VIT®

Vellore Institute of Technology

(Deemed to be University under section 3 of UGC Act, 1956)

PROJECT FINAL REPORT

Submitted by

19BCE2119	-	GAURAV KUMAR SINGH
19BCI0202	-	CHIRAG AGARWAL SANJAY
19BCE2069	-	P LOHITH SASI ANVESH

TITLE

AMAZON WEB SERVICE(AWS) CLOUD SECURITY

INTRODUCTION:

AWS is an extensively an accessible cloud stage that offers a few on-request activities like compute power, database storage, content delivery, etc., to help corporates to scale and develop. The main reason why numerous organizations use AWS is on their businesses is that it offers various sorts of capacity to browse and is effectively available also. It tends to be utilized for capacity and document ordering just as to run basic business applications.

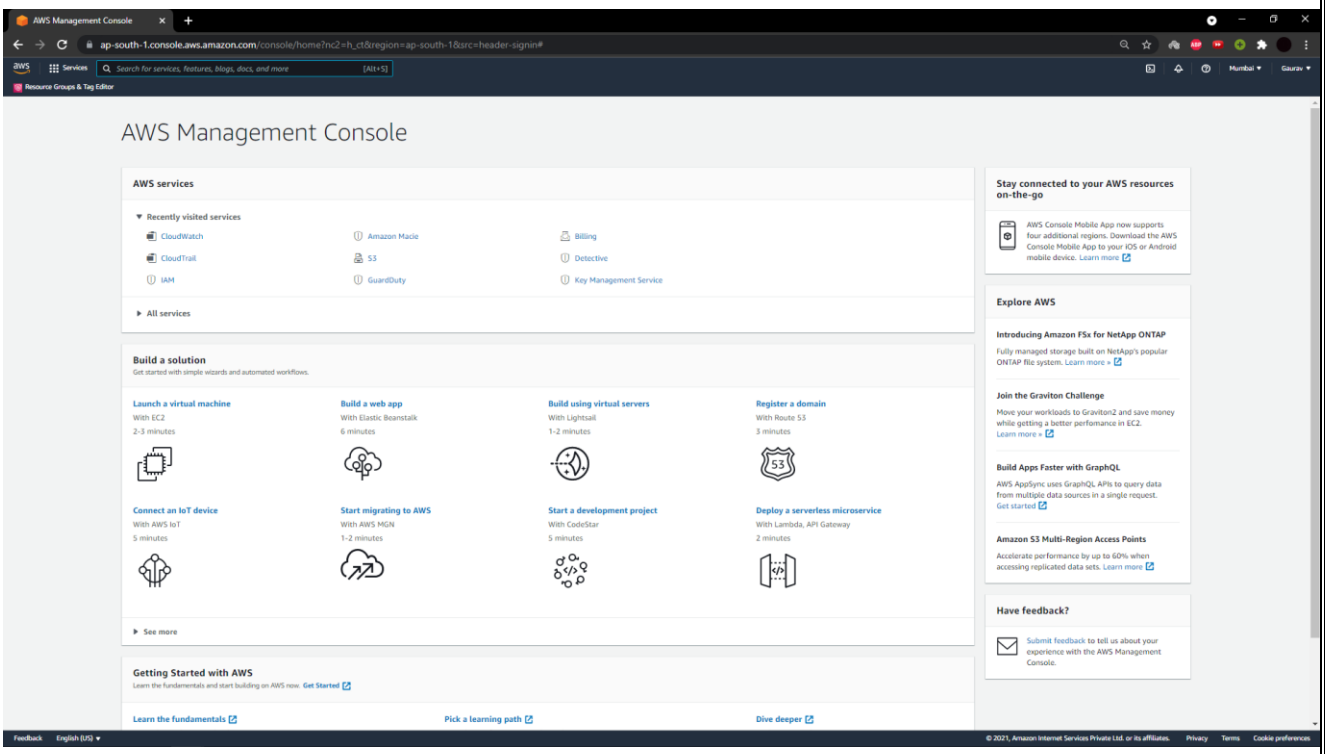
In this project we mainly focussed on network cloud security. In database we have done on cloud storage security so, we have used S3 buckets nothing but storage buckets. And for log details we have used cloud watch and cloud security services. We have used cloud tail for getting alerts and we have guard duty service for complete log analysis, for providing access controls we have used IAM(identify and access management). And we have used Amazon macie for policy findings and sensitive data findings.

OBJECTIVE :

Our main motto is to develop secure cloud computing environment with Amazon web services (AWS).

Home Page:

This the home page of AWS management console which consists of AWS services like cloud tail, cloud watch, S3, GuardDuty, IAM(identify and access management), billing, detective and key management service.

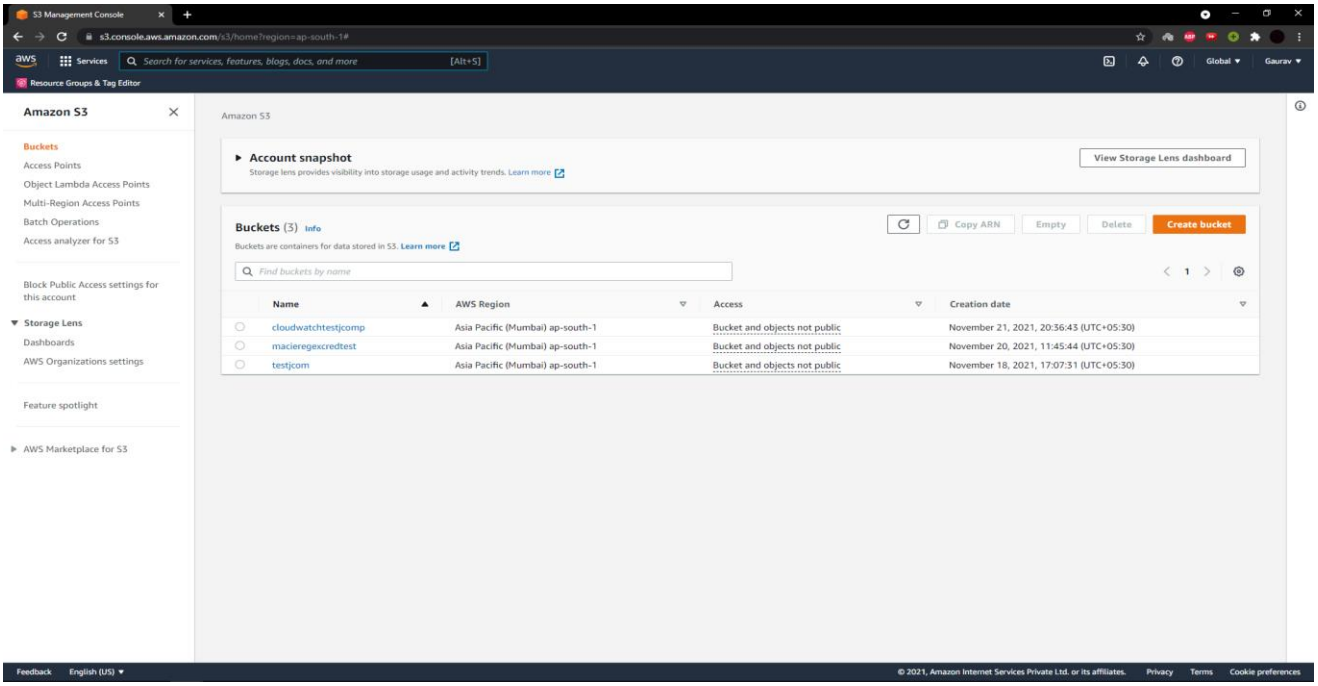


S3 (storage bucket):

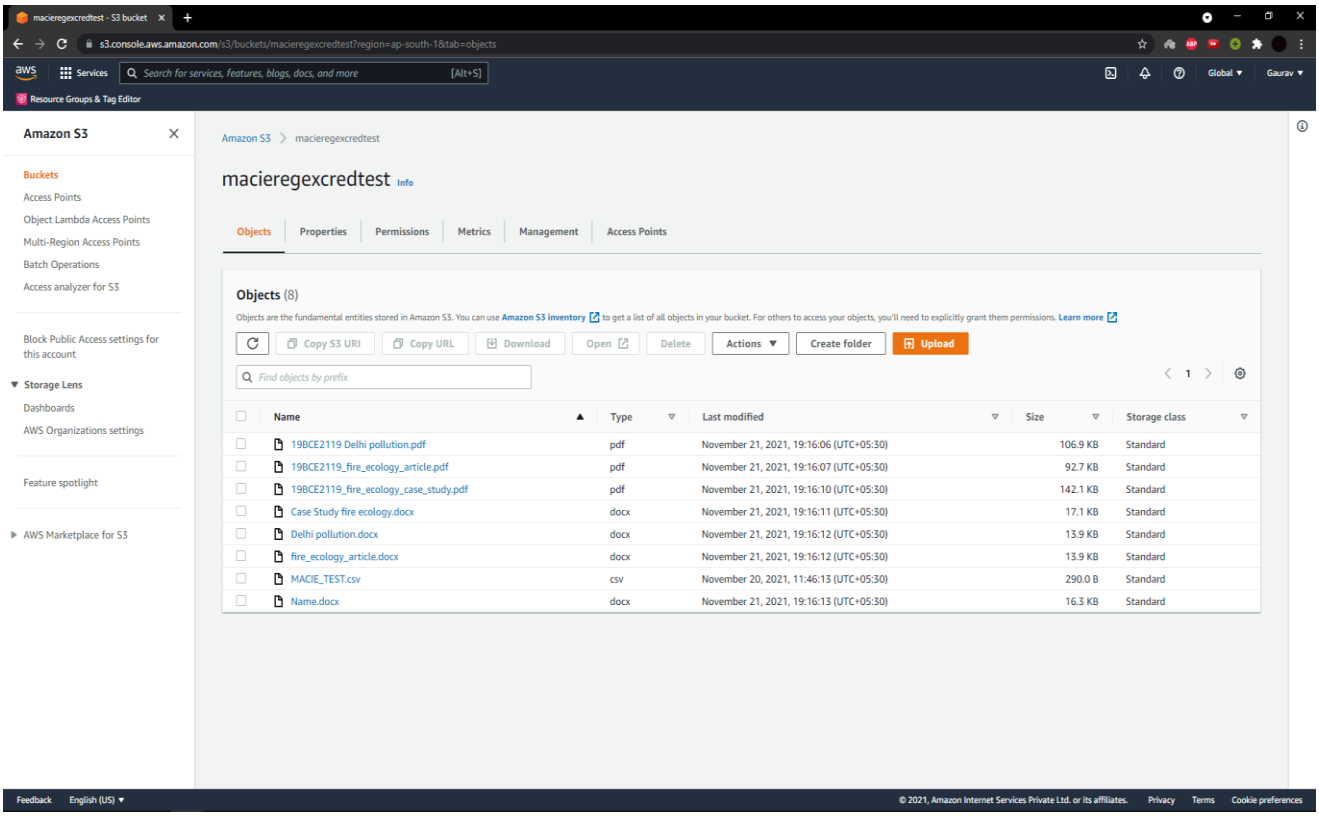
Amazon S3 gives object storage through a web interface. Its worked to store, protect and recover information from buckets whenever from anyplace on any gadget. A client makes a bucket, and the bucket stores objects in the cloud.

- S3 is basically a storage service which amazon provides for free and buckets are folders.
- And we have created the three buckets in S3.

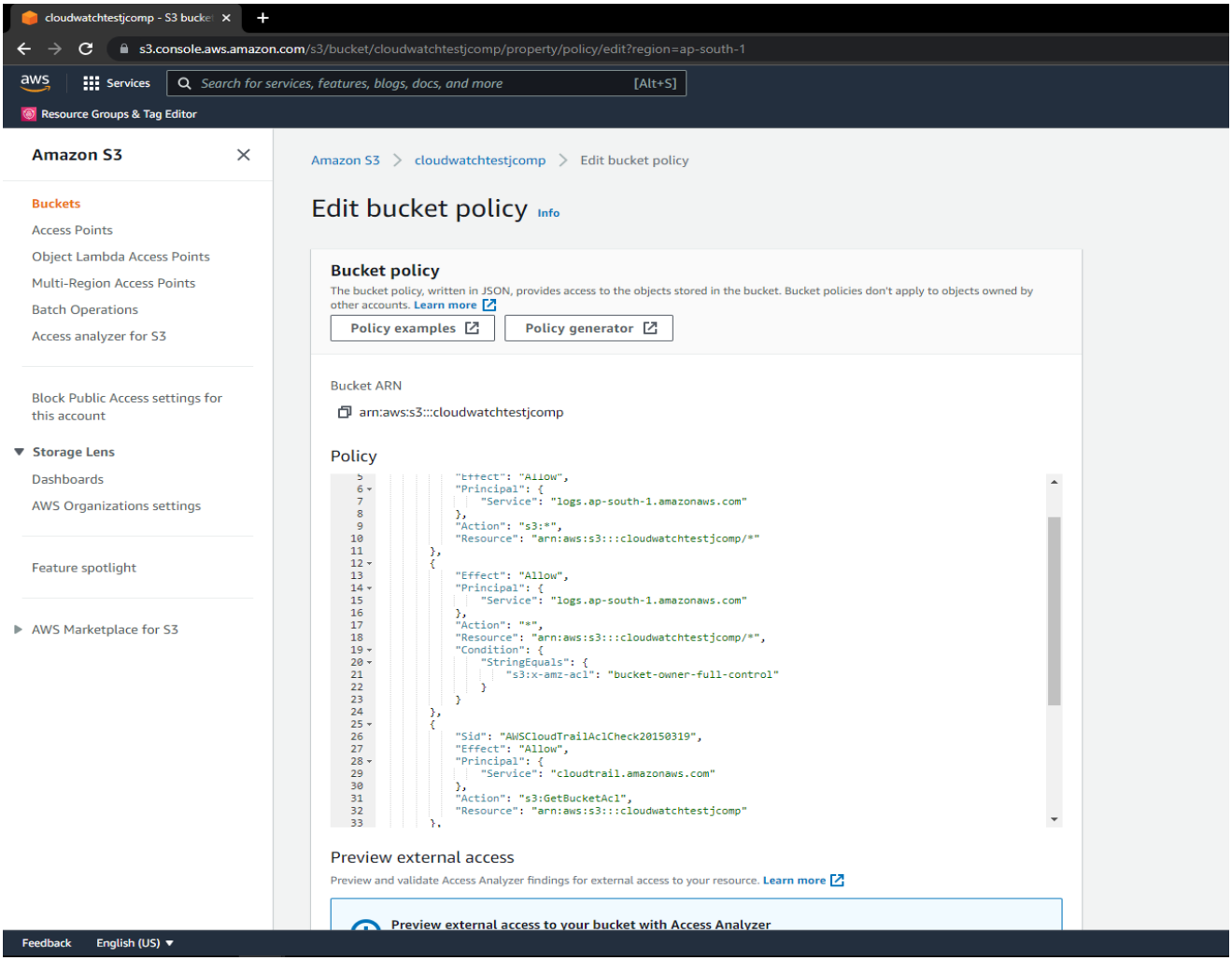
This is the page shwing the stored buckets in S3 with name.



This are the macie of some assignments randomly uploaded here.



These are some S3 buckets policy course of actions which AWS services allowing to access S3 buckets.

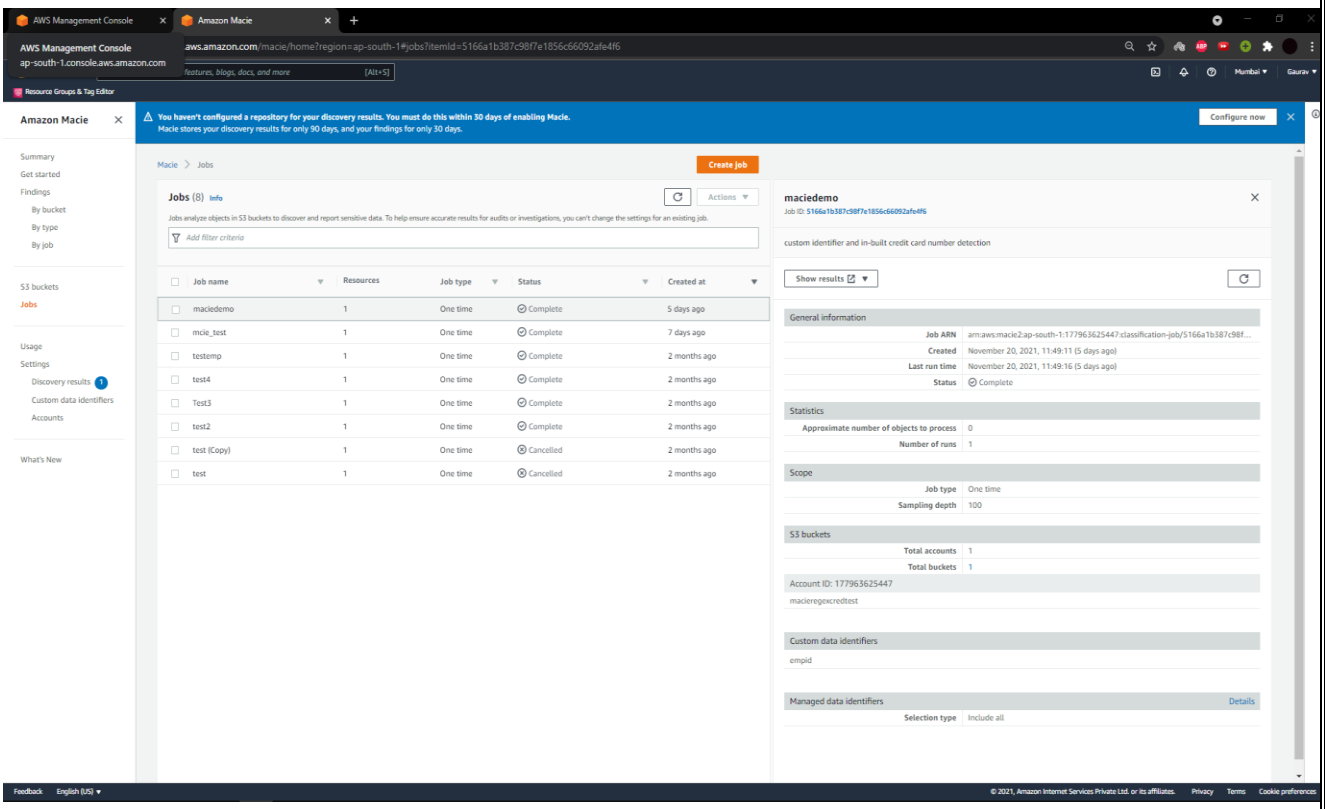


AMAZON MACIE:

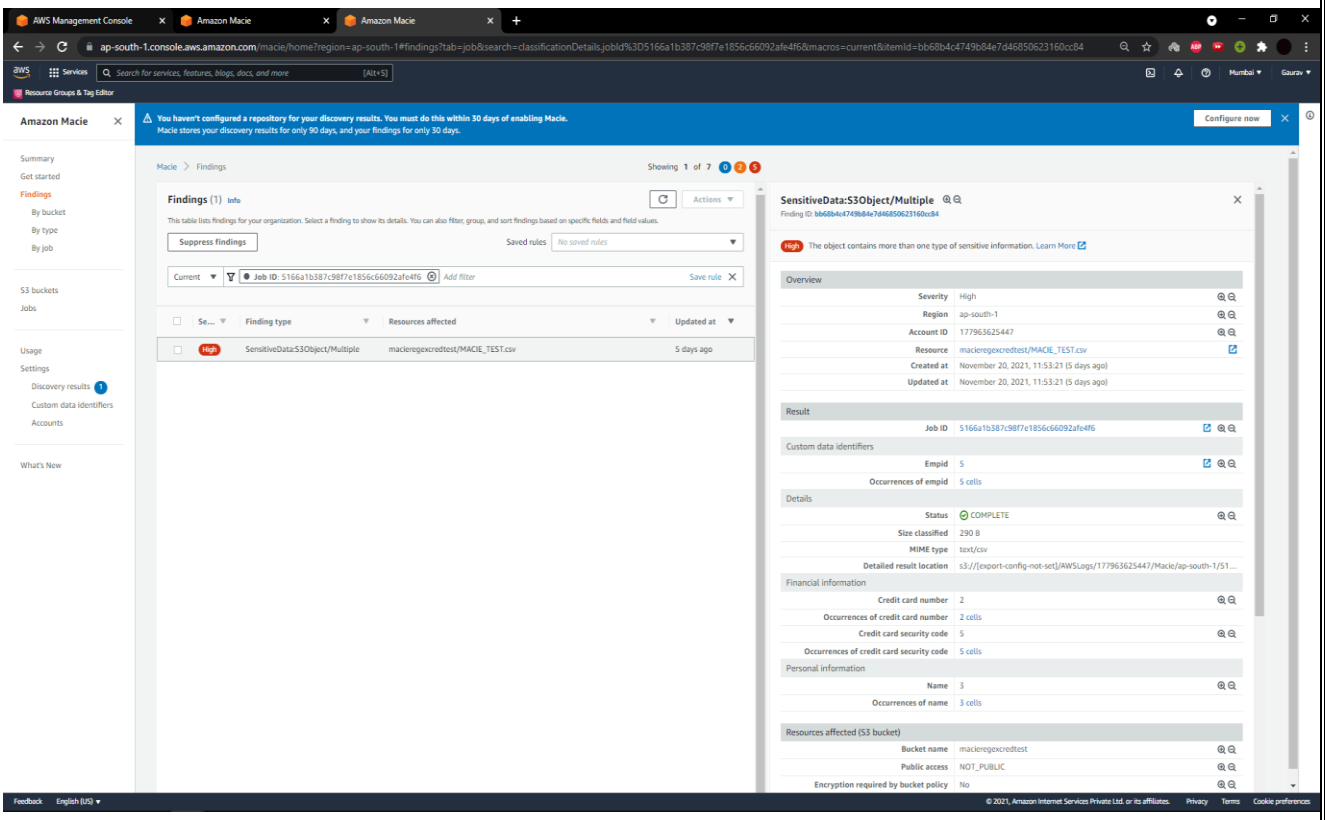
Macie is a completely overseen information security and information protection administration that uses machine learning to find sensitive information. Macie can distinguish two classifications of findings i.e policy findings and sensitive data findings. A policy finding is a point to point report of a strategy violation for a S3 bucket and sensitive data finding is an complete report of sensitiveinformation in a S3 object.

- In this project we have used it for sensitive data recognition.
- In this we have created one job which scans MACIE.CSV file which was uploaded for sensitive data and it will take nearly 10 – 15 minutes to completely scans the data.
- And it gave the credit card details as sensitive data as credit card details are considered as sensitive data by default.
- Macie has predefined classes in which it scans for sensitive data so it has detected from the MACIE.CSV that credit card details as financial information.

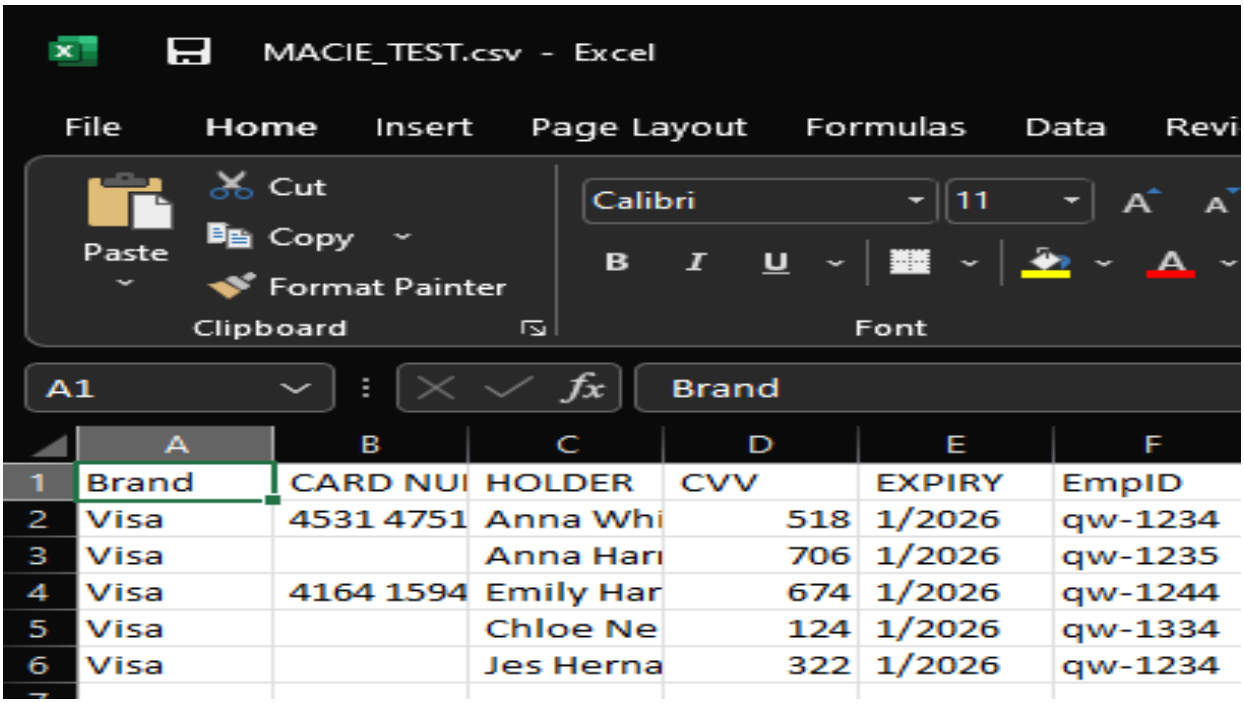
This is the page it shows the list of jobs that we have created.



This the page shows the results of MACIE.CSV file after scanning it for sensitive data.



These are the randomly generated credit card numbers and emp details are randomly given.



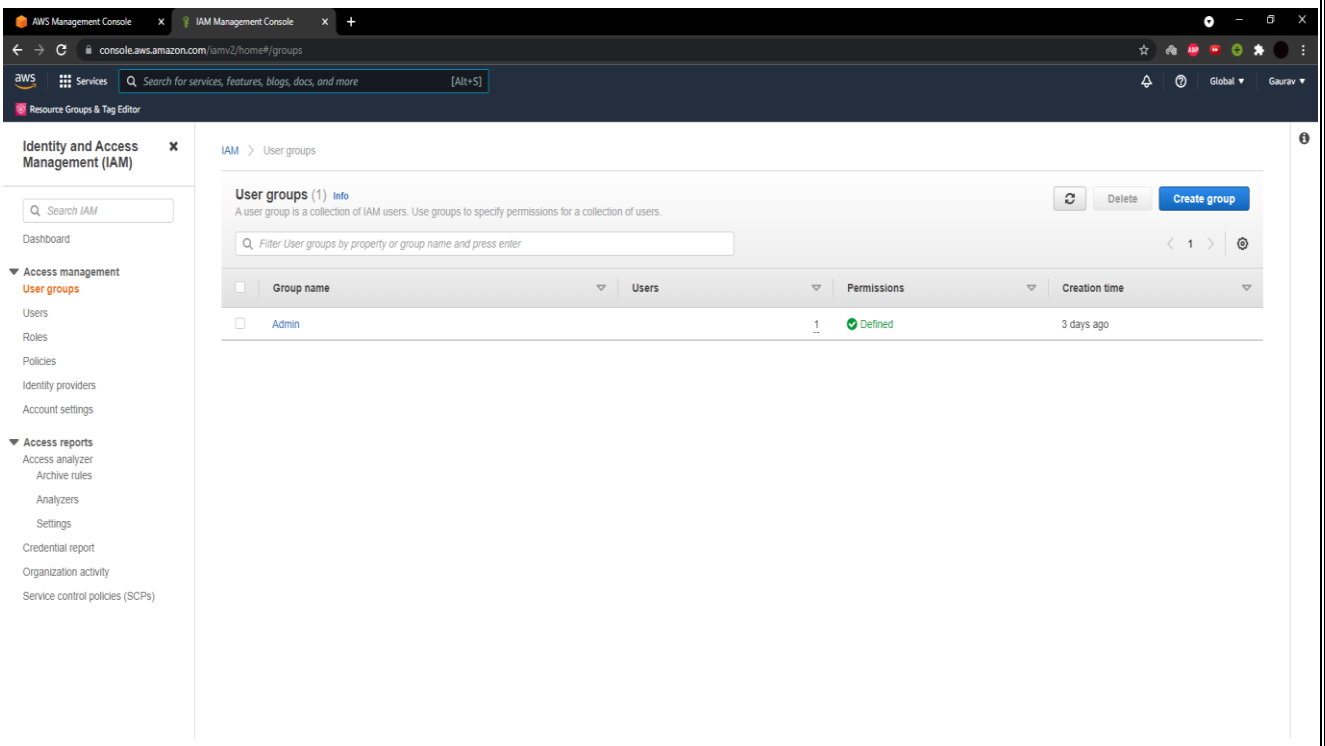
	A	B	C	D	E	F
1	Brand	CARD NUI	HOLDER	CVV	EXPIRY	EmpID
2	Visa	4531 4751	Anna Whi	518	1/2026	qw-1234
3	Visa		Anna Hari	706	1/2026	qw-1235
4	Visa	4164 1594	Emily Har	674	1/2026	qw-1244
5	Visa		Chloe Ne	124	1/2026	qw-1334
6	Visa		Jes Herna	322	1/2026	qw-1234

IAM(identify and access management):

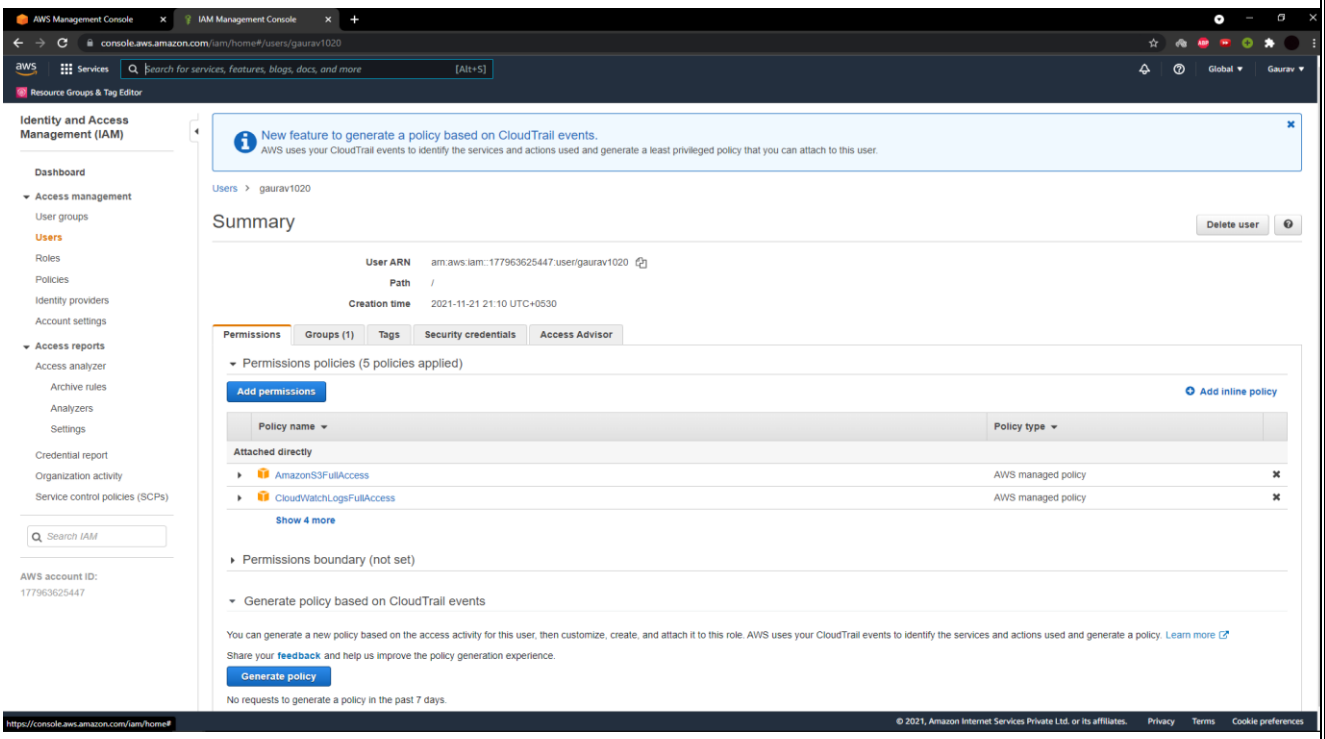
AWS Identity and Access Management (IAM) is a web administration for safely controlling access to AWS services. It authorizes you to make and control administrations for client verification or limit access to a specific set of individuals who utilize AWS services.

- In ths project We have created user with name and created user group with name as admin as shown below
- we have assigned admin permissions to S3 and cloud watch. So whenever we add anyone in this group by default they will get full details and they can access the group.
- We assigned some premissions so that we don't need to assign different permissions often to user. So if user has to access S3 bucket direct he cant, the permission has to be given by admin.

This is the page where we have created the admin for user group.



This the admin permission page showing permisions like full access for amazon S3 buckets, full access for cloud watch logs and soon.

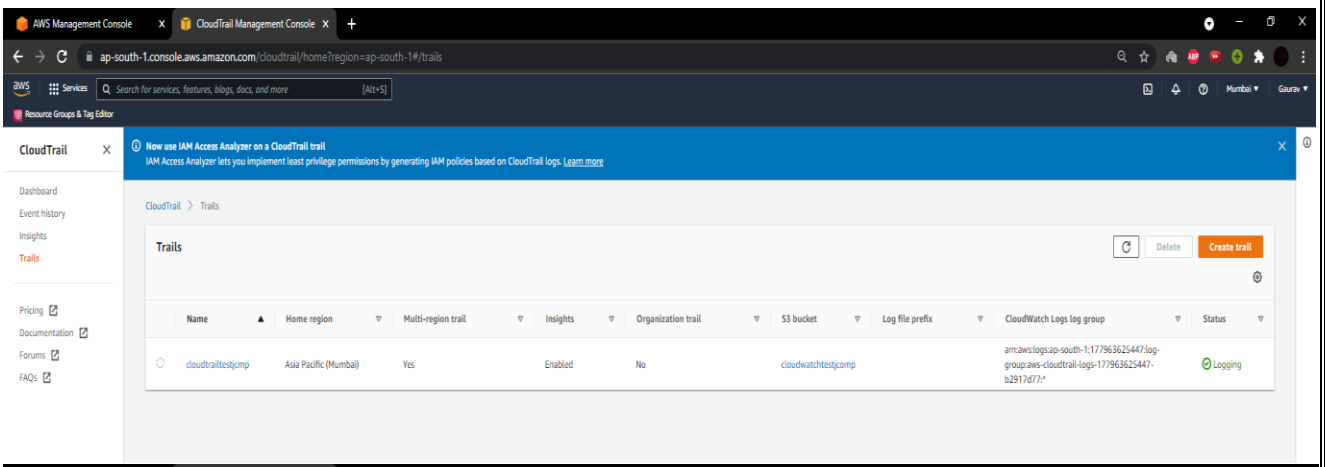


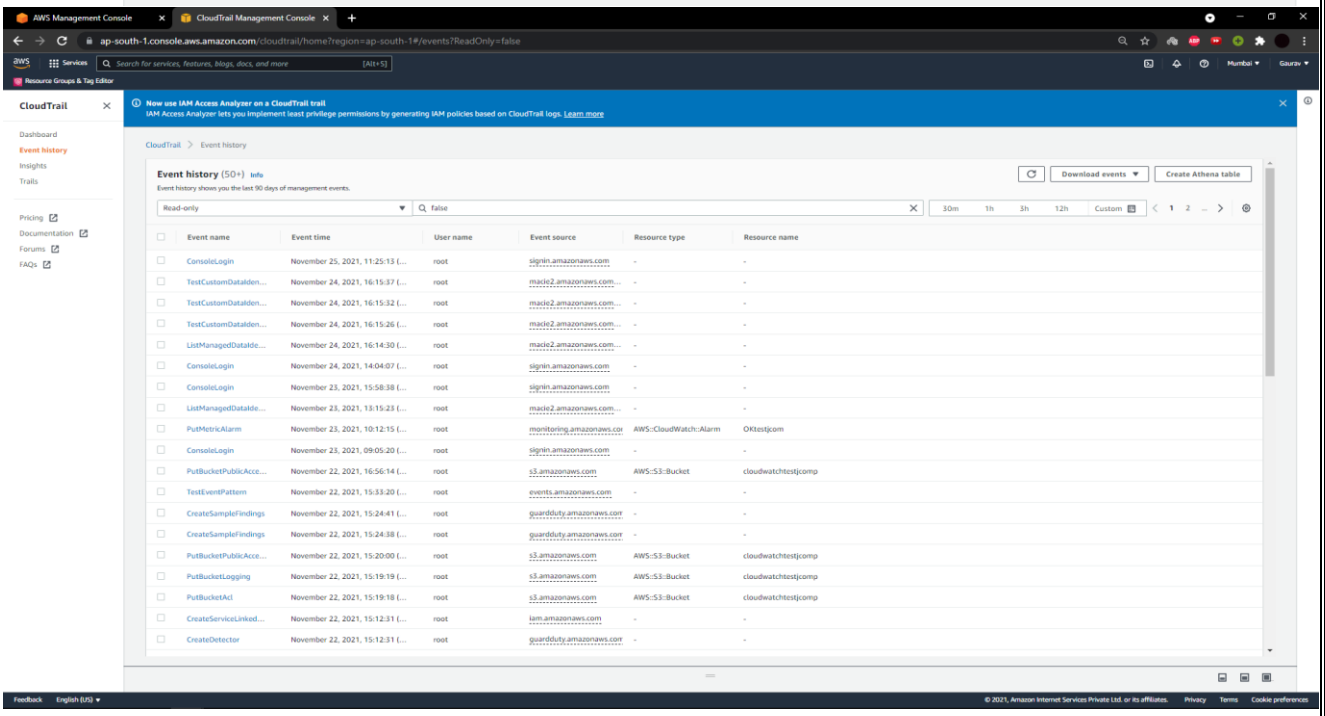
CLOUDTRAIL

CloudTrail permits to monitor AWS organizations at the API level, including all API calls made by means of AWS Management Console, AWS SDKs and AWS Command Line tools. Like cloud watch it allows you to recognize which records and clients called AWS APIs for services that supports CloudTrail, the source IP address the calls were produced in addition where and when the calls developed.

- In our project it is used generate the logs of entire AWS. So logging is done by cloud trail.
- We have allowed cloud trail in S3 bucket policy so cloud trail able to access particular and then cloud trail then logged in the cloud watch itself.

This below two screenshots shows the history of S3 buckets accessed by cloud trail.





CLOUDWATCH

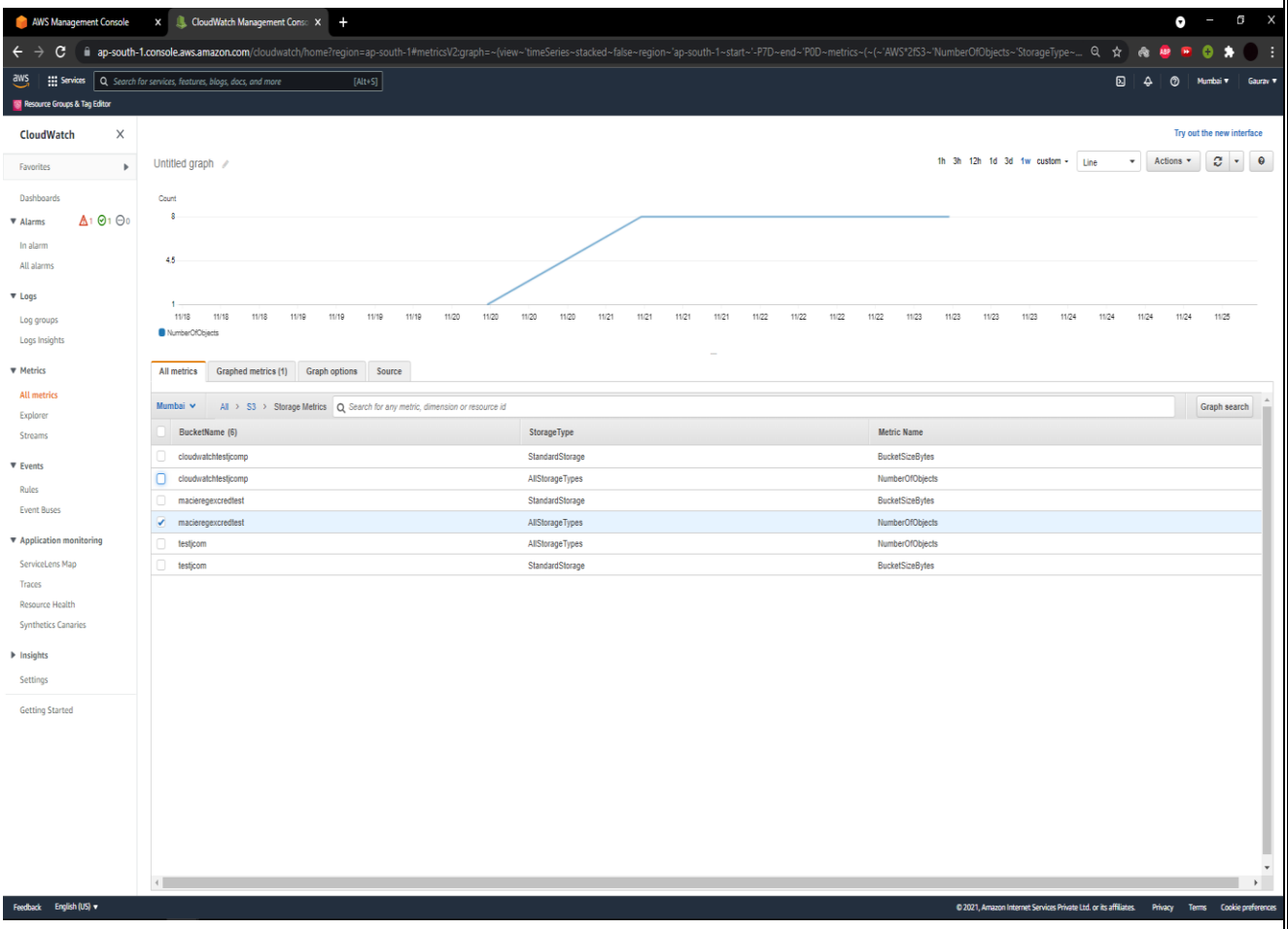
Amazon CloudWatch is AWS observing and management service which is intended to keep up with the management services and resources which are utilized Amazon CloudWatch is quite possibly the most utilized service presented by Amazon. It allows clients to monitor what's happening in their AWS Architecture. Especially, this is intended for designers, IT administrators, and framework administrators to make their work easier.

- It will perform the same task what SIM(security information management) tool

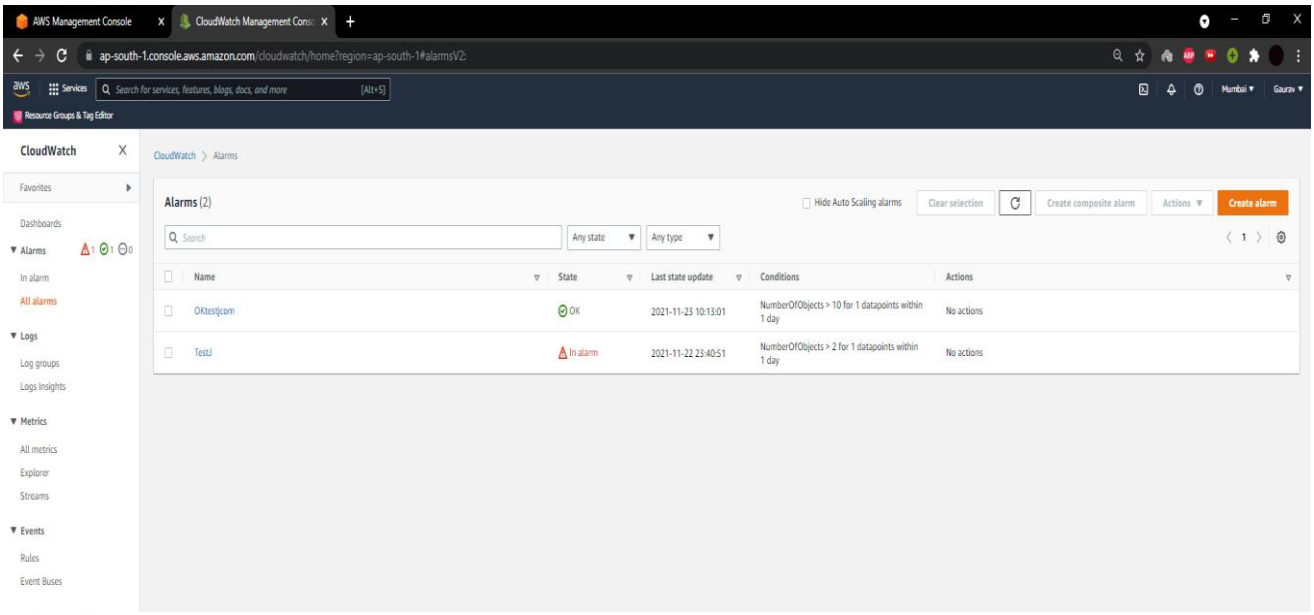
does and it is hosted in cloud.

- In this project we have used to manage the log analysis according our possibility it will give us the alert.
- And in the metrices it shows the object added date and no of objects added in graphical form.
- Here we have configured some alarms and set the alarms for limit of 2 objects
- We have cofigured some alarms in cloud watch by specifying metric and conditions.

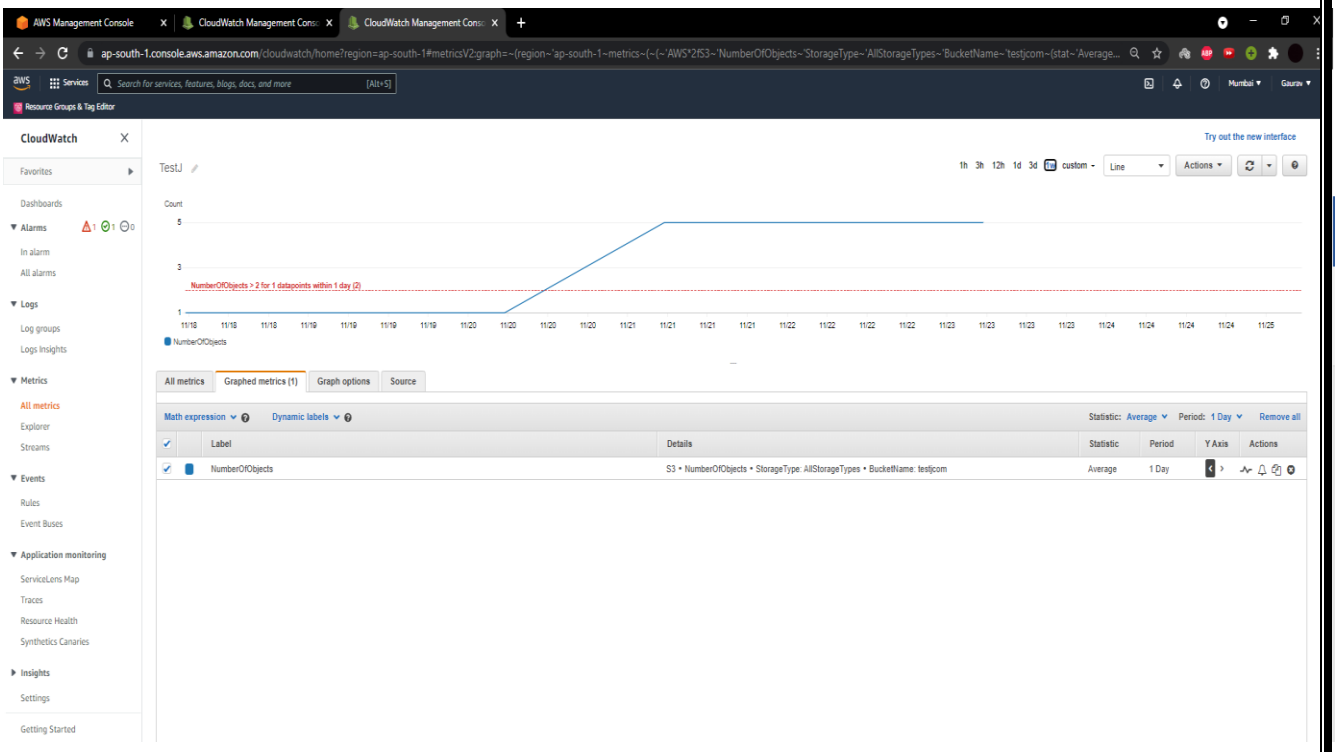
This is the graphical result after selecting the bucket name in the tab list which shows the log activity



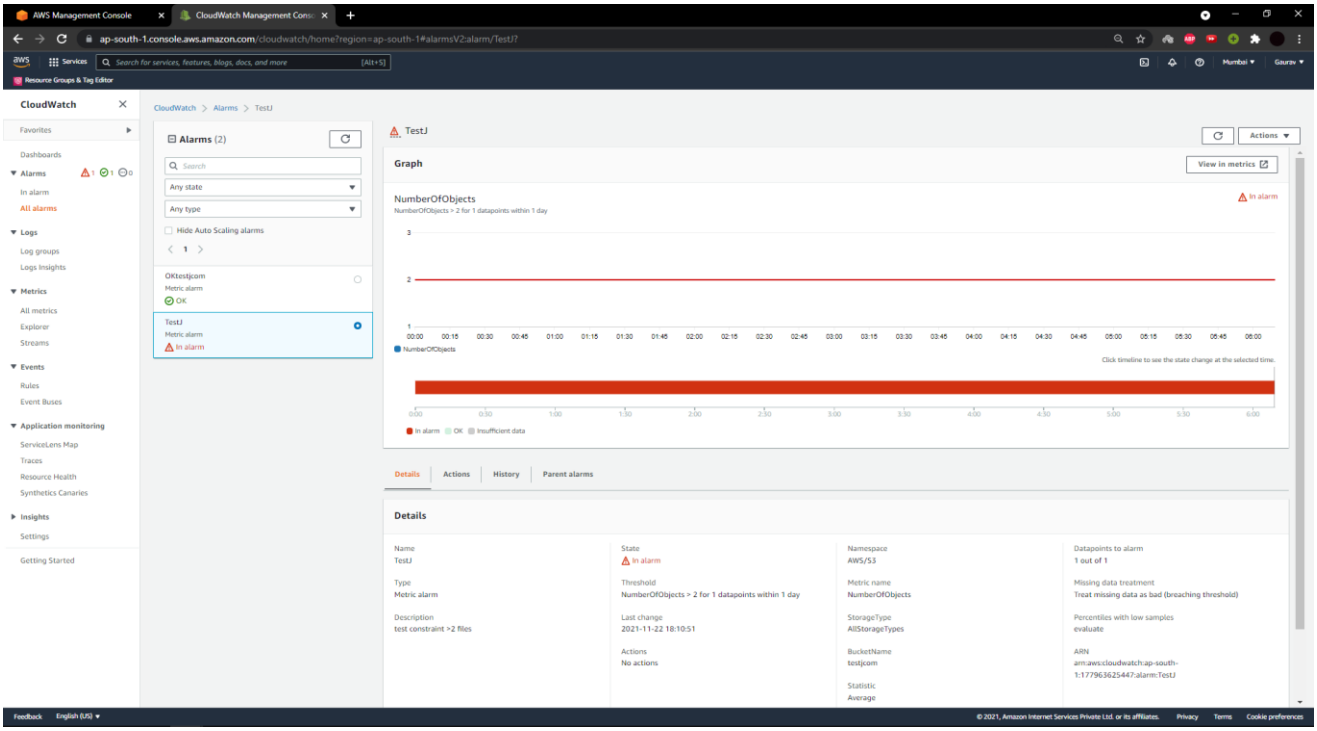
This is the page where alarm were set with name of testj and opentestj.com



This page shows the limit set for no of objects in a day in graphical form



This page shows the graph of alarms set by us with time vs no of objects.

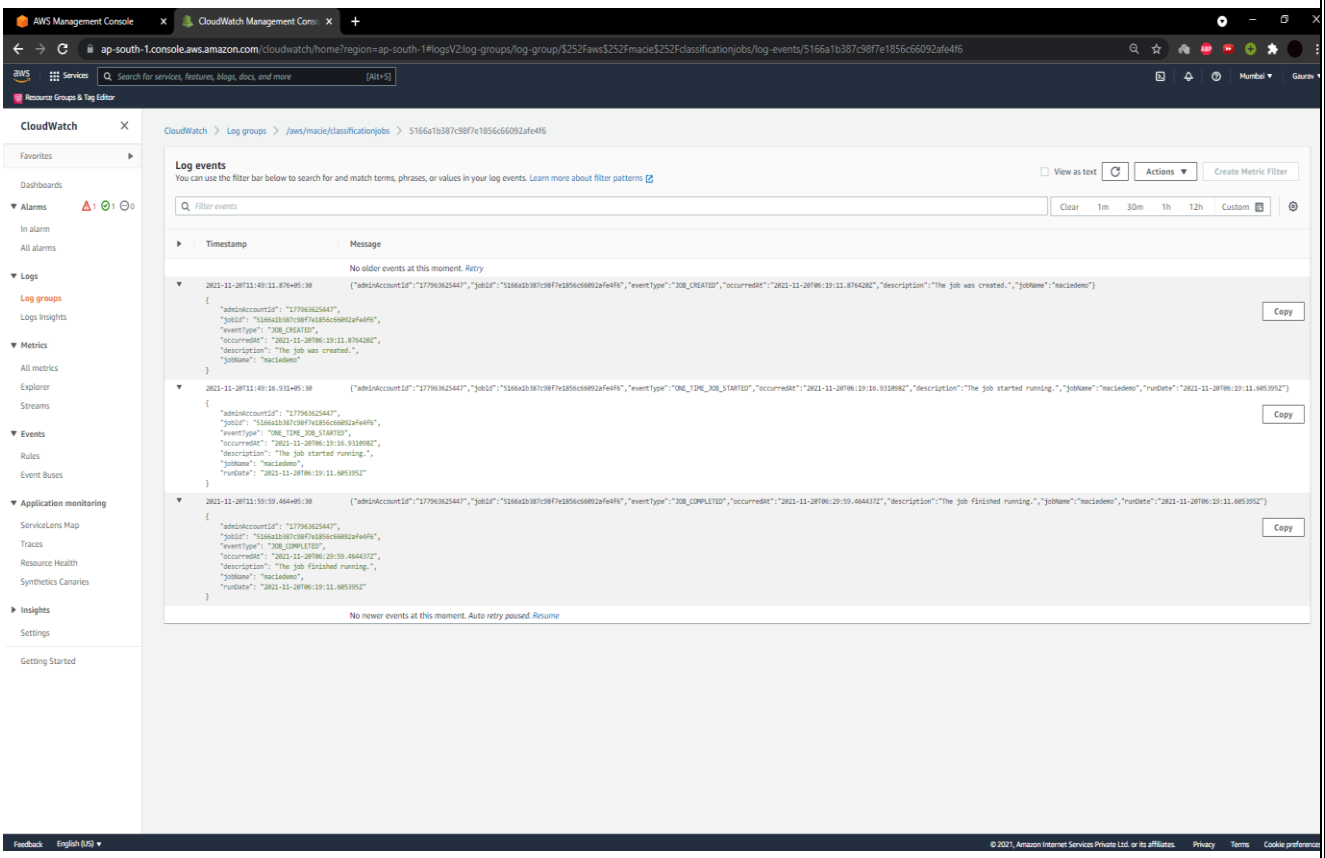


CLOUDWATCH LOGS

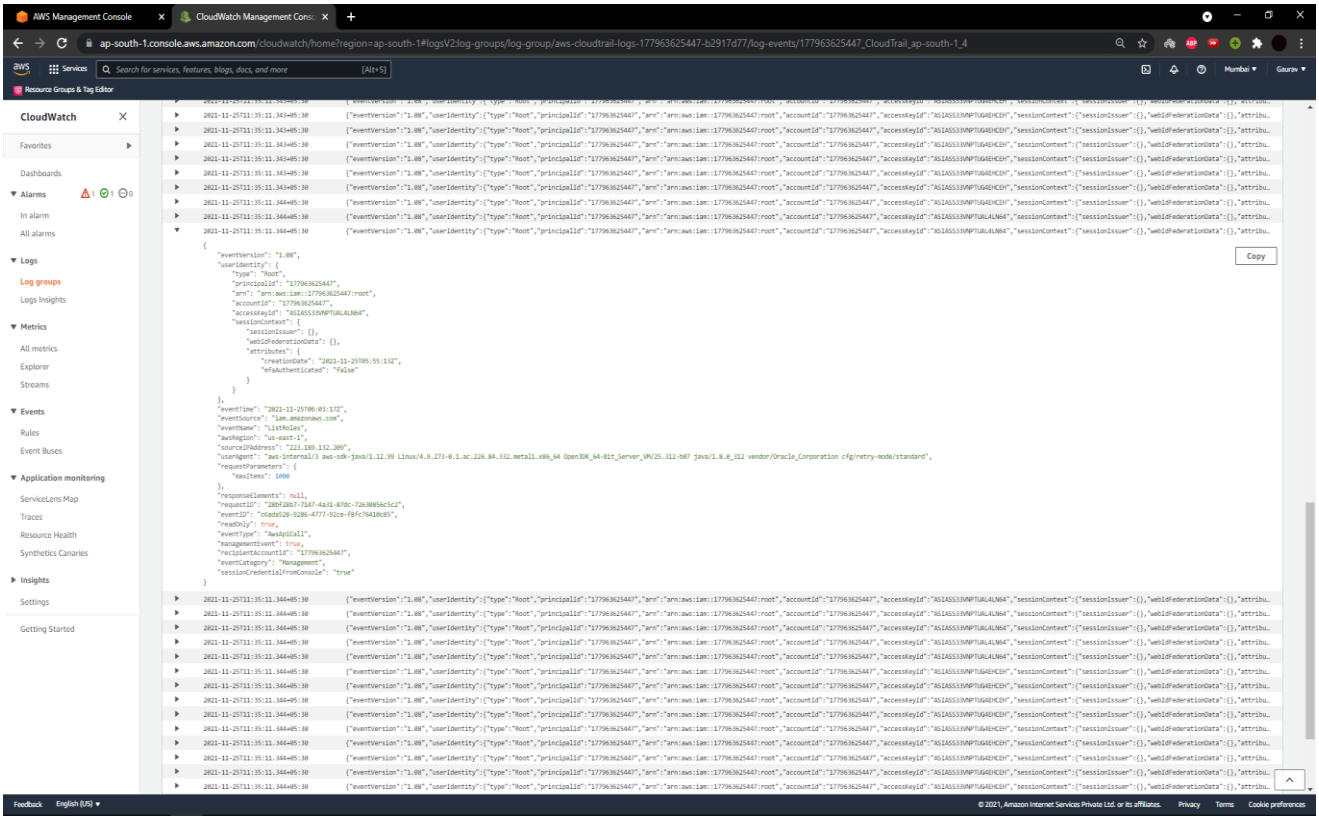
Amazon CloudWatch Logs to screen, store, and access your log documents from Amazon Elastic Compute Cloud (Amazon EC2) examples, AWS CloudTrail, Route 53, and different sources. CloudWatch Logs permits you to see your logs in general, irrespective of their source, as a single and consistent flow of events ordered by time, and you can query them and sort them based on different aspects, combine them by particular fields, make custom computations with an dominant query language, and visualize log information in dashboards.

- Any API call which anyone makes on a specific S3 buckets which we configured to cloud trail will be imposed and the data would be stored in cloud watch itself.

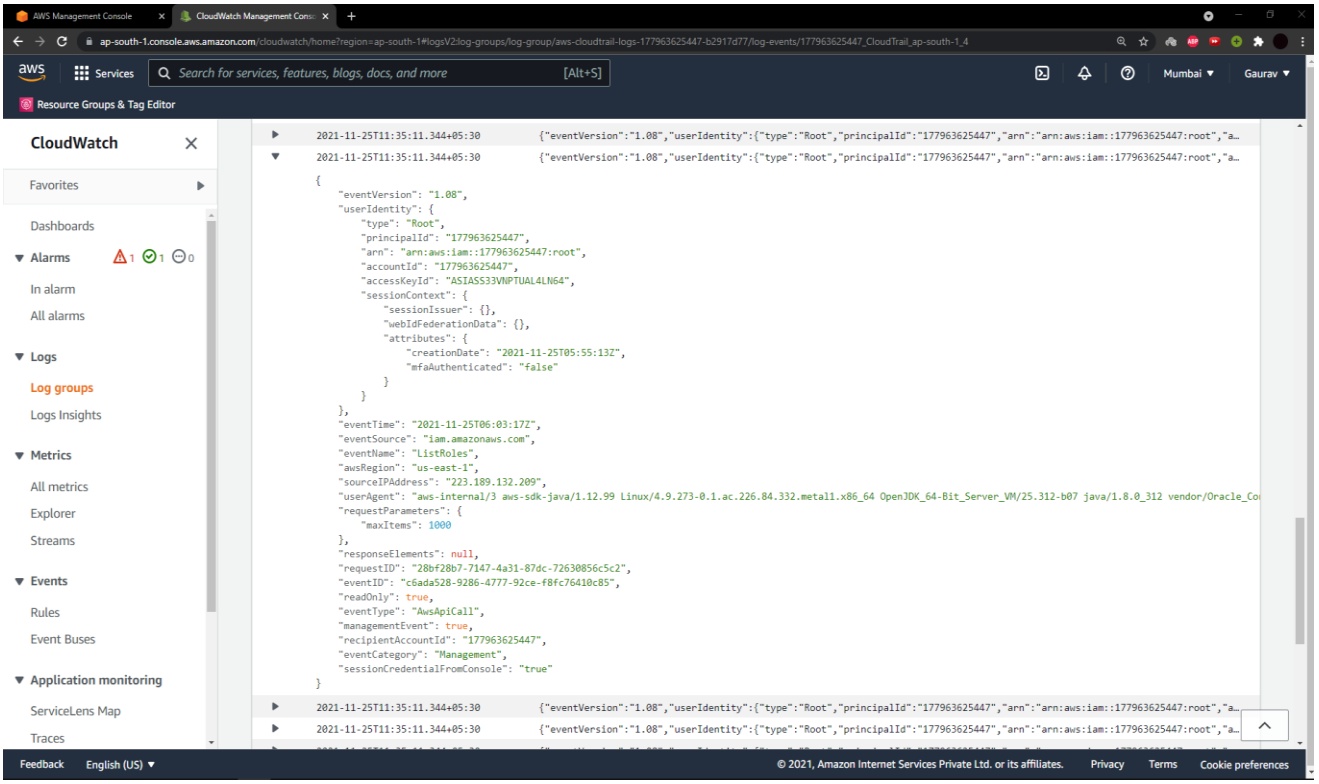
This page shows the all API calls.



This is for entire one API call with event name, event type, event region, etc,…



This is the another API call

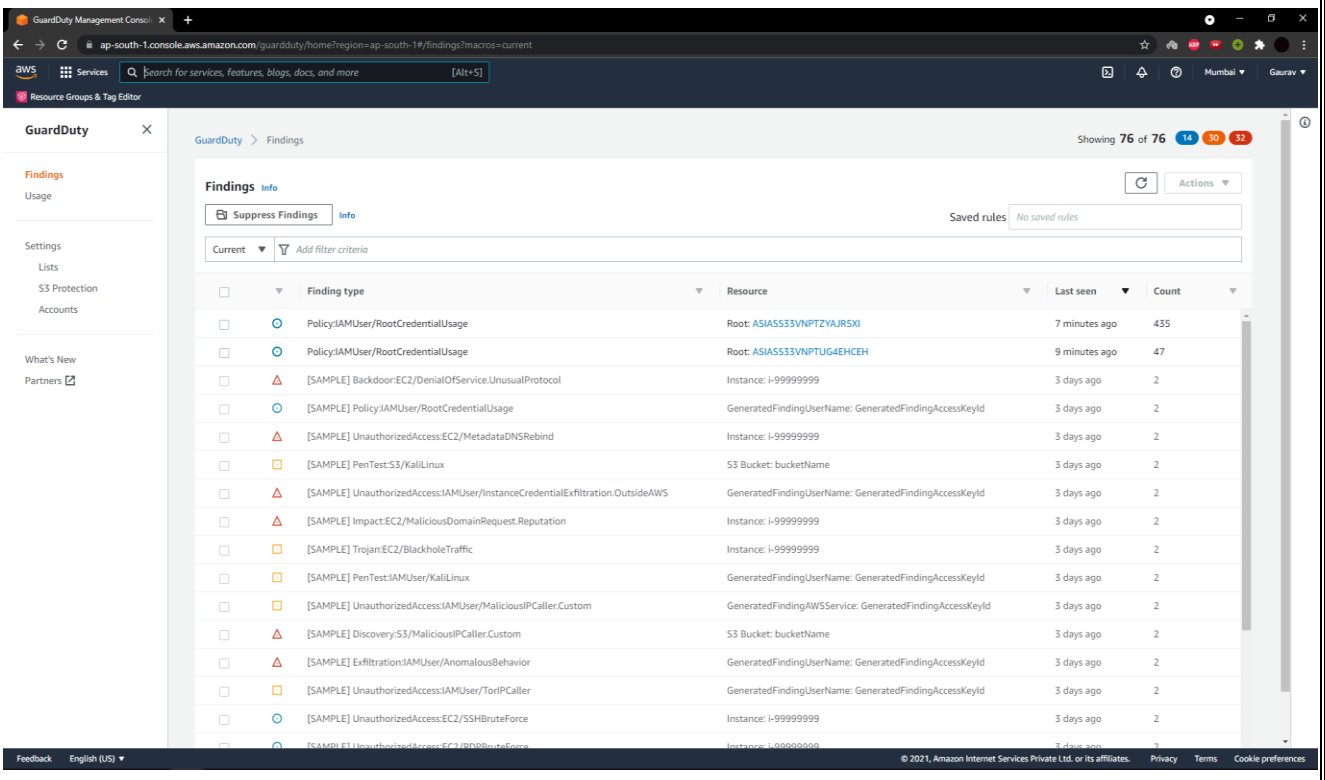


GUARDDUTY

Amazon GuardDuty service is an threat detection administration service that constantly screens our sending for malicious activity and unapproved conduct.

- In this service we have used the root user for accessing the buckets it will just log here.
- And the sample findings which AWS launches these attacks on the particular S3 buckets and it just stops it and these are some sample findings shown below.
- This is how the findings will be shown if these kind of attacks are performed by any third party vendors. It will show from which IP address we were attacked.
- So we can test them in the settings by clicking on generating sample findings and some of the sample findings are shown below.

This page shows the generated sample findings



This the page in the guardDuty for enabling and disabling the S3 protection