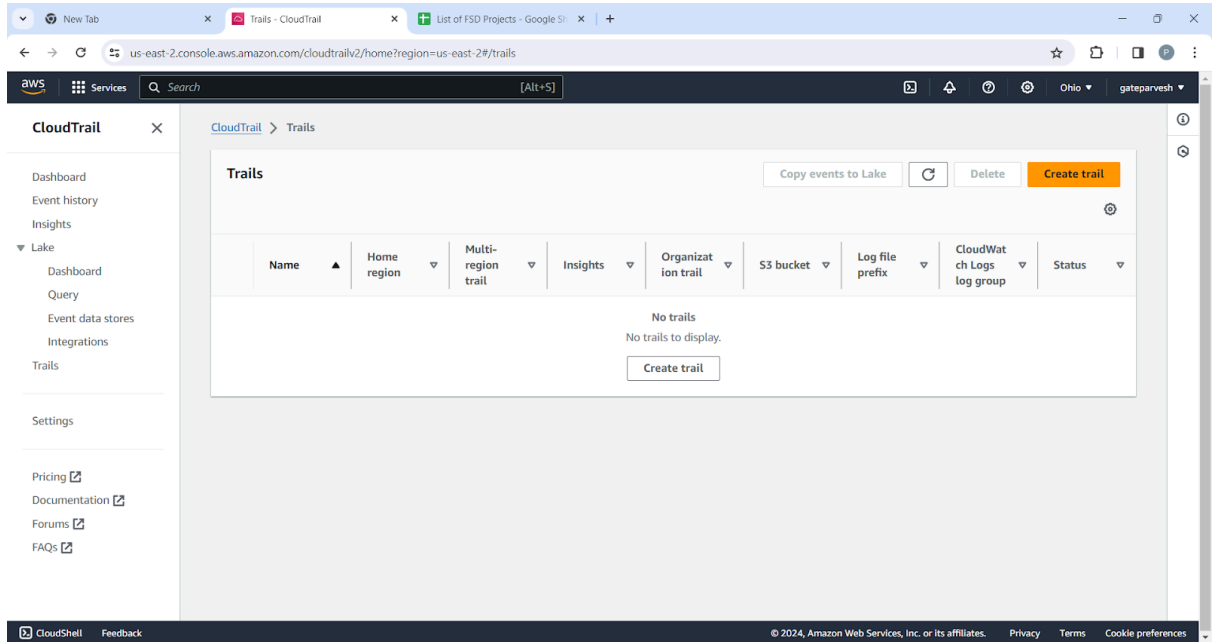


#AWS CloudTrail

1. Track Users activity and API usages. f

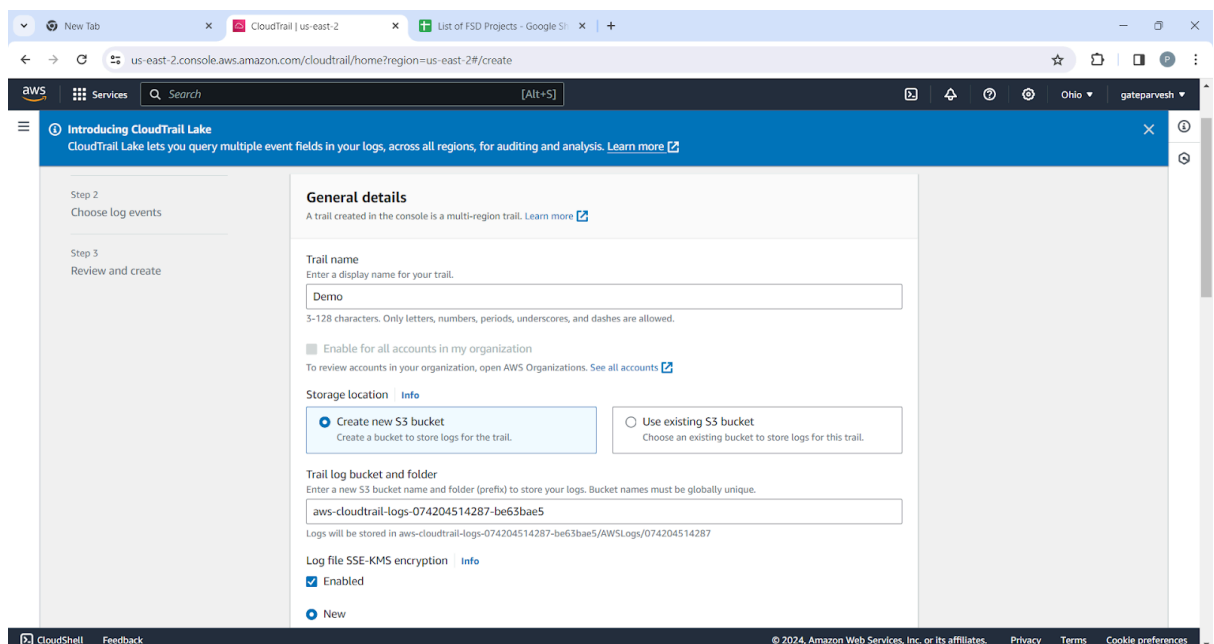
1. Open Aws console → CloudTrail → create trails.



This have three steps →

i. Choose trail attributes.

1.



2

The screenshot shows the AWS CloudTrail console in the 'us-east-2' region. The main heading is 'Introducing CloudTrail Lake', with a subtext 'CloudTrail Lake lets you query multiple event fields in your logs, across all regions, for auditing and analysis. [Learn more](#)'. The 'Log file SSE-KMS encryption' section is expanded, showing 'Enabled' as the selected option. Below this, there are radio buttons for 'New' (selected) and 'Existing'. An input field for 'AWS KMS alias' contains the text 'Enter KMS alias'. A note states 'KMS key and S3 bucket must be in the same region.' The 'Additional settings' section is also expanded, showing 'Log file validation' and 'SNS notification delivery' both set to 'Enabled'. Below these, there are radio buttons for 'New' (selected) and 'Existing'. An input field for 'SNS topic' contains the text 'aws-cloudtrail-logs-074204514287-5ba769aa'. The footer of the console shows 'CloudShell', 'Feedback', and copyright information for Amazon Web Services, Inc. or its affiliates.

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

Introducing CloudTrail Lake
CloudTrail Lake lets you query multiple event fields in your logs, across all regions, for auditing and analysis. [Learn more](#)

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

☒ Enabled

☒ New
☐ Existing

AWS 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

☒ New
☐ Existing

SNS topic

CloudShell Feedback © 2024, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

3

The screenshot shows the AWS CloudTrail console in the 'us-east-2' region. The main heading is 'Introducing CloudTrail Lake', with a subtext 'CloudTrail Lake lets you query multiple event fields in your logs, across all regions, for auditing and analysis. [Learn more](#)'. The 'CloudWatch Logs - optional' section is expanded, showing 'Enabled' as the selected option. Below this, there are radio buttons for 'New' (selected) and 'Existing'. An input field for 'Log group name' contains the text 'aws-cloudtrail-logs-074204514287-4751f150'. A note states '1-512 characters. Only letters, numbers, dashes, underscores, forward slashes, and periods are allowed.' Below this, there is a note 'AWS CloudTrail assumes this role to send CloudTrail events to your CloudWatch Logs log group.' Below this, there are radio buttons for 'New' (selected) and 'Existing'. An input field for 'Role name' contains the text 'demo'. A link for 'Policy document' is visible at the bottom of the section. The footer of the console shows 'CloudShell', 'Feedback', and copyright information for Amazon Web Services, Inc. or its affiliates.

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

Introducing CloudTrail Lake
CloudTrail Lake lets you query multiple event fields in your logs, across all regions, for auditing and analysis. [Learn more](#)

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

☒ New
☐ Existing

Log group name

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

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

☒ New
☐ Existing

Role name

[Policy document](#)

CloudShell Feedback © 2024, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

ii. Choose log events.

1

The screenshot shows the 'Choose log events' step in the AWS CloudTrail console. The left sidebar indicates the current step is 'Step 3: Choose log events'. The main content area is titled 'Events' and includes a description: 'Record API activity for individual resources, or for all current and future resources in AWS account. Additional charges apply'. Below this, the 'Event type' section allows choosing the type of events to log, with three options: 'Management events' (checked), 'Data events' (checked), and 'Insights events' (checked). The 'Management events' section provides a description and a note: 'No additional charges apply to log management events on this trail because this is your first copy of management events.' The 'API activity' section allows choosing the activities to log, with 'Read' and 'Write' both checked.

2

The screenshot shows the 'Data events' configuration step in the AWS CloudTrail console. The left sidebar indicates the current step is 'Step 4: Review and create'. The main content area is titled 'Data events' and includes a description: 'Data events show information about the resource operations performed on or within a resource. Additional charges apply'. Below this, the 'Advanced event selectors are enabled' section provides a description and a 'Switch to basic event selectors' button. The 'Data event type' section allows choosing the source of data events to log, with 'S3 Access Point' selected. The 'Log selector template' section allows choosing the log selector template, with 'Log all events' selected. The 'Selector name - optional' section allows entering a name, with 'Enter a name' entered.

3

The screenshot shows the 'Insights events' configuration step in the AWS CloudTrail console. The left sidebar indicates the current step is 'Step 5: Review and create'. The main content area is titled 'Insights events' and includes a description: 'Identify unusual activity, errors, or user behavior in your account. Additional charges apply'. Below this, the 'Choose Insights types' section allows choosing the types of insights to log, with 'API call rate' and 'API error rate' both checked. The 'API call rate' section provides a description: 'A measurement of write-only management API calls that occur per minute against a baseline API call volume.' The 'API error rate' section provides a description: 'A measurement of management API calls that result in error codes. The error is shown if the API call is unsuccessful.' At the bottom, there are 'Cancel', 'Previous', and 'Next' buttons.

iii. Review and create.

1.

The screenshot shows the AWS CloudTrail console in the 'us-east-2' region. The page title is 'Review and create'. The left sidebar shows the navigation menu with 'CloudTrail' selected and 'Create trail' as the current action. The main content area is titled 'Step 1: Choose trail attributes' and contains a form with the following fields:

General details		
Trail name	Trail log location	Log file validation
Demo	aws-cloudtrail-logs-074204514287-be63bae5/AWSLogs/074204514287	Enabled
Multi-region trail		SNS notification delivery
Yes		aws-cloudtrail-logs-074204514287-5ba769aa
Apply trail to my organization	Log file SSE-KMS encryption	
Not enabled	Enabled	
	AWS KMS key alias	
	KMS	

Below the form is a section for 'CloudWatch Logs'.

2

The screenshot shows the AWS CloudTrail console in the 'us-east-2' region. The page title is 'Choose log events'. The left sidebar shows the navigation menu with 'CloudTrail' selected and 'Create trail' as the current action. The main content area is titled 'Step 2: Choose log events' and contains a form with the following fields:

CloudWatch Logs	
Log group	IAM Role
aws-cloudtrail-logs-074204514287-4751f150	demo

Below the form is a section for 'Tags'.

Key	Value
No tags	
No tags associated with this trail	

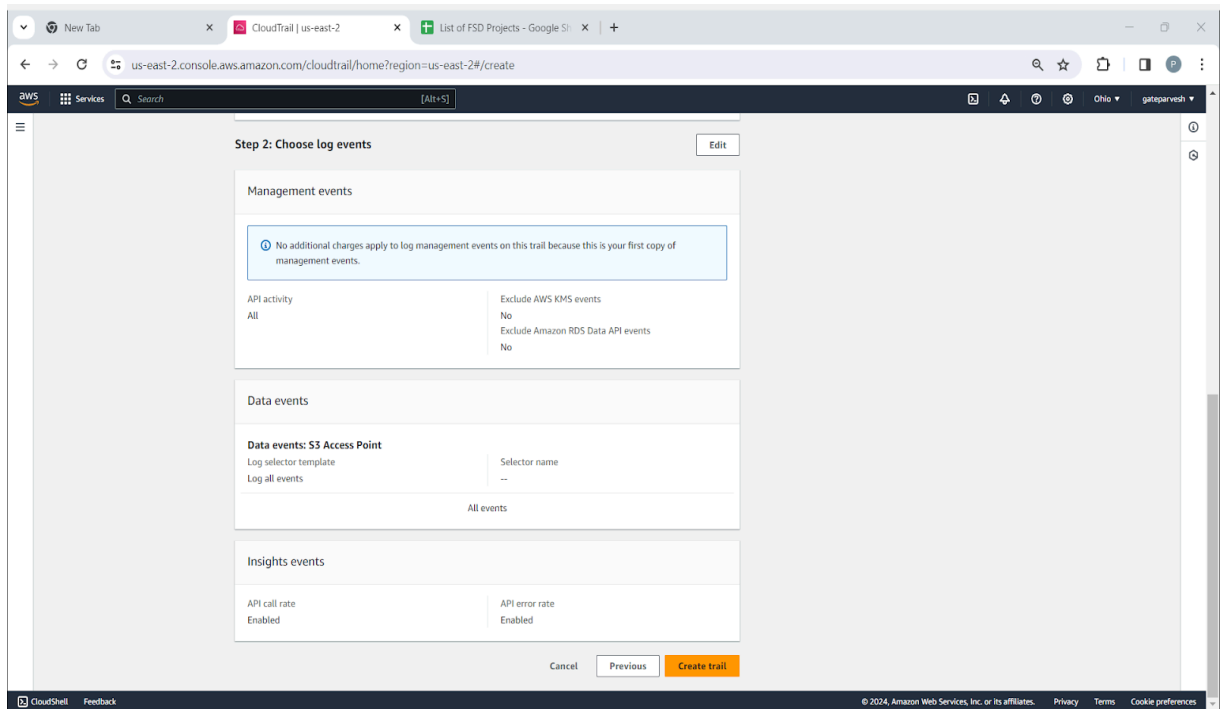
Below the form is a section for 'Management events'.

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

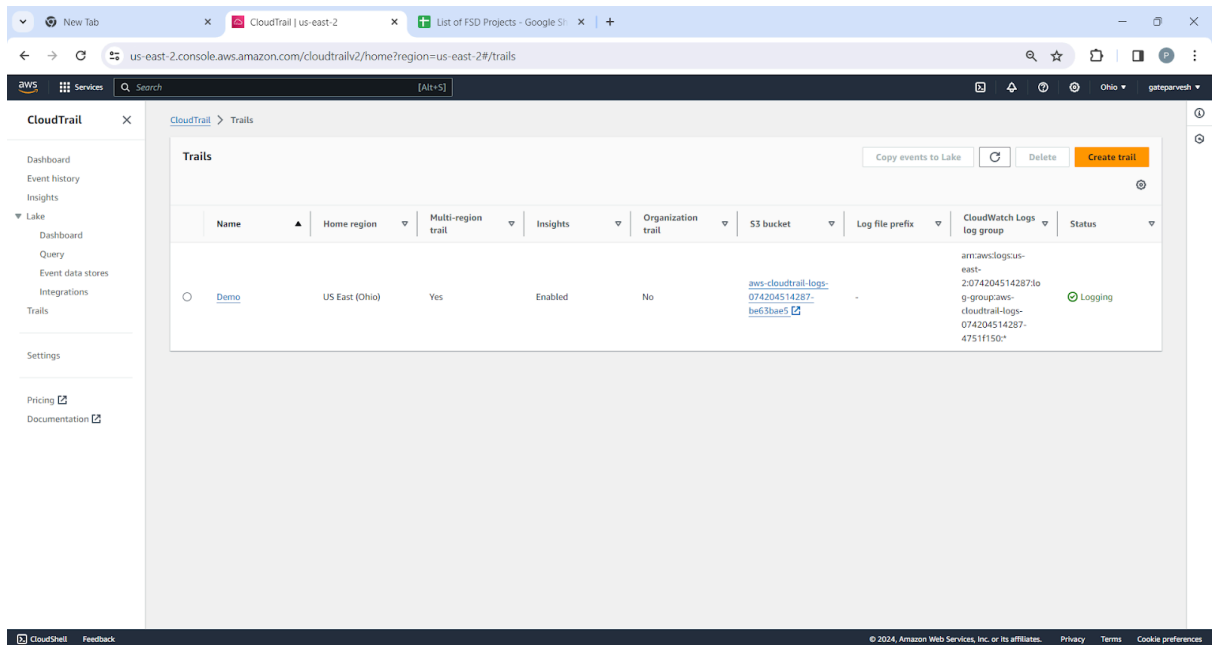
API activity

Exclude AWS KMS events

3.

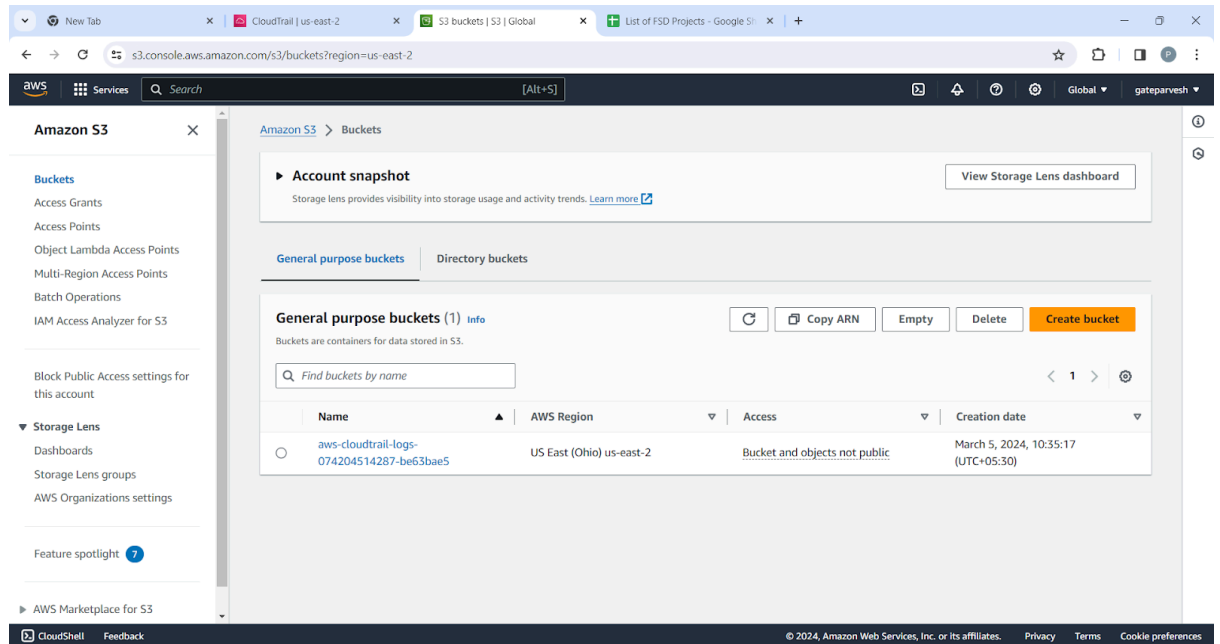


2. Create Trails (by clicking on Button).

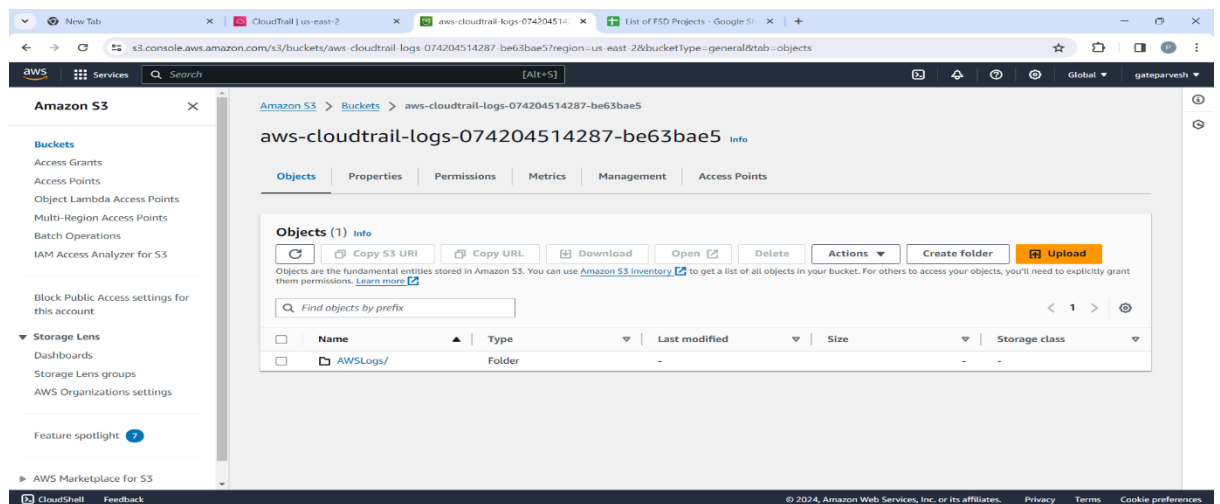


3. Now go to S3 bucket and see the log file folder.

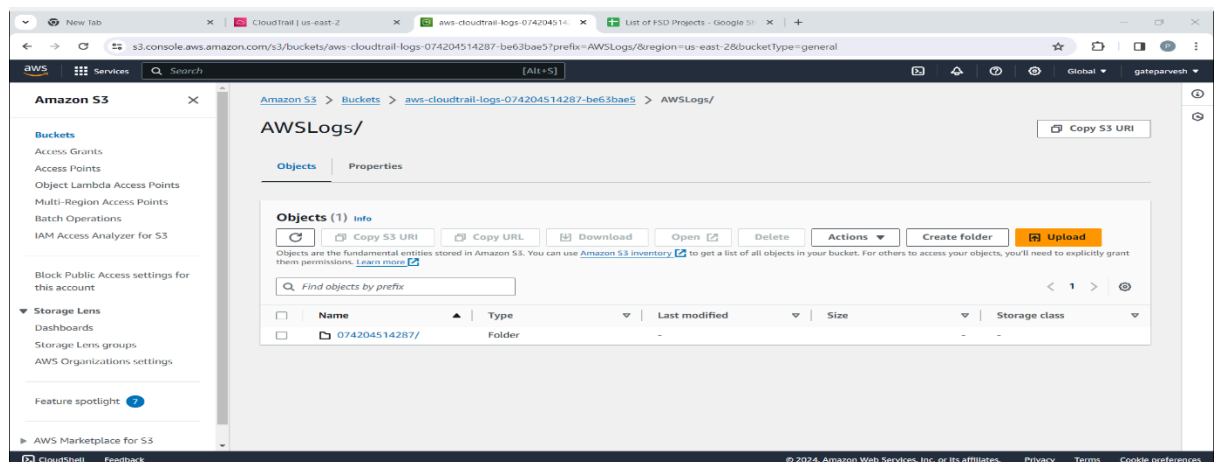
1



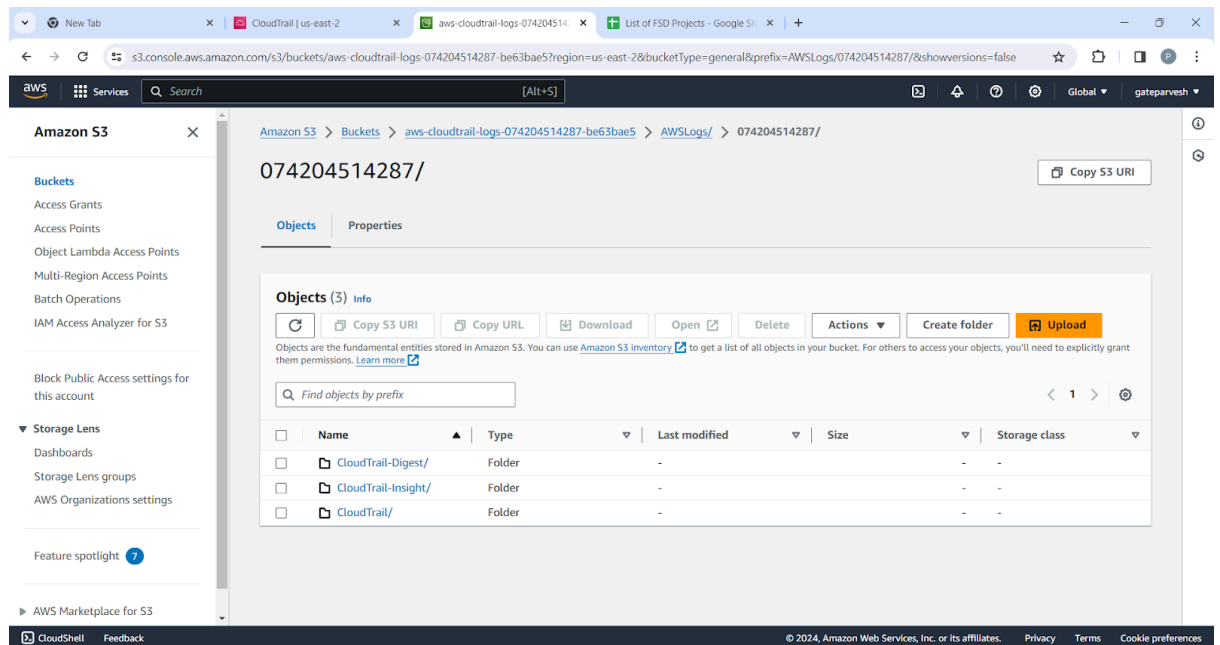
2.



3.

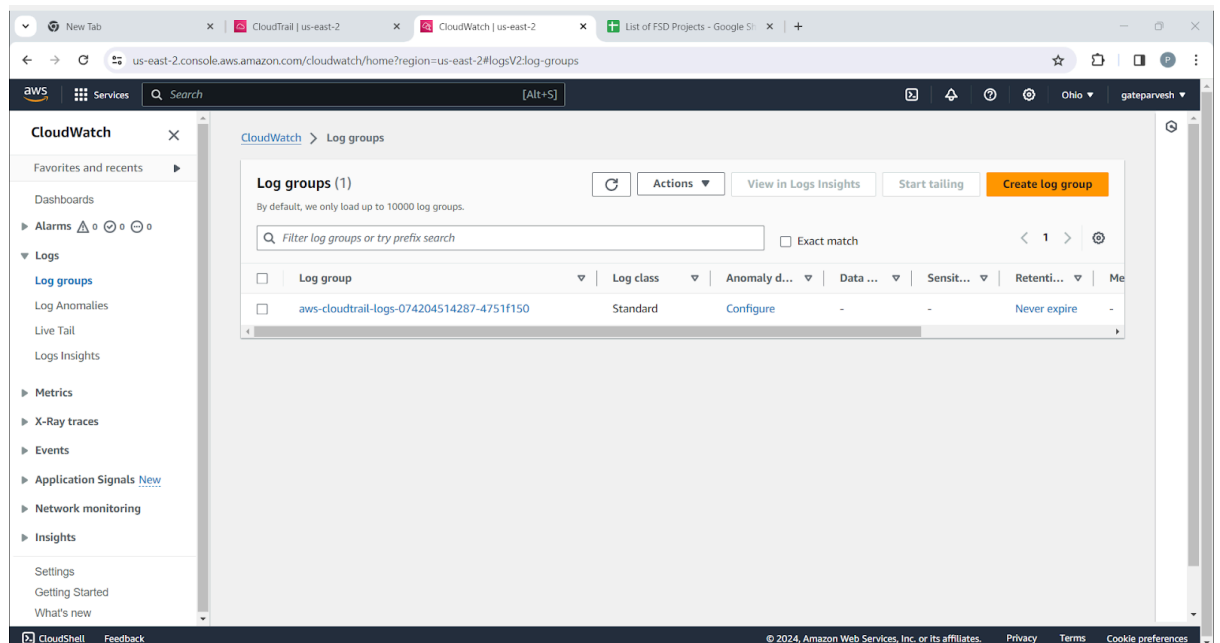


4.

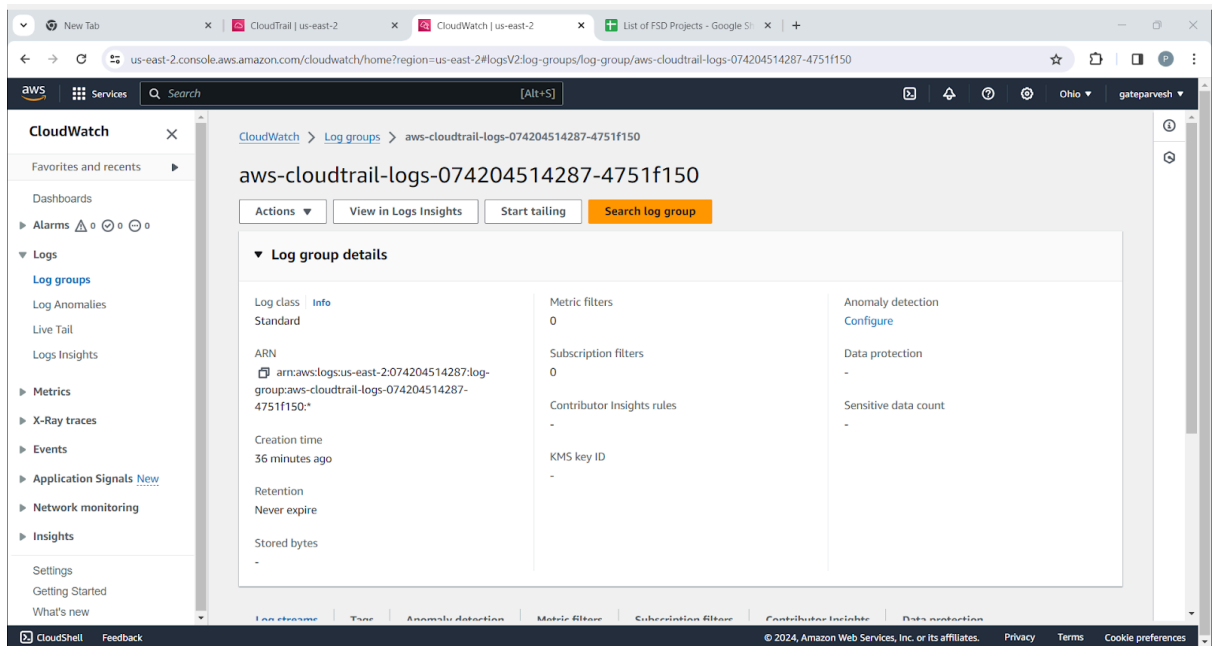


Now you can see 3 folders are created with Name CloudTrail-Digest, CloudTrail-Insight, CloudTrail.

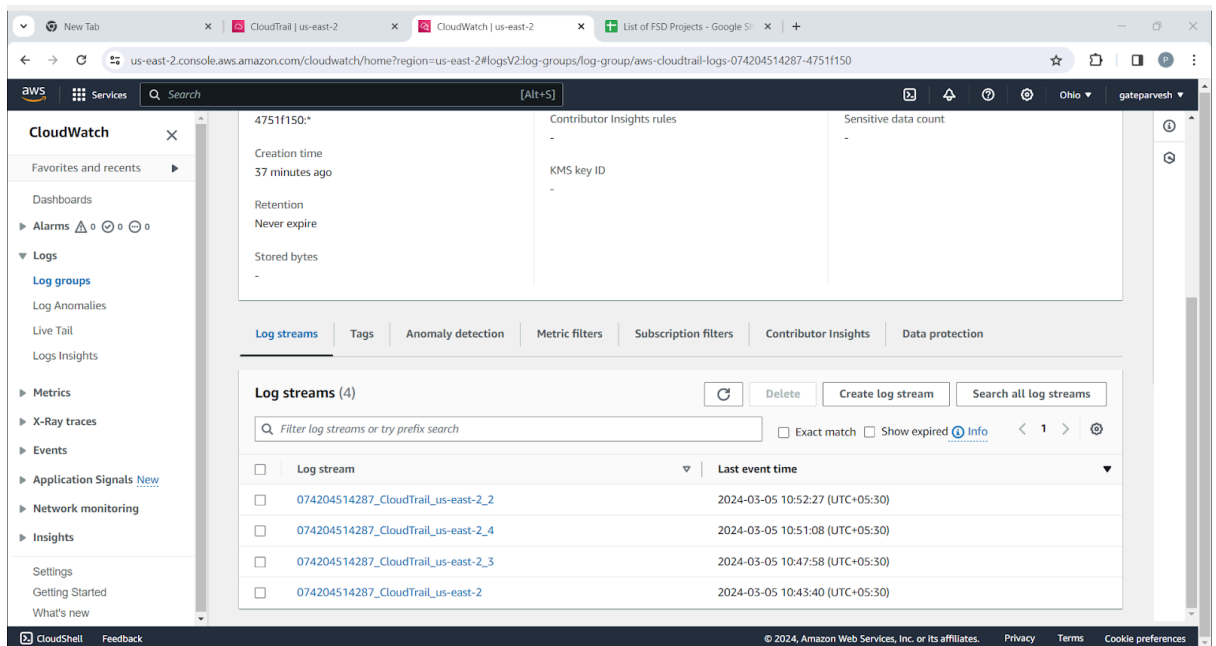
4. Go to CloudWatch → Logs.
1.



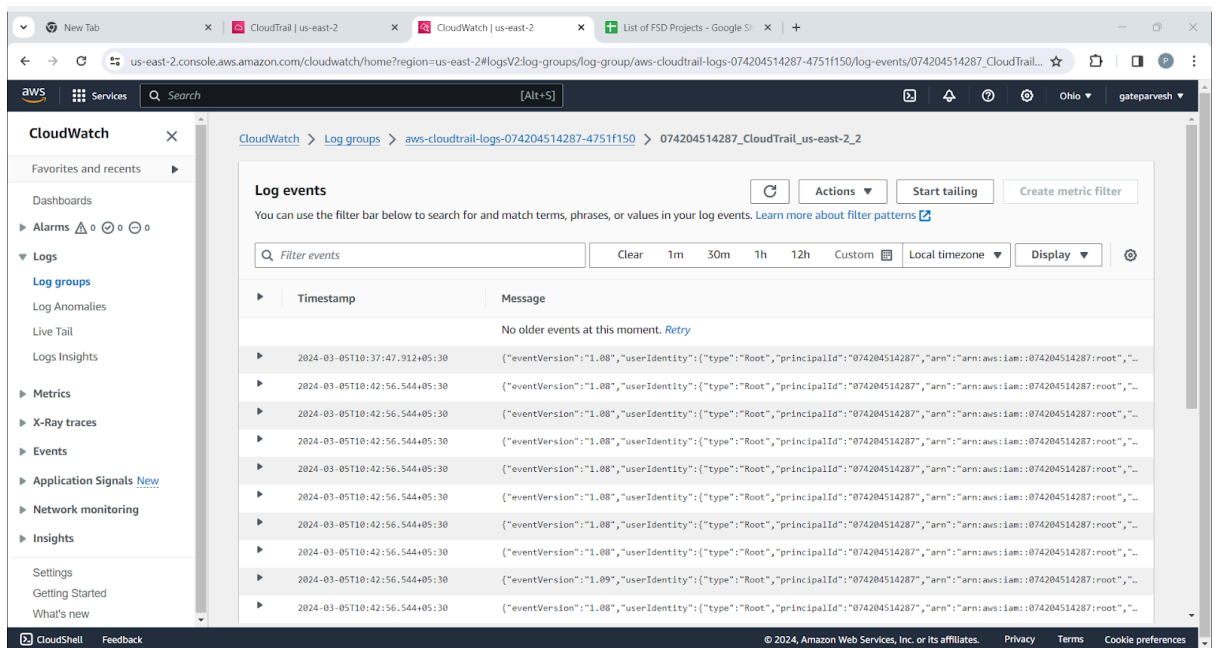
2. You can see logs details



3. Now you also see log stream.



4. Log stream click on any log you get below interface.



That's all about CloudTrail.