(AWS) - PART III

accendnetworks

A Beginner's Guide to AMAZON WEB SERVICES

Introduction to Data Management, Storage, Compute and Serverless

BY: **PAULA WONG**, CEO AND FOUNDER, CEH-MASTER,
CCIE SECURITY AND SWITCHING, C-7 #1086962
AWS CERTIFIED CLOUD PRACTITIONER

Data Management and Storage

Compute and Serverless

Secure File Uploads and Downloads in S3 Using Presigned URLs

Amazon Simple Storage Service (S3) is a highly scalable object storage service used for storing and retrieving large amounts of data. While S3 provides a straightforward way to manage files, ensuring secure access to these files is crucial. One effective method to securely upload and download files from S3 is by using presigned URLs. This article delves into what presigned URLs are, how they work, and a hands-on demo.

S3 Presigned URL

Presigned URLs are URLs that provide temporary access to objects in S3 without requiring AWS credentials directly from the user. When you create a presigned URL, you essentially generate a URL that includes a signature, allowing anyone with the URL to perform specific actions (like upload or download) on the specified S3 object within a limited time frame.

When you create an S3 bucket, it is private by default, and it is up to you to change this setting based on your needs. If you want a user to upload or download files in a private bucket without making the bucket public or requiring AWS credentials or IAM permissions, you can create a presigned URL.

Presigned URLs work even if the bucket is public, but the main purpose of presigned URLs is to help you keep objects private while allowing limited and controlled access when necessary.

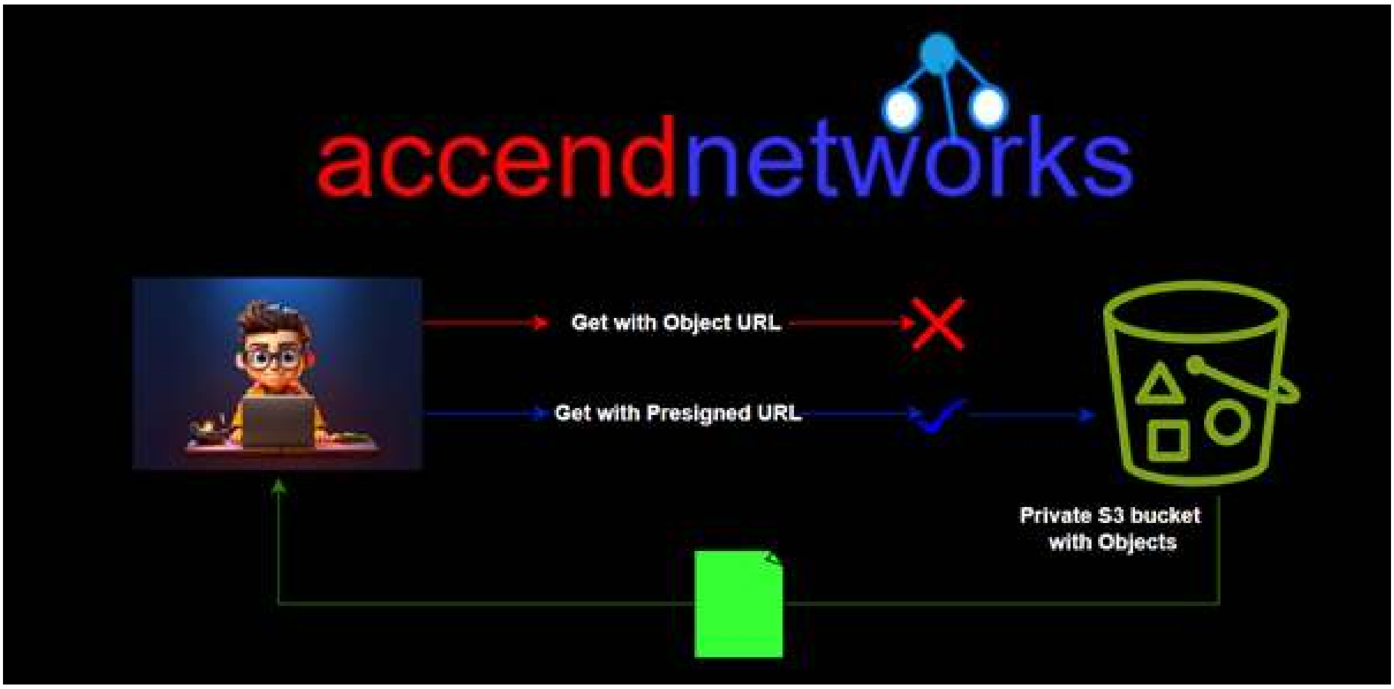
Requirements for Generating Presigned URLs

A presigned URL must be generated by an AWS user or an AWS application that has access to the bucket and the object in the bucket at the time of creation. When a user makes an HTTP call with the presigned URL, AWS processes the request as if it was performed by the entity that generated the presigned URL.

Usage and Expiration

Presigned URLs can be shared with temporarily authorized users to allow them to download or upload objects. They can only be used for the method specified when generating the URL. For example, a GET-presigned URL cannot be used for a PUT operation.

There is no default limit on the number of times a presigned URL can be used until it expires.



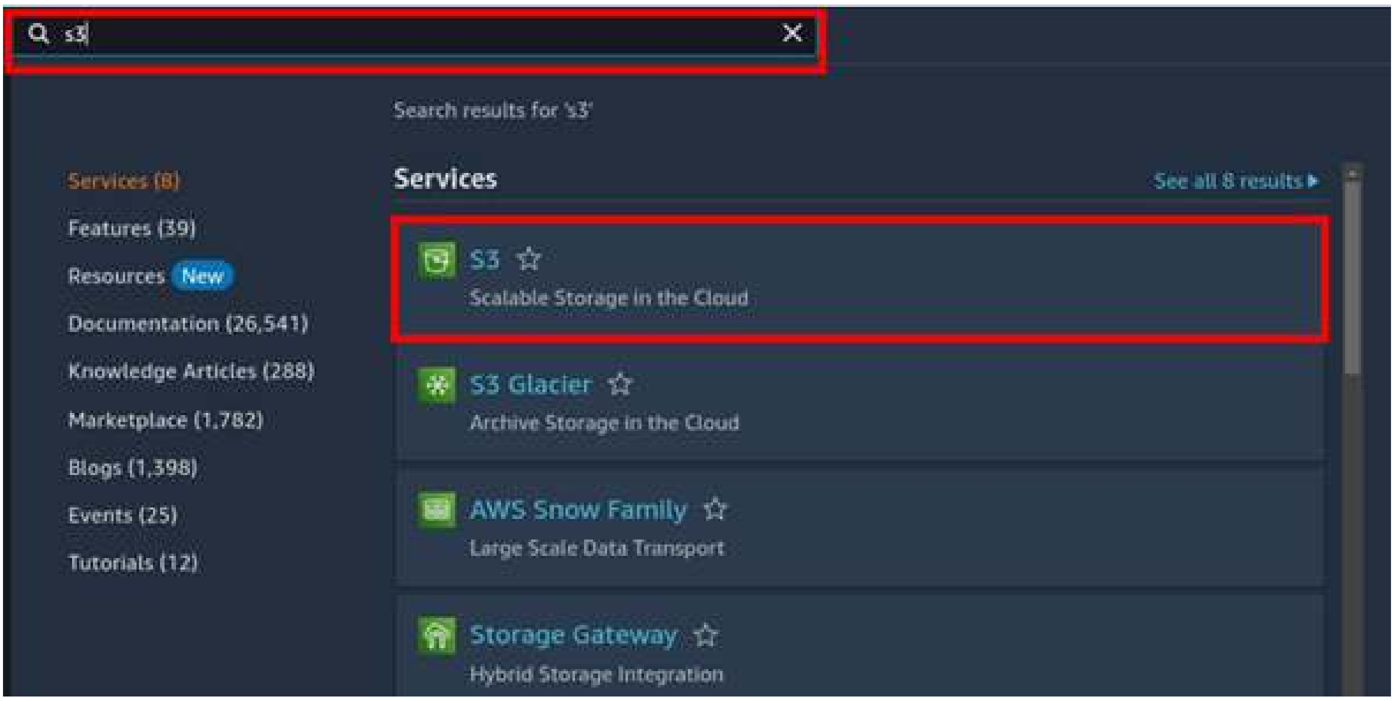
Get presigned URLs

A GET-presigned URL can be used directly in a browser or integrated into an application or webpage to download an object from an S3 bucket. It can be generated using the AWS Management Console, AWS CLI, or AWS SDK.

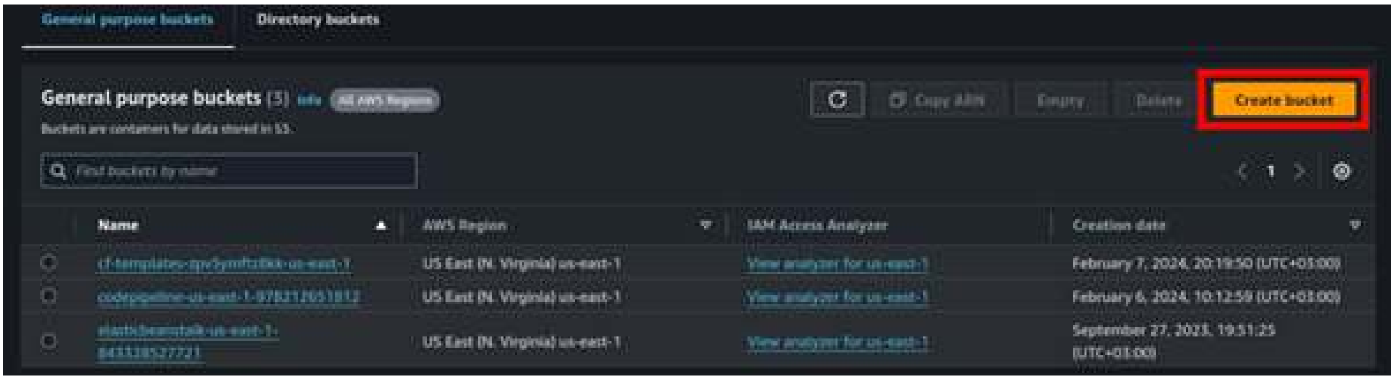
In the following, I will demonstrate how to generate a GET-presigned URL using the AWS Management Console.

Generating Get presigned URL with the console

Log in to the management console, in the search box, type s3 then select s3 under services.

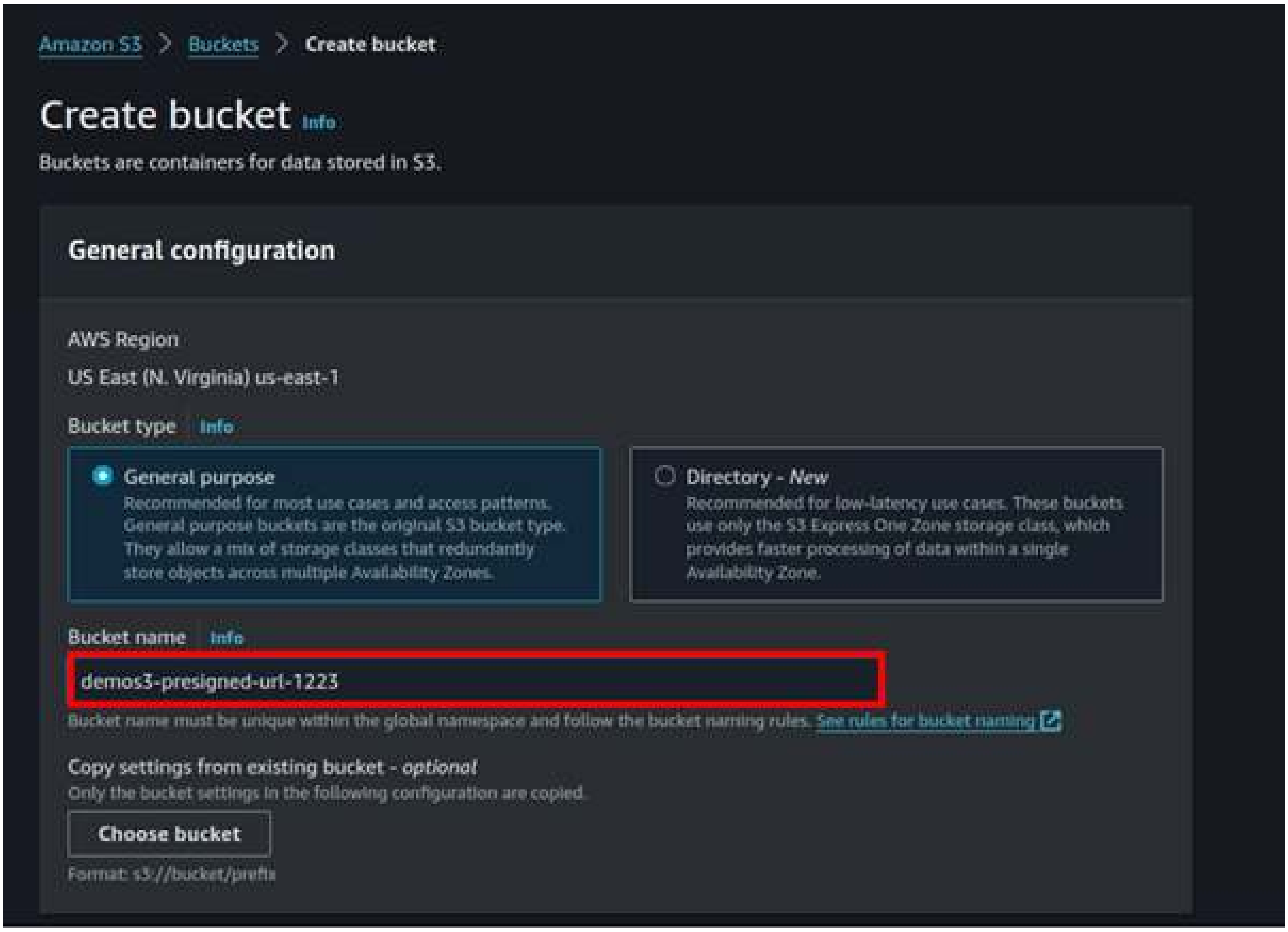


In the s3 UI select Create Bucket.


General purpose buckets
Directory buckets
General purpose buckets (3) Info All AWS Regions
Buckets are containers for data stored in S3.
Copy ARN
Empty
Delete
Create bucket
Find buckets by name
1

	Name	AWS Region	IAM Access Analyzer	Creation date
○	cf-templates-zpv5ymftzlkk-us-east-1	US East (N. Virginia) us-east-1	View analyzer for us-east-1	February 7, 2024, 20:19:50 (UTC+03:00)
○	codepipeline-us-east-1-978212651812	US East (N. Virginia) us-east-1	View analyzer for us-east-1	February 6, 2024, 10:12:59 (UTC+03:00)
○	elasticbeanstalk-us-east-1-843328527721	US East (N. Virginia) us-east-1	View analyzer for us-east-1	September 27, 2023, 19:51:25 (UTC+03:00)

In the create bucket UI, select a unique name for your bucket then Scroll down.



Amazon S3 > Buckets > Create bucket

Create bucket Info

Buckets are containers for data stored in S3.

General configuration

AWS Region

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

Bucket type Info

● General purpose
Recommended for most use cases and access patterns. General purpose buckets are the original S3 bucket type. They allow a mix of storage classes that redundantly store objects across multiple Availability Zones.

○ Directory - *New*
Recommended for low-latency use cases. These buckets use only the S3 Express One Zone storage class, which provides faster processing of data within a single Availability Zone.

Bucket name Info

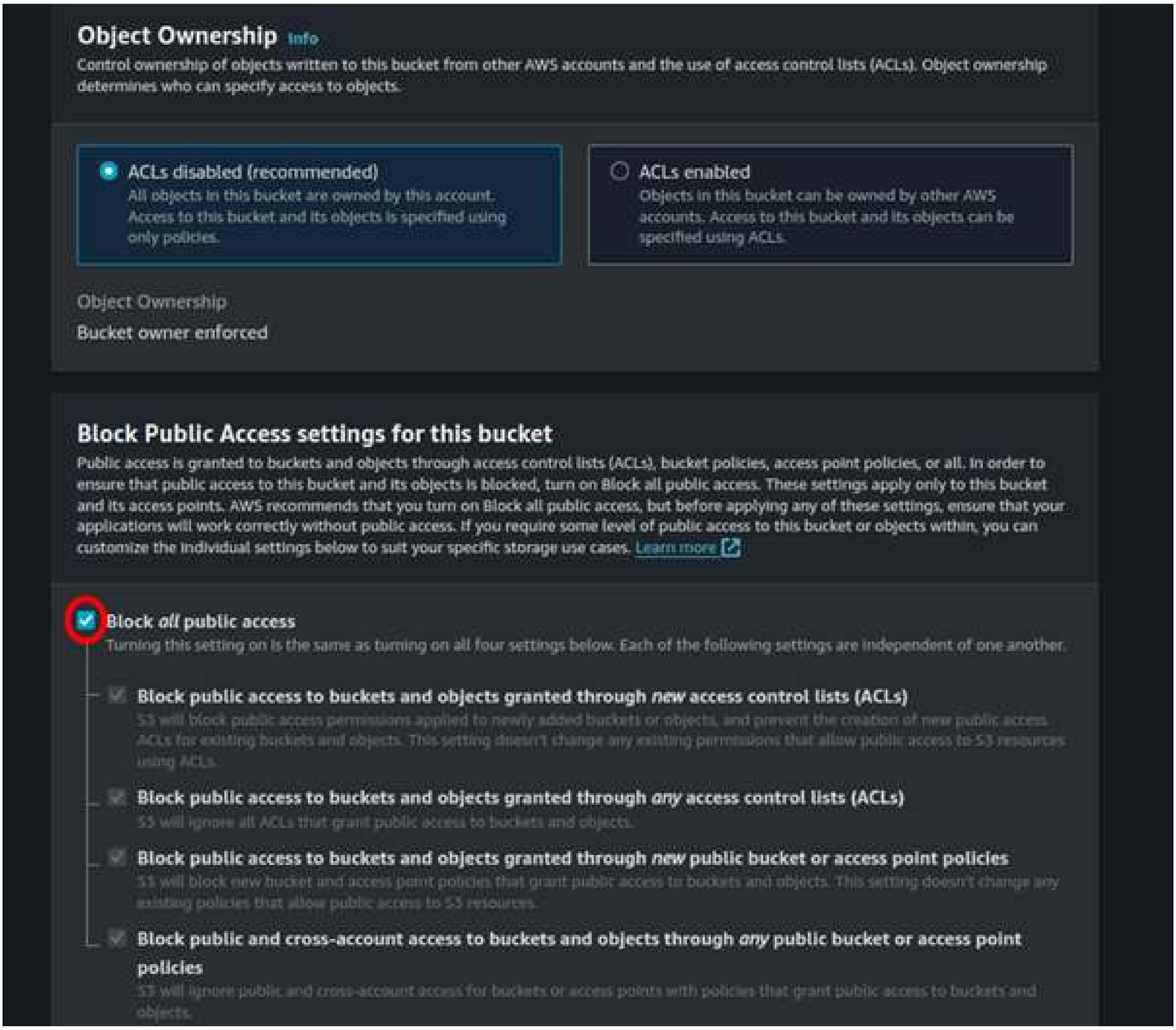
demos3-presigned-url-1223

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

Make sure all public access is blocked.



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

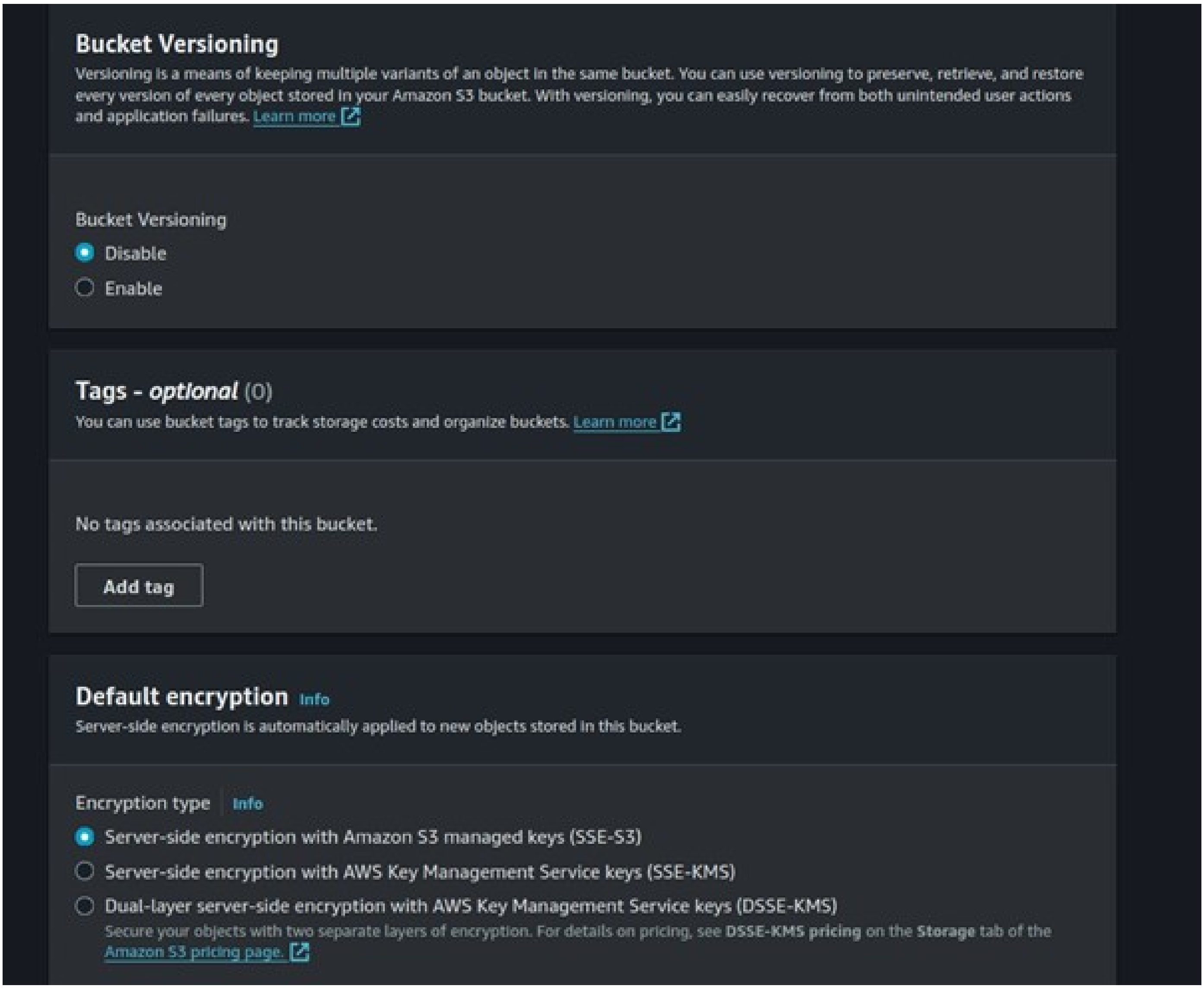
Block Public Access settings for this bucket

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 *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.

We will leave the remaining settings as default, then scroll down and click Create Bucket.



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 - *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

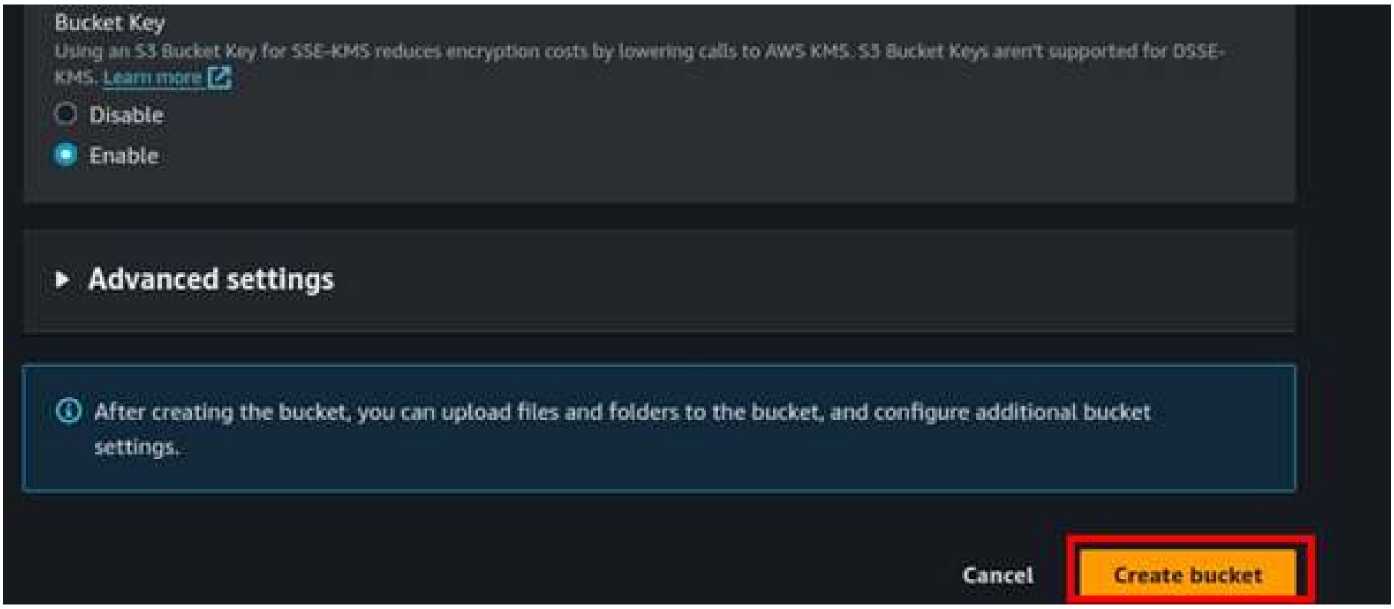
Server-side encryption is automatically applied to new objects stored in this bucket.

Encryption type Info

● Server-side encryption with Amazon S3 managed keys (SSE-S3)

○ 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.



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

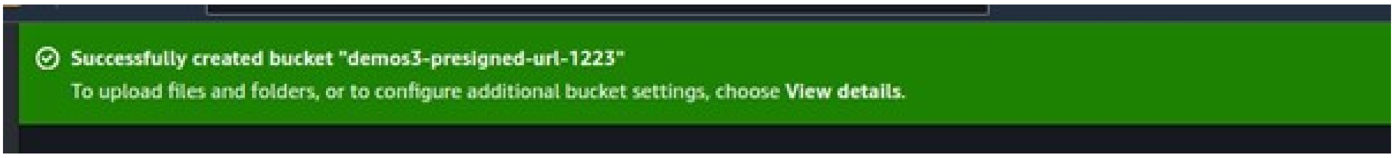
○ Disable

● Enable

▸ Advanced settings

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

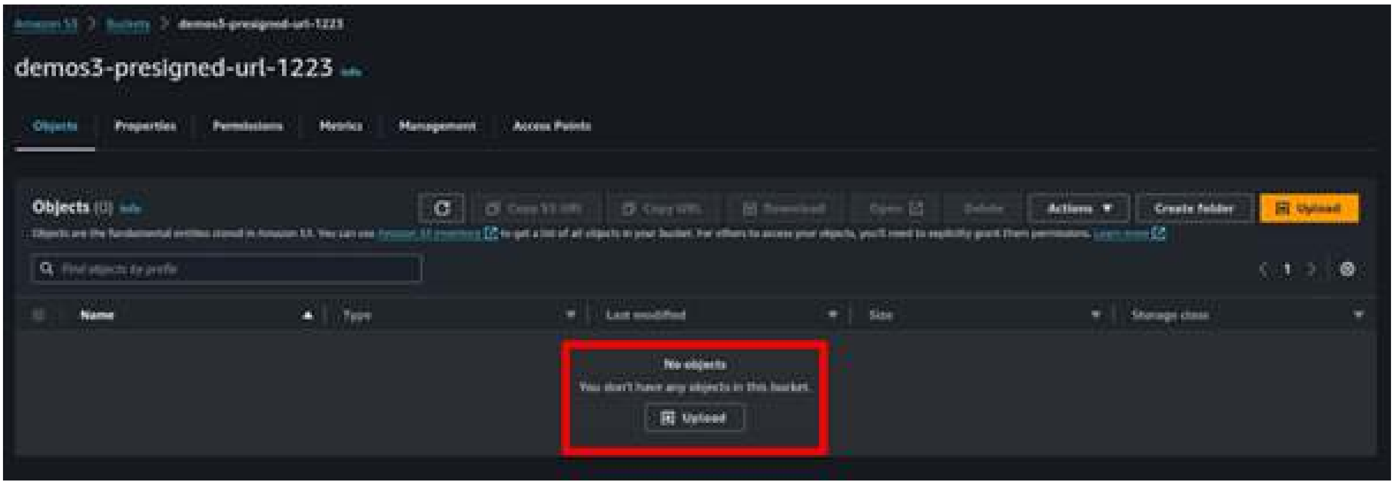
Our s3 bucket has been successfully created.



Successfully created bucket "demos3-presigned-url-1223"

To upload files and folders, or to configure additional bucket settings, choose **View details**.

Select your bucket then select upload.

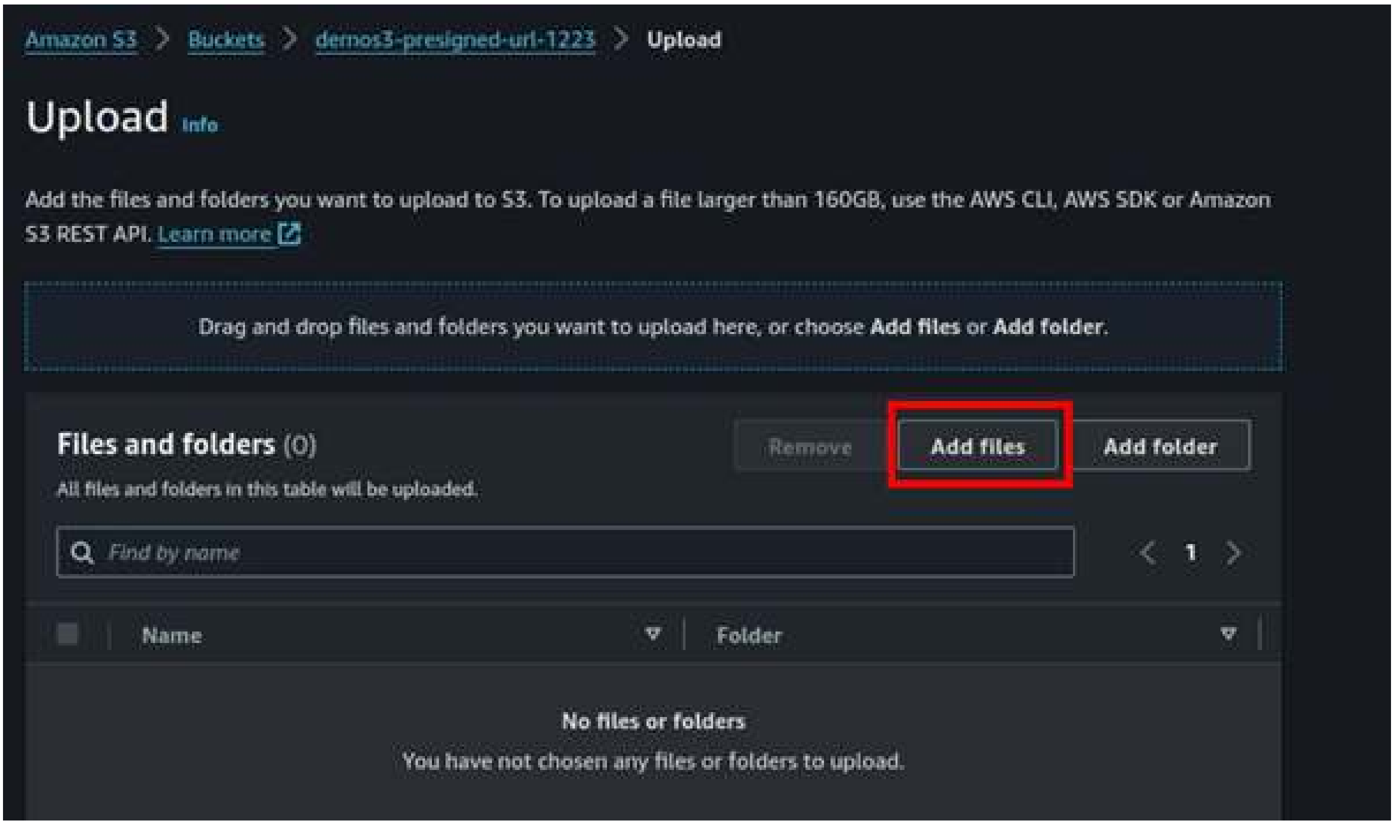


Objects are the fundamental entities stored in Amazon S3. You can use Amazon S3 inventory to get a list of all objects in your bucket. For others to access your objects, you'll need to explicitly grant them permissions. Learn more

No objects

You don't have any objects in this bucket.

In the upload UI, select add files



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 folder**.

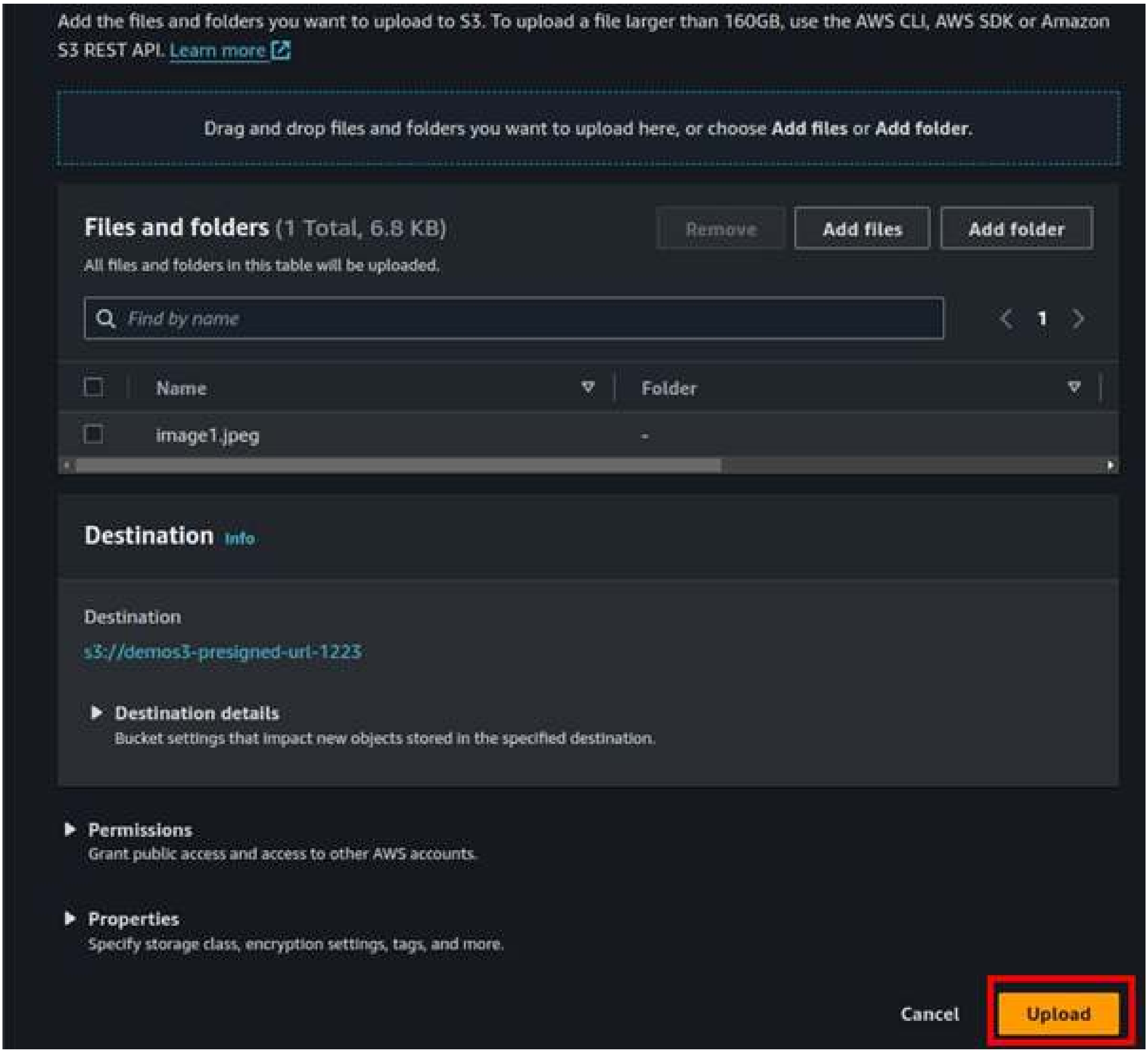
Files and folders (0)

All files and folders in this table will be uploaded.

No files or folders

You have not chosen any files or folders to upload.

Select your file then click 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 folder**.

Files and folders (1 Total, 6.8 KB)

All files and folders in this table will be uploaded.

□	Name	Folder
□	image1.jpeg	-

Destination Info

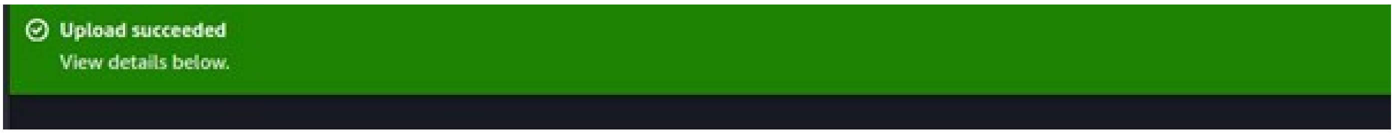
Destination

s3://demos3-presigned-url-1223

▶ **Destination details**
Bucket settings that impact new objects stored in the specified destination.

▶ **Permissions**
Grant public access and access to other AWS accounts.

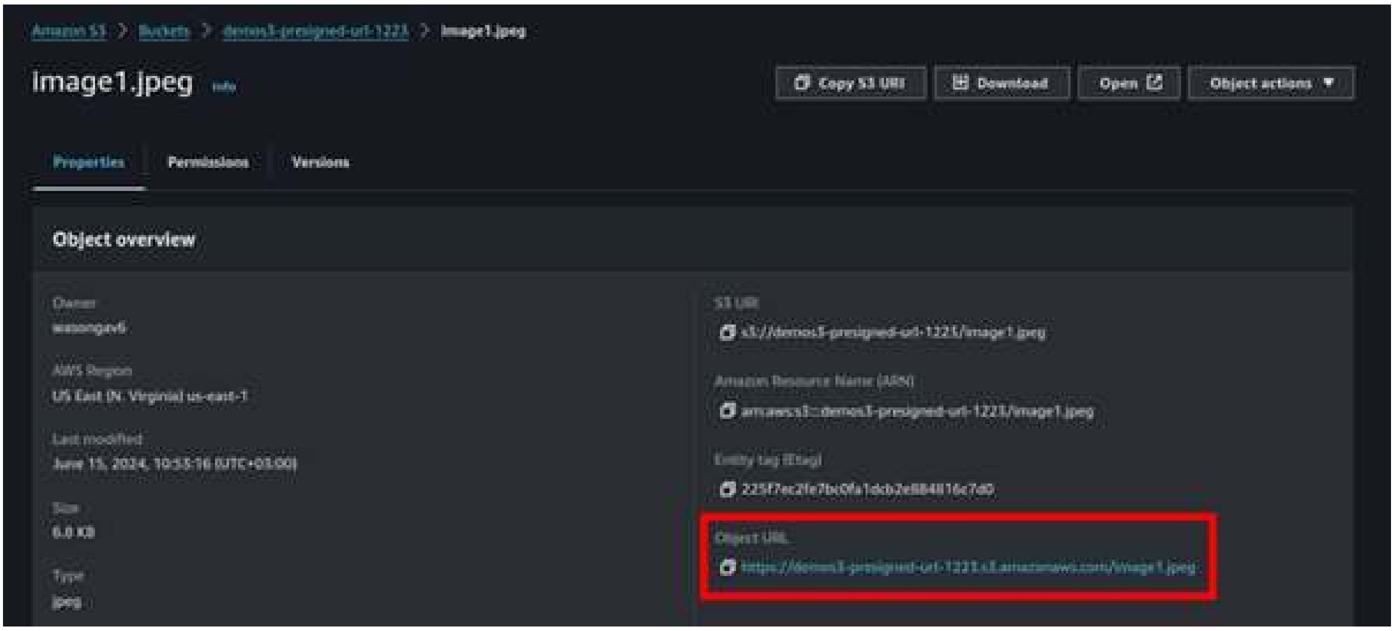
▶ **Properties**
Specify storage class, encryption settings, tags, and more.



Upload succeeded
View details below.

Once our object has been successfully uploaded, remember our bucket is private since we blocked all public access.

Click the object you uploaded select the object URL then paste it into your Favorite browser.



Object overview

Owner
wasongav6

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

Last modified
June 15, 2024, 10:53:16 (UTC+03:00)

Size
6.8 KB

Type
jpeg

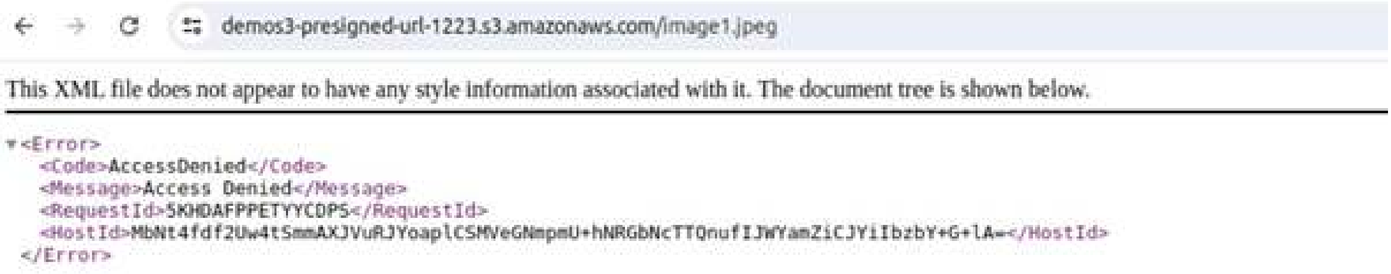
S3 URI
s3://demos3-presigned-url-1223/image1.jpeg

Amazon Resource Name (ARN)
arn:aws:s3:::demos3-presigned-url-1223/image1.jpeg

Entity tag (Etag)
225f7ec2fe7bc0fa1dcb2e884816c7d0

Object URL
https://demos3-presigned-url-1223.s3.amazonaws.com/image1.jpeg

This was expected, we could not access our object since our bucket is private. We will now leverage the s3 presigned URL to securely access our object without making our bucket public.

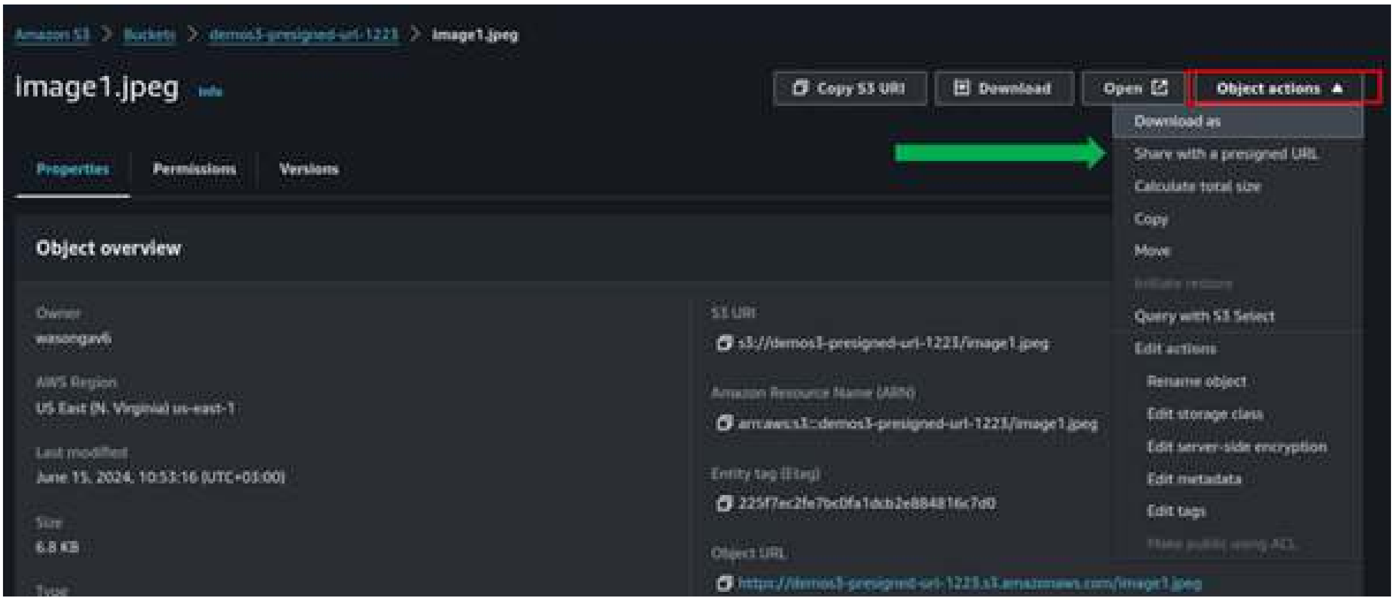


demos3-presigned-url-1223.s3.amazonaws.com/image1.jpeg

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>SKHDAFPPETYYCDPS</RequestId>
   <HostId>MbNt4fdf2Uw4tSmmAXJVuRJYoaplCSMVeGNmpmU+hNRGbNcTTQnufIJWYamZiCJYiIbzbY+G+lA=</HostId>
 </Error>
```

Still, in the object UI, select the drop-down object action. Then select Share with the presigned URL.



Object overview

Owner
wasongav6

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

Last modified
June 15, 2024, 10:53:16 (UTC+03:00)

Size
6.8 KB

S3 URI
s3://demos3-presigned-url-1223/image1.jpeg

Amazon Resource Name (ARN)
arn:aws:s3:::demos3-presigned-url-1223/image1.jpeg

Entity tag (Etag)
225f7ec2fe7bc0fa1dcb2e884816c7d0

Object URL
https://demos3-presigned-url-1223.s3.amazonaws.com/image1.jpeg

For time interval until the URL expires can be minutes to several hours, for this demo I will only give it 2 minutes. So, select minutes then for number of minutes, select two then click Create presigned URL.

accendnetworks

www.accendnetworks.com