

## Hands-on with AWS CloudTrail – Monitor User Activity

### What is CloudTrail?

**CloudTrail** is a service in AWS that is used to **monitor and log user activity** in our AWS account.

With CloudTrail, we can track **which user performed specific actions** and **identify the source** of those actions.

#### Important:

- CloudTrail is a **region-specific** service, meaning it records events in the **region where it is enabled**.

### Difference Between CloudWatch and CloudTrail

Feature	CloudWatch	CloudTrail
Purpose	Monitor AWS <b>resources and applications</b> (e.g., EC2, RDS, Lambda)	Monitor <b>user activity</b> and API usage
Data Type	<b>Performance metrics, logs, alarms</b>	<b>Event logs of AWS API calls and actions</b>
Use Case	Troubleshooting, performance monitoring, and setting alarms	Governance, compliance, auditing, and security investigations
Example	Set alarm if EC2 CPU > 80%	Track which user deleted an S3 bucket or launched an EC2 instance
Region Scope	Regional, but can be configured to aggregate data	Region-specific by default, but can be enabled across all regions

### Hands-on Lab: Set Up AWS CloudTrail

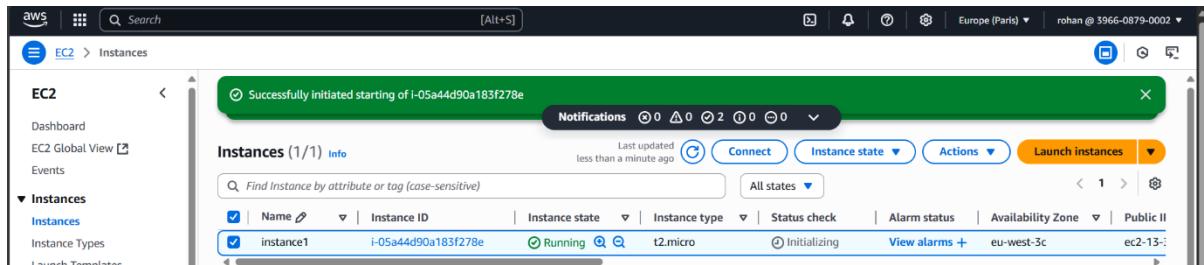
#### Prerequisites

- AWS account (Free Tier)
- IAM user with admin privileges or cloudtrail:\* permissions

## Step-by-Step Setup

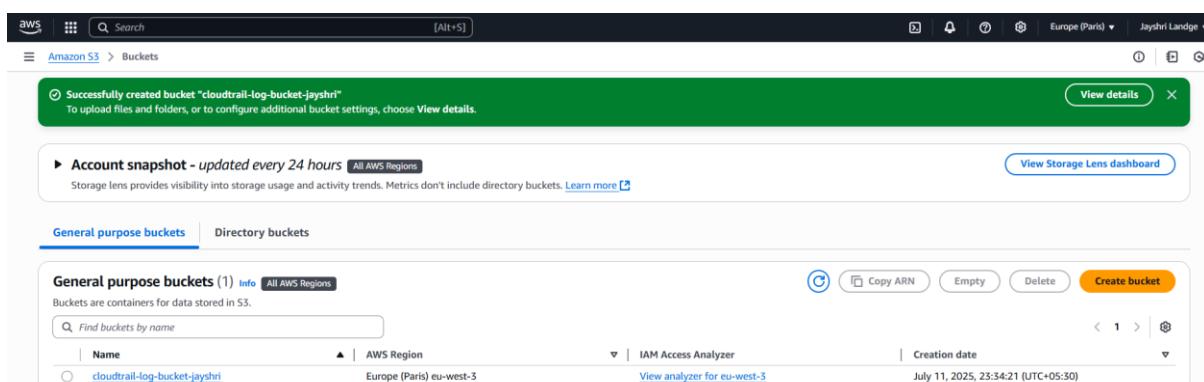
### Step 1: Log in to AWS Console

- ◆ Go to <https://console.aws.amazon.com>
- ◆ Sign in with IAM credentials



### Step 2: Create an S3 Bucket for CloudTrail Logs

1. Go to **S3** from the Services menu
2. Click **Create Bucket**
3. Enter bucket name: **cloudtrail-log-bucket-jayshri**
4. Keep default settings or uncheck "Block all public access" if testing only
5. Click **Create Bucket**



### Step 3: Enable CloudTrail

1. Go to the **CloudTrail** service
2. Click **Create trail**
3. Trail name: MyTrail
4. Choose “**Apply trail to all regions**”

5. Under “Storage location”, select your previously created S3 bucket

6. Leave other defaults and click **Create Trail**

The screenshot shows the AWS CloudTrail 'Trails' page. A single trail named 'MyTrail' is listed. The details are as follows:

Name	Home region	Multi-region trail	ARN	Insights	Organization trail	S3 bucket	Log file prefix	CloudWatch Logs log group	Status
MyTrail	Europe (Paris)	Yes	arn:aws:cloudtrail:eu-west-3:396608790002:trail/MyTrail	Disabled	No	aws-cloudtrail-logs-396608790002-99b70fed	-	-	Logging

**Screenshot 3: CloudTrail Create Trail Page**

The screenshot shows the AWS CloudTrail 'MyTrail' details page. The general details are:

General details	Trail log location	Log file validation	SNS notification delivery
Trail logging Logging	aws-cloudtrail-logs-396608790002-99b70fed/AWSLogs/396608790002	Disabled	Disabled
Trail name MyTrail	Last log file delivered July 11, 2025, 23:37:34 (UTC+05:30)	Last file validation delivered -	Last SNS notification -
Multi-region trail Yes	Log file SSE-KMS encryption Not enabled		
Apply trail to my organization Not enabled			

**Screenshot 4: Trail creation summary**

#### Step 4: Perform an AWS Action

- ◆ Example: Go to **EC2** and launch a new instance or stop/start an existing one
- ◆ This generates an event CloudTrail will record

The screenshot shows the AWS EC2 'Instances' page. A green success message at the top states: "Successfully attached role\_for\_ec2\_to\_amazonssmmanagedinstancecore to instance i-081645094d45e18a1". The main list shows one instance named 'instance1' with the ID 'i-081645094d45e18a1'. The instance is running and has an 't2.micro' type.

**Screenshot 5: EC2 Instance Launch or Action Performed**

#### Step 5: View Event Logs in CloudTrail

1. Go back to the **CloudTrail Dashboard**
2. Click on **Event History**
3. Filter by **Event Name** or **User Name**

4. Click any event to see:

- User identity
  - Event source (e.g., ec2.amazonaws.com)
  - Time, region, request and response JSON

## Screenshot 7: CloudTrail Event History Page

The screenshot shows the AWS CloudTrail Event history page. The left sidebar includes links for Dashboard, Event history, Insights, Lake (selected), Dashboards, Query, Event data stores, Integrations, Trails, Settings, Pricing, Documentation, Forums, and FAQs. The main content area has a header: "You can now enrich CloudTrail events with additional information by adding resource tags and IAM global keys in CloudTrail Lake. Learn more". Below it, the "Event history (50+)" section displays a table of events from the last 90 days. The table columns are: Event name, Event time, User name, Event source, Resource type, and Resource name. The table rows show various AWS S3 operations like DeleteBucket, CreateBucket, ListBuckets, and DescribeInstances, all performed by the user 'rohan' on July 8, 2025, at different times between 00:39:47 and 00:59:39 UTC.

User name	Event name	Event time	User name	Event source	Resource type	Resource name
rohan	DeleteBucket	July 08, 2025, 00:39:47 (UTC+0)	rohan	s3.amazonaws.com	AWS::S3::Bucket	jayshri67859
rohan	DeleteBucket	July 08, 2025, 00:39:59 (UTC+0)	rohan	s3.amazonaws.com	AWS::S3::Bucket	jayshri67859
rohan	DeleteBucket	July 08, 2025, 00:39:26 (UTC+0)	rohan	s3.amazonaws.com	AWS::S3::Bucket	jayshri67859
rohan	CreateBucket	July 08, 2025, 00:36:52 (UTC+0)	rohan	s3.amazonaws.com	AWS::S3::Bucket	jayshri67859
rohan	CreateBucket	July 08, 2025, 00:36:12 (UTC+0)	rohan	s3.amazonaws.com	AWS::S3::Bucket	jayshri67859
rohan	ListBuckets	July 08, 2025, 00:35:29 (UTC+0)	rohan	s3.amazonaws.com	-	-
rohan	ListBuckets	July 08, 2025, 00:34:04 (UTC+0)	rohan	s3.amazonaws.com	-	-
rohan	DescribeInstances	July 08, 2025, 00:33:17 (UTC+0)	rohan	ec2.amazonaws.com	-	-
rohan	ListNotificationHubs	July 07, 2025, 20:29:37 (UTC+0)	rohan	notifications.amazonaws.com	-	-
rohan	DescribeRegions	July 07, 2025, 20:29:36 (UTC+0)	rohan	ec2.amazonaws.com	-	-

## Screenshot 8: Detailed View of a Selected Attribute

### **Optional Step: Enable CloudTrail Insights**

To track **unusual activity**, enable **Insights events**:

- Go to Trail → Edit
  - Enable **Insights for Write-only management events**
  - This will help detect spikes in traffic or anomalous behavior.

## Conclusion

By completing this hands-on lab with **CloudTrail**, you have learned how to:

- **Log user activity** and API calls in AWS
  - Use S3 as a **central storage** for activity logs
  - Use **Event History** to view, filter, and analyze user actions
  - Understand the **difference** between resource monitoring (CloudWatch) and user monitoring (CloudTrail)