

Assignment No: 5

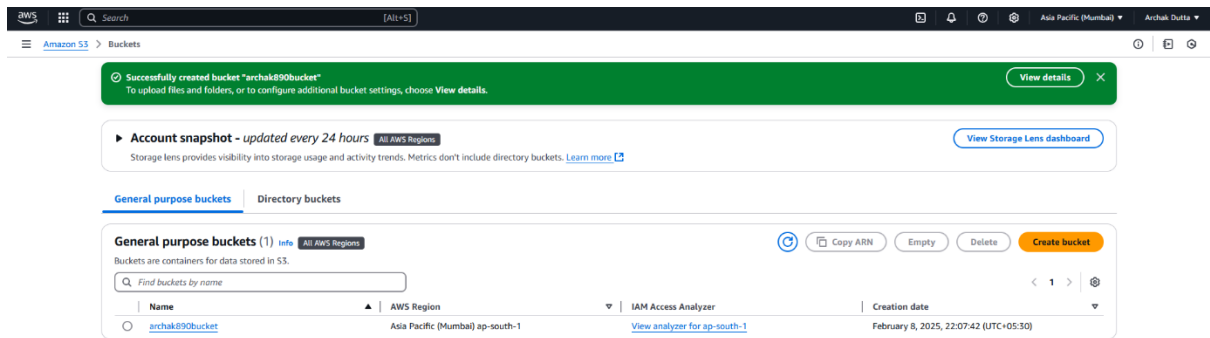
Problem Statement: Create a public bucket in AWS. Upload a file and give the necessary permission to check whether the file URL is working.

Solution:

1. At first go to the S3 bucket and click on the create bucket option.
2. Give a name to the bucket.
3. Then in the object ownership section click on the ACLs enabled option.

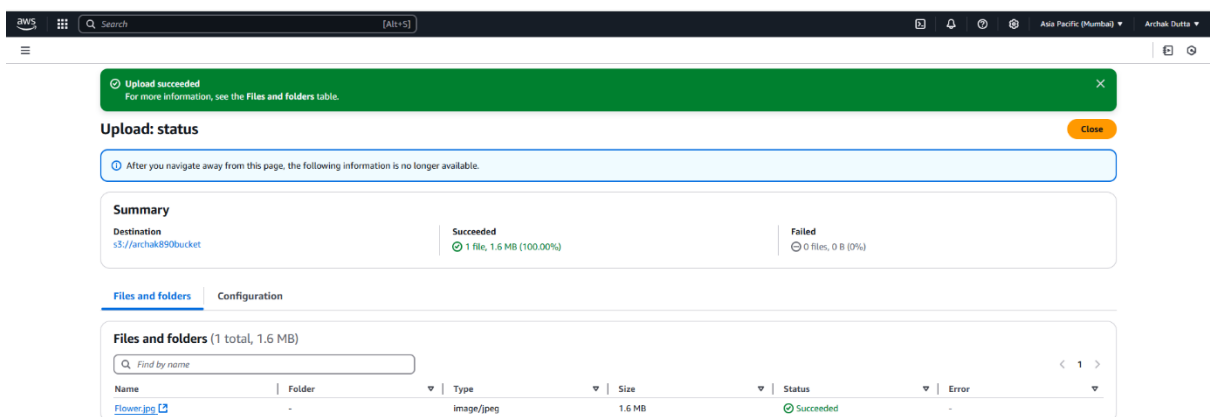
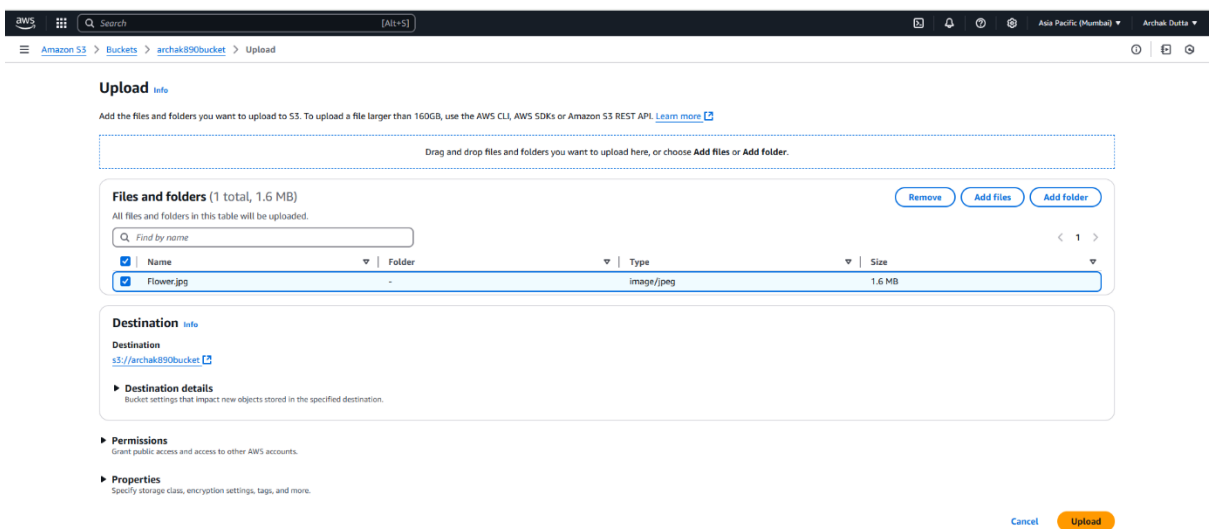
The screenshot shows the AWS 'Create bucket' console. The 'General configuration' section is active, showing the 'Bucket type' as 'General purpose' (selected) and 'Directory' (unselected). The 'Bucket name' is 'archak890bucket'. Below this, the 'Object Ownership' section is visible, with 'ACLs enabled' selected. A warning message states: 'We recommend disabling ACLs, unless you need to control access for each object individually or to have the object writer own the data they upload. Using a bucket policy instead of ACLs to share data with users outside of your account simplifies permissions management and auditing.'

The screenshot shows the 'Create bucket' console with the 'Tags - optional' section, 'Default encryption' section, and 'Advanced settings' section. The 'Tags' section shows 'No tags associated with this bucket.' The 'Default encryption' section shows 'Server-side encryption with Amazon S3 managed keys (SSE-S3)' selected. The 'Advanced settings' section shows a note: 'After creating the bucket, you can upload files and folders to the bucket, and configure additional bucket settings.'



4.Go to the created bucket and click on the upload option.

5.And upload a file(.jpg,.png,.pdf etc) in the bucket.



6. Then tick the bucket and copy the URL to check whether it is working or not.

7. But it is not working.



8. Hence, we made some necessary changes regarding access control permissions in ACL (Access Control List) of the object and then use the URL again.

9. And now we can access the files in the bucket using the object URL and thus a public bucket is created.

