CLOUDTRAIL

* It is used to monitor API calls made by all users in an aws account.
* It stores all logs in S3 buckets that we mentioned while creating cloudtrail. It saves logs with sourceip, timestamp, region, action occurred, username and instance id. So, we can find easily who did what actions with this cloudtrail.
* You can see all the activities in event activity of last 7 days in aws console. As in that console, they mention ip, username, action, instance id etc.
* Go to cloudtrail console,

**Type a trail name**

**Select Bucket(to store logs)**

**Apply to all regions = yes (or) No.**

**Click Save.**

* Now, go to S3 and check, there will be folders created in the bucket that we mentioned while creating trail. All the logs are store here.
* You can integrate cloud trail with cloud watch logs to monitor api calls from aws console.
* You can integrate cloud trail with cloud watch logs only after creating a trail.
* Go to cloud trail, Select an existing trail.
* In cloud watch logs Section,

**Click, Configure.**

**Create new log group (or) select existing group.**

* A cloud watch logs role and cloud watch logs policy will be created automatically on behalf of ourselves. Select the role and policy in next page.

**Click, View details. And Select.**

**IAM Role = cloud watch logs role.**

**Policy Name = Cloud watch logs.**

**Click Allow.**

* Wait for few minutes, you will see a log group storing all your API calls from cloud trail.