**CloudTrail**

## Service Overview

*AWS CloudTrail is a service that enables governance, compliance, operational auditing, and risk auditing of your AWS account. With CloudTrail, you can log, continuously monitor, and retain account activity related to actions across your AWS infrastructure. CloudTrail provides event history of your AWS account activity, including actions taken through the AWS Management Console, AWS SDKs, command line tools, and other AWS services. This event history simplifies security analysis, resource change tracking, and troubleshooting. In addition, you can use CloudTrail to detect unusual activity in your AWS accounts. These capabilities help simplify operational analysis and troubleshooting.*

## Use cases / Considerations

*AWS CloudTrail allows AWS customers to record API calls, sending log files to Amazon S3 buckets for storage. The service provides API activity data including the identity of an API caller, the time of an API call, the source of the IP address of an API caller, the request parameters and the response elements returned by the AWS service.*

*You can get more detailed information from this links:*

*• General overview of CloudTrail* [*https://docs.aws.amazon.com/awscloudtrail/latest/userguide/cloudtrail-user-guide.html*](https://docs.aws.amazon.com/awscloudtrail/latest/userguide/cloudtrail-user-guide.html)

*• Actions covered by CloudTrail* [*https://docs.aws.amazon.com/awscloudtrail/latest/userguide/cloudtrail-concepts.html#cloudtrail-concepts-events*](https://docs.aws.amazon.com/awscloudtrail/latest/userguide/cloudtrail-concepts.html#cloudtrail-concepts-events)

*• CloudTrail supported services* [*https://docs.aws.amazon.com/awscloudtrail/latest/userguide/cloudtrail-aws-service-specific-topics.html*](https://docs.aws.amazon.com/awscloudtrail/latest/userguide/cloudtrail-aws-service-specific-topics.html)

## Cautions

*There are number of limitations in CloudTrail service, that you should know:*

* *You can have only 5 trails per region*
* *You have only 10 transactions per second (TPS) for Get, describe, and list APIs*
* *You have only 2 TPS for LookupEvents API*
* *You have 1 TPS for all other APIs*
* *Limits of Events Selectors are 5 per trail*
* *For all Advanced Event Selectors you have 500 conditions*
* *You can use 250 Data resources in event selectors across all Event Selectors in a trail*
* *Events over 256 KB size can’t be sent to CloudWatch Logs*
* *Event version 1.05 and newer has total event size limit of 256 KB*
* *CloudTrail file size sent to Amazon S3 limited by 50 MB ZIP file, after compression*
* *To view events for Route 53 API requests, you must choose US East (N. Virginia) in the region selector at the top of the console*

*You can get detailed information by this link:*

[*https://docs.aws.amazon.com/awscloudtrail/latest/userguide/WhatIsCloudTrail-Limits.html*](https://docs.aws.amazon.com/awscloudtrail/latest/userguide/WhatIsCloudTrail-Limits.html)

## Pricing considerations

*You can get started with AWS CloudTrail for free ( see* [*https://aws.amazon.com/free/*](https://aws.amazon.com/free/) *for more details about Free Tier ):*

* *Log and search events with Event History AWS CloudTrail logs management events across AWS services by default. You can view, search, and download the most recent 90-day history of your account’s management events for free using CloudTrail in the AWS console or the AWS CLI Lookup API.*
* *Deliver events by creating trails You can deliver one copy of your ongoing management events to Amazon S3 for free by creating trails. This lets you store events in S3 past 90 days.*

*You will pay for:*

* *Deliver additional copies of events and data events by using trails You can deliver additional copies of events, including data events, using trails. Trails can be created for a single AWS account, or for multiple AWS accounts using AWS Organizations. See pricing in the table below.*
* *Identify unusual activity in your account AWS CloudTrail Insights analyzes write management event API calls in your AWS account and detects unusual activity. See pricing in the table below.*

| **Feature** | **Pricing** |
| --- | --- |
| Management events delivered to S3 | First copy of management events is delivered free; additional  copies: $2.00 per 100,000 management events delivered |
| Data events delivered to S3 | $0.10 per 100,000 data events delivered |
| CloudTrail Insights | $0.35 per 100,000 events analyzed |

[*https://aws.amazon.com/cloudtrail/pricing/*](https://aws.amazon.com/cloudtrail/pricing/)

## More details

* CloudTrail using sample

<https://docs.aws.amazon.com/awscloudtrail/latest/userguide/cloudtrail-tutorial.html>

* Creating IAM user and grant him right permissions for using CloudTrail:

[*https://docs.aws.amazon.com/awscloudtrail/latest/userguide/security\_iam\_id-based-policy-examples.html#grant-permissions-for-cloudtrail-administration*](https://docs.aws.amazon.com/awscloudtrail/latest/userguide/security_iam_id-based-policy-examples.html#grant-permissions-for-cloudtrail-administration)