



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 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.

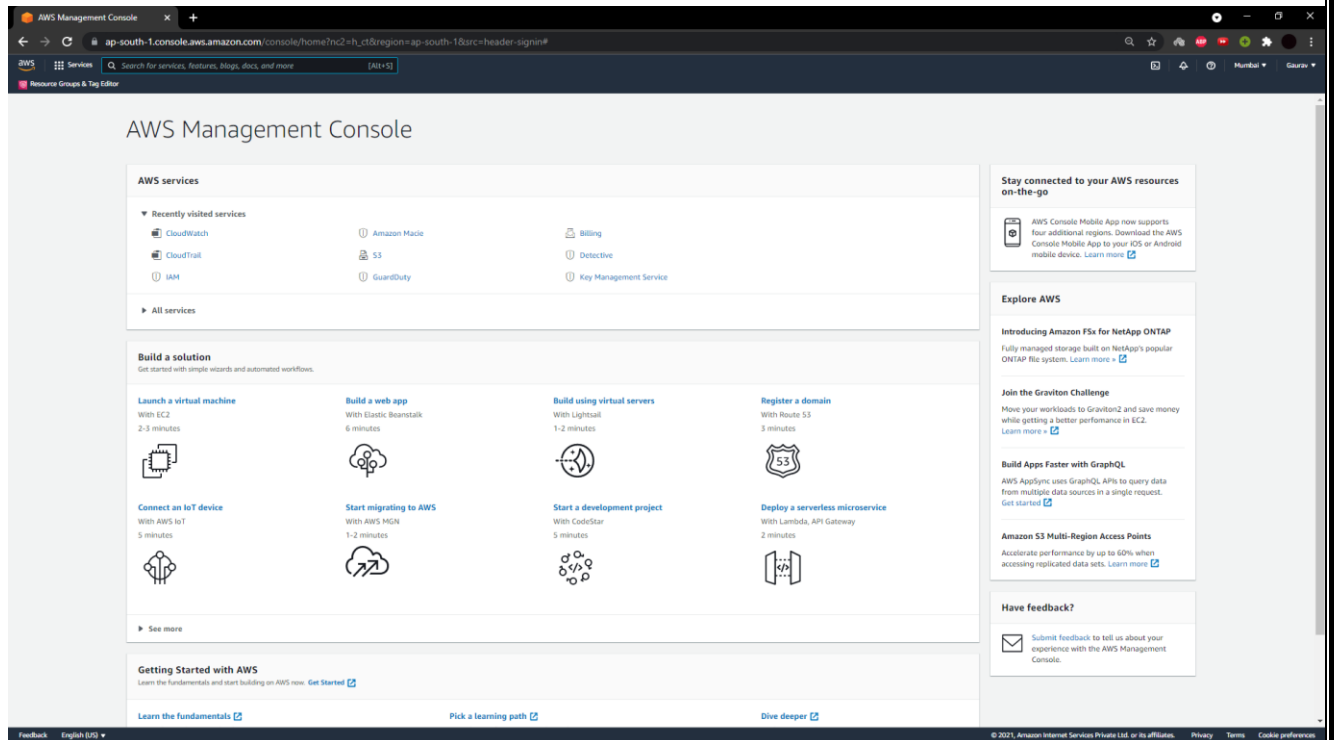
In this project we mainly focussed on network cloud security. In database we have done on cloud storage security so, we have used S3 buckets nothing but storage buckets. And for log details we have used cloud watch and cloud security services. We have used cloud trail for getting alerts and we have guard 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 is the home page of the AWS management console, which consists of AWS services like CloudTrail, CloudWatch, S3, GuardDuty, IAM (Identify and Access Management), billing, Detective, and Key Management Service.

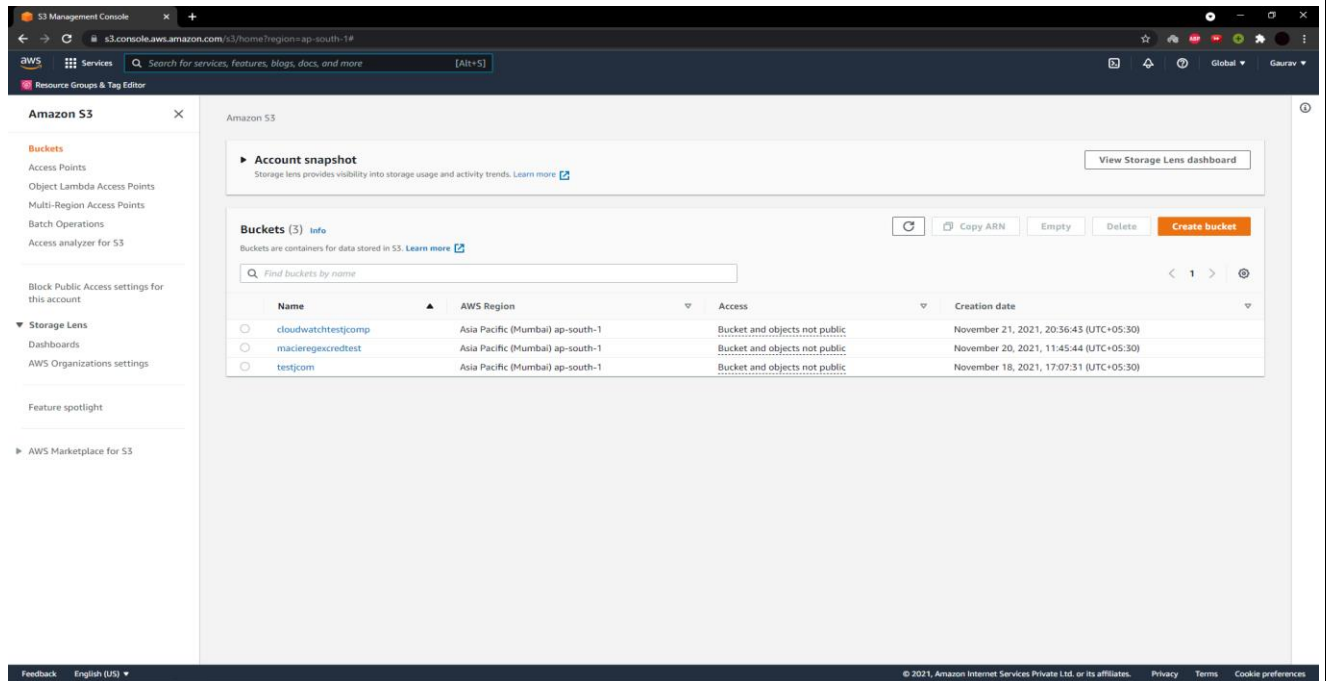


S3 (storage bucket):

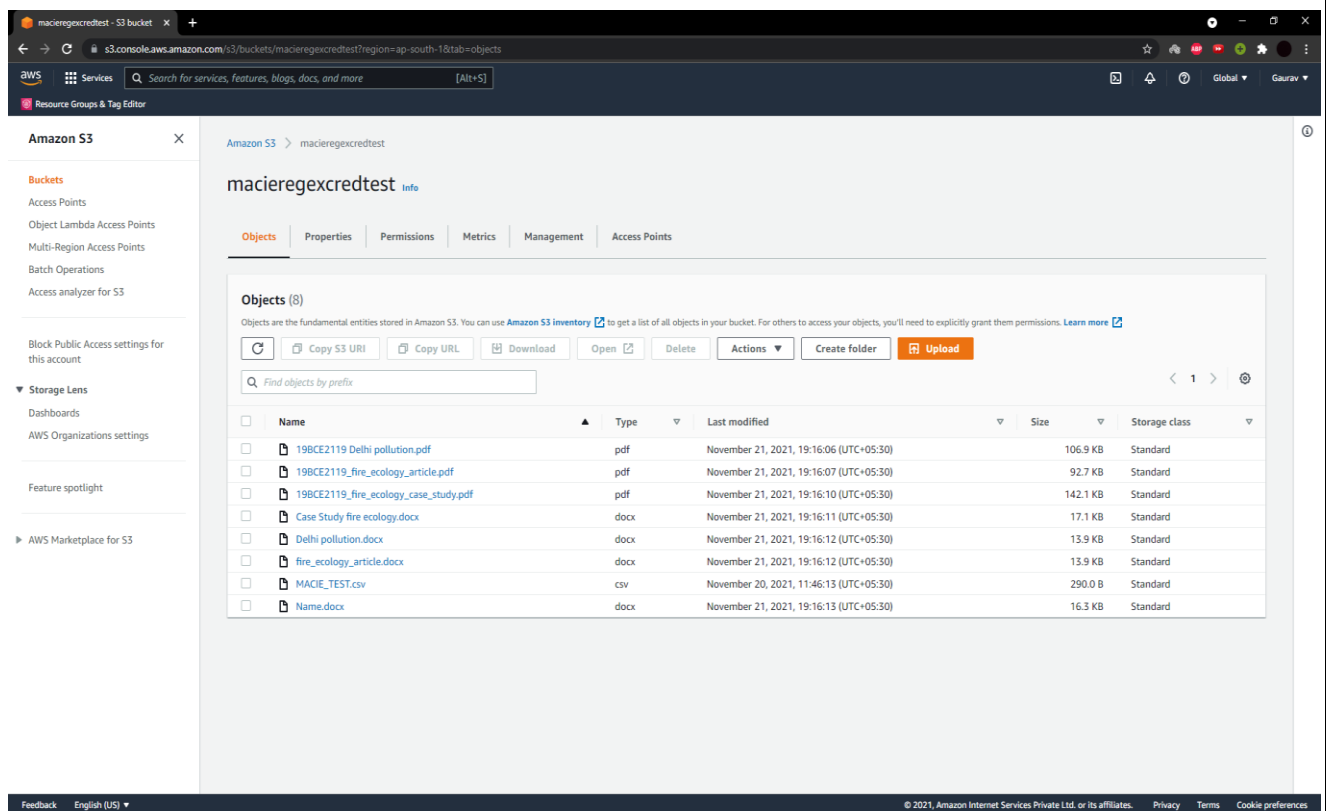
Amazon S3 gives object storage through a web interface. It works to store, protect and recover information from buckets whenever from anywhere on any gadget. A client makes a bucket, and the bucket stores objects in the cloud.

- 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.

The screenshot displays the AWS Management Console interface for editing the bucket policy of 'cloudwatchtestjcomp' in the 'ap-south-1' region. The left-hand navigation pane shows the 'Amazon S3' section with options like Buckets, Access Points, and Storage Lens. The main content area is titled 'Edit bucket policy' and includes a 'Bucket policy' section with a description and links to 'Policy examples' and 'Policy generator'. Below this, the 'Bucket ARN' is listed as 'arn:aws:s3:::cloudwatchtestjcomp'. The 'Policy' section contains a JSON policy document with three statements: one for 'logs.ap-south-1.amazonaws.com' to perform all S3 actions on the bucket, another for 'logs.ap-south-1.amazonaws.com' to perform all actions on the bucket with a condition for 'bucket-owner-full-control', and a third for 'cloudtrail.amazonaws.com' to perform the 's3:GetBucketAcl' action on the bucket. At the bottom, there is a 'Preview external access' section with a button to 'Preview external access to your bucket with Access Analyzer'.

cloudwatchtestjcomp - S3 bucket

s3.console.aws.amazon.com/s3/bucket/cloudwatchtestjcomp/property/policy/edit?region=ap-south-1

aws Services Search for services, features, blogs, docs, and more [Alt+S]

Resource Groups & Tag Editor

Amazon S3

Buckets

Access Points

Object Lambda Access Points

Multi-Region Access Points

Batch Operations

Access analyzer for S3

Block Public Access settings for this account

Storage Lens

Dashboards

AWS Organizations settings

Feature spotlight

AWS Marketplace for S3

Amazon S3 > cloudwatchtestjcomp > Edit bucket policy

Edit bucket policy

Info

Bucket policy

The bucket policy, written in JSON, provides access to the objects stored in the bucket. Bucket policies don't apply to objects owned by other accounts. [Learn more](#)

Policy examples Policy generator

Bucket ARN

arn:aws:s3:::cloudwatchtestjcomp

Policy

```
3  {
4    "Effect": "Allow",
5    "Principal": {
6      "Service": "logs.ap-south-1.amazonaws.com"
7    },
8    "Action": "s3:*",
9    "Resource": "arn:aws:s3:::cloudwatchtestjcomp/*"
10  },
11  {
12    "Effect": "Allow",
13    "Principal": {
14      "Service": "logs.ap-south-1.amazonaws.com"
15    },
16    "Action": "*",
17    "Resource": "arn:aws:s3:::cloudwatchtestjcomp/*",
18    "Condition": {
19      "StringEquals": {
20        "s3:x-amz-acl": "bucket-owner-full-control"
21      }
22    }
23  },
24  {
25    "Sid": "AWSCloudTrailAclCheck20150319",
26    "Effect": "Allow",
27    "Principal": {
28      "Service": "cloudtrail.amazonaws.com"
29    },
30    "Action": "s3:GetBucketAcl",
31    "Resource": "arn:aws:s3:::cloudwatchtestjcomp"
32  },
33  }
```

Preview external access

Preview and validate Access Analyzer findings for external access to your resource. [Learn more](#)

Preview external access to your bucket with Access Analyzer

Feedback English (US)

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 sensitive information 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.

The screenshot displays the Amazon Macie console interface. On the left, a navigation sidebar includes links for Summary, Get started, Findings, By bucket, By type, By job, S3 buckets, Jobs, Usage, Settings, Discovery results, Custom data identifiers, Accounts, and What's New. The main content area is titled 'Macie > Jobs' and features a 'Create job' button. Below this, a table lists eight jobs. The job 'maciedemo' is highlighted, showing it is a 'One time' job that is 'Complete' and was created '5 days ago'. To the right of the table, a detailed view for the 'maciedemo' job is shown, including its Job ID, ARN, and various settings.

Job name	Resources	Job type	Status	Created at
maciedemo	1	One time	Complete	5 days ago
mcie_test	1	One time	Complete	7 days ago
testemp	1	One time	Complete	2 months ago
test4	1	One time	Complete	2 months ago
Test3	1	One time	Complete	2 months ago
test2	1	One time	Complete	2 months ago
test (Copy)	1	One time	Cancelled	2 months ago
test	1	One time	Cancelled	2 months ago

maciedemo
Job ID: 5166a1b387c987e1856c66092afe4f6

custom identifier and in-built credit card number detection

Show results

General information

Job ARN	arn:aws:macie2:ap-south-1:177963625447:classification-job/5166a1b387c987...
Created	November 20, 2021, 11:49:11 (5 days ago)
Last run time	November 20, 2021, 11:49:16 (5 days ago)
Status	Complete

Statistics

Approximate number of objects to process	0
Number of runs	1

Scope

Job type	One time
Sampling depth	100

S3 buckets

Total accounts	1
Total buckets	1

Account ID: 177963625447
macieregiontest

Custom data identifiers

empid

Managed data identifiers

Selection type: Include all

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

The screenshot shows the Amazon Macie console interface. On the left, there's a navigation menu with options like Summary, Get started, Findings, S3 buckets, Jobs, Usage, Settings, and What's New. The main area displays a list of findings. One finding, 'SensitiveData:S3Object/Multiple', is selected, and its details are shown on the right. The details include an overview with severity (High), region (ap-south-1), account ID (177963625447), and resource (macierexcredtest/MACIE_TEST.csv). The result section shows the job ID and a list of custom data identifiers. The details section shows the status (COMPLETE), size (290 B), MIME type (text/csv), and a detailed result location. The financial information section shows credit card numbers and security codes. The personal information section shows names and occurrences. The resources affected section shows the bucket name (macierexcredtest), public access (NOT_PUBLIC), and encryption required (No).

Severity	Region	Account ID	Resource	Created at	Updated at
High	ap-south-1	177963625447	macierexcredtest/MACIE_TEST.csv	November 20, 2021, 11:53:21 (5 days ago)	November 20, 2021, 11:53:21 (5 days ago)

Job ID
5166a1b387c987e1856c66092afe4f6

Custom data identifiers
Empid
Occurrences of empid

Status
COMPLETE

Size classified
290 B

MIME type
text/csv

Detailed result location
s3://[export-config-not-set]/AWSLogs/177963625447/Macie/ap-south-1/51...

Financial information
Credit card number
Occurrences of credit card number
Credit card security code
Occurrences of credit card security code

Personal information
Name
Occurrences of name

Resources affected (S3 bucket)
Bucket name
Public access
Encryption required by bucket policy

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

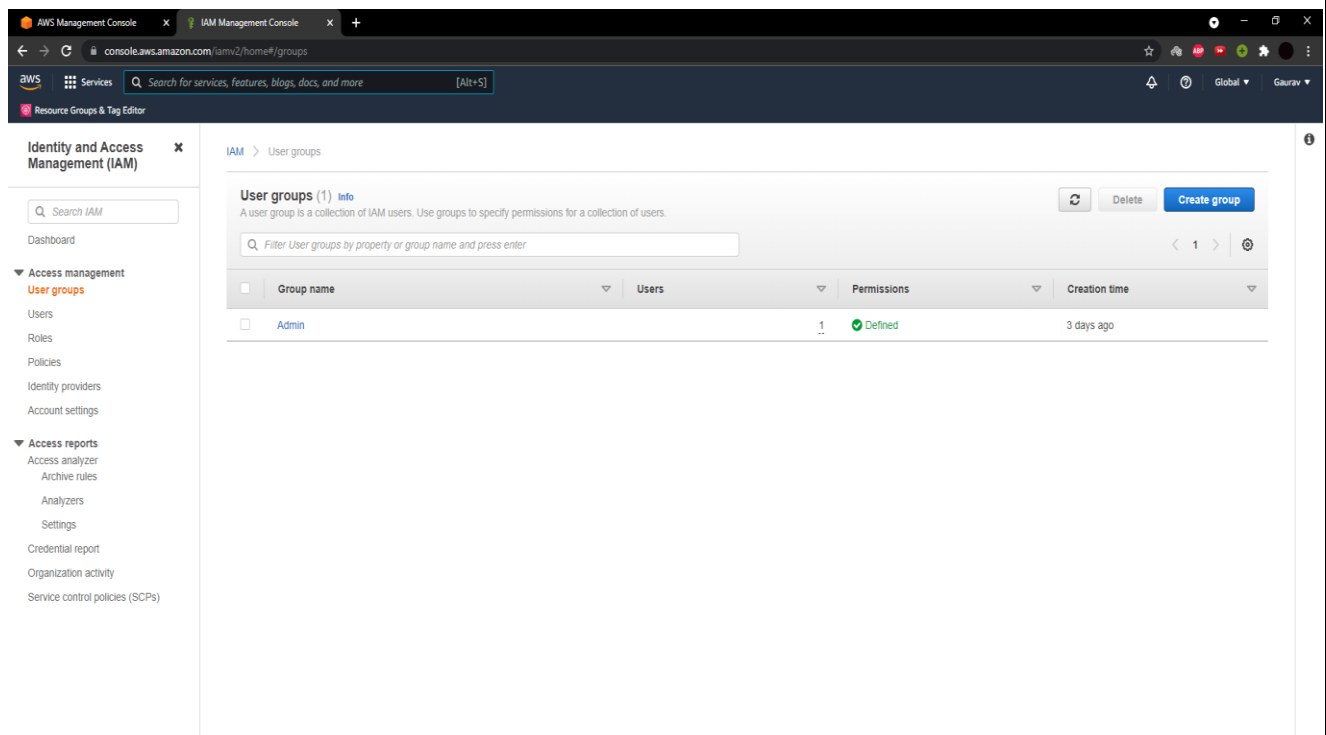
Brand	CARD NUMBER	HOLDER	CVV	EXPIRY	EmpID
Visa	4531 4751	Anna Whi	518	1/2026	qw-1234
Visa		Anna Har	706	1/2026	qw-1235
Visa	4164 1594	Emily Har	674	1/2026	qw-1244
Visa		Chloe Ne	124	1/2026	qw-1334
Visa		Jes Herna	322	1/2026	qw-1234

IAM(identify and access management):

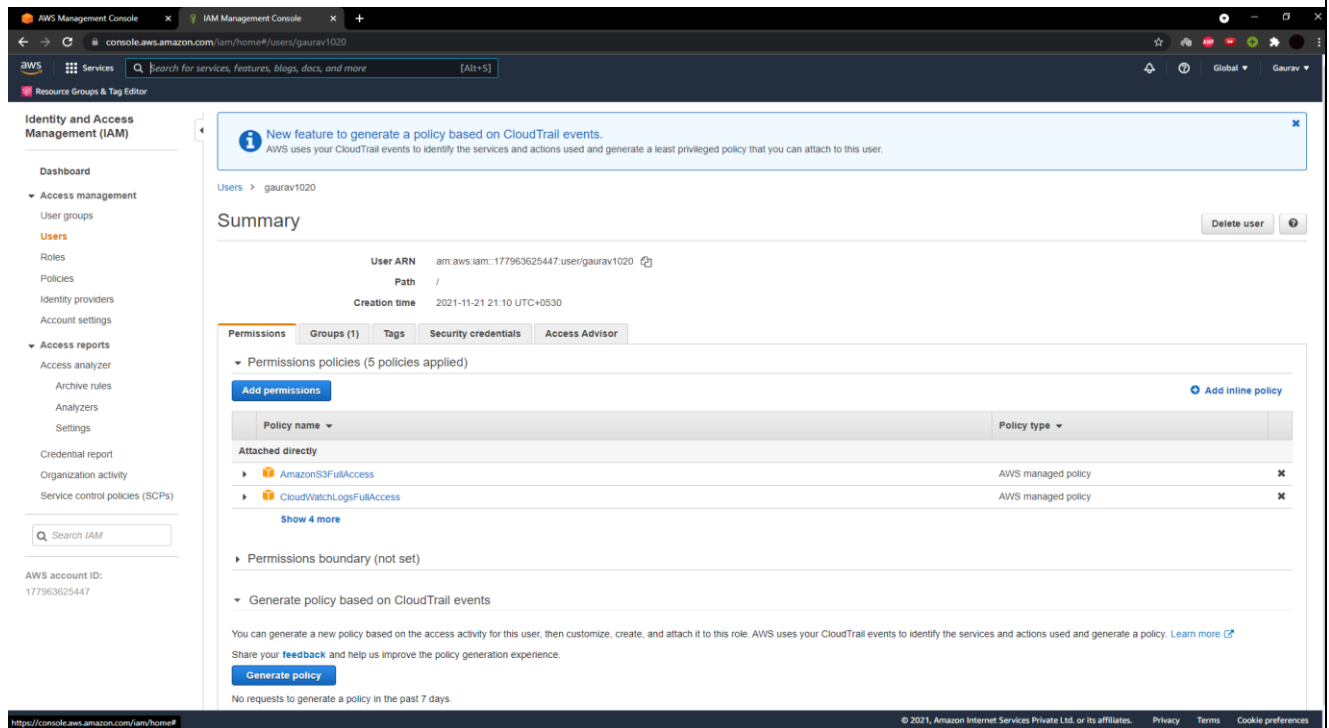
AWS Identity and Access Management (IAM) is a web administration for safely controlling access to AWS services. It authorizes you to make and control administrations for client verification or limit access to a specific set of individuals who utilize AWS services.

- In this 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 permissions 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.

The top screenshot shows the AWS CloudTrail console 'Trails' page. It displays a table with the following data:

Name	Home region	Multi-region trail	Insights	Organization trail	S3 bucket	Log file prefix	CloudWatch Logs log group	Status
cloudtrailtestcomp	Asia Pacific (Mumbai)	Yes	Enabled	No	cloudwatchtestcomp		arn:aws:logs:ap-south-1:177963625447:log-group:aws-cloudtrail-logs-177963625447-b2917d77*	Logging

The bottom screenshot shows the AWS CloudTrail console 'Event history' page. It displays a table with the following data:

Event name	Event time	User name	Event source	Resource type	Resource name
ConsoleLogin	November 25, 2021, 11:25:13	root	signin.amazonaws.com	-	-
TestCustomDataIden...	November 24, 2021, 16:15:37	root	maci2.amazonaws.com	-	-
TestCustomDataIden...	November 24, 2021, 16:15:32	root	maci2.amazonaws.com	-	-
TestCustomDataIden...	November 24, 2021, 16:15:26	root	maci2.amazonaws.com	-	-
ListManagedDataId...	November 24, 2021, 16:14:30	root	maci2.amazonaws.com	-	-
ConsoleLogin	November 24, 2021, 14:04:07	root	signin.amazonaws.com	-	-
ConsoleLogin	November 23, 2021, 15:58:38	root	signin.amazonaws.com	-	-
ListManagedDataId...	November 23, 2021, 15:15:23	root	maci2.amazonaws.com	-	-
PutMetricAlarm	November 23, 2021, 10:12:15	root	monitoring.amazonaws.com	AWS::CloudWatch::Alarm	OKtestcomp
ConsoleLogin	November 23, 2021, 09:05:20	root	signin.amazonaws.com	-	-
PutBucketPublicAcc...	November 22, 2021, 16:56:14	root	s3.amazonaws.com	AWS::S3::Bucket	cloudwatchtestcomp
TestEventPattern	November 22, 2021, 15:33:20	root	events.amazonaws.com	-	-
CreateSampleFindings	November 22, 2021, 15:24:41	root	guardduty.amazonaws.com	-	-
CreateSampleFindings	November 22, 2021, 15:24:38	root	guardduty.amazonaws.com	-	-
PutBucketPublicAcc...	November 22, 2021, 15:20:00	root	s3.amazonaws.com	AWS::S3::Bucket	cloudwatchtestcomp
PutBucketLogging	November 22, 2021, 15:19:19	root	s3.amazonaws.com	AWS::S3::Bucket	cloudwatchtestcomp
PutBucketAcl	November 22, 2021, 15:19:18	root	s3.amazonaws.com	AWS::S3::Bucket	cloudwatchtestcomp
CreateServiceLinked...	November 22, 2021, 15:12:31	root	iam.amazonaws.com	-	-
CreateDetector	November 22, 2021, 15:12:31	root	guardduty.amazonaws.com	-	-

CLOUDWATCH

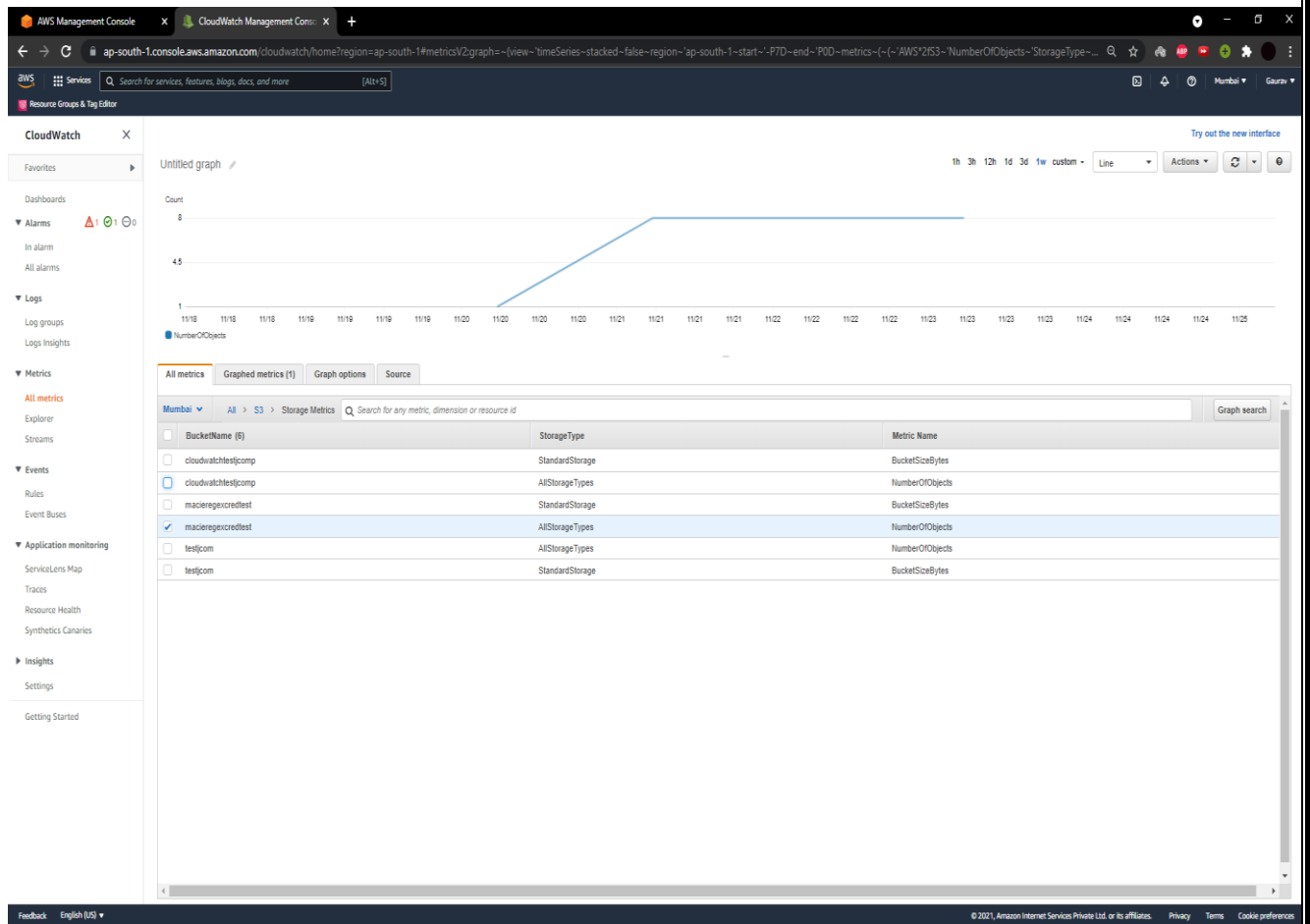
Amazon CloudWatch is AWS observing and management service which is intended to keep up with the management services and resources which are utilized Amazon CloudWatch is quite possibly the most utilized service presented by Amazon. It allows clients to monitor what's happening in their AWS Architecture. 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

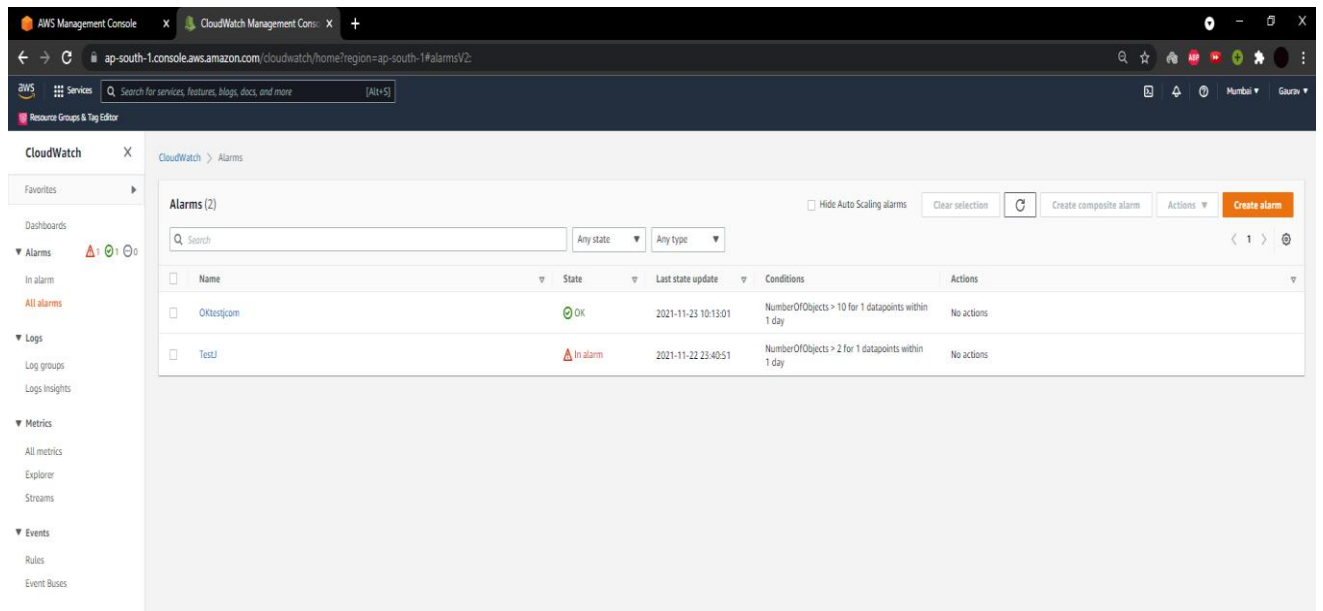
does and it is hosted in cloud.

- 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.

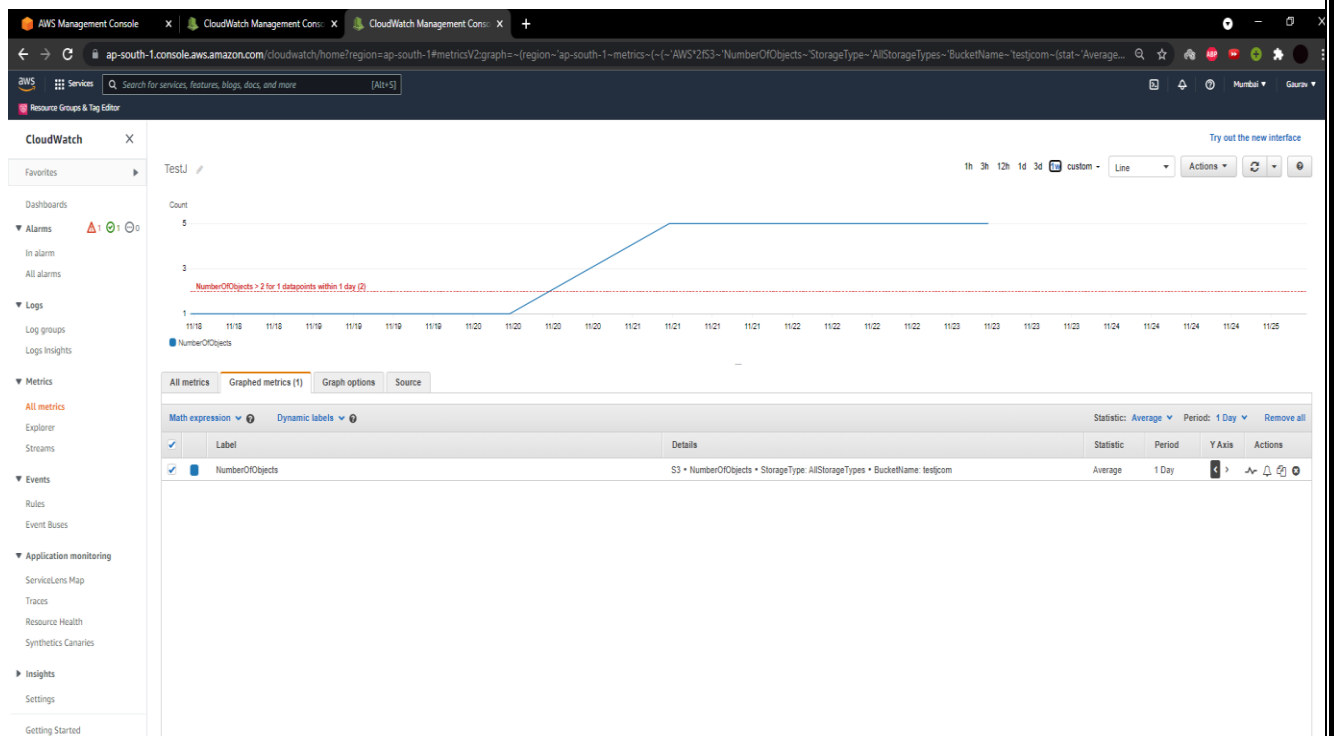
This is the graphical result after selecting the bucket name in the tab list which shows the log activity



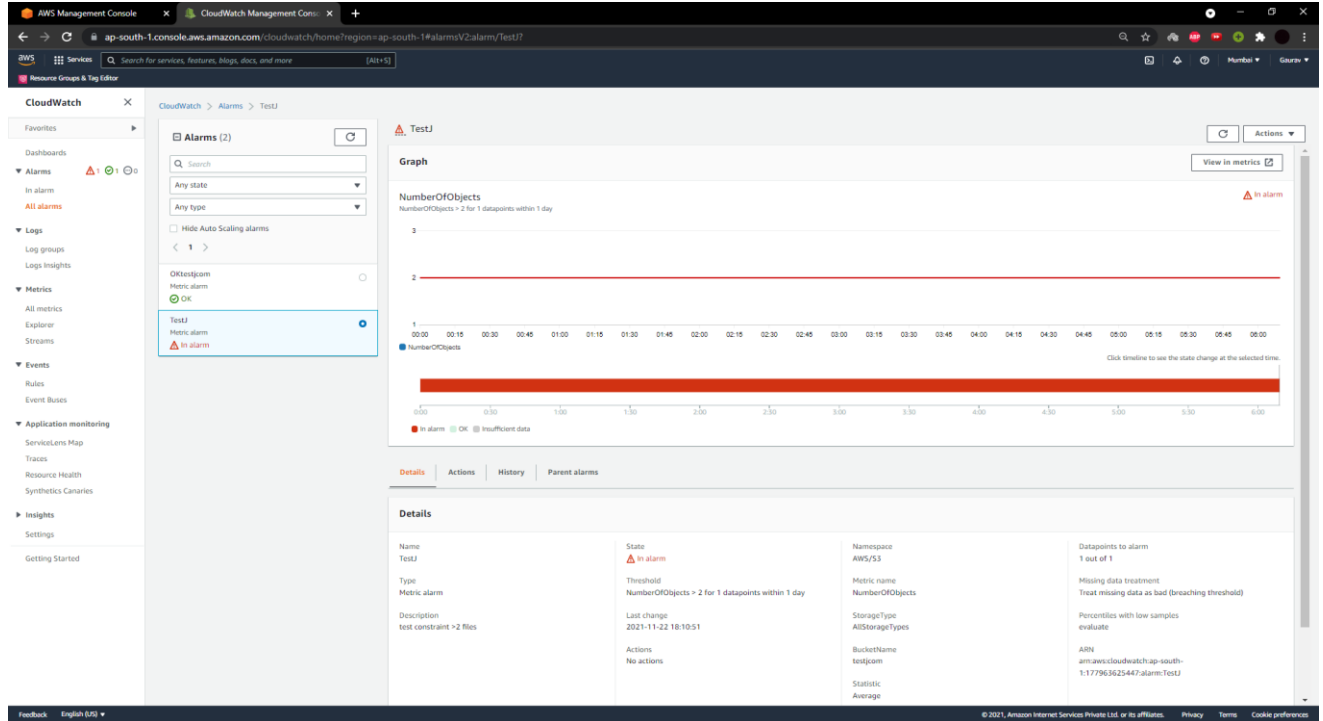
This is the page where alarm were set with name of testj and opentestj.com



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.

The screenshot displays the AWS CloudWatch console interface. The left-hand navigation pane includes sections for Dashboards, Alarms, Logs, Metrics, Events, and Application monitoring. The 'Logs' section is currently selected, showing 'Log groups' and 'Logs Insights'. The main content area is titled 'Log events' and shows a list of log events for the log group '/aws/macie/classificationjobs'. The events are filtered by the account ID '177963625447'. The table below shows three log events, each with a timestamp and a message. The first event is 'JOB_CREATED', the second is 'JOB_STARTED', and the third is 'JOB_FINISHED'. Each event message is a JSON object containing details about the job, including the account ID, job ID, event type, occurredAt, description, jobName, and runData. The 'Log events' section also includes a search bar, a 'Filter events' button, and a 'Copy' button for each event. The bottom of the console shows the 'Feedback' and 'English [US]' links.

CloudWatch > Log groups > /aws/macie/classificationjobs > 5166a1b387c987e1856c66092afe46

Log events

You can use the filter bar below to search for and match terms, phrases, or values in your log events. [Learn more about filter patterns](#)

Filter events

View as text Actions Create Metric Filter

Clear 1m 30m 1h 12h Custom

Timestamp	Message
No older events at this moment. Retry	
2021-11-20T11:49:11.876485:30	<pre>{ "accountId": "177963625447", "jobId": "1086a2b387c987e1856c66092afe46", "eventType": "JOB_CREATED", "occurredAt": "2021-11-20T06:19:11.876485Z", "description": "The job was created.", "jobName": "maciedemo" }</pre>
2021-11-20T11:49:18.932485:30	<pre>{ "accountId": "177963625447", "jobId": "1086a2b387c987e1856c66092afe46", "eventType": "JOB_STARTED", "occurredAt": "2021-11-20T06:19:18.932485Z", "description": "The job started running.", "jobName": "maciedemo", "runData": "2021-11-20T06:19:11.885395Z" }</pre>
2021-11-20T11:59:59.464437:30	<pre>{ "accountId": "177963625447", "jobId": "1086a2b387c987e1856c66092afe46", "eventType": "JOB_FINISHED", "occurredAt": "2021-11-20T06:29:59.464437Z", "description": "The job finished running.", "jobName": "maciedemo", "runData": "2021-11-20T06:19:11.885395Z" }</pre>

No newer events at this moment. Auto retry paused. Resume

Feedback English [US]

© 2021 Amazon Internet Services Private Ltd. or its affiliates. Privacy Terms Cookie preferences

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

The screenshot shows the AWS CloudWatch console interface. On the left, there's a sidebar with navigation options like Dashboards, Alarms, Logs, Metrics, Events, and Application monitoring. The main area displays a list of log events. One event is selected and expanded, showing the following details:

```
{
  "eventVersion": "1.08",
  "userIdentity": {
    "type": "Root",
    "principalId": "177963625447",
    "arn": "arn:aws:iam::177963625447:root",
    "accountId": "177963625447",
    "accessKeyId": "ASIA5533VNP7U4L4N64",
    "sessionContext": {
      "sessionIssuer": {},
      "webIdentityData": {},
      "attributes": {
        "creationDate": "2021-11-25T06:55:13Z",
        "mfaAuthenticated": "false"
      }
    }
  },
  "eventTime": "2021-11-25T06:03:17Z",
  "eventSource": "iam.amazonaws.com",
  "eventName": "ListRoles",
  "awsRegion": "us-east-1",
  "sourceIPAddress": "223.189.132.209",
  "userAgent": "aws-internal/3 aws-sdk-java/1.12.99 Linux/4.9.273-0.1.ac.226.84.332.metal1.x86_64 OpenJDK_64-Bit_Server_VM/25.312-b07 java/1.8.0_312 vendor/Oracle_Corporation cfp/retry-mode/standard",
  "requestParameters": {
    "maxItems": 1000
  },
  "responseElements": null,
  "requestID": "28bf28b7-7147-4a31-87dc-72630856c5c2",
  "eventID": "c6ada528-9286-4777-92ce-f8fc76410c85",
  "readOnly": true,
  "eventType": "AwsApiCall",
  "managementEvent": true,
  "recipientAccountId": "177963625447",
  "eventCategory": "Management",
  "sessionCredentialFromConsole": "true"
}
```

This is the another API call

The screenshot shows the AWS CloudWatch console interface. On the left, there's a sidebar with navigation options like Dashboards, Alarms, Logs, Metrics, Events, and Application monitoring. The main area displays a list of log events. One event is selected and expanded, showing the following details:

```
{
  "eventVersion": "1.08",
  "userIdentity": {
    "type": "Root",
    "principalId": "177963625447",
    "arn": "arn:aws:iam::177963625447:root",
    "accountId": "177963625447",
    "accessKeyId": "ASIA5533VNP7U4L4N64",
    "sessionContext": {
      "sessionIssuer": {},
      "webIdentityData": {},
      "attributes": {
        "creationDate": "2021-11-25T06:55:13Z",
        "mfaAuthenticated": "false"
      }
    }
  },
  "eventTime": "2021-11-25T06:03:17Z",
  "eventSource": "iam.amazonaws.com",
  "eventName": "ListRoles",
  "awsRegion": "us-east-1",
  "sourceIPAddress": "223.189.132.209",
  "userAgent": "aws-internal/3 aws-sdk-java/1.12.99 Linux/4.9.273-0.1.ac.226.84.332.metal1.x86_64 OpenJDK_64-Bit_Server_VM/25.312-b07 java/1.8.0_312 vendor/Oracle_Corporation cfp/retry-mode/standard",
  "requestParameters": {
    "maxItems": 1000
  },
  "responseElements": null,
  "requestID": "28bf28b7-7147-4a31-87dc-72630856c5c2",
  "eventID": "c6ada528-9286-4777-92ce-f8fc76410c85",
  "readOnly": true,
  "eventType": "AwsApiCall",
  "managementEvent": true,
  "recipientAccountId": "177963625447",
  "eventCategory": "Management",
  "sessionCredentialFromConsole": "true"
}
```

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

The screenshot displays the Amazon GuardDuty console interface. The left sidebar contains navigation links for Findings, Usage, Settings, Lists, S3 Protection, Accounts, What's New, and Partners. The main content area is titled 'GuardDuty > Findings' and shows a list of findings. At the top, there are buttons for 'Suppress Findings' and 'Info', and a 'Saved rules' section indicating 'No saved rules'. The findings are listed in a table with columns for Finding type, Resource, Last seen, and Count. The findings include various types such as PolicyIAMUser/RootCredentialUsage, [SAMPLE] Backdoor:EC2/DenialOfService.UnusualProtocol, [SAMPLE] PolicyIAMUser/RootCredentialUsage, [SAMPLE] UnauthorizedAccess:EC2/MetadataDNSRebind, [SAMPLE] PenTest:S3/KaliLinux, [SAMPLE] UnauthorizedAccess:IAMUser/InstanceCredentialExfiltration.OutsideAWS, [SAMPLE] Impact:EC2/MaliciousDomainRequest.Reputation, [SAMPLE] Trojan:EC2/BlackholeTraffic, [SAMPLE] PenTest:IAMUser/KaliLinux, [SAMPLE] UnauthorizedAccess:IAMUser/MaliciousIPCaller.Custom, [SAMPLE] Discovery:S3/MaliciousIPCaller.Custom, [SAMPLE] Exfiltration:IAMUser/AnomalousBehavior, [SAMPLE] UnauthorizedAccess:IAMUser/TorIPCaller, [SAMPLE] UnauthorizedAccess:EC2/SSHBruteForce, and [SAMPLE] UnauthorizedAccess:EC2/DDOSBruteForce.

Finding type	Resource	Last seen	Count
PolicyIAMUser/RootCredentialUsage	Root: ASIASS33VNP7ZVJUR5XI	7 minutes ago	435
PolicyIAMUser/RootCredentialUsage	Root: ASIASS33VNP7UG4EHCEH	9 minutes ago	47
[SAMPLE] Backdoor:EC2/DenialOfService.UnusualProtocol	Instance: i-999999999	3 days ago	2
[SAMPLE] PolicyIAMUser/RootCredentialUsage	GeneratedFindingUserName: GeneratedFindingAccessKeyid	3 days ago	2
[SAMPLE] UnauthorizedAccess:EC2/MetadataDNSRebind	Instance: i-999999999	3 days ago	2
[SAMPLE] PenTest:S3/KaliLinux	S3 Bucket: bucketName	3 days ago	2
[SAMPLE] UnauthorizedAccess:IAMUser/InstanceCredentialExfiltration.OutsideAWS	GeneratedFindingUserName: GeneratedFindingAccessKeyid	3 days ago	2
[SAMPLE] Impact:EC2/MaliciousDomainRequest.Reputation	Instance: i-999999999	3 days ago	2
[SAMPLE] Trojan:EC2/BlackholeTraffic	Instance: i-999999999	3 days ago	2
[SAMPLE] PenTest:IAMUser/KaliLinux	GeneratedFindingUserName: GeneratedFindingAccessKeyid	3 days ago	2
[SAMPLE] UnauthorizedAccess:IAMUser/MaliciousIPCaller.Custom	GeneratedFindingAWSName: GeneratedFindingAccessKeyid	3 days ago	2
[SAMPLE] Discovery:S3/MaliciousIPCaller.Custom	S3 Bucket: bucketName	3 days ago	2
[SAMPLE] Exfiltration:IAMUser/AnomalousBehavior	GeneratedFindingUserName: GeneratedFindingAccessKeyid	3 days ago	2
[SAMPLE] UnauthorizedAccess:IAMUser/TorIPCaller	GeneratedFindingUserName: GeneratedFindingAccessKeyid	3 days ago	2
[SAMPLE] UnauthorizedAccess:EC2/SSHBruteForce	Instance: i-999999999	3 days ago	2
[SAMPLE] UnauthorizedAccess:EC2/DDOSBruteForce	Instance: i-000000000	3 days ago	2

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

The screenshot shows the AWS GuardDuty Management Console interface. The browser address bar displays the URL: `ap-south-1.console.aws.amazon.com/guardduty/home?region=ap-south-1#/s3-protection`. The top navigation bar includes the AWS logo, a 'Services' menu, a search bar with the placeholder text 'Search for services, features, blogs, docs, and more', and a '[Alt+S]' shortcut. Below the navigation bar, the left sidebar contains the 'GuardDuty' header with a close button, followed by a list of items: 'Findings', 'Usage', 'Settings' (with sub-items 'Lists', 'S3 Protection' (highlighted in orange), and 'Accounts'), 'What's New', and 'Partners' with an external link icon. The main content area shows the breadcrumb 'GuardDuty > Settings > S3 Protection'. The title 'S3 Protection' is displayed with an 'Info' link. To the right of the title, it indicates '28 days remaining' and a 'Free trial' button. A box titled 'S3 Protection' contains the description 'Monitor and generate findings on S3 data events'. Below this, a green checkmark icon is followed by the text 'S3 Protection is enabled on this account' and a 'Disable' link. At the bottom of the box, there is a link to 'Learn more about how GuardDuty processes S3 Data Events' and another 'Learn more' link.

GuardDuty Management Console

ap-south-1.console.aws.amazon.com/guardduty/home?region=ap-south-1#/s3-protection

Services Search for services, features, blogs, docs, and more [Alt+S]

Resource Groups & Tag Editor

GuardDuty X

Findings

Usage

Settings

Lists

S3 Protection

Accounts

What's New

Partners

GuardDuty > Settings > S3 Protection

S3 Protection Info

28 days remaining Free trial

S3 Protection

Monitor and generate findings on S3 data events

✔ S3 Protection is enabled on this account Disable

Learn more about how GuardDuty processes S3 Data Events. Learn more