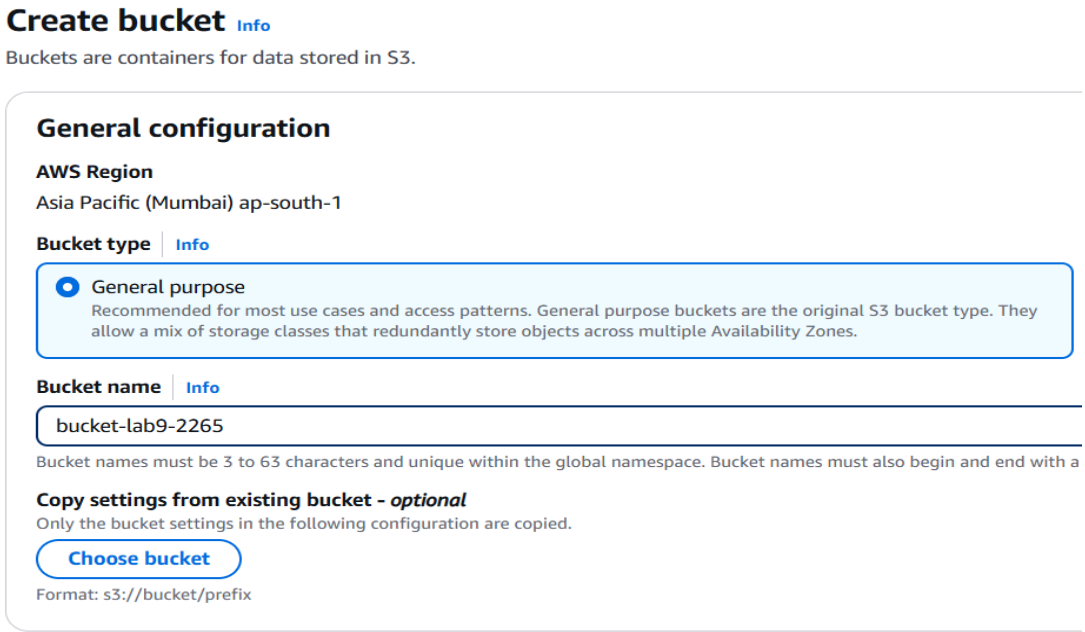
School of Computer Science, Engineering and Applications (SCSEA)
B. Tech TY (CCSA)
Subject: Cloud Architecture And Protocol

Name of the Student: Sahil S. Mandawgade PRN: 20220802265

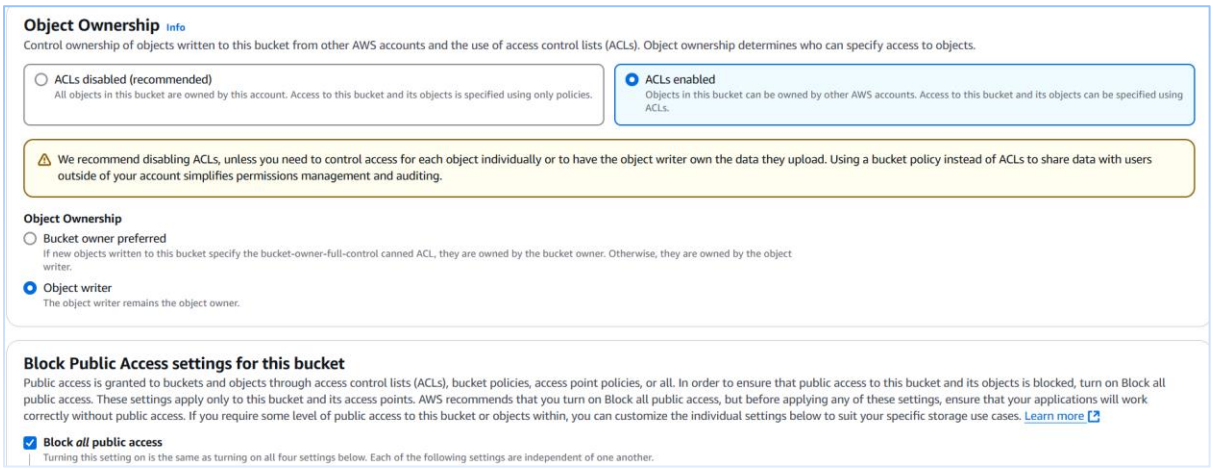
Title of Practical: 9. Implementing S3 Encryption with AWS KMS and Activity Monitoring via CloudTrail.

Step 1: Create one S3 Bucket.

- Go to S3 in AWS Dashboard.
- Click on Create bucket.
- Select Bucket type as "General Purpose".
- Give proper name to bucket as 'bucket-lab9-2265'.

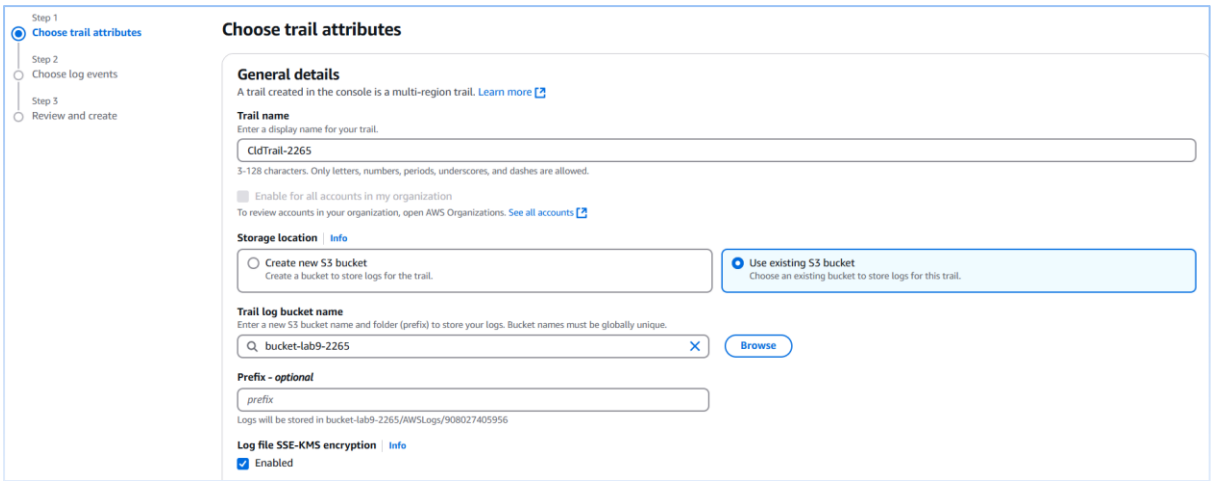


- In "Object Ownership" click on "ACLs enabled".
- In "Object Ownership" select "Object writer".
- Block all Public Access and then click Create Bucket.

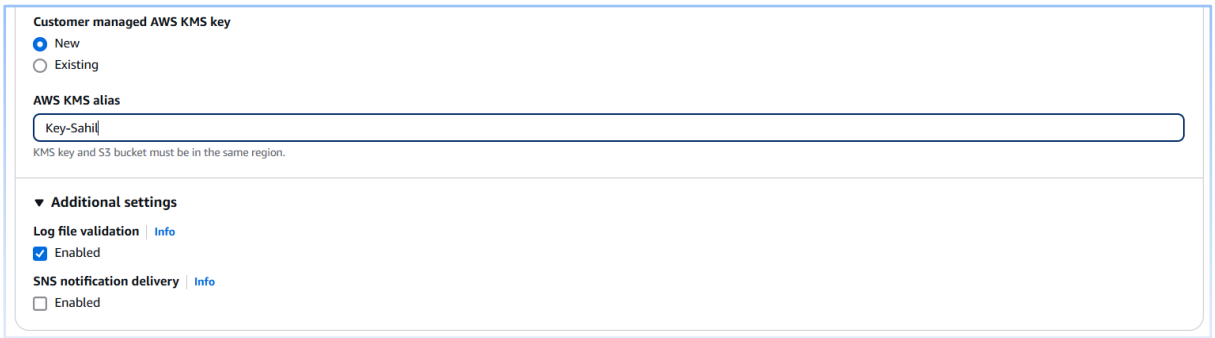


Step 2: In CloudTrail create one Trail.

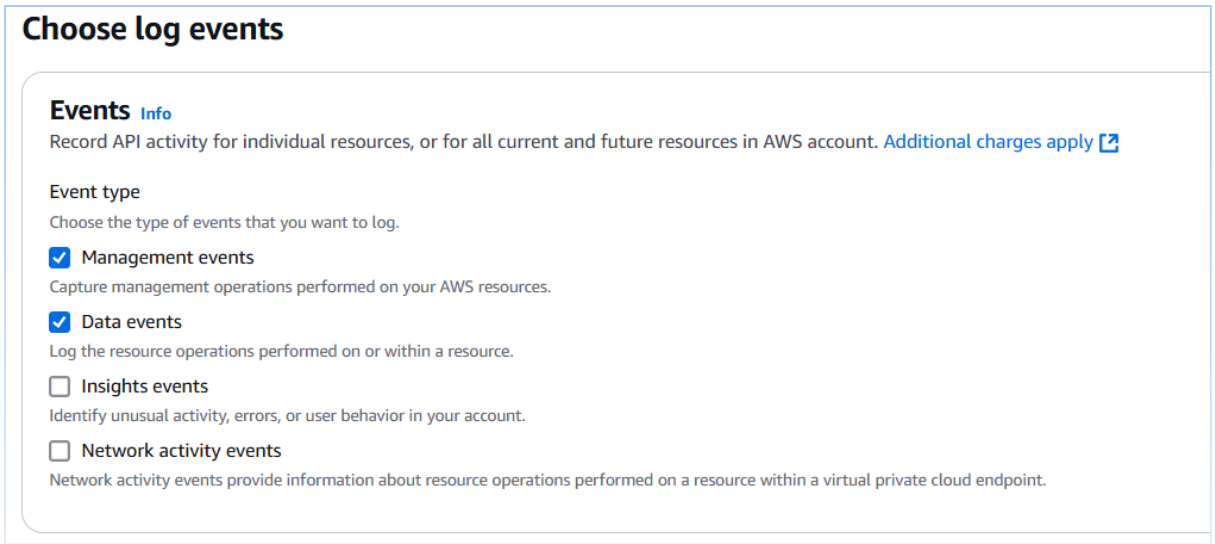
- Go to CloudTrail in AWS Dashboard.
- Click on Create Trail.
- Give proper name to trail as 'CldTrail-2265'.
- Select our existing Bucket i.e. – bucket-lab9-2265.
- Enable "Log file SSE-KMS encryption".



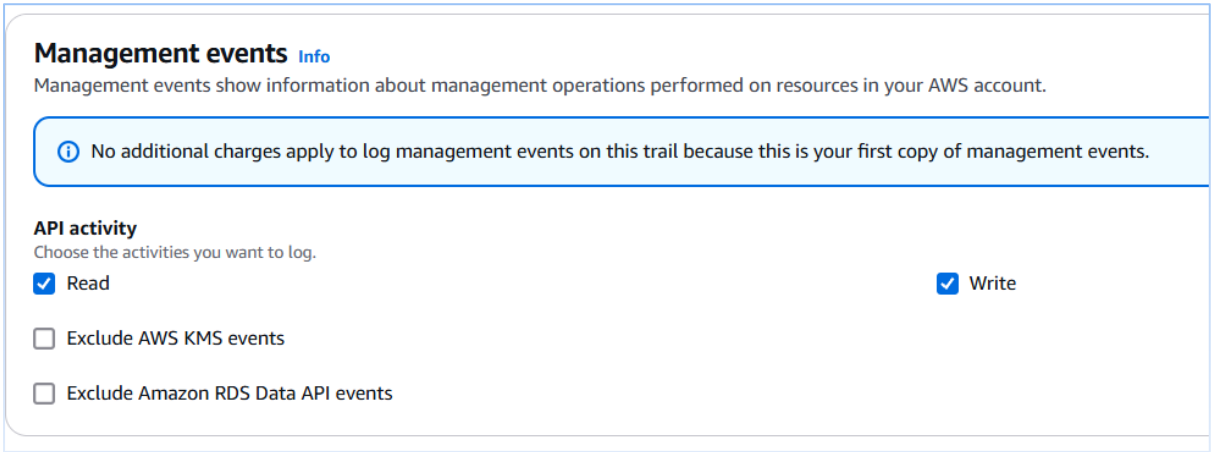
- Select "New" in Customer managed AWS KMS keys.
- Give proper key alias.
- Enable "Log file validation".



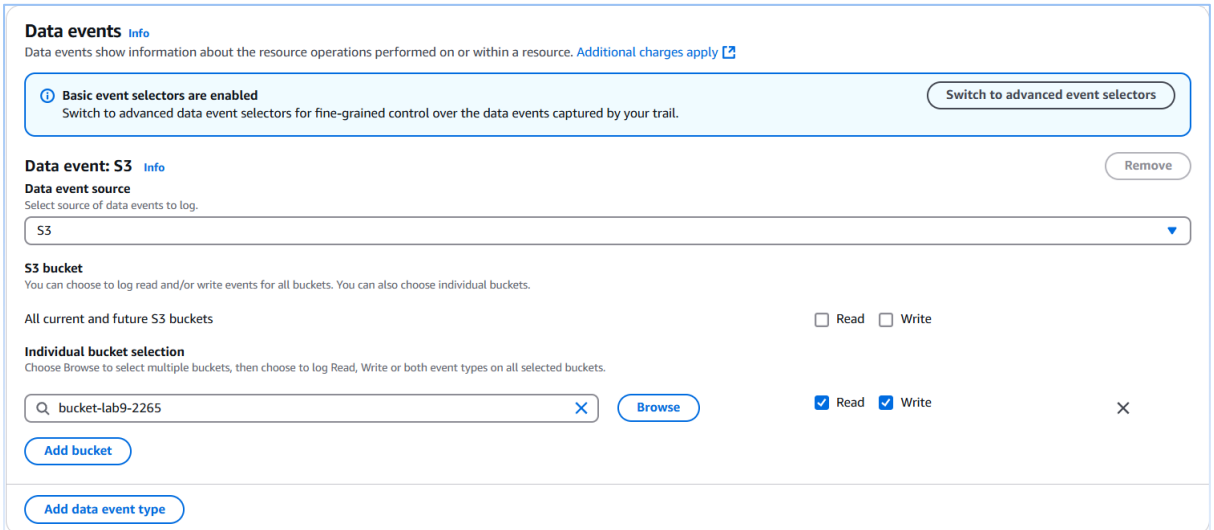
- In Events click on "Management" & "Data" events.



- In Management Event Select "Read" & "Write".



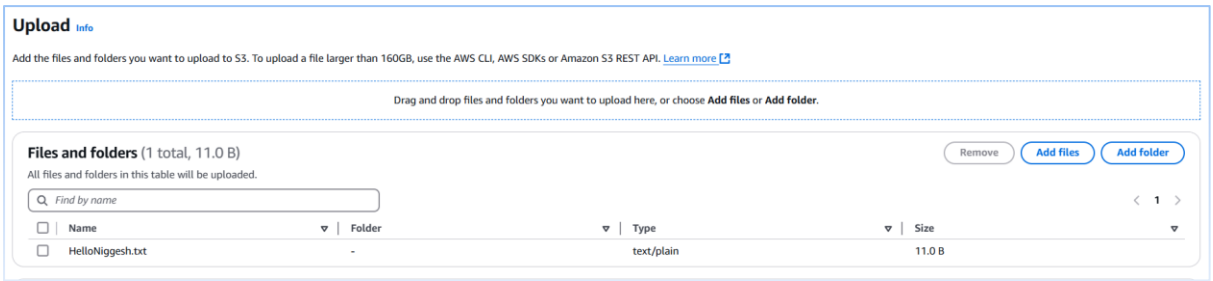
- In Data Event : Switch to basic event selectors – Select "Read" & "Write" on our created bucket.



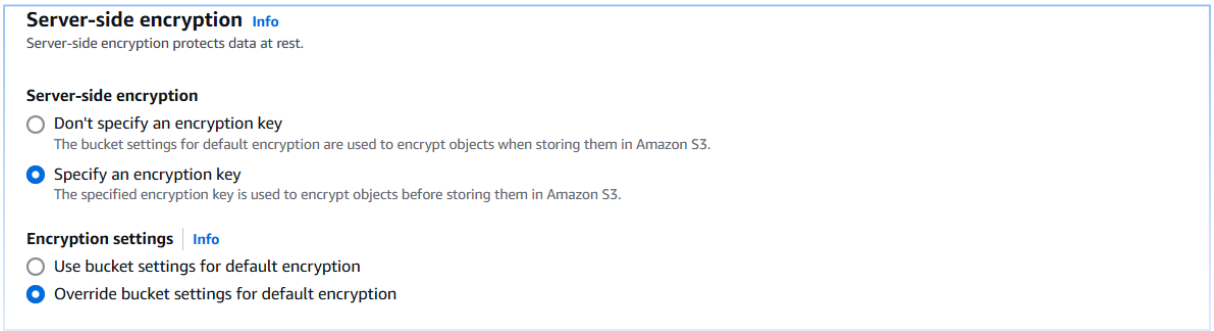
- Review all the settings and Create the Trail.

Step 3: Upload file in S3 bucket with encryption.

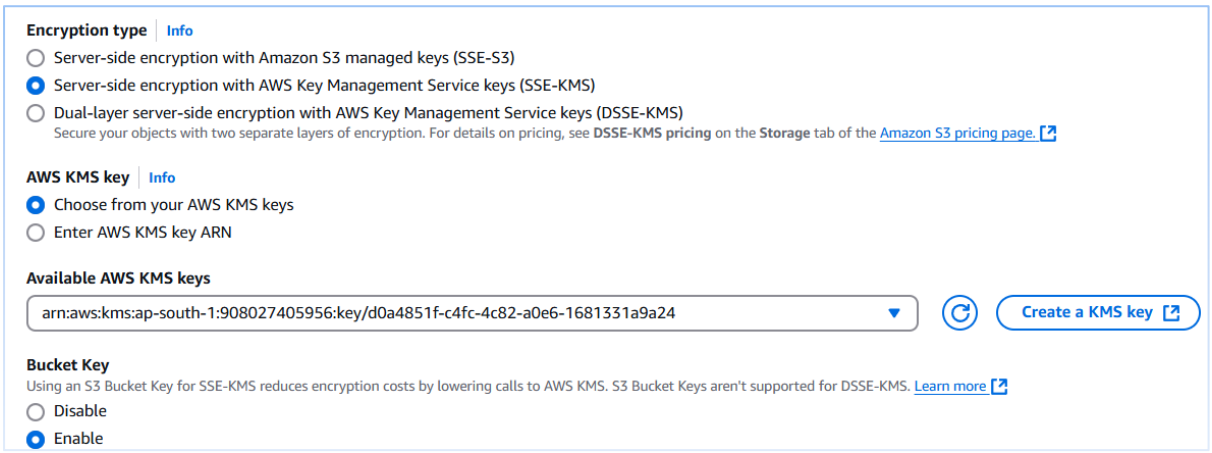
- Select our created bucket and click on “upload”.
- Add one file in bucket.



- Go in properties and in “server-side encryption” select “specify an encryption key”.

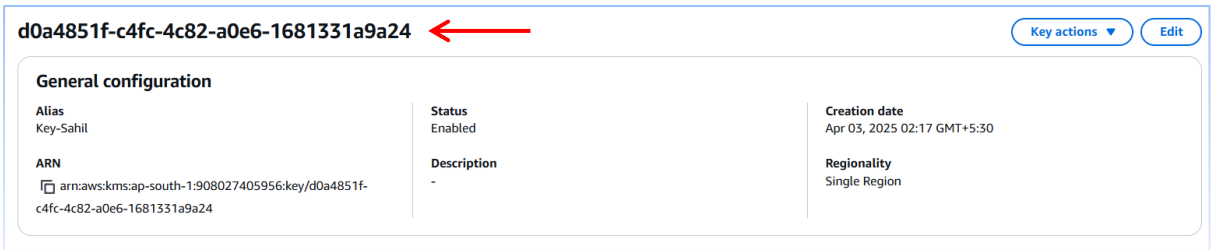


- In “Encryption Type” select “Server-side encryption with AWS Key
- Management Service (SSE-KMS)”.
- In AWS KMS Key select our created key.

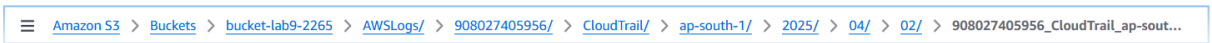


Step 4: Check if our key is used for Encryption using Key ID.

- Go to KMS and copy the Key ID.



- Now in S3 click on our bucket.
- In Bucket go in following Path:



- Open the logs -> Ctrl+f.

- Paste our key ID and see if it's used.

School of Computer Science, Engineering and Applications (SCSEA)
B. Tech TY (CCSA)
Subject: Cloud Architecture And Protocol

Name of the Student: Sahil S. Mandawgade PRN: 20220802265

Title of Practical: 9. Implementing S3 Encryption with AWS KMS and Activity Monitoring via CloudTrail.

https://bucket-lab9-2265.s3.ap-south-1.amazonaws.com/AWSLogs/908027405956/CloudTrail/ap-south-1/2025/04/02/908027405956_CloudTrail_ap-south-1_20250402T2100...

Import favorites For quick access, place your favorites here on the favorites bar. Manage favorites now

-c4fc-4c82-a0e6-1681331a9a24 1/8

Pretty-print


```
{"Records":[{"eventVersion":"1.11","userIdentity":{"type":"AWSService","invokedBy":"cloudtrail.amazonaws.com"},"eventTime":"2025-04-
02T20:52:17Z","eventSource":"kms.amazonaws.com","eventName":"GenerateDataKey","awsRegion":"ap-south-
1","sourceIPAddress":"cloudtrail.amazonaws.com","userAgent":"cloudtrail.amazonaws.com","requestParameters":{"keyId":"arn:aws:kms:ap-south-1:908027405956:key/d0a4851f-
c4fc-4c82-a0e6-1681331a9a24","encryptionContext":{"aws:cloudtrail:arn":"arn:aws:cloudtrail:ap-south-1:908027405956:trail/CldTrail-
2265","aws:s3:arn":"arn:aws:s3:::bucket-lab9-2265"},"keySpec":"AES_256"},"responseElements":null,"requestID":"24d1feba-591a-403d-8a9e-f71a4c63bc6f","eventID":"31b3e532-
d365-349e-b8f9-6ea5f38078c4","readOnly":true,"resources":[{"accountId":"908027405956","type":"AWS::KMS::Key","ARN":"arn:aws:kms:ap-south-1:908027405956:key/d0a4851f-
c4fc-4c82-a0e6-1681331a9a24"}],"eventType":"AwsApiCall","managementEvent":true,"recipientAccountId":"908027405956","sharedEventID":"8ca94786-0558-46c6-9f1e-
5f25d9c2f0a0","eventCategory":"Management"},{"eventVersion":"1.11","userIdentity":{"type":"AWSService","invokedBy":"cloudtrail.amazonaws.com"},"eventTime":"2025-04-
02T20:52:15Z","eventSource":"s3.amazonaws.com","eventName":"GetBucketAcl","awsRegion":"ap-south-
1","sourceIPAddress":"cloudtrail.amazonaws.com","userAgent":"cloudtrail.amazonaws.com","requestParameters":{"bucketName":"bucket-lab9-2265","Host":"bucket-lab9-
2265.s3.ap-south-1.amazonaws.com","acl":""},"responseElements":null,"additionalEventData":
{"SignatureVersion":"SigV4","CipherSuite":"TLS_AES_128_GCM_SHA256","bytesTransferredIn":0,"AuthenticationMethod":"AuthHeader","x-amz-id-
2":"Qso61zXg4H7BLVfoejJHKnfE20KmFWTnZE59mBOnbSbKgyGLRBbAgXY7cCpl4wkqlkXSW9eaAHsg6aUkrxwCqQ==","bytesTransferredOut":480},"requestID":"DZ7CFF4X5G1WAGM4","eventID":"af4d67
79-2d34-3c87-a78d-ccf76ed32b87","readOnly":true,"resources":[{"accountId":"908027405956","type":"AWS::S3::Bucket","ARN":"arn:aws:s3:::bucket-lab9-
2265"}],"eventType":"AwsApiCall","managementEvent":true,"recipientAccountId":"908027405956","sharedEventID":"31afd941-16a6-4f18-b9ec-
9866892c6465","vpcEndpointId":"cloudtrail.amazonaws.com","vpcEndpointAccountId":"cloudtrail.amazonaws.com","eventCategory":"Management"},
{"eventVersion":"1.11","userIdentity":{"type":"AWSService","invokedBy":"cloudtrail.amazonaws.com"},"eventTime":"2025-04-
02T20:53:38Z","eventSource":"s3.amazonaws.com","eventName":"GetBucketAcl","awsRegion":"ap-south-
1","sourceIPAddress":"cloudtrail.amazonaws.com","userAgent":"cloudtrail.amazonaws.com","requestParameters":{"bucketName":"bucket-lab9-2265","Host":"bucket-lab9-
2265.s3.ap-south-1.amazonaws.com","acl":""},"responseElements":null,"additionalEventData":
{"SignatureVersion":"SigV4","CipherSuite":"TLS_AES_128_GCM_SHA256","bytesTransferredIn":0,"AuthenticationMethod":"AuthHeader","x-amz-id-
2":"3seYxHsEj4y/YLEa3xks+mwCmyZ9yJqZJ2hPGBOMgARarNZDCVyY6trCz/H4jUyL49q8BR5GEww=","bytesTransferredOut":480},"requestID":"MAWNMD9W43SV2XDS","eventID":"a96c1c0c-332f-
3aca-9fe3-907616891cc7","readOnly":true,"resources":[{"accountId":"908027405956","type":"AWS::S3::Bucket","ARN":"arn:aws:s3:::bucket-lab9-
2265"}],"eventType":"AwsApiCall","managementEvent":true,"recipientAccountId":"908027405956","sharedEventID":"1af4ecfe-1c34-448b-9320-
bb8dfc8dbd8f","eventCategory":"Management"},{"eventVersion":"1.11","userIdentity":
{"type":"Root","principalId":"908027405956","arn":"arn:aws:iam::908027405956:root","accountId":"908027405956","accessKeyId":"ASIA5G2VGU2CAR7SOBJA","userName":"sahil021",
"sessionContext":{"attributes":{"creationDate":"2025-04-02T18:01:56Z","mfaAuthenticated":"true"}},"invokedBy":"AWS Internal"},"eventTime":"2025-04-
02T20:54:47Z","eventSource":"kms.amazonaws.com","eventName":"GenerateDataKey","awsRegion":"ap-south-1","sourceIPAddress":"AWS Internal","userAgent":"AWS
Internal","requestParameters":{"keyId":"arn:aws:kms:ap-south-1:908027405956:key/d0a4851f-c4fc-4c82-a0e6-1681331a9a24","encryptionContext":
{"aws:s3:arn":"arn:aws:s3:::bucket-lab9-2265"},"keySpec":"AES_256"},"responseElements":null,"requestID":"08bb12ed-c9c4-4d6f-b3e7-5d6c8ac36615","eventID":"67f2c8c8-3f49-
4238-bb1b-827c9f8c88f1","readOnly":true,"resources":[{"accountId":"908027405956","type":"AWS::KMS::Key","ARN":"arn:aws:kms:ap-south-1:908027405956:key/d0a4851f-c4fc-
4c82-a0e6-
1681331a9a24"}],"eventType":"AwsApiCall","managementEvent":true,"recipientAccountId":"908027405956","eventCategory":"Management","sessionCredentialFromConsole":"true"},
{"eventVersion":"1.10","userIdentity":
```