CloudTrail

Logs API calls between AWS services.
When you need to know who to blame.

Introduction to CloudTrail

AWS CloudTrail is a service that enables **governance**, **compliance**, **operational auditing**, and **risk auditing** of your AWS account.

AWS CloudTrail is used to **monitor API calls** and **Actions** made on an AWS account.

Easily identify which users and accounts made the call to AWS eg.

- **Where** Source IP Address
- **When** EventTime
- **Who** User, UserAgent
- **What** Region, Resource, Action

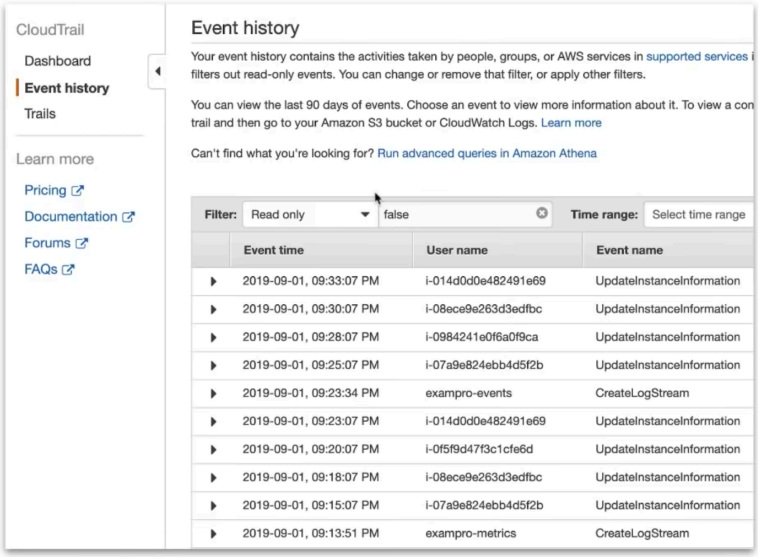

```
{"Records": [{
    "eventVersion": "1.0",
    "userIdentity": {
        "type": "IAMUser",
        "principalId": "EX_PRINCIPAL_ID",
        "arn": "arn:aws:iam::123456789012:user/Worf",
        "accountId": "123456789012",
        "accessKeyId": "EXAMPLE_KEY_ID",
        "userName": "Worf"
    },
    "eventTime": "2014-03-24T21:11:59Z",
    "eventSource": "iam.amazonaws.com",
    "eventName": "CreateUser",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "127.0.0.1",
    "userAgent": "aws-cli/1.3.2 Python/2.7.5 Windows/10",
    "requestParameters": {"userName": "LaForge"},
    "responseElements": {"user": {
        "createDate": "Mar 24, 2014 9:11:59 PM",
        "userName": "LaForge",
        "arn": "arn:aws:iam::123456789012:user/LaForge",
        "path": "/",
        "userId": "EXAMPLEUSERID"
    }}
}]}
```


CloudTrail - Event History

CloudTrail is already logging by default and will collect logs for **last 90 days** via **Event History**

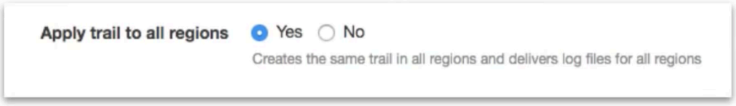
If you need more than 90 days you need to create a **Trail**

Trails are output to S3 and do not have GUI like Event History. To analyze a Trail you'd have to use **Amazon Athena.**

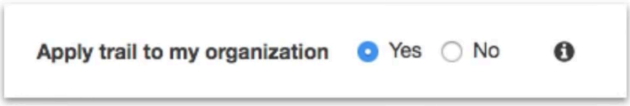


CloudTrail – Trail Options

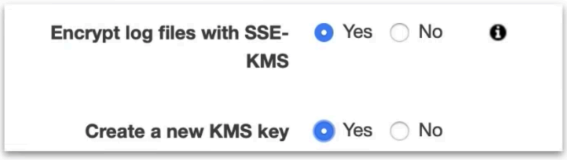
A Trail can be set to **log to all regions**



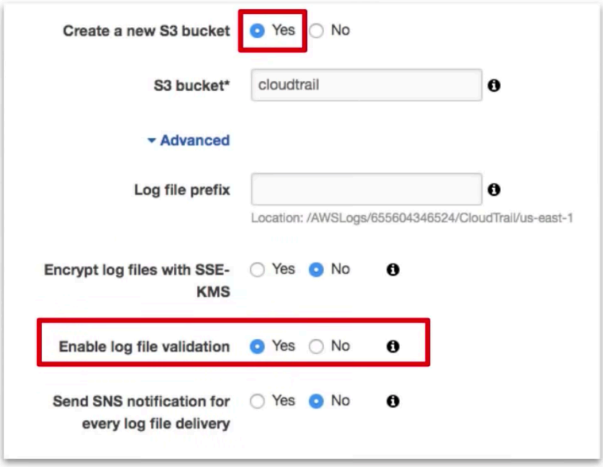
A Trail can be set to **across all accounts in an Organization**



You can **Encrypt your Logs** using Server Side Encryption via Key Management Service (SSE-KMS)

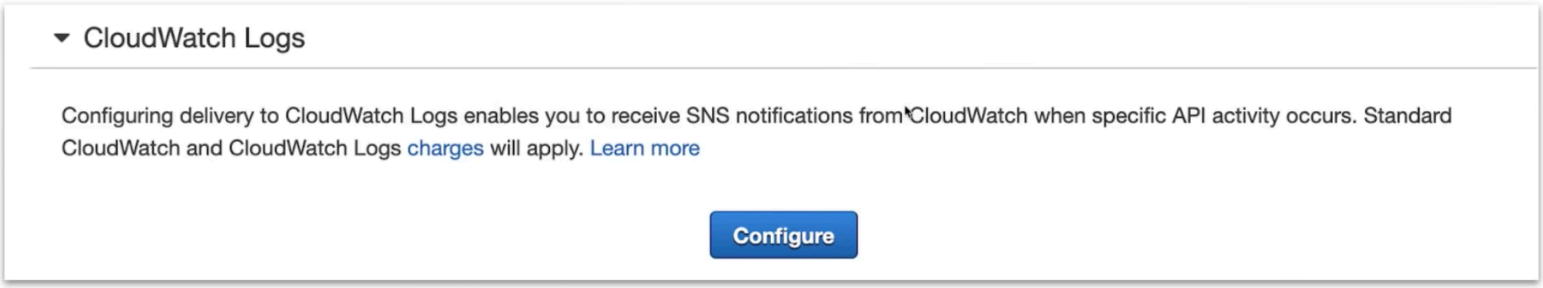


We can ensure the Integrity of our logs to see if they have been tampered we need to turn on **Log File Validation**



CloudTrail to CloudWatch

CloudTrail can be set to deliver events to a CloudWatch log.



CloudTrail – Management Events vs Data Events

Management Events

Tracks management operations. Turned on by default. Can't be turned off.

- **Configuring security**
  eg. IAM AttachRolePolicy API operations
- **Registering devices**
  eg. Amazon EC2 CreateDefaultVpc API operations)
- **Configuring rules for routing data**
  eg. Amazon EC2 CreateSubnet API operations
- **Setting up logging**
  eg. AWS CloudTrail CreateTrail API operations

Data Events

Tracks specific operations for specific AWS Services. Data events are high volume logging and will result in additional charges. **Turned off by default**

The two services that can be tracked is S3 and Lambda. So it would track action such as: GetObject, DeleteObject, PutObject

CloudTrail *CheatSheet*

- CloudTrail logs calls between AWS services
- **governance**, **compliance**, **operational auditing**, and **risk auditing** are keywords relating to CloudTrail
- When you need to know **who to blame** *think* CloudTrail
- CloudTrail by default logs event data for the past 90s days via **Event History**
- To track beyond 90 days you need to create **Trail**
- To ensure logs have not been tampered with you need to turn on **Log File Validation** option
- CloudTrail logs can be encrypted using **KMS (Key Management Service)**
- CloudTrail can be set to log across all AWS accounts in an Organization and all regions in an account.
- CloudTrail logs can be streamed to CloudWatch logs
- Trails are outputted to an S3 bucket that you specify
- CloudTrail logs two kinds of events: **Management Events** and **Data Events**
- **Management events** log management operations eg. AttachRolePolicy
- **Data Events** log data operations for resources (S3, Lambda) eg. GetObject, DeleteObject, and PutObject
- Data Events are **disabled** by default when creating a Trail.
- Trail logs in S3 can be analyzed using Athena