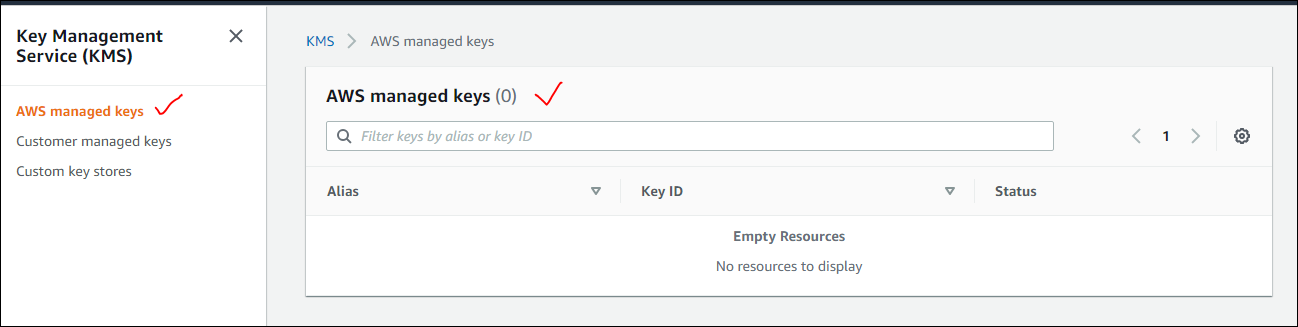
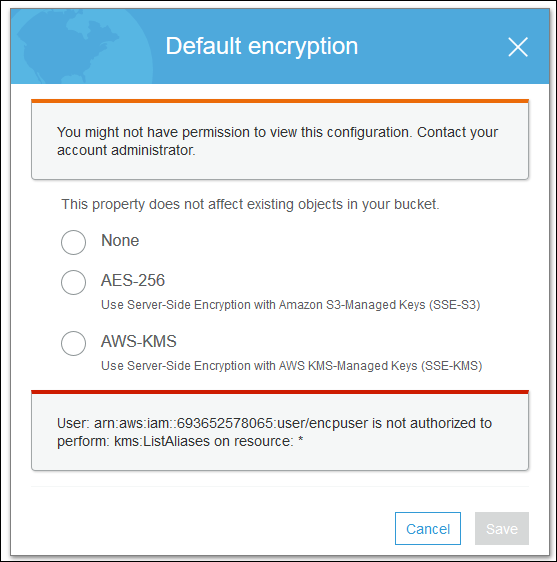
13-06-20

Not able to see the KMS managed keys [ aws/s3 ]



------------------------------------------------------------------------------------------

IAM user who has only S3 admin access permissions, but doesn’t have full admin access. when he tries to apply the encryption at bucket level it is showing an error message. Cant he give KMS encryption to any bucket.



**User: arn:aws:iam::693652578065:user/test is not authorized to perform: kms:ListAliases on resource: \* --** this is the error fro IAM user who doesn’t have Amdin permission. To create the encryption at object level. He is failing, so we have given admin access to “test” user then he is able to apply encrypt the object.

this is the error, IAM should have admin access to give AWS-KMS encryption.

--------------------------------------------------------------------------------------------------------------------------------------

1. Cant we apply any policy to restrict the IAM user to create a new bucket.

Inn line policy can be applied to restrict the user to create a new bucket.

1. Do we really need to make a policy at bucket level to restrict user to create a bucket or upload a bucket instead of this we can make an INLINE policy at IAM level while we are creating him, there we can deny him to perform certain actions for specific Resources by providing the ARN. Correct me if iam wrong.