Cloud Trail

What is CloudTrail?

-AWS CloudTrail is a service that enables governance, compliance, and operational and risk auditing of your AWS account. It records and logs every API call made on your AWS account, capturing details such as the identity of the API caller, the time of the API call, the source IP address, the request parameters, and the response elements returned by the AWS service. This comprehensive logging allows you to track changes and activities across your AWS infrastructure, helping with security analysis, resource change tracking, troubleshooting, and meeting compliance requirements.

-AWS CloudTrail is an auditing, compliance monitoring and governance tool from Amazon Web Services (AWS).

-With CloudTrail, AWS account owners can ensure every API call made to every resource in their AWS account is recorded and written to a log. An API call request can be made when:

-A user accesses a resource from the AWS console

Someone runs an AWS Command Line Interface (AWS CLI).

-A representational state transfer (REST) API call is made to an AWS resource.

Why AWS CloudTrail?

-DevSecOps professionals can view, search for or analyze CloudTrail logs to find:

1. Any particular action that happened in the account
2. The time the action happened
3. The user or process that initiated the action
4. The resource(s) affected by the action

-CloudTrail Lake event data stores and queries incur charges. When you create an event data store, you choose the pricing option you want to use for the event data store. The pricing option determines the cost for ingesting and storing events, and the default and maximum retention period for the event data store. When you run queries in Lake, you pay based upon the amount of data scanned. For information about CloudTrail pricing and managing Lake costs, see AWS CloudTrail Pricing and Managing CloudTrail Lake costs.

CloudTrail channels

-CloudTrail supports two types of channels:

-Channels for CloudTrail Lake integrations with event sources outside of AWS

-CloudTrail Lake uses channels to bring events from outside of AWS into --CloudTrail Lake from external partners that work with CloudTrail, or from your own sources. When you create a channel, you choose one or more event data stores to store events that arrive from the channel source. You can change the destination

event data stores for a channel as needed, as long as the destination event data stores are set to log activity events. When you create a channel for events from an external partner, you provide a channel ARN to the partner or source application. The resource policy attached to the channel allows the source to transmit events through the channel. For more information, see Create an integration with an event source outside of AWS and CreateChannel in the AWS CloudTrail API Reference.

Service-linked channels

-AWS services can create a service-linked channel to receive CloudTrail events on your behalf. The AWS service creating the service-linked channel configures advanced event selectors for the channel and specifies whether the channel applies to all Regions, or the current Region.

-You can use the CloudTrail console or AWS CLI to view information about any CloudTrail service-linked channels created by AWS services.

CloudTrail APIs-----

-In addition to the console and the CLI, you can also use the CloudTrail RESTful APIs to program CloudTrail directly. For more information, see the AWS CloudTrail API Reference and the CloudTrail-Data API Reference.