**Difference between CloudWatch and CloudTrail**

**Amazon CloudWatch** is a service provided by Amazon Web Services (AWS) that helps to keep an eye on our applications and resources running in the AWS cloud. It allows us to collect and track important data, such as metrics (performance measurements) and logs (recorded events), and set alarms to get notified when something goes wrong.

Let's say we have a web application running on AWS EC2 instances and we want to monitor the CPU utilization and network throughput of those instances. We can use CloudWatch to collect and visualize metrics such as CPU usage percentage and network bytes in and out. CloudWatch can help in setting up alarms to notify us when the CPU utilization exceeds a certain threshold, allowing us to take proactive actions like scaling up our instances to handle the increased load.

Step 1: Create an EC2 Instance

* Sign in to the AWS Management Console and navigate to the EC2 service.
* Launch a new EC2 instance or select an existing one.

Step 2: Enable Detailed Monitoring

* Select the EC2 instance and go to the "Monitoring" tab.
* Enable detailed monitoring for the instance.

Step 3: Create a CloudWatch Alarm

* Go to the CloudWatch service in the AWS Management Console.
* Select "Alarms" from the sidebar and click "Create Alarm."
* Choose the EC2 metric you want to monitor, such as "CPUUtilization."
* Set the threshold and conditions for the alarm.
* Configure actions, such as sending a notification or triggering an automated response.

Step 4: Test the Alarm

* Generate load on the EC2 instance to trigger high CPU utilization.
* Monitor the CloudWatch alarm and observe if it goes into the "ALARM" state.

**AWS CloudTrail** is a service provided by Amazon Web Services (AWS) that keeps a record of all the actions taken within the AWS account. It creates a detailed trail or log of every API call made by users, services, or resources in the account. It helps to keep track of who did what, when they did it, and from where, allowing us to monitor and audit the activity in our AWS environment. This log can be used for security analysis, troubleshooting, compliance auditing, and maintaining a secure and accountable AWS infrastructure.

Suppose we have a team of administrators who manage various resources in your AWS account. With CloudTrail, we can monitor and track every action they perform, such as creating or deleting EC2 instances, modifying security groups, or changing IAM policies. CloudTrail provides you with an event history, including details such as the identity of the user who made the API call, the time of the action, and the source IP address. This audit trail is valuable for troubleshooting issues, investigating security incidents, or ensuring compliance with regulatory requirements.

Step 1: Enable CloudTrail

* Go to the AWS Management Console and navigate to the CloudTrail service.
* Click "Create trail" to set up a trail.
* Specify the trail details, including trail name and storage settings.
* Choose the AWS resources for which you want to log API calls.

Step 2: Configure Event History

* In the CloudTrail console, click on "Event history."
* Set the retention period for storing events.
* Choose if you want to log management events, data events, or both.

Step 3: Review and Analyze Events

* Once CloudTrail is enabled, it automatically starts recording API calls.
* Go to the CloudTrail console and select your trail to view the events.
* Use filters and search options to locate specific events.
* Analyze the event details, including the user, action, and timestamp.

Step 4: Integrate with Other Services

* CloudTrail can send logs to Amazon S3 for long-term storage or to Amazon CloudWatch Logs for real-time analysis.
* Configure integration with the desired services based on your requirements.

|  |  |  |
| --- | --- | --- |
| **Parameters** | **AWS CloudWatch** | **AWS CloudTrail** |
| **Definition** | CloudWatch is a monitoring service for AWS resources and applications. | CloudTrail is a web service that records API activity in your AWS account. |
| **Monitoring Tool** | CloudWatch monitors applications and infrastructure performance in the AWS environment. | CloudTrail monitors actions in the AWS environment. |
| **Usage** | With CloudWatch, we can Collect and track metricsCollect and monitor log filesSet alarms and visualize | CloudTrail answers these questions:Who made a request?Which services were used?What actions were performed?What were the parameters for those actions?What were the response elements returned by the AWS service? |
| **Example Scenario** | CloudWatch: Monitoring the CPU utilization of EC2 instances and setting alarms to trigger actions based on predefined threshold | CloudTrail: Tracking and logging API calls made by administrators to identify who made changes to resources, when the changes were made, and what actions were taken. |

Reference link -

[CloudTrail vs. CloudWatch: Tutorials & Examples - OpsRamp](https://www.opsramp.com/guides/aws-monitoring-tool/cloudtrail-vs-cloudwatch/#:~:text=CloudWatch%20is%20a%20monitoring%20service,activity%20in%20your%20AWS%20account.&text=CloudWatch%20monitors%20applications%20and%20infrastructure,actions%20in%20the%20AWS%20environment.)

[AWS CloudWatchs vs. CloudTrail - What's the Difference? | PullRequest Blog](https://www.pullrequest.com/blog/aws-cloudwatch-vs-cloudtrail-whats-the-difference/)