AWS CloudTrail FAQs

aws.amazon.com (https://aws.amazon.com/cloudtrail/faqs/)

General

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.

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 (https://d1.awsstatic.com/whitepapers/aws-security-at-scale-logging-in-aws.pdf)”.

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.

Getting started

Q: If I am a new AWS customer or existing AWS customer and don’t have CloudTrail setup, do I need to enable or setup anything to view my account activity?

No, nothing is required to begin viewing your account activity. You can visit the AWS CloudTrail console (https://console.aws.amazon.com/cloudtrail/) or AWS CLI and begin viewing up to the past 90 days of account activity.

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 (http://docs.aws.amazon.com/awscloudtrail/latest

/userguide/view-cloudtrail-events-supported-services.html). 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.

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.

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 (https://console.aws.amazon.com/cloudtrail/) or use the CloudTrail API/CLI and begin viewing the past 90 days of account activity.

Q: What additional CloudTrail features are available by setting up CloudTrail and creating a trail?

By setting up a CloudTrail trail you can deliver your CloudTrail events to Amazon S3, Amazon CloudWatch Logs, and Amazon CloudWatch Events. This enables you to leverage features to help you archive, analyze, and respond to changes in your AWS resources.

Q: Can I restrict access for users in my account from seeing the CloudTrail Event History?

Yes, CloudTrail integrates with AWS Identity and Access Management (IAM), which allows you to control access to CloudTrail and to other AWS resources that CloudTrail requires, including the 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.

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.

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.

Services and region support

Q: What services are supported by CloudTrail?

AWS CloudTrail records account activity and service events from most AWS services. For the list of supported

services, see CloudTrail Supported Services (http://docs.aws.amazon.com/awscloudtrail/latest/userguide/cloudtrail-supported-services.html) in the *CloudTrail User Guide*.

Q: Are API calls made from the AWS Management Console recorded?

Yes. CloudTrail records API calls made from any client. The AWS Management Console, AWS SDKs, command line tools, and higher level AWS services call AWS APIs, so these calls are recorded.

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.

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 (http://docs.aws.amazon.com/general/latest/gr/aws-arns-and-namespaces.html).

Q: What are the benefits of applying a trail to all regions?

You can create and manage a trail across all regions in the partition in one API call or few clicks. You will receive a record of account activity made in your AWS account across all regions to one S3 bucket or CloudWatch logs log group. When AWS launches a new region, you will receive the log files containing event history for the new region without taking any action.

Q: How do I apply a trail to all regions?

In the CloudTrail console, you select yes to apply to all regions in the trail configuration page. If you are using the SDKs or AWS CLI, You set the IsMultiRegionTrail to true.

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.

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 (https://console.aws.amazon.com/cloudtrail/home).

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

Typically, it will take less than 30 seconds to replicate the trail configuration to all regions.

Multiple trails

Q: How many trails can I create in an AWS region?

You can create up to five trails in an AWS region. A trail that applies to all regions exists in each region and is counted as one trail in each region.

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.

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 (http://docs.aws.amazon.com/awscloudtrail/latest/userguide/grant-custom-permissions-for-cloudtrail-users.html#grant-custom-permissions-for-cloudtrail-users-resource-level%C2%A0).

Security and expiration

Q: How can I secure my CloudTrail log files?

By default, CloudTrail log files are encrypted using S3 Server Side Encryption (SSE) and placed into your S3 bucket. You can control access to log files by applying IAM or S3 bucket policies. You can add an additional layer of security by enabling S3 Multi Factor Authentication (MFA) Delete (http://docs.aws.amazon.com/AmazonS3/latest/dev/MultiFactorAuthenticationDelete.html) on your S3 bucket. For more details on creating and updating a trail, see the CloudTrail documentation (http://docs.aws.amazon.com/awscloudtrail/latest/userguide/setupyourtrail.html).

Q: Where can I download a sample S3 bucket policy and an SNS topic policy?
You can download a sample S3 bucket policy (https://awscloudtrail.s3.amazonaws.com/policy/S3/AWSCloudTrail-S3BucketPolicy-2013-11-01.json) and an SNS topic policy (https://awscloudtrail.s3.amazonaws.com/policy/SNS/AWSCloudTrail-SnsTopicPolicy-2013-11-01.json) from CloudTrail S3 bucket. You need to update the sample policies with your information before you apply them to your S3 bucket or SNS topic.

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 (http://docs.aws.amazon.com/AmazonS3/latest/dev/object-lifecycle-mgmt.html) to define your own retention policy. For example, you may want to delete old log files or archive them to Amazon Glacier.

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 (http://docs.aws.amazon.com/awscloudtrail/latest/userguide/eventreference.html) section of the user guide.

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

Typically, CloudTrail delivers an event within 15 minutes of the API call.

Q: How often will CloudTrail deliver log files to my Amazon S3 bucket?

CloudTrail delivers log files to your S3 bucket approximately every 5 minutes. CloudTrail does not deliver log files if no API calls are made on your account.

Q: Can I be notified when new log files are delivered to my Amazon S3 bucket?

Yes. You can turn on Amazon SNS notifications so that you can take immediate action on delivery of new log files.

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.

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.

Q: How can I consume Data events?

Data events that are recorded by AWS CloudTrail are delivered to S3, similar to management events. Once enabled, these events are also available in Amazon CloudWatch Events.

Q: What are Amazon S3 Data events? How do I record them?

Amazon S3 data events represent API activity on Amazon S3 Objects. To get CloudTrail to record these actions, you specify a S3 bucket in the data events section when creating a new trail or modifying an existing one. Any API actions on the objects within the specified S3 bucket are recorded by CloudTrail.

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.

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 (http://docs.aws.amazon.com/awscloudtrail/latest /userguide/aggregatinglogs.html) of the AWS CloudTrail User Guide.

Integration with CloudWatch Logs

Q: What is CloudTrail integration with CloudWatch Logs?

CloudTrail integration with CloudWatch Logs delivers management and data events captured by CloudTrail to a CloudWatch Logs log stream in the CloudWatch Logs log group you specify.

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.

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.

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.

Q: In which AWS regions is CloudTrail integration with CloudWatch Logs supported?

This integration is supported in the regions where CloudWatch Logs is supported. For more information, see Regions and Endpoints (http://docs.aws.amazon.com/general/latest/gr/rande.html#cwl_region) in the *Amazon Web Services General Reference*.

Q: How does CloudTrail deliver events containing account activity to my CloudWatch Logs?

CloudTrail assumes the IAM role you specify to deliver account activity to CloudWatch Logs. You limit the IAM role to only the permissions it requires to deliver events to your CloudWatch Logs log stream. To review IAM role policy, go to the user guide (http://docs.aws.amazon.com/awscloudtrail/latest/userguide/cw_role_policy.html) of the CloudTrail documentation.

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.

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 (http://docs.aws.amazon.com/AmazonS3/latest/dev/UsingKMSEncryption.html) 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.

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

With SSE-KMS, Amazon S3 will automatically decrypt the log files so that you do not need to make any changes to your application. As always, you need to make sure that your application has appropriate permissions, i.e. Amazon S3 GetObject and KMS Decrypt permissions.

Q: How do I configure CloudTrail log file encryption?

You can use the AWS Management Console, or AWS CLI or the AWS SDKs to configure log file encryption. For detailed instructions, refer to the documentation (http://docs.aws.amazon.com/awscloudtrail/latest/userguide/encrypting-cloudtrail-log-files-with-aws-kms.html).

Q: What charges do I incur once I configure encryption using SSE-KMS?

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

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.

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.

Q: How do I enable CloudTrail log file integrity validation?

You can enable the CloudTrail log file integrity validation feature from the AWS Management Console, AWS CLI or AWS SDKs.

Q: What happens once I turn on the log file integrity validation feature?

Once you turn on the log file integrity validation feature, CloudTrail will deliver digest files on an hourly basis. The digest files contain information about the log files that were delivered to your Amazon S3 bucket, hash values for those log files, digital signatures for the previous digest file, and the digital signature for the current digest file in the Amazon S3 metadata section. For more information about digest files, digital signatures and hash values, go to CloudTrail documentation (http://docs.aws.amazon.com/awscloudtrail/latest/userguide/cloudtrail-log-file-validation-intro.html).

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 (http://docs.aws.amazon.com/awscloudtrail/latest/userguide/cloudtrail-log-file-validation-digest-file-structure.html).

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 (http://docs.aws.amazon.com/awscloudtrail/latest/userguide/cloudtrail-log-file-validation-cli.html).

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 processing library

Q: What is AWS CloudTrail Processing Library?

AWS CloudTrail Processing Library is a Java library that makes it easy to build an application that reads and processes CloudTrail log files. You can download CloudTrail Processing Library from GitHub (https://github.com/aws/aws-cloudtrail-processing-library).

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 (http://docs.aws.amazon.com/awscloudtrail/latest/userguide/using_processing_lib.html) of the CloudTrail documentation.

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.

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.

There is no charge from AWS CloudTrail for creating a CloudTrail trail and the first copy of management events within each region is delivered to the S3 bucket specified in your trail free of charge. Once a CloudTrail trail is setup, Amazon S3 charges apply based on your usage. You will be charged for any data events or additional copies of management events recorded in that region, per the published pricing plan. For example, if you create a multi-region trail and a single-region trail within the same region, you will be charged for a copy of management events recorded in that region.

Q: If I have only one trail with management Events, and apply it to all regions, will I incur charges?

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

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.

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.

Other

Q: Will turning on CloudTrail impact the performance of my AWS resources, or increase API call latency?

No. Turning on CloudTrail has no impact on performance of your AWS resources or API call latency.

Learn more about AWS CloudTrail partners

Visit the partners page
Ready to build?
Get started with AWS CloudTrail (https://console.aws.amazon.com/cloudtrail/home)
Have more questions?
Contact us
Page Content
General Getting started Services and region support Applying a trail to all regions Multiple trails Security and expiration Event payload, timeliness and delivery frequency Data events Log file aggregation Integration with CloudWatch Logs CloudTrail log file encryption using AWS Key Management Service (KMS) CloudTrail log file integrity validation AWS CloudTrail processing library Pricing Partners Other

aws.amazon.com (https://aws.amazon.com/cloudtrail/faqs/)