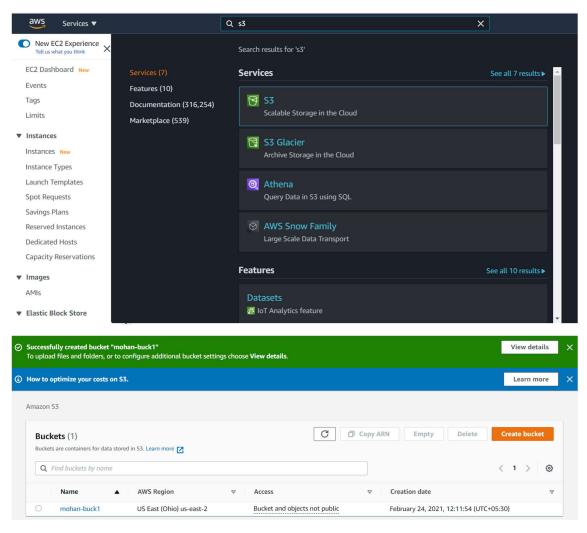
## Working with S3 Buckets

- Bucket Creation: Step 1
- File/folder upload: Step 2, 3,5
- Setting Public permission: Step 4

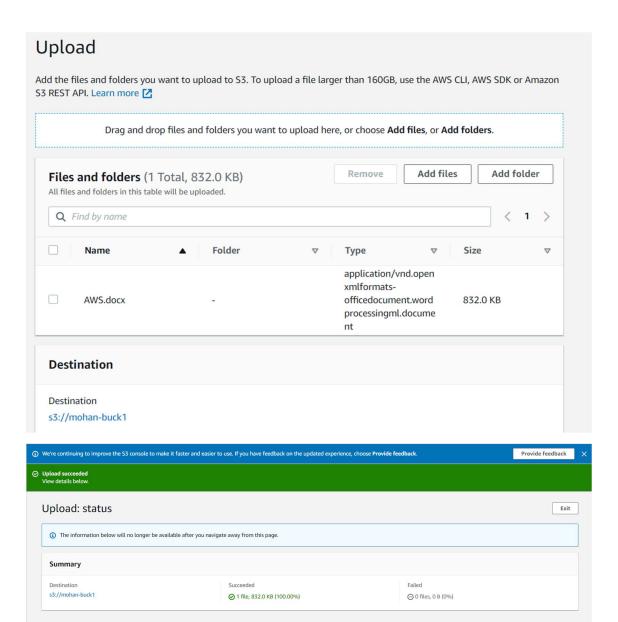
## 1. Create Bucket

- a. To create S3 bucket, Search for S3 and select S3
- b. In create Bucket Page
  - i. Add unique name 'mohan\_buck\_1'
  - ii. choose a region
  - iii. Select 'create bucket'
  - iv. Bucket name contains invalid characters: \_
  - v. Change the name to 'mohan-buck1

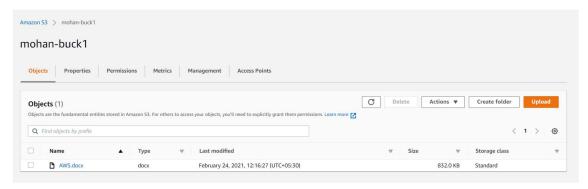
c.



- 2. Now we can upload files or folder
  - a. Added aws.docx file (sample)
  - b. Upload success



3. One item in my bucket



4. Edit Block public access and disable Block all public access. Save changes

## Edit Block public access (bucket settings) 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 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 S3 will ignore public and cross-account access for buckets or access points with policies that grant public access to buckets and Save changes Cancel Successfully edited Block Public Access settings for bucket. Amazon S3 > mohan-buck1 mohan-buck1 Permissions Metrics **Access Points** Objects **Properties** Management Permissions overview Objects can be public

5. Adding a folder and adding file in it

