AWS Management Tools

AWS Tools

- AWS CloudWatch
- AWS CloudTrail
- AWS Config
- AWS Systems Manager

AWS Management Tools

- When deploying critical business workloads to the AWS Cloud, it is essential to maintain visibility, security, and operational efficiency in your cloud environment.

- **Operational transparency** — Tracking who is doing what in your cloud environment and monitoring the performance of your resources.

- **Security assurance** — Detecting unusual API calls or resource utilization that might indicate a security threat.

- **Regulatory compliance** — Maintaining detailed logs of user activities and infrastructure changes for audit purposes.

AWS Management Tools

- **Performance management** — Monitoring resource utilization and application performance metrics.
- **Incident response** — data and alerts to quickly identify and respond to operational issues.
- **Cost control** — insights into resource usage to help manage cloud spending.
- **Automation** — automated responses to specific events or performance thresholds.

AWS CloudTrail

- Focused on governance, compliance, and operational auditing
- logs **all API calls** made within your AWS environment
- **Tracks all AWS account activities**, including API calls, actions taken in the AWS Management Console, AWS SDKs, command line tools, and other AWS services.
- Provides a **detailed log of every action**, including who made the call, the service used, and what resources were affected.
- Useful **for security auditing, tracking user activity, and identifying potentially malicious actions.**

Amazon CloudWatch

- A **monitoring and observability service** that provides data and actionable insights for AWS, on-premises, and hybrid applications and infrastructure

- Monitors AWS **resources and the applications** running on AWS in real-time, including **metrics, logs, and alarms**.

- Provides detailed insights into system performance, error rates, resource utilization, and more.

- Allows setting up alarms to trigger actions (for example, scaling resources) based on specific conditions.

Primary Purpose :
AWS CloudTrail Vs. Amazon CloudWatch

AWS CloudTrail

- Provides a comprehensive audit trail of all API activity within an AWS account. Focuses on recording who did what, when, and from where.
- This includes actions taken through the AWS Management Console, AWS SDKs, command line tools, and other AWS services.
- CloudTrail answers questions like "**Who terminated this EC2 instance?**" or "**What changes were made to this IAM policy?**"

Primary Purpose :
AWS CloudTrail Vs. Amazon CloudWatch

Amazon CloudWatch

- **Monitors** the operational health and performance of AWS resources and applications.
- CloudWatch **collects and tracks metrics**, collects and monitors log files, and sets alarms.
- It helps you understand how your applications are performing and respond to system-wide performance changes.
- CloudWatch answers questions like "**Is my Amazon EC2 instance's CPU utilization too high?**" or "**How many errors is my Lambda function generating**?"

Data collected:
AWS CloudTrail Vs. Amazon CloudWatch

Amazon CloudTrail

- Focuses on capturing **detailed logs of all API** activity within your AWS environment.
- This includes information on **who made the API** call, **when** it was made, the **action** taken, and the resources involved.
- CloudTrail's logs provide a comprehensive **audit trail**, essential for tracking changes, ensuring **compliance**, and investigating **security incidents**.

Data collected:
AWS CloudTrail Vs. Amazon CloudWatch

Amazon CloudWatch

- **Collects** performance and operational data from your AWS resources and applications.

- This includes metrics such as **CPU usage, memory utilization, network traffic, and application logs**, as well as **custom metrics** you can define.

- The data collected by CloudWatch is used for **real-time monitoring, performance optimization, and setting alarms** to trigger automated actions based on specific conditions.

Use Cases :
AWS CloudTrail Vs. Amazon CloudWatch

Amazon CloudTrail

- CloudTrail is useful in scenarios where you need to monitor who accessed specific resources, track changes made to configurations, or audit activity across multiple AWS accounts.

Amazon CloudWatch

- monitoring application performance
- managing resource utilization
- detecting anomalies
- ensuring your systems are running optimally to prevent downtime

Log retention
AWS CloudTrail Vs. Amazon CloudWatch

AWS CloudTrail

- By default, the CloudTrail event history records the **last 90 days** of management events for your account.
- Users can create a trail to store logs **indefinitely in an S3 bucket**.
- There's **no automatic deletion of logs stored in Amazon S3**, allowing for long-term retention.
- Users can implement lifecycle policies on S3 buckets to manage long-term storage costs.
- CloudTrail can be **configured to send logs to CloudWatch Logs** for more flexible retention options.

Log retention
AWS CloudTrail Vs. Amazon CloudWatch

Amazon CloudWatch

- Log retention in CloudWatch Logs is **more flexible and configurable**.
- Default retention period varies by log group, typically set to **"Never Expire".**
- Users can set **custom retention periods** ranging from one day to 10 years, or choose indefinite retention.
- Different log groups can have different retention periods.
- **After** the retention period, **logs are automatically deleted** to manage storage costs.
- CloudWatch Logs can be **exported to Amazon S3** for longer-term storage if needed.

Alarms and notifications

AWS CloudTrail Vs. Amazon CloudWatch

CloudTrail : Not primarily used for alarms, but can trigger actions based on API activity

CloudWatch : Enables setting alarms for specific metrics or log events, with automated responses

Integration
AWS CloudTrail Vs. Amazon CloudWatch

- **CloudTrail integrations**
  - **Amazon S3:** Store logs long-term for archival and analysis
  - **CloudWatch Logs:** Enable real-time log analysis and alerting
  - **Amazon EventBridge:** Trigger automated actions based on API events
  - **AWS Config:** Provide input for configuration tracking and compliance
  - **AWS Security Hub:** Contribute to centralized security posture management
  - **AWS Lake Formation:** Enable data lake governance of CloudTrail logs
  - **Amazon Athena:** Perform SQL queries on CloudTrail logs stored in Amazon S3

Integration
AWS CloudTrail Vs. Amazon CloudWatch

- **CloudWatch integrations**
  - ✓ **Amazon SNS**: Send notifications for alarms and events
  - ✓ **AWS Lambda:** Trigger serverless functions based on metrics or logs
  - ✓ **Amazon EC2 Auto Scaling:** Adjust capacity based on performance metrics
  - ✓ **AWS Systems Manager:** Automate operational tasks based on CloudWatch data
  - ✓ **AWS X-Ray:** Combine with trace data for in-depth application insights
  - ✓ **Container services** (Amazon ECS, Amazon EKS): Monitor containerized applications
  - ✓ **Third-party tools:** Export metrics and logs to external monitoring platforms

Cost considerations

AWS CloudTrail Vs. Amazon CloudWatch

CloudTrail : Costs based on the volume of logs generated and stored

CloudWatch : Costs based on the number of metrics, logs, and alarms monitored

Data granularity

AWS CloudTrail Vs. Amazon CloudWatch

CloudTrail : Provides detailed logs of every API call with granular information

CloudWatch : Provides aggregated metrics and log data for real-time monitoring

Resource coverage- Real-time tracking

AWS CloudTrail Vs. Amazon CloudWatch

CloudTrail : AWS account-wide :: Near real-time (within 5 minutes)

CloudWatch : Individual AWS resources :: Real-time or near real-time

Aspect	CloudWatch	CloudTrail
Purpose	Monitors **performance, health, and operational data** of AWS resources.	Records **API activity & user actions** across the AWS account for auditing & compliance.
Scope	Focuses on **individual resources** (EC2, Lambda, RDS, S3, etc.).	**Account-wide**, covering all AWS services and regions.
Data Type	**Metrics, logs, and events** (e.g., CPU usage, errors, latency, request counts).	**API calls/events** (e.g., CreateBucket, RunInstances, PutItem).
Latency	Real-time or near real-time (seconds to 1 min with detailed monitoring).	Near real-time (usually within ~5 minutes).
Retention	Metrics stored from **15 months** (with granularity decreasing over time). Logs retention is configurable.	Event history retained for **90 days** by default (can send to S3 for long-term storage).
Integration	Works with **alarms, dashboards, EventBridge, Auto Scaling, SNS**.	Works with **CloudWatch Logs, Athena, GuardDuty, Security Hub** for analysis.
Use Case	- Monitor EC2 CPU/memory - Set alarms for high latency - Automate scaling - Debug app logs	- Audit who deleted an S3 bucket - Investigate unauthorized login attempts - Compliance & security forensics
Example	**Doctor & monitoring devices** 🩺 → Keeps checking health (heartbeat, temperature, BP).	**CCTV camera & visitor log** 📹✍️ → Records who entered, what they did, and when.
Access Method	CloudWatch Console, CLI, SDK, API.	CloudTrail Console, CL

References

- https://docs.aws.amazon.com/awscloudtrail/latest/userguide/cloudtrail-user-guide.html
- https://docs.aws.amazon.com/AmazonCloudWatch/latest/monitoring/WhatIsCloudWatch.html
- https://docs.aws.amazon.com/decision-guides/latest/cloudtrail-or-cloudwatch/cloudtrail-or-cloudwatch.html