



Module 10 - CloudTrail

CloudTrail

CloudTrail enables governance, compliance, operational auditing, and risk auditing of AWS accounts. It records and stores API calls made on your AWS account, providing visibility into actions taken by users, services, and resources within the account.

Setup.

Search for CloudTrail service and then click on Create Trail. Also, for storing the trails we will be using S3 bucket.

General details

A trail created in the console is a multi-region trail.[Learn more](#)

Trail name
Enter a display name for your trail.

Demo-Trail

3-128 characters. Only letters, numbers, periods, underscores, and dashes are allowed.

☐ Enable for all accounts in my organization
To review accounts in your organization, open AWS Organizations. [See all accounts](#)

Storage location [Info](#)

☒ Create new S3 bucket
Create a bucket to store logs for the trail.

☐ Use existing S3 bucket
Choose an existing bucket to store logs for this trail.

Trail log bucket and folder
Enter a new S3 bucket name and folder (prefix) to store your logs. Bucket names must be globally unique.

aws-cloudtrail-logs-550387307646-cb2c0222

Logs will be stored in aws-cloudtrail-logs-550387307646-cb2c0222/AWSLogs/550387307646

Log file SSE-KMS encryption [Info](#)

☐ Enabled

▼ **Additional settings**

Log file validation [Info](#)

☒ Enabled

SNS notification delivery [Info](#)

☐ Enabled

Event type - Select Management events, Data events, Insights events.

Management events – Read and Write.

Data Events – S3

Insights events – API call rate and error rate.

Click on Next and then Click on Create Trail.

Now go back to S3 bucket and see the data.