1. Overview

1. The main objective of CloudTrail is to **monitor the API calls**

2. AWS CloudTrail is **Enabled by Default on your account**. When activity occurs in your AWS account, that activity is recorded in a CloudTrail event.

3. You can easily view recent events in the CloudTrail console by going to **Event history**

4. The default setup will **log 90 days worth of API calls.**

5. AWS CloudTrail is a service **that helps you enable**
    - Governance
    - Compliance
    - Operational auditing
    - Risk auditing of your AWS account

6. With CloudTrail, you can log, continuously monitor, and retain account activity related to actions across your AWS infrastructure.

7 Any actions taken by **a User, Role or AWS Services** are recorded as events in AWS Cloud Trail

8. You can identify who or what took which action, what resources were acted upon, when the event occurred, and other details to help you analyze and respond to activity in your AWS account.

9. Logs every API call to your resources (AWS Console, AWS CLI, SDK)

10. Every interaction with AWS is an API call

11. It can provide information for many types of activities:
    1. Enables governance
    2. Risk Auditing
    3. Operational Auditing
    4. Operational Troubleshooting (Teva, Note **Operational Health** is used to detect by **CloudWatch**)
    5. Security automation
    6. Security Analysis and troubleshooting

7. Automatic Compliance **Remediation** (**Compliance Auditing is done by AWS Config**)
8. Detect data exfiltration (By Collecting Activity data from your S3 bucket)
9. Audit all API calls

11. Trail: Configuration allowing for event logging from **all regions to a single S3 bucket.**

Can also report to CloudWatch Logs for near real-time monitoring and alerting

12. What is **AWS CloudTrail Integrity Validation**?
Use case: Your security team has asked for you to provide a way to validate that AWS CloudTrail log files have not been modified since being placed in the S3 bucket.

Optionally, you can enable **AWS CloudTrail Insights** on a trail to help you identify and respond to unusual activity.

2. How it works

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 events in the CloudTrail console by going to **Event history**.

Event history allows you to view, search, and download the past 90 days of activity in your AWS account

In addition, you can create a CloudTrail trail to archive, analyze, and respond to changes in your AWS resources.

A trail is a configuration that enables delivery of events to an Amazon S3 bucket that you specify.

You can create two types of trails for an AWS account:

A trail that applies to all regions:

When you create a trail that applies to **all regions**, CloudTrail records events in each region and delivers the CloudTrail event log files to an S3 bucket that you specify.

If a region is added after you create a trail that applies to all regions, that new region is automatically included, and events in that region are logged.

Because creating a trail in all regions is a recommended best practice, so you capture activity in all regions in your account, an all-regions trail is the default option when you create a trail in the CloudTrail console.

A trail that applies to one region

When you create a trail that applies to one region, CloudTrail records the events in that region only. It then delivers the CloudTrail event log files to an Amazon S3 bucket that you specify.

Organization trails

If you have created an organization in AWS Organizations, you can also create a trail that will log all events for all AWS accounts in that organization. This is referred to as an *organization trail*.

Organization trails can apply to all AWS Regions or one Region. Organization trails must be created in the **management account**, and when specified as applying to an organization, are automatically applied to all member accounts in the organization.

Member accounts will be able to see the organization trail, but **cannot modify or delete it**. By default, member accounts will not have access to the log files for the organization trail in the Amazon S3 bucket.

Edit Cloud Trail

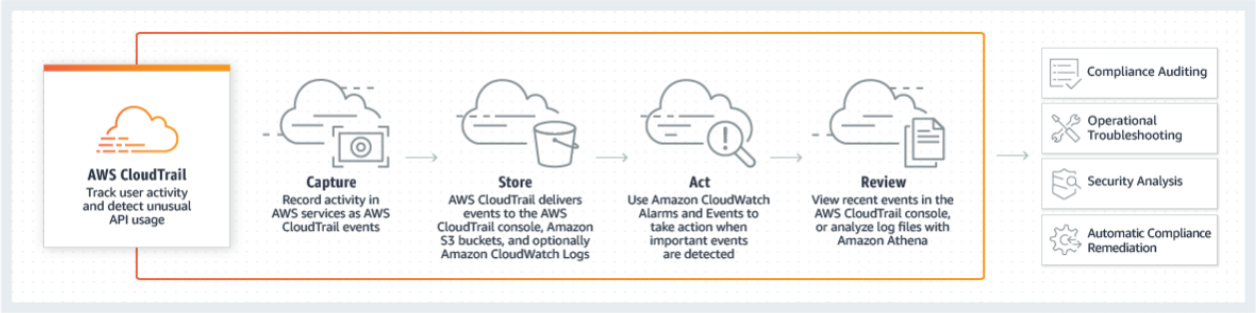
You can change the configuration of a trail after you create it, including whether it logs events in one region or all regions. To change a single-region trail to an all-region trail, or vice-versa, you must run the AWS CLI **update-trail** command.

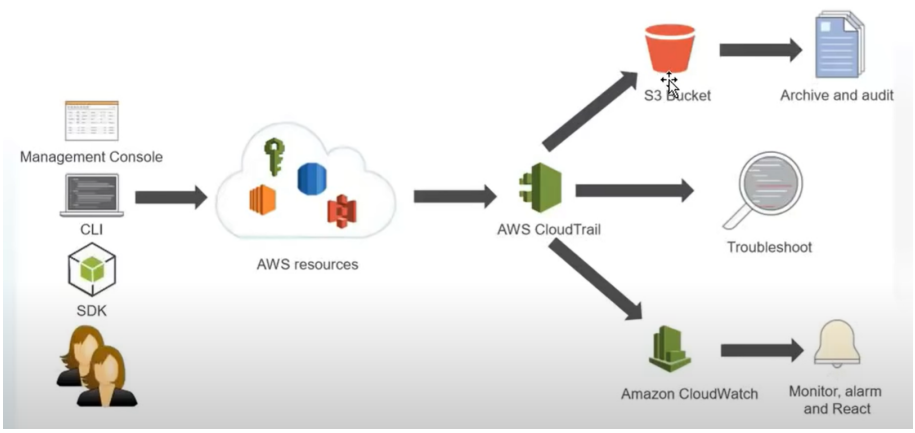
Encryption

By default, CloudTrail event log files are encrypted using Amazon S3 server-side encryption (SSE).
You can also choose to encrypt your log files with an AWS Key Management Service (AWS KMS) key.

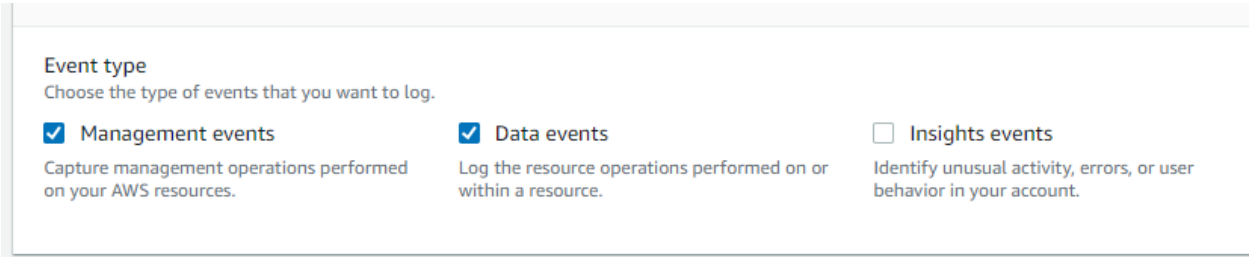
You can store your log files in your bucket for as long as you want. You can also define Amazon S3 lifecycle rules to archive or delete log files automatically.

If you want notifications about log file delivery and validation, you can set up Amazon SNS notifications.





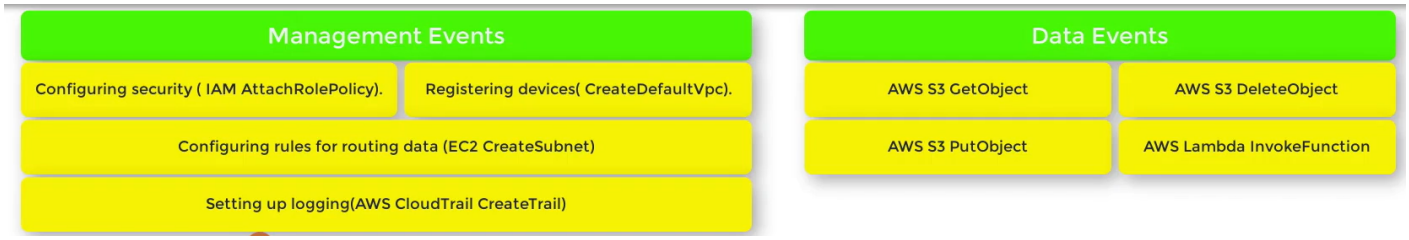
3. CloudTrail Events

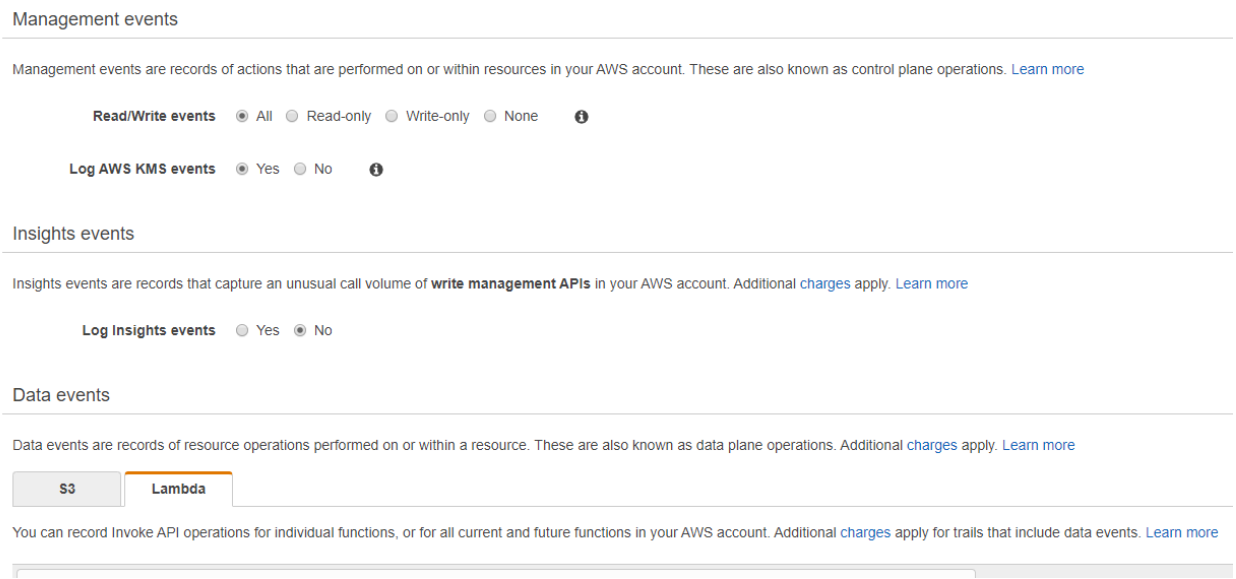


There are 2 types of Events

1. Management Events
2. Data Events

By Default CloudTrail tracks Management Events and **NOT the Data Events**

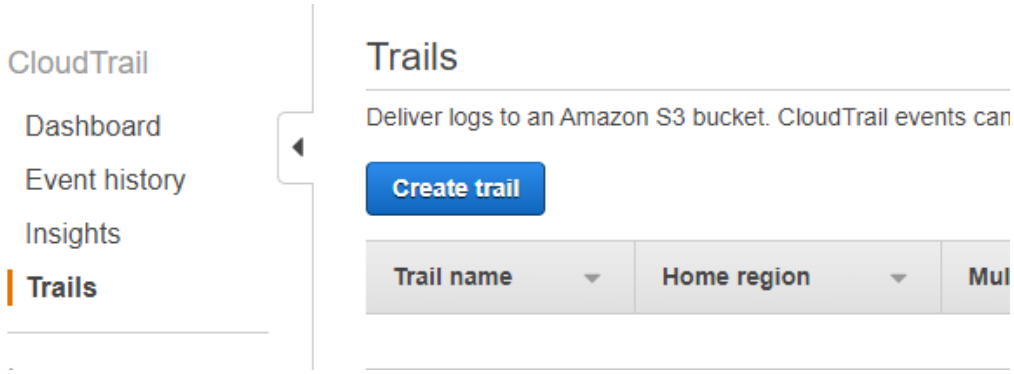




You can view and search the **last 90 days** of events recorded by Cloud Trail in the CloudTrail console:

4. CloudTrail Options

Teva ask yourself what is EventHistoy used for and Insights used for and Trails are used for



5. CloudTrail Logs

By default the CloudTrail logs delivered to the S3 buckets are **encrypted by server side encryption using AWS SSE-S3**
Delivered **every 5 minutes** with upto **15 minutes delay**

CloudTrail Logs have the following:

1. Metadata around API calls
2. The identity of the API caller
3. The time of the API call
4. The **Source IP of the API caller** (TEVA, NOTE THIS IS SOURCE IP and NOT CLIENT IP. IF you need CLIENT IP, you need LOAD BALANCER LOGS)
5. The request parameters
6. The response elements returned by the service
7. Time of the API caller and Request Parameter

You can send the Trail Logs to S3 or CloudWatch Logs

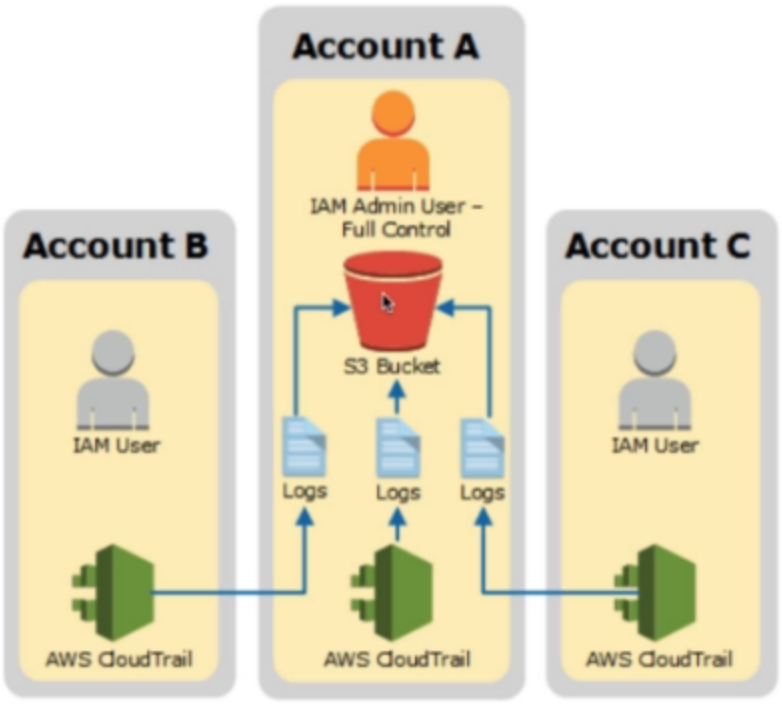
6. CloudTrail Log File Integrity Validation

This provides a way to validate AWS CloudTrail log files that have not been modified since being placed in the S3.

7. Multiple Account CloudTrail Logs

You need to add the other Account in the S3 bucket Policy

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AWSCloudTrailAclCheck20131101",
      "Effect": "Allow",
      "Principal": {
        "Service": "cloudtrail.amazonaws.com"
      },
      "Action": "s3:GetBucketAcl",
      "Resource": "arn:aws:s3:::myBucketName"
    },
    {
      "Sid": "AWSCloudTrailWrite20131101",
      "Effect": "Allow",
      "Principal": {
        "Service": "cloudtrail.amazonaws.com"
      },
      "Action": "s3:PutObject",
      "Resource": [
        "arn:aws:s3:::myBucketName/[optional] myLogFilePrefix/AWSLogs/111111111111/*",
        "arn:aws:s3:::myBucketName/[optional] myLogFilePrefix/AWSLogs/222222222222/*"
      ],
      "Condition": {
        "StringEquals": {
          "s3:x-amz-acl": "bucket-owner-full-control"
        }
      }
    }
  ]
}
```



7. Questions?

How can you configure CloudTrail to support multi-region?
There are 2 methods you can use to configure AWS CloudTrail to support multiregion:

1. Ensure that AWS CloudTrail uses all regions, including new regions that are added. You can select **Yes to apply to all regions** while you are in the trail configuration page.
2. You set **IsMultiRegionTrail** to True if you are using AWS CLI/SDKs/

8. NOTE:

If you login to your EC2 via SSH or RDP to your EC2 then the cloud trail is not going to log that. Since this is not an API call.

9. Digest Delivery time

Digest in Cloud Delivery is generated on an hourly basis. That's why sometimes you can't see if you make any changes in Cloud Trail log data even though you enabled Log File Integrity validation