AWS CloudTrail

Records Account Activity

AWS CloudTrail is enabled on all AWS accounts and is designed to record your account activity upon account creation. You can view, search, and download your recent recorded account activity for create, modify, and delete operations of supported services without the need to manually set up CloudTrail.

Event history

You can view, search, and download your recent recorded AWS account activity. This helps allow you to gain visibility into changes in your AWS account resources so you can strengthen your security processes and simplify operational issue resolution.

Multi-region configuration

You can configure AWS CloudTrail to deliver log files from multiple regions to a single Amazon S3 bucket for a single account. A configuration that applies to all regions is designed to help you ensure that all settings apply consistently across all existing and newly launched regions.

Log file integrity validation

You can validate the integrity of AWS CloudTrail log files stored in your Amazon S3 bucket and detect whether the log files were unchanged, modified, or deleted since CloudTrail delivered them to your Amazon S3 bucket. You can use log file integrity validation in your IT security and auditing processes.

Log file encryption

By default, AWS CloudTrail is designed to encrypt all log files delivered to your specified Amazon S3 bucket using Amazon S3 server-side encryption (SSE). Optionally, you can add a layer of security to your CloudTrail log files by encrypting the log files with your AWS Key Management Service (AWS KMS) key. Amazon S3 is designed to decrypt your log files if you have decrypt permissions.

Data events

By enabling data event logging in CloudTrail, the service is designed to help you record object-level API activity, and receive detailed information such as who made the request, where, when the request was made, and other details. Data events are designed to record the resource operations (data plane actions) performed on or within the resource itself. Data events are often high-volume activities. CloudTrail data event logging is designed to include operations such as Amazon S3 object-level APIs, AWS Lambda function Invoke APIs, and Amazon DynamoDB item-level APIs. For example, you can log API actions on all or specific DynamoDB tables to determine which items were created, read, updated, or deleted.

Management events

Management events provide insights into the management (“control plane”) operations performed on resources in your AWS account. For example, you can log administrative actions such as creation, deletion, and modification of Amazon EC2 instances. For each logged event, you can get details such as the AWS account, IAM user role, and IP address of the user that initiated the action, time of the action, and which resources were affected.

CloudTrail Insights

AWS CloudTrail Insights help you identify unusual activity in your AWS accounts, such as spikes in resource provisioning, bursts of AWS Identity and Access Management (IAM) actions, or gaps in periodic maintenance activity. You can enable CloudTrail Insights events across your AWS organization, or in individual AWS accounts in your CloudTrail trails.

CloudTrail Lake

AWS CloudTrail Lake is an audit and security lake, which helps customers aggregate, store, and query their recorded activity logs for auditing, security investigation, and operational troubleshooting.

Integrations

AWS Lambda

You can take advantage of the Amazon S3 bucket notification feature to direct Amazon S3 to publish object-created events to AWS Lambda. When CloudTrail writes logs to your S3 bucket, Amazon S3 can invoke your Lambda function to process the access records logged by CloudTrail.

Amazon CloudWatch Logs

AWS CloudTrail integration with Amazon CloudWatch Logs helps you to send management and data events recorded by CloudTrail to CloudWatch Logs. CloudWatch Logs allows you to create metric filters to monitor events, search events, and stream events to other AWS services, such as AWS Lambda and Amazon Elasticsearch Service.

Amazon CloudWatch Events

AWS CloudTrail integration with Amazon CloudWatch Events helps you to respond to changes to your AWS resources. With CloudWatch Events, you are able to define actions to execute when specific events are logged by AWS CloudTrail. For example, if CloudTrail logs a change to an Amazon EC2 security group, such as adding a new ingress rule, you can create a CloudWatch Events rule is designed to send send this activity to an AWS Lambda function. Lambda can then help you execute a workflow to create a ticket in your IT Helpdesk system.

Additional Information

For additional information about service controls, security features and functionalities, including, as applicable, information about storing, retrieving, modifying, restricting, and deleting data, please see https://docs.aws.amazon.com/index.html. This additional information does not form part of the Documentation for purposes of the AWS Customer Agreement available at http://aws.amazon.com/agreement, or other agreement between you and AWS governing your use of AWS's services.