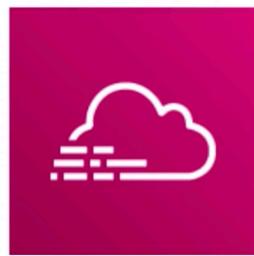


CloudTrail



**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

```
1 {"Records": [
2     "eventVersion": "1.0",
3     "userIdentity": {
4         "type": "IAMUser",
5         "principalId": "EX_PRINCIPAL_ID",
6         "arn": "arn:aws:iam::123456789012:user/Worf",
7         "accountId": "123456789012",
8         "accessKeyId": "EXAMPLE_KEY_ID",
9         "userName": "Worf"
10    },
11    "eventTime": "2014-03-24T21:11:59Z",
12    "eventSource": "iam.amazonaws.com",
13    "eventName": "CreateUser",
14    "awsRegion": "us-east-1",
15    "sourceIPAddress": "127.0.0.1",
16    "userAgent": "aws-cli/1.3.2 Python/2.7.5 Windows/10",
17    "requestParameters": {"userName": "LaForge"},
18    "responseElements": {"user": {
19        "createDate": "Mar 24, 2014 9:11:59 PM",
20        "userName": "LaForge",
21        "arn": "arn:aws:iam::123456789012:user/LaForge",
22        "path": "/",
23        "userId": "EXAMPLEUSERID"
24    }}
25 ]}
```



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

Dashboard

Event history

Trails

Learn more

Pricing ↗

Documentation ↗

Forums ↗

FAQs ↗

Event history

Your event history contains the activities taken by people, groups, or AWS services in supported services. It filters out read-only events. You can change or remove that filter, or apply other filters.

You can view the last 90 days of events. Choose an event to view more information about it. To view a complete trail and then go to your Amazon S3 bucket or CloudWatch Logs. [Learn more](#)

Can't find what you're looking for? [Run advanced queries in Amazon Athena](#)

| Event time | User name | Event name |
|-------------------------|---------------------|---------------------------|
| 2019-09-01, 09:33:07 PM | i-014d0d0e482491e69 | UpdateInstanceInformation |
| 2019-09-01, 09:30:07 PM | i-08ece9e263d3edfbc | UpdateInstanceInformation |
| 2019-09-01, 09:28:07 PM | i-0984241e0f6a0f9ca | UpdateInstanceInformation |
| 2019-09-01, 09:25:07 PM | i-07a9e824ebb4df2b | UpdateInstanceInformation |
| 2019-09-01, 09:23:34 PM | exapro-events | CreateLogStream |
| 2019-09-01, 09:23:07 PM | i-014d0d0e482491e69 | UpdateInstanceInformation |
| 2019-09-01, 09:20:07 PM | i-0f59d47f3c1cfe6d | UpdateInstanceInformation |
| 2019-09-01, 09:18:07 PM | i-08ece9e263d3edfbc | UpdateInstanceInformation |
| 2019-09-01, 09:15:07 PM | i-07a9e824ebb4df2b | UpdateInstanceInformation |
| 2019-09-01, 09:13:51 PM | exapro-metrics | CreateLogStream |



CloudTrail – Trail Options

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

Apply trail to all regions Yes No

Creates the same trail in all regions and delivers log files for all regions

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

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

Apply trail to my organization Yes No (i)

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

Encrypt log files with SSE-KMS Yes No (i)

Create a new KMS key Yes No

Create a new S3 bucket Yes No

S3 bucket* (i)

▼ Advanced

Log file prefix (i)

Location: /AWSLogs/655604346524/CloudTrail/us-east-1

Encrypt log files with SSE-KMS Yes No (i)

Enable log file validation Yes No (i)

Send SNS notification for every log file delivery Yes No (i)

(A)
SUBSCRIBE



CloudTrail to CloudWatch

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

▼ CloudWatch Logs

Configuring delivery to CloudWatch Logs enables you to receive SNS notifications from CloudWatch when specific API activity occurs. Standard CloudWatch and CloudWatch Logs charges will apply. [Learn more](#)

[Configure](#)



SUBSCRIBE



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

▼ Data events

Data events are logs of resource operations performed on or within a resource.

S3 Lambda



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 90 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