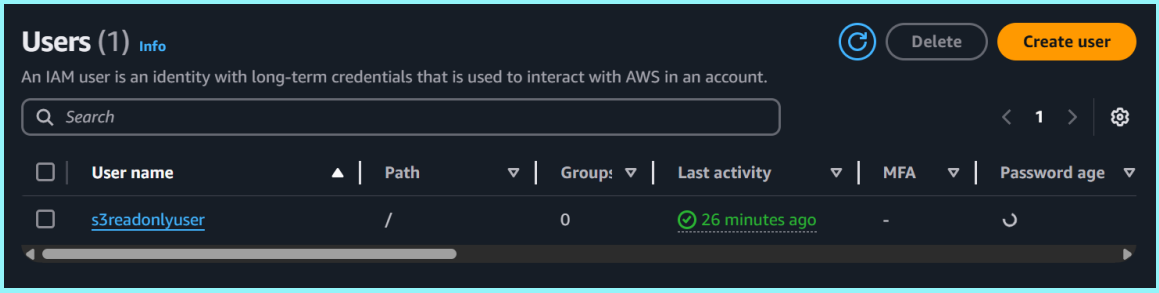
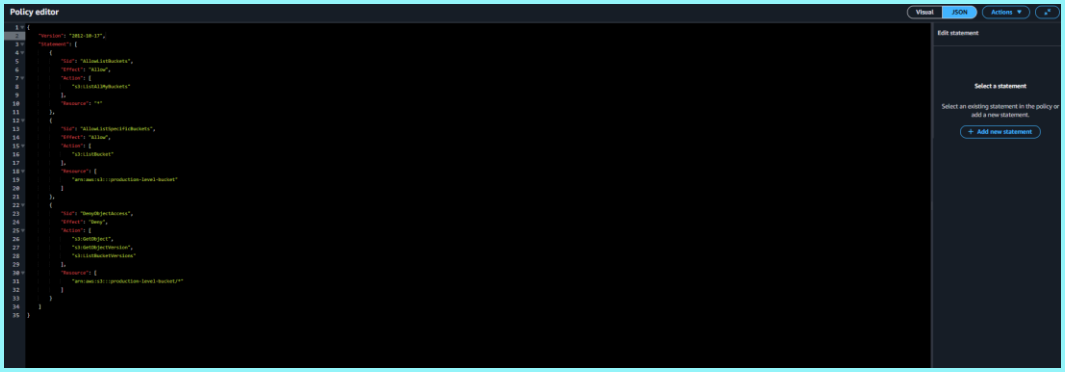
SECURE AWS S3 WITH IAM POLICIES AND ENCRYPTION

1. IAM Policies & User Setup

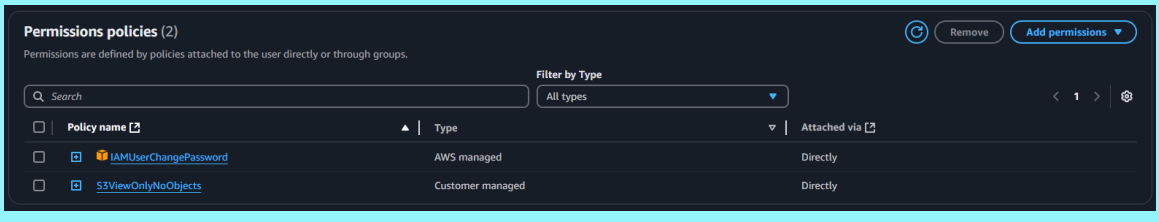
An IAM user named '**s3readonlyuser**' was created with programmatic and console access. A custom IAM policy was attached to grant limited access to an S3 bucket. This policy only allowed listing the bucket.



The custom IAM policy used is shown below:

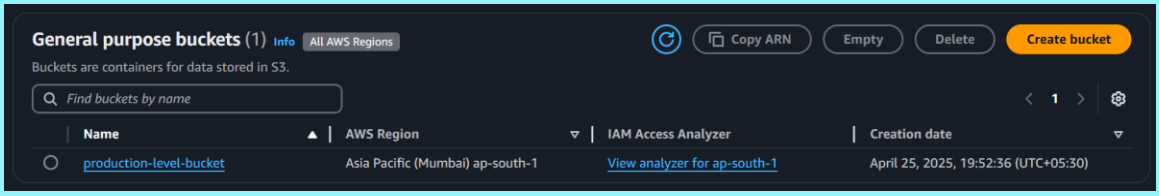


Attached Policy:



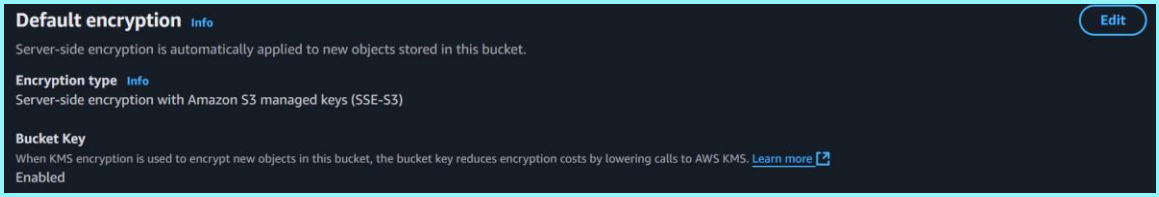
2. Secure S3 Bucket Configuration

An S3 bucket named '**production-level-bucket**' was created with all public access blocked. Bucket versioning was optionally enabled, and Server-side encryption with Amazon S3 managed keys (SSE-S3) was configured to protect data at rest.



3. Data Encryption on S3

Default encryption was enabled on the S3 bucket using SSE-S3 (AES-256 encryption). This ensured that all data stored in the bucket is encrypted automatically at rest.



5. IAM User Restrictions

The IAM user was configured with minimal permissions, enabling only viewing of bucket contents without any permissions to modify, delete, or upload files. Below is a summary of the user's permissions:

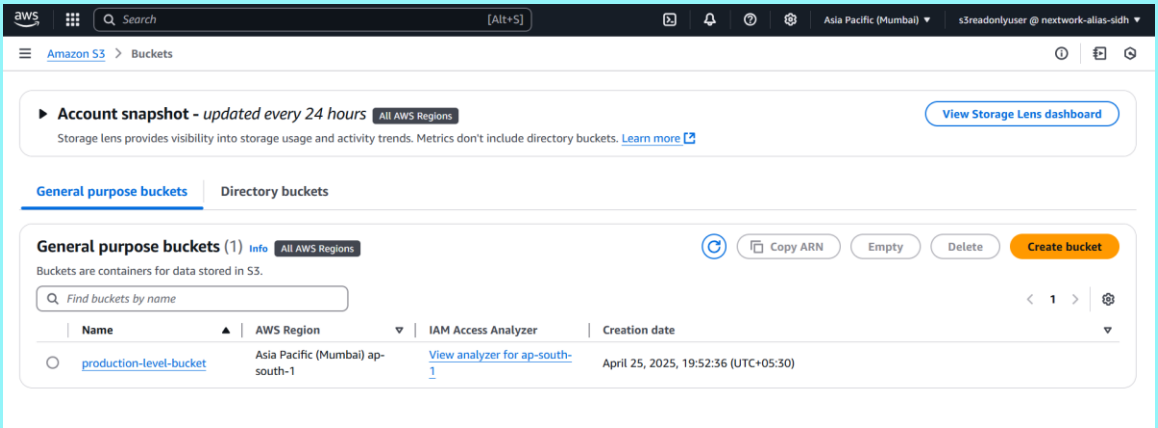
Feature	Permission	Allowed
View Bucket	s3:ListBucket	✅ Yes
Download Files	s3:GetObject	❌ No
Upload Files	s3:PutObject	❌ No
Delete Files	s3:DeleteObject	❌ No
Modify Bucket	s3:PutBucketPolicy	❌ No

6. Testing IAM User Access

The IAM user's access was tested to confirm the security policies.

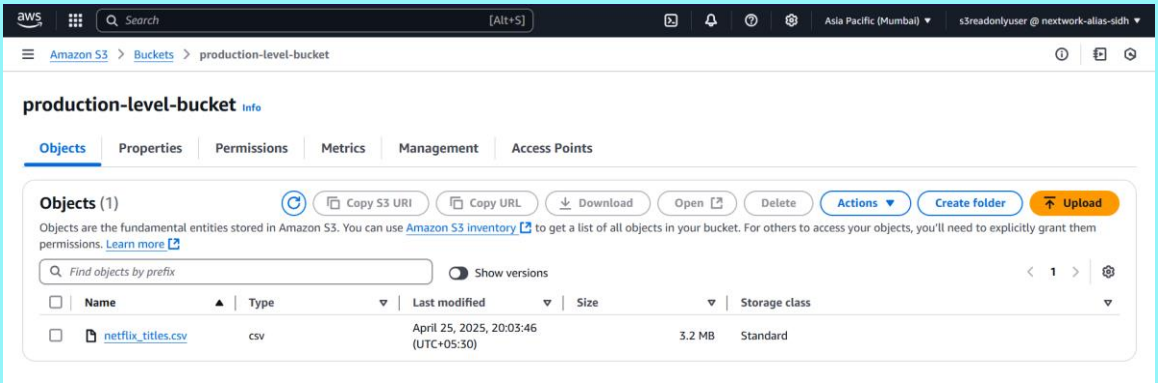
Test Case 1: Listing Buckets

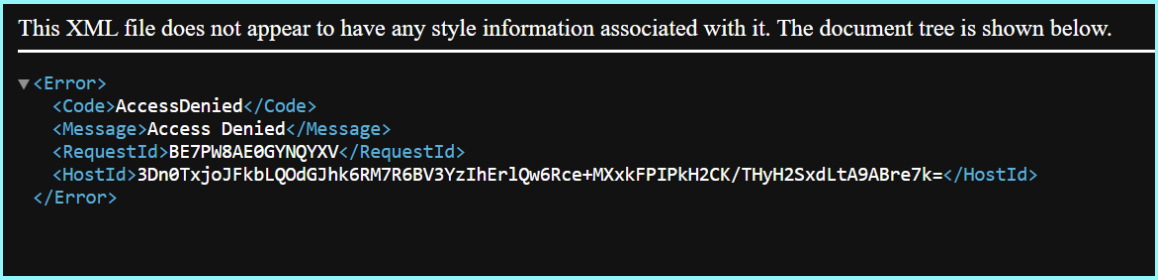
The user was able to list all S3 buckets in the account. This access was confirmed from the console.



Test Case 2: Accessing Objects in the Bucket

The user attempted to access an object inside the bucket but received an 'Access Denied' error, as expected due to the bucket policy restrictions.





Summary of IAM User Behavior

Feature	Status	Remarks
List all buckets	✅ Yes	Allowed by default IAM policy
View objects in the bucket	❌ No	Denied by bucket policy
Download objects	❌ No	Access Denied
Upload/Delete objects	❌ No	Access Denied
Modify bucket settings	❌ No	Access Denied