1. How does AWS CloudWatch differ from AWS CloudTrail?

Amazon CloudWatch is basically the **monitoring and observability** service in AWS. It helps us **track metrics, collect logs, set alarms, and even trigger actions** based on thresholds.
For example, I use CloudWatch to monitor:

- CPU usage on EC2
- Memory and disk space (with custom scripts)
- Application logs from services like Lambda, ECS, etc.

👉 CloudTrail, on the other hand, is more about auditing and governance. It records who did what in your AWS account — like when someone starts an EC2 instance, or updates an S3 bucket policy.
Simple difference:

- CloudWatch = **What is happening (metrics, logs**)
- CloudTrail = **Who did what (API calls, security)**

Amazon CloudWatch
📌 **Purpose:** *Tells you **what is happening*** (e.g., performance, usage, errors)
📄 **Sample Log Output (from an EC2 instance)**
json

```
{
 "timestamp": "2025-07-20T10:12:34Z",
 "instanceId": "i-0abc1234def5678gh",
 "logStream": "webserver-logs",
 "message": "ERROR: Failed to connect to database at 10.0.1.45:5432 - Timeout",
 "logGroup": "/aws/ec2/webserver"
}
```

📌 **Explanation:**

- Shows an **application error** logged by a web server on EC2.

- Useful for **debugging**, **performance monitoring**, and **alerting**.
- **Metric examples**: CPUUtilization, DiskReadOps, NetworkIn

---

✅ **AWS CloudTrail**

📌 **Purpose:** *Tells you **who did what** in your AWS account* (security, auditing)

📄 **Sample Log Output (for an EC2 API call)**

json

```
{
 "eventTime": "2025-07-20T10:12:30Z",
 "eventSource": "ec2.amazonaws.com",
 "eventName": "StartInstances",
 "awsRegion": "us-east-1",
 "sourceIPAddress": "123.45.67.89",
 "userAgent": "aws-cli/2.15.0",
 "userIdentity": {
  "type": "IAMUser",
  "userName": "devops_engineer"
 },
 "requestParameters": {
  "instancesSet": {
   "items": [{ "instanceId": "i-0abc1234def5678gh" }]
  }
 },
 "responseElements": {
  "instancesSet": {
   "items": [{
    "instanceId": "i-0abc1234def5678gh",
    "currentState": { "name": "pending" }
   }]
  }
 }
}
```


📌 **Explanation:**

- Shows that **devops_engineer** started an EC2 instance using **AWS CLI**.
- Useful for **security auditing**, **compliance**, **tracing malicious activity**, and **change tracking**.

Summary Table

Feature	CloudWatch	CloudTrail
Purpose	What is happening	Who did what
Data Type	Metrics, Logs	API Calls, User Actions
Audience	Developers, Ops teams	Security, Audit, Compliance teams
Example Use	CPU > 90%, App Crash Log	EC2 StopInstance by user 'X'

Which AWS service is primarily used for *security auditing*?
A. CloudWatch
B. CloudTrail
C. GuardDuty
D. Config
✅ **Answer: B** — CloudTrail tracks *who did what* via API call logs.

You want to monitor *CPU usage* of an EC2 instance in real time. Which AWS service should you use?
A. CloudTrail
B. CloudWatch
C. IAM
D. Inspector
✅ **Answer: B** — CloudWatch monitors metrics like CPU, memory, and logs.

Which data type is stored in CloudTrail logs?
A. System performance metrics
B. API call history with user identity
C. Application error logs
D. Network throughput
✅ **Answer: B** — CloudTrail logs API call details and identity information.
