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 **resources and applications** (e.g., EC2, RDS, Lambda)	Monitor **user activity** and API usage
Data Type	**Performance metrics, logs, alarms**	**Event logs of AWS API calls and actions**
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

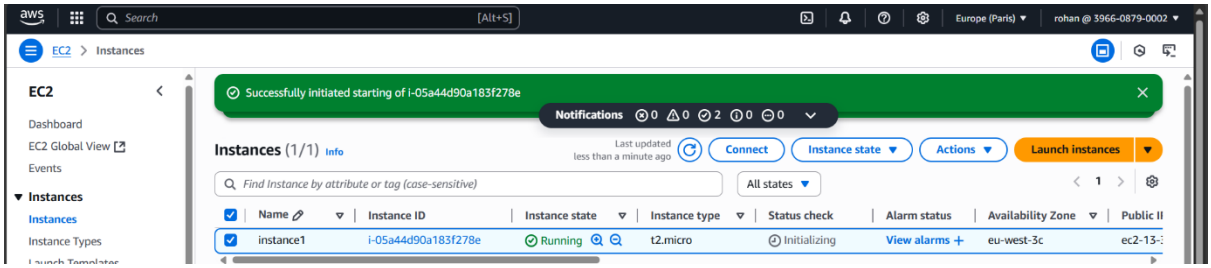
Prerequisites

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

Step-by-Step Setup

Step 1: Log in to AWS Console

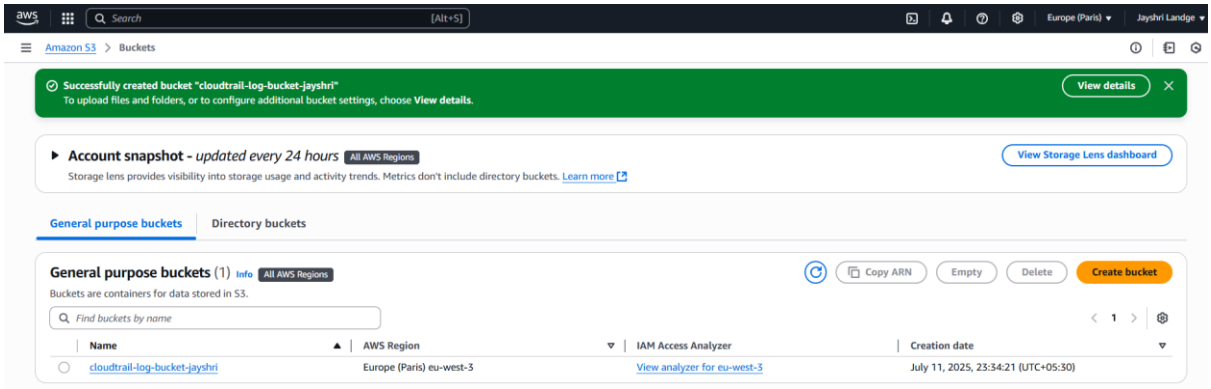
- Go to https://console.aws.amazon.com
- Sign in with IAM credentials



Screenshot 1: AWS Console Home Page after login

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**

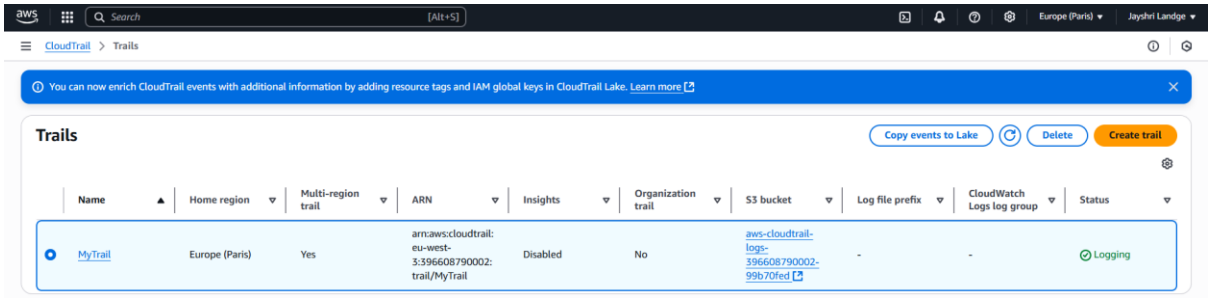


Screenshot 2: S3 Bucket Creation Page

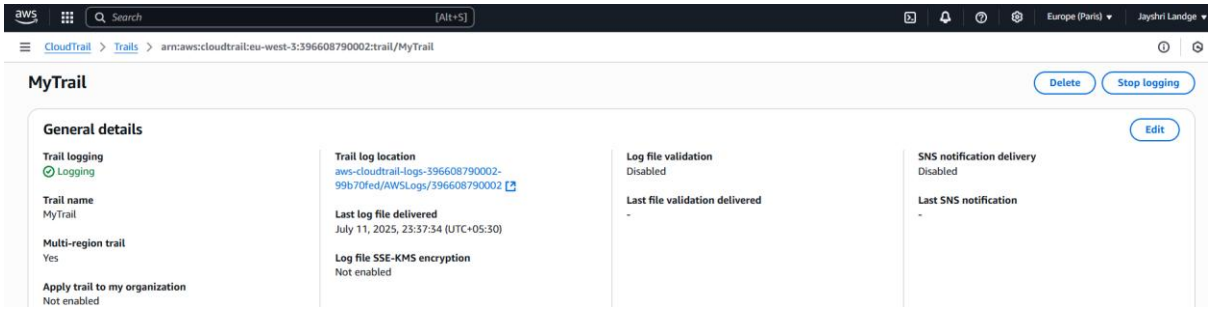
Step 3: Enable CloudTrail

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**



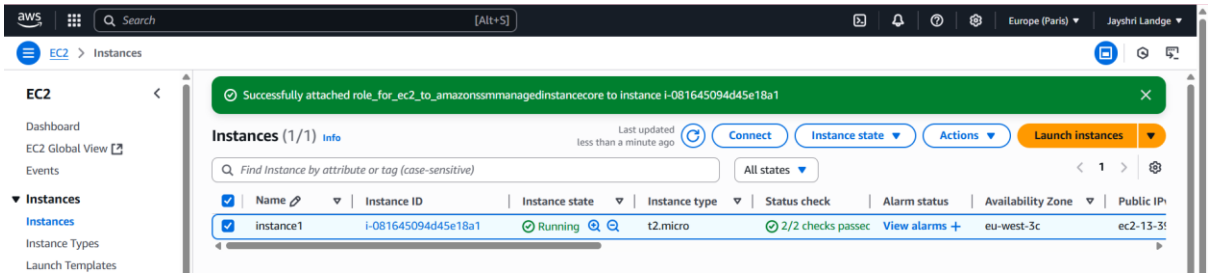
Screenshot 3: CloudTrail Create Trail Page



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

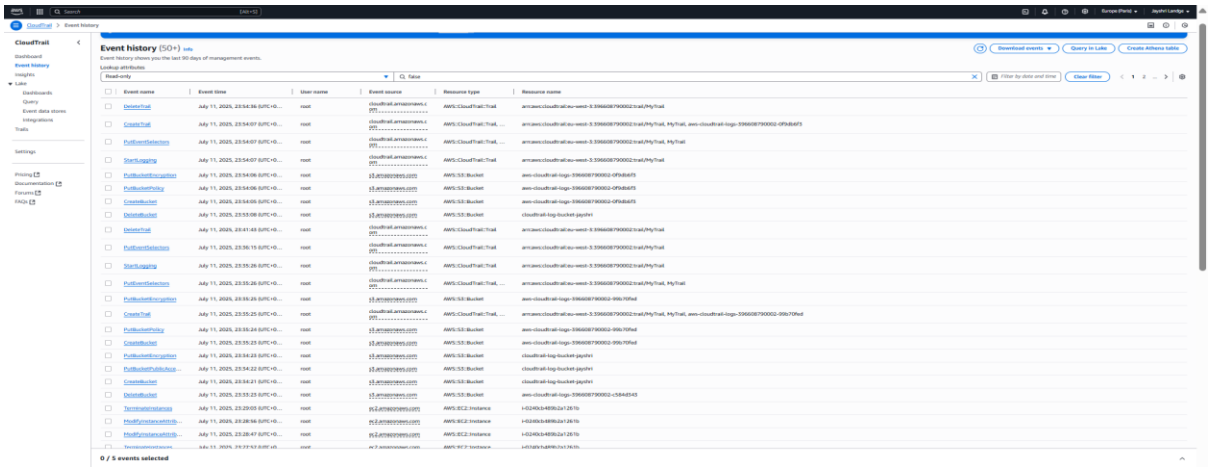


Screenshot 5: EC2 Instance Launch or Action Performed

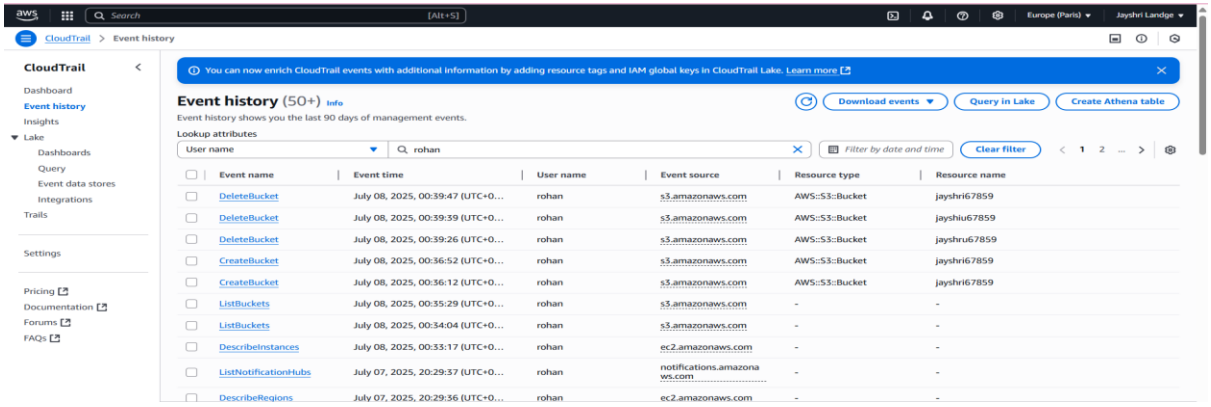
Step 5: View Event Logs in CloudTrail

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



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)