Intern ID: CT06DG1150

TASK 4

Step 1: Create an IAM Policy and User

Goal: Restrict access to specific resources using IAM.

1. **Navigate to IAM Console**:
   - Go to **AWS Management Console** > **Services** > **IAM**.
   - **Screenshot 1**: Capture the IAM dashboard.
     Heading: *IAM Dashboard Overview*.
2. **Create a Custom IAM Policy**:
   - In IAM, go to **Policies** > **Create Policy** > Switch to **JSON** tab.
   - Paste this policy (replace YOUR_BUCKET_NAME with your bucket name):

json

Copy

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": ["s3:GetObject", "s3:PutObject"],
      "Resource": "arn:aws:s3:::YOUR_BUCKET_NAME/*"
    }
  ]
}
```

   - Name the policy (e.g., S3-ReadWrite-Access).
   - **Screenshot 2**: Capture the JSON policy editor.
     Heading: *Custom IAM Policy JSON Configuration*.

3. **Create an IAM User**:

- Go to **Users** > **Add user**.
- Enter a username (e.g., SecureS3User).
- Select **Programmatic access** and **AWS Management Console access**.
- Attach the policy S3-ReadWrite-Access created earlier.
- **Screenshot 3**: Capture the user summary page with the attached policy.
  Heading: *IAM User Creation with Custom Policy*.

Step 2: Create a Secure S3 Bucket

Goal: Configure an S3 bucket with encryption, versioning, and blocking public access.

1. **Create an S3 Bucket**:
   - Go to **S3 Console** > **Create bucket**.
   - Enter a **unique bucket name** and ensure the region is unchanged.
   - **Screenshot 4**: Capture the bucket creation page (region visible).
     Heading: *S3 Bucket Creation in Default Region*.
2. **Block Public Access**:
   - Under **Block Public Access settings**, check **Block all public access**.
   - **Screenshot 5**: Capture the public access blocking settings.
     Heading: *S3 Bucket Public Access Block Configuration*.
3. **Enable Versioning**:
   - Go to the bucket's **Properties** tab > **Bucket Versioning** > **Enable**.
   - **Screenshot 6**: Capture the versioning settings.
     Heading: *S3 Bucket Versioning Enabled*.
4. **Enable Server-Side Encryption**:
   - Go to the bucket's **Properties** tab > **Default encryption**.
   - Select **AWS Key Management Service (SSE-KMS)**.
   - Choose **AWS managed key (aws/s3)** or create a new KMS key (see Step 3).
   - **Screenshot 7**: Capture the encryption settings.
     Heading: *S3 Bucket Default Encryption Configuration*.

Step 3: Configure AWS KMS Encryption

Goal: Create a KMS key for S3 encryption.

1. **Create a KMS Key**:
   - Go to **AWS KMS Console** > **Customer managed keys** > **Create key**.
   - Set **Key type** as **Symmetric** and **Usage** as **Encrypt and decrypt**.
   - Add a key alias (e.g., S3-Encryption-Key).
   - Assign the IAM user as a **key user** in the key policy.
   - **Screenshot 8**: Capture the KMS key policy configuration.
     Heading: *KMS Key Policy with IAM User Permissions*.
2. **Apply KMS Key to S3 Bucket**:
   - Return to the S3 bucket's **Default encryption** settings.
   - Select the KMS key you created (e.g., S3-Encryption-Key).
   - **Screenshot 9**: Capture the S3 bucket's KMS key selection.
     Heading: *S3 Bucket KMS Encryption Key Assignment*.

Step 4: Test and Validate

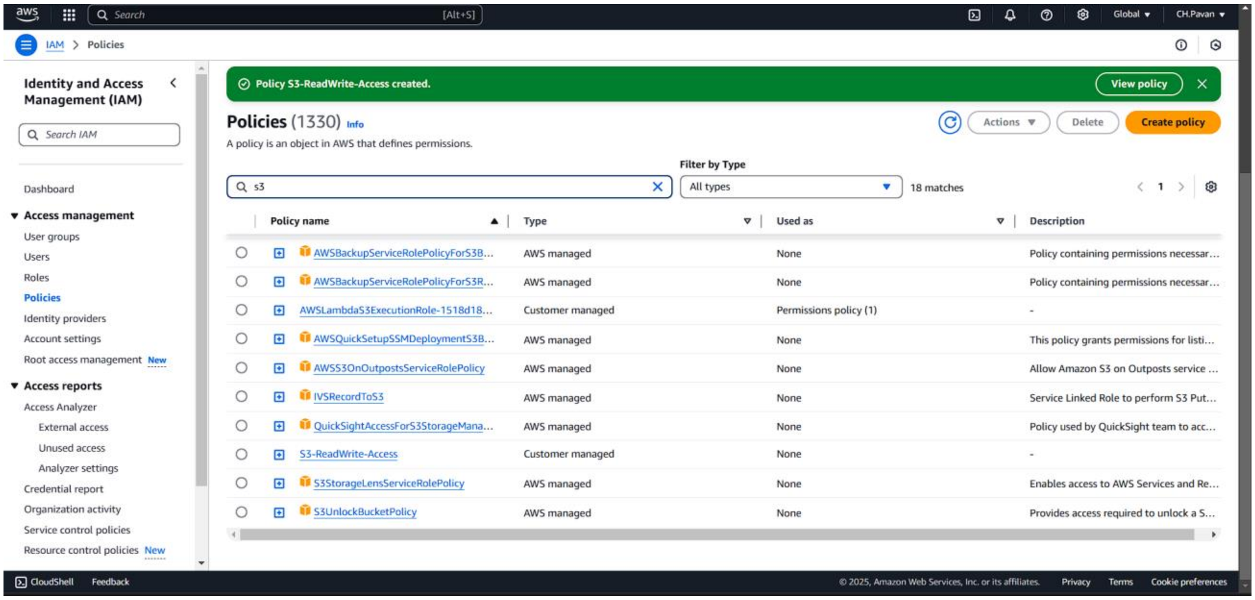
Goal: Verify security policies and encryption.

1. **Upload a Test File**:
   - Use the IAM user credentials to log in to the AWS Console.
   - Upload a file to the S3 bucket.
   - **Screenshot 10**: Capture the successful upload.
     Heading: *File Upload to S3 Using Restricted IAM User*.
2. **Check Encryption Status**:
   - Select the uploaded file in S3 > **Properties** > **Server-Side Encryption**.
   - Confirm encryption is enabled with the KMS key.
   - **Screenshot 11**: Capture the file's encryption details.
     Heading: *S3 Object Encryption Status with KMS*.

Final Deliverable: Report Structure

1. **Introduction**: Explain the purpose of securing AWS resources.
2. **IAM Configuration**: Include Screenshots 1-3.
3. **S3 Security**: Include Screenshots 4-7.
4. **KMS Encryption**: Include Screenshots 8-9.
5. **Validation**: Include Screenshots 10-11.
6. **Conclusion**: Summarize how IAM, S3, and KMS enhance security.

S3 Read Write



Policy S3-ReadWrite-Access created.

Policies (1330) Info

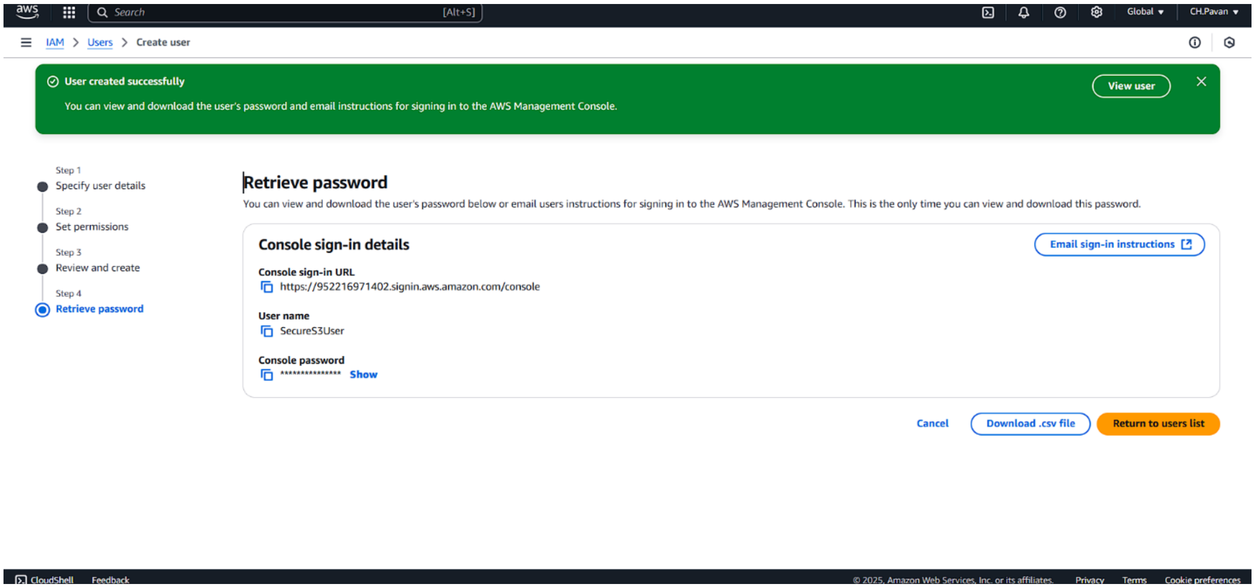
A policy is an object in AWS that defines permissions.

Filter by Type: All types

s3 — 18 matches

Policy name	Type	Used as	Description
AWSBackupServiceRolePolicyForS3B...	AWS managed	None	Policy containing permissions necessar...
AWSBackupServiceRolePolicyForS3R...	AWS managed	None	Policy containing permissions necessar...
AWSLambdaS3ExecutionRole-1518d18...	Customer managed	Permissions policy (1)	-
AWSQuickSetupSSMDeploymentS3B...	AWS managed	None	This policy grants permissions for listi...
AWSS3OnOutpostsServiceRolePolicy	AWS managed	None	Allow Amazon S3 on Outposts service ...
IVSRecordToS3	AWS managed	None	Service Linked Role to perform S3 Put...
QuickSightAccessForS3StorageMana...	AWS managed	None	Policy used by QuickSight team to acc...
S3-ReadWrite-Access	Customer managed	None	-
S3StorageLensServiceRolePolicy	AWS managed	None	Enables access to AWS Services and Re...
S3UnlockBucketPolicy	AWS managed	None	Provides access required to unlock a S...

Created a User



User created successfully

You can view and download the user's password and email instructions for signing in to the AWS Management Console.

Retrieve password

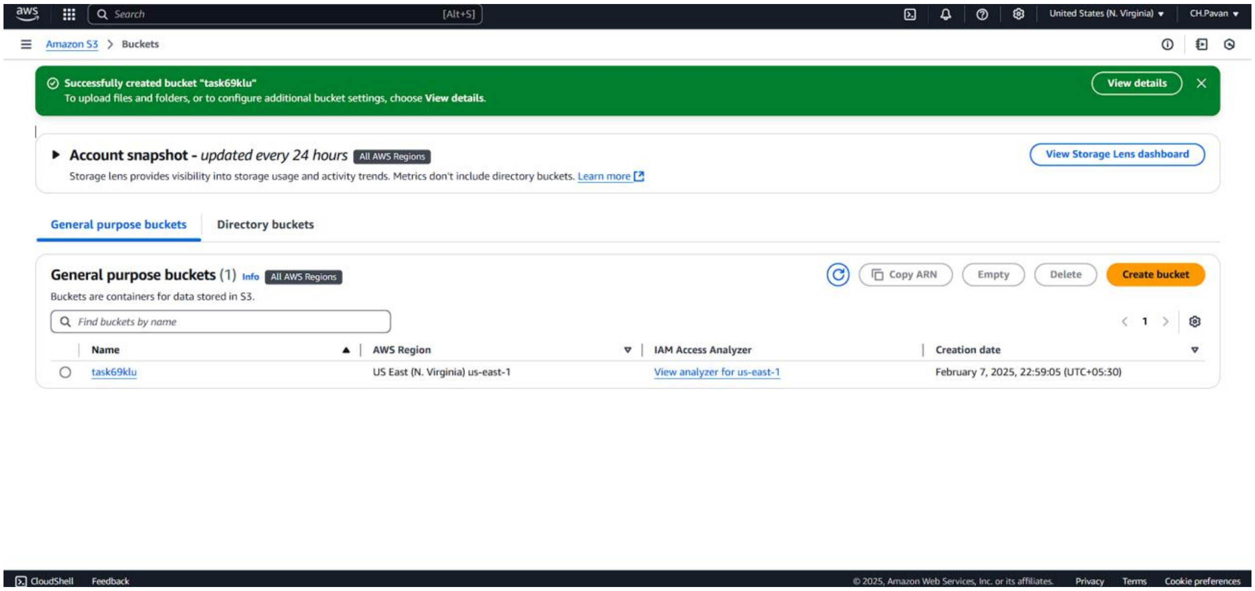
You can view and download the user's password below or email users instructions for signing in to the AWS Management Console. This is the only time you can view and download this password.

Console sign-in details

Console sign-in URL
https://952216971402.signin.aws.amazon.com/console

User name
SecureS3User

Console password
****



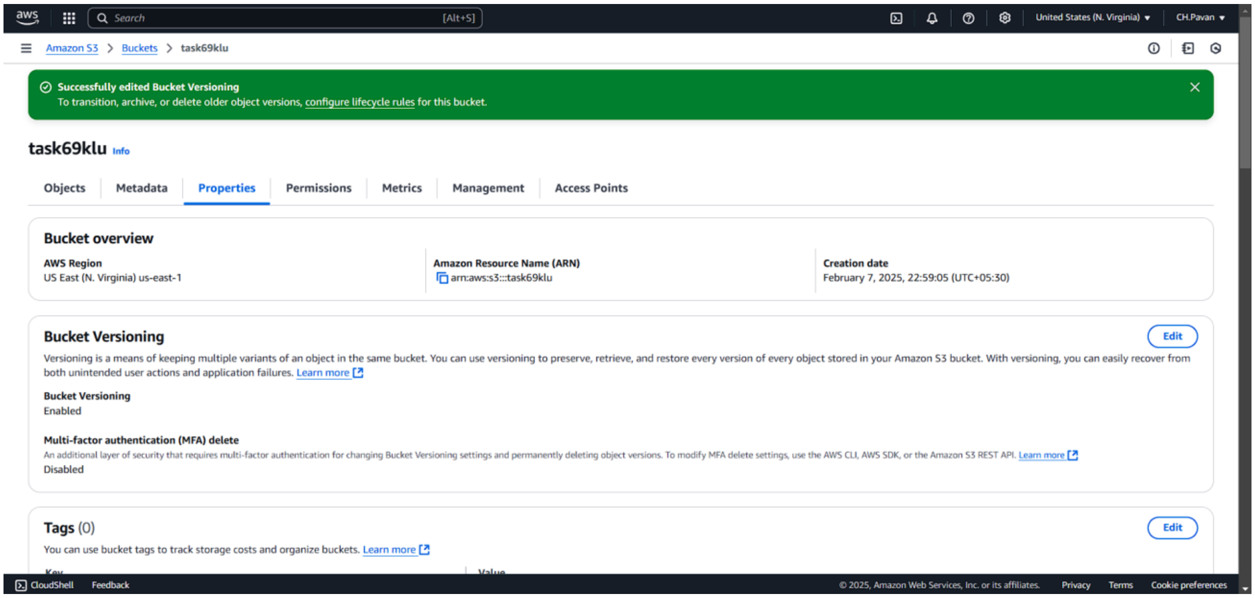
Successfully created bucket "task69klu"
To upload files and folders, or to configure additional bucket settings, choose **View details**.

Account snapshot - *updated every 24 hours* All AWS Regions
Storage lens provides visibility into storage usage and activity trends. Metrics don't include directory buckets. Learn more

General purpose buckets (1)
Buckets are containers for data stored in S3.

Name	AWS Region	IAM Access Analyzer	Creation date
task69klu	US East (N. Virginia) us-east-1	View analyzer for us-east-1	February 7, 2025, 22:59:05 (UTC+05:30)

Bucket Visionary setting



Successfully edited Bucket Versioning
To transition, archive, or delete older object versions, configure lifecycle rules for this bucket.

task69klu Info

Bucket overview

AWS Region
US East (N. Virginia) us-east-1

Amazon Resource Name (ARN)
arn:aws:s3:::task69klu

Creation date
February 7, 2025, 22:59:05 (UTC+05:30)

Bucket Versioning

Versioning is a means of keeping multiple variants of an object in the same bucket. You can use versioning to preserve, retrieve, and restore every version of every object stored in your Amazon S3 bucket. With versioning, you can easily recover from both unintended user actions and application failures. Learn more

Bucket Versioning
Enabled

Multi-factor authentication (MFA) delete
An additional layer of security that requires multi-factor authentication for changing Bucket Versioning settings and permanently deleting object versions. To modify MFA delete settings, use the AWS CLI, AWS SDK, or the Amazon S3 REST API. Learn more
Disabled

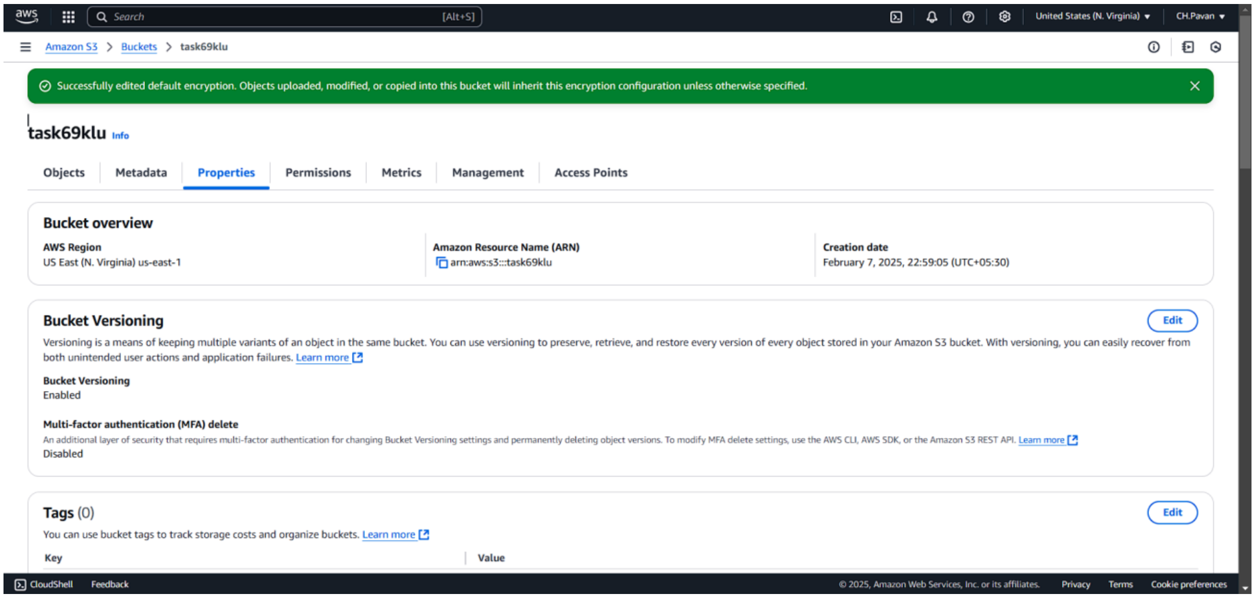
Tags (0)

You can use bucket tags to track storage costs and organize buckets. Learn more

Key | Value

© 2025, Amazon Web Services, Inc. or its affiliates.

Default Encryption



Successfully edited default encryption. Objects uploaded, modified, or copied into this bucket will inherit this encryption configuration unless otherwise specified.

task69klu Info

Bucket overview

AWS Region
US East (N. Virginia) us-east-1

Amazon Resource Name (ARN)
arn:aws:s3:::task69klu

Creation date
February 7, 2025, 22:59:05 (UTC+05:30)

Bucket Versioning

Versioning is a means of keeping multiple variants of an object in the same bucket. You can use versioning to preserve, retrieve, and restore every version of every object stored in your Amazon S3 bucket. With versioning, you can easily recover from both unintended user actions and application failures. Learn more

Bucket Versioning
Enabled

Multi-factor authentication (MFA) delete
An additional layer of security that requires multi-factor authentication for changing Bucket Versioning settings and permanently deleting object versions. To modify MFA delete settings, use the AWS CLI, AWS SDK, or the Amazon S3 REST API. Learn more
Disabled

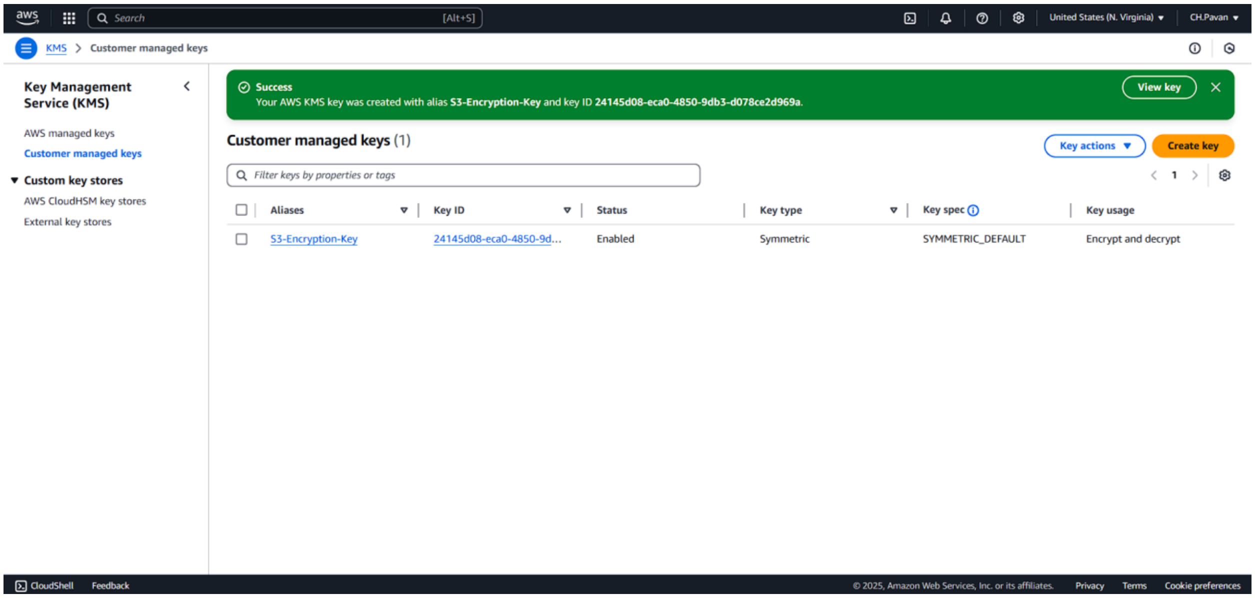
Tags (0)

You can use bucket tags to track storage costs and organize buckets. Learn more

Key | Value

© 2025, Amazon Web Services, Inc. or its affiliates.

Created Key User

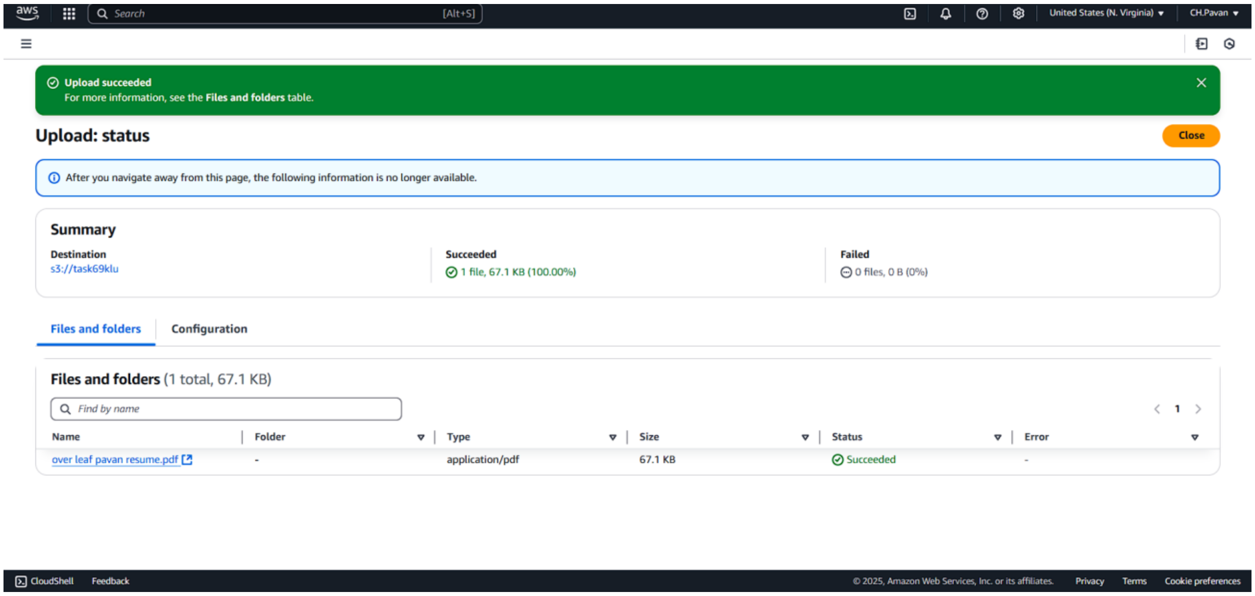


Success
Your AWS KMS key was created with alias **S3-Encryption-Key** and key ID **24145d08-eca0-4850-9db3-d078ce2d969a**.

Customer managed keys (1)

□	Aliases	Key ID	Status	Key type	Key spec	Key usage
□	S3-Encryption-Key	24145d08-eca0-4850-9d...	Enabled	Symmetric	SYMMETRIC_DEFAULT	Encrypt and decrypt

File Uploaded



Upload succeeded
For more information, see the **Files and folders** table.

Upload: status

After you navigate away from this page, the following information is no longer available.

Summary

Destination: s3://task69klu

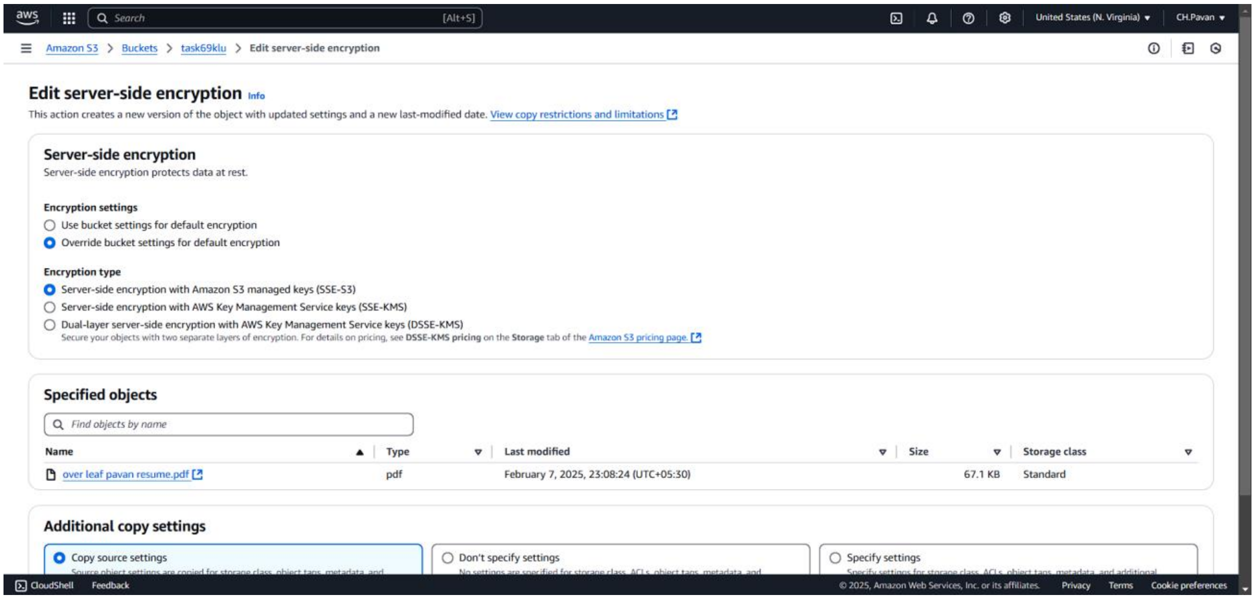
Succeeded: 1 file, 67.1 KB (100.00%)

Failed: 0 files, 0 B (0%)

Files and folders (1 total, 67.1 KB)

Name	Folder	Type	Size	Status	Error
over leaf pavan resume.pdf	-	application/pdf	67.1 KB	Succeeded	-

Server side Encryption


Search [Alt+S]
United States (N. Virginia) ▾
CH.Pavan ▾
Amazon S3 > Buckets > task69klu > Edit server-side encryption

Edit server-side encryption Info

This action creates a new version of the object with updated settings and a new last-modified date. View copy restrictions and limitations

Server-side encryption

Server-side encryption protects data at rest.

Encryption settings

○ Use bucket settings for default encryption

● Override bucket settings for default encryption

Encryption type

● Server-side encryption with Amazon S3 managed keys (SSE-S3)

○ Server-side encryption with AWS Key Management Service keys (SSE-KMS)

○ Dual-layer server-side encryption with AWS Key Management Service keys (DSSE-KMS)
Secure your objects with two separate layers of encryption. For details on pricing, see DSSE-KMS pricing on the Storage tab of the Amazon S3 pricing page.

Specified objects

Name	Type	Last modified	Size	Storage class
over leaf pavan resume.pdf	pdf	February 7, 2025, 23:08:24 (UTC+05:30)	67.1 KB	Standard

Additional copy settings

● Copy source settings ○ Don't specify settings ○ Specify settings

Final Deliverable: Report Structure

1. **Introduction**: Explain the purpose of securing AWS resources.
2. **IAM Configuration**: Include Screenshots 1-3.
3. **S3 Security**: Include Screenshots 4-7.
4. **KMS Encryption**: Include Screenshots 8-9.
5. **Validation**: Include Screenshots 10-11.
6. **Conclusion**: Summarize how IAM, S3, and KMS enhance security.