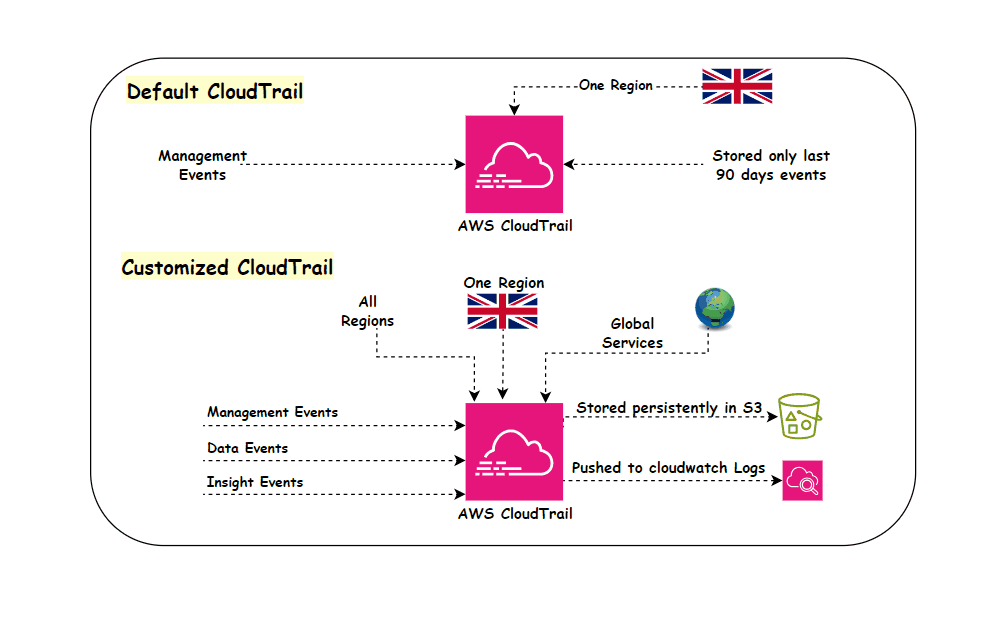
# AWS CloudTrail

# Introduction

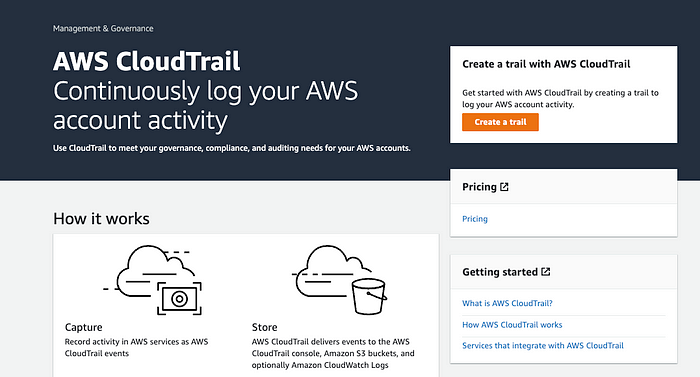
* AWS CloudTrail is like a detailed journal for your AWS account. It keeps track of everything that happens, like starting or stopping an instance, changing security settings, or creating and deleting buckets in S3.
* It’s like a detective that watches what every User, Role, or Service in your AWS account is doing. These records are called CloudTrail events and are super handy for finding out if something went wrong or just keeping a record of what’s happening.

**Note:** in CloudTrail Event history default enable in all region and it show the all activities in AWS account, delete logs is not possible in CloudTrail event

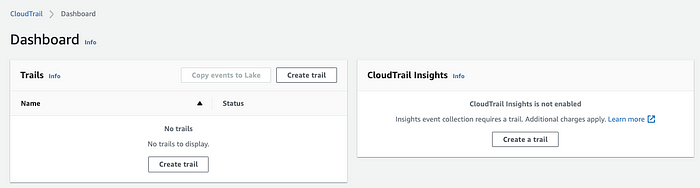


**Getting Started**

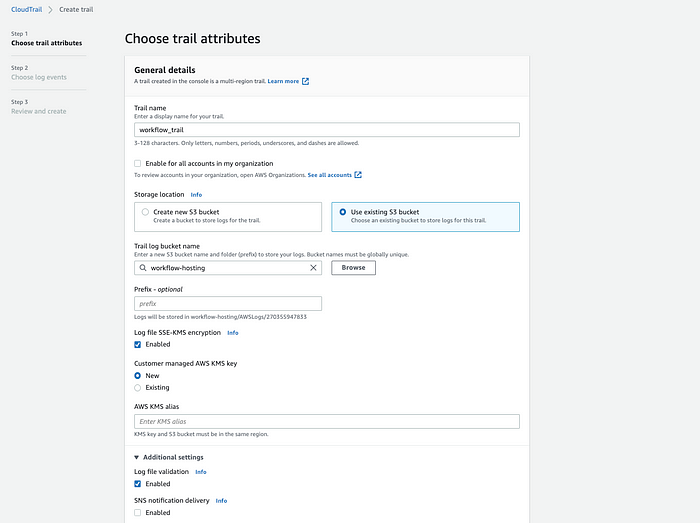
* In your AWS Management Console, search and click on AWS CloudTrail.



* Create a New Trail by clicking on Create Trail.



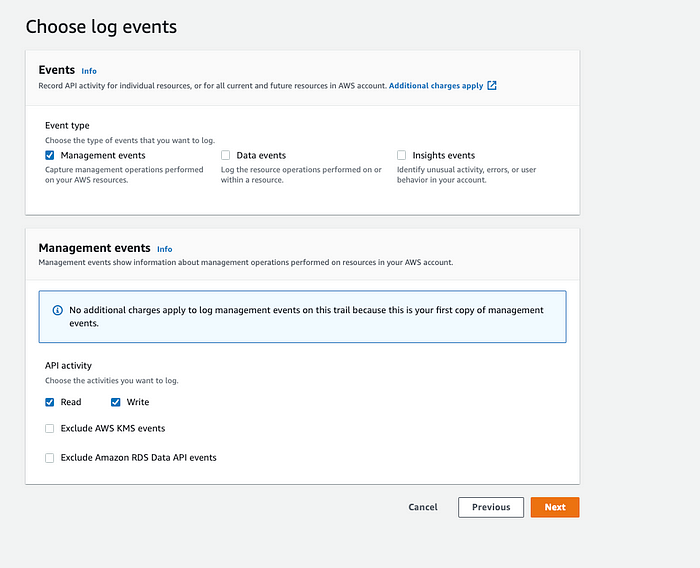
* Choose your Trail attributes. Enter your Trail name and storage location (select an existing S3 bucket or create a new S3 bucket). Enable your log file encryption with your file validation. This will ensure all aws resources are encrypted.



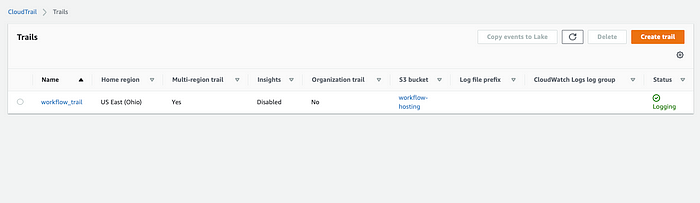
* When you’re done configuring your Trail attributes, click on **Next.**
* Next, choose your log events. In AWS CloudTrail, there are three types of events. Management events, Data events, and Insights events.
* Management events are free and can be viewed in the event history tab for 90 days. Data events are not free to the user and cannot be viewed in the event history tab. Insights events let you identify unusual activity, errors, or user behavior in your account.

**Why cloud trial event history tab for 90 day**

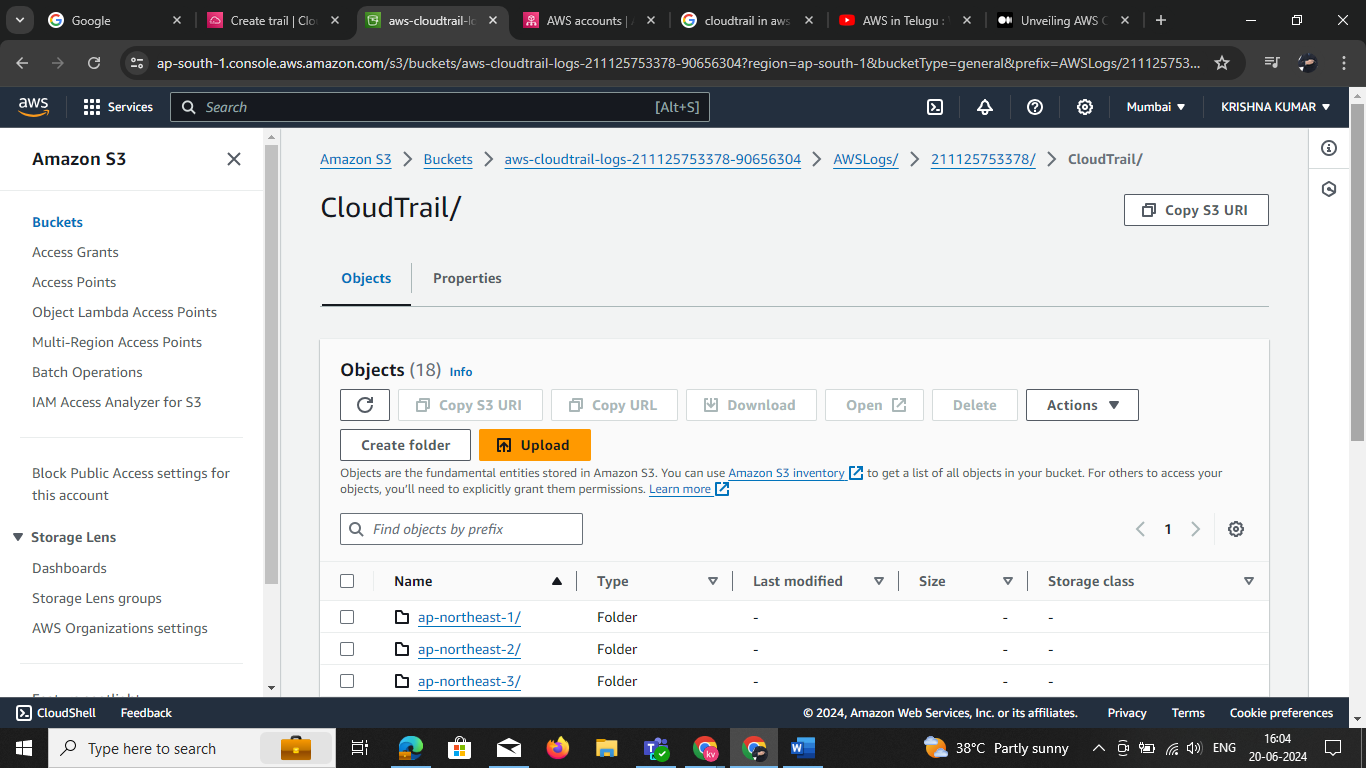
* Cloud trial logs typically store data for only 90 days due to several reasons:
* Cost Management: Storing logs incurs storage costs. By limiting the retention period to 90 days, cloud service providers can manage these costs effectively, especially for trial accounts which are often free or low-cost.
* Resource Optimization: Cloud infrastructure resources, including storage, are finite. Limiting log retention helps optimize the use of these resources, ensuring that they are available for active users and more critical data.
* Security and Compliance: Shorter log retention periods can mitigate risks associated with data breaches and ensure compliance with certain data protection regulations that mandate minimal data storage.
* Performance: Managing and querying a large volume of logs can degrade performance. By limiting the log retention period, providers ensure that the system remains efficient and responsive.
* Encouraging Upgrades: Trial accounts are meant to give users a taste of the full service. By limiting log retention, providers encourage users to upgrade to paid plans that offer longer retention periods and additional features.
* In summary, the 90-day log retention policy for cloud trials is a balanced approach to manage costs, optimize resources, maintain security, and ensure good system performance while encouraging users to transition to paid services.
* Only Management events are free for your workloads. Data and Insights events will incur costs. In this tutorial, we’ll be using **Management Events.**



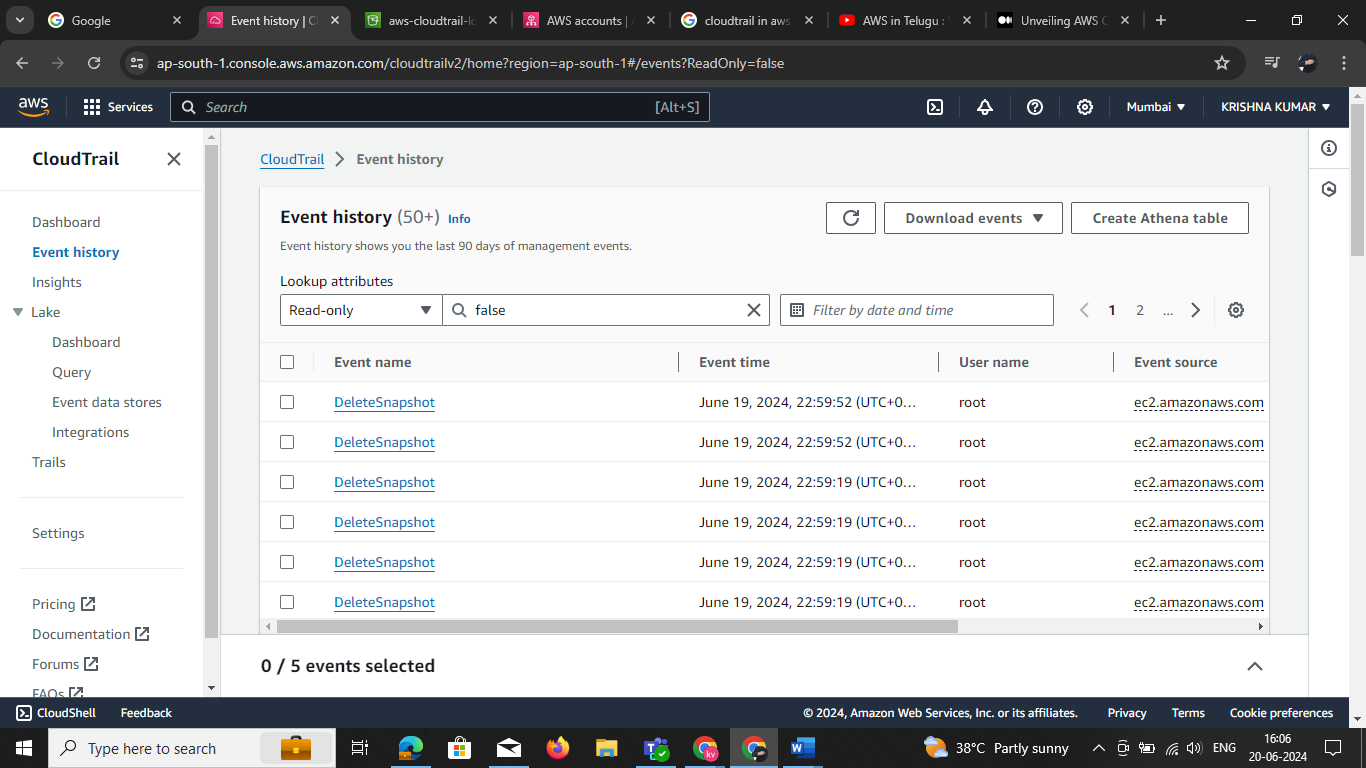
* When you’re done configuring log events, click on **Next**, you’ll see the overview and general details of your configuration, and click on **Create Trail.**
* In your Trails dashboard, you’ll see the Trail you just created.



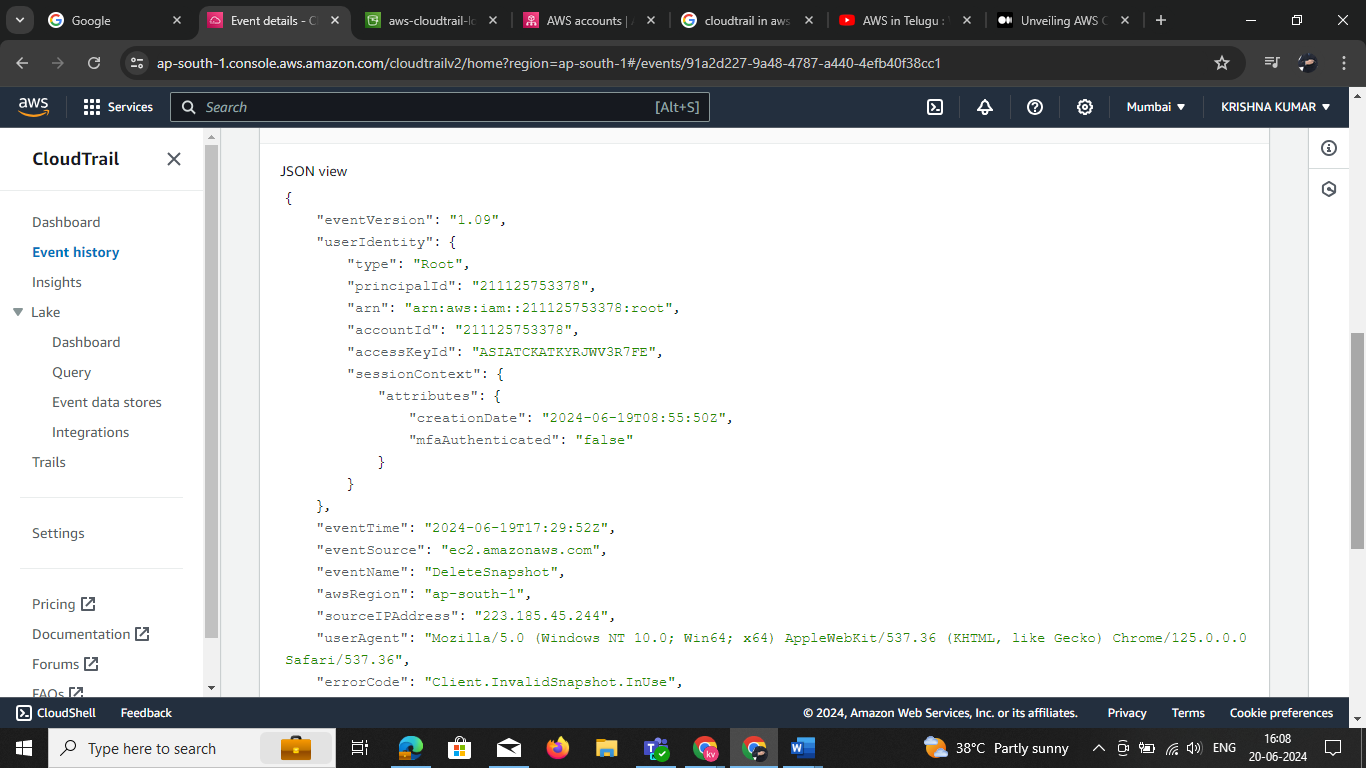
* Integrate other AWS resources with your trail to see how it works and see different log events. For example, in my S3 bucket, I’ll upload a new file into my S3 bucket. Once I’m done uploading the file, I’ll automatically see the events in my CloudTrail.



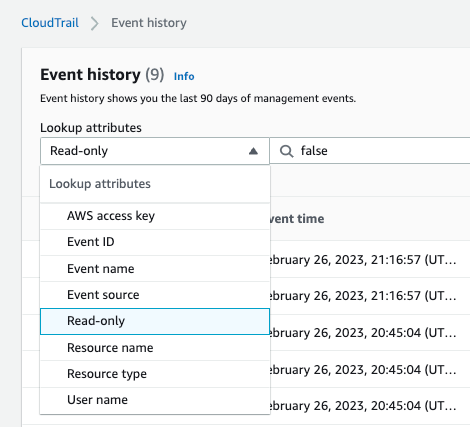
* In your CloudTrail event history, you’ll see all your events and logs from your S3 bucket.



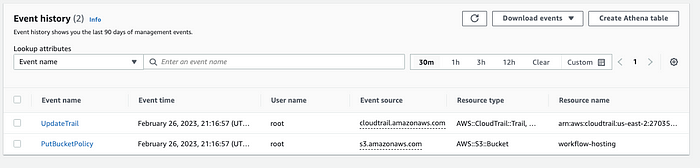
* You’ll see your event records and referenced resources when you click on them.



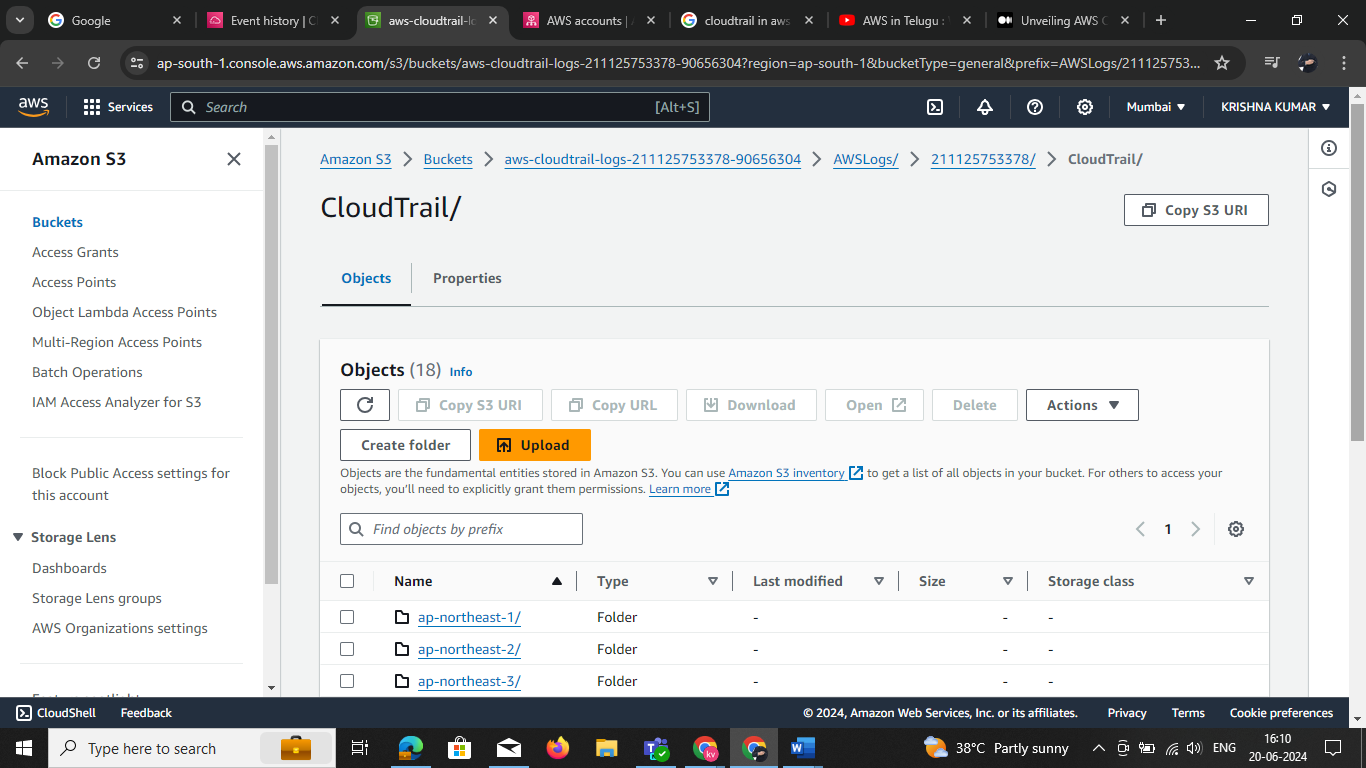
* You can also filter your event history based on AWS access key, Event ID, Event Name, Event Source, Resource name, and user type.



* You’ll see the PUT event history in your Event Name, the S3 bucket we updated earlier.



* In your AWS S3 storage bucket, you’ll see your CloudTrail log events in the AWS logs folder.



* When you click on Cloud Trail, you can see the logs from each AWS Region.

