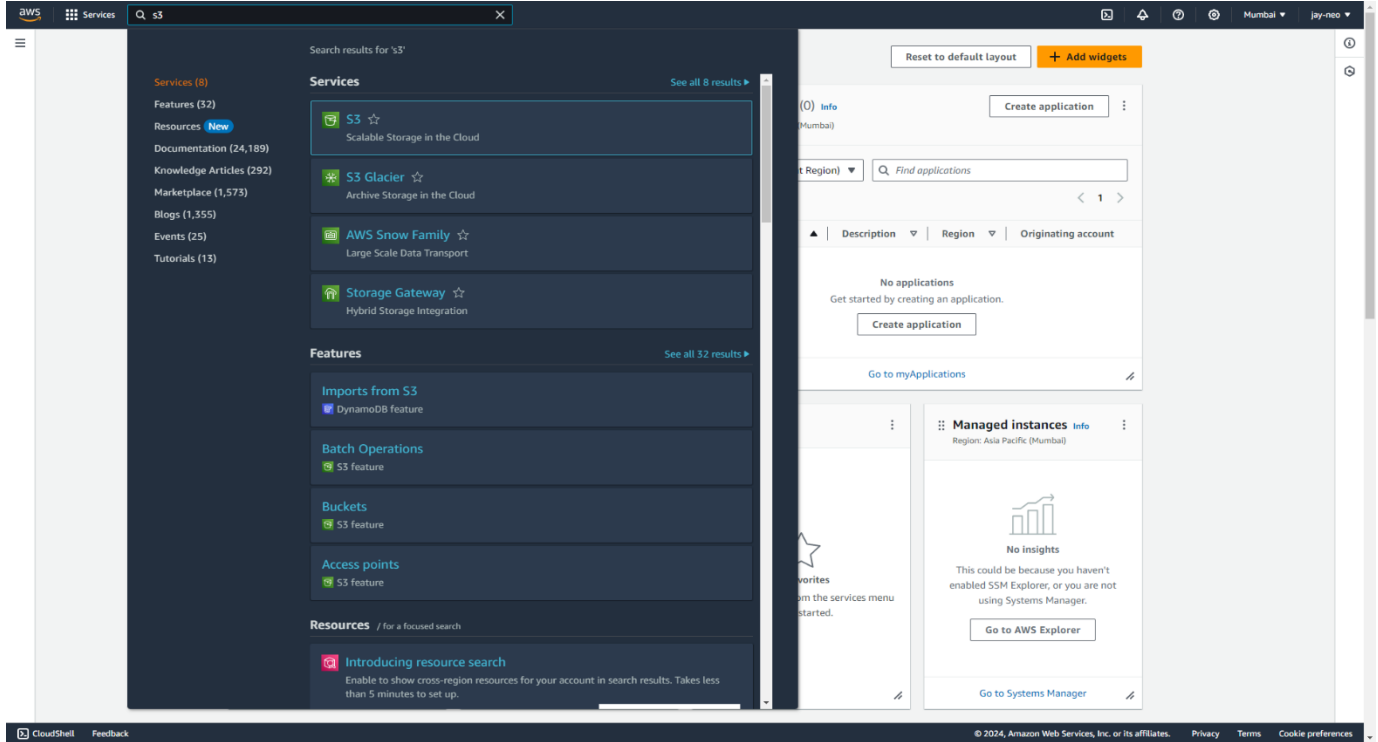


Assignment : 4

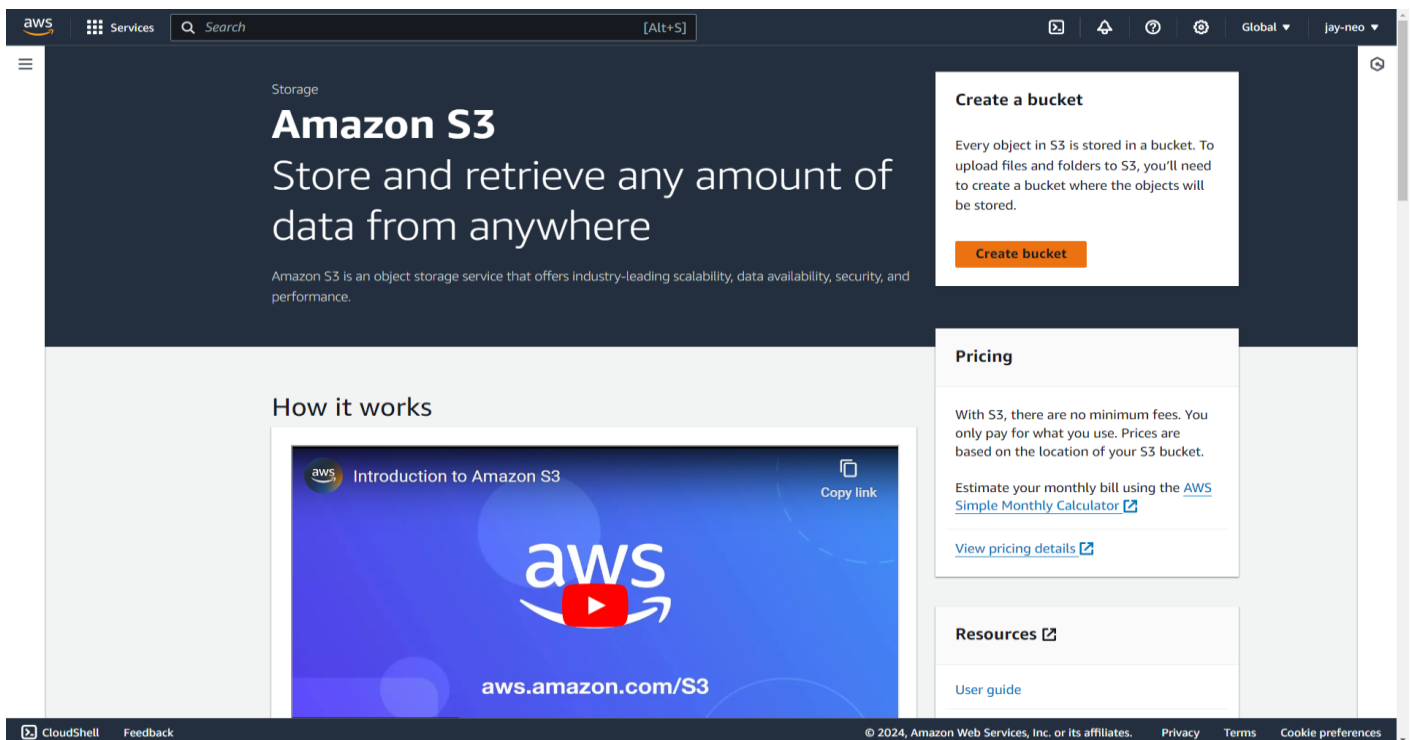
Statement : Create a private bucket in AWS. Upload a file and check by reassigned URL whether you can access the file or not.

Steps---

1. First sign in to your AWS account and search for “S3” (Simple Storage Services - where we will create the Bucket) in the search bar.



2. Now click in “Create Bucket” option.



3. Now set the configuration of the bucket -

- i. Bucket name
- ii. AWS Region
- iii. Object Ownership information (ACLs disabled)
- iv. Check all public access block

After filling click on “Create Bucket” option.

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](#)

neoFolder

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.

Choose bucket

Format: s3://bucket/prefix

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.

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.

Add tag

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.

CancelCreate bucket

4.you can see the bucket is successfully created. Next click on the <Bucket name>.

Services

Search

[Alt+S]

Global

jay-neo

Amazon S3 > Buckets

Account snapshot

Storage lens provides visibility into storage usage and activity trends. [Learn more](#)

View Storage Lens dashboard

General purpose buckets

Directory buckets

General purpose buckets (1) [Info](#)

Buckets are containers for data stored in S3. [Learn more](#)

Find buckets by name

Copy

Copy ARN

Empty

Delete

Create bucket

Name

AWS Region

Access

Creation date

neofolder

Asia Pacific (Mumbai) ap-south-1

Objects can be public

February 7, 2024, 15:49:13 (UTC+05:30)

5.Click on the “Upload” option.

Services

Search

[Alt+S]

Global

jay-neo

Amazon S3 > Buckets > neofolder

neofolder [Info](#)

Objects

Properties

Permissions

Metrics

Management

Access Points

Objects (0) [Info](#)

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](#)

Find objects by prefix

Copy

Copy S3 URI

Copy URL

Download

Open

Delete

Actions

Create folder

Upload

Name

Type

Last modified

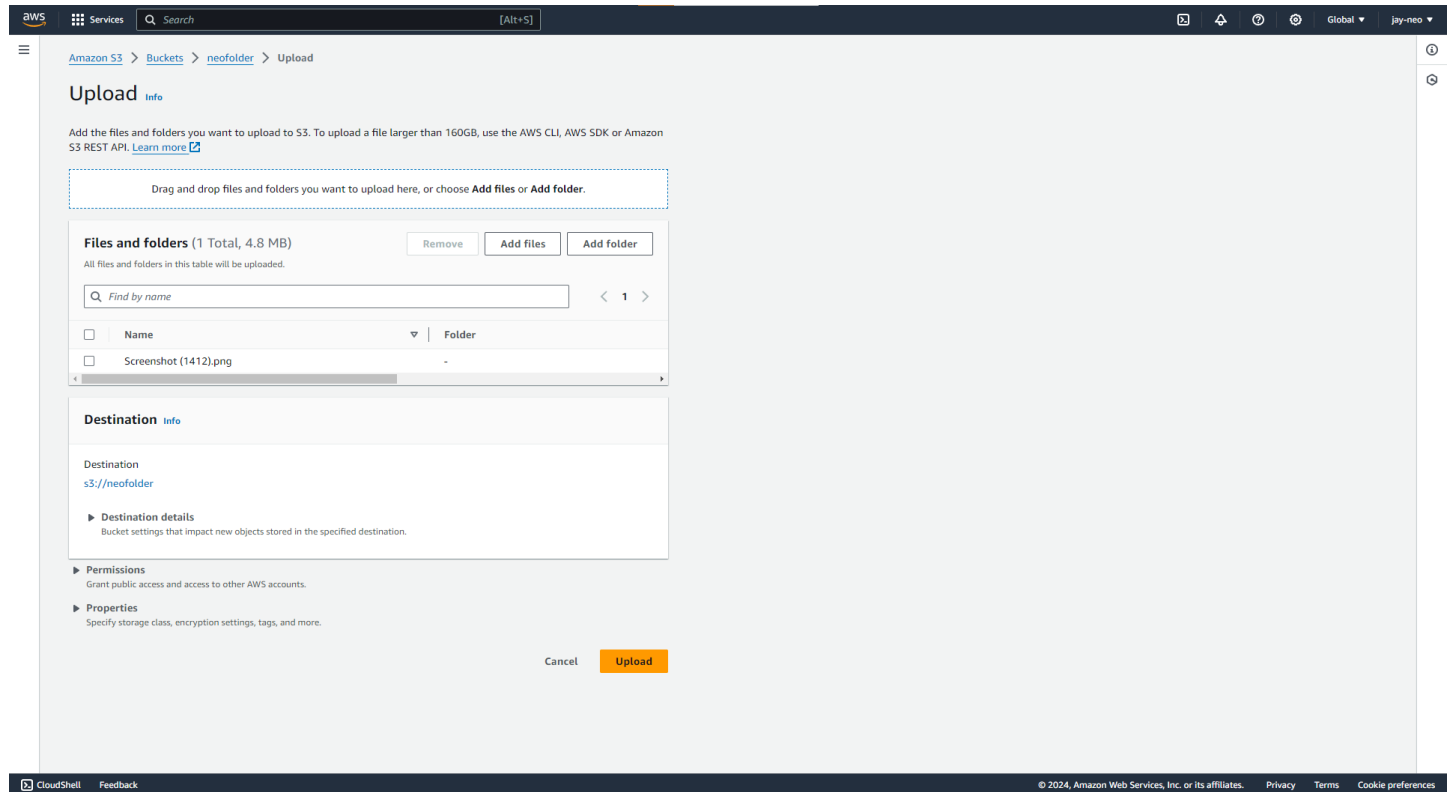
Size

Storage class

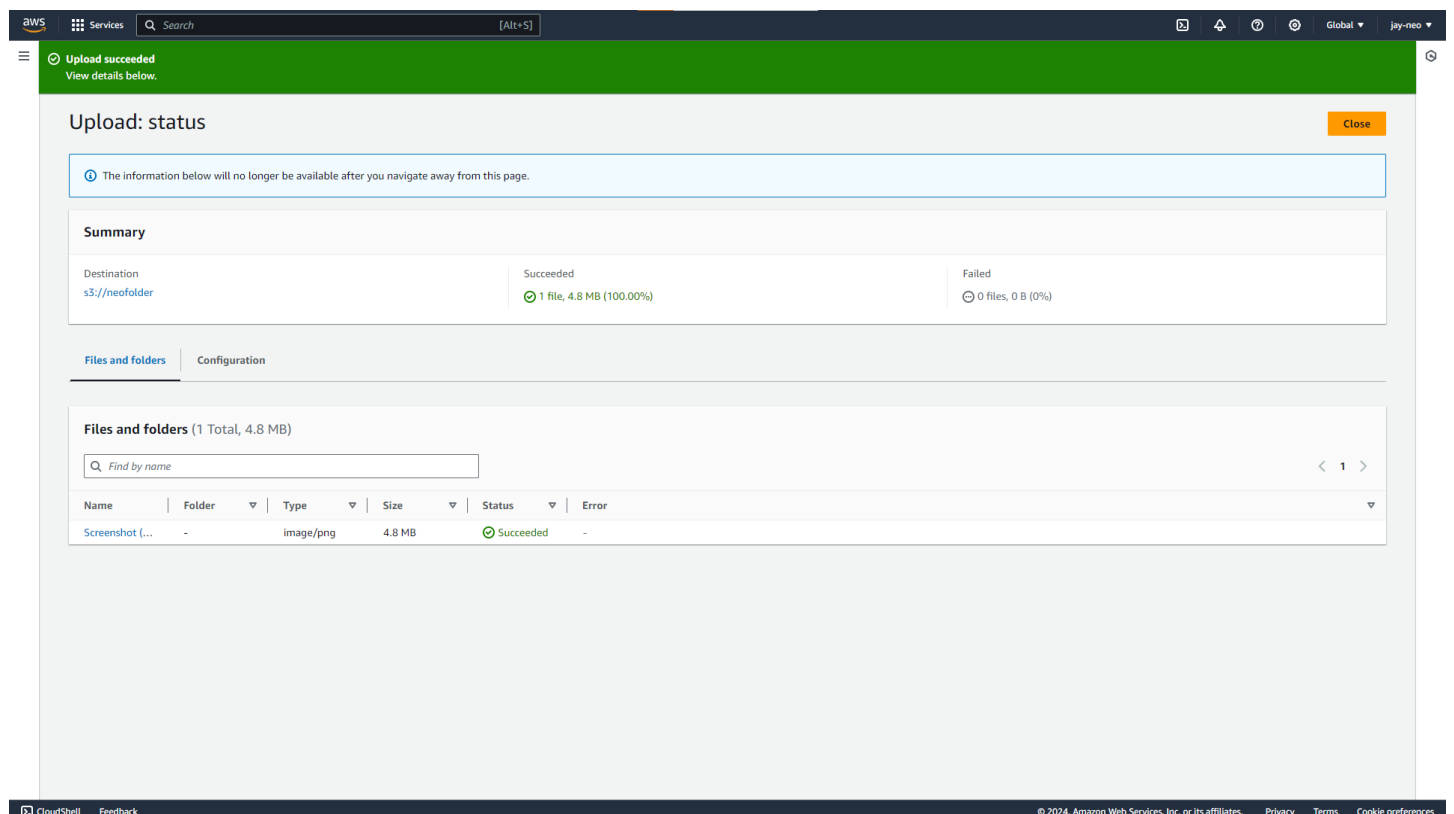
No objects
You don't have any objects in this bucket.

Upload

6. Click “Add files” and upload a file.



7. File is uploaded. Now click on the <uploaded file name >



8.Copy the object URL from this.

Amazon S3

Amazon S3 > Buckets > neofolder > Screenshot (1412).png

Copy S3 URI Download Open Object actions

Properties Permissions Versions

Object overview

Owner: 2491a160e8e1030d09e1415c11e07...

AWS Region: Asia Pacific (Mumbai) ap-south-1

Last modified: February 21, 2024, 11:12:37 (UTC+05:30)

Size: 4.8 MB

Type: png

Key: Screenshot (1412).png

S3 URI: s3://neofolder/Screenshot (1412).png

Amazon Resource Name (ARN): arn:aws:s3::neofolder/Screenshot (1412).png

Entity tag (Etag): ff67818c6dac6cdd...

Object URL: https://neofolder.s3.ap-south-1.amazonaws.com/Screenshot+(1412).png

Object management overview

The following bucket properties and object management configurations impact the behavior of this object.

Bucket properties

Bucket Versioning: When enabled, multiple variants of an object can be stored in the bucket to easily recover from unintended user actions and application failures. **Disabled**

Management configurations

Replication status: When a replication rule is applied to an object the replication status indicates the progress of the operation.

View replication rules

Expiration rule: You can use a lifecycle configuration to define expiration rules to schedule the removal of this object after a pre-defined time period.

9.Open the URL in another browser. It will show access denied.

neofolder.s3.ap-south-1.amazonaws.com/Screenshot+(1412).png

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

```
<?xml version="1.0" encoding="UTF-8" ?>
<Error>
  <Code>AccessDenied</Code>
  <Message>Access Denied</Message>
  <RequestId>46NXFK7KXANPWFFG</RequestId>
  <HostId>IQUKt0pnYTIcIs68CgPVxIYgC5SzlKPa2C1/tZh7MhwUwSE0ID2UVnIYgbTi8UPfI6UiJVtDj6c</HostId>
</Error>
```

10.Now click on “Object actions” and select “Share with a presigned URL” option.

Amazon S3

Amazon S3 > Buckets > neofolder

neofolder Info

Objects Properties Permissions Metrics Management Access Points

Objects (1) Info

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 the

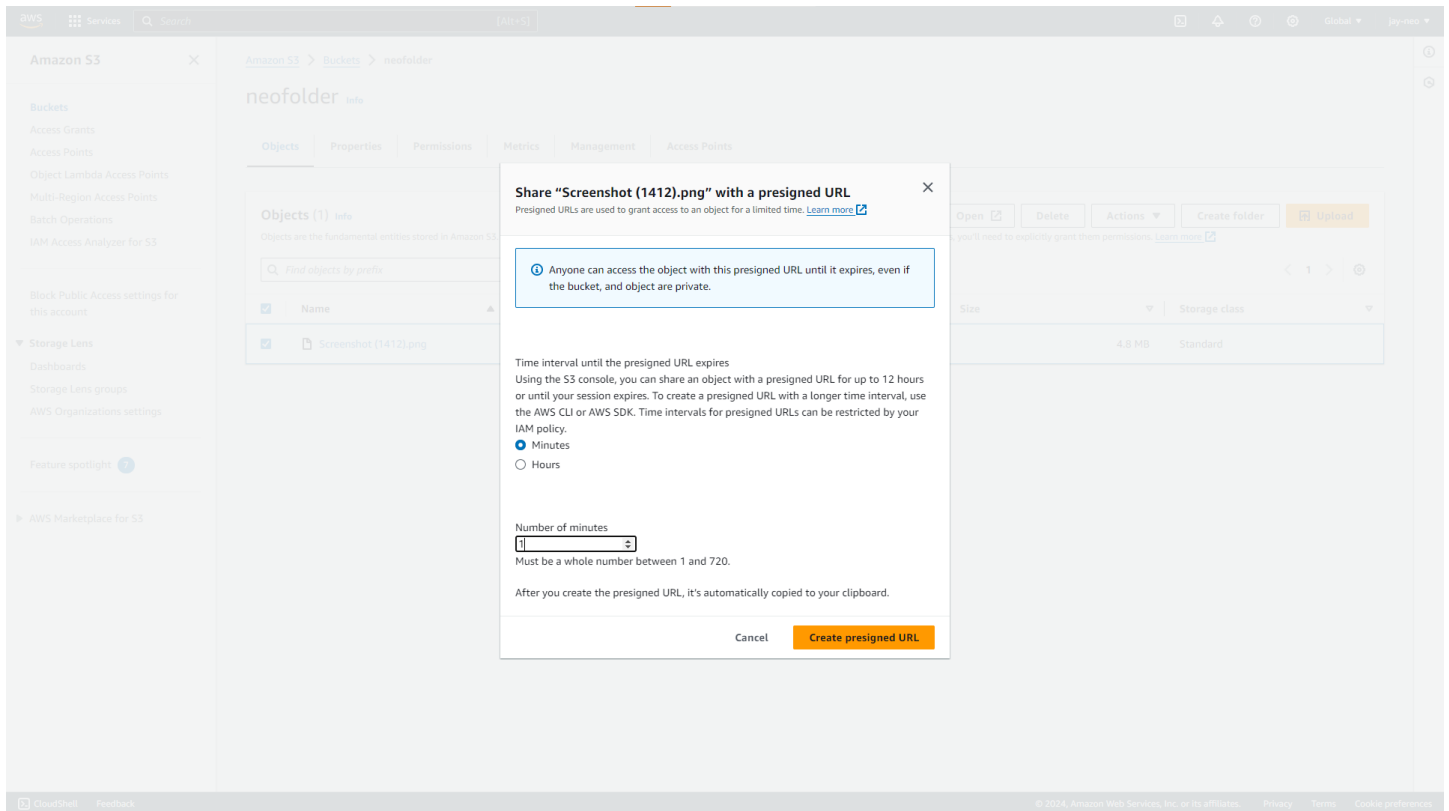
Find objects by prefix

<input checked="" type="checkbox"/>	Name	Type	Last modified	Size
<input checked="" type="checkbox"/>	Screenshot (1412).png	png	February 21, 2024, 11:12:37 (UTC+05:30)	

Object actions menu:

- Download as
- Share with a presigned URL
- Calculate total size
- Copy
- Move
- Initiate restore
- Query with S3 Select
- Edit actions
- Rename object
- Edit storage class
- Edit server-side encryption
- Edit metadata
- Edit tags
- Make public using ACL

11. Now set the number of minutes (here 1 minutes) and click on “Create presigned URL”.



12. Next copy the Presigned URL and paste it on an another browser. The file will be visible for the given time.

