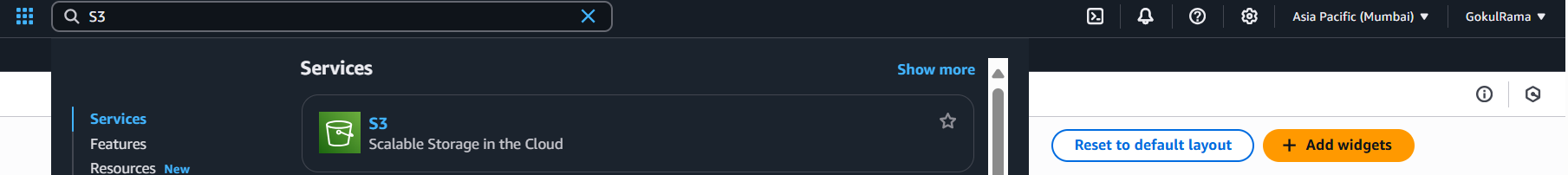
**AWS Task-3**

**Task Description:**

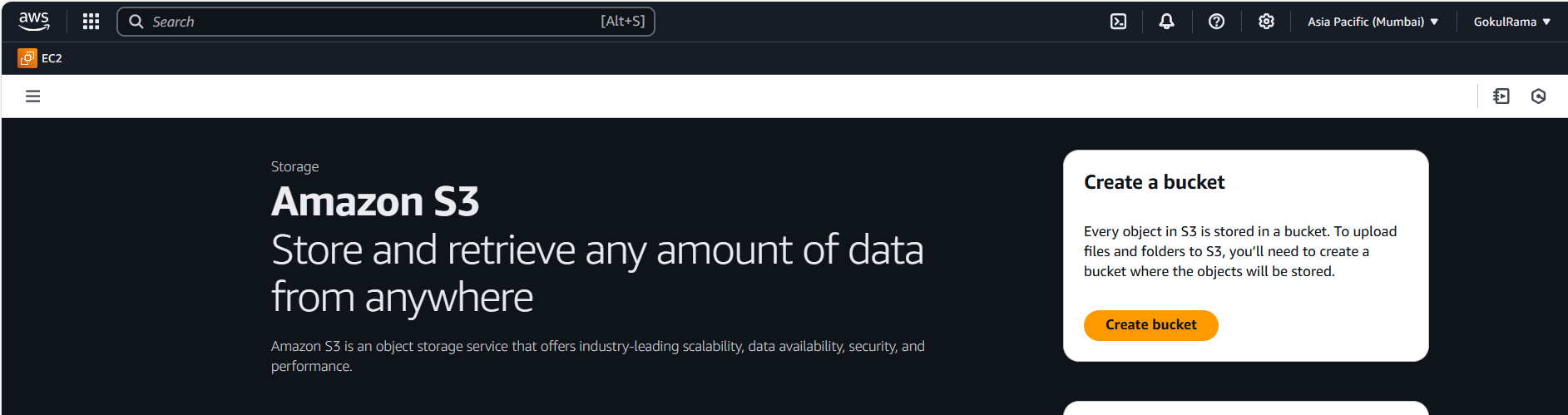
1. Create a S3 bucket, with no public access and upload files to the bucket & view the logs using CloudWatch for the uploaded files.

===========================================================

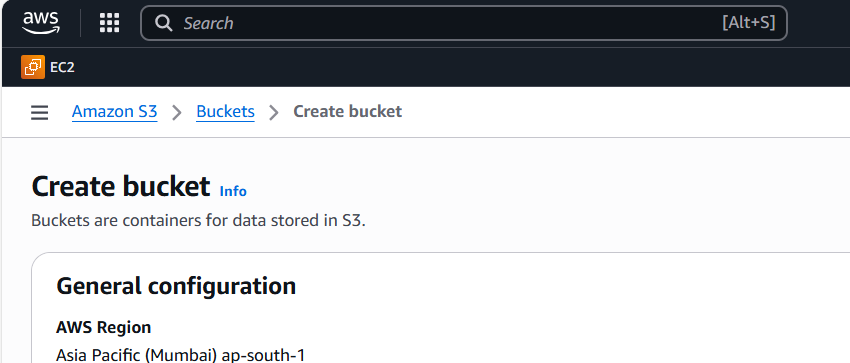
* 1. **Creating a S3 bucket: -**
* Logged into AWS account and search “**S3**”

****

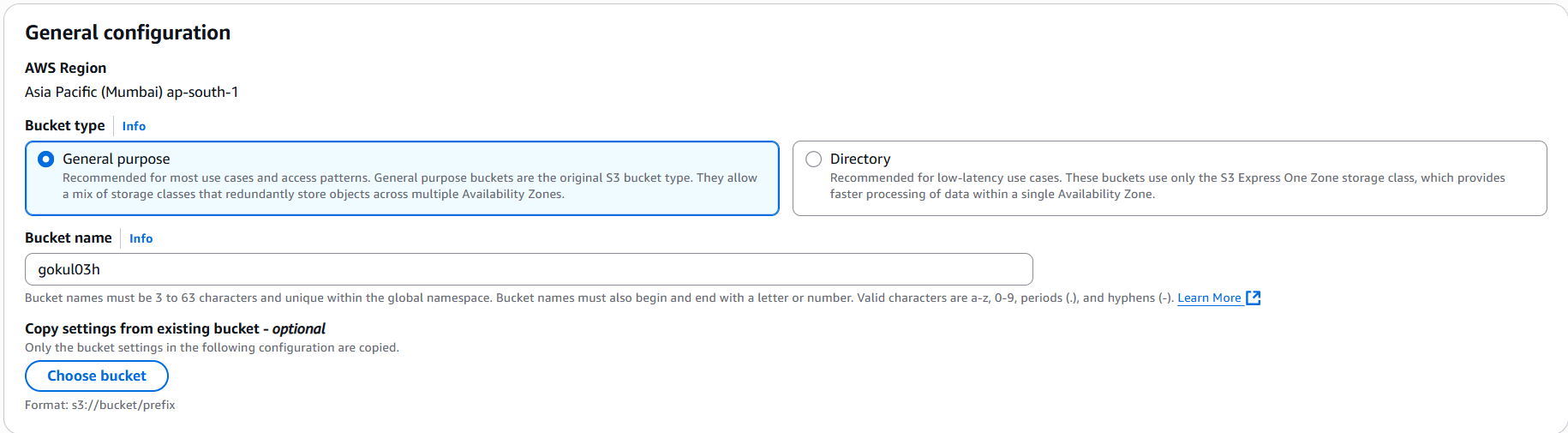
* Once navigated into “**S3**” -> Click “**Create bucket**”

****

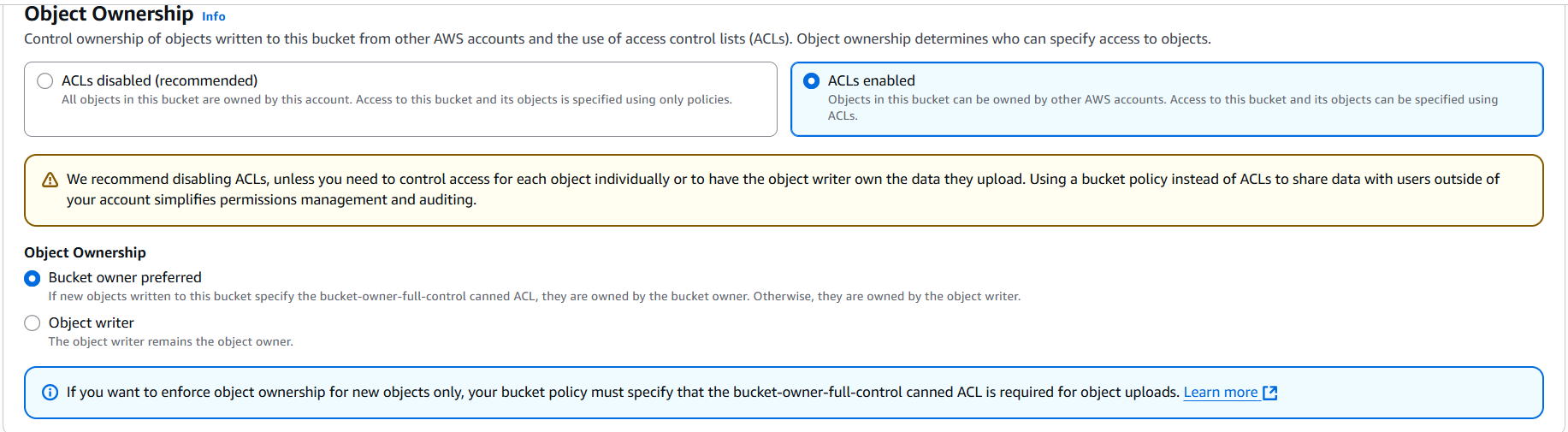
* Below is the “**Create bucket**” screen -> **General Configuration** settings

****

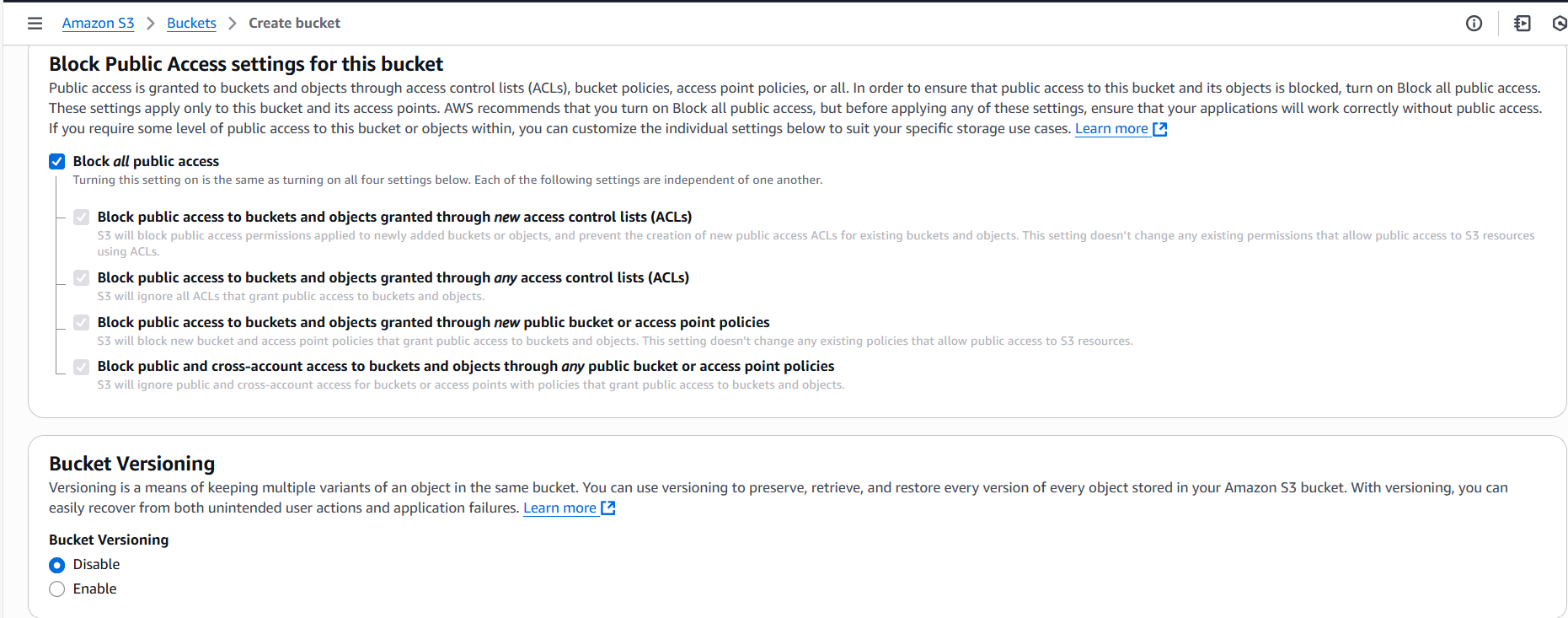
* Select **Bucket type – General Purpose**
* Give **Bucket Name – gokul03h** (Unique name across AWS)

****

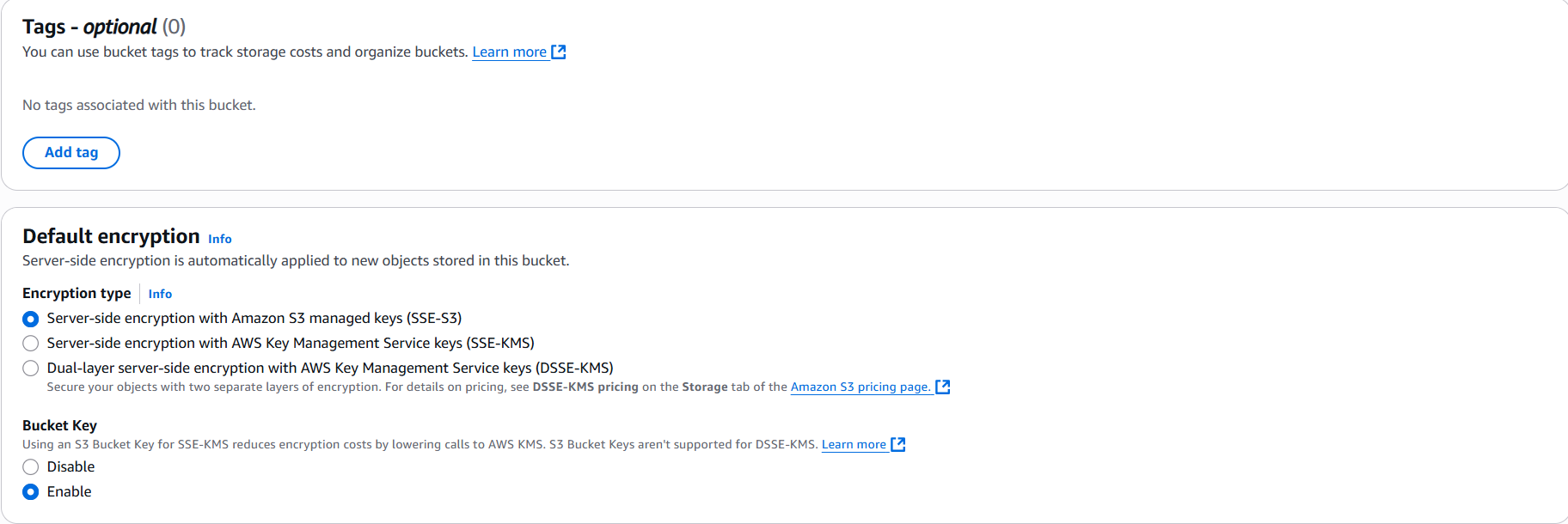
* Select **Object Ownership – ACLs enabled.**
* Choose **Bucker owner preferred** option

****

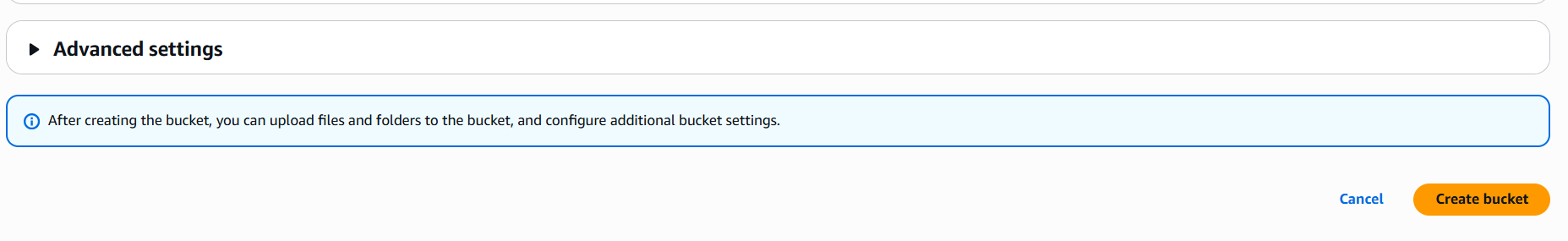
* Below is the setting of **No Public Access to the bucket**
* **Bucket Versioning - Disabled**

****

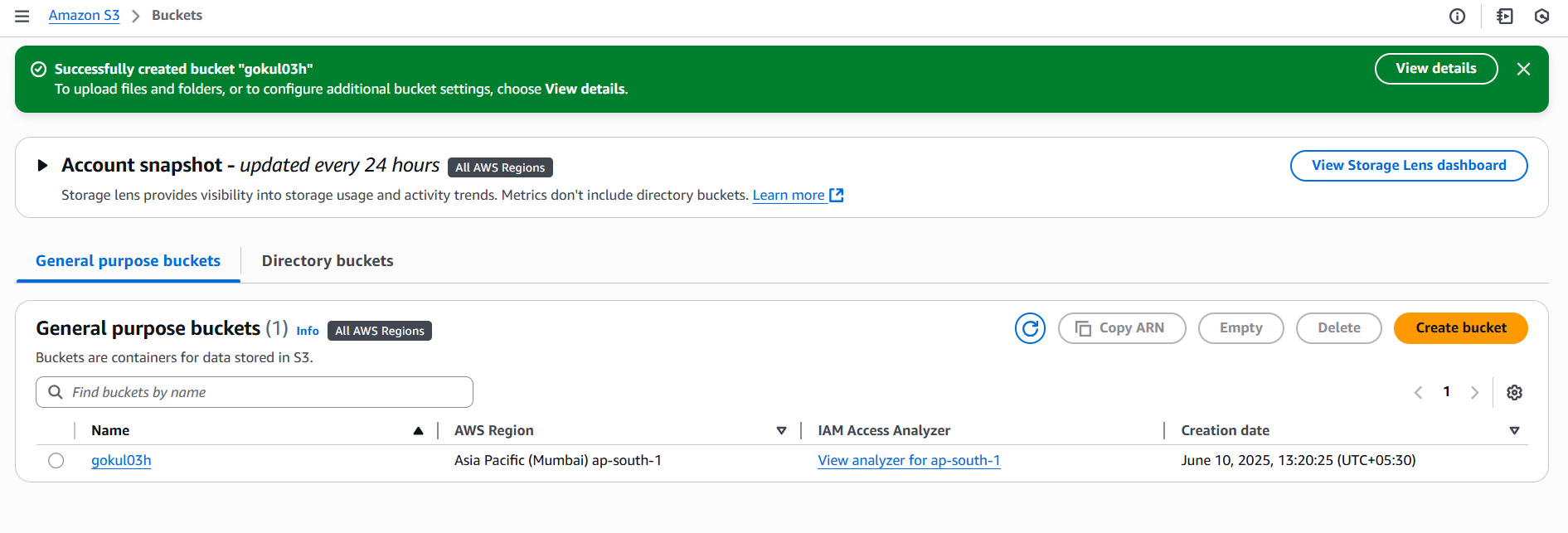
* Choose **Default encryption (Encryption type) – Server-side encryption with Amazon S3 managed keys (SSE-S3).**

****

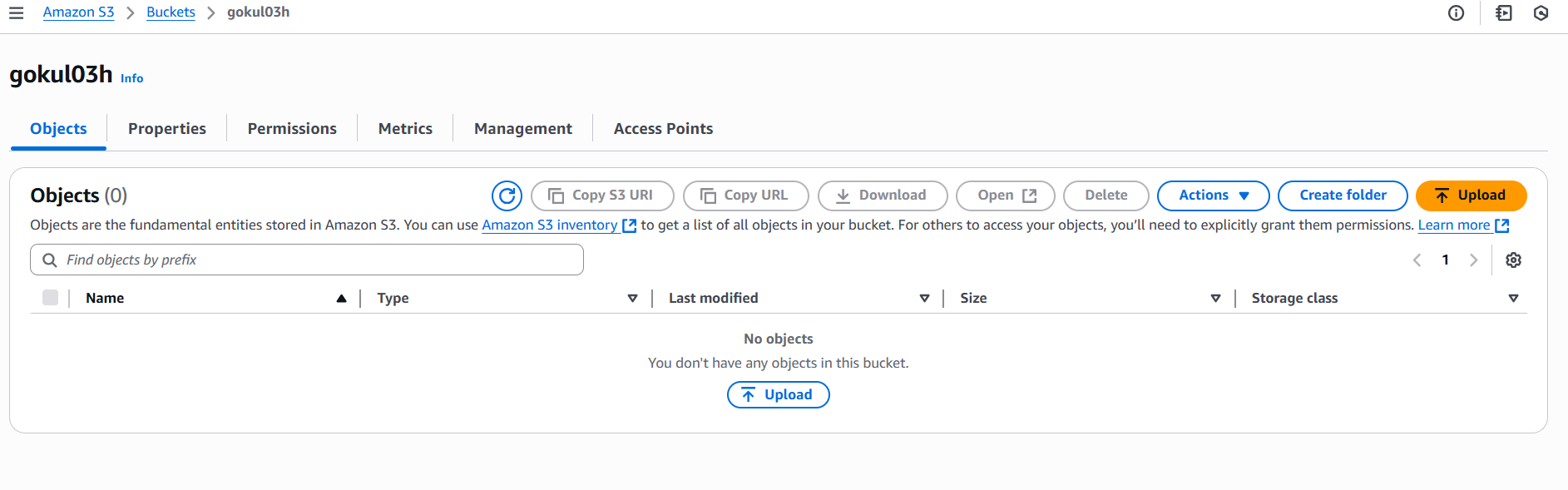
* Click **Create bucket** option

****

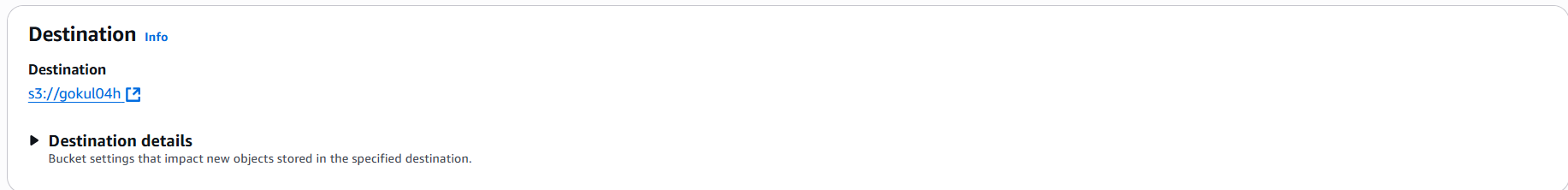
* **Now the bucket has been created successfully** (Refer the below snapshot).

****

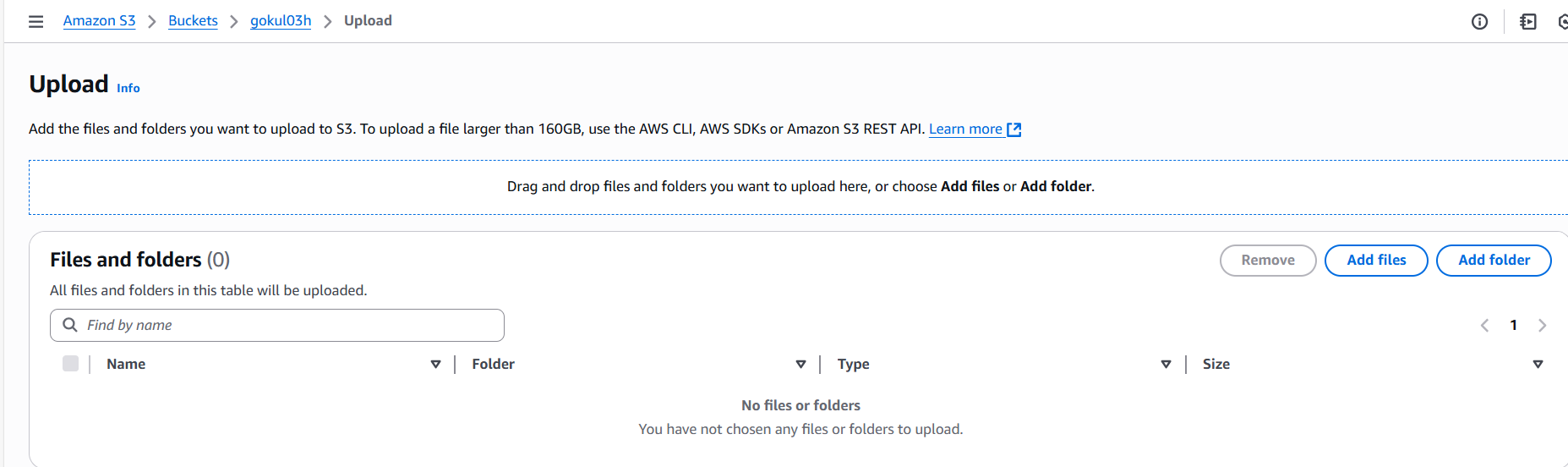
* **Uploading Files into S3 Bucket ->** Click “**Upload**” button (Refer the below snapshot).

****

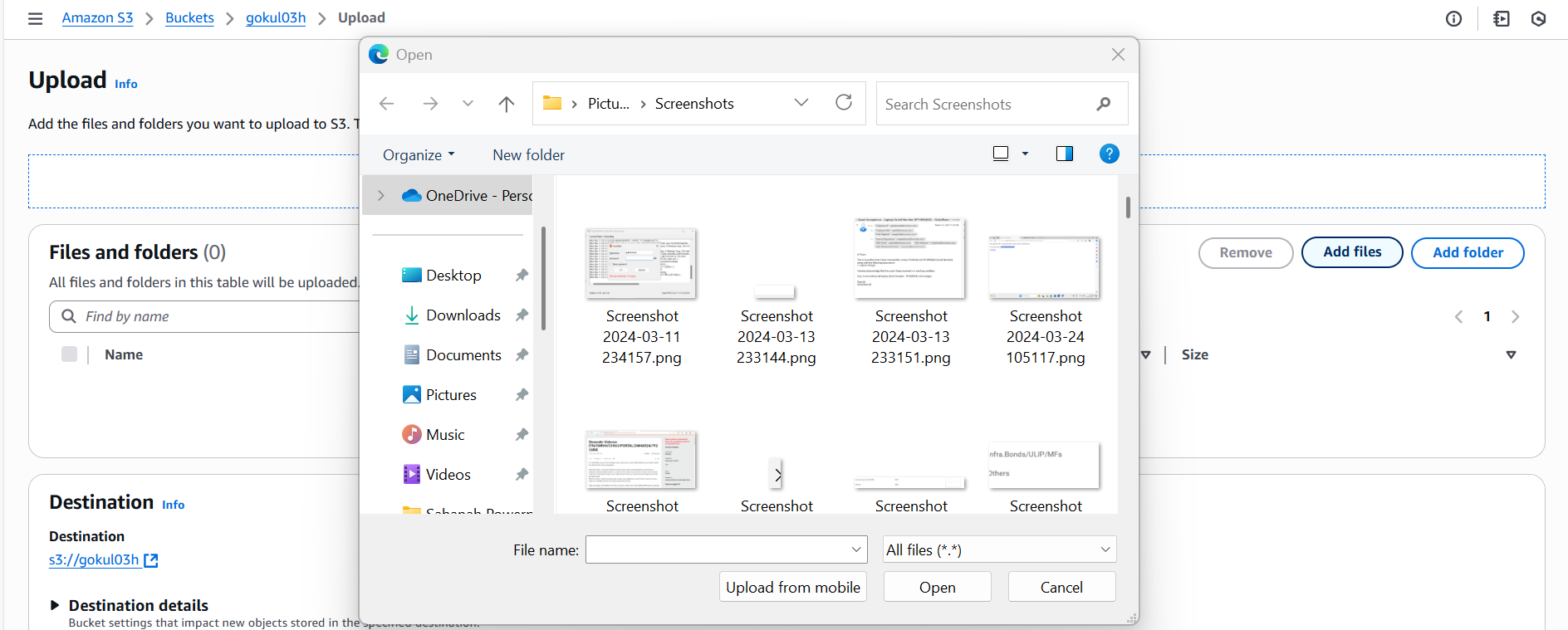
* The Destination is **s3:/gokul04h** it will automatically take by AWS.



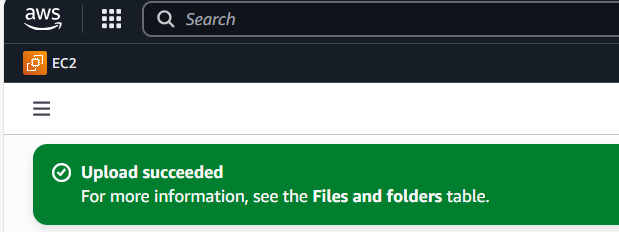
* Click “**Add files**”

****

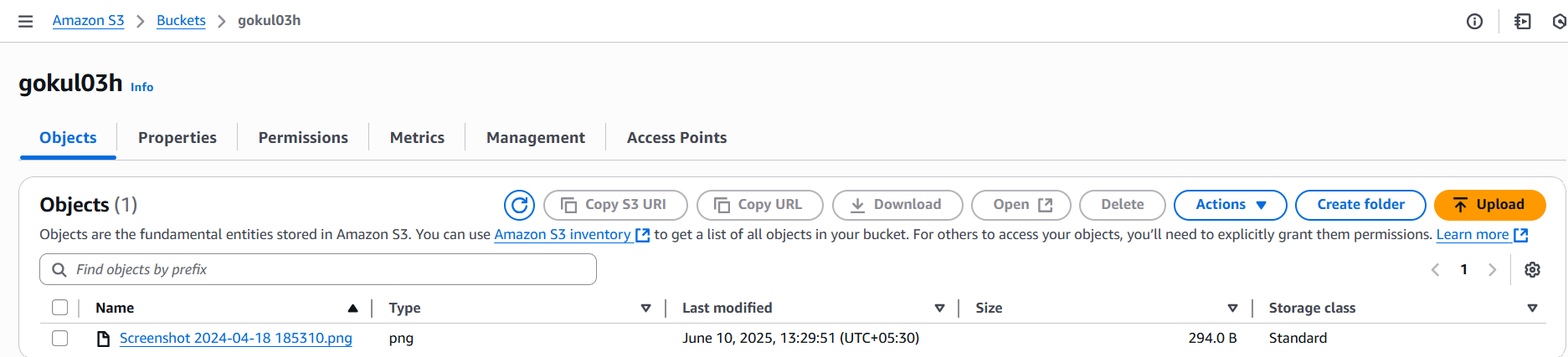
* Select the file that you want to upload and click Open

****

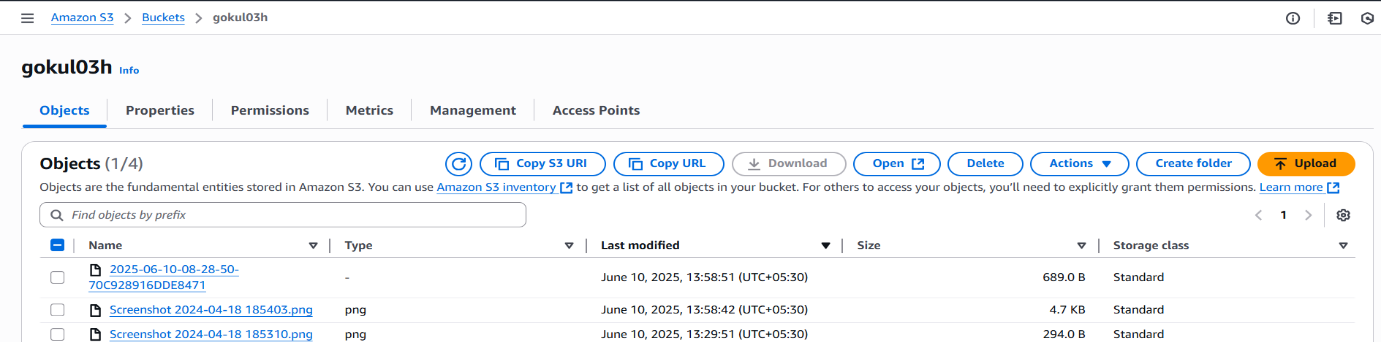
* Once the **file uploaded successfully into S3 bucket (Refer the below snapshot).**

****

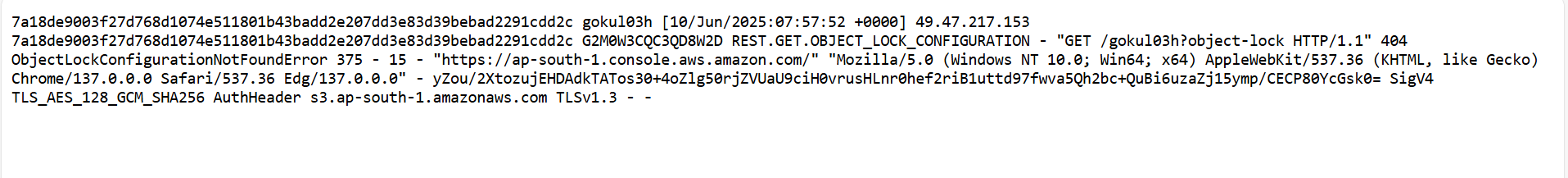
* Now the **file is available in S3 bucket**.

****

* **Post file uploaded in S3 bucket**, AWS create logs **automatically** after some time [ Refer the below screenshot of logs]

****

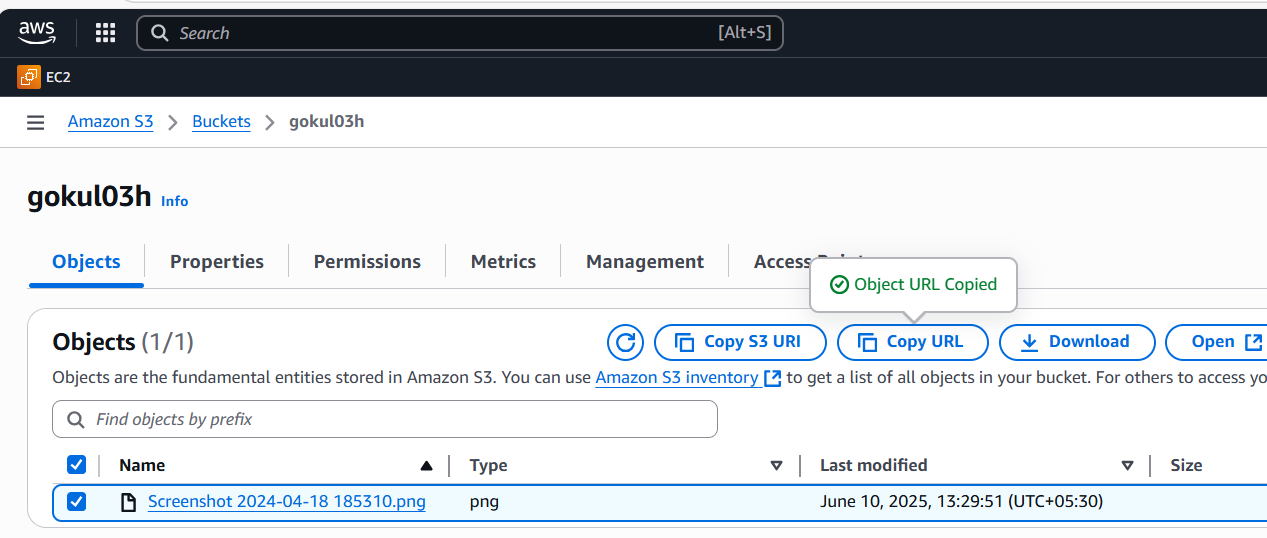
* Log is,

****

**======================================================================**

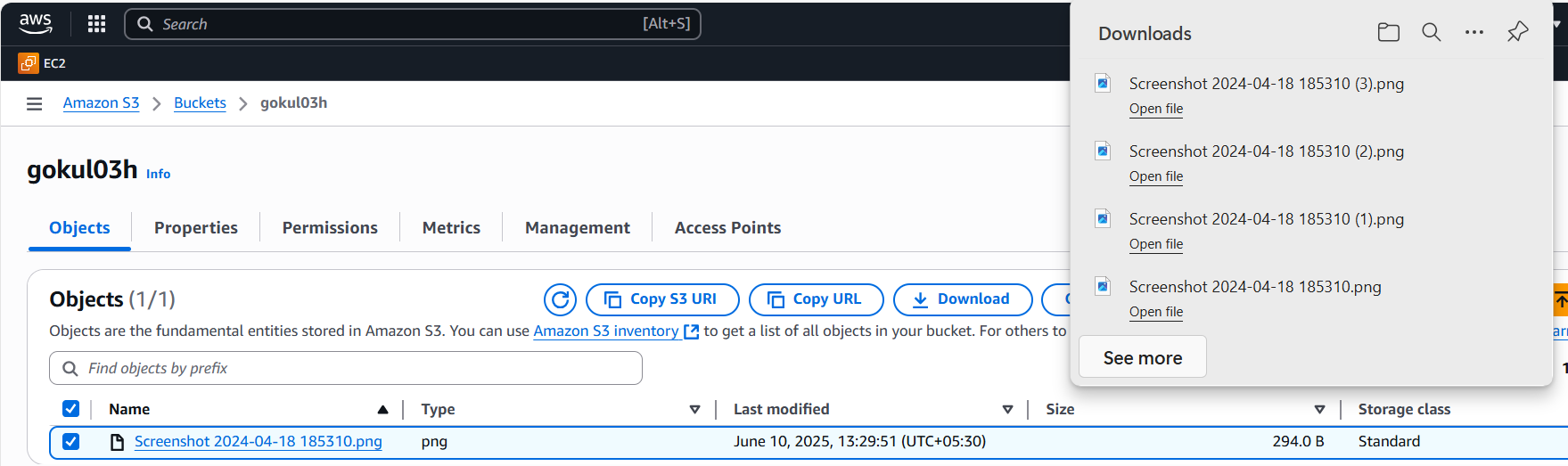
1. **Block All Public Access: -**

* Check the files available in S3 bucket is accessible or not

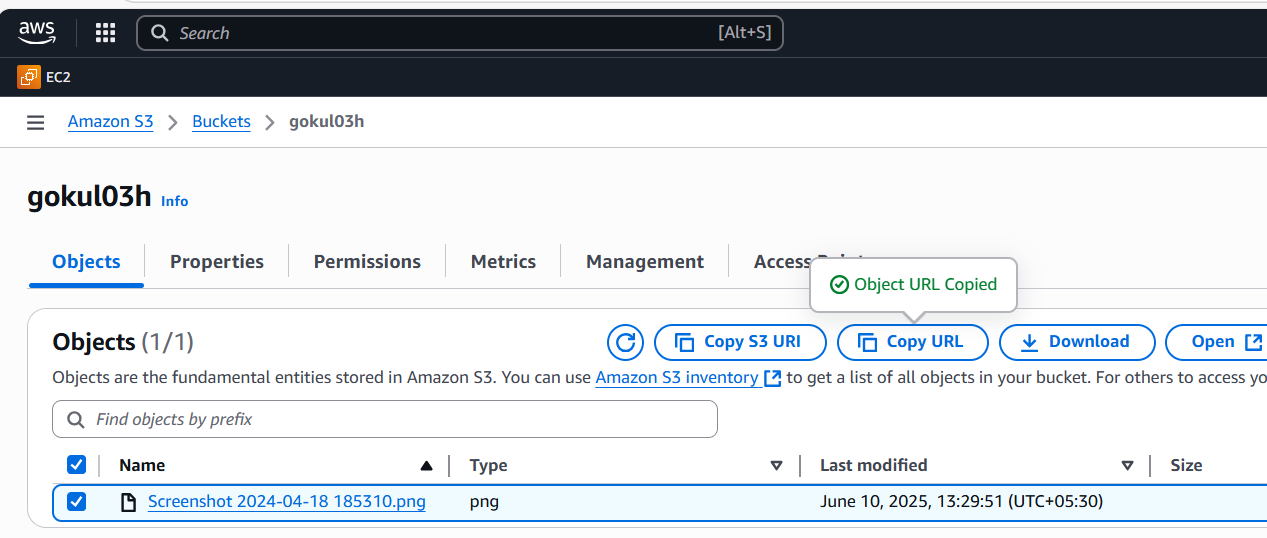
****

* **Inside AWS Account** 🡪 Select any file and click **Download** option and able to download the file (Refer the below snapshot).

**Note** - Inside AWS account able to access the file.

****

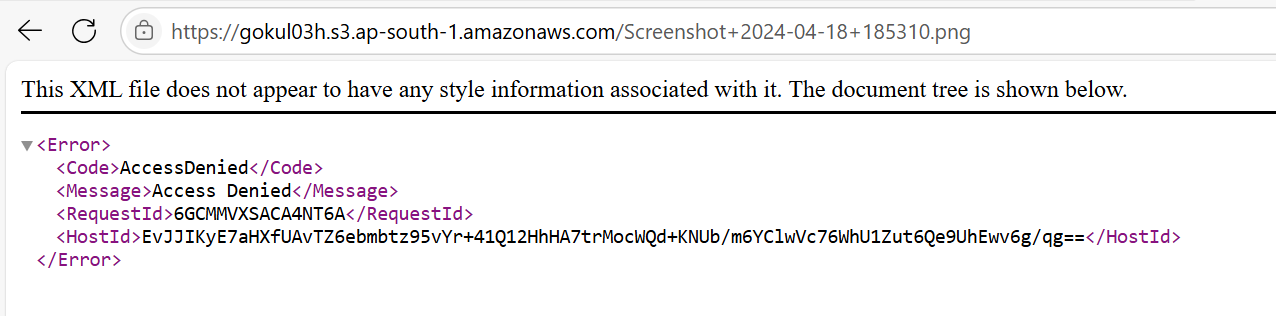
* **Outside AWS Account ->** Select the respective file and copy the URL using **“Copy URL**” button.



**Note: Outside the AWS account ->** We are getting “**AccessDenied**” for the

same URL (Refer the below screenshot).

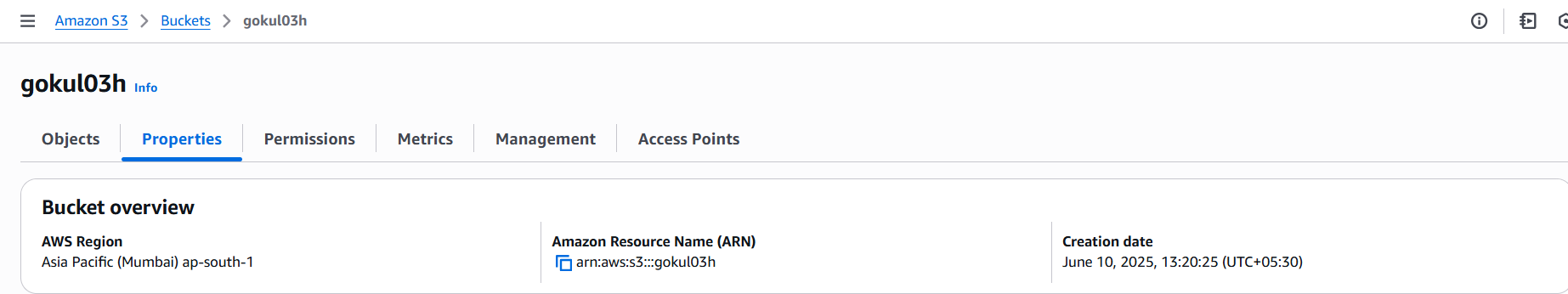
**Reason is – While creating S3 bucket we enabled “Block all Public Access” option under network settings.**

****

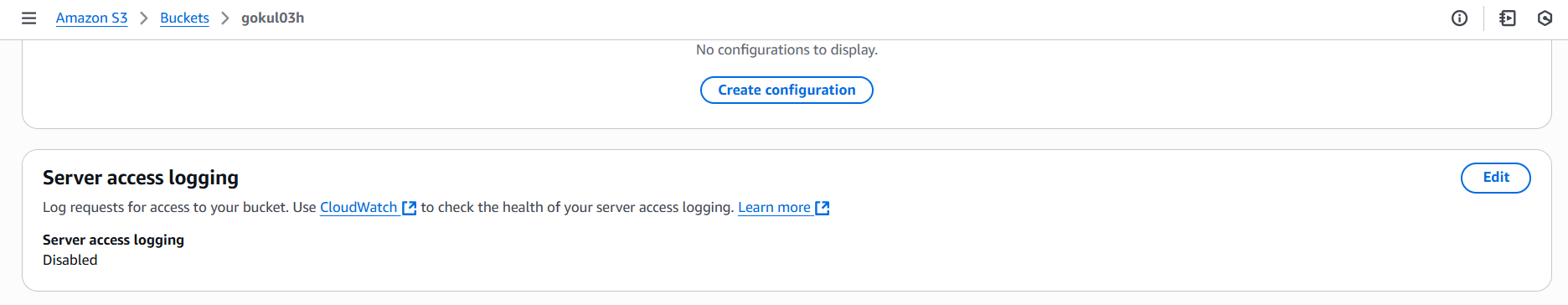
**======================================================================**

**3.View the logs using cloudwatch for the uploaded files: -**

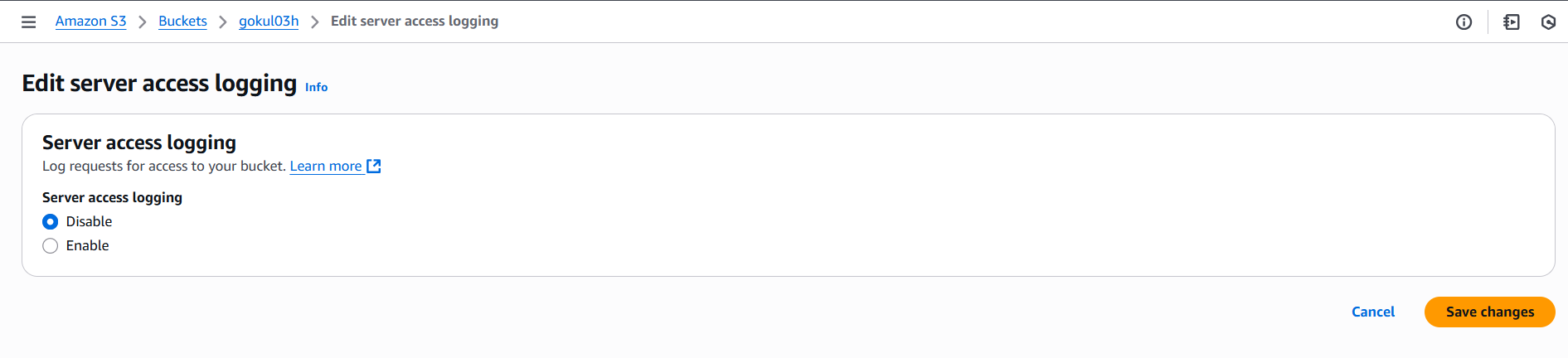
* Before creating “**Cloudwatch**” need to do “**Server access logging**” configuration.
* Select the respective “**S3**” bucket -> Go to “**Properties**”

****

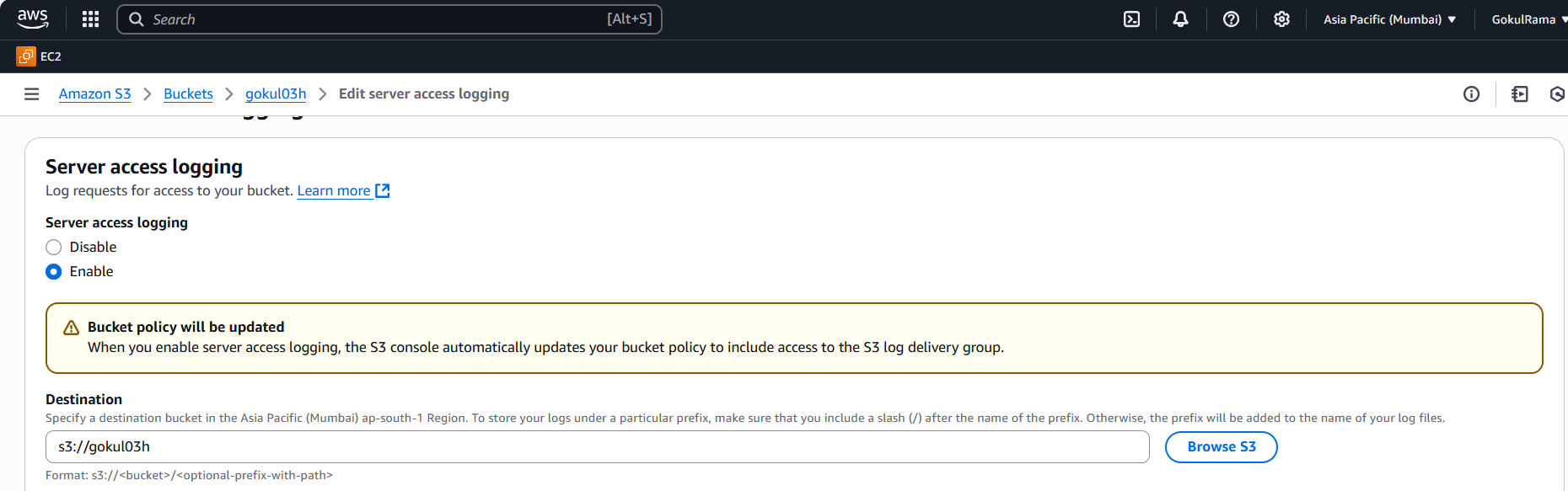
* Go to “**Server access logging** “(Scroll down the page).



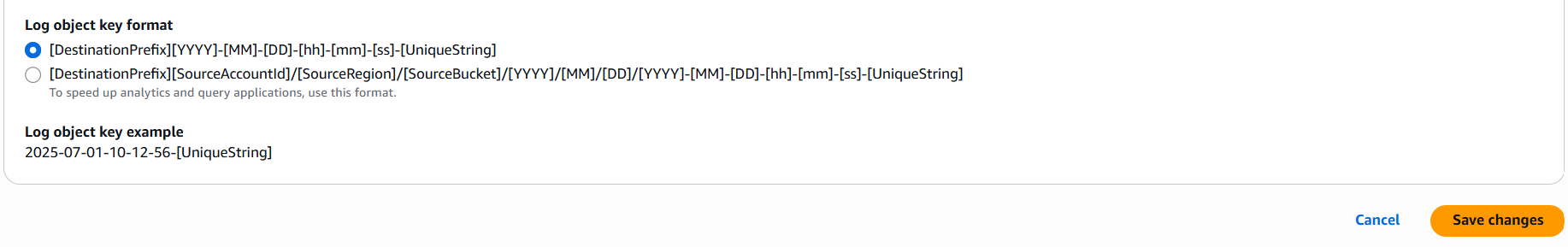
* Click “**Edit**” button in server access logging.

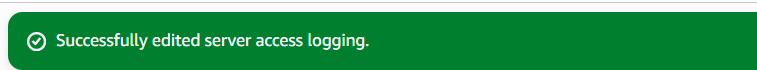
****

* Select “**Enable**” option in server access logging
* Clicking “**Browse S3**” button to choose the **Destination** is “**s3://gokul03h**”

****

* Choose **Log object key format** is “**Destinationprefix**” [ Refer the below screenshot].
* Click **“Save changes”**

****

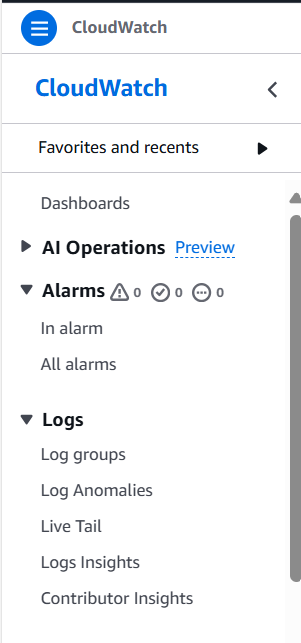
****

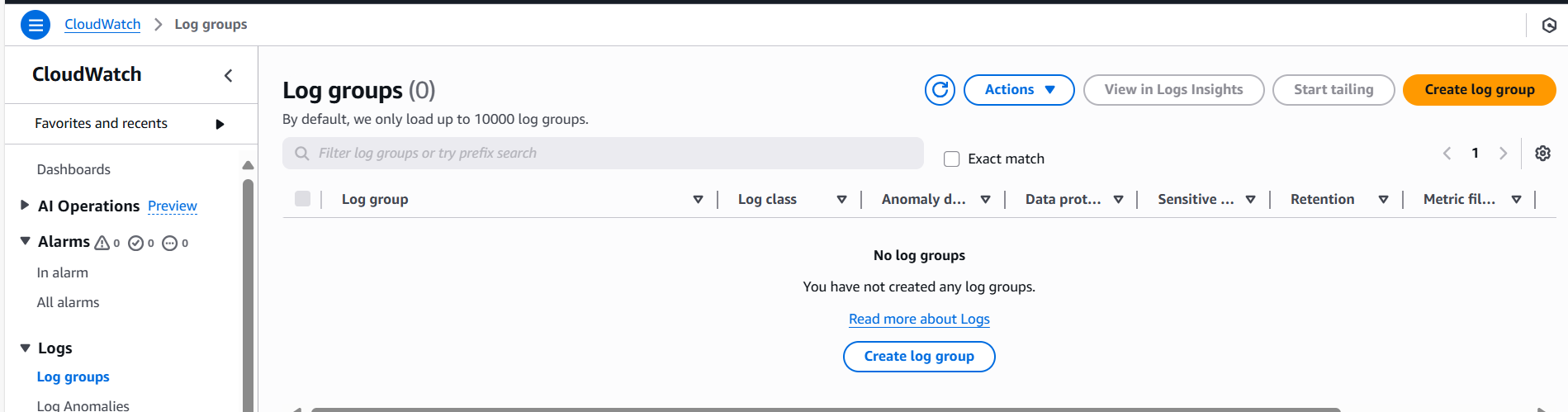
**Setting up the Cloudwatch: -**

* Search “**CloudWatch**” in search box.

****

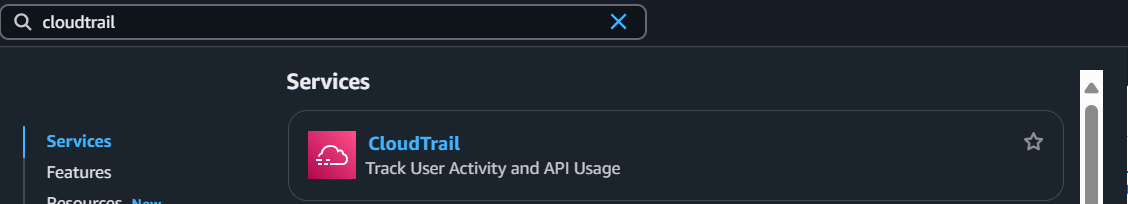
* Here go to “**Log groups**”, S3 bucket will not store logs directly in **“CloudWatch-> Log groups”**
* So, we need to use “**Cloud trail**” service.
* **Cloud trail service** is **used to capture whatever activity you performed in AWS account.**

****

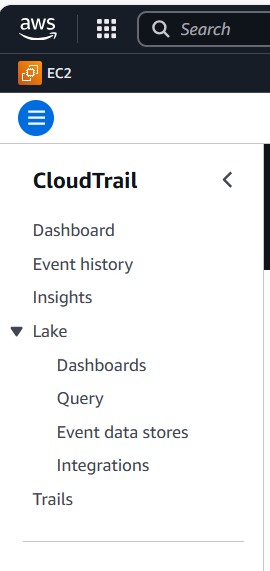
****

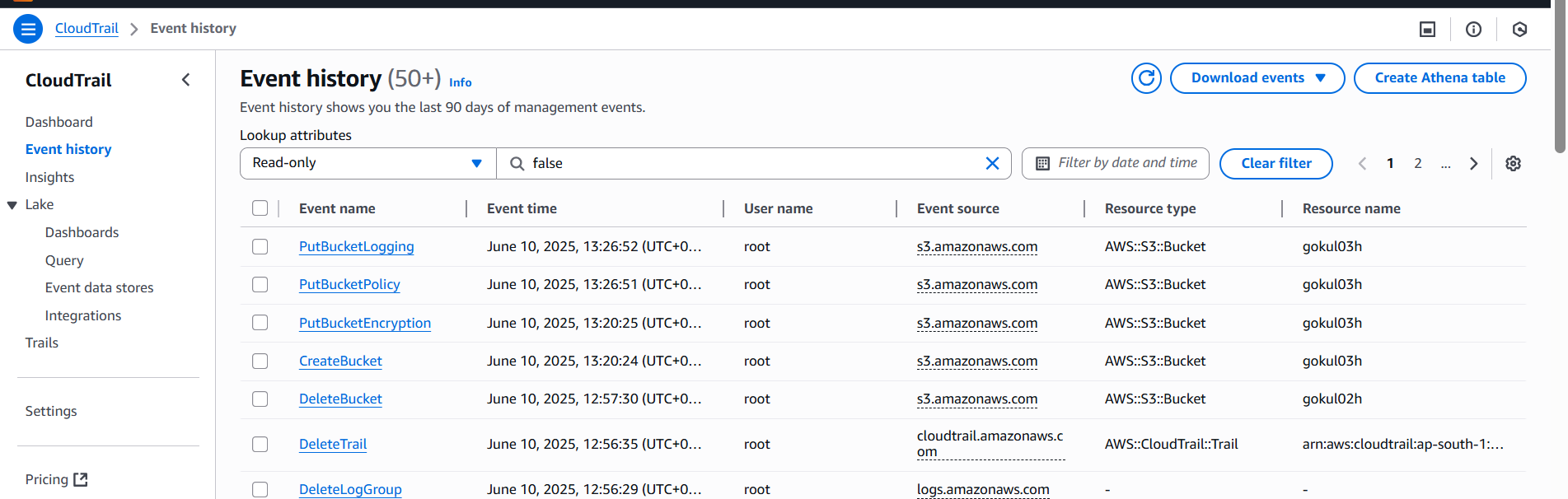
**Cloud Trail Service: -**

* Search “**CloudTrail**” service in search box.

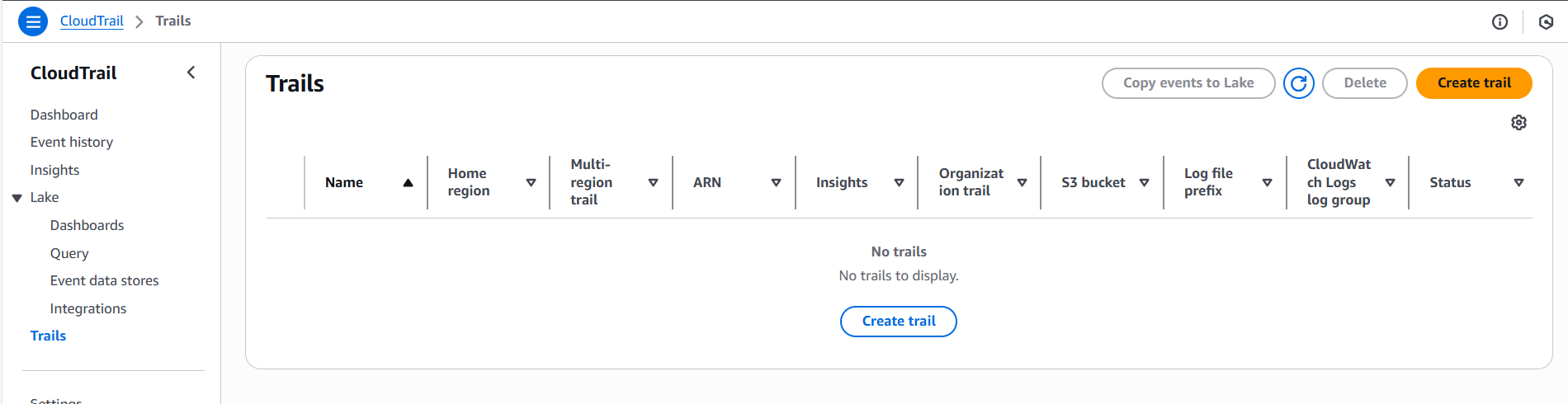
****

* Go to **“Event history”** it will show all events performing in AWS account.

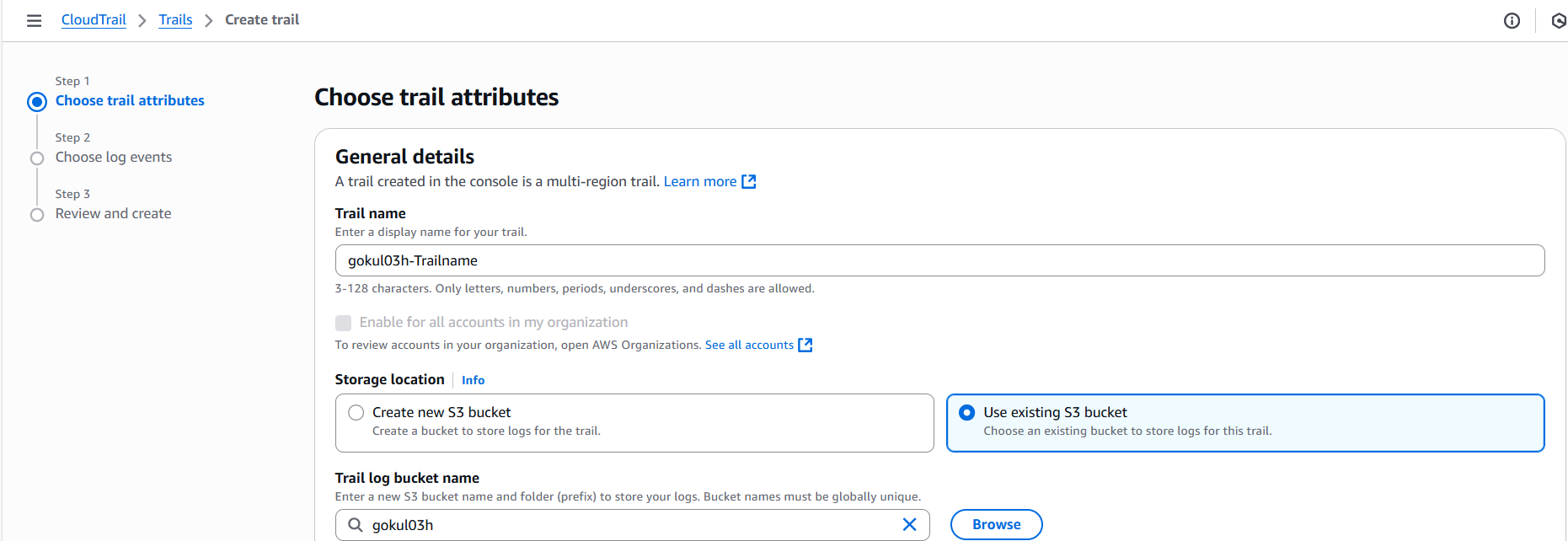
****

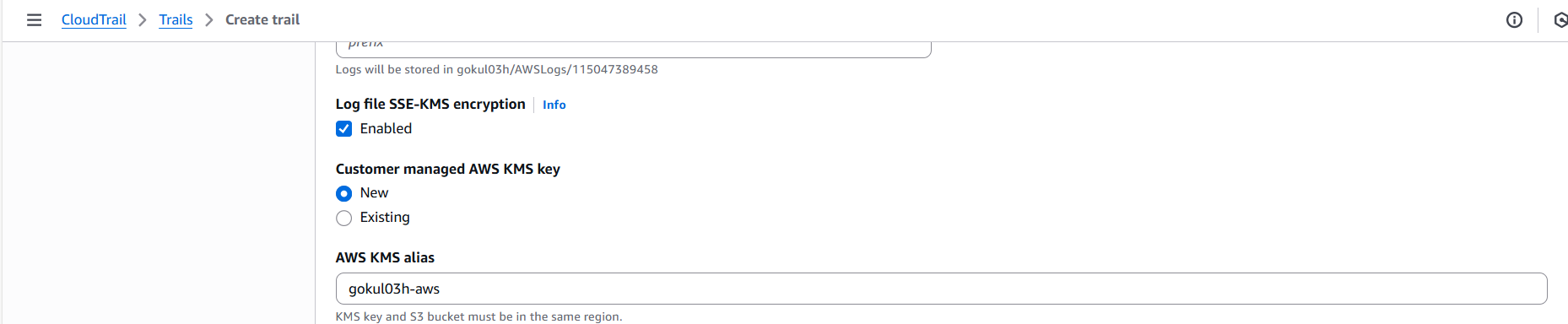
****

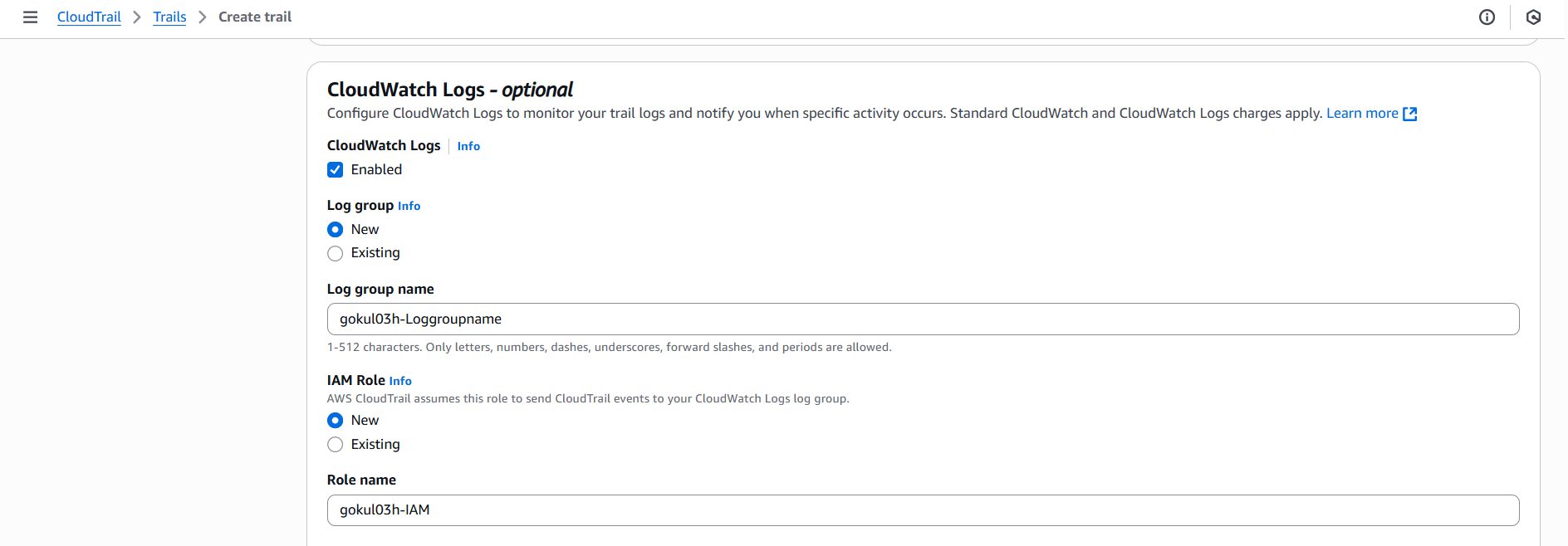
* In the above event history, it will show all events performing in AWS account but I need to segregate logs for S3 bucket alone
* So, we need to “**Create trail**” for **S3 bucket logs alone.**
* Select **“Create trail”** button**.**

****

* **Choose trail attributes,**
  + Give “**Trail name**” – **gokul03h-Trailname**
  + Choose **“Use existing S3 bucket”**
  + **Trail log bucket name - Browse “S3 bucket” that you created above**
  + **Log file SSE-KMS encryption** – **Enabled** only
  + **Customer managed AWS KMS key** – Select **New** option
  + **AWS KMS alias** – Give name as gokul03h-aws
  + **CloudWatch Logs ->** Select **Enabled**
  + **Log group –** Choose **New**
  + **Give Log group name – gokul03h-Loggroupname**
  + **IAM Role –** Choose **New**
  + **Give Role name – gokul03h-IAM**
  + Click **Next**

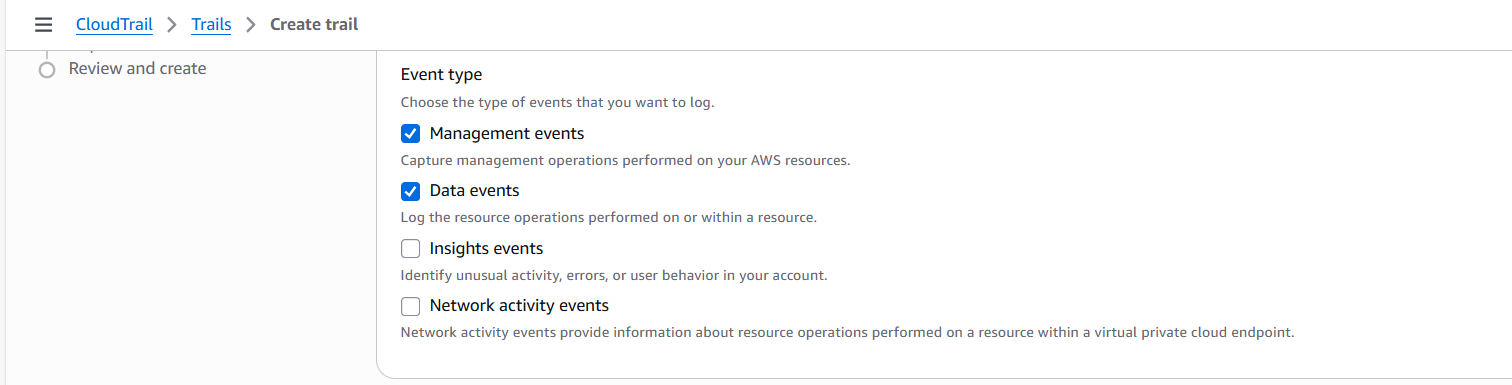
****

****

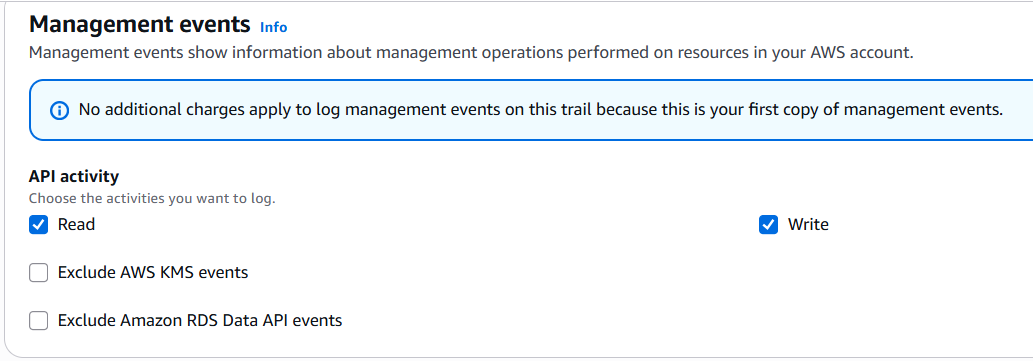
****

****

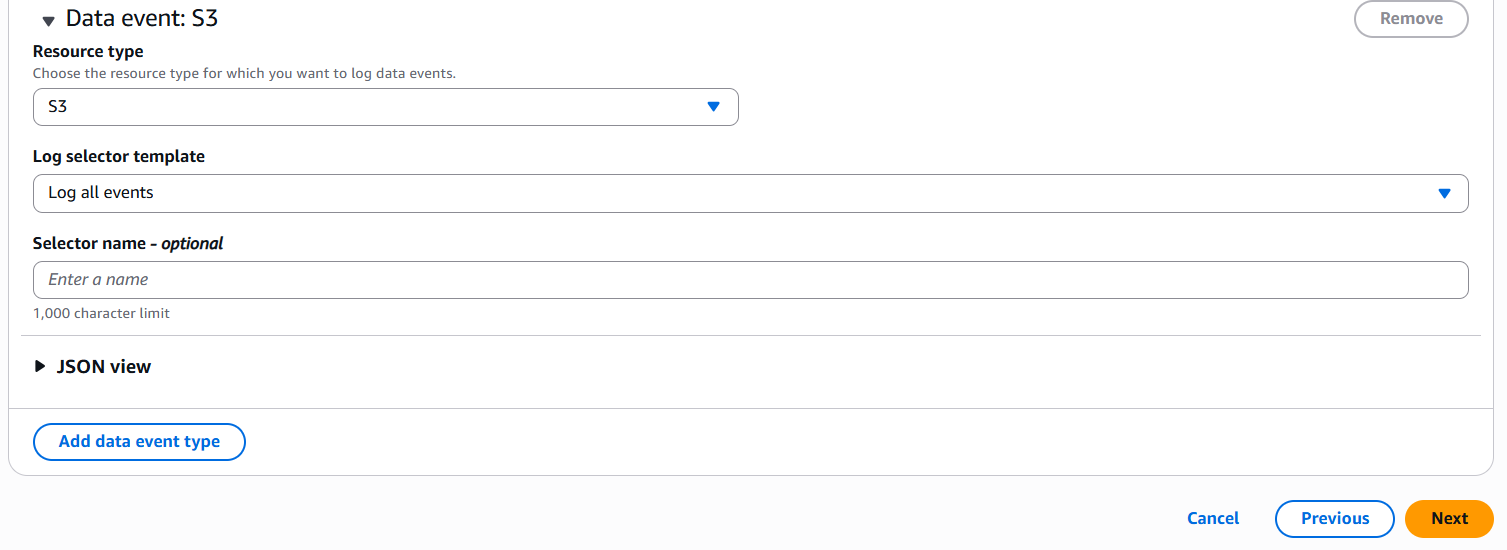
* **Choose Log Events: -**
  + Select “**Management events**” & “**Data events**” option

****

* + **Management events: -**

****

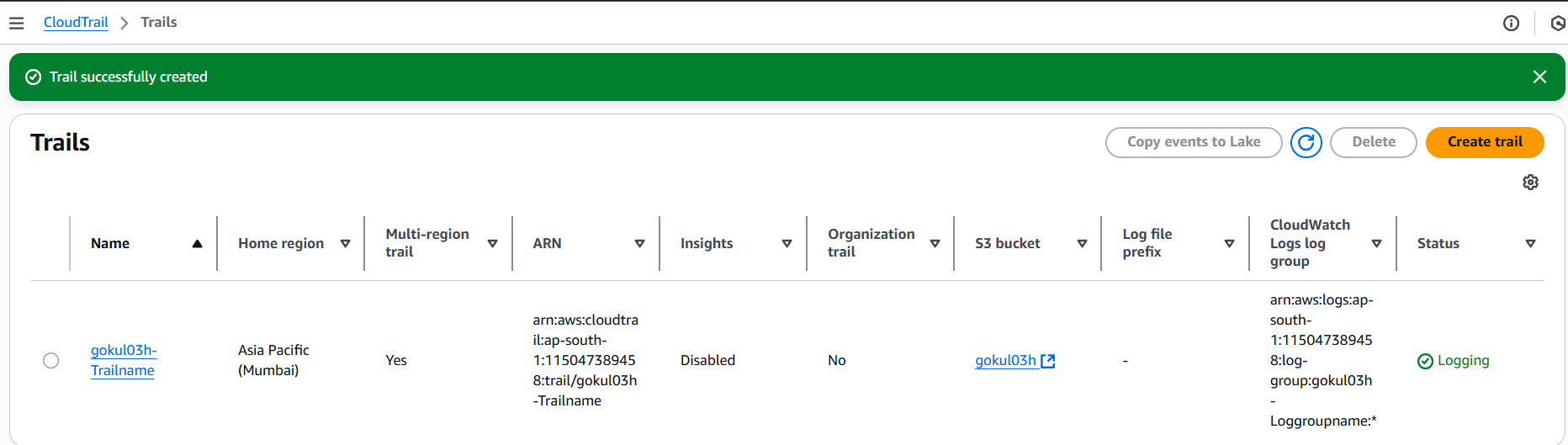
* + **Data events: -**

****

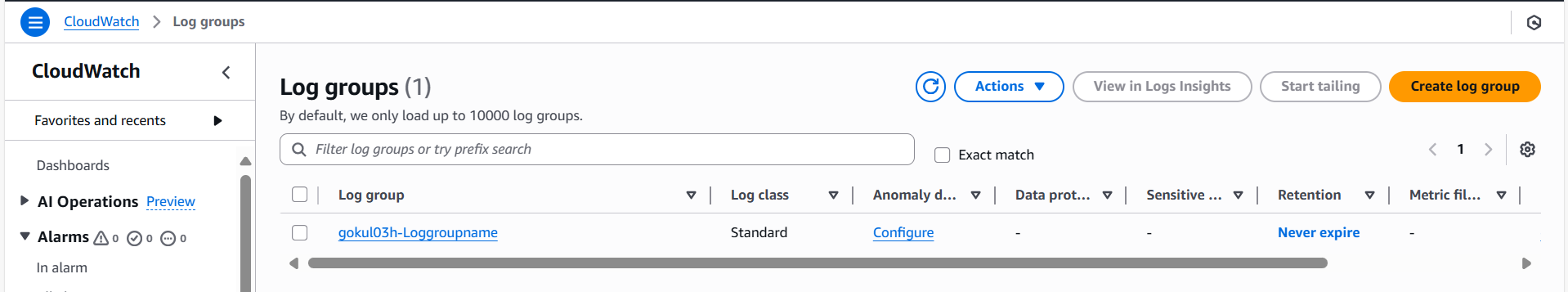
* + Click **Next**
  + Click **Create trail**

****

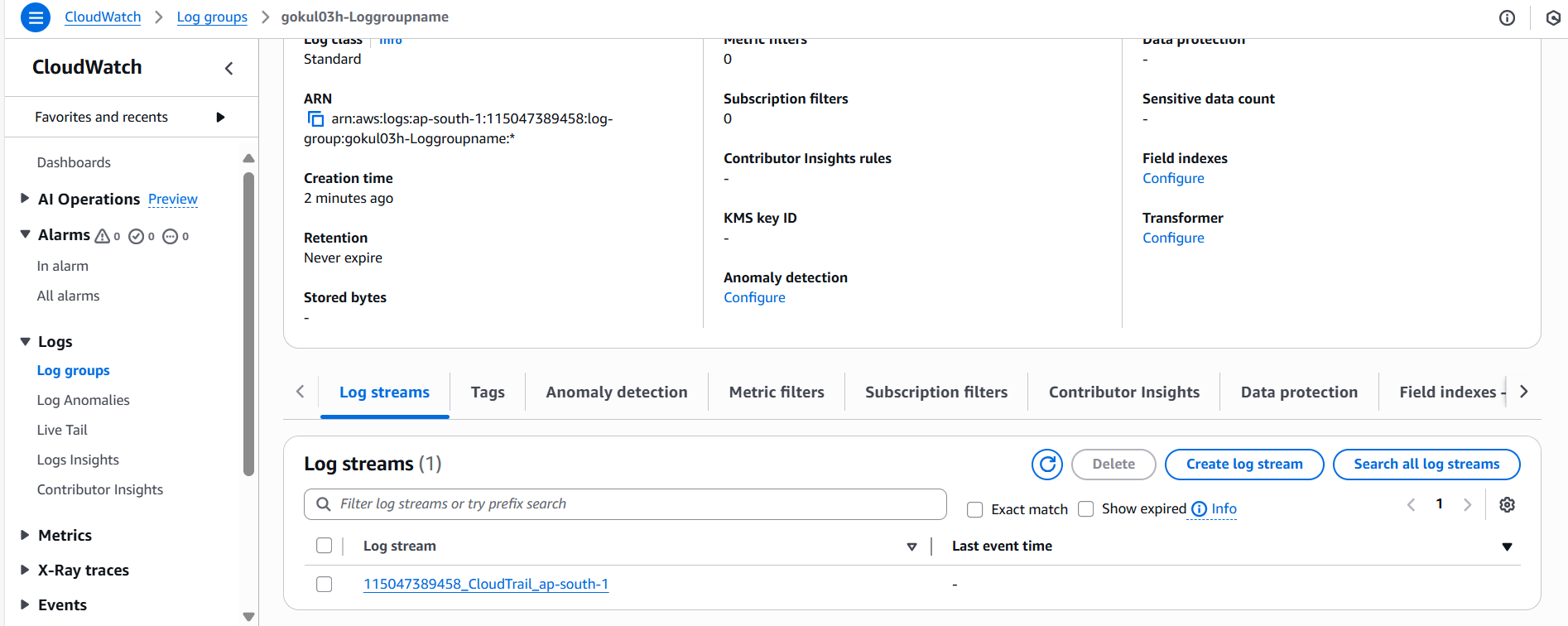
* Once **created trail successfully** and **trail** look like below,

****

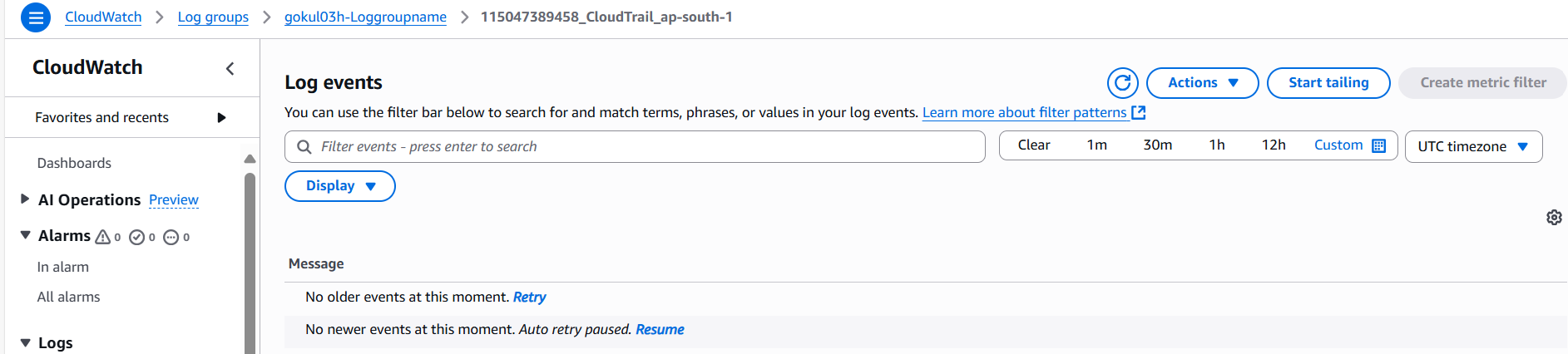
* Now in **“CloudWatch-> Log groups”** 🡺 New **Log group** has been created [ Refer the below screenshot].

****

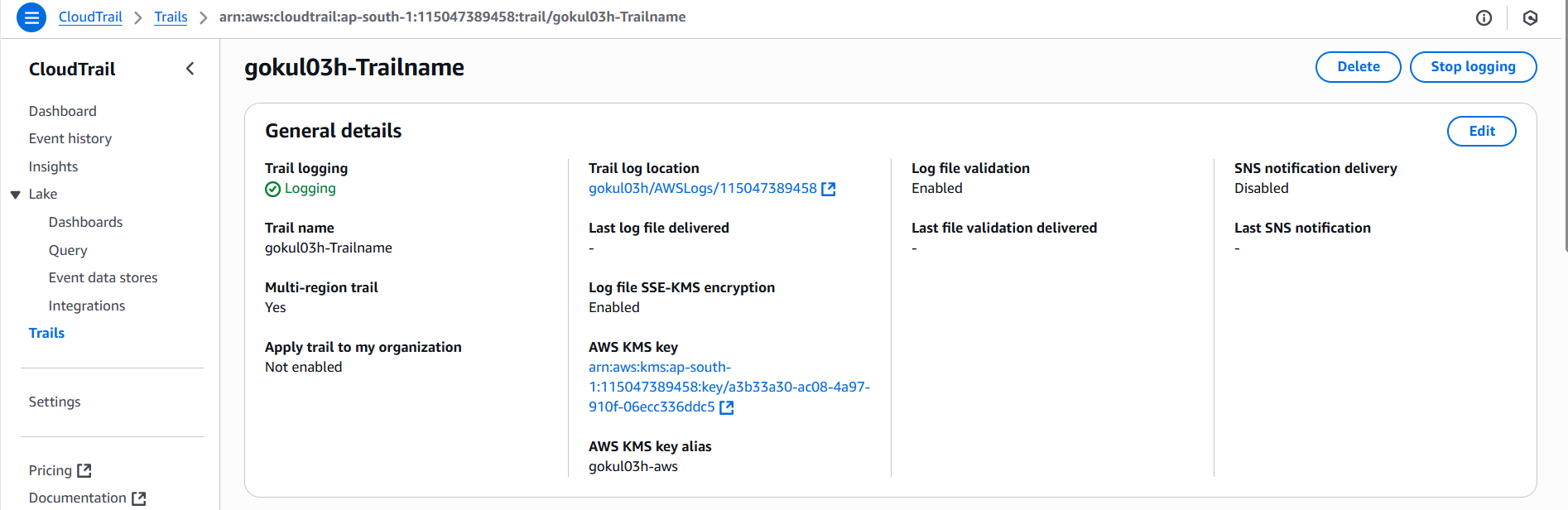
* Open **“Log group”** that created above -> Go to **“Log streams” -> Click Refresh option.**

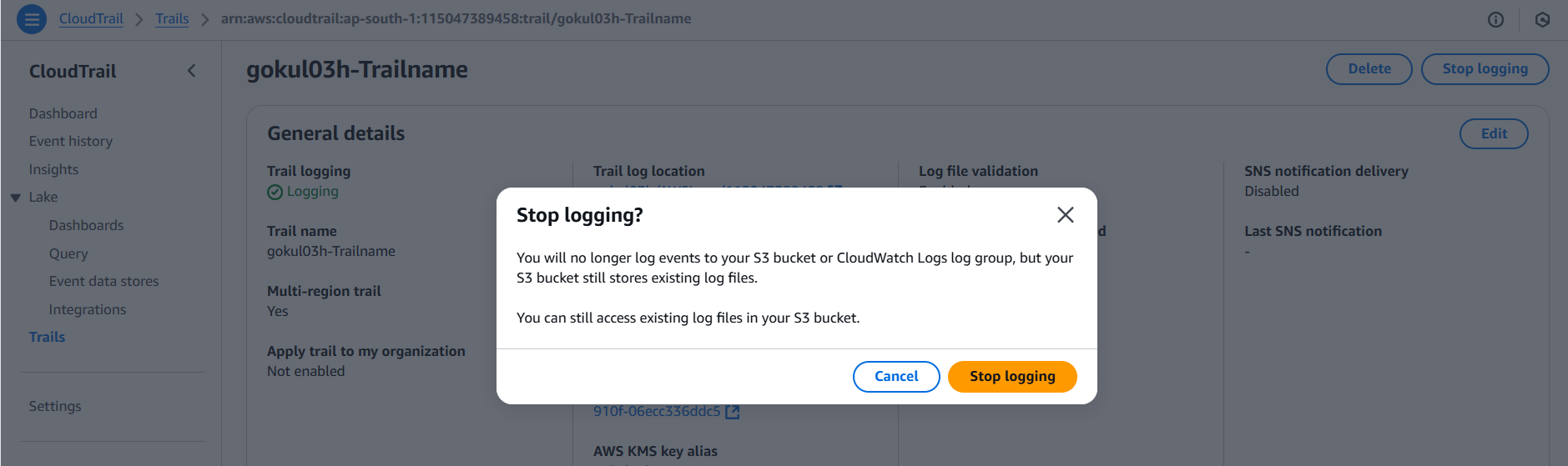
****

* Open **Log stream** there is **no logs** shown.

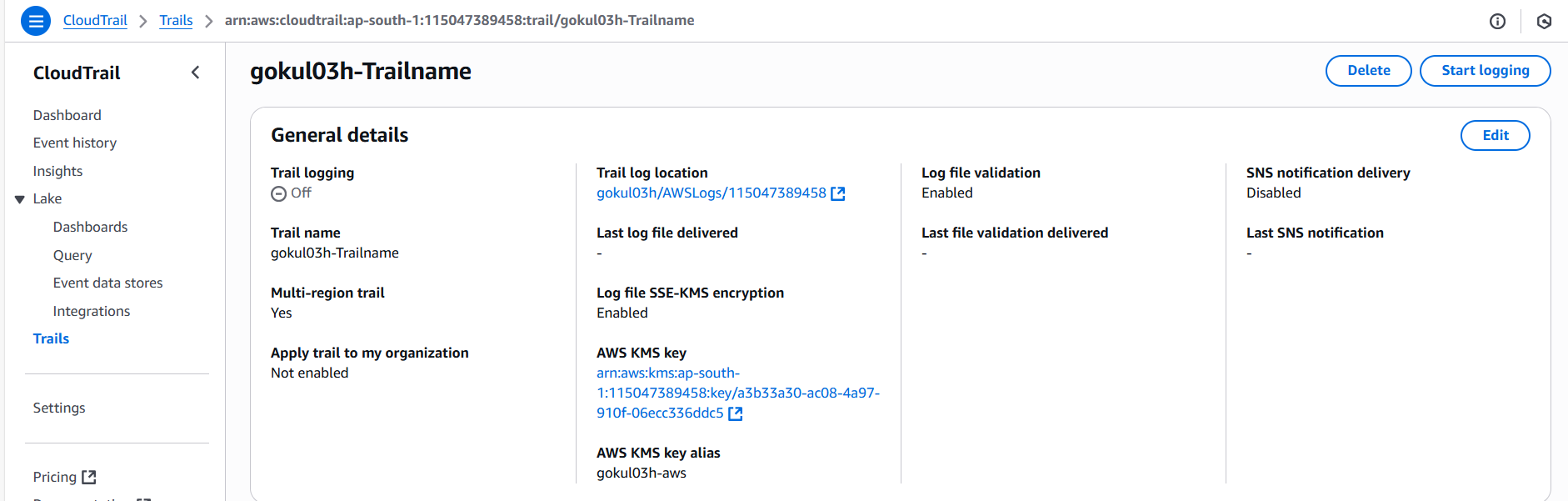
****

* Go to **CloudTrail -> Trails -> Select Trail** that created above
* Click **“Stop logging”**

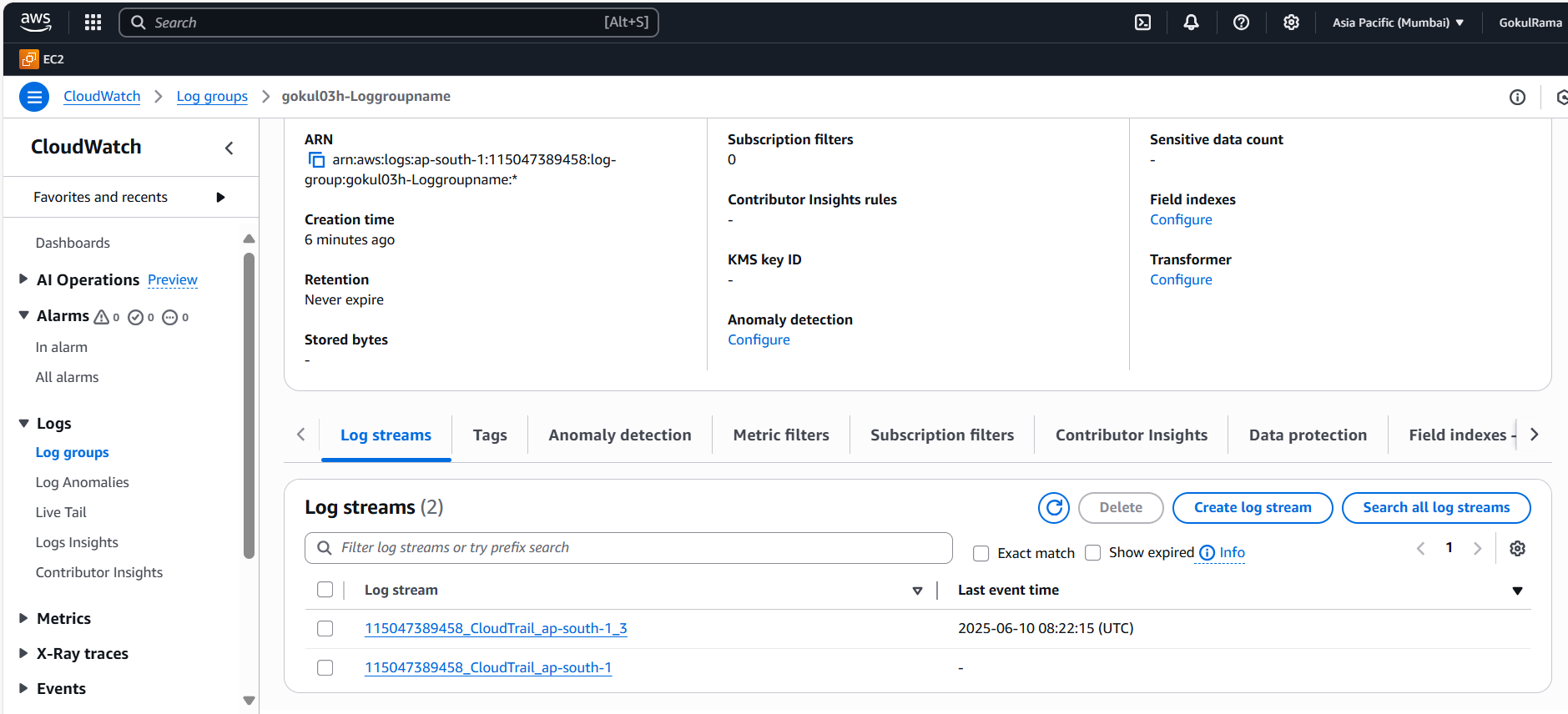
****

****

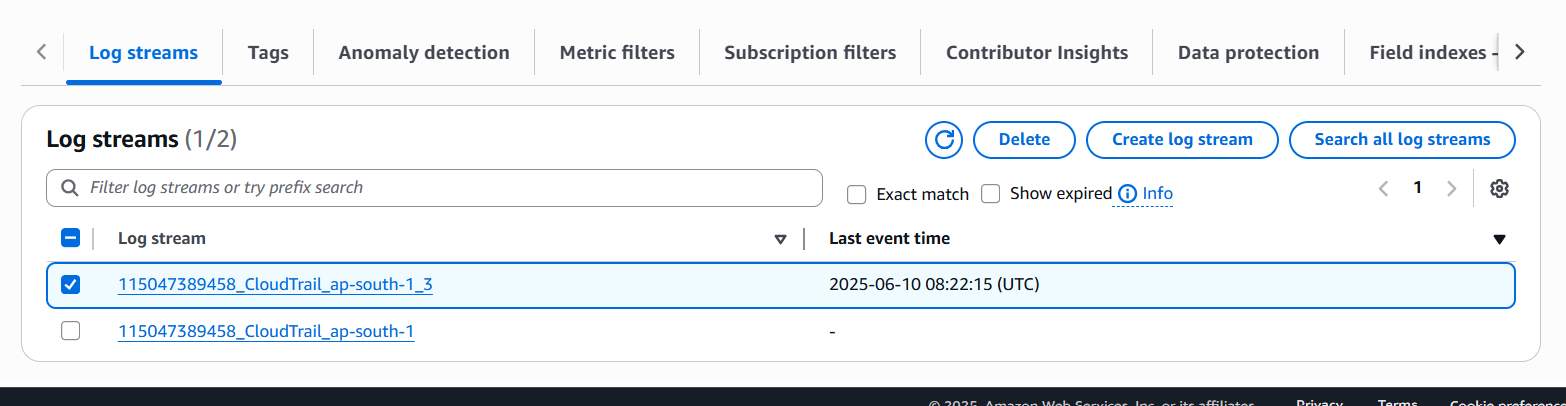
* Once **stopped**, select **“Start logging”**

****

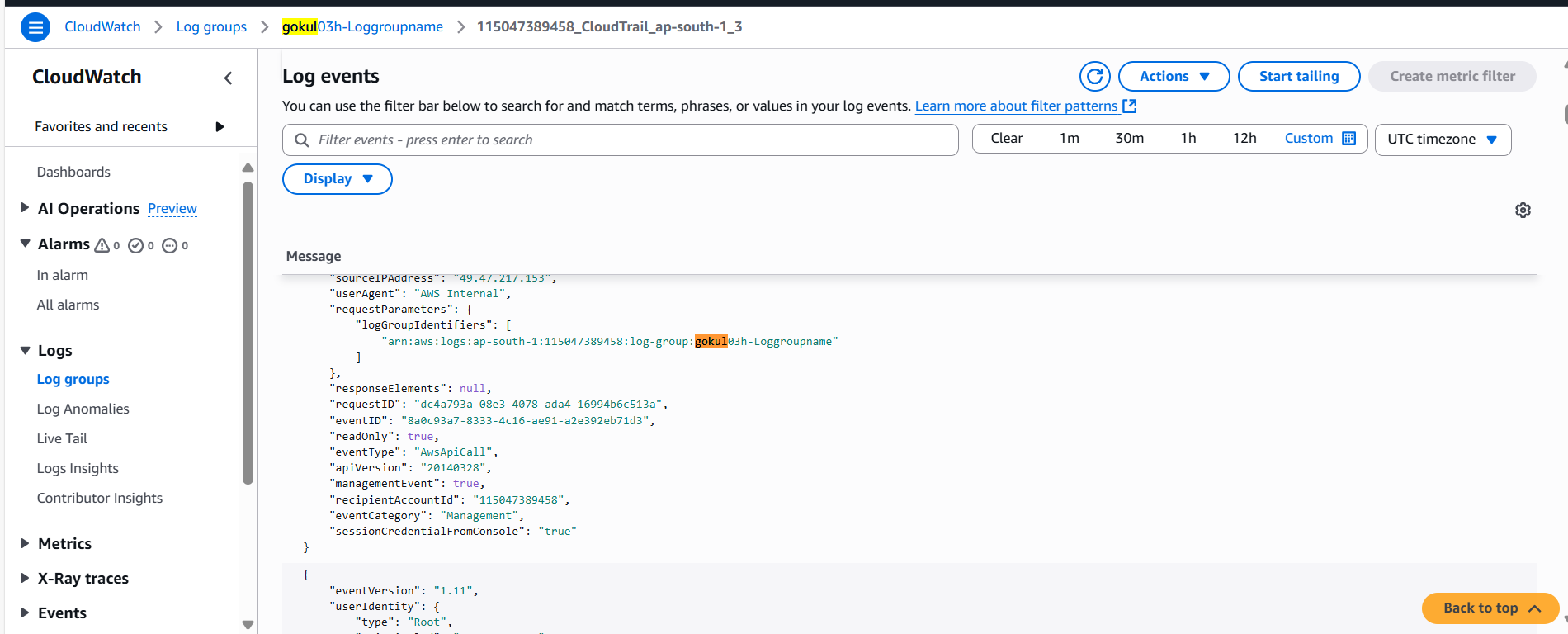
* Go to **“CloudWatch -> Log groups -> Log group name: gokul03h-Loggroupname”**
* Go to **“Log streams” ->** Click **Refresh.**

****

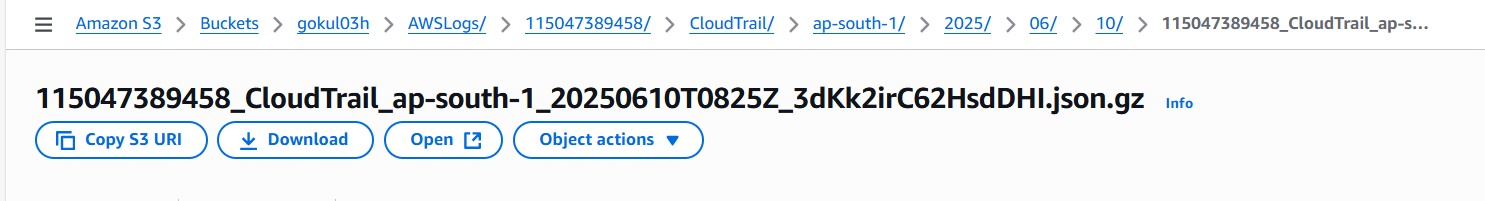
* **Select** and **open** the “**Latest log**” that got created.

****

* Now the **log** is,

****

* **Accessing the CloudWatch logs in S3 bucket: -**

****