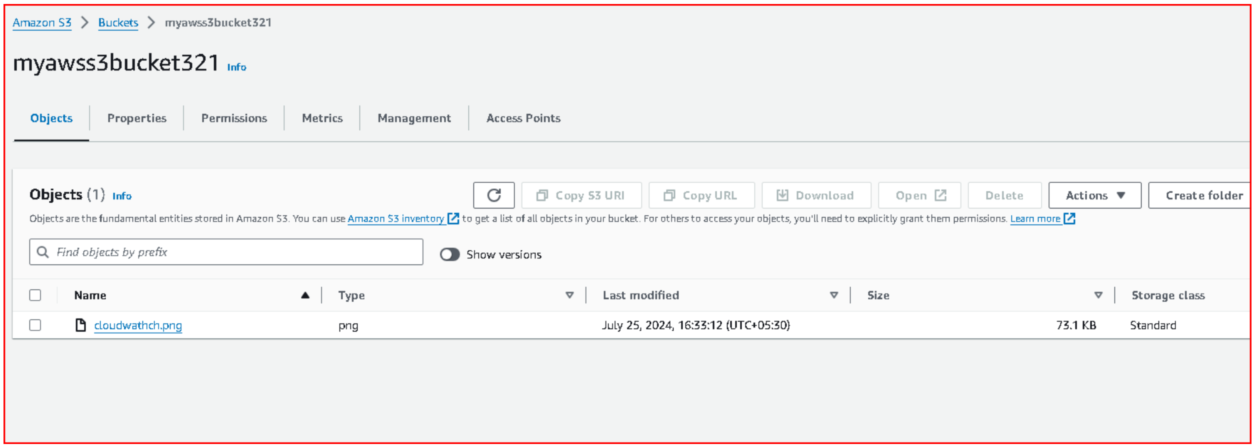
AWS S3, CloudWatch and CloudTrail - POC

Step 1: Create Two S3 Buckets

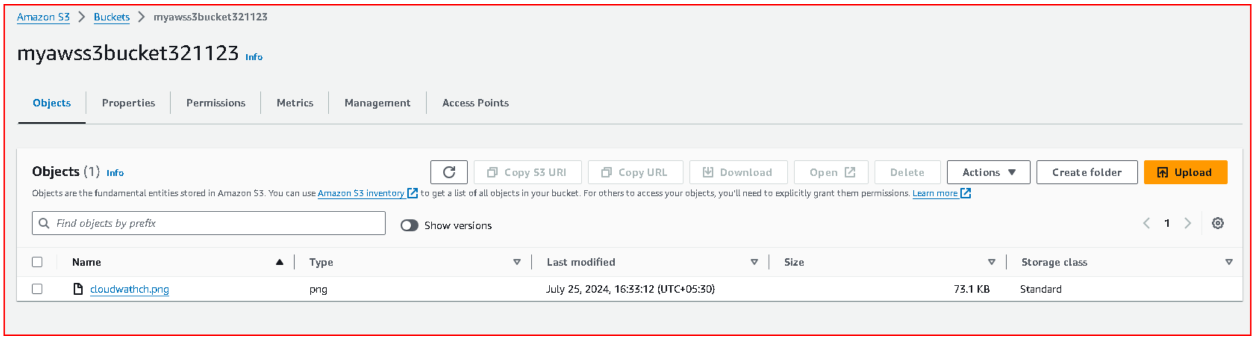
Primary Bucket: This is where your objects will initially be uploaded.



Objects are the fundamental entities stored in Amazon S3. You can use Amazon S3 inventory to get a list of all objects in your bucket. For others to access your objects, you'll need to explicitly grant them permissions. Learn more

□	Name	Type	Last modified	Size	Storage class
□	cloudwatchh.png	png	July 25, 2024, 16:33:12 (UTC+05:30)	73.1 KB	Standard

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



Objects are the fundamental entities stored in Amazon S3. You can use Amazon S3 inventory to get a list of all objects in your bucket. For others to access your objects, you'll need to explicitly grant them permissions. Learn more

□	Name	Type	Last modified	Size	Storage class
□	cloudwatchh.png	png	July 25, 2024, 16:33:12 (UTC+05:30)	73.1 KB	Standard

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.

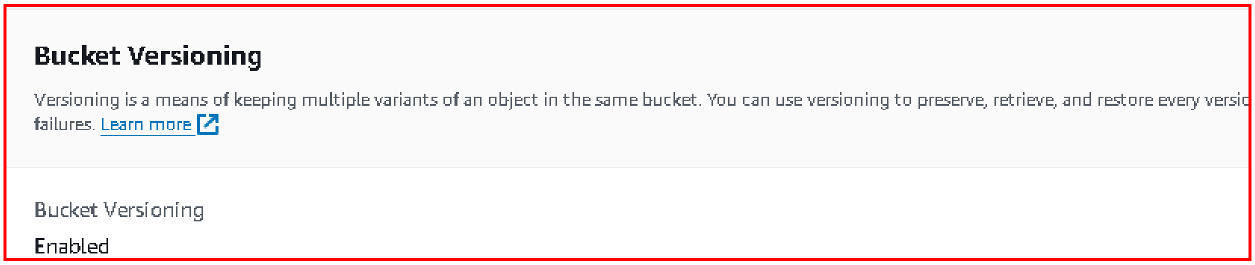
Navigate to the S3 service.

Select your primary bucket.

Go to the Properties tab.

Click on Versioning and enable versioning.

Repeat these steps for the replica bucket.



Bucket Versioning

Versioning is a means of keeping multiple variants of an object in the same bucket. You can use versioning to preserve, retrieve, and restore every versio failures. Learn more

Bucket Versioning

Enabled

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.

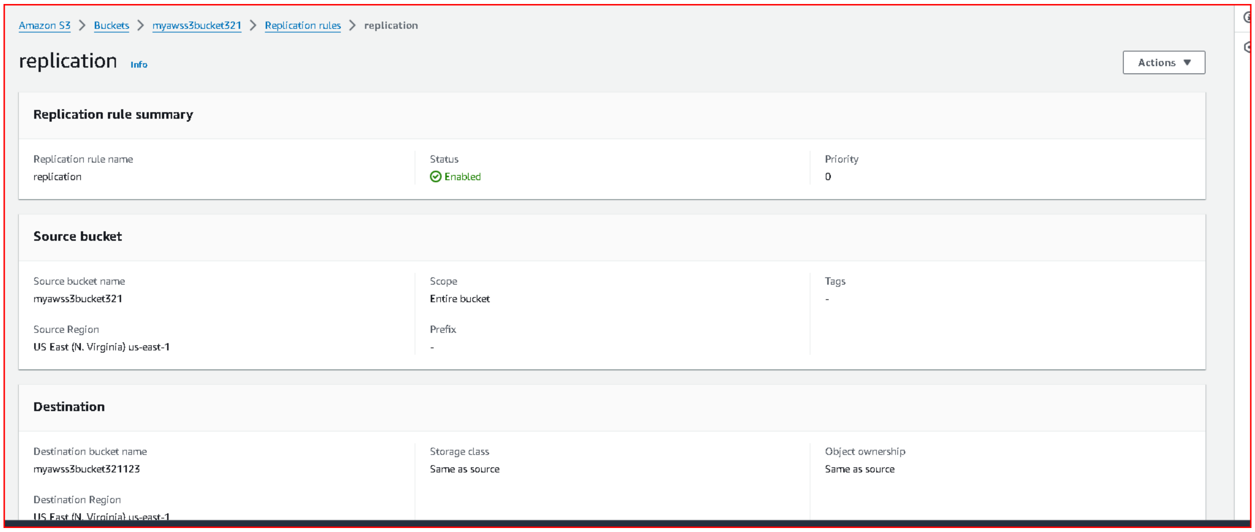
Click on Replication and then + Add rule.

Follow the prompts to configure replication:

Source: Choose the primary bucket.

Destination: Choose the replica bucket.

Choose the replication options as per your needs.



Amazon S3 > Buckets > myawss3bucket321 > Replication rules > replication

replication

Replication rule summary

Replication rule name
replication

Status
✓ Enabled

Priority
0

Source bucket

Source bucket name
myawss3bucket321

Source Region
US East (N. Virginia) us-east-1

Scope
Entire bucket

Prefix
-

Tags
-

Destination

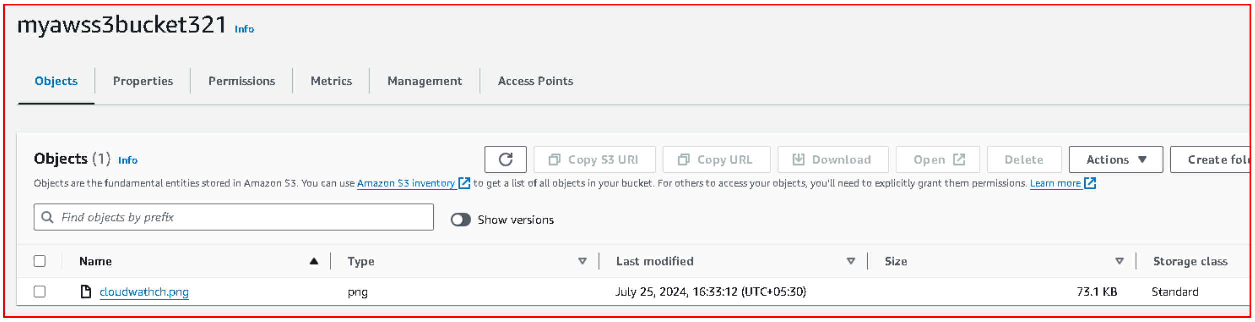
Destination bucket name
myawss3bucket321123

Destination Region
US East (N. Virginia) us-east-1

Storage class
Same as source

Object ownership
Same as source

Upload the object in source bucket.



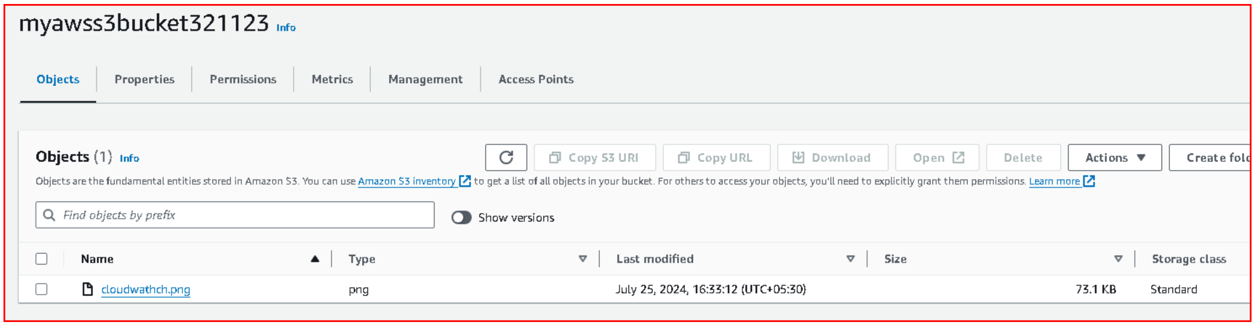
myawss3bucket321 Info

Objects (1) Info

Objects are the fundamental entities stored in Amazon S3. You can use Amazon S3 inventory to get a list of all objects in your bucket. For others to access your objects, you'll need to explicitly grant them permissions. Learn more

□	Name ▲	Type	Last modified	Size	Storage class
□	cloudwathch.png	png	July 25, 2024, 16:33:12 (UTC+05:30)	73.1 KB	Standard

Object is reflected in destination bucket



myawss3bucket321123 Info

Objects (1) Info

Objects are the fundamental entities stored in Amazon S3. You can use Amazon S3 inventory to get a list of all objects in your bucket. For others to access your objects, you'll need to explicitly grant them permissions. Learn more

□	Name ▲	Type	Last modified	Size	Storage class
□	cloudwathch.png	png	July 25, 2024, 16:33:12 (UTC+05:30)	73.1 KB	Standard

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.

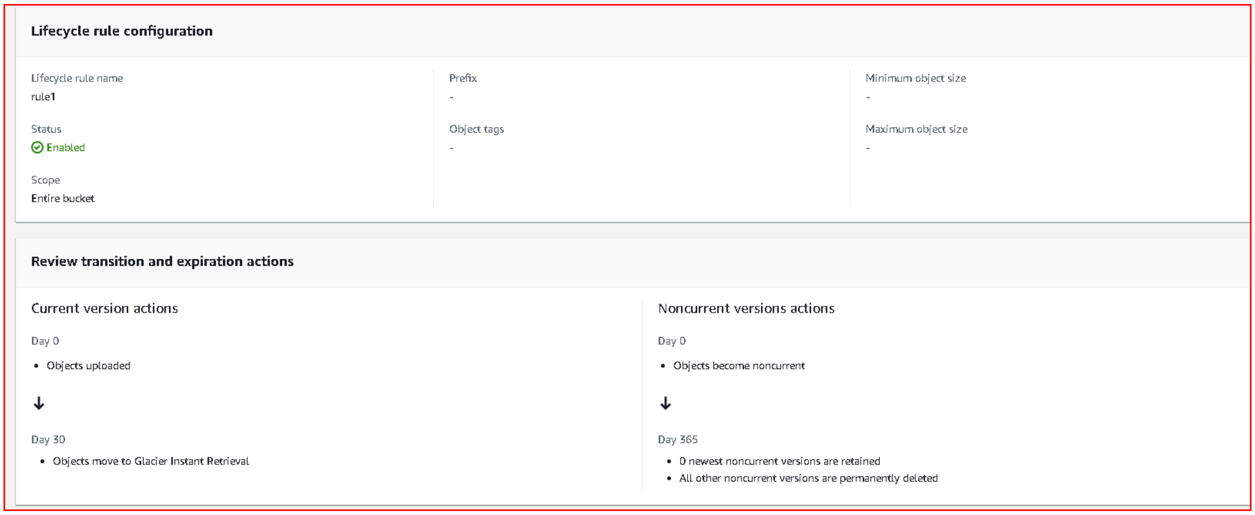
Configure the rule:

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



Lifecycle rule configuration

Lifecycle rule name
rule1

Status
✓ Enabled

Scope
Entire bucket

Prefix
-

Object tags
-

Minimum object size
-

Maximum object size
-

Review transition and expiration actions

Current version actions

Day 0

- Objects uploaded

↓

Day 30

- Objects move to Glacier Instant Retrieval

Noncurrent versions actions

Day 0

- Objects become noncurrent

↓

Day 365

- 0 newest noncurrent versions are retained
- All other noncurrent versions are permanently deleted

Step 5: Enable Server-Side Encryption

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

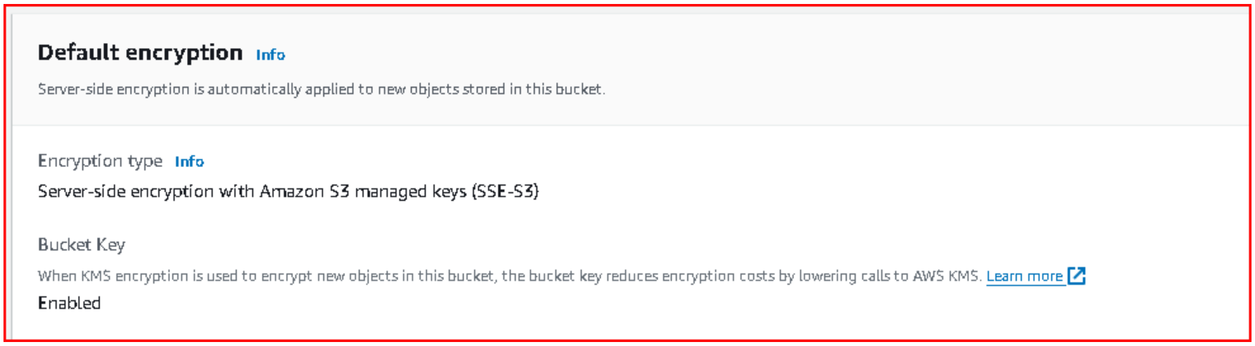
Enable Encryption:

Select your primary bucket.

Go to the Properties tab.

Click on Default encryption.

Choose the encryption option.



Default encryption Info

Server-side encryption is automatically applied to new objects stored in this bucket.

Encryption type Info
Server-side encryption with Amazon S3 managed keys (SSE-S3)

Bucket Key
When KMS encryption is used to encrypt new objects in this bucket, the bucket key reduces encryption costs by lowering calls to AWS KMS. Learn more
Enabled

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.

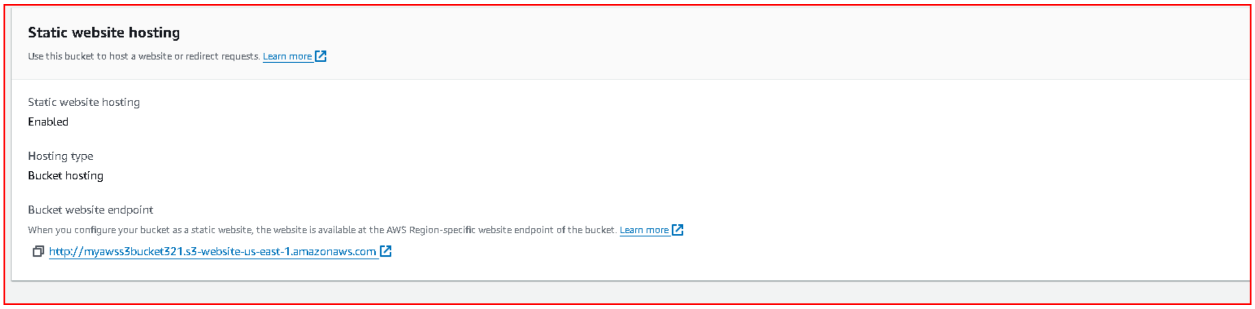
Go to the Properties tab.

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.



Static website hosting

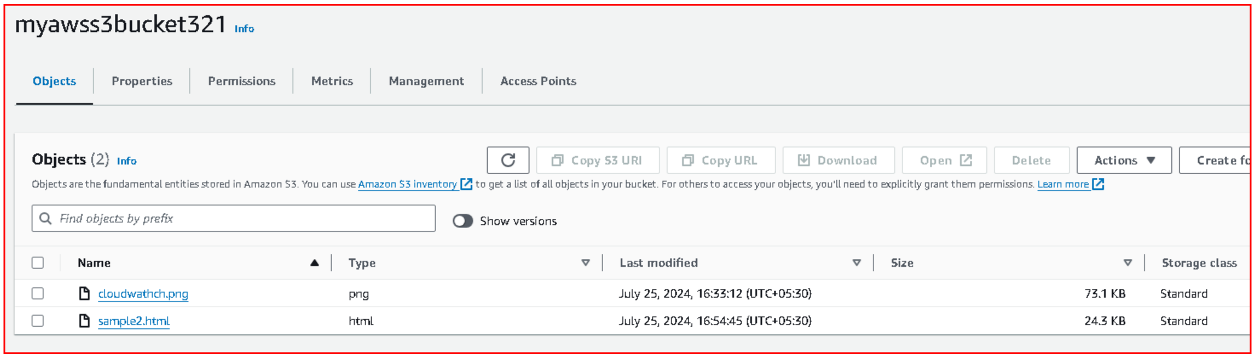
Use this bucket to host a website or redirect requests. Learn more

Static website hosting
Enabled

Hosting type
Bucket hosting

Bucket website endpoint
When you configure your bucket as a static website, the website is available at the AWS Region-specific website endpoint of the bucket. Learn more
http://myawss3bucket321.s3-website-us-east-1.amazonaws.com

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

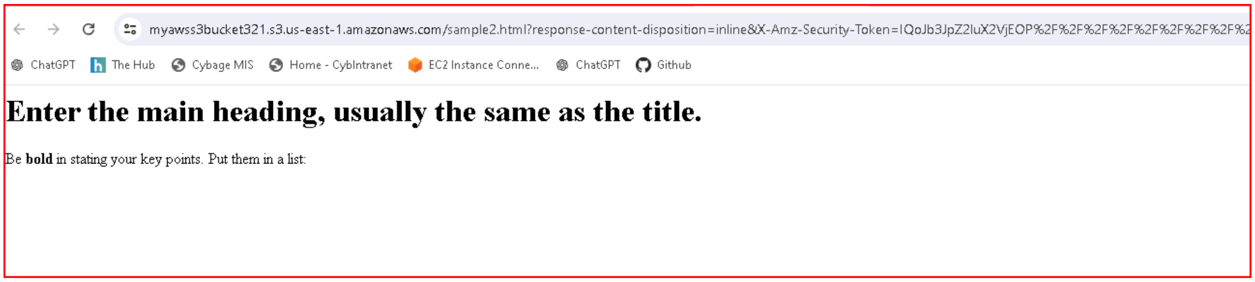


myawss3bucket321 Info

Objects (2) Info

Objects are the fundamental entities stored in Amazon S3. You can use Amazon S3 inventory to get a list of all objects in your bucket. For others to access your objects, you'll need to explicitly grant them permissions. Learn more

□	Name	Type	Last modified	Size	Storage class
□	cloudwathch.png	png	July 25, 2024, 16:33:12 (UTC+05:30)	73.1 KB	Standard
□	sample2.html	html	July 25, 2024, 16:54:45 (UTC+05:30)	24.3 KB	Standard



myawss3bucket321.s3.us-east-1.amazonaws.com/sample2.html?response-content-disposition=inline&X-Amz-Security-Token=IQoJb3JpZ2luX2VjEOP%2F%2F%2F%2F%2F%2F%2F%2F%2F%2

Enter the main heading, usually the same as the title.

Be **bold** in stating your key points. Put them in a list:

Task List for CloudWatch and CloudTrail :

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

EC2 Instances:

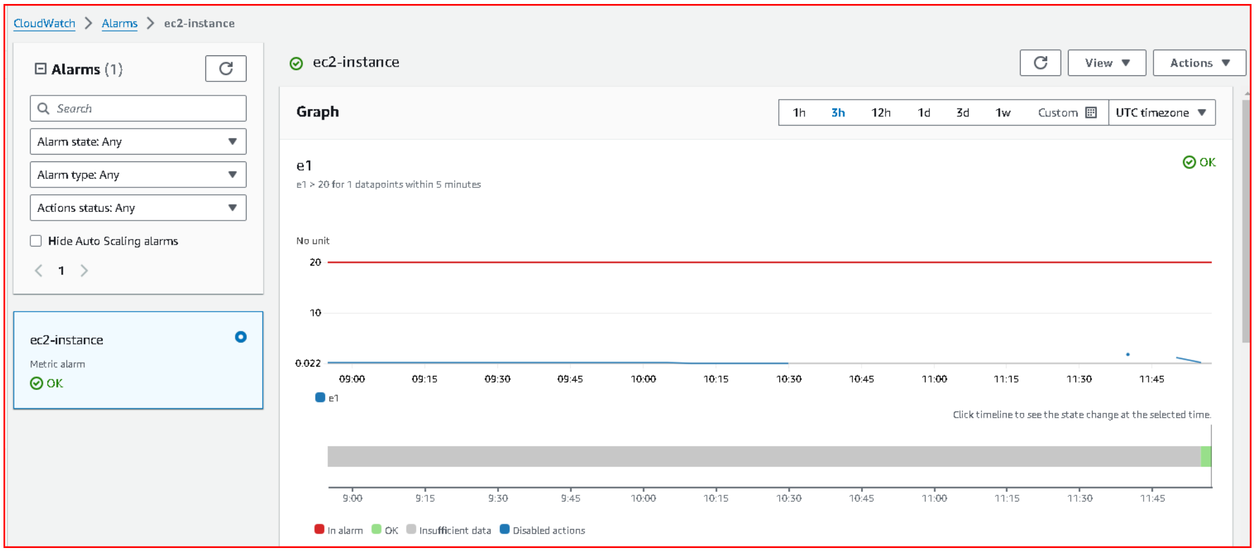
Navigate to the AWS Management Console and go to the CloudWatch service.

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.



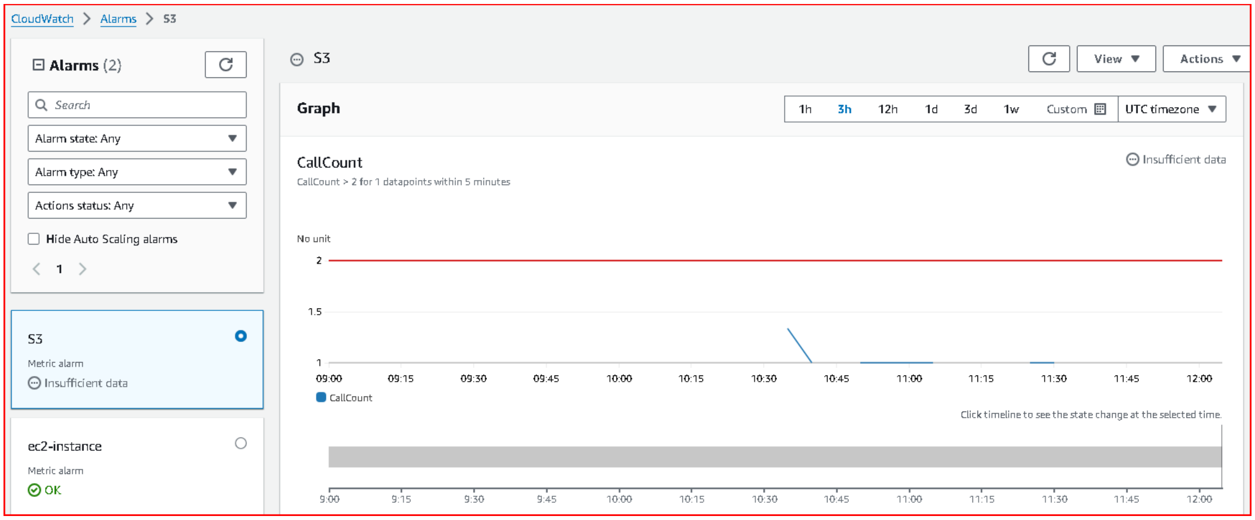
Alarm state: Any

Alarm type: Any

Actions status: Any

e1 > 20 for 1 datapoints within 5 minutes

S3 Buckets:



Alarm state: Any

Alarm type: Any

Actions status: Any

CallCount > 2 for 1 datapoints within 5 minutes

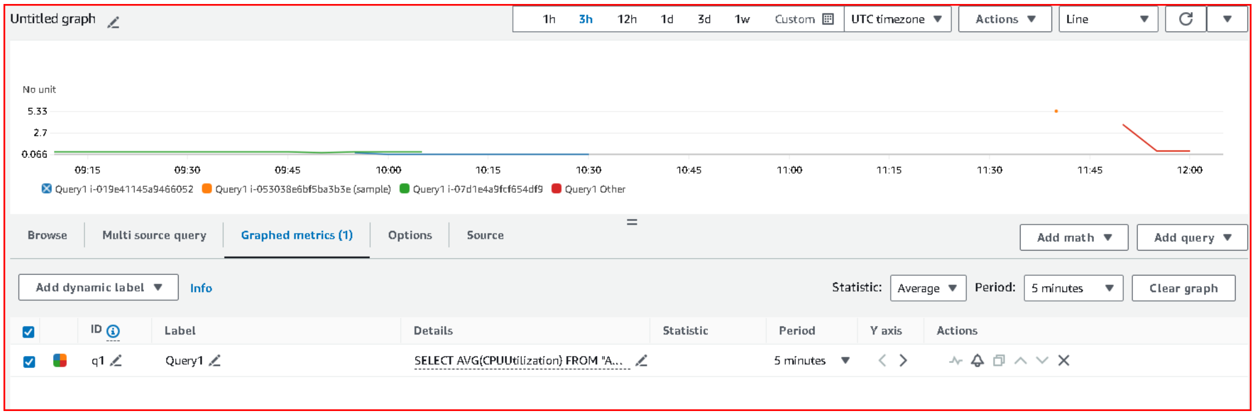
2. Perform mathematical operations on EC2 and S3 metrics to derive new insights(Using Metric Math feature)

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.



Statistic: Average ▼ Period: 5 minutes ▼

☑		ID	Label	Details	Statistic	Period	Y axis	Actions
☑		q1	Query1	SELECT AVG(CPUUtilization) FROM "A...		5 minutes ▼	< >	

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

Dashboard Creation:

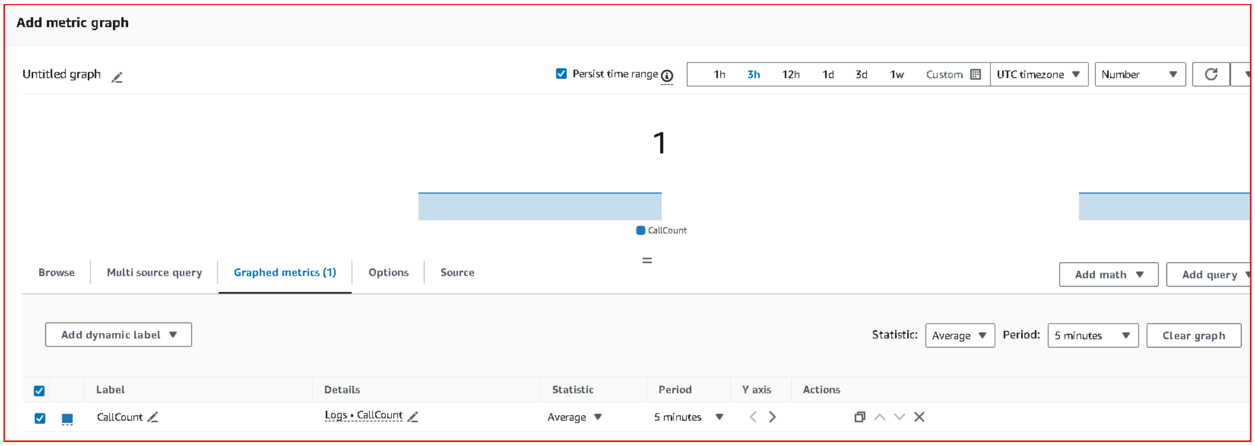
In the CloudWatch console, click on "Dashboards" in the left-hand navigation pane.

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.

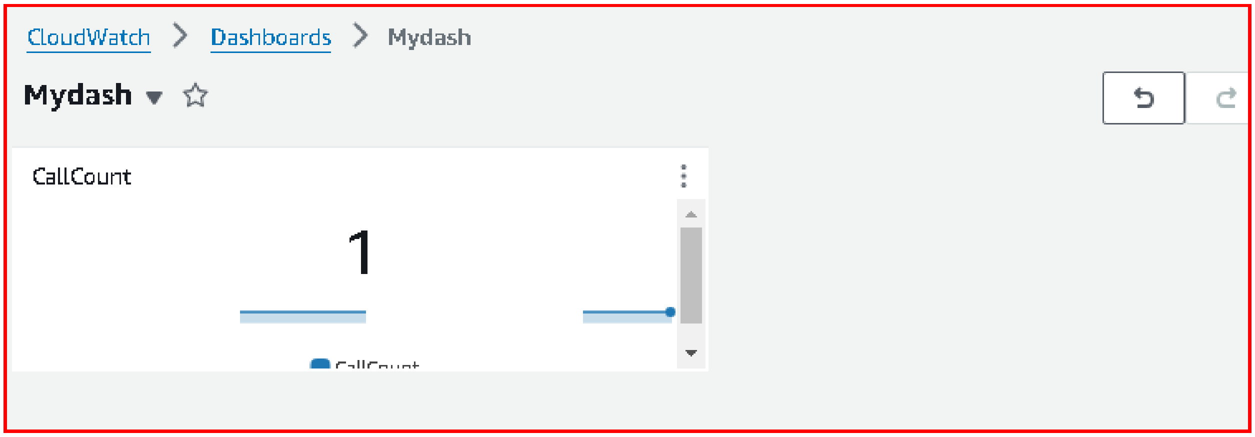
Save the dashboard and give it a meaningful name.



☑ Persist time range

Statistic: Average ▼ Period: 5 minutes ▼

☑		Label	Details	Statistic	Period	Y axis	Actions
☑		CallCount	Logs • CallCount	Average ▼	5 minutes ▼	< >	



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

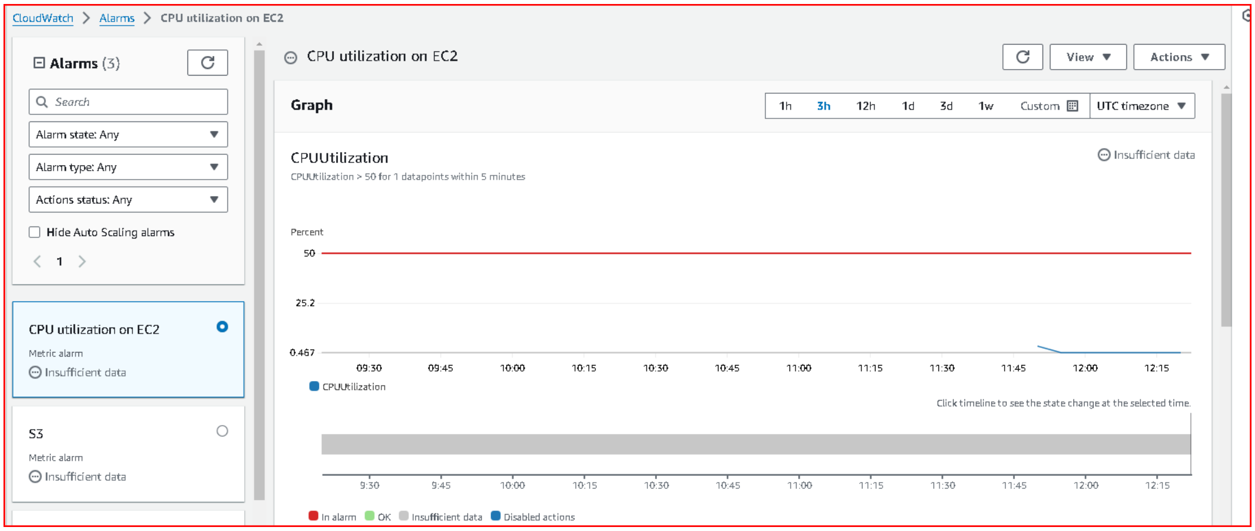
Alarm Configuration:

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.



5. **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
```

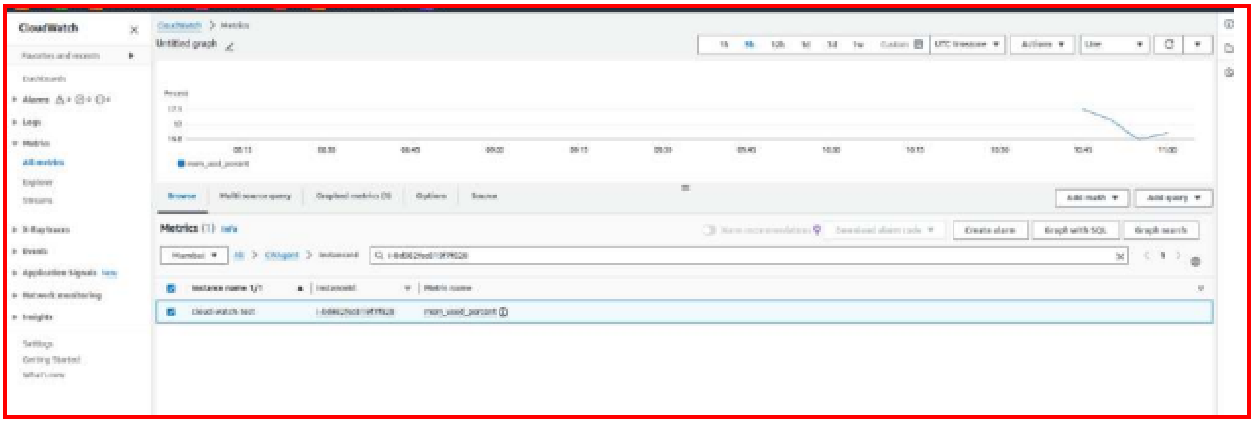
```
sudo /opt/aws/amazon-cloudwatch-agent/bin/amazon-cloudwatch-agent-ctl -a fetch-config -m

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



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

Query Log Data:

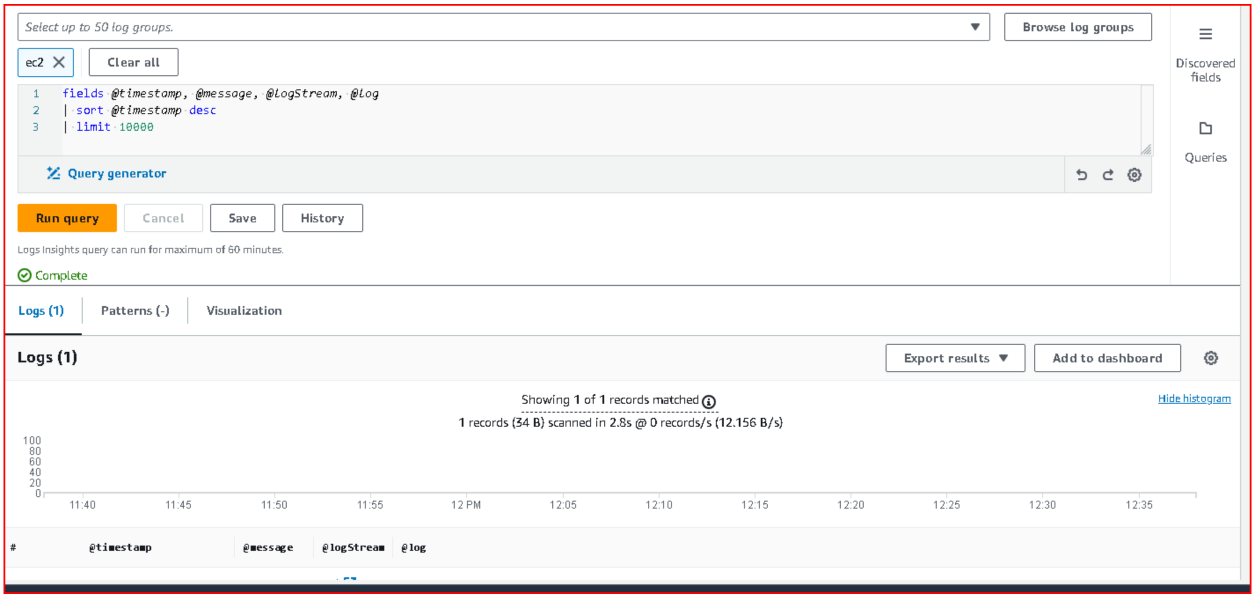
In the CloudWatch console, go to "Logs" in the left-hand navigation pane.

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.



```
fields @timestamp, @message, @logStream, @log
| sort @timestamp desc
| limit 10000
```

Logs Insights query can run for maximum of 60 minutes.

Complete

Logs (1)

Showing 1 of 1 records matched

1 records (34 B) scanned in 2.8s @ 0 records/s (12.156 B/s)

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

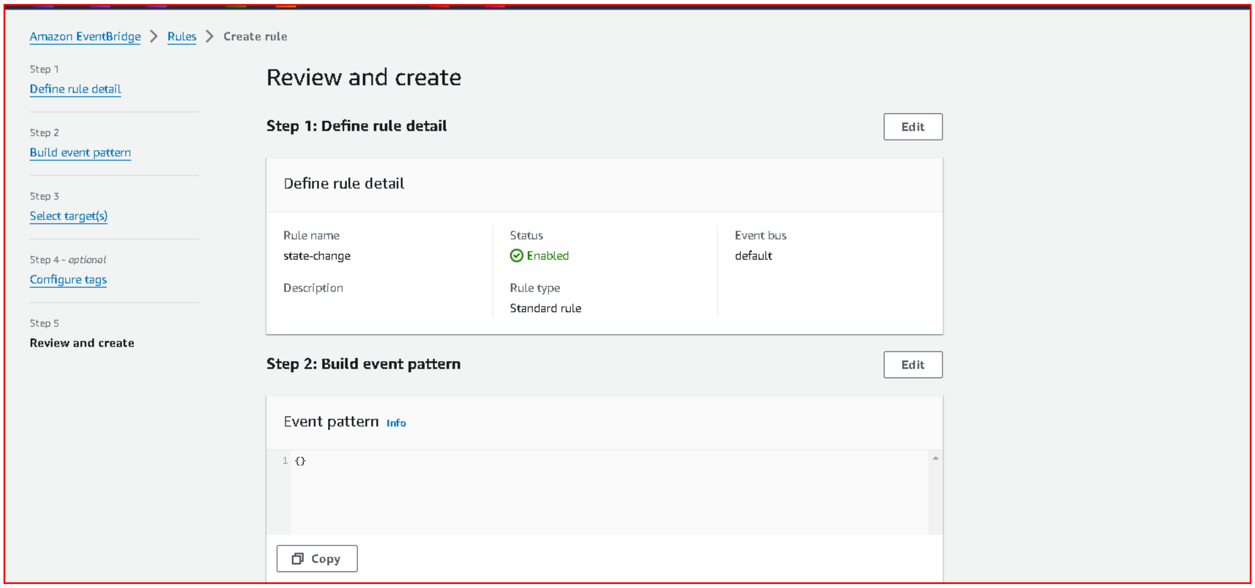
Create Event Rules:

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.



Review and create

Step 1: Define rule detail

Define rule detail

Rule name
state-change

Status
Enabled

Event bus
default

Description

Rule type
Standard rule

Step 2: Build event pattern

Event pattern

```
{}
```

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

Enable CloudTrail:

Go to the CloudTrail console in the AWS Management Console.

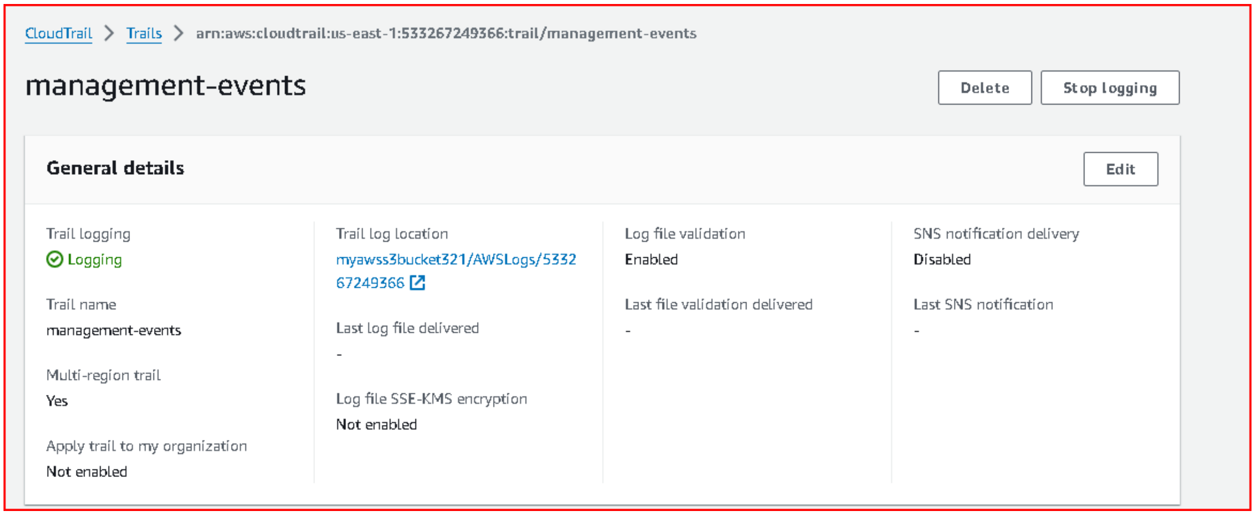
Click on "Trails" in the left-hand navigation pane.

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.



CloudTrail > Trails > arn:aws:cloudtrail:us-east-1:533267249366:trail/management-events

management-events

General details

Trail logging: Logging

Trail name: management-events

Multi-region trail: Yes

Apply trail to my organization: Not enabled

Trail log location: myawss3bucket321/AWSLogs/533267249366

Last log file delivered: -

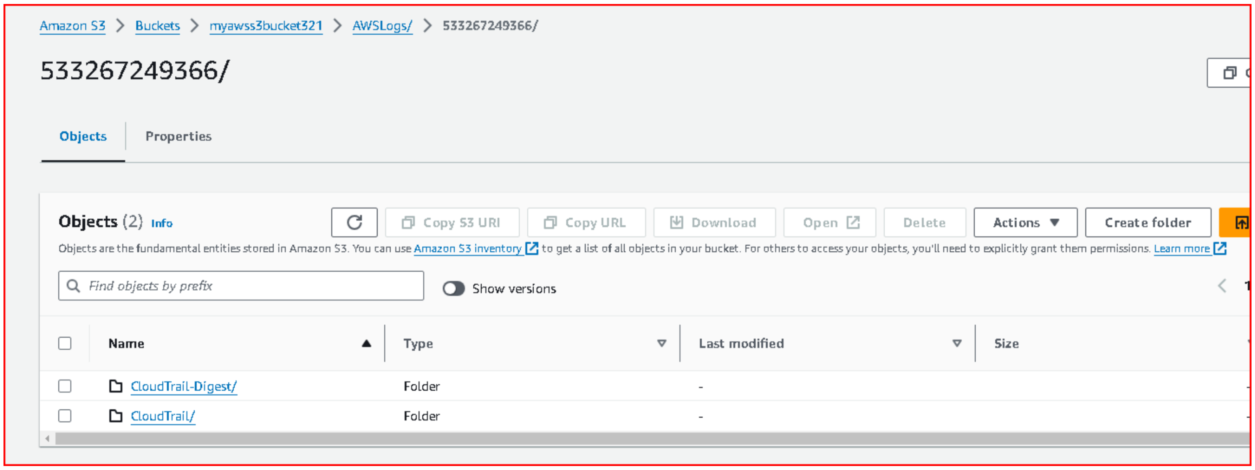
Log file SSE-KMS encryption: Not enabled

Log file validation: Enabled

Last file validation delivered: -

SNS notification delivery: Disabled

Last SNS notification: -



Amazon S3 > Buckets > myawss3bucket321 > AWSLogs/ > 533267249366/

533267249366/

Objects (2) Info

Objects are the fundamental entities stored in Amazon S3. You can use Amazon S3 inventory to get a list of all objects in your bucket. For others to access your objects, you'll need to explicitly grant them permissions. Learn more

Name	Type	Last modified	Size
CloudTrail-Digest/	Folder	-	
CloudTrail/	Folder	-	