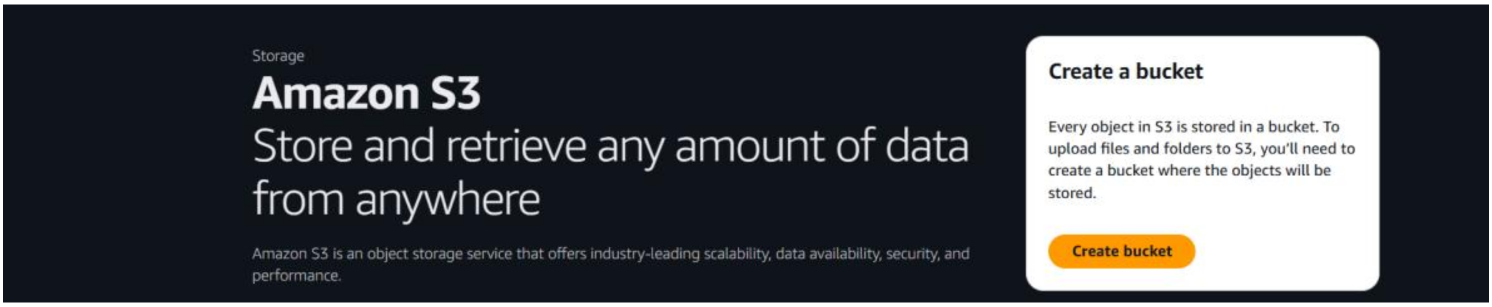
Enable server access login for an S3 bucket and setup a CloudWatch Event rule to track and alert when a new object is uploaded

- Prplevamp20

Overview

The task involves enabling **S3 Server Access Logging** for an S3 bucket to monitor access requests, uploading an object to see the logs, and setting up a **CloudWatch Event Rule** to notify when new objects are uploaded. This helps ensure better observability and real-time monitoring of S3 bucket activities.



Storage

Amazon S3

Store and retrieve any amount of data from anywhere

Amazon S3 is an object storage service that offers industry-leading scalability, data availability, security, and performance.

Create a bucket

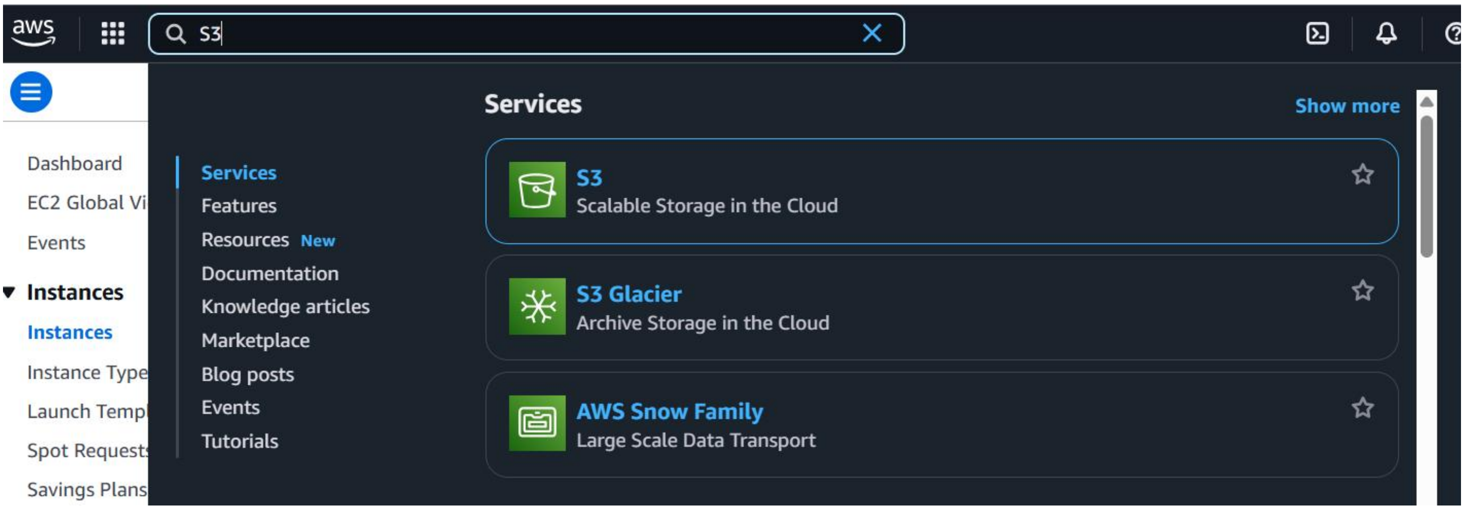
Every object in S3 is stored in a bucket. To upload files and folders to S3, you'll need to create a bucket where the objects will be stored.

Prerequisites

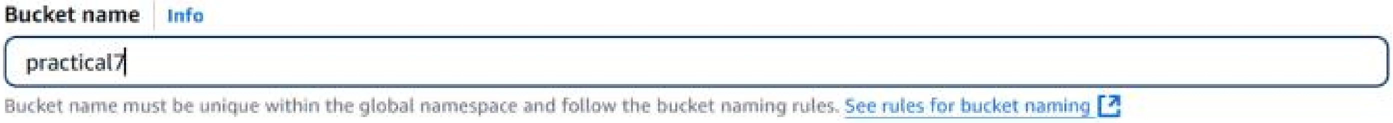
- **AWS Account:**: Ensure you have access to the AWS Management Console.
- **S3 Bucket:**: Create an S3 bucket if you don't already have one.
- **IAM Permissions**: Ensure your IAM role/user has sufficient permissions to configure S3 logging, CloudWatch rules, and SNS.
- **SNS Topic:**: Optional but recommended for notification setup.

STEP 1:

1. Login to AWS console and navigate to S3 service.



2. Click on create bucket or can use the existing one.
3. Give the bucket name and it should be unique, keep everything at default and create bucket.

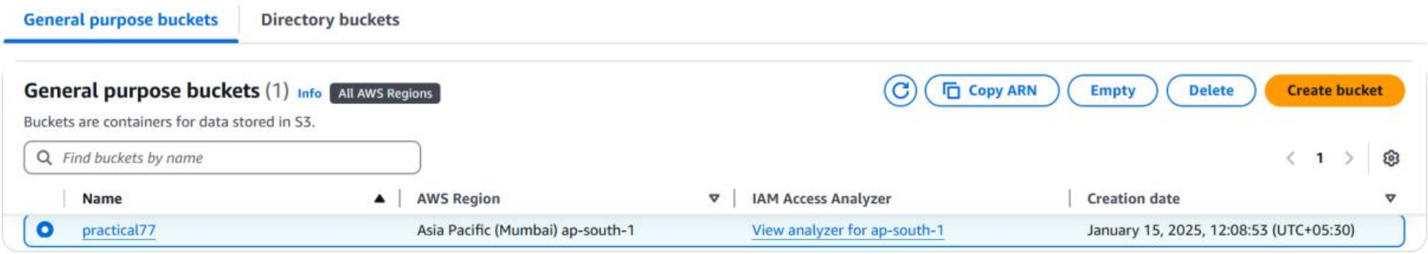


Bucket name Info

practical7

Bucket name must be unique within the global namespace and follow the bucket naming rules. See rules for bucket naming

4. From the S3 dashboard, click on the name of the bucket.

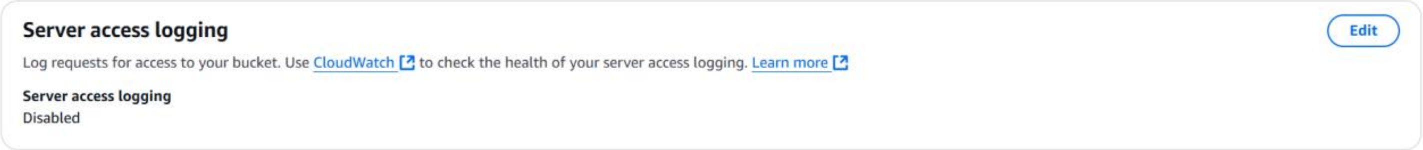


General purpose buckets (1)

Buckets are containers for data stored in S3.

	Name	AWS Region	IAM Access Analyzer	Creation date
●	practical77	Asia Pacific (Mumbai) ap-south-1	View analyzer for ap-south-1	January 15, 2025, 12:08:53 (UTC+05:30)

5. Go to properties tab
6. Enable the server access logging and select the bucket under Destination.

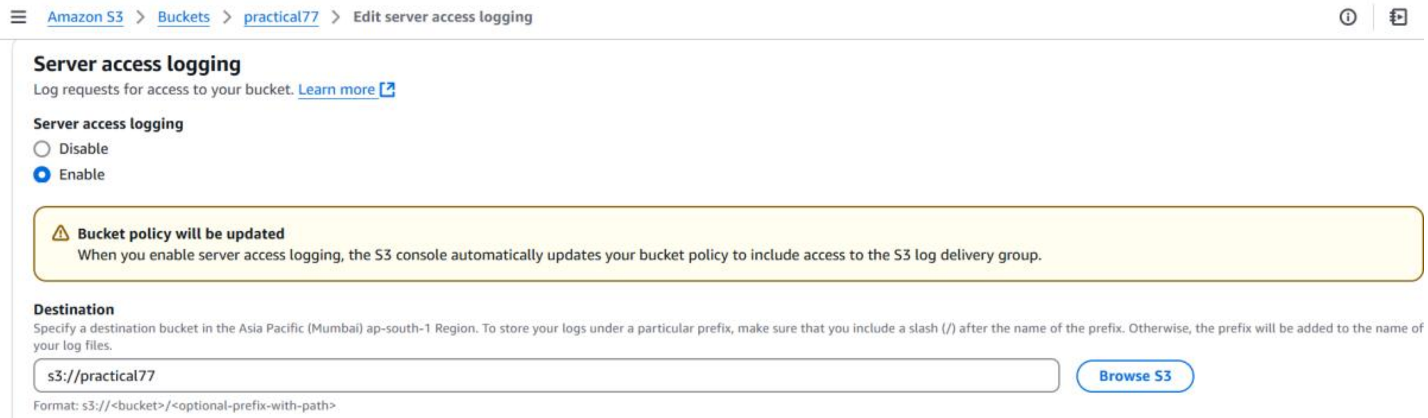


Server access logging

Log requests for access to your bucket. Use CloudWatch to check the health of your server access logging. Learn more

Server access logging
Disabled

7. Enable the server access logging and select the bucket under Destination.


Amazon S3 > Buckets > practical77 > Edit server access logging
Browse S3

Server access logging

Log requests for access to your bucket. Learn more

Server access logging

○ Disable

● Enable

Bucket policy will be updated

When you enable server access logging, the S3 console automatically updates your bucket policy to include access to the S3 log delivery group.

Destination

Specify a destination bucket in the Asia Pacific (Mumbai) ap-south-1 Region. To store your logs under a particular prefix, make sure that you include a slash (/) after the name of the prefix. Otherwise, the prefix will be added to the name of your log files.

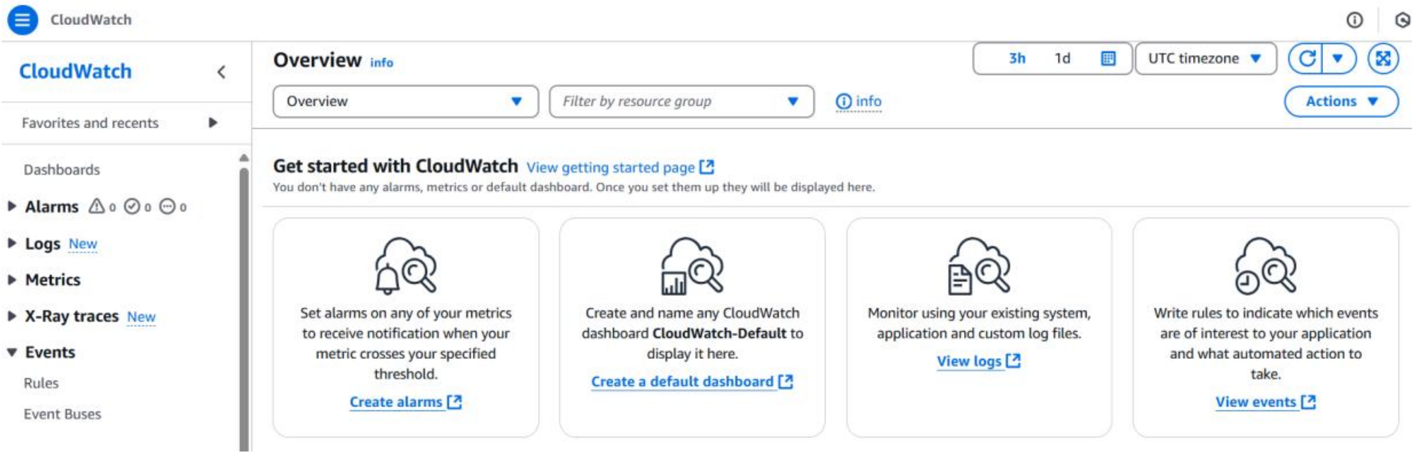
s3://practical77

Format: s3://<bucket>/<optional-prefix-with-path>

8. Click save changes.

STEP 2:

1. Navigate to Cloudwatch
2. In the left sidebar of CloudWatch, Click on Rules under Events section



Get started with CloudWatch View getting started page

You don't have any alarms, metrics or default dashboard. Once you set them up they will be displayed here.

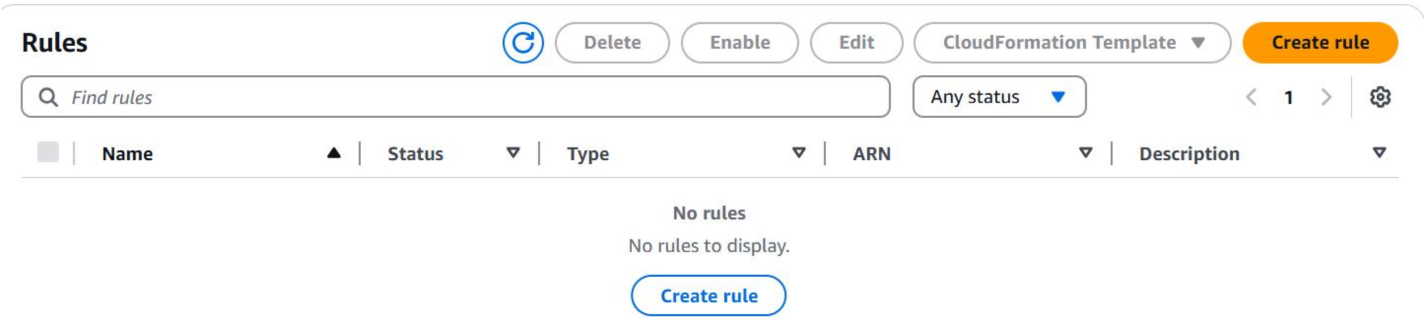
Set alarms on any of your metrics to receive notification when your metric crosses your specified threshold.

Create and name any CloudWatch dashboard **CloudWatch-Default** to display it here.

Monitor using your existing system, application and custom log files.

Write rules to indicate which events are of interest to your application and what automated action to take.

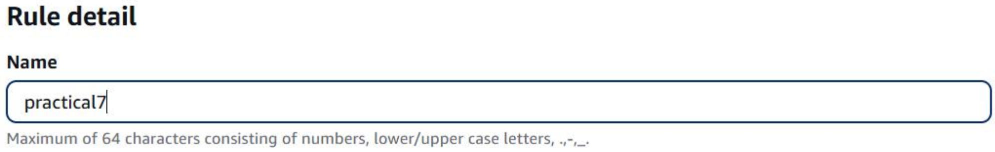
3. Click on Create Rule



No rules

No rules to display.

4. Give the name of the rule and click next



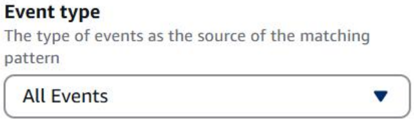
Rule detail

Name

practical7

Maximum of 64 characters consisting of numbers, lower/upper case letters, .,-,_.

5. Under Event Source, Choose event source as AWS Services, AWS services as S3 and Event type as All Events.

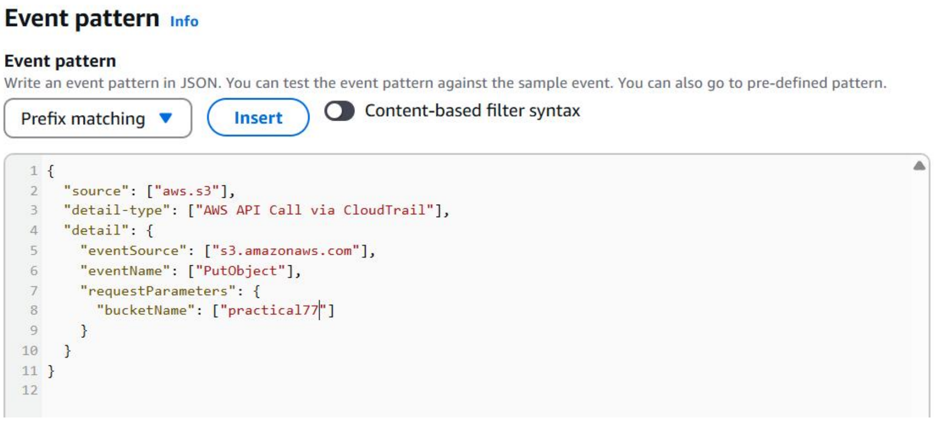


Event type

The type of events as the source of the matching pattern

All Events

6. In the event pattern, you need to specify the S3 bucket you want to track. Add the JSON filter and click next.



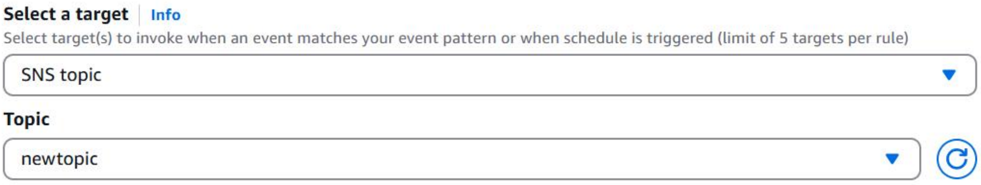
Event pattern

Event pattern

Write an event pattern in JSON. You can test the event pattern against the sample event. You can also go to pre-defined pattern.

```
{
  "source": ["aws.s3"],
  "detail-type": ["AWS API Call via CloudTrail"],
  "detail": {
    "eventSource": ["s3.amazonaws.com"],
    "eventName": ["PutObject"],
    "requestParameters": {
      "bucketName": ["practical77"]
    }
  }
}
```

7. Select the target type as SNS and give topic name (if there is no SNS topic create one and confirm the subscription through email) and click next and create rule.



Select a target

Select target(s) to invoke when an event matches your event pattern or when schedule is triggered (limit of 5 targets per rule)

SNS topic

Topic

newtopic

8. If it worked then you will get the notification on your Email if you perform any event on S3.

This setup ensures your S3 bucket activities are logged and monitored with real-time alerts for new uploads.