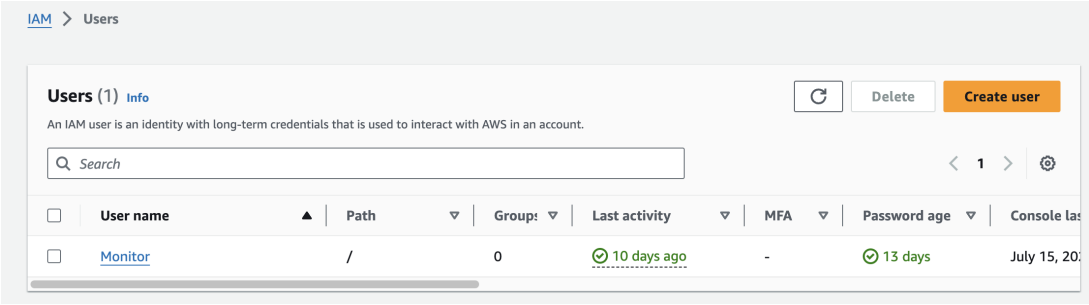
Summer Training : Monitor Infrastructure with AWS CloudWatch and CloudTrail

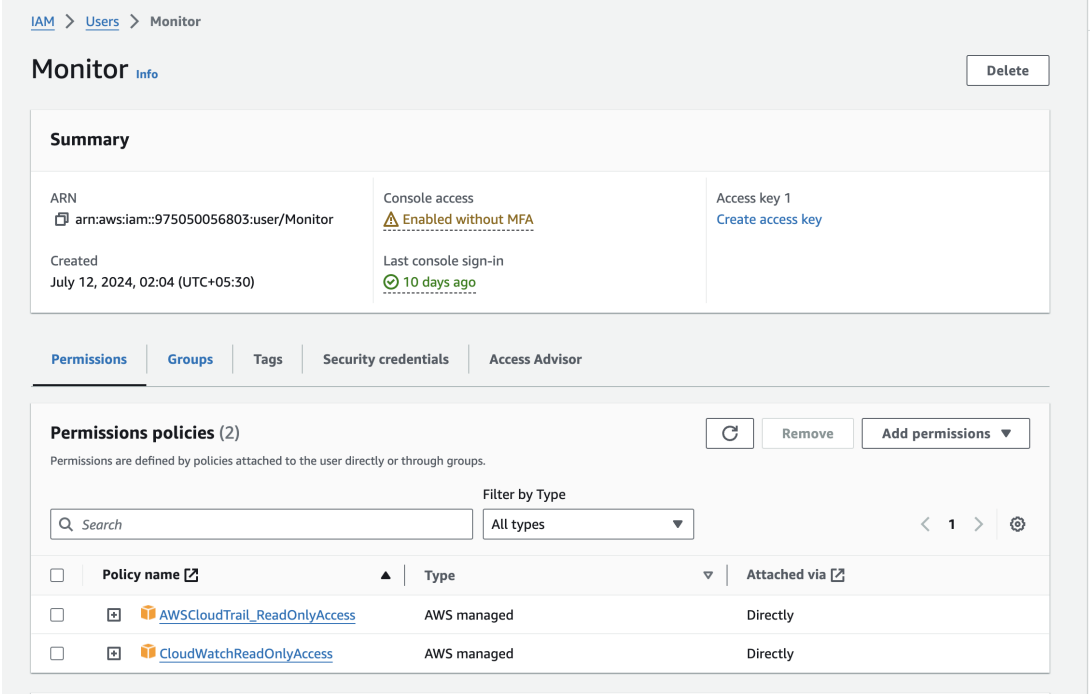
Project Objective:

To utilize AWS CloudWatch and CloudTrail for comprehensive monitoring and logging of infrastructure activities, aiming to enhance resource management, security, and compliance.

IAM User Creation

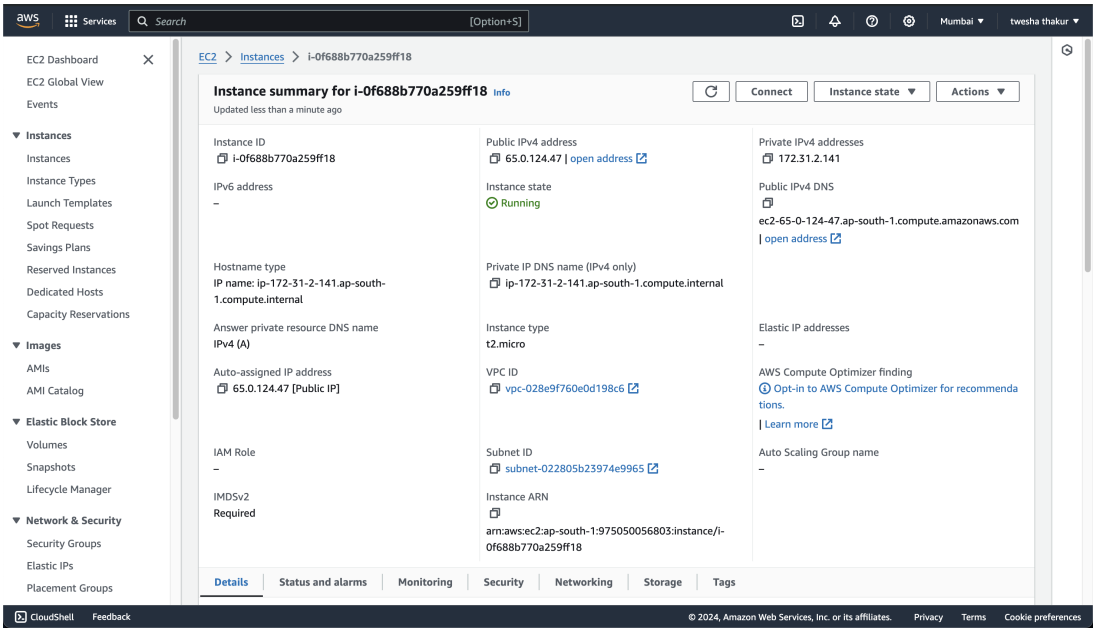
- Monitor user - user with permissions to just read cloudwatch dashboard and logs.

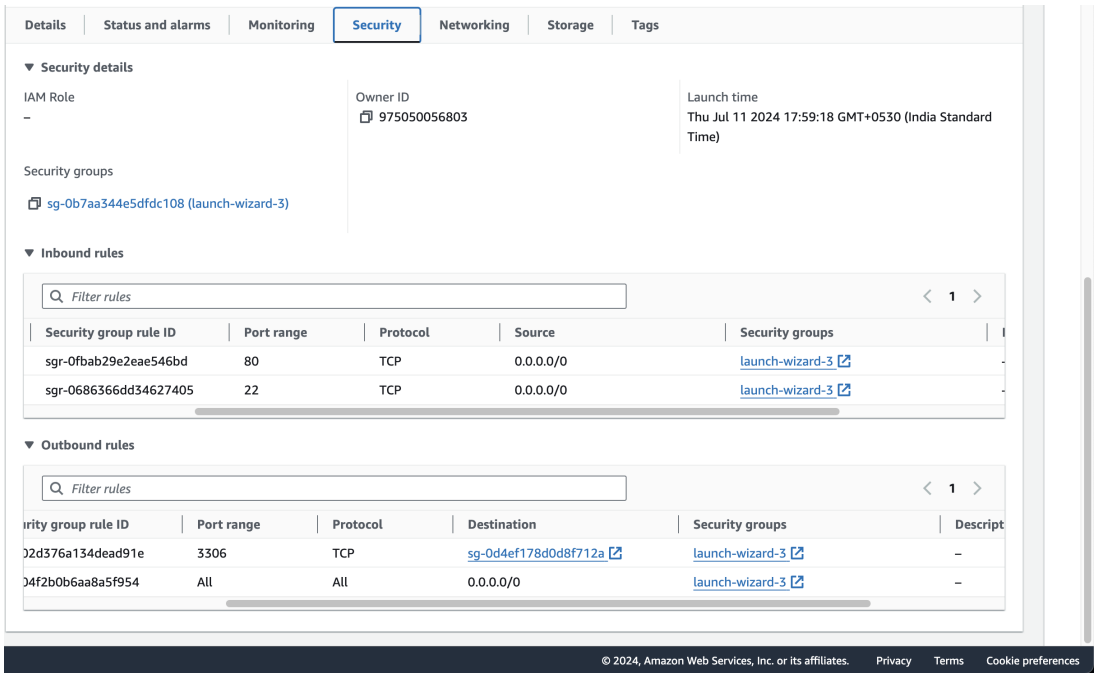




EC2 Instance

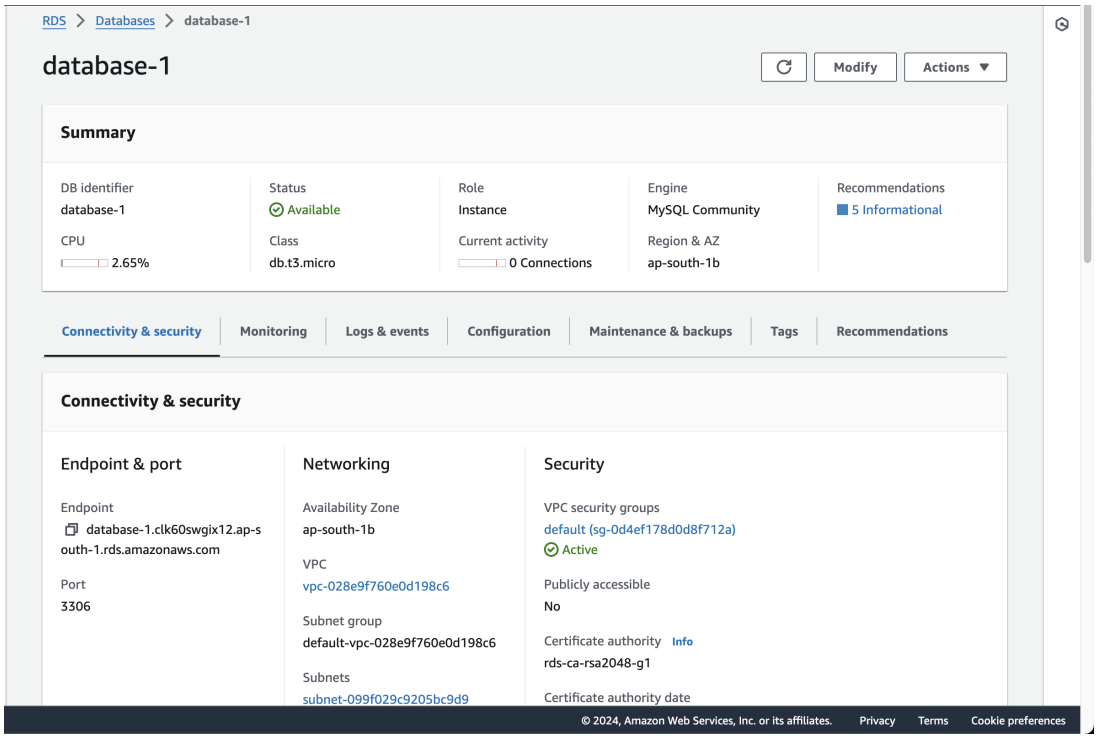
- apache (httpd) server deployed on it where a basic html file is deployed
- ec2 instance's metrics like cpu utilization and network in and out metrics are noted

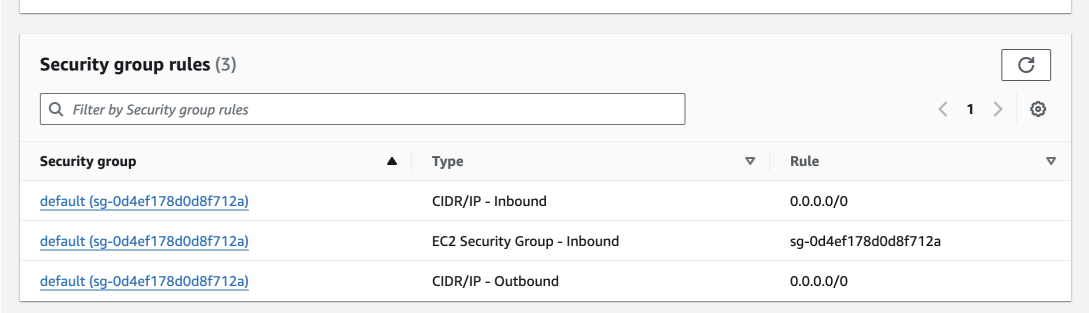




RDS Database

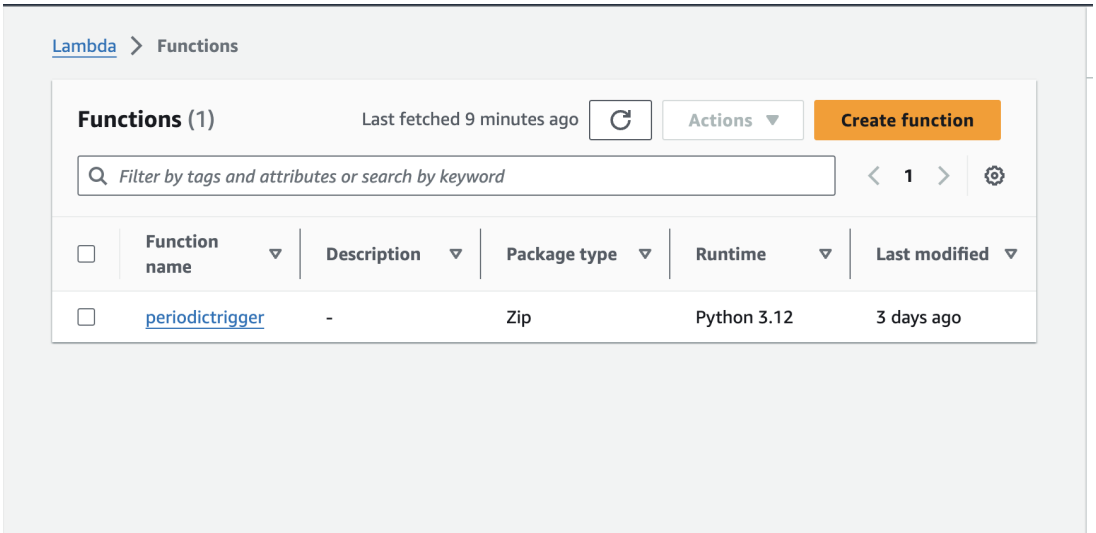
- test database is made
- metrics like disk read write, cpu utilizations, and database connectionss such things are monitored

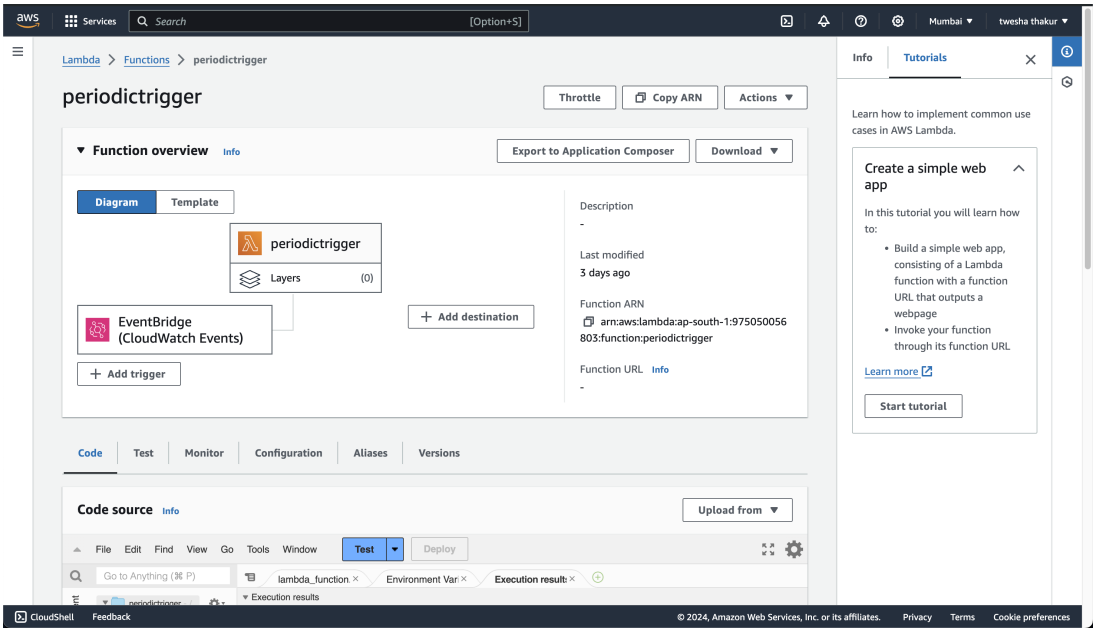


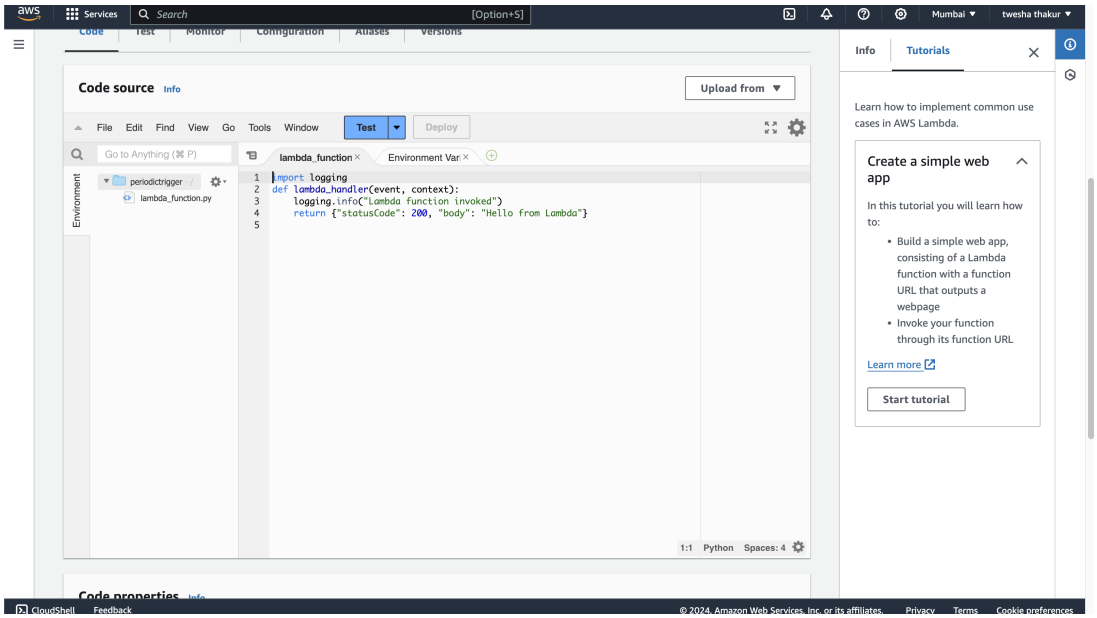


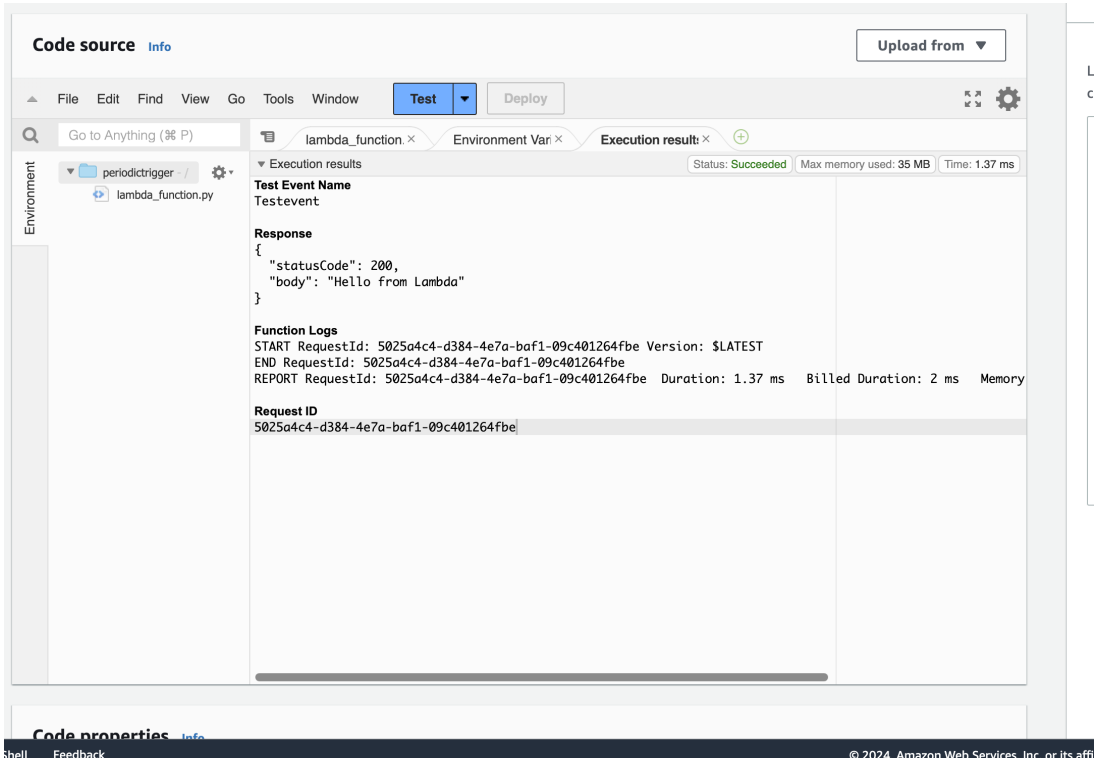
Lambda Function

- periodic triggering this lambda, manually invoking to create logs so that i can monitor it on cloudwatch
- cron job is used triggering lambda periodictrigger function every five minutes





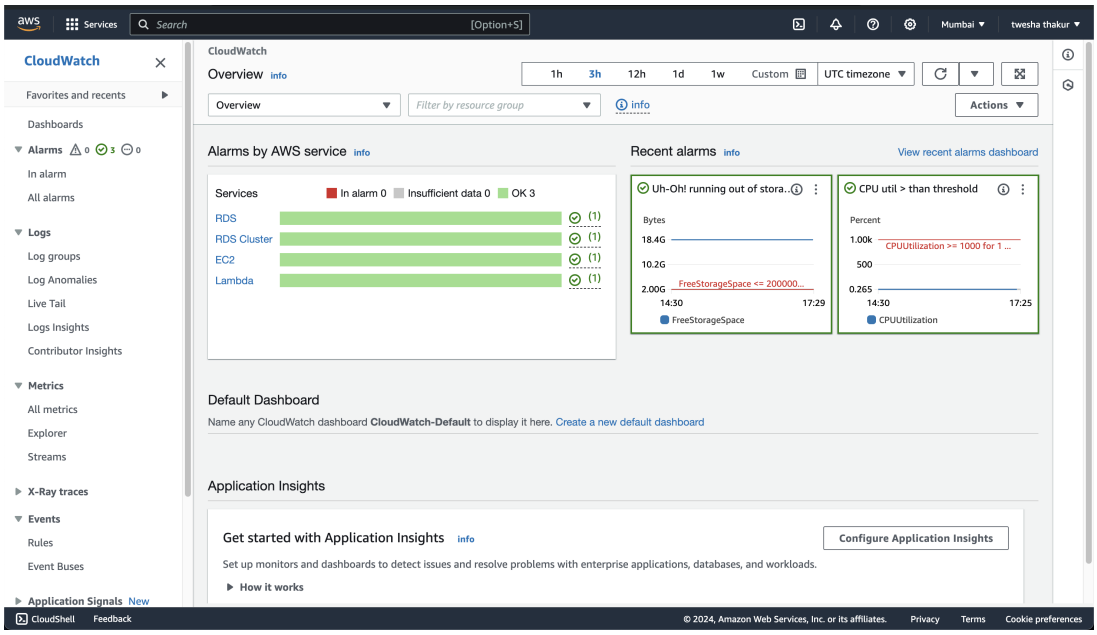


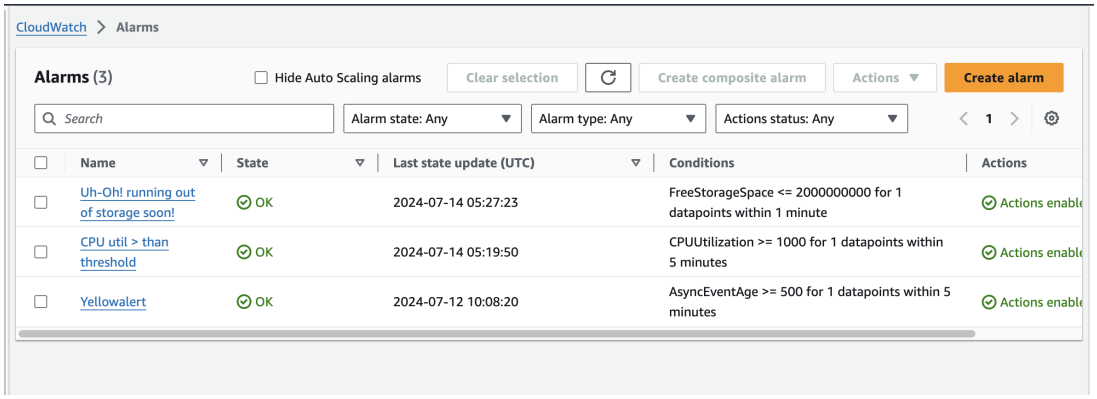


AWS CloudWatch Configuration

CloudWatch Alarms

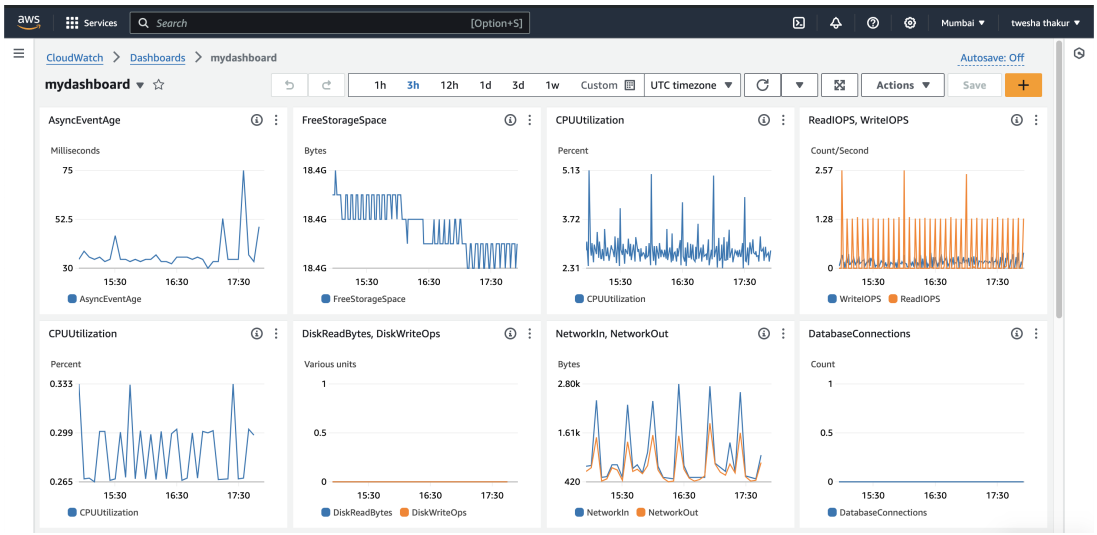
- 4 alarms about storage, cpulitilizaion and asynceventage have been set up

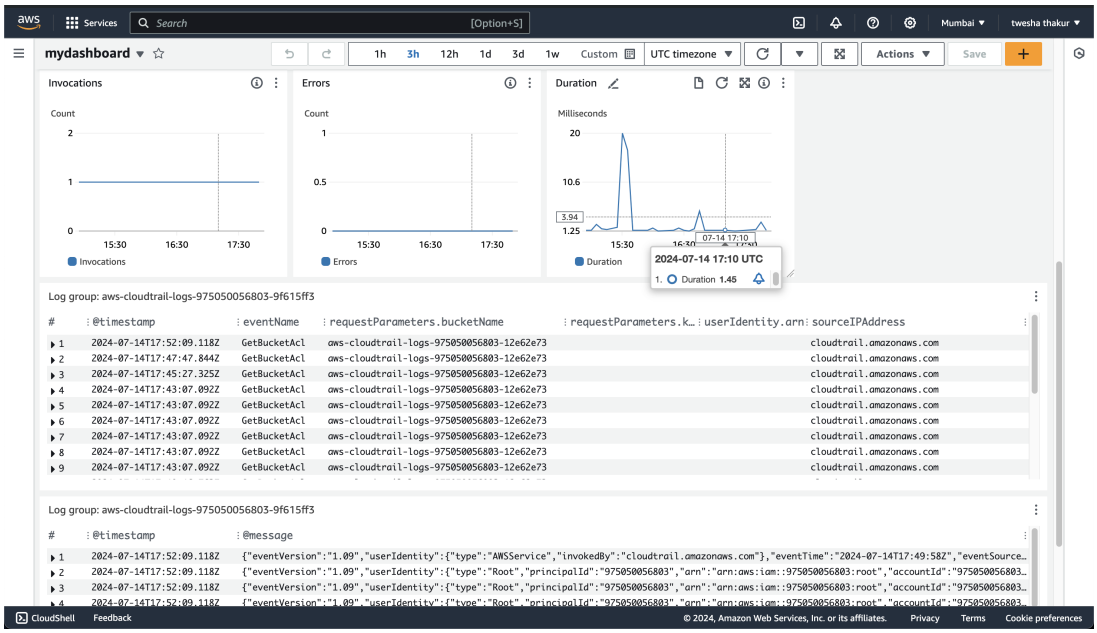




CloudWatch Dashboards

- Mydashboard is created for monitoring cloudwatch dashboard
- Row 1 widgets - EC2 instance metrics
- Row 2 widgets - RDS database metrics
- Row 3 widgets - Lambda function metrics





AWS CloudTrail Configuration

Creating a Trail

- **Why**: CloudTrail captures and logs all API calls and actions within the AWS account, providing a comprehensive record of activity. This is crucial for auditing, security, and compliance purposes.

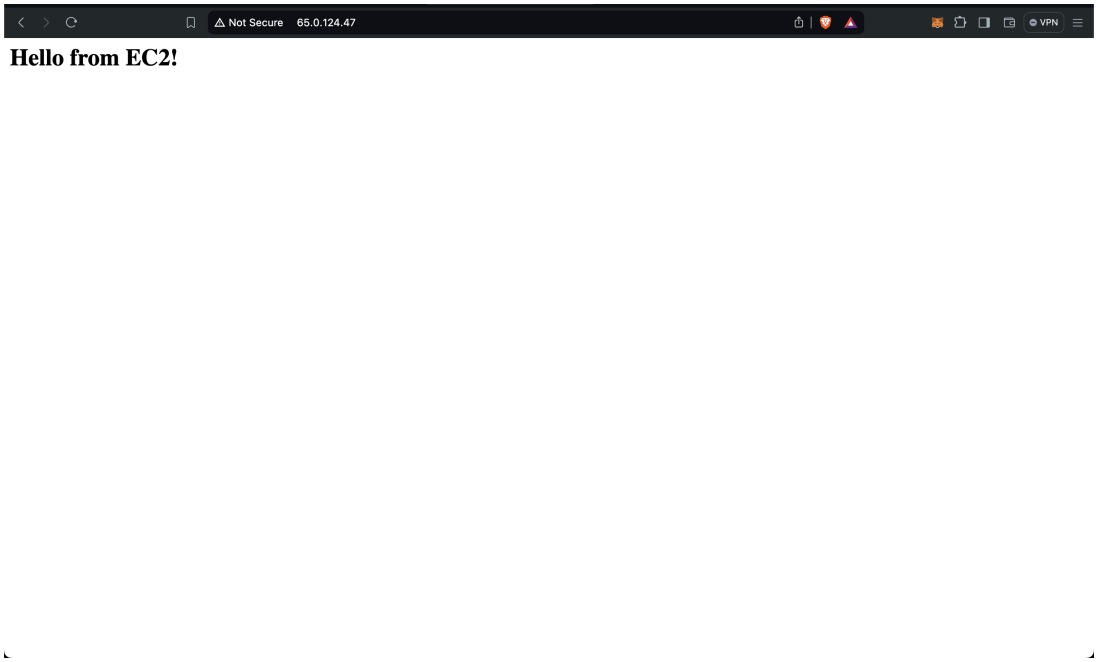
Configuring Data Events

- **Why**: Enabling data events for specific resources like S3 buckets or Lambda functions allows us to monitor access and changes to sensitive data. This enhances security by providing detailed visibility into data operations.

Traffic Generation

EC2 Instance Traffic

- Visiting this html page from browser generates traffic on ec2 instance.
- This html page is installed in apache server in ec2 instance
- This web page traffic can also be generated through cli using curl command.



RDS Database Traffic

- Connecting to mysql client and fetching data from test database generates traffic on RDS database

Lambda Function Traffic

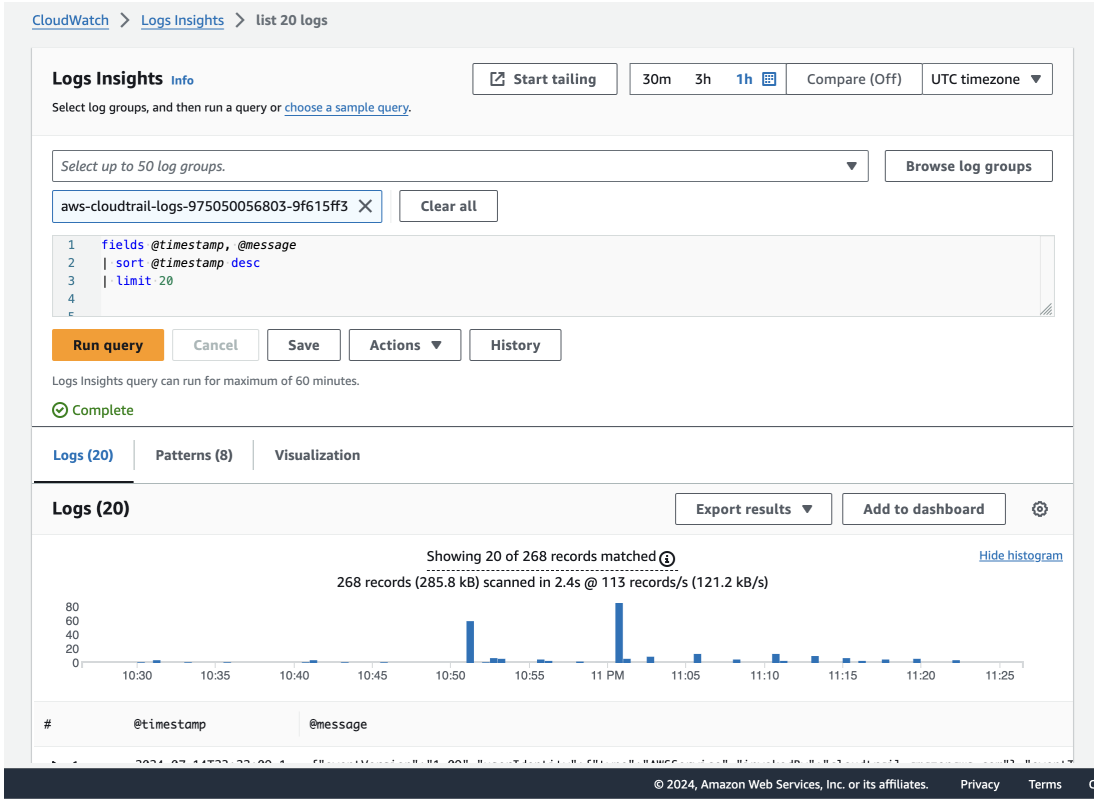
- A cron job in periodictrigger lambda function triggers the function every 5 minutes and generate a good amount of traffic to monitor

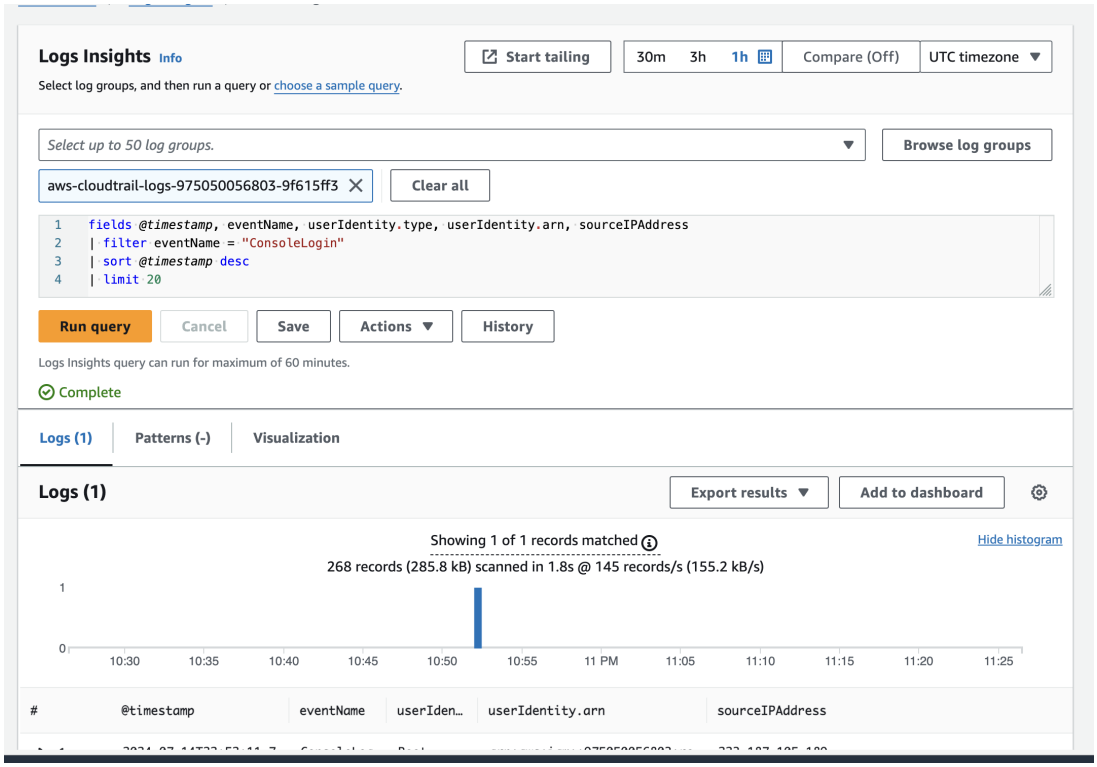
---

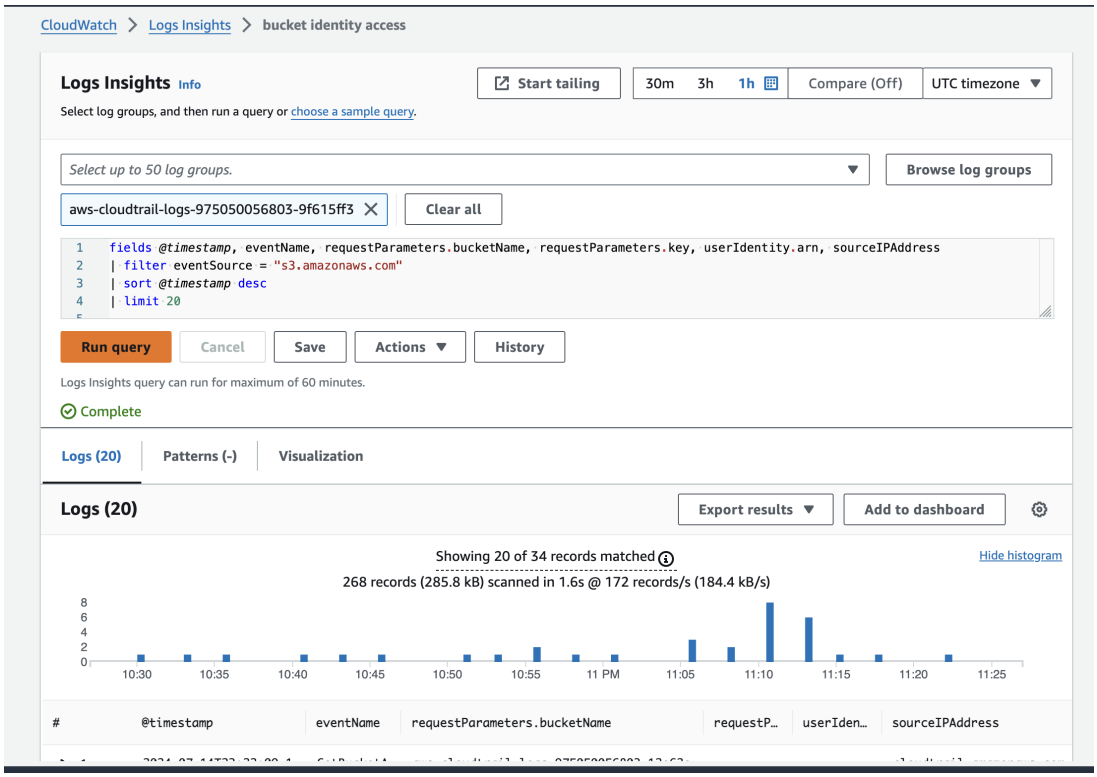
Monitoring and Analysis

CloudWatch Metrics

- **Why**: Metrics provide quantitative data on resource performance. Analyzing these metrics helps identify trends, detect anomalies, and optimize resource utilization.
- Invoking the Lambda function periodically generates logs and metrics that can be monitored. This demonstrates how serverless functions can be tracked and managed using CloudWatch and CloudTrail.

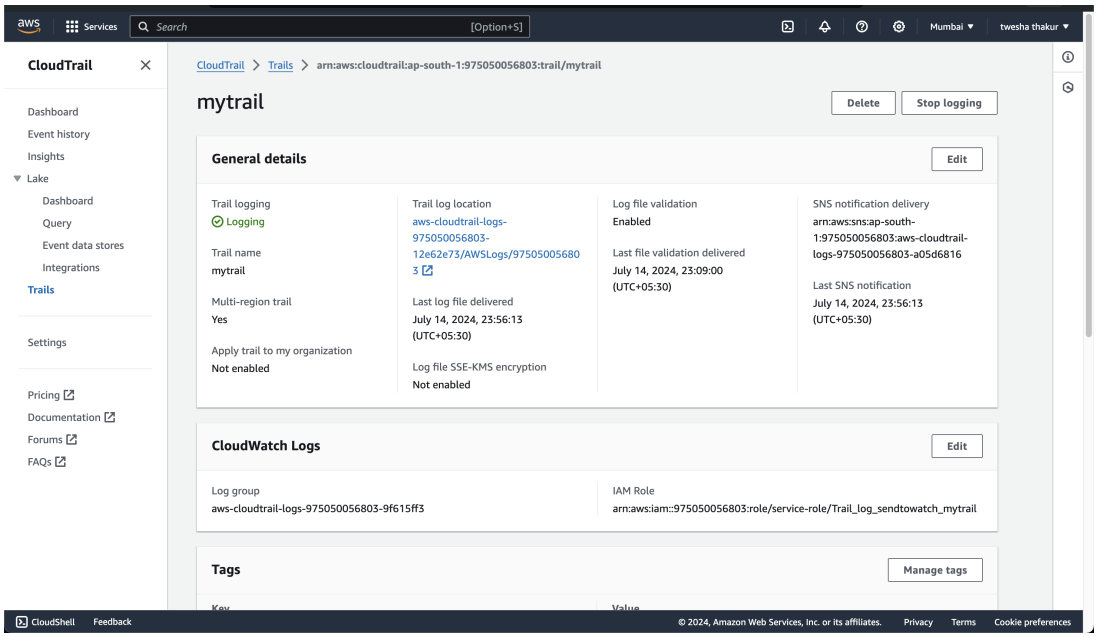

CloudWatch > Logs Insights > list 20 logs
Logs Insights Info
Start tailing
30m 3h 1h
Compare (Off)
UTC timezone
Select log groups, and then run a query or choose a sample query.
Select up to 50 log groups.
Browse log groups
aws-cloudtrail-logs-975050056803-9f615ff3
Clear all
fields @timestamp, @message
| sort @timestamp desc
| limit 20
Run query
Cancel
Save
Actions
History
Logs Insights query can run for maximum of 60 minutes.
Complete
Logs (20)
Patterns (8)
Visualization
Logs (20)
Export results
Add to dashboard
Showing 20 of 268 records matched
Hide histogram
268 records (285.8 kB) scanned in 2.4s @ 113 records/s (121.2 kB/s)
80
60
40
20
0
10:30
10:35
10:40
10:45
10:50
10:55
11 PM
11:05
11:10
11:15
11:20
11:25
#
@timestamp
@message
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms

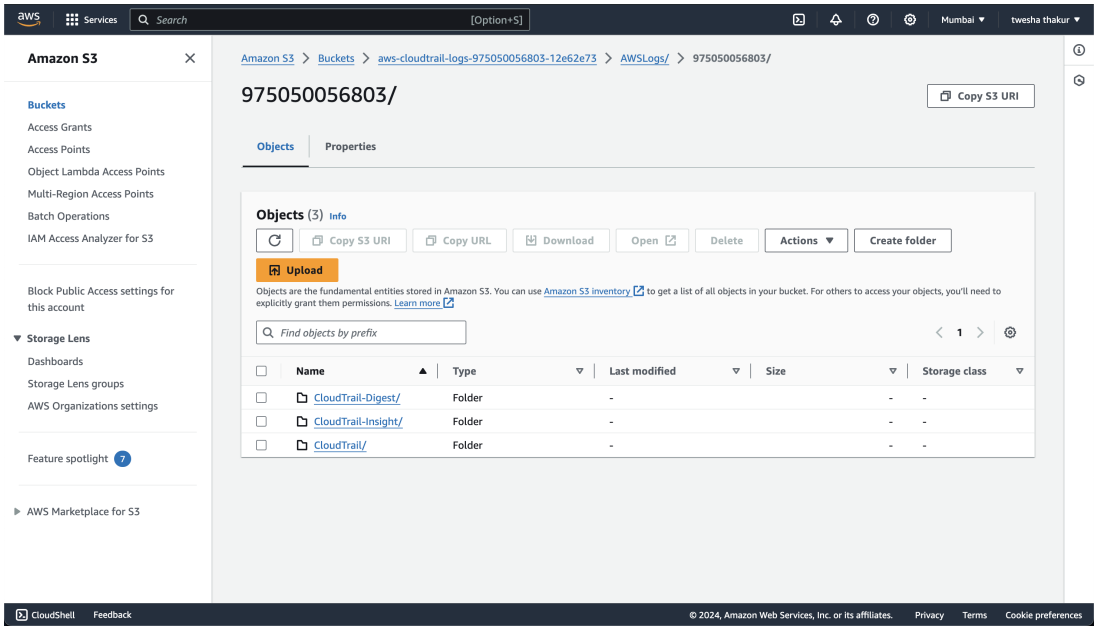

Logs Insights Info
Start tailing
30m 3h 1h
Compare (Off)
UTC timezone
Select log groups, and then run a query or choose a sample query.
Select up to 50 log groups.
Browse log groups
aws-cloudtrail-logs-975050056803-9f615ff3
Clear all
fields @timestamp, eventName, userIdentity.type, userIdentity.arn, sourceIPAddress
| filter eventName = "ConsoleLogin"
| sort @timestamp desc
| limit 20
Run query
Cancel
Save
Actions
History
Logs Insights query can run for maximum of 60 minutes.
Complete
Logs (1)
Patterns (-)
Visualization
Logs (1)
Export results
Add to dashboard
Showing 1 of 1 records matched
Hide histogram
268 records (285.8 kB) scanned in 1.8s @ 145 records/s (155.2 kB/s)
1
0
10:30
10:35
10:40
10:45
10:50
10:55
11 PM
11:05
11:10
11:15
11:20
11:25
#
@timestamp
eventName
userIden…
userIdentity.arn
sourceIPAddress

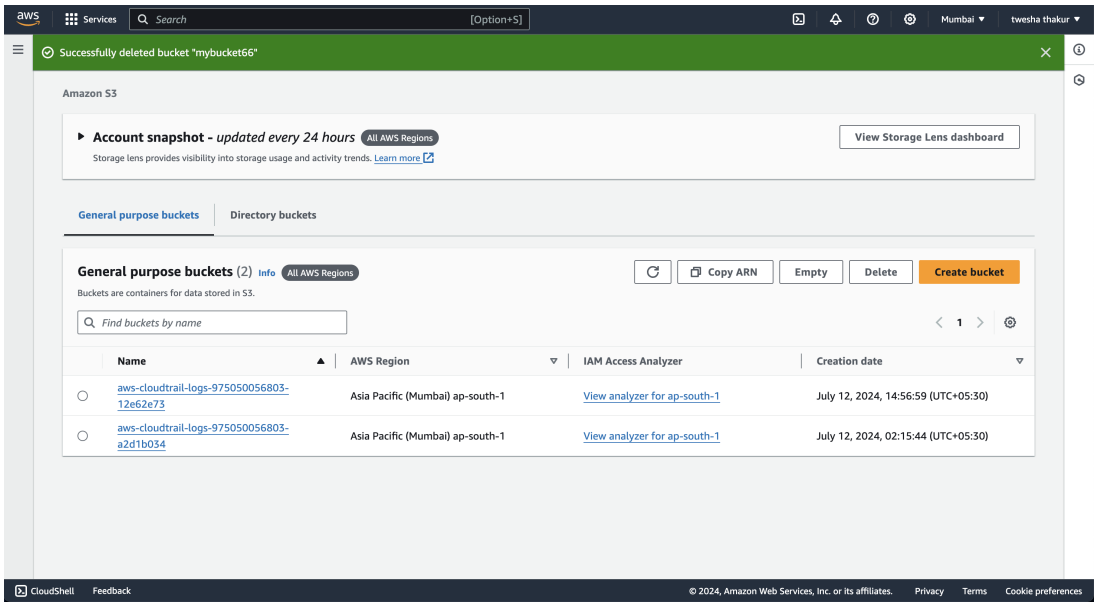


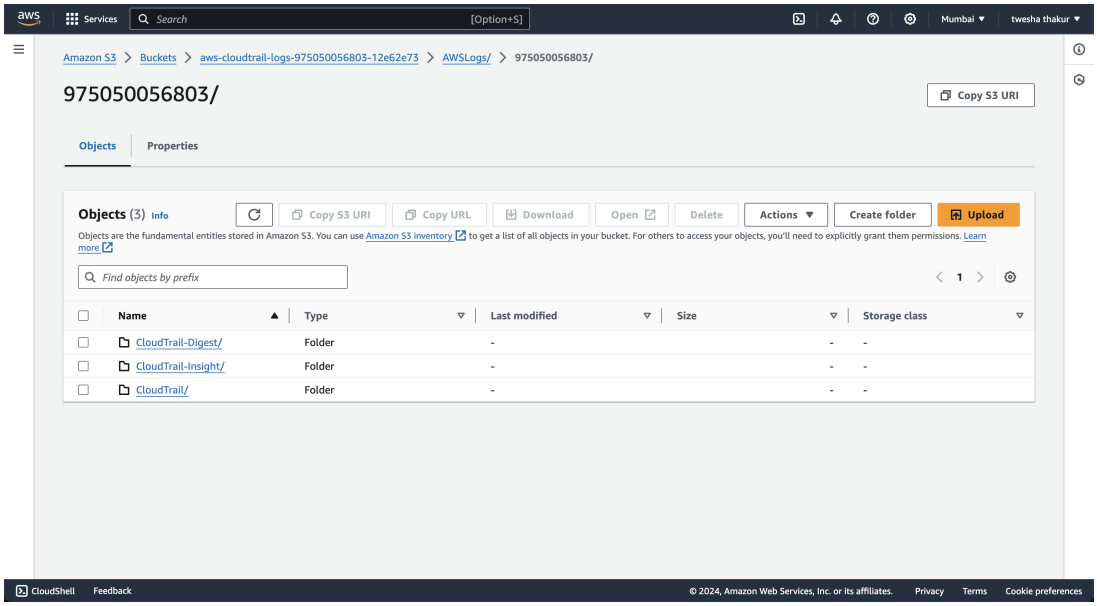
CloudTrail Logs

- Logs from CloudTrail offer a detailed account of all actions within the AWS account. Analyzing these logs helps ensure compliance, detect unauthorized activities, and maintain security.
- mytrail - this cloudtrail log is created to log all activity in the account
- all the cloudtrail generated log data is then stored in an S3 bucket


aws
Services
Search
[Option+S]
Mumbai
twesha thakur
CloudTrail
Dashboard
Event history
Insights
Lake
Dashboard
Query
Event data stores
Integrations
Trails
Settings
Pricing
Documentation
Forums
FAQs
CloudTrail > Trails > arn:aws:cloudtrail:ap-south-1:975050056803:trail/mytrail
mytrail
Delete
Stop logging
General details
Edit
Trail logging
Logging
Trail name
mytrail
Multi-region trail
Yes
Apply trail to my organization
Not enabled
Trail log location
aws-cloudtrail-logs-975050056803-12e62e73/AWSLogs/975050056803
Last log file delivered
July 14, 2024, 23:56:13 (UTC+05:30)
Log file SSE-KMS encryption
Not enabled
Log file validation
Enabled
Last file validation delivered
July 14, 2024, 23:09:00 (UTC+05:30)
SNS notification delivery
arn:aws:sns:ap-south-1:975050056803:aws-cloudtrail-logs-975050056803-a05d6816
Last SNS notification
July 14, 2024, 23:56:13 (UTC+05:30)
CloudWatch Logs
Edit
Log group
aws-cloudtrail-logs-975050056803-9f615ff3
IAM Role
arn:aws:iam::975050056803:role/service-role/Trail_log_sendtowatch_mytrail
Tags
Manage tags
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

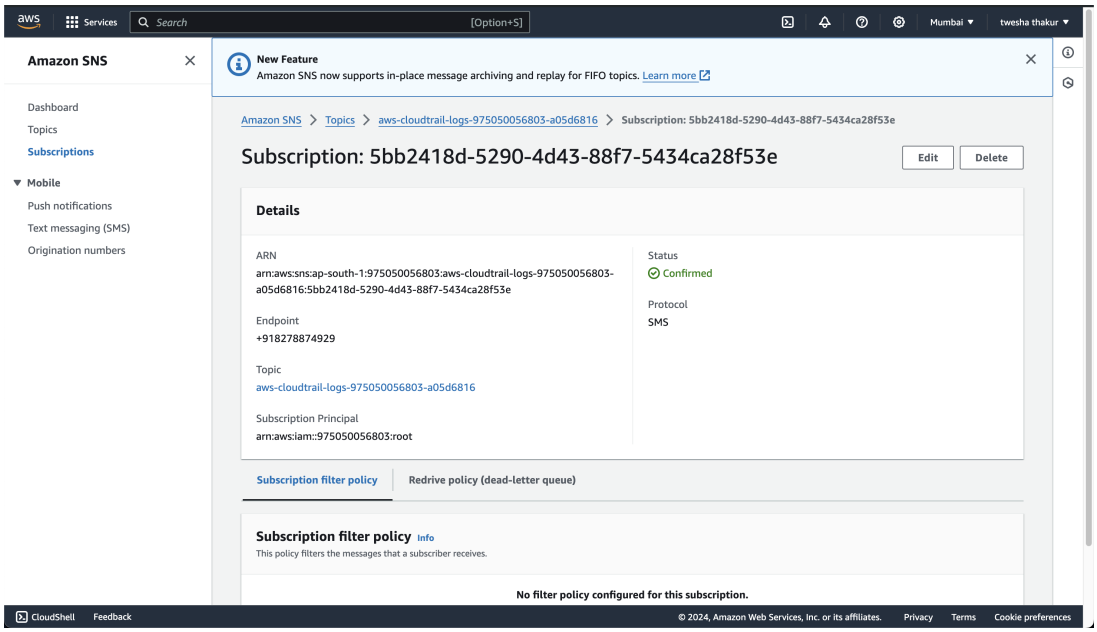

aws
Services
Search
[Option+S]
Mumbai
twesha thakur
Amazon S3
Buckets
Access Grants
Access Points
Object Lambda Access Points
Multi-Region Access Points
Batch Operations
IAM Access Analyzer for S3
Block Public Access settings for this account
Storage Lens
Dashboards
Storage Lens groups
AWS Organizations settings
Feature spotlight
7
AWS Marketplace for S3
Amazon S3 > Buckets > aws-cloudtrail-logs-975050056803-12e62e73 > AWSLogs/ > 975050056803/
975050056803/
Copy S3 URI
Objects
Properties
Objects (3) Info
Copy S3 URI
Copy URL
Download
Open
Delete
Actions
Create folder
Upload
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
1
Name
Type
Last modified
Size
Storage class
CloudTrail-Digest/
Folder
CloudTrail-Insight/
Folder
CloudTrail/
Folder
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

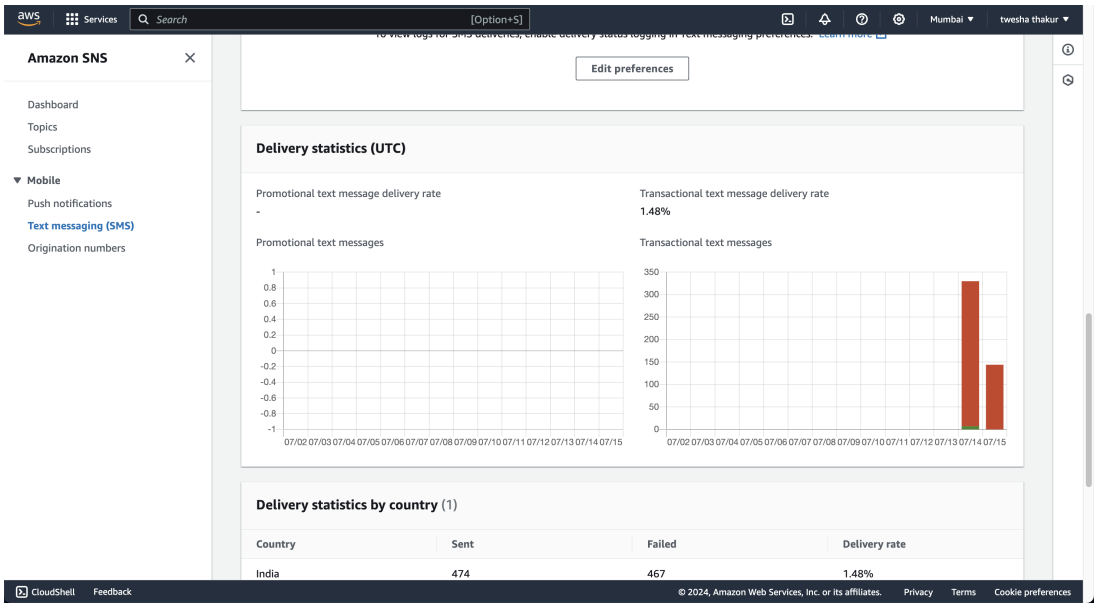


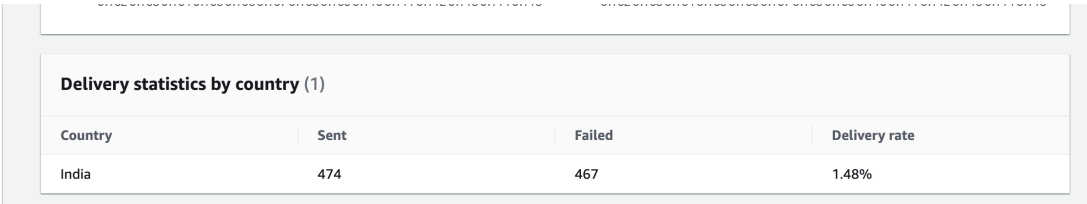


SNS

- Simple Notification Service enables push, text notification to alert about the alarms and activity happening in logs







Findings and Insights

- A badly configured SNS led to increased cost

References

Documentation

1. **AWS CloudWatch**:
   - Amazon CloudWatch Documentation: https://docs.aws.amazon.com/cloudwatch/index.html
   - CloudWatch Alarms: https://docs.aws.amazon.com/AmazonCloudWatch/latest/monitoring/AlarmThatSendsEmail.html
   - CloudWatch Logs: https://docs.aws.amazon.com/AmazonCloudWatch/latest/logs/WhatIsCloudWatchLogs.html
   - CloudWatch Dashboards: https://docs.aws.amazon.com/AmazonCloudWatch/latest/monitoring/CloudWatch_Dashboards.html
2. **AWS CloudTrail**:
   - AWS CloudTrail Documentation: https://docs.aws.amazon.com/cloudtrail/index.html
   - Creating a Trail: https://docs.aws.amazon.com/awscloudtrail/latest/userguide/cloudtrail-create-and-update-a-trail.html
   - CloudTrail to S3: https://docs.aws.amazon.com/awscloudtrail/latest/userguide/cloudtrail-create-and-validate-logs.html
3. **AWS SNS (Simple Notification Service)**:
   - Amazon SNS Documentation: https://docs.aws.amazon.com/sns/index.html
   - Setting Up Amazon SNS Notifications: https://docs.aws.amazon.com/sns/latest/dg/sns-getting-started.html
4. **AWS IAM (Identity and Access Management)**:
   - AWS IAM Documentation: https://docs.aws.amazon.com/iam/index.html
   - IAM Roles: https://docs.aws.amazon.com/IAM/latest/UserGuide/id_roles.html
   - IAM Policies: https://docs.aws.amazon.com/IAM/latest/UserGuide/access_policies.html
5. **AWS Lambda**:
   - AWS Lambda Documentation: https://docs.aws.amazon.com/lambda/index.html
   - Using AWS Lambda with Other Services: https://docs.aws.amazon.com/lambda/latest/dg/lambda-services.html
6. **AWS CloudFormation**:
   - AWS CloudFormation Documentation: https://docs.aws.amazon.com/cloudformation/index.html
   - Creating CloudFormation Stacks: https://docs.aws.amazon.com/AWSCloudFormation/latest/UserGuide/cfn-console-create-stack.html

Tools:

1. **AWS Cost Explorer**:
   - AWS Cost Explorer Documentation: https://docs.aws.amazon.com/cost-management/latest/userguide/ce-what-is.html

2. **AWS Budgets**:
    - AWS Budgets Documentation: https://docs.aws.amazon.com/cost-management/latest/userguide/budgets-managing-costs.html