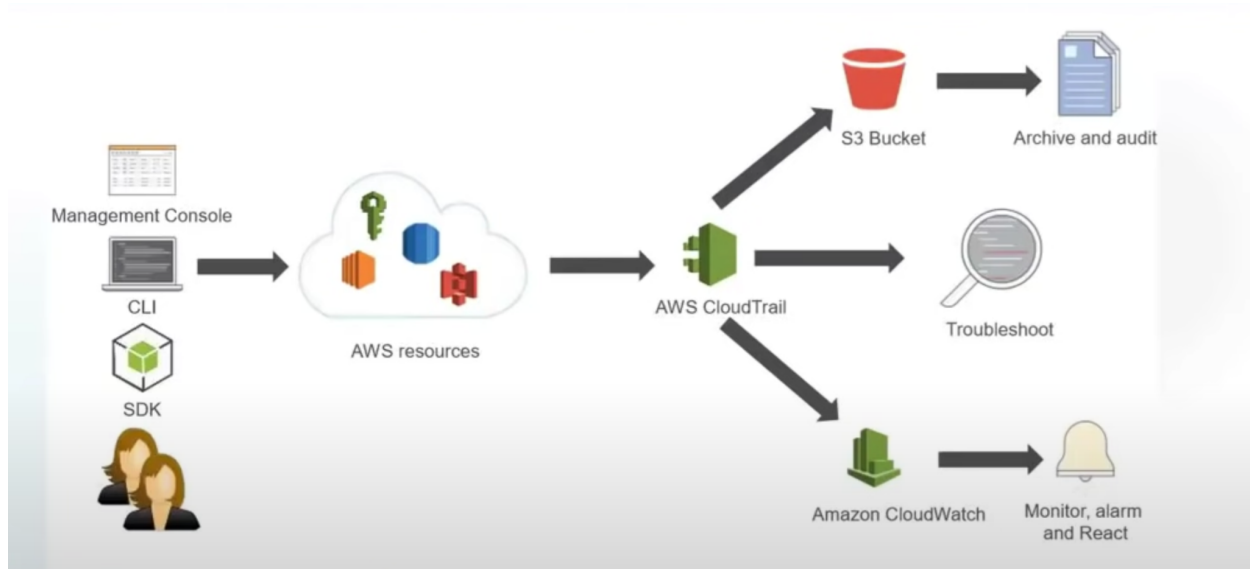


CloudTrail

“CloudTrail enables auditing (inspection, who is doing what, why, when, etc), security monitoring, and operational troubleshooting by tracking user activity and AWS API usage (for e.g, AWS api call to create an EC2 instance, who made this api call?, when?, etc). CloudTrail logs, continuously monitors, and retains account activity related to actions across your AWS infrastructure, giving you control over storage, analysis, and remediation actions.”



Whenever an AWS api call is made, cloudtrail records all the details (request information + response information) of that API call and can deliver the logs to S3, cloudwatch, etc for auditing, monitoring, alarms, reactions, etc. The log files contains the access key of the caller, sourceIP address of the caller, request parameters, time of the api call, response details, etc

Cloudtrail can save events of the last 90 days, you can also store them in s3, and cloudwatch if you need them for a longer time.

Steps to store CloudTrail log files in S3 bucket

- Create a trail

CloudTrail > Dashboard > Create trail

Step 1
Choose trail attributes

Step 2
Choose log events

Step 3
Review and create

Choose trail attributes

General details

A trail created in the console is a multi-region trail. [Learn more](#)

Trail name
Enter a display name for your trail.

3-128 characters. Only letters, numbers, periods, underscores, and dashes are allowed.

☐ Enable for all accounts in my organization
To review accounts in your organization, open AWS Organizations. [See all accounts](#)

Storage location [Info](#)

☒ **Create new S3 bucket**
Create a bucket to store logs for the trail.

☐ **Use existing S3 bucket**
Choose an existing bucket to store logs for this trail.

Trail log bucket and folder
Enter a new S3 bucket name and folder (prefix) to store your logs. Bucket names must be globally unique.

Logs will be stored in aws-cloudtrail-logs-006574496183-c581dcf3/AWSLogs/006574496183

Log file SSE-KMS encryption [Info](#)

☒ Enabled

Customer managed AWS KMS key

☒ New

☐ Existing

- **Management events** (All those events that perform CRUDs on AWS resources for e.g, creating EC2, deleting S3, etc)

Management events

Management events provide insights into the management operations that are performed on resources in your AWS account.

[Learn more](#)

Read/Write events ☒ All ☐ Read-only ☐ Write-only ☐ None 

- **Data events** (Once the S3, Lambda are created, they get triggered multiple times for e.g, insertion in S3 is a data event, execution of lambda after creation is also a data event, etc. But, getting a list of S3, Lambda OR creation of S3 and Lambda are management events) In short, → Events performed inside of a resource like S3, Lambda are called data events (Currently only S3 and Lambda data events are supported by AWS)


Data events

Data events provide insights into the resource operations performed on or within a resource. Additional charges apply. [Learn more](#)

S3

Lambda

You can record S3 object-level API activity (for example, GetObject and PutObject) for individual buckets, or for all current and future buckets in your AWS account. Additional charges apply. [Learn more](#)

| Showing 0 of 0 resources | | | | |
|--|--------|--|---|--|
| Bucket name | Prefix | Read | Write | |
| <input type="checkbox"/> Select all S3 buckets in your account  | | <input checked="" type="checkbox"/> Read | <input checked="" type="checkbox"/> Write | |

Management events

Management events provide insights into the management ("control plane") operations performed on resources in your AWS account. For example, CloudTrail delivers management events for API calls such as launching Amazon EC2 instances or creating Amazon S3 buckets. Management events are enabled by default when you configure a trail and record supported activity at the account level. The first copy of management events within each region is delivered free of charge. Additional copies of management events are charged **\$2.00 per 100,000 events**.

Data events

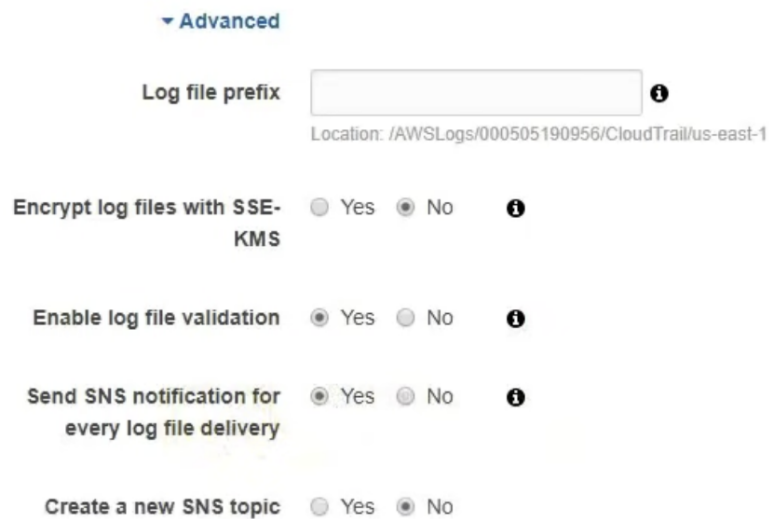
Data events provide insights into the resource ("data plane") operations performed on or within the resource itself. Data events are often high volume activities and include operations such as Amazon S3 object level APIs and Lambda function invoke API. For example, CloudTrail delivers data events for AWS Lambda Invoke API calls and Amazon S3 object level APIs such as Get, Put, Delete and List actions. Data events are recorded only for the Lambda functions and S3 buckets you specify and are charged at **\$0.10 per 100,000 events**.

- **Integrity**

Log validation allows us to validate the logs files. It means, it protects and makes sure that no modification is done by any outsider to the log files. **Digest file** are created and stored which helps us in checking if the log files are modified or not using the following AWS cli command,

```
aws cloudtrail validate-logs --trail-arn
arn:aws:cloudtrail:<REGION_HERE>:<ACCOUNT_NUMBER_HERE>:trail/<TRAIL_NAME_HERE> --start-time <timestamp for e.g 2015-09-24T00:00:00z>
--region=<REGION_HERE>
```

- SNS notifications can also be sent when an event is triggered.



The screenshot shows the 'Advanced' settings section of the AWS CloudTrail console. It includes the following options:

- Log file prefix:** A text input field with a placeholder box and an information icon. Below it, the location is specified as `/AWSLogs/000505190956/CloudTrail/us-east-1`.
- Encrypt log files with SSE-KMS:** Radio buttons for 'Yes' and 'No', with 'No' selected and an information icon.
- Enable log file validation:** Radio buttons for 'Yes' and 'No', with 'Yes' selected and an information icon.
- Send SNS notification for every log file delivery:** Radio buttons for 'Yes' and 'No', with 'Yes' selected and an information icon.
- Create a new SNS topic:** Radio buttons for 'Yes' and 'No', with 'No' selected.

- AWS will automatically update the log bucket policy (allowing it to store log files inside the bucket) when the bucket is integrated with cloudtrail to forward/store log files.
- Cloudtrail stores log files in separate folders for each region, each month, each year in the same S3 bucket.

- There are some AWS partners (AlertLogic, Boundary, CloudCheckr, DataDog, GrayLog2, LogEntries, Splunk, SumoLogic, etc) who have developed some visualization tools that can consume/ingest these cloudtrail log files and can give meaningful information in the form of graphs, charts, etc.

OR

We can use AWS cloudwatch to monitor meaningful information from cloudtrail logs and can also generate alarms, react using it.

CloudWatch Logs - optional
Configure CloudWatch Logs to monitor your trail logs and notify you when specific activity occurs. Standard CloudWatch and CloudWatch Logs charges apply. [Learn more](#)

CloudWatch Logs [Info](#)

☒ Enabled

Log group [Info](#)

☒ New
☐ Existing

Log group name

aws-cloudtrail-logs-006574496183-9e7c0fed

1-512 characters. Only letters, numbers, dashes, underscores, forward slashes, and periods are allowed.

IAM Role [Info](#)

AWS CloudTrail assumes this role to send CloudTrail events to your CloudWatch Logs log group.

☒ New
☐ Existing

Role name

CloudTrailRoleForCloudWatchLogs_{trail-name}

[► Policy document](#)

- Security

“Always store cloudtrail logs of one account in a S3 bucket of another AWS accounts because if one account is compromised, you can see all the activities of the compromised account from the S3 bucket of another account”

Steps:



1. Create a bucket in the first account.
2. In the first account, give S3 bucket permission to the second account to write log files in it by creating a policy manually.

```
6      "Effect": "Allow",
7      "Principal": {
8        "Service": "cloudtrail.amazonaws.com"
9      },
10     "Action": "s3:GetBucketAcl",
11     "Resource": "arn:aws:s3:::ki3"
12   },
13   {
14     "Sid": "AWSCloudTrailWrite20150319",
15     "Effect": "Allow",
16     "Principal": {
17       "Service": "cloudtrail.amazonaws.com"
18     },
19     "Action": "s3:PutObject",
20     "Resource": [
21       "arn:aws:s3:::ki3/AWSLogs/000505190956/*",
22       "arn:aws:s3:::ki3/AWSLogs/758233867720/*"
23     ]
24   }
25 }
```

See last two lines of the above image. The first line is allowing the same account to write cloudtrail logs to the same account (Ki3) bucket and the second line is also allowing to write logs of cloudtrail **but of another account on the same S3 bucket resource** (this can be verified by the different account number mentioned in the last line starting from 758....)

3. Create a trail in the second account and select “existing bucket” and provide name of the bucket of the first account (created in step # 1).
4. Create a trail in your second account.
5. After the creation, In the S3 bucket of the first account, you will see two different folders for 2 different account numbers having their own logs in different regions, months, etc.

Viewing 1 to 2

| <input type="checkbox"/> | Name ▼ | Last modified ▼ | Size ▼ | Storage class ▼ |
|--------------------------|--|-----------------|--------|-----------------|
| <input type="checkbox"/> |  00050514256 | -- | -- | -- |
| <input type="checkbox"/> |  758233867720 | -- | -- | -- |

Viewing 1 to 2

- Pricing

- One trail per region is free means the **management events inside your first trail in a region are completely free** but for **data events you will have to pay**.
- If you have more than 1 trail in your region, then you will have to **pay for the management events** of the other trails as well.