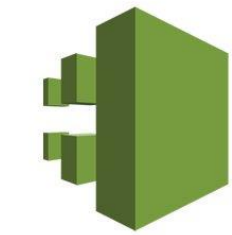
AWS CloudTrail

❖ AWS CLOUDTRAIL:

- CloudTrail captures API calls and related events made by or on behalf of your AWS account and delivers the log files to an Amazon S3 bucket that you specify.
- It Provides governance, compliance and audit for your AWS account.
- Cloud Trail is enabled on your AWS account when you create it. When the activity occurs in your account, that activity is recorded in cloud trail event.
- This event history simplifies security analysis, resource change tracking, and troubleshooting.

➢ USE CASES:

- Audit activity
- Identify security incidents
- Troubleshoot operational issues

➢ EVENT HISTORY:

- When activity occurs in your AWS account, that activity is recorded in a CloudTrail event. You can easily view events in the CloudTrail console by going to Event history.
- Event history allows you to view, search, and download the past 90 days of activity in your AWS account.

➢ TRAIL:

- CloudTrail trail to archive, analyze, and respond to changes in your AWS resources.
- A trail is a configuration that enables delivery of events to an Amazon S3 bucket that you specify.
- You can also deliver and analyze events in a trail with Amazon CloudWatch Logs and Amazon CloudWatch Events.
- CloudTrail events can be processed by one trail for free.
- There is a charge for processing events with additional trails.
- can create two types of trails:
  - A trail that applies to all regions
  - A trail that applies to one region