CloudTrail

Tech Data

INFINITY

13. CloudTrail

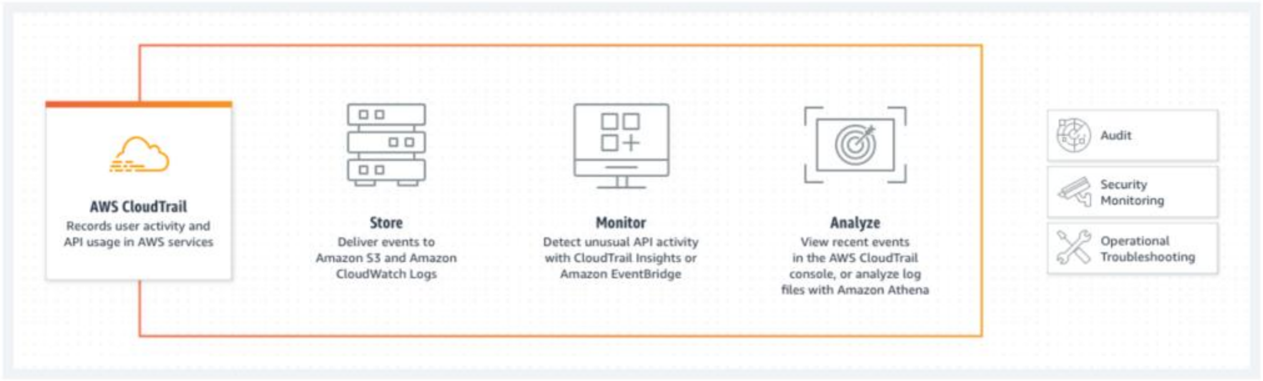
What is AWS CloudTrail?

AWS CloudTrail enables auditing, security monitoring, and operational troubleshooting by tracking user activity and API usage. CloudTrail logs, continuously monitors, and retains account activity related to actions across your AWS infrastructure, giving you control over storage, analysis, and remediation actions.

You should use CloudTrail if you need to audit activity, monitor security, or troubleshoot operational issues.

- AWS CloudTrail is an AWS service that helps you enable governance, compliance, and operational and risk auditing of your AWS account.
- Actions taken by a user, role, or an AWS service are recorded as events in CloudTrail.
- Events include actions taken in the AWS Management Console, AWS Command Line Interface, and AWS SDKs and APIs.
- CloudTrail is enabled on your AWS account when you create it.
- When activity occurs in your AWS account, that activity is recorded in a CloudTrail event.
- You can easily view recent events in the CloudTrail console by going to Event history. For an ongoing record of activity and events in your AWS account, create a trail.

AWS CloudTrail monitors and records account activity across your AWS infrastructure, giving you control over storage, analysis, and remediation actions.


AWS CloudTrail
Records user activity and API usage in AWS services
Store
Deliver events to Amazon S3 and Amazon CloudWatch Logs
Monitor
Detect unusual API activity with CloudTrail Insights or Amazon EventBridge
Analyze
View recent events in the AWS CloudTrail console, or analyze log files with Amazon Athena
Audit
Security Monitoring
Operational Troubleshooting

Benefits of CloudTrail:

CloudTrail helps you prove compliance, improve security posture, and consolidate activity records across regions and accounts. CloudTrail provides visibility into user activity by recording actions taken on your account. CloudTrail records important information about each action, including who made the request, the services used, the actions performed, parameters for the actions, and the response elements returned by the AWS service. This information helps you track changes made to your AWS resources and troubleshoot operational issues. CloudTrail makes it easier to ensure compliance with internal policies and regulatory standards.

Types of Trails:

- **A trail that applies to all regions —**

When you create a trail that applies to all regions, CloudTrail records events in each region and delivers the CloudTrail event log files to an S3 bucket that you specify.

If a region is added after you create a trail that applies to all regions, that new region is automatically included, and events in that region are logged.

Because creating a trail in all regions is a recommended best practice, so you capture activity in all regions in your account, an all-regions trail is the default option when you create a trail in the CloudTrail console.

- **A trail that applies to one region**

When you create a trail that applies to one region, CloudTrail records the events in that region only. It then delivers the CloudTrail event log files to an Amazon S3 bucket that you specify.

Pillars of CloudTrail:

- **Capture** :- capture the activity recorded in the AWS CT events
- **Store** :- store in S3 and CW logs
- **Act**:- Set CW alarms using CW log metrics, send notifications using SNS
- **Review** :- Analyze the logs using AWS CW logs, CT console or CW insights query or any 3rd party compatible software.

CloudTrail records two types of events:

1. Management events that capture control plane actions on resources, such as creating or deleting Amazon Simple Storage Service (Amazon S3) buckets.
2. Data events that capture data plane actions within a resource, such as reading or writing an Amazon S3 object.

1. **Management Events:**

- Management events provide information about management operations that are performed on resources in your AWS account.
- These are also known as control plane operations.
- Example management events include:
- Configuring security (for example, AWS Identity and Access Management AttachRolePolicy API operations).
- Registering devices (for example, Amazon EC2 CreateDefaultVpc API operations).
- Configuring rules for routing data (for example, Amazon EC2 CreateSubnet API operations).
- Setting up logging (for example, AWS CloudTrail CreateTrail API operations).

1. **Data Events:**

- Data events provide information about the resource operations performed on or in a resource.
- These are also known as data plane operations.
- Data events are often high-volume activities.
- The following data types are recorded:
- Amazon S3 object-level API activity (for example, GetObject, DeleteObject, and PutObject API operations) on buckets and objects in buckets
- AWS Lambda function execution activity (the Invoke API)

- Amazon DynamoDB object-level API activity on tables (for example, PutItem, DeleteItem, and UpdateItem API operations)

CloudTrail uses these events in three features:

- Event history provides a 90-day history of control plane actions at no additional cost. As part of its core audit capabilities, CloudTrail provides customer managed keys for encryption and log file validation to enable immutability. You pay only for what you use of the paid features. Some of the following features are provided at no additional charge. No minimum fees or upfront commitments are required.

- CloudTrail Lake is a managed data lake for capturing, storing, accessing, and analyzing user and API activity on AWS for audit and security purposes. You can aggregate, immutably store your activity logs (control plane and data plane) for up to seven years, and query logs within seconds for search and analysis. IT auditors can use CloudTrail Lake as an immutable record of all activities to meet audit requirements. Security administrators can ensure that user activity is in accordance with internal policies, and DevOps engineers can troubleshoot operational issues such as an unresponsive Amazon Elastic Compute Cloud (EC2) instance or a resource being denied access.

- Trails capture a record of AWS account activities, delivering and storing these events in Amazon S3, with optional delivery to Amazon CloudWatch Logs and Amazon Event Bridge. These events can be fed into your security monitoring solutions. You can use your own third-party solutions or solutions such as Amazon Athena for searching and analyzing logs captured by CloudTrail. You can create trails for a single AWS account or for multiple AWS accounts by using AWS Organizations. AWS CloudTrail Insights analyzes control plane events for anomalous behavior in API call volumes, and can detect unusual activity such as spikes in resource provisioning or gaps in periodic activity.