# AWS CloudTrail

**Topics :** AWS
**Written on** December 09, 2023

AWS CloudTrail is a service that provides visibility into user activity and resource changes across your AWS infrastructure. It records AWS API calls made on your account, including who made the call, the services used, and the parameters provided. CloudTrail logs are stored in an Amazon S3 bucket and can be analyzed to monitor and audit AWS usage, enhance security, and meet compliance requirements.

1. **Logging API Activity:**
    - CloudTrail logs API calls made on your AWS account, including calls from the AWS Management Console, AWS Command Line Interface (CLI), SDKs, and other AWS services.
2. **Trail Configuration:**
    - A CloudTrail trail is a configuration that enables logging for an AWS region. You can create and configure trails to capture specific events or all events for a region.
3. **S3 Bucket Storage:**
    - CloudTrail logs are stored in an Amazon S3 bucket. You can specify an existing S3 bucket or create a new one for storing CloudTrail log files.
4. **Event History:**
    - CloudTrail maintains an event history that shows a summary of the past seven days of activity. The event history includes basic information about events, such as event name, time, user, and source IP address.
5. **Log File Integrity:**
    - CloudTrail logs are digitally signed and stored in an S3 bucket with limited access. This ensures the integrity and security of log files.
6. **CloudWatch Logs Integration:**
    - CloudTrail logs can be optionally delivered to Amazon CloudWatch Logs. This integration allows you to set up alarms and notifications based on specific events or patterns in the logs.
7. **Multi-Region Trails:**

- You can configure CloudTrail to deliver logs from multiple AWS regions to a single S3 bucket. This is useful for centralized monitoring and auditing in multi-region architectures.

8. **Advanced Event Selectors:**
   - CloudTrail allows you to use advanced event selectors to filter the events that are logged. You can define rules based on specific services, resources, or event attributes.
9. **Insight Events:**
   - CloudTrail Insight Events provide additional visibility into activities that may impact the security of your account. These events highlight unusual API activities and potential security risks.
10. **Management Events:**
    - CloudTrail logs management events that relate to the configuration of your AWS resources, such as creating, modifying, or deleting resources. This helps in tracking changes to your environment.
11. **Global Services:**
    - CloudTrail logs global services events that are not tied to a specific region. Global services, such as IAM (Identity and Access Management), are logged in the US East (N. Virginia) region.
12. **Integrations with AWS Services:**
    - CloudTrail integrates with other AWS services, including AWS CloudWatch, AWS Config, AWS Lambda, and AWS CloudWatch Events. This allows you to automate responses based on CloudTrail events.
13. **Compliance and Auditing:**
    - CloudTrail logs can be used for compliance auditing and investigation. They provide a detailed record of actions taken on your AWS resources, supporting regulatory requirements.
14. **Event History Dashboards:**
    - CloudTrail Event History Dashboards in the AWS Management Console provide a visual representation of activity, making it easier to analyze and understand events over time.