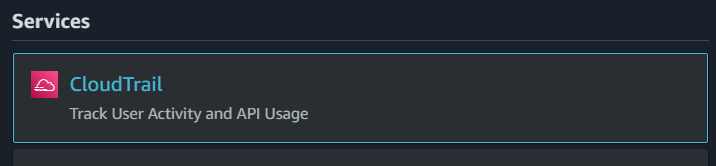
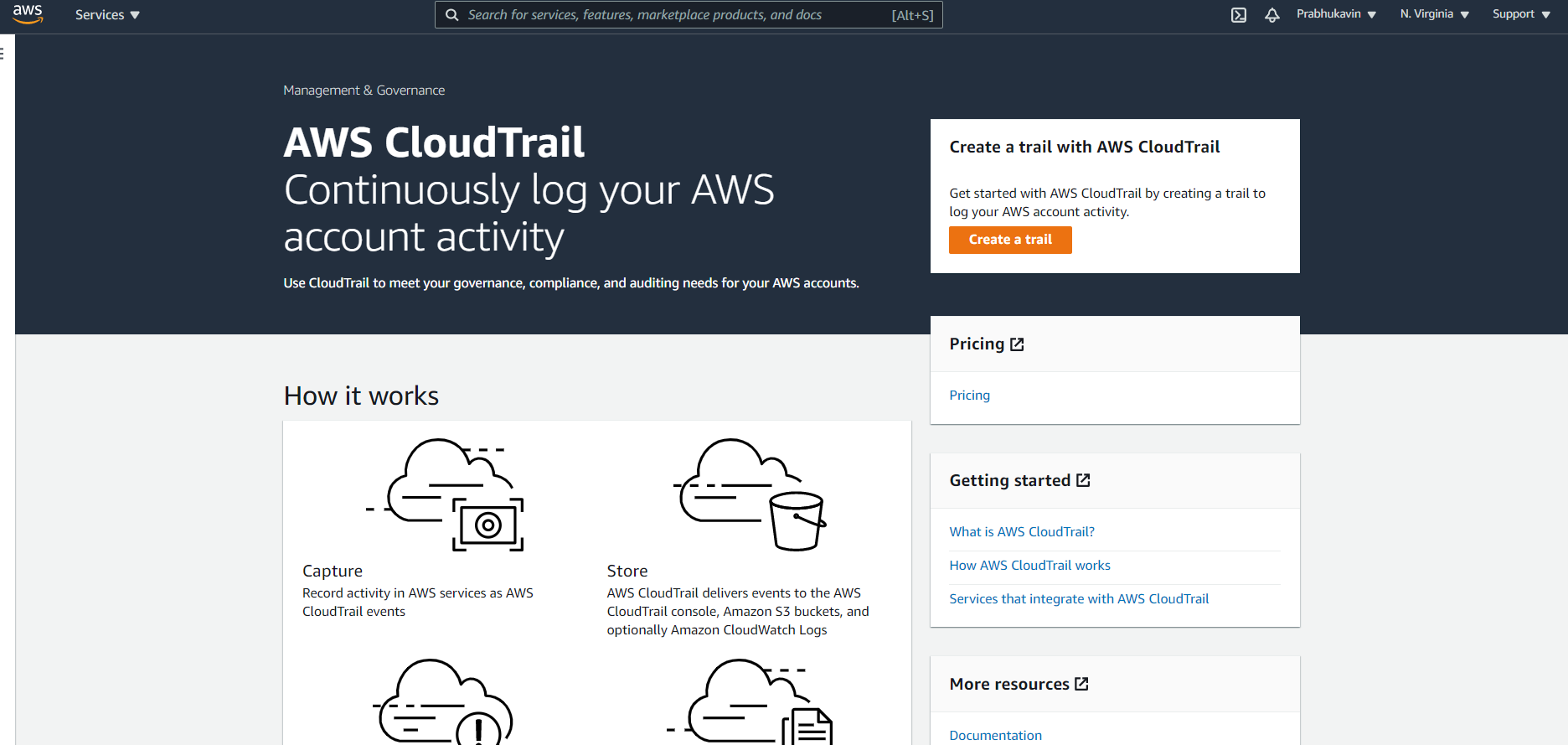
**AWS CloudTrail**

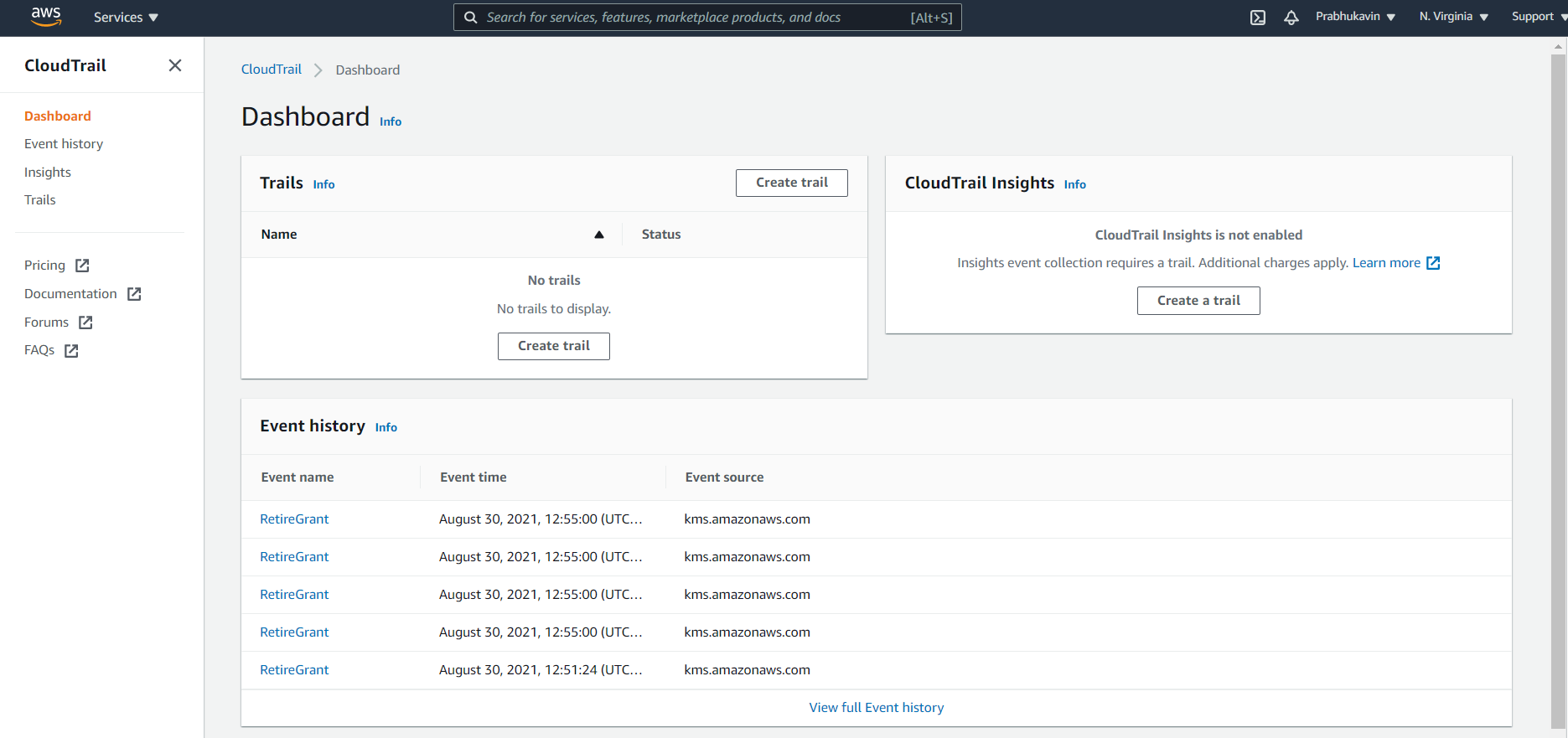
1. **Open CloudTrail**



**Click on cloud trail**

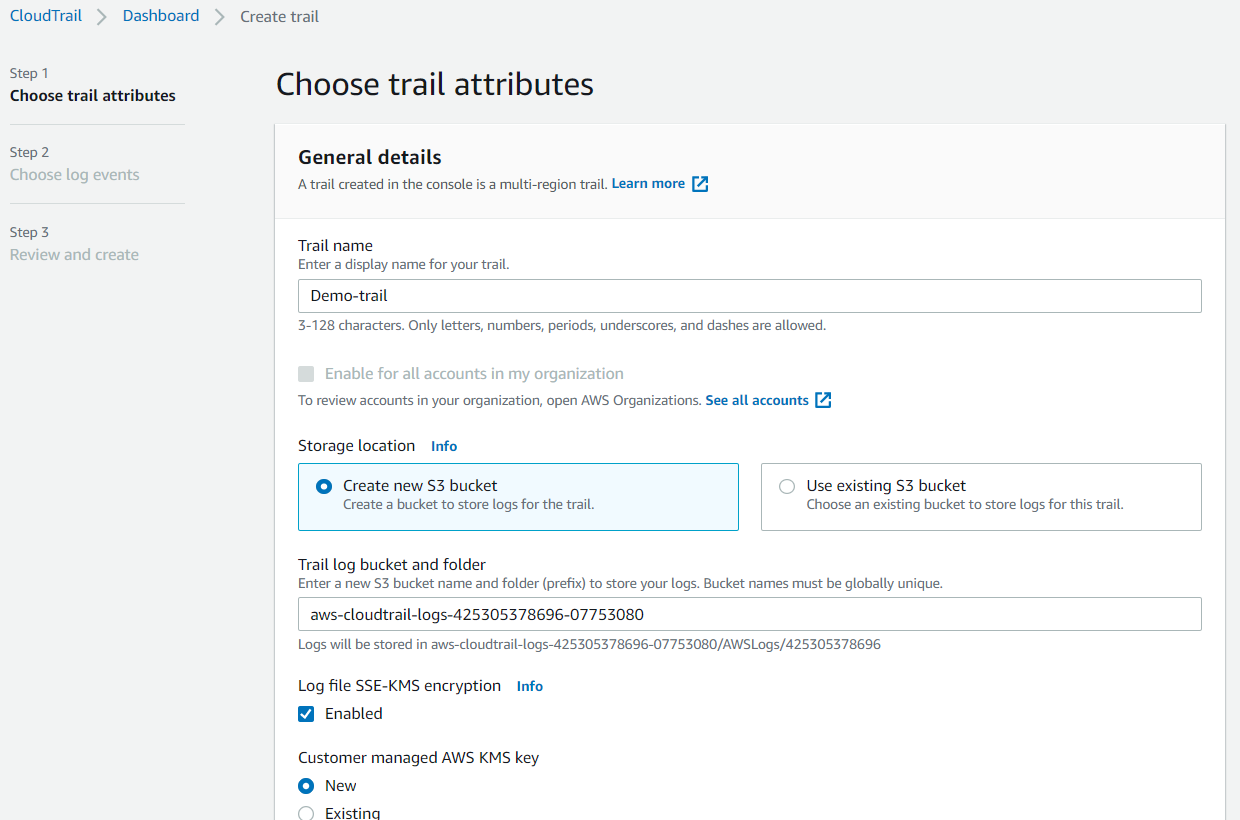


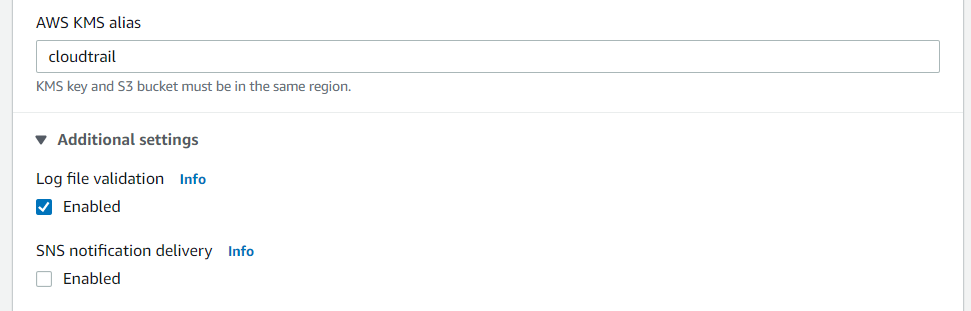
**Click on dashboard:**



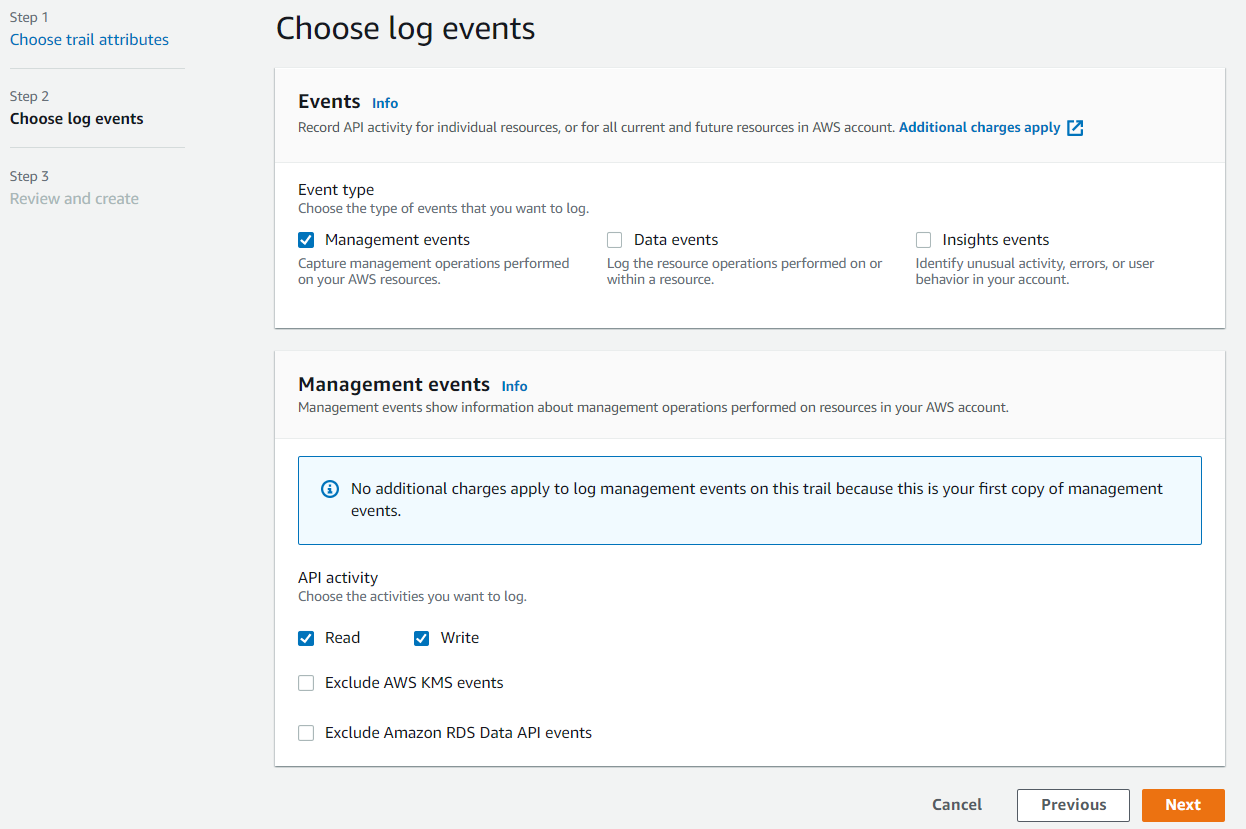
**This event history will be updated every 5 mins.**

**Click create trail:**





**Click Next.**

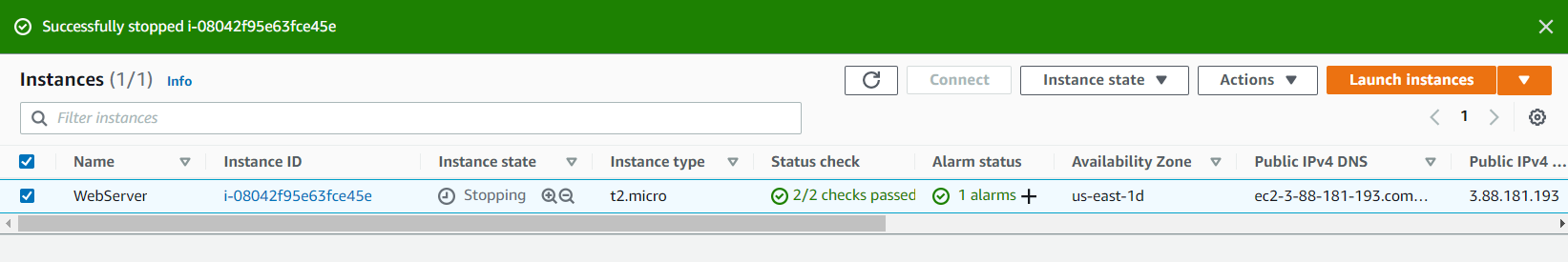


**Click Next**

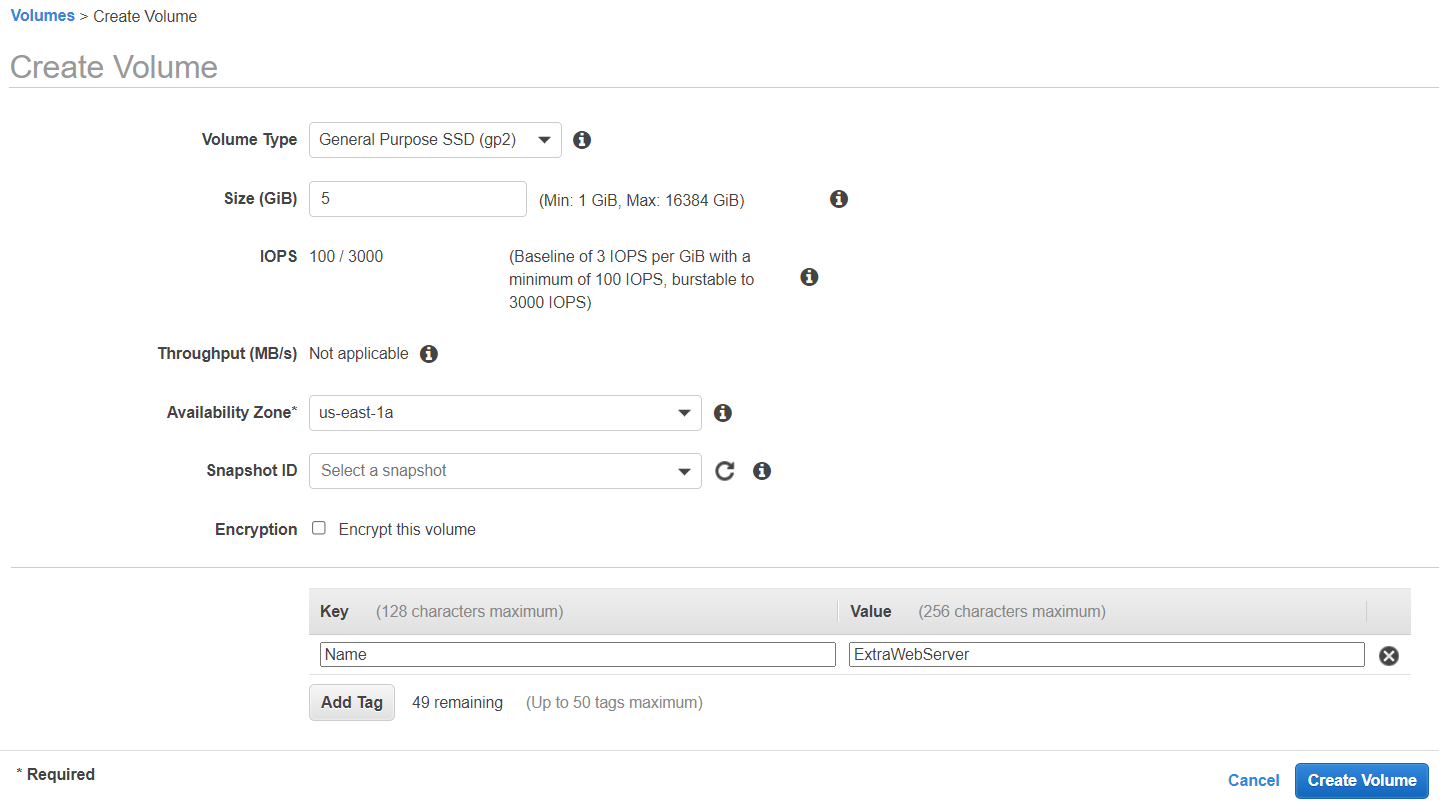
**Click “Create trail”.**

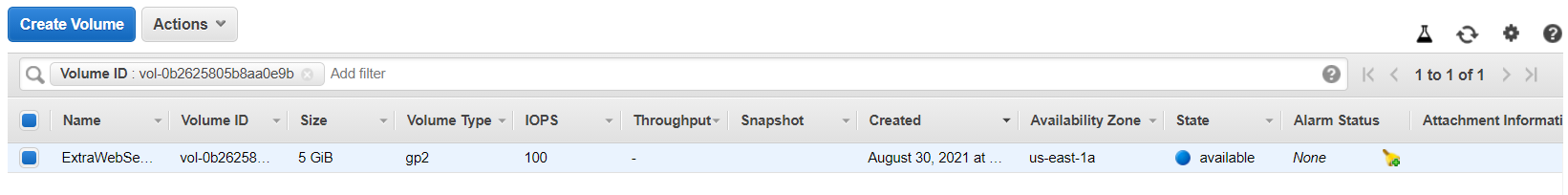
**Perform some activities in AWS**

**The running instance “WebServer” have been stopped.**



**Next new volume has been created**



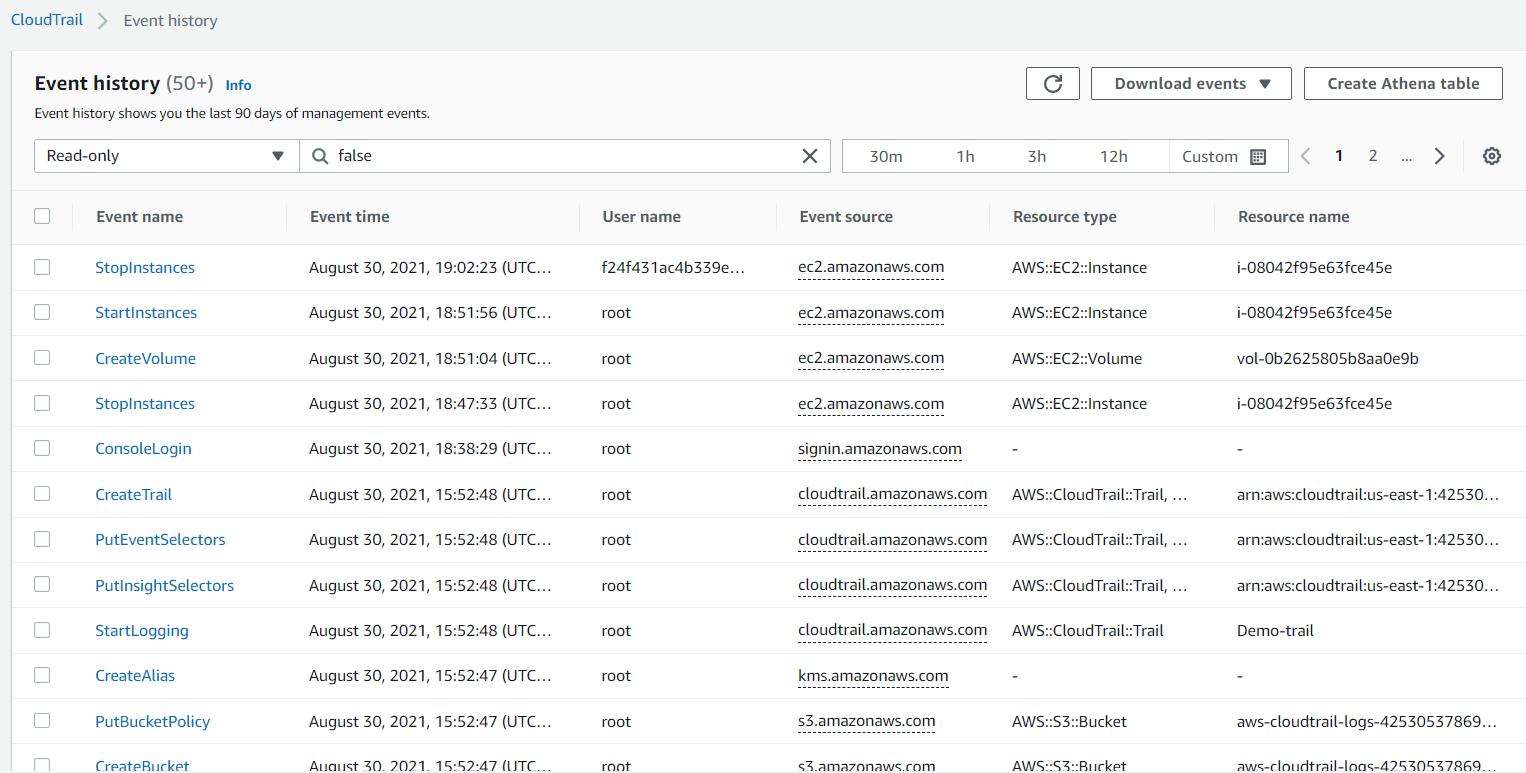


**You can do any activity as per your convenience.**

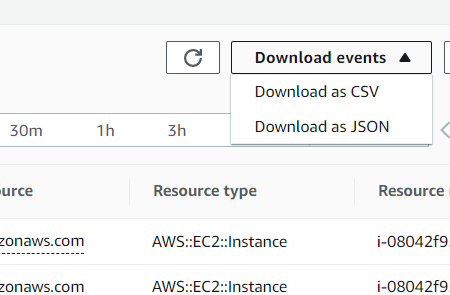
**So that these activities will be recorded in logs.**

**Now goto cloudtrail.**

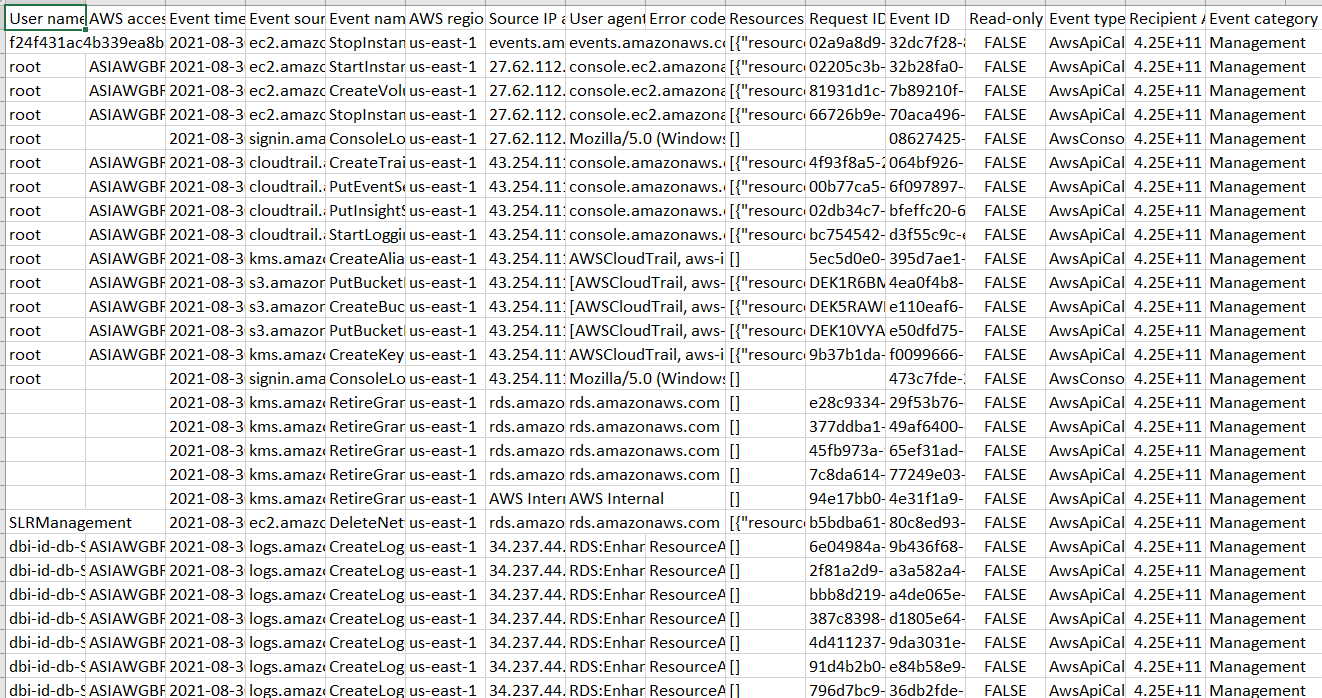
**At event history you can find the logs of the activities that were performed.**



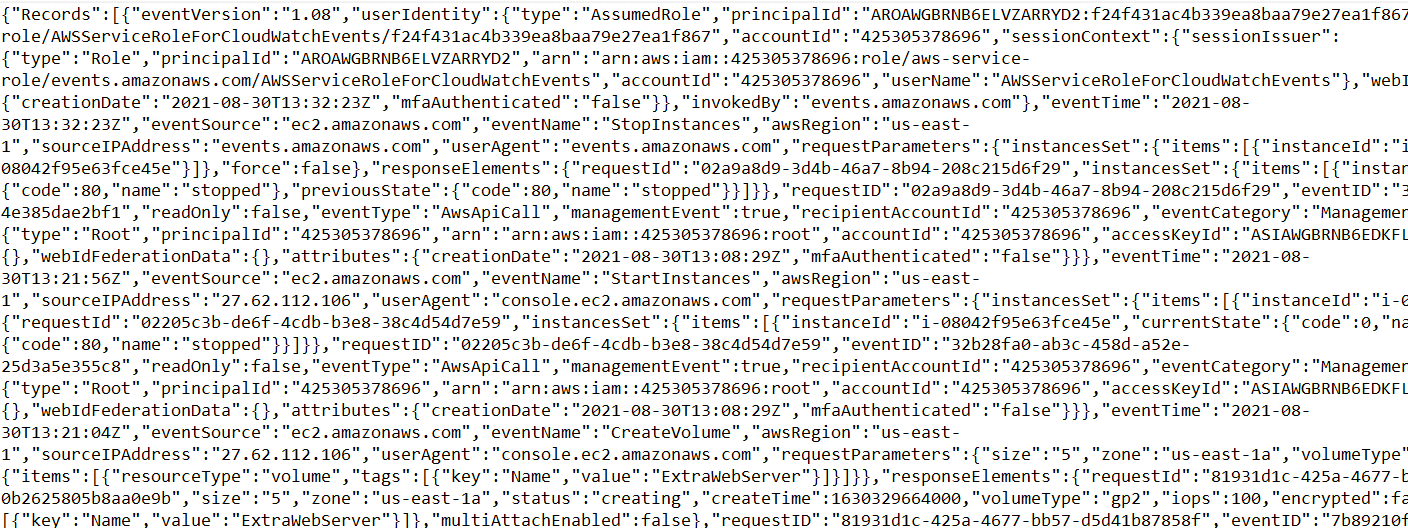
**We can download it in the CSV & JSON format.**



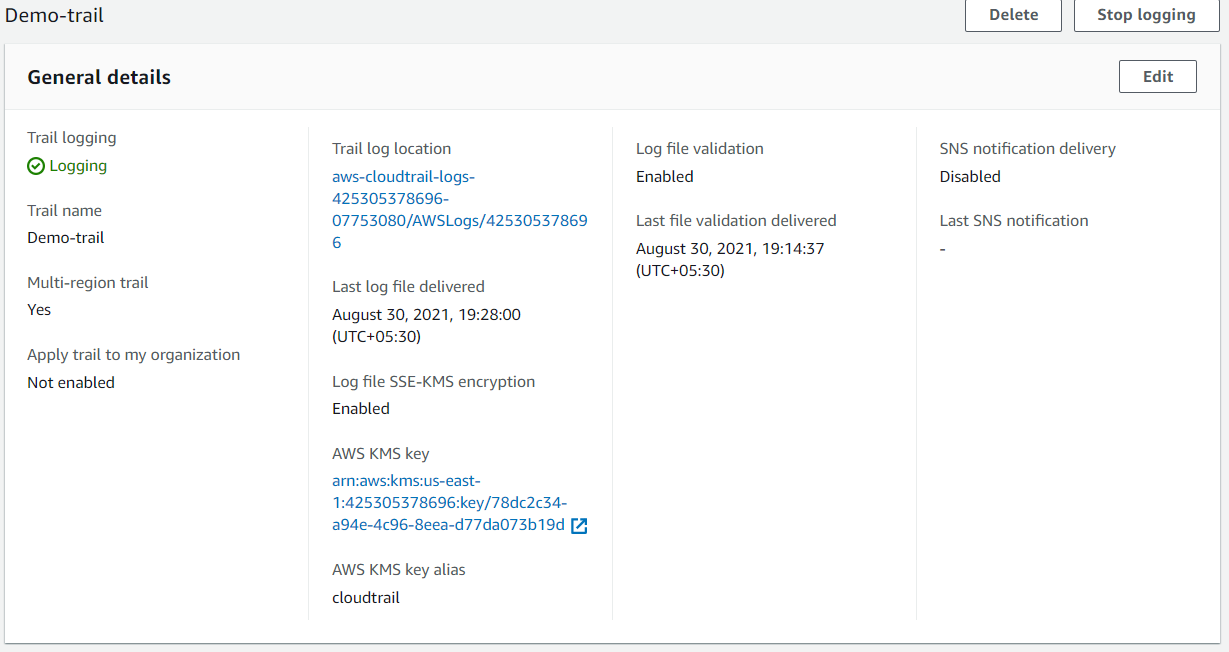
**CSV file:**



**JSON file:**

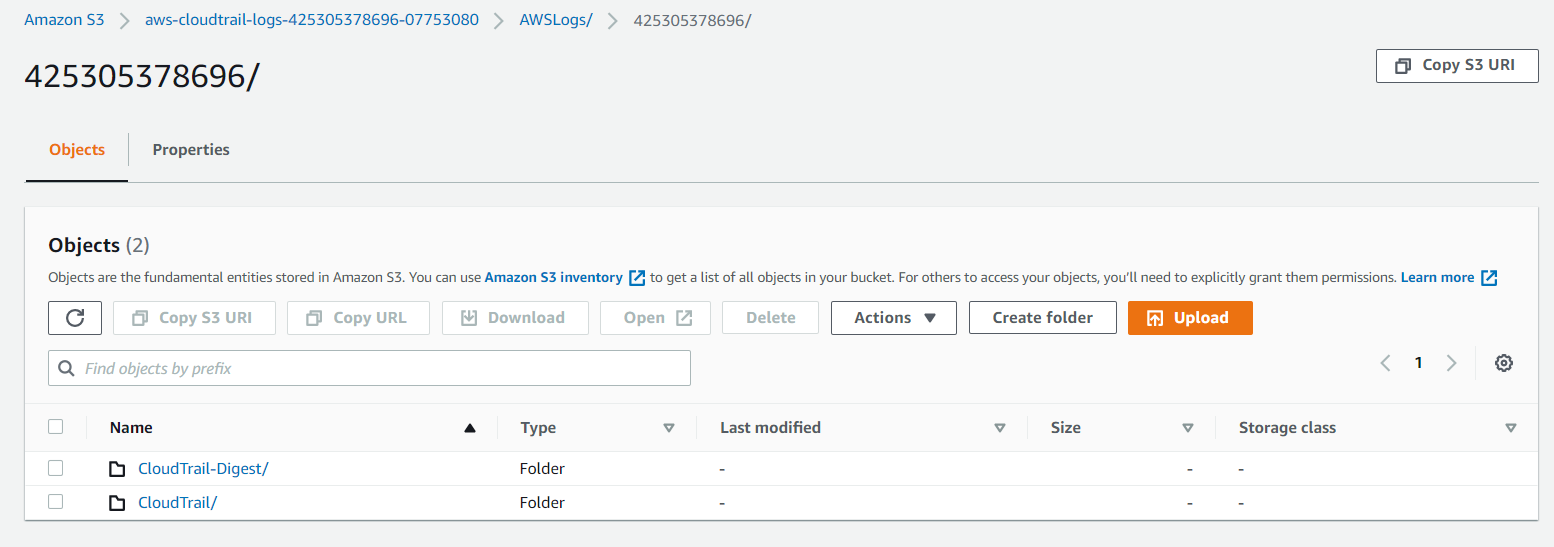


**Here you can find the Trail log location & Last log file delivery time.**



**Click on the “Trail log location”.**

**We can see the S3 bucket location where the log details are stored.**



Validating CloudTrail log file integrity with the AWS CLI

## **validate-logs**

### Syntax

The following is the syntax for validate-logs. Optional parameters are shown in brackets.

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

### Options

The following are the command-line options for validate-logs. The --trail-arn and --start-time options are required.

--start-time

Specifies that log files delivered on or after the specified UTC timestamp value will be validated. Example: 2015-01-08T05:21:42Z.

--end-time

Optionally specifies that log files delivered on or before the specified UTC timestamp value will be validated. The default value is the current UTC time (Date.now()). Example: 2015-01-08T12:31:41Z.

**Note**

For the time range specified, the validate-logs command checks only the log files that are referenced in their corresponding digest files. No other log files in the Amazon S3 bucket are checked. For more information, see [Checking whether a particular file was delivered by CloudTrail](https://docs.aws.amazon.com/awscloudtrail/latest/userguide/cloudtrail-log-file-validation-cli.html#cloudtrail-log-file-validation-cli-validate-logs-check-file).

--s3-bucket

Optionally specifies the Amazon S3 bucket where the digest files are stored. If a bucket name is not specified, the AWS CLI will retrieve it by calling DescribeTrails().

--prefix

Optionally specifies the Amazon S3 prefix where the digest files are stored. If not specified, the AWS CLI will retrieve it by calling DescribeTrails().

**Note**

You should use this option only if your current prefix is different from the prefix that was in use during the time range that you specify.

--trail-arn

Specifies the Amazon Resource Name (ARN) of the trail to be validated. The format of a trail ARN follows.

arn:aws:cloudtrail:us-east-2:111111111111:trail/MyTrailName

**Note**

To obtain the trail ARN for a trail, you can use the describe-trails command before running validate-logs.

You may want to specify the bucket name and prefix in addition to the trail ARN if log files have been delivered to more than one bucket in the time range that you specified, and you want to restrict the validation to the log files in only one of the buckets.

--verbose

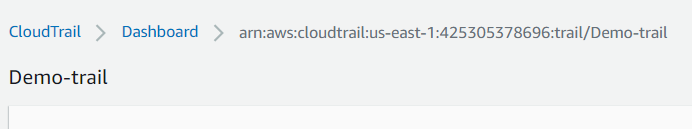
Optionally outputs validation information for every log or digest file in the specified time range. The output indicates whether the file remains unchanged or has been modified or deleted. In non-verbose mode (the default), information is returned only for those cases in which there was a validation failure.

**Example Validation Log file:**

aws cloudtrail validate-logs --start-time 2015-08-27T00:00:00Z --end-time 2015-08-28T00:00:00Z --trail-arn arn:aws:cloudtrail:us-east-2:111111111111:trail/my-trail-name –verbose

**Our Validation Log file:**

aws cloudtrail validate-logs --start-time 2021-08-23T10:00:00Z ~~--end-time 2015-08-28T00:00:00Z~~ --trail-arn arn:aws:cloudtrail:us-east-1:425305378696:trail/Demo-trail ~~–verbose~~

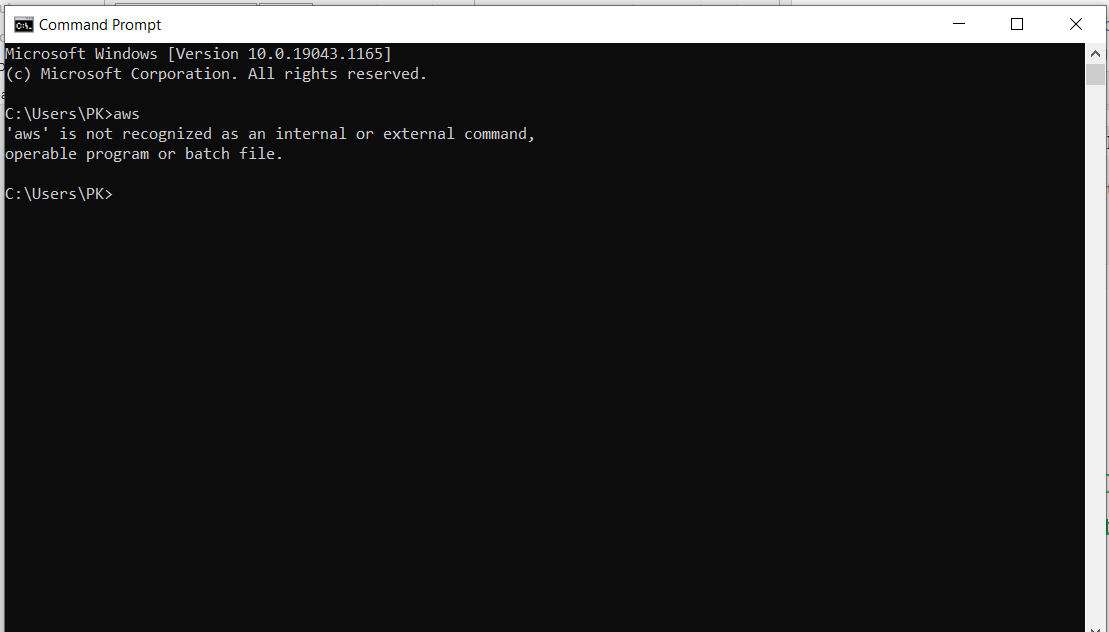
* We can remove the end time, so that it will take the existing end time.
* Copy the ARN address of the CloudTrail and paste it here 
* Verbose can be skipped.

**Our Validation Log file:**

aws cloudtrail validate-logs --start-time 2021-08-23T10:00:00Z --trail-arn arn:aws:cloudtrail:us-east-1:425305378696:trail/Demo-trail

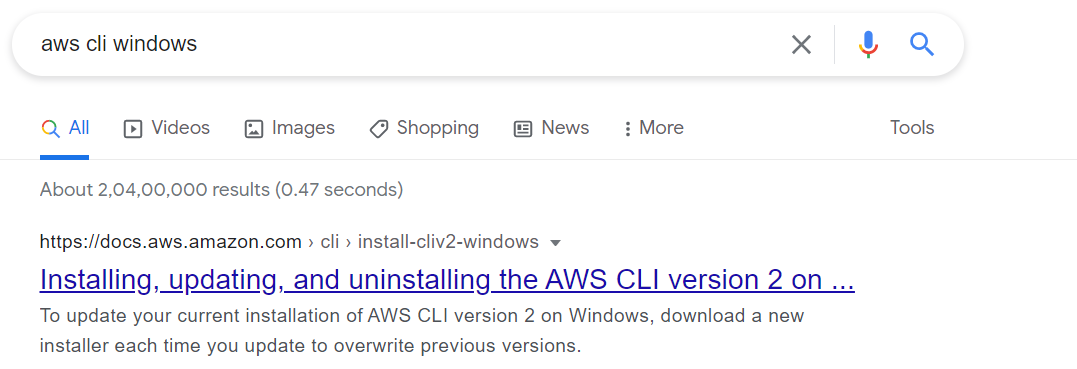
**Here is the instruction to set up an AWS CLI in our Windows Machine:**

**1.Open CMD and type AWS:**



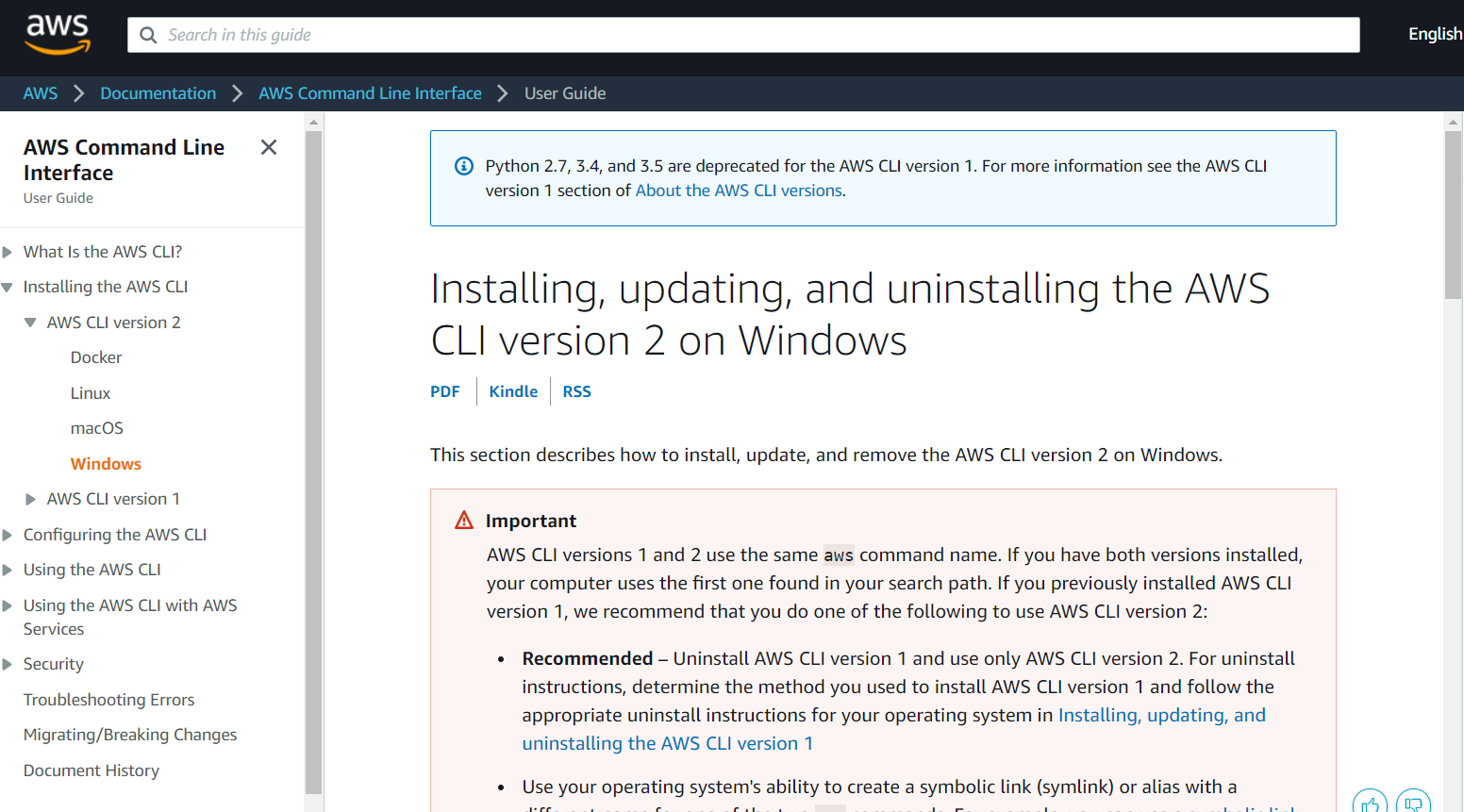
**Aws is not recognized.**

1. **Type AWS CLi Windows in google search.**

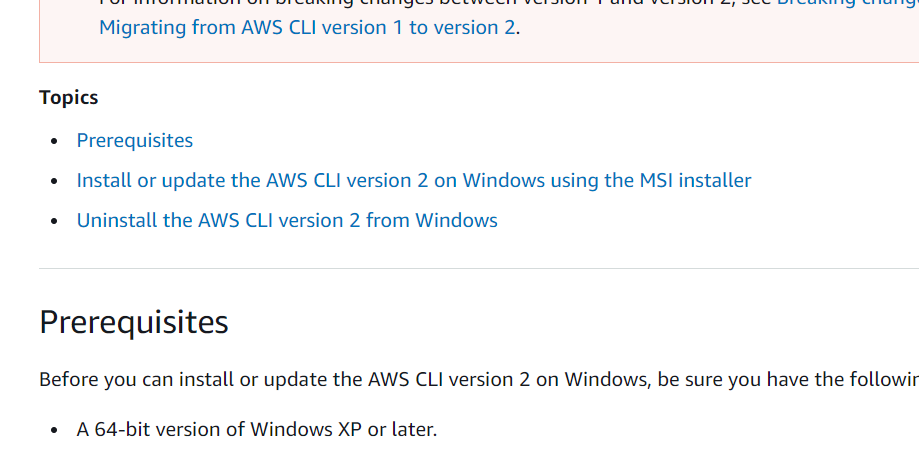


**Click on the first link.**

1. **This page will appear**



* **Scroll down and click on “**[Install or update the AWS CLI version 2 on Windows using the MSI installer](https://docs.aws.amazon.com/cli/latest/userguide/install-cliv2-windows.html#cliv2-windows-install)**”**



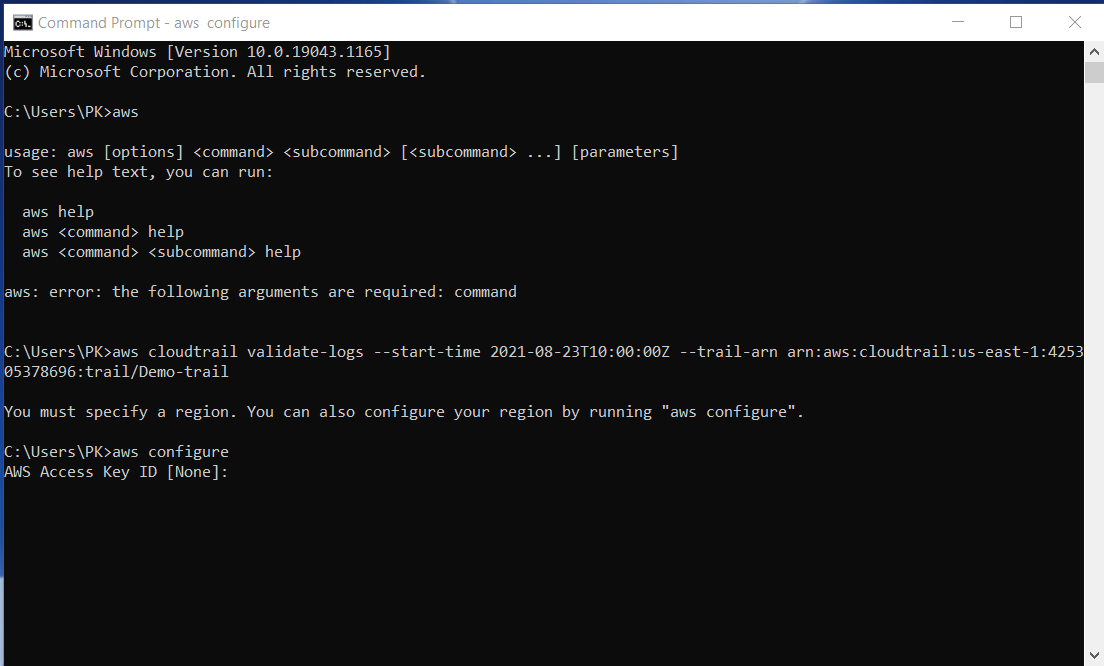
Click on the .msi link



AWSCLIV2.msi will be downloaded.

Click and install the CLI in you windows machine.

Now open the Command prompt and type aws.

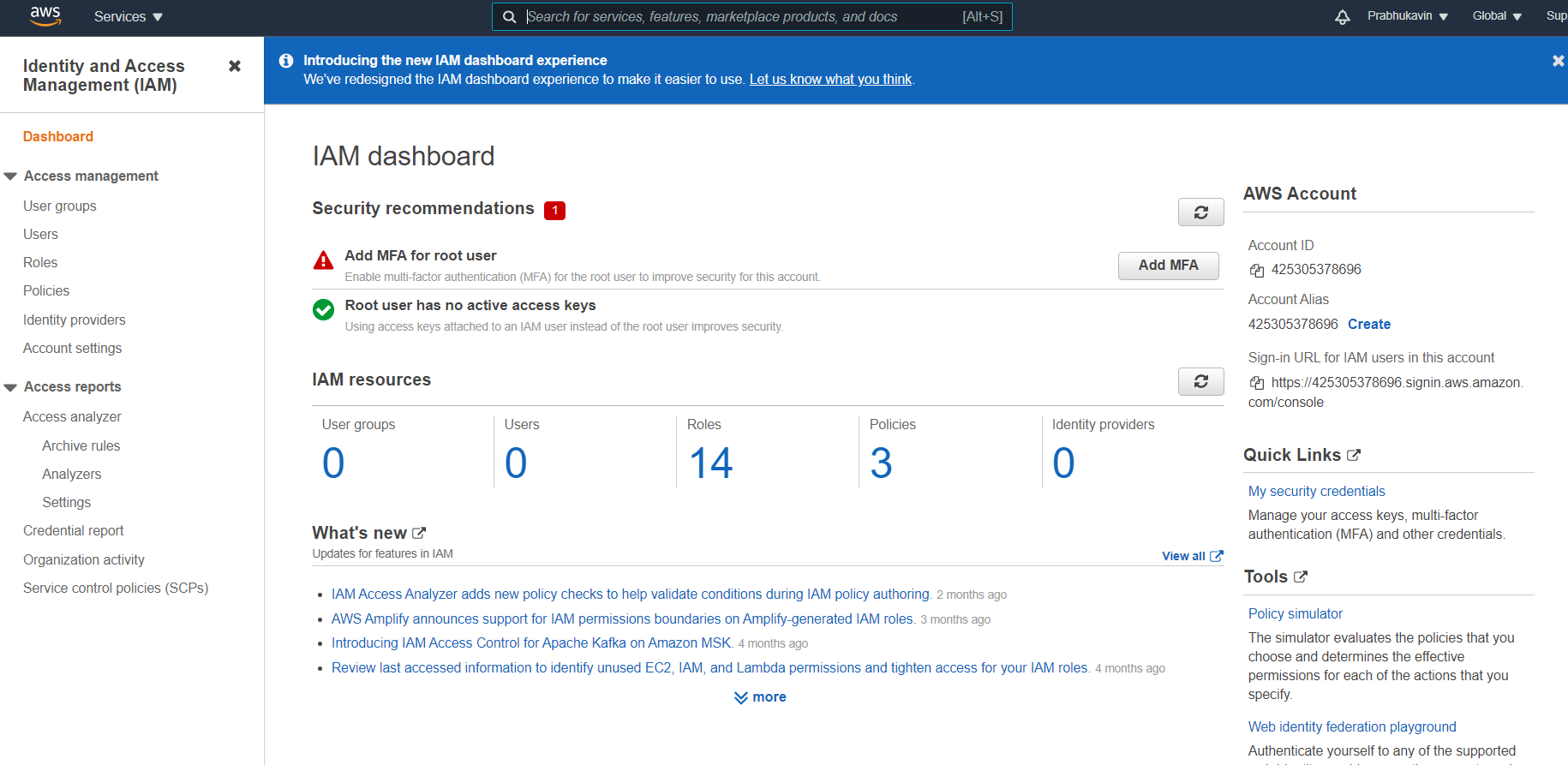


Everything is installed and ready to go but if it is the first time signing up the CLI there are some additional steps that makes you interact with the AWS.

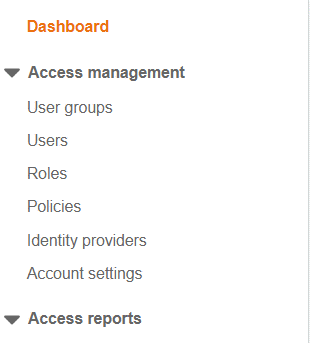
We need to create an user that has some certain set of permissions.

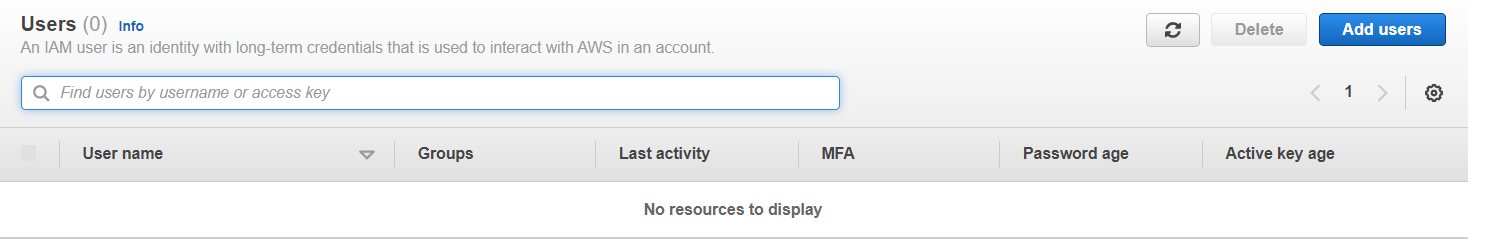
Go into the AWS console.

Go into IAM

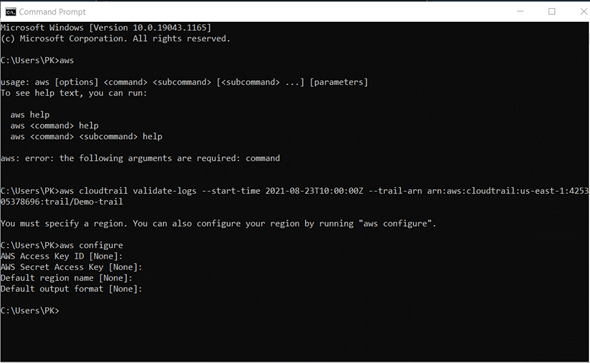


Click on users and add user

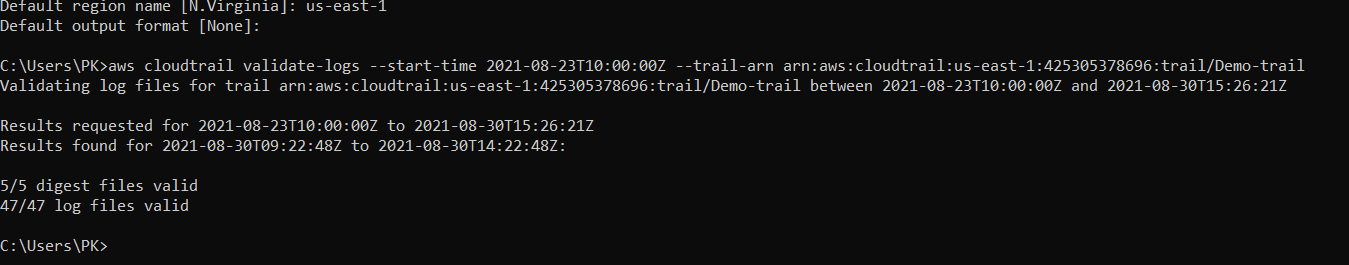




Create an IAM user and fetch the – Access key ID and Secret access key.

v

Now you can paste the validation command here.



The message “valid” shows that there is no modification in the log file and the files are genuine.