

Intern ID: CT06DG1190

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.*

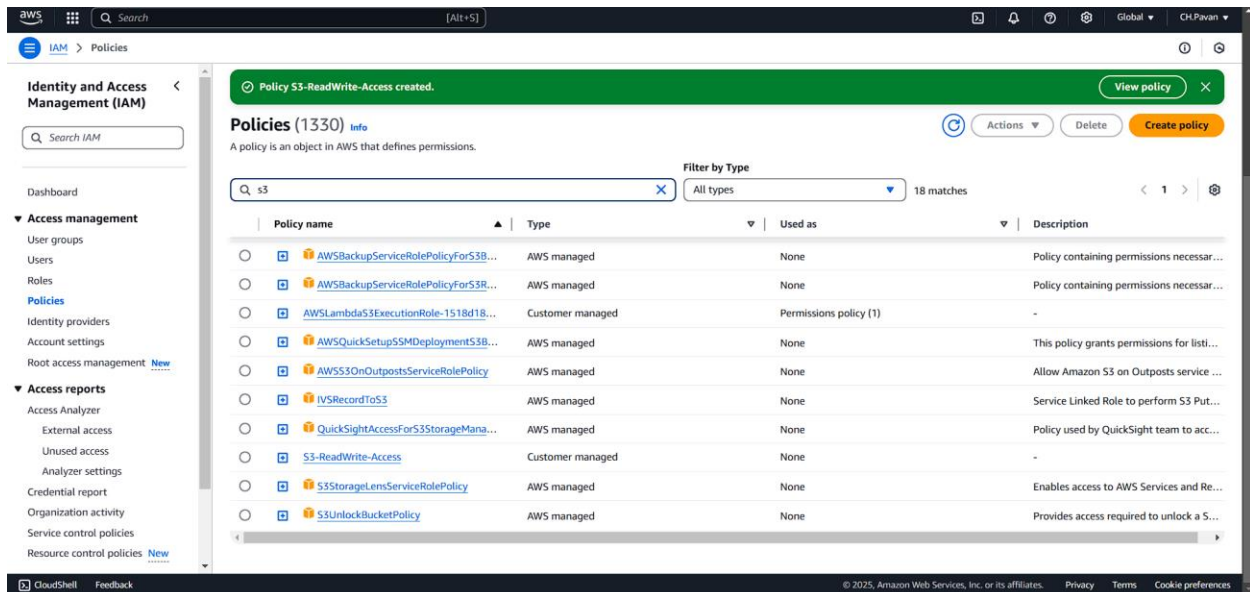
2. Check Encryption Status:

- 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



Created a User

aws

Search

[Alt+5]

Global

CH.Pavan

IAM > Users > Create user

0

Q

User created successfully

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

View user

X

- Step 1
- Specify user details
- Step 2
- Set permissions
- Step 3
- Review and create
- Step 4
- Retrieve password

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

[Email sign-in instructions](#)

Console sign-in URL

<https://952216971402.signin.aws.amazon.com/console>

User name

[Secure53User](#)

Console password

[***** Show](#)

[Cancel](#)[Download .csv file](#)[Return to users list](#)

Amazon S3 > Buckets

0

Q

Successfully created bucket "task69klu"

To upload files and folders, or to configure additional bucket settings, choose [View details](#).

View details

X

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](#)

[View Storage Lens dashboard](#)

General purpose buckets

Directory buckets

General purpose buckets (1)

[Info](#) [All AWS Regions](#)

Buckets are containers for data stored in S3.

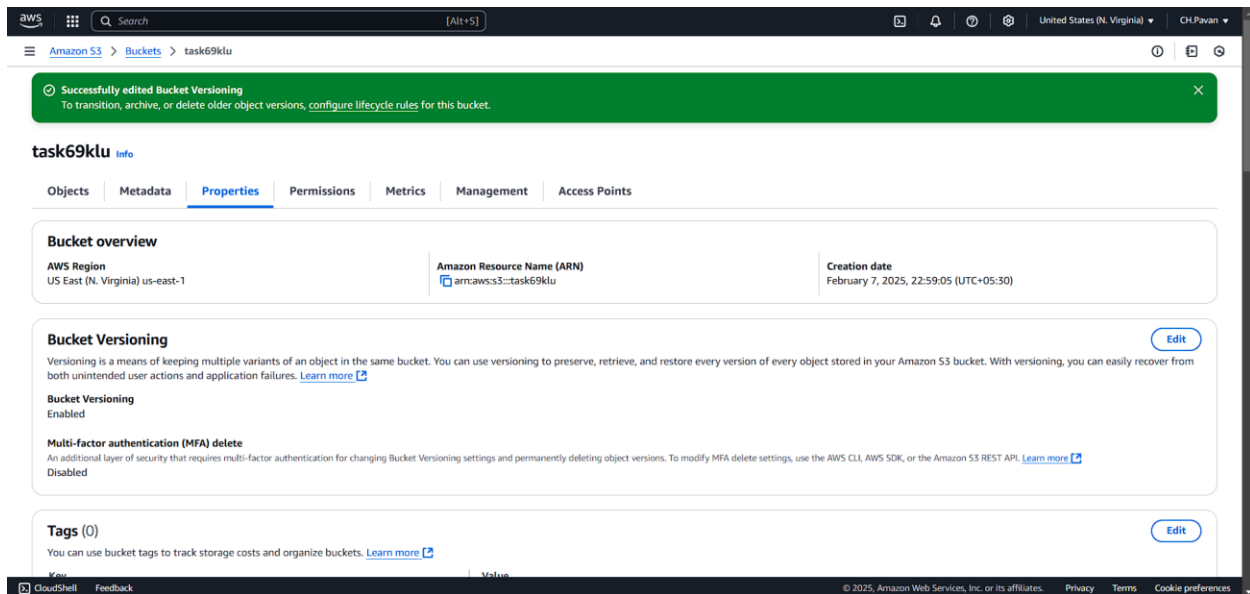
[Find buckets by name](#)

[Copy ARN](#)[Empty](#)[Delete](#)[Create bucket](#)

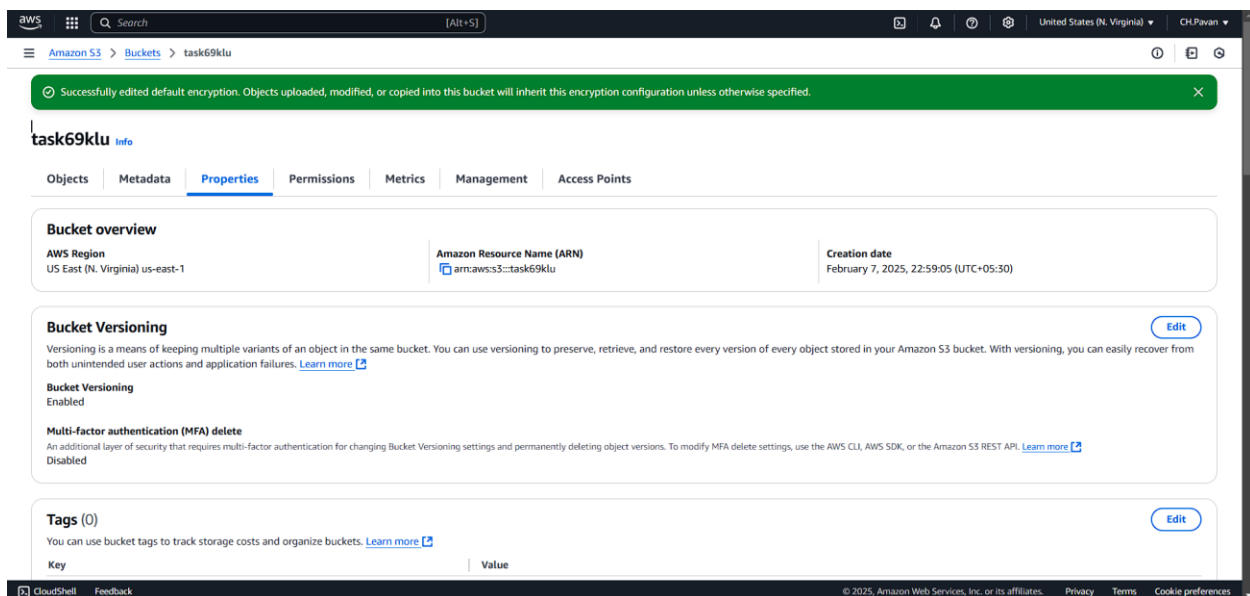
< 1 >

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



Default Encryption



Created Key User

Key Management Service (KMS)

AWS managed keys

Customer managed keys

Custom key stores

AWS CloudHSM key stores

External key stores

Success

Your AWS KMS key was created with alias [S3-Encryption-Key](#) and key ID [24145d08-eca0-4850-9db3-d078ce2d969a](#).

View key

Customer managed keys (1)

Filter keys by properties or tags

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

Key actionsCreate key

CloudShellFeedback

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

File Uploaded

Upload succeeded

For more information, see the [Files and folders](#) table.

Close

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

Configuration

Files and folders (1 total, 67.1 KB)

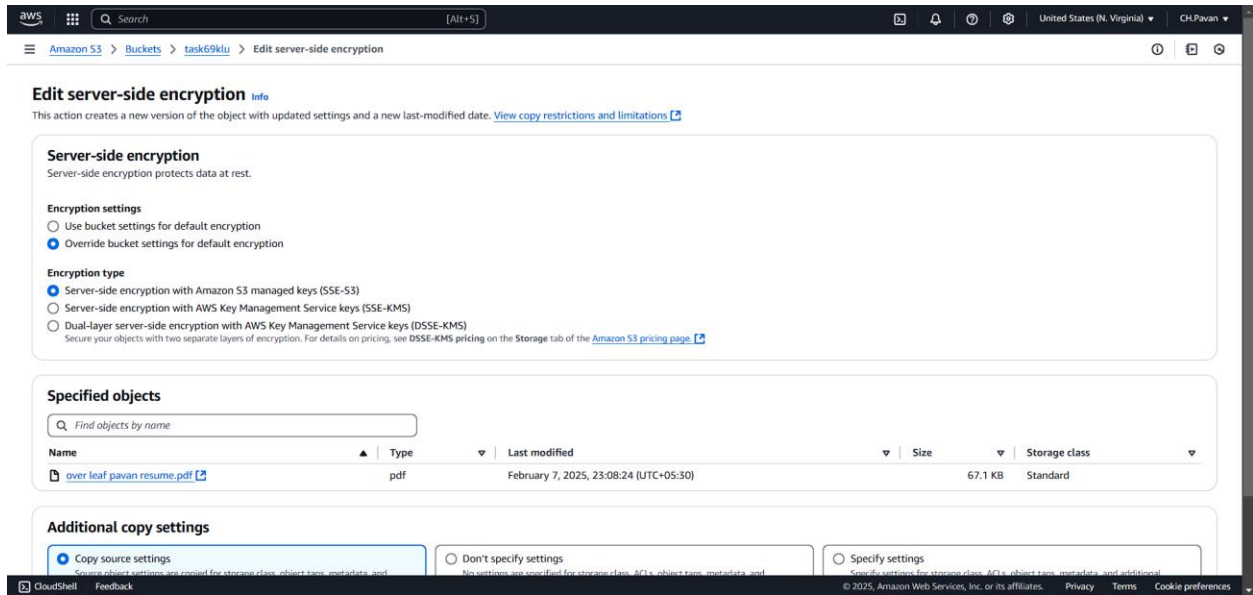
Find by name

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

CloudShellFeedback

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

Server side Encryption



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.