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

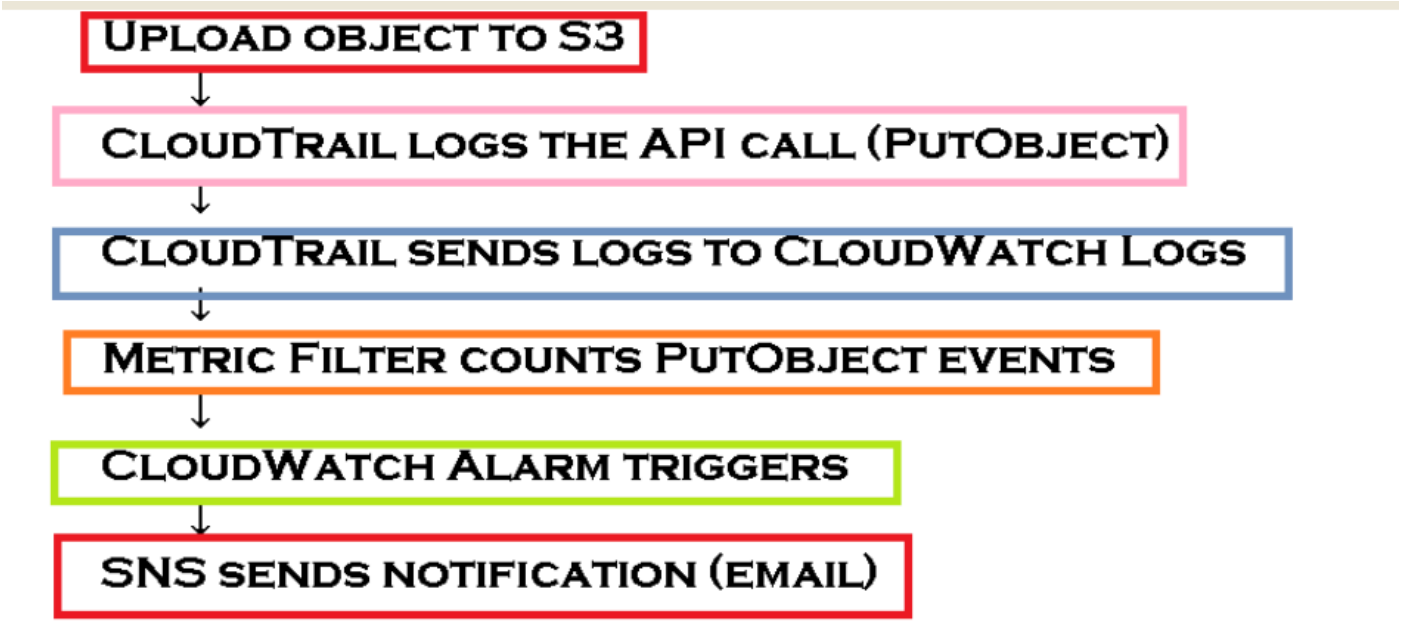
AWS CloudTrail – Captures S3 API calls and delivers logs

Amazon CloudWatch Logs – Stores and analyzes CloudTrail logs

CloudWatch Metric Filters & Alarms – Detects object creation events

Amazon SNS – Sends alert notifications to subscribers

Architecture :

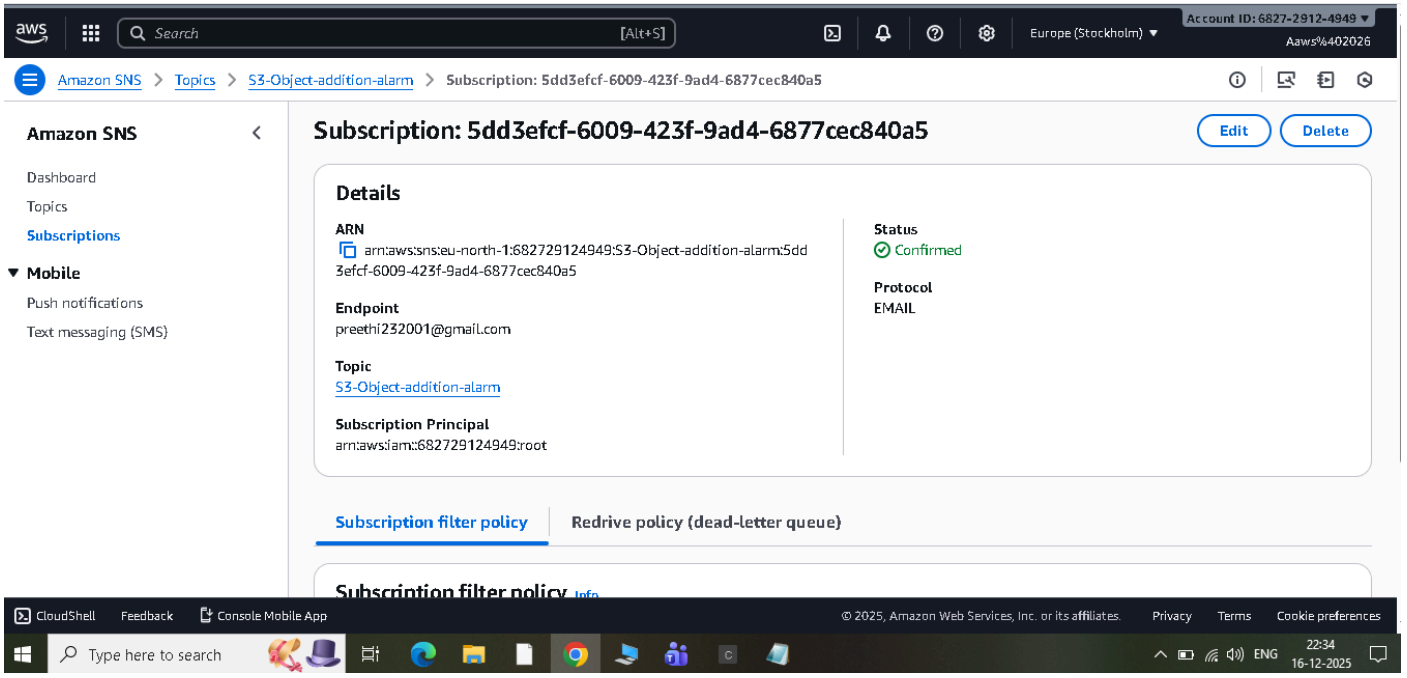


Steps Followed :

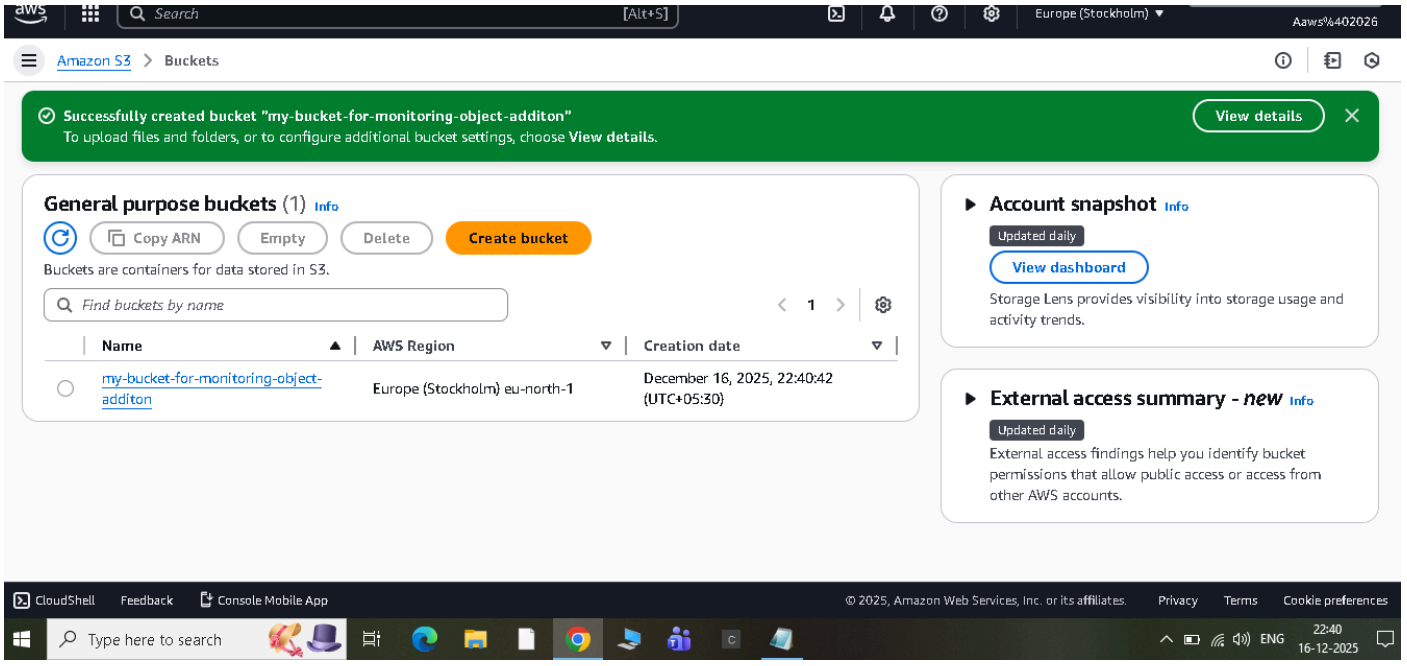
1. Create an Amazon SNS Topic for publishing Notifications

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.



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



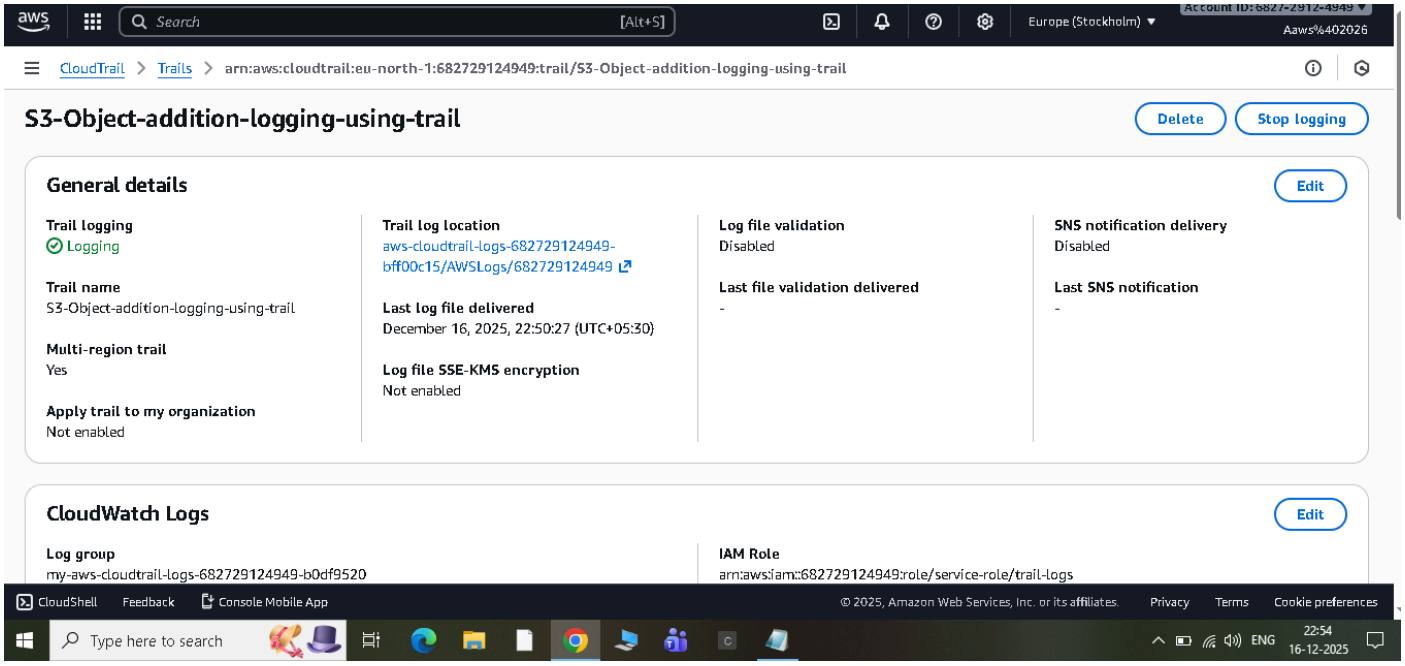
3. Create a CloudTrail Trail to Log S3 Events

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.

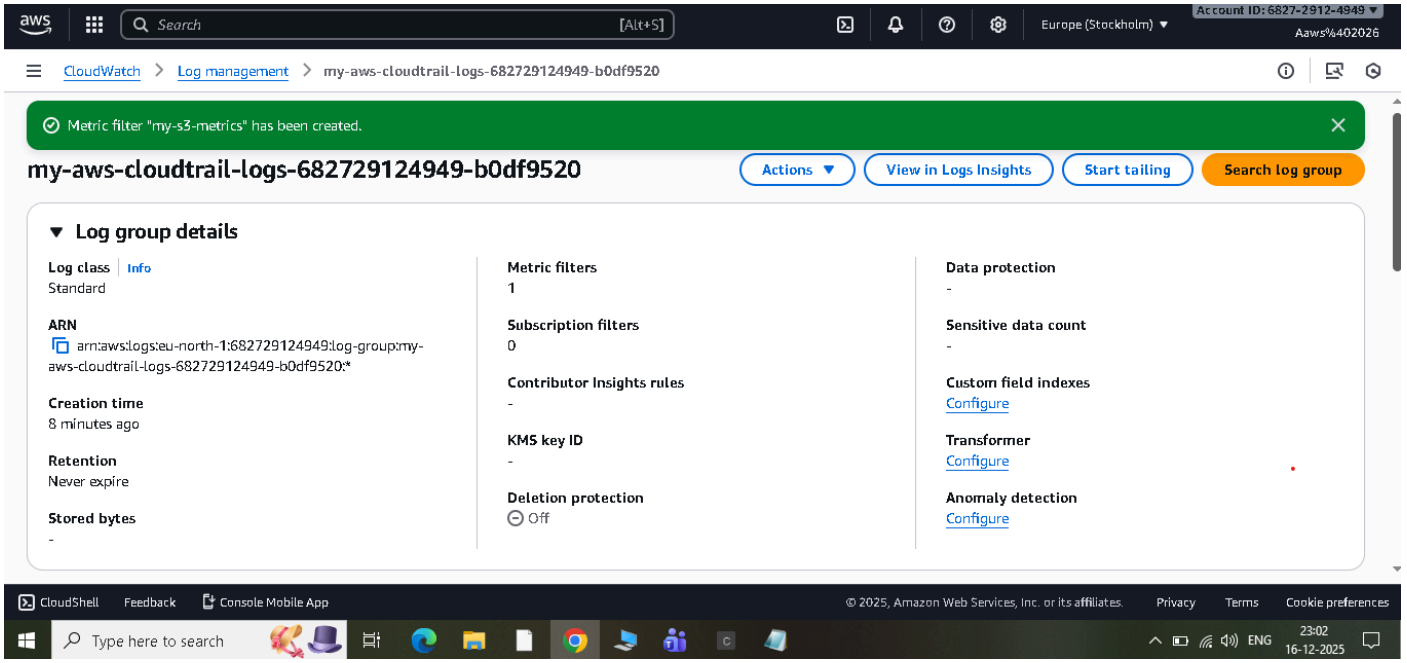


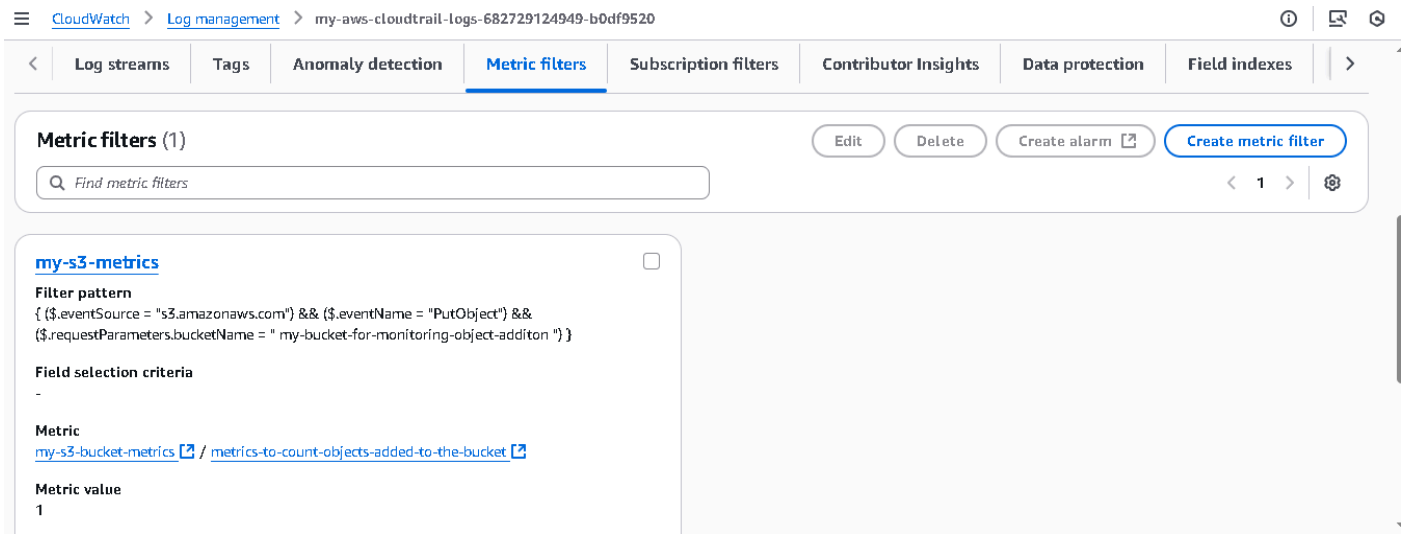
4. Create a CloudWatch Metric Filter to count the PutObject events.

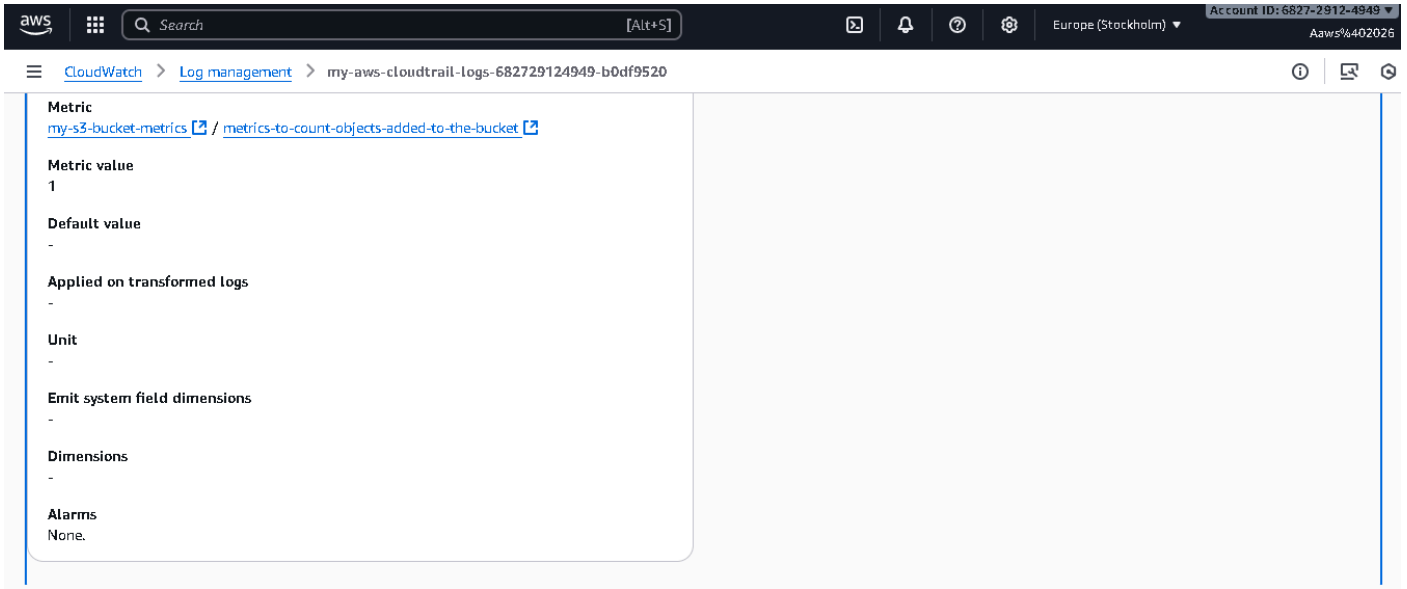
Amazon CloudWatch console-->(navigation pane)--> Logs-->Log groups or Log Management
Select the log group that was specified in the previous step (e.g., /aws/cloudtrail/s3-object-events).
Choose Actions-->Create metric filter.

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.


Search [Alt+S]
Europe (Stockholm)
Account ID: 6827-2912-4949
Aaws%402026
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
Standard
ARN
arn:aws:logs:eu-north-1:682729124949:log-group:my-aws-cloudtrail-logs-682729124949-b0df9520:*
Creation time
8 minutes ago
Retention
Never expire
Stored bytes
-
Metric filters
1
Subscription filters
0
Contributor Insights rules
-
KMS key ID
-
Deletion protection
Off
Data protection
-
Sensitive data count
-
Custom field indexes
Configure
Transformer
Configure
Anomaly detection
Configure
CloudShell
Feedback
Console Mobile App
© 2025, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences
Type here to search
ENG
23:02
16-12-2025

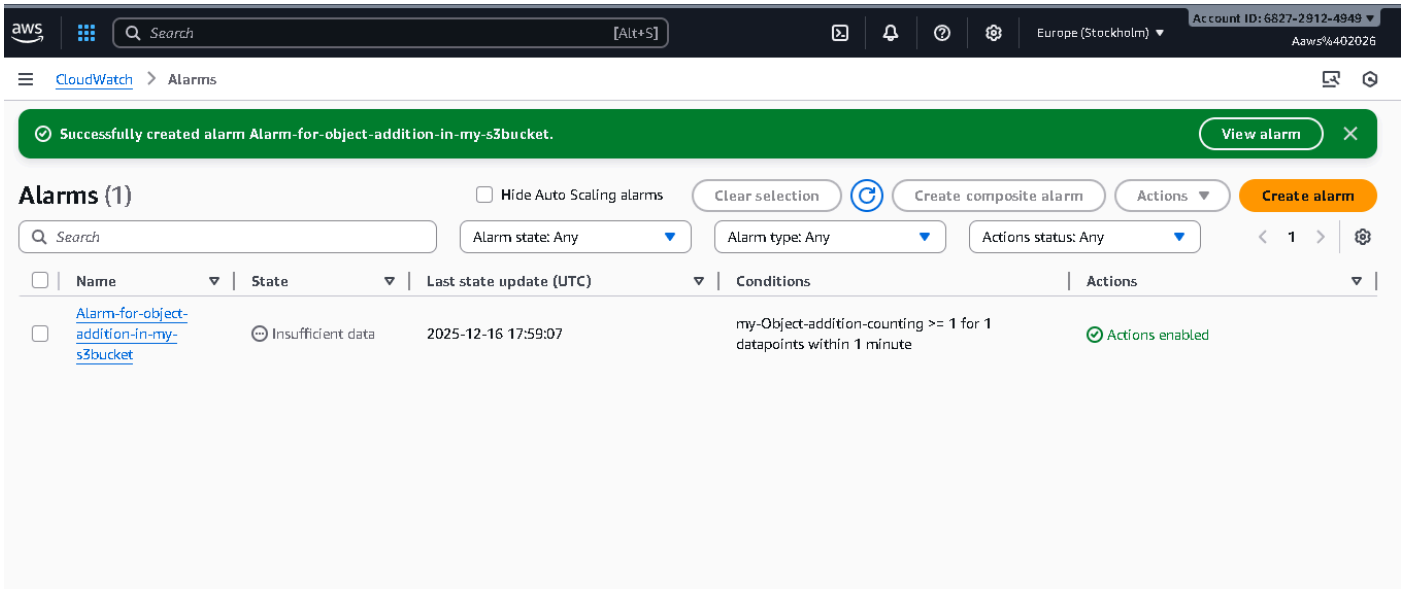

CloudWatch > Log management > my-aws-cloudtrail-logs-682729124949-b0df9520
Log streams
Tags
Anomaly detection
Metric filters
Subscription filters
Contributor Insights
Data protection
Field indexes
Metric filters (1)
Edit
Delete
Create alarm
Create metric filter
Find metric filters
1
my-s3-metrics
Filter 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


Search [Alt+S]
Europe (Stockholm)
Account ID: 6827-2912-4949
Aaws%402026
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.

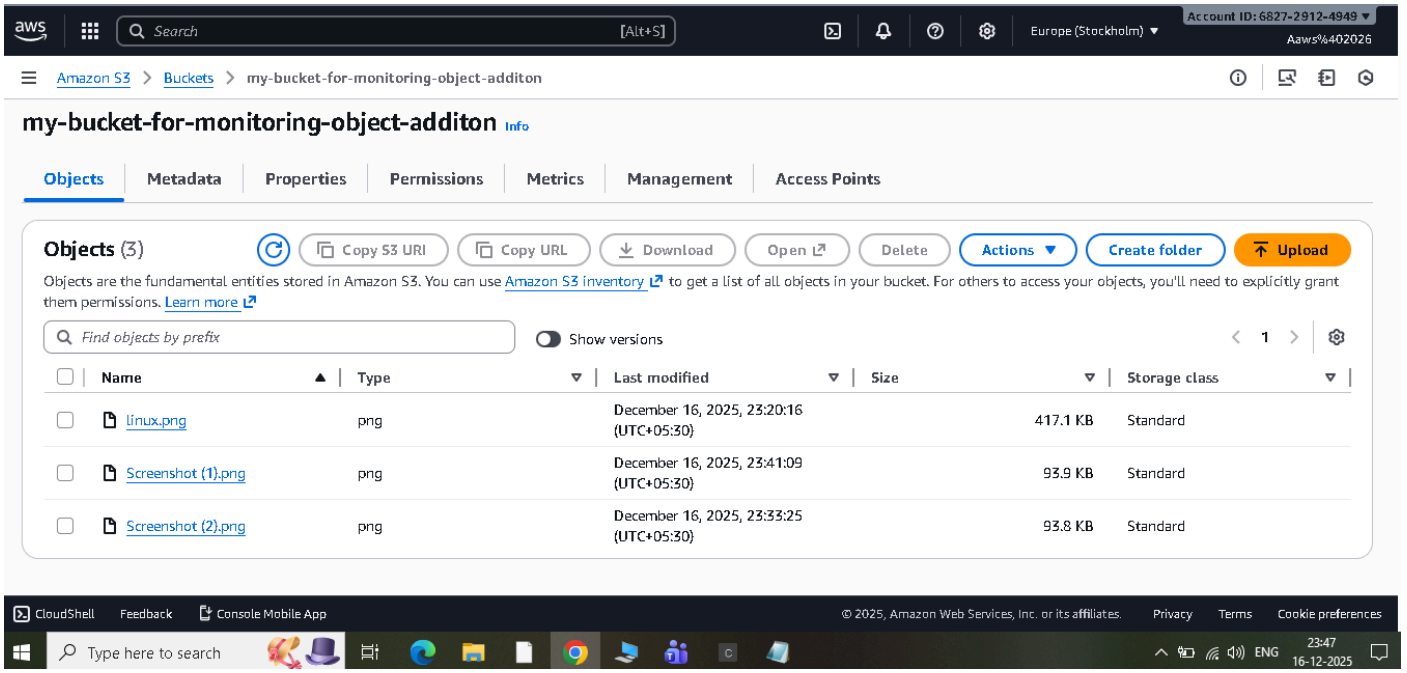
5. Create the CloudWatch Alarm that triggers when the count from the metric filter exceeds a certain threshold

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.

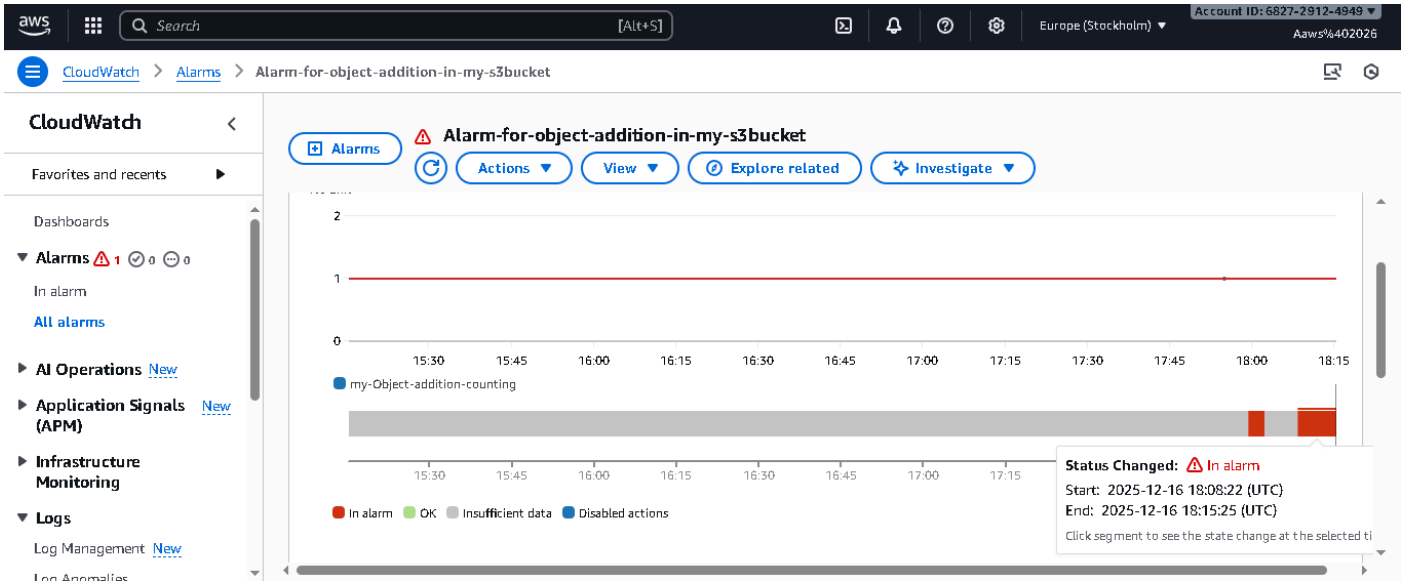
In the Configure actions section, ensure the Alarm state is In ALARM.
For Select an SNS topic, choose the SNS topic that was created in Step 1 (e.g., S3ObjectAdditionAlerts).
Choose Next, provide an Alarm name and description, and complete the process by choosing Create alarm.



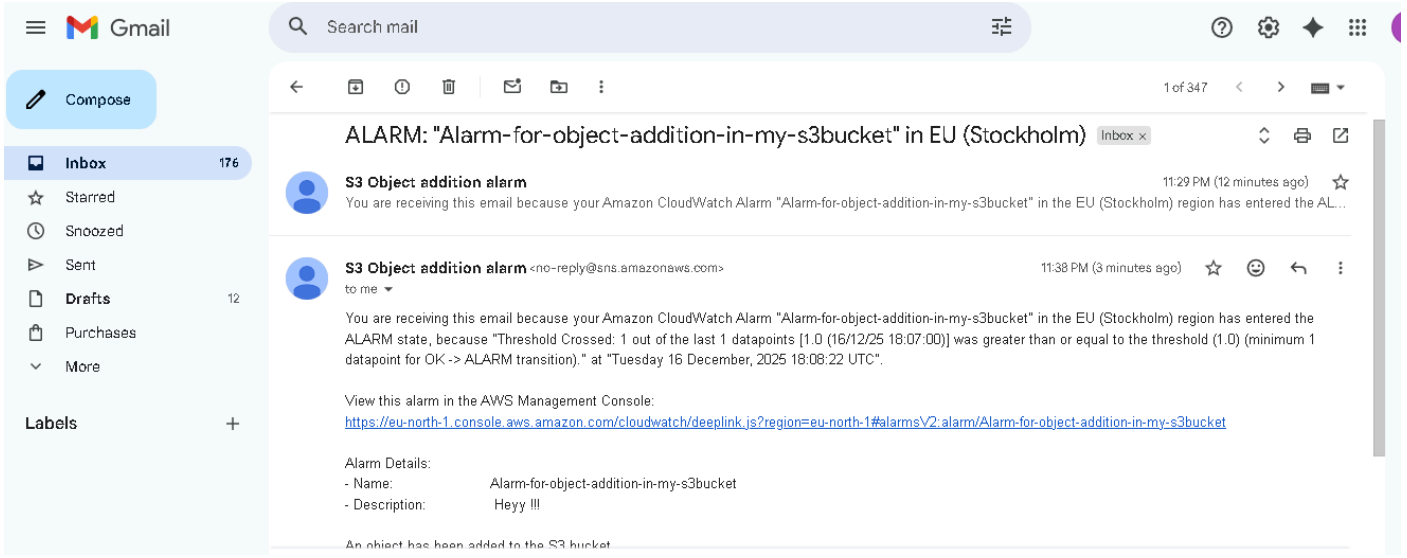
6.Add objects in the created S3 bucket

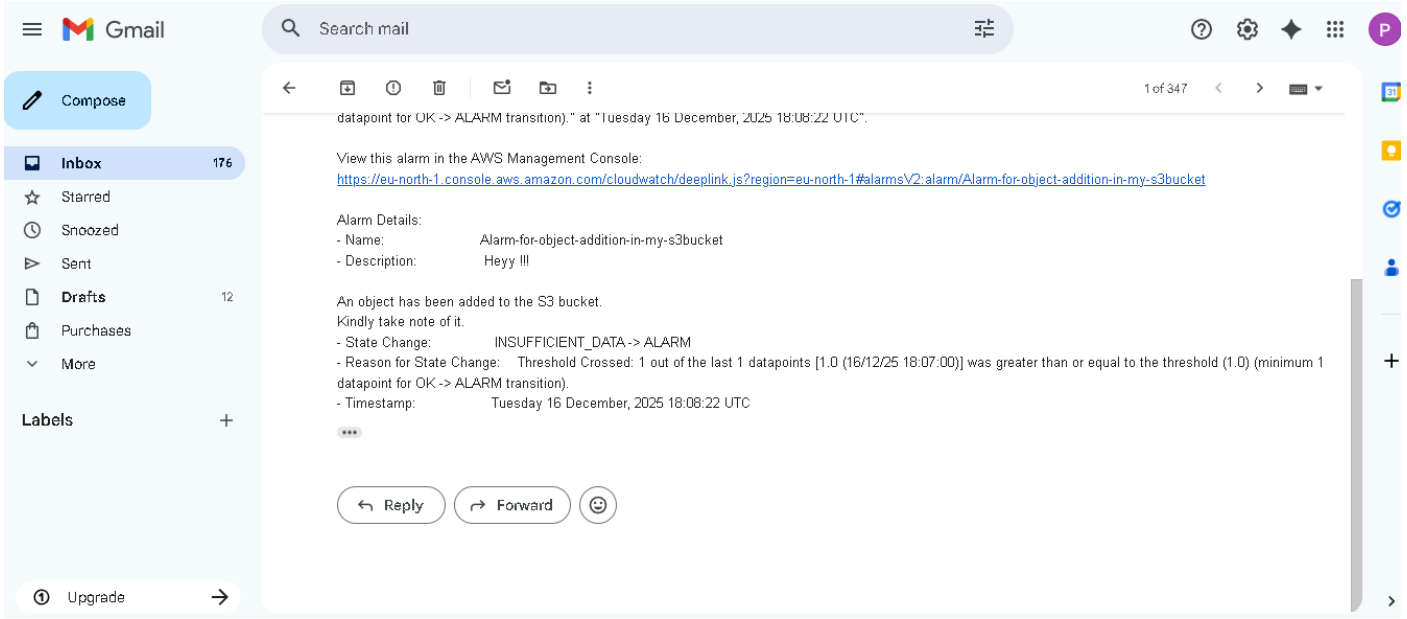


7.Alarm and Cloudwatch graph monitoring after the threshold value exceeded



8.Alert message sent by SNS to the subscribers





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.