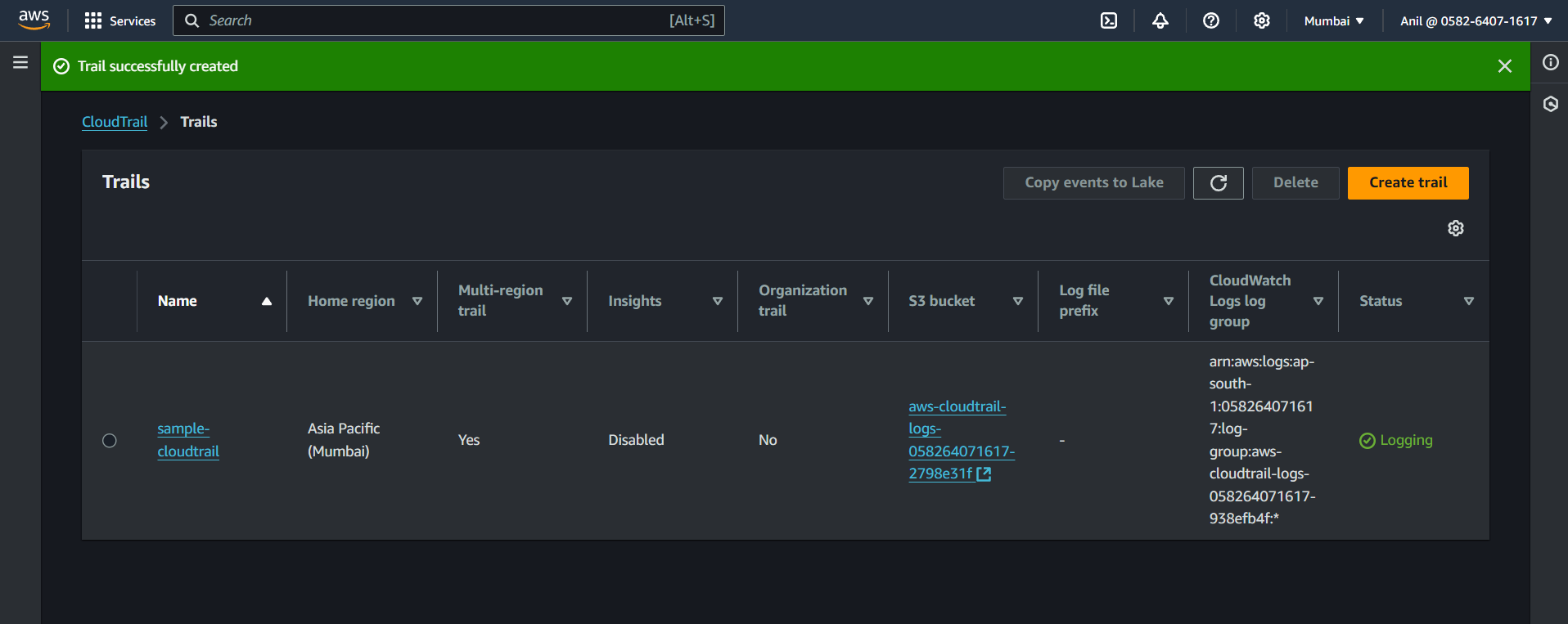
**1) Enable cloudtrail monitoring and store the events in s3 and cloudwatch log events.**

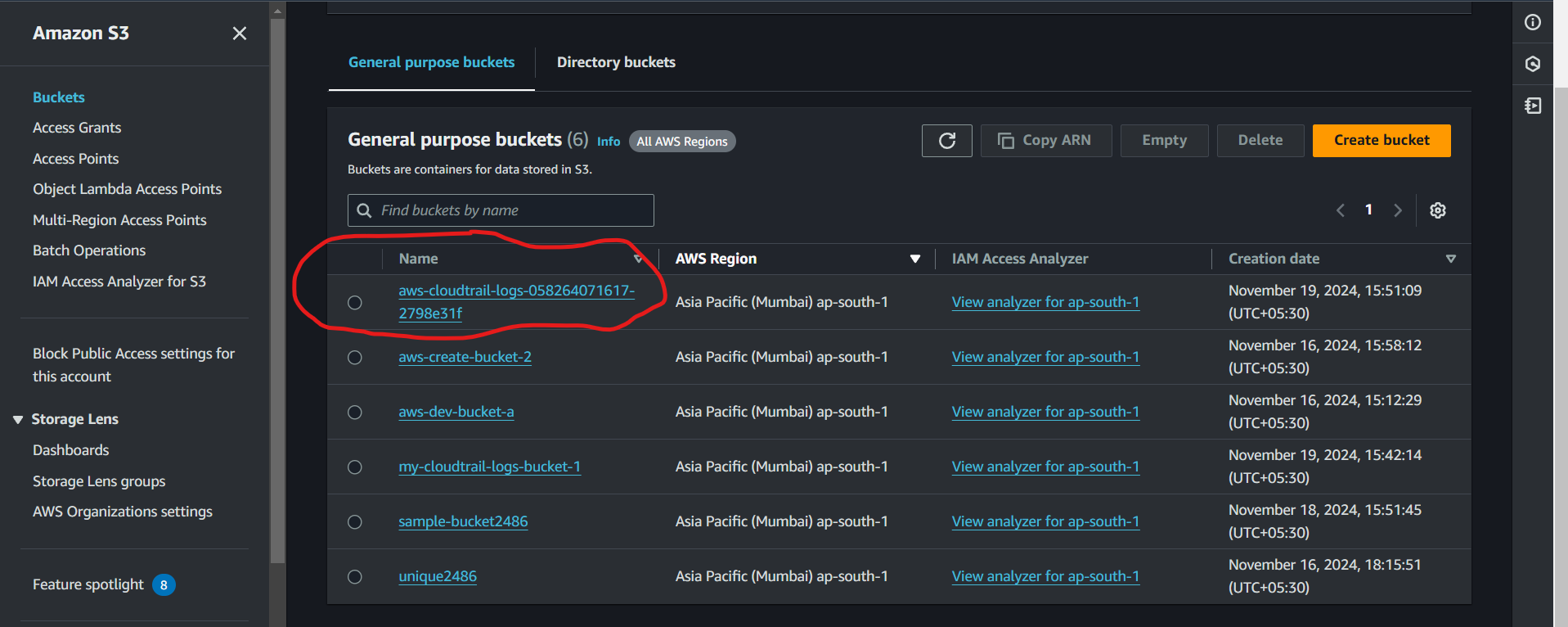
**1. Create an S3 Bucket for CloudTrail Logs**

1. **Log in to AWS Management Console.**
2. Navigate to **S3**.
3. Create a new bucket:
   * Choose a unique name (e.g., my-cloudtrail-logs-bucket).
   * Enable **versioning** for the bucket (optional but recommended for log integrity).
4. Update bucket permissions:
   * Add permissions for CloudTrail to write logs to the bucket. Ensure the bucket policy includes the necessary permissions.



**2. Enable CloudTrail**

1. Go to the **CloudTrail** service in the AWS Management Console.
2. Click **Create trail** or **Add trail**.
3. Configure the trail:
   * **Trail Name**: Provide a name for the trail.
   * **Storage location**:
     + Choose the S3 bucket created earlier.
     + Optionally configure a folder (prefix) for logs.
   * Enable **Log file validation** (recommended).
4. Under **CloudWatch Logs**, do the following:
   * Enable the **Send to CloudWatch Logs** option.
   * Create or select a CloudWatch Logs group (e.g., /aws/cloudtrail).
   * Create or select an IAM role with permissions to publish logs to CloudWatch Logs.



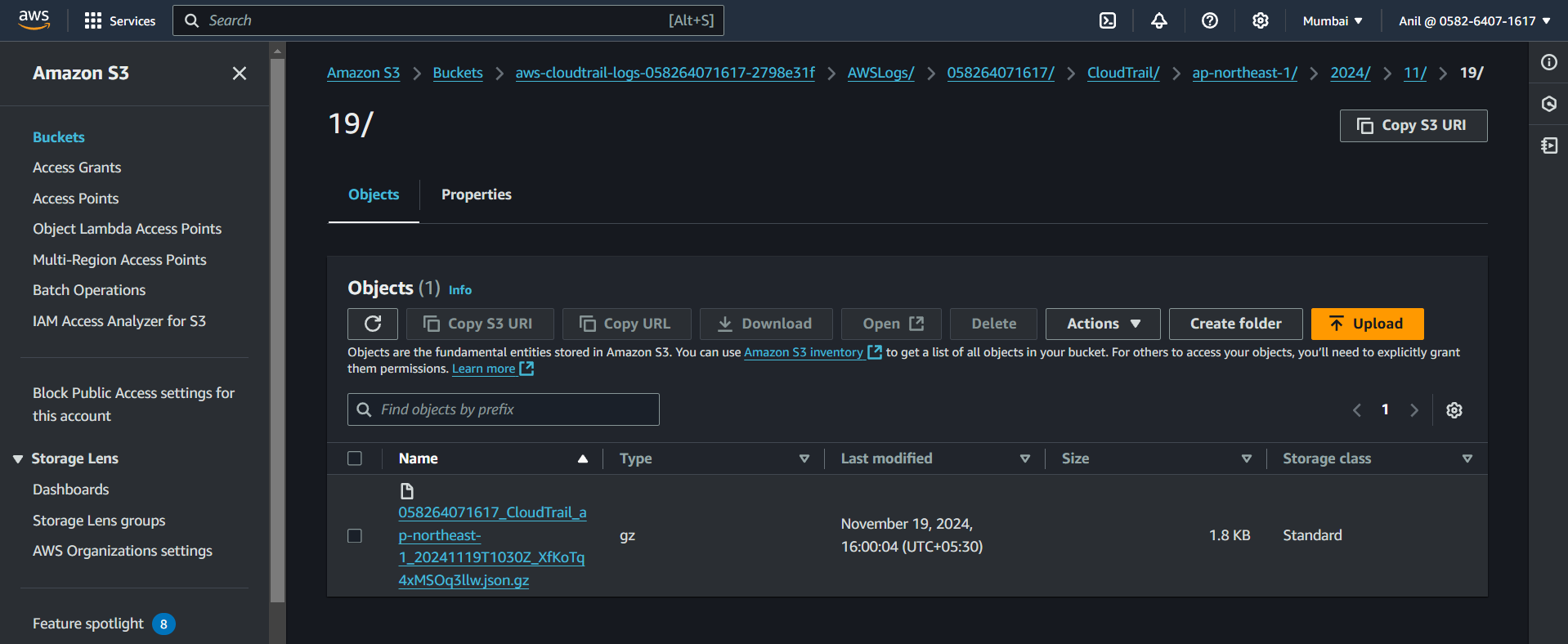
**3. Configure IAM Role for CloudTrail**

Ensure CloudTrail has sufficient permissions to write logs to both S3 and CloudWatch:

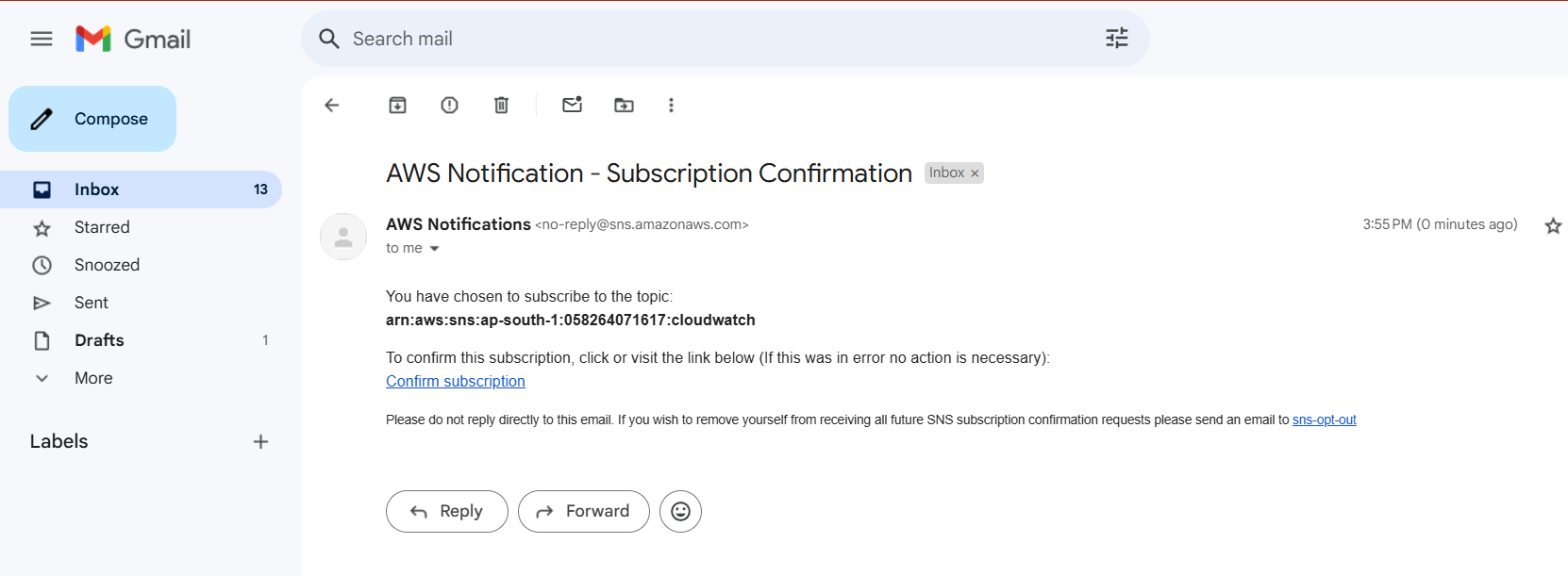
* Attach the **AWSCloudTrailFullAccess** policy to the IAM role used by CloudTrail.
* Customize the role policies as needed for additional security.

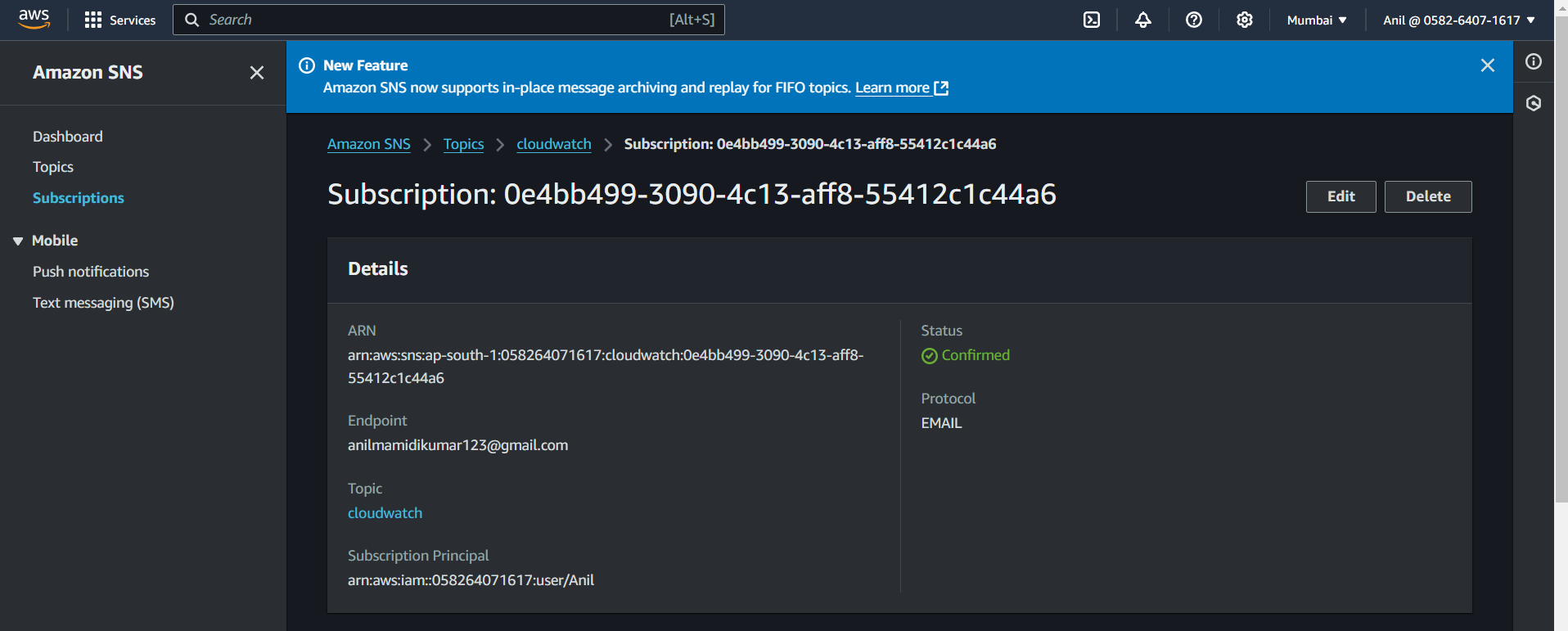
**4. Test the Setup**

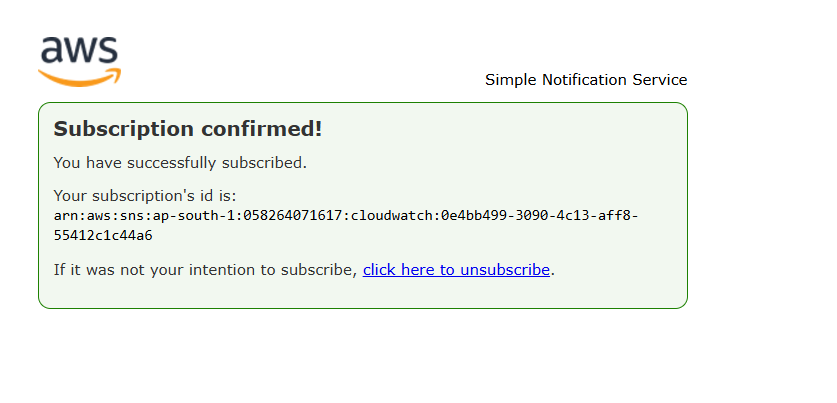
1. Perform some activities in the AWS Management Console, CLI, or API (e.g., creating or deleting a resource).
2. Check:
   * **S3 Bucket**: Navigate to the bucket and verify that CloudTrail logs are being written.
   * **CloudWatch Logs**: Go to CloudWatch → Logs, and verify that CloudTrail events are being recorded in the log group.

****

**2) Enable SNS for cloudtrial to send alert on email.**

****

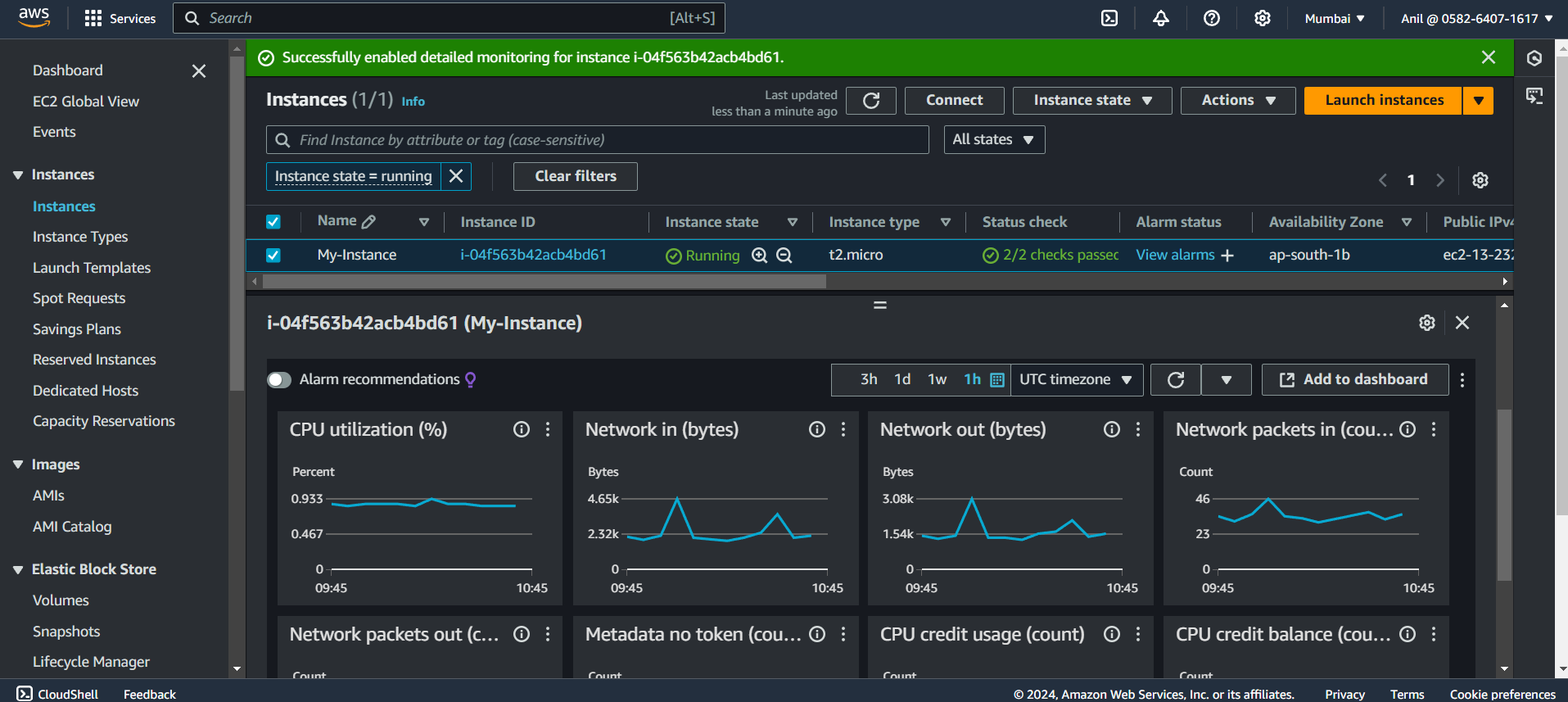
****

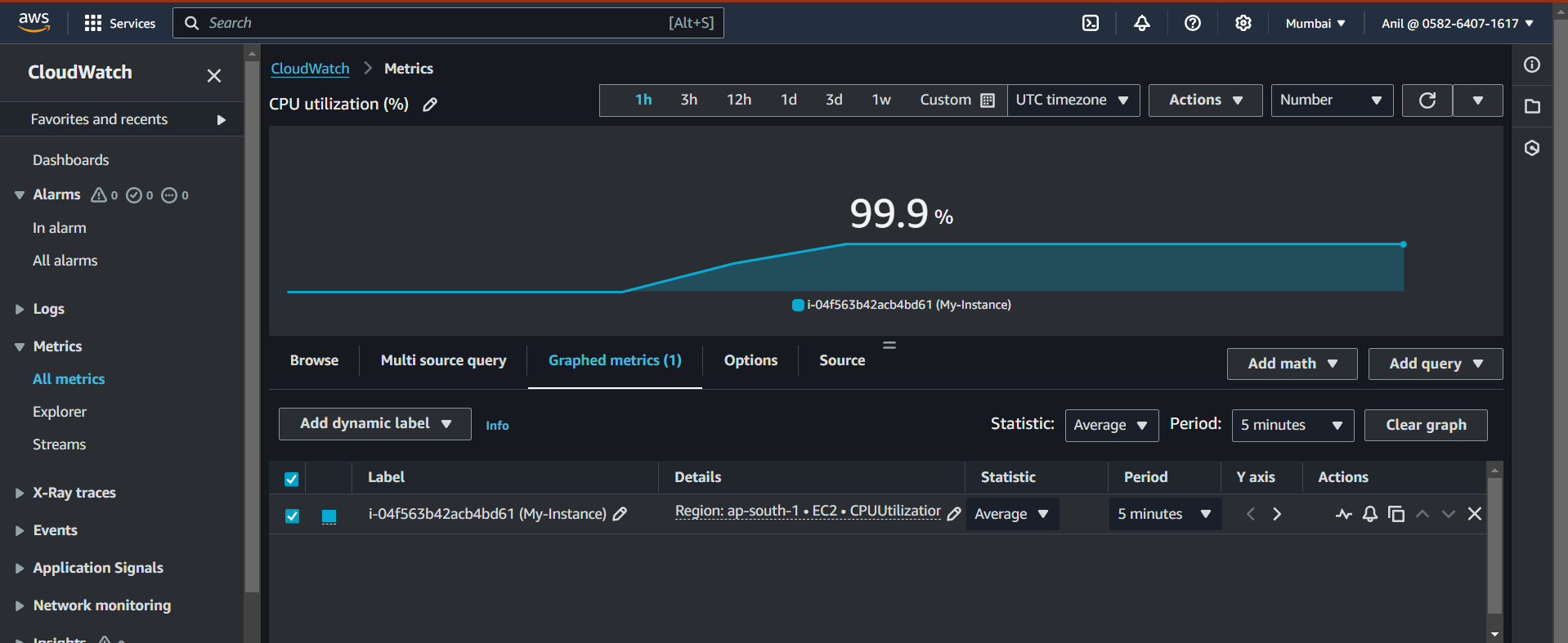
****

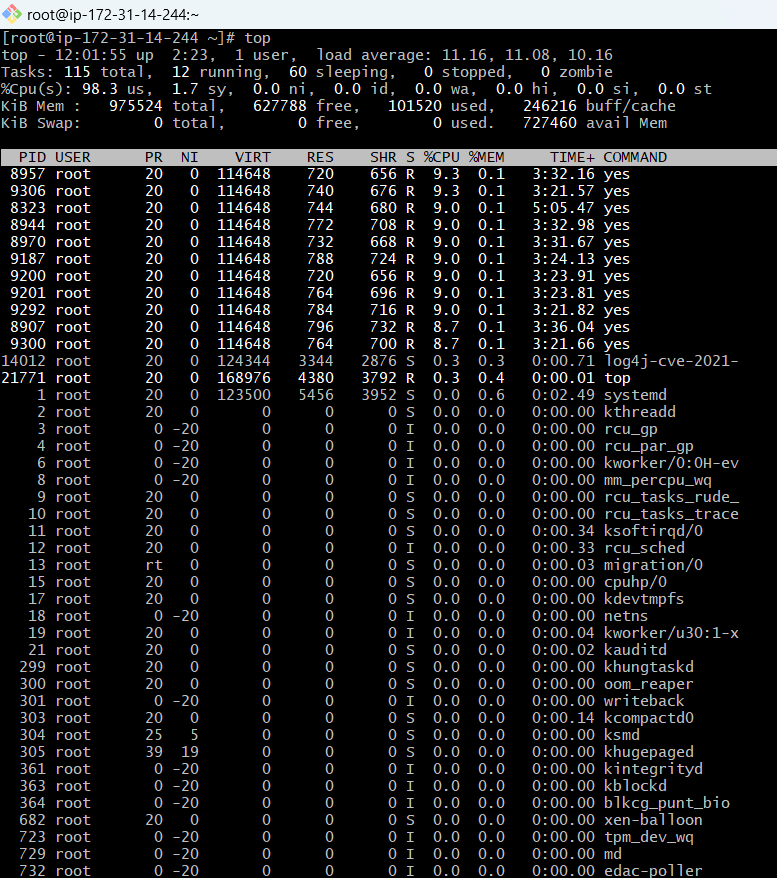
**3) Configure cloud watch monitoring and record the cpu utilization and other metrics of ec2.**

**Enable Detailed Monitoring for EC2**

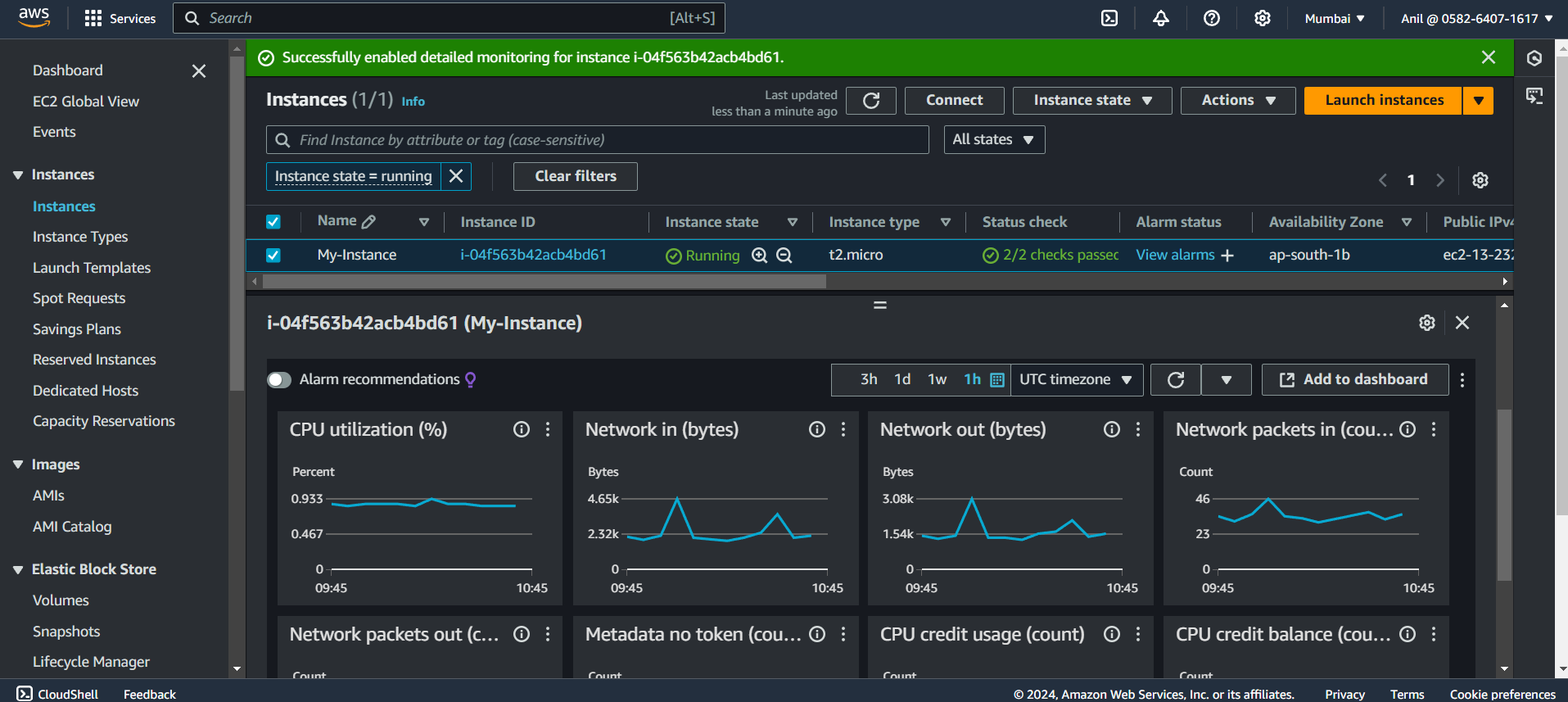
1. Log in to the AWS Management Console.
2. Navigate to **EC2 Dashboard** > **Instances**.
3. Select the EC2 instance you want to monitor.
4. Click on the **Actions** menu > **Manage monitoring**.
5. Enable **Detailed Monitoring** (additional charges apply for detailed metrics).
   * With detailed monitoring, metrics are collected every minute (default is every 5 minutes).

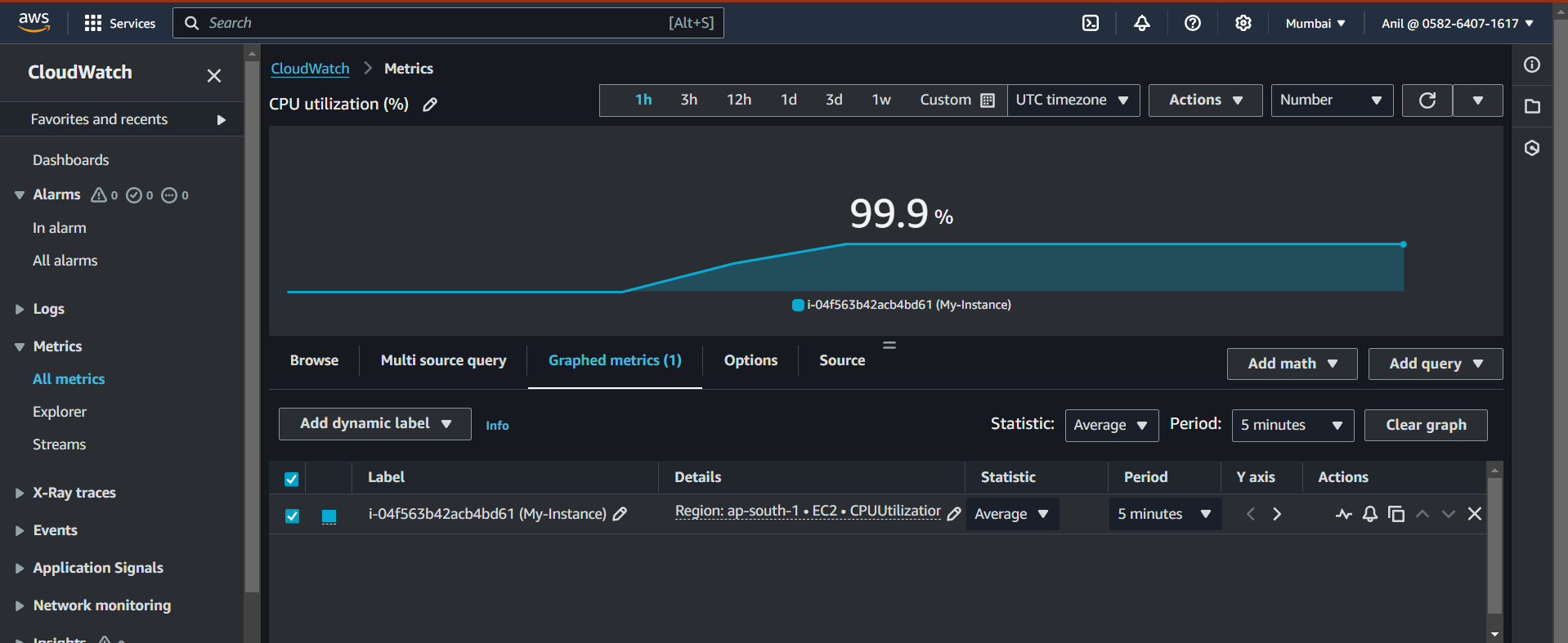


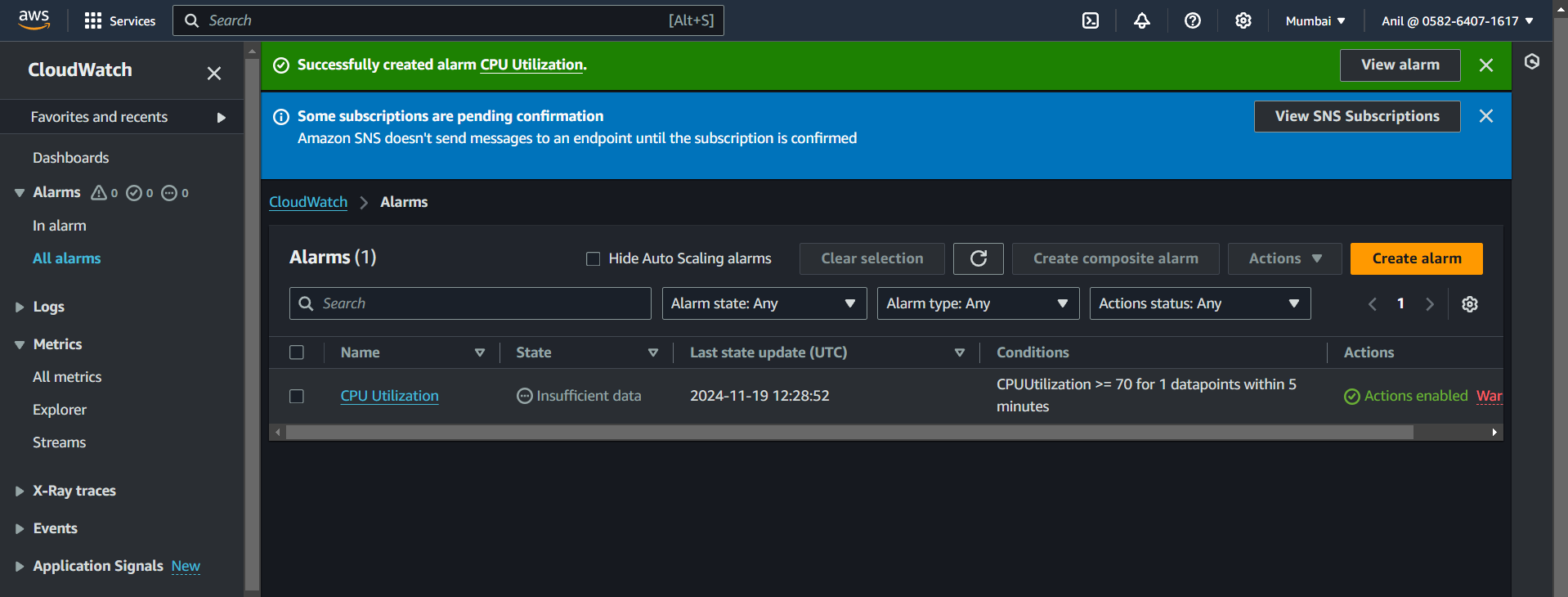




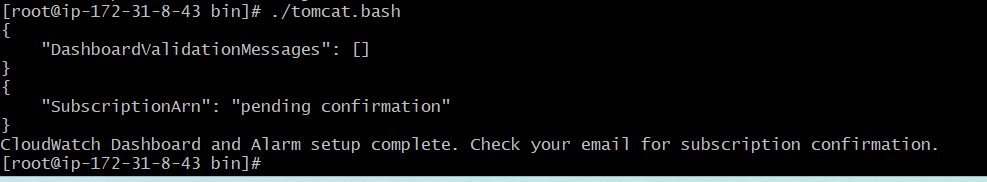
4) Create one alarm to send alert to email if the cpu utilization is more than 70 percent.



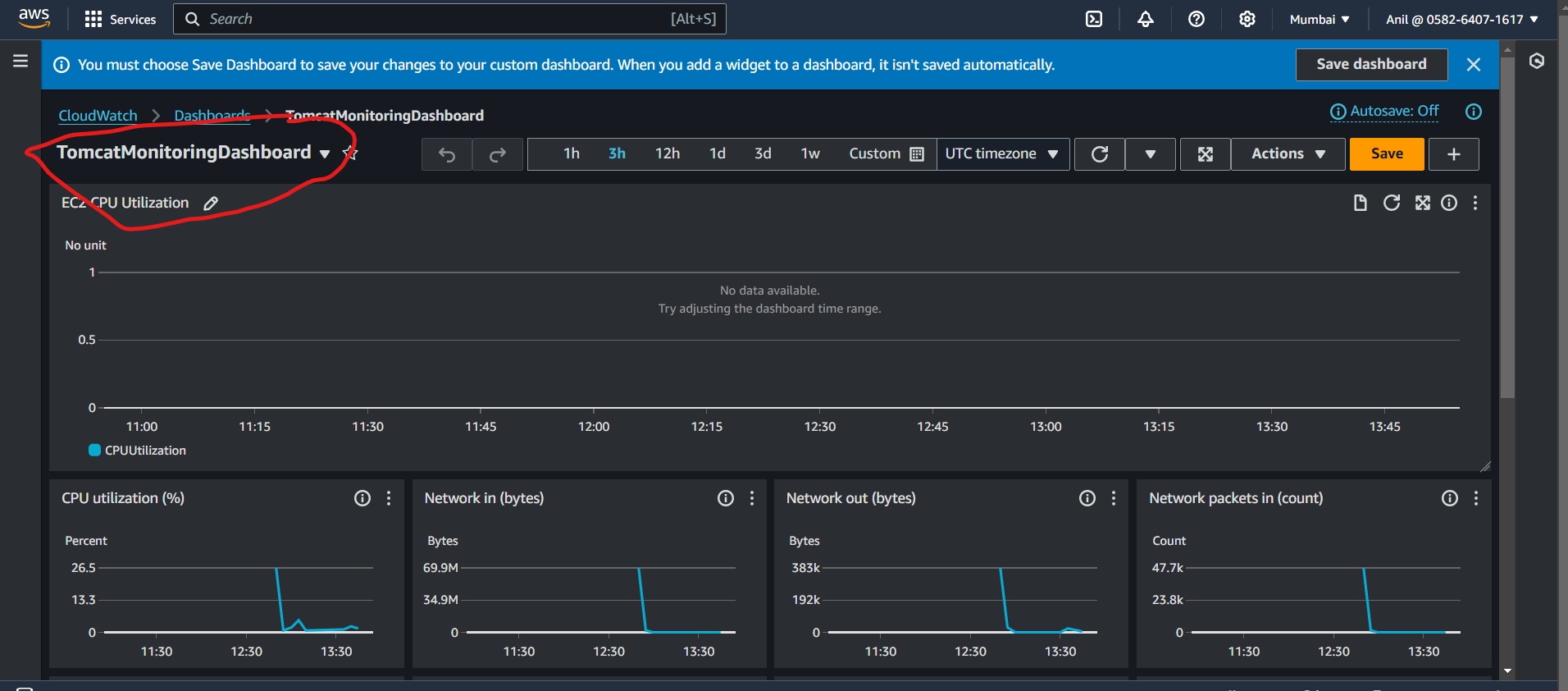




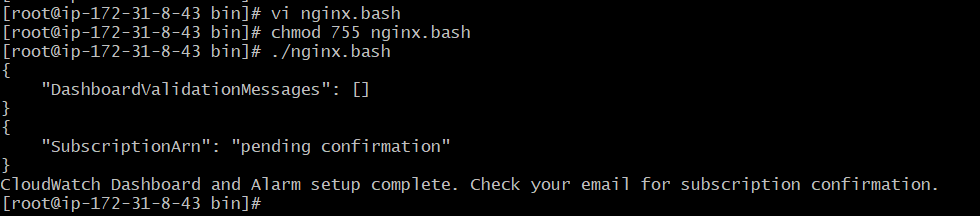
**5) Create Dashboard and monitor tomcat service wether it is running or not and send the alert.**

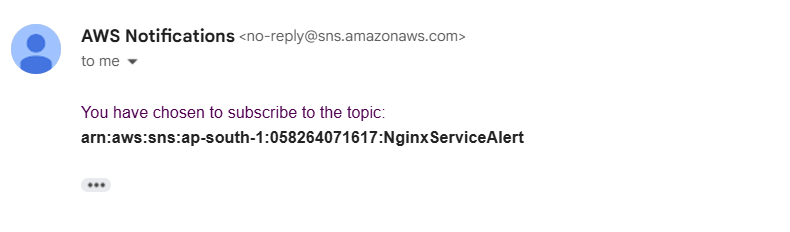
****

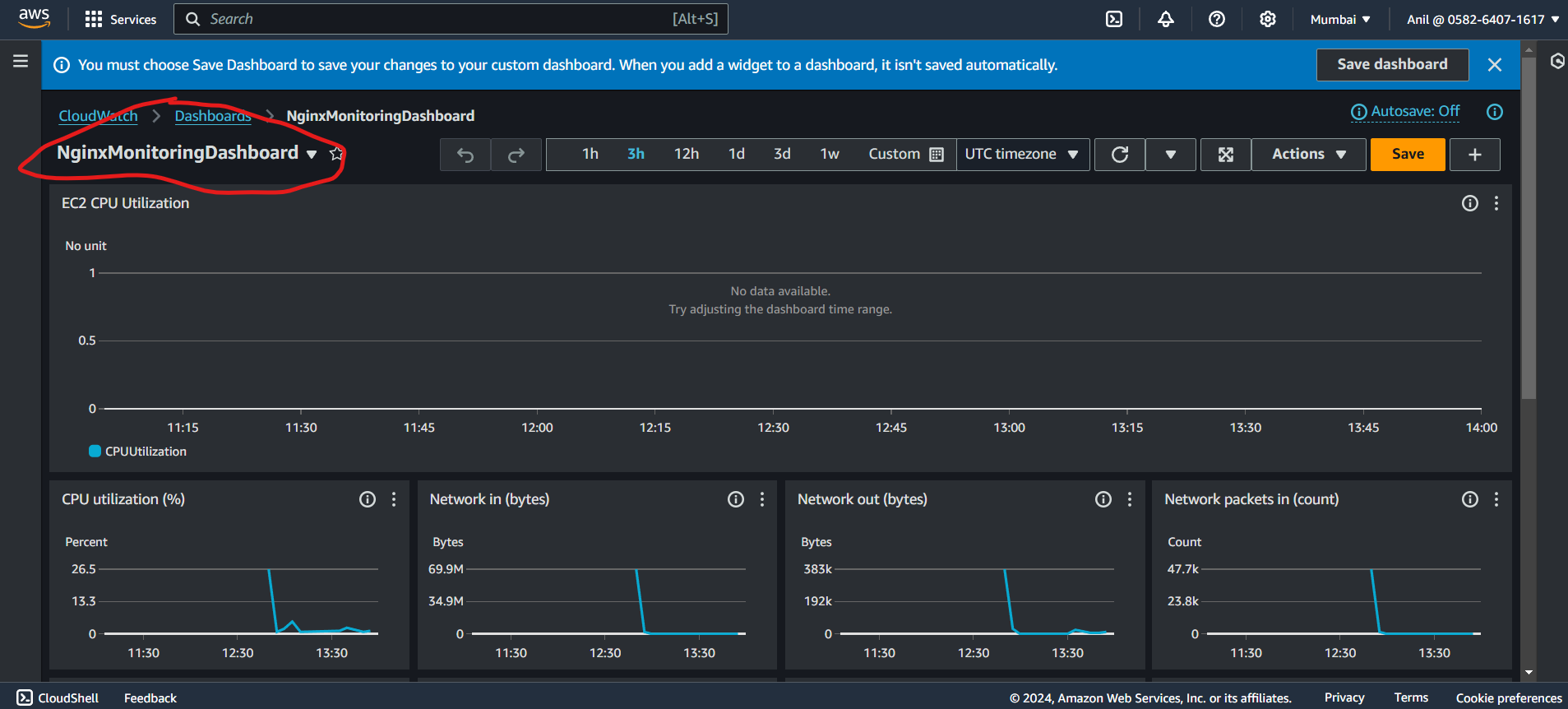
****

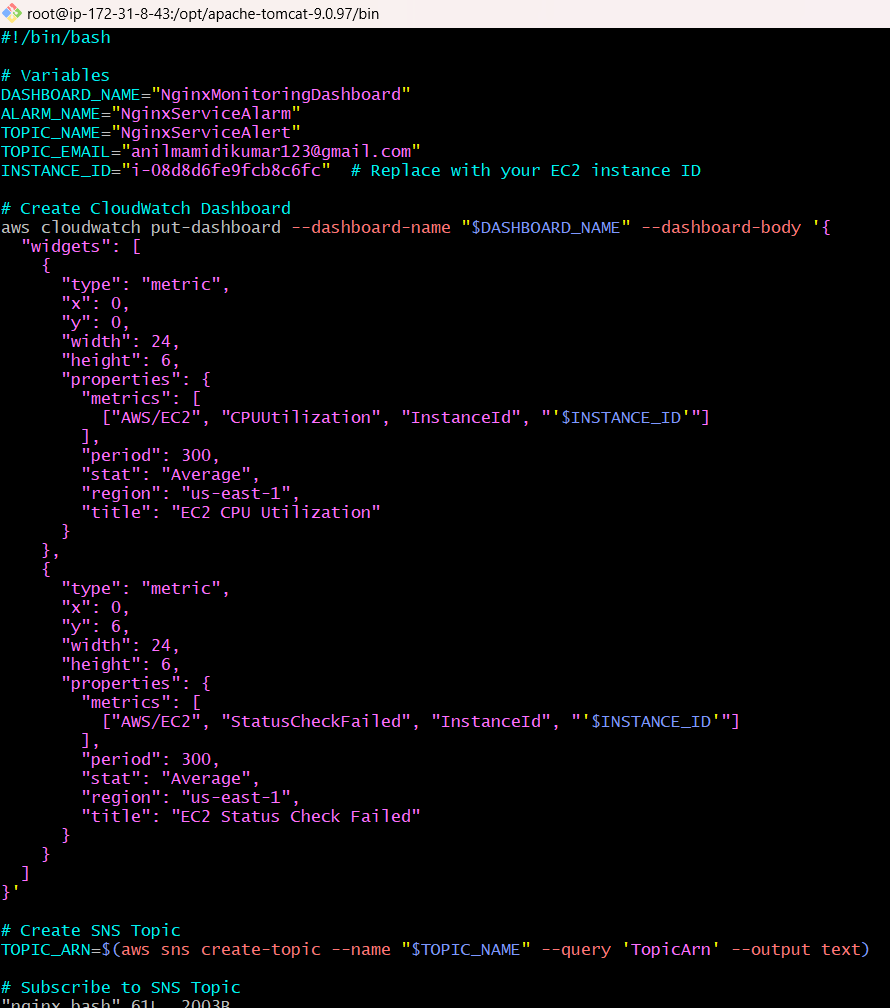
****

**6) Create Dashboard and monitor nginx service to send the alert if nginx is not running.**

****

****

****

****