



# 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.

The screenshot shows the AWS IAM 'Users' page. At the top, there is a breadcrumb navigation 'IAM > Users'. Below the header, a table displays a single user entry:

User name	Path	Group	Last activity	MFA	Password age	Console last used
Monitor	/	0	10 days ago	-	13 days	July 15, 2023

At the top right of the table, there are buttons for 'Create user' (orange), 'Delete' (grey), and a refresh icon. To the right of the table, there are navigation arrows and a settings gear icon.

IAM > Users > Monitor

## Monitor Info

[Delete](#)

Summary			
ARN arn:aws:iam::975050056803:user/Monitor	Console access <span style="color: red;">⚠ Enabled without MFA</span>	Last console sign-in <span style="color: green;">10 days ago</span>	Access key 1 <a href="#">Create access key</a>
Created July 12, 2024, 02:04 (UTC+05:30)			

[Permissions](#) | [Groups](#) | [Tags](#) | [Security credentials](#) | [Access Advisor](#)

Permissions policies (2)		
Permissions are defined by policies attached to the user directly or through groups. Filter by Type <input type="text" value="Search"/> <input type="button" value="All types"/> Policy name □ <span style="float: right;">Type</span> ▲ <span style="float: right;">Attached via □</span> AWSCloudTrail_ReadOnlyAccess <span style="float: right;">Directly</span> CloudWatchReadOnlyAccess <span style="float: right;">Directly</span>		

## 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

aWS Services Search [Option+S]

Mumbai twesha thakur

EC2 Dashboard EC2 > Instances i-0f688b770a259ff18

Instance summary for i-0f688b770a259ff18 Info

Updated less than a minute ago

Instance ID i-0f688b770a259ff18	Public IPv4 address 65.0.124.47   <a href="#">open address</a>	Private IPv4 addresses 172.31.2.141
IPv6 address -	Instance state Running	Public IPv4 DNS ec2-65-0-124-47.ap-south-1.compute.amazonaws.com   <a href="#">open address</a>
Hostname type IP name: ip-172-31-2-141.ap-south-1.compute.internal	Private IP DNS name (IPv4 only) ip-172-31-2-141.ap-south-1.compute.internal	Elastic IP addresses -
Answer private resource DNS name IPv4 (A)	Instance type t2.micro	AWS Compute Optimizer finding Opt-in to AWS Compute Optimizer for recommendations.
Auto-assigned IP address 65.0.124.47 [Public IP]	VPC ID vpc-028e9f760e0d198c6	Learn more
IAM Role -	Subnet ID subnet-022805b23974e9965	Auto Scaling Group name -
IMDSv2 Required	Instance ARN arn:aws:ec2:ap-south-1:975050056803:instance/i-0f688b770a259ff18	

[Details](#) | [Status and alarms](#) | [Monitoring](#) | [Security](#) | [Networking](#) | [Storage](#) | [Tags](#)

© 2024, Amazon Web Services, Inc. or its affiliates. [Privacy](#) [Terms](#) [Cookie preferences](#)

**Security details**

IAM Role	Owner ID	Launch time
-	975050056803	Thu Jul 11 2024 17:59:18 GMT+0530 (India Standard Time)

**Inbound rules**

Security group rule ID	Port range	Protocol	Source	Security groups
sgr-0fbab29e2ae546bd	80	TCP	0.0.0.0/0	launch-wizard-3
sgr-0686366dd34627405	22	TCP	0.0.0.0/0	launch-wizard-3

**Outbound rules**

Security group rule ID	Port range	Protocol	Destination	Security groups	Description
02d376a134dead91e	3306	TCP	sg-0d4ef178d0d8f712a	launch-wizard-3	-
04f2b0b6aa8a5f954	All	All	0.0.0.0/0	launch-wizard-3	-

## RDS Database

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

**Summary**

DB identifier	Status	Role	Engine	Recommendations
database-1	Available	Instance	MySQL Community	5 Informational
CPU	Class	Current activity	Region & AZ	
2.65%	db.t3.micro	0 Connections	ap-south-1b	

**Connectivity & security**

Endpoint & port	Networking	Security
Endpoint database-1.clk60swgix12.ap-south-1.rds.amazonaws.com	Availability Zone ap-south-1b	VPC security groups default (sg-0d4ef178d0d8f712a) Active
Port 3306	VPC vpc-028e9f760e0d198c6	Publicly accessible No
	Subnet group default-vpc-028e9f760e0d198c6	Certificate authority Info rds-ca-rsa2048-g1
	Subnets subnet-099f029c9205bc9d9	Certificate authority date

Security group rules (3)		
<input type="text"/> Filter by Security group rules		
Security group	Type	
default (sg-0d4ef178d0d8f712a)	CIDR/IP - Inbound	0.0.0.0/0
default (sg-0d4ef178d0d8f712a)	EC2 Security Group - Inbound	sg-0d4ef178d0d8f712a
default (sg-0d4ef178d0d8f712a)	CIDR/IP - Outbound	0.0.0.0/0

## 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 periodicttrigger function every five minutes

Functions (1)					Last fetched 9 minutes ago	<input type="button"/> C	Actions	<input type="button" value="Create function"/>	
<input type="text"/> Filter by tags and attributes or search by keyword						<	1	>	⚙️
<input type="checkbox"/>	Function name	Description	Package type	Runtime	Last modified				
<input type="checkbox"/>	<a href="#">periodicttrigger</a>	-	Zip	Python 3.12	3 days ago				

The screenshot shows the AWS Lambda Functions page. The function 'periodicttrigger' is listed with a single trigger from 'EventBridge (CloudWatch Events)'. The 'Code source' tab is active, showing the function code and deployment status.

The screenshot shows the AWS Lambda code editor interface. At the top, there's a navigation bar with 'Services' (selected), 'Search', and tabs like 'Code', 'Test', 'Monitor', 'Configuration', 'Aliases', and 'Versions'. Below the navigation is a toolbar with 'File', 'Edit', 'Find', 'View', 'Go', 'Tools', 'Window', 'Test' (selected), 'Deploy', and 'Upload from'. A search bar says 'Go to Anything (⌘ P)'. The main area has tabs for 'Code source' (selected) and 'Info'. Under 'Code source', there's a file tree with 'periodictrigger' and 'lambda\_function.py'. The code in 'lambda\_function.py' is:

```

1 import logging
2 def lambda_handler(event, context):
3     logging.info("Lambda Function invoked")
4     return {"statusCode": 200, "body": "Hello From Lambda"}
5

```

Below the code editor is a status bar with '1:1 Python Spaces: 4'. To the right, there's a sidebar titled 'Create a simple web app' with a 'Start tutorial' button. At the bottom, there's a 'Code properties' tab and a footer with 'CloudShell', 'Feedback', and copyright information.

The second part of the screenshot shows the results of a test execution. It has tabs for 'Code source' (selected) and 'Info'. The 'Info' tab shows an 'Execution result' with a status of 'Succeeded', max memory used of 35 MB, and a time of 1.37 ms. The results pane displays the test event name 'Testevent', the response object, and function logs. The logs show the start, end, and report requests with their respective IDs and durations.

## AWS CloudWatch Configuration

### CloudWatch Alarms

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

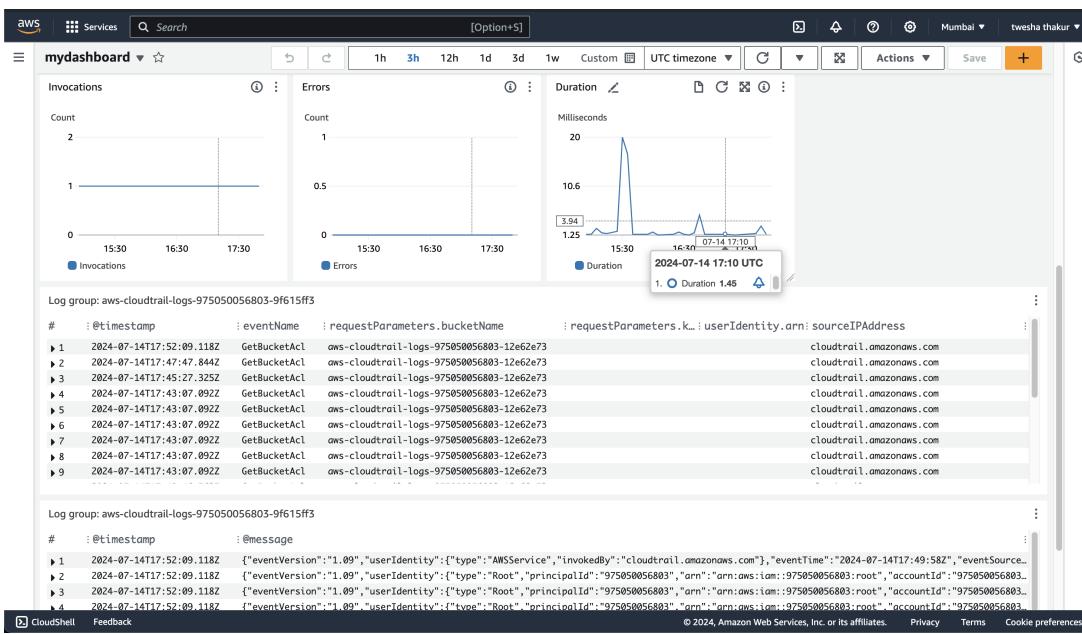
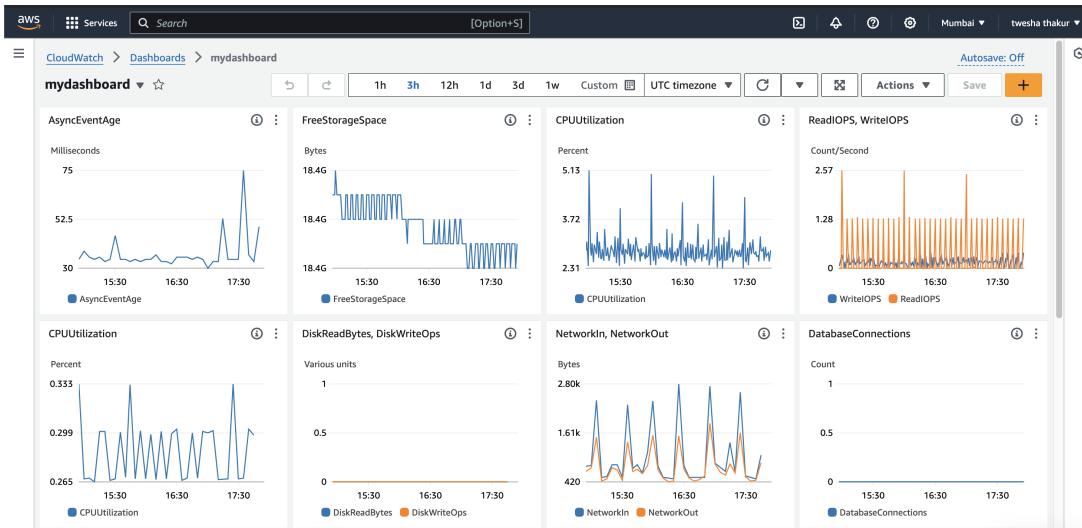
The screenshot shows the AWS CloudWatch Overview page. On the left, there's a navigation sidebar with sections like CloudWatch, Favorites and recent, Dashboards, Alarms, Logs, Metrics, X-Ray traces, Events, and Application Signals. The main area has tabs for Overview, Alarms by AWS service, Recent alarms, and Default Dashboard. Under Alarms by AWS service, it lists RDS, RDS Cluster, EC2, and Lambda. Under Recent alarms, two are shown: 'Uh-Oh! running out of storage soon!' and 'CPU util > than threshold'. The Default Dashboard section is empty.

The screenshot shows the AWS CloudWatch Alarms page. It displays a table of three alarms:

Name	State	Last state update (UTC)	Conditions	Actions
Uh-Oh! running out of storage soon!	OK	2024-07-14 05:27:23	FreeStorageSpace <= 2000000000 for 1 datapoints within 1 minute	Actions enabled
CPU util > than threshold	OK	2024-07-14 05:19:50	CPUUtilization >= 1000 for 1 datapoints within 5 minutes	Actions enabled
Yellowalert	OK	2024-07-12 10:08:20	AsyncEventAge >= 500 for 1 datapoints within 5 minutes	Actions enabled

## 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.

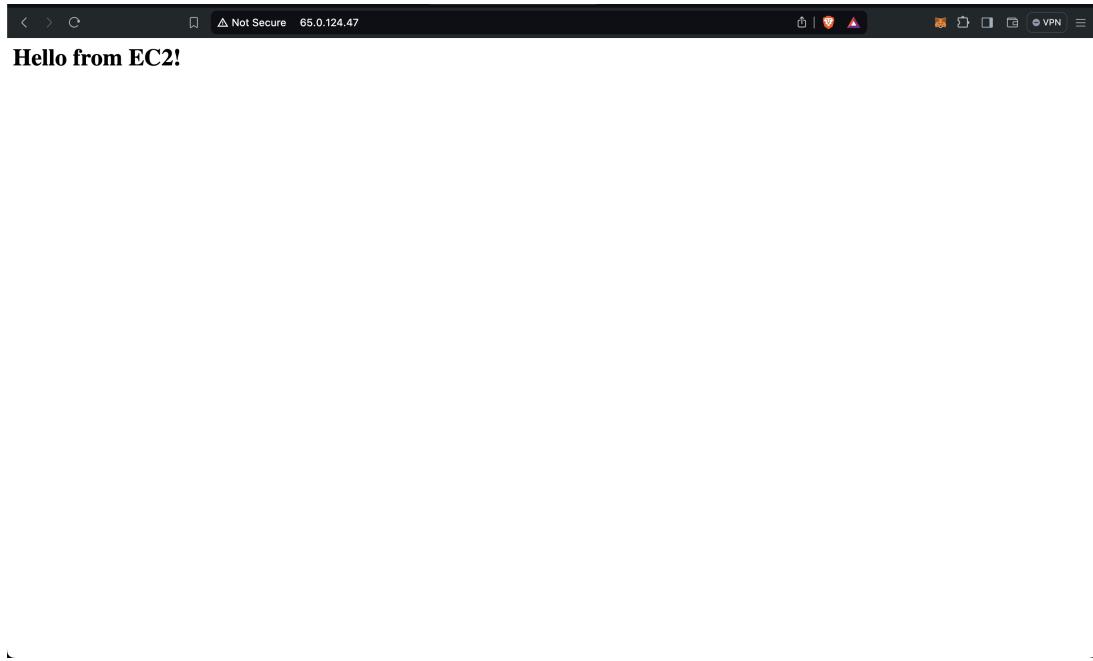
### Configuring Data Events

- 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 periodicttrigger 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**

Select log groups, and then run a query or [choose a sample query](#).

Select up to 50 log groups.

aws-cloudtrail-logs-975050056803-9f615ff3 X Clear all

```
1 fields @timestamp, @message
2 | sort @timestamp desc
3 | limit 20
4
```

Run query Cancel Save Actions History

Logs Insights query can run for maximum of 60 minutes.

Complete

Logs (20) Patterns (8) Visualization

Logs (20)

Showing 20 of 268 records matched ⓘ  
268 records (285.8 kB) scanned in 2.4s @ 113 records/s (121.2 kB/s)

Hide histogram

# @timestamp @message

© 2024, Amazon Web Services, Inc. or its affiliates. Privacy Terms

Logs Insights Info

Select log groups, and then run a query or [choose a sample query](#).

Select up to 50 log groups.

aws-cloudtrail-logs-975050056803-9f615ff3 X Clear all

```
1 fields @timestamp, eventName, userIdentity.type, userIdentity.arn, sourceIPAddress
2 | filter eventName = "ConsoleLogin"
3 | sort @timestamp desc
4 | 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)

Showing 1 of 1 records matched ⓘ  
268 records (285.8 kB) scanned in 1.8s @ 145 records/s (155.2 kB/s)

Hide histogram

# @timestamp eventName userIden... userIdentity.arn sourceIPAddress

2024-07-14T22:22:00Z ConsoleLogin Root 075050056803-9f615ff3 222.167.105.120

CloudWatch > Logs Insights > bucket identity access

**Logs Insights Info**

Select log groups, and then run a query or [choose a sample query](#).

aws-cloudtrail-logs-975050056803-9f615ff3 X Clear all

```

1   fields @timestamp, eventName, requestParameters.bucketName, requestParameters.key, userIdentity.arn, sourceIPAddress
2   | filter eventSource = "s3.amazonaws.com"
3   | sort @timestamp desc
4   | limit 20

```

Run query Cancel Save Actions History

Logs Insights query can run for maximum of 60 minutes.

Complete

Logs (20) Patterns (-) Visualization

Logs (20)

Showing 20 of 34 records matched ⓘ  
268 records (285.8 kB) scanned in 1.6s @ 172 records/s (184.4 kB/s)

Hide histogram

#	@timestamp	eventName	requestParameters.bucketName	requestP...	userIdent...	sourceIPAddres...
1	2021-07-14T10:30:00.000Z	PutObject	my-trail-test-bucket	my-trail-test-bucket	arn:aws:iam::123456789012:root	123.45.67.89
2	2021-07-14T10:35:00.000Z	PutObject	my-trail-test-bucket	my-trail-test-bucket	arn:aws:iam::123456789012:root	123.45.67.89
3	2021-07-14T10:40:00.000Z	PutObject	my-trail-test-bucket	my-trail-test-bucket	arn:aws:iam::123456789012:root	123.45.67.89
4	2021-07-14T10:45:00.000Z	PutObject	my-trail-test-bucket	my-trail-test-bucket	arn:aws:iam::123456789012:root	123.45.67.89
5	2021-07-14T10:50:00.000Z	PutObject	my-trail-test-bucket	my-trail-test-bucket	arn:aws:iam::123456789012:root	123.45.67.89
6	2021-07-14T10:55:00.000Z	PutObject	my-trail-test-bucket	my-trail-test-bucket	arn:aws:iam::123456789012:root	123.45.67.89
7	2021-07-14T11:00:00.000Z	PutObject	my-trail-test-bucket	my-trail-test-bucket	arn:aws:iam::123456789012:root	123.45.67.89
8	2021-07-14T11:05:00.000Z	PutObject	my-trail-test-bucket	my-trail-test-bucket	arn:aws:iam::123456789012:root	123.45.67.89
9	2021-07-14T11:10:00.000Z	PutObject	my-trail-test-bucket	my-trail-test-bucket	arn:aws:iam::123456789012:root	123.45.67.89
10	2021-07-14T11:15:00.000Z	PutObject	my-trail-test-bucket	my-trail-test-bucket	arn:aws:iam::123456789012:root	123.45.67.89
11	2021-07-14T11:20:00.000Z	PutObject	my-trail-test-bucket	my-trail-test-bucket	arn:aws:iam::123456789012:root	123.45.67.89
12	2021-07-14T11:25:00.000Z	PutObject	my-trail-test-bucket	my-trail-test-bucket	arn:aws:iam::123456789012:root	123.45.67.89

## 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

**General details**

Trail logging	Trail log location	Log file validation	SNS notification delivery
Logging	aws-cloudtrail-logs-975050056803-12e62e73/AWSLogs/975050056803/	Enabled	arnaws:sns:ap-south-1:975050056803:aws-cloudtrail-logs-975050056803-a05d6816
Trail name	mytrail	Last file validation delivered	Last SNS notification
Multi-region trail	Yes	July 14, 2024, 23:09:00 (UTC+05:30)	July 14, 2024, 23:56:13 (UTC+05:30)
Apply trail to my organization	Not enabled	Log file SSE-KMS encryption	
		Not enabled	

**CloudWatch Logs**

Log group	IAM Role
aws-cloudtrail-logs-975050056803-9f615ff3	arn:aws:iam::975050056803:role/service-role/Trail_log_sendtowatch_mytrail

**Tags**

Key	Value

**Buckets**

- Access Grants
- Access Points
- Object Lambda Access Points
- Multi-Region Access Points
- Batch Operations
- IAM Access Analyzer for S3

**Storage Lens**

- Dashboards
- Storage Lens groups
- AWS Organizations settings

**Objects (3) Info**

Name	Type	Last modified	Size	Storage class
CloudTrail-Digest/	Folder	-	-	-
CloudTrail-Insight/	Folder	-	-	-
CloudTrail/	Folder	-	-	-

The screenshot shows the AWS S3 console with a green header bar indicating "Successfully deleted bucket 'mybucket66'". Below the header, there's a summary section with an "Account snapshot" update every 24 hours and a "View Storage Lens dashboard" button. The main area displays two general purpose buckets: "aws-cloudtrail-logs-975050056803-12e62e73" and "aws-cloudtrail-logs-975050056803-a2d1b034", both created on July 12, 2024.

Name	AWS Region	IAM Access Analyzer	Creation date
aws-cloudtrail-logs-975050056803-12e62e73	Asia Pacific (Mumbai) ap-south-1	<a href="#">View analyzer for ap-south-1</a>	July 12, 2024, 14:56:59 (UTC+05:30)
aws-cloudtrail-logs-975050056803-a2d1b034	Asia Pacific (Mumbai) ap-south-1	<a href="#">View analyzer for ap-south-1</a>	July 12, 2024, 02:15:44 (UTC+05:30)

The screenshot shows the AWS S3 console navigating to the "aws-cloudtrail-logs-975050056803-12e62e73" bucket. It then drills down into the "AWSLogs/" folder, specifically the "975050056803/" subfolder. The "Objects" tab is selected, displaying three objects: "CloudTrail-Digest/", "CloudTrail-Insight/", and "CloudTrail/". All three objects are folders.

Name	Type	Last modified	Size	Storage class
CloudTrail-Digest/	Folder	-	-	-
CloudTrail-Insight/	Folder	-	-	-
CloudTrail/	Folder	-	-	-

## SNS

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

The screenshot shows the AWS SNS console. On the left, the navigation menu includes 'Dashboard', 'Topics', 'Subscriptions' (selected), and 'Mobile' sections. The main content area displays a 'Subscription' details page for a specific topic. The subscription ARN is listed as `arn:aws:sns:ap-south-1:975050056803:aws-cloudtrail-logs-975050056803-a05d6816`. The status is 'Confirmed'. The endpoint is '+918278874929'. The topic is 'aws-cloudtrail-logs-975050056803-a05d6816'. The subscription principal is 'arn:aws:iam::975050056803:root'. A 'New Feature' banner at the top indicates support for in-place message archiving and replay for FIFO topics.

The screenshot shows the AWS SNS console. The left navigation menu includes 'Dashboard', 'Topics', 'Subscriptions' (selected), and 'Text messaging (SMS)' (selected). The main content area displays 'Delivery statistics (UTC)'. It shows a chart for promotional text message delivery rate (1.48%) and a bar chart for transactional text messages sent (300+). Below this, there are two tables for 'Delivery statistics by country': one for India (474 Sent, 467 Failed, 1.48% Delivery rate) and another for a single entry (1 Sent, 0 Failed, 100% Delivery rate).

## 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](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](https://docs.aws.amazon.com/IAM/latest/UserGuide/id_roles.html)
- IAM Policies: [https://docs.aws.amazon.com/IAM/latest/UserGuide/access\\_policies.html](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>