AWS S3 Security Project

By Syeda Umaima Abeer

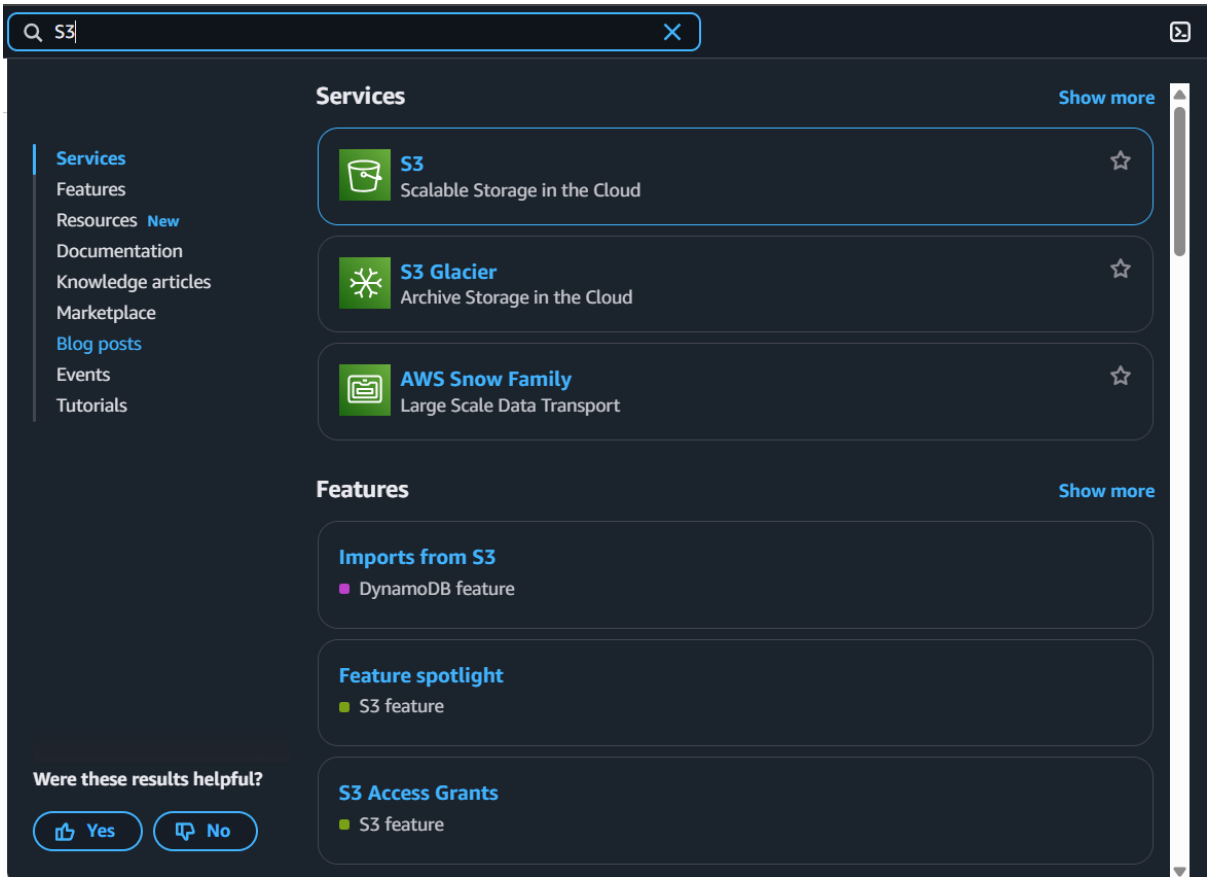
July 2025

This project demonstrates how to securely configure an Amazon S3 bucket using AWS Identity and Access Management (IAM), bucket policies, server-side encryption, and logging. The goal was to apply core cloud security principles like least privilege access, data encryption at rest, version control, and access monitoring using AWS native tools.

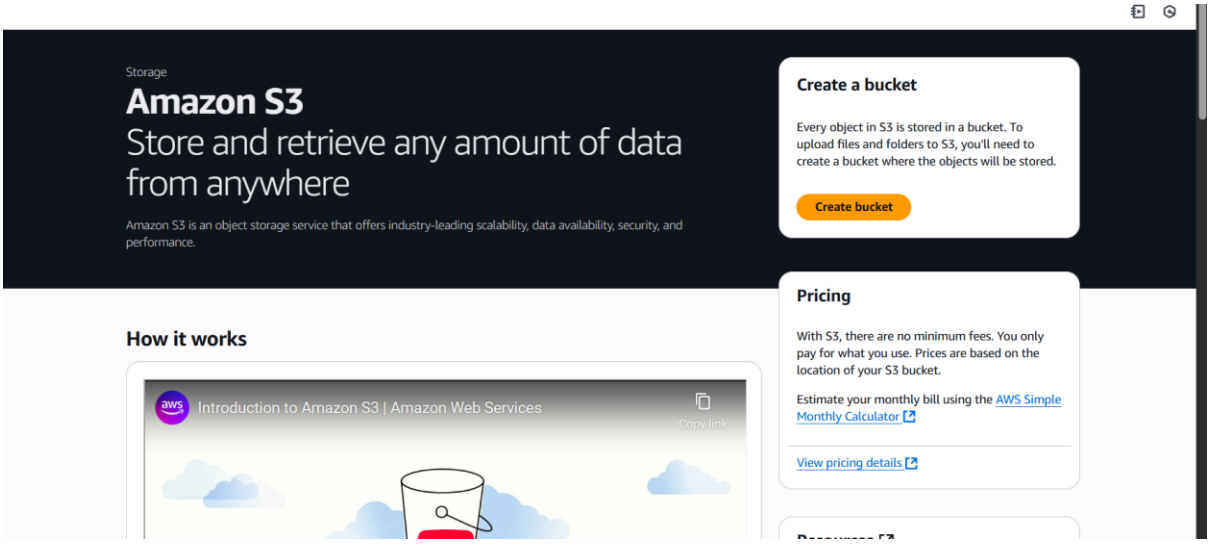
Table of Contents (Optional)

➔Create a New S3 Bucket

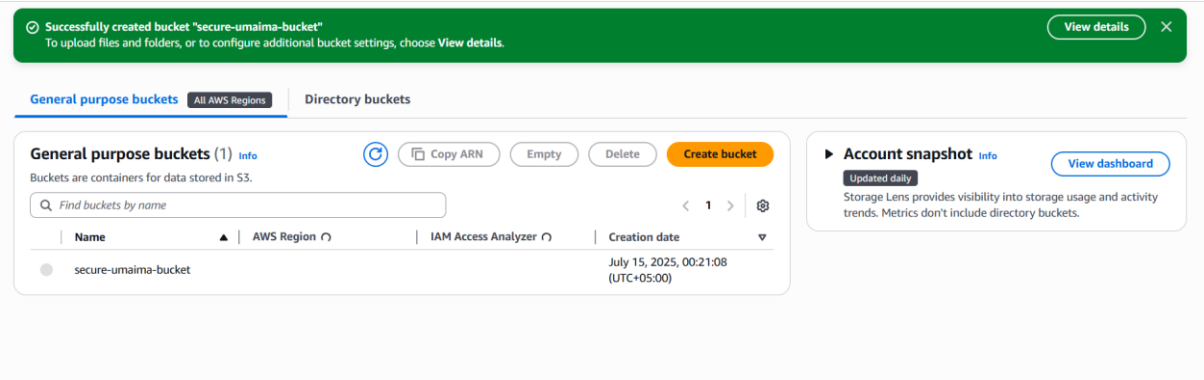
Opened the S3 service from the AWS Management Console to start bucket creation.



Named the bucket and selected region. Disabled public access to ensure security.

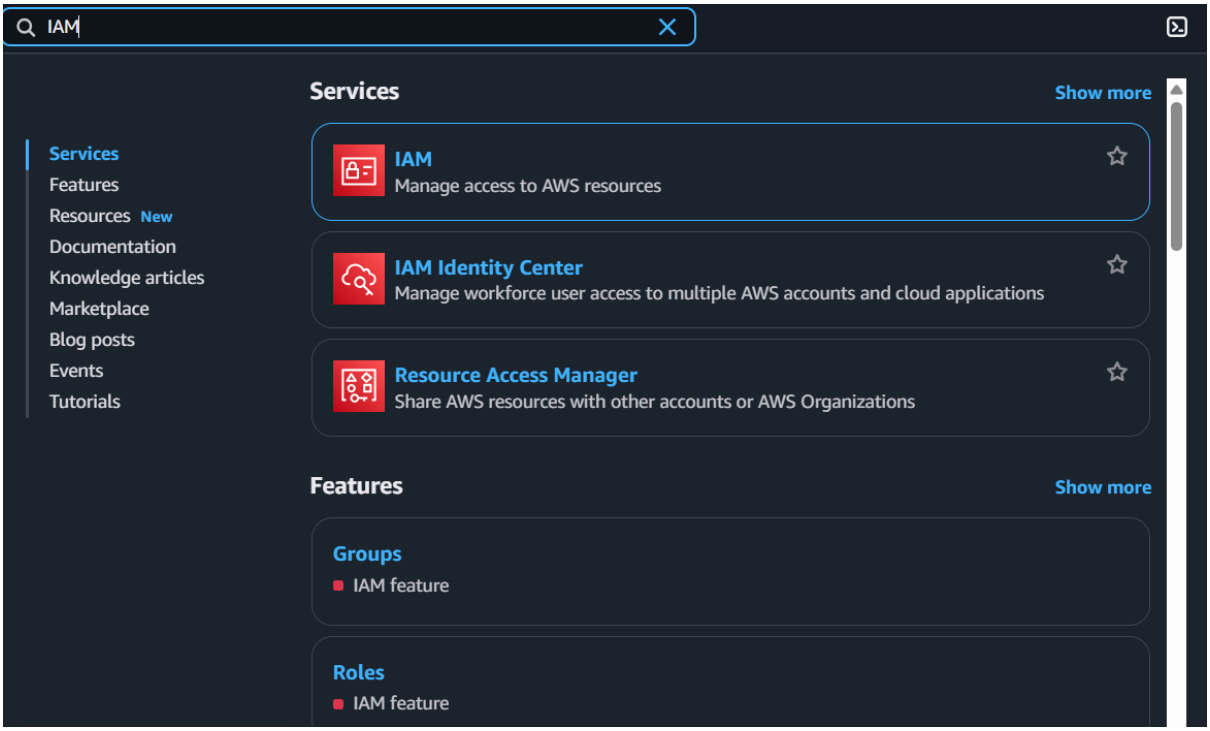


The secure S3 bucket was created and is now listed in the console.

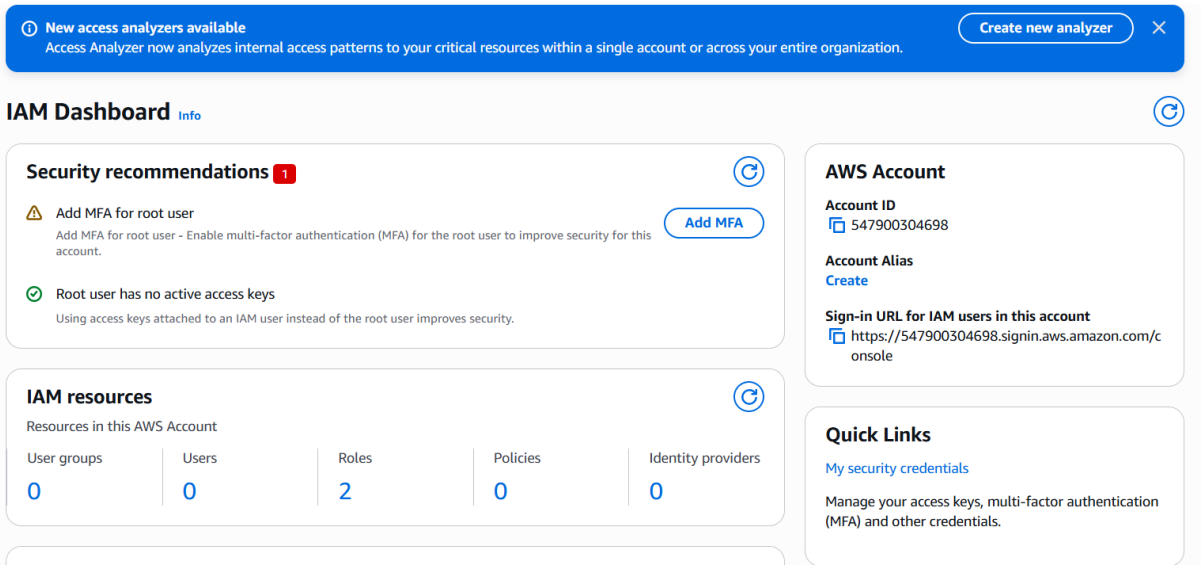


Create IAM User with Limited Permissions

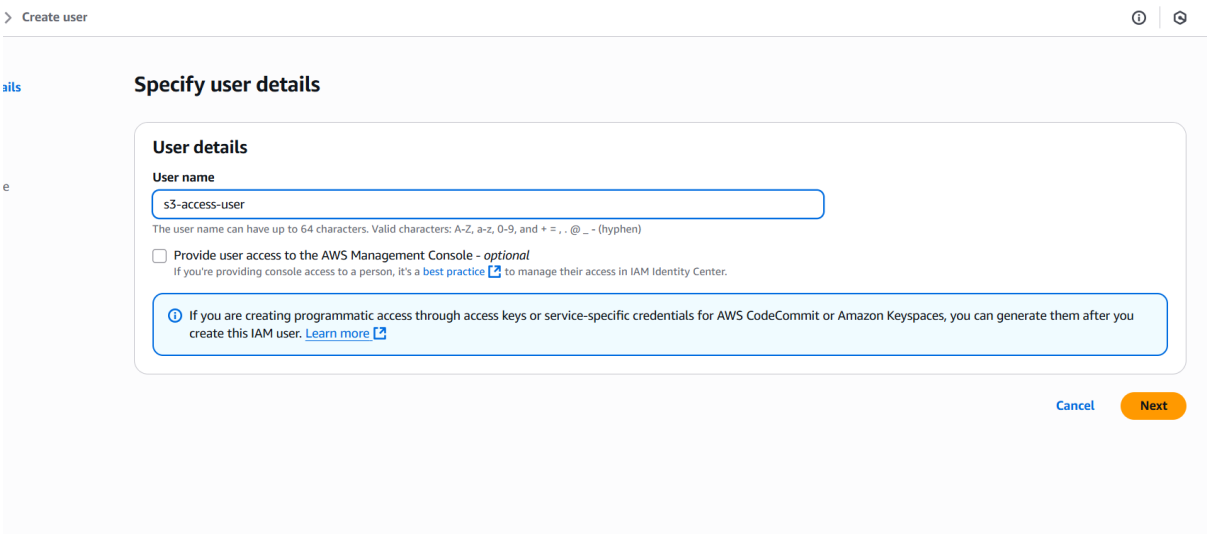
Opened the AWS IAM service from the console to create a new user.



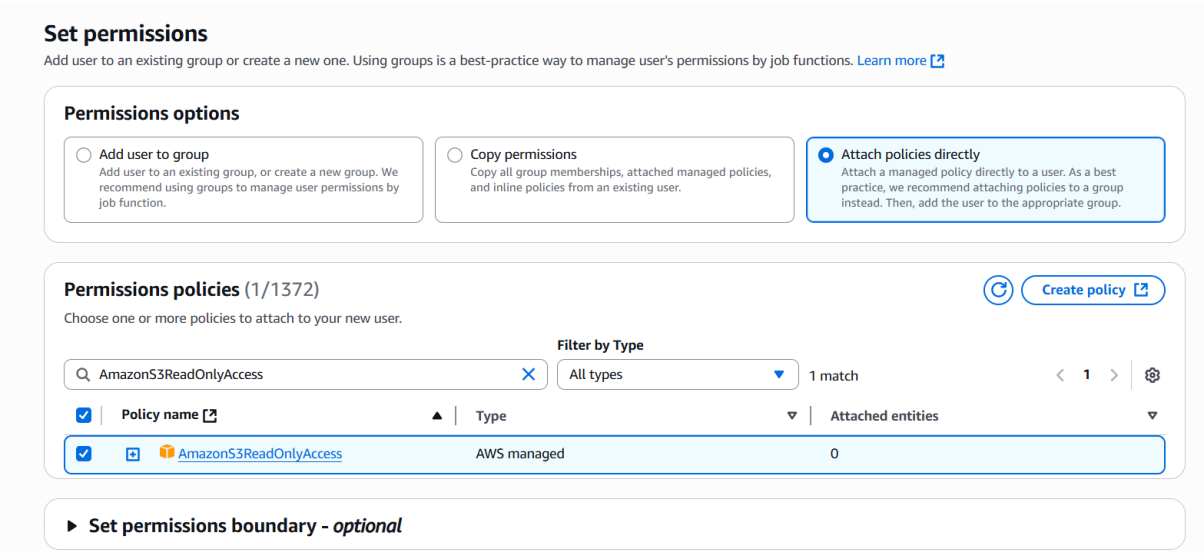
Created a new IAM user with programmatic access for S3 usage.



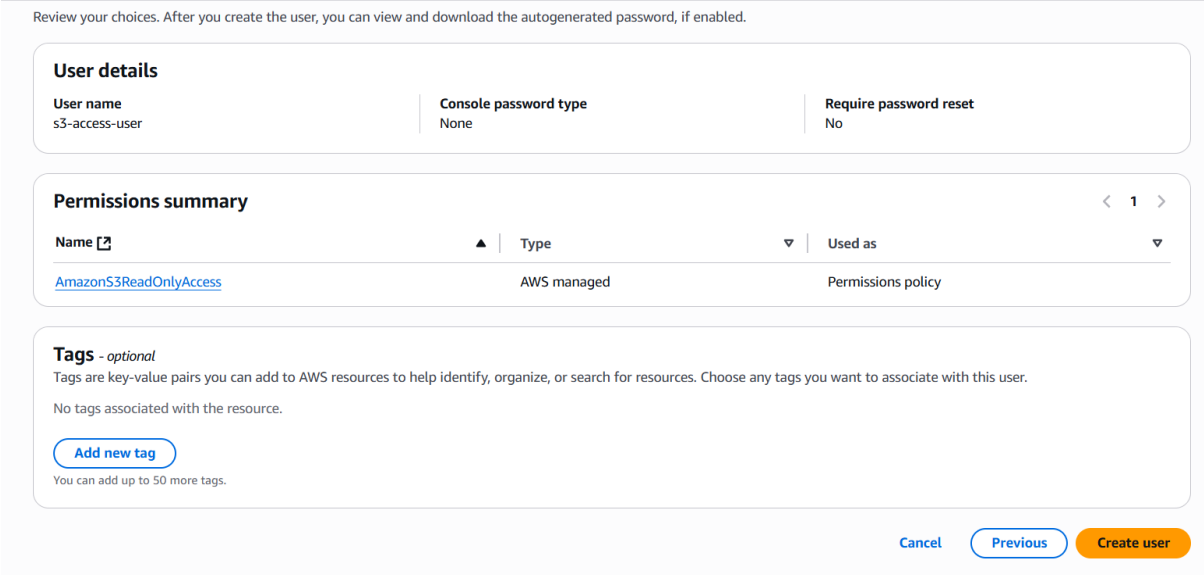
Created a new IAM user with programmatic access to securely access S3 buckets.



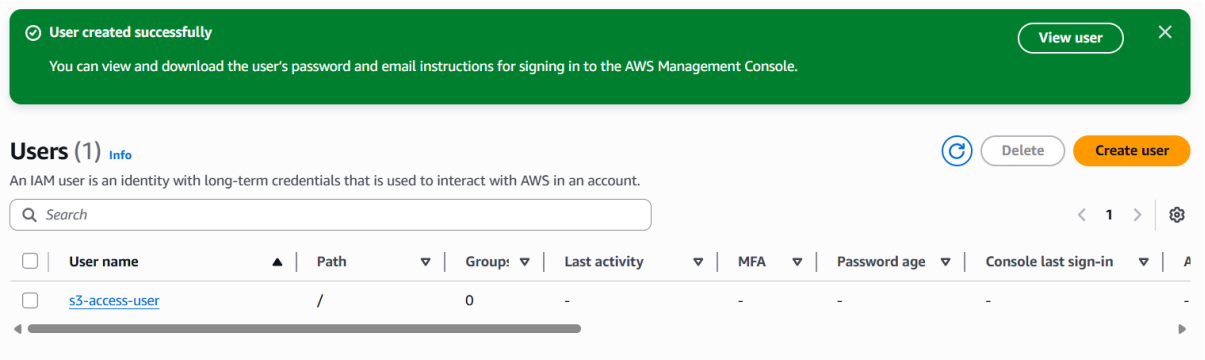
Attached AmazonS3ReadOnlyAccess managed policy to the IAM user for limited S3 access.



Reviewed IAM user details and attached policy before final creation.

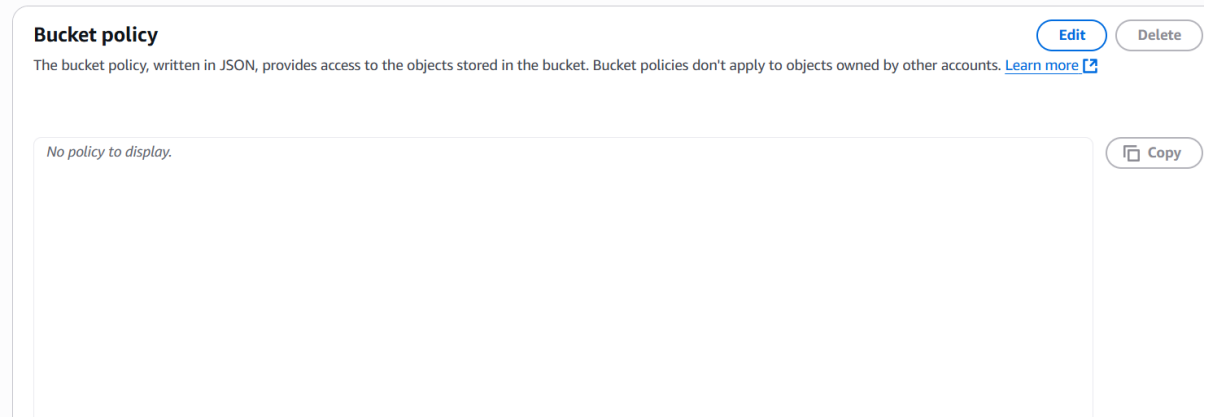


IAM user created successfully with secure programmatic access to Amazon S3.



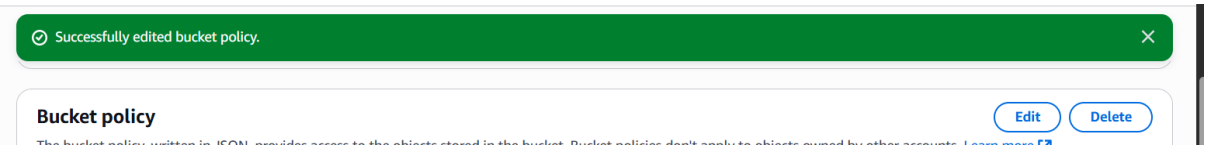
Add a Bucket Policy to Control Access

Opened the bucket policy editor to define user-level access to objects in the bucket.



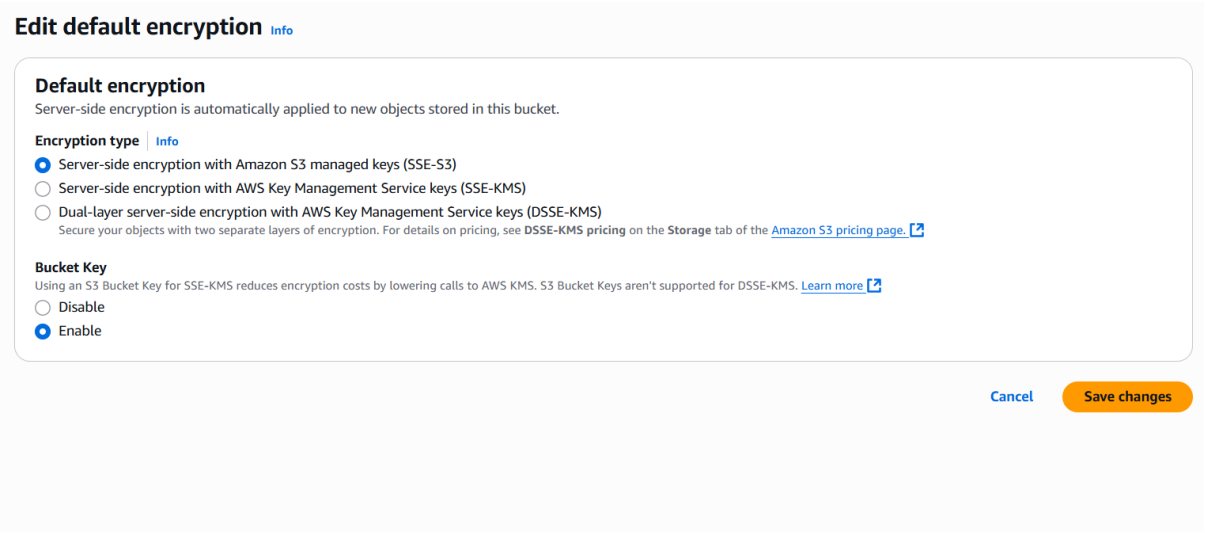
Added a JSON policy to allow read-only access to a specific IAM user.

I change Account-ID by my account ID

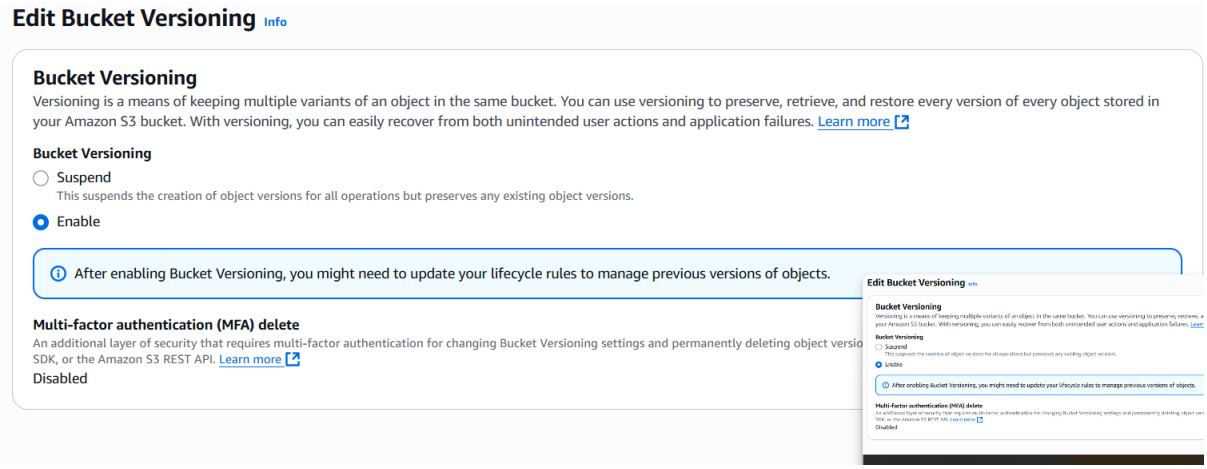


Enable Server-Side Encryption (SSE)

Enabled server-side encryption to protect data at rest using Amazon S3-managed keys.

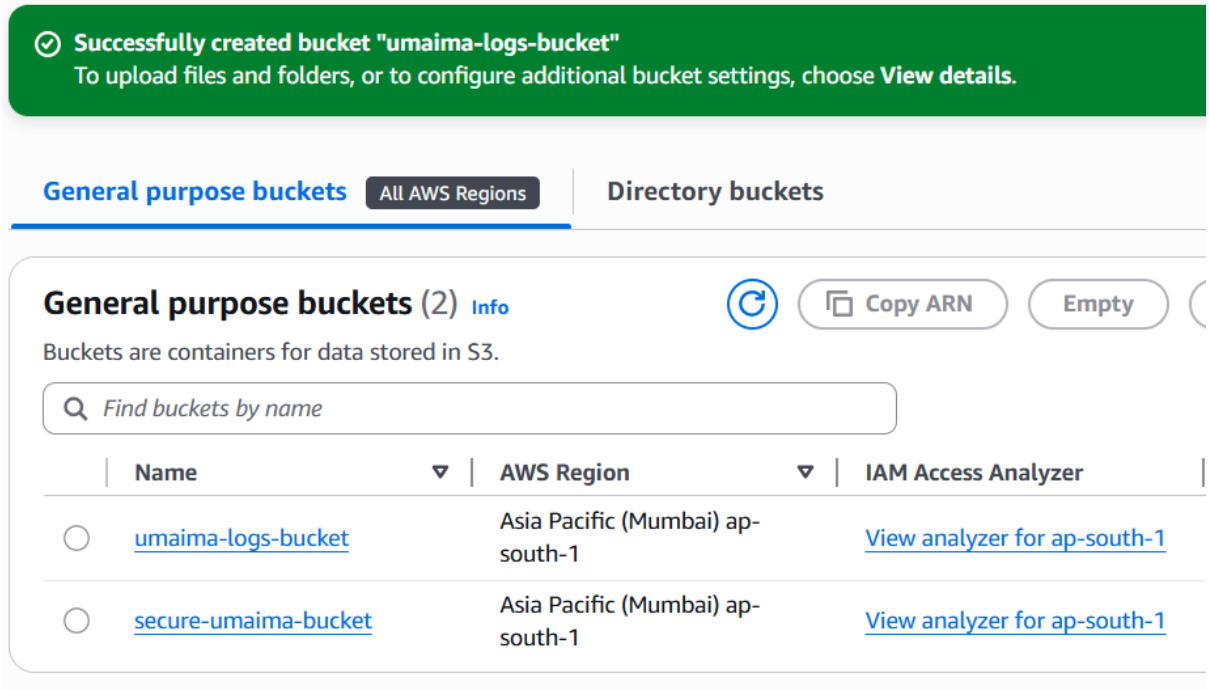


Turned on versioning to retain old versions of files for better data recovery and protection.



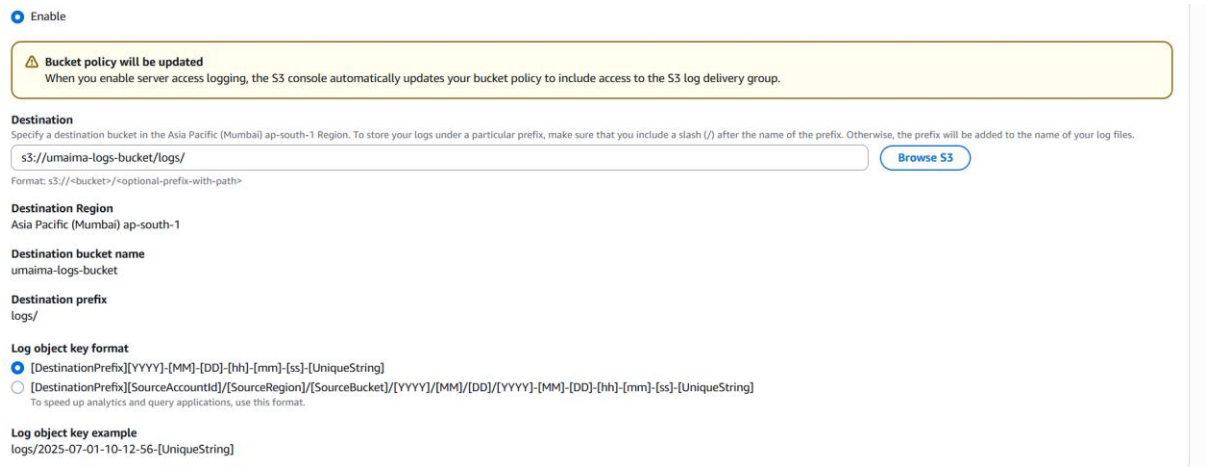
Enable Server Access Logging

Enabled access logging for monitoring all access events on the secure S3 bucket.



Created a dedicated bucket to receive access logs from the main secure S3 bucket.

Enabled Access Logging to Target Bucket: Configured logging to send all access events to umaima-logs-bucket with prefix logs/



Final Summary

The AWS S3 Security Project was completed by implementing a secure and private S3 bucket with strict IAM-based access, custom bucket policies, encryption at rest using SSE-S3, object versioning, and full access logging. This project helped solidify key concepts in cloud security and gave practical experience in AWS console-based configurations.