Task-3:

Create a Storage account in any cloud AWS/Azure and try securing it to protect your data.

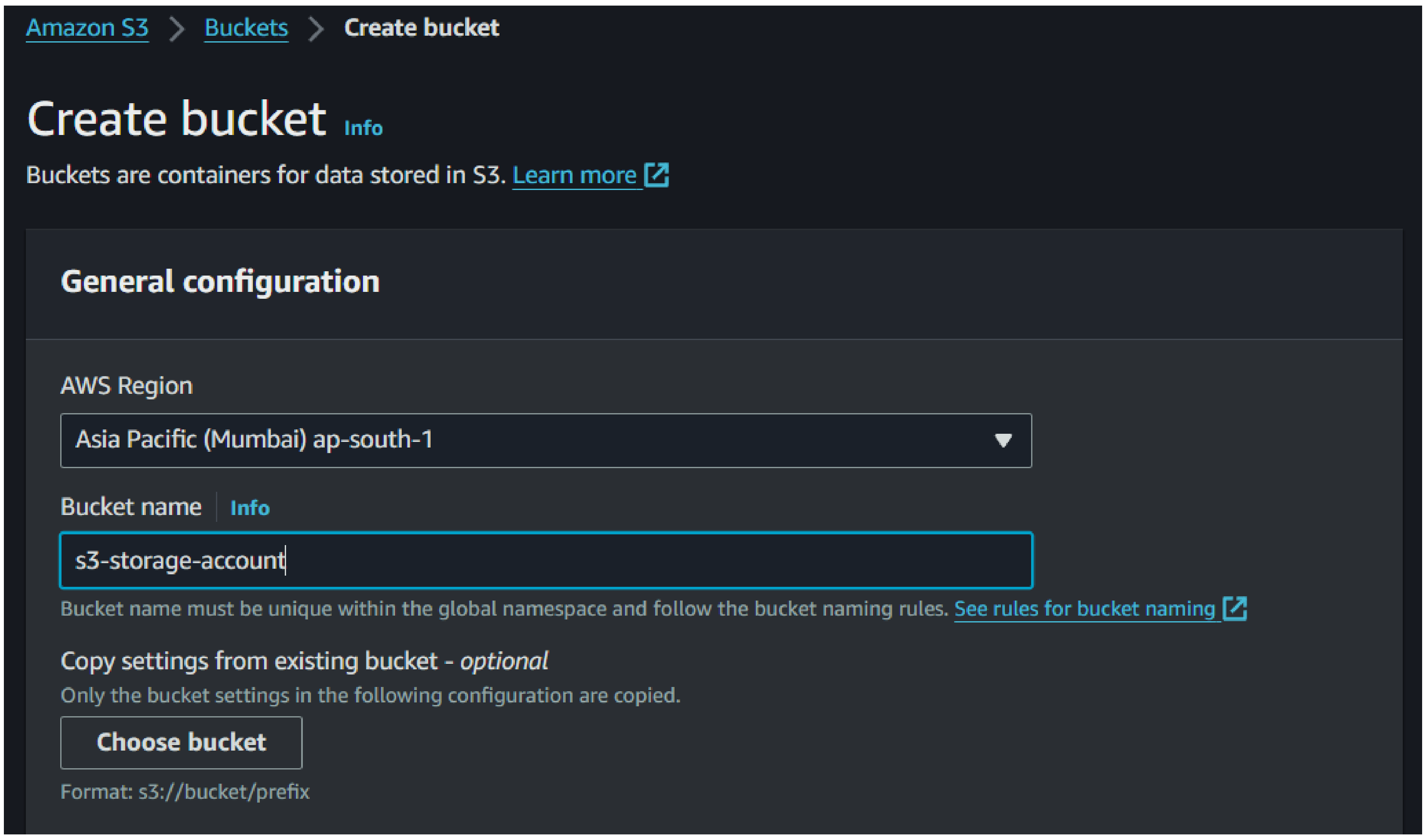
Here I am using AWS cloud platform

Now, I am creating s3 bucket

Go to AWS console, go to s3 service

Region: ap-south-1

Bucket name: s3-storage-account



Create bucket Info

Buckets are containers for data stored in S3. Learn more

General configuration

AWS Region

Asia Pacific (Mumbai) ap-south-1

Bucket name Info

s3-storage-account

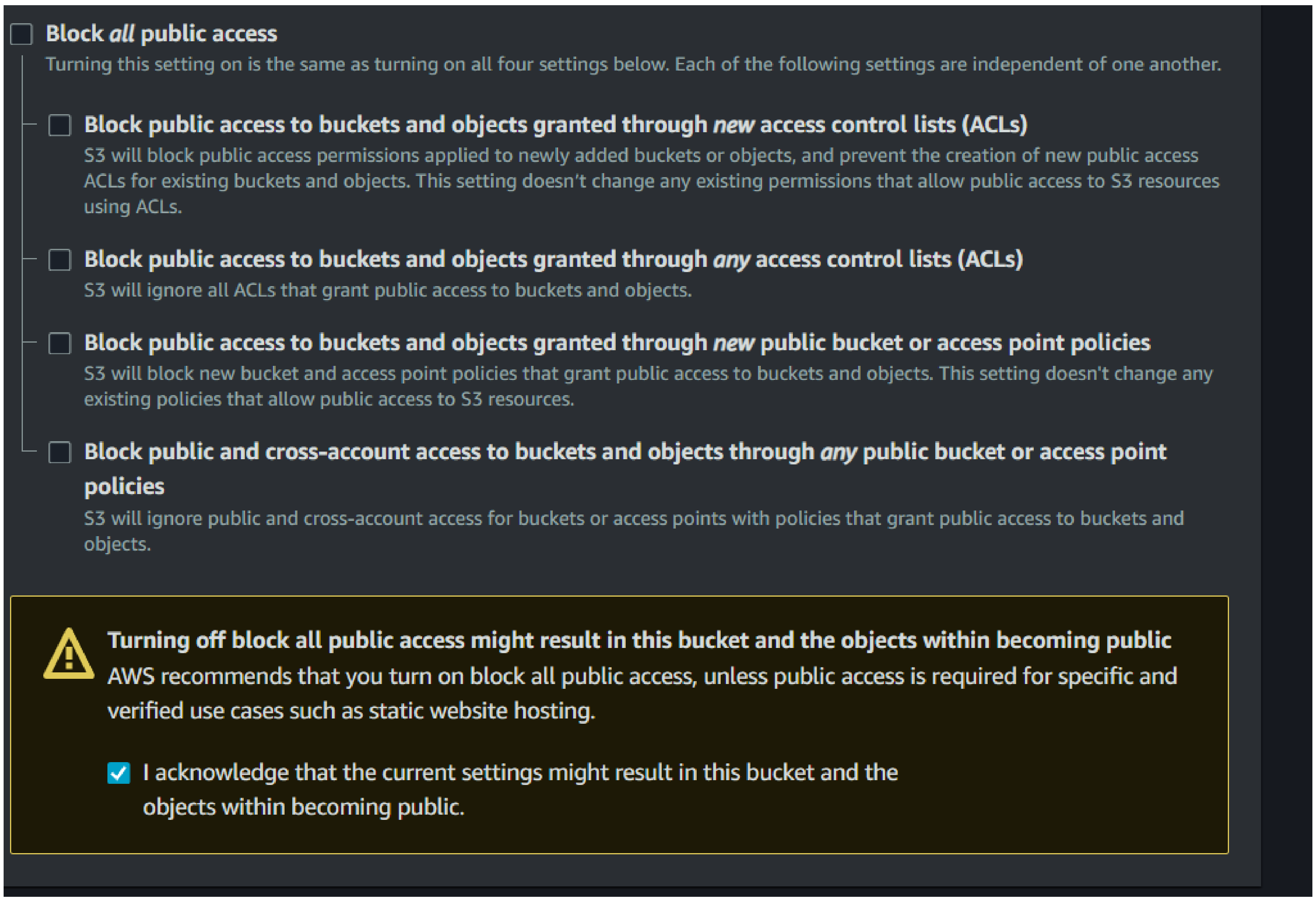
Bucket name must be unique within the global namespace and follow the bucket naming rules. See rules for bucket naming

Copy settings from existing bucket - *optional*

Only the bucket settings in the following configuration are copied.

Format: s3://bucket/prefix

Enable public access



□ **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.

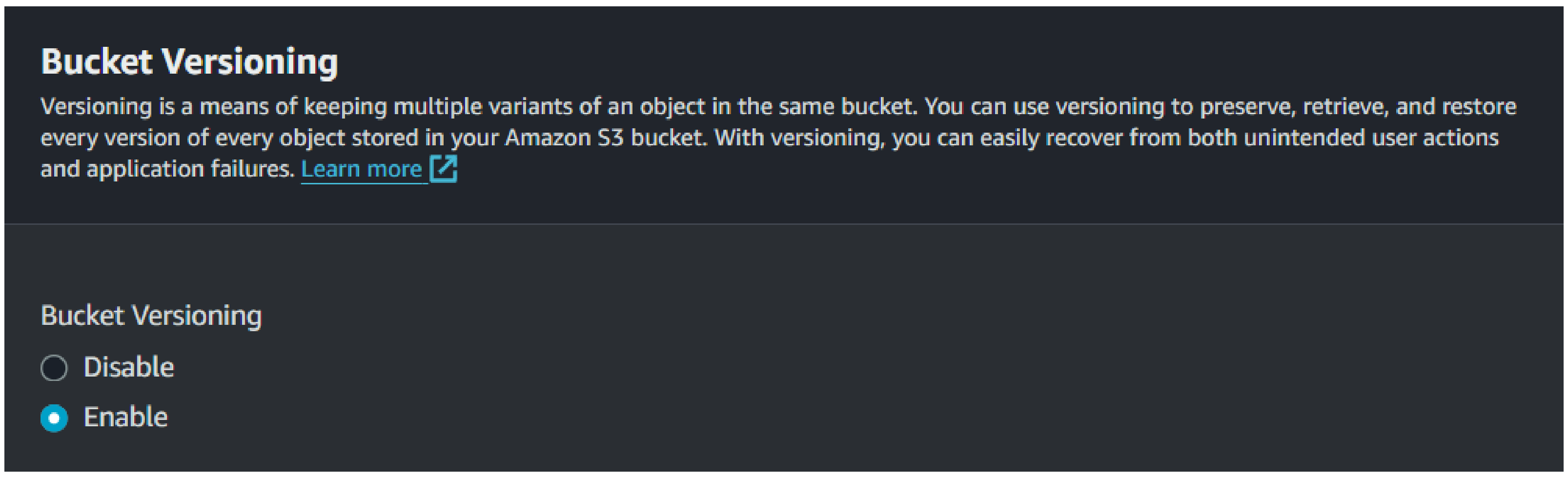
⚠ **Turning off block all public access might result in this bucket and the objects within becoming public**

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 (related GitHub version)

Easily recover our data and applications failures, restore and retrieve, every version and objects stored in this s3 buckets



Bucket Versioning

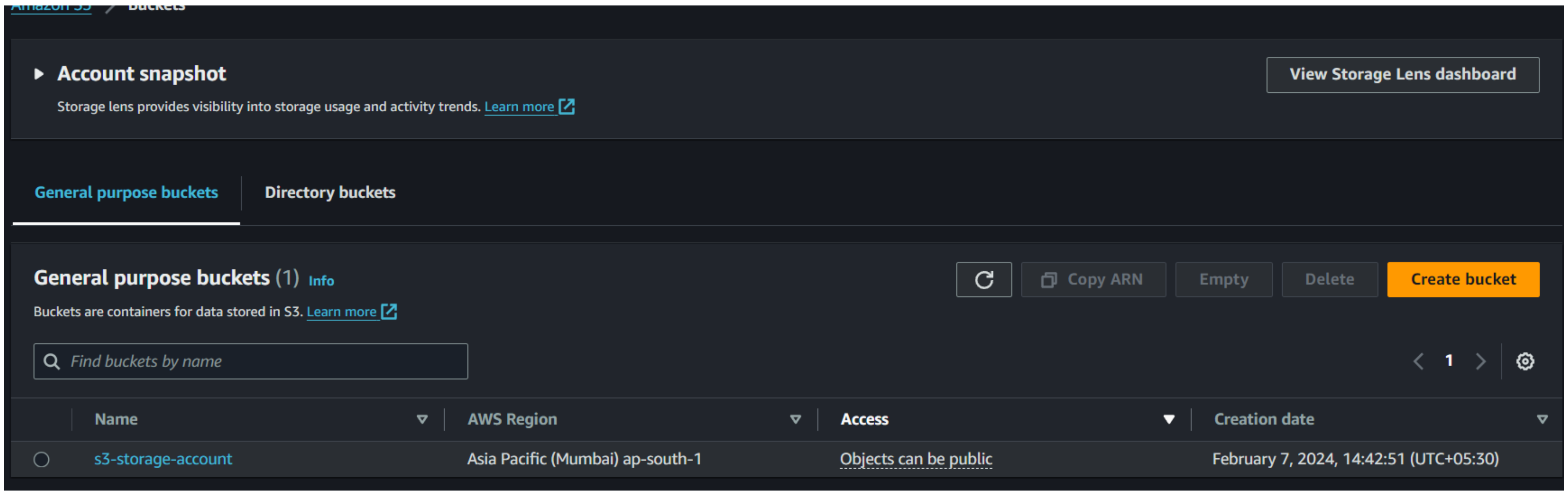
Versioning is a means of keeping multiple variants of an object in the same bucket. You can use versioning to preserve, retrieve, and restore every version of every object stored in your Amazon S3 bucket. With versioning, you can easily recover from both unintended user actions and application failures. Learn more

Bucket Versioning

○ Disable

● Enable

Created my s3 bucket



Amazon S3 > Buckets

▸ Account snapshot

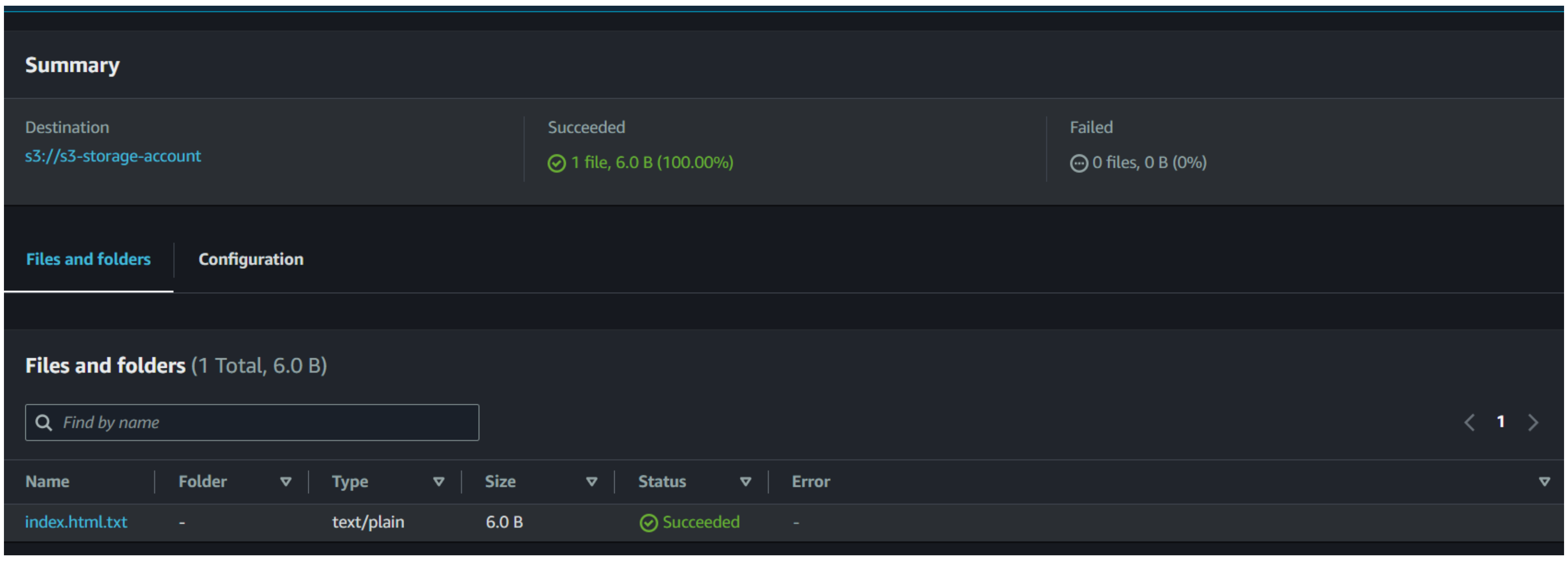
Storage lens provides visibility into storage usage and activity trends. Learn more

General purpose buckets (1) Info

Buckets are containers for data stored in S3. Learn more

	Name	AWS Region	Access	Creation date
○	s3-storage-account	Asia Pacific (Mumbai) ap-south-1	Objects can be public	February 7, 2024, 14:42:51 (UTC+05:30)

I am upload one data file within the s3 bucket



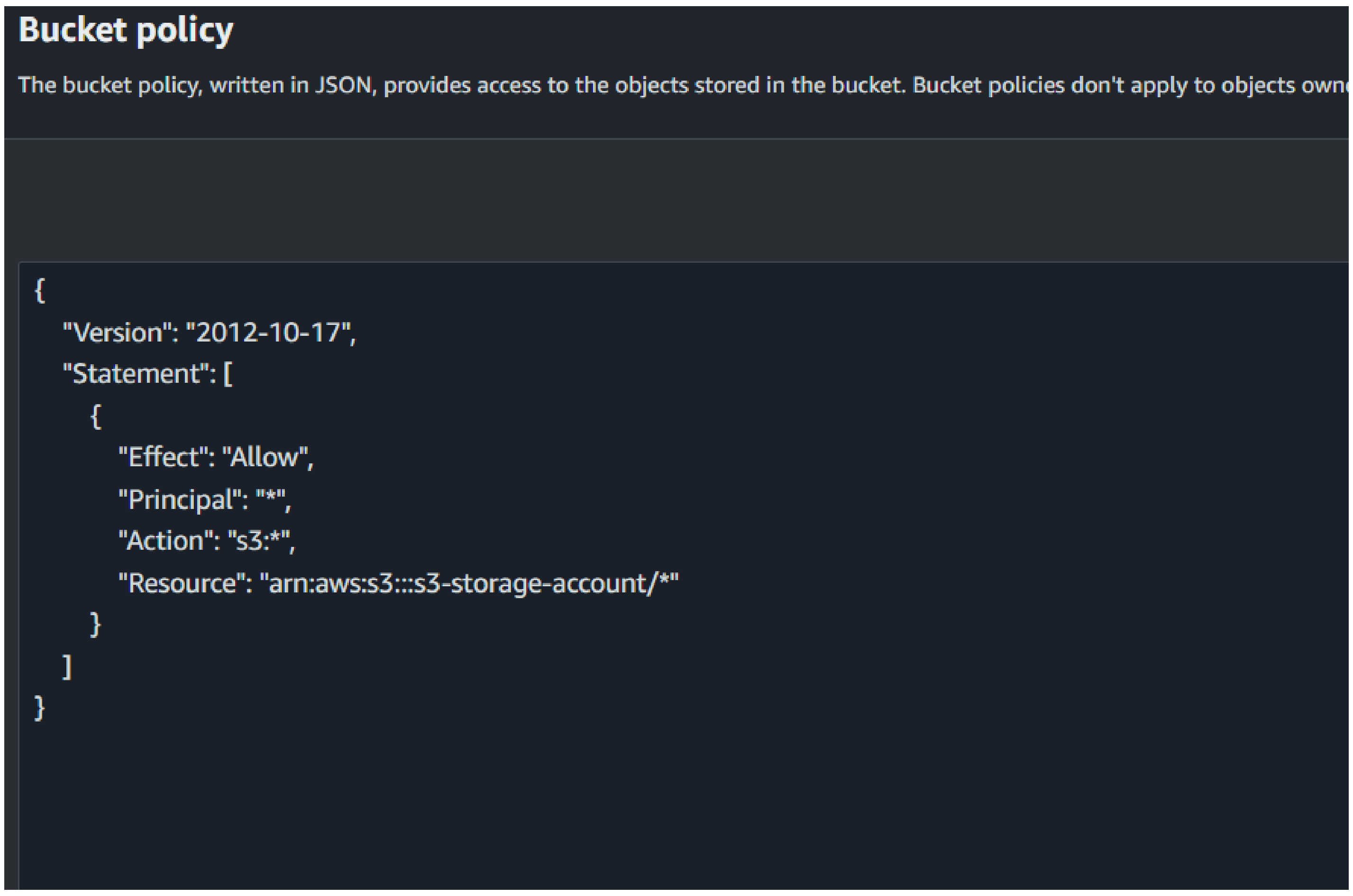
Summary

Destination	Succeeded	Failed
s3://s3-storage-account	✓ 1 file, 6.0 B (100.00%)	0 files, 0 B (0%)

Files and folders (1 Total, 6.0 B)

Name	Folder	Type	Size	Status	Error
index.html.txt	-	text/plain	6.0 B	✓ Succeeded	-

Create bucket policy



Bucket policy

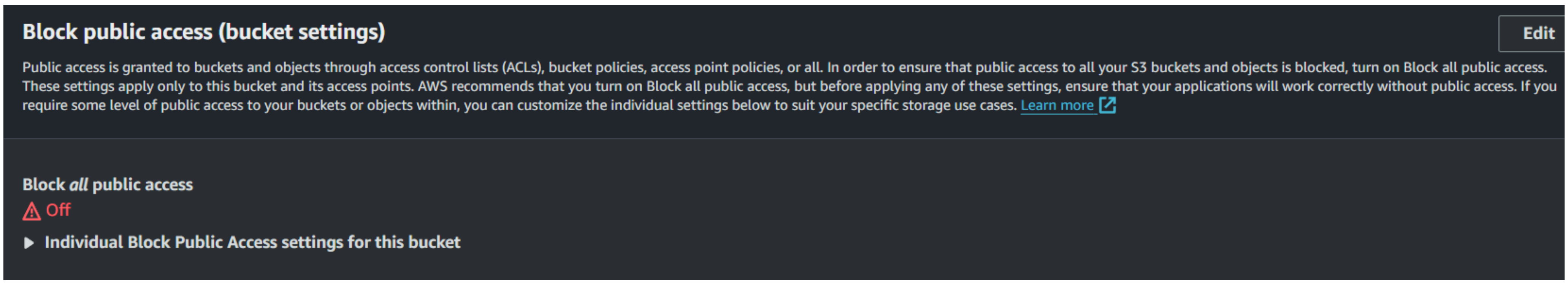
The bucket policy, written in JSON, provides access to the objects stored in the bucket. Bucket policies don't apply to objects own

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": "*",
      "Action": "s3:*",
      "Resource": "arn:aws:s3:::s3-storage-account/*"
    }
  ]
}
```

This my bucket object URL

https://s3-storage-account.s3.ap-south-1.amazonaws.com/index.html.txt

My file data



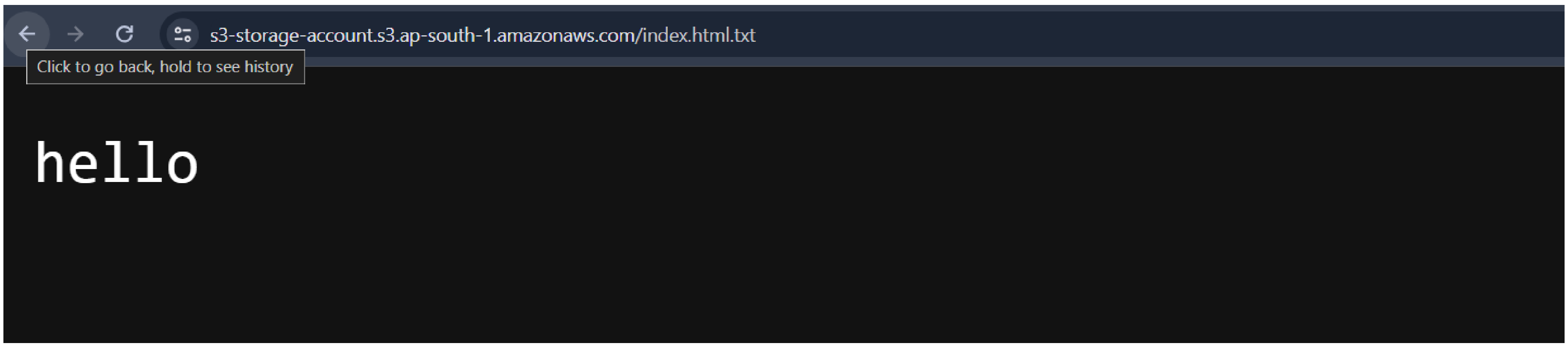
Block public access (bucket settings)

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

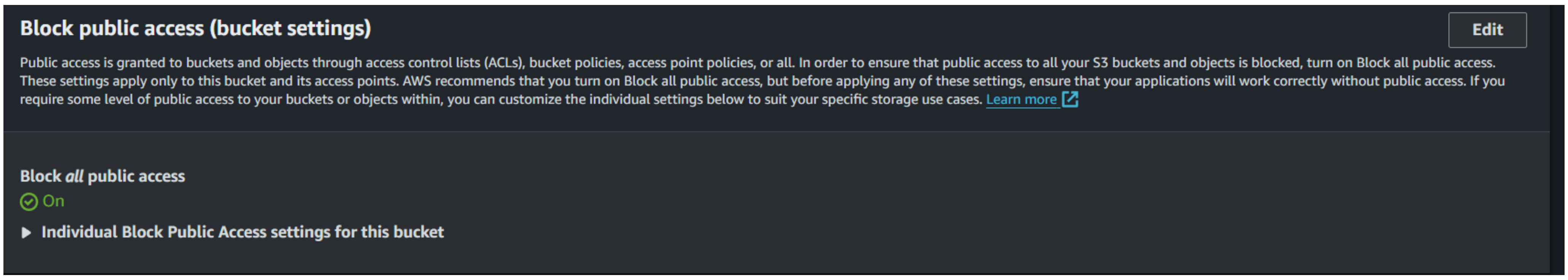
▶ Individual Block Public Access settings for this bucket



s3-storage-account.s3.ap-south-1.amazonaws.com/index.html.txt
Click to go back, hold to see history

```
hello
```

Block public access



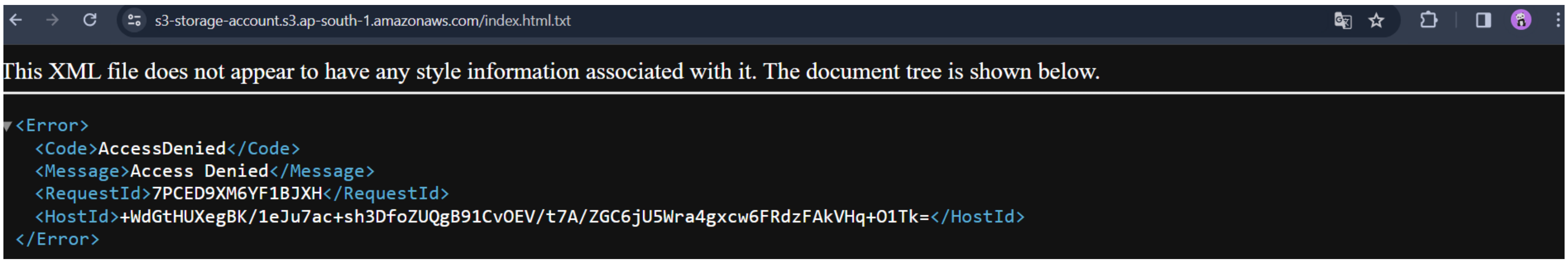
Block public access (bucket settings)

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

✓ On

▶ Individual Block Public Access settings for this bucket



This XML file does not appear to have any style information associated with it. The document tree is shown below.

```
▼<Error>
   <Code>AccessDenied</Code>
   <Message>Access Denied</Message>
   <RequestId>7PCED9XM6YF1BJXH</RequestId>
   <HostId>+WdGtHUXegBK/1eJu7ac+sh3DfoZUQgB91CvOEV/t7A/ZGC6jU5Wra4gxcw6FRdzFAkVHq+O1Tk=</HostId>
 </Error>
```