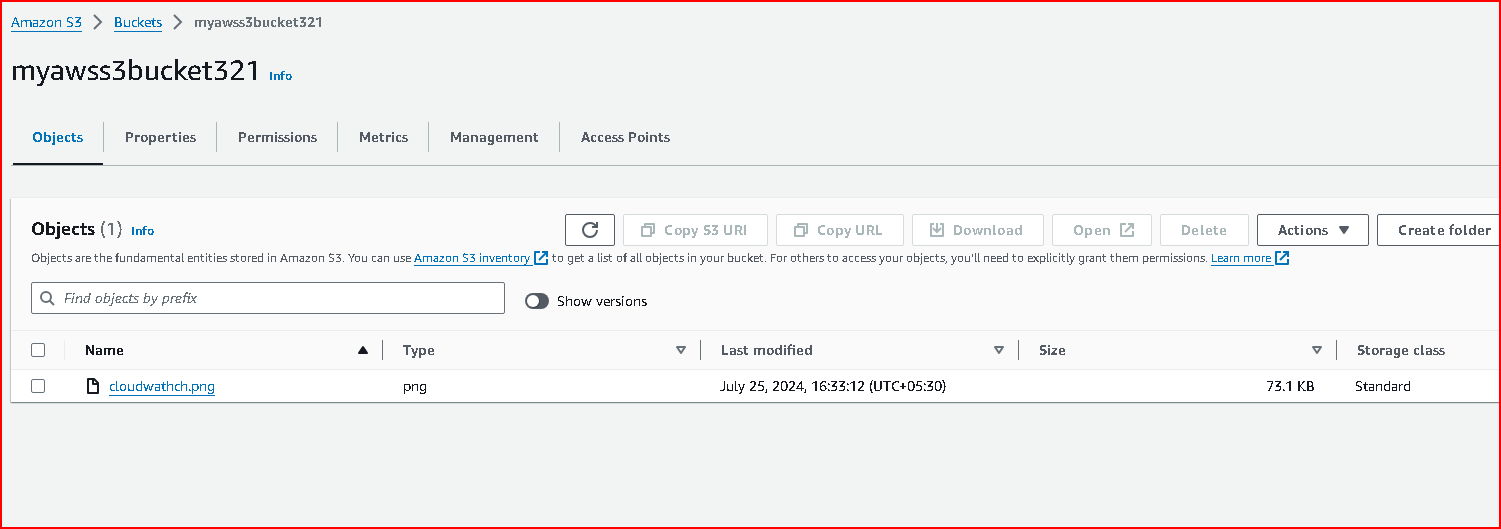
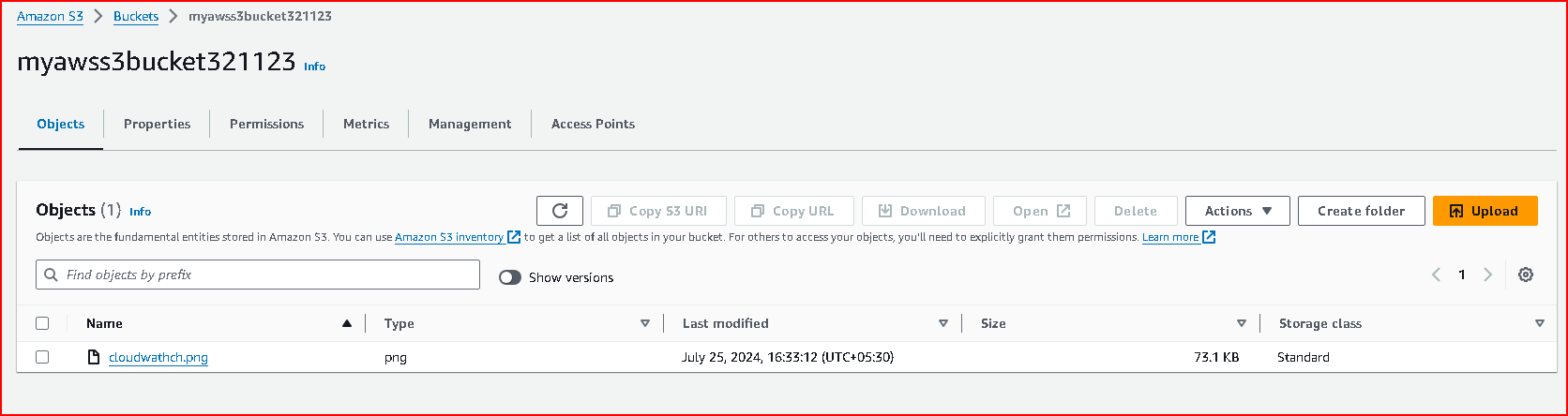
**AWS S3, CloudWatch and CloudTrail - POC**

Step 1: Create Two S3 Buckets

Primary Bucket: This is where your objects will initially be uploaded.



Replica Bucket: Objects from the primary bucket will be replicated to this bucket.



Ensure both buckets are in the same AWS region.

Step 2: Enable Versioning on the Buckets

Versioning must be enabled on both the primary and replica buckets for replication to work properly.

Enable Versioning:

Go to the AWS Management Console.

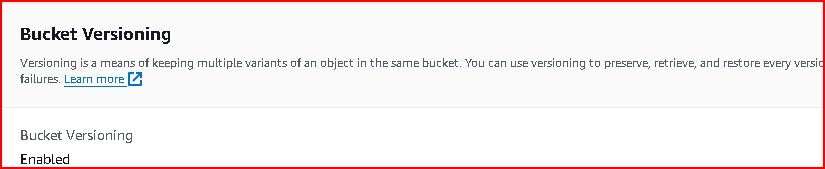
Navigate to the S3 service.

Select your primary bucket.

Go to the Properties tab.

Click on Versioning and enable versioning.

Repeat these steps for the replica bucket.



Step 3: Configure Cross-Region Replication (CRR)

Since both buckets are in the same region, you will configure Same-Region Replication (SRR) instead of Cross-Region Replication.

Configure Same-Region Replication:

Select your primary bucket.

Go to the Management tab.

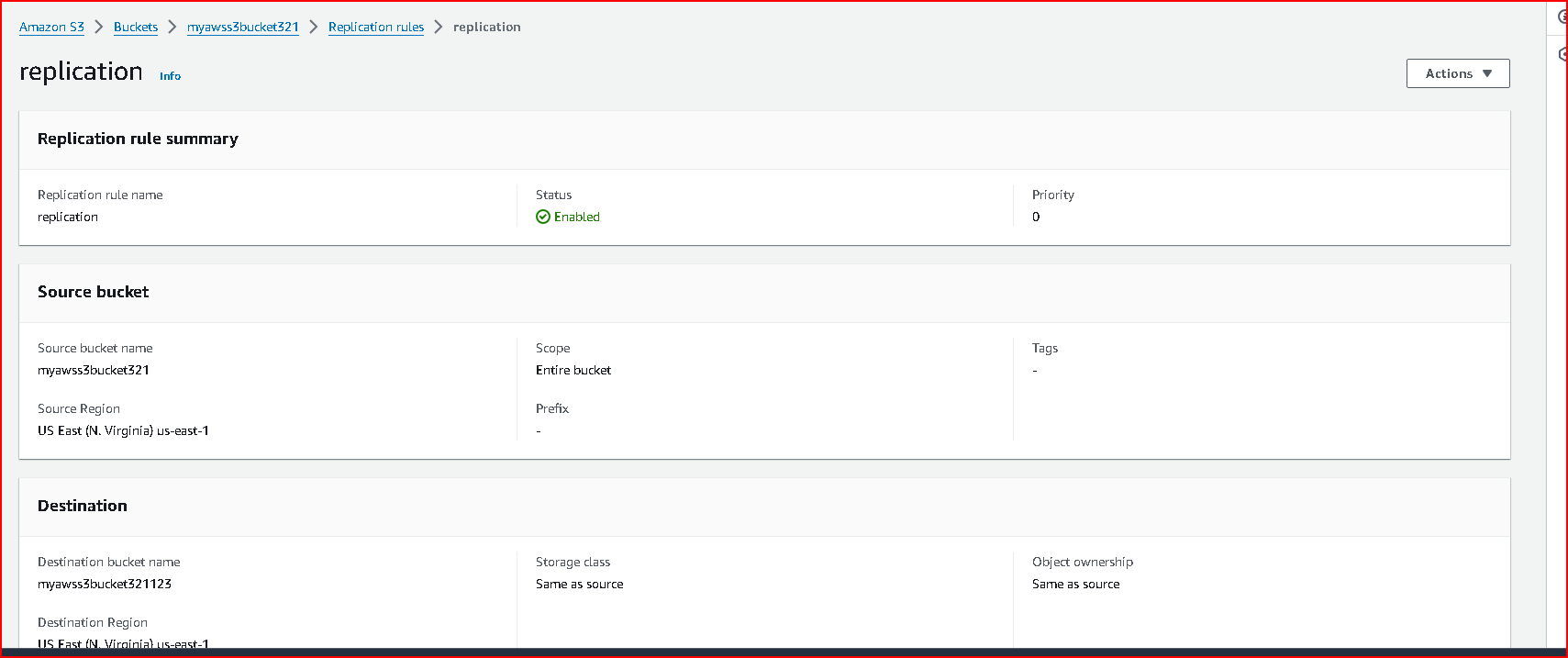
Click on Replication and then + Add rule.

Follow the prompts to configure replication:

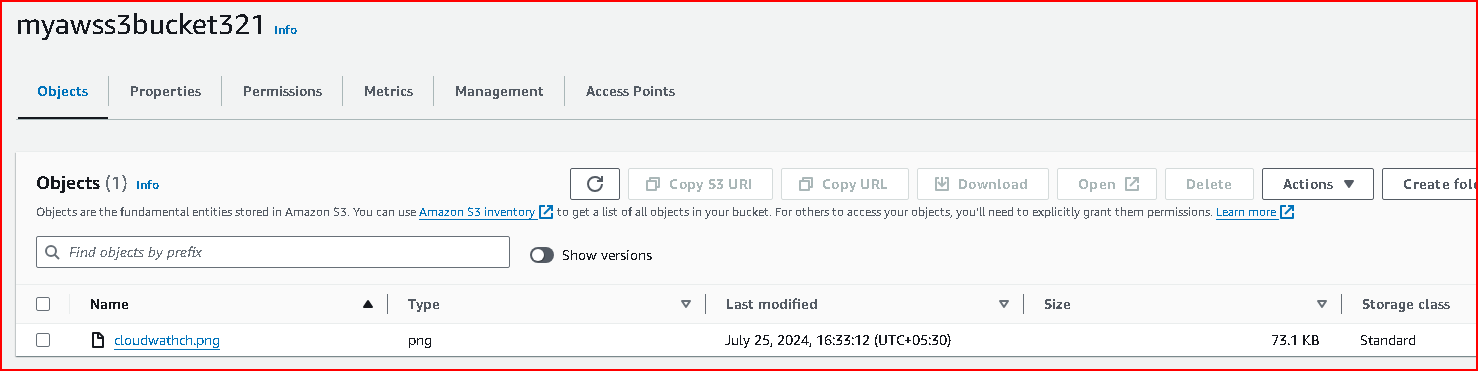
Source: Choose the primary bucket.

Destination: Choose the replica bucket.

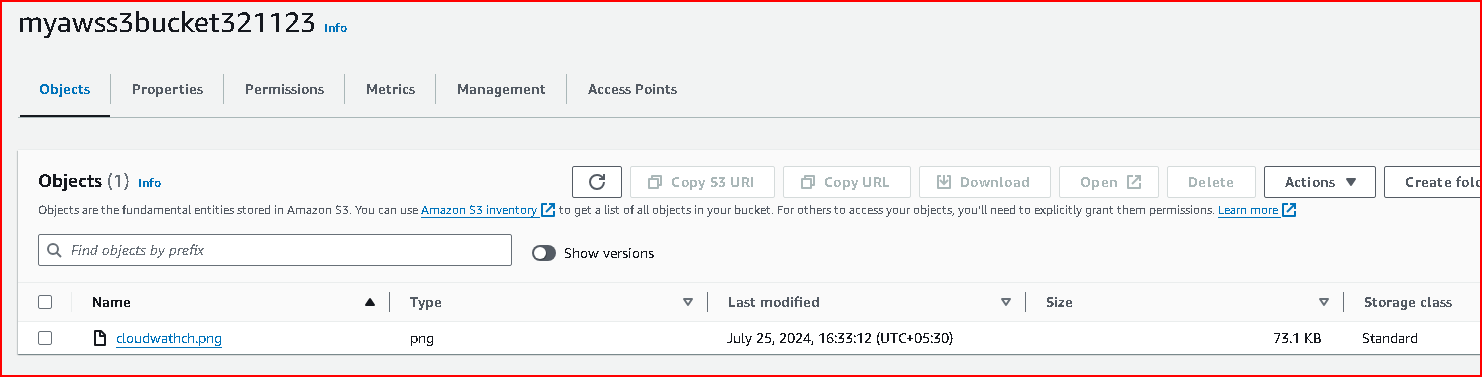
Choose the replication options as per your needs.



Upload the object in source bucket.



Object is reflected in destination bucket



Step 4: Apply Lifecycle Policies

Lifecycle policies will transition objects to Glacier storage class after 30 days and delete them after 365 days.

Create Lifecycle Policy:

Select your primary bucket.

Go to the Management tab.

Click on Lifecycle and then + Add lifecycle rule.

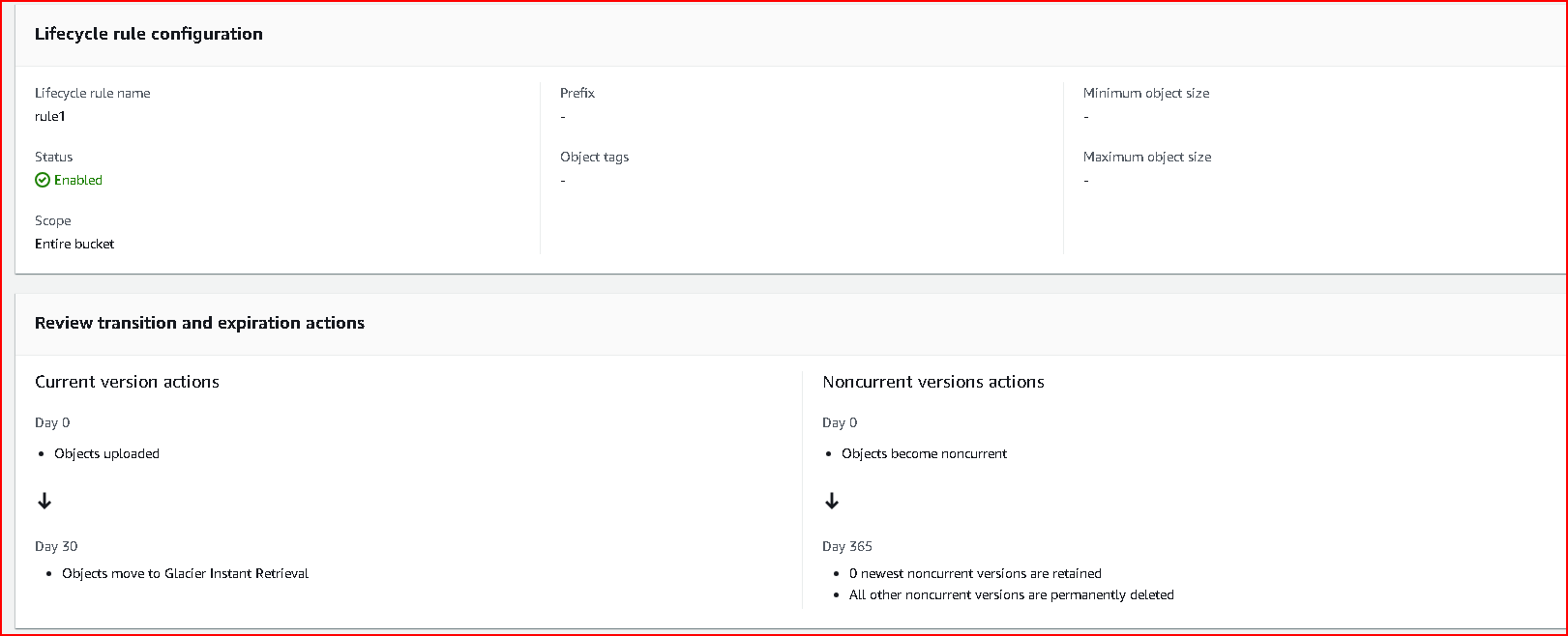
Configure the rule:

Name: Give your rule a name.

Scope: Apply the rule to all objects or filter by prefix/tag.

Transitions: Add a transition to Glacier after 30 days.

Expiration: Permanently delete objects after 365 days



Step 5: Enable Server-Side Encryption

Enable server-side encryption to ensure that objects stored in S3 are encrypted at rest.

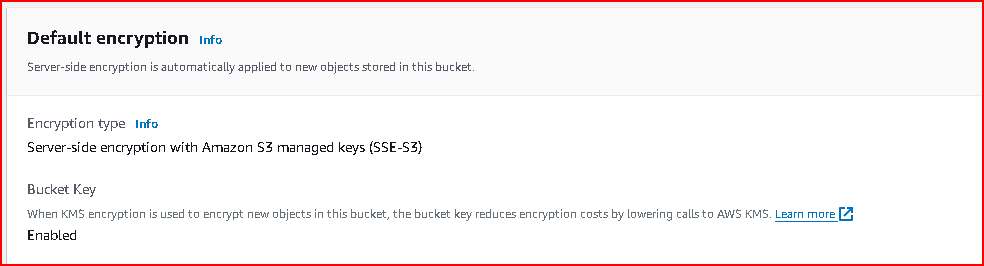
Enable Encryption:

Select your primary bucket.

Go to the Properties tab.

Click on Default encryption.

Choose the encryption option.



Ensure that you also enable encryption on the replica bucket.

Step 6: Set Up Static Website Hosting

You can configure your bucket to host a static website.

Configure Static Website Hosting:

Select your primary bucket.

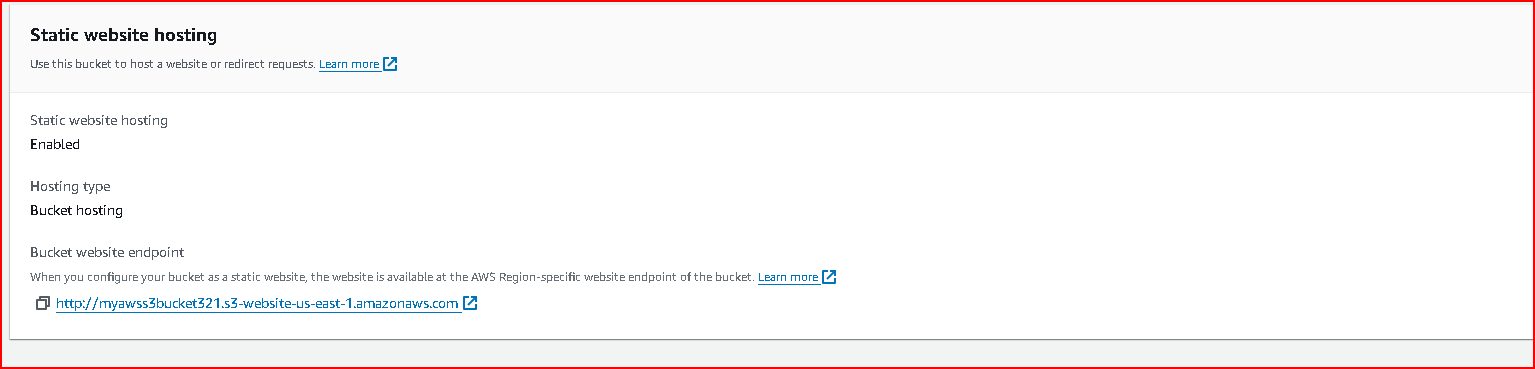
Go to the Properties tab.

Click on Static website hosting.

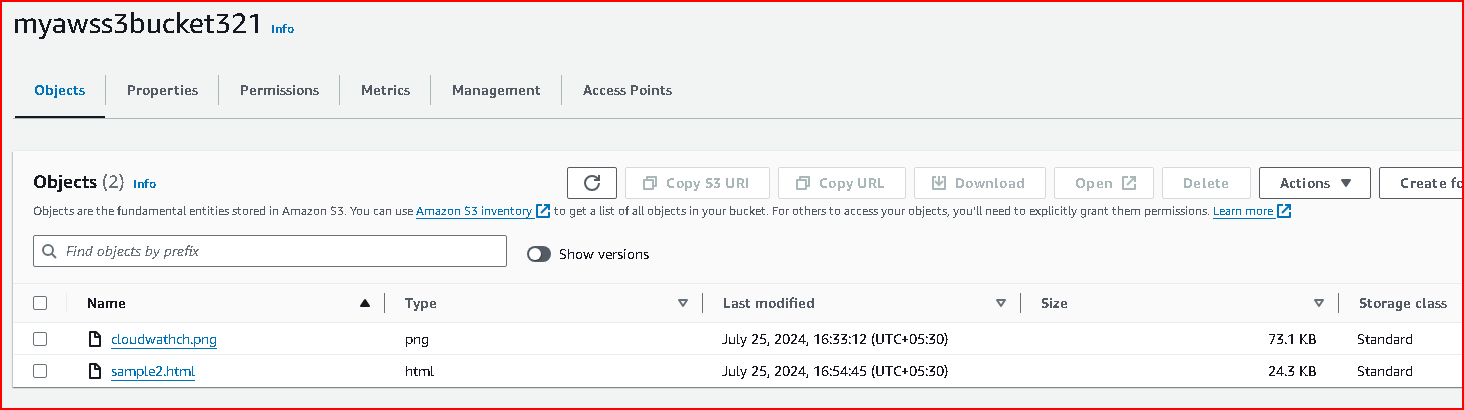
Choose Use this bucket to host a website.

Specify the index document and error document if needed.

Save the configuration.



Upload the index.html file and check if it is working.





**Task List for CloudWatch and CloudTrail :**

1. **Collect and track key performance metrics for EC2 instances and S3 buckets**

EC2 Instances:

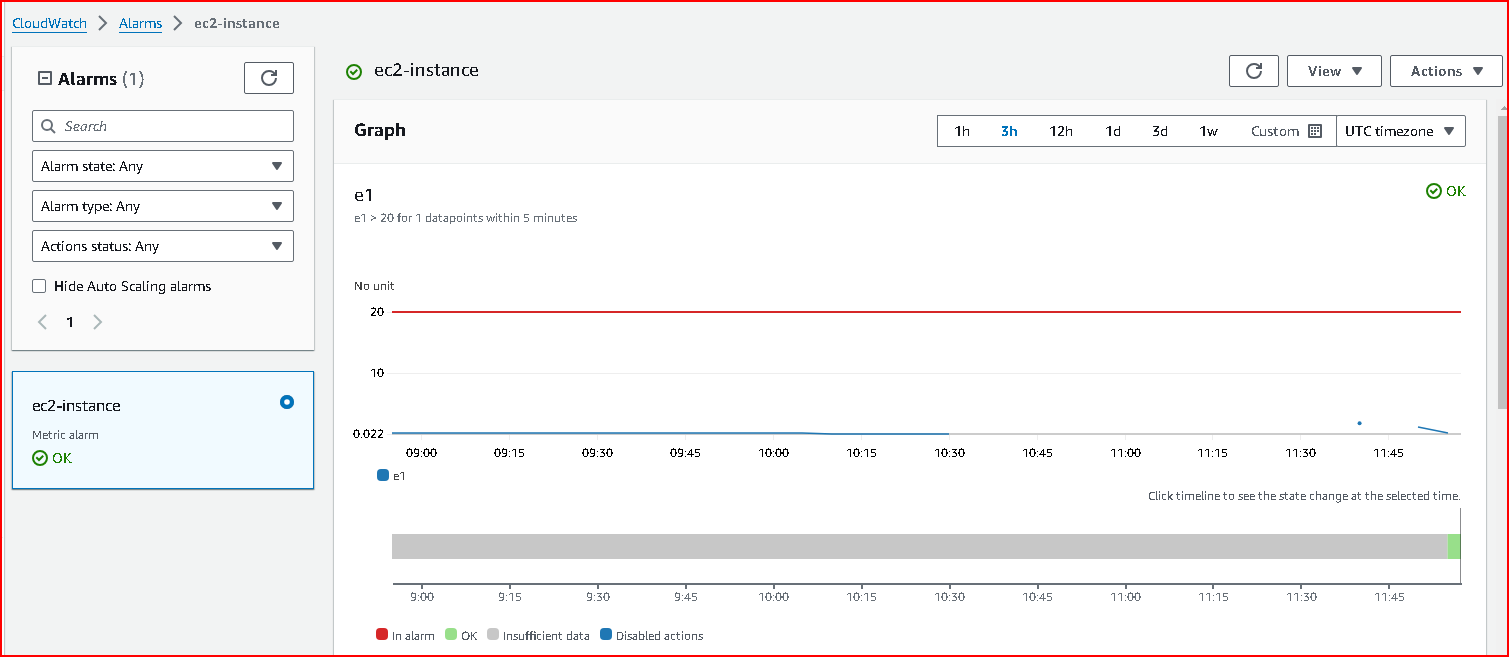
Navigate to the AWS Management Console and go to the CloudWatch service.

In the left-hand navigation pane, click on "Metrics".

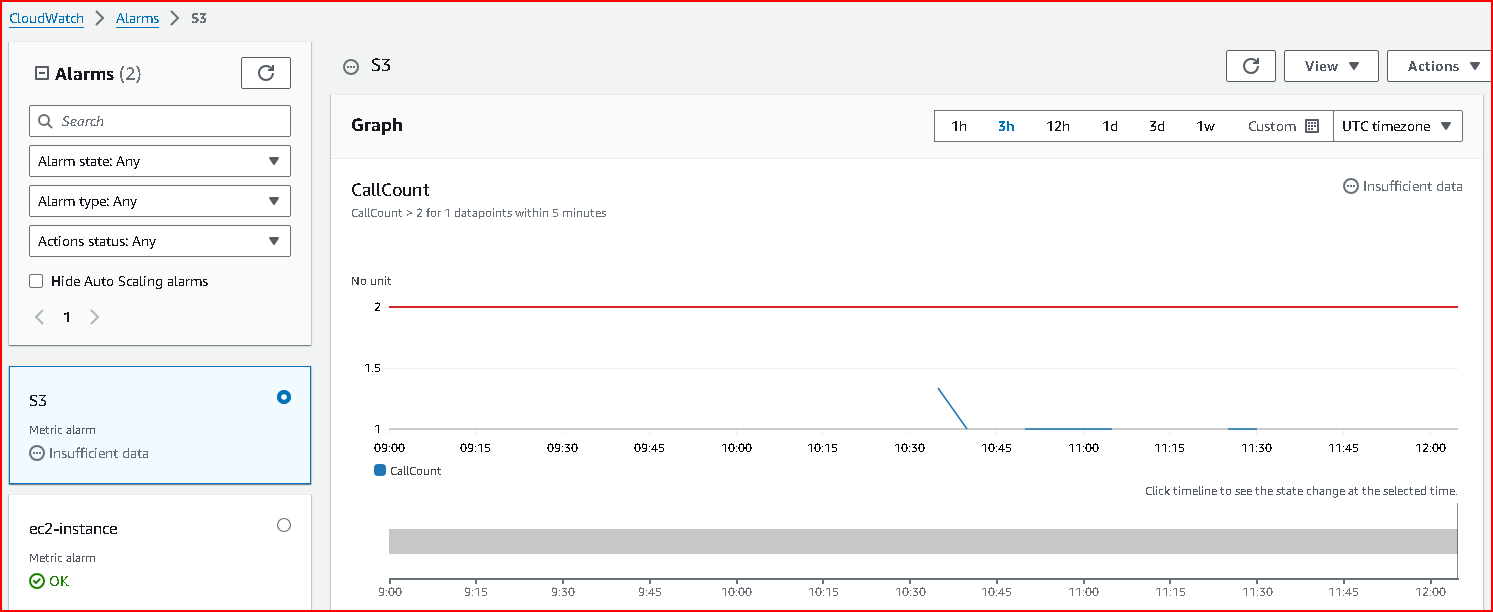
Select "EC2" from the list of services.

Choose the specific metric you want to monitor (e.g., CPU utilization).

Click on "Create Alarm" to set up alarms if needed, or simply monitor the metrics.



S3 Buckets:



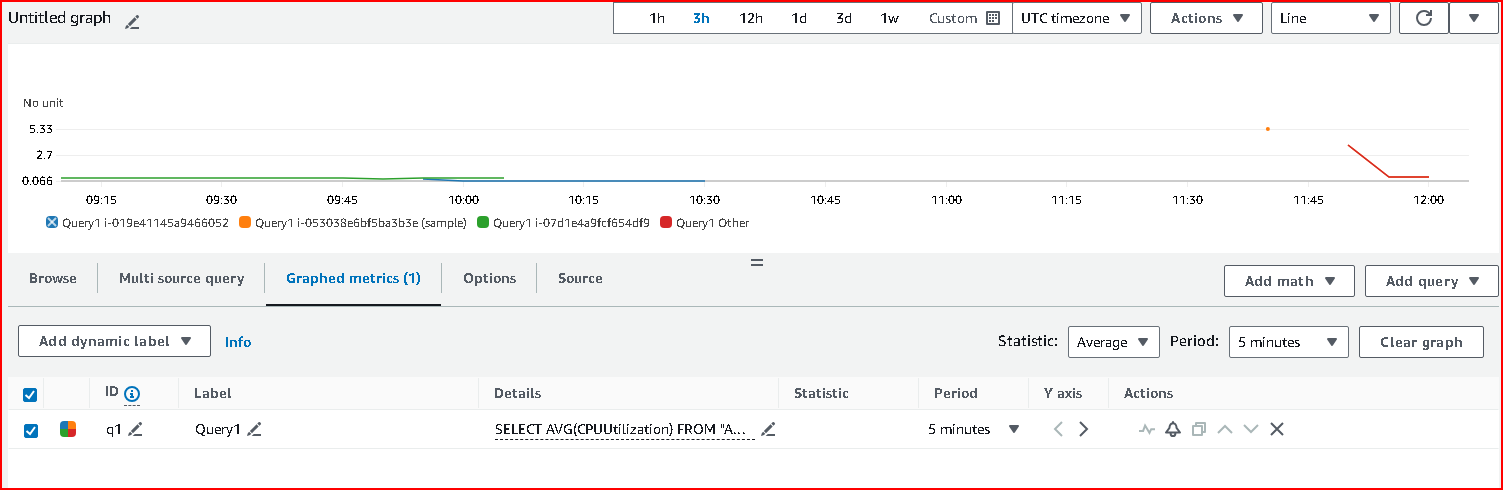
1. **Perform mathematical operations on EC2 and S3 metrics to derive new insights(Using Metric Math feature)**

Go to the CloudWatch console and navigate to the Metrics section.

Select a metric and click on "View/edit math expression" to open the Metric Math editor.

Write your mathematical expressions to perform operations on EC2 and S3 metrics.

Click on "Save" to apply the math expression and derive new metrics.



1. **Create a CloudWatch dashboard that visualizes EC2 and S3 metrics and trends**

Dashboard Creation:

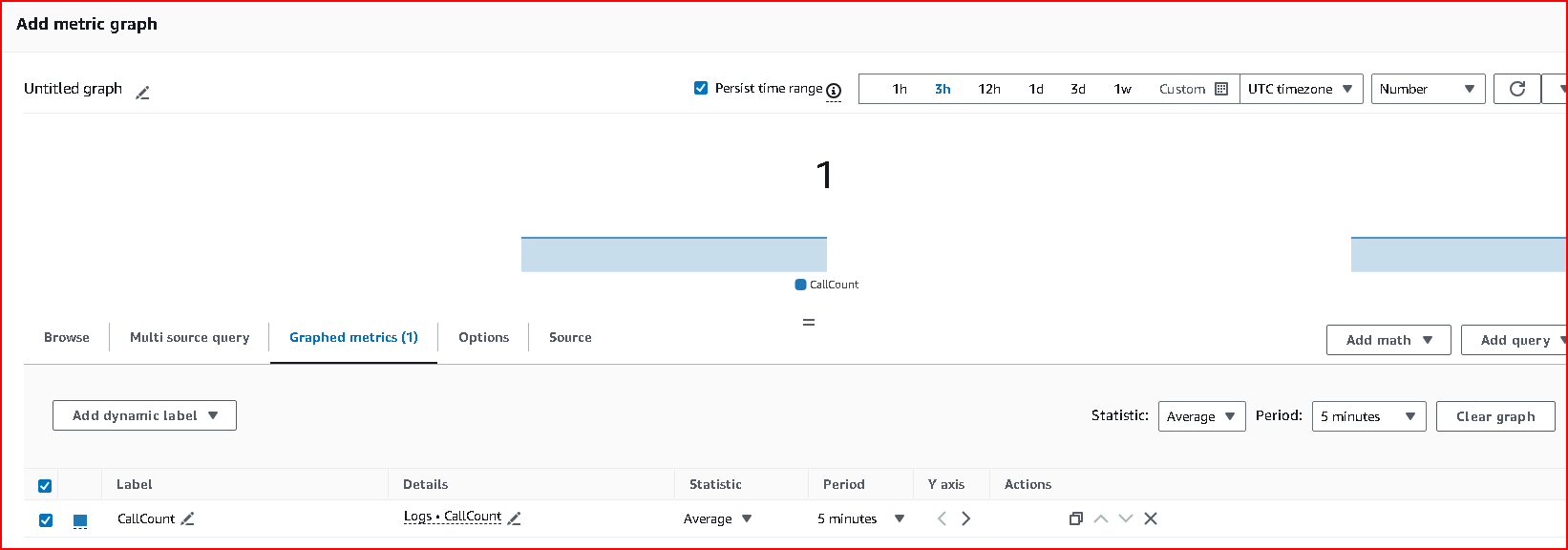
In the CloudWatch console, click on "Dashboards" in the left-hand navigation pane.

Click on "Create dashboard".

Add widgets to the dashboard by selecting metrics from EC2 and S3 that you want to visualize.

Customize widgets to display graphs, charts, and statistics as per your monitoring needs.

Save the dashboard and give it a meaningful name.





1. **Create alarms for metrics like CPU utilization on EC2 and bucket size for S3 and configure notifications**

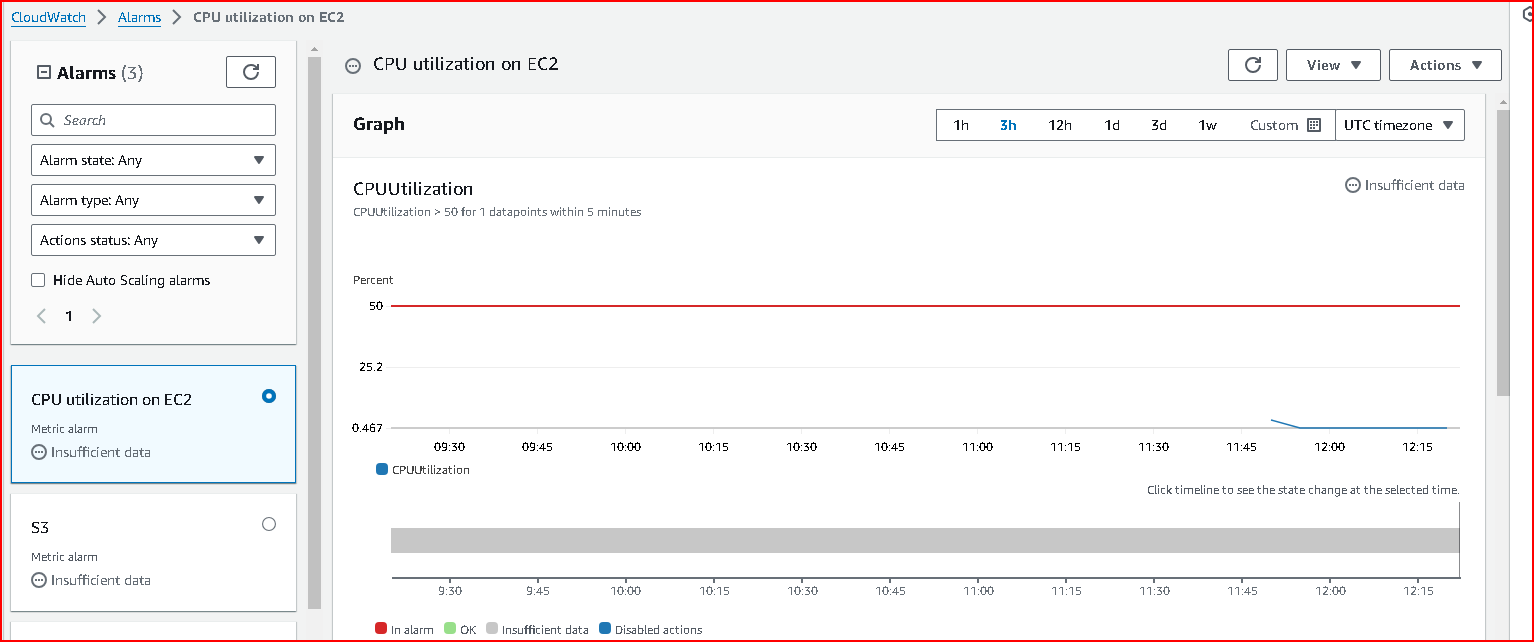
Alarm Configuration:

While viewing a metric in CloudWatch, click on "Create Alarm".

Define the conditions for the alarm (e.g., threshold for CPU utilization, bucket size).

Configure actions such as sending notifications via Amazon SNS.

Specify alarm actions like sending notifications to specific email addresses or triggering other AWS services.



1. **Set up CloudWatch Logs to collect and store log files from EC2 instances and S3 buckets ( using agent)**

Wget https://s3.amazonaws.com/amazoncloudwatchagent/linux/amd64/latest/AmazonCloudWatchAgent.zip

unzip AmazonCloudWatchAgent.zip

sudo ./install.sh

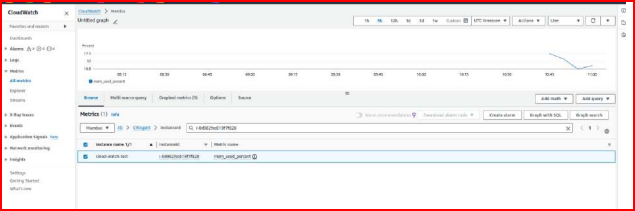
sudo /opt/aws/amazon-cloudwatch-agent/bin/amazon-cloudwatch-agent-ctl -a fetch-config -m

ec2 -c ssm:/alarm/AWS-CWAgentLinConfig –s

Check if EC2 Instance has CWAgent Installed or not:

sudo /opt/aws/amazon-cloud watch-agent/bin/amazon-cloud watch-agent-ctl -m ec2 -a status

go to cloud watch click on agent and search your ec2 instance ID and see the memory utilization log



1. **Perform queries on logs to analyze log data using CloudWatch Logs Insights (Using natural language query generation feature)**

Query Log Data:

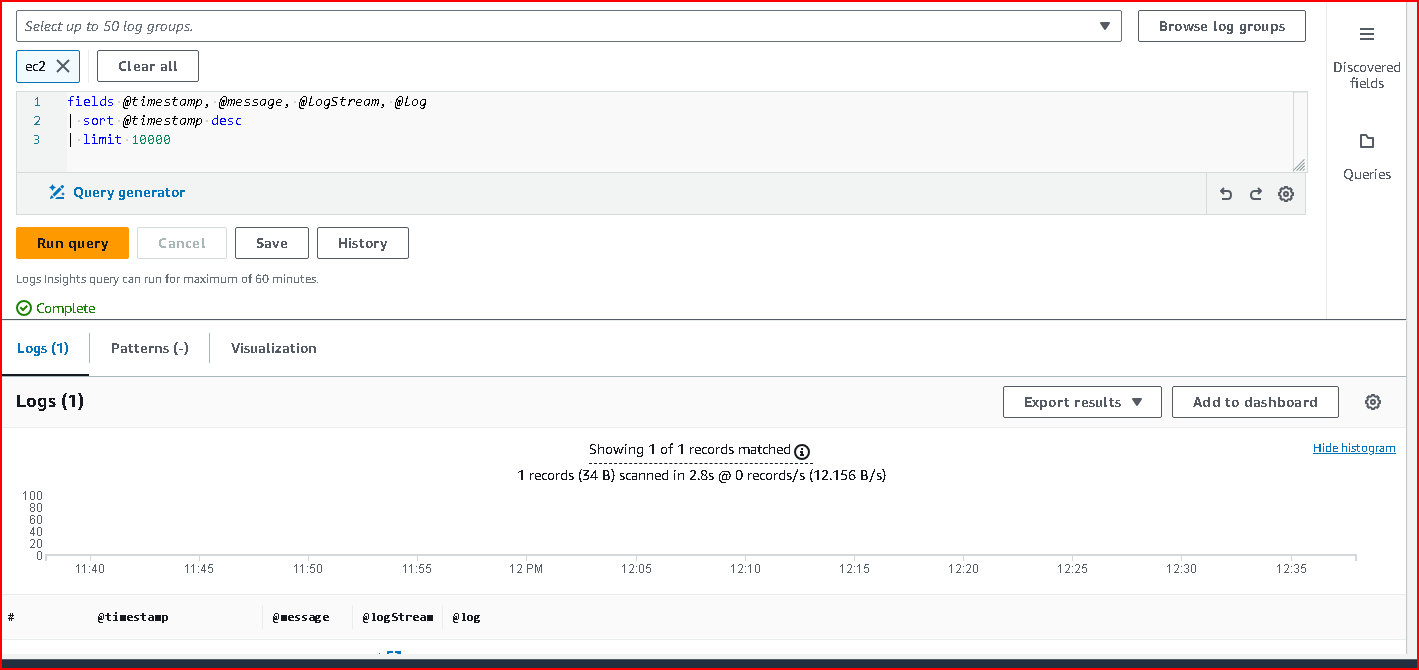
In the CloudWatch console, go to "Logs" in the left-hand navigation pane.

Select the log group containing your EC2 instance or S3 bucket logs.

Click on "Query logs" to open CloudWatch Logs Insights.

Use the query language or natural language query generation feature to analyze log data.

Run queries to extract insights and troubleshoot issues based on log entries.



1. **Set up CloudWatch Events to route EC2 state change events to SNS**

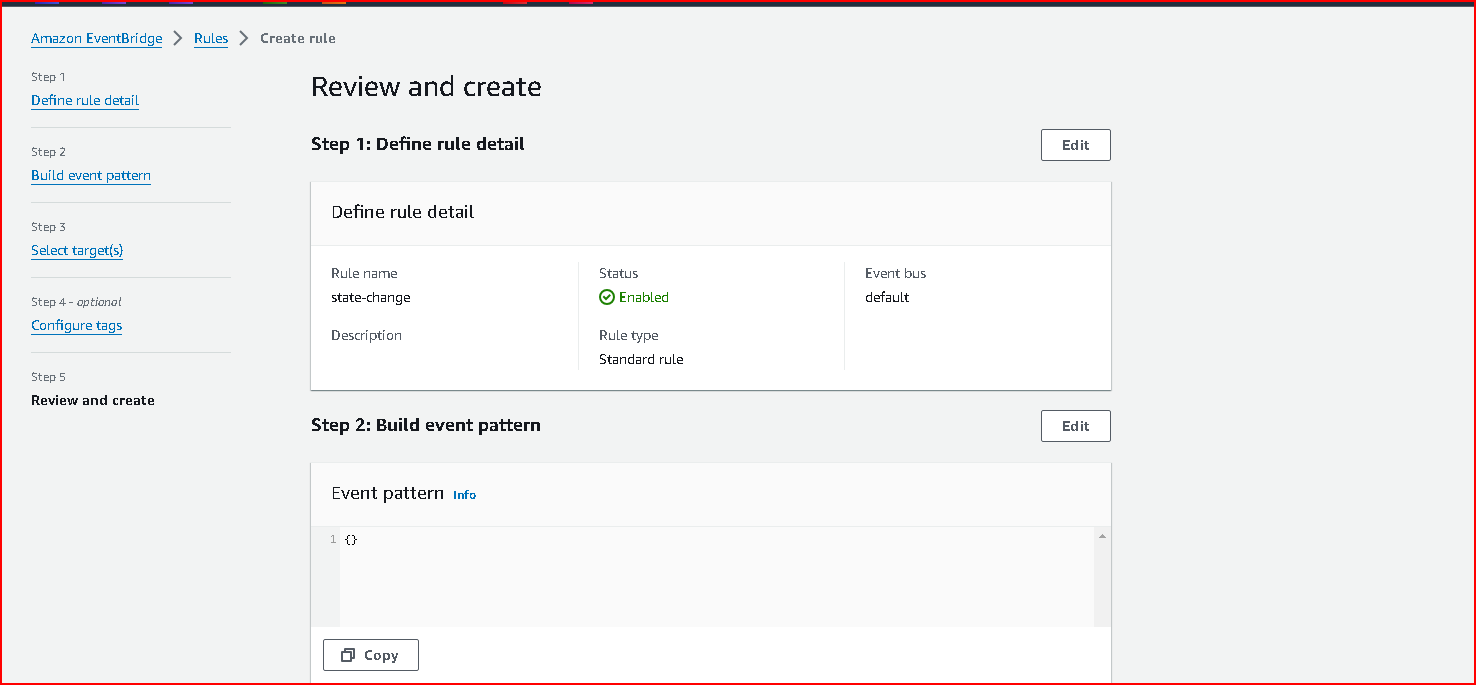
Create Event Rules:

Navigate to the CloudWatch console and click on "Events" in the left-hand navigation pane.

Click on "Create rule".

Define the event source (e.g., EC2 instance state changes).

Configure targets, such as Amazon SNS topics, to send notifications or Lambda functions to automate responses.



1. **Set up CloudTrail to collect API activity for EC2 and S3**

Enable CloudTrail:

Go to the CloudTrail console in the AWS Management Console.

Click on "Trails" in the left-hand navigation pane.

Click on "Create trail" to set up a new trail or select an existing one.

Choose the S3 bucket where CloudTrail logs will be stored.

Enable logging for API activity for EC2 and S3 services.

Configure additional settings like log file encryption and CloudWatch Logs integration if needed.

