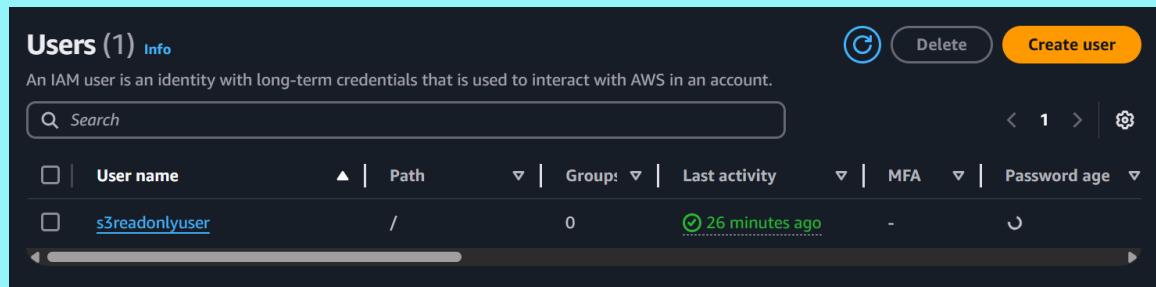


# SECURE AWS S3 WITH IAM POLICIES AND ENCRYPTION

## 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 screenshot shows the AWS IAM 'Users' page with one user listed:

User name	Path	Groups	Last activity	MFA	Password age
s3readonlyuser	/	0	26 minutes ago	-	

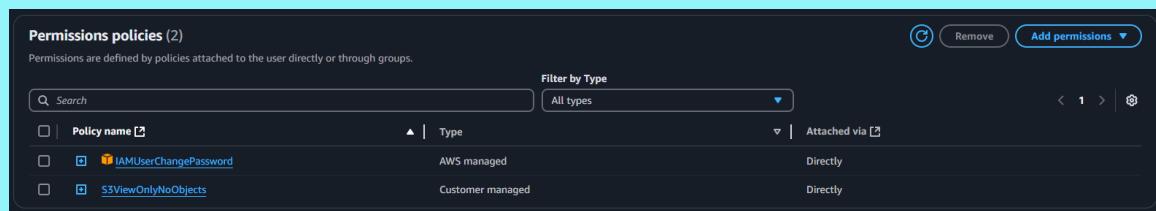
The custom IAM policy used is shown below:



The screenshot shows the AWS IAM 'Policy editor' page with the following JSON policy code:

```
1. { "Version": "2012-10-17", "Statement": [ 2. { "Effect": "Allow", "Action": "AmazonS3ListBucket", "Resource": "arn:aws:s3:::production-bucket", "Condition": { "StringEquals": "s3readonlyuser", "StringNotLike": "arn:aws:s3:::production-*" } }, 3. { "Effect": "Allow", "Action": "AmazonS3ListBucket", "Resource": "arn:aws:s3:::test", "Condition": { "StringEquals": "s3readonlyuser", "StringNotLike": "arn:aws:s3:::production-*" } }, 4. { "Effect": "Allow", "Action": "AmazonS3ListBucket", "Resource": "arn:aws:s3:::test", "Condition": { "StringEquals": "s3readonlyuser", "StringNotLike": "arn:aws:s3:::production-*" } } ] }
```

## Attached Policy:

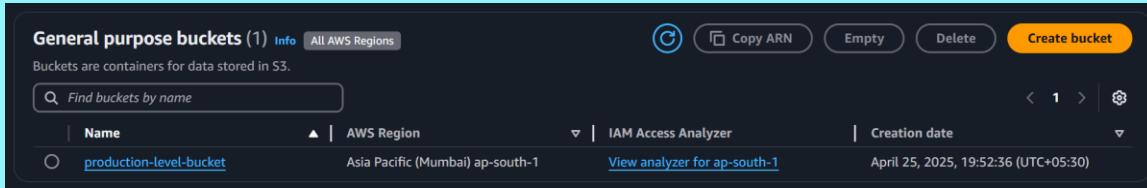


The screenshot shows the AWS IAM 'Permissions policies' page with two attached policies:

Policy name	Type	Attached via
IAMUserChangePassword	AWS managed	Directly
S3ViewOnlyNoObjects	Customer managed	Directly

## 2. Secure S3 Bucket Configuration

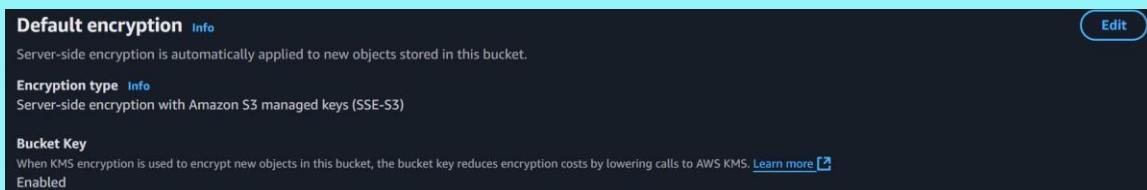
An S3 bucket named '**production-level-bucket**' was created with all public access blocked. Bucket versioning was optionally enabled, and Server-side encryption with Amazon S3 managed keys (SSE-S3) was configured to protect data at rest.



The screenshot shows the AWS S3 console interface. At the top, it says 'General purpose buckets (1) Info All AWS Regions'. Below that, a message says 'Buckets are containers for data stored in S3.' There is a search bar labeled 'Find buckets by name'. The main table has columns for 'Name', 'AWS Region', 'IAM Access Analyzer', and 'Creation date'. One row is visible for the bucket 'production-level-bucket', which was created in 'Asia Pacific (Mumbai)' on 'ap-south-1' on 'April 25, 2025, 19:52:36 (UTC+05:30)'. Action buttons include 'Copy ARN', 'Empty', 'Delete', and 'Create bucket'.

## 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.



The screenshot shows the 'Encryption' section of the S3 bucket configuration. It includes three sections: 'Default encryption' (Info), 'Encryption type' (Info), and 'Bucket Key'. The 'Default encryption' section states 'Server-side encryption is automatically applied to new objects stored in this bucket.' The 'Encryption type' section states 'Server-side encryption with Amazon S3 managed keys (SSE-S3)'. The 'Bucket Key' section states 'When KMS encryption is used to encrypt new objects in this bucket, the bucket key reduces encryption costs by lowering calls to AWS KMS.' A link 'Learn more' is provided, and the status is 'Enabled'.

## 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	s3GetObject	✗ No
Upload Files	s3PutObject	✗ No
Delete Files	s3DeleteObject	✗ No
Modify Bucket	s3PutBucketPolicy	✗ 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.

The screenshot shows the AWS S3 Buckets page. At the top, there's an account snapshot and a link to the Storage Lens dashboard. Below that, tabs for 'General purpose buckets' and 'Directory buckets' are shown, with 'General purpose buckets' being selected. A table lists one bucket:

Name	AWS Region	IAM Access Analyzer	Creation date
production-level-bucket	Asia Pacific (Mumbai) ap-south-1	<a href="#">View analyzer for ap-south-1</a>	April 25, 2025, 19:52:36 (UTC+05:30)

Actions available for the bucket include Copy ARN, Empty, Delete, and Create bucket.

## 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.

The screenshot shows the AWS S3 Object details page for the file 'netflix\_titles.csv'. The file was uploaded on April 25, 2025, at 20:03:46 (UTC+05:30) and is 3.2 MB in size, stored in the Standard storage class. The 'Actions' menu is visible, showing options like Copy S3 URI, Copy URL, Download, Open, Delete, Actions, Create folder, and Upload.

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

```

▼<Error>
  <Code>AccessDenied</Code>
  <Message>Access Denied</Message>
  <RequestId>BE7PW8AE0GYNQYX</RequestId>
  <HostId>3Dn0TxjoJFkbLQ0dGJhk6RM7R6BV3YzIhEr1Qw6Rce+MXxkFPIPkH2CK/THyH2SxdLtA9ABre7k=</HostId>
</Error>

```

## 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