**AWS CloudTrail**

* AWS CloudTrail is an AWS service that helps you empower governance, compliance, and operational and inspect auditing of your AWS account. Actions taken by a client, role, or an AWS service are recorded as events in CloudTrail. Events incorporate actions taken in the AWS Management Console, AWS Command Line Interface, and AWS SDKs and APIs.
* CloudTrail is empowered on your AWS account when you make it. At the point when activity occurs in your AWS account, that action is recorded in a CloudTrail occasion. You can without much of a stretch view late occasions in the CloudTrail console by going to Event history. For a progressing record of activity and events in your AWS account, make a trail.
* Visibility into your AWS account activity is a key feature of security and operational best practices. You can utilize CloudTrail to view, search, download, archive, analyze, and react to account activity over your AWS framework.
* You can distinguish who or what made which action, what resources were followed up on when the event occurred, and different details to assist you with analyzing and react to activity in your AWS account. Alternatively, you can enable AWS CloudTrail Insights on a trail to assist you with identify and respond to unusual activity.
* You can integrate CloudTrail into applications utilizing the API, automate trail creation for your organization, check the status of trails you make, and control how clients see CloudTrail events.

**Features**

**Always on**

AWS CloudTrail is enabled on all AWS accounts and records your account activity upon account creation. You can see and download the most recent 90 days of your account activity for creating, modify, and delete methods of supported services without the need to physically set up CloudTrail.

**Event history**

You can view, search, and download your ongoing AWS account activity. This permits you to gain visibility into changes in your AWS account resources so you can strengthen your security forms and simplify operational issue resolution.

**Multi-region configuration**

You can configure AWS CloudTrail to convey log files from various regions to a solitary Amazon S3 bucket for a solitary record. A configuration that applies to all regions guarantees that all settings apply consistently across all current and recently launched regions. For detailed instructions, see Aggregating CloudTrail Log Files to a Single Amazon S3 Bucket in the AWS CloudTrail User Guide.

**Log file encryption**

By default, AWS CloudTrail encrypts all log files delivered to your predetermined Amazon S3 bucket utilizing Amazon S3 server-side encryption (SSE). Optionally, add a layer of security to your CloudTrail log records by encrypting the log files with your AWS Key Management Service (AWS KMS) key. Amazon S3 automatically decrypts your log files if you have to decrypt permissions.

**Log file integrity validation**

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

**Data events**

Data occasions give insights into the resource ("data plane") operations performed on or inside the resource itself. Data events are regularly high volume activities and incorporate operations like Amazon S3 object-level APIs and AWS Lambda function invoke APIs. For instance, you can log API actions on Amazon S3 objects and get detailed information like the AWS account, IAM user role, and IP address of the caller, time of the API call, and various other details. You can likewise record the activity of your Lambda functions, and get details on Lambda function executions, like the IAM client or service that made the Invoke API call, when the call was made, and which function was executed.

**CloudTrail Insights**

Distinguish unusual action in your AWS accounts, like spikes in resource provisioning, explosions of AWS Identity and Access Management (IAM) actions, or spaces in periodic maintenance activity. You can empower CloudTrail Insights events over your AWS organization, or in individual AWS accounts in your CloudTrail trails.

**Management events**

Management events provide insights into the management ("control plane") activities performed on resources in your AWS account. For instance, you can log administrative actions like creation, deletion, and modification of Amazon EC2 instances. For every event, you can get details like the AWS account, IAM user role, and IP address of the client that initiated the event, time of the event, and which resources were affected.

**Integrations**

**AWS Lambda**

You can exploit the Amazon S3 bucket notification feature to coordinate Amazon S3 to distribute 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 empowers you to send the management and data events recorded by CloudTrail to CloudWatch Logs. CloudWatch Logs permits you to make metric filters to monitor events, search events, and stream events to different AWS services, like AWS Lambda and Amazon Elasticsearch Service.

**Amazon CloudWatch Events**

AWS CloudTrail alliance with Amazon CloudWatch Events empowers you to consequently react to changes to your AWS resources. With CloudWatch Events, you can characterize actions to execute when explicit events are logged by AWS CloudTrail. For instance, if CloudTrail logs a change to an Amazon EC2 security group, like including another access rule, you can make a CloudWatch Events rule that sends this activity to an AWS Lambda function. Lambda would then be able to execute a workflow to generate a ticket in your IT Helpdesk system.

**Monitoring**

* Use CloudWatch Logs to monitor log data. CloudTrail events that are sent to CloudWatch Logs can trigger alarms according to the metric filters you define.
* To determine whether a log file was modified, deleted, or unchanged after CloudTrail delivered it, you can use CloudTrail log file integrity validation.

**Price**

* The first copy of management events within each region is delivered free of charge. Additional copies of management events are charged.
* Data events are recorded and charged only for the Lambda functions, DynamoDB tables, and S3 buckets you specify.
* Once a CloudTrail trail is set up, S3 charges apply based on your usage, since CloudTrail delivers logs to an S3 bucket.