Amazon - CloudTrail

What is CloudTrail?

"AWS CloudTrail is a service that enables governance, compliance, operational auditing, and risk auditing of your AWS account. With CloudTrail, user can log, continuously monitor, and retain account activity related to actions across AWS infrastructure."

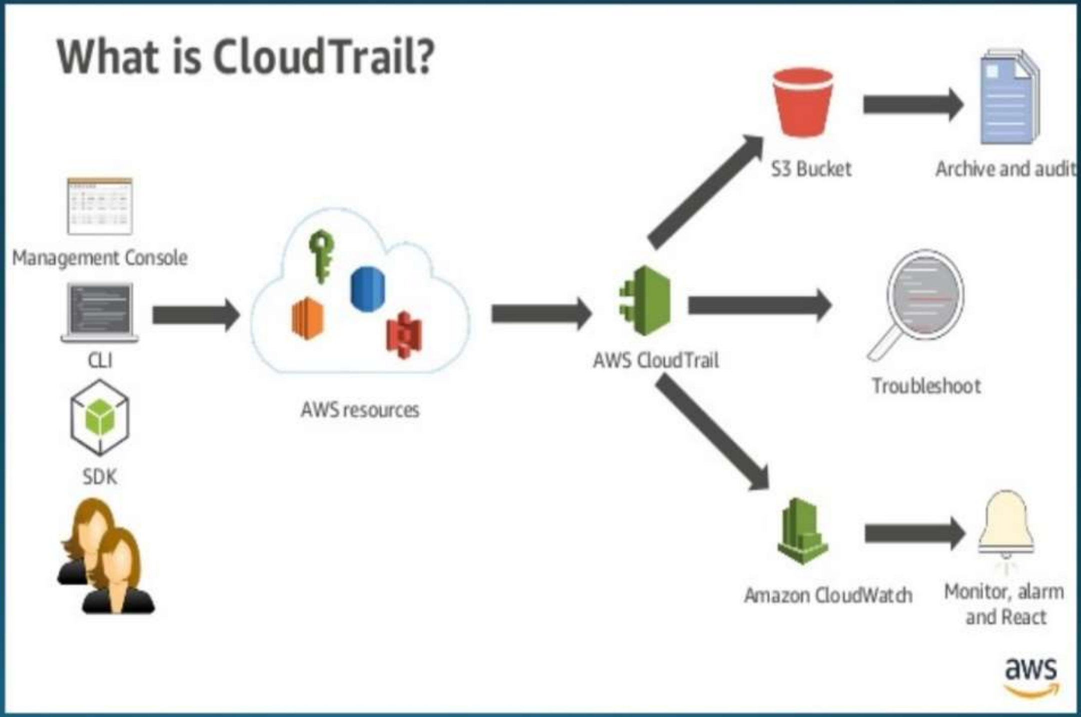
Amazon - CloudTrail

What is CloudTrail?

CloudTrail provides event history of AWS account activity, including actions taken through the AWS Management Console, AWS SDKs, command line tools, and other AWS services.

This event history simplifies

- security analysis.
- resource change tracking.
- troubleshooting.



Amazon - CloudTrail

CloudTrail Benefits

Simplified Compliance:

- With AWS CloudTrail, simplify your compliance audits by automatically recording and storing event logs for actions made within your AWS account.
- Integration with Amazon CloudWatch Logs provides a convenient way to search through log data, identify out-of-compliance events, accelerate incident investigations, and expedite responses to auditor requests.

Visibility into user and resource activity:

- AWS CloudTrail increases visibility into your user and resource activity by recording AWS Management Console actions and API calls.
- You can identify which users and accounts called AWS, the source IP address from which the calls were made, and when the calls occurred.

Amazon - CloudTrail

CloudTrail Benefits

Security Analysis and Troubleshooting:

With AWS CloudTrail, you can discover and troubleshoot security and operational issues by capturing a comprehensive history of changes that occurred in your AWS account within a specified period.

ALWAYS ON:

AWS CloudTrail is enabled on all AWS accounts and records account activity upon account creation.

User can view and download the last 90 days of the account activity for create, modify, and delete operations of supported services without the need to manually setup CloudTrail.

Amazon - CloudTrail

CloudTrail Features

EVENT HISTORY:

User can view, search, and download the recent AWS account activity.

This allows to gain visibility into changes in the AWS account resources

User can strengthen the security processes and simplify operational issue resolution.

LOG FILE ENCRYPTION:

By default, AWS CloudTrail encrypts all log files delivered to the specified Amazon S3 bucket using Amazon S3 server-side encryption (SSE).

Optionally, add a layer of security to CloudTrail log files by encrypting the log files with AWS Key Management Service (AWS KMS) key.

Amazon S3 automatically decrypts log files if user have decrypt permissions.

Amazon - CloudTrail

CloudTrail Features

LOG FILE INTEGRITY VALIDATION:

User can validate the integrity of AWS CloudTrail log files stored in the Amazon S3 bucket and detect whether the log files were unchanged, modified, or deleted since CloudTrail delivered them to the Amazon S3 bucket.

Amazon - CloudTrail

CloudTrail Features

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, AWS Lambda function Invoke APIs, and Amazon DynamoDB item-level APIs

MANAGEMENT EVENTS:

Management events provide insights into the management ("control plane") operations performed on resources in your AWS account.

For each event, user 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.

Web Services

Amazon - CloudTrail

CloudTrail Features

CloudTrail Insights:

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.

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 ensures that all settings apply consistently across all existing and newly launched region

Amazon - CloudTrail

CloudTrail Integration

AWS LAMBDA:

User 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 S3 bucket, Amazon S3 can invoke Lambda function to process the access records logged by CloudTrail.

AMAZON CLOUDWATCH LOGS:

AWS CloudTrail integration with Amazon CloudWatch Logs enables to send management and data events recorded by CloudTrail to CloudWatch Logs.

CloudWatch Logs allows 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 - CloudTrail

Pricing Example

1. The last 90 days and can be viewed and searched free of charge from the AWS CloudTrail console, or by using the AWS CLI.
2. You pay the S3 storage cost for these events, but pay no CloudTrail charges, because the first copy of management events is free.