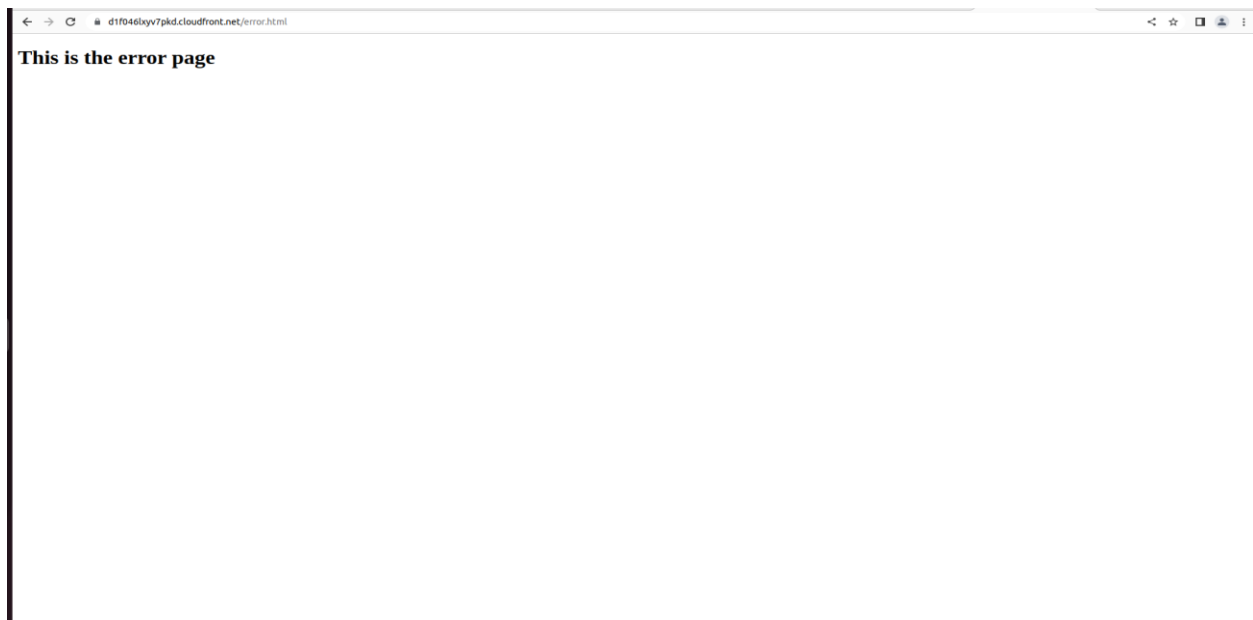
From this point forward and for our project the rest of the options can remain as default and click on “Create Distribution”.



A domain name has been provided to you which can be used to access your static website.

Note: When pasting the domain on the url make sure you enter “/index.html” at the end.





S3 versioning

S3 Versioning, as the name implies, allows you to “version control” objects within your Bucket. This allows you to recover from unintended user changes and actions (including deletions) that might occurred through misuse or corruption. Enabling Versioning on the bucket will keep multiple copies of the object. Each time the object changes, a new version of that object is created and acts as the new current ‘version’.

One thing to be wary of with Versioning is the additional storage costs applied in S3. Storing multiple copies of the same object will use additional space and increase your storage costs.

Once Versioning on a Bucket is enabled, it can’t be disabled – only suspended.

Amazon S3

Buckets

Access Points

Object Lambda Access Points

Multi-Region Access Points

Batch Operations

IAM Access Analyzer for S3

Block Public Access settings for this account

Storage Lens

Dashboards

AWS Organizations settings

Feature spotlight

AWS Marketplace for S3

Amazon S3 > Buckets > mihir-cloudfront-s3-task

mihir-cloudfront-s3-task

Publicly accessible

Info

Objects

Properties

Permissions

Metrics

Management

Access Points

Bucket overview

AWS Region

US West (N. California) us-west-1

Amazon Resource Name (ARN)

arn:aws:s3::mihir-cloudfront-s3-task

Creation date

March 28, 2023, 10:10:18 (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](#)

Edit

Bucket Versioning

Disabled

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

Tags (0)

You can use bucket tags to track storage costs and organize buckets. [Learn more](#)

Edit

Key

Value

No tags associated with this resource.

Feedback

Language

© 2023, Amazon Web Services India Private Limited or its affiliates. [Privacy](#) [Terms](#) [Cookie preferences](#)

Amazon S3

Buckets

Access Points

Object Lambda Access Points

Multi-Region Access Points

Batch Operations

IAM Access Analyzer for S3

Block Public Access settings for this account

Storage Lens

Dashboards

AWS Organizations settings

Feature spotlight

AWS Marketplace for S3

Amazon S3 > Buckets > mihir-cloudfront-s3-task > Edit Bucket Versioning

Edit Bucket Versioning

Info

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

☐ Suspend

This suspends the creation of object versions for all operations but preserves any existing object versions.

☒ Enable

This bucket has one or more lifecycle rules. After enabling Bucket Versioning, you might need to update your lifecycle rules to manage previous versions of objects.

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

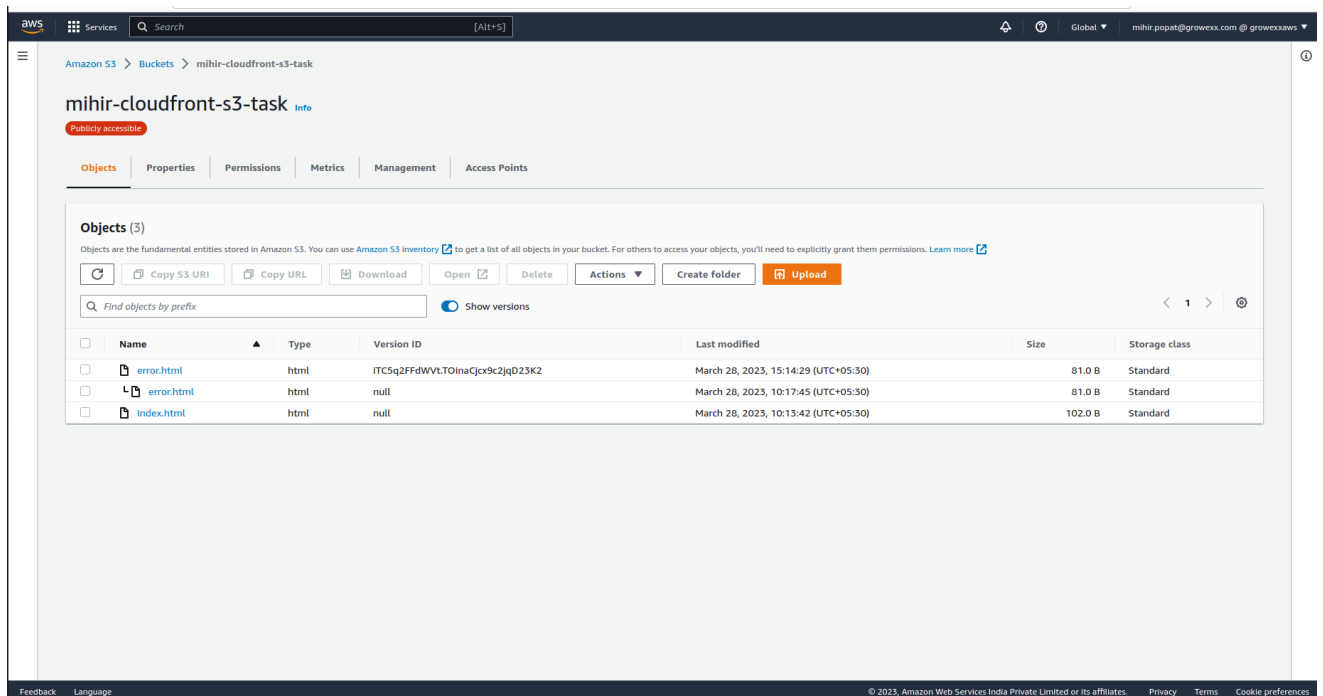
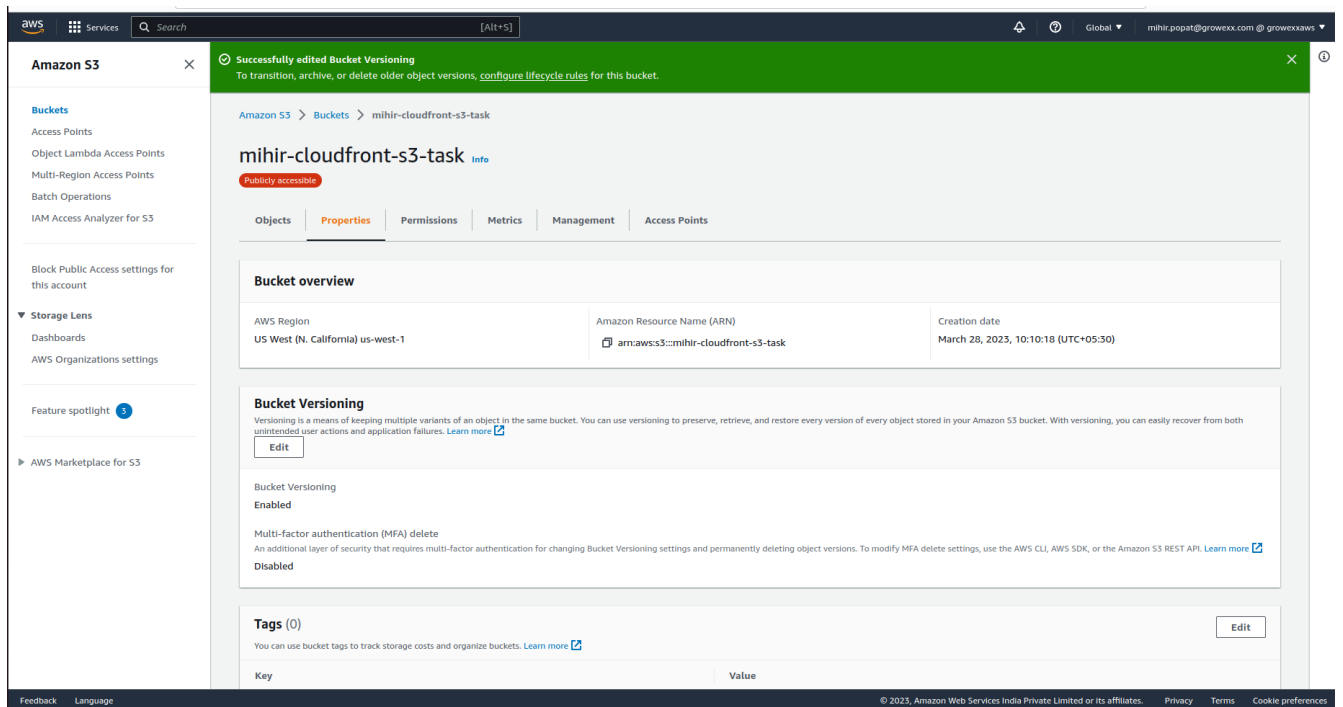
Cancel

Save changes

Feedback

Language

© 2023, Amazon Web Services India Private Limited or its affiliates. [Privacy](#) [Terms](#) [Cookie preferences](#)



S3 Object Life Cycle policy

Object Life Cycle policy is used to move the objects in your bucket from one storage class to another automatically. Let's say we have objects in our bucket which are stored in Standard Storage.

Now we have to move those files from Standard Storage to Infrequent Access Storage after 60 days of creation

After 120 days we have to move those files from Infrequent Access Storage to Glacier.

Now in order to implement the above statements

You have to log in to AWS and navigate to S3, choose the bucket you want to implement object life cycle rules.

Now you can add new life cycle rules under the management section.

Click on Add life cycle rules it will open a new window

The screenshot shows the AWS S3 console interface for the bucket 'mihir-cloudfront-s3-task'. The 'Management' tab is active, displaying two sections: 'Lifecycle rules (0)' and 'Replication rules (0)'. Both sections indicate that there are no rules currently configured and provide a 'Create' button to add new rules. The left sidebar shows the navigation menu with options like Buckets, Access Points, and Storage Lens. The top navigation bar includes the AWS logo, search bar, and user information.

Lifecycle rules (0)

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](#)

[View details](#) [Edit](#) [Delete](#) [Actions](#) [Create lifecycle rule](#)

Lifecycle rule name	Status	Scope	Current version actions	Noncurrent versions actions	Expired object delete markers	Incomplete multipart uploads
No lifecycle rules						
There are no lifecycle rules for this bucket.						
Create lifecycle rule						

Replication rules (0)

Use replication rules to define options you want Amazon S3 to apply during replication such as server-side encryption, replica ownership, transitioning replicas to another storage class, and more. [Learn more](#)

[View details](#) [Edit rule](#) [Delete](#) [Actions](#) [Create replication rule](#)

Replication rule name	Status	Destination bucket	Destination Region	Priority	Scope	Storage class	Replica owner	Replication Time Control	KMS-encrypted objects	Replica modification sync
No replication rules										
You don't have any rules in the replication configuration.										
Create replication rule										

The first step adding life cycle rule is giving a name to it and adding prefix or tags if required.

ServicesSearch[Alt+S]

Globalmihr.papat@growexx.com @ growexxaws

Amazon S3> Buckets> mihr-cloudfront-s3-task> Lifecycle configuration> Create lifecycle rule

Create lifecycle rule

Lifecycle rule configuration

Lifecycle rule name

mihr-s3-cloudfront-task

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. Per-request fees apply. [Learn more](#) or see [Amazon S3 pricing](#)

☒ Move current versions of objects between storage classes

☐ Move noncurrent versions of objects between storage classes

☒ 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](#)

FeedbackLanguage

© 2023, Amazon Web Services India Private Limited or its affiliates. PrivacyTermsCookie preferences

ServicesSearch[Alt+S]

Globalmihr.papat@growexx.com @ growexxaws

Amazon S3> Buckets> mihr-cloudfront-s3-task> Lifecycle configuration

The lifecycle configuration was updated. Lifecycle rule "mihr-s3-cloudfront-task" was successfully added. It may take some time for the configuration to be updated. Press the refresh button if changes to the rule are not displayed.

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](#)

View details

Edit

Delete

Actions

Create lifecycle rule

Find lifecycle rules by name

Lifecycle rule name	Status	Scope	Current version actions	Noncurrent versions actions	Expired object delete markers	Incomplete multipart uploads
<input type="radio"/> mihr-s3-cloudfront-task	Enabled	Entire bucket	Transition to Standard-IA, then Glacier Instant Retrieval, then expires	-	-	Permanently delete

FeedbackLanguage

© 2023, Amazon Web Services India Private Limited or its affiliates. PrivacyTermsCookie preferences

Services

Search

[Alt+S]

Global

mihir.popat@growexx.com @ growexxaws

Amazon S3 > Buckets > mihir-cloudfront-s3-task > Lifecycle configuration > Create lifecycle rule

Create lifecycle rule

Lifecycle rule configuration

Lifecycle rule name

mihir-s3-cloudfront-task

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

Filter type

You can filter objects by prefix, object tags, object size, or whatever combination suits your usecase.

Prefix

Add filter to limit the scope of this rule to a single prefix.

Enter prefix

Don't include the bucket name in the prefix. Using certain characters in key names can cause problems with some applications and protocols. [Learn more](#)

Object tags

You can limit the scope of this rule to the key/value pairs added below.

Add tag

Object size

You can limit the scope of this rule to apply to objects based on their size. For example, you can filter out objects that might not be cost effective to transition to Glacier Flexible Retrieval (formerly Glacier) because of per-object fees.

☐ Specify minimum object size

☐ Specify maximum object size

Lifecycle rule actions

Feedback

Language

© 2023, Amazon Web Services India Private Limited or its affiliates. [Privacy](#) [Terms](#) [Cookie preferences](#)

Services

Search

[Alt+S]

Global

mihir.popat@growexx.com @ growexxaws

Lifecycle rule actions

Choose the actions you want this rule to perform. Per-request fees apply. [Learn more](#) or see [Amazon S3 pricing](#)

☒ Move current versions of objects between storage classes

☐ Move noncurrent versions of objects between storage classes

☒ 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

Days after object creation

Standard-IA

60

Remove

Glacier Instant Retrieval

120

Remove

Add transition

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

485

Delete expired object delete markers or incomplete multipart uploads

Expired object delete markers

This action will remove expired object delete markers and may improve performance. An expired object delete marker is removed if all noncurrent versions of an object expire after deleting a versioned object. This action is not available when "Expire current versions of objects" is selected. [Learn more](#)

Feedback

Language

© 2023, Amazon Web Services India Private Limited or its affiliates. [Privacy](#) [Terms](#) [Cookie preferences](#)

