AWS Solution Architect Associate Certification Training – Module 22

22. Cloudtrail

Introduction to Cloudtrail

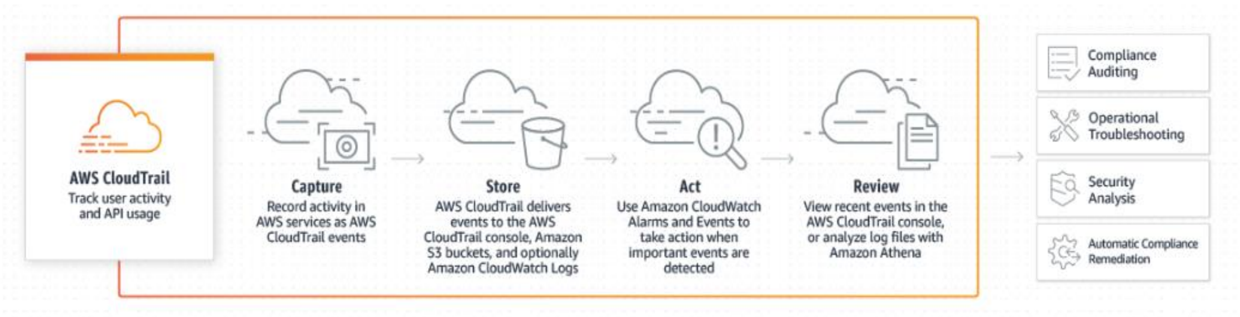
AWS CloudTrail is an AWS service that helps you enable governance, compliance, and operational and risk auditing of your AWS account. Actions taken by a user, role, or an AWS service are recorded as events in CloudTrail. Events include actions taken in the AWS Management Console, AWS Command Line Interface, and AWS SDKs and APIs.CloudTrail is enabled on your AWS account when you create it. When activity occurs in your AWS account, that activity is recorded in a CloudTrail event. You can easily view recent events in the CloudTrail console by going to Event history.

AWS CloudTrail is enabled on all AWS accounts and records your account activity upon account creation. You can view and download the last 90 days of your account activity for create, modify, and delete operations of supported services without the need to manually setup CloudTrail. You can view, search, and download your recent AWS account activity. This allows you to gain visibility into changes in your AWS account resources so you can strengthen your security processes and simplify operational issue resolution. You can configure AWS CloudTrail to deliver log files from multiple regions to a single Amazon S3 bucket for a single account. By default, AWS CloudTrail encrypts all log files delivered to your specified Amazon S3 bucket using Amazon S3 server-side encryption (SSE). Optionally, add a layer of security to your CloudTrail log files by encrypting the log files with your AWS Key Management Service (AWS KMS) key.

Benefits

- ✓ Simplified compliance (automatic recording and saving events)
- ✓ Visibility into user and resource activity
- ✓ Security analysis and trouble shooting (can discover security and operational issues by capturing a comprehensive history of changes that occurred in your AWS account within a specified period of time)
- ✓ Security automation (track and automatically respond to account activity threatening the security of your AWS resources)

How it works


AWS CloudTrail
Track user activity and API usage
Capture
Record activity in AWS services as AWS CloudTrail events
Store
AWS CloudTrail delivers events to the AWS CloudTrail console, Amazon S3 buckets, and optionally Amazon CloudWatch Logs
Act
Use Amazon CloudWatch Alarms and Events to take action when important events are detected
Review
View recent events in the AWS CloudTrail console, or analyze log files with Amazon Athena
Compliance Auditing
Operational Troubleshooting
Security Analysis
Automatic Compliance Remediation

Use cases

- *Compliance AID:* AWS CloudTrail makes it easier to ensure compliance with internal policies and regulatory standards by providing a history of activity in your AWS account
- *Security Analysis:* You can perform security analysis and detect user behavior patterns by ingesting AWS CloudTrail events into your log management and analytics solutions.
- *Data Exfilteration:* You can detect data exfiltration(unauthorized) by collecting activity data on S3 objects through object-level API events recorded in CloudTrail.
- *Operational Issue Troubleshooting:* Can troubleshoot operational issues by leveraging AWS API calls history produced by cloud trail.

For example, you can quickly identify the most recent changes made to resources in your environment, including creation, modification, and deletion of AWS resources (e.g., Amazon EC2 instances, Amazon VPC security groups, and Amazon EBS volumes).