AWS Decision guide

AWS CloudTrail or Amazon CloudWatch?

AWS CloudTrail or Amazon CloudWatch?: AWS Decision guide

Table of Contents

AWS CloudTrail or Amazon CloudWatch?

Understand the differences and pick the one that's right for you

Purpose	To help you determine whether AWS CloudTrail or Amazon CloudWatch is the right choice for maintaining the visibility, security, and operational efficiency of your cloud environment.
Last updated	September 20, 2024
Covered services	• AWS CloudTrail • Amazon CloudWatch

Introduction

When deploying critical business workloads to the AWS Cloud, it is essential to maintain visibility, security, and operational efficiency in your cloud environment. There are a number of key areas to address:

- **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.
- **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 offers two key services to assist in addressing these concerns:

- **AWS CloudTrail** is primarily focused on governance, compliance, and operational auditing. It logs all API calls made within your AWS environment. Key features:
  - 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** is a monitoring and observability service that provides data and actionable insights for AWS, on-premises, and hybrid applications and infrastructure. Key features include:
  - 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.

While both services are critical to a robust, secure cloud environment, they differ in their use cases, and the capabilities they offer.

Here's a high-level view of the key differences between these services to get you started.

Category	CloudTrail	CloudWatch
Primary purpose	API activity tracking and auditing	Real-time monitoring and performance management
Data collected	Logs of API calls, including who made the call, when, and what resources were affected	Metrics, logs, and events related to resource performance and application behavior
Use cases	Security auditing, compliance, and tracking changes in the environment	Monitoring resource utilization, setting alarms, and performance management
Security and compliance	Helps meet security and compliance requirements by	Monitors system performance for security anomalies and

Category	CloudTrail	CloudWatch
	providing detailed activity logs	helps maintain operational integrity
Log retention	Last 90 days of event history. Can create trails and event data stores (using CloudTrai l Lake) to keep a record of activity for longer than 90 days.	Short-term data retention for real-time monitoring and troubleshooting
Alarms and notifications	Not primarily used for alarms, but can trigger actions based on API activity	Enables setting alarms for specific metrics or log events, with automated responses
Integration	Often used with security services like AWS Config and IAM for enhanced security management	Integrates with a wide range of AWS services for comprehensive monitoring and automation
Cost considerations	Costs based on the volume of logs generated and stored	Costs based on the number of metrics, logs, and alarms monitored
Data granularity	Provides detailed logs of every API call with granular information	Provides aggregated metrics and log data for real-time monitoring
Access control	Allows you to track access patterns and changes in user permissions	Helps you monitor and optimize access to resources based on performance metrics
Resource coverage	AWS account-wide	Individual AWS resources
Real-time tracking	Near real-time (within 5 minutes)	Real-time or near real-time

Category	CloudTrail	CloudWatch
Visualization	Limited; often used with other tools	Built-in dashboards and graphing

Differences between CloudTrail and CloudWatch

Explore the differences between CloudTrail and CloudWatch in a number of key areas.

Primary purpose

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?"

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?"

Summary

CloudTrail helps you track and audit user activity for security and compliance, while CloudWatch is about monitoring and optimizing system performance and operational health. Both tools serve distinct, yet complementary, roles in managing a cloud environment.

Data collected

AWS 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.

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.

Summary

CloudTrail collects data related to user activity and API usage for auditing and security purposes, while CloudWatch collects metrics and logs to monitor, manage, and optimize system performance and operational health. Both provide critical insights but serve different aspects of cloud management.

Use cases

AWS CloudTrail

- Primarily used for security auditing, compliance, and operational auditing. CloudTrail provides a detailed record of API calls and user activity within your AWS environment, making it essential for tracking changes, investigating security incidents, and ensuring that your organization meets regulatory requirements. For example, 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

- Designed for real-time monitoring, performance management, and operational efficiency. CloudWatch is used to monitor the health of your AWS resources and applications by collecting and tracking metrics, logs, and events. CloudWatch enables you to set alarms that trigger automated actions, such as scaling resources or sending notifications when certain thresholds are met. Use cases for CloudWatch include monitoring application performance, managing resource utilization, detecting anomalies, and ensuring your systems are running optimally to prevent downtime.

Security and compliance

AWS CloudTrail

- Crucial for maintaining security and compliance in AWS environments. CloudTrail provides a comprehensive audit trail of all API calls, including who made the call, when it was made, and the actions taken. This detailed logging is essential for meeting compliance standards, conducting security audits, and investigating incidents. By tracking user activity and changes to resources, CloudTrail helps ensure accountability and transparency, which are key requirements for many regulatory frameworks.

Amazon CloudWatch

- Plays a role in security by enabling the detection of operational anomalies. For example, you can use CloudWatch to monitor metrics that indicate potential security issues, such as unusual spikes in network traffic or CPU usage. Additionally, CloudWatch can trigger alarms and automated responses when certain thresholds are met, allowing for proactive incident management. Logs captured in CloudWatch can also be used to track operational events, which can be vital for understanding the context of security incidents.

Summary

Together, CloudTrail provides the audit logs necessary for compliance, while CloudWatch offers real-time monitoring that helps detect and respond to security threats, contributing to a secure and compliant cloud environment.

Log retention

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.

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

- Primarily focuses on logging API activity and does not have built-in alarm or notification capabilities. However, you can integrate with CloudWatch Logs and CloudWatch alarms to configure alarms for CloudTrail events. This setup is typically used to alert you about security-related events, such as unauthorized access attempts or changes to critical resources.

Amazon CloudWatch

- Specifically designed for real-time monitoring and includes robust alarm and notification features. CloudWatch allows you to set alarms based on metrics, log data, or custom-defined thresholds. When these thresholds are breached, CloudWatch can send notifications via Amazon SNS (Amazon Simple Notification Service), trigger automated actions like scaling instances, or perform custom remediation steps using AWS Lambda. This makes CloudWatch an essential tool for proactive system management, alerting you to performance issues or operational anomalies as they happen.

Integration

CloudTrail and CloudWatch offer extensive integration options with other AWS services and external tools, enhancing their functionality and utility.

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

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

- CloudTrail is priced primarily on the number of events logged and stored. By default, CloudTrail event history records and stores, without charge, the last 90 days of management events for your account. However, if you enable data events (such as S3 object-level actions) or create multiple trails, you incur charges based on the volume of events and the storage required in Amazon S3. Additional costs might arise if you use advanced features like CloudTrail Insights, which provide deeper analysis of unusual API activity.

Amazon CloudWatch

- CloudWatch has a more complex pricing structure based on several factors, including the number of custom metrics you monitor, the number of log events ingested and stored, and the use of alarms and dashboards. Basic monitoring for AWS services is without charge, but detailed monitoring and custom metrics incur charges. Log storage is priced based on the volume of data ingested and retained, with additional costs for setting up and maintaining alarms or using CloudWatch Logs Insights for advanced log analysis.

Data granularity

AWS CloudTrail

- CloudTrail provides high granularity by logging every individual API call made within your AWS environment. Each log entry includes detailed information such as who made the request, the action performed, the resources affected, and the time of the action. This level of detail is crucial for auditing, security monitoring, and compliance, as it allows you to trace specific user actions and changes down to the exact API call.

Amazon CloudWatch

- CloudWatch focuses on aggregated data for monitoring and performance management. It collects metrics at regular intervals (typically every minute or five minutes) and logs operational data from AWS resources. While CloudWatch provides detailed insights into system performance and application behavior, its data is more aggregated compared to CloudTrail. For instance, you can monitor average CPU usage over time rather than individual requests or actions. CloudWatch Logs, however, can provide more granular data similar to CloudTrail but is often used for analyzing operational logs rather than tracking API calls.

Real-time tracking

AWS CloudTrail

- CloudTrail is not inherently designed for real-time tracking but can be configured to provide near-real-time alerts. By default, CloudTrail records API activity, but there is a slight delay in log delivery. For more immediate tracking, you can integrate CloudTrail with Amazon CloudWatch Events or AWS Lambda to trigger actions based on specific API calls or activities as soon as they are logged. This setup allows for near-real-time monitoring of critical security events or configuration changes.

Amazon CloudWatch

- CloudWatch, on the other hand, is built for real-time tracking of system and application performance. It continuously monitors metrics from AWS resources and can instantly trigger alarms or notifications when predefined thresholds are exceeded. CloudWatch also collects and analyzes log data in real-time, enabling you to monitor application logs, detect anomalies, and respond to operational issues as they occur. This makes CloudWatch an essential tool for maintaining the health and performance of your AWS environment in real time.

Use

Now that you've read about the criteria for choosing between AWS CloudTrail and Amazon CloudWatch, you can select the service that meets your needs, and use the following information to help you get started using each of them.

AWS CloudTrail

- **Getting started with AWS CloudTrail**

  AWS CloudTrail is an AWS service that helps you enable operational and risk auditing, governance, and compliance of your AWS account. Here's how to get started with it.

  Explore the guide
- **Review AWS account activity**

  Learn how to review recent AWS API activity in your AWS account using CloudTrail's event history feature.

  Use the tutorial
- **Create a trail**

  Learn how to create a trail to log AWS API activity in all Regions including data and Insights events.

  Use the tutorial
- **Security best practices in AWS CloudTrail**

  This guide provides detective and preventative security best practices for using AWS CloudTrail in your organization.

Explore the guide

Amazon CloudWatch

- **Getting Started with Amazon CloudWatch**

  Monitor your AWS resources and the applications you run on AWS in real time using Amazon CloudWatch. You can use CloudWatch to collect and track metrics, which are variables you can measure for your resources and applications.

  Explore the guide
- **Getting started with Amazon CloudWatch Metrics**

  This guide discusses basic monitoring and detailed monitoring, how to graph metrics, and how to use CloudWatch anomaly detection.

  Explore the guide
- **Set up Container Insights on Amazon EKS and Kubernetes**

  Set up the Amazon CloudWatch Observability ESK add-on and ADTO on your EKS cluster to send metrics to CloudWatch. You will also learn how to set up Fluent Bit or Fluentd to send logs to CloudWatch Logs.

  Explore the guide
- **Getting started with Amazon CloudWatch Application Insights**

  Learn how to use the console to enable CloudWatch Application Insights to manage your applications for monitoring.

  Explore the guide
- **Using Container Insights**

  Learn how CloudWatch Container Insights collects, aggregates, and summarizes metrics and logs from your containerized applications and microservices.

  Explore the guide
- **Setting up Container Insights on Amazon ECS**

Learn to configure cluster and service level metrics, deploy ADOT to collect EC2 instance level metrics, and set up FireLens to send logs to CloudWatch Logs.

Explore the guide

Document history for AWS CloudTrail or Amazon CloudWatch?

The following table describes the important changes to this decision guide. For notifications about updates to this guide, you can subscribe to an RSS feed.

Change	Description	Date
Initial release	Initial release of the decision guide.	September 20, 2024