**CLOUD TRAIL**

AWS CloudTrail increases visibility into your user and resources activity by recording AWS Management Console actions and API call

You can identify which users and accounts called AWS, the sources IP address from which the calls were made, and when the calls occurred.

**CloudWatch VS Trail**

CloudWatch monitor performance AWS

CloudTrail monitors API calls in the AWS Platform

CloudWatch is all about performance

CloudTrail is all about auditing (i.e. it’s an auditing service)

**Example**

Let’s Say, someone has deleted S3 bucket?

How to know, which users has done this?

At what time, it has happened?

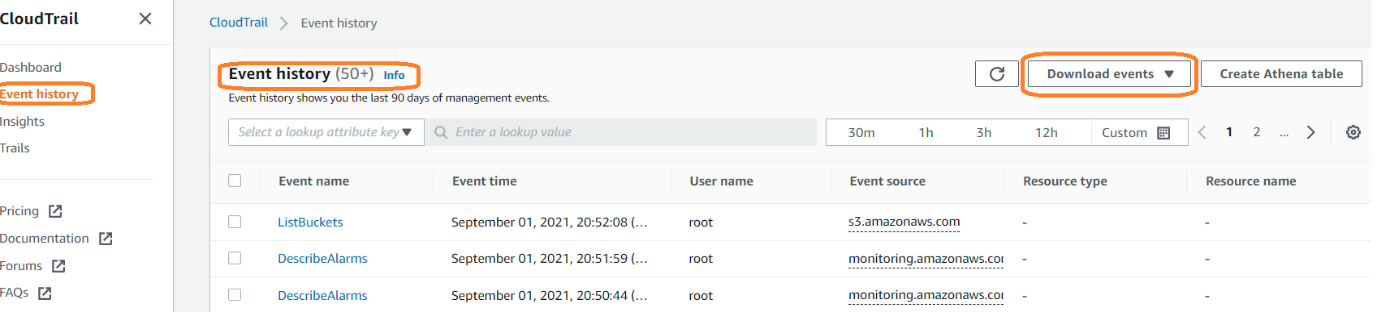
We can track this information using cloud trail.

All the activities can be tracked by user using cloud trail.

Go to CloudTrail dashboard

**CloudTrail 🡪 Event history**

Event history shows you the last 90 days of management events.

****

**Observation**: We can see the records of the events which we have performed.

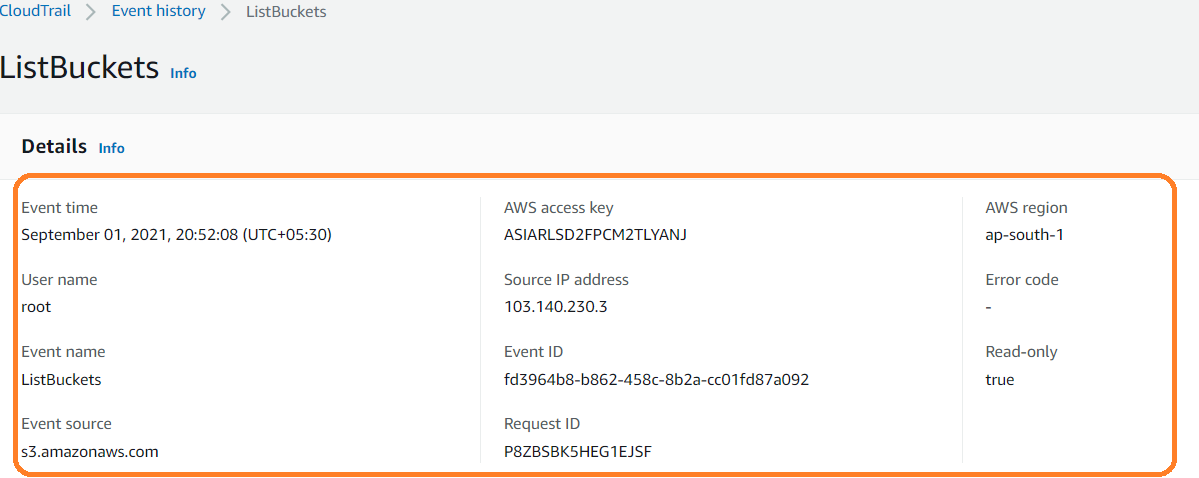
Select a particular event, we can get more detail information.

We can apply filter based on time period.

We can filter the event and download the list of events.

**Note:** Root user can see the Event history.

IAM users will not have access to see the event history.



We can’t delete it it’s just read only

By default, Cloud track from root user

**Free Tier**

You can get started with AWS CloudTrail for free.

**Log and search events with Event History**

AWS CloudTrail logs management events across AWS services by default. You can view, search, and download the most recent 90-day history of your account’s management events for free using CloudTrail in the AWS console or the AWS CLI Lookup API