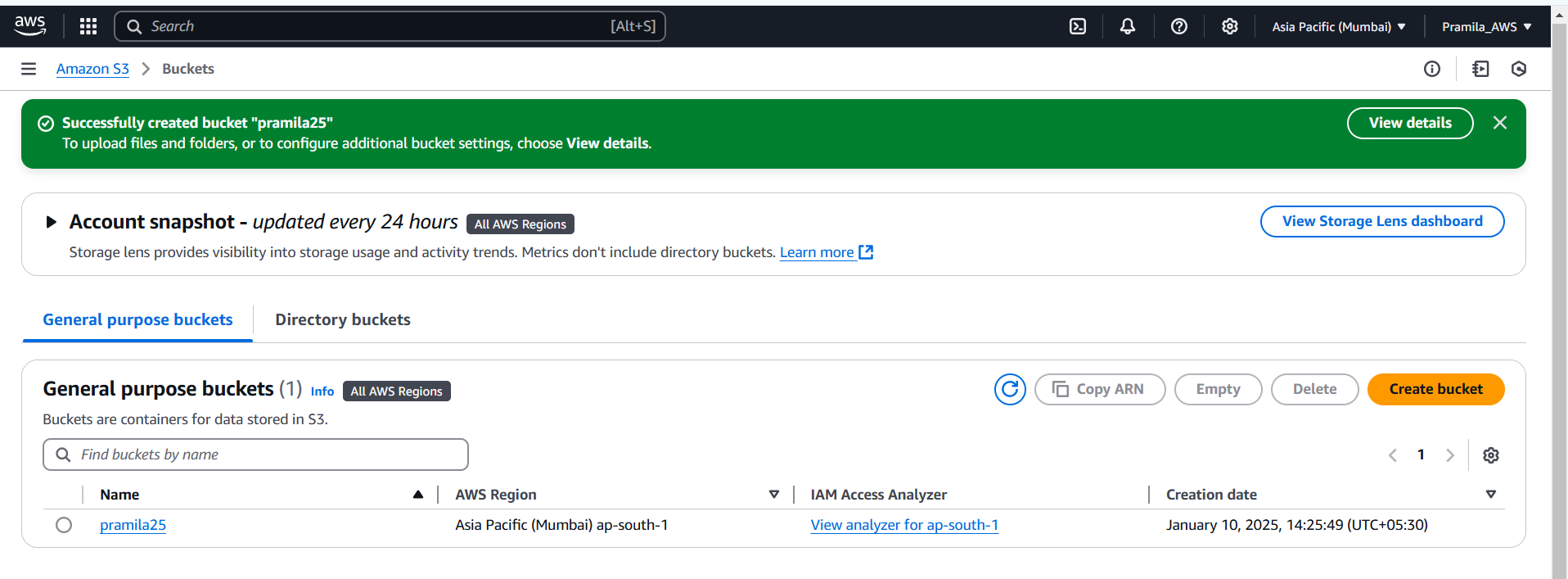
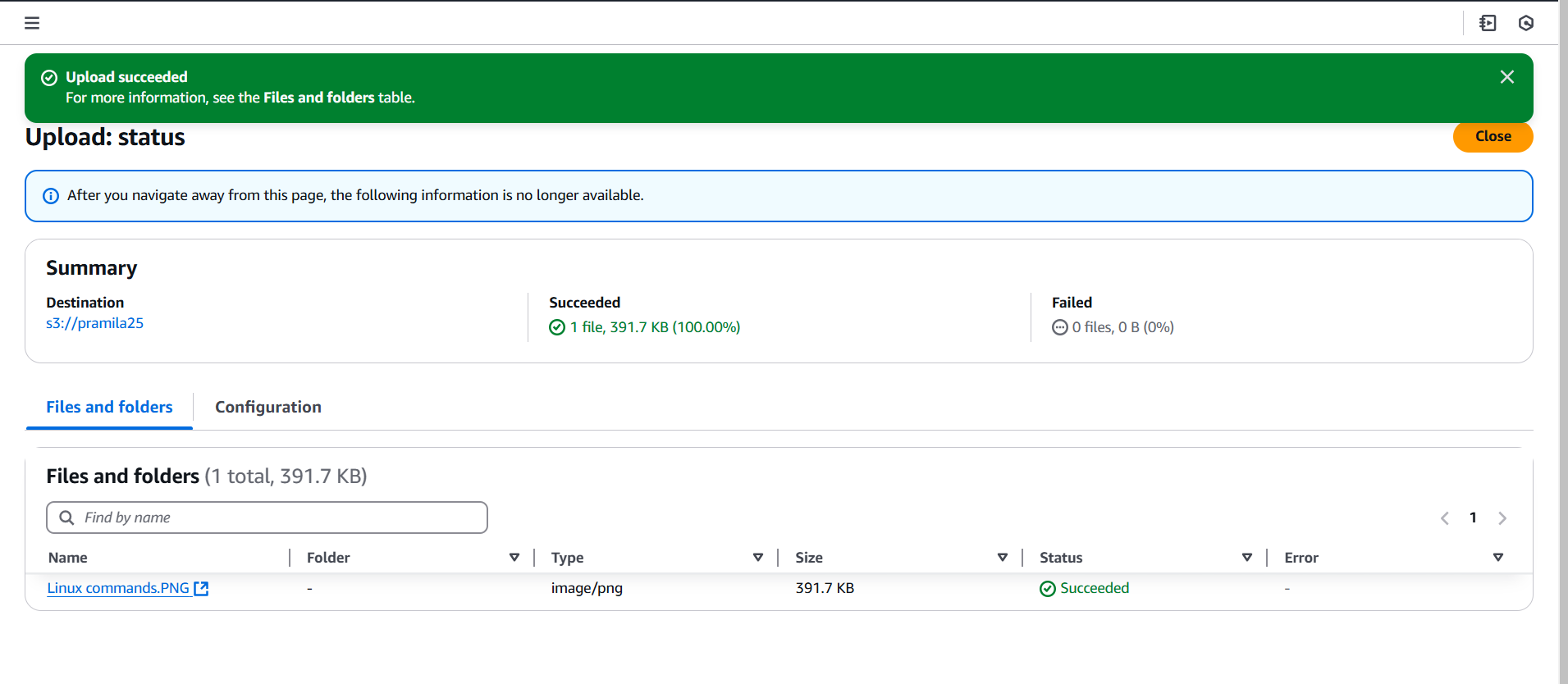
**S3 Storage**

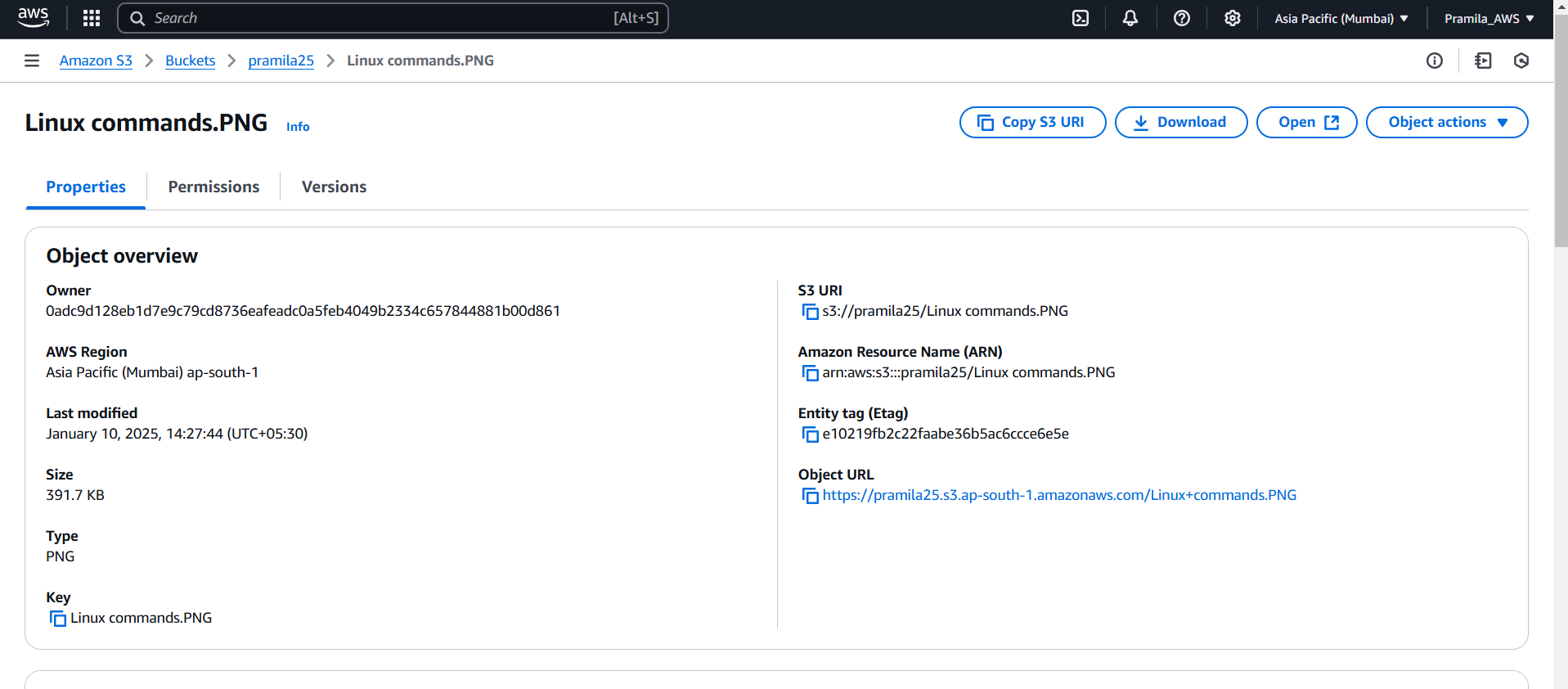
1. **Create bucket name “pramila25”**

****

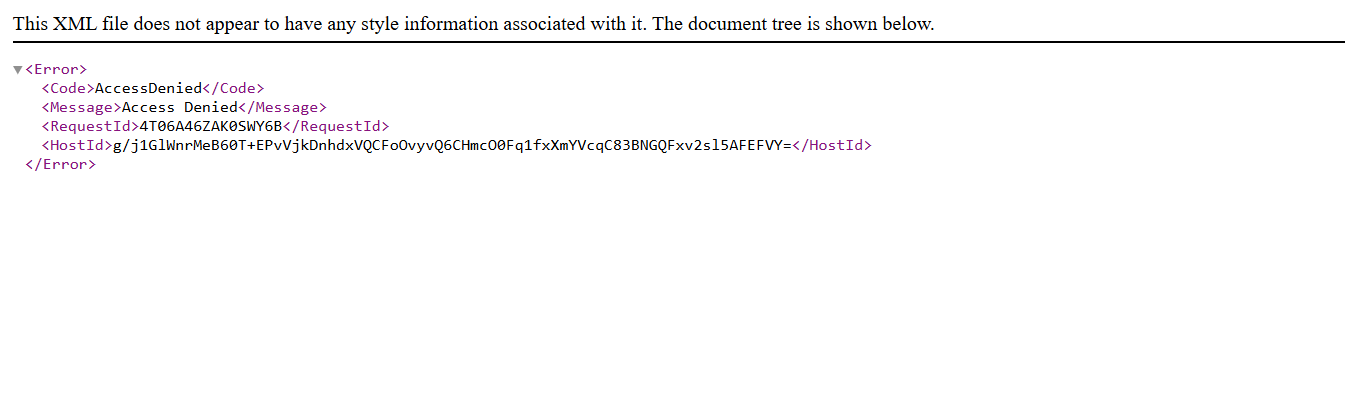
1. **Added object in “pramila25” bucket**

****

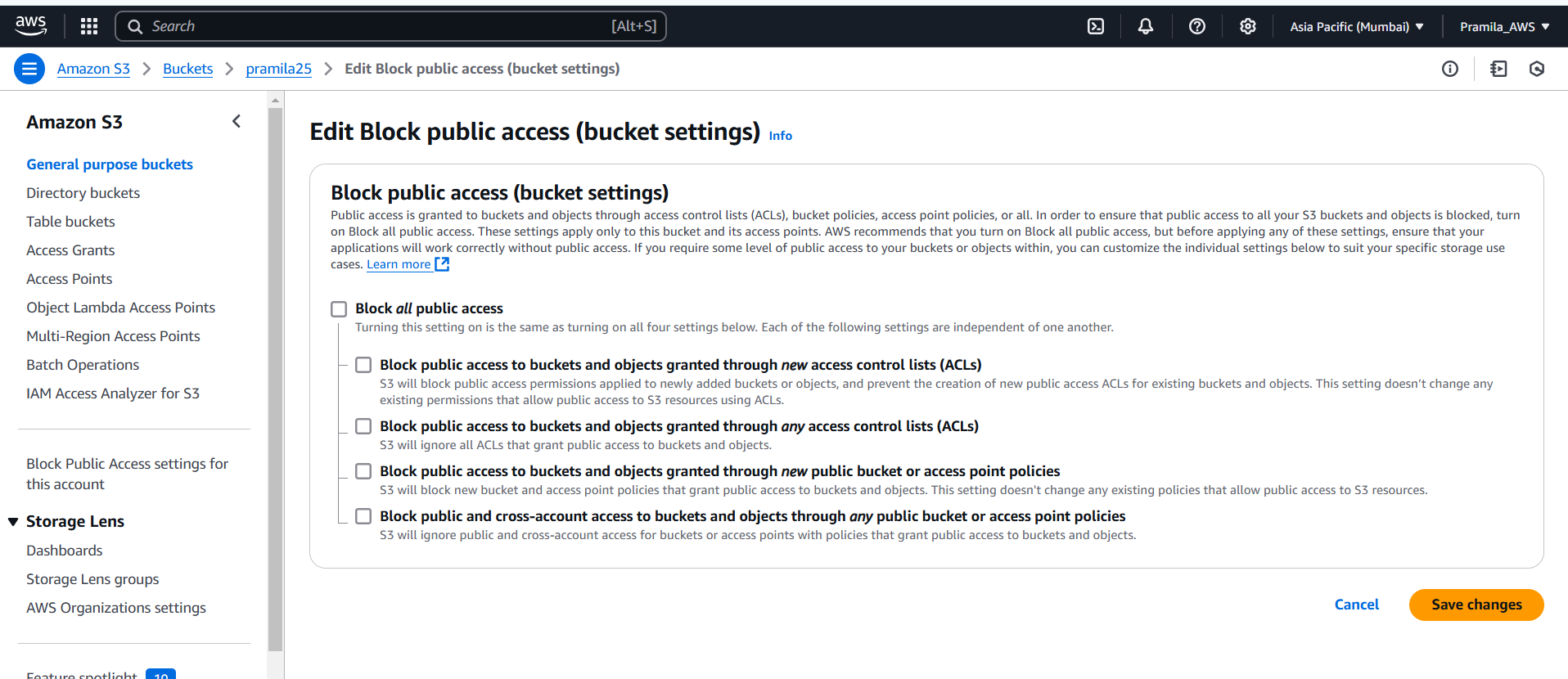
1. **Object details**

****

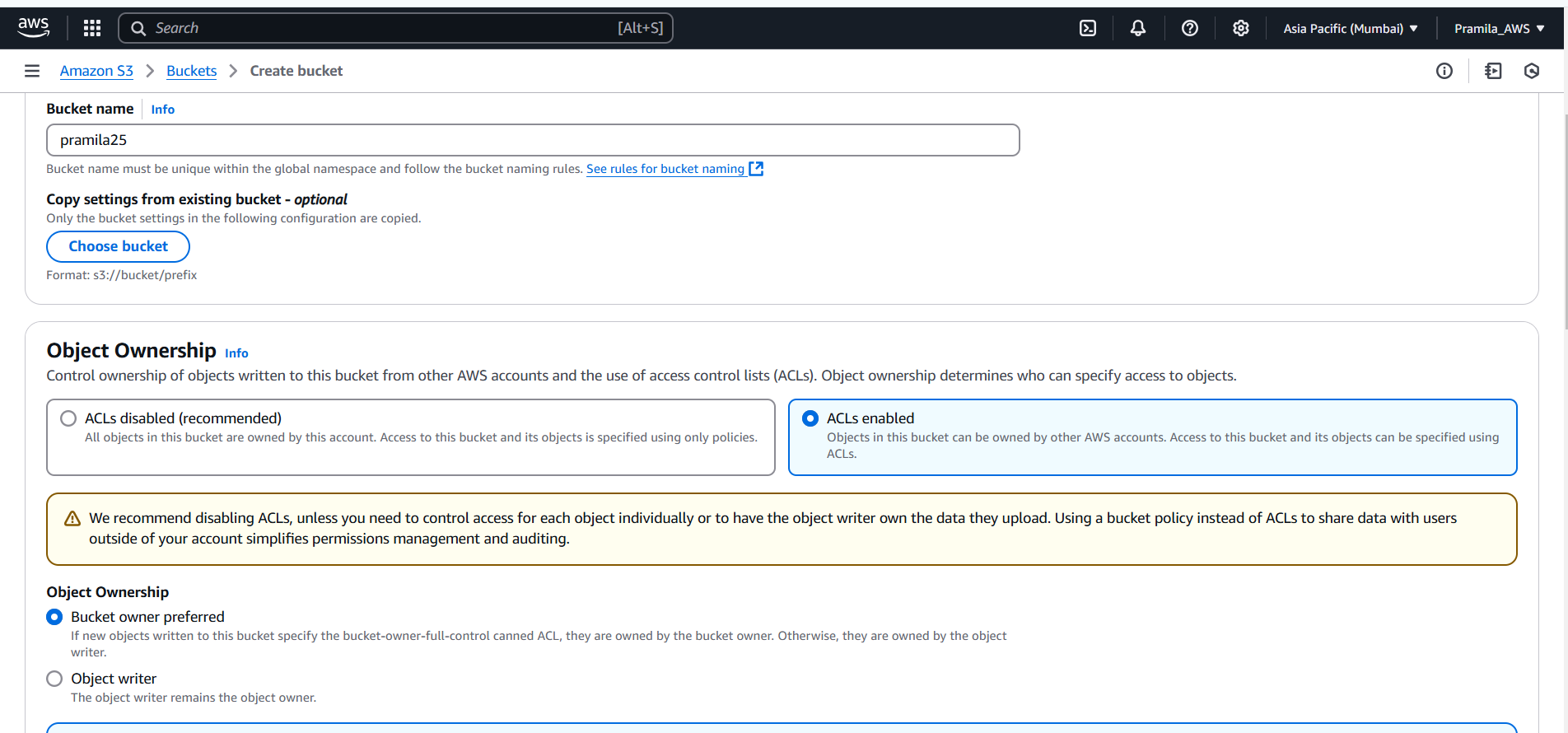
1. **By default Object are private we are not able to access it using url**

****

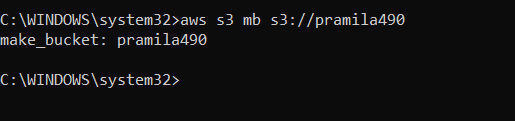
1. **To make bucket as private we need to uncheck “block all public access”**

****

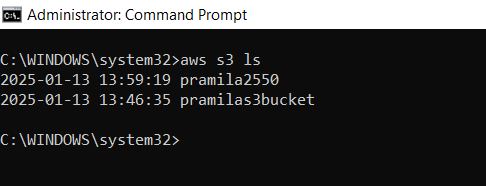
1. **To make object as private first we need to click “ACL enabled” at time of bucket creation**

****

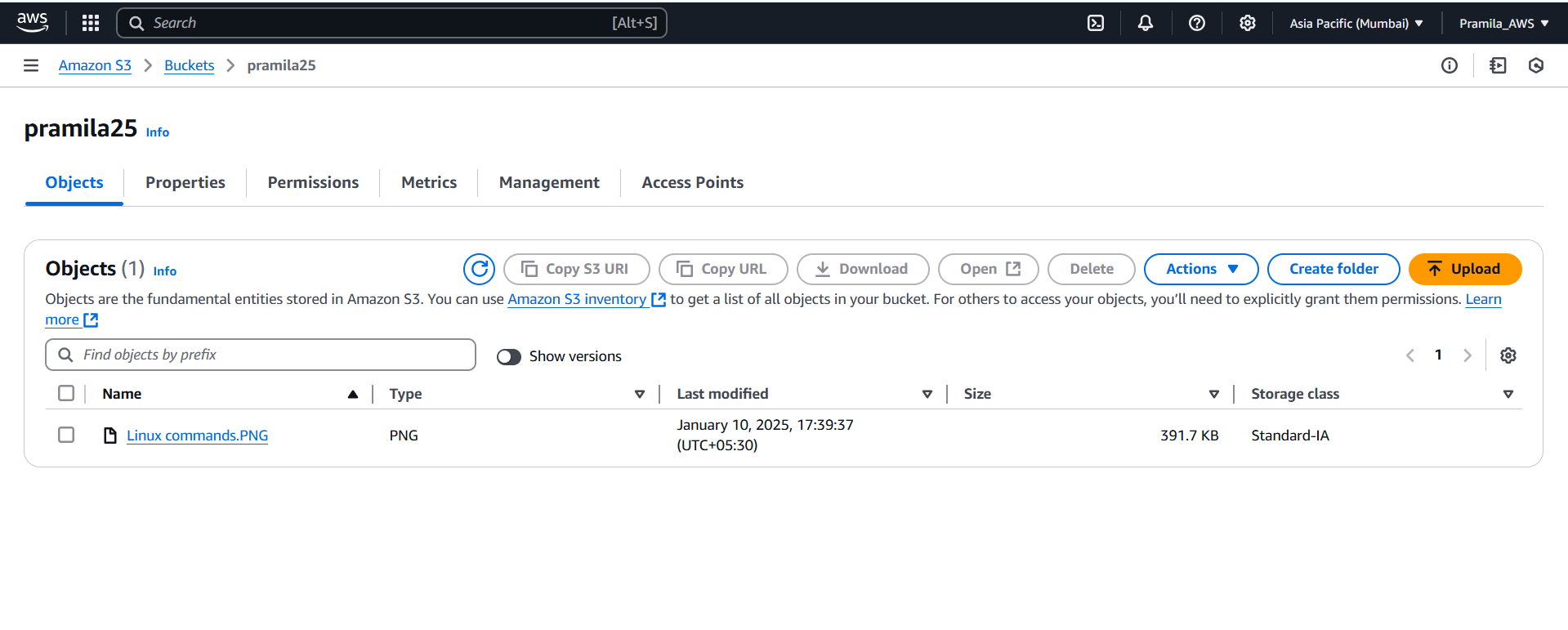
1. **Create bucket using CLI**

****

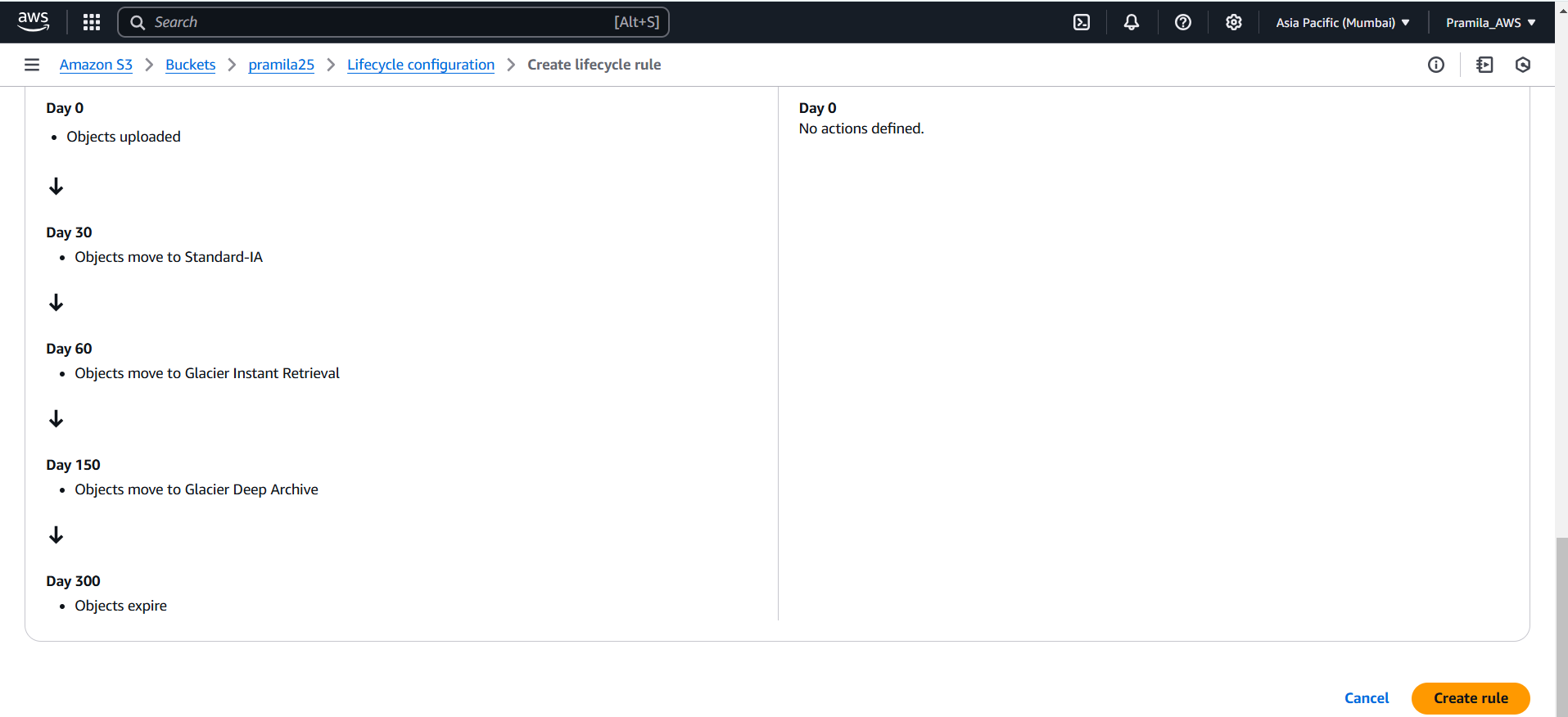
1. **List bucket using CLI**

****

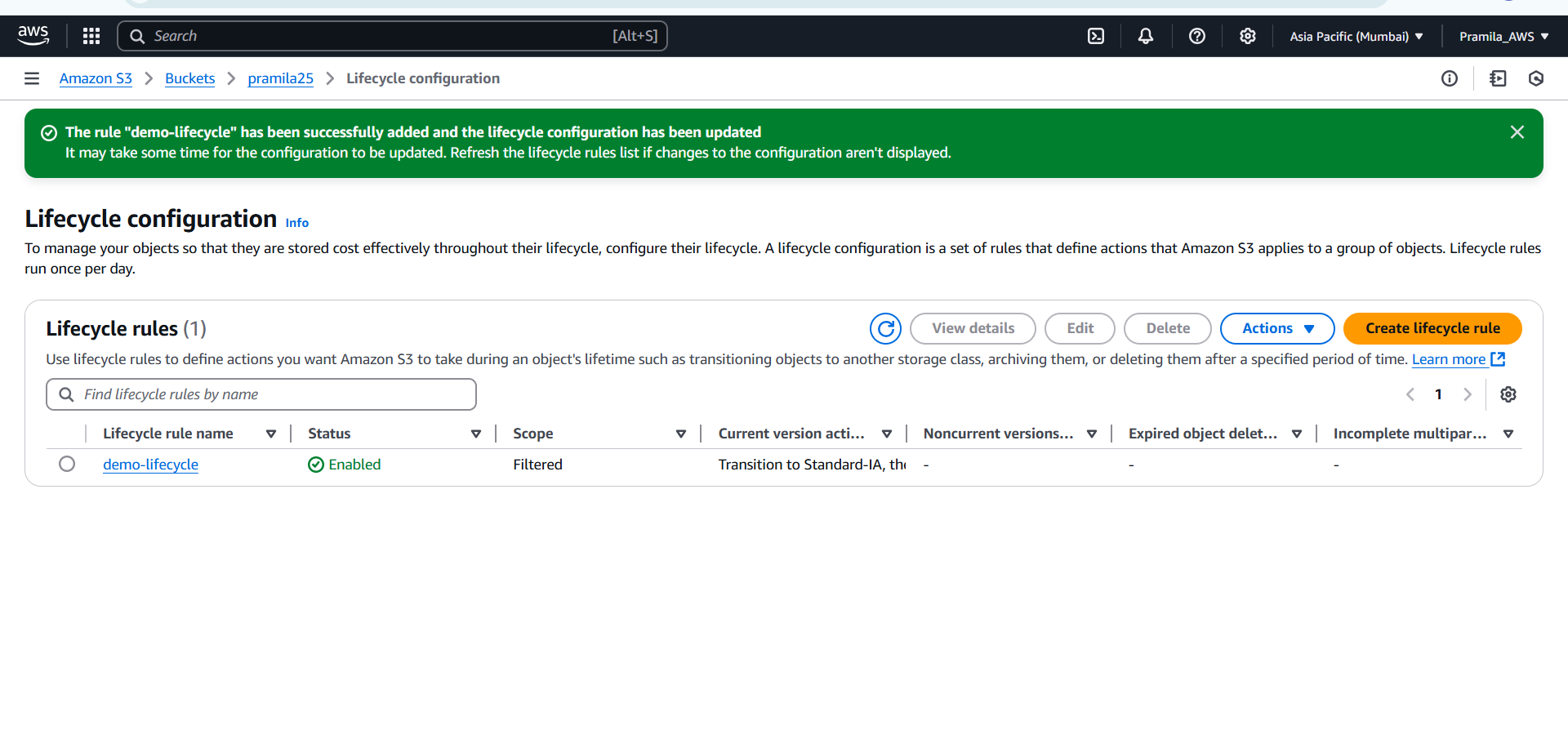
1. **By Default object goes to standard storage class, I have changed standard storage class to Standard infrequent access**

****

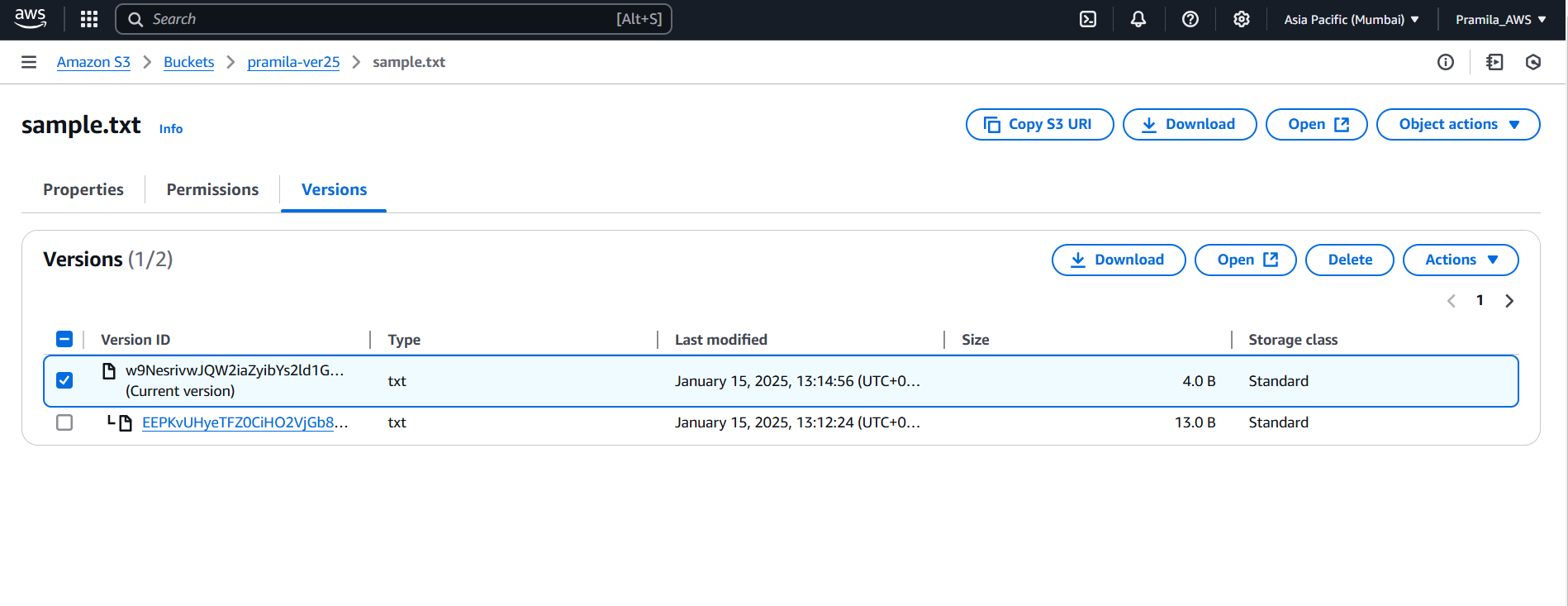
1. **Lifecycle rule for bucket**

****

1. **Created lifecycle rule for bucket “pramila25”**

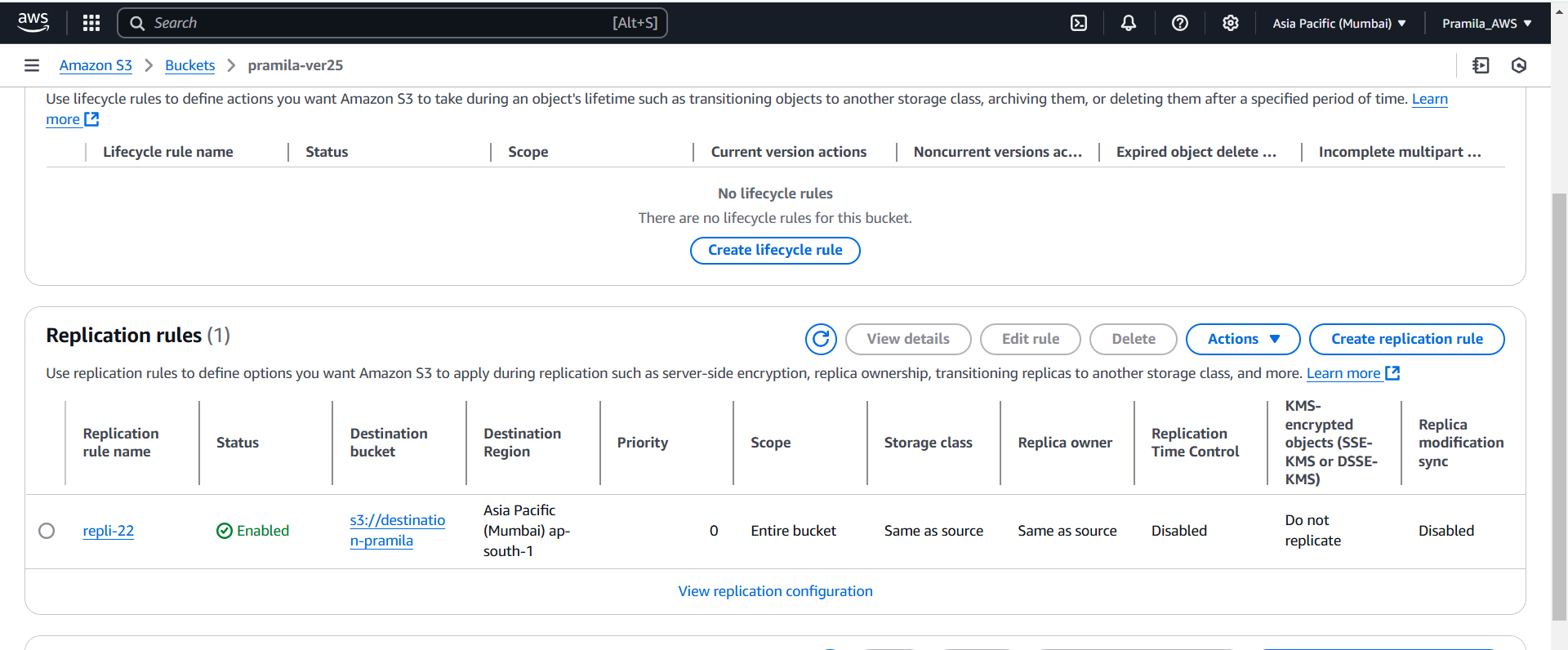
****

1. **Created versioning**

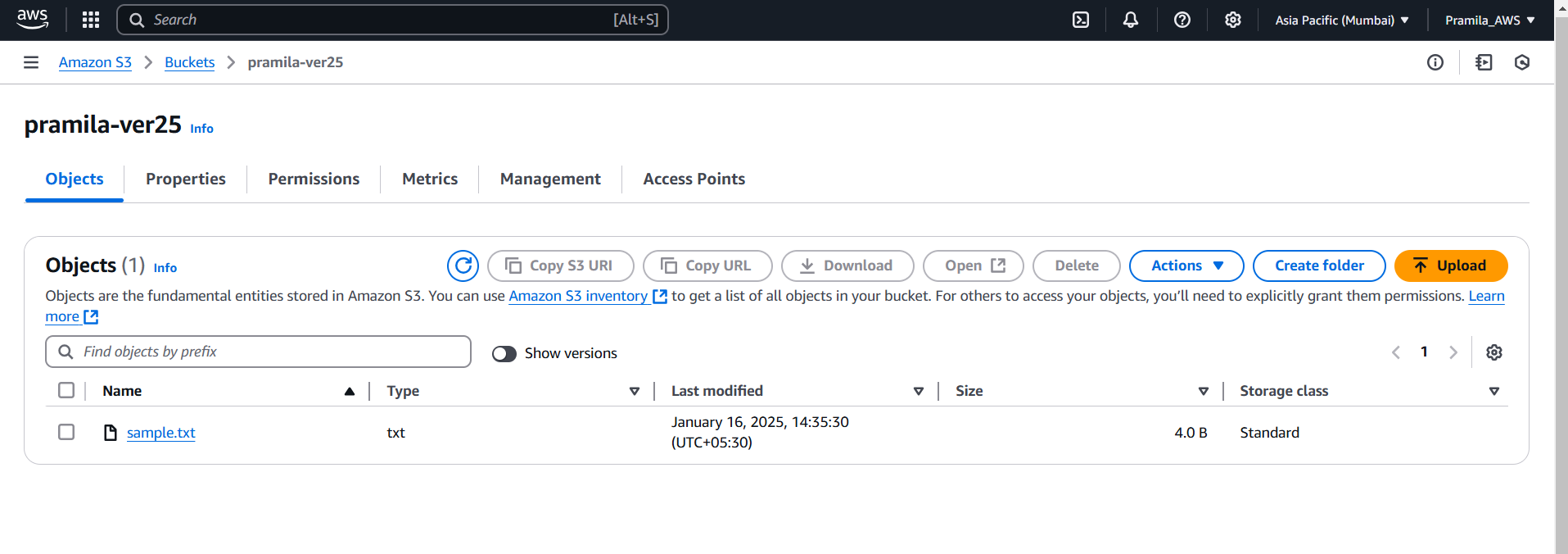
****

1. **Cross replication rule(CRR) – created replication rule at bucket level**

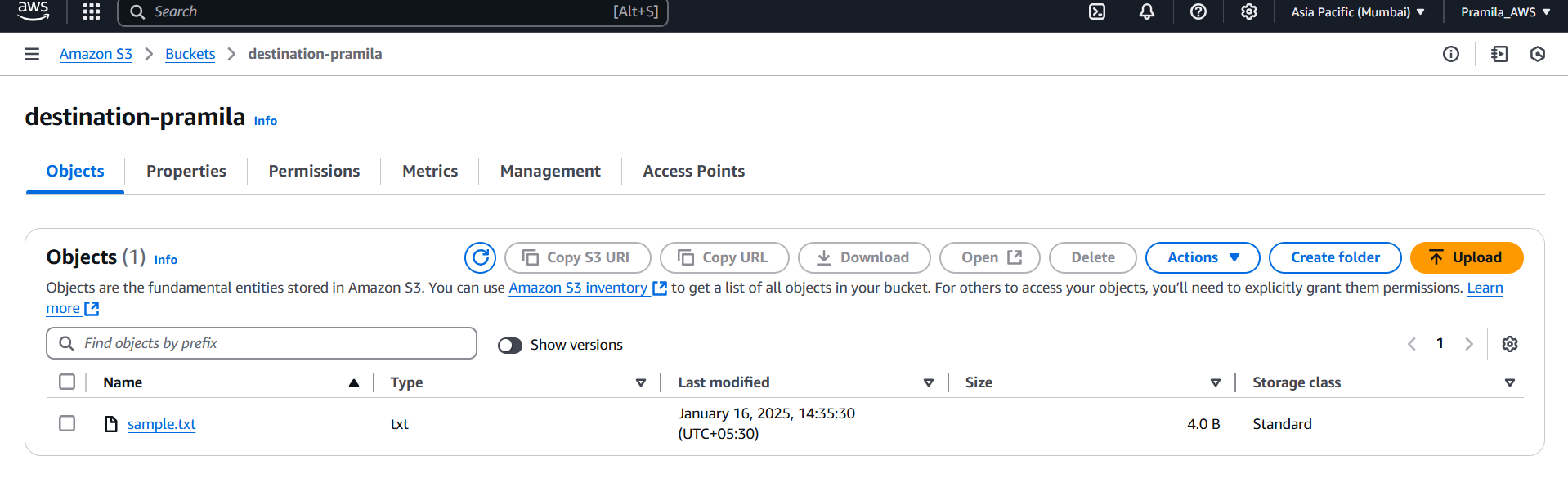
**Source bucket “pramila-ver25” and destination bucket “destination-pramila”**

****

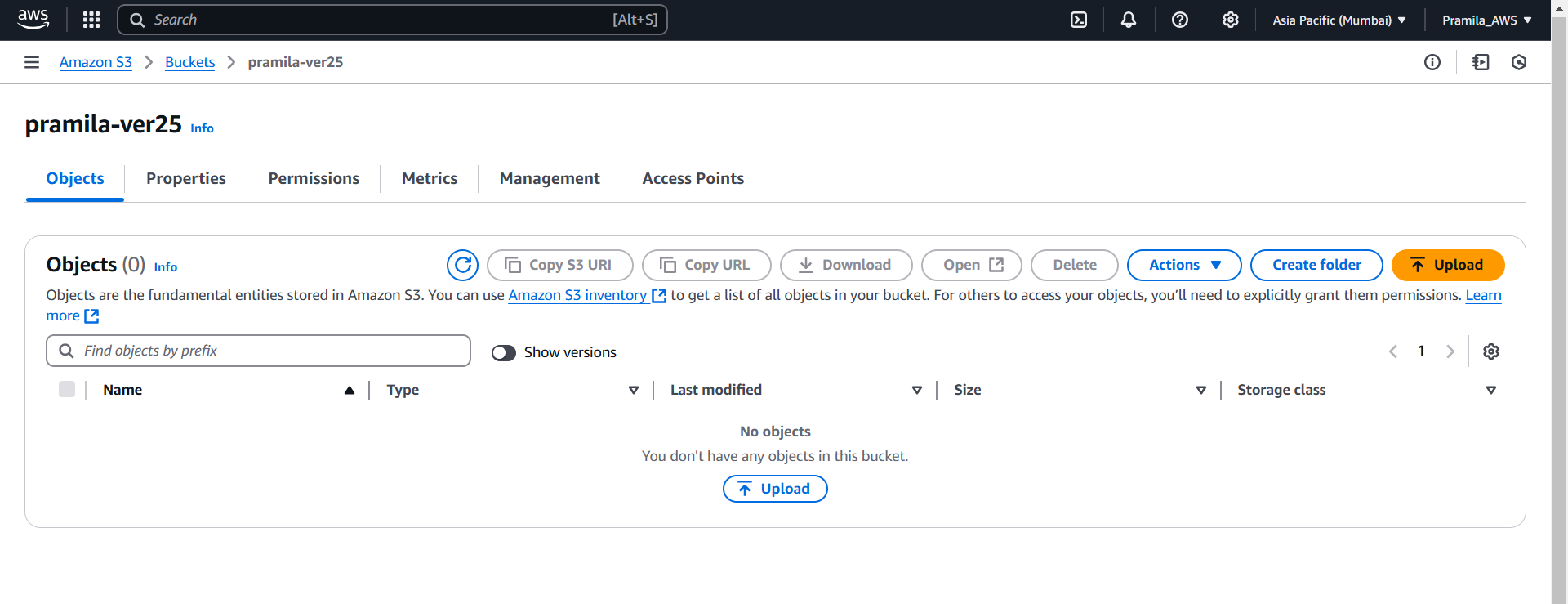
1. **Added object in source bucket “pramila-ver25”**

****

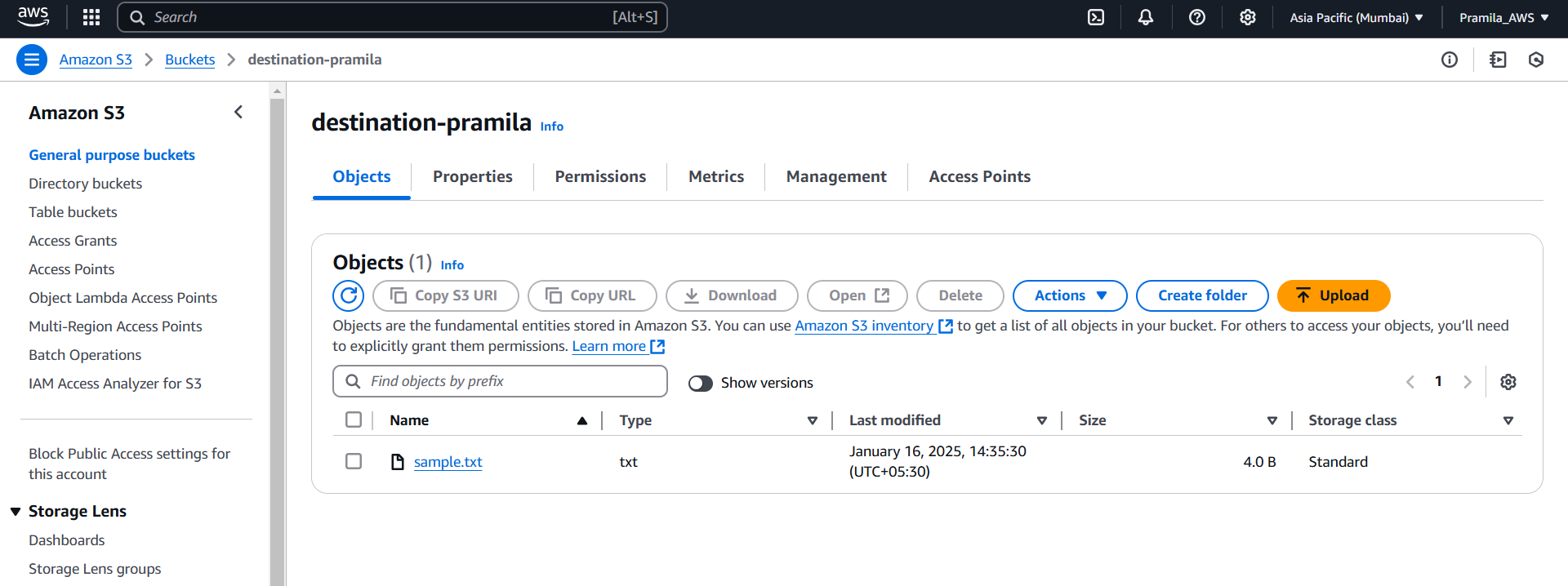
1. **Object get automatically added into destination bucket “destination-pramila”**

****

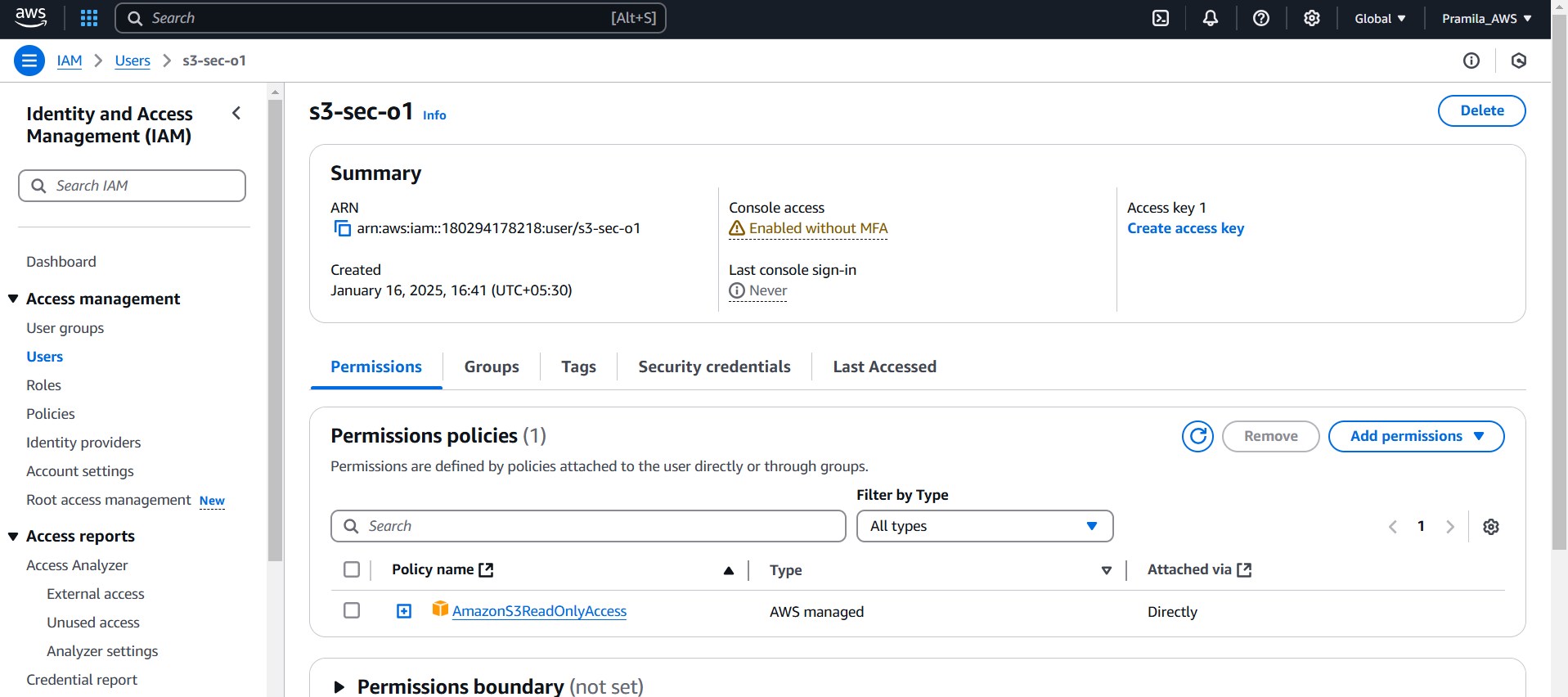
1. **Now I have deleted object from Source bucket “pramila-ver25”**

****

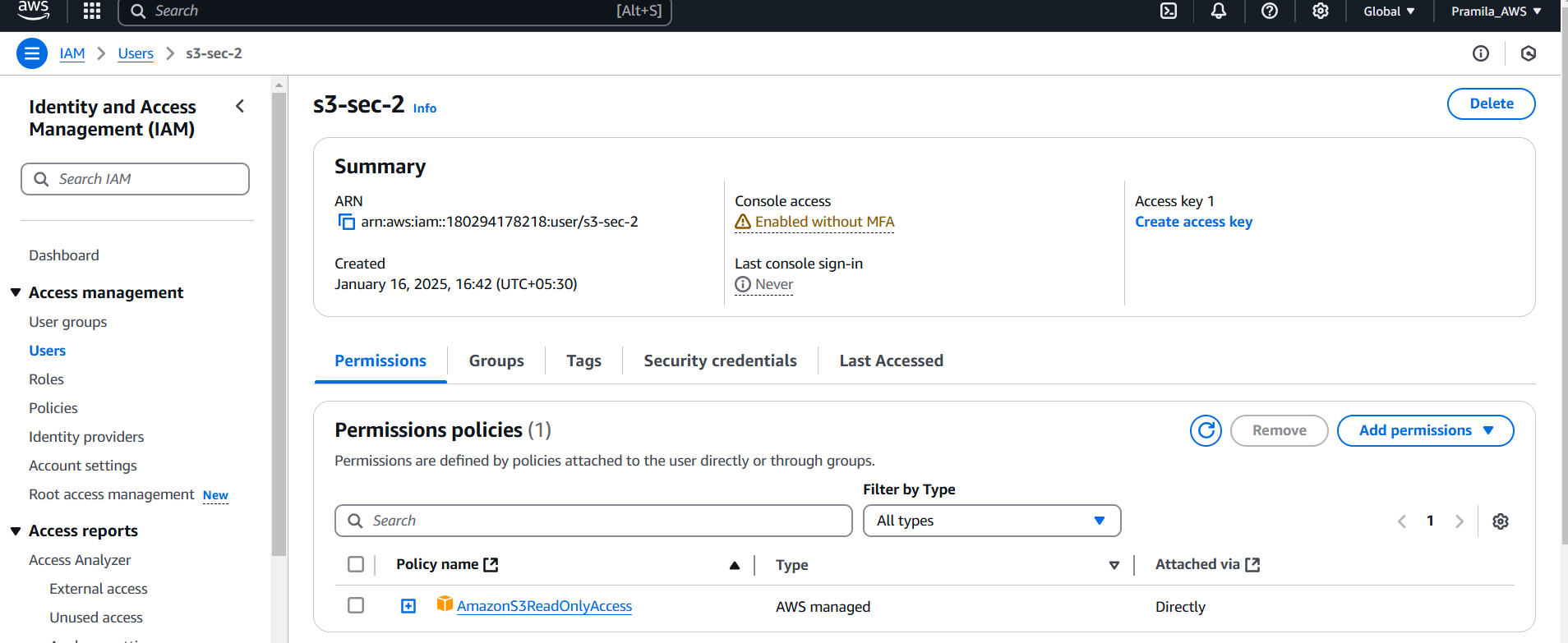
1. **Destination object remains as it is**

****

1. **Bucket level Policy, created “s3-sec-o1” IAM user with AWSS3readonly policy document**

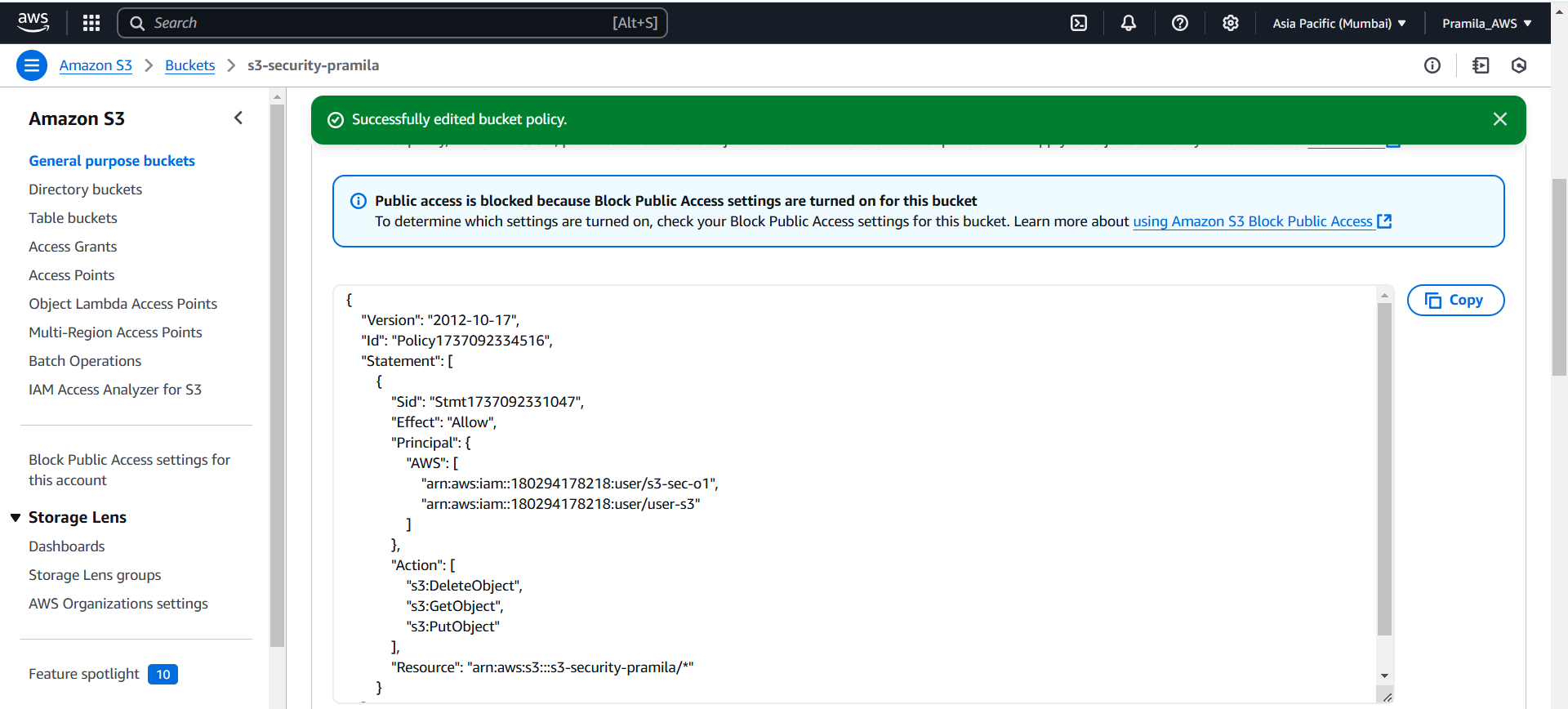
****

1. **Created “s3-sec-2” IAM user with AWSS3readonly policy document**

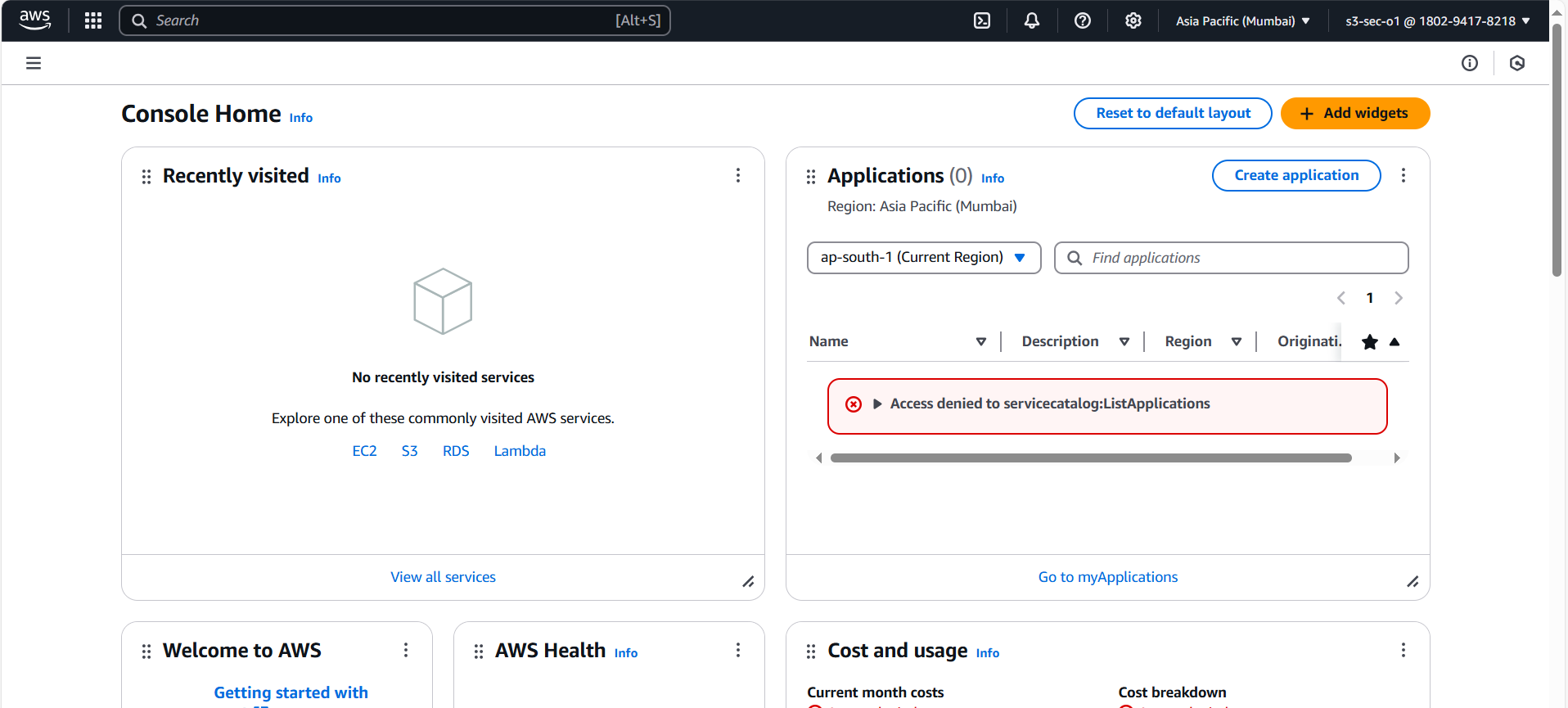
****

1. **Created bucket policy ,**

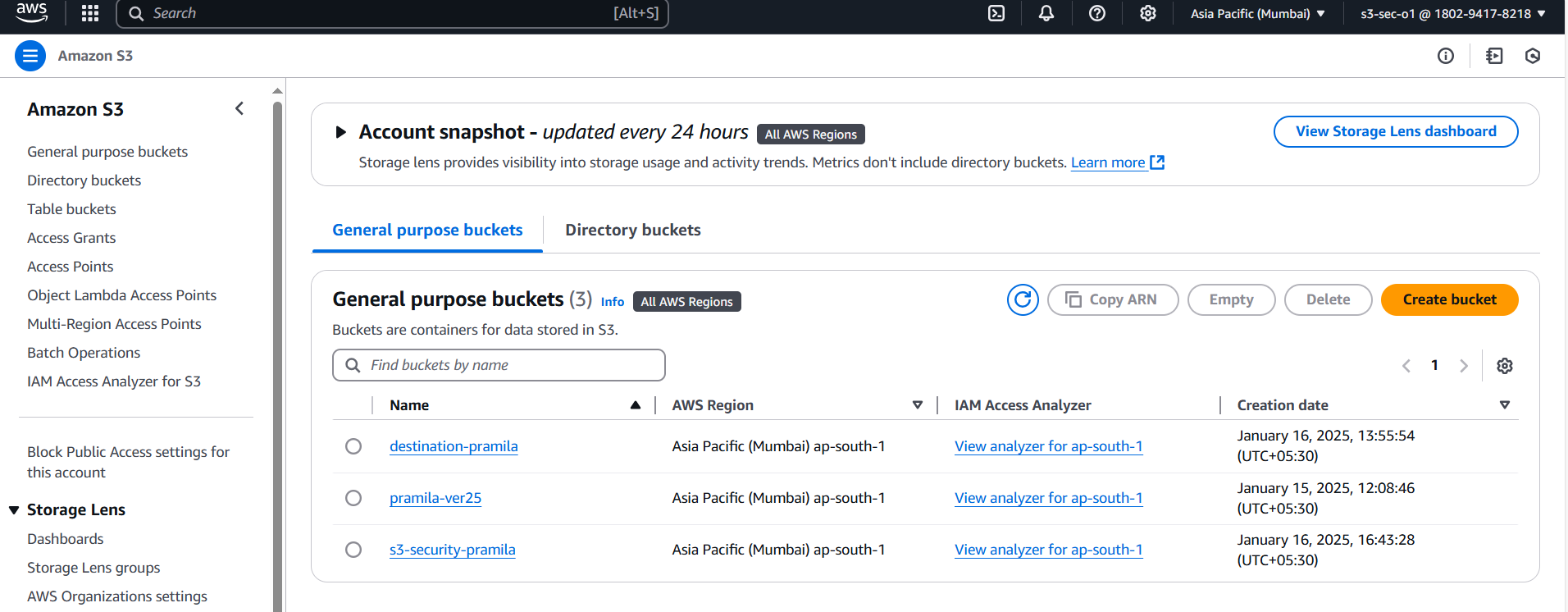
**Give get, put and delete access to “s3-sec-o1” IAM user and bucket s3-security-pramila**

****

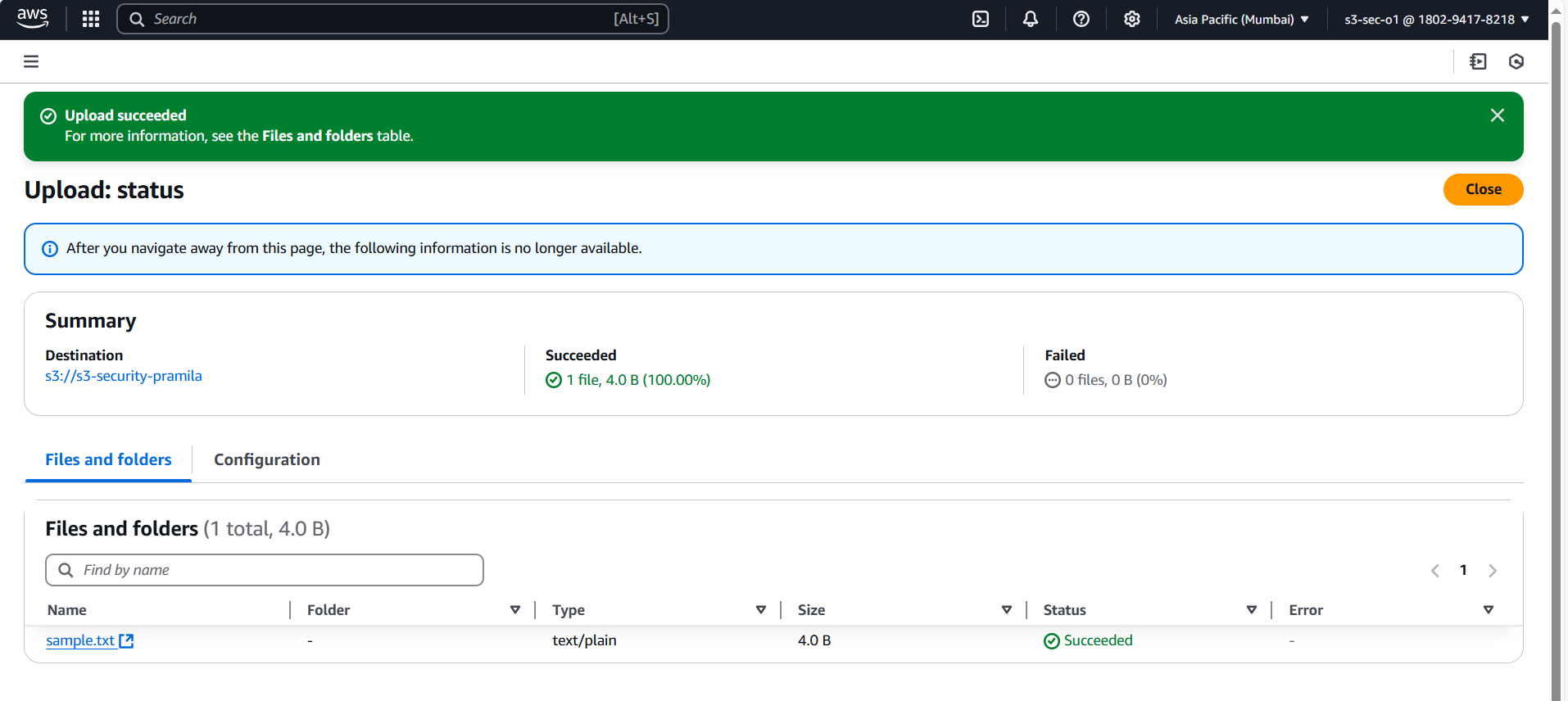
1. **Login using “s3-sec-o1” IAM user**

****

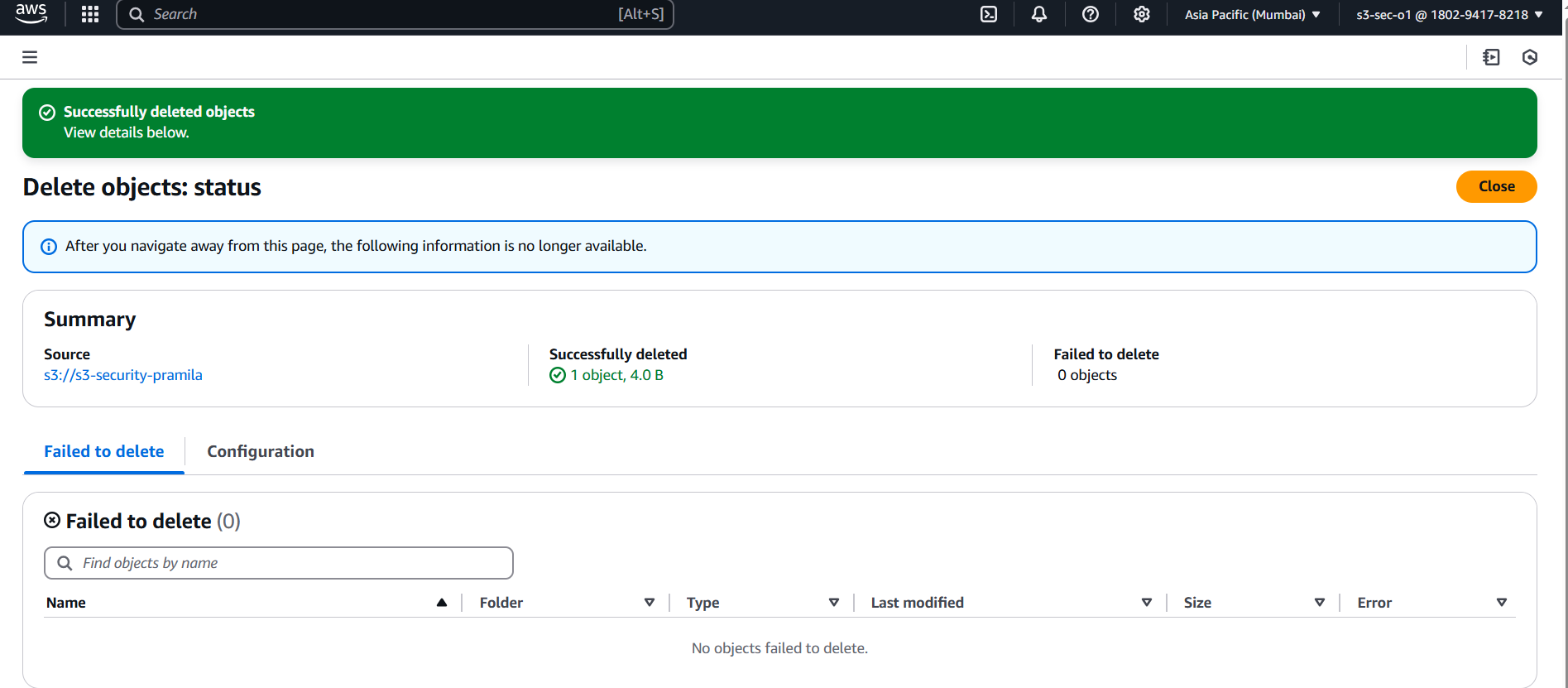
1. **“s3-sec-o1” IAM user able to see list of bucket**

****

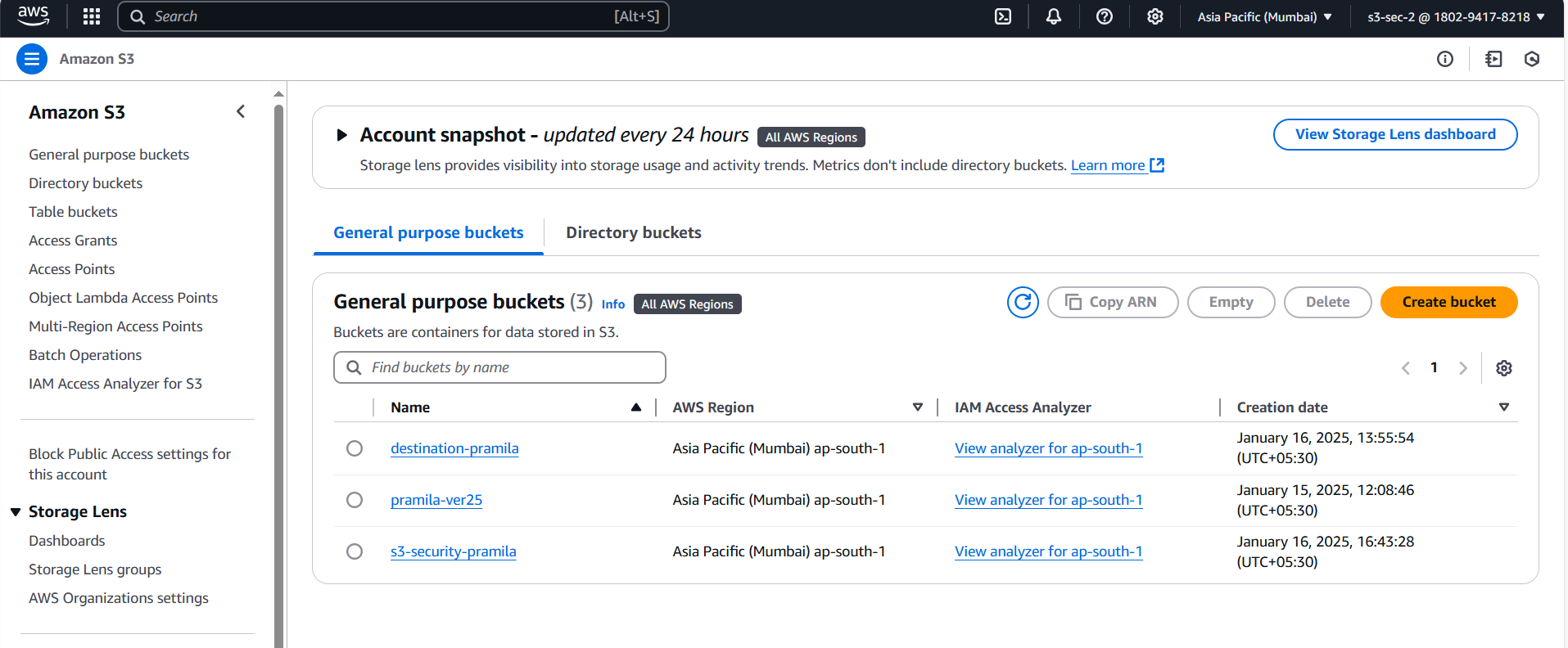
1. **Due to bucket policy “s3-sec-o1” IAM user able to upload object**



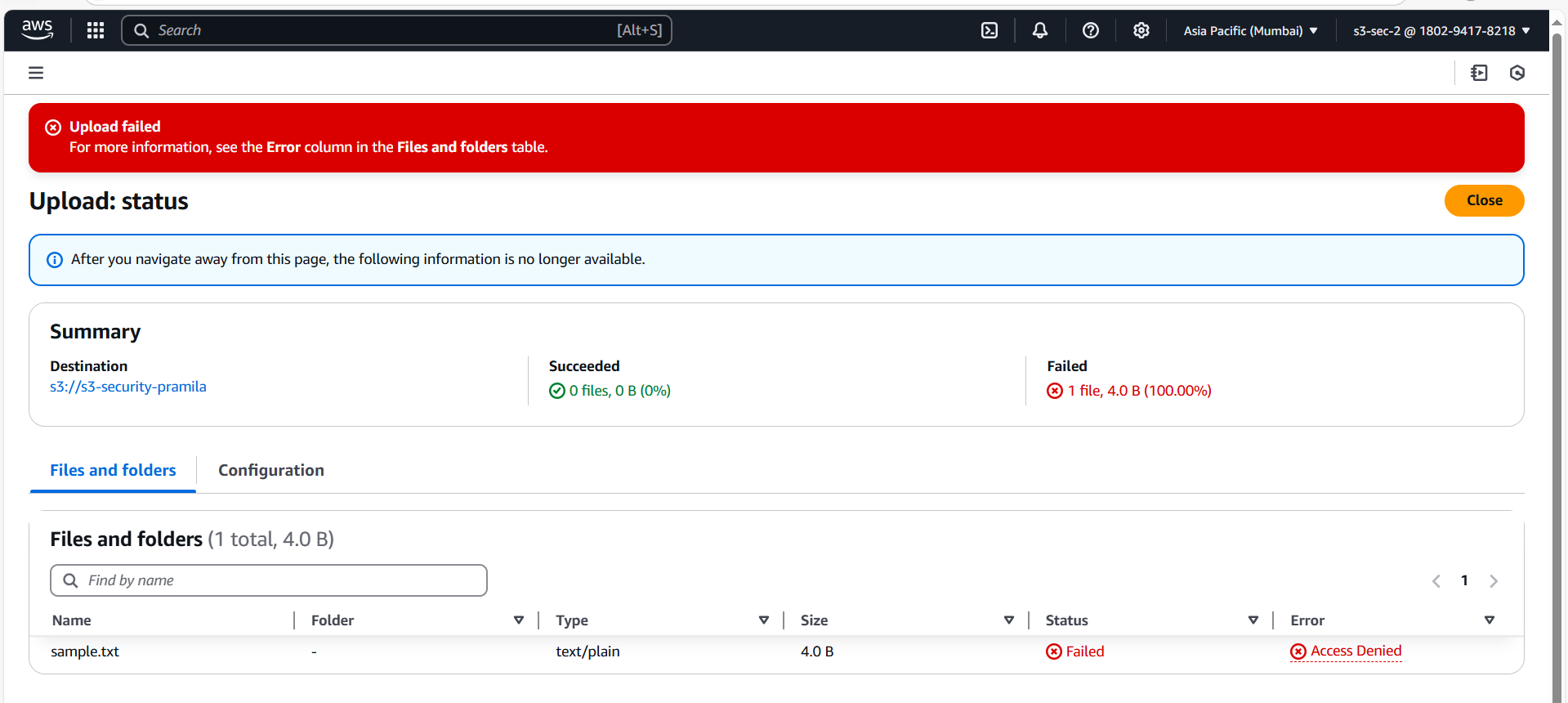
1. **Due to bucket policy “s3-sec-o1” IAM user able to delete object**

****

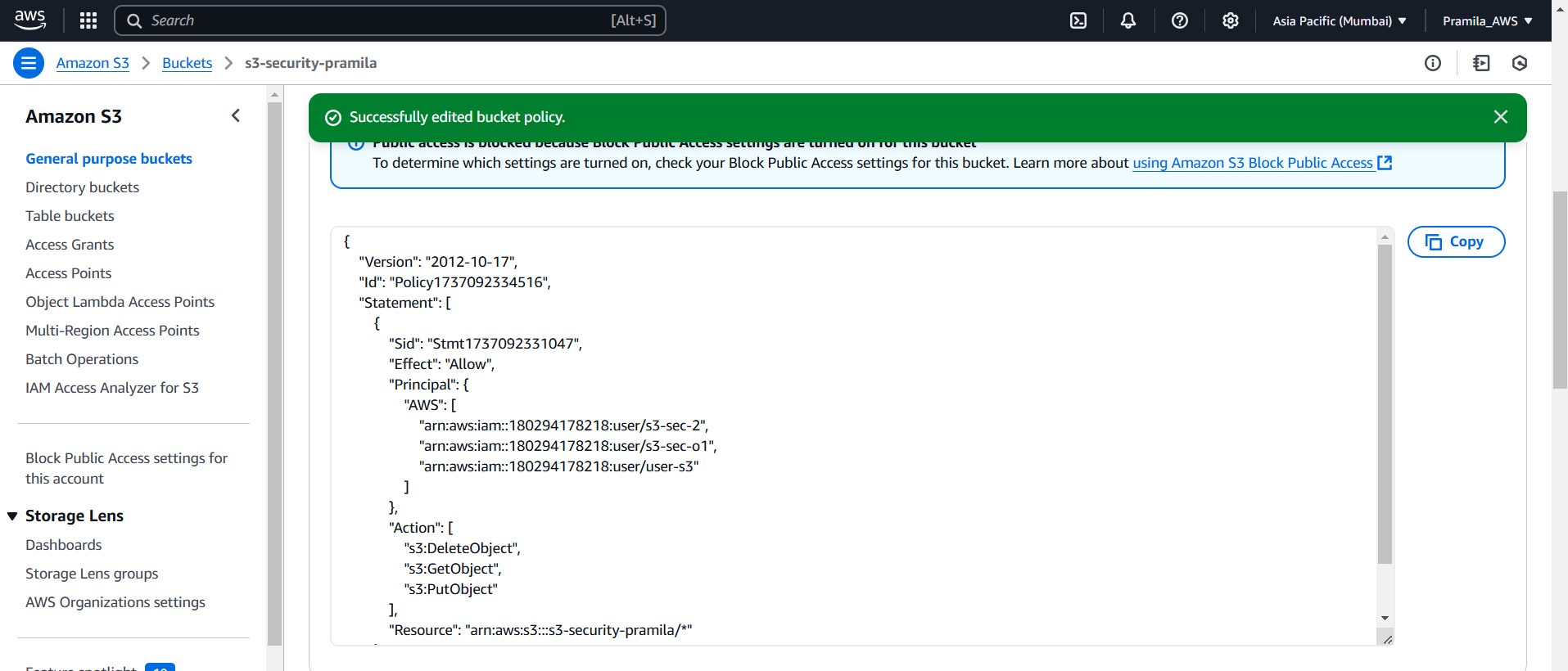
1. **Now login with “s3-sec-2” IAM user, “s3-sec-2” IAM user able to list of bucket due to IAM PD**

****

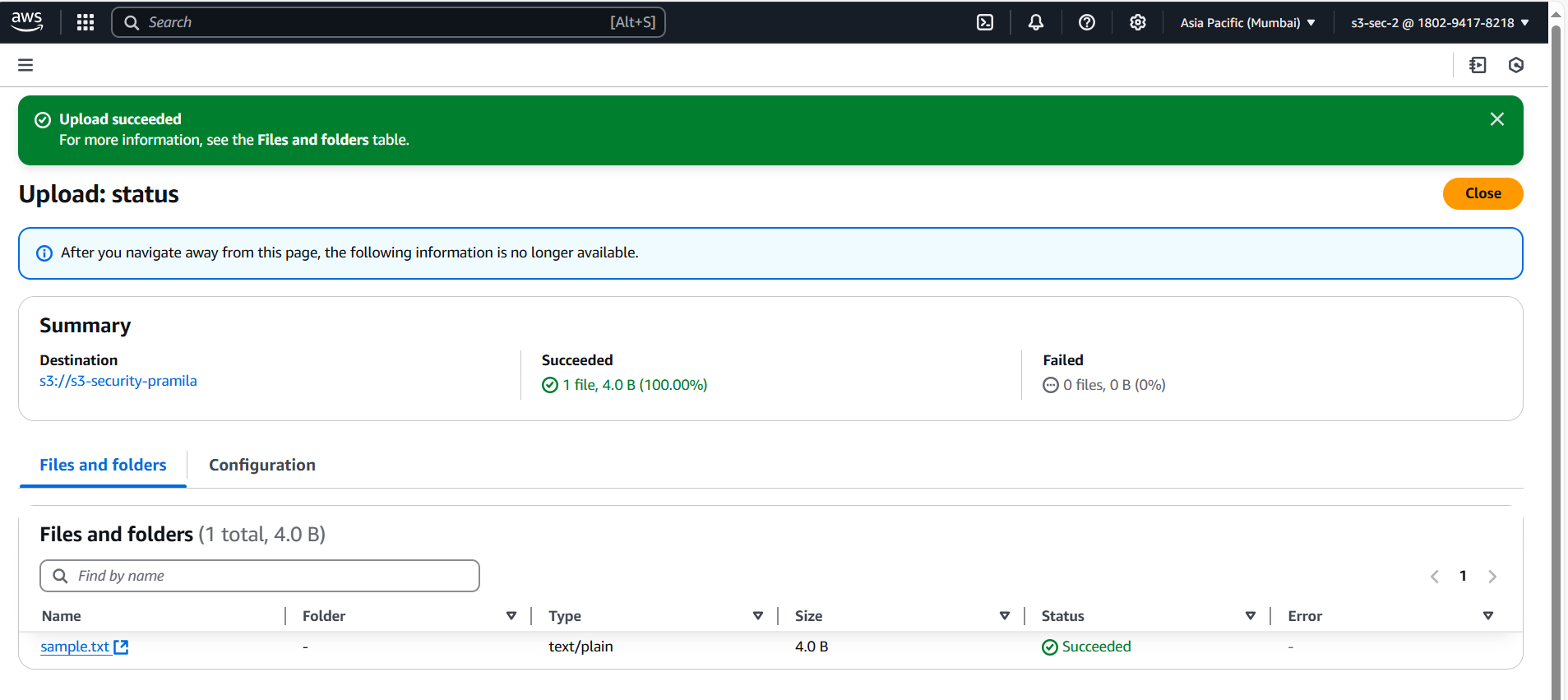
1. **But “s3-sec-2” IAM user not able to upload object in bucket**

****

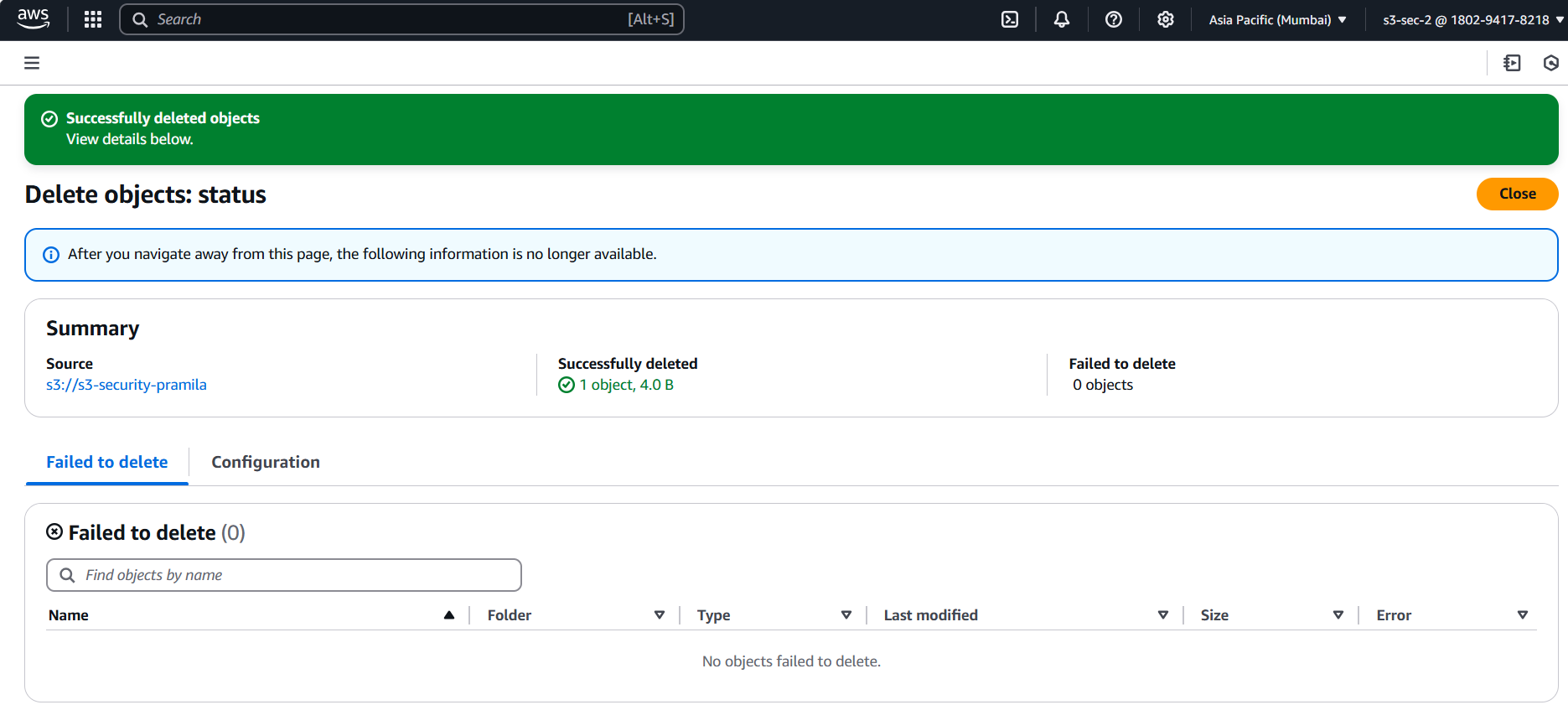
1. **Now we update bucket policy document and added get, put and delete access to “s3-sec-2” IAM user**

****

1. **Now “s3-sec-2” IAM user able to upload object in bucket**

****

1. **And also able to delete object from bucket’**

****