Reference:

FAQs

Category:

Management and Governance

AWS CloudTrail

What?

- AWS CloudTrail is an AWS service that helps you enable governance, compliance, and operational and risk auditing of your AWS account. Actions taken by a user, role, or an AWS service are recorded as events in CloudTrail.
- Events include actions taken in the AWS Management Console, AWS Command Line Interface, and AWS SDKs and APIs.

Why?

- CloudTrail helps you prove compliance, improve security posture, and consolidate activity records across regions and accounts. It provides visibility into user activity by recording actions taken on your account.
- CloudTrail makes it easier to ensure compliance with internal policies and regulatory standards.

When?

- You should use CloudTrail if you need to audit activity, monitor security, or troubleshoot operational issues.
- You want to capture and consolidate user activity and API usage across AWS Regions and accounts on a single, centrally controlled platform.

Where?

- Activity information for services with regional end points (EC2, RDS etc.) is captured and processed in the same region as the action is made, and delivered to the region associated with your Amazon S3 bucket.
- You can create two types of trails - A trail that applies to all regions and a trail that applies to one region.

Who?

- CloudTrail is enabled on your AWS account when you create it.
- If you have created an organization in AWS Organizations, you can create a trail that will log all events for all AWS accounts in that organization. Creating an organization trail helps you define a uniform event logging strategy for your organization.

How?

- You can view and search the last 90 days of events recorded by CloudTrail in the CloudTrail console or by using the AWS CLI.
- For an ongoing record of activity and events in your AWS account, create a trail. A trail is a configuration that enables delivery of CloudTrail events to an Amazon S3 bucket, CloudWatch Logs, and CloudWatch Events.

Created by:

Ashish Prajapati

How much?

- You can deliver one copy of your ongoing management events to Amazon S3 for free by creating a trail.
- You can deliver additional copies of events, including data events, using trails. You will be charged for data events or additional copies of management events. Once a CloudTrail trail is set up, Amazon S3 charges apply based on your usage.