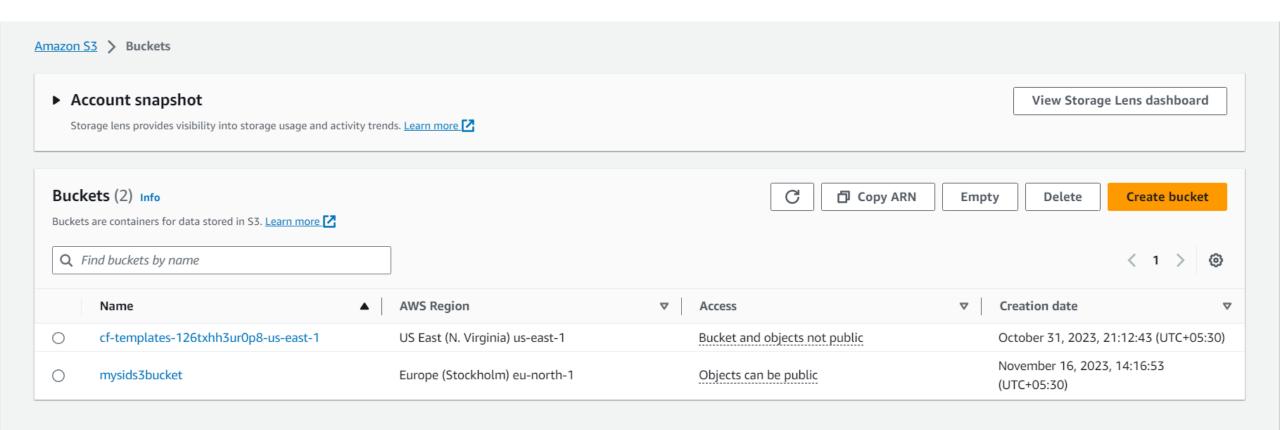
S3 Bucket creation

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:

- Create an S3 Bucket for file storage.
- Upload 5 objects with different file extensions.



Amazon S3	>	Buckets	>	Create	bucket
-----------	---	----------------	---	--------	--------

Create bucket Info

Buckets are containers for data stored in S3. Learn more

Bucket name	
sidaws-bucket	
ucket name must be unique within the global namespace ar	nd follow the bucket naming rules. See rules for bucket naming
WS Region	
Europe (Stockholm) eu-north-1	▼
opy settings from existing bucket - optional nly the bucket settings in the following configuration are co	ppied.
Object Ownership Info	
ontrol ownership of objects written to this bucket from other etermines who can specify access to objects.	ACLs enabled Objects in this bucket can be owned by other AWS.
ontrol ownership of objects written to this bucket from othe etermines who can specify access to objects.	
Control ownership of objects written to this bucket from othe 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. We recommend disabling ACLs, unless you need to be a control of the commend disabling ACLs, unless you need to be a control of the commend disabling ACLs, unless you need to be a control of the commend disabling ACLs, unless you need to be a control of the commend disabling ACLs, unless you need to be a control of the commend disabling ACLs, unless you need to be a control of the commend disabling ACLs, unless you need to be a control of the commend disabling ACLs, unless you need to be a control of the commend disabling ACLs, unless you need to be a control of the commend disabling ACLs, unless you need to be a control of the commend disabling ACLs, unless you need to be a control of the commend disabling ACLs, unless you need to be a control of the commend disabling ACLs, unless you need to be a control of the commend disabling ACLs, unless you need to be a control of the commend disabling ACLs.	Objects in this bucket can be owned by other AWS accounts. Access to this bucket and its objects can be specified using ACLs. Deed to control access for each object individually or to have the ga bucket policy instead of ACLs to share data with users
Control ownership of objects written to this bucket from othe 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. We recommend disabling ACLs, unless you ne object writer own the data they upload. Using	Objects in this bucket can be owned by other AWS accounts. Access to this bucket and its objects can be specified using ACLs. Deed to control access for each object individually or to have the ga bucket policy instead of ACLs to share data with users
Control ownership of objects written to this bucket from othe letermines 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. We recommend disabling ACLs, unless you ne object writer own the data they upload. Using outside of your account simplifies permission	Objects in this bucket can be owned by other AWS accounts. Access to this bucket and its objects can be specified using ACLs. Deed to control access for each object individually or to have the grabucket policy instead of ACLs to share data with users as management and auditing.

OI:	by the bucket owner. Otherwise, they are owned by the object writer.
	t writer ject writer remains the object owner.
THE OL	ect writer remains the object owner.
(i) If	you want to enforce object ownership for new objects only, your bucket policy must specify that the
bı	cket-owner-full-control canned ACL is required for object uploads. Learn more [2]
ock I	ublic Access settings for this bucket
ure tha	ss is granted to buckets and objects through access control lists (ACLs), bucket policies, access point policies, or all. In order to public access to this bucket and its objects is blocked, turn on Block all public access. These settings apply only to this bucket
licatio	ess points. AWS recommends that you turn on Block all public access, but before applying any of these settings, ensure that your swill work correctly without public access. If you require some level of public access to this bucket or objects within, you can the individual settings below to suit your specific storage use cases. Learn more
Block	all public access
Turnin	this setting on is the same as turning on all four settings below. Each of the following settings are independent of one another.
□В	ock public access to buckets and objects granted through <i>new</i> access control lists (ACLs)
A	will block public access permissions applied to newly added buckets or objects, and prevent the creation of new public access Ls for existing buckets and objects. This setting doesn't change any existing permissions that allow public access to S3 resources ng ACLs.
□в	ock public access to buckets and objects granted through <i>any</i> access control lists (ACLs)
S	will ignore all ACLs that grant public access to buckets and objects.
□в	ock public access to buckets and objects granted through <i>new</i> public bucket or access point policies
S	will block new bucket and access point policies that grant public access to buckets and objects. This setting doesn't change any isting policies that allow public access to S3 resources.
□В	ock public and cross-account access to buckets and objects through <i>any</i> public bucket or access point
	licies
	will ignore public and cross-account access for buckets or access points with policies that grant public access to buckets and jects.
Λ	Turning off block all public access might result in this bucket and the objects within becoming public
<u>ٺ</u>	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.
	Versioning
cket	is a means of keeping multiple variants of an object in the same bucket. You can use versioning to preserve, retrieve, and restore
sioning	
sioning ry vers	on of every object stored in your Amazon S3 bucket. With versioning, you can easily recover from both unintended user actions ation failures. Learn more [7]
sioning ry vers	on of every object stored in your Amazon S3 bucket. With versioning, you can easily recover from both unintended user actions stion failures. <u>Learn more</u>

lucket Versioning		
Disable		
) Enable		

Tags - optional (0)

You can use bucket tags to track storage costs and organize buckets. Learn more

No tags associated with this bucket.

Default encryption Info

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

Encryption type Info

- Server-side encryption with Amazon S3 managed keys (SSE-S3)
- O Server-side encryption with AWS Key Management Service keys (SSE-KMS)
- Dual-layer server-side encryption with AWS Key Management Service keys (DSSE-KMS)
 Secure your objects with two separate layers of encryption. For details on pricing, see DSSE-KMS pricing on the Storage tab of the Amazon S3 pricing page. [7]

Bucket Key

Using an S3 Bucket Key for SSE-KMS reduces encryption costs by lowering calls to AWS KMS. S3 Bucket Keys aren't supported for DSSE-KMS. Learn more [2]

- 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. Object Lock works only in versioned buckets. Learn more

- Disable
- Enable

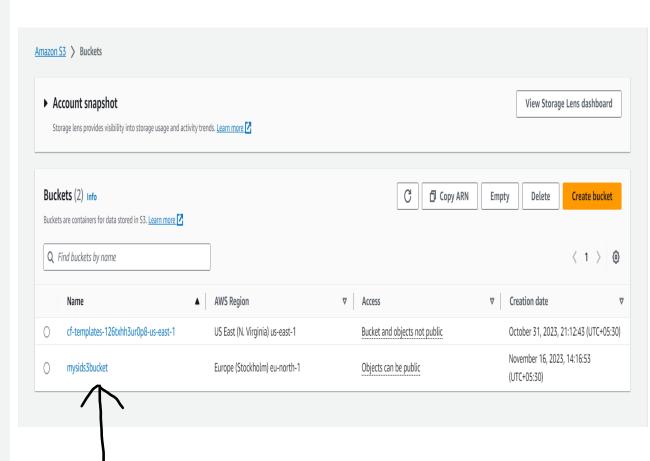
Permanently allows objects in this bucket to be locked. Additional Object Lock configuration is required in bucket details after bucket creation to protect objects in this bucket from being deleted or overwritten.

(i) Object Lock works only in versioned buckets. Enabling Object Lock automatically enables Versioning.

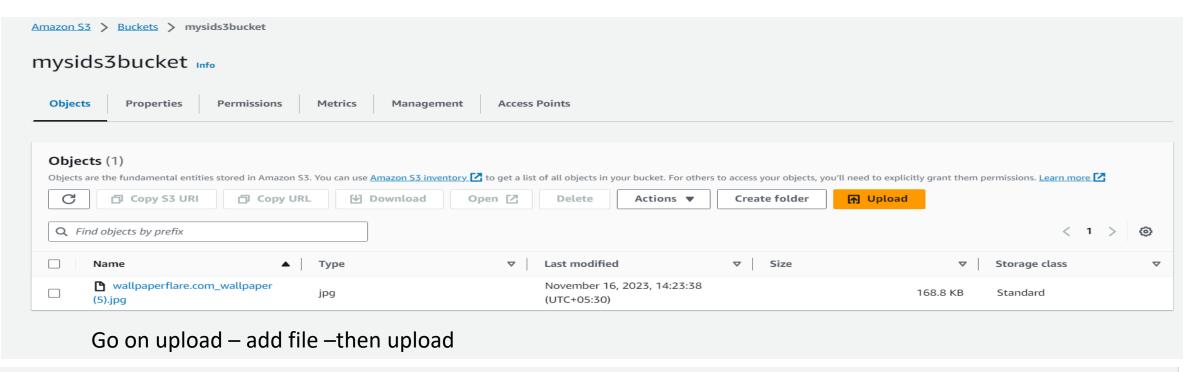
(i) After creating the bucket, you can upload files and folders to the bucket, and configure additional bucket settings.

Cancel

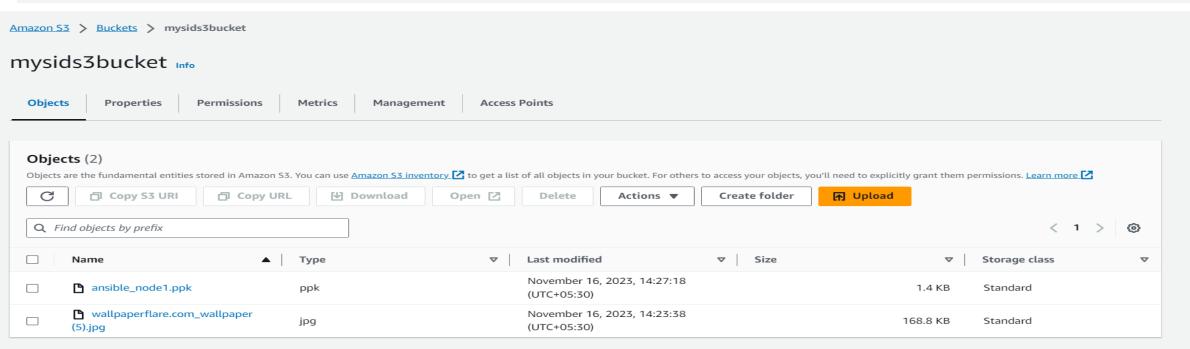
Create bucket



Click this bucket



(i)



S3 Bucket Versioning

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:

- Enable versioning for the bucket created in task 1.
- Re-upload any 2 files already uploaded to verify if versioning works.

Bucket overview

AWS Region

Europe (Stockholm) eu-north-1

Amazon Resource Name (ARN)

arn:aws:s3:::mysids3bucket

Creation date

November 16, 2023, 14:16:53 (UTC+05:30)

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

Enabled

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



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

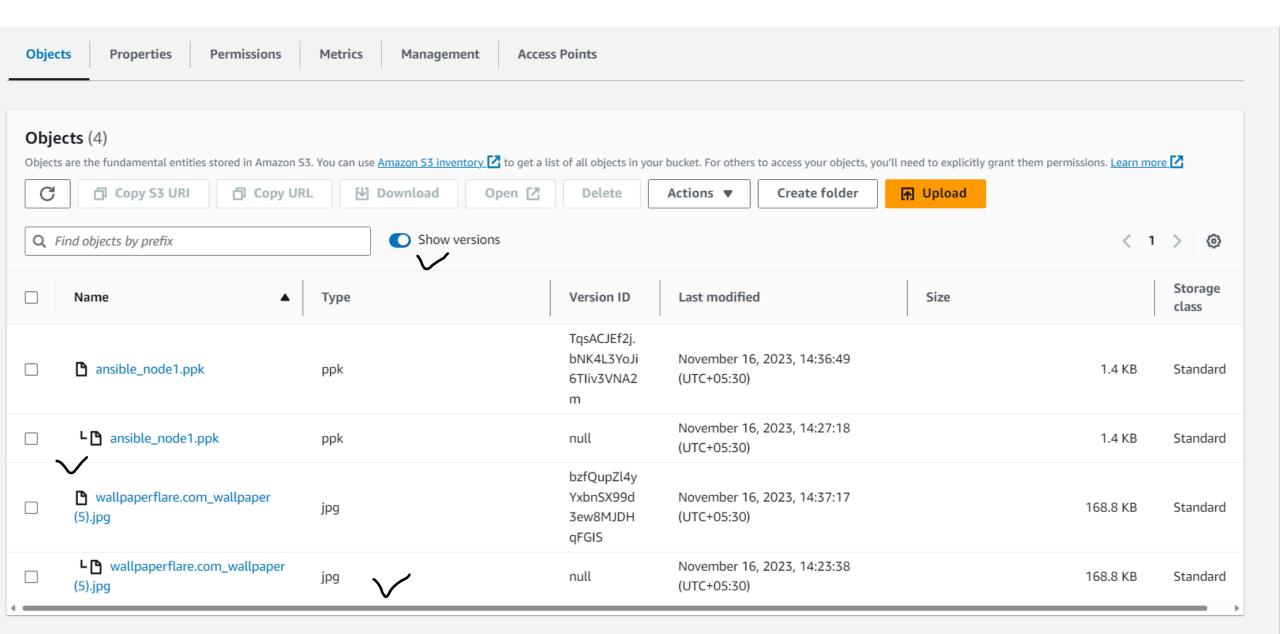
After enabling Bucket Versioning, you might need to update your lifecycle rules to manage previous versions of objects.

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 [7]

Disabled

Reupload the same file again –enable show version



S3 Website Hosting

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.

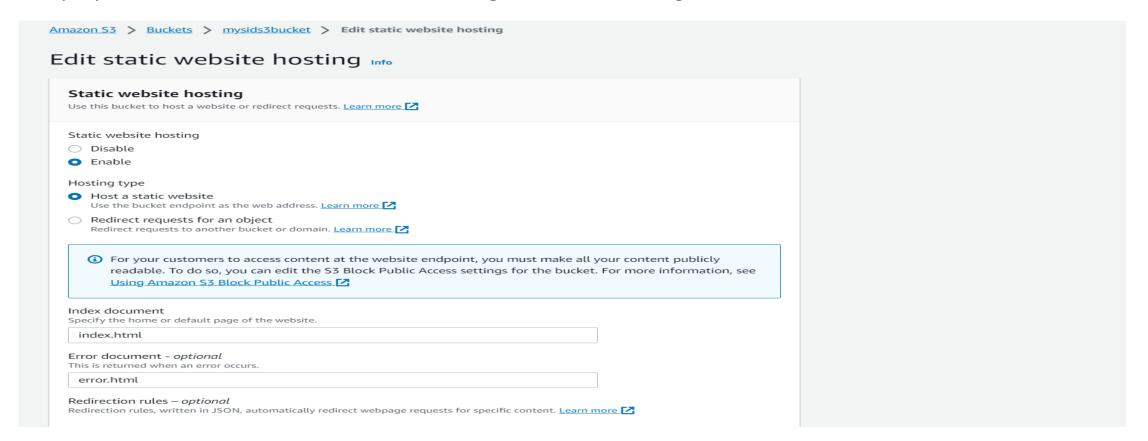
Tasks To Be Performed:

- 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

Create two files index, error with statement this is an index and error file and save it as index.html file in notepad. Then upload these files in s3 bucket.

error.html	html	November 16, 2023, 14:58:43 (UTC+05:30)	34.0 B	Standard
index.html	html	November 16, 2023, 14:59:07 (UTC+05:30)	22.0 B	Standard

Go on properties – down below –static web hosting –edit – save changes



Static website hosting

Edit

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

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://mysids3bucket.s3-website.eu-north-1.amazonaws.com



403 Forbidden

Code: AccessDenied

Message: Access Denied

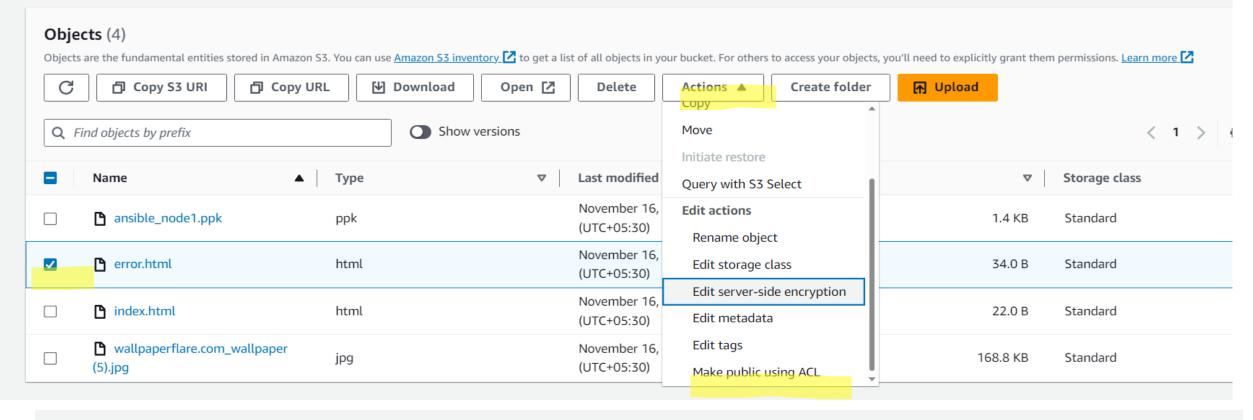
• RequestId: T852PGQA04GPK9B2

HostId: xaHnWXxEwU0gUff3EW3tIRsRie/eeM2lTH5DkFLPr/2751g8EgvoUoOKQpfZkmJtnaFYUB0G/NU=

An Error Occurred While Attempting to Retrieve a Custom Error Document

Code: AccessDenied

Message: Access Denied





The make public action enables public read access in the object access control list (ACL) settings. Learn more .

⚠ When public read access is enabled and not blocked by Block Public Access settings, anyone in the world can access the specified objects.

 Specified objects

 Q Find objects by name

 1 >

 Name
 ▲ Type ♥ Last modified
 ♥ Size ♥

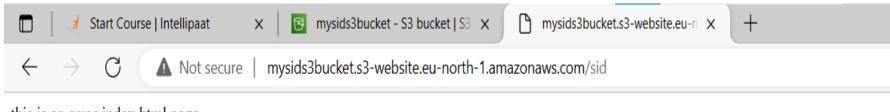
 Least modified
 ▼ Size ♥

 Perror.html
 html
 November 16, 2023, 14:58:43 (UTC+05:30)
 34.0 B

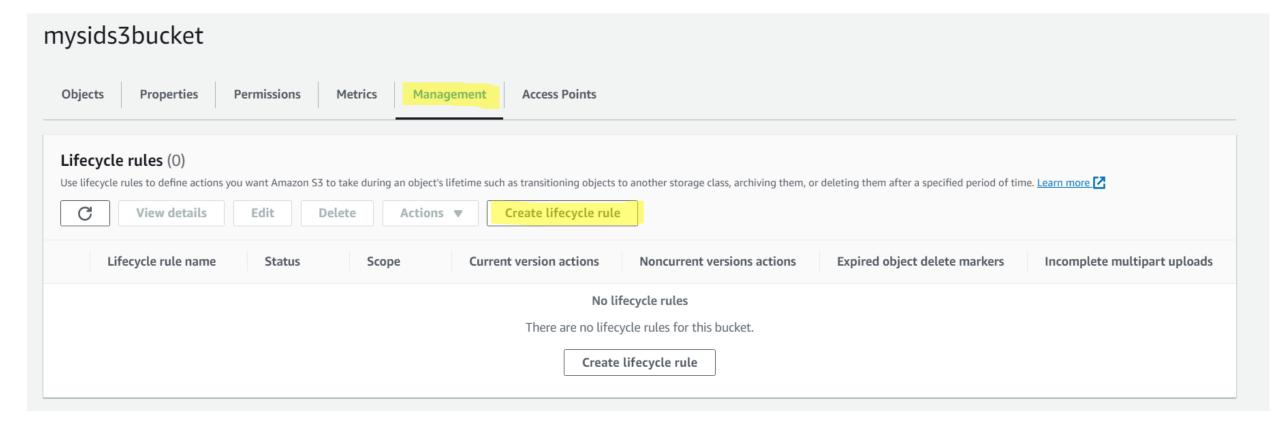
Did same with both error and index.html file.

Refresh the page and you see
Again when you use the same link and write something after / abcdefgh you see an error page

this is my index file



this is an error index.html page.



Create lifecycle rule Info

Lifecycle rule configuration

Lifecycle rule name

sid-lifecycle-rule1

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 [2]

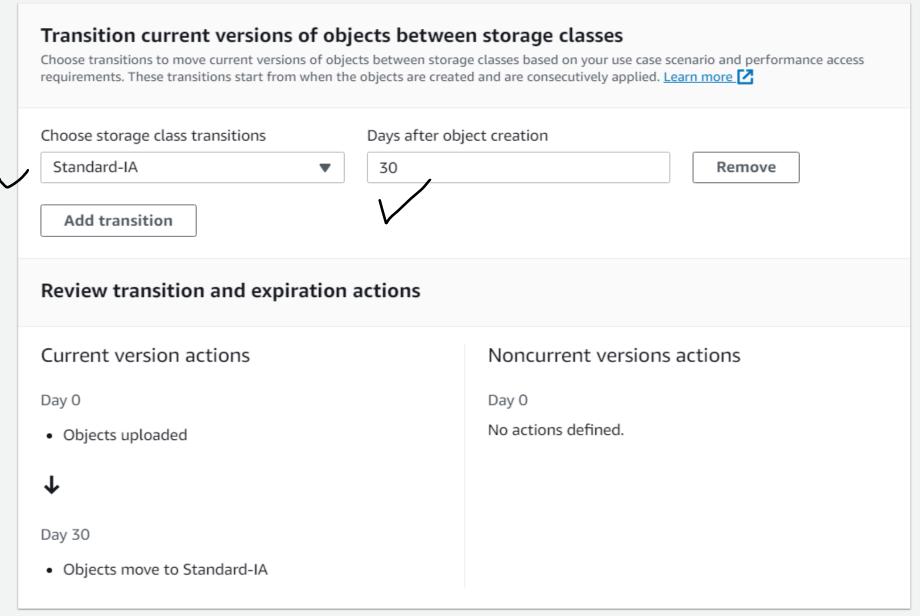
✓ I acknowledge that this rule will apply to all objects in the bucket.

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.



The lifecycle configuration was updated. Lifecycle rule "sid-lifecycle-rule1" 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.

Amazon S3 > Buckets > mysids3bucket > Lifecycle configuration

Lifecycle configuration Info

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.

