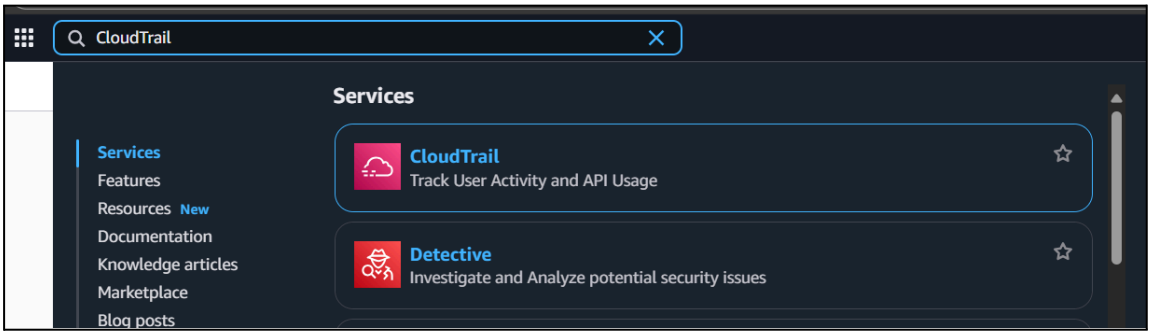
Week 4: Implementing Cloud Logging and Monitoring

Name- Saish Dhiwar
PRN- 2124UCSM2011
Email- saish.dhiwar_24ucs@sanjivani.edu.in

Task- 1) Enable CloudTrail/Cloud Audit Logs.
2) Configure alerts for suspicious activity.
3) Document findings.

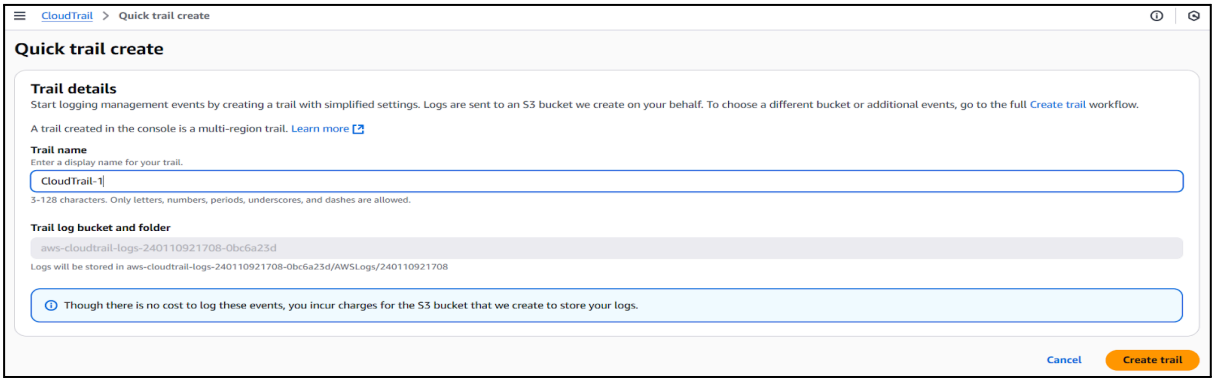
Task 1- Enable Cloud Trail/ Cloud Audit Logs.

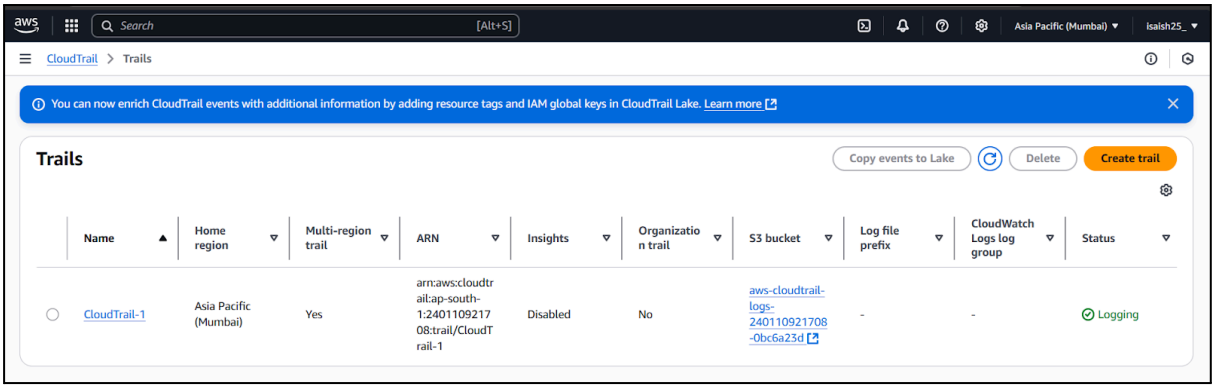
1) Log in to AWS Console.
2) Search & open CloudTrail from the Services menu.



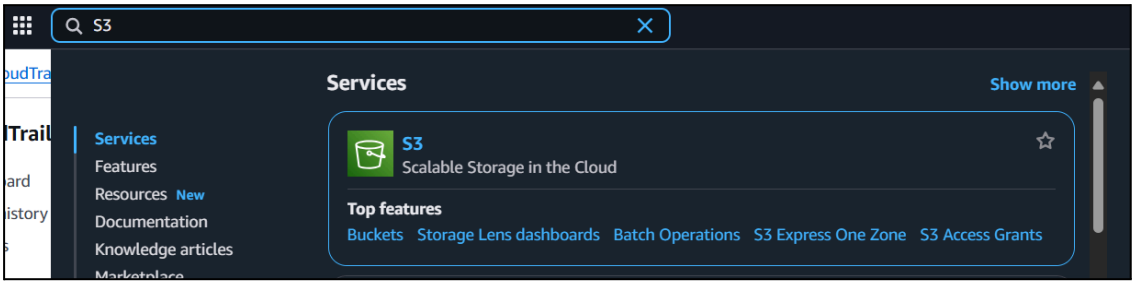
3) Click to Create Trail.

4) Fill in Trail Name CloudTrail-1, and then click to create Trail.





5) Set up S3 Bucket to store logs: Create a new bucket.

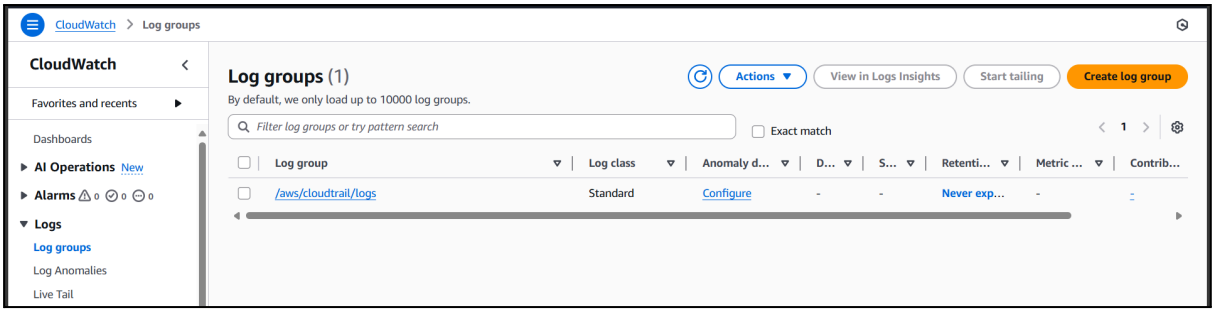


6) Enable CloudWatch Logs, Create new Log Group:/aws/cloudtrail/logs, Allow to create IAM role automatically, then click Create trail.

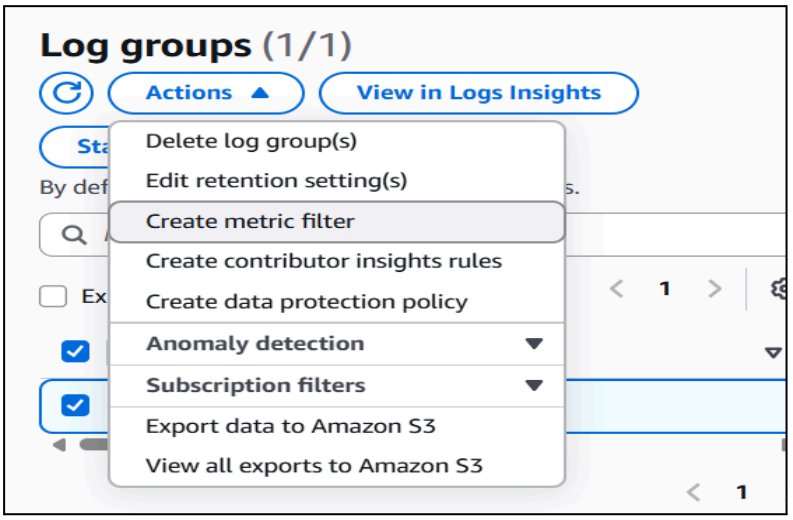
Task 2- Configure alerts for suspicious activity.

1) Go to CloudWatch, Log Groups.

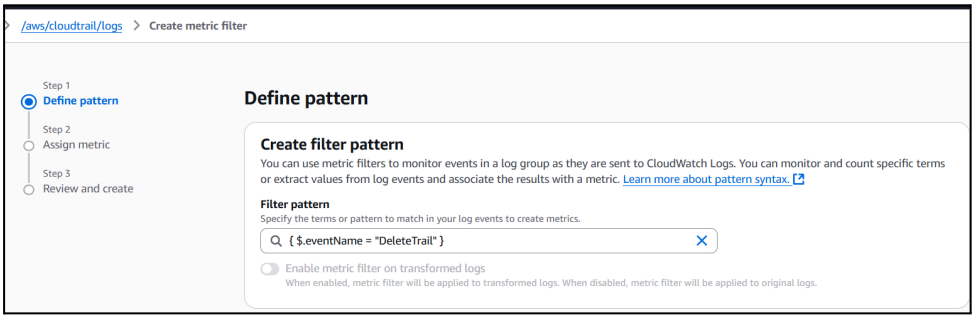
2) Select your log group: /aws/cloudtrail/logs



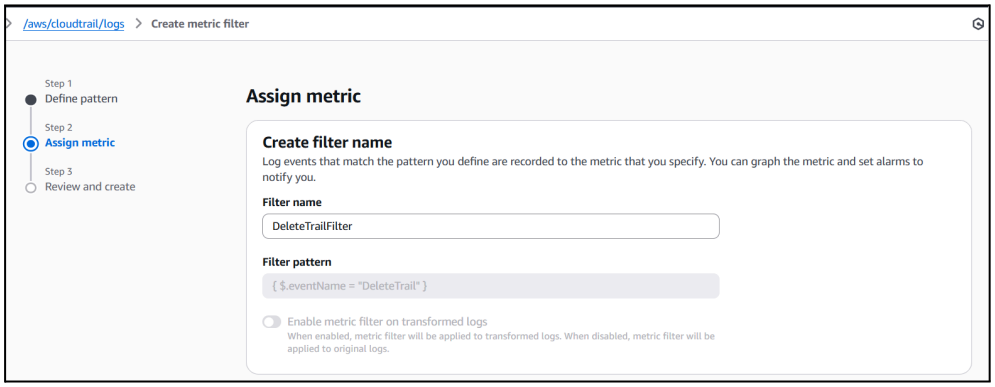
3) Click Actions→ Create Metric Filter.



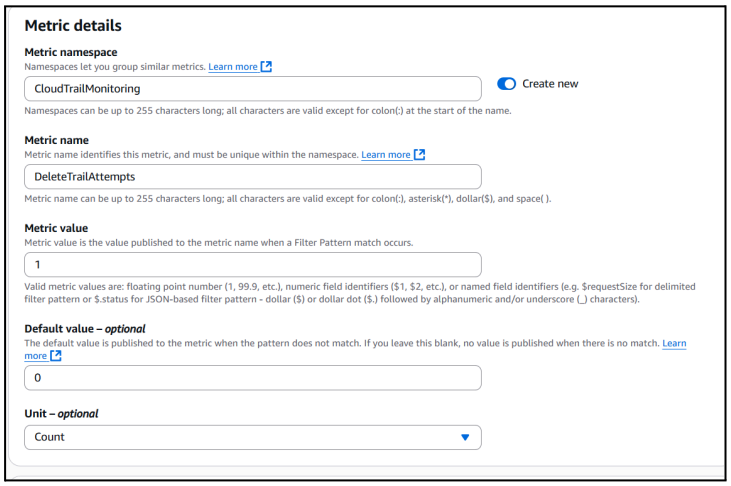
4) Paste the filter pattern, and then click Next.



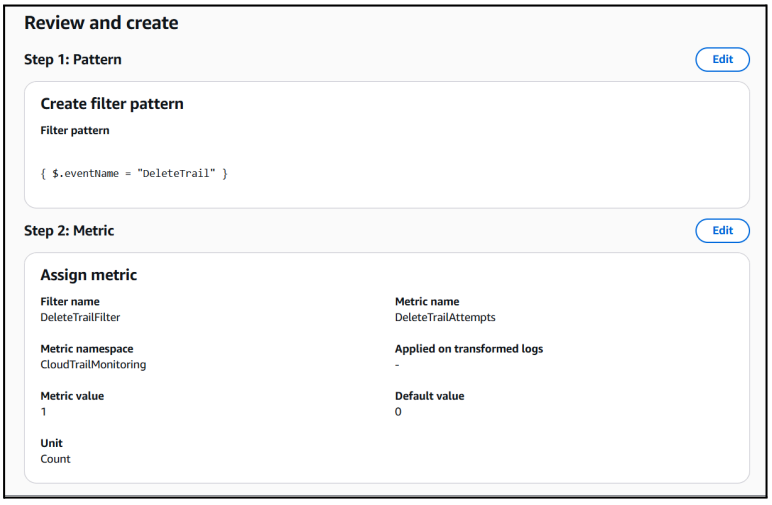
5) Next step is to create a filter name. Enter the filter Name.



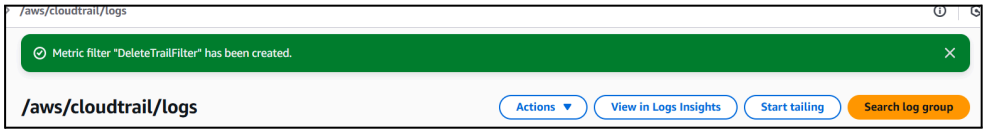
6) Then Enter the Matrix Details.



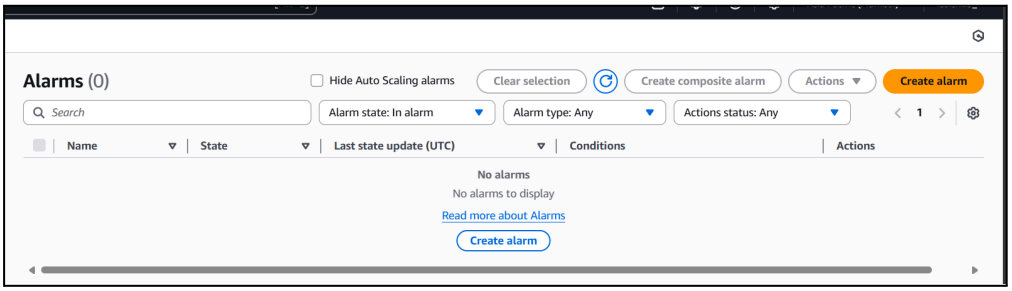
7) Then click Create Matrix.



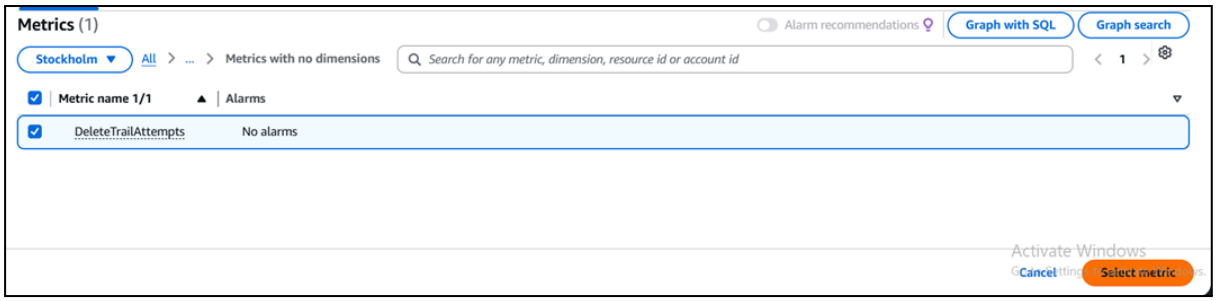
8) Matrix filter created successfully.



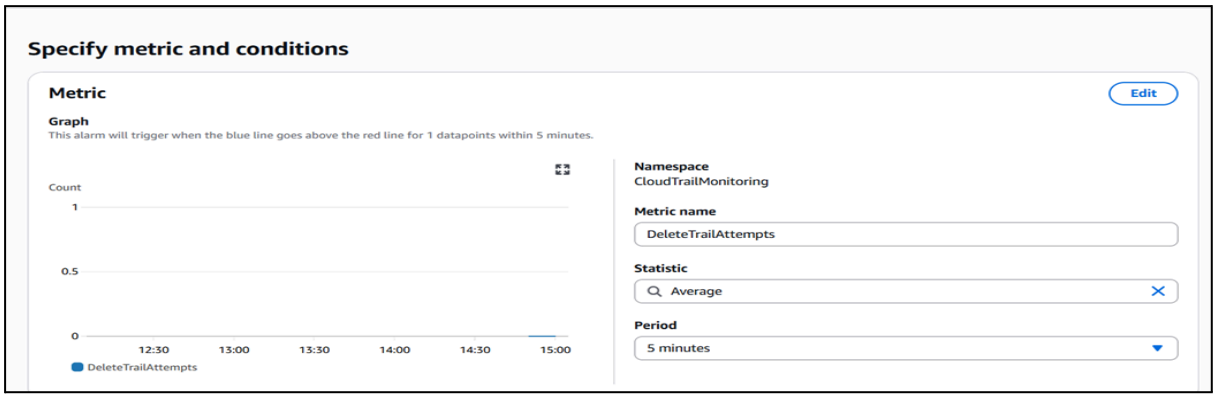
9) Go to CloudWatch→ Alarms→ Create Alarm.



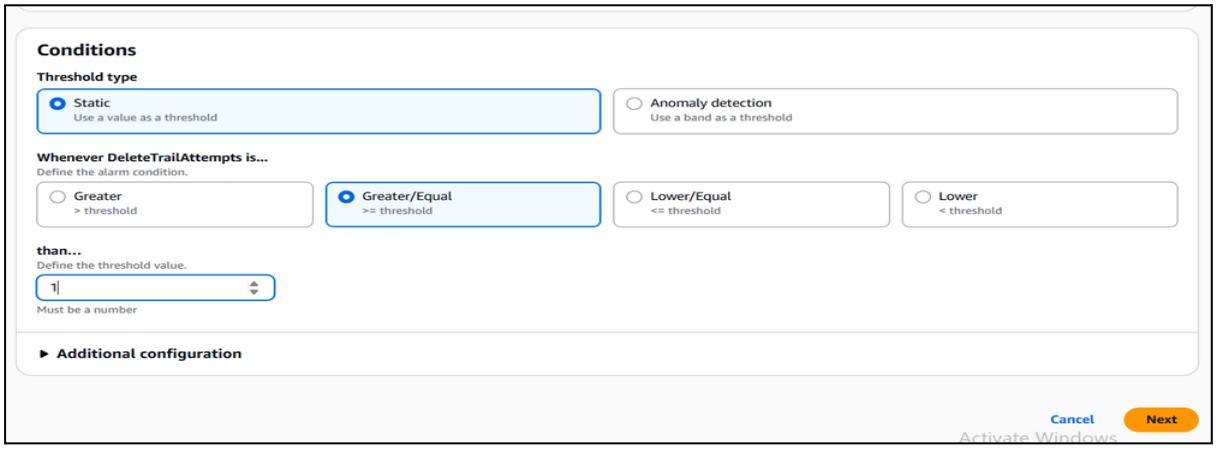
10) Select Metric



11) Set threshold: Static, Condition: Greater than or equal to 1, Period: 5 minutes.

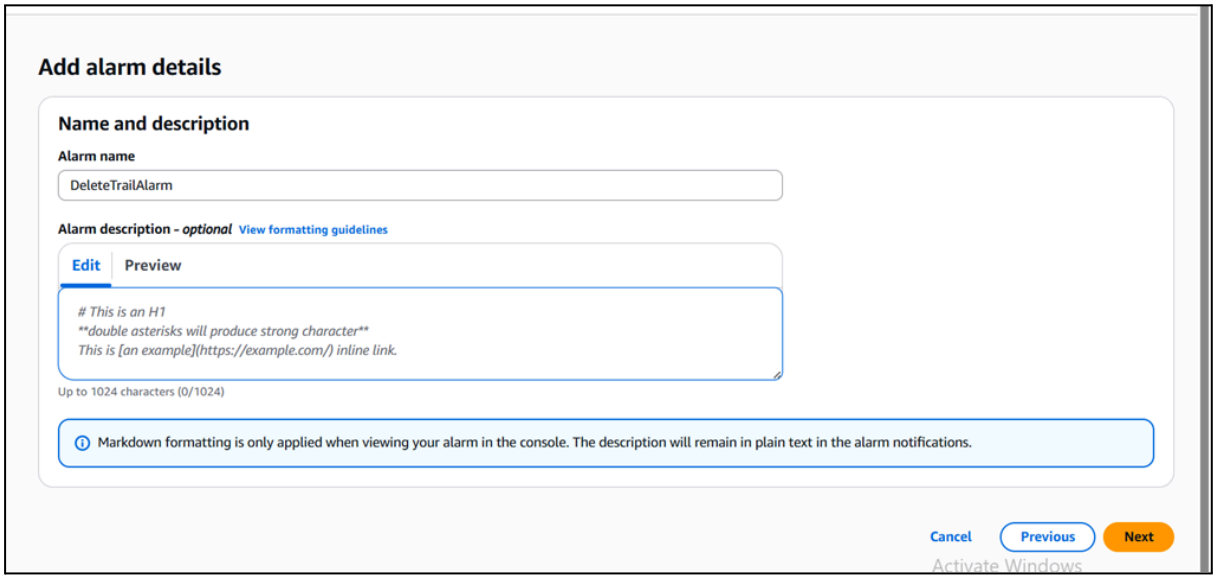


12) Set Condition, and then click Next



13) Add Configure action Details

14) Add Alarm Details, and then click Next.



15) Set Alarm Successfully