What is AWS CloudTrail?

AWS CloudTrail is an auditing, compliance monitoring, and governance tool from Amazon Web Services (AWS). It's classed as a "Management and Governance" tool in the AWS console.

With CloudTrail, AWS account owners can ensure every API call made to every resource in their AWS account is recorded and written to a log. An API call can be made:

- when a resource is accessed from the AWS console
- when someone runs an AWS CLI command
- when a REST API call is made to an AWS resource

These actions can be coming from:

- Human users (e.g. when someone spins-up an EC2 instance from the console)
- Applications (e.g. when a bash script calls an AWS CLI command)
- another AWS service (e.g. when a Lambda function writes to an S3 bucket)

CloudTrail saves the API events in a secured, immutable format which can be used for later analysis.

In this article, we will learn the basics of AWS CloudTrail, see how to create and enable custom trails, and see where the trail logs are saved. We will also compare CloudTrail with another AWS service: CloudWatch Logs.

Why AWS CloudTrail?

Someone working in DevSecOps can view, search for, or analyze CloudTrail logs to find:

- any particular action that happened in the account
- the time the action happened
- the user or process that initiated the action
- the resource(s) that were affected by the action

Having this kind of visibility can be useful for post security breach reviews, proactive monitoring for account vulnerabilities or ensuring adherence to compliance standards. What's more, events from custom trail events can be used to trigger specific actions.

Is AWS CloudTrail Enabled By Default?

AWS CloudTrail is now enabled for all users by default.

AWS CloudTrail Features

Amazon CloudTrail has a number of features you would expect from a monitoring and governance tool. These features include:

- AWS CloudTrail is “Always On,” enabling you to view data from the most recent 90 days.
- Event History to allow you to see all changes made.
- Multi-region configuration.
- Log file integrity validation and encryption.
- Data events, management events, and CloudTrail Insights.

Amazon CloudTrail Pricing

Amazon CloudTrail pricing is free of charge if you set up a single trail to deliver a single copy of management events in each region. With CloudTrail, you can even download, filter, and view data from the most recent 90 days for all management events at no cost.

Keep in mind Amazon S3 charges will apply based on your usage.

Additionally, you can use AWS CloudTrail Insights by enabling Insights events in your trails. AWS CloudTrail Insights are charged per the number of events in each region. Pricing is as follows:

- Management Events: $2.00 per 100,000 events
- Data Events: $0.10 per 100,000 events
- CloudTrail Insights: $0.35 per 100,000 write management events

CloudTrail Event History

AWS account administrators don’t have to do anything to enable CloudTrail: it’s enabled by default when an account is created. This is the default trail. Information in this trail is kept for the last 90 days in a rolling fashion.