**CloudTrail**

* CloudTrail records all the AWS API calls which are happening in your account. like if you want to run ec2 instance in API i.e. ec2 run instance or terminate it i.e. ec2 terminate instance or for the s3 buckets like running and terminating it.
* The benefit is, it records all the records which you have made and stores it in a s3 bucket of your choice.
* By checking into the log files you can see all the details of that call which you had made.
* When activity occurs in your AWS account, that activity is recorded in a CloudTrail event. This can be seen in **Event History.**

**CloudTrail Workflow**

* View event history for your AWS account
* Download events
* Create a trail
* Create and subscribe to an Amazon SNS topic
* View your log files
* Manage user permissions
* Monitor events with CloudWatch Logs
* Log management and data events
* Log CloudTrail Insights events
* Enable log encryption
* Enable log file integrity
* Share log files with other AWS accounts
* Aggregate logs from multiple accounts
* Work with partner solutions

**CloudTrail concepts**

* **CloudTrail Events:** An event in CloudTrail is the record of an activity in an AWS account. This activity can be an action taken by a user, role, or service that is monitorable by CloudTrail. There are 3 types of events: Management events, Data events and Insight events.
* **Trails:** A trail is a configuration that enables delivery of CloudTrail events to an Amazon S3 bucket, CloudWatch Logs, and CloudWatch Events.
* **CloudTrail Management:** It can be done through various means like

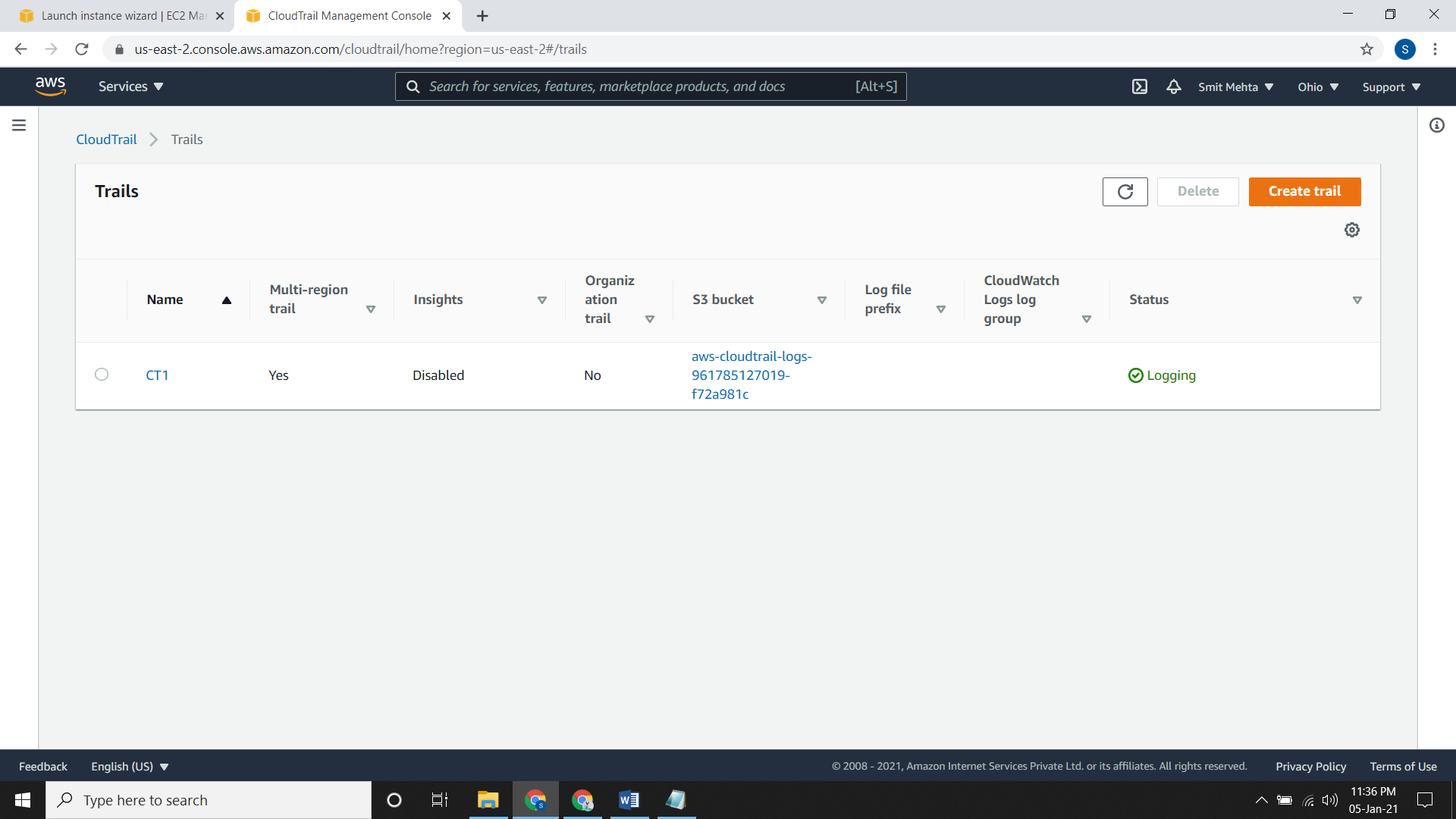
1. CloudTrail Console
2. CloudTrail CLI
3. CloudTrail APIs
4. AWS SDKs

**Creating a Trail**

* Go to cloudtrail dashboard and create a trail. Give a name, choose a storage location i.e. if you have a s3 bucket select it or create a new one.
* Now enable or disable **Log file SSE-KMS encryption and SNS notification delivery** according to your requirement.
* In additional setting enable the **Log file Validation** box.
* CloudWatch Logs and Tags are optional.
* Choose the event type

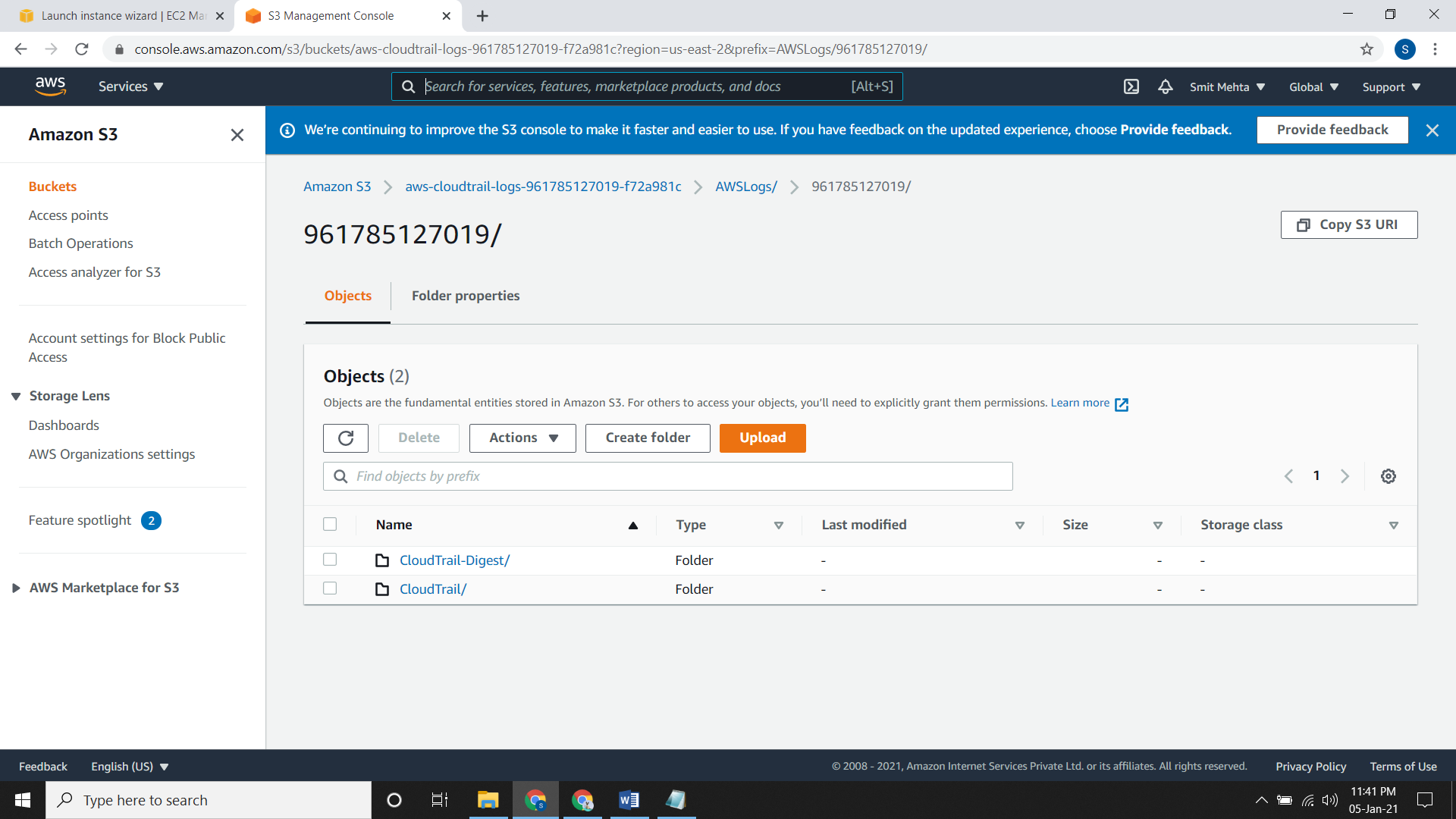
1. If **Management events,** then select the API activity.
2. If **Data events,** then give the data event source as S3 or Lambda.
3. If **Insight events,** then check the charged which are applied.

* Here in events you can choose multiple events. Preview it and create the trail.



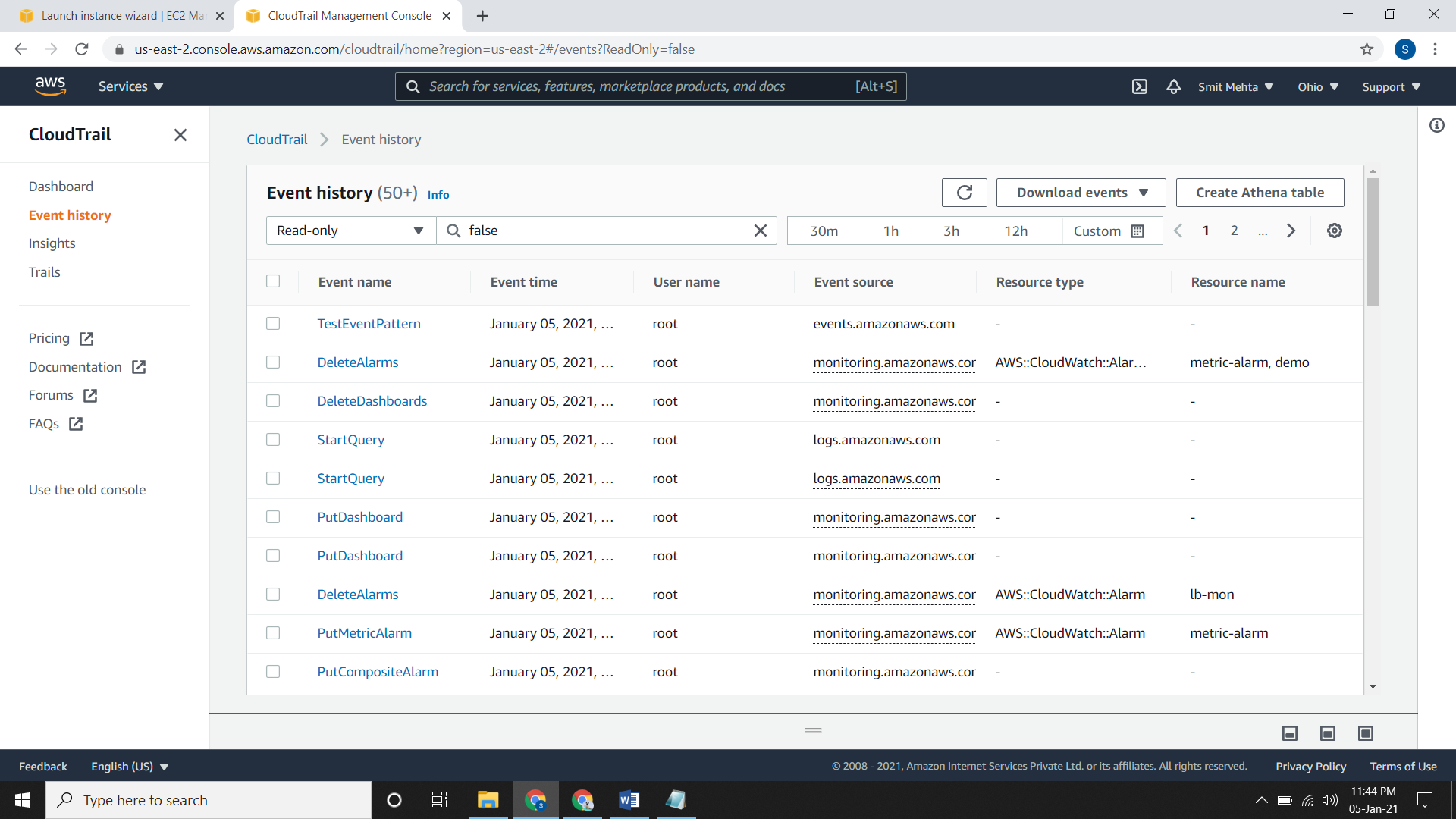
**View your log files**

* Go to S3 bucket which you had assigned to the trail or else go to the trail and click on the **trail log location**

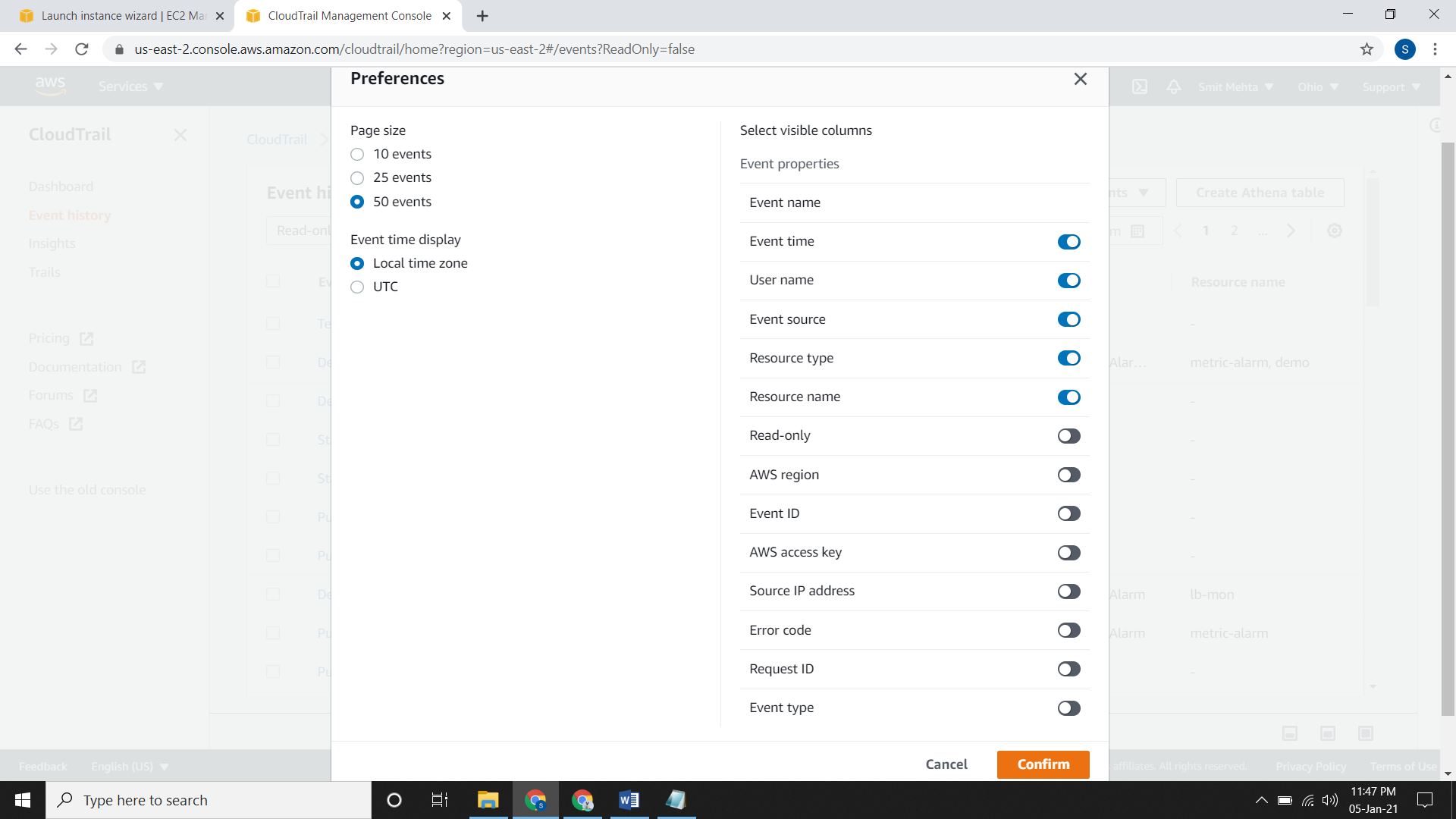


**To view CloudTrail events**

* Go to CloudTrail, choose Event history a list will appear.
* You can download any of the event in CSV or JSON file.



* If you want to display some other option click on the gear icon and select accordingly.

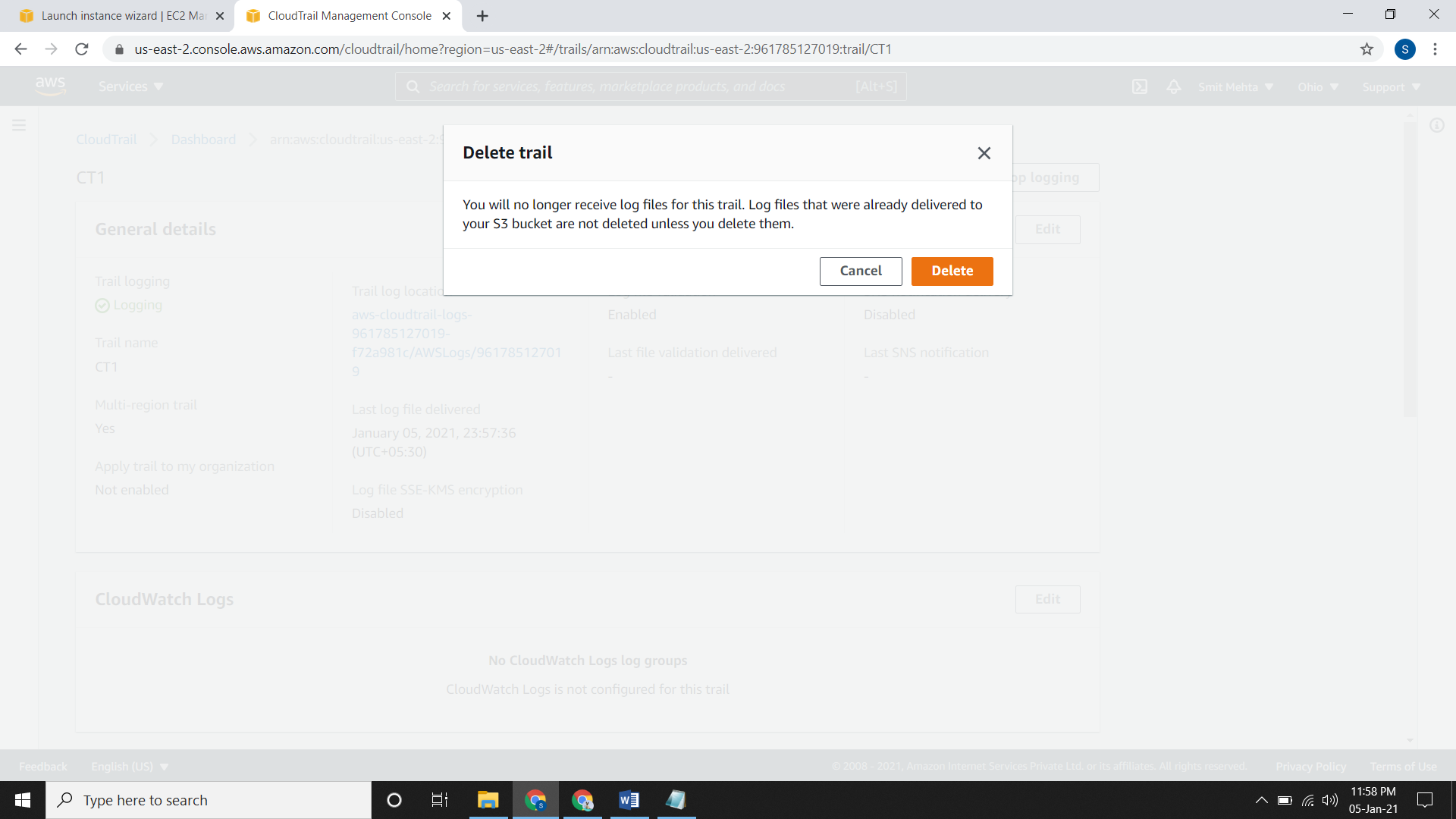


**Updating a Trail**

* Go to CloudTrail dashboard, click on the trail open it and choose the **EDIT** option.
* Make the changes which you want to make and save it.

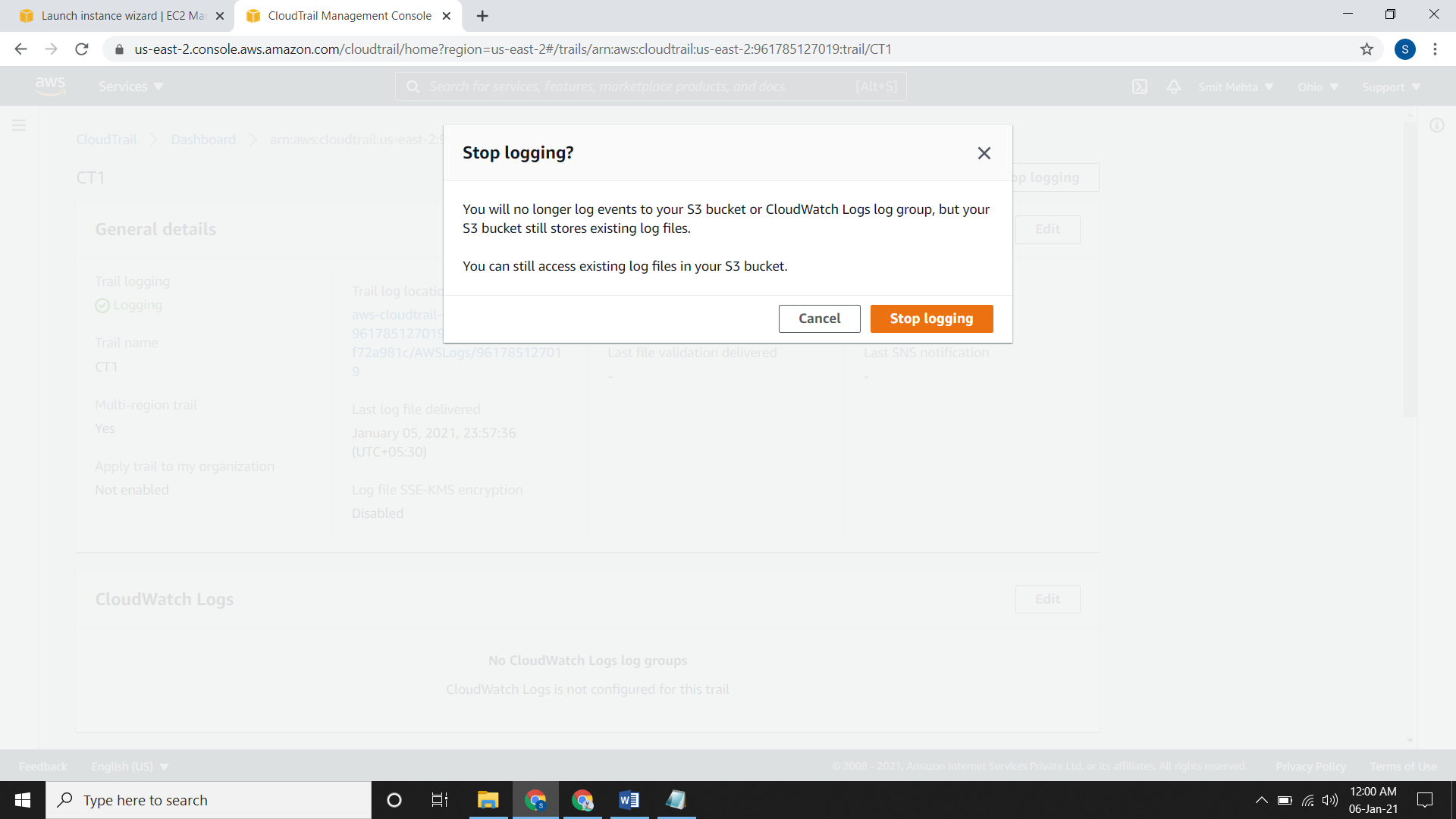
**Deleting a Trail**

* Go to CloudTrail dashboard, click on the trail open it and choose the **DELETE** option.



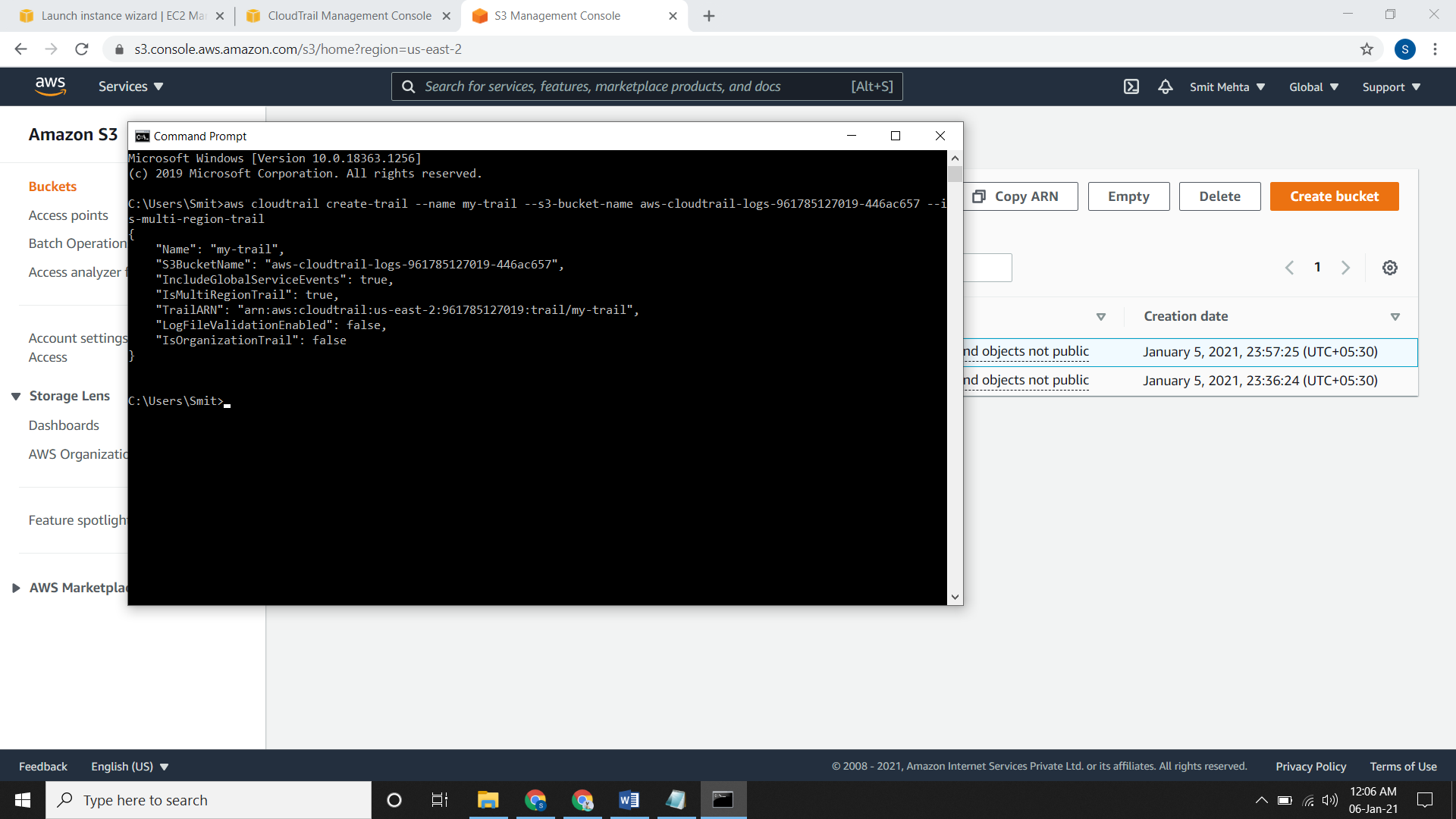
**Turning off Logging for a Trail**

* Go to CloudTrail dashboard, click on the trail open it and choose the **STOP LOGGING** option.

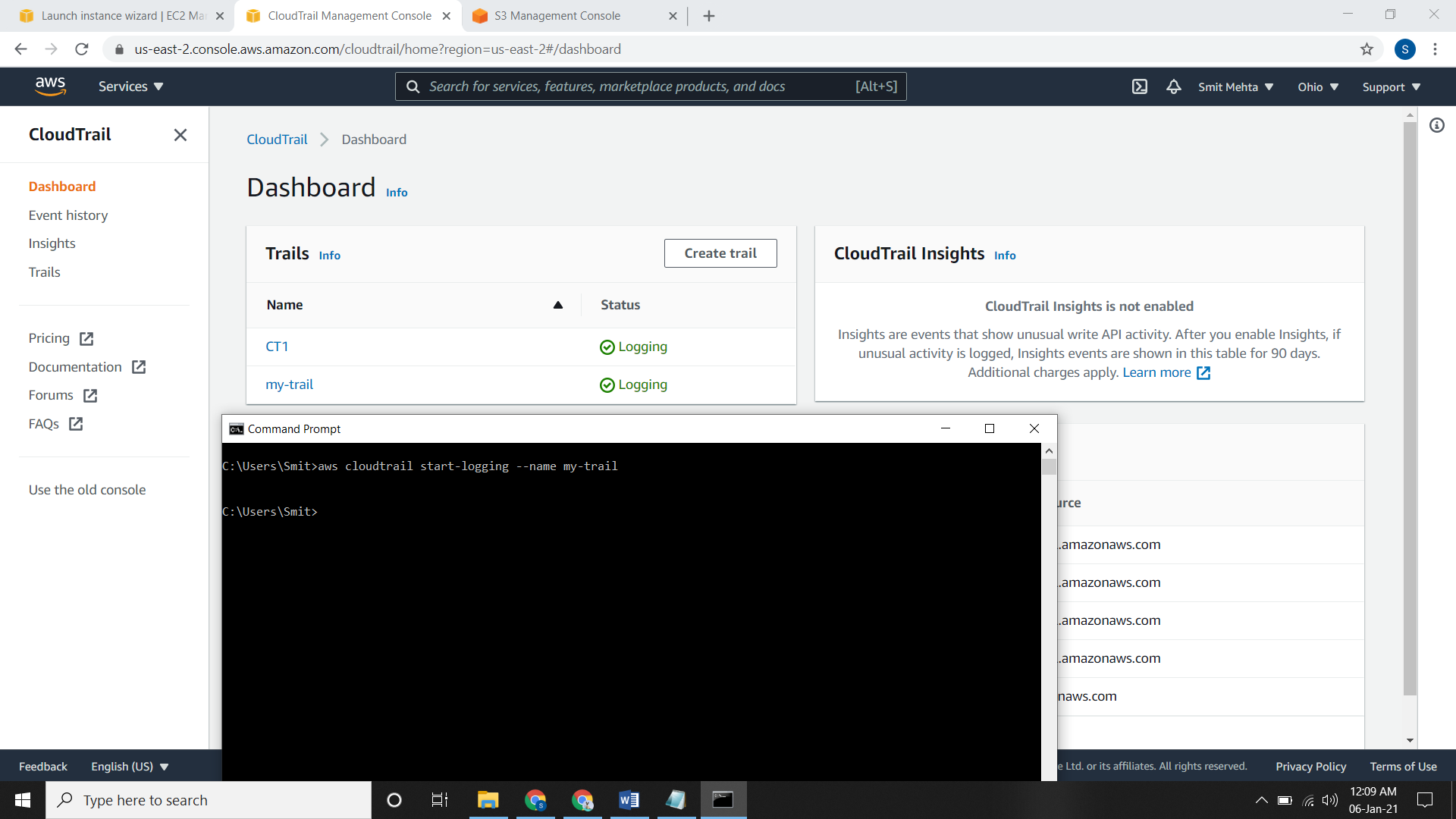


**Creating a Trail using AWS CLI**

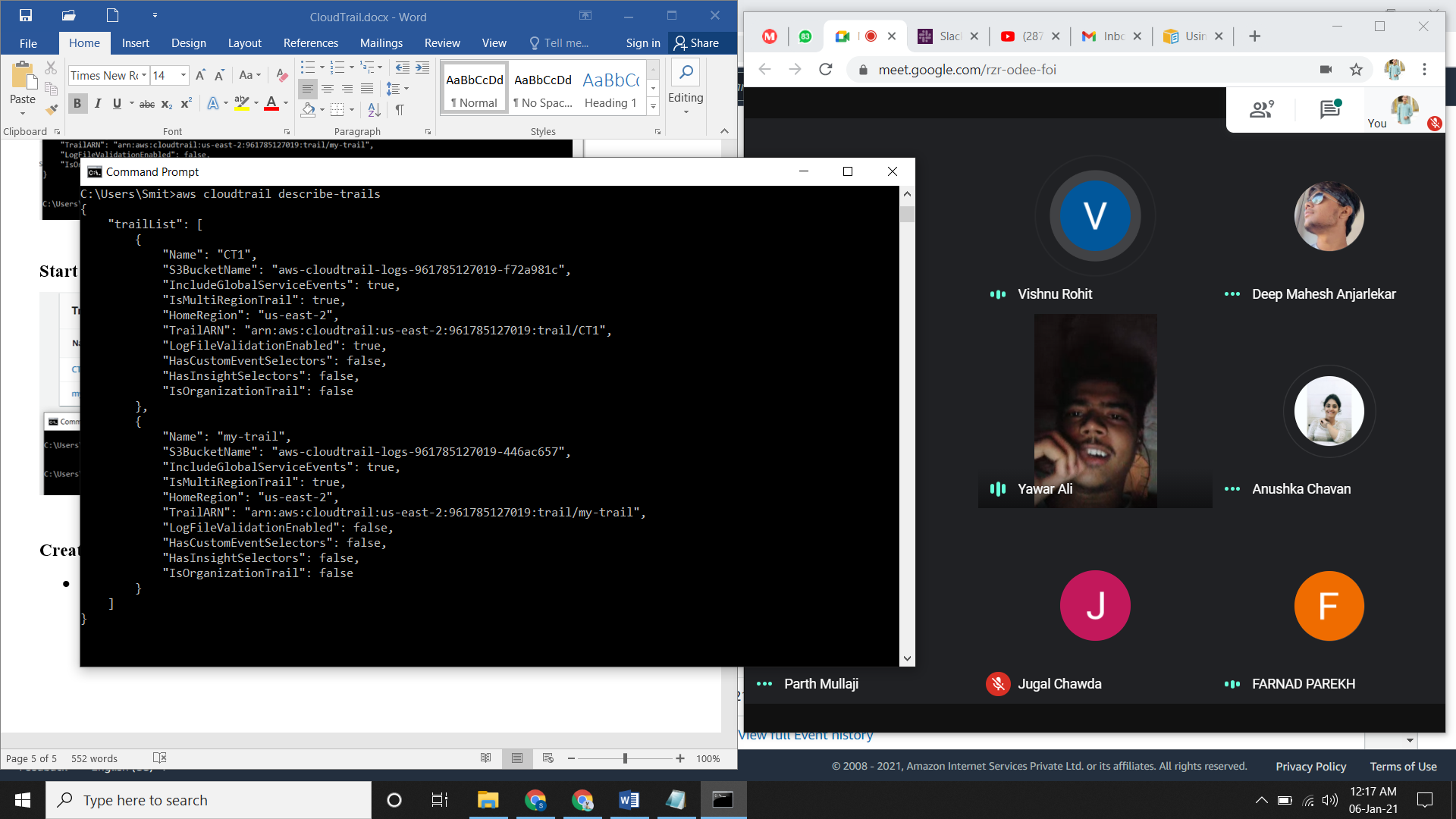
* create-trail command is used



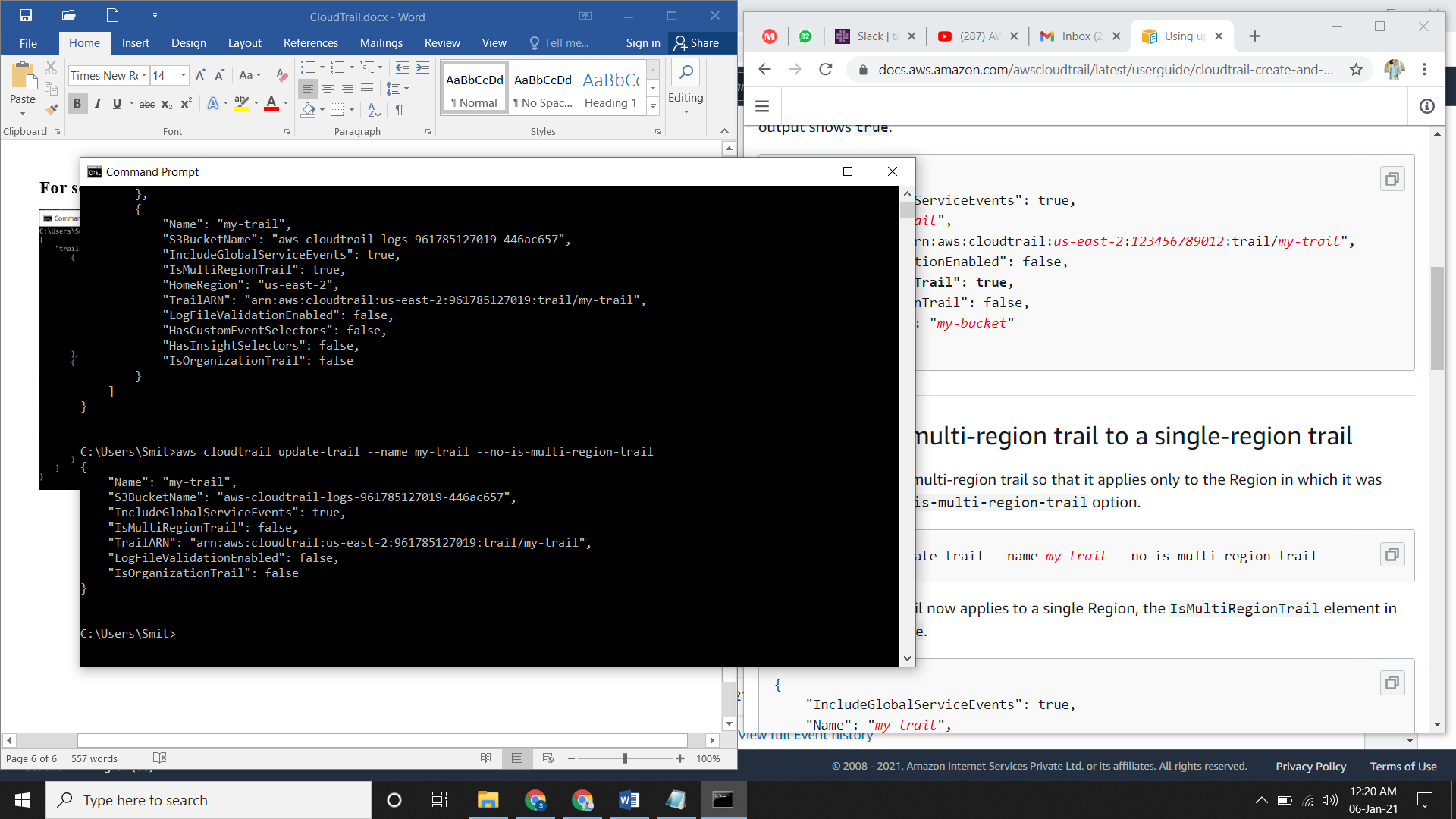
**Start logging for the trail**



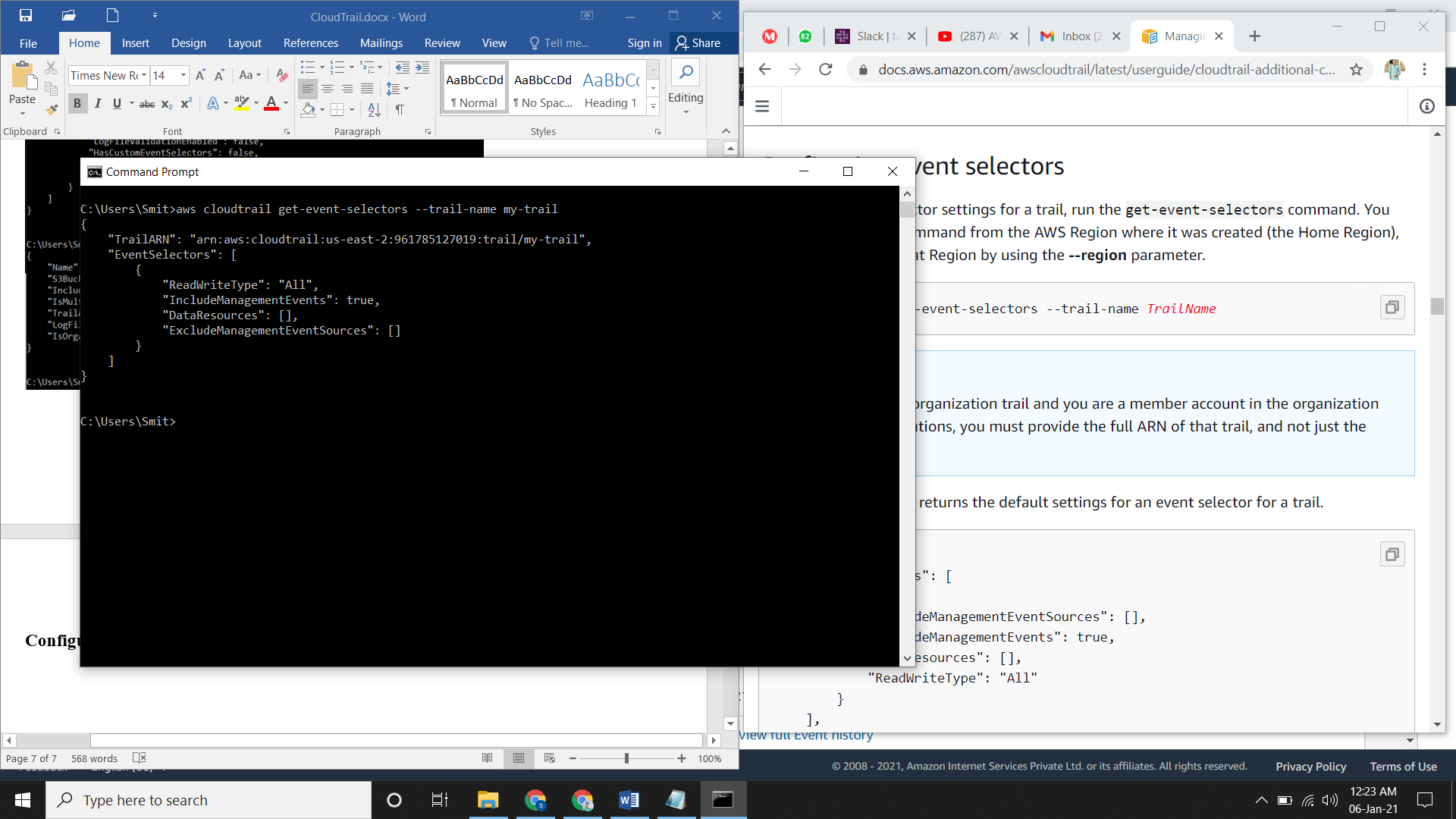
**For seeing all the trails**



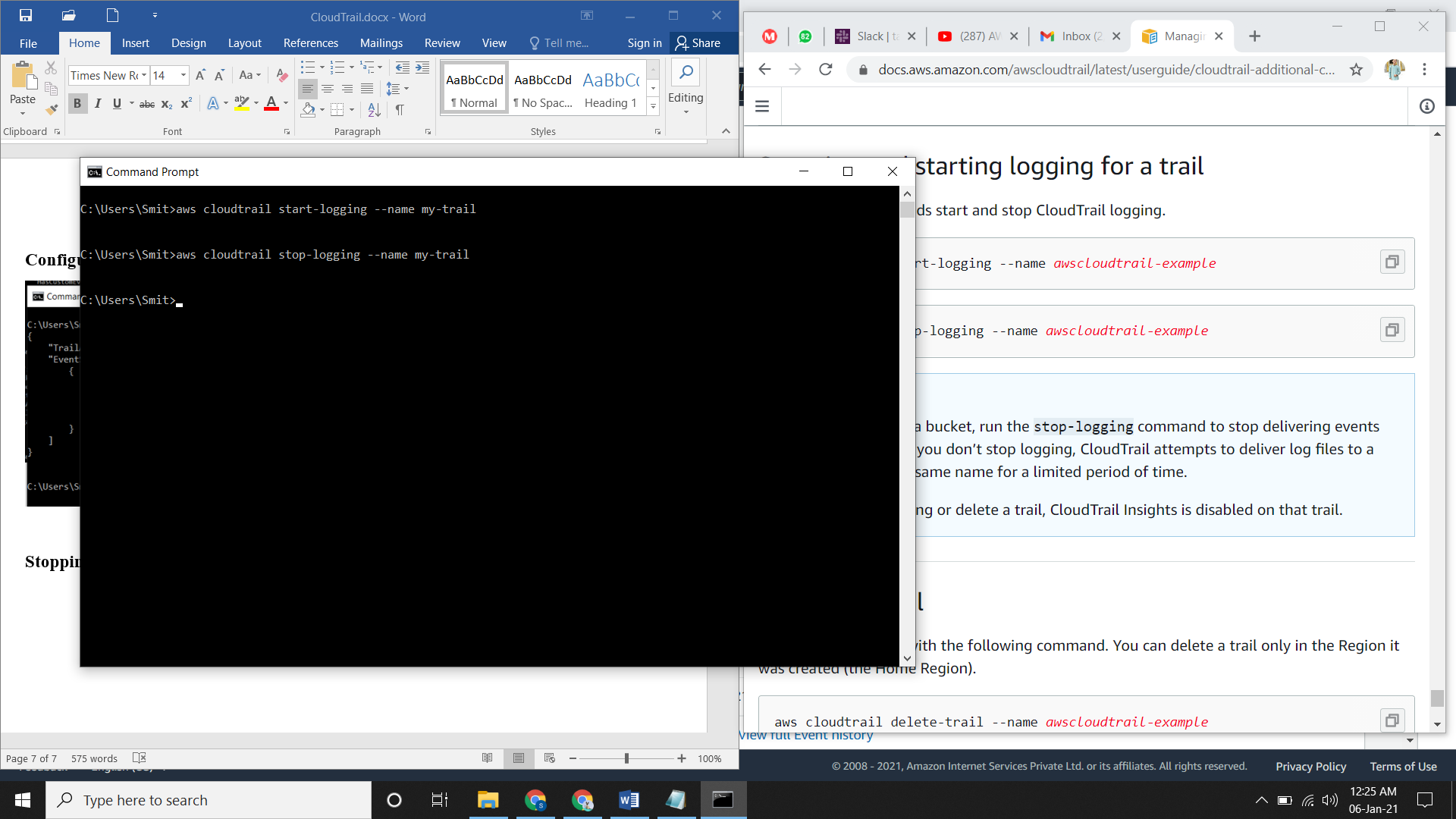
**Converting a multi-region trail to a single-region trail**



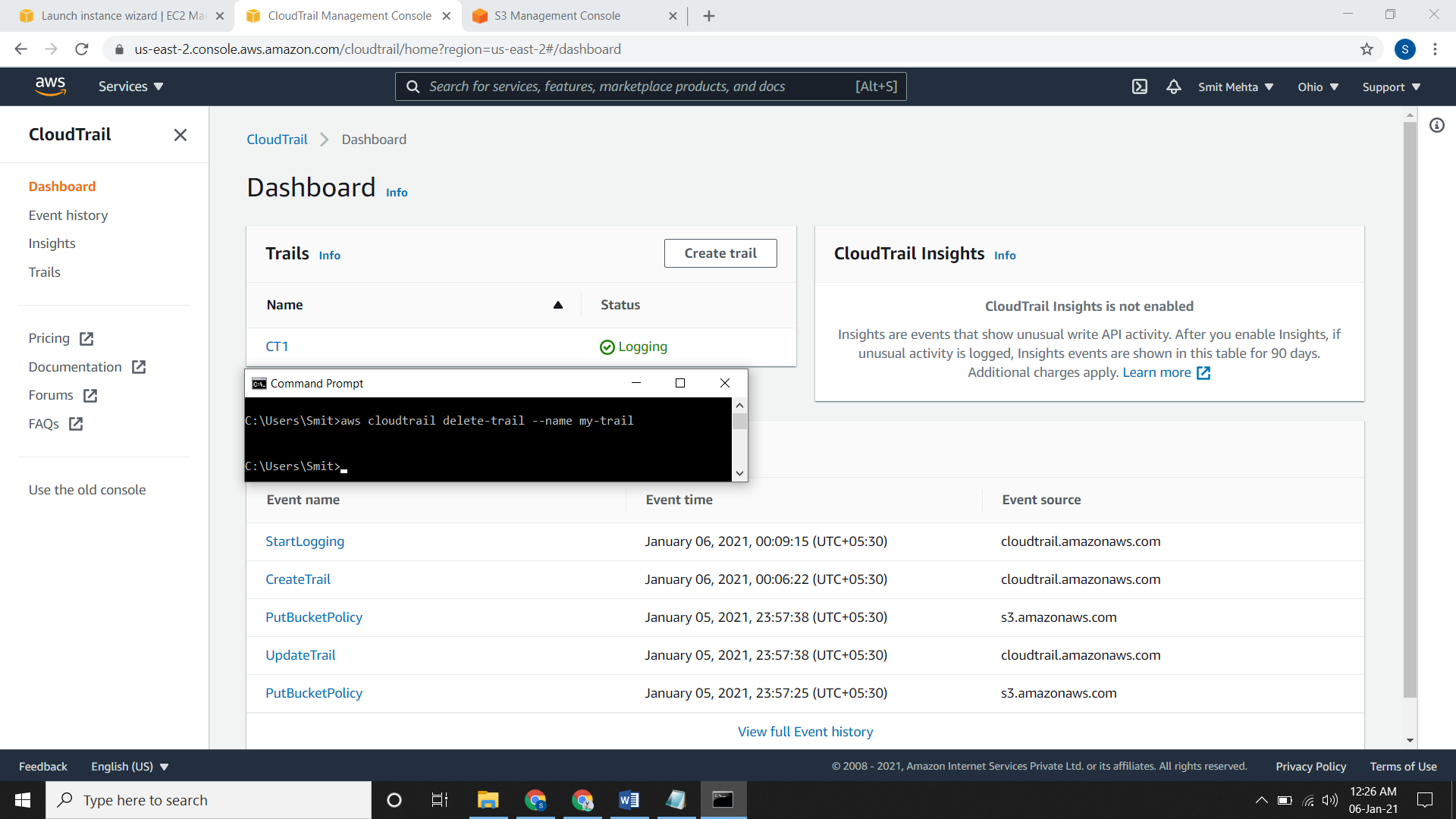
**Configuring event selectors**



**Stopping and starting logging for a trail**

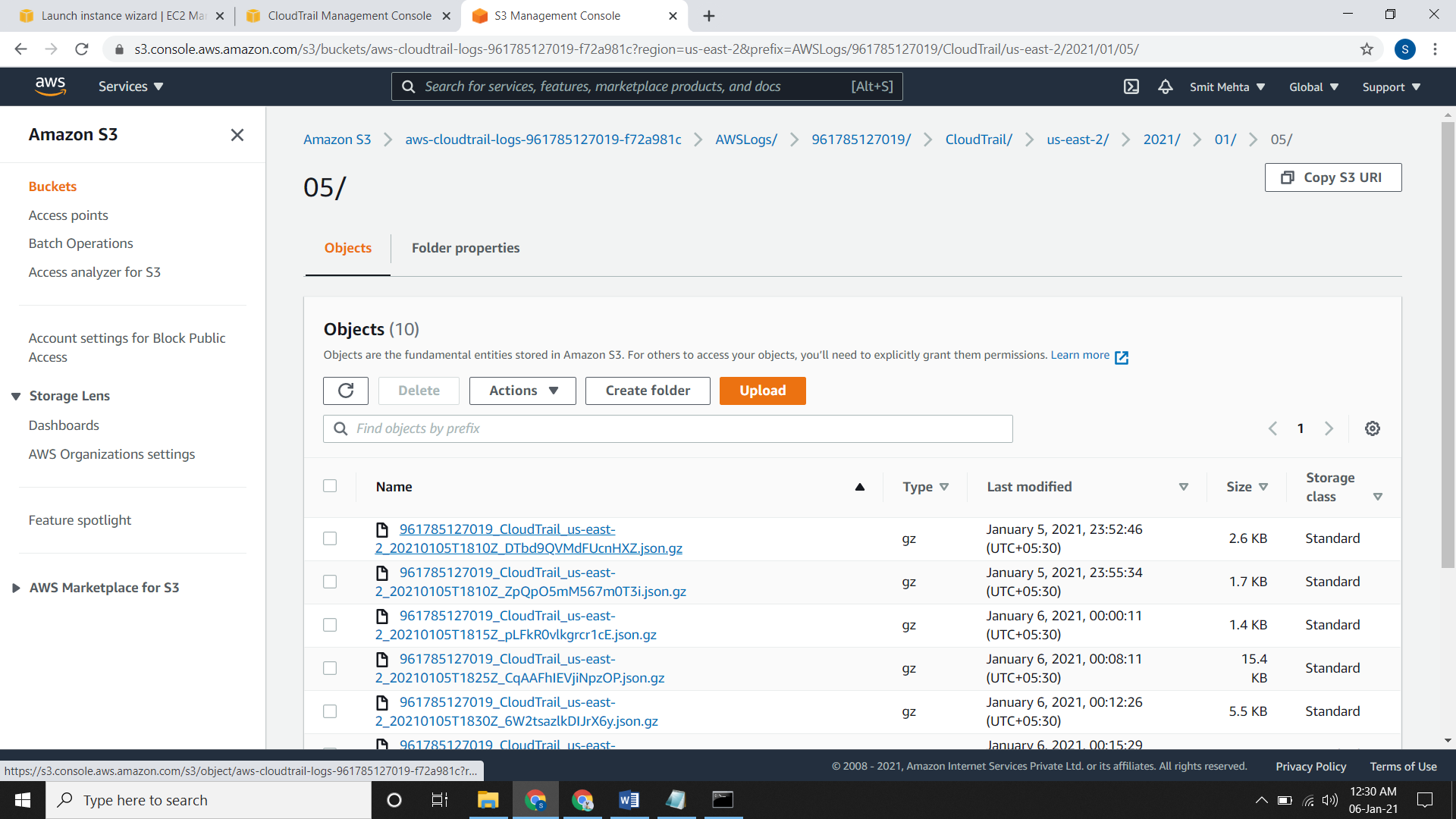


**Deleting a trail**



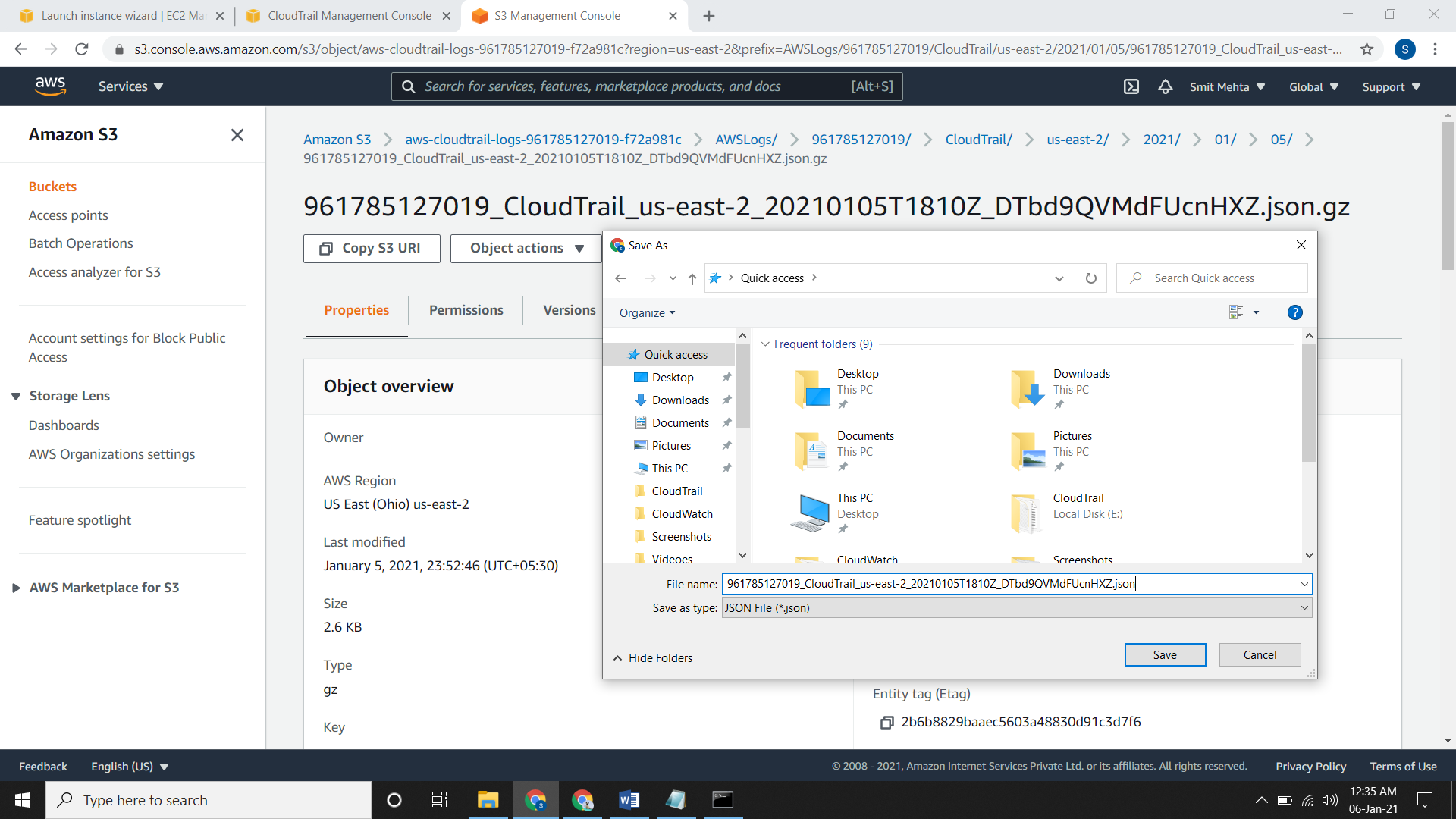
**Finding Your CloudTrail Log Files**

* The syntax for finding your desired log file is bucket\_name/prefix\_name/AWSLogs/AccountID/CloudTrail/region/YYYY/MM/DD/file\_name.json.gz
* Here the prefix\_name is optional.



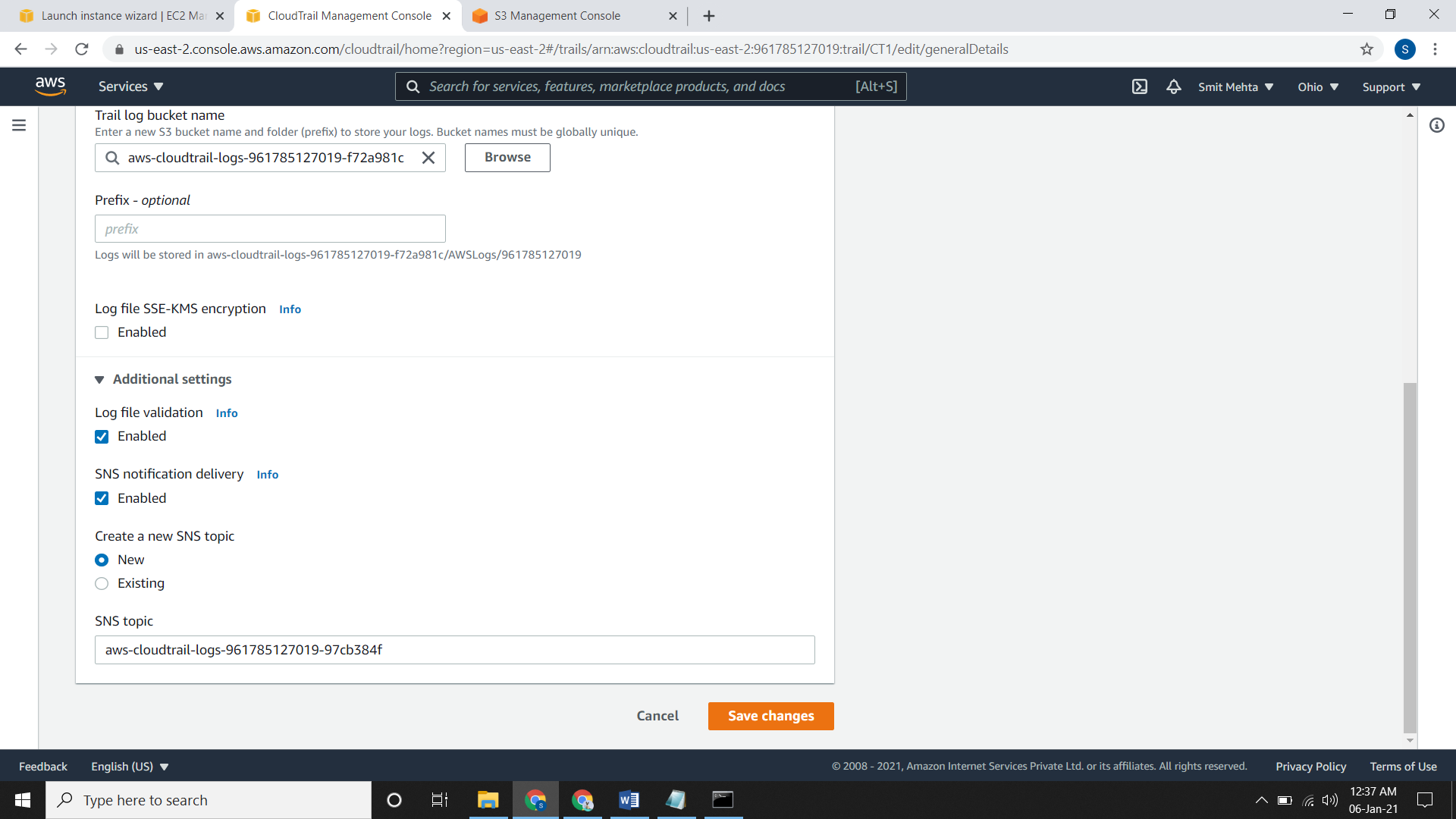
**Downloading Your CloudTrail Log Files**

* For downloading any log files, go to the location of the file in S3 bucket and open it.
* After opening that file click on **Object actions** and then download it. Your file will be in JSON format



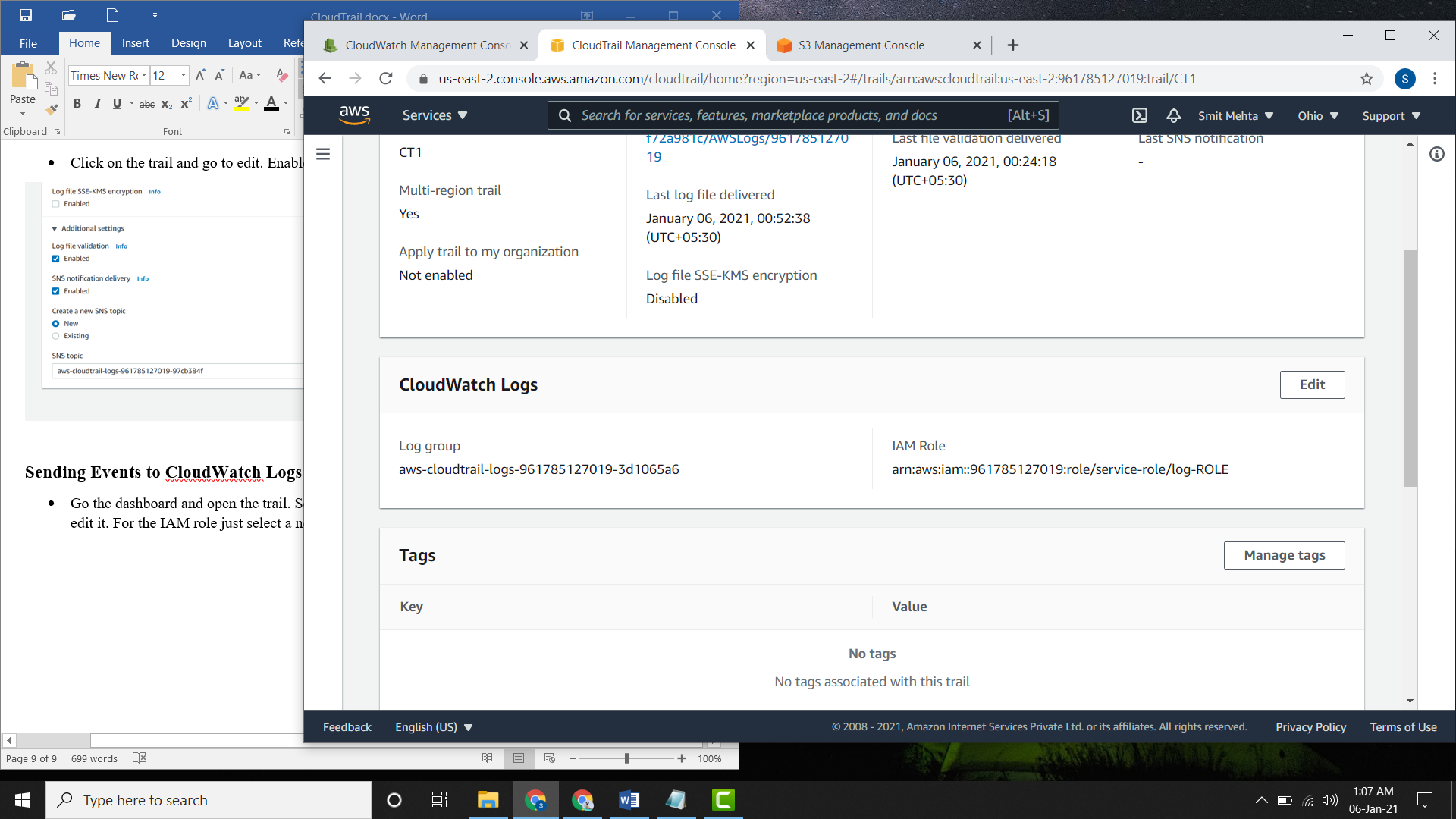
**Configuring Amazon SNS Notifications for CloudTrail**

* Click on the trail and go to edit. Enable the **SNS notification delivery** and save it.

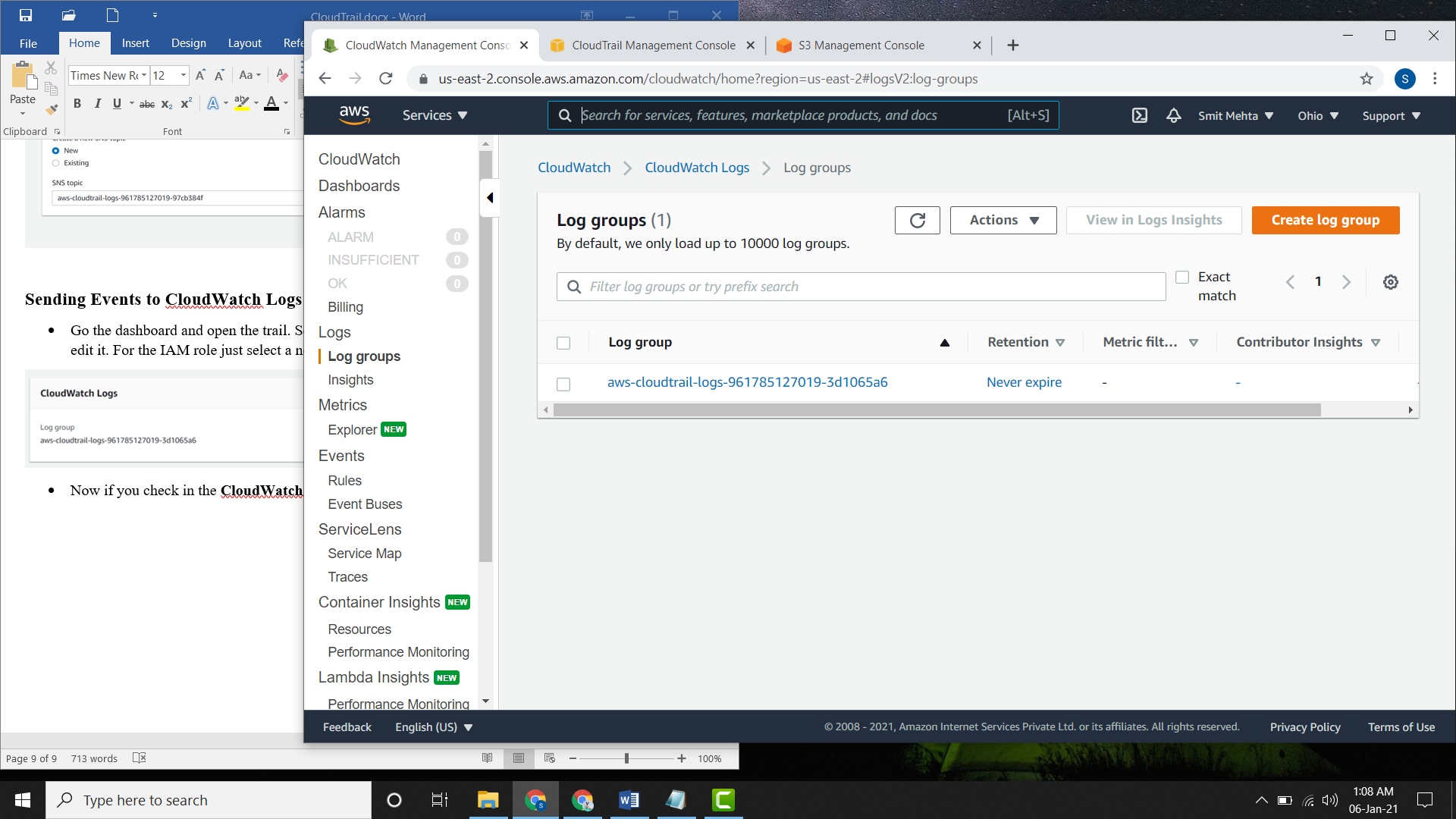


**Sending Events to CloudWatch Logs**

* Go the dashboard and open the trail. Scroll down and you will see **CloudWatch Logs** edit it. For the IAM role just select a new role and give a name. Save it.



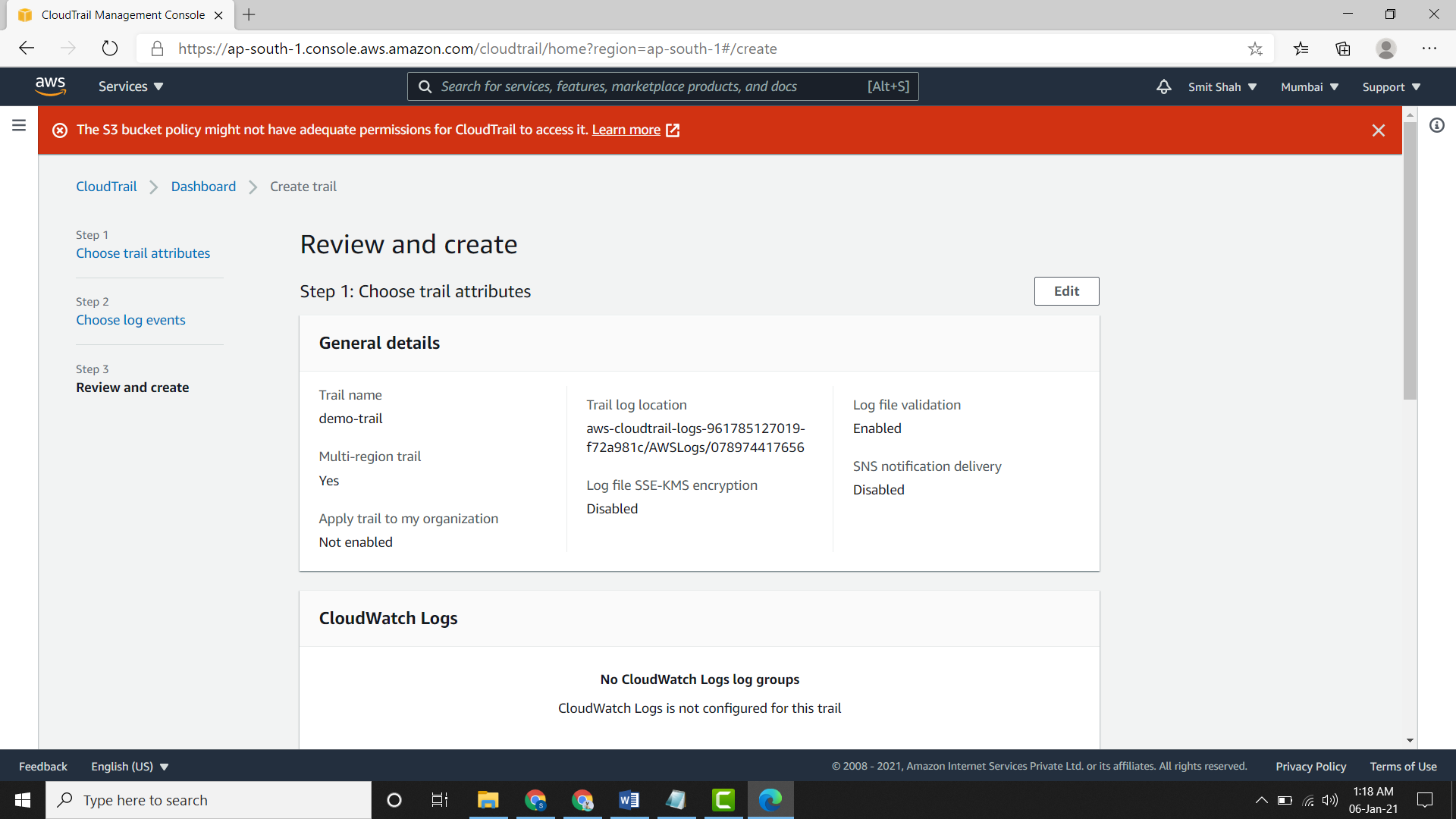
* Now if you check in the **CloudWatch Log Group** page you can see this log group.



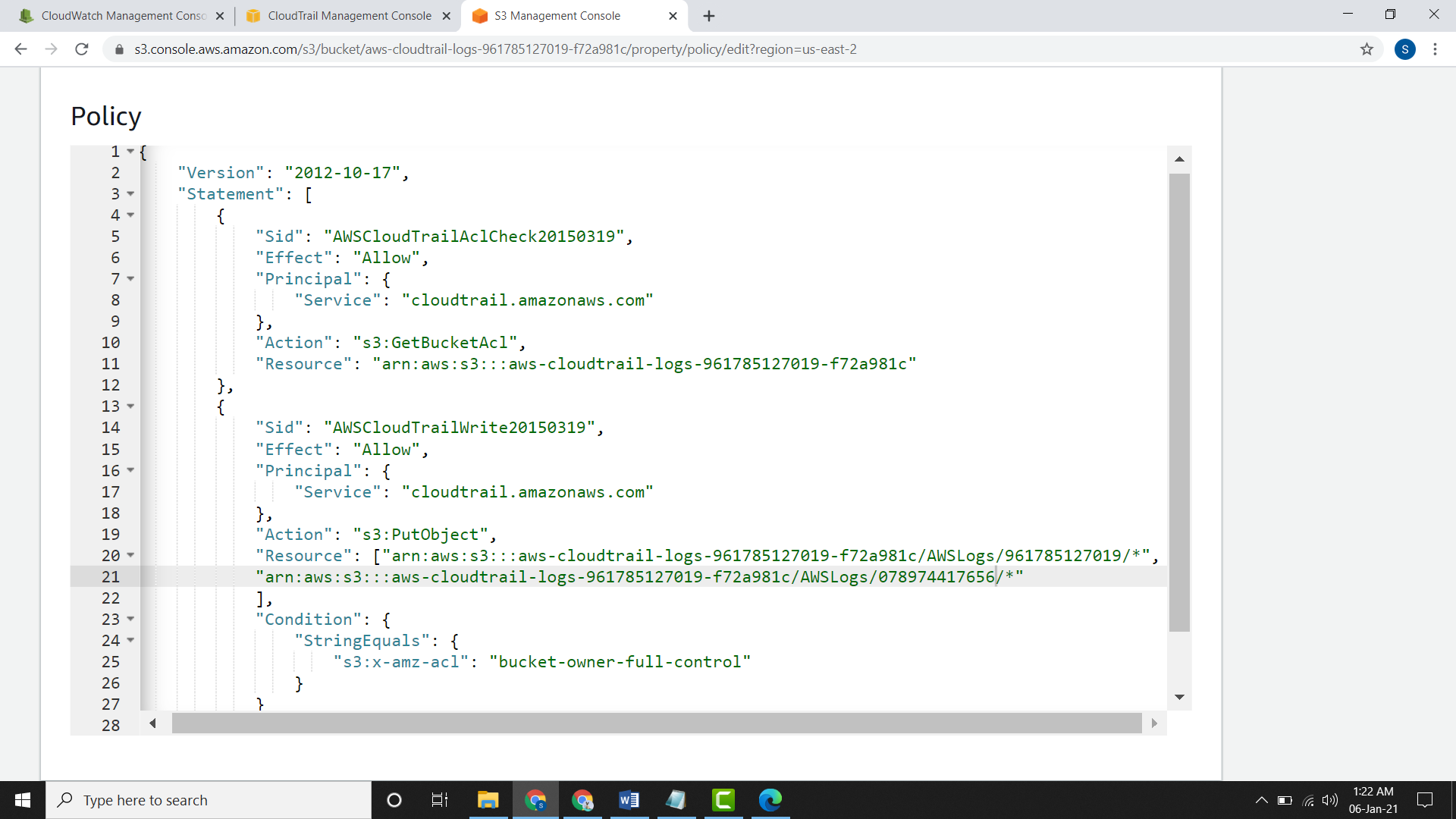
* If you create an alarm for it and the alarm goes on then by the use of SNS notification you will be notified that this thing has occurred.

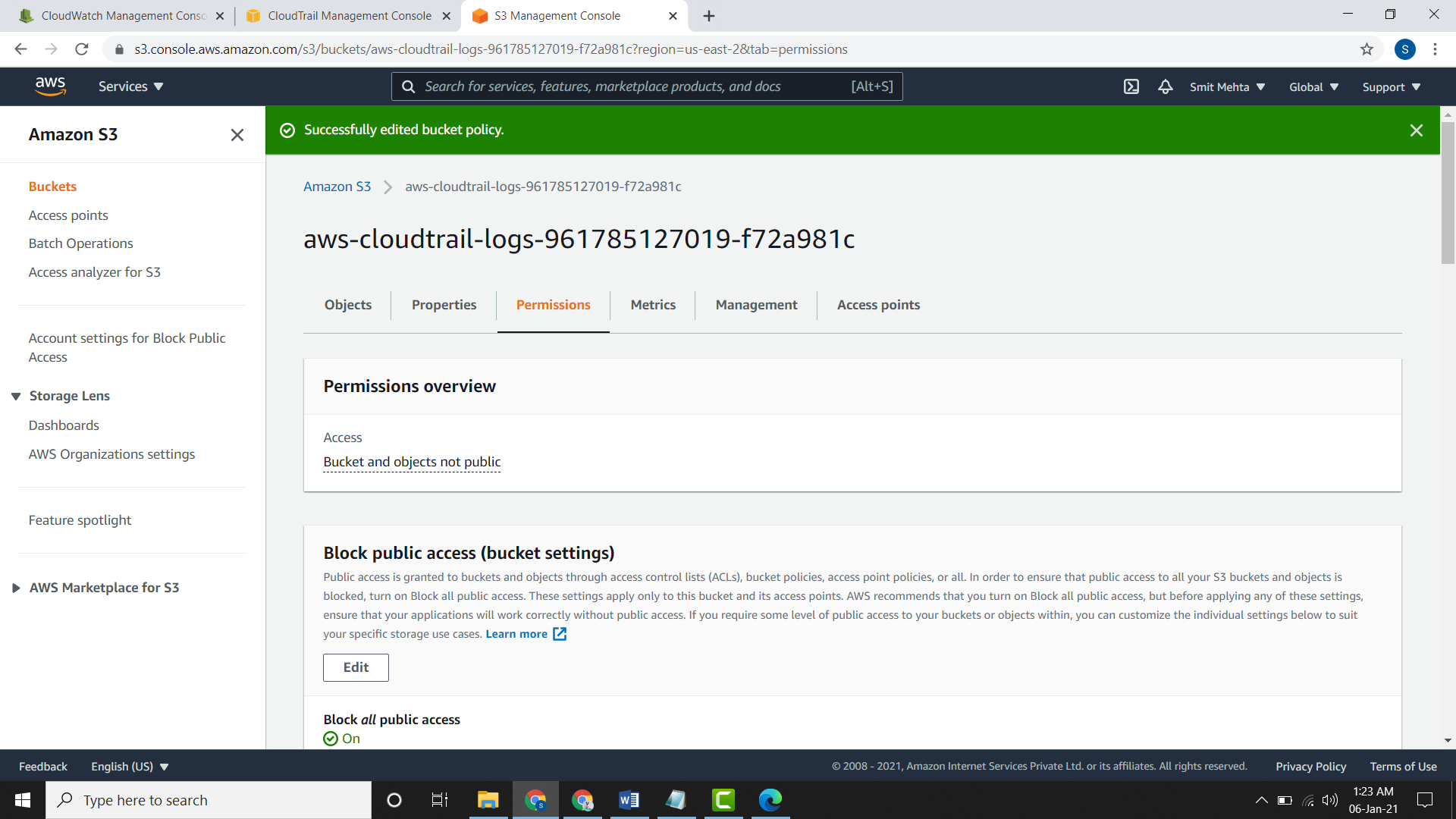
**CloudTrail Logs from multiple accounts to one S3 Bucket**

* Creating a trail in new account and adding the same bucket name of the old account.
* An error occurred because the bucket doesn’t have adequate permissions.

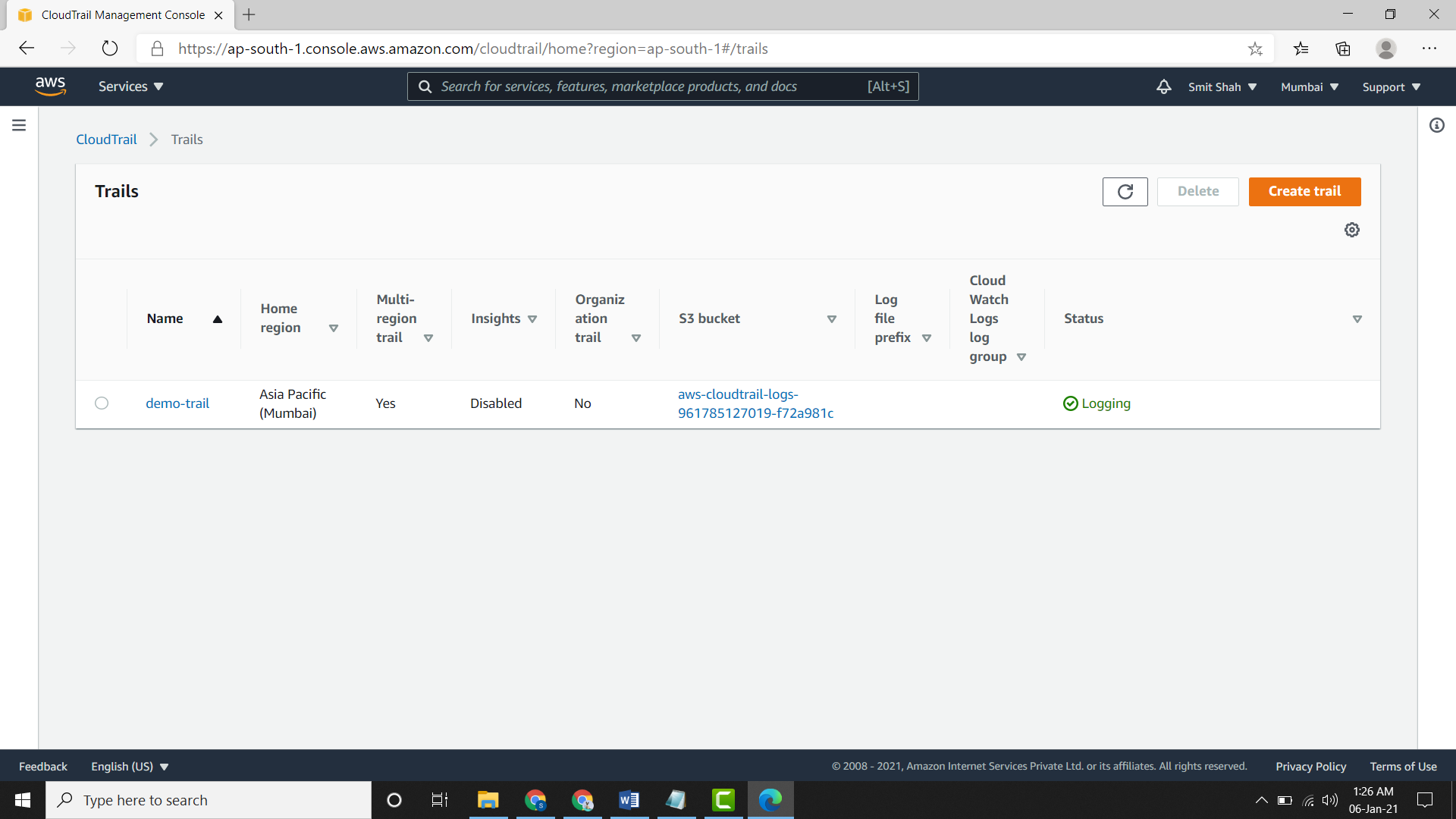


* For updating the bucket policy, go to the bucket and then to permissions. Now scroll down and edit the bucket policy where "Action": "s3:PutObject"

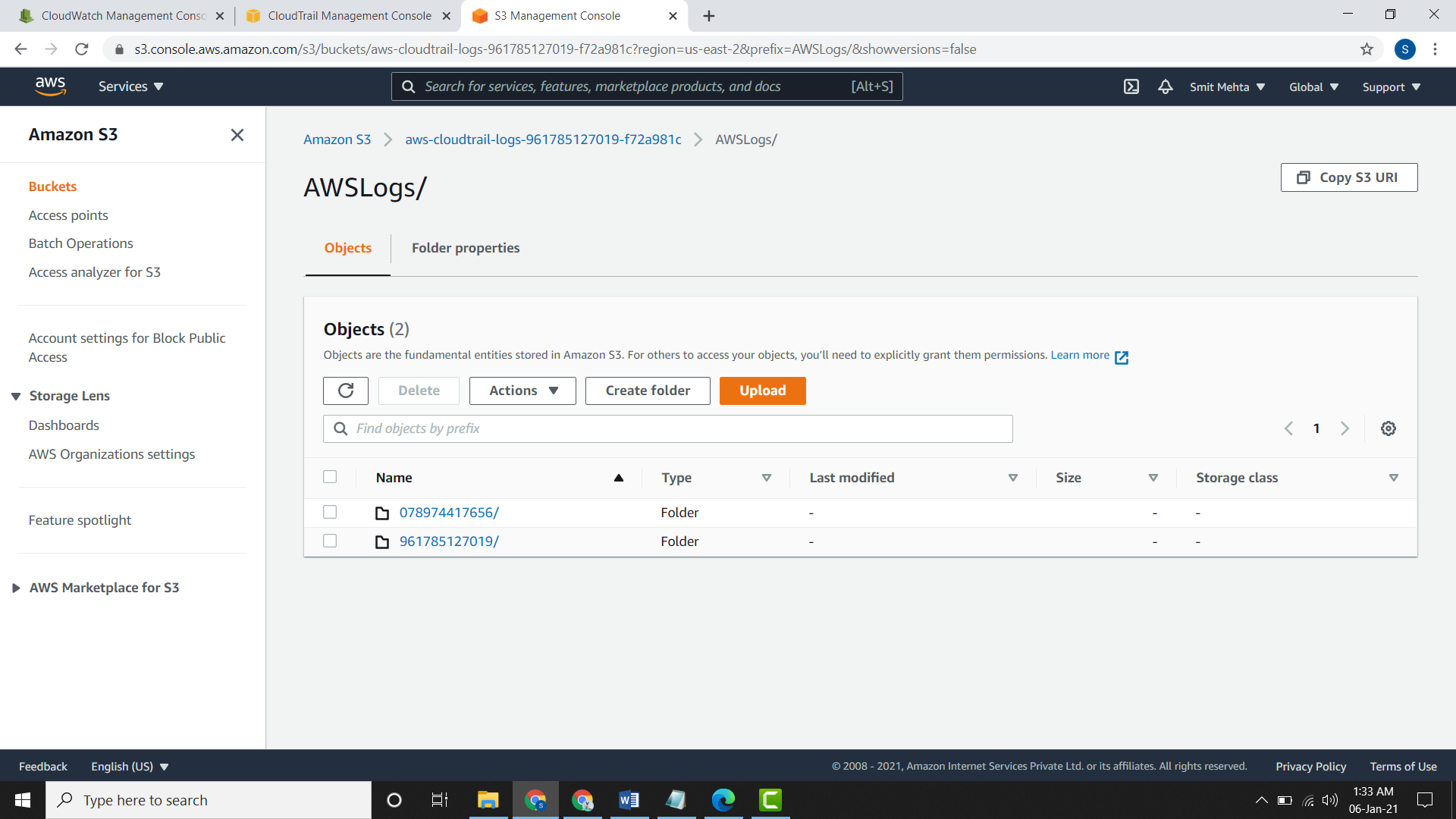




* After the policy has been successfully edited you can create a trail in another account.
* Here you can create alarms if required.



* After this if you check the s3 bucket you will find **2 account no**. assigned to it.



**Integrity of log files OR Validating CloudTrail Log File Integrity**

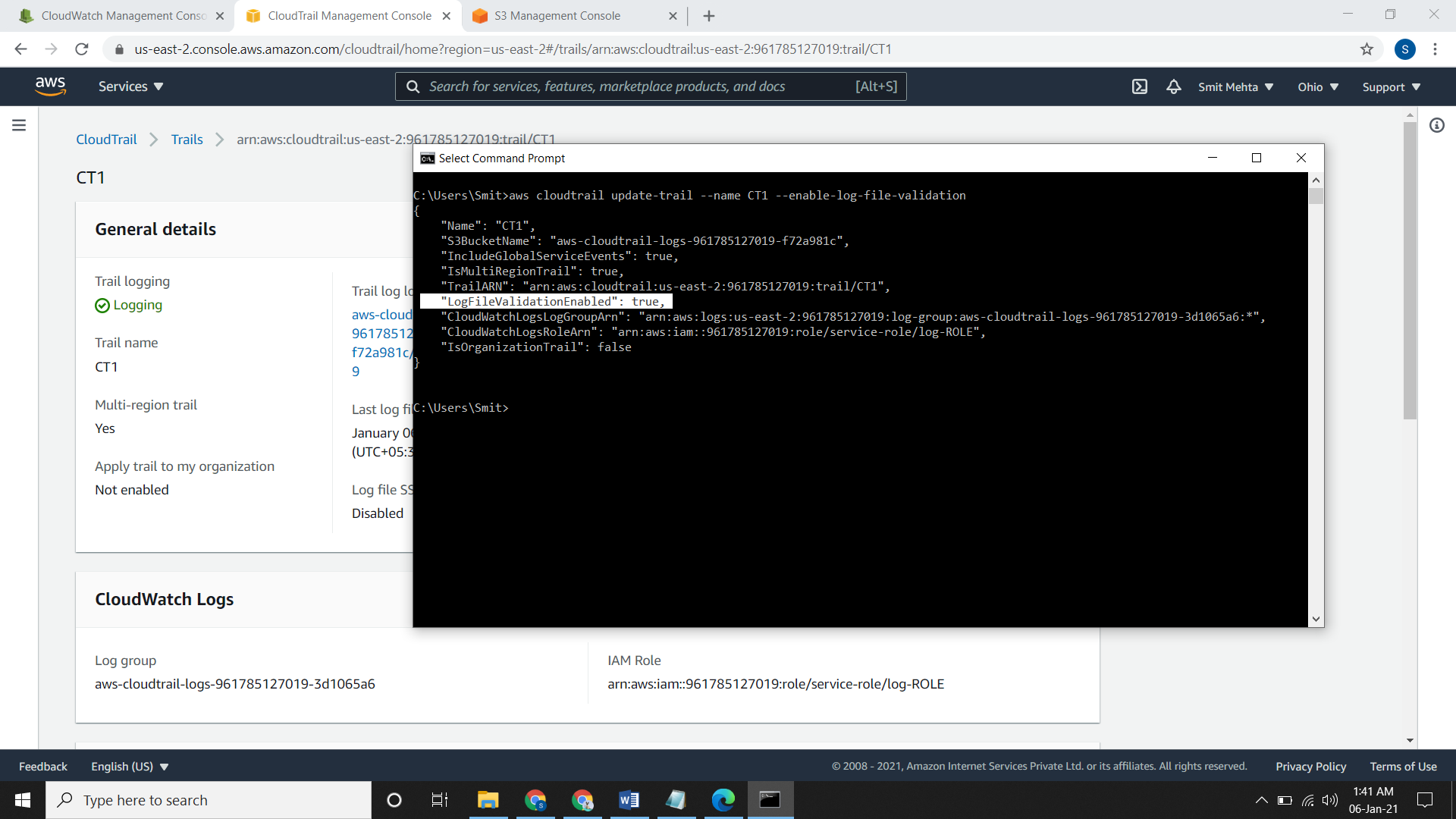
* In your S3 bucket you might find 2 types of folder after you go into your account no.

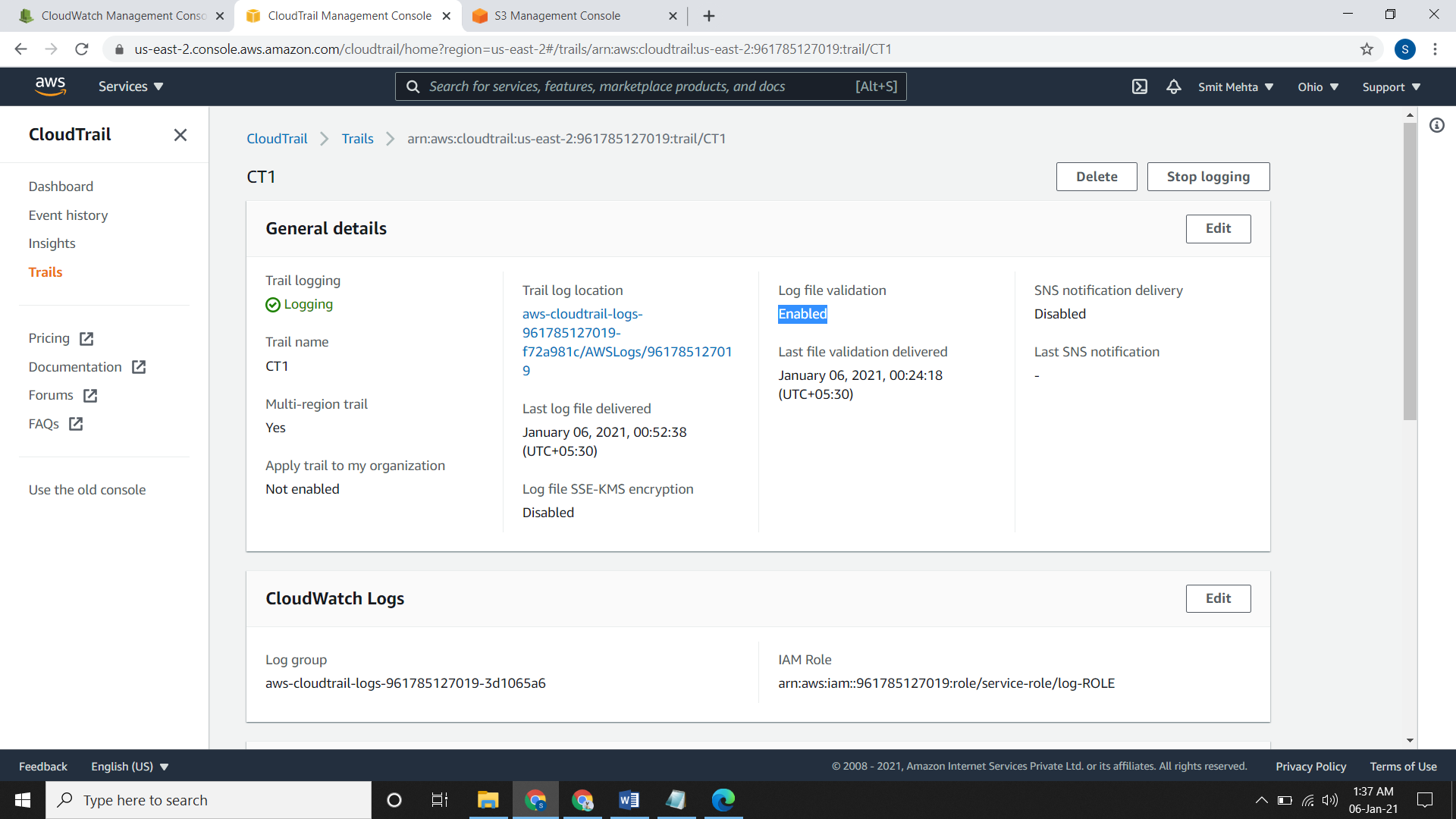
1. CloudTrail – Here normal log files are stored.
2. CloudTrail Digest - This folder contains some has values of the log files delivered and are signed by cloudtrail.

* Now go to the trail and check the status of **Log file validation.**



* If it is disable you can enable it from console via the **Edit** option or through CLI





* For checking which file is updated or modified or changed or deleted the following command is used. Syntax of the command is

aws cloudtrail validate-logs --trail-arn <trailARN> --start-time <start-time> --end-time <end-time> --s3-bucket <bucket-name> --s3-prefix <prefix> --verbose

* Here end time and s3 prefix is not mandatory.
* The **verbose** command specifies each and every file name and accordingly their details.