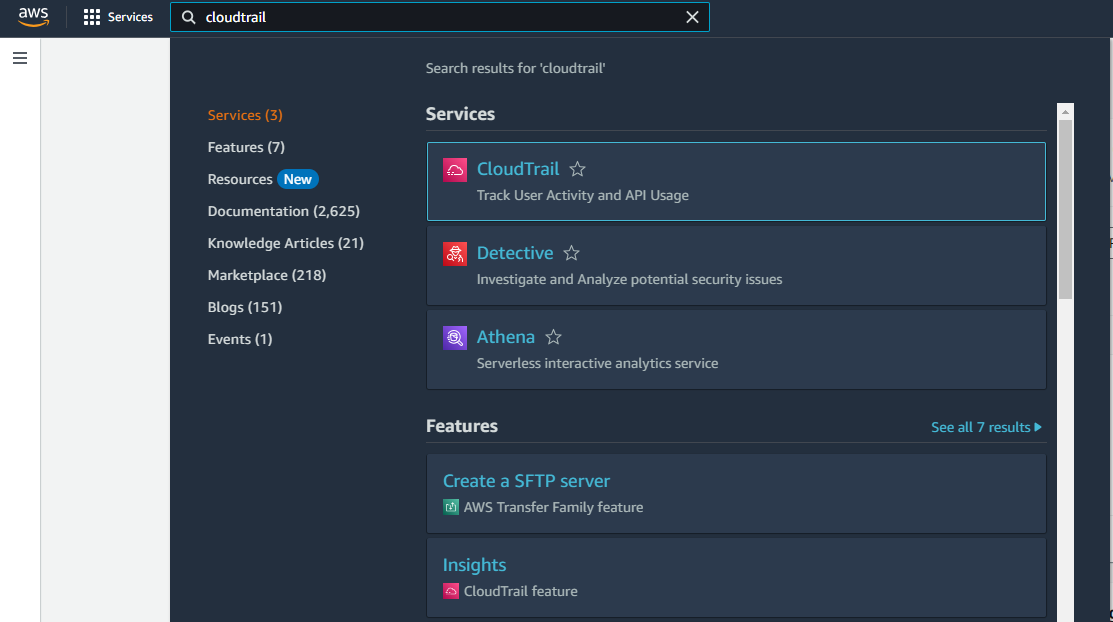
Diksha Sharma

Monitor Infrastructure with AWS CloudWatch and CloudTrail

STEP 1:

I searched for CloudTrail in the search bar from the main AWS dashboard.



STEP 2:

I clicked on ‘Create a trail’

A screenshot of a web page

Description automatically generated

STEP 3:

I gave it an appropriate name and created the Trail.

A screenshot of a computer

Description automatically generated

STEP 4: Under Data Events, I enabled S3, Lambda

A screenshot of a computer

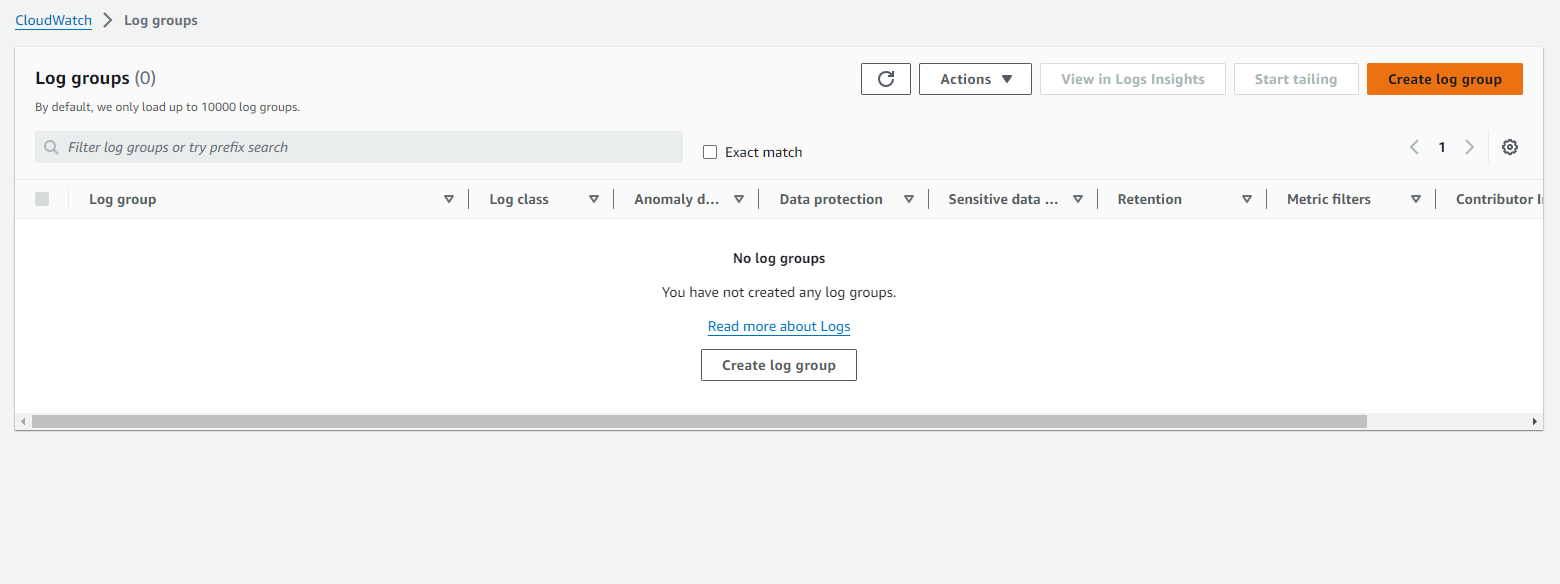
Description automatically generated

STEP 5: Searched for CloudWatch

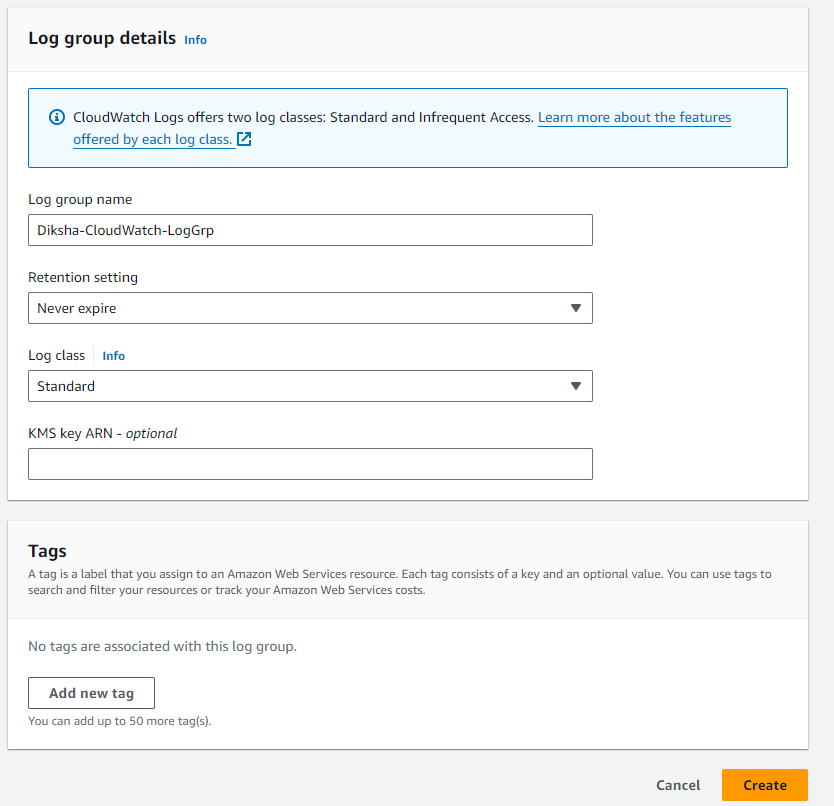
A screenshot of a computer

Description automatically generated

STEP 6: I clicked on Create Log Group



STEP 7: Created the log group



STEP 8: Enabled CloudWatch Logs for Diksha-Monitor-Trail

A screenshot of a computer

Description automatically generated

STEP 9: Creating Alarm

A screenshot of a computer

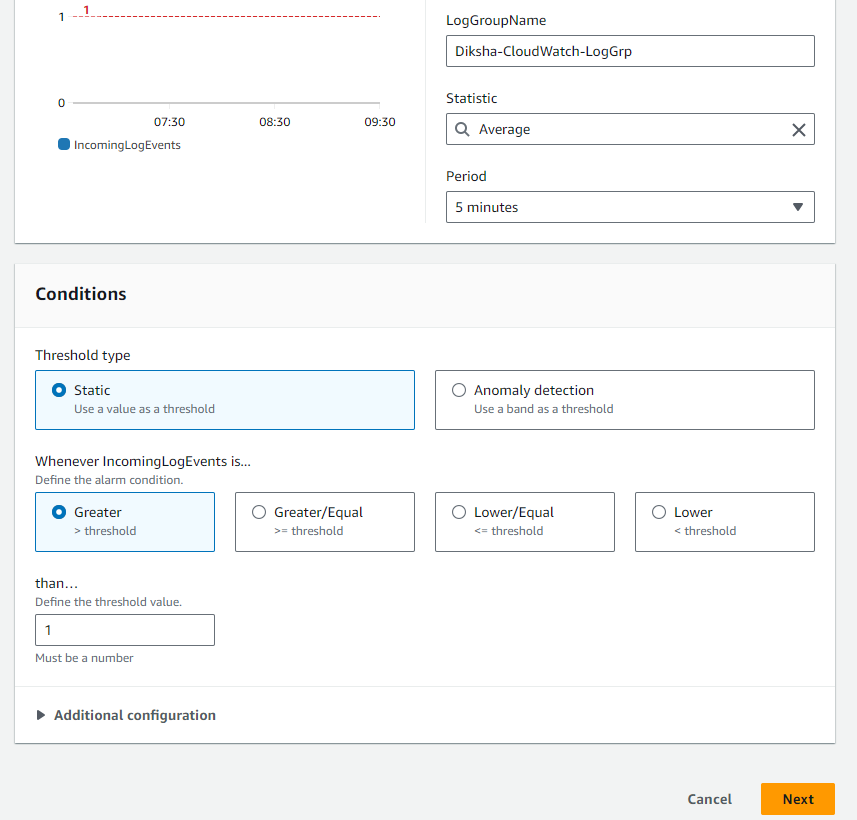
Description automatically generated

STEP 10: Selected Diksha-CloudWatch-LogGrp as the metric

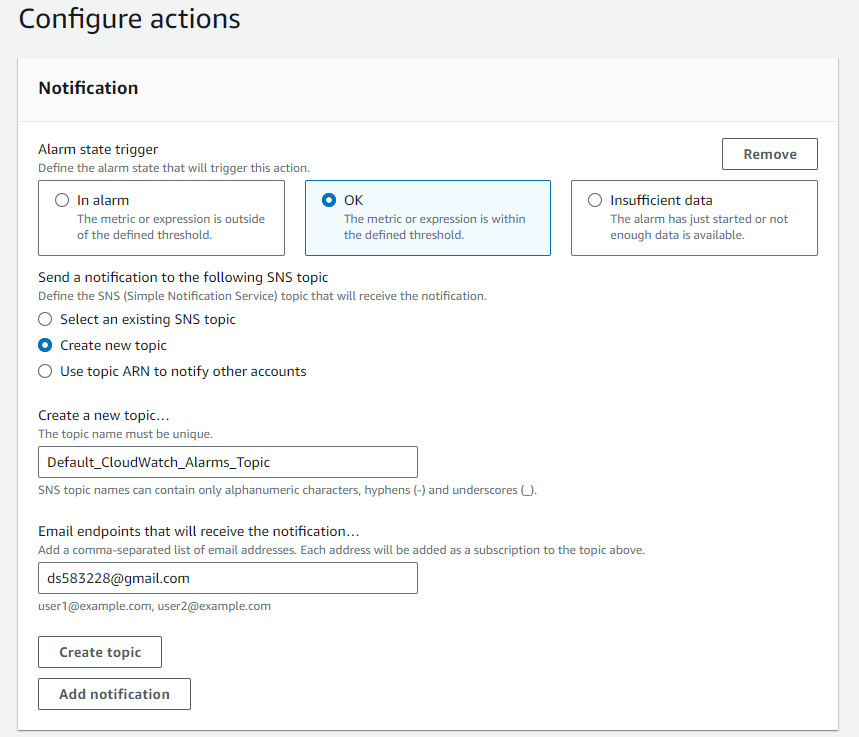
A screenshot of a graph

Description automatically generated

STEP 11: Set threshold to greater than 1

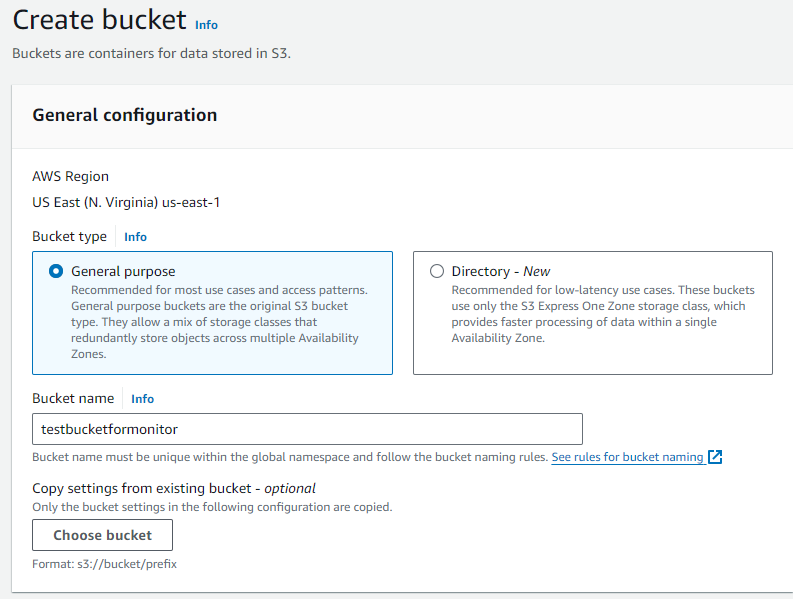


STEP 12: Created new notification action



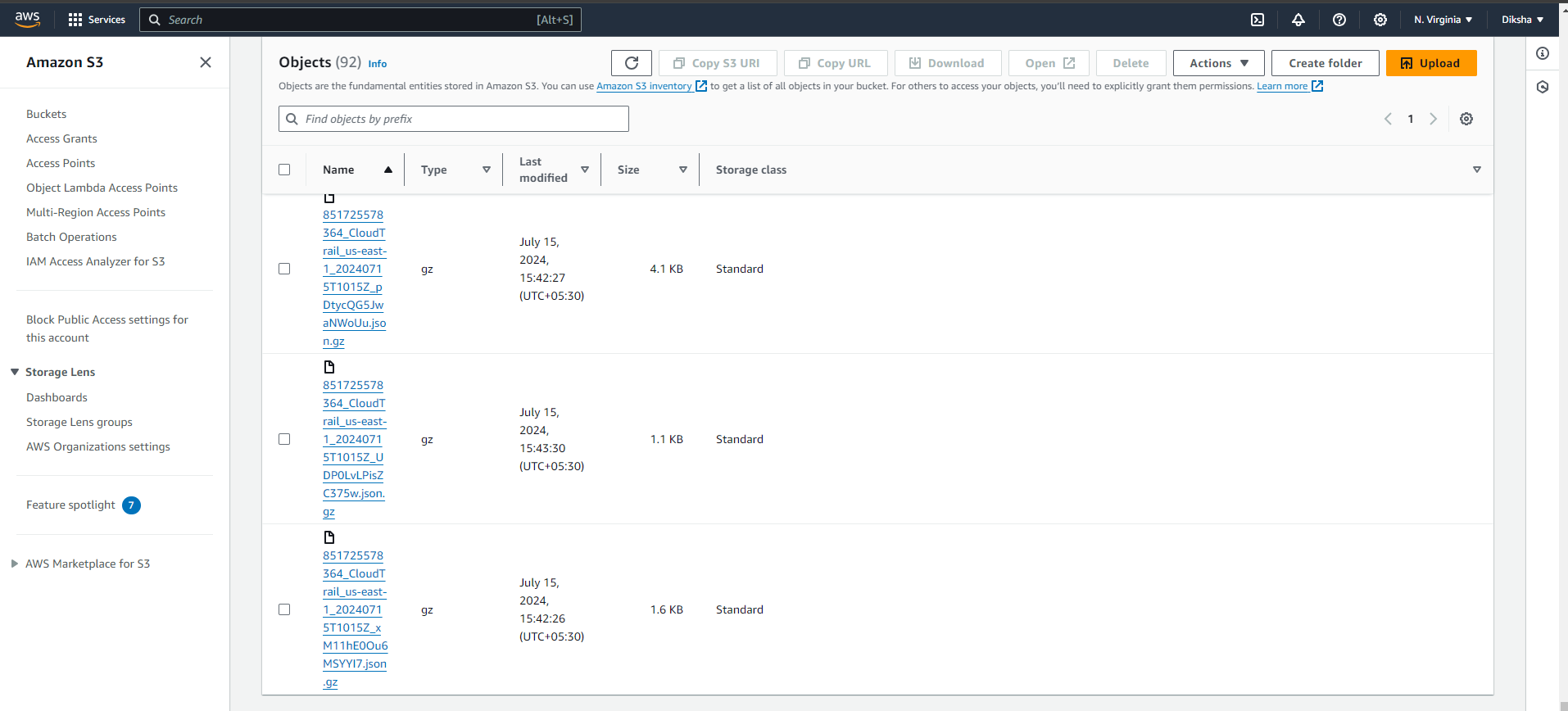
TESTING THE SETUP

Step 1: Creating a test S3 bucket

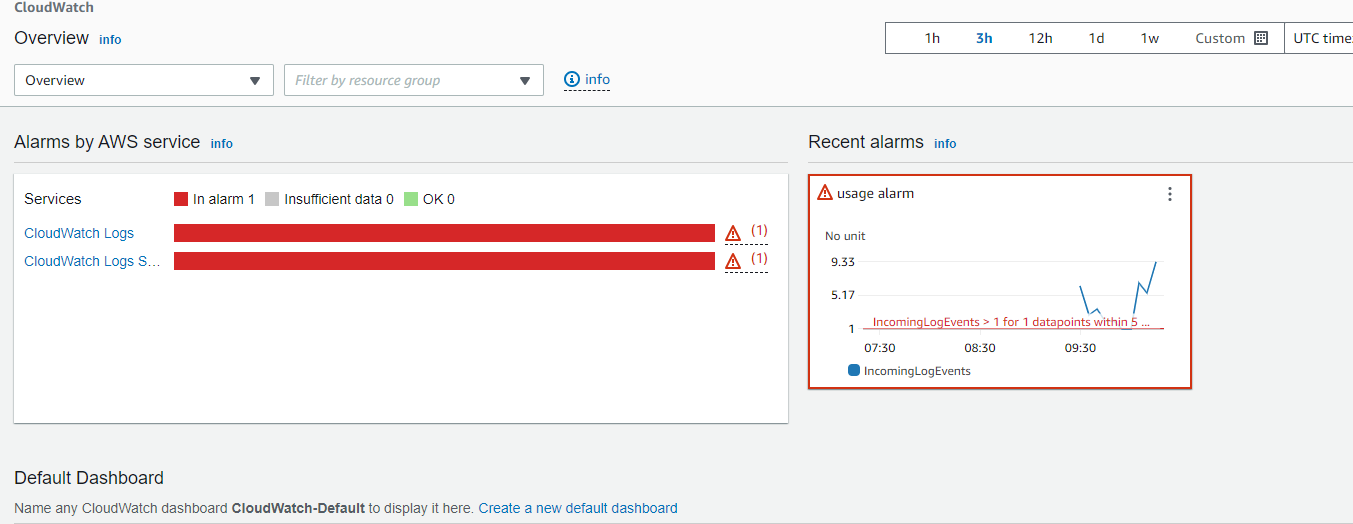


Final Conclusion

By visiting Amazon S3 > Buckets > aws-cloudtrail-logs-851725578364-4dcb0dd8 > AWSLogs/851725578364/CloudTrail/us-east-1/2024/07/15/, I verified that the monitor is working and correct log files have been created as per my activity. The log files range from July 15, 2024 13:16:36 to July 15, 2024 15:42:26 (This is when I created the test S3 bucket).

I had also created an alarm for email notification, but that is still pending verification and should work once approved. 

I have verified the same on my CloudWatch Dashboard here:



The scenario: The usage log file was created and alarm was hit when I created 1 S3 bucket (As mentioned in my preferences, where I had set the usage limit as 1). The dashboard correctly displays the data. The email however wasn’t triggered as it was still under verification.