

Real-Time Object Addition Alert System for Amazon S3 using CloudTrail, CloudWatch, and SNS

Project Overview :

This project implements a real-time monitoring and alerting mechanism for Amazon S3. Whenever a new object is added to a specific S3 bucket, the event is captured using AWS CloudTrail, analyzed through Amazon CloudWatch Logs and Metric Filters, and an alert notification is sent via Amazon SNS to subscribed users (email/SMS).

The solution improves visibility, security monitoring, and operational awareness of S3 bucket activities.

Goals :

- ❖ Monitor object creation events in an Amazon S3 bucket
- ❖ Capture S3 API activity logs using AWS CloudTrail
- ❖ Create CloudWatch Metric Filters for object upload events
- ❖ Trigger alerts using CloudWatch Alarms
- ❖ Send real-time notifications via Amazon SNS
- ❖ Demonstrate event-driven monitoring in AWS

AWS Services Used :

Amazon S3 – Storage service where object addition is monitored

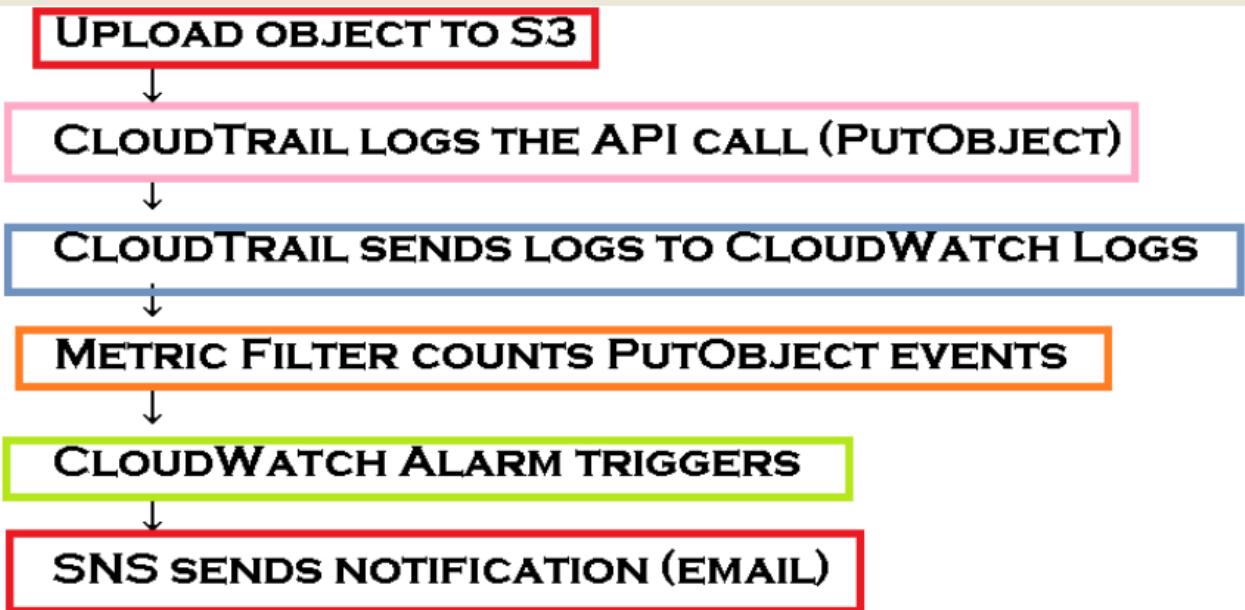
AWS CloudTrail – Captures S3 API calls and delivers logs

Amazon CloudWatch Logs – Stores and analyzes CloudTrail logs

CloudWatch Metric Filters & Alarms – Detects object creation events

Amazon SNS – Sends alert notifications to subscribers

Architecture :



Steps Followed :

1. Create an Amazon SNS Topic for publishing Notifications
 - a.Amazon SNS console -->(navigation pane)-->Topics --> Create topic.
Enter a name for topic (e.g., S3-Object-Addition-Alerts)--> Create topic.
 - b.On the new topic's details page, choose Create subscription.
For Protocol: Email.
For Endpoint: enter the email address --> Create subscription.
Check the email specified above and confirm the subscription by clicking the link in the message from AWS Notifications.

The screenshot shows the AWS SNS console. In the left sidebar, under 'Subscriptions', there is a link to 'S3-Object-addition-alarm'. The main content area displays a subscription named 'Subscription: 5dd3efcf-6009-423f-9ad4-6877cec840a5'. The 'Details' section includes fields for ARN (arn:aws:sns:eu-north-1:682729124949:S3-Object-addition-alarm:5dd3efcf-6009-423f-9ad4-6877cec840a5), Endpoint (preethi232001@gmail.com), Topic (S3-Object-addition-alarm), and Subscription Principal (arn:aws:iam::682729124949:root). The status is 'Confirmed'. Below this, tabs for 'Subscription filter policy' and 'Redrive policy (dead-letter queue)' are visible. The bottom navigation bar includes links for CloudShell, Feedback, and Console Mobile App.

2. Create a S3 bucket to add objects and test the scenario.

The screenshot shows the AWS S3 console. A green banner at the top indicates 'Successfully created bucket "my-bucket-for-monitoring-object-additon"'. The main area displays a table for 'General purpose buckets (1)'. The single entry is 'my-bucket-for-monitoring-object-additon' located in 'Europe (Stockholm) eu-north-1' with a creation date of 'December 16, 2025, 22:40:42 (UTC+05:30)'. Action buttons for 'Copy ARN', 'Empty', 'Delete', and 'Create bucket' are available. To the right, sections for 'Account snapshot' (updated daily) and 'External access summary - new' (updated daily) are shown. The bottom navigation bar includes links for CloudShell, Feedback, and Console Mobile App.

3. Create a CloudTrail Trail to Log S3 Events

You need to log "PutObject" events (object additions) in your S3 bucket using CloudTrail.

AWS CloudTrail console-->(navigation pane) --> Trails -->Create trail (or use an existing one). Enter a name for the trail (e.g., s3-object-creation-trail).

For Storage location, use a new or existing S3 bucket to store the logs.

For Log events, choose Data events.

Under Data event sources, select S3.

Choose the specific S3 bucket that has to be monitored.

For Event type, select at least Write events, specifically the PutObject operation.

Ensure CloudWatch Logs is enabled and specify a new or existing log group (e.g., /aws/cloudtrail/s3-object-events).

Choose Next--> Create trail.

The screenshot shows the AWS CloudTrail console with the following details:

General details

Trail Logging Logging	Trail log location aws-cloudtrail-logs-682729124949-bff00c15/AWSLogs/682729124949	Log file validation Disabled	SNS notification delivery Disabled
Trail name S3-Object-addition-logging-using-trail	Last log file delivered December 16, 2025, 22:50:27 (UTC+05:30)	Last file validation delivered -	Last SNS notification -
Multi-region trail Yes	Log file SSE-KMS encryption Not enabled		
Apply trail to my organization Not enabled			

CloudWatch Logs

Log group my-aws-cloudtrail-logs-682729124949-b0df9520	IAM Role arn:aws:iam::682729124949:role/service-role/trail-logs
--	---

At the bottom, there is a Windows taskbar with various icons and a search bar.

4. Create a CloudWatch Metric Filter to count the PutObject events.

Amazon CloudWatch console-->(navigation pane)--> Logs-->Log groups or Log Management
Select the log group that was specified in the previous step (e.g., /aws/cloudtrail/s3-object-events).
Choose Actions-->Create metric filter.

For Filter pattern, enter the following pattern to match PutObject events for the specific bucket:

```
{ ($.eventSource = "s3.amazonaws.com") && ($.eventName = "PutObject") &&  
($.requestParameters.bucketName = "YOUR_BUCKET_NAME") }
```

(Replace YOUR_BUCKET_NAME with the actual bucket name)--> Next.

Enter a Metric namespace (e.g., MyS3Metrics)

Metric name (e.g., ObjectCreationCount).

For Metric value, enter 1 (each matching log event increments the metric by 1).

Choose Create metric filter.

AWS CloudWatch Log management my-aws-cloudtrail-logs-682729124949-b0df9520

Metric filter "my-s3-metrics" has been created.

my-aws-cloudtrail-logs-682729124949-b0df9520

[Actions](#) [View in Logs Insights](#) [Start tailing](#) [Search log group](#)

Log group details

Log class Info	Metric filters 1	Data protection
Standard	Subscription filters 0	Sensitive data count
ARN arn:aws:logs:eu-north-1:682729124949:log-group:my-aws-cloudtrail-logs-682729124949-b0df9520*	Contributor Insights rules -	Custom field indexes Configure
Creation time 8 minutes ago	KMS key ID -	Transformer Configure
Retention Never expire	Deletion protection <input checked="" type="radio"/> Off	Anomaly detection Configure
Stored bytes -		

CloudShell Feedback Console Mobile App © 2025, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

Type here to search                         

23:02 ENG 16-12-2025

CloudWatch Log management my-aws-cloudtrail-logs-682729124949-b0df9520

[Log streams](#) [Tags](#) [Anomaly detection](#) [Metric filters](#) [Subscription filters](#) [Contributor Insights](#) [Data protection](#) [Field indexes](#)

Metric filters (1)

[Edit](#) [Delete](#) [Create alarm](#) [Create metric filter](#)

Find metric filters

my-s3-metrics

Filter pattern
`{ ($.eventSource = "s3.amazonaws.com") && ($.eventName = "PutObject") && ($.requestParameters.bucketName = "my-bucket-for-monitoring-object-additon") }`

Field selection criteria

Metric [my-s3-bucket-metrics](#) / [metrics-to-count-objects-added-to-the-bucket](#)

Metric value 1

AWS CloudWatch Log management my-aws-cloudtrail-logs-682729124949-b0df9520

Metric [my-s3-bucket-metrics](#) / [metrics-to-count-objects-added-to-the-bucket](#)

Metric value 1

Default value

Applied on transformed logs

Unit

Emit system field dimensions

Dimensions

Alarms None.

5. Create the CloudWatch Alarm that triggers when the count from the metric filter exceeds a certain threshold

CloudWatch-->Select the custom metric you just created (e.g., MyS3Metrics > ObjectCreationCount). For Metric name, select the metric you created.

Choose a 1-minute period and the Sum statistic.s

In the Conditions section, set the Threshold type to Static.

Define the condition: select Greater than or equal to and enter 1 as the threshold value. This will trigger the alarm if one or more objects are added in a 1-minute period.

Choose Next.

In the Configure actions section, ensure the Alarm state is In ALARM.

For Select an SNS topic, choose the SNS topic that was created in Step 1 (e.g., S3ObjectAdditionAlerts).

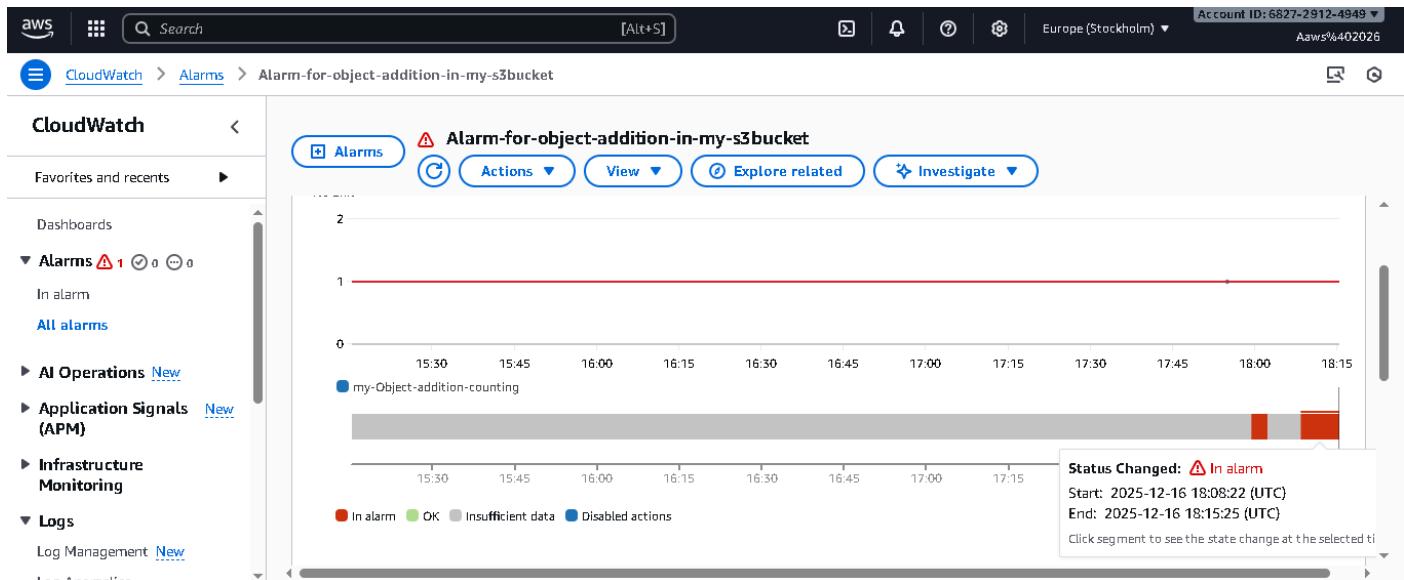
Choose Next, provide an Alarm name and description, and complete the process by choosing Create alarm.

The screenshot shows the AWS CloudWatch Alarms interface. At the top, there's a green success message: "Successfully created alarm Alarm-for-object-addition-in-my-s3bucket." Below it, the "Alarms (1)" list is displayed. The single alarm entry is for "Alarm-for-object-addition-in-my-s3bucket". It shows the state as "Insufficient data" (last updated 2025-12-16 17:59:07), the condition as "my-Object-addition-counting >= 1 for 1 datapoints within 1 minute", and the status as "Actions enabled". There are buttons for "View alarm", "Create alarm", and other actions.

6.Add objects in the created S3 bucket

The screenshot shows the AWS Amazon S3 Buckets interface. The bucket "my-bucket-for-monitoring-object-additon" is selected. The "Objects" tab is active, showing three files: "linux.png", "Screenshot (1).png", and "Screenshot (2).png". Each file has its name, type (png), last modified date (December 16, 2025), size (417.1 KB, 93.9 KB, 93.8 KB), and storage class (Standard). There are buttons for "Actions", "Create folder", and "Upload". A note at the bottom says "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](#)".

7. Alarm and Cloudwatch graph monitoring after the threshold value exceeded



8. Alert message sent by SNS to the subscribers

The screenshot shows a Gmail inbox with two new messages. The first message is from 'S3 Object addition alarm' and the second is from 'no-reply@sns.amazonaws.com'. Both messages are notifications about an alarm state change. The first message contains a link to view the alarm in the AWS Management Console. The second message provides more details about the alarm configuration and the event that triggered it.

This screenshot shows a detailed view of an SNS alert email in a Gmail inbox. The email is from 'no-reply@sns.amazonaws.com' and contains information about an alarm named 'Alarm-for-object-addition-in-my-s3bucket'. It includes a link to the AWS Management Console, a description of the alarm details, and a note about an object being added to an S3 bucket. The email also includes a timestamp for the event.

Use Cases :

- Security monitoring for sensitive S3 buckets
- Compliance and audit logging
- Data upload tracking in production environments
- Early detection of unauthorized access

Conclusion :

This project demonstrates an effective and scalable approach to monitoring Amazon S3 object uploads using native AWS services. By integrating CloudTrail, CloudWatch, and SNS, the system provides real-time alerts, enhancing security, compliance, and operational efficiency in cloud environments.