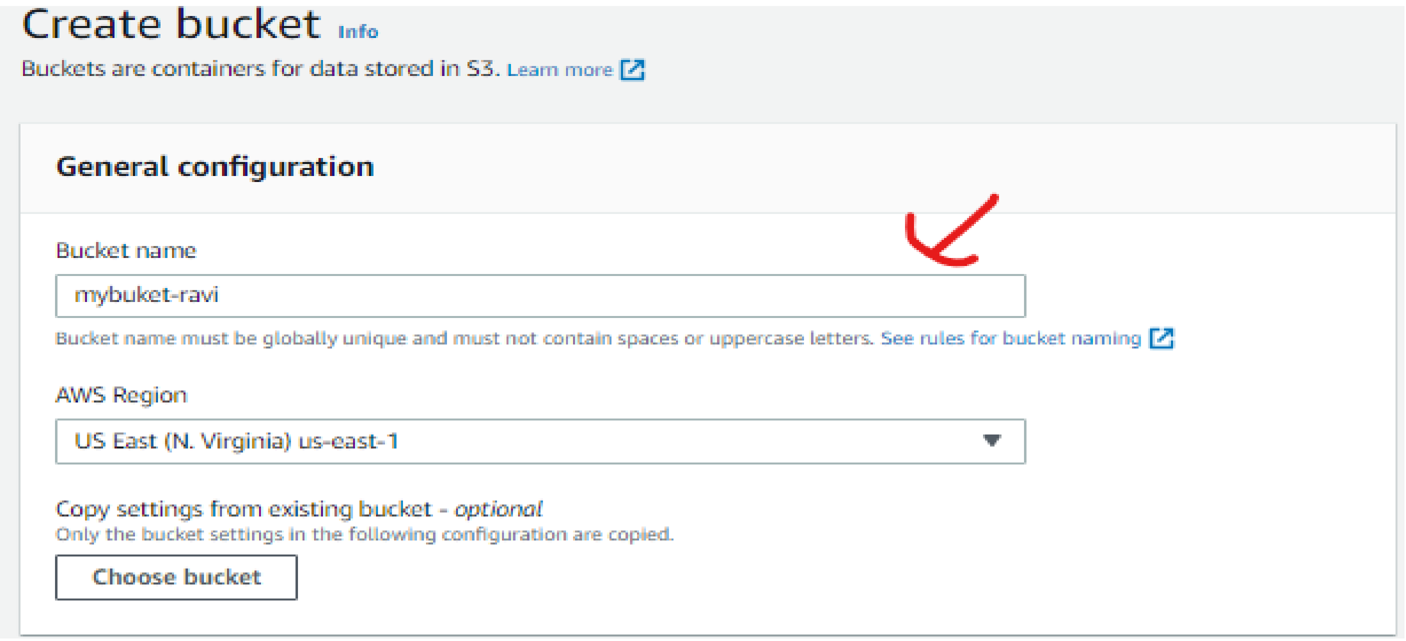


Create bucket Info

Buckets are containers for data stored in S3. Learn more

General configuration

Bucket name

mybuket-ravi

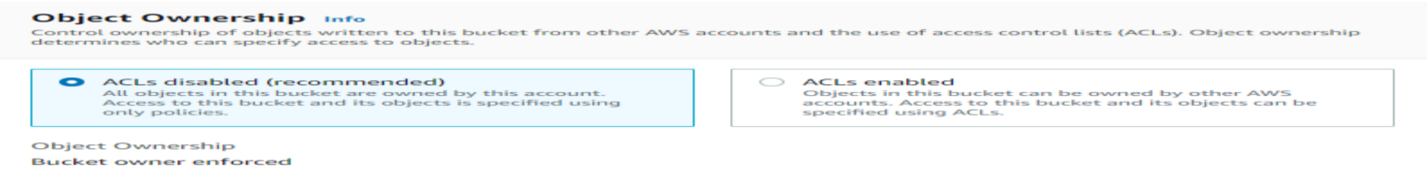
Bucket name must be globally unique and must not contain spaces or uppercase letters. See rules for bucket naming

AWS Region

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

Copy settings from existing bucket - *optional*

Only the bucket settings in the following configuration are copied.



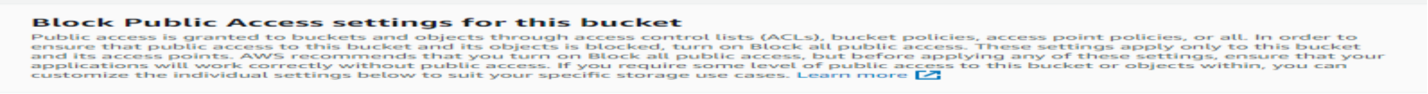
Object Ownership Info

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.

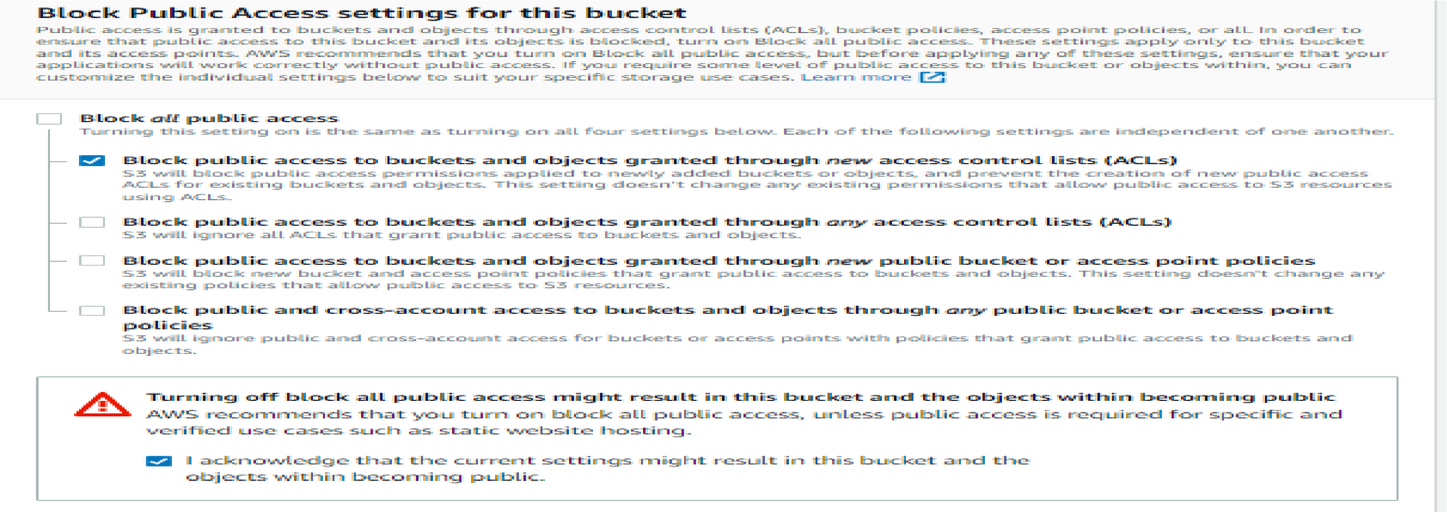
○ ACLs enabled
Objects in this bucket can be owned by other AWS accounts. Access to this bucket and its objects can be specified using ACLs.

Object Ownership
Bucket owner enforced



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 Public Access settings for this bucket

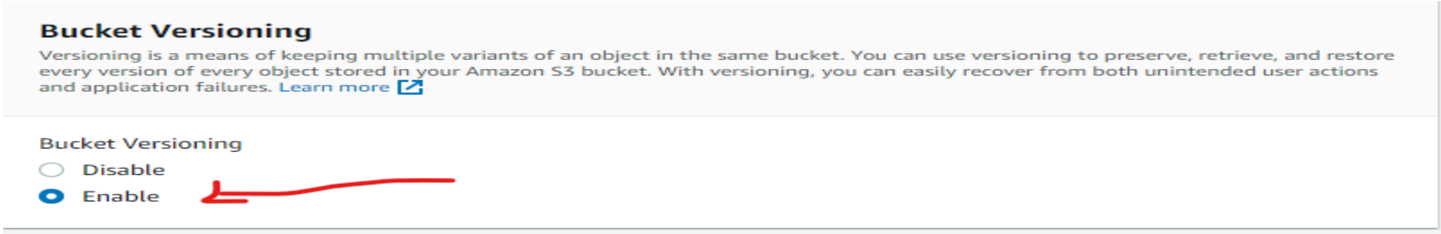
Public access is granted to buckets and objects through access control lists (ACLs), bucket policies, access point policies, or all. In order to ensure that public access to this bucket and its objects is blocked, turn on Block all public access. These settings apply only to this bucket and its access 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.

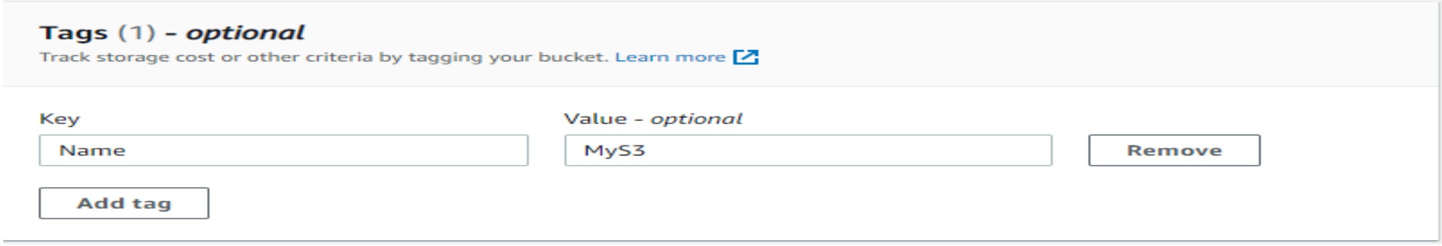
☑ I acknowledge that the current settings might result in this bucket and the objects within becoming public.



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

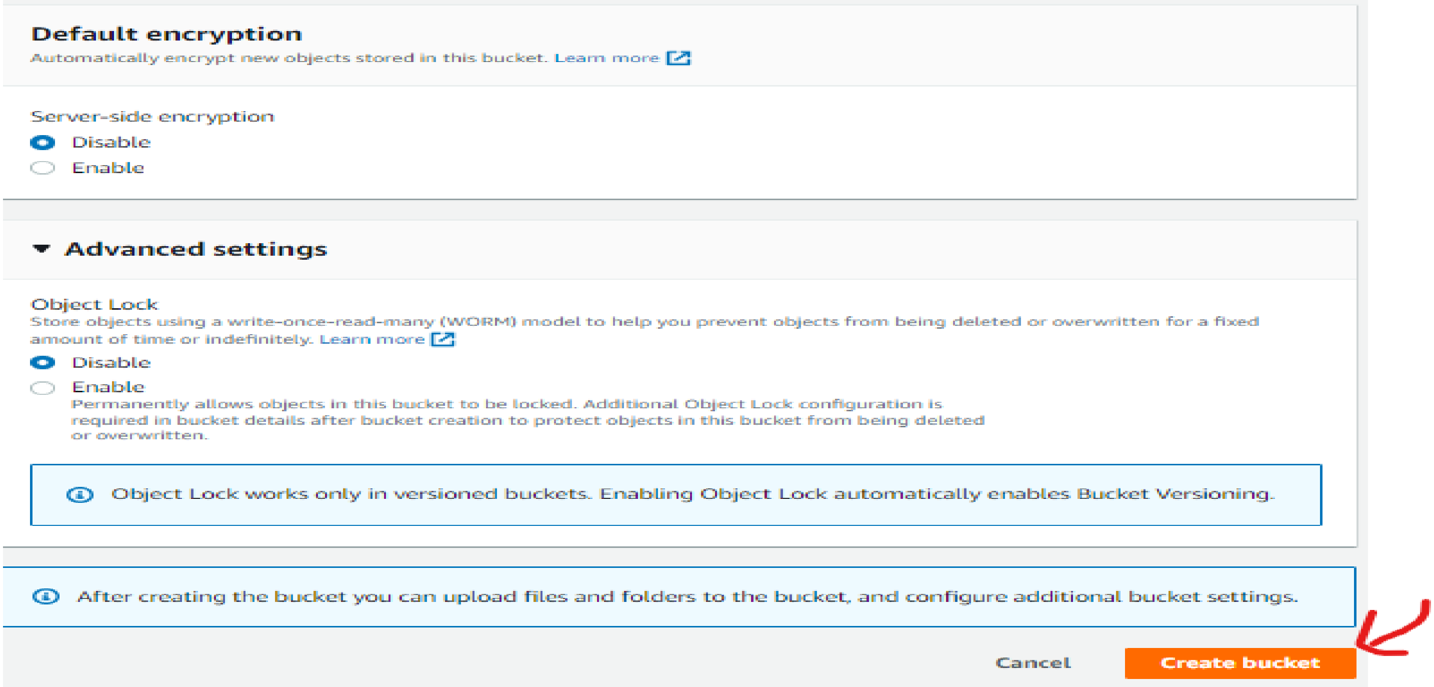
Bucket Versioning
○ Disable
● Enable



Tags (1) - *optional*

Track storage cost or other criteria by tagging your bucket. Learn more

Key	Value - *optional*	
Name	MyS3	Remove



Default encryption

Automatically encrypt new objects stored in this bucket. Learn more

Server-side encryption

● 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

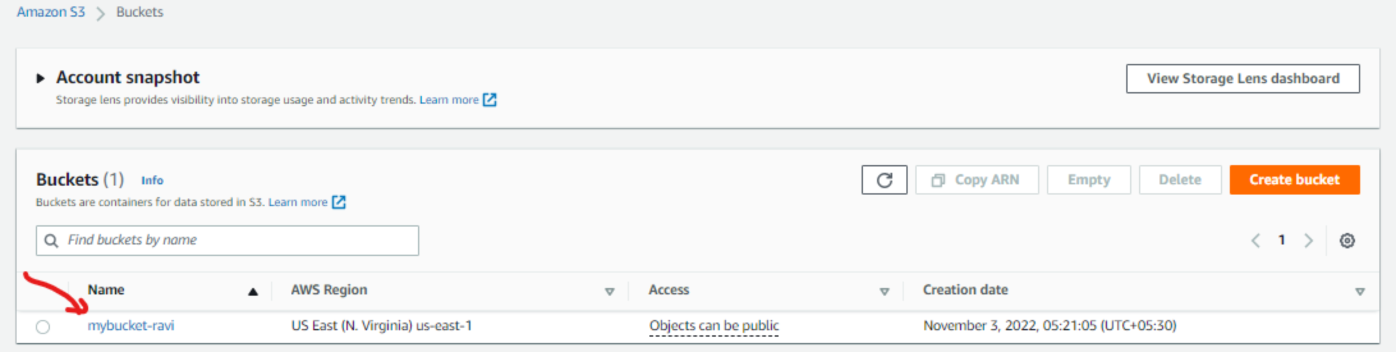
Permanently allows objects in this bucket to be locked. Additional Object Lock configuration is required in bucket details after bucket creation to protect objects in this bucket from being deleted or overwritten.

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.

Click **Create Bucket**

Bucket Created



Account snapshot

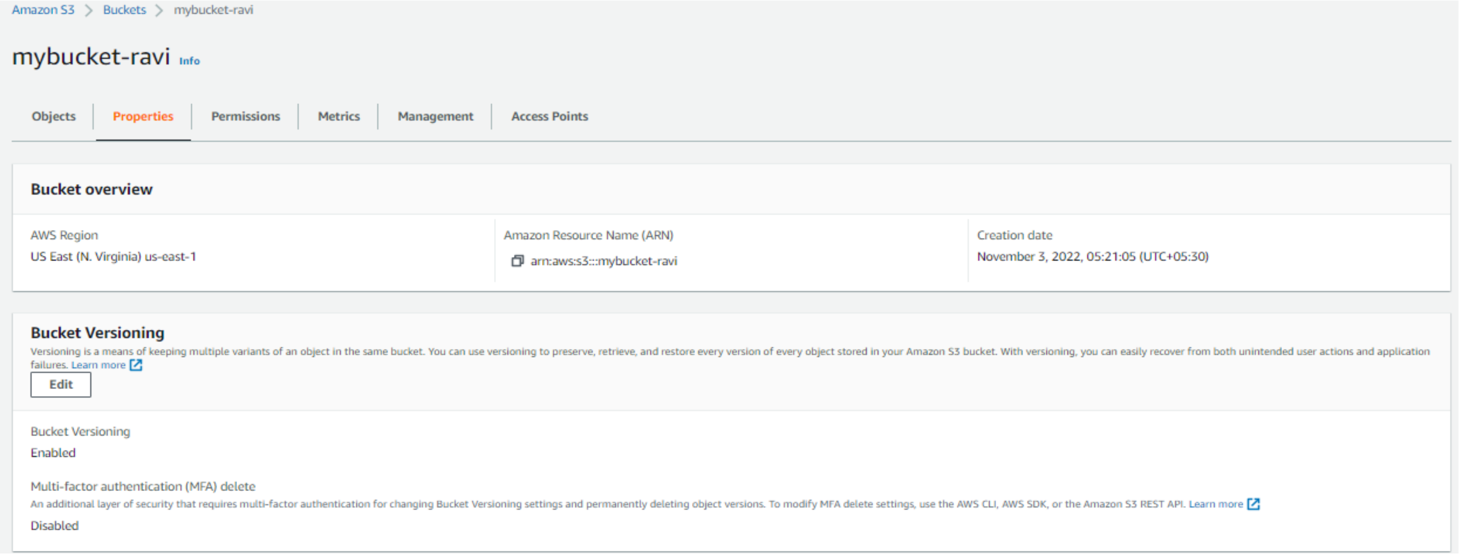
Storage lens provides visibility into storage usage and activity trends. Learn more

Buckets (1) Info

Buckets are containers for data stored in S3. Learn more

Name	AWS Region	Access	Creation date
mybucket-ravi	US East (N. Virginia) us-east-1	Objects can be public	November 3, 2022, 05:21:05 (UTC+05:30)

- ➔ Enable Version for S3 Bucket.
  - ○ Select the S3 Bucket and click the **Properties**
    - ▪ **Under Bucket Version click Edit Button**



Bucket overview

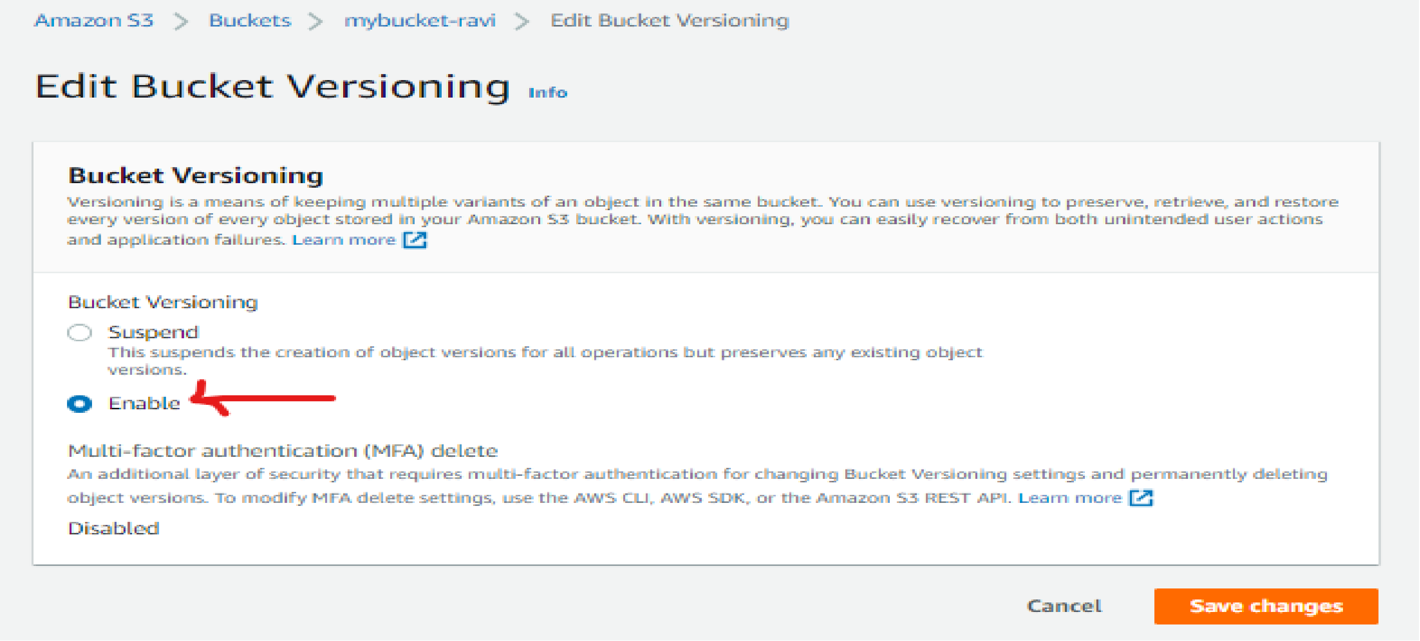
AWS Region	Amazon Resource Name (ARN)	Creation date
US East (N. Virginia) us-east-1	arn:aws:s3:::mybucket-ravi	November 3, 2022, 05:21:05 (UTC+05:30)

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
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



Amazon S3 > Buckets > mybucket-ravi > 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

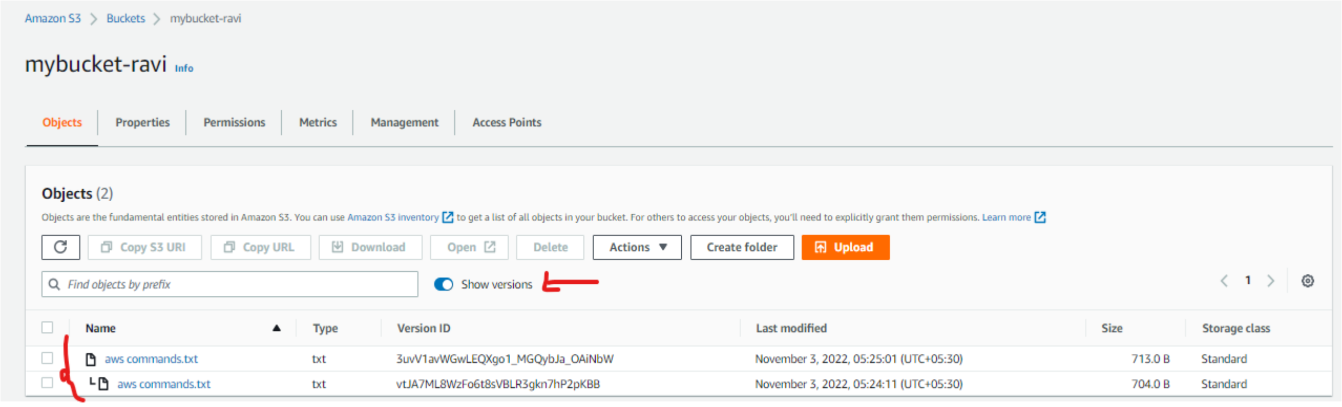
Bucket Versioning

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

● Enable

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

- ➔ To upload sample files, click the bucket name and click on **Upload** button.
    - o Upload the multiple versions of same file, toggle **Show Version, View multiple files.**

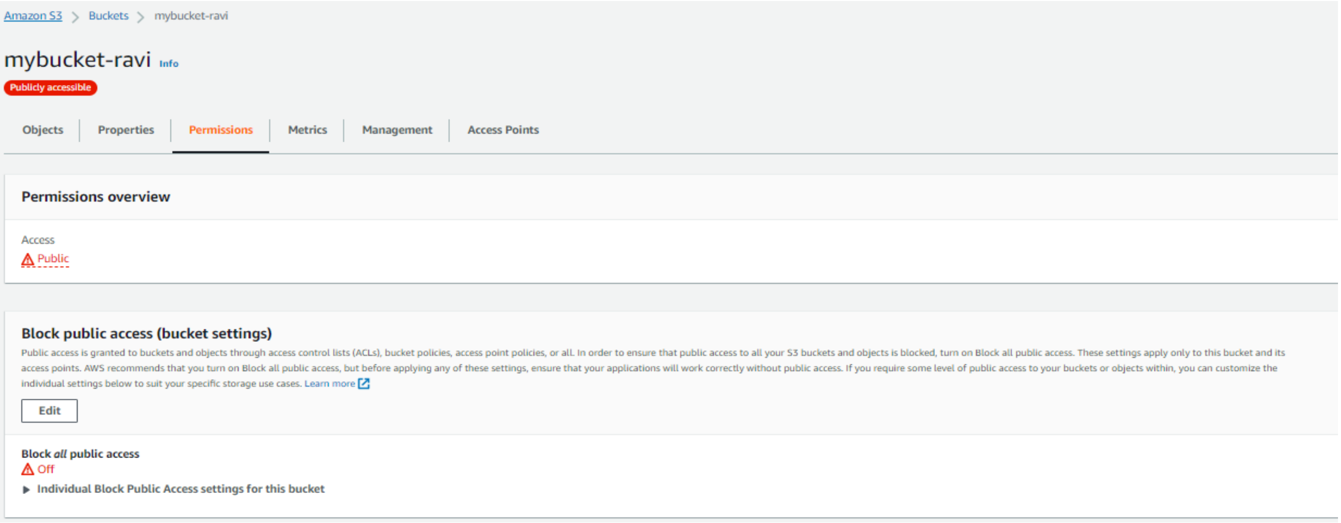


Objects (2)

Objects are the fundamental entities stored in Amazon S3. You can use Amazon S3 inventory to get a list of all objects in your bucket. For others to access your objects, you'll need to explicitly grant them permissions. Learn more

□	Name ▲	Type	Version ID	Last modified	Size	Storage class
□	aws commands.txt	txt	3uvV1avWGwLEQXgo1_MGQybJa_OAiNbW	November 3, 2022, 05:25:01 (UTC+05:30)	713.0 B	Standard
□	└ aws commands.txt	txt	vtJA7ML8WzFo6t8sVBLR3gkn7hP2pKBB	November 3, 2022, 05:24:11 (UTC+05:30)	704.0 B	Standard

Edit the Permissions of the Files/Object



Amazon S3 > Buckets > mybucket-ravi

mybucket-ravi Info

Publicly accessible

Permissions overview

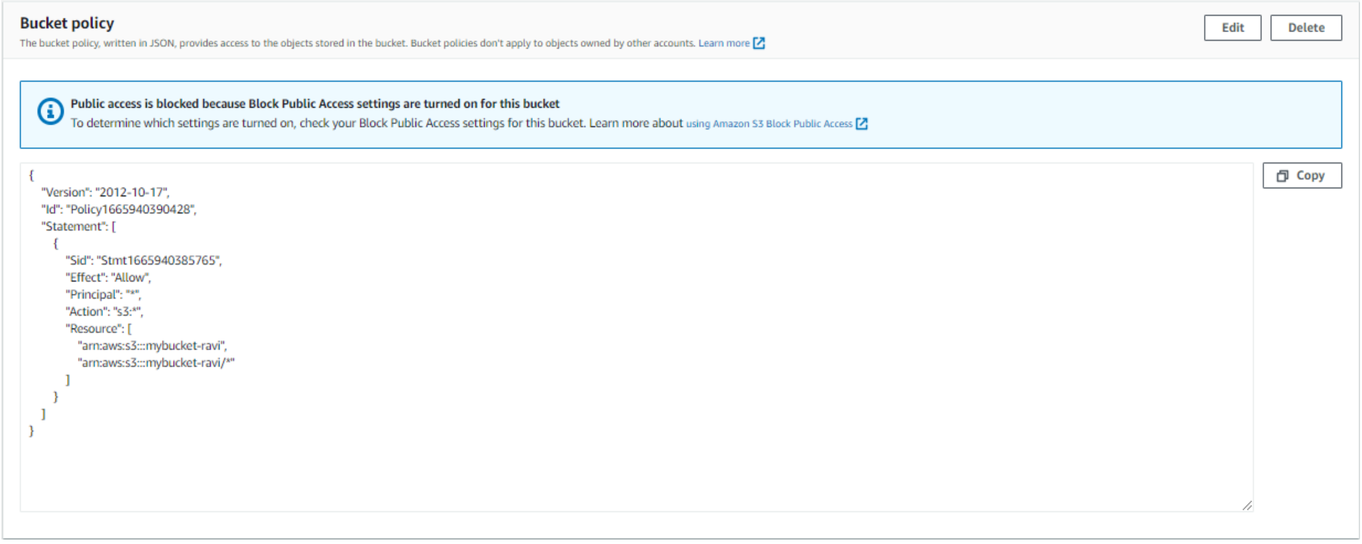
Access
⚠ Public

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
⚠ Off

▶ Individual Block Public Access settings for this bucket



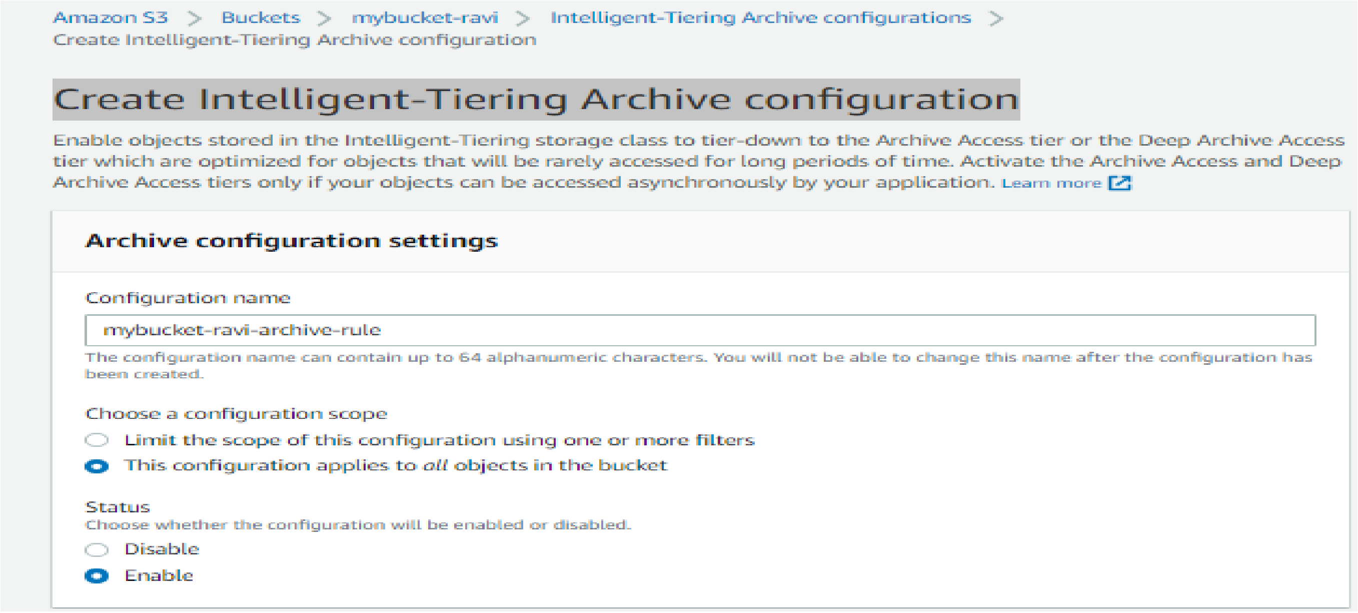
Bucket policy

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": "Policy1665940390428",
  "Statement": [
    {
      "Sid": "Stmt1665940385765",
      "Effect": "Allow",
      "Principal": "*",
      "Action": "s3:*",
      "Resource": [
        "arn:aws:s3:::mybucket-ravi",
        "arn:aws:s3:::mybucket-ravi/*"
      ]
    }
  ]
}
```

Create Intelligent-Tiering Archive configuration



Amazon S3 > Buckets > mybucket-ravi > Intelligent-Tiering Archive configurations > Create Intelligent-Tiering Archive configuration

Create Intelligent-Tiering Archive configuration

Enable objects stored in the Intelligent-Tiering storage class to tier-down to the Archive Access tier or the Deep Archive Access tier which are optimized for objects that will be rarely accessed for long periods of time. Activate the Archive Access and Deep Archive Access tiers only if your objects can be accessed asynchronously by your application. Learn more

Archive configuration settings

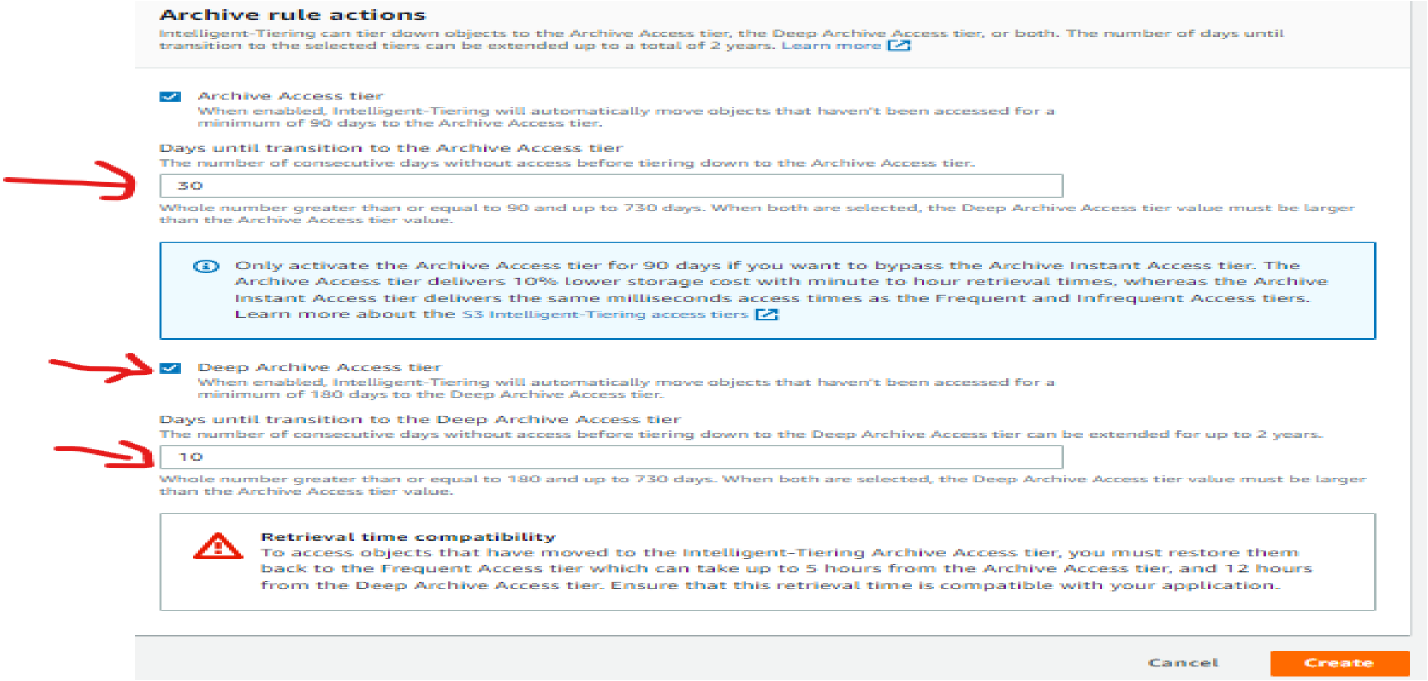
Configuration name
mybucket-ravi-archive-rule
The configuration name can contain up to 64 alphanumeric characters. You will not be able to change this name after the configuration has been created.

Choose a configuration scope
○ Limit the scope of this configuration using one or more filters
● This configuration applies to *all* objects in the bucket

Status
Choose whether the configuration will be enabled or disabled.
○ Disable
● Enable

- Provide the how many days file need to Archive

- Once Archive send file to Deep Archive (Provide the Days)



Archive rule actions

Intelligent-Tiering can tier down objects to the Archive Access tier, the Deep Archive Access tier, or both. The number of days until transition to the selected tiers can be extended up to a total of 2 years. Learn more

☑ Archive Access tier
When enabled, Intelligent-Tiering will automatically move objects that haven't been accessed for a minimum of 90 days to the Archive Access tier.

Days until transition to the Archive Access tier
The number of consecutive days without access before tiering down to the Archive Access tier.
30
Whole number greater than or equal to 90 and up to 730 days. When both are selected, the Deep Archive Access tier value must be larger than the Archive Access tier value.

Only activate the Archive Access tier for 90 days if you want to bypass the Archive Instant Access tier. The Archive Access tier delivers 10% lower storage cost with minute to hour retrieval times, whereas the Archive Instant Access tier delivers the same milliseconds access times as the Frequent and Infrequent Access tiers. Learn more about the S3 Intelligent-Tiering access tiers

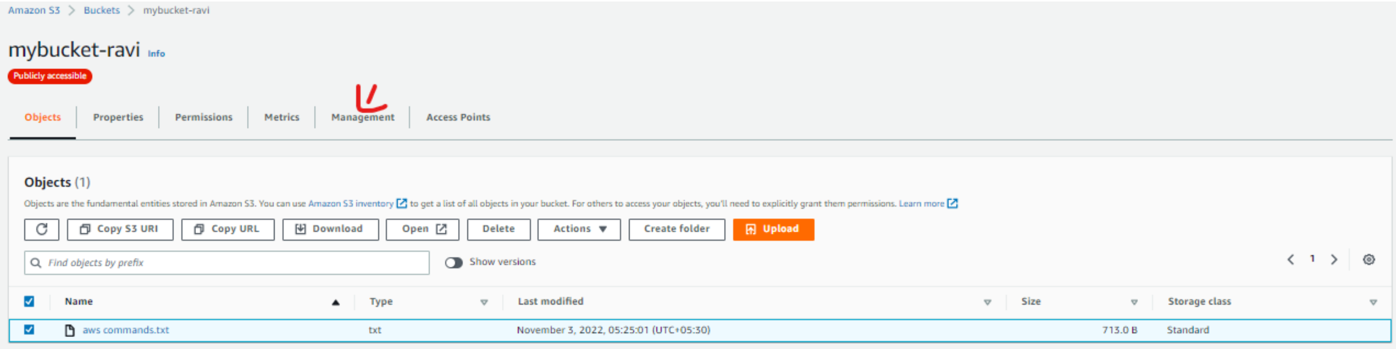
☑ Deep Archive Access tier
When enabled, Intelligent-Tiering will automatically move objects that haven't been accessed for a minimum of 180 days to the Deep Archive Access tier.

Days until transition to the Deep Archive Access tier
The number of consecutive days without access before tiering down to the Deep Archive Access tier can be extended for up to 2 years.
10
Whole number greater than or equal to 180 and up to 730 days. When both are selected, the Deep Archive Access tier value must be larger than the Archive Access tier value.

Retrieval time compatibility
To access objects that have moved to the Intelligent-Tiering Archive Access tier, you must restore them back to the Frequent Access tier which can take up to 5 hours from the Archive Access tier, and 12 hours from the Deep Archive Access tier. Ensure that this retrieval time is compatible with your application.

Define the Life Cycle Management of the Bucket

→ **Click the Management Tab**

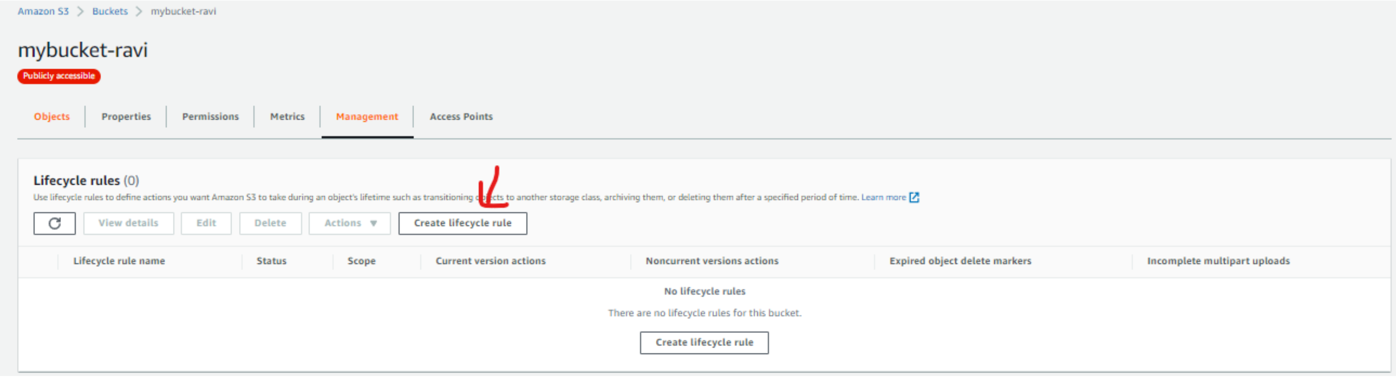


Objects (1)

Objects are the fundamental entities stored in Amazon S3. You can use Amazon S3 inventory to get a list of all objects in your bucket. For others to access your objects, you'll need to explicitly grant them permissions. Learn more

☑	Name	Type	Last modified	Size	Storage class
☑	aws commands.txt	txt	November 3, 2022, 05:25:01 (UTC+05:30)	713.0 B	Standard

→ **Click Create Lifecycle rule**



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

Lifecycle rule name	Status	Scope	Current version actions	Noncurrent versions actions	Expired object delete markers	Incomplete multipart uploads

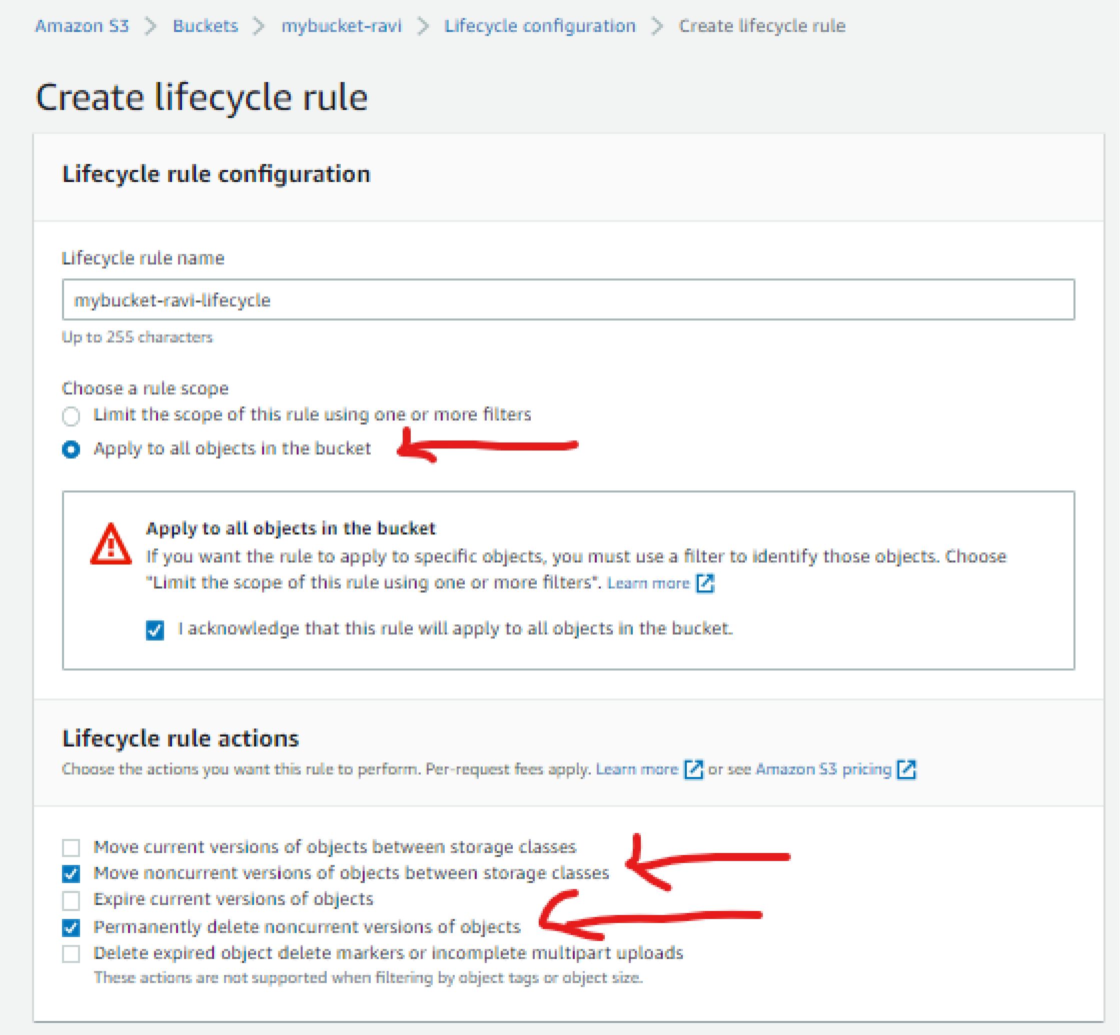
No lifecycle rules

There are no lifecycle rules for this bucket.

- **Provide the Name of the Lifecycle Rule**

→ **Check box selected apply the Lifecycle rule to all objects in the Bucket**

- ➔ **Lifecycle Rule Actions**
  - **Move noncurrent versions of objects between storage classes**
    - **The above option selected to move the objects based on the conditions/days to archive**
  - **Permanently delete noncurrent versions of objects**
    - **The above options delete the files once it reaches provide value/days from Archive**



Amazon S3 > Buckets > mybucket-ravi > Lifecycle configuration > Create lifecycle rule

Create lifecycle rule

Lifecycle rule configuration

Lifecycle rule name

mybucket-ravi-lifecycle

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

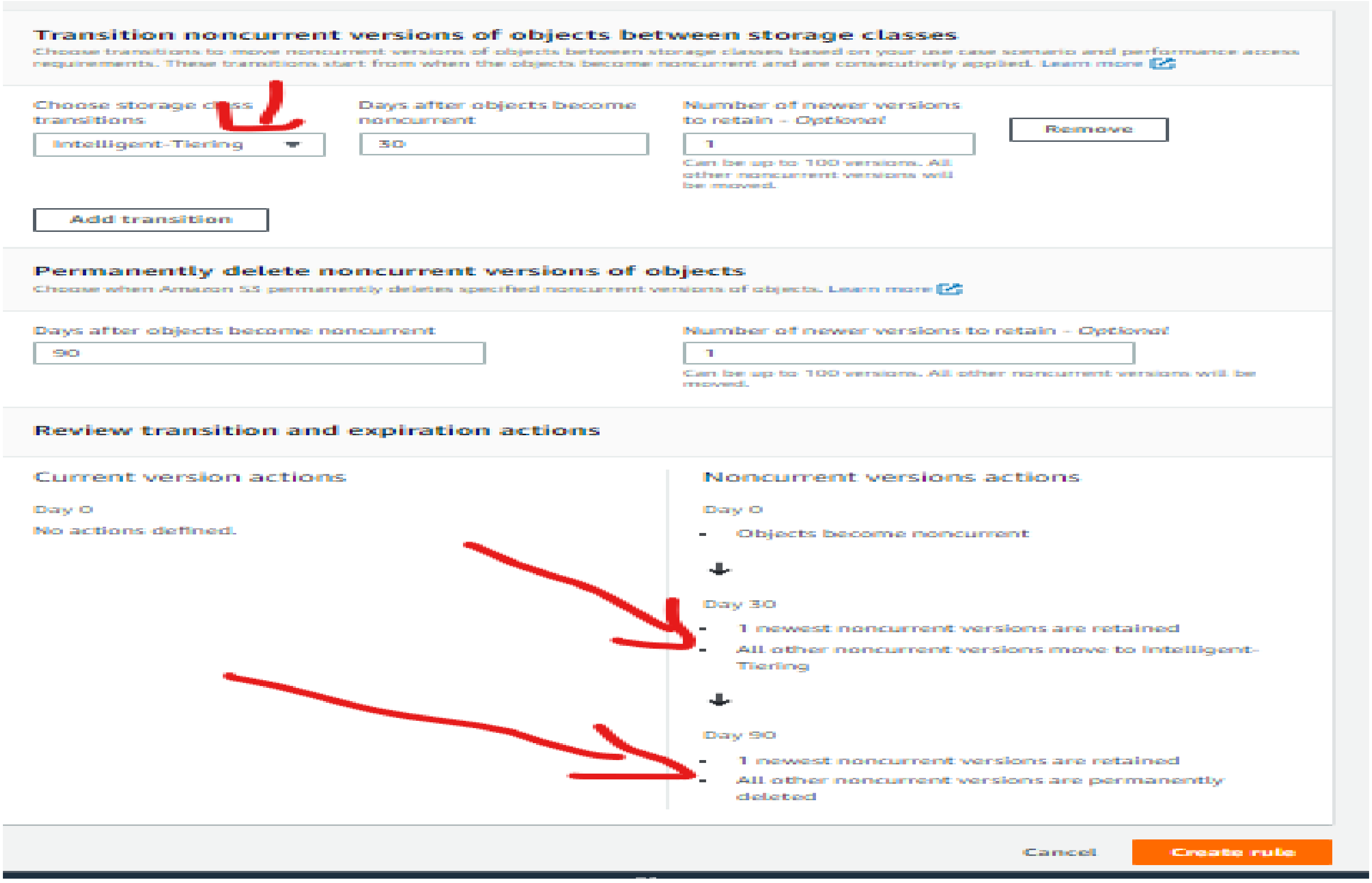
□ Expire current versions of objects

☑ 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.

- ➔ **After selecting two check box in Lifecycle Rule Actions.**
  - **Provide the values/Days below.**



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: Intelligent-Tiering

Days after objects become noncurrent: 30

Number of newer versions to retain - Optional: 1

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

Permanently delete noncurrent versions of objects

Choose when Amazon S3 permanently deletes specified noncurrent versions of objects. Learn more

Days after objects become noncurrent: 90

Number of newer versions to retain - Optional: 1

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

Review transition and expiration actions

Current version actions

Day 0

No actions defined.

Noncurrent versions actions

Day 0

- Objects become noncurrent

Day 30

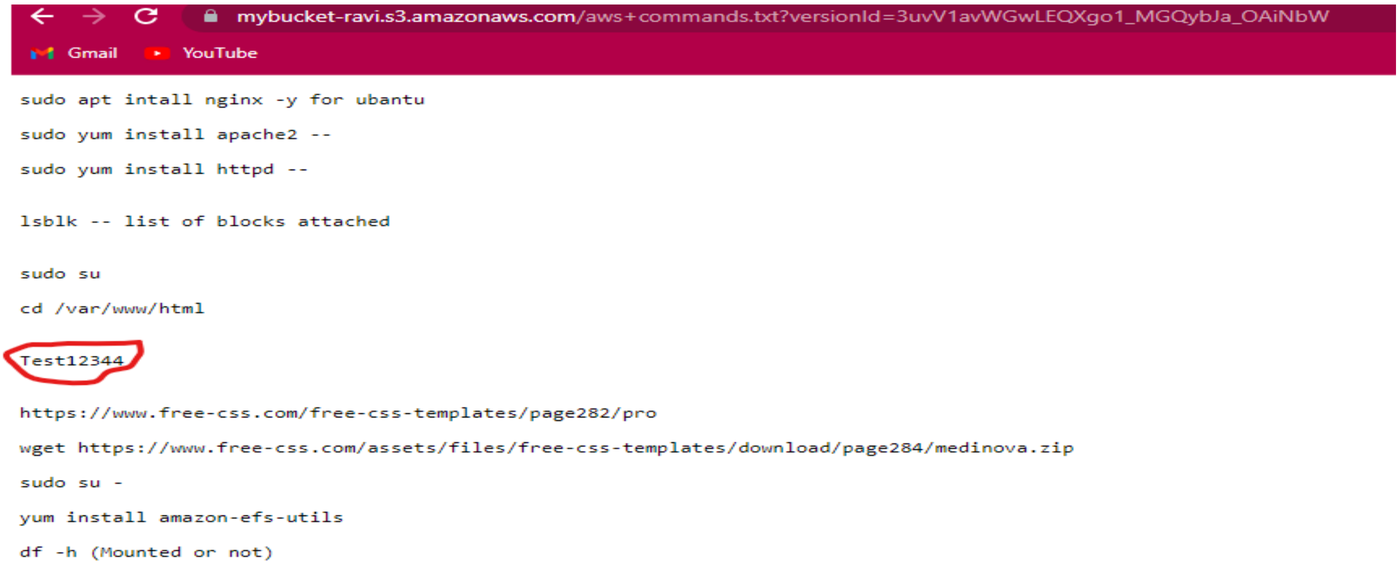
- 1 newest noncurrent versions are retained
- All other noncurrent versions move to Intelligent-Tiering

Day 90

- 1 newest noncurrent versions are retained
- All other noncurrent versions are permanently deleted

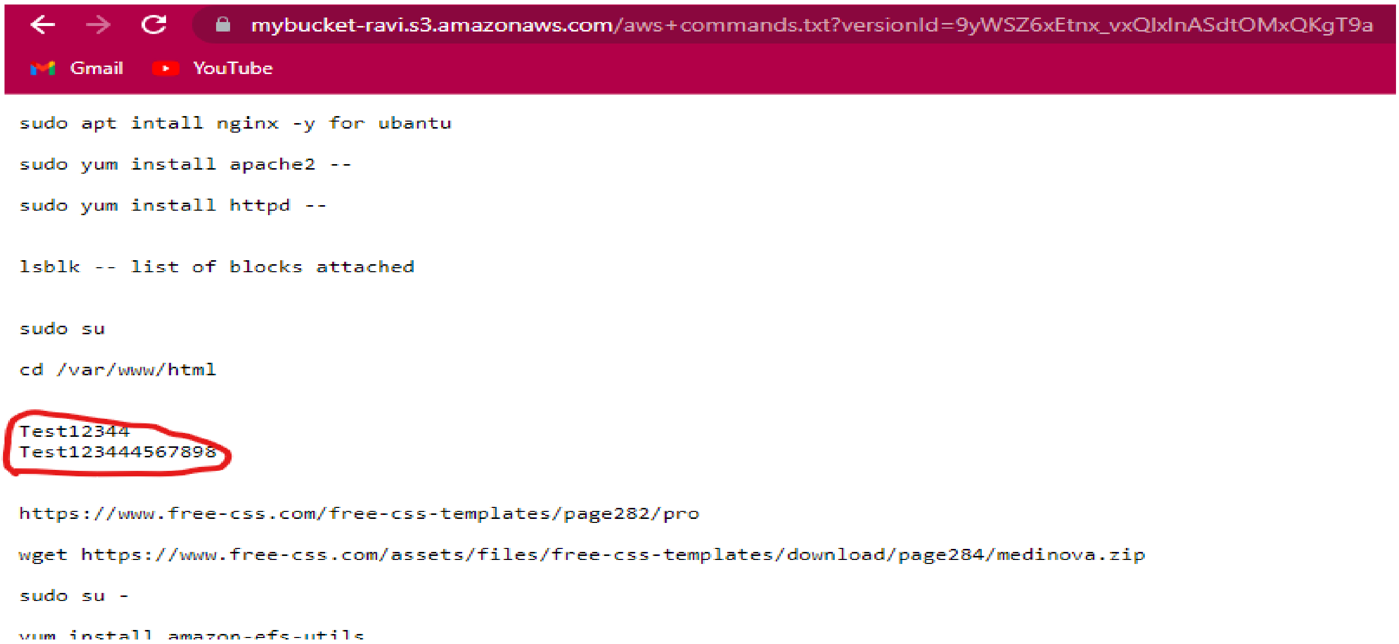
Click on **Create Rule**

- ➔ **Select the file and click on Copy URL, Paste in IE/Edge etc., it will open the file**



mybucket-ravi.s3.amazonaws.com/aws+commands.txt?versionId=3uvV1avWGwLEQXgo1_MGQybJa_OAiNbW

```
sudo apt intall nginx -y for ubantu
sudo yum install apache2 --
sudo yum install httpd --

lsblk -- list of blocks attached

sudo su
cd /var/www/html

Test12344

https://www.free-css.com/free-css-templates/page282/pro
wget https://www.free-css.com/assets/files/free-css-templates/download/page284/medinova.zip
sudo su -
yum install amazon-efs-utils
df -h (Mounted or not)
```

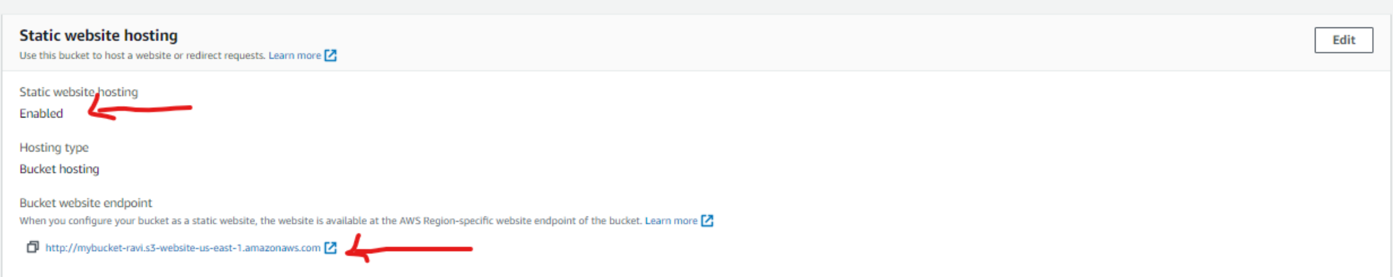


mybucket-ravi.s3.amazonaws.com/aws+commands.txt?versionId=9yWSZ6xEtnx_vxQlxInASdtOMxQKgT9a

```
sudo apt intall nginx -y for ubantu

sudo yum install apache2 --

sudo yum install httpd --


lsblk -- list of blocks attached


sudo su

cd /var/www/html


Test12344
Test123444567898


https://www.free-css.com/free-css-templates/page282/pro

wget https://www.free-css.com/assets/files/free-css-templates/download/page284/medinova.zip

sudo su -

yum install amazon-efs-utils
```

- **Creating Static Web Site**
  - **Static Web Site can access simple web page upload in to S3 and can access.**

- **Properties-> Static Website hosting->Edit**



Static website hosting

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

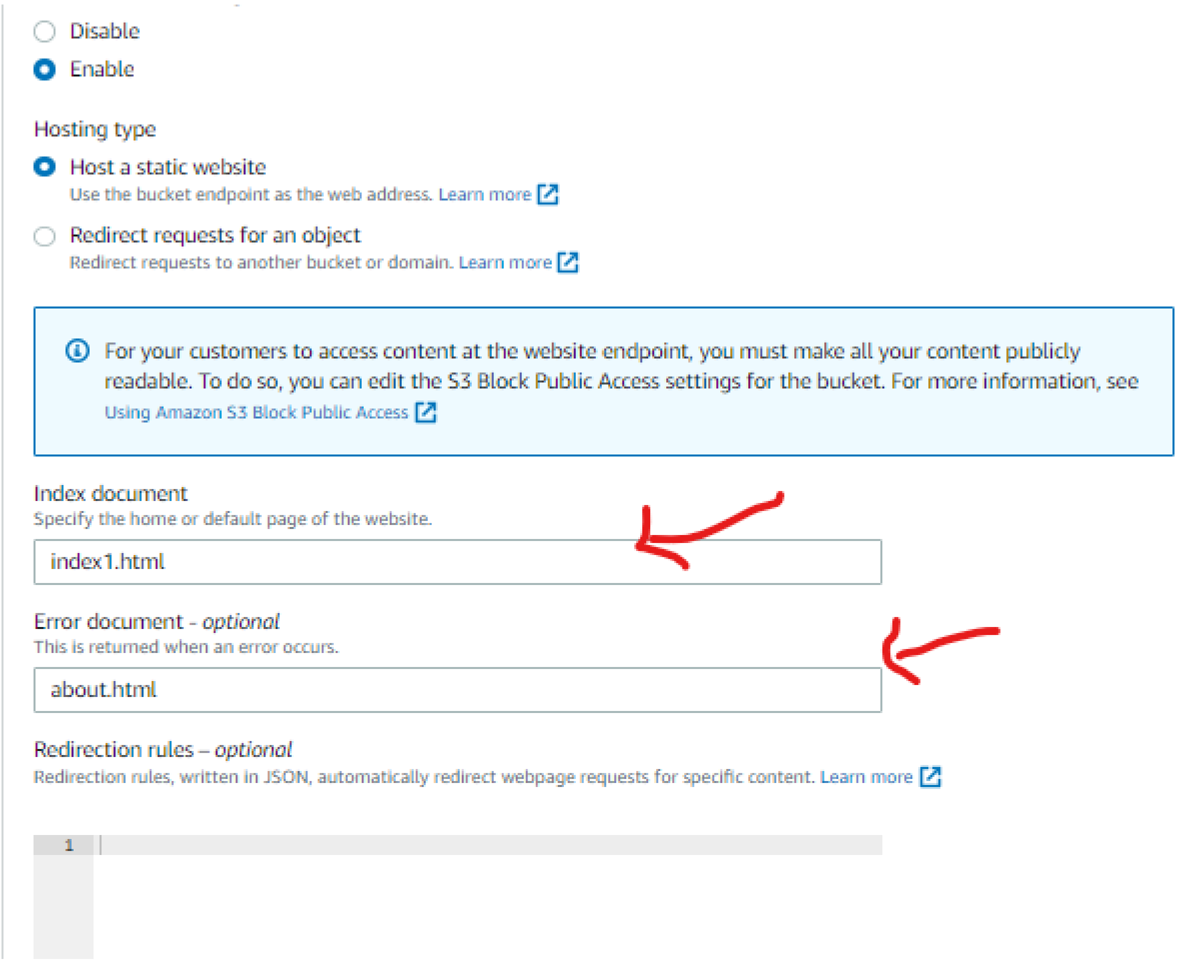
Static website hosting
Enabled

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://mybucket-ravi.s3-website-us-east-1.amazonaws.com

- **Provided Error document and it is diverted to Error Document.**
  - **Provided wrong file in Index document section, then it is diverted to show About.html.**



○ 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.

index1.html

Error document - *optional*

This is returned when an error occurs.

about.html

Redirection rules – *optional*

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