CloudTrail

AWS CloudTrail is an application program interface (API) call-recording and log-monitoring Web service offered by Amazon Web Services (AWS).

AWS CloudTrail allows AWS customers to record API calls, sending log files to Amazon S3 buckets for storage. The service provides API activity data including the identity of an API caller, the time of an API call, the source of the IP address of an API caller, the request parameters and the response elements returned by the AWS service.

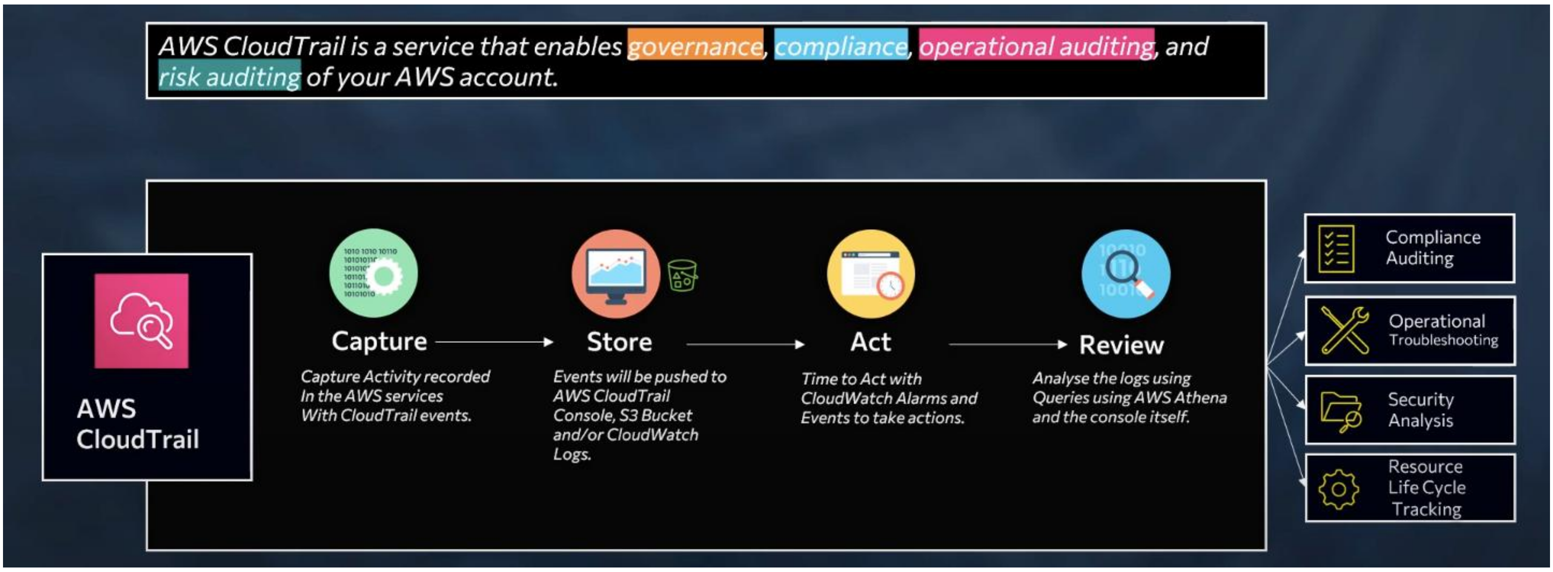
CloudTrail can be configured to publish a notification for each log file delivered, allowing users to take action upon log file delivery -- a process that according to AWS should only take about 15 minutes. It can also be configured to aggregate log files across multiple accounts so that log files are delivered to a single S3 bucket.

The service can facilitate regulatory compliance reporting for organizations that use AWS and need to track the API calls for one or more AWS account. CloudTrail can also be configured to support security information (SIEM) and event management platforms and and resource management.

OR

AWS CloudTrail is an auditing, compliance monitoring, and governance tool from Amazon Web Services (AWS). It's classed as a "Management and Governance" tool in the AWS console.
Basically CloudTrail is a log of all actions that have taken place inside your AWS environment.

How it Works?



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

Capture Activity recorded In the AWS services With CloudTrail events.

Events will be pushed to AWS CloudTrail Console, S3 Bucket and/or CloudWatch Logs.

Time to Act with CloudWatch Alarms and Events to take actions.

Analyse the logs using Queries using AWS Athena and the console itself.

Following are the steps in which Cloud trail works:

1. Capture
2. Store
3. Act
4. Review

CloudTrail: “Who did what on AWS?”   or Who is doing What ? and the API calls to the service or resource.

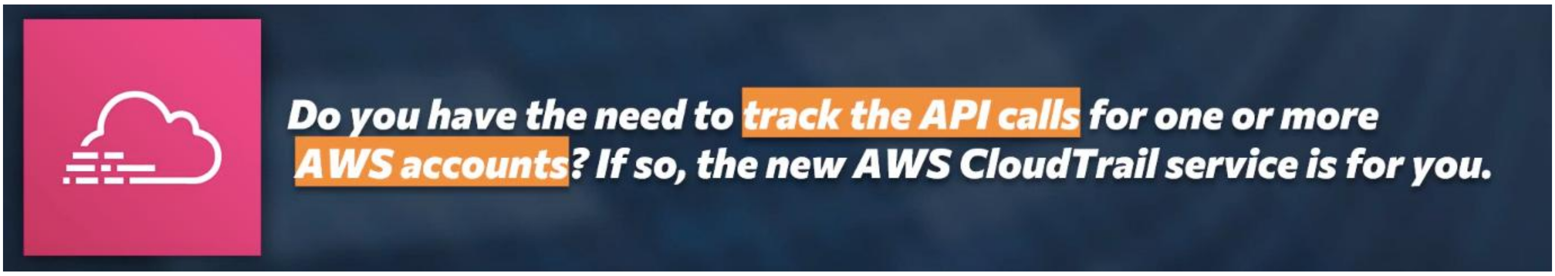
With CloudTrail, AWS account owners can ensure every API call made to every resource in their AWS account is recorded and written to a log. An API call can be made:

- when a resource is accessed from the AWS console
- when someone runs an AWS CLI command
- when a REST API call is made to an AWS resource

These actions can be coming from:

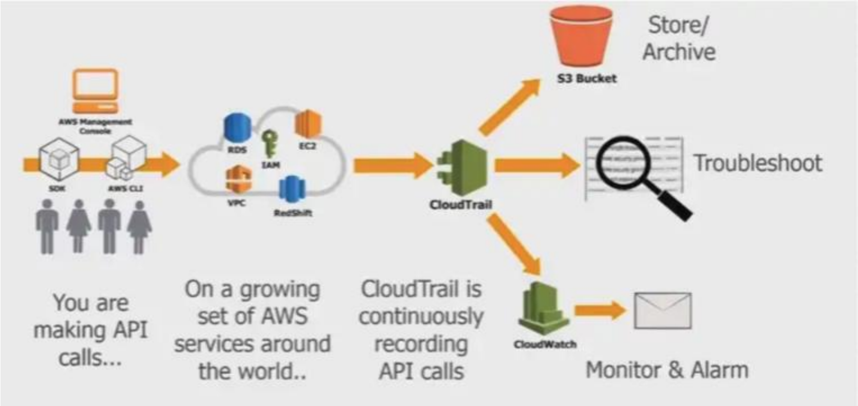
- Human users (e.g. when someone spins-up an EC2 instance from the console)
- Applications (e.g. when a bash script calls an AWS CLI command)
- another AWS service (e.g. when a Lambda function writes to an S3 bucket)

CloudTrail saves the API events in a secured, immutable format which can be used for later analysis.

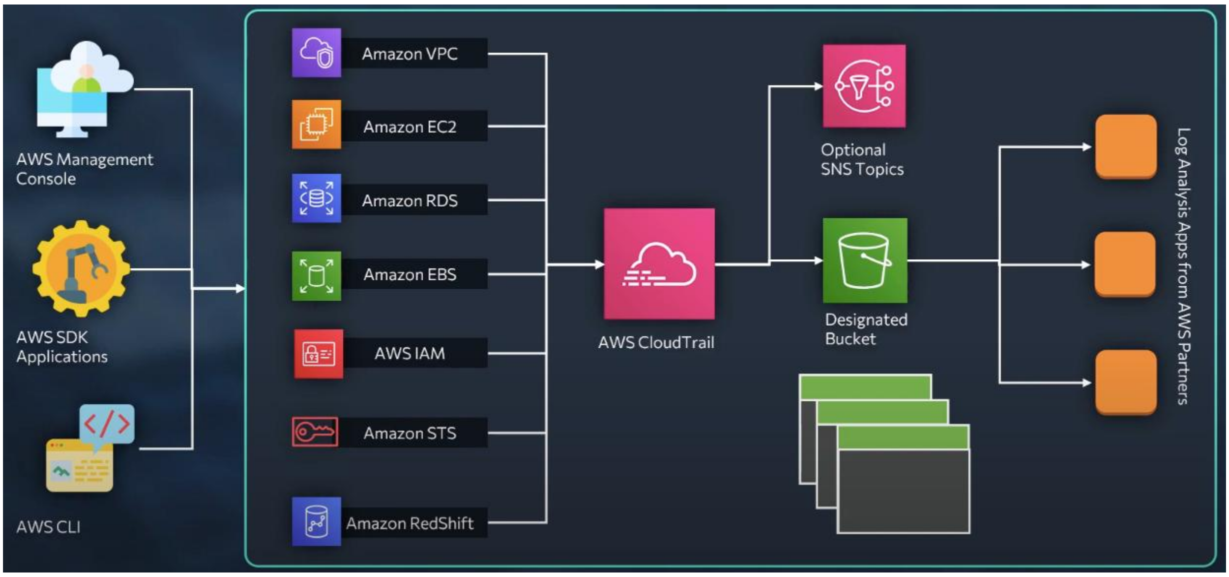

Do you have the need to track the API calls for one or more AWS accounts? If so, the new AWS CloudTrail service is for you.

Every Action that going to be take place it will be monitor by CloudTrail.

AWS CloudTrail


AWS Management Console
SDK
AWS CLI
RDS
EC2
IAM
VPC
RedShift
CloudTrail
S3 Bucket
Store/ Archive
Troubleshoot
CloudWatch
You are making API calls...
On a growing set of AWS services around the world..
CloudTrail is continuously recording API calls
Monitor & Alarm

,



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

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

CloudTrail provides event history of your AWS account activity, including actions taken through the AWS Management Console, AWS SDKs, command line tools, and other AWS services.

This event history simplifies security analysis, resource change tracking, and troubleshooting.

Why AWS CloudTrail?

Someone working in DevSecOps can view, search for, or analyze CloudTrail logs to find:

- any particular action that happened in the account?
- the time the action happened?
- the user or process that initiated the action?
- the resource(s) that were affected by the action?

Having this kind of visibility can be useful for post security breach reviews, proactive AWS monitoring for account vulnerabilities or ensuring adherence to compliance standards. What’s more, events from custom trail events can be used to trigger specific actions.

Is AWS CloudTrail Enabled By Default?

AWS CloudTrail is now enabled for all users by default.

What you can analyze with CloudTrail Data?

- What actions did a given user take over a specific time period?
- For a given resource, which AWS user has take action on it over a given time period?
- What is the source IP address of a particular activity?

What You Can Answer?

- Who Made the API call?
- When was the API call made?
- What was the API call?
- Which resources were acted up on in the API call?
- Where was the API call made from and made to?

AWS CloudTrail Features

Amazon CloudTrail has a number of features you would expect from a monitoring and governance tool. These features include:

- Always on/Event History:AWS CloudTrail is enabled on all AWS Accounts you to view data from the most recent 90 days , and records your activity upon account creation.Keep track of what’s going on with the insights you get with data.
- Event History to allow you to see all changes made.
- Multi-region configuration:Using aggregating log file in S3, with CloudTrail, you can get logs from multiple regions to a single Amazon S3 bucket from a single account.
- Log file integrity validation /encryption:With SHA-256 for hashing and SHA-256 with RSA for digital Signing, CloudTrail makes it secure enough that the logs can never be edited without detection. Use SSE and KMS Encryption.
- CloudTrail Insights:Identify unusual activity in your aws accounts, such as spikes in resource provisioning, bursts of AWS Identity and Access Management(IAM) actions or gaps in periodic maintenance activity.

Few CloudTrail Partners:

- 2nd Watch
- Alert Logic
- Boundary
- Stack Driver
- Splunk
- SumoLogic
- CloudCheckr
- DataDog
- Graylog2
- LogEntries

Amazon CloudTrail Pricing

Amazon CloudTrail pricing is free of charge if you set up a single trail to deliver a single copy of management events in each region. With CloudTrail, you can even download, filter, and view data from the most recent 90 days for all management events at no cost. Keep in mind Amazon S3 charges will apply based on your usage.

There's no charge for CloudTrail you will pay the usual S3 and SNS Charges to store the data and to receive the notification.

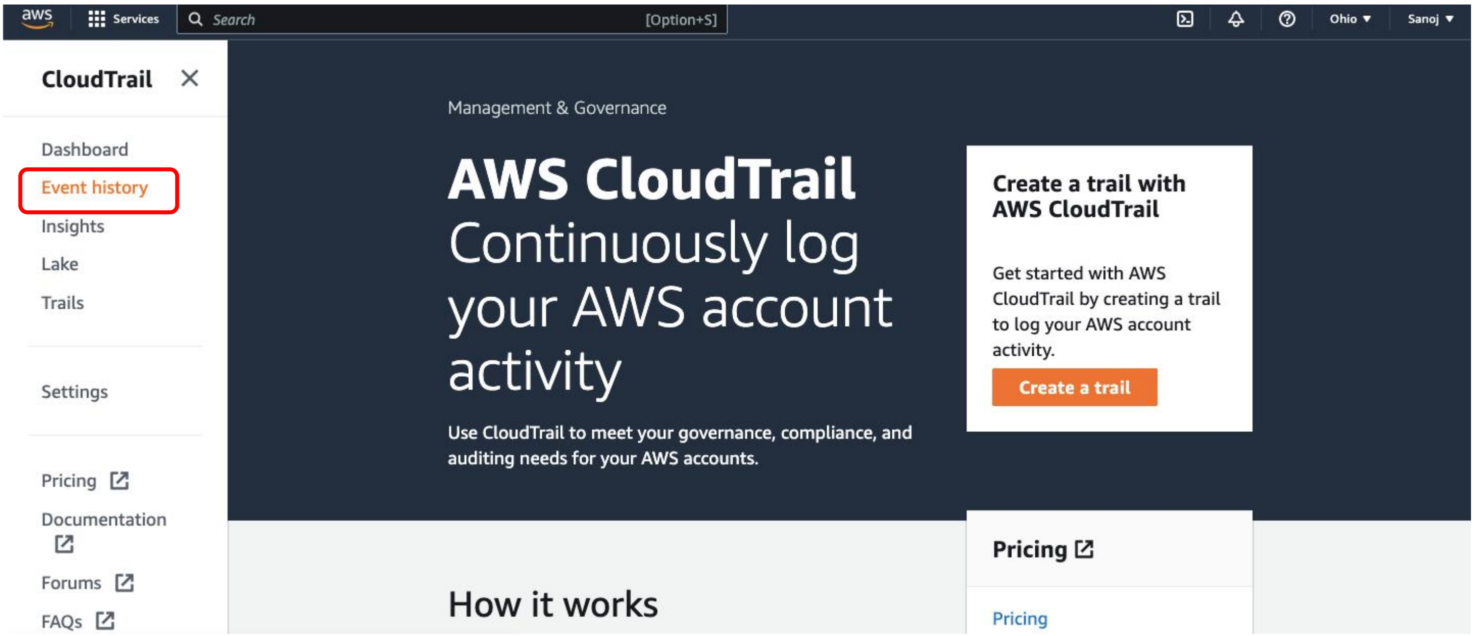
Additionally, you can use AWS CloudTrail Insights by enabling Insights events in your trails. AWS CloudTrail Insights are charged per the number of events in each region. Pricing is as follows:

- Management Events: $2.00 per 100,000 events
- Data Events: $0.10 per 100,000 events
- CloudTrail Insights: $0.35 per 100,000 write management events

CloudTrail Event History

AWS account administrators don't have to do anything to enable CloudTrail: it's enabled by default when an account is created. This is the default trail. Information in this trail is kept for the last 90 days in a rolling fashion.

To view the default trail, we can open the CloudTrail console, and choose "Event history" from the navigation pane:


aws
Services
Search
[Option+S]
Ohio ▾
Sanoj ▾
CloudTrail
Dashboard
Event history
Insights
Lake
Trails
Settings
Pricing
Documentation
Forums
FAQs
Management & Governance
AWS CloudTrail
Continuously log your AWS account activity
Use CloudTrail to meet your governance, compliance, and auditing needs for your AWS accounts.
Create a trail with AWS CloudTrail
Get started with AWS CloudTrail by creating a trail to log your AWS account activity.
Create a trail
Pricing
Pricing
How it works

From the event history, it's possible to choose a date range, a particular resource type or resource name, event name, AWS access key ID and other filters to narrow down the search.

Before Creating A cloud Trail Lets understand the some key points.

Key Terms Definition:

- Log Events : There are 3 types of log events
  - ✓ Management Events:Management events capture actually management events such as API usage that are performed on AWS resources in your AWS Account like who logged in ,and what time, who signed in those types of API calls, management events are set aws by default.

  - ✓ Data Events: (*Charge Able)This shows resource operations on resources or within resources such as when a user has uploaded a file on S3 buckets,did it delete it or when it downloaded these type of operation.

  - ✓ Insights Events:(*Charge Able) It helps to identify and responds unusual activity associated with right API Calls, so basically it helps identify pattern base behaviour activity changes with a API calls made in the aws account which appears be unusual in nature.

- Trail name: A trail name is a unique identifier that you can assign to a CloudTrail Configuration.The name you choose for a trail is used to distinguish it from other trails that you might create in your AWS account.

  - ✓ A Trail name serves as a label for the configuration and the data that is recorded and stored.Its used to organize and Identify different trails within your account and it can be used in various AWS services such as CloudWatch Logs and Amazon S3.

  - ✓ When you create a trail, you can choose a name that is meaningful to you and your organization and it can include up to 128 alphanumeric characters, such as "production-trail" or "finance-trail". Once a name is assigned to a trail, it can't be changed its name, but you can stop or delete the trail, and then create a new one with a different name.

- Storage location: refers to the location where the logs file generated by CloudTrail are stored. By default , CloudTrail stores log files in an S3 bucket that you specify when you create or update a trail.You can also choose to have the log files delivered to an Amazon S3 bucket, an Amazon SNS topic or an AWS lambda function.

  - ✓ When you configure a trail you can specify the S3 bucket where you want CloudTrail to store the log files.This bucket must exist within the same AWS region as the trail, and you must have the necessary permissions to write to the bucket.
  - ✓ Cloud Trail also provides the option to encrypt the log files at rest in the S3 bucket, using either S3-managed encryption keys (SSE-S3) or customer-managed encryption keys (SSE-KMS). This can be specified as part of the S3 bucket policy.

  - ✓ You can also configured CloudTrail to send log files to an Amazon SNS topic, which can then be used to trigger an AWS Lambda function or any other service that can consume an SNS topic.

  - ✓ Alternatively, you can configure CloudTrail to deliver log files to an AWS Lambda functions, where they can be processed in near real-time and trigger custom actions.

  - ✓ CloudTrail stores log files in the target location in a compressed format and they are encrypted while in transit and at rest.

- Trail log bucket and folder: is an Amazon Simple Storage Service(S3) bucket where CloudTrail delivers the log files it generates. The buckets is specified when you create a new trail and can be an existing bucket or a new one.The log files will be delivered to the bucket in a format like "bucket_Name/AWSLogs/Account_ID/CloudTrail/region/yyyy/mm/dd/".

- ✓ A “trail log folder” refers to the subdirectory within the S3 bucket where CloudTrail will deliver the log files. This folder is automatically created by CloudTrail and follows the format of “AWSLogs/account_ID/CloudTrail/region/yyyy/mm/dd/”.

- ✓ It organizes the log files by year, month and day making it easy to find and manage the log files.

- ✓ For example , if the trail name is “ProdTrail”, the trail log bucket is “mylogbucket” and the region is “us-west-2”, the log files would be delivered to the folder “mylogbucket/AWSLogs/1234567890/CloudTrail/us-west-2/yyyy/mm/dd/”

- ✓ It’s worth mentioning that it’s possible to configure the trail to deliver the logs directly to CloudWatch log groups, in this case the logs will be stored in the CloudWatch logs and no need to specify the bucket and folder.

- ➢ Log file SSE-KMS encryption: “log file SSE-KMS encryption” refers to the use of AWS key Management Service (KMS) to encrypt the log files that are stored in an S3 bucket. SSE-KMS(Server-Side-Encryption with AWS KMS-Managed Keys) is a way to encrypt the data in the S3 bucket using a key that is managed by AWS KMS.

  - ✓ When you enable log file SSE-KMS encryption for a CloudTrail, the log files that are delivered to the specified S3 bucket are encrypted using a key that you choose from the KMS. This means that the log files are protected at rest and can only be decrypted by someone who has the access to the key.

  - ✓ Enabling log file SSE-KMS encryption provides an extra layer of security for your CloudTrail log files, and helps ensure that they are not compromised even if the S3 bucket is accessed by unauthorized users.Its important to note that KMS encryption key must be created and owned by the same AWS account that owns the CloudTrail and S3 Bucket.

- ➢ Log file validation: it is a features that allows you to ensure the authenticity and integrity of the log files that CloudTrail records.
  - ✓ When “log file validation” is enabled, CloudTrail will create a digital signature for each log file using a private key,and include the signature in the log file.

  - ✓ When you or someone else retrieves the log file, they can use the corresponding public key to verify the signature and Confirm that the log file has not been tampered with.This way you can ensure that the logs you are viewing haven’t been Altered or manipulated in any way.

- ➢ SNS notification delivery: “SNS notification delivery” refers to the ability to receive notifications when certain events occur in your CloudTrail logs. Amazon Simple notification service(SNS) is a fully managed messaging service that allows you to send messages to one or more recipients, such as email address, phone numbers, or SQS queues.

  - ✓ When you enable SNS notification delivery for a CloudTrail , you can specify an SNS topic to which CloudTrail will send a message whenever a specific events occurs in the logs.For Example you can set up a notification to be sent when a new log file is delivered to the S3 bucket, or when a specific API call is made.

  - ✓ SNS notification can be useful for alerting you when certain events occur in CloudTrail logs, so you can take actions needed.For example , you might set up a notification to be sent when an IAM user is created, so you can review the user’s permissions and make sure they are appropriate.

  - ✓ You can also configure CloudTrail to send the notifications to multiple topics, or to multiple recipients(Phone numbers, email address, SQS queues) using the same topic. This enables you ti have different settings for different use cases.

- CloudWatch Logs: CloudWatch Logs is a service that allows you to monitor, store and access your log files.It enables you to collect and track log events from various AWS resources and custom applications in a centralized location.

    - ✓ When it comes to CloudTrail CloudWatch Logs can be used to store and access the log files generated by CloudTrail.You can create a CloudWatch Logs log group and configure a trail to deliver logs to the log group.

    - ✓ With CloudWatch Logs, you can set up alarms to be triggered based on specific conditions in the logs, and you can use CloudWatch Logs Insights to search and analyze your logs.This can be helpful for troubleshooting and identifying patterns in your CloudTrail logs.

    - ✓ Additionally , you can also use CloudWatch Logs to aggregate logs from multiple trails, this allows you to have a centralized view of all your CloudTrail logs.

    - ✓ It's worth noting that while CloudWatch Logs is a separate service, it's often used in conjunction with CloudTrail to provide additional functionality and insights into your AWS environment.

- API Activity: API activity in CloudTrail refers to the logging of events related to API calls made to AWS services.This includes information about the caller, the service being called, the parameters passed to the service, and the response returned by the service.This information can be used to track and troubleshoot issues, monitor for security-related events, and comply with regulatory requirements.

Creating a Trail:

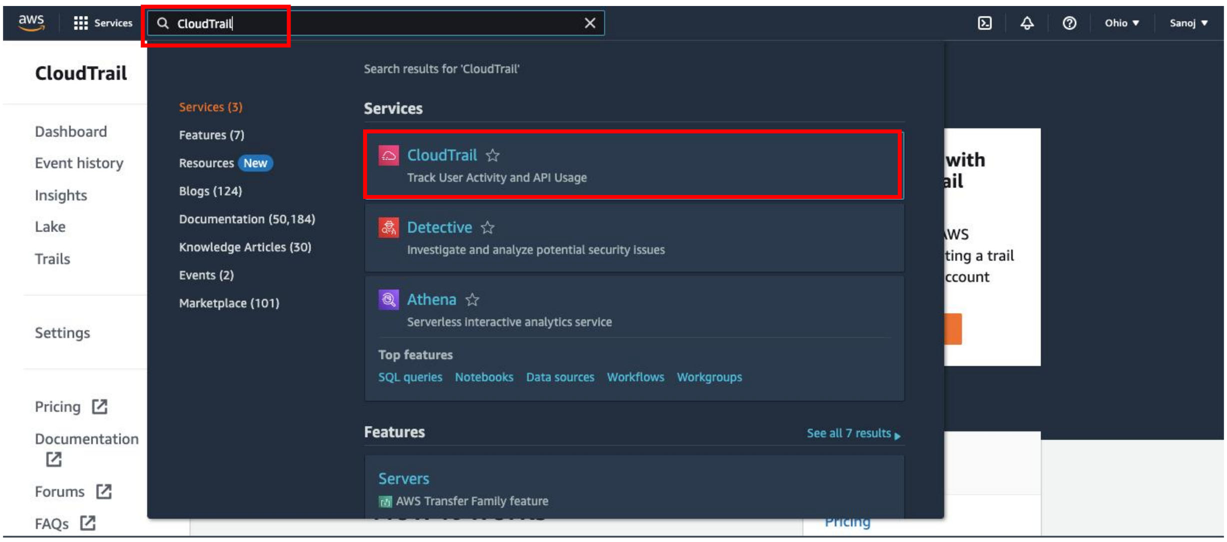
- It's also possible to create custom trails. A trail is a user-created audit definition that can capture one or more types of events. Unlike Event history, CloudTrail trail logs are not limited to 90 days retention.

- They can be delivered to an S3 bucket or to AWS CloudWatch Logs and configured to send SNS notifications when a particular event happens.

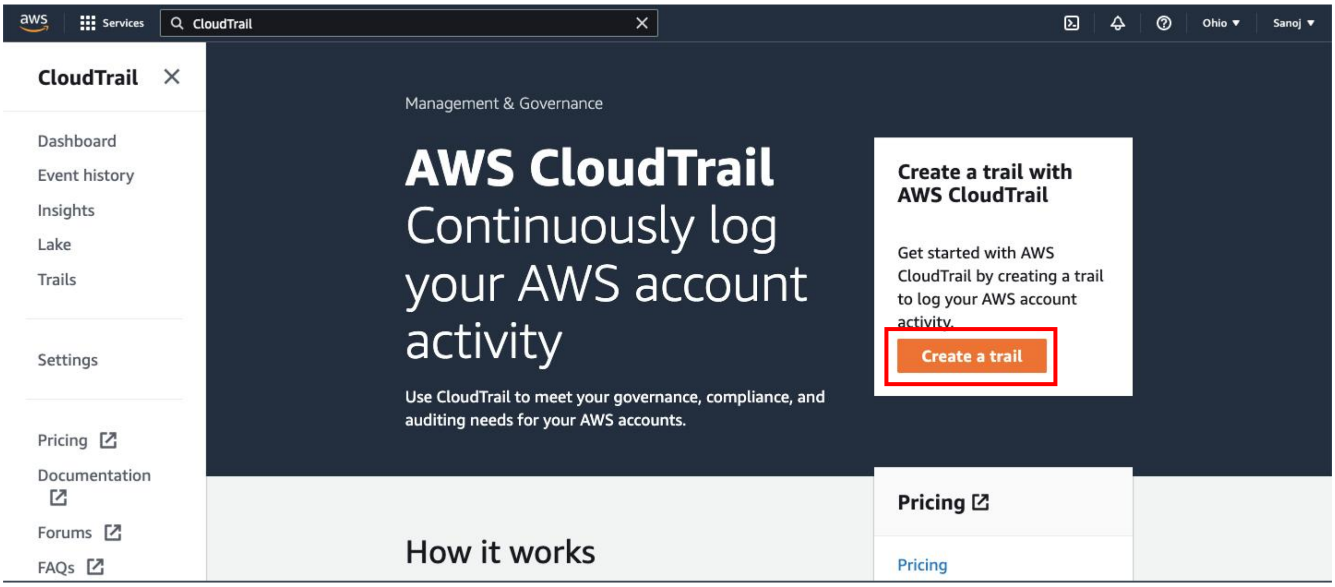
By default multi-region trail created when you create a Trail

Step1: Go to the AWS Console and search cloudTrail and hit enter.

https://us-east-2.console.aws.amazon.com/cloudtrail/home?region=us-east-2#/



Step2: After hitting Enter you will see below interface click on **"create a trail"**



Management & Governance

AWS CloudTrail Continuously log your AWS account activity

Use CloudTrail to meet your governance, compliance, and auditing needs for your AWS accounts.

Create a trail with AWS CloudTrail

Get started with AWS CloudTrail by creating a trail to log your AWS account activity.

Create a trail

Pricing

Pricing

How it works

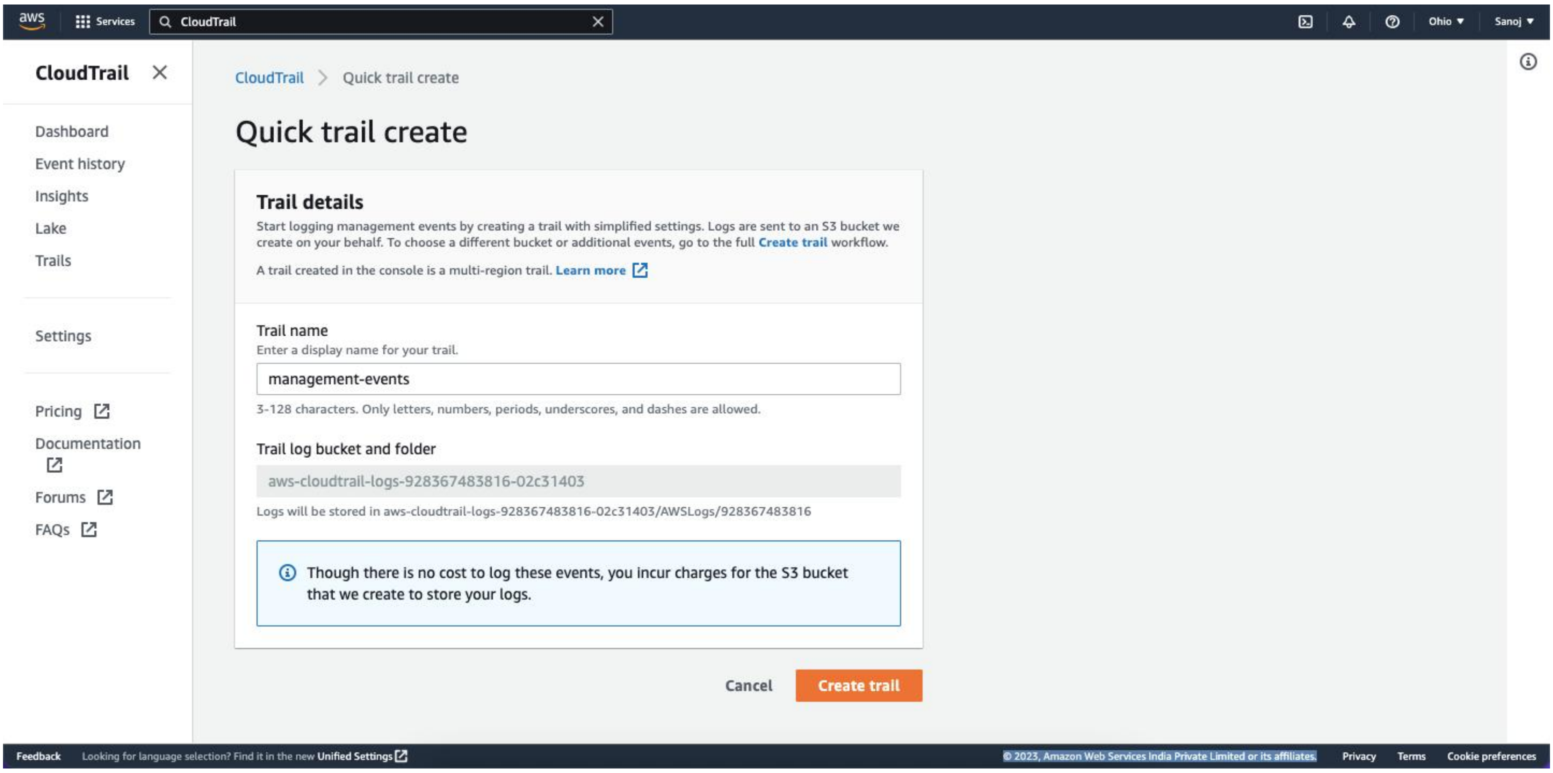
Step3: Once you click on "create a trail" you will see following interface.

There are two methods to create a trail.

1. You can use default way in which just put your cloud trail name and S3 bucket automatically created by AWS.
2. You can use Create trail workflow in which you can select your own S3 bucket and some custom

Default Way to create:

You can give your own Trail Name or you can use default name.



Quick trail create

Trail details

Start logging management events by creating a trail with simplified settings. Logs are sent to an S3 bucket we create on your behalf. To choose a different bucket or additional events, go to the full Create trail workflow.

A trail created in the console is a multi-region trail. Learn more

Trail name
Enter a display name for your trail.
management-events
3-128 characters. Only letters, numbers, periods, underscores, and dashes are allowed.

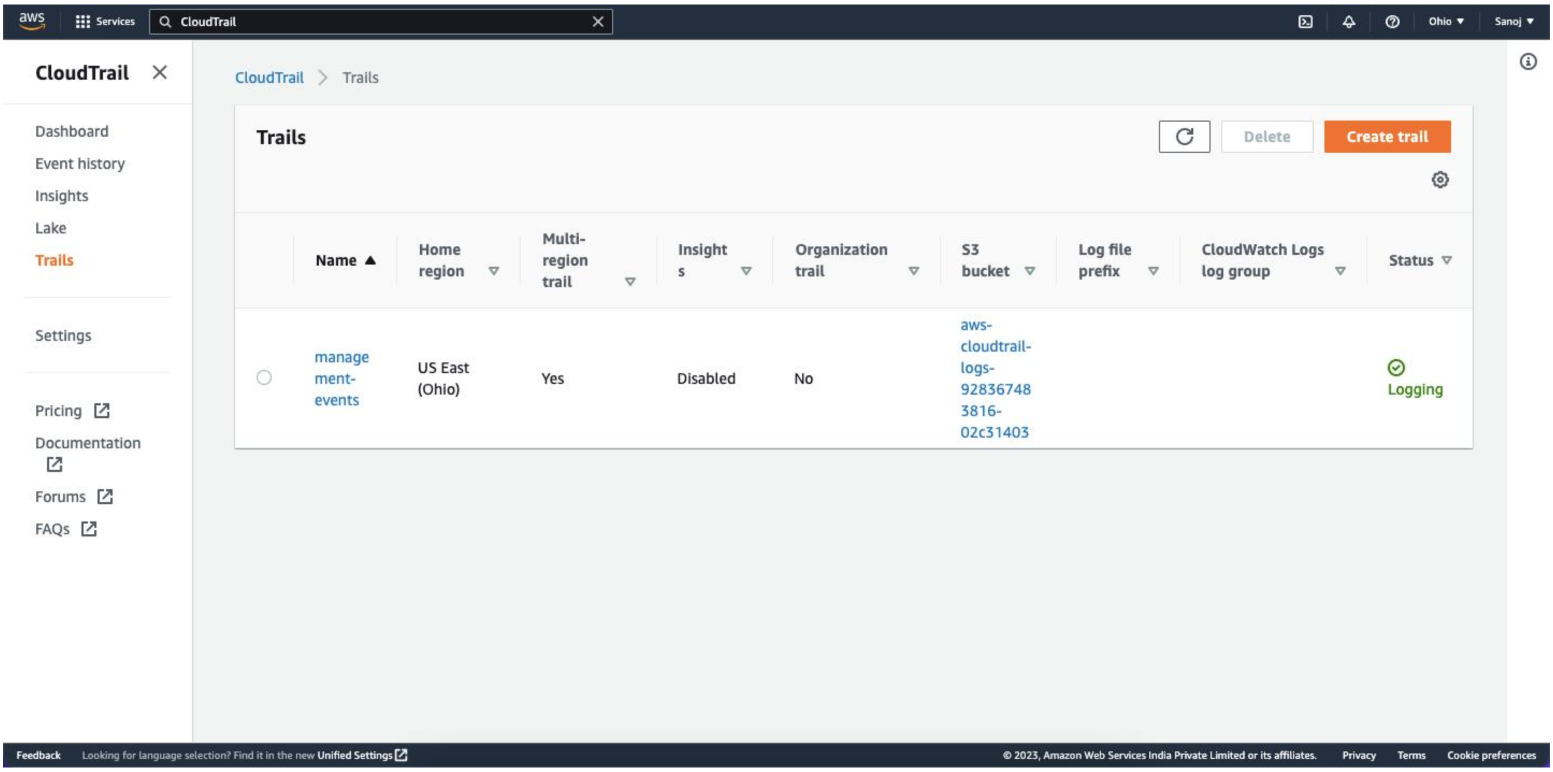
Trail log bucket and folder
aws-cloudtrail-logs-928367483816-02c31403
Logs will be stored in aws-cloudtrail-logs-928367483816-02c31403/AWSLogs/928367483816

Though there is no cost to log these events, you incur charges for the S3 bucket that we create to store your logs.

Cancel   Create trail

Feedback   Looking for language selection? Find it in the new Unified Settings   © 2023, Amazon Web Services India Private Limited or its affiliates.   Privacy   Terms   Cookie preferences

Step4: After click on create trail you will see following interface.

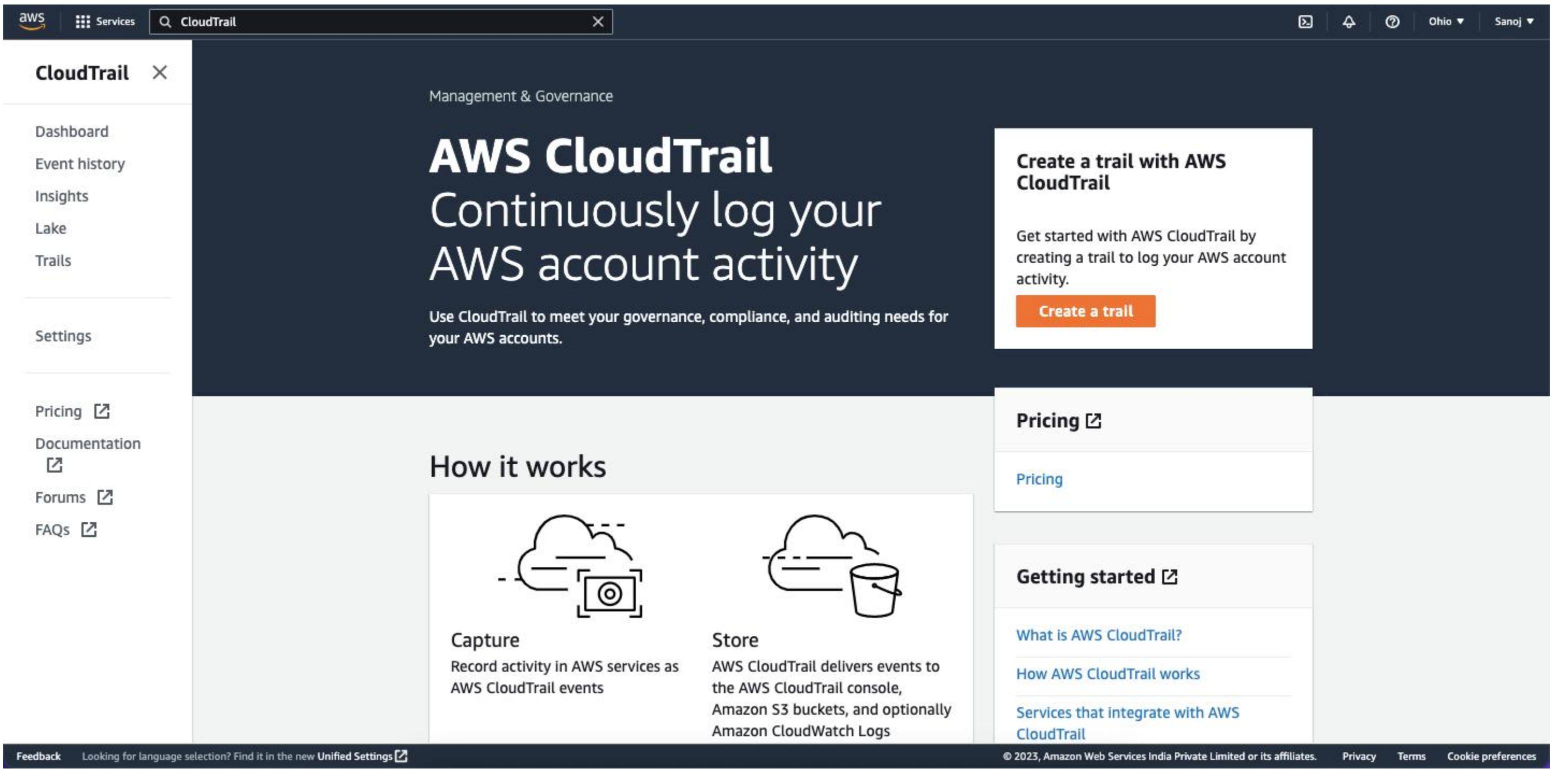


Trails

	Name ▲	Home region	Multi-region trail	Insights	Organization trail	S3 bucket	Log file prefix	CloudWatch Logs log group	Status
○	management-events	US East (Ohio)	Yes	Disabled	No	aws-cloudtrail-logs-928367483816-02c31403			✓ Logging

Second way(Cloud Trail WorkFlow) to create Trail

Step1:Click on the “Create a Trail”



Management & Governance

AWS CloudTrail

Continuously log your AWS account activity

Use CloudTrail to meet your governance, compliance, and auditing needs for your AWS accounts.

Create a trail with AWS CloudTrail

Get started with AWS CloudTrail by creating a trail to log your AWS account activity.

How it works

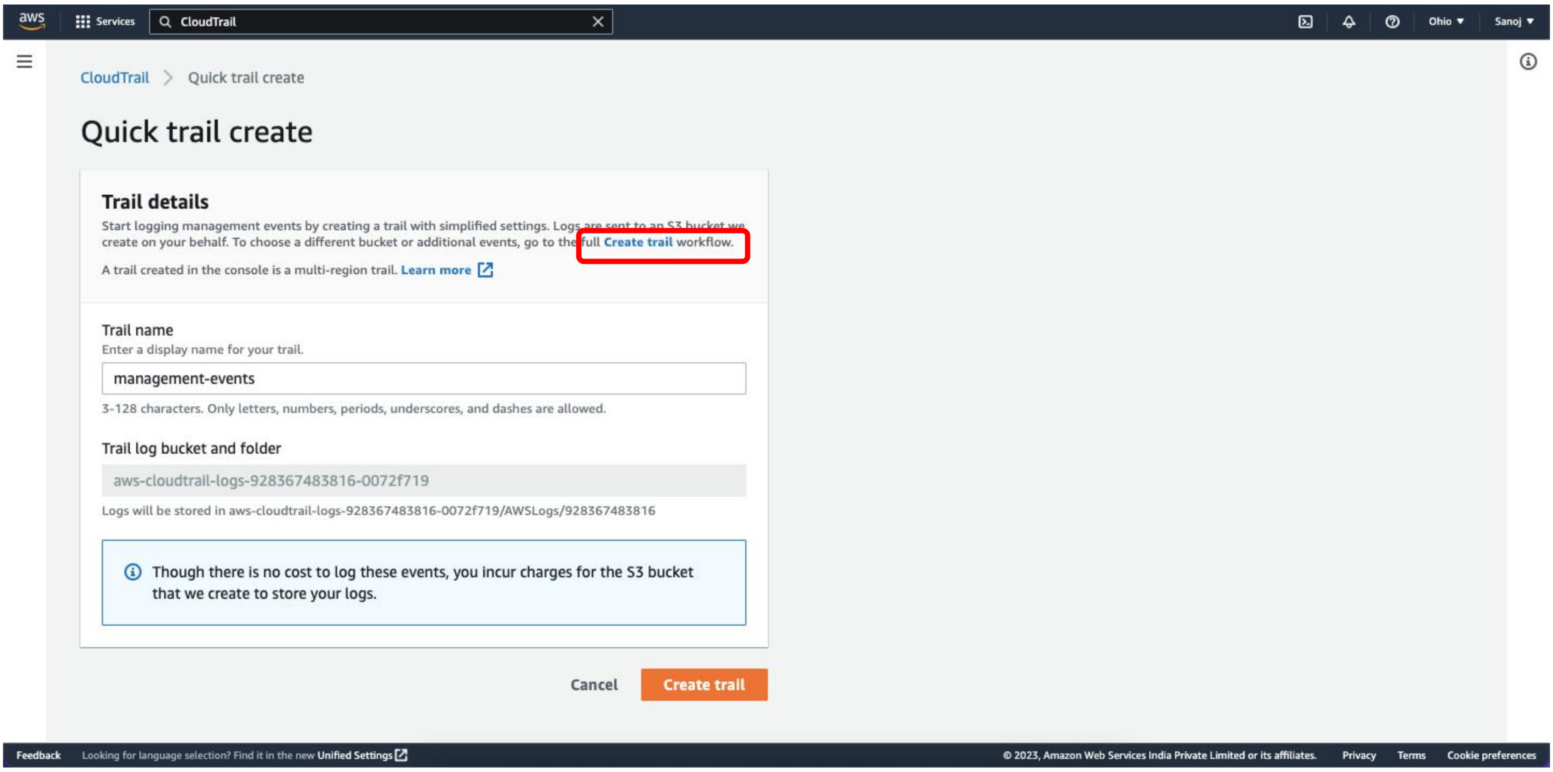
Capture

Record activity in AWS services as AWS CloudTrail events

Store

AWS CloudTrail delivers events to the AWS CloudTrail console, Amazon S3 buckets, and optionally Amazon CloudWatch Logs

Step2: Click on “Create Trail” on highlighted portion of below image.



CloudTrail > Quick trail create

Quick trail create

Trail details

Start logging management events by creating a trail with simplified settings. Logs are sent to an S3 bucket we create on your behalf. To choose a different bucket or additional events, go to the full Create trail workflow.

A trail created in the console is a multi-region trail. Learn more

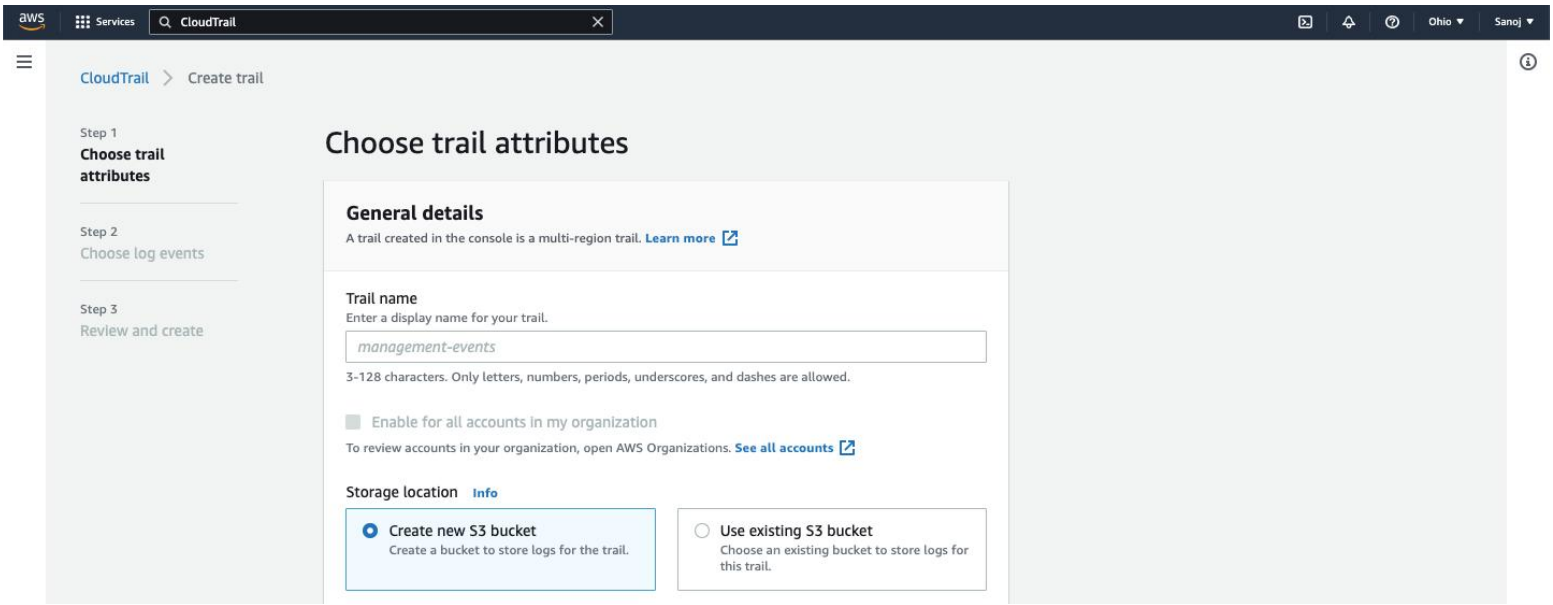
Trail name
Enter a display name for your trail.
management-events
3-128 characters. Only letters, numbers, periods, underscores, and dashes are allowed.

Trail log bucket and folder
aws-cloudtrail-logs-928367483816-0072f719
Logs will be stored in aws-cloudtrail-logs-928367483816-0072f719/AWSLogs/928367483816

Though there is no cost to log these events, you incur charges for the S3 bucket that we create to store your logs.

Cancel
Create trail
Feedback
Looking for language selection? Find it in the new Unified Settings
© 2023, Amazon Web Services India Private Limited or its affiliates.
Privacy
Terms
Cookie preferences

Step3: Once you click on the above Highlighted portion “Create trail” you will see following interface.



CloudTrail > 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

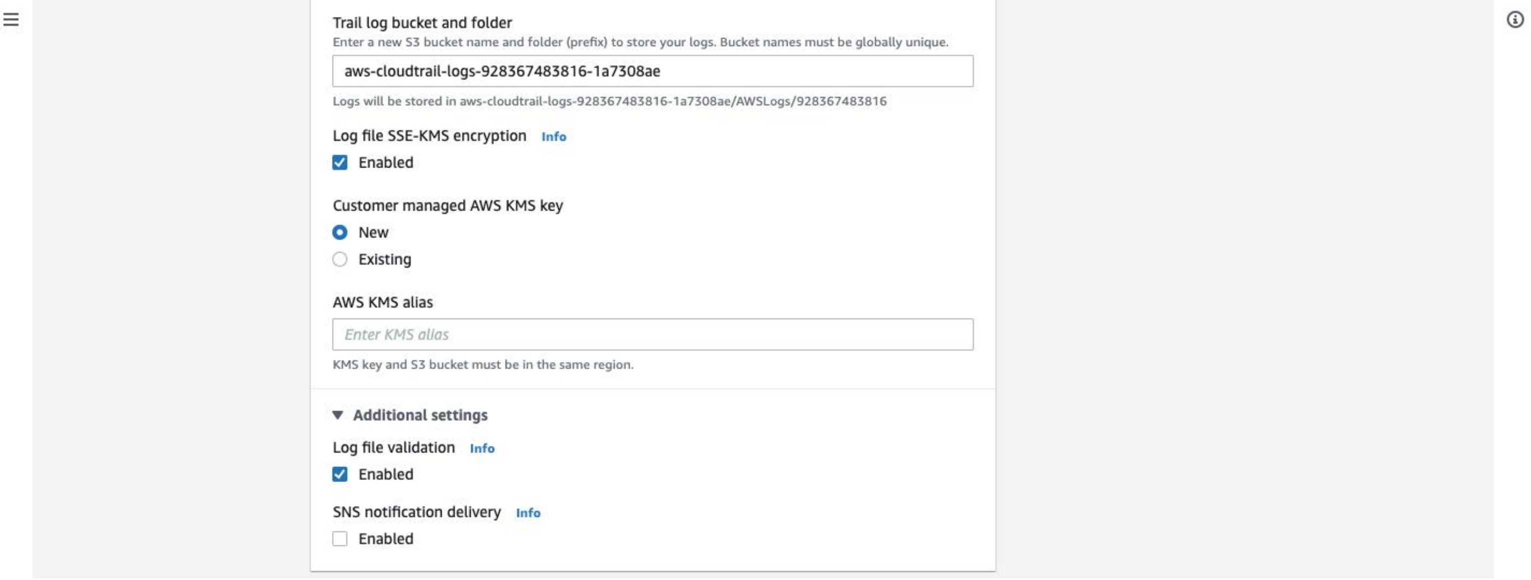
Trail name
Enter a display name for your trail.
management-events
3-128 characters. Only letters, numbers, periods, underscores, and dashes are allowed.

□ 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.
aws-cloudtrail-logs-928367483816-1a7308ae
Logs will be stored in aws-cloudtrail-logs-928367483816-1a7308ae/AWSLogs/928367483816

Log file SSE-KMS encryption Info
☑ Enabled

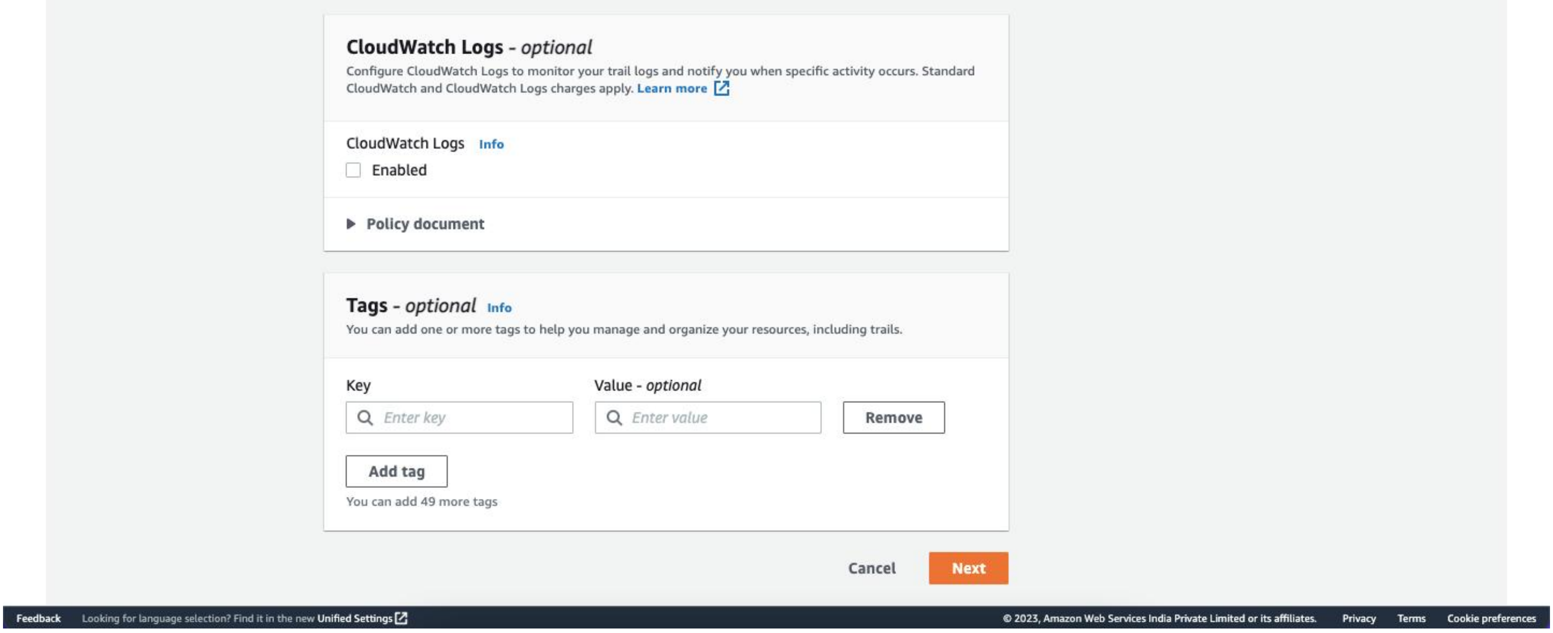
Customer managed AWS KMS key
● New
○ Existing

AWS KMS alias
Enter KMS alias
KMS key and S3 bucket must be in the same region.

▼ Additional settings

Log file validation Info
☑ Enabled

SNS notification delivery Info
□ Enabled



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

▶ Policy document

Tags - *optional* Info

You can add one or more tags to help you manage and organize your resources, including trails.

Key: Enter key

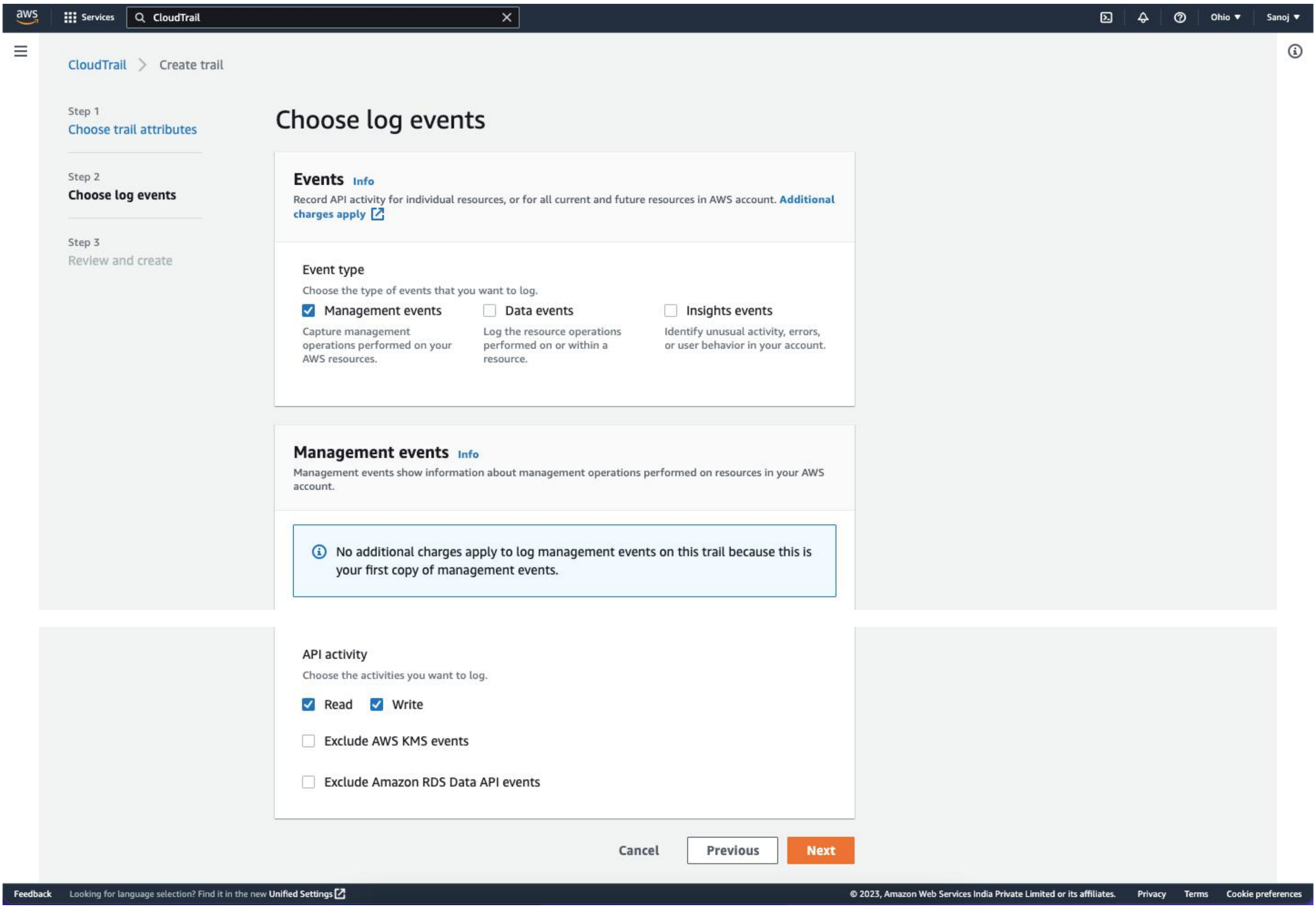
Value - *optional*: Enter value

You can add 49 more tags

Cancel
Next
Feedback
Looking for language selection? Find it in the new Unified Settings
© 2023, Amazon Web Services India Private Limited or its affiliates.
Privacy
Terms
Cookie preferences

You can select options as per your choice and after that click on “Next”

After click on “Next” Button you will be see following interface.



Step 1 Choose trail attributes

Step 2 Choose log events

Step 3 Review and create

Choose log events

Events Info

Record API activity for individual resources, or for all current and future resources in AWS account. Additional charges apply

Event type

Choose the type of events that you want to log.

☑ Management events — Capture management operations performed on your AWS resources.

□ Data events — Log the resource operations performed on or within a resource.

□ Insights events — Identify unusual activity, errors, or user behavior in your account.

Management events Info

Management events show information about management operations performed on resources in your AWS account.

No additional charges apply to log management events on this trail because this is your first copy of management events.

API activity

Choose the activities you want to log.

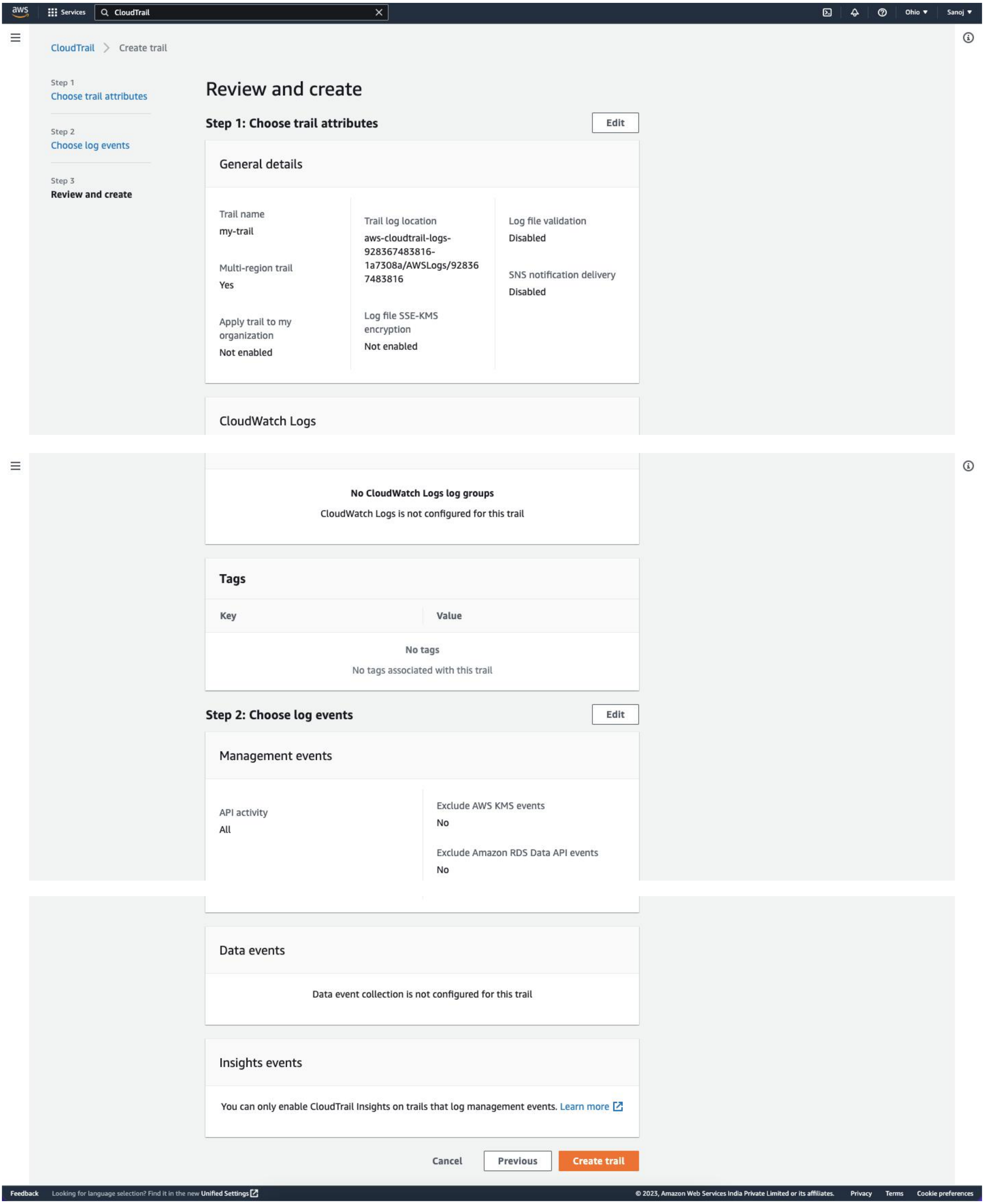
☑ Read ☑ Write

□ Exclude AWS KMS events

□ Exclude Amazon RDS Data API events

Cancel
Previous
Next
Feedback
Looking for language selection? Find it in the new Unified Settings
© 2023, Amazon Web Services India Private Limited or its affiliates.
Privacy
Terms
Cookie preferences

Step4: Now click on “Next” you will be see following interface just review all things and click on “Create trail”



Review and create

Step 1: Choose trail attributes

Edit

General details

Trail name
my-trail

Multi-region trail
Yes

Apply trail to my organization
Not enabled

Trail log location
aws-cloudtrail-logs-928367483816-1a7308a/AWSLogs/928367483816

Log file SSE-KMS encryption
Not enabled

Log file validation
Disabled

SNS notification delivery
Disabled

CloudWatch Logs

No CloudWatch Logs log groups

CloudWatch Logs is not configured for this trail

Tags

Key	Value

No tags

No tags associated with this trail

Step 2: Choose log events

Edit

Management events

API activity
All

Exclude AWS KMS events
No

Exclude Amazon RDS Data API events
No

Data events

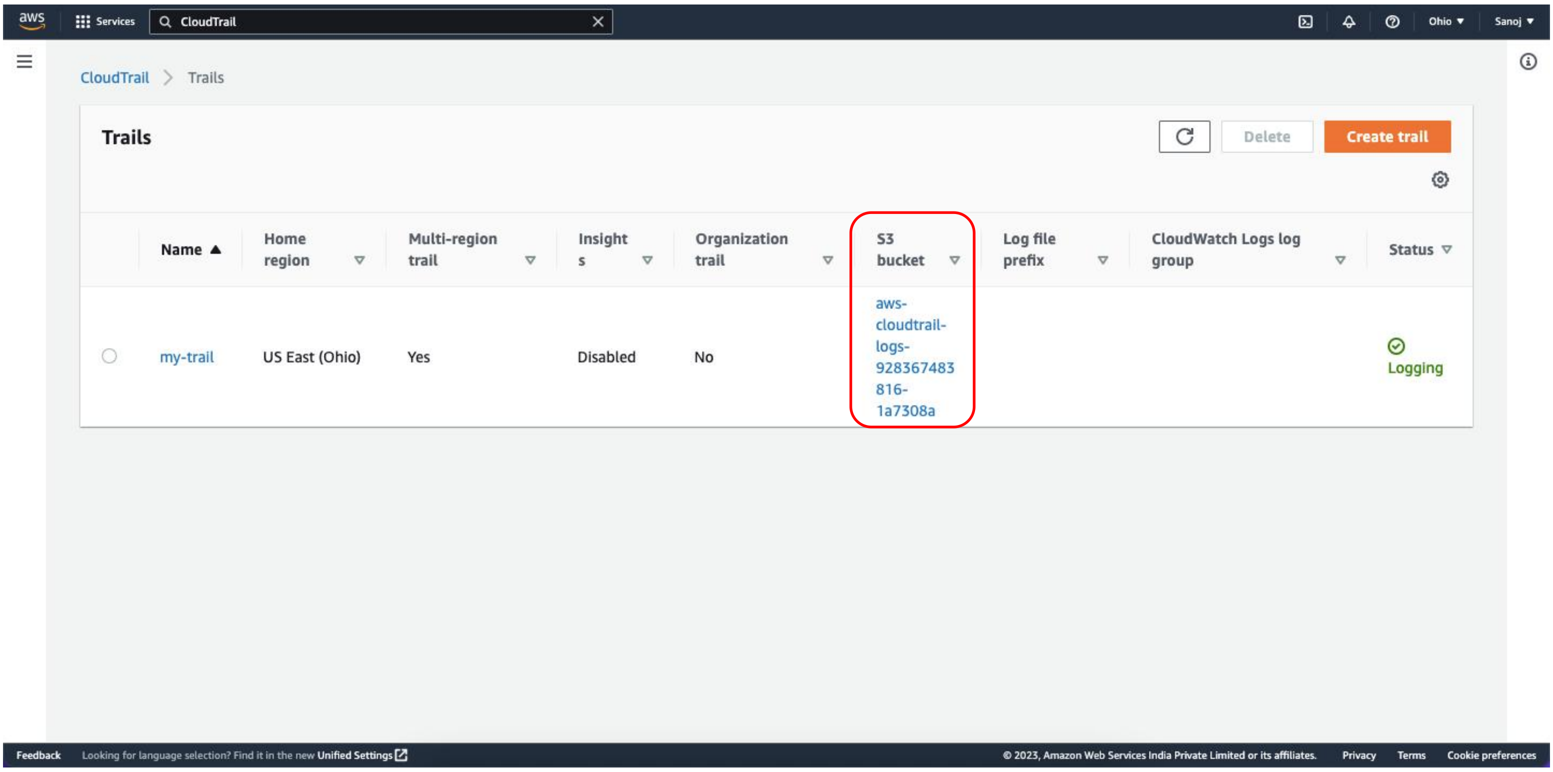
Data event collection is not configured for this trail

Insights events

You can only enable CloudTrail Insights on trails that log management events. Learn more

Cancel
Previous
Create trail
Feedback
Looking for language selection? Find it in the new Unified Settings
© 2023, Amazon Web Services India Private Limited or its affiliates.
Privacy
Terms
Cookie preferences

Once you Create your trail you will see following interface.

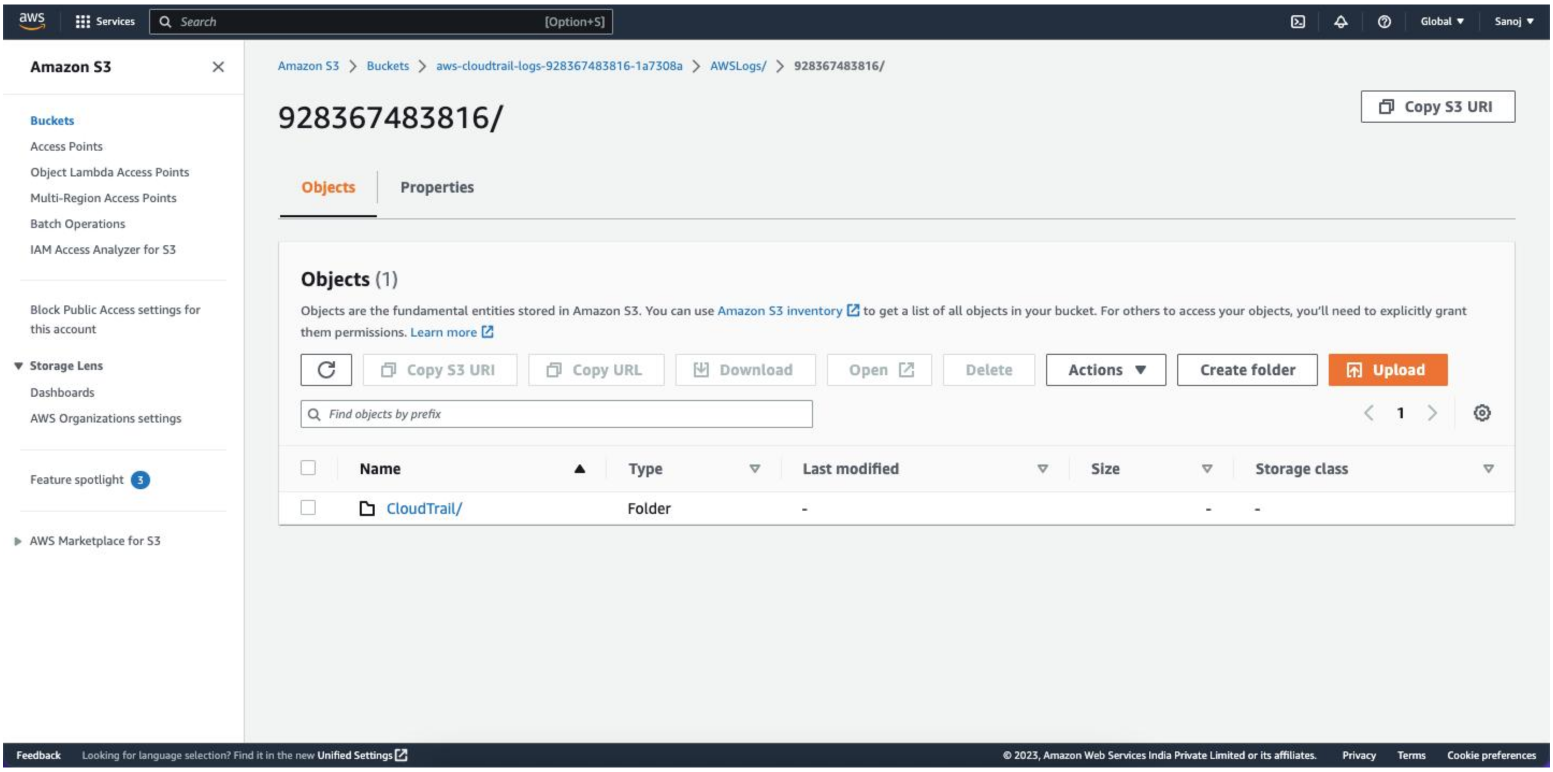

aws
Services
CloudTrail
Ohio ▾
Sanoj ▾
CloudTrail > Trails
Delete
Create trail
Feedback
Looking for language selection? Find it in the new Unified Settings
© 2023, Amazon Web Services India Private Limited or its affiliates.
Privacy
Terms
Cookie preferences

Trails

	Name ▲	Home region	Multi-region trail	Insights	Organization trail	S3 bucket	Log file prefix	CloudWatch Logs log group	Status
○	my-trail	US East (Ohio)	Yes	Disabled	No	aws-cloudtrail-logs-928367483816-1a7308a			Logging

If you want to see your located trails logs you can click on “S3 bucket” section or you can open your S3 bucket separately its up to you.

For example i have clicked on the above mentioned S3 bucket link so i got following interface.


aws
Services
Search
[Option+S]
Global ▾
Sanoj ▾
Amazon S3
Buckets
Access Points
Object Lambda Access Points
Multi-Region Access Points
Batch Operations
IAM Access Analyzer for S3
Block Public Access settings for this account
Storage Lens
Dashboards
AWS Organizations settings
Feature spotlight 3
AWS Marketplace for S3
Amazon S3 > Buckets > aws-cloudtrail-logs-928367483816-1a7308a > AWSLogs/ > 928367483816/
Copy S3 URI
Objects
Properties
Copy S3 URI
Copy URL
Download
Open
Delete
Actions ▼
Create folder
Upload
Find objects by prefix
1
Feedback
Looking for language selection? Find it in the new Unified Settings
© 2023, Amazon Web Services India Private Limited or its affiliates.
Privacy
Terms
Cookie preferences

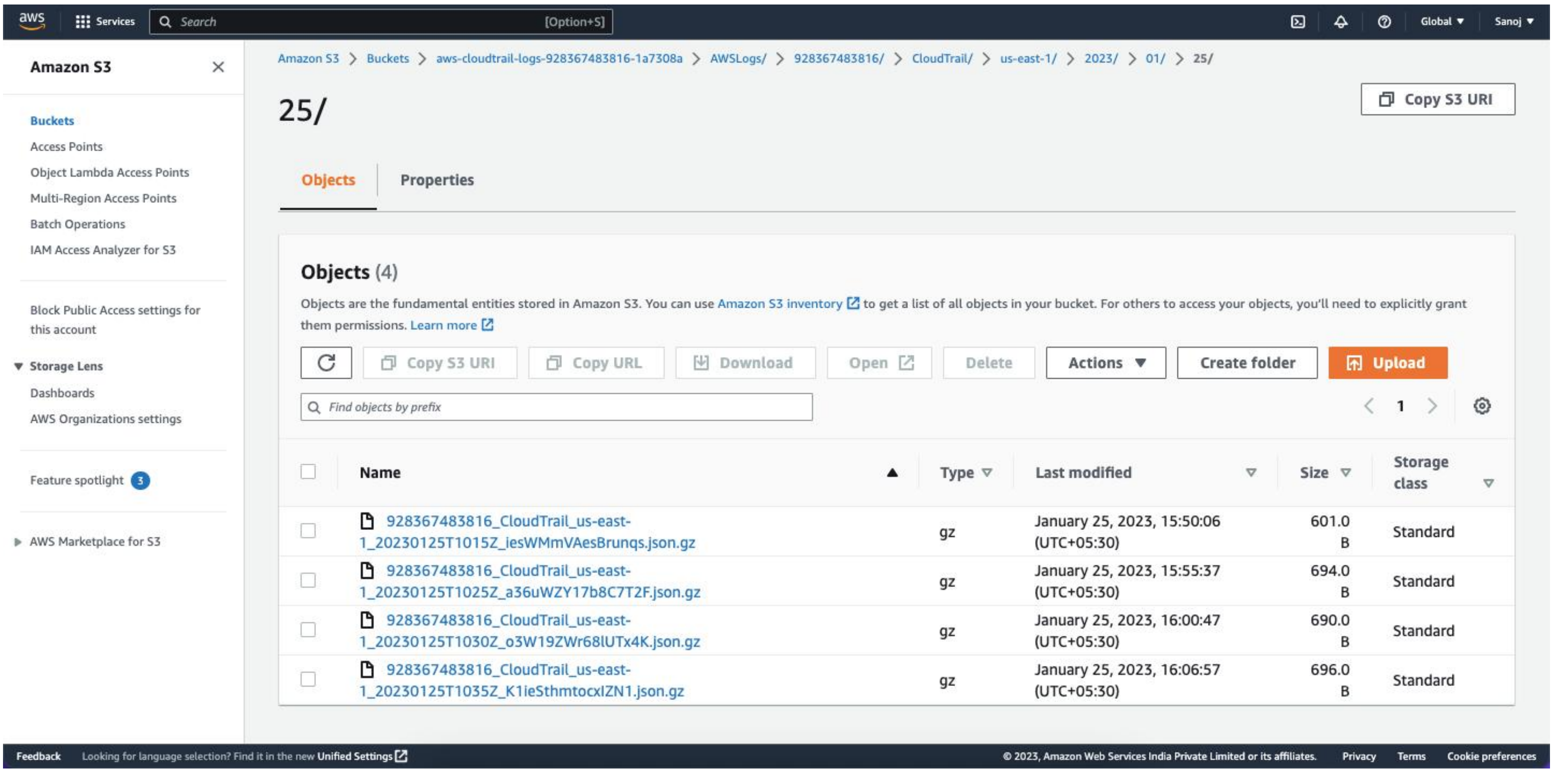
928367483816/

Objects (1)

Objects are the fundamental entities stored in Amazon S3. You can use Amazon S3 inventory to get a list of all objects in your bucket. For others to access your objects, you'll need to explicitly grant them permissions. Learn more

□	Name ▲	Type	Last modified	Size	Storage class
□	CloudTrail/	Folder	-	-	-

If we go inside the bucket folder, there will be many folder inside the folder at the end you we will see following kind interface.



Amazon S3 > Buckets > aws-cloudtrail-logs-928367483816-1a7308a > AWSLogs/ > 928367483816/ > CloudTrail/ > us-east-1/ > 2023/ > 01/ > 25/

25/

Objects (4)

Objects are the fundamental entities stored in Amazon S3. You can use Amazon S3 inventory to get a list of all objects in your bucket. For others to access your objects, you'll need to explicitly grant them permissions. Learn more

□	Name ▲	Type ▽	Last modified ▽	Size ▽	Storage class ▽
□	928367483816_CloudTrail_us-east-1_20230125T1015Z_iesWMmVAesBrunqs.json.gz	gz	January 25, 2023, 15:50:06 (UTC+05:30)	601.0 B	Standard
□	928367483816_CloudTrail_us-east-1_20230125T1025Z_a36uWZY17b8C7T2F.json.gz	gz	January 25, 2023, 15:55:37 (UTC+05:30)	694.0 B	Standard
□	928367483816_CloudTrail_us-east-1_20230125T1030Z_o3W19ZWr68lUTx4K.json.gz	gz	January 25, 2023, 16:00:47 (UTC+05:30)	690.0 B	Standard
□	928367483816_CloudTrail_us-east-1_20230125T1035Z_K1ieSthmtocxIZN1.json.gz	gz	January 25, 2023, 16:06:57 (UTC+05:30)	696.0 B	Standard