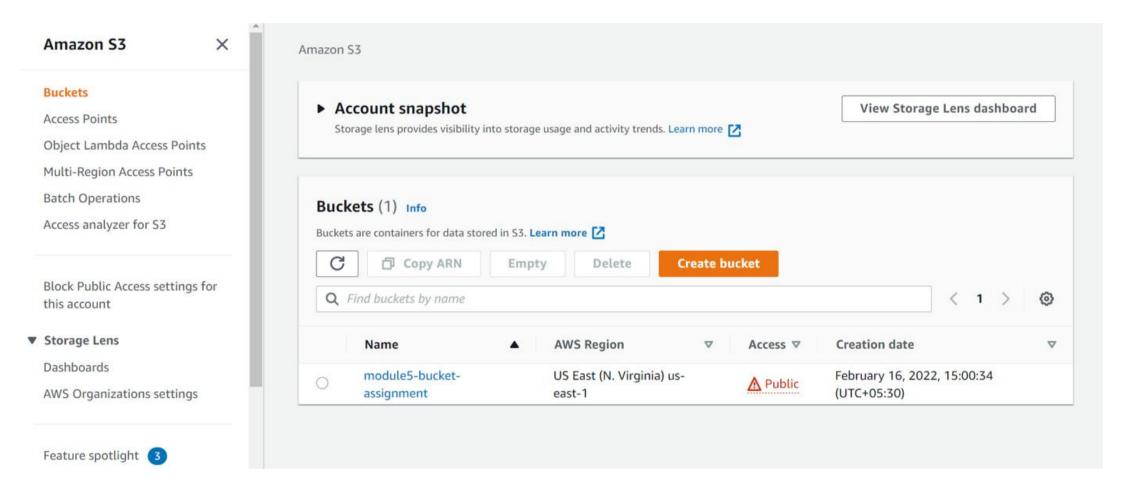
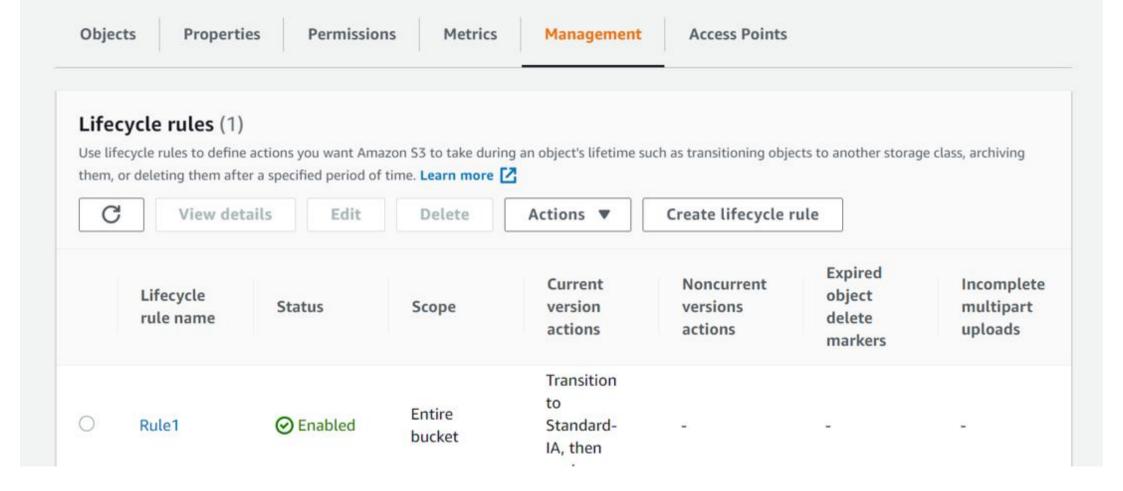
Use the same bucket in assignments



module5-bucket-assignment

Publicly accessible



Lifecycle rule configuration

Lifecycle rule name

Rule2

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

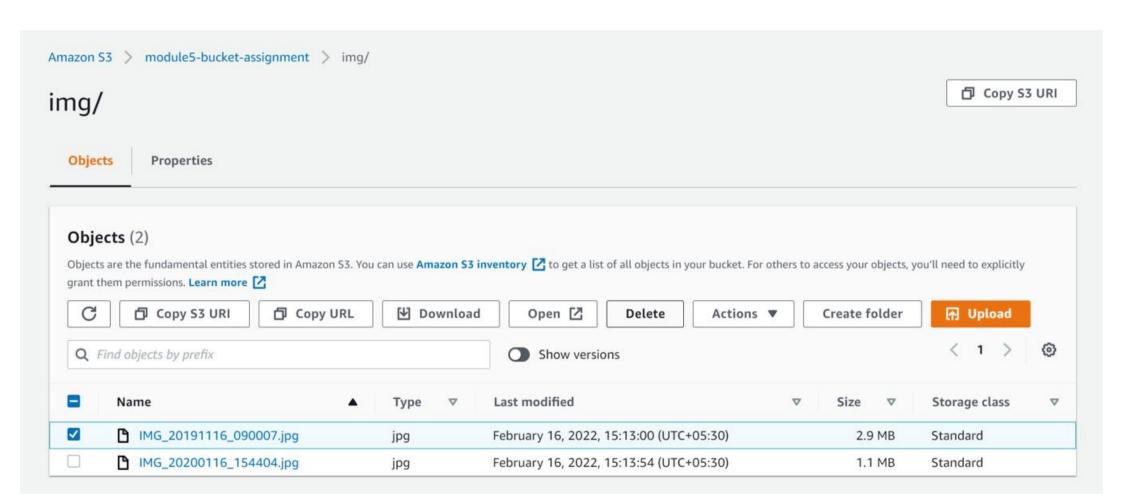
Choose the actions you want this rule to perform. Per-request fees apply. Learn more 🔀 or see Amazon S3 pricing 🖸

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. 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 75

Review transition and expiration actions

For version-enabled buckets, Amazon S3 adds a delete mannen-versioned buckets, Amazon S3 permanently removes to	rker and the current version of an object is retained as a noncurrent version. For the object. Learn more
Days after object creation	
75	
Permanently delete noncurrent version	ons of objects
Permanently delete noncurrent version Choose when Amazon S3 permanently deletes specified no	oncurrent versions of objects. Learn more

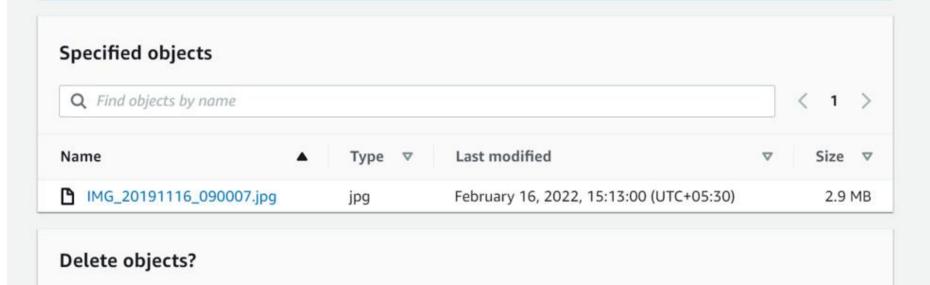
Can be up to 100 versions. All other noncurrent versions will be moved.





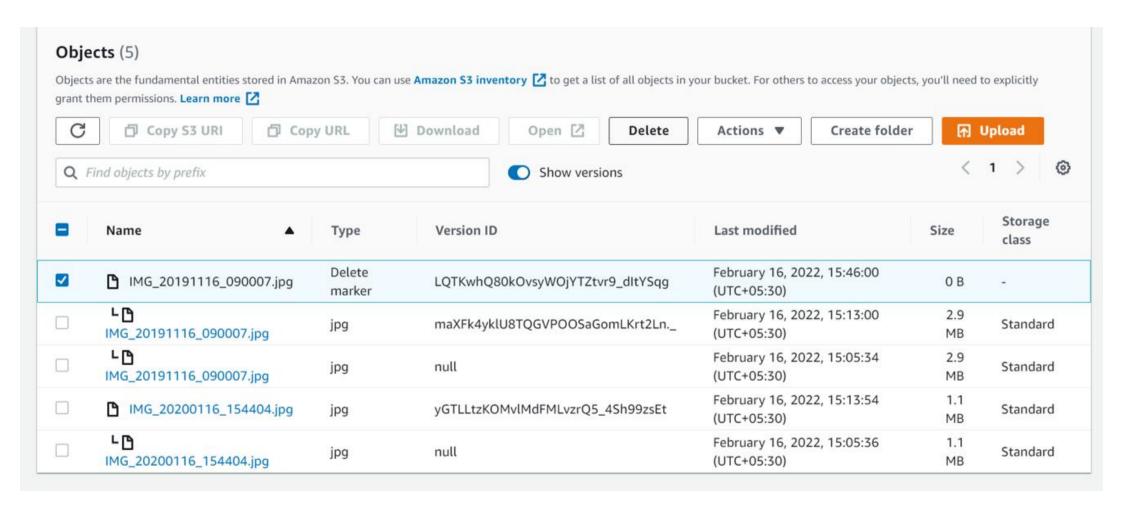
Deleting the specified objects adds delete markers to them

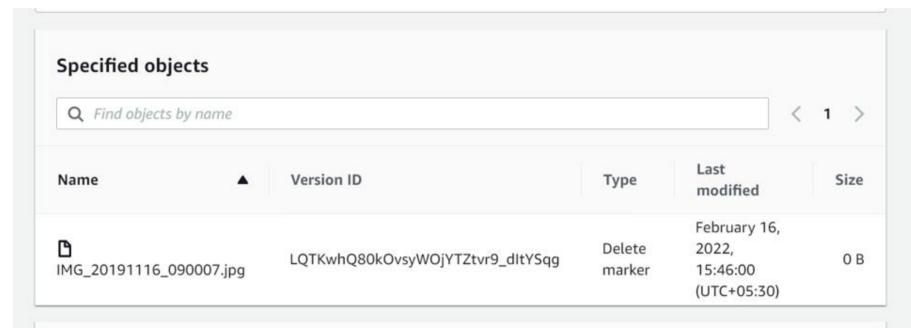
If you need to undo the delete action, you can delete the delete markers. Learn more 🔀



To confirm deletion, type delete in the text input field.

delete

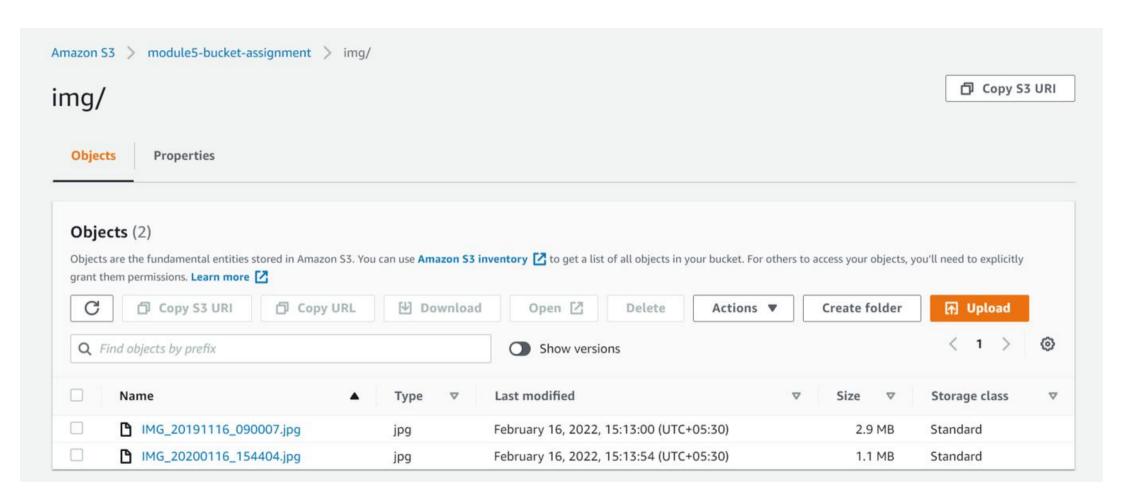




Permanently delete objects?

To confirm deletion, type permanently delete in the text input field.

permanently delete



Hosted zone configuration

A hosted zone is a container that holds information about how you want to route traffic for a domain, such as example.com, and its subdomains.

Domain name Info

This is the name of the domain that you want to route traffic for.

anithatest.ga

Valid characters: a-z, 0-9, ! " # \$ % & '() * +, - / :; < = > ? @ [\] ^_ `{|}. ~

Description - optional Info

This value lets you distinguish hosted zones that have the same name.

The hosted zone is used for...

The description can have up to 256 characters. 0/256

Type Info

The type indicates whether you want to route traffic on the internet or in an Amazon VPC.



Public hosted zone

A public hosted zone determines how traffic is routed on the internet.



Private hosted zone

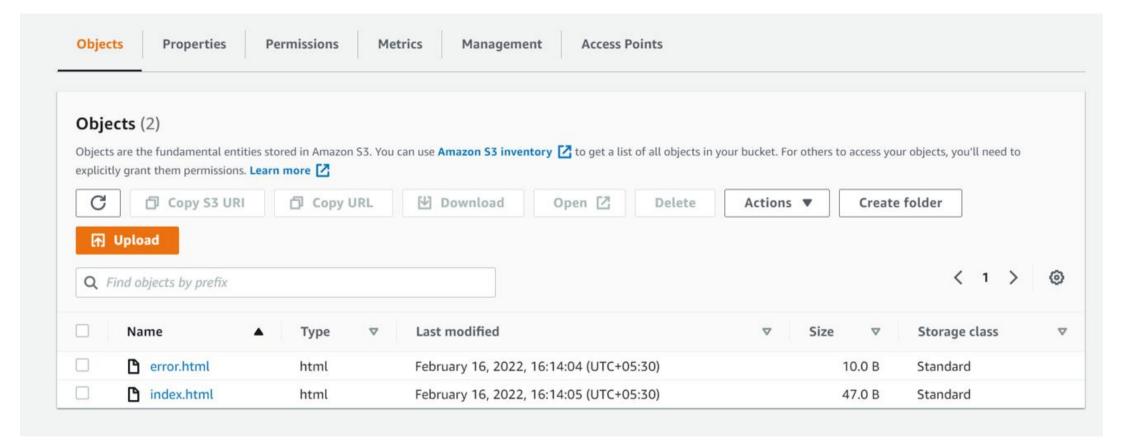
A private hosted zone determines how traffic is routed within an Amazon VPC.

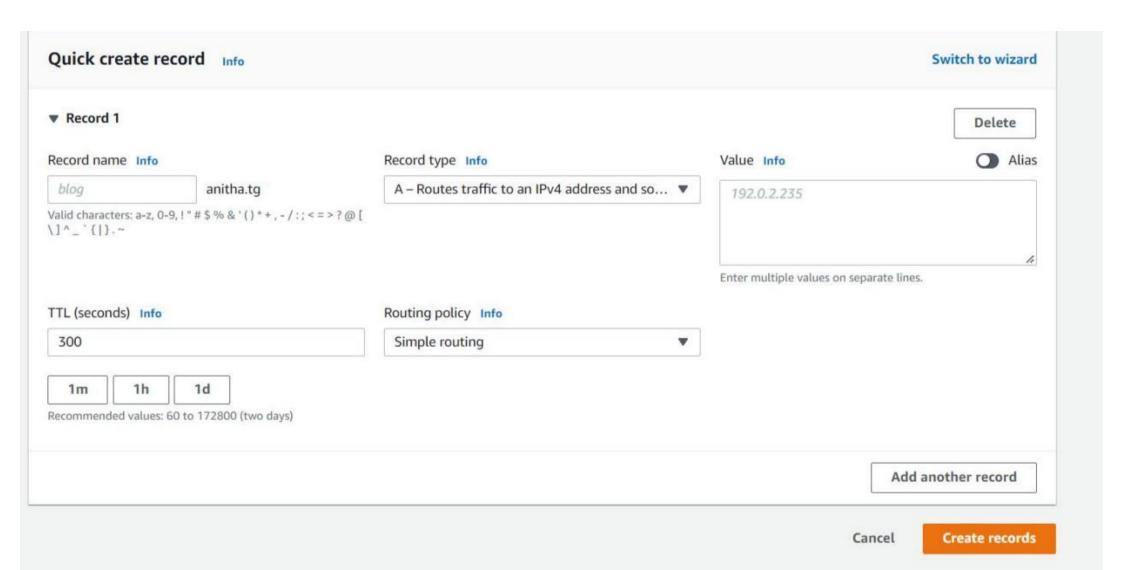
Tags Info

Apply tags to hosted zones to help organize and identify them.

1612 Edit Block public access (bucket settings) Info ss Points ect Lambda Access Points Block public access (bucket settings) ti-Region Access Points Public access is granted to buckets and objects through access control lists (ACLs), bucket policies, access point policies, or all. In order to h Operations 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 ess analyzer for S3 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 k Public Access settings for account 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. age Lens Block public access to buckets and objects granted through new access control lists (ACLs) boards 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 Organizations settings 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. ure spotlight Block public access to buckets and objects granted through new public bucket or access point policies

Edit the bucket policy





Winn oxisting records

Hi this is sample html file

error page