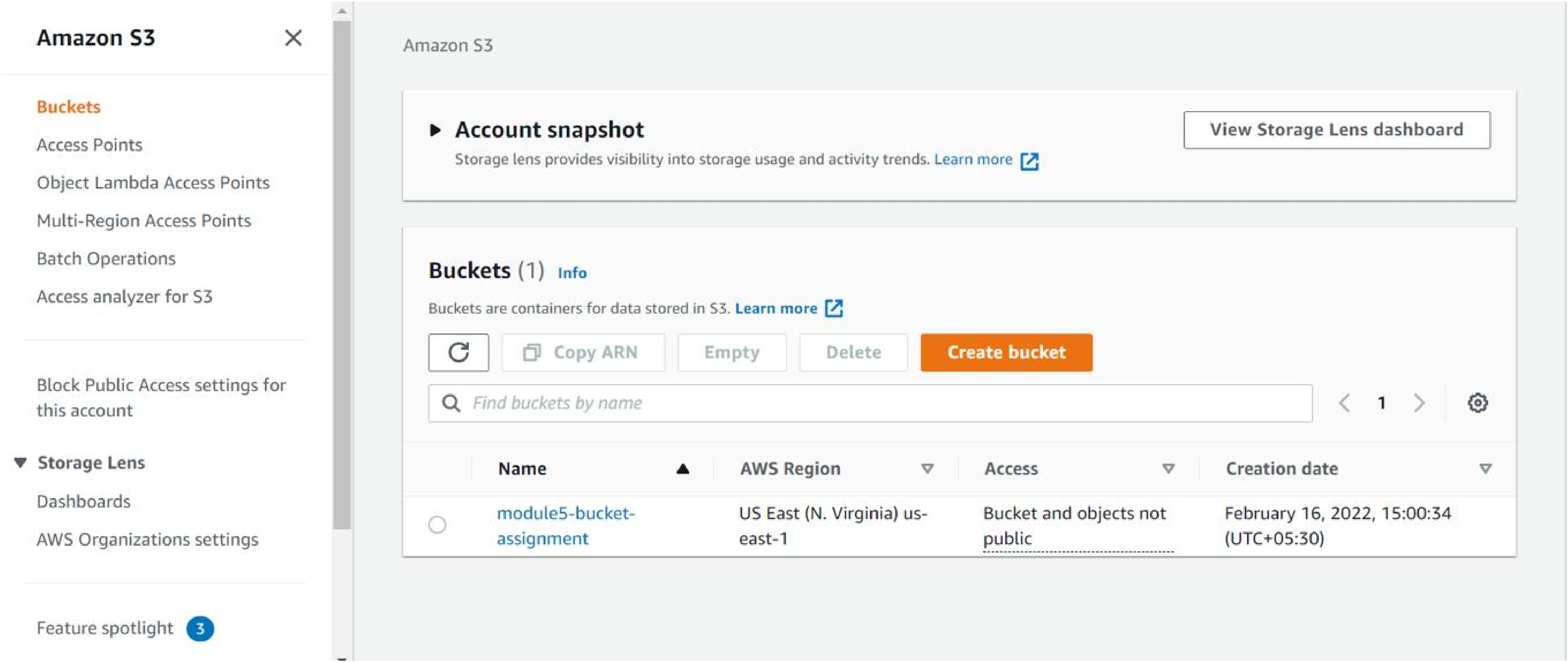


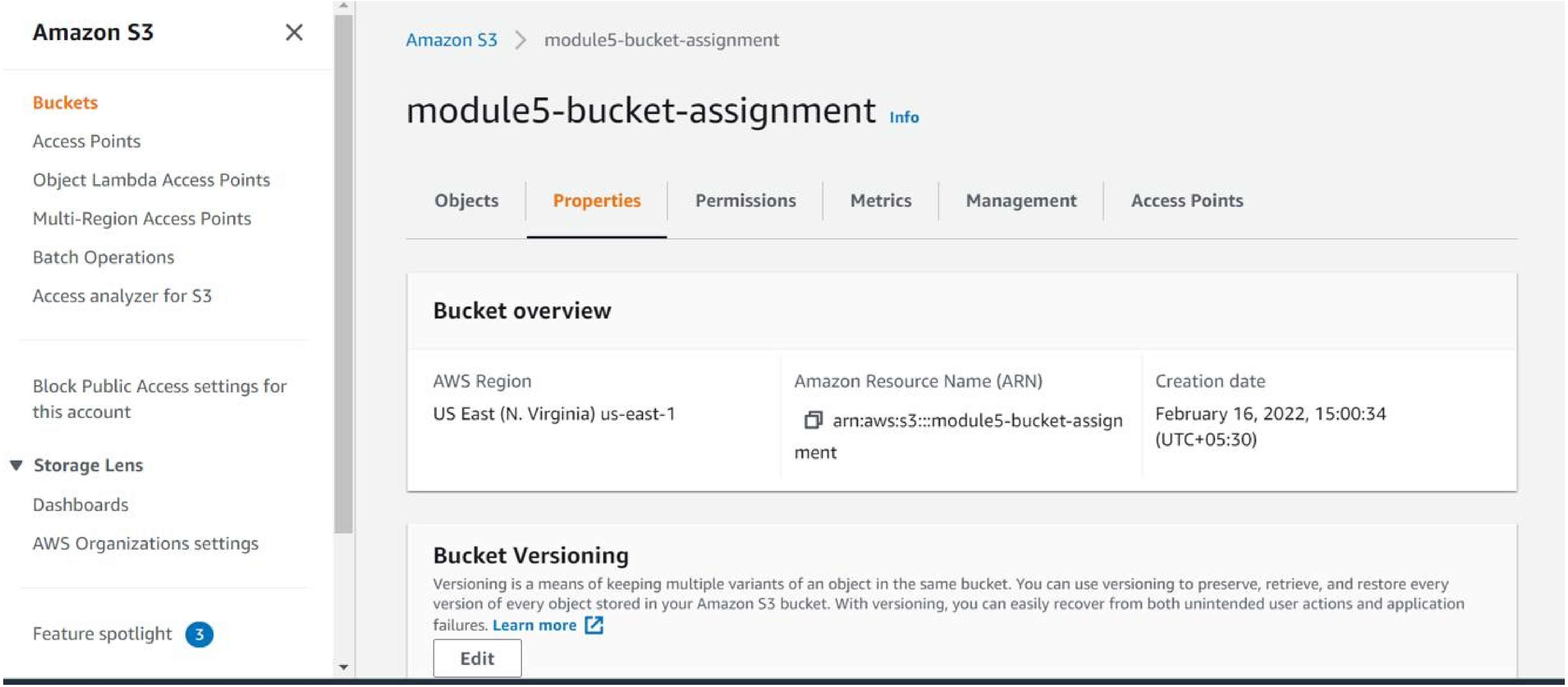
▶ Account snapshot

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 ▽
○	module5-bucket-assignment	US East (N. Virginia) us-east-1	Bucket and objects not public	February 16, 2022, 15:00:34 (UTC+05:30)



module5-bucket-assignment

Bucket overview

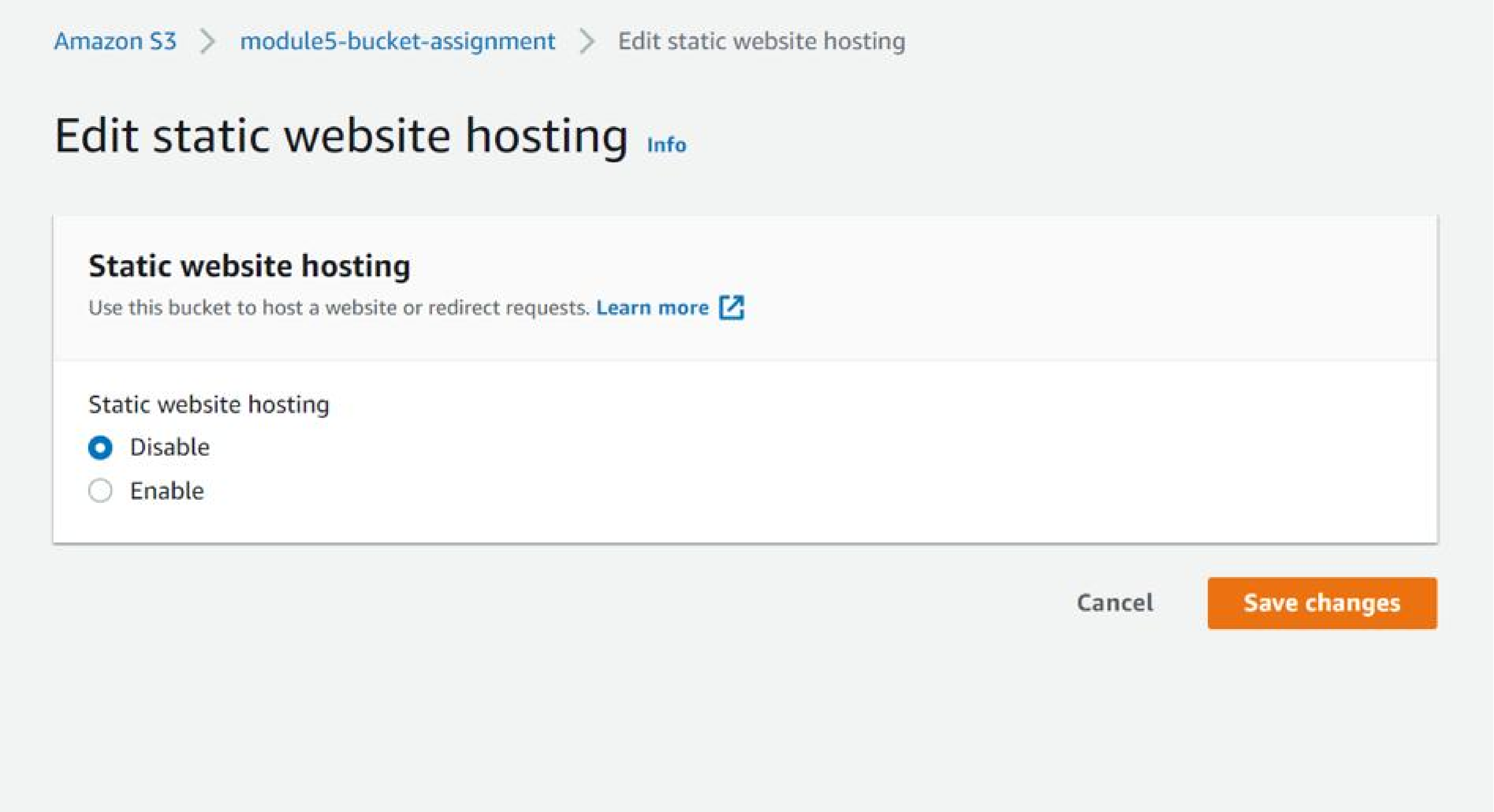
AWS Region: US East (N. Virginia) us-east-1

Amazon Resource Name (ARN): arn:aws:s3:::module5-bucket-assignment

Creation date: February 16, 2022, 15:00:34 (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



Amazon S3 > module5-bucket-assignment > Edit static website hosting

Edit static website hosting Info

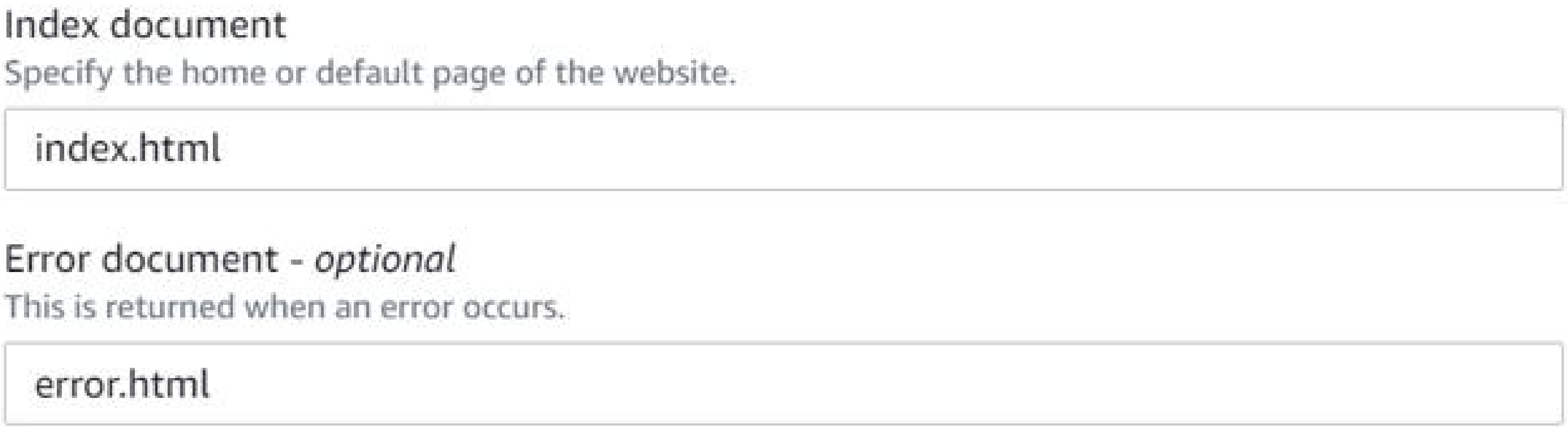
Static website hosting

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

Static website hosting

● Disable

○ Enable



Index document

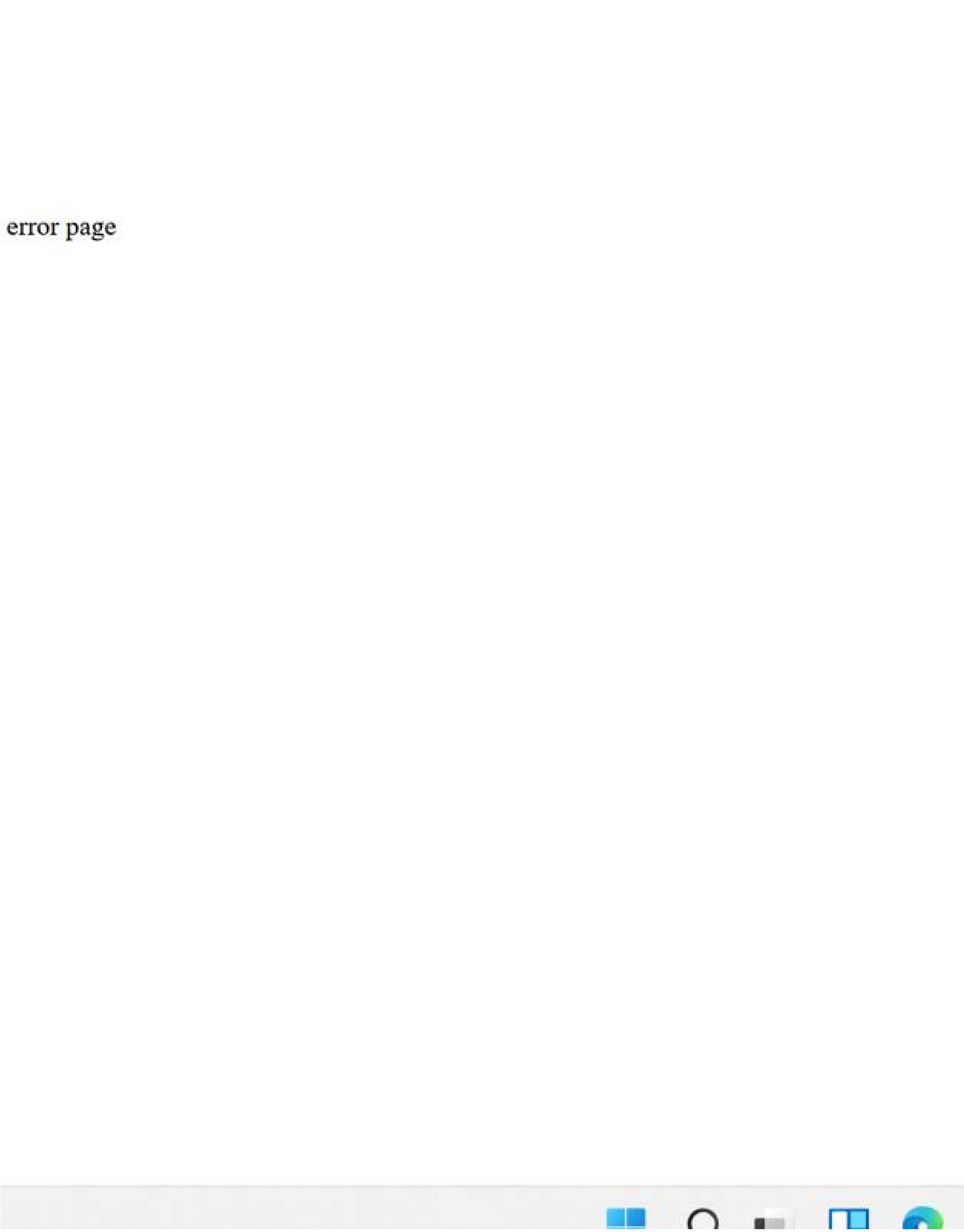
Specify the home or default page of the website.

index.html

Error document - *optional*

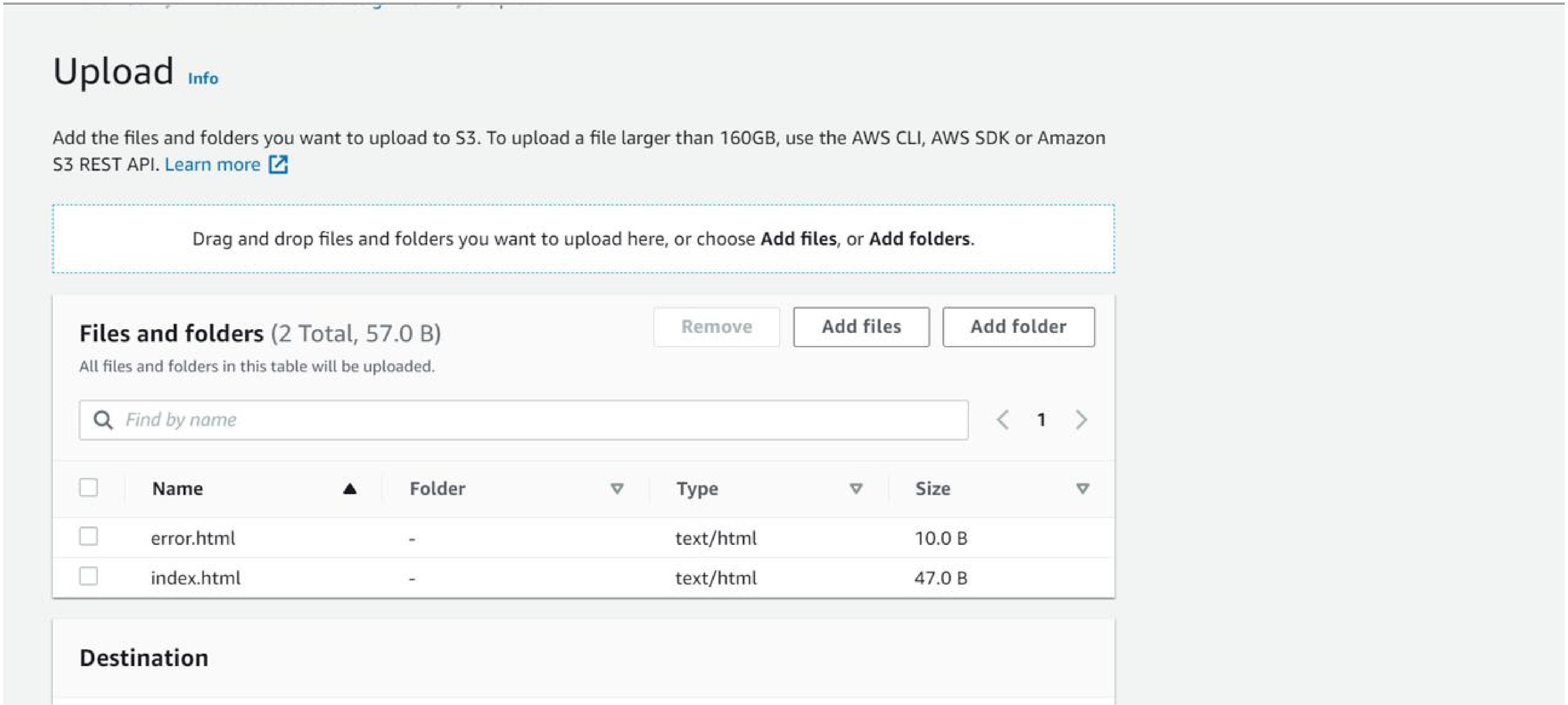
This is returned when an error occurs.

error.html



error page

Hi this is sample html file



Upload

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

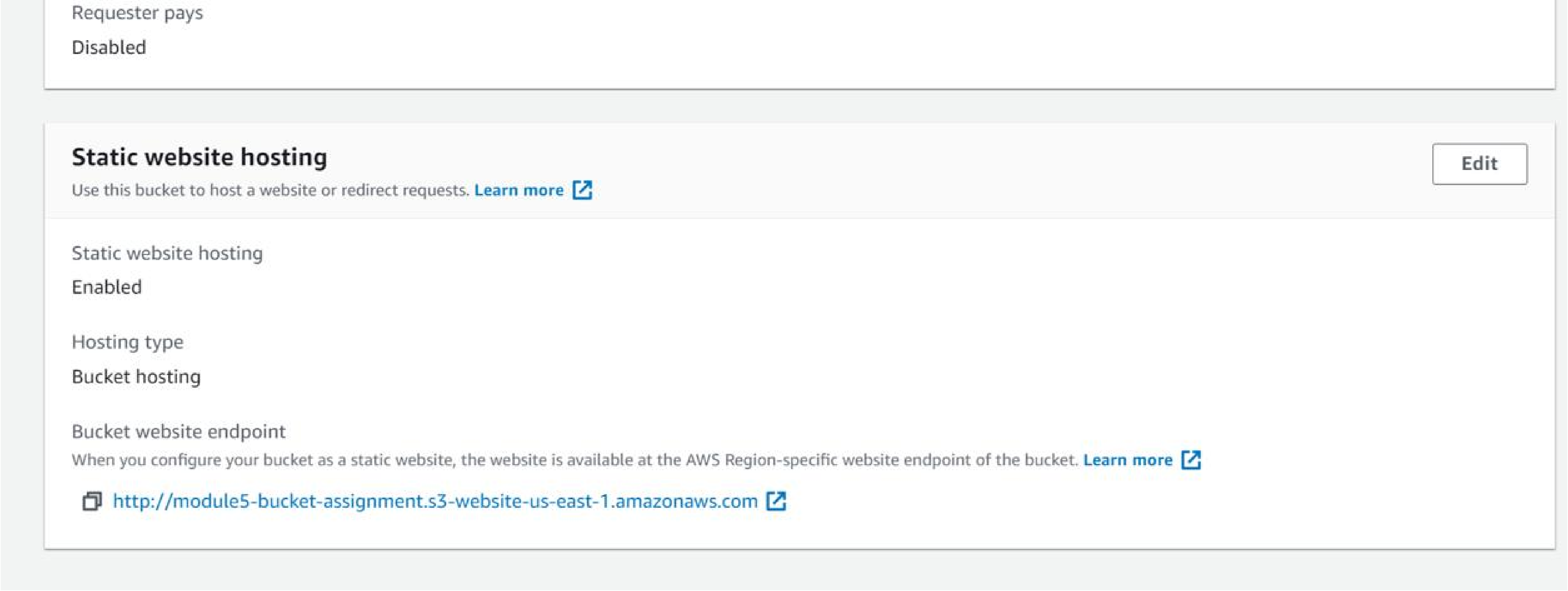
Drag and drop files and folders you want to upload here, or choose **Add files**, or **Add folders**.

Files and folders (2 Total, 57.0 B)

All files and folders in this table will be uploaded.

□	Name ▲	Folder ▽	Type ▽	Size ▽
□	error.html	-	text/html	10.0 B
□	index.html	-	text/html	47.0 B

Destination



Requester pays

Disabled

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

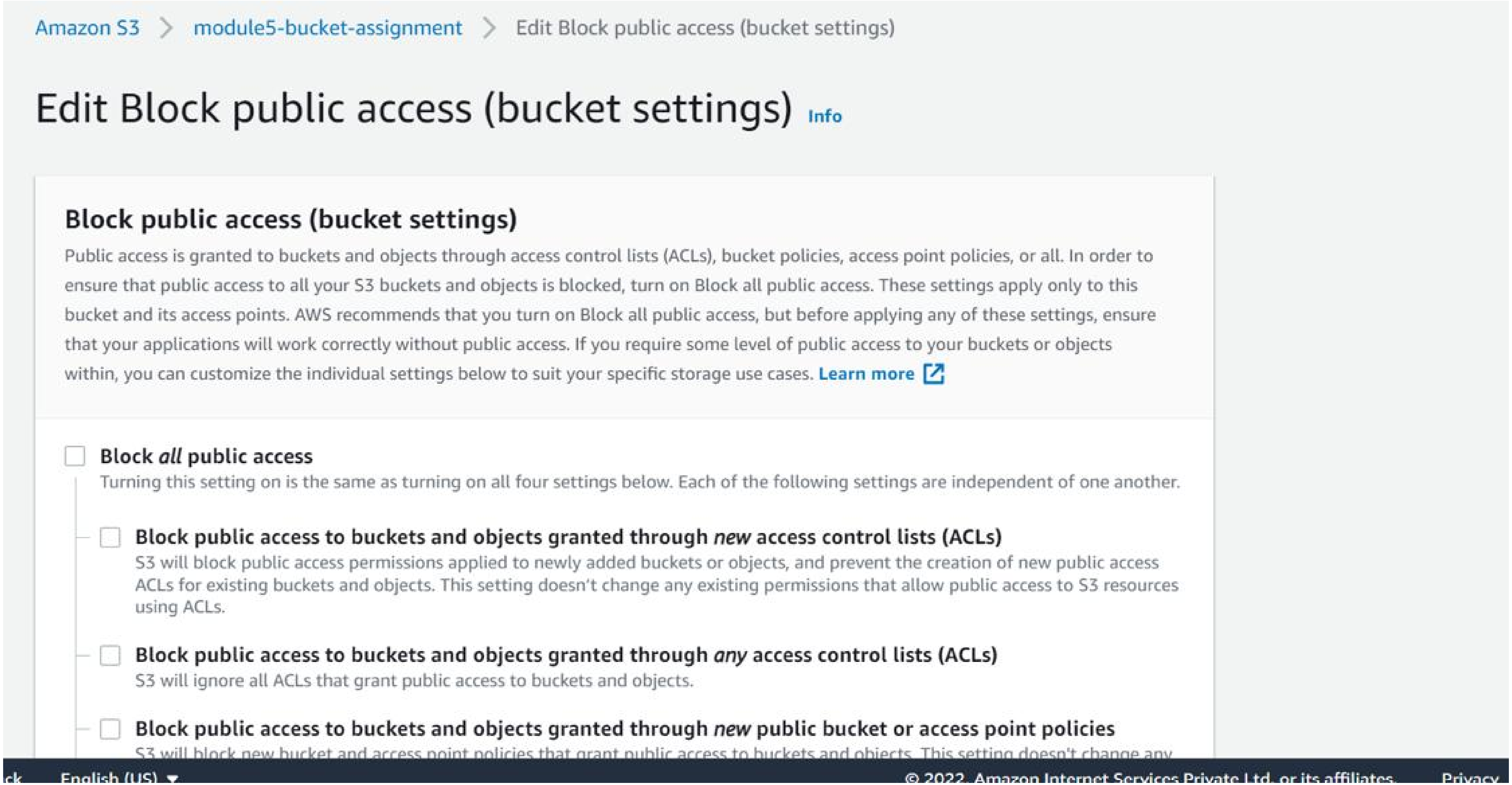
http://module5-bucket-assignment.s3-website-us-east-1.amazonaws.com

403 Forbidden

- Code: AccessDenied
- Message: Access Denied
- RequestId: 5R5RD6X0TVR9DV2J
- HostId: Z5O9gqBqMZjmRM6rnIeDguUU6O0+wr+uZI/9B7c+5/jJWsKStZsialygtukQg3kdR9AApECJFKA=

An Error Occurred While Attempting to Retrieve a Custom Error Document

- Code: AccessDenied
- Message: Access Denied



Amazon S3 > module5-bucket-assignment > Edit Block public access (bucket settings)

Edit Block public access (bucket settings) Info

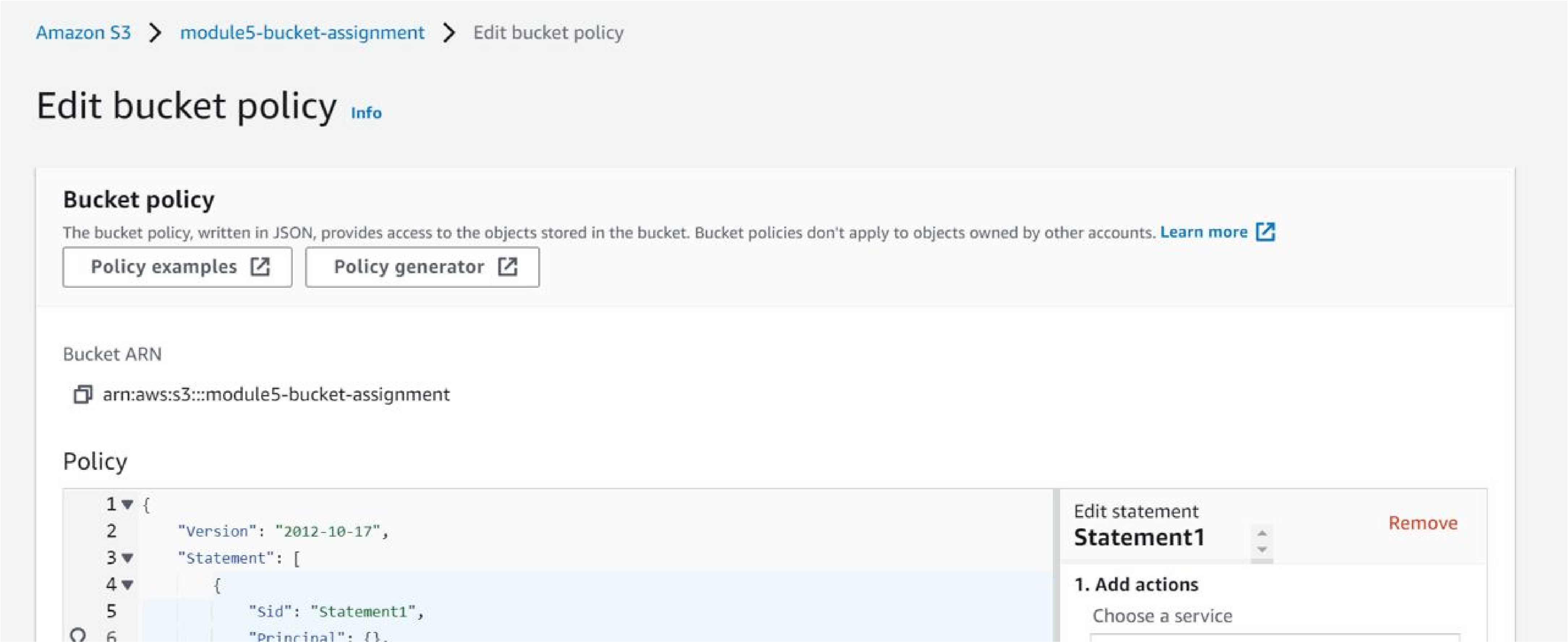
Block public access (bucket settings)

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

ck
English (US) ▼
© 2022, Amazon Internet Services Private Ltd. or its affiliates.
Privacy



Amazon S3 > module5-bucket-assignment > Edit bucket policy

Edit bucket policy

Info

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

Bucket ARN

arn:aws:s3:::module5-bucket-assignment

Policy

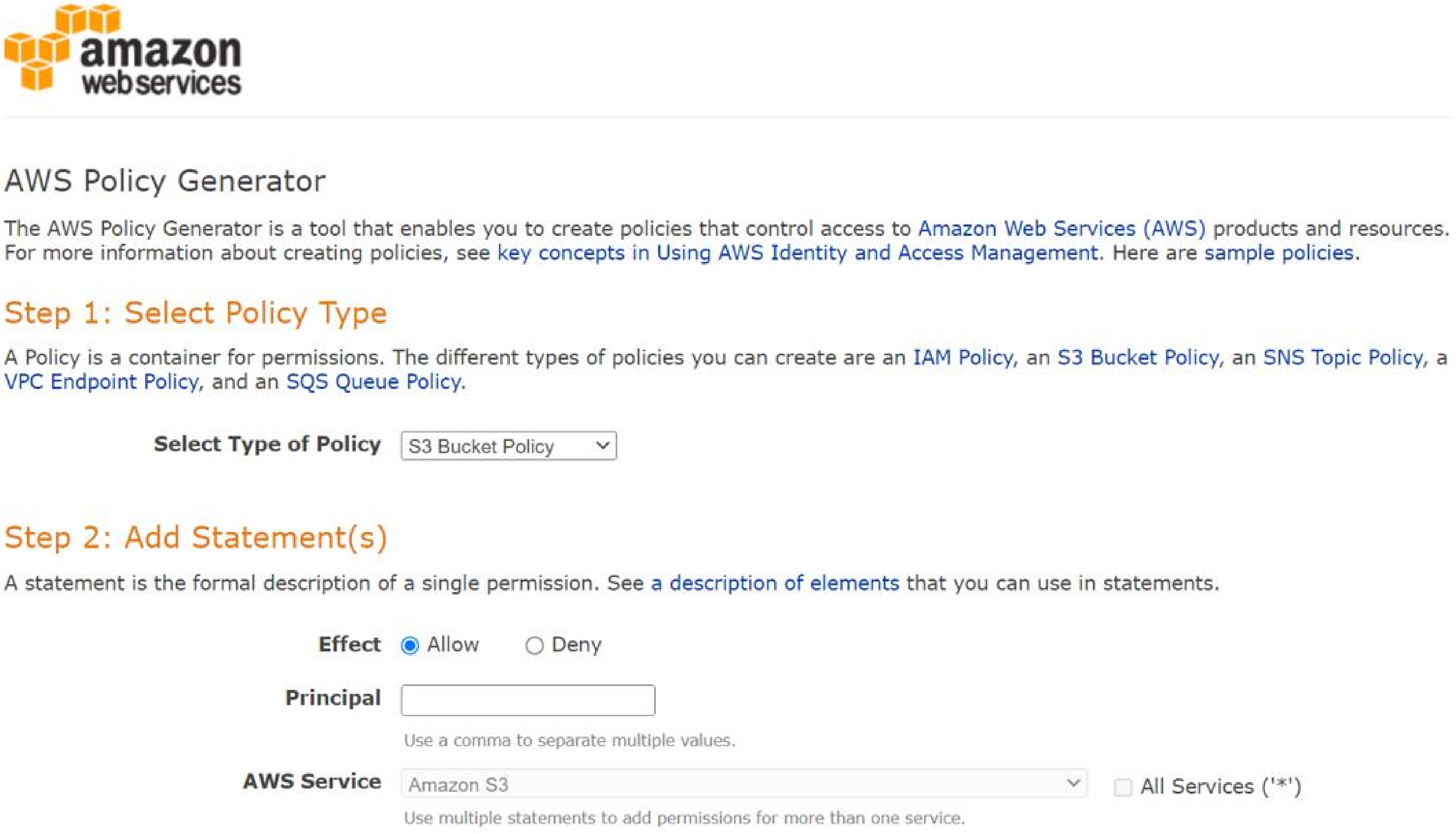
```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "Statement1",
            "Principal": {},
```

Edit statement

Statement1

1. Add actions

Choose a service



AWS Policy Generator

The AWS Policy Generator is a tool that enables you to create policies that control access to Amazon Web Services (AWS) products and resources. For more information about creating policies, see key concepts in Using AWS Identity and Access Management. Here are sample policies.

Step 1: Select Policy Type

A Policy is a container for permissions. The different types of policies you can create are an IAM Policy, an S3 Bucket Policy, an SNS Topic Policy, a VPC Endpoint Policy, and an SQS Queue Policy.

Select Type of Policy S3 Bucket Policy

Step 2: Add Statement(s)

A statement is the formal description of a single permission. See a description of elements that you can use in statements.

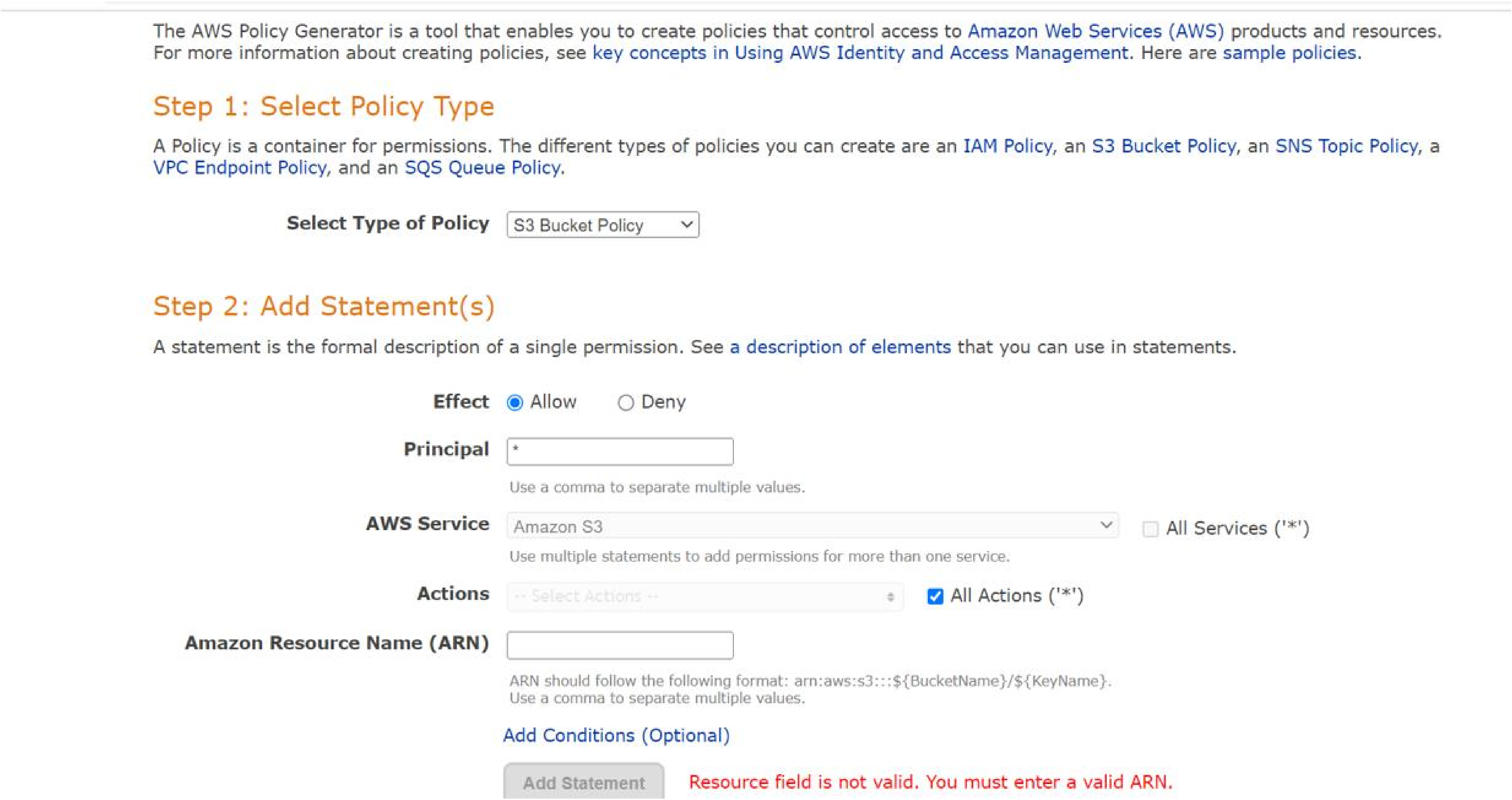
Effect ● Allow ○ Deny

Principal

Use a comma to separate multiple values.

AWS Service Amazon S3 □ All Services ('*')

Use multiple statements to add permissions for more than one service.



The AWS Policy Generator is a tool that enables you to create policies that control access to Amazon Web Services (AWS) products and resources. For more information about creating policies, see key concepts in Using AWS Identity and Access Management. Here are sample policies.

Step 1: Select Policy Type

A Policy is a container for permissions. The different types of policies you can create are an IAM Policy, an S3 Bucket Policy, an SNS Topic Policy, a VPC Endpoint Policy, and an SQS Queue Policy.

Select Type of Policy S3 Bucket Policy

Step 2: Add Statement(s)

A statement is the formal description of a single permission. See a description of elements that you can use in statements.

Effect ● Allow ○ Deny

Principal *

Use a comma to separate multiple values.

AWS Service Amazon S3 ☐ All Services ('*')

Use multiple statements to add permissions for more than one service.

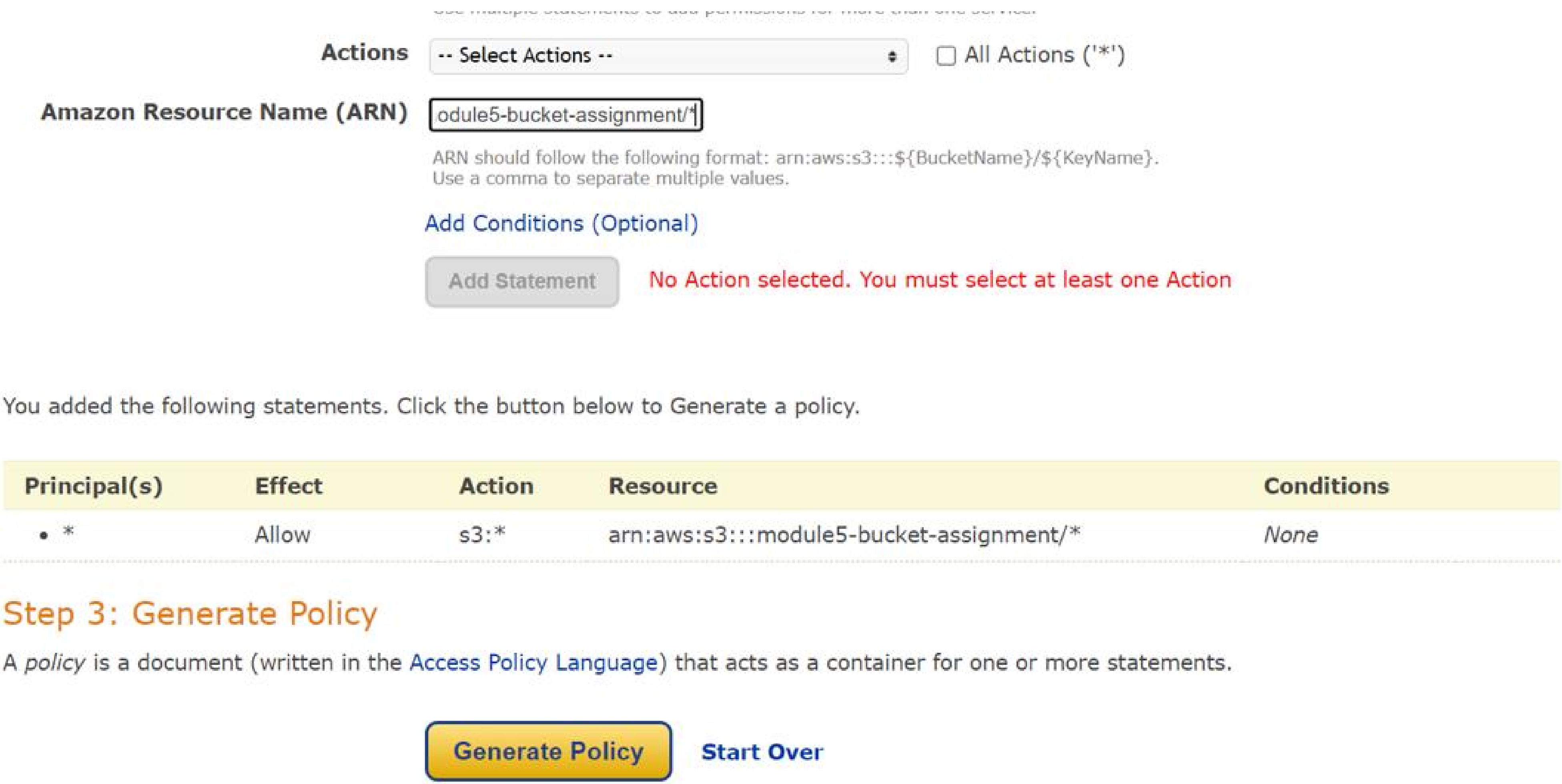
Actions -- Select Actions -- ☑ All Actions ('*')

Amazon Resource Name (ARN)

ARN should follow the following format: arn:aws:s3:::${BucketName}/${KeyName}.
Use a comma to separate multiple values.

Add Conditions (Optional)

Resource field is not valid. You must enter a valid ARN.



Use multiple statements to add permissions for more than one service.

Actions -- Select Actions -- □ All Actions ('*')

Amazon Resource Name (ARN) odule5-bucket-assignment/*

ARN should follow the following format: arn:aws:s3:::${BucketName}/${KeyName}.
Use a comma to separate multiple values.

Add Conditions (Optional)

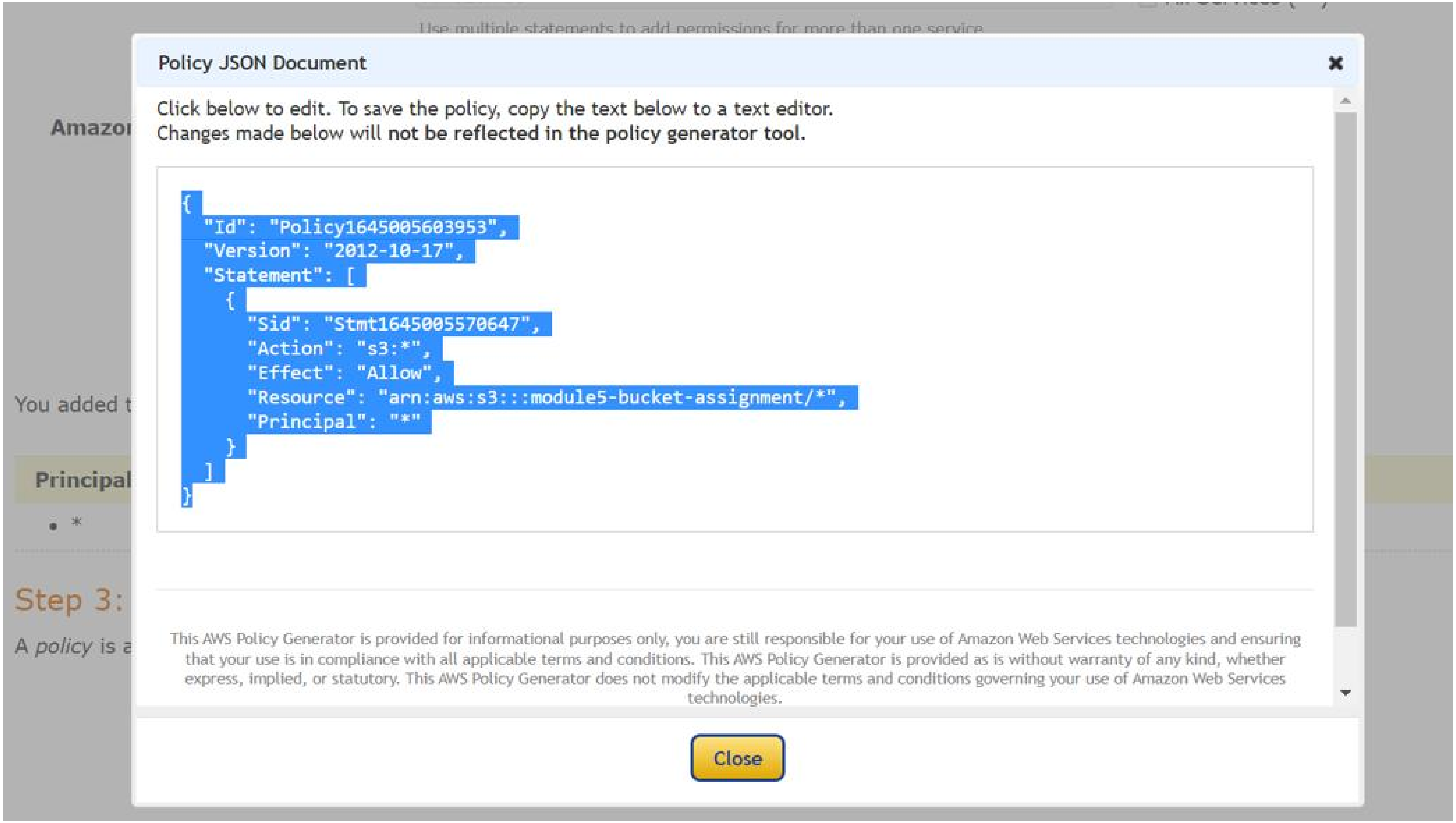
No Action selected. You must select at least one Action

You added the following statements. Click the button below to Generate a policy.

Principal(s)	Effect	Action	Resource	Conditions
• *	Allow	s3:*	arn:aws:s3:::module5-bucket-assignment/*	*None*

Step 3: Generate Policy

A *policy* is a document (written in the Access Policy Language) that acts as a container for one or more statements.



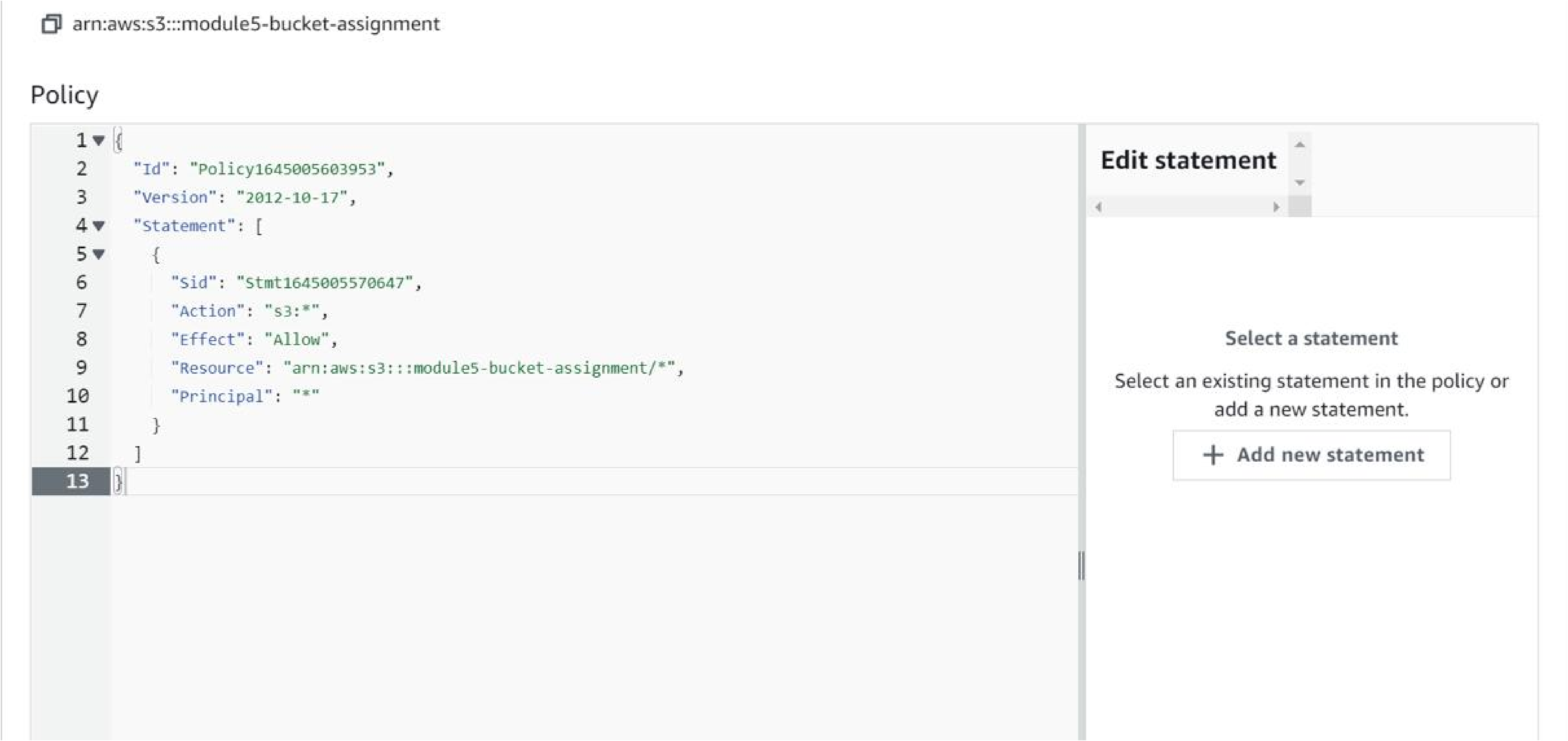
Use multiple statements to add permissions for more than one service.
Amazon
You added t
Principal
• *
Step 3:
A *policy* is a

Policy JSON Document

Click below to edit. To save the policy, copy the text below to a text editor.
Changes made below will **not be reflected in the policy generator tool.**

```
{
  "Id": "Policy1645005603953",
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "Stmt1645005570647",
      "Action": "s3:*",
      "Effect": "Allow",
      "Resource": "arn:aws:s3:::module5-bucket-assignment/*",
      "Principal": "*"
    }
  ]
}
```

This AWS Policy Generator is provided for informational purposes only, you are still responsible for your use of Amazon Web Services technologies and ensuring that your use is in compliance with all applicable terms and conditions. This AWS Policy Generator is provided as is without warranty of any kind, whether express, implied, or statutory. This AWS Policy Generator does not modify the applicable terms and conditions governing your use of Amazon Web Services technologies.

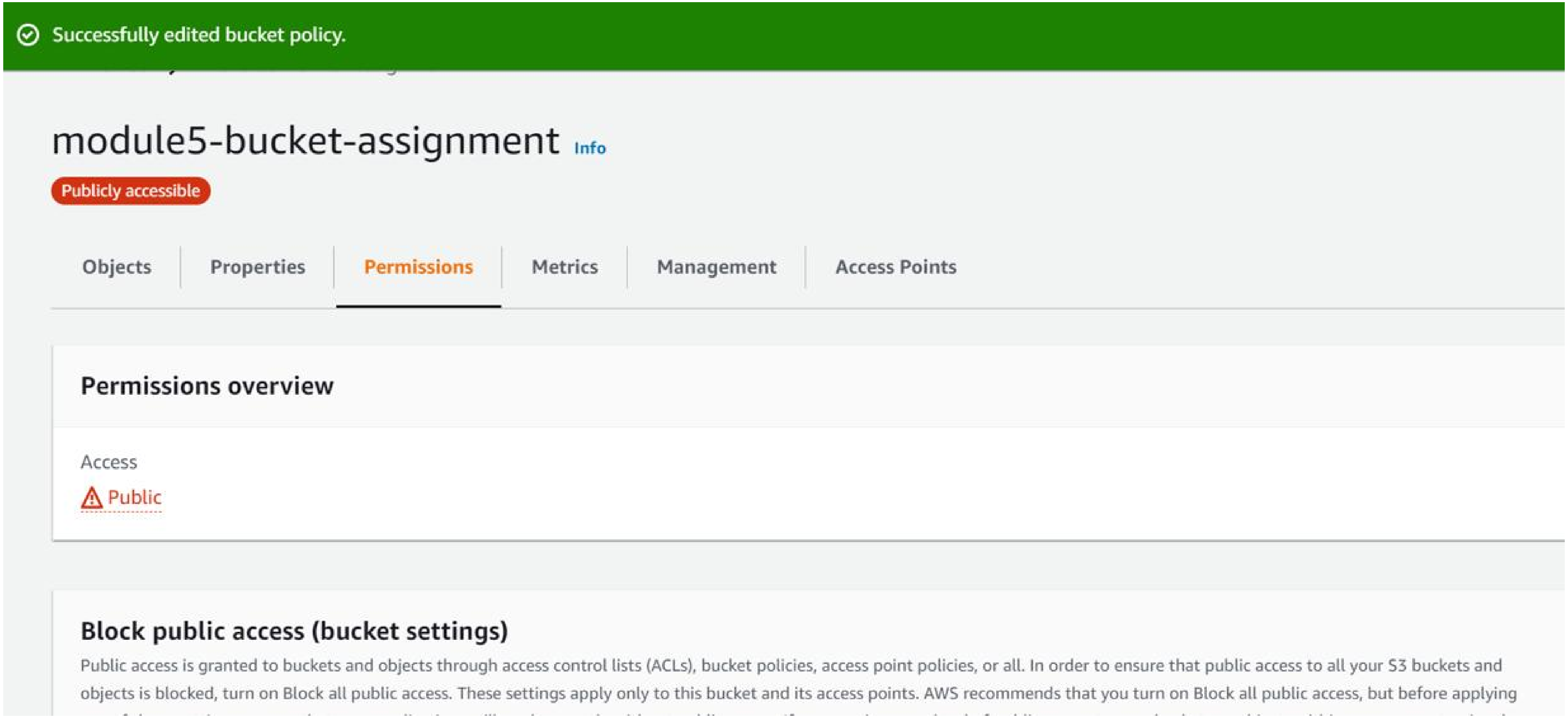


arn:aws:s3:::module5-bucket-assignment

Policy

```
{
  "Id": "Policy1645005603953",
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "Stmt1645005570647",
      "Action": "s3:*",
      "Effect": "Allow",
      "Resource": "arn:aws:s3:::module5-bucket-assignment/*",
      "Principal": "*"
    }
  ]
}
```

Edit statement
Select a statement
Select an existing statement in the policy or add a new statement.
+ Add new statement



Successfully edited bucket policy.

module5-bucket-assignment

Publicly accessible

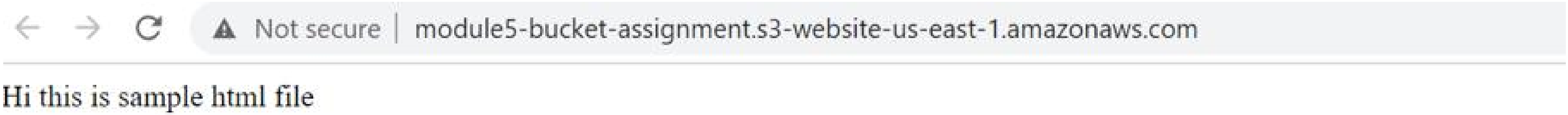
Permissions overview

Access

Public

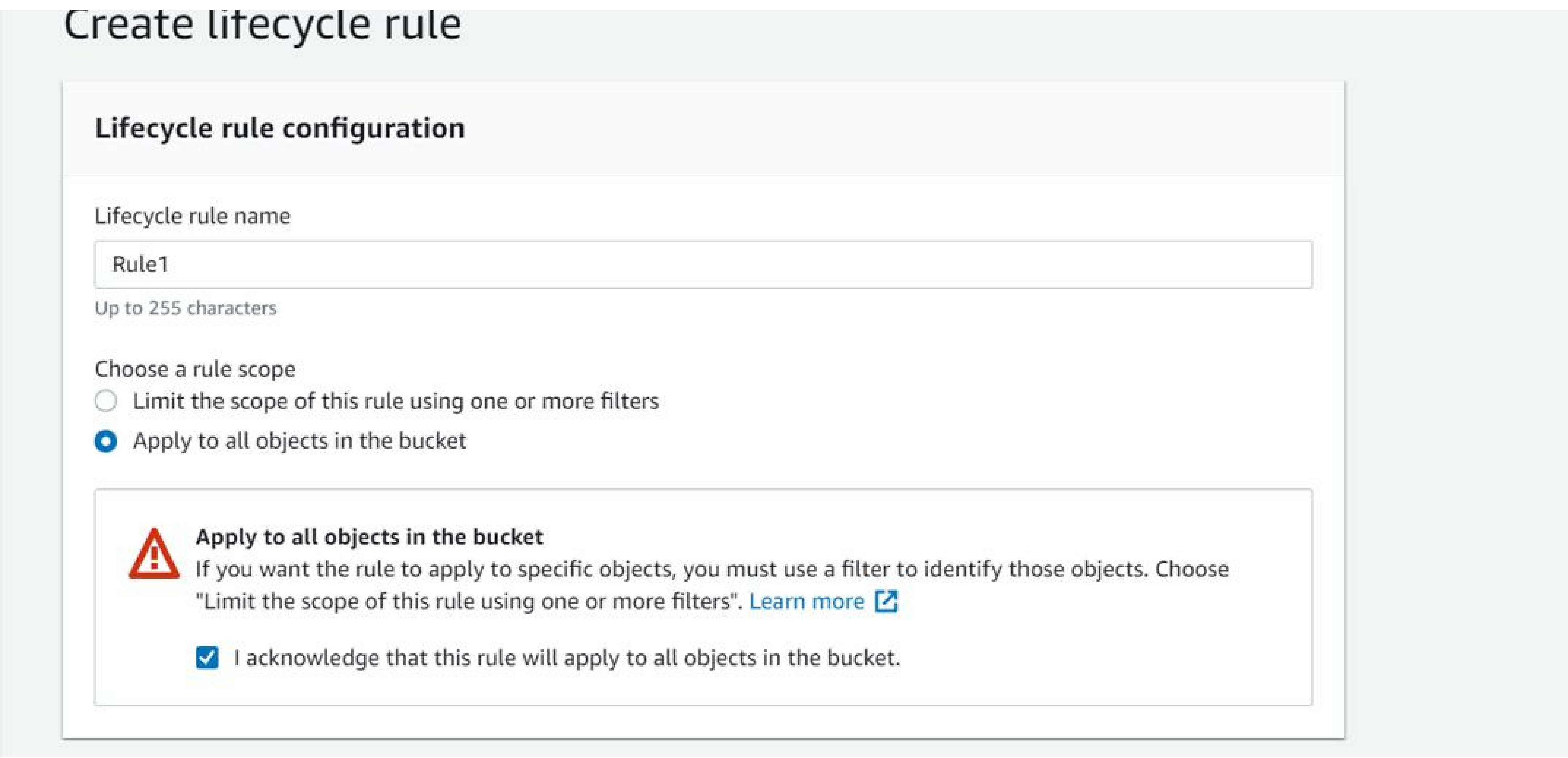
Block public access (bucket settings)

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



module5-bucket-assignment.s3-website-us-east-1.amazonaws.com

Hi this is sample html file



Create lifecycle rule

Lifecycle rule configuration

Lifecycle rule name

Rule1

Up to 255 characters

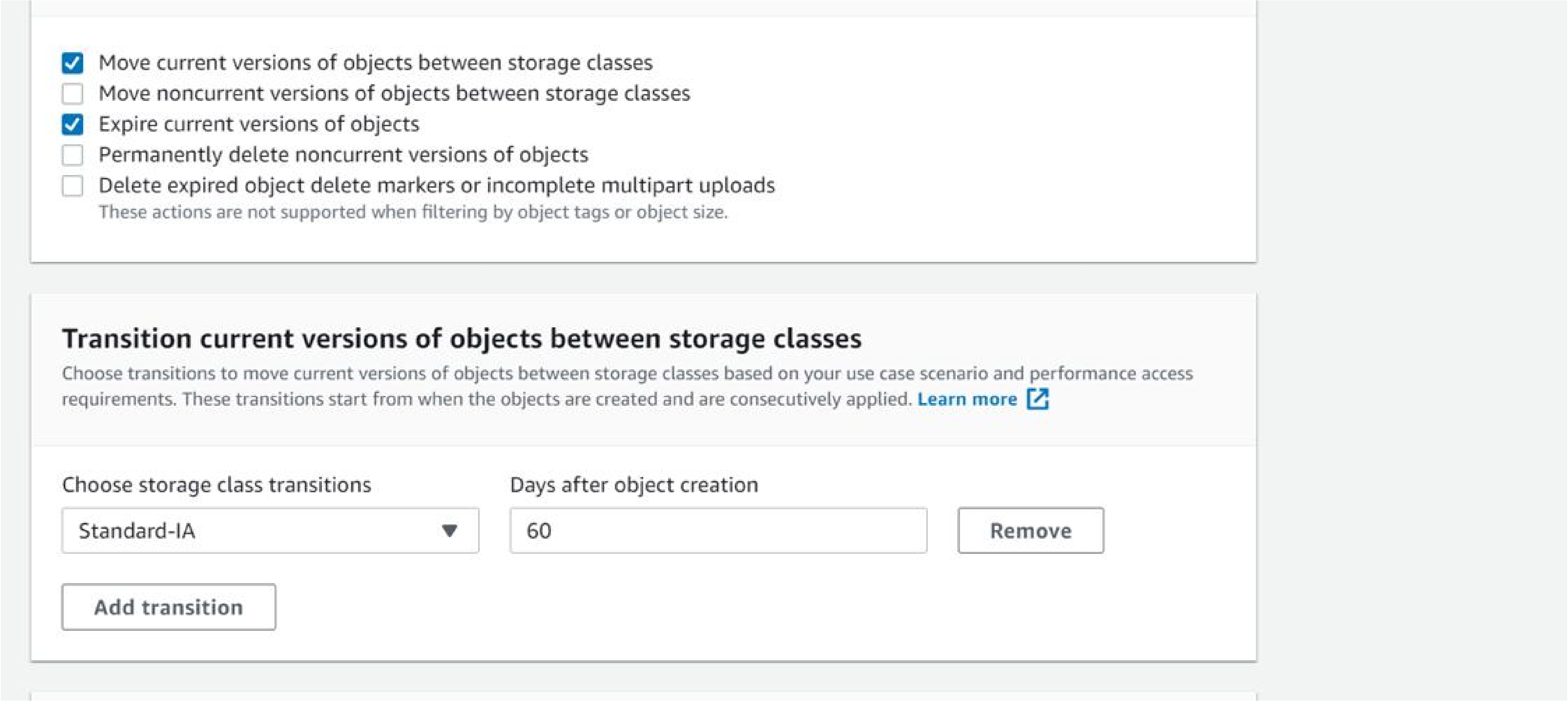
Choose a rule scope

○ 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

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



☑ Move current versions of objects between storage classes

□ Move noncurrent versions of objects between storage classes

☑ Expire current versions of objects

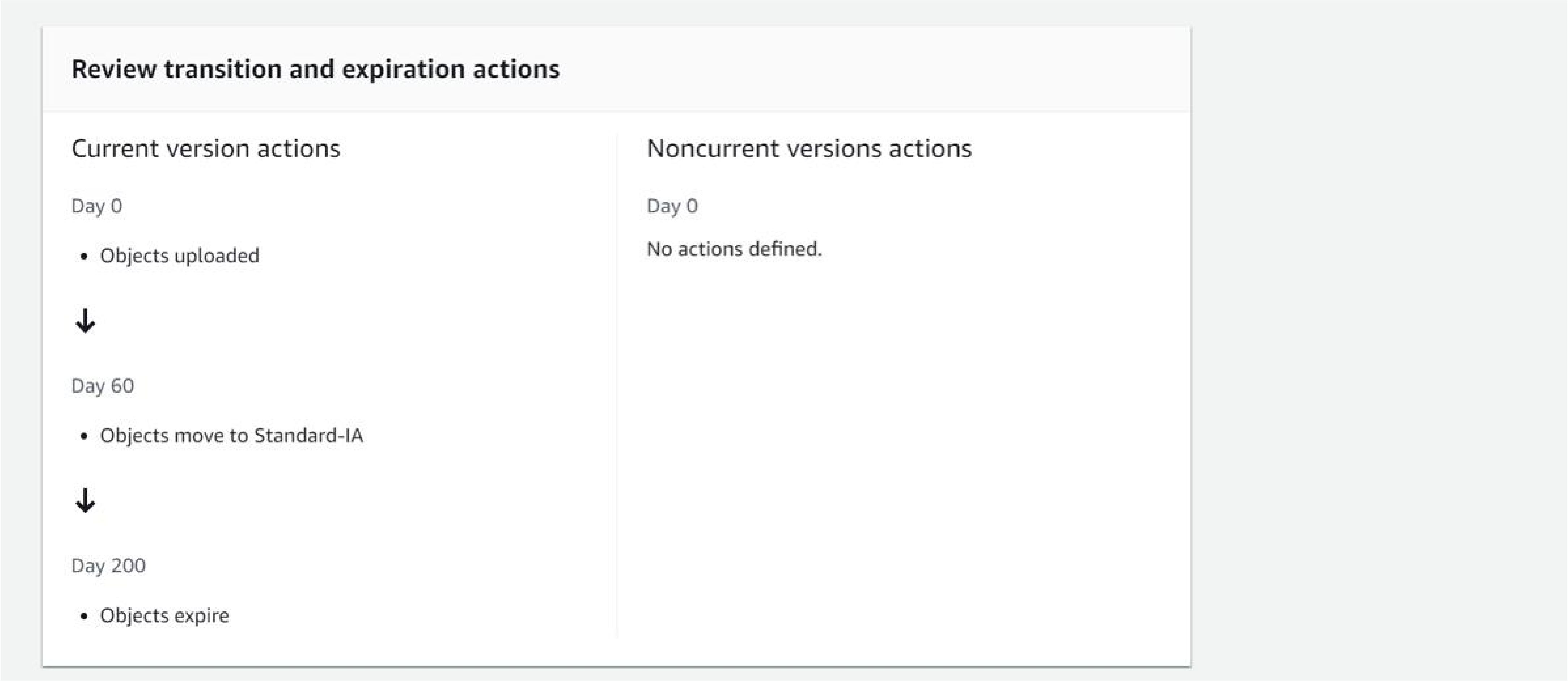
□ Permanently delete noncurrent versions of objects

□ 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



Review transition and expiration actions

Current version actions

Day 0

- Objects uploaded

↓

Day 60

- Objects move to Standard-IA

↓

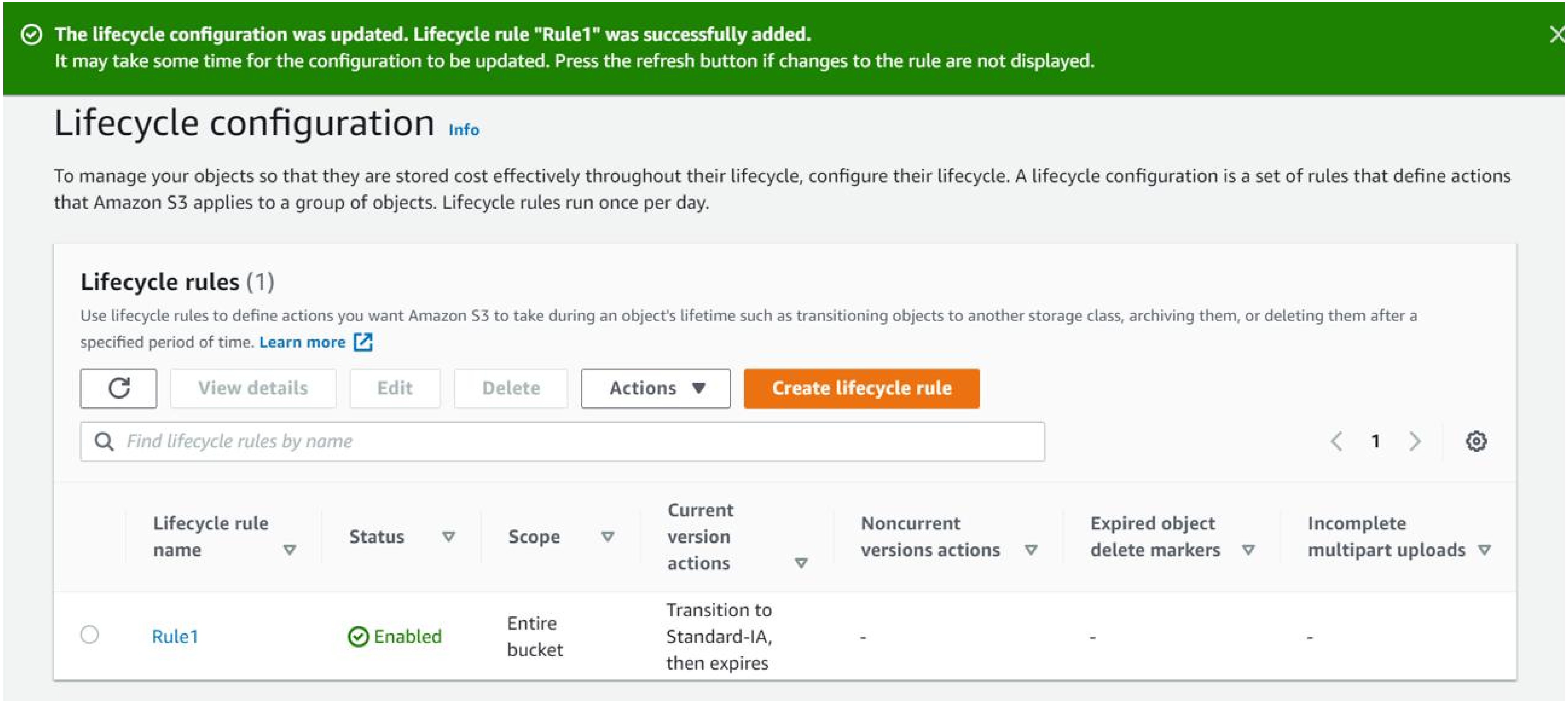
Day 200

- Objects expire

Noncurrent versions actions

Day 0

No actions defined.



The lifecycle configuration was updated. Lifecycle rule "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.

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
○	Rule1	Enabled	Entire bucket	Transition to Standard-IA, then expires	-	-	-