



What does CloudTrail track in your AWS account?

Answer:

CloudTrail tracks **all API calls** made in your AWS account — **who did what, from where, and when**.

That includes:

- Which user or service made the call
- What action they performed (e.g., StartInstances, PutObject)
- What resources were involved (like an EC2 instance or S3 bucket)
- The IP address and timestamp of the action
- Whether the action succeeded or failed

CloudTrail Log– Delete S3 Bucket

```
-----
{
  "eventVersion": "1.08",
  "userIdentity": {
    "type": "IAMUser",
    "userName": "data_admin"
  },
  "eventTime": "2025-07-20T13:05:45Z",
  "eventSource": "s3.amazonaws.com",
  "eventName": "DeleteBucket",
  "awsRegion": "ap-south-1",
  "sourceIPAddress": "203.0.113.10",
  "userAgent": "console.amazonaws.com",
  "requestParameters": {
    "bucketName": "important-data-backup"
  },
  "responseElements": null,
  "requestID": "8F7B8B13E4D6C123",
  "eventID": "d9c123ab-4d87-4cde-9c88-xyz9876a1234",
  "eventType": "AwsApiCall"
}
```

Explanation:

- **User data_admin deleted the bucket important-data-backup**
- **Action taken from the AWS Console in region ap-south-1 (Mumbai)**
- **Contains timestamp, source IP, and request ID**

What does AWS CloudTrail primarily track in your AWS account?

- A. Network traffic between AWS services**
- B. All API calls, including who made them, when, from where, and on which resources**
- C. CPU and memory usage of EC2 instances**
- D. Real-time application logs**

Correct Answer:  **B**

Explanation:

CloudTrail logs all API activity in your AWS account, including the user/service, action performed, resources involved, time, IP address, and request details.

In the provided CloudTrail log, which of the following actions occurred?

- A. An IAM role was created by user data_admin.**
- B. A bucket named important-data-backup was deleted from the ap-south-1 region.**
- C. An EC2 instance was started in ap-south-1.**
- D. An S3 object was uploaded.**

Correct Answer:  **B**

Explanation:

The "eventName": "DeleteBucket" shows the action was deleting an S3 bucket named important-data-backup in the Mumbai (ap-south-1) region by the IAM user data_admin.

Which of these details can you NOT directly get from a CloudTrail log?

- A. The exact time an action happened.**
- B. The IP address from which the request originated.**
- C. Whether the action succeeded or failed.**
- D. The amount of CPU used during the action.**

Correct Answer:  **D**

Explanation:

CloudTrail does not capture resource performance metrics like CPU usage — that is the role of CloudWatch.

In a CloudTrail log, the eventSource field value "s3.amazonaws.com" indicates:

- A. The request was made by the AWS CLI.**
- B. The request targeted the Amazon S3 service.**
- C. The request was sent from an EC2 instance.**
- D. The request was related to IAM permissions.**

Correct Answer:  **B**

Explanation:

eventSource identifies which AWS service handled the request — here "s3.amazonaws.com" means it was an Amazon S3 operation.