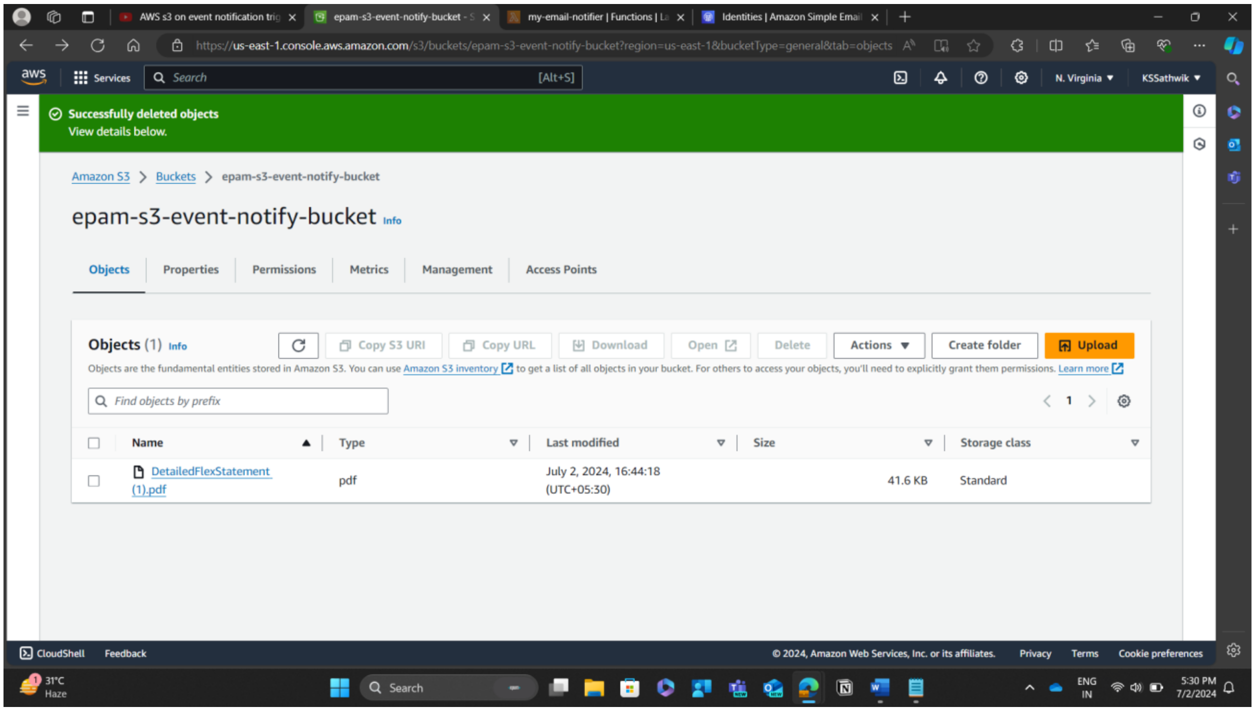
EMAIL



https://us-east-1.console.aws.amazon.com/s3/buckets/epam-s3-event-notify-bucket?region=us-east-1&bucketType=general&tab=objects

Successfully deleted objects
View details below.

Amazon S3 > Buckets > epam-s3-event-notify-bucket

epam-s3-event-notify-bucket Info

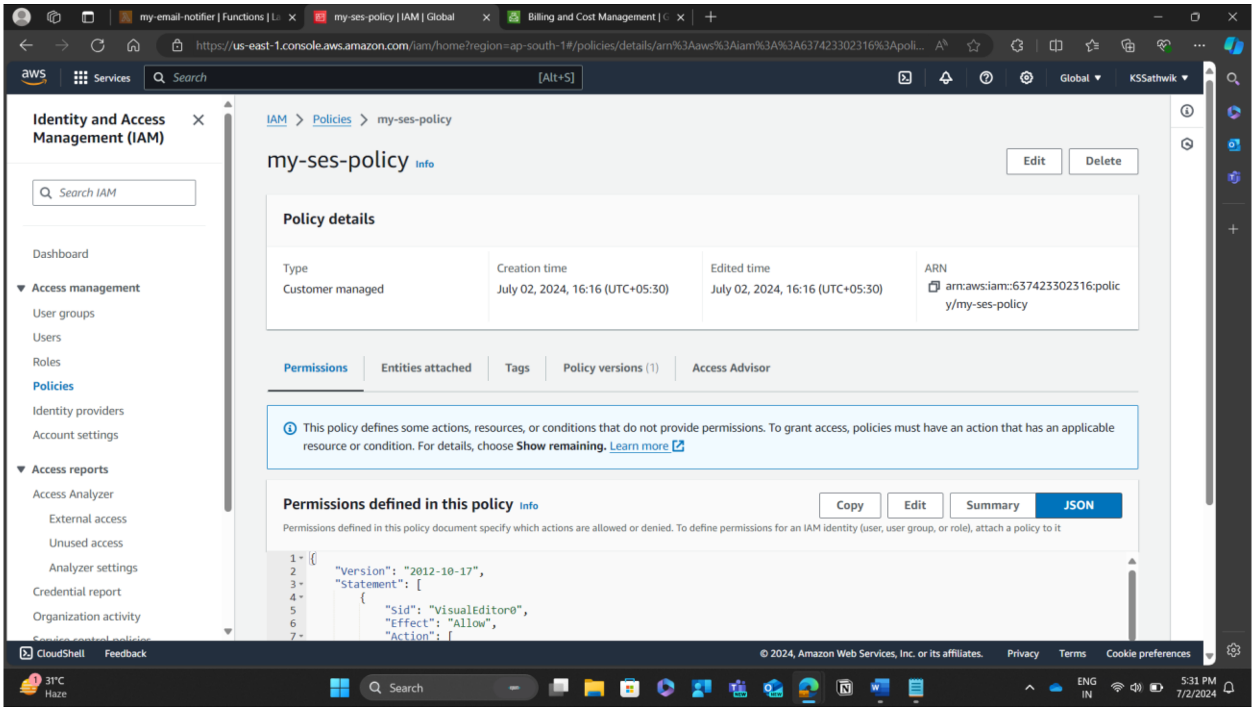
Objects (1) Info

Objects are the fundamental entities stored in Amazon S3. You can use Amazon S3 inventory to get a list of all objects in your bucket. For others to access your objects, you'll need to explicitly grant them permissions. Learn more

Find objects by prefix

□	Name	Type	Last modified	Size	Storage class
□	DetailedFlexStatement (1).pdf	pdf	July 2, 2024, 16:44:18 (UTC+05:30)	41.6 KB	Standard

© 2024, Amazon Web Services, Inc. or its affiliates.



https://us-east-1.console.aws.amazon.com/iam/home?region=ap-south-1#/policies/details/arn%3Aaws%3Aiam%3A%3A637423302316%3Apoli...

IAM > Policies > my-ses-policy

my-ses-policy Info

Policy details

Type	Creation time	Edited time	ARN
Customer managed	July 02, 2024, 16:16 (UTC+05:30)	July 02, 2024, 16:16 (UTC+05:30)	arn:aws:iam::637423302316:policy/my-ses-policy

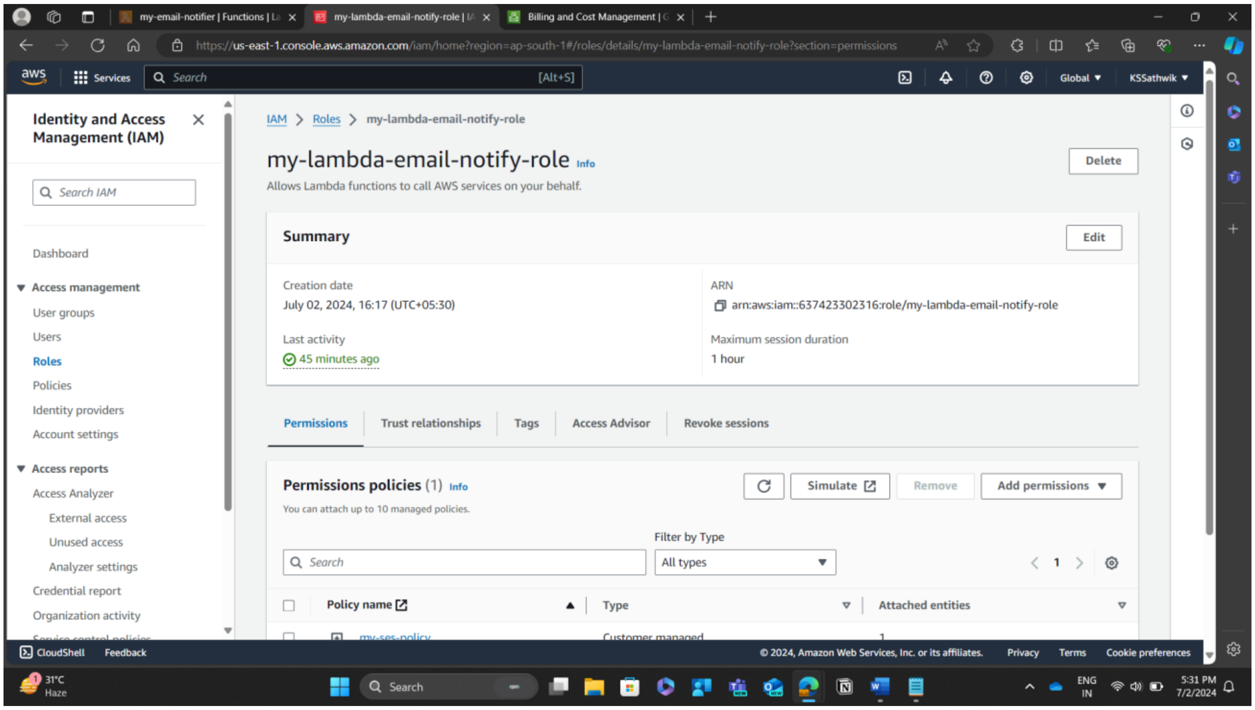
This policy defines some actions, resources, or conditions that do not provide permissions. To grant access, policies must have an action that has an applicable resource or condition. For details, choose **Show remaining.** Learn more

Permissions defined in this policy Info

Permissions defined in this policy document specify which actions are allowed or denied. To define permissions for an IAM identity (user, user group, or role), attach a policy to it

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "VisualEditor0",
            "Effect": "Allow",
            "Action": [
```

© 2024, Amazon Web Services, Inc. or its affiliates.



my-lambda-email-notify-role

Allows Lambda functions to call AWS services on your behalf.

Summary

Creation date
July 02, 2024, 16:17 (UTC+05:30)

Last activity
45 minutes ago

ARN
arn:aws:iam::637423302316:role/my-lambda-email-notify-role

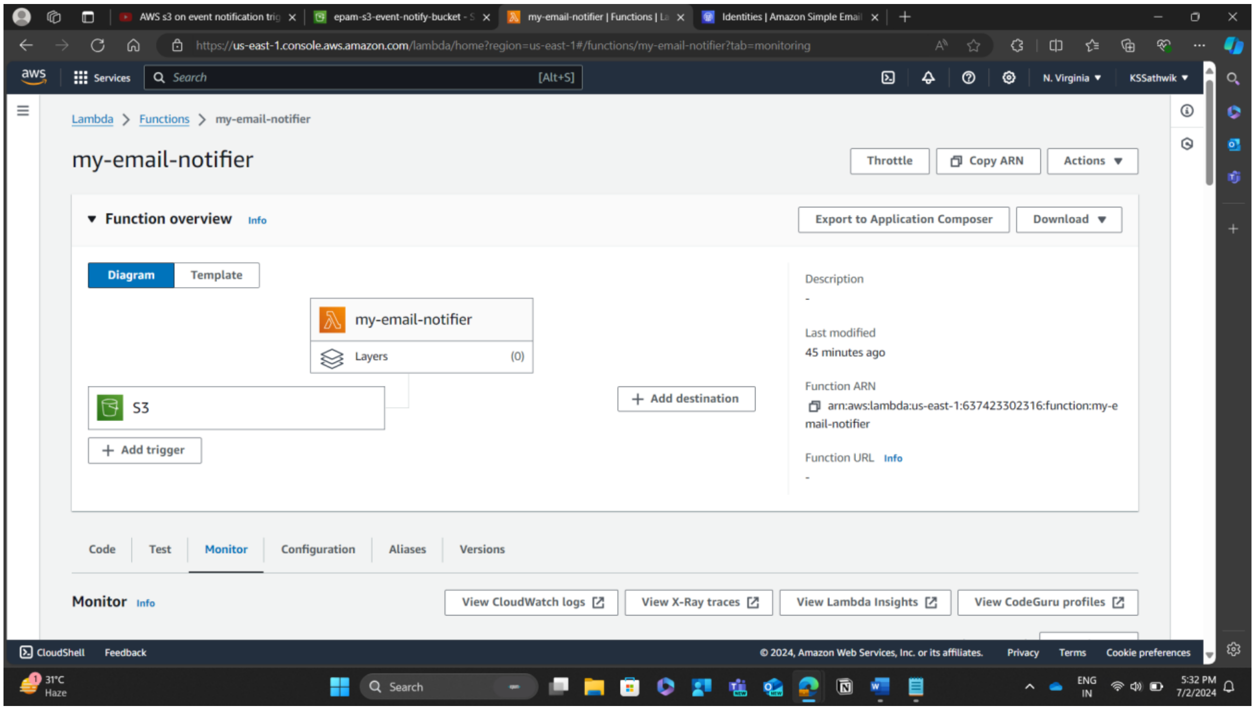
Maximum session duration
1 hour

Permissions policies (1)

You can attach up to 10 managed policies.

Policy name	Type	Attached entities
my-ses-policy	Customer managed	1

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "VisualEditor0",
      "Effect": "Allow",
      "Action": [
        "ec2:Describe*",
        "ec2:RunInstances",
        "ec2:StartInstances",
        "ec2:StopInstances",
        "cloudwatch:DescribeAlarms",
        "compute-optimizer:GetEnrollmentStatus",
        "elasticloadbalancing:Describe*"
      ],
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "ec2:Region": "us-east-1"
        }
      }
    },
    {
      "Sid": "SESLimitedAccess",
      "Effect": "Allow",
      "Action": [
        "ses:CreateCustomVerificationEmailTemplate",
        "ses:Describe*",
        "ses:Get*",
        "ses:List*",
        "ses:VerifyEmailAddress",
        "ses:VerifyEmailIdentity",
        "ses:CreateEmailIdentity",
        "ses:TagResource",
        "route53:List*",
        "ses:SendEmail",
        "ses:SendRawEmail",
        "ses:SendTemplatedEmail"
      ],
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "aws:RequestedRegion": "us-east-1"
        }
      }
    },
    {
      "Effect": "Allow",
      "Action": [
        "logs:*"
      ],
      "Resource": "arn:aws:logs:*:*:*"
    },
    {
      "Effect": "Allow",
      "Action": [
        "s3:GetObject",
        "s3:PutObject"
      ],
      "Resource": "arn:aws:s3:::*"
    }
  ]
}
```



Description
-

Last modified
45 minutes ago

Function ARN
arn:aws:lambda:us-east-1:637423302316:function:my-email-notifier

Function URL Info
-

```
import boto3

import json


def lambda_handler(event, context):


  for e in event["Records"]:

    bucketName = e["s3"]["bucket"]["name"]

    objectName = e["s3"]["object"]["key"]

    eventName = e["eventName"]


  bClient = boto3.client("ses")


  eSubject = 'AWS' + str(eventName) + 'Event'


  eBody = """
```

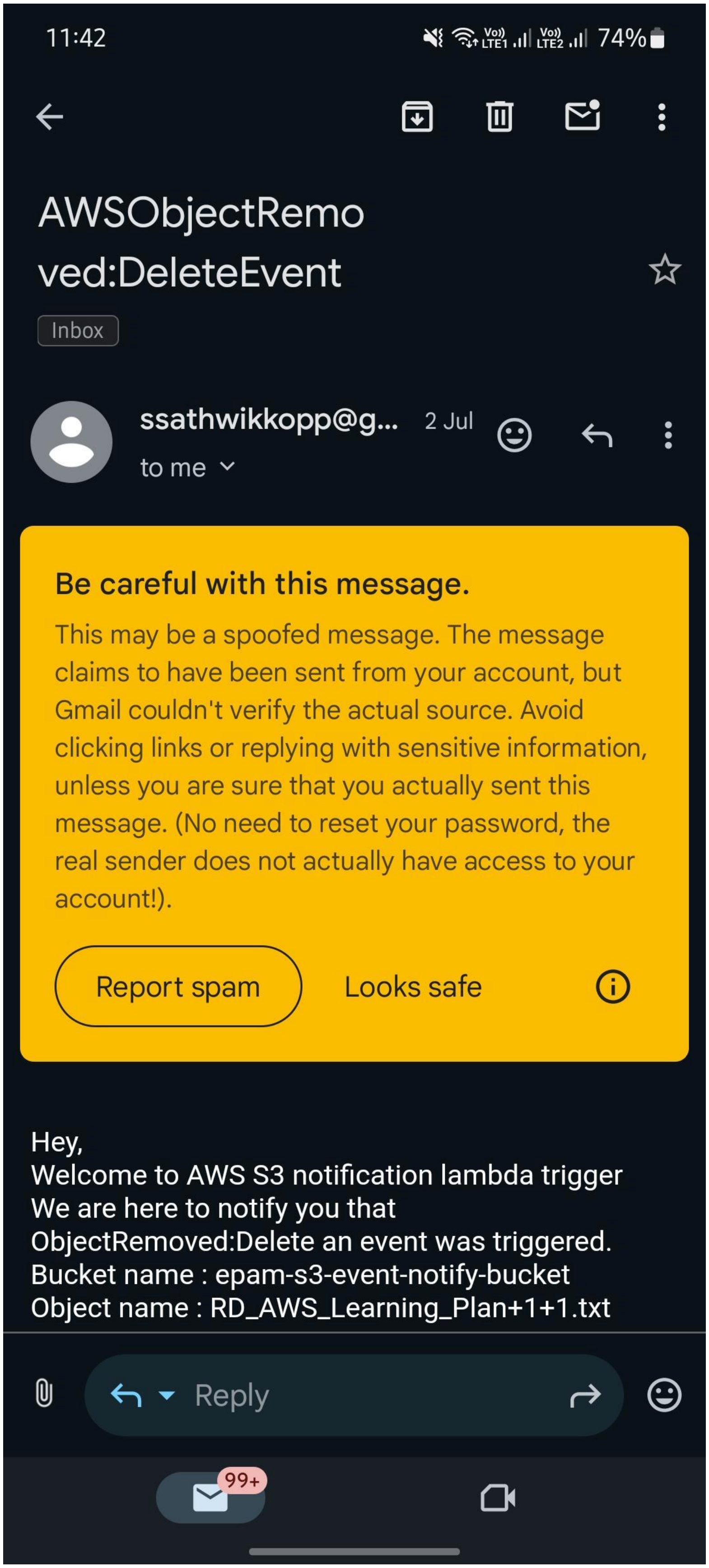
```
        <br>
        Hey,<br>

        Welcome to AWS S3 notification lambda trigger<br>

        We are here to notify you that {} an event was triggered.<br>
        Bucket name : {} <br>
        Object name : {}
        <br>
    """.format(eventName, bucketName, objectName)

    send = {"Subject": {"Data": eSubject}, "Body": {"Html": {"Data": eBody}}}
    result = bClient.send_email(Source= "ssathwikkopp@gmail.com", Destination= {"ToAddresses": ["ssathwikkopp@gmail.com"]}, Message= send)

    return {
        'statusCode': 200,
        'body': json.dumps(result)
    }
```



AWSObjectRemoved:DeleteEvent

ssathwikkopp@g... 2 Jul

to me

Be careful with this message.

This may be a spoofed message. The message claims to have been sent from your account, but Gmail couldn't verify the actual source. Avoid clicking links or replying with sensitive information, unless you are sure that you actually sent this message. (No need to reset your password, the real sender does not actually have access to your account!).

Hey,
Welcome to AWS S3 notification lambda trigger
We are here to notify you that
ObjectRemoved:Delete an event was triggered.
Bucket name : epam-s3-event-notify-bucket
Object name : RD_AWS_Learning_Plan+1+1.txt