CloudTrail & CloudWatch Monitoring Project

AWS Cloud Security Series – Project 6

by:

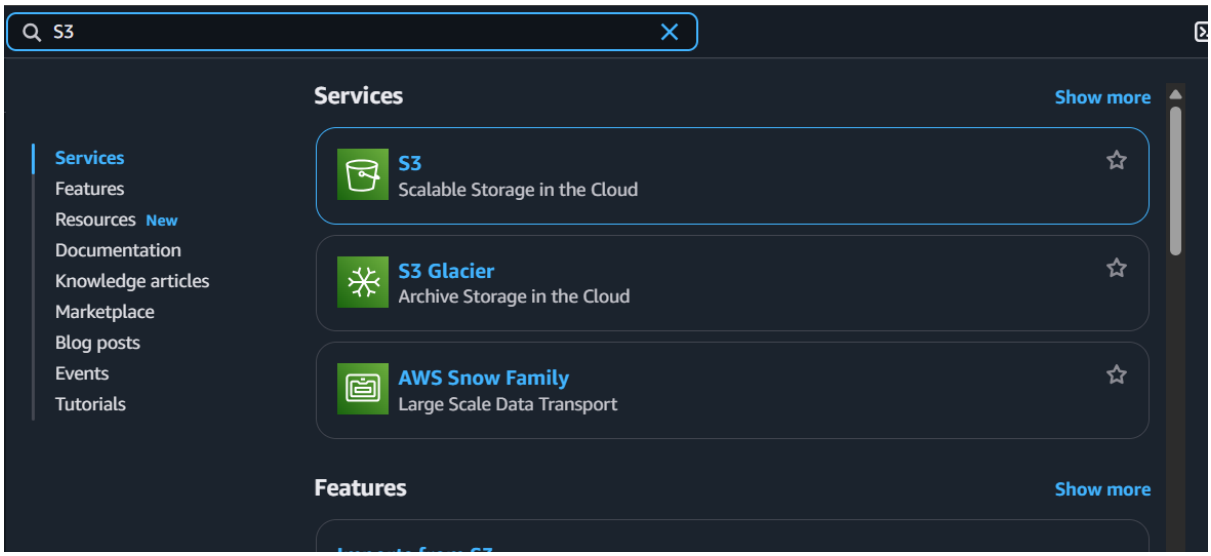
Syeda Umaima Abeer

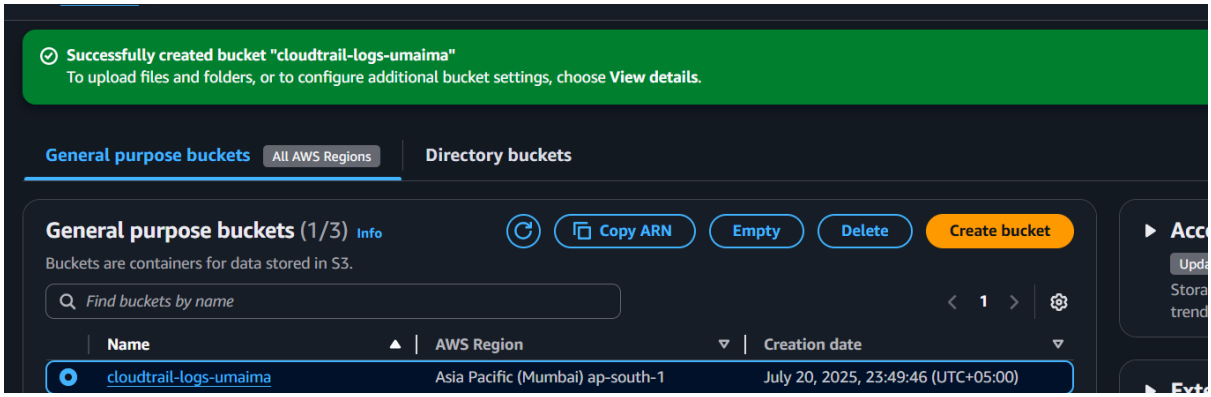
Cloud Security Student

Date:

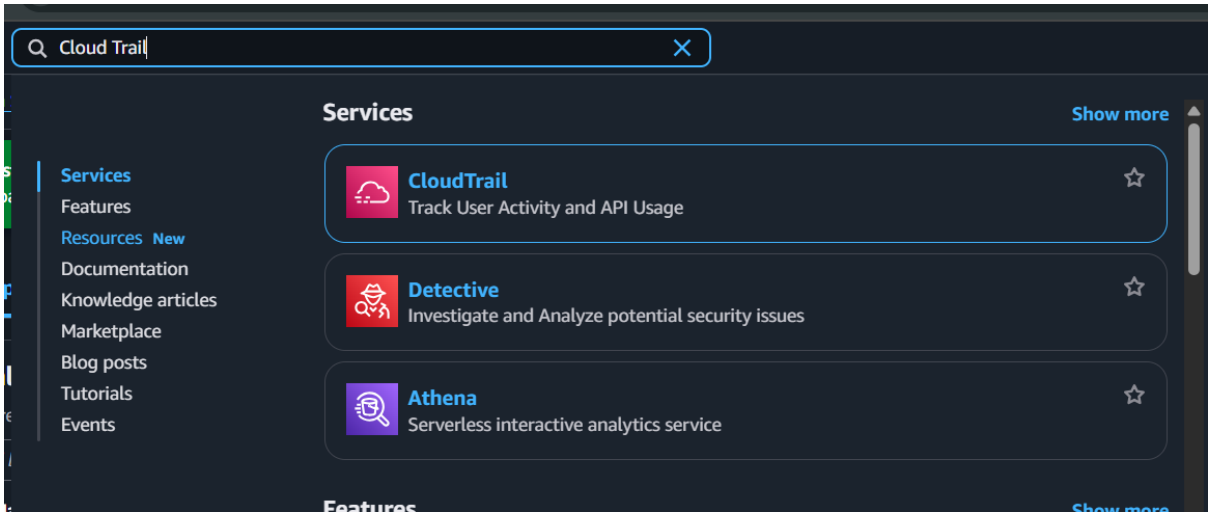
21 July 2025

This project focuses on implementing effective monitoring and logging practices in AWS using CloudTrail and CloudWatch. It demonstrates how to set up a multi-region CloudTrail trail to log API activities, configure an S3 bucket with SSE-KMS encryption for secure log storage, and integrate CloudTrail with CloudWatch for real-time monitoring and alerting. The goal is to enhance visibility, detect unusual activities, and ensure compliance with security best practices in a cloud environment.

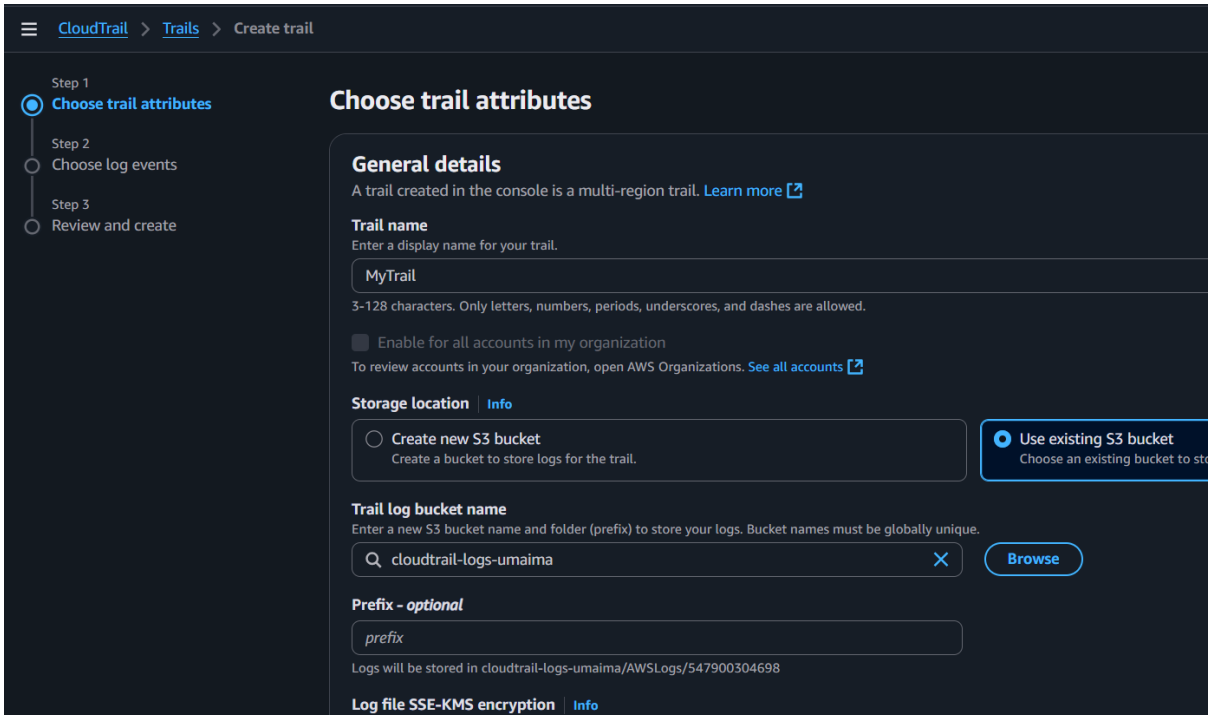




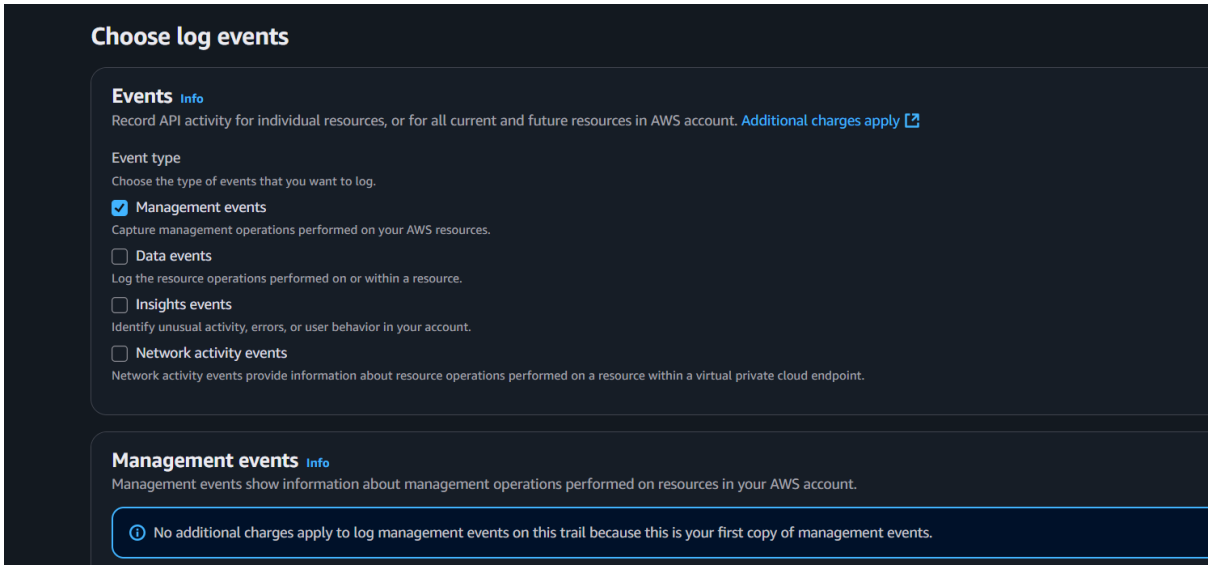
This screenshot shows the creation of an S3 bucket named cloudtrail-logs-umaima, with versioning enabled to store CloudTrail logs securely.



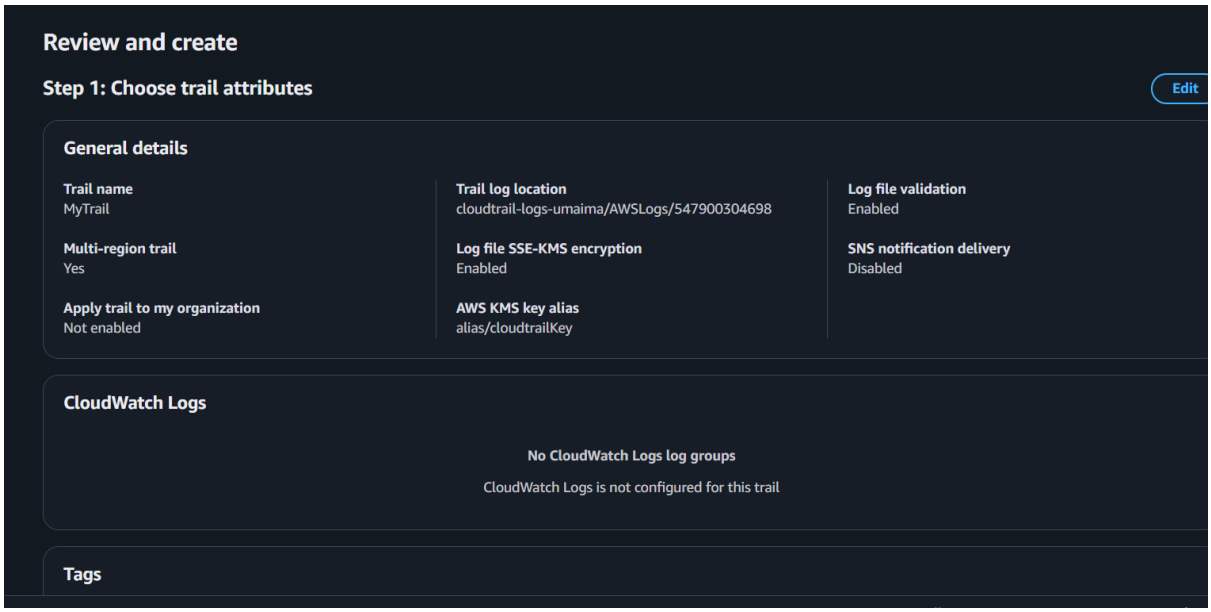
Go to CloudTrail



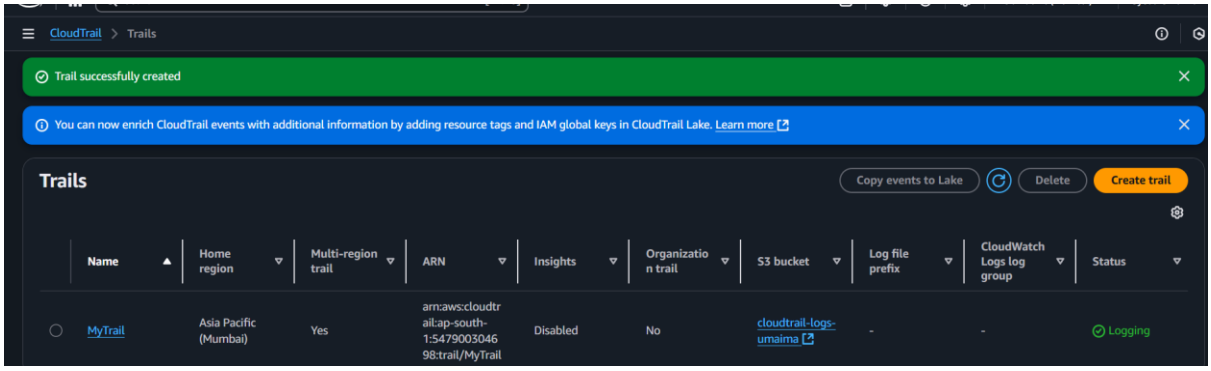
CloudTrail trail was configured to store logs in the S3 bucket cloudtrail-logs-umaima with an optional prefix.
KMS encryption was enabled using a **Customer Managed Key** (alias/cloudtrailKey) to ensure enhanced security of log files.



Management events were enabled for the trail to capture both **Read** and **Write** API activity.
KMS and Amazon RDS Data API events were excluded to reduce unnecessary logs.
Other event types like Data, Insights, and Network activity were left disabled to optimize cost and relevance.

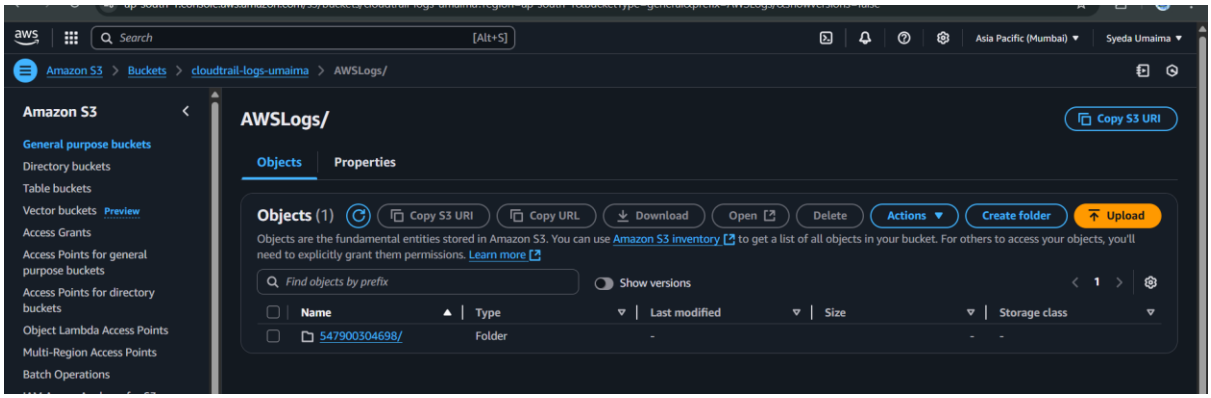


A summary of the CloudTrail configuration was reviewed. All chosen options were verified before final creation. The trail was then successfully created with logging enabled for management API activity.

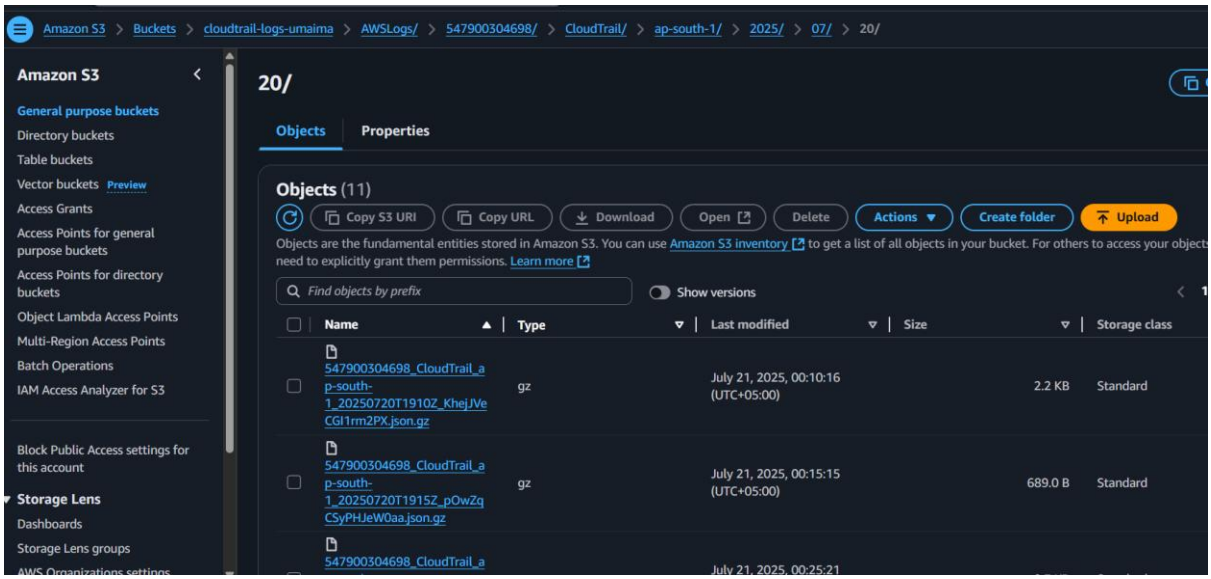


The complete trail setup was reviewed, including multi-region support, SSE-KMS encryption, and logging of all management events. The trail was then successfully created.

The CloudTrail trail named MyTrail is now actively logging events, with status confirmed as 'Logging'. This indicates successful setup of multi-region event monitoring.



S3 bucket cloudtrail-logs-umaima showing CloudTrail log files under the folder path AWSLogs/.



The CloudTrail logs are successfully delivered in the S3 bucket under the path AWSLogs/547900304698/CloudTrail/ap-south-1/2025/07/**20/**, with log files in compressed .gz format.

By enabling CloudTrail and integrating it with CloudWatch, this project successfully established a secure and centralized logging mechanism. It provides a detailed audit trail of AWS account activities and supports proactive security monitoring. This setup not only improves operational transparency but also strengthens incident response capabilities, making it a crucial component of any AWS cloud security strategy.