



AWS CloudTrail

Overview

Features

Pricing

Getting Started

Resources

FAQs

Partners

Q: What is AWS CloudTrail?

AWS CloudTrail is a web service that records activity made on your account and delivers log files to your Amazon S3 bucket.

[Show less](#)

Q: What are the benefits of CloudTrail?

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 to track changes made to your AWS resources and to troubleshoot operational issues. CloudTrail makes it easier to ensure compliance with internal policies and regulatory standards. For more details, refer to the AWS compliance white paper "[Security at scale: Logging in AWS](#)".

[Show less](#)

Q: Who should use CloudTrail?

Customers who need to track changes to resources, answer simple questions about user activity, demonstrate compliance, troubleshoot, or perform security analysis should use CloudTrail.



AWS CloudTrail

Overview

Features

Pricing

Getting Started

Resources

FAQs

Partners

Q: Does the CloudTrail Event History show all account activity within my account?

AWS CloudTrail will only show the results of the CloudTrail Event History for the current region you are viewing for the last 90 days and support the AWS services found [here](#). These events are limited to management events with create, modify, and delete API calls and account activity. For a complete record of account activity, including all management events, data events, and read-only activity, you'll need to configure a CloudTrail trail.

[Show less](#)

Q: What search filters can I use to view my account activity?

You can specify Time range and one of the following attributes: Event name, User name, Resource name, Event source, Event ID, and Resource type.

[Show less](#)

Q: Can I use the lookup-events CLI command even if I don't have a trail configured?

Yes, you can visit the [CloudTrail console](#) or use the CloudTrail API/CLI and begin viewing the past 90 days of account activity.

[Show less](#)



AWS CloudTrail

Overview

Features

Pricing

Getting Started

Resources

FAQs

Partners

ability to restrict permissions to view and search account activity. This is accomplished by removing the "cloudtrail:LookupEvents" from the Users IAM policy which will then prevent that IAM user from viewing account activity.

[Show less](#)

Q: Is there any cost associated with CloudTrail Event History being enabled on my account upon creation?

There is no cost for viewing or searching account activity with CloudTrail Event History.

[Show less](#)

Q: Can I turn CloudTrail Event History off for my account?

For any CloudTrail trails that you have created, you can stop logging or delete the trails which will also stop the delivery of account activity to the S3 bucket you had designated as part of your trail configuration as well as delivery to CloudWatch Logs if configured. Account activity for the past 90 days will still be collected and visible within the CloudTrail console and through the AWS CLI.

[Show less](#)



AWS CloudTrail

Overview

Features

Pricing

Getting Started

Resources

FAQs

Partners

[Show less](#)

Q: Where are my log files stored and processed before they are delivered to my Amazon S3 bucket?

Activity information for services with regional end points (EC2, RDS etc.) is captured and processed in the same region as to which the action is made and delivered to the region associated with your Amazon S3 bucket. Action information for services with single end points (IAM, STS, etc.) is captured in the region where the end point is located, processed in the region where the CloudTrail trail is configured and delivered to the region associated with your Amazon S3 bucket.

[Show less](#)

Applying a trail to all regions

Q: What is applying a trail to all regions?

Applying a trail to all regions refers to creating a trail that will record AWS account activity in all regions. This setting also applies to any new regions that are added. For more details on regions and partitions, refer to the [Amazon Resource Names and AWS Service Namespaces page](#).



AWS CloudTrail

Overview

Features

Pricing

Getting Started

Resources

FAQs

Partners

you are using the SDKs or AWS CLI, You set the `IsMultiRegionTrail` to true.

[Show less](#)

Q: What happens when I apply a trail to all regions?

Once you apply a trail in all regions, CloudTrail will create a new trail in all regions by replicating the trail configuration. CloudTrail will record and process the log files in each region and will deliver log files containing account activity across all AWS regions to a single S3 bucket and a single CloudWatch Logs log group. If you specified an optional SNS topic, CloudTrail will deliver SNS notifications for all log files delivered to a single SNS topic.

[Show less](#)

Q: Can I apply an existing trail to all regions?

Yes. You can apply an existing trail to all regions. When you apply an existing trail to all regions, CloudTrail will create a new trail for you in all regions. If you previously created trails in other regions, you can view, edit and delete those trails from the [CloudTrail console](#).

[Show less](#)

Q: How long will it take for CloudTrail to replicate the trail configuration to all regions?



AWS CloudTrail

Overview

Features

Pricing

Getting Started

Resources

FAQs

Partners

Q: What is the benefit of creating multiple trails in an AWS region?

With multiple trails, different stakeholders such as security administrators, software developers and IT auditors can create and manage their own trails. For example, a security administrator can create a trail that applies to all regions and configure encryption using one KMS key. A developer can create a trail that applies to one region for troubleshooting operational issues.

[Show less](#)

Q: Does CloudTrail support resource level permissions?

Yes. Using resource level permissions, you can write granular access control policies to allow or deny access to specific users for a particular trail. For more details, go to CloudTrail [documentation](#).

[Show less](#)

Security and expiration

Q: How can I secure my CloudTrail log files?



AWS CloudTrail

Overview

Features

Pricing

Getting Started

Resources

FAQs

Partners

Q: How long can I store my activity log files?

You control the retention policies for your CloudTrail log files. By default, log files are stored indefinitely. You can use [Amazon S3 object lifecycle management rules](#) to define your own retention policy. For example, you may want to delete old log files or archive them to Amazon Glacier.

[Show less](#)

Event payload, timeliness, and delivery frequency

Q: What information is available in an event?

An event contains information about the associated activity: who made the request, the services used, the actions performed, and parameters for the action, and the response elements returned by the AWS service. For more details, see the [CloudTrail Event Reference](#) section of the user guide.

[Show less](#)

Q: How long does it take CloudTrail to deliver an event for an API call?



AWS CloudTrail

Overview

Features

Pricing

Getting Started

Resources

FAQs

Partners

or new log files.

[Show less](#)

Q: What happens if CloudTrail is turned on for my account but my Amazon S3 bucket is not configured with the correct policy?

CloudTrail log files are delivered in accordance with the S3 bucket policies that you have in place. If the bucket policies are misconfigured, CloudTrail will not be able to deliver log files.

[Show less](#)

Data events

Q: What are Data events?

Data events provide insights into the resource ("data plane") operations performed on or within the resource itself. Data events are often high volume activities and include operations such as Amazon S3 object level APIs and Lambda function invoke API. Data events are disabled by default when you configure a trail. To record CloudTrail data events, you must explicitly add the supported resources or resource types you want to collect activity on. Unlike management events, data events incur additional costs. For more information, see CloudTrail [pricing](#).



AWS CloudTrail

Overview

Features

Pricing

Getting Started

Resources

FAQs

Partners

recorded by CloudTrail.

[Show less](#)

Q: What are AWS Lambda Data Events? How do I record them?

AWS Lambda data events record execution activity of your Lambda functions. With Lambda data events, you can get details on Lambda function executions, such as the IAM user or service that made the Invoke API call, when the call was made, and which function was executed. All Lambda data events are delivered to an Amazon S3 bucket and Amazon CloudWatch Events. You can turn on logging for AWS Lambda data events using the AWS CLI or AWS CloudTrail console and select which Lambda functions get logged by creating a new trail or editing an existing trail.

[Show less](#)

Log file aggregation

Q: I have multiple AWS accounts. I would like log files for all the accounts to be delivered to a single S3 bucket. Can I do that?

Yes. You can configure one S3 bucket as the destination for multiple accounts. For detailed instructions, refer to [aggregating log files to a single Amazon S3 bucket section](#) of the AWS



AWS CloudTrail

Overview

Features

Pricing

Getting Started

Resources

FAQs

Partners

Q: What are the benefits of CloudTrail integration with CloudWatch Logs?

This integration enables you to receive SNS notifications of account activity captured by CloudTrail. For example, you can create CloudWatch alarms to monitor API calls that create, modify and delete Security Groups and Network ACL's.

[Show less](#)

Q: How do I turn on CloudTrail integration with CloudWatch Logs?

You can turn on CloudTrail integration with CloudWatch Logs from the CloudTrail console by specifying a CloudWatch Logs log group and an IAM role. You can also use the AWS SDKs or the AWS CLI to turn on this integration.

[Show less](#)

Q: What happens when I turn on CloudTrail integration with CloudWatch Logs?

After you turn on the integration, CloudTrail continuously delivers account activity to a CloudWatch Logs log stream in the CloudWatch Logs log group you specified. CloudTrail also continues to deliver logs to your Amazon S3 bucket as before.

[Show less](#)

**AWS CloudTrail** ▾[Overview](#)[Features](#)[Pricing](#)[Getting Started](#)[Resources](#)[FAQs](#)[Partners](#)**Q: What charges do I incur once I turn on CloudTrail integration with CloudWatch Logs?**

After you turn on CloudTrail integration with CloudWatch Logs, you incur standard CloudWatch Logs and CloudWatch charges. For details, go to CloudWatch [pricing](#) page.

[Show less](#)

CloudTrail log file encryption using AWS Key Management Service (KMS)

Q: What is the benefit of CloudTrail log file encryption using Server-side Encryption with KMS?

CloudTrail log file encryption using [SSE-KMS](#) allows you to add an additional layer of security to CloudTrail log files delivered to an Amazon S3 bucket by encrypting the log files with a KMS key. By default, CloudTrail will encrypt log files delivered to your Amazon S3 bucket using Amazon S3 server-side encryption.

[Show less](#)

Q: I have an application that ingests and processes CloudTrail log files. Do I need to make any changes to my application?



AWS CloudTrail

Overview

Features

Pricing

Getting Started

Resources

FAQs

Partners

Once you configure encryption using SSE-KMS, you will incur standard AWS KMS charges. For details, go to AWS KMS [pricing](#) page.

[Show less](#)

CloudTrail log file integrity validation

Q: What is CloudTrail log file integrity validation?

CloudTrail log file integrity validation feature allows you to determine whether a CloudTrail log file was unchanged, deleted, or modified since CloudTrail delivered it to the specified Amazon S3 bucket.

[Show less](#)

Q: What is the benefit of CloudTrail log file integrity validation?

You can use the log file integrity validation as an aid in your IT security and auditing processes.

[Show less](#)



AWS CloudTrail

Overview

Features

Pricing

Getting Started

Resources

FAQs

Partners

[Show less](#)

Q: Where are the digest files delivered to?

The digest files are delivered to the same Amazon S3 bucket where your log files are delivered to. However, they are delivered to a different folder so that you can enforce granular access control policies. For details, refer to the digest file structure section of the [CloudTrail documentation](#).

[Show less](#)

Q: How can I validate the integrity of a log file or digest file delivered by CloudTrail?

You can use the AWS CLI to validate that the integrity of log file or digest file. You can also build your own tools to do the validation. For more details on using the AWS CLI for validating the integrity of a log file, refer to the [CloudTrail documentation](#).

[Show less](#)

Q: I aggregate all my log files across all regions and multiple accounts into one single Amazon S3 bucket. Will the digest files be delivered to the same Amazon S3 bucket?

Yes. CloudTrail will deliver the digest files across all regions and multiple accounts into the same Amazon S3 bucket.



AWS CloudTrail

Overview

Features

Pricing

Getting Started

Resources

FAQs

Partners

Q: What functionality does CloudTrail Processing Library provide?

CloudTrail Processing Library provides functionality to handle tasks such as continuously polling a SQS queue, reading and parsing SQS messages, downloading log files stored in S3, parsing and serializing events in the log file in a fault tolerant manner. For more information, go to the [user guide section](#) of the CloudTrail documentation.

[Show less](#)

Q: What software do I need to start using the CloudTrail Processing Library?

You need aws-java-sdk version 1.9.3 and Java 1.7 or higher.

[Show less](#)

Pricing

Q: How do I get charged for AWS CloudTrail?

AWS CloudTrail allows you to view and download the last 90 days of your account activity for create, modify, and delete operations of supported services free of charge.



AWS CloudTrail

Overview

Features

Pricing

Getting Started

Resources

FAQs

Partners

No. The first copy of management events is delivered free of charge in each region.

[Show less](#)

Q: If I enable data events on an existing trail with free management events, will I get charged?

Yes. You will only be charged for the data events. The first copy of management events is delivered free of charge.

[Show less](#)

Partners

Q: How do the AWS partner solutions help me analyze the events recorded by CloudTrail?

Multiple partners offer integrated solutions to analyze CloudTrail log files. These solutions include features like change tracking, troubleshooting, and security analysis. For more information, see the [CloudTrail partners](#) section.

[Show less](#)



AWS CloudTrail

Overview

Features

Pricing

Getting Started

Resources

FAQs

Partners

[Visit the partners page](#)

Ready to build?

[Get started with AWS CloudTrail](#)

Have more questions?

[Contact us](#)

AWS CLOUD PRACTITIONER ESSENTIALS

Learn about AWS fundamentals to get an understanding of the AWS Cloud



WHAT'S NEW WITH AWS

Learn about the latest products, services, and more



[Sign In to the Console](#)



AWS CloudTrail

Overview

Features

Pricing

Getting Started

Resources

FAQs

Partners

[AWS Blog](#)

[Events](#)

[Sustainable Energy](#)

[Press Releases](#)

[AWS in the News](#)

[Analyst Reports](#)

[Legal](#)

Solutions

[Websites & Website Hosting](#)

[Business Applications](#)

[Backup & Recovery](#)

[Disaster Recovery](#)

[Data Archive](#)

[DevOps](#)

[Serverless Computing](#)

[Big Data](#)

[High Performance Computing](#)

[Mobile Services](#)

[Digital Marketing](#)

[Game Development](#)

[Digital Media](#)

[Government & Education](#)

[Health](#)

[Financial Services](#)

[Windows on AWS](#)

[Retail](#)

[Power & Utilities](#)



AWS CloudTrail

Overview

Features

Pricing

Getting Started

Resources

FAQs

Partners

Support Plans

[Service Health Dashboard](#)

[Discussion Forums](#)

[FAQs](#)

[Documentation](#)

[Articles & Tutorials](#)

[Quick Starts](#)

Manage Your Account

[Management Console](#)

[Billing & Cost Management](#)

[Subscribe to Updates](#)

[Personal Information](#)

[Payment Method](#)

[AWS Identity & Access Management](#)

[Security Credentials](#)

[Request Service Limit Increases](#)

[Contact Us](#)

Amazon Web Services is Hiring.

Amazon Web Services (AWS) is a dynamic, growing business unit within Amazon.com. We are currently hiring Software Development Engineers, Product Managers, Account Managers, Solutions Architects, Support Engineers, System Engineers, Designers and more. Visit our [careers](#) page to learn more.

Amazon.com is an Equal Opportunity-Affirmative Action Employer – Minority / Female / Disability / Veteran / Gender Identity / Sexual Orientation.



AWS CloudTrail ▾

- Overview
- Features
- Pricing
- Getting Started
- Resources
- FAQs**
- Partners