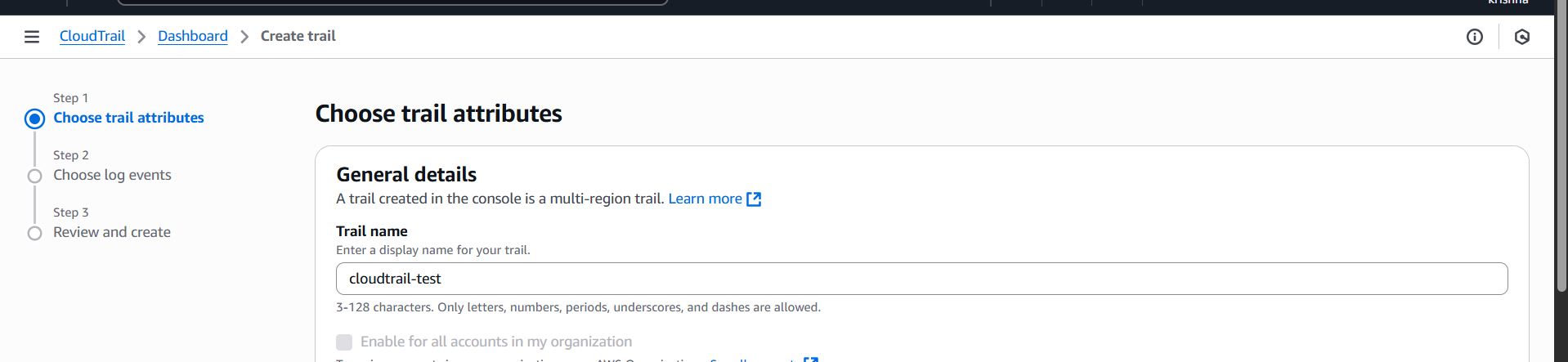
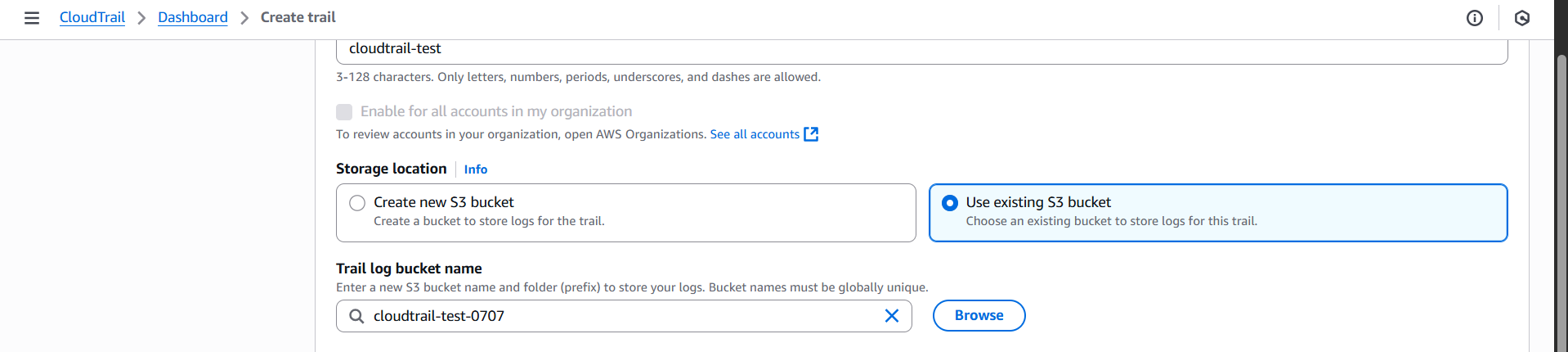
1) Enable cloudtrail monitoring and store the events in s3 and cloudwatch log events.

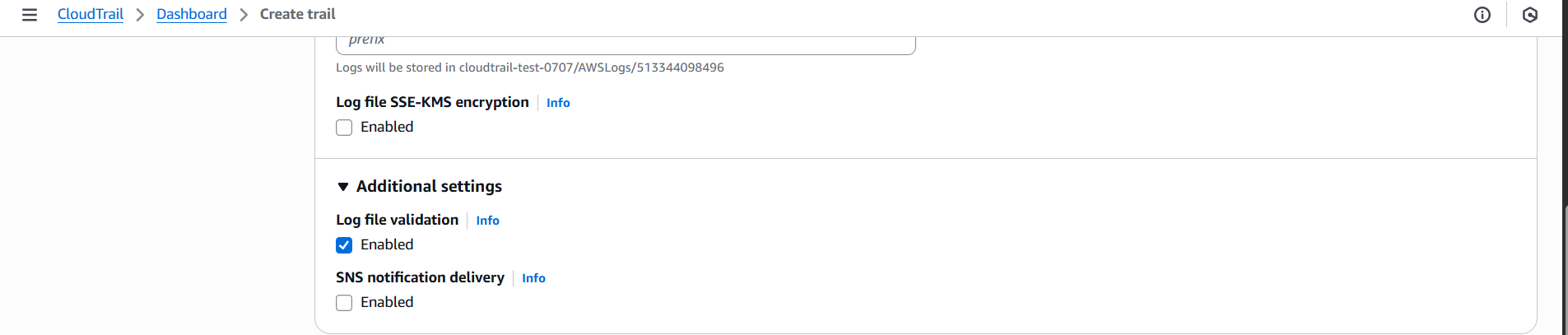
Step 1: Go to CloudTrail  
1. Open the AWS Console  
2. Search for CloudTrail in the Services menu  
3. Click “Trails” on the left  
4. Click “Create trail”

  
Step 2: Choose S3 Bucket for Log Storage

Select Create new S3 bucket or use an existing one

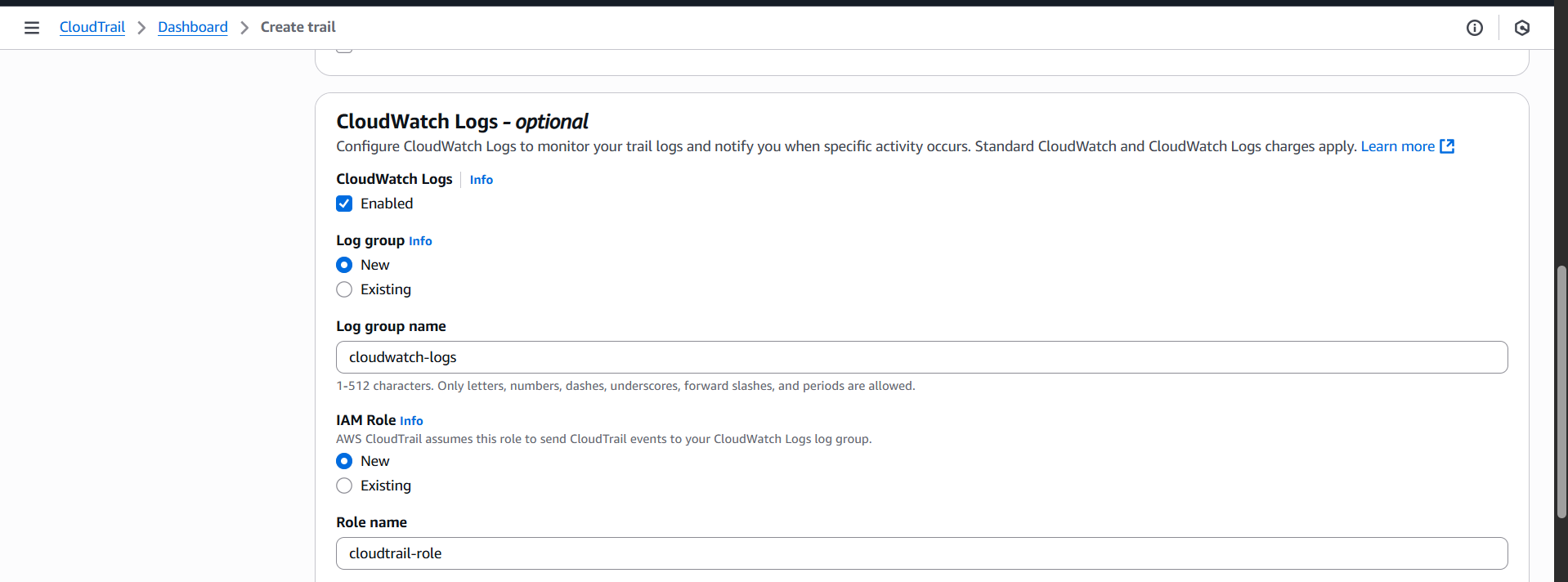


Step 3: Enable log validation



Step 4: Send Logs to CloudWatch Logs  
1. Enable CloudWatch Logs integration   
2. Choose Create new log group (cloudwatch-logs)  
3. CloudTrail needs permission to send logs:  
Click “Create a new IAM role”

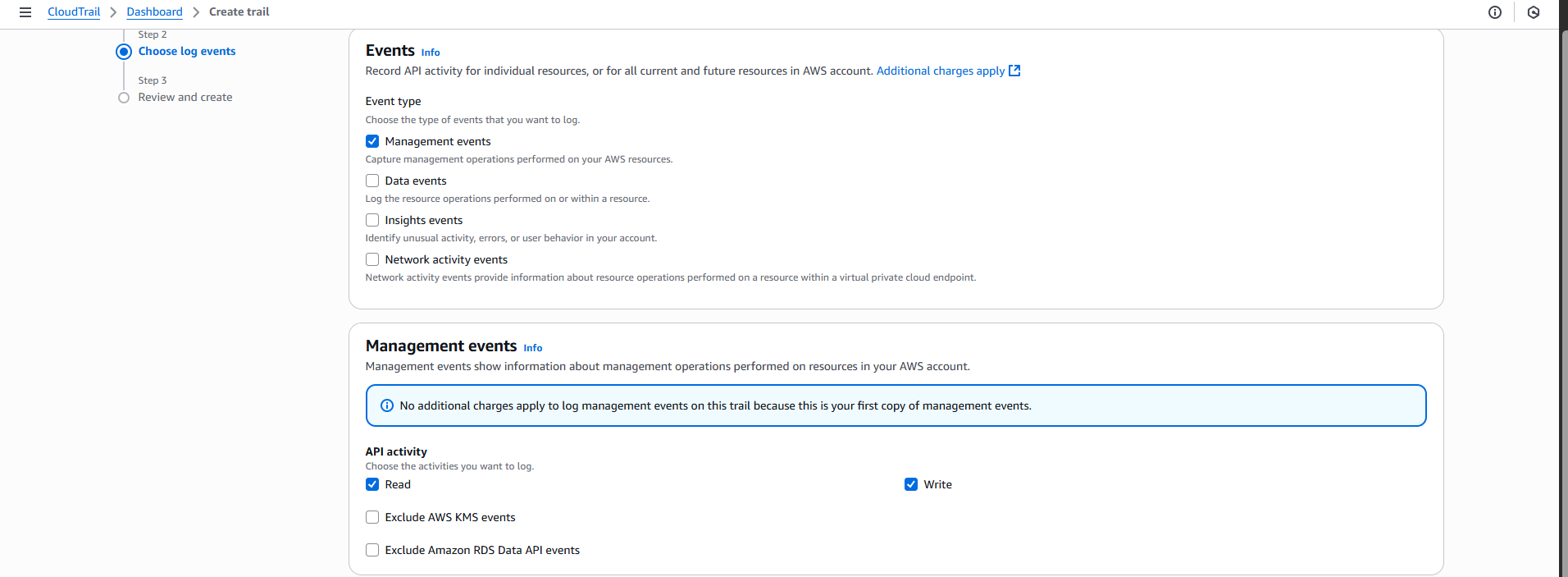
It will create a role like: CloudTrail-Role



Click “Next”

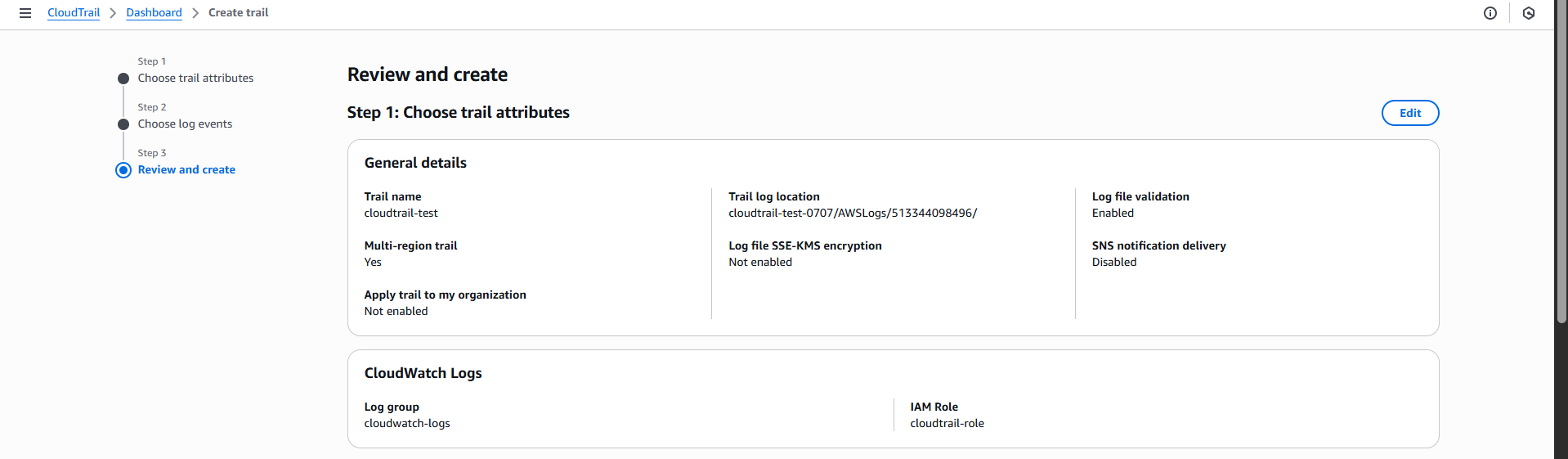
Step 5: Select management events

Then, in API activity select read and write

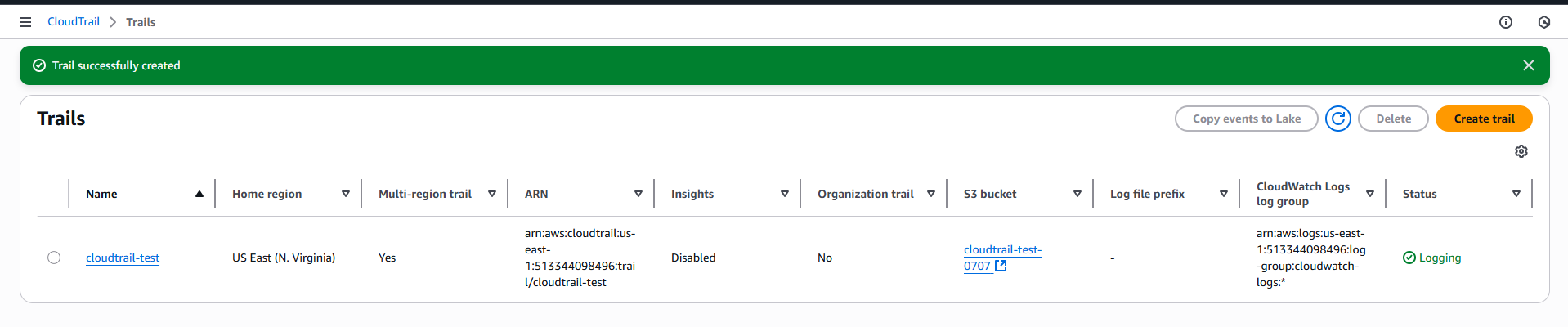


Click “Next”

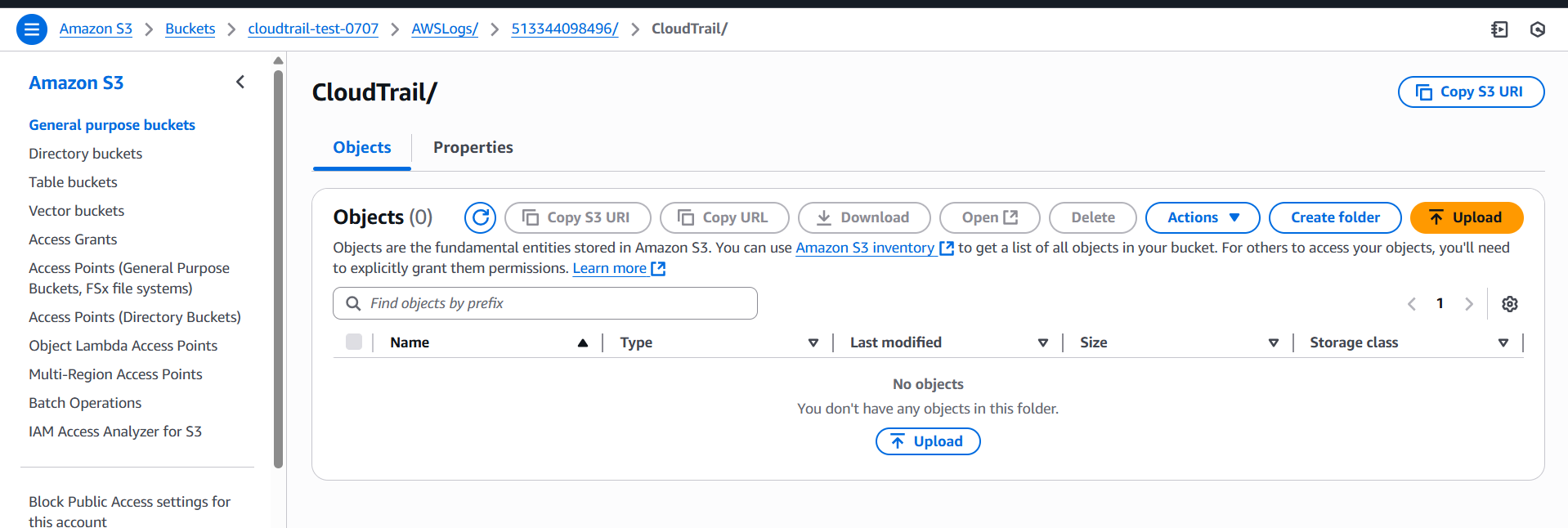
Step 6: Review and Create

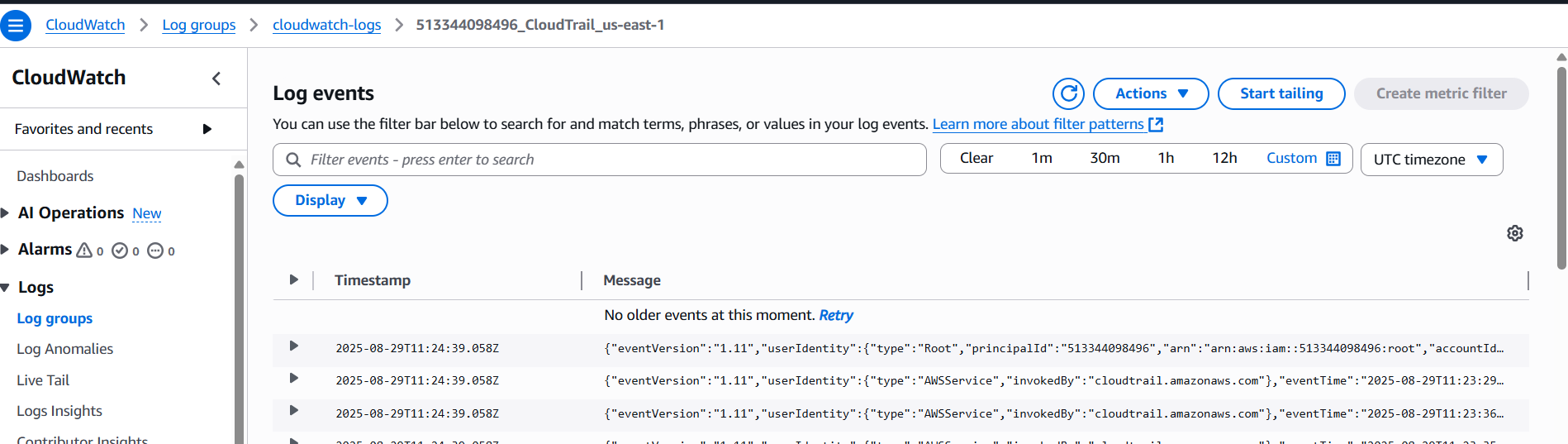


Click “Create trail”



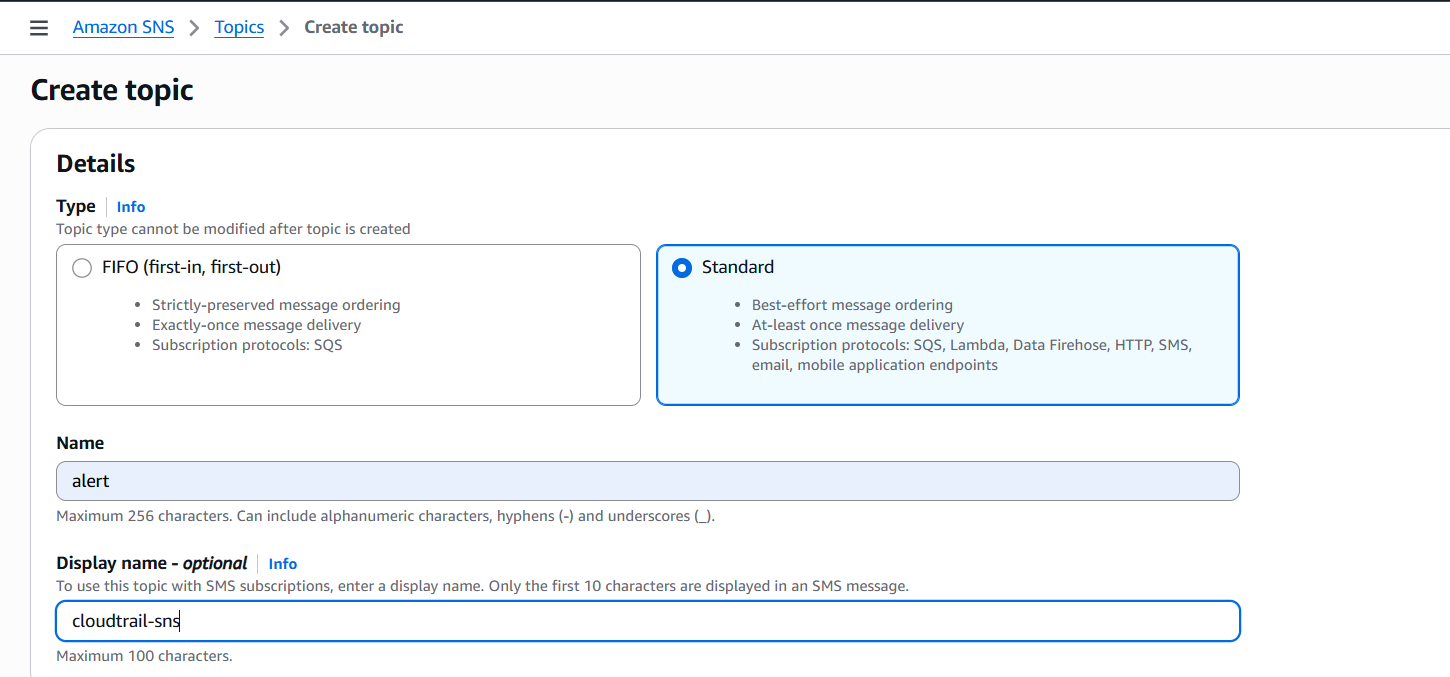
Go to s3 bucket to check default bucket created from Cloudtrail for attachment

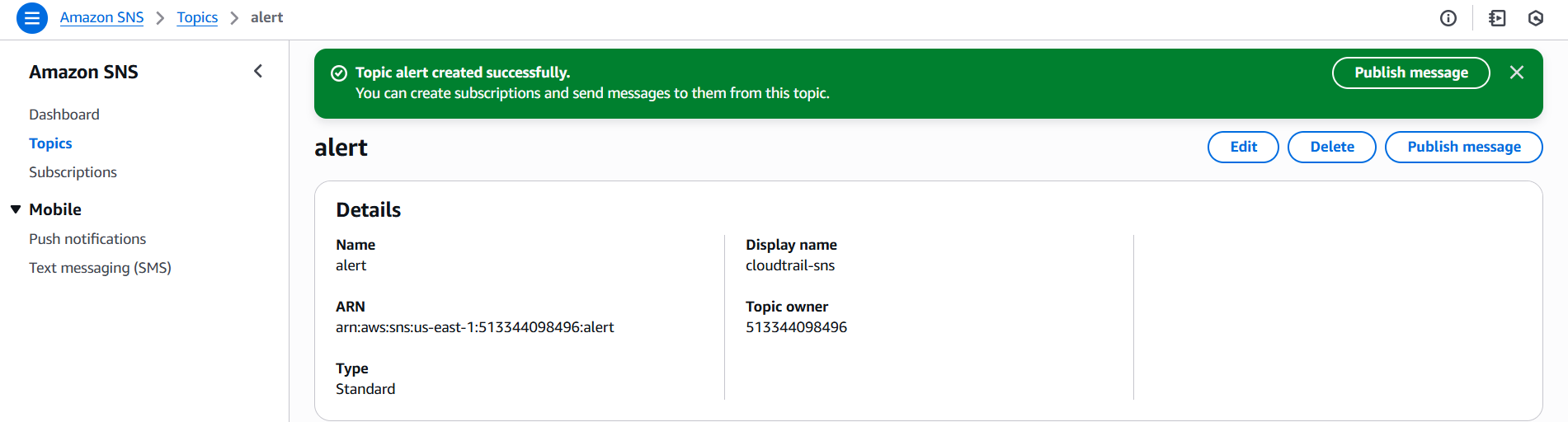
  
Go to Cloudwatch to check default Log groups created from Cloudtrail for attachment



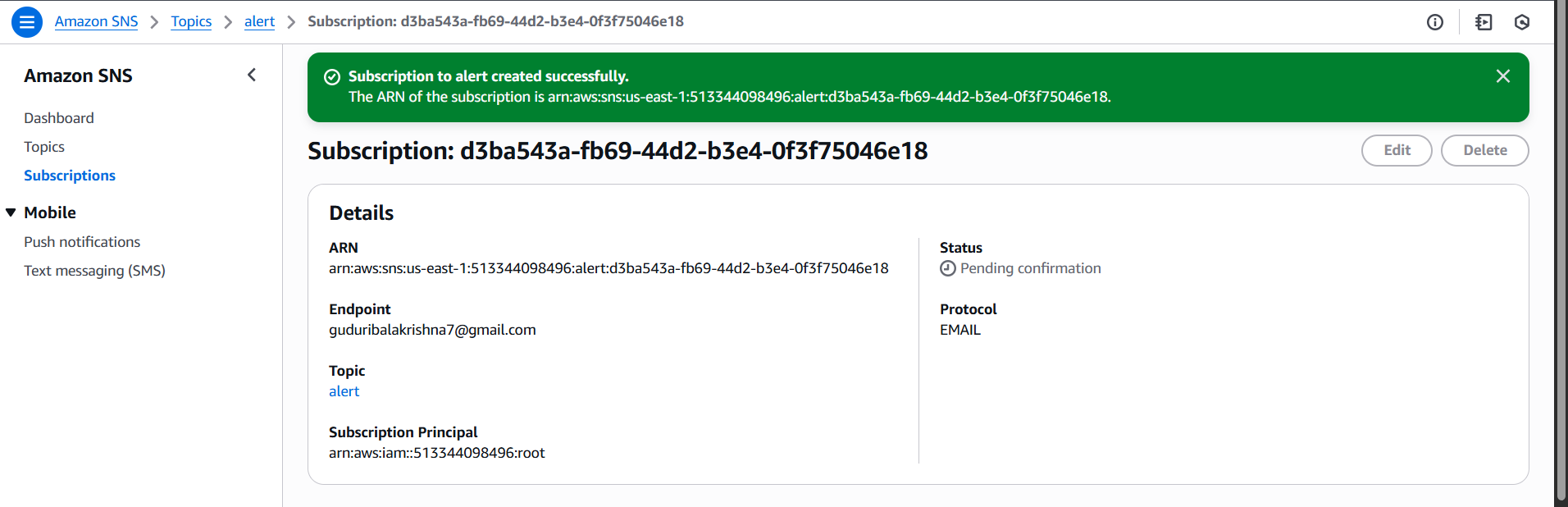
2) Enable SNS for cloudtrial to send alert on email.

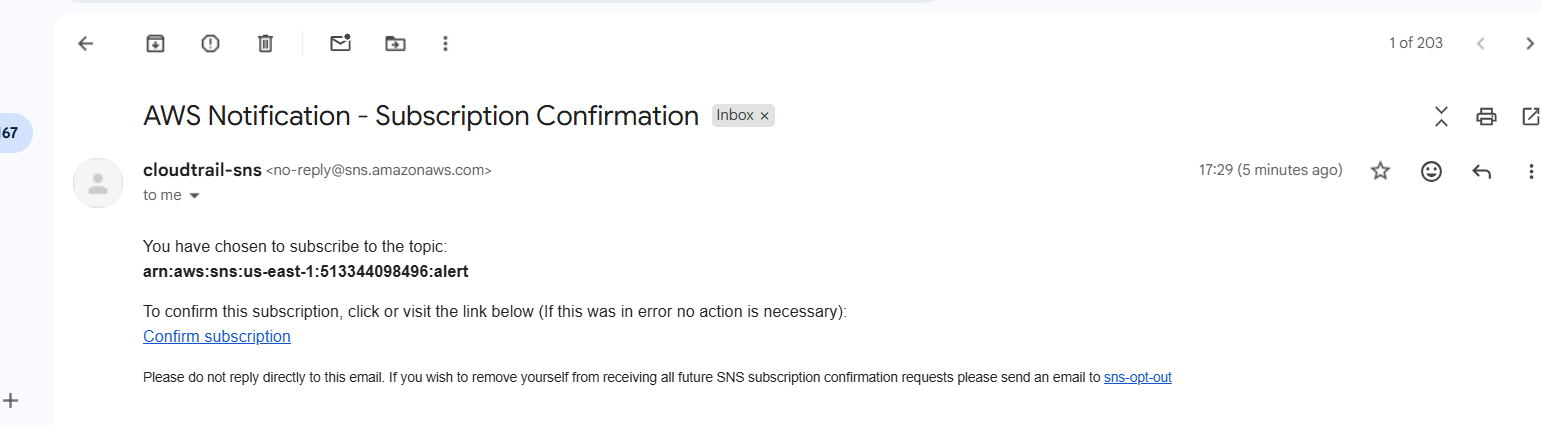
Step 1: Create an SNS Topic  
1. Go to SNS → Topics  
2. Click Create topic  
3. Select Standard  
4. Enter Name (e.g., cloudtrail-sns)

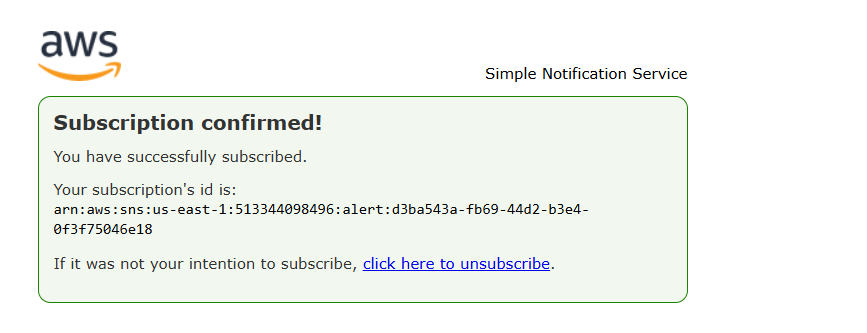


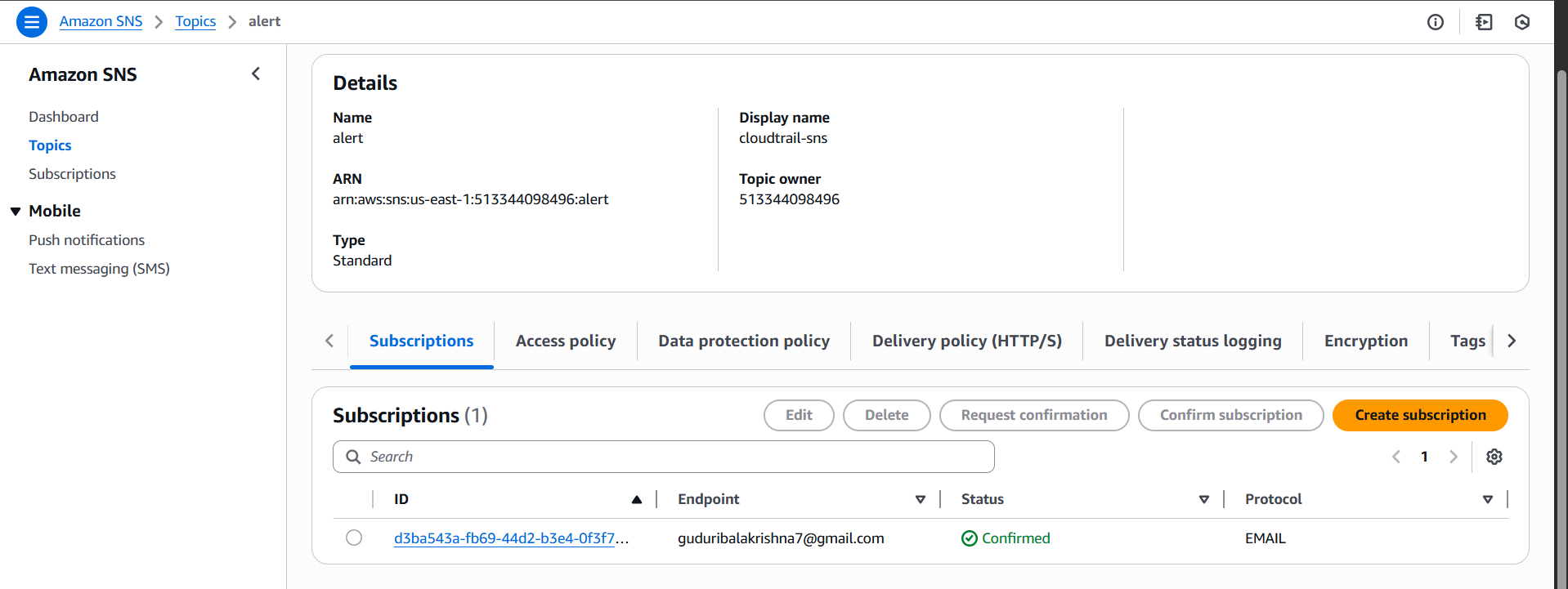


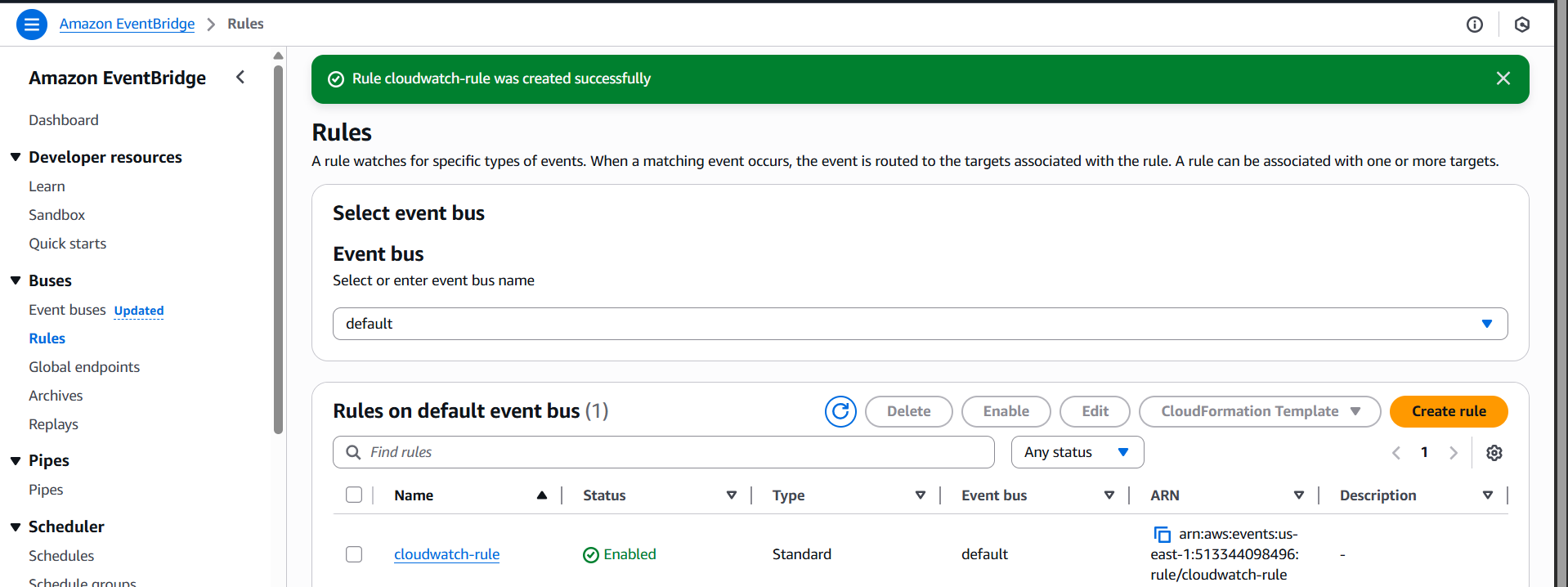
Step 2: Subscribe to the Topic via Email  
Amazon SNS 🡪 topics 🡪 select your topic 🡪 subscription 🡪 create subscription







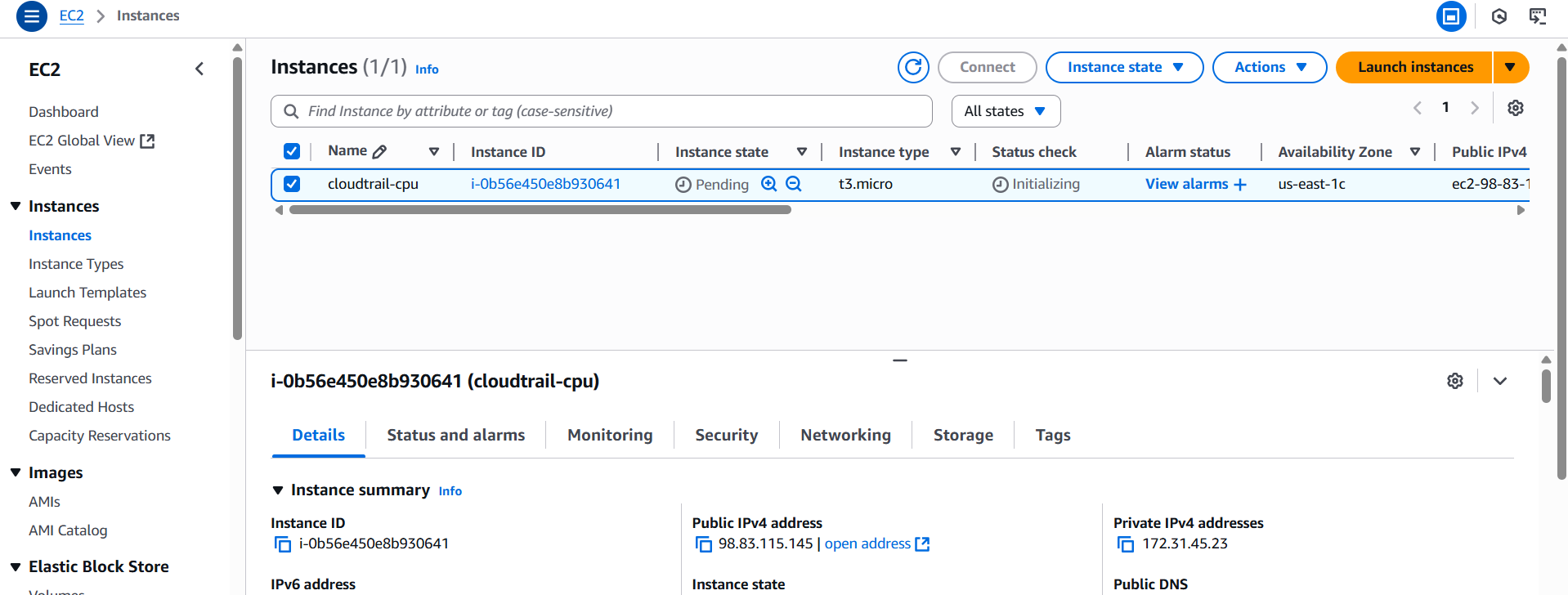


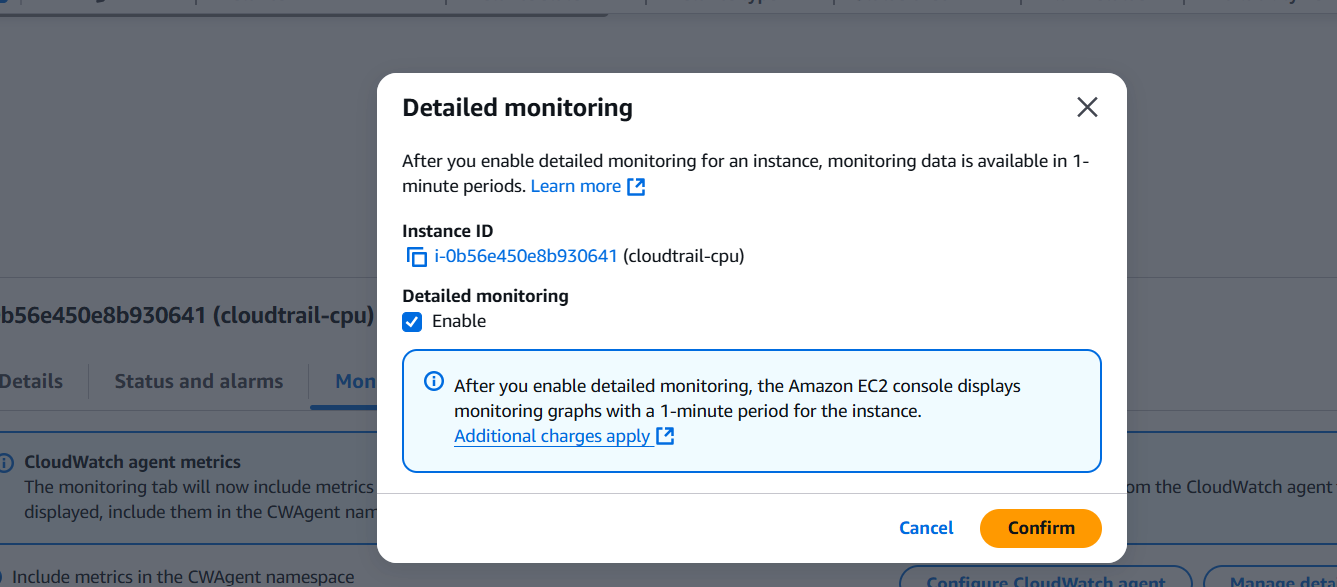
Step 3: Create Event Rule for CloudTrail  
1. Go to CloudWatch → Rules (or EventBridge → Rules)  
2. Click Create rule  
3. Choose Event source:  
 Service Name: CloudTrail  
 Event Type: e.g., Management events or specific actions  
4. Under Target, choose:  
 SNS Topic  
 Select the topic you created (alert)  
5. Click Next, give the rule a name, and click Create rule  


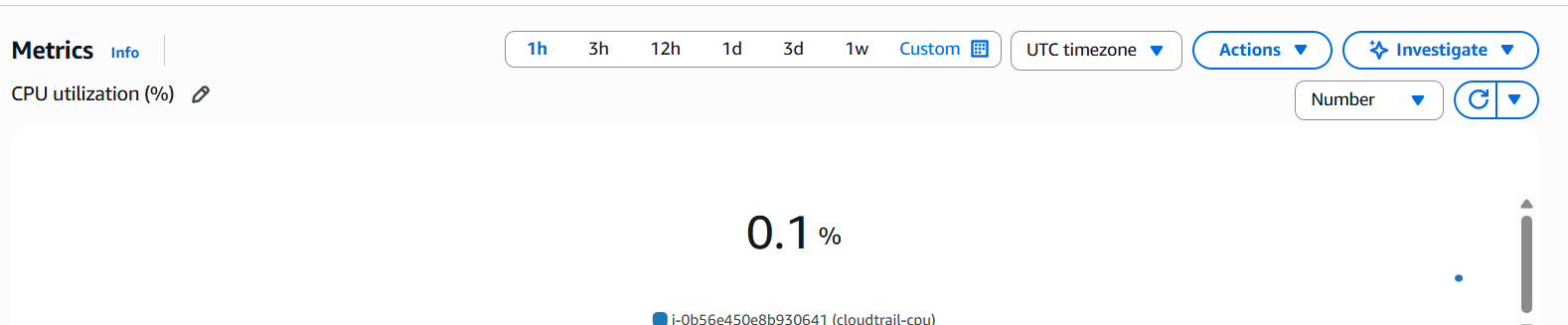
You’ll now receive email alerts when the selected CloudTrail events occur

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

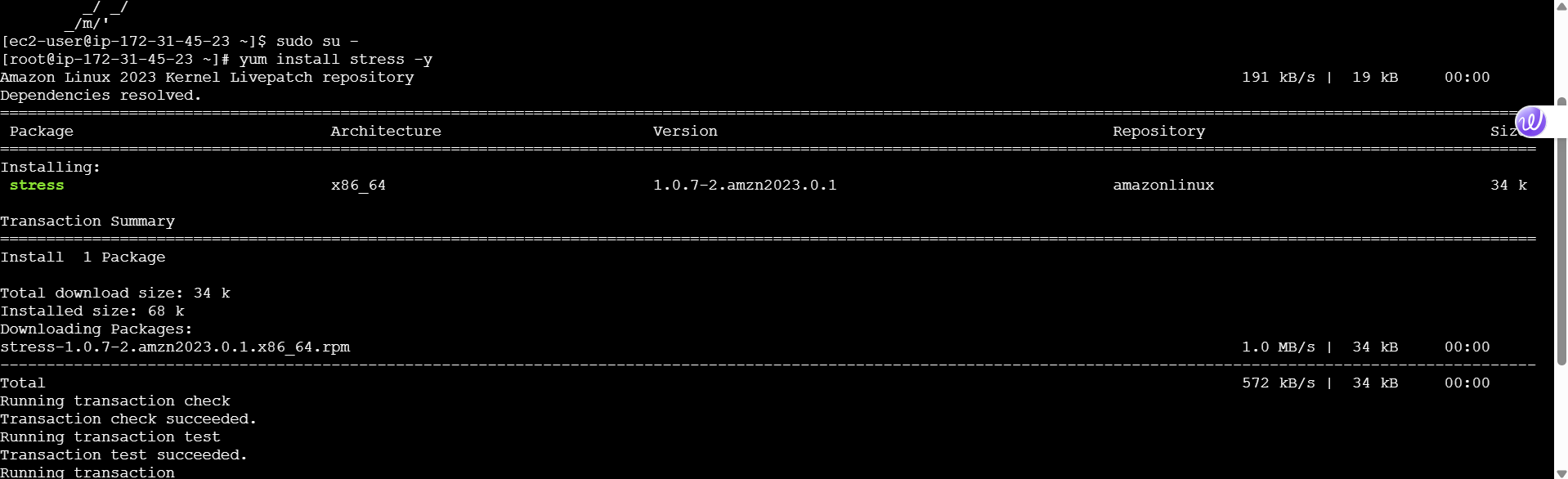
Step 1: Open EC2 Console  
1. Go to EC2 → Instances  
2. Select the instance you want to monitor

  
Step 2: Enable Detailed Monitoring (Optional for 1-min data)  
1. In the Details tab, check Monitoring  
2. Click Actions → Monitor and troubleshoot → Manage detailed

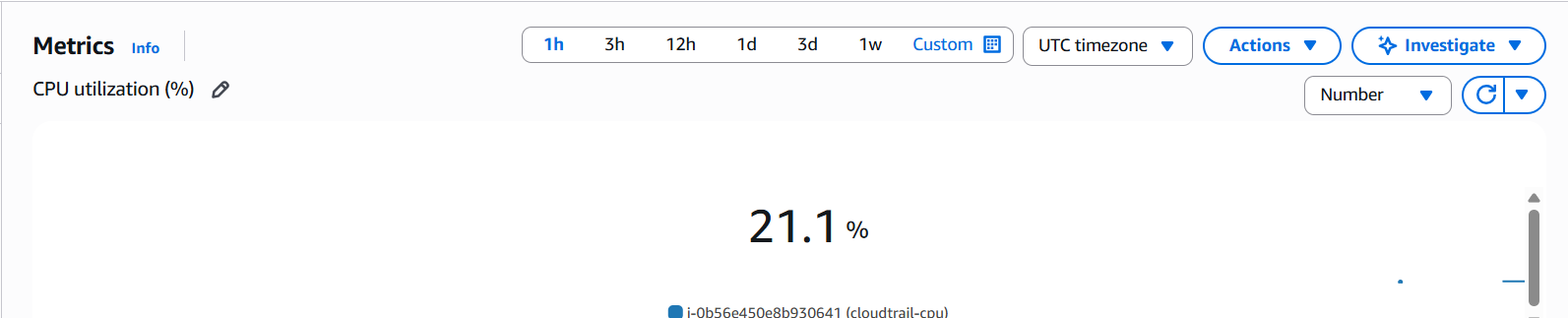


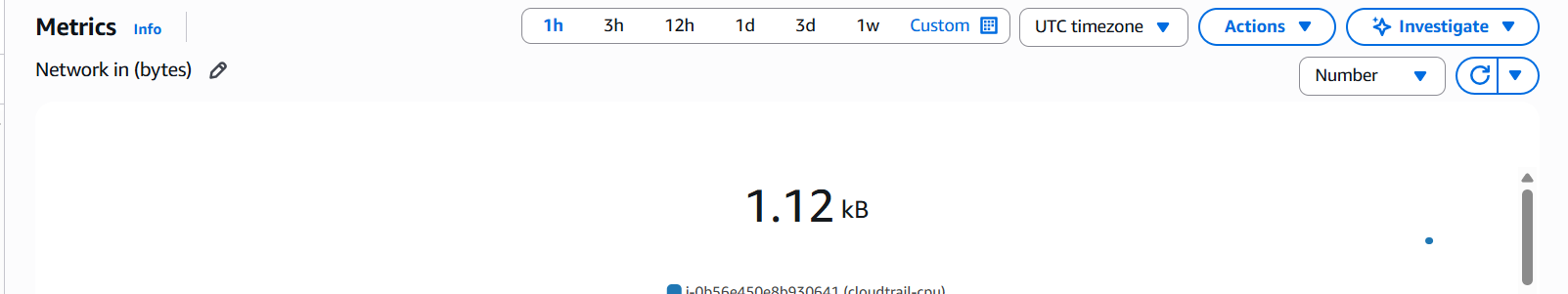


utilization and other metrics of ec2.  
Fake stress or load for CPU.  
Yum install stress -y



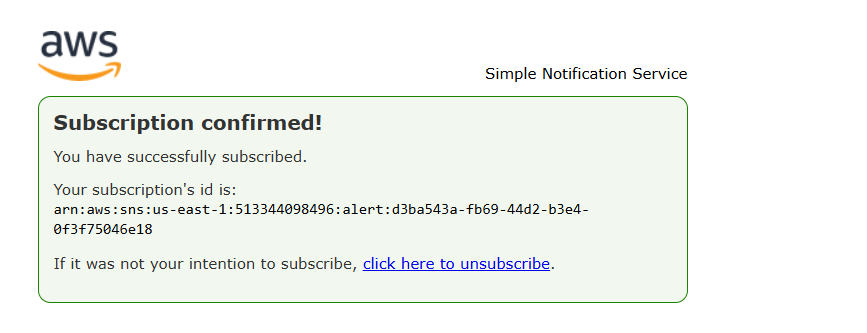
Step 3: View CPU & Other Metrics  
1. Go to CloudWatch → Metrics  
2. Click Browse → EC2 → Per-Instance Metrics  
3. Select your Instance ID  
4. View metrics like:  
 CPUUtilization  
 DiskReadBytes, DiskWriteBytes

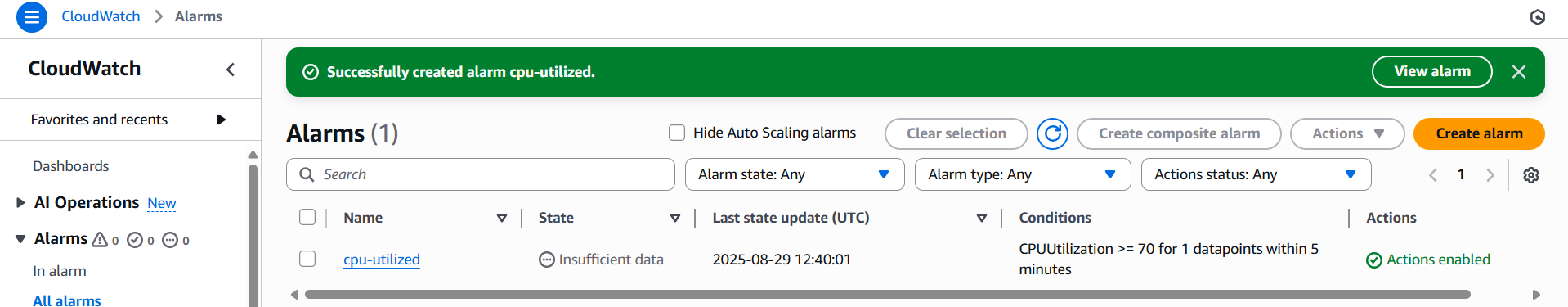
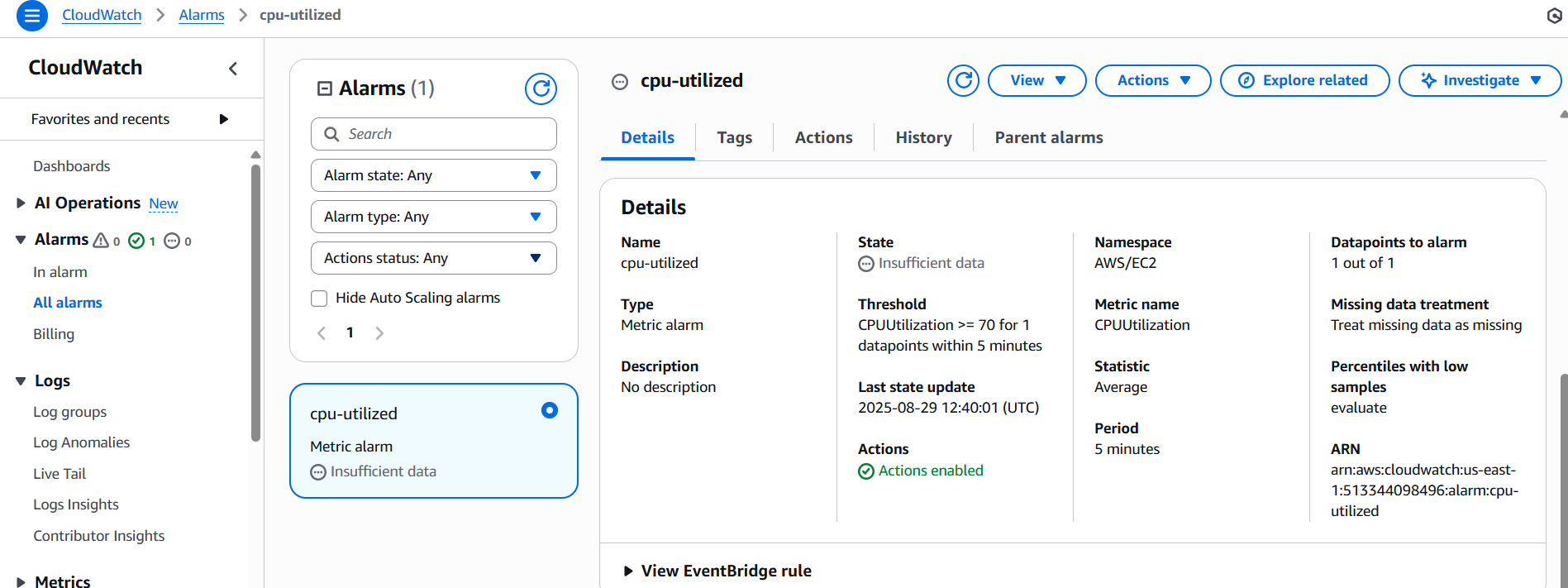


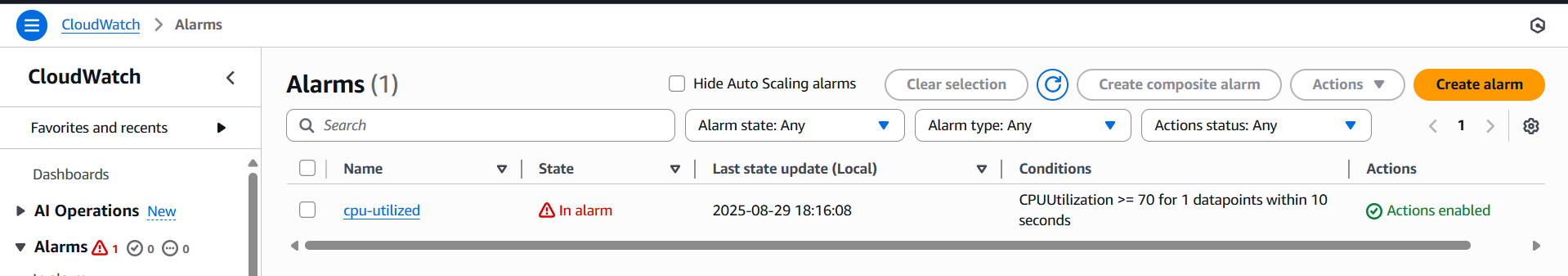


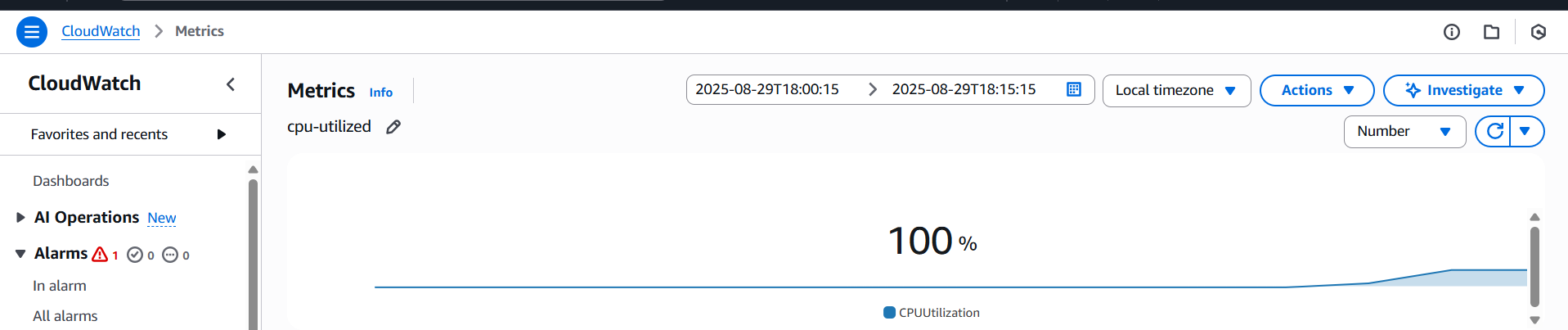
4) Create one alarm to send alert to email if the cpu utilization is more than 70 percent.

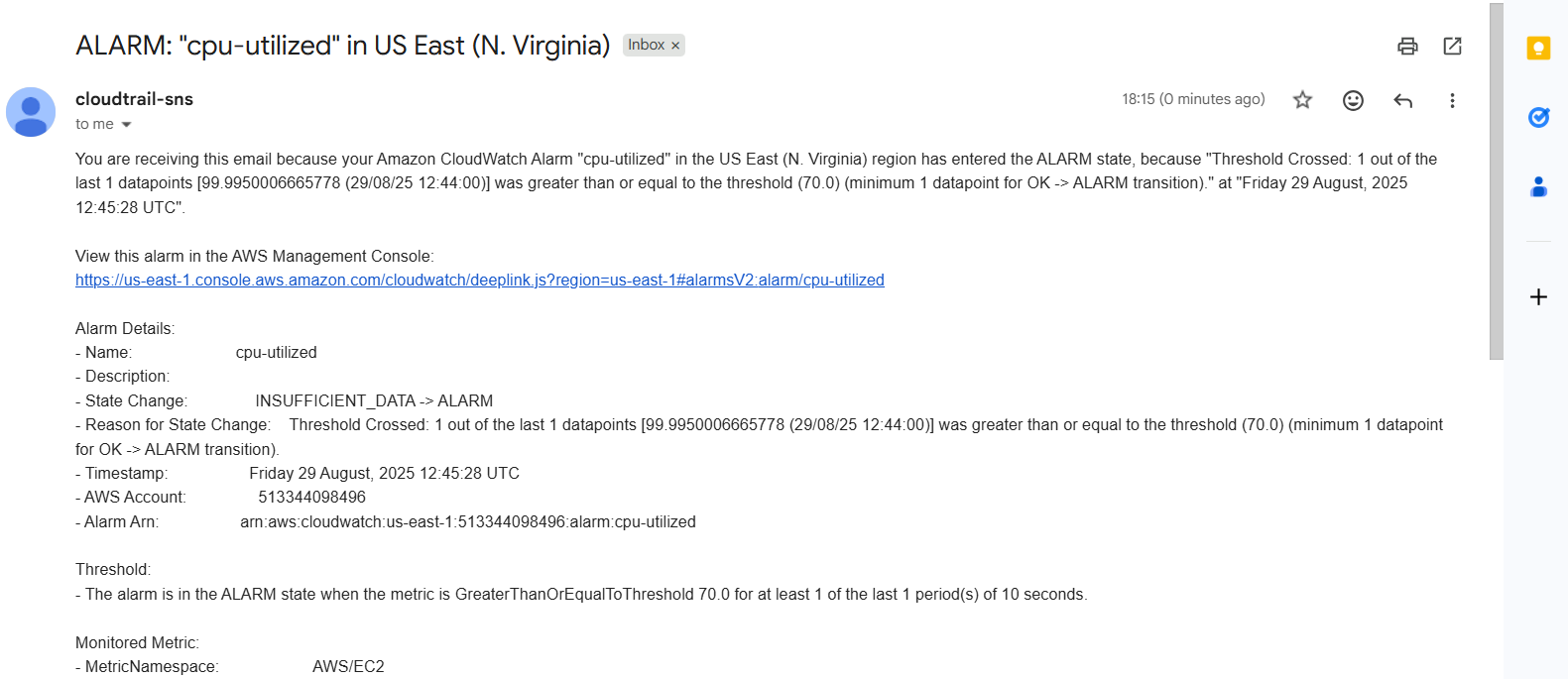
Step 1: Create an SNS Topic for Email Alerts  
Confirm SNS subscription from email



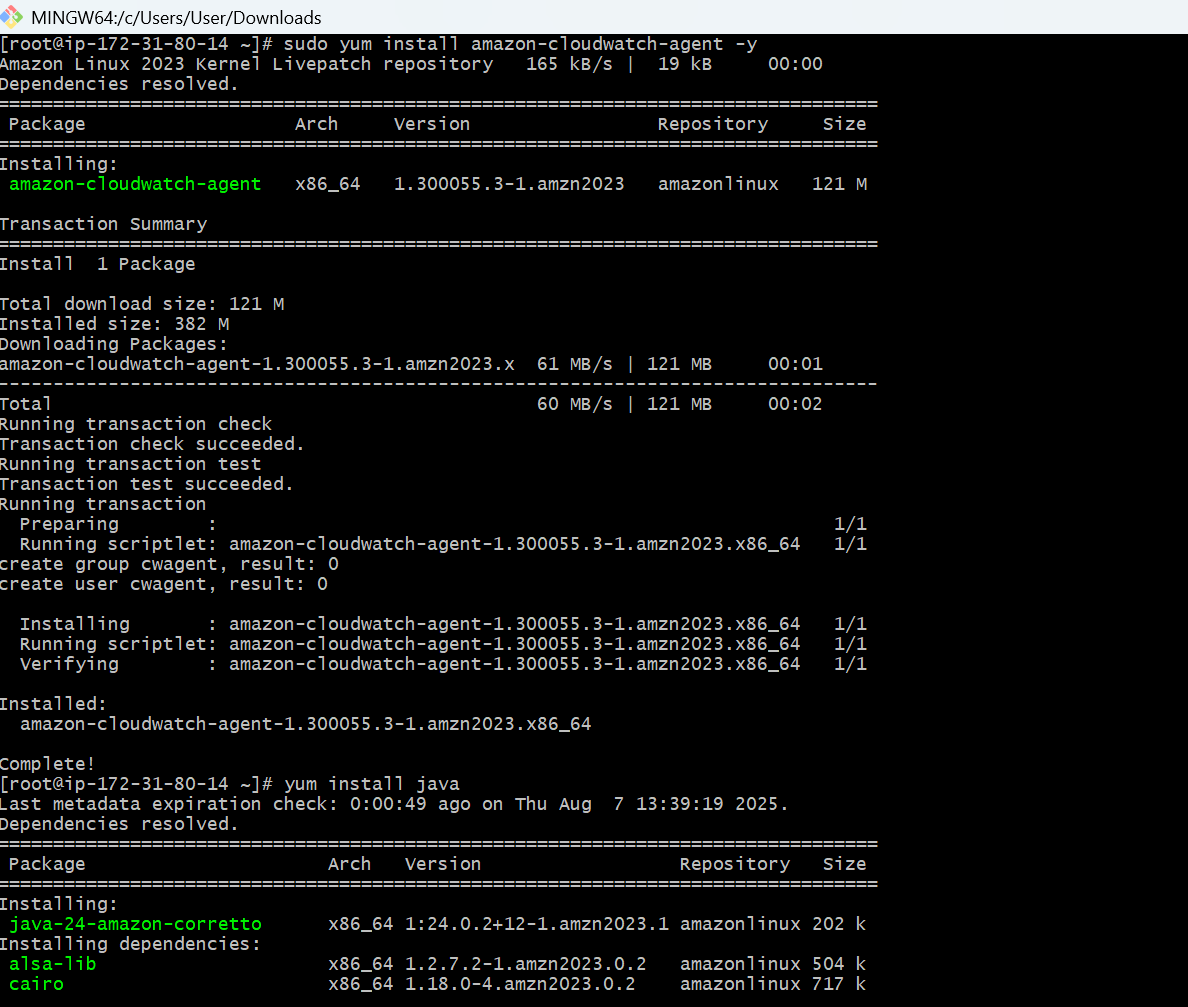
Step 2: Create CloudWatch Alarm for EC2 CPU  
Cloudwatch ---> Alarms ---> create alarm ---> Select Metric  
1. Click Select metric  
2. Go to EC2 → Per-Instance Metrics  
3. Select your Instance ID  
4. Choose CPUUtilization  
  


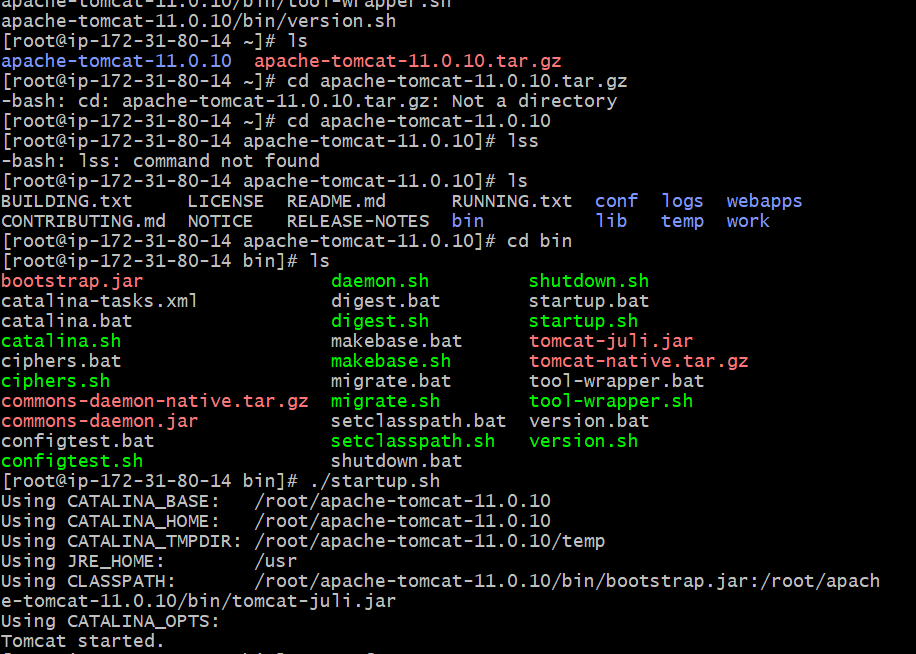


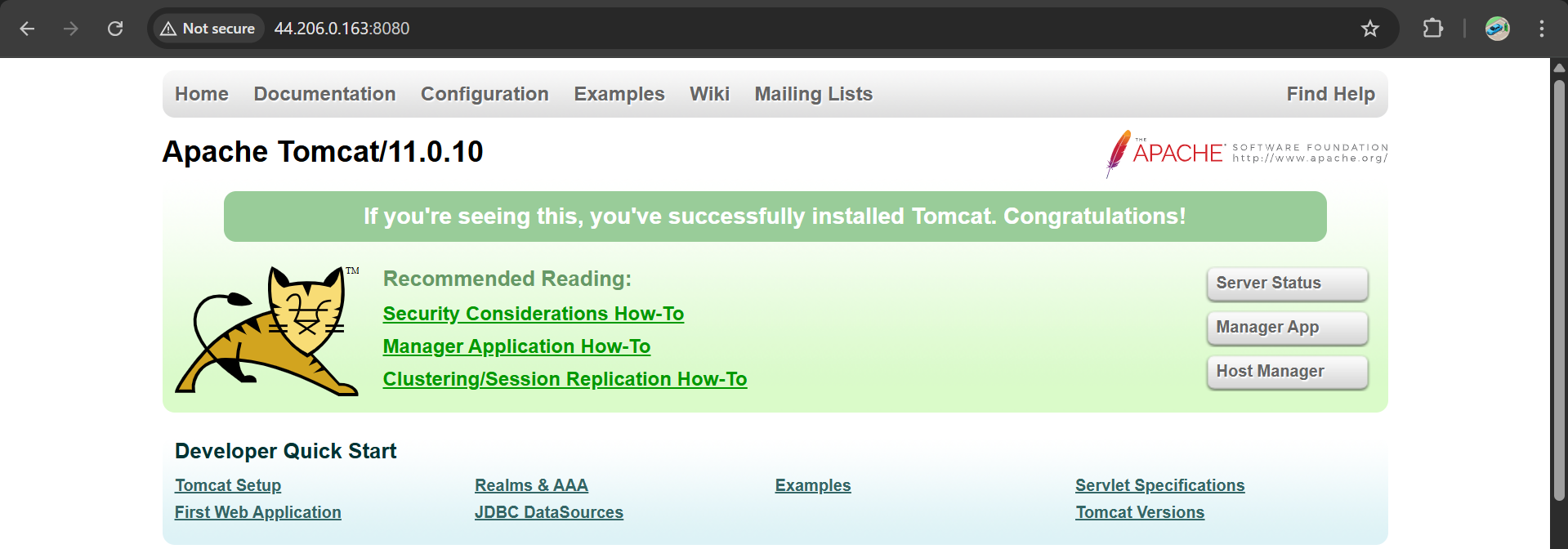


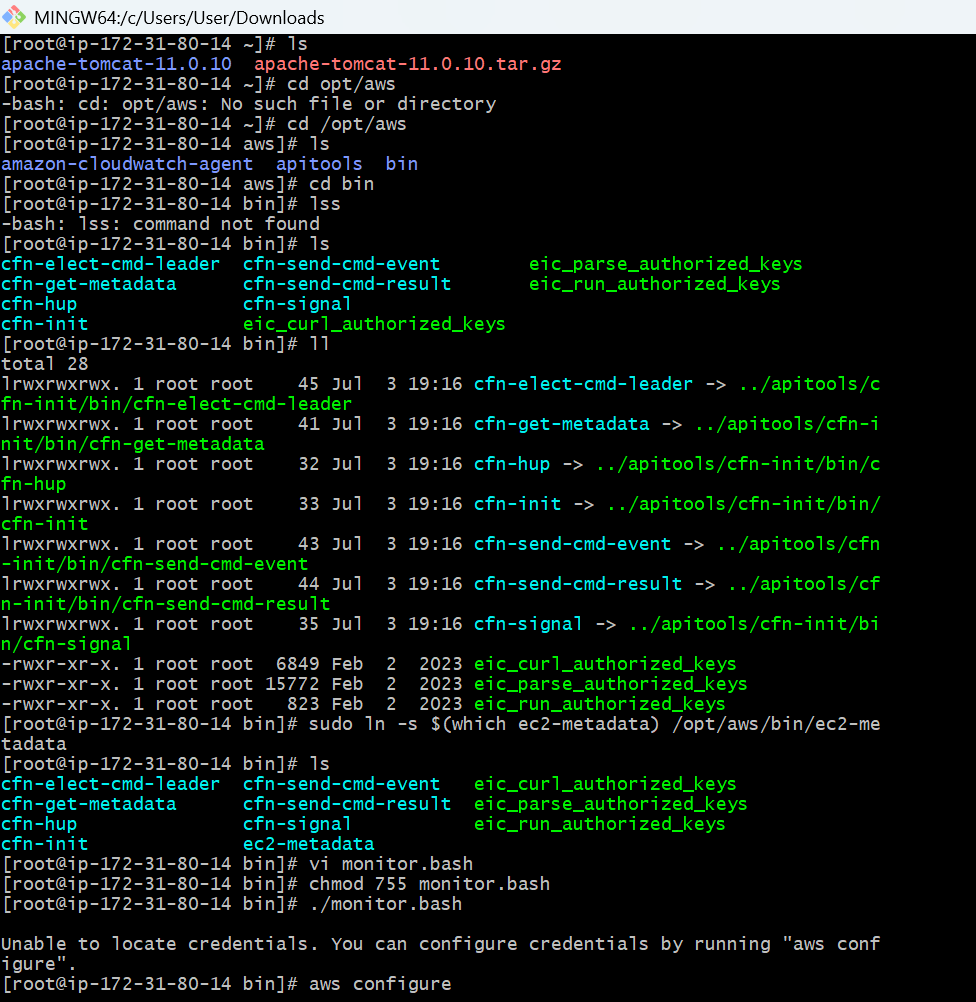


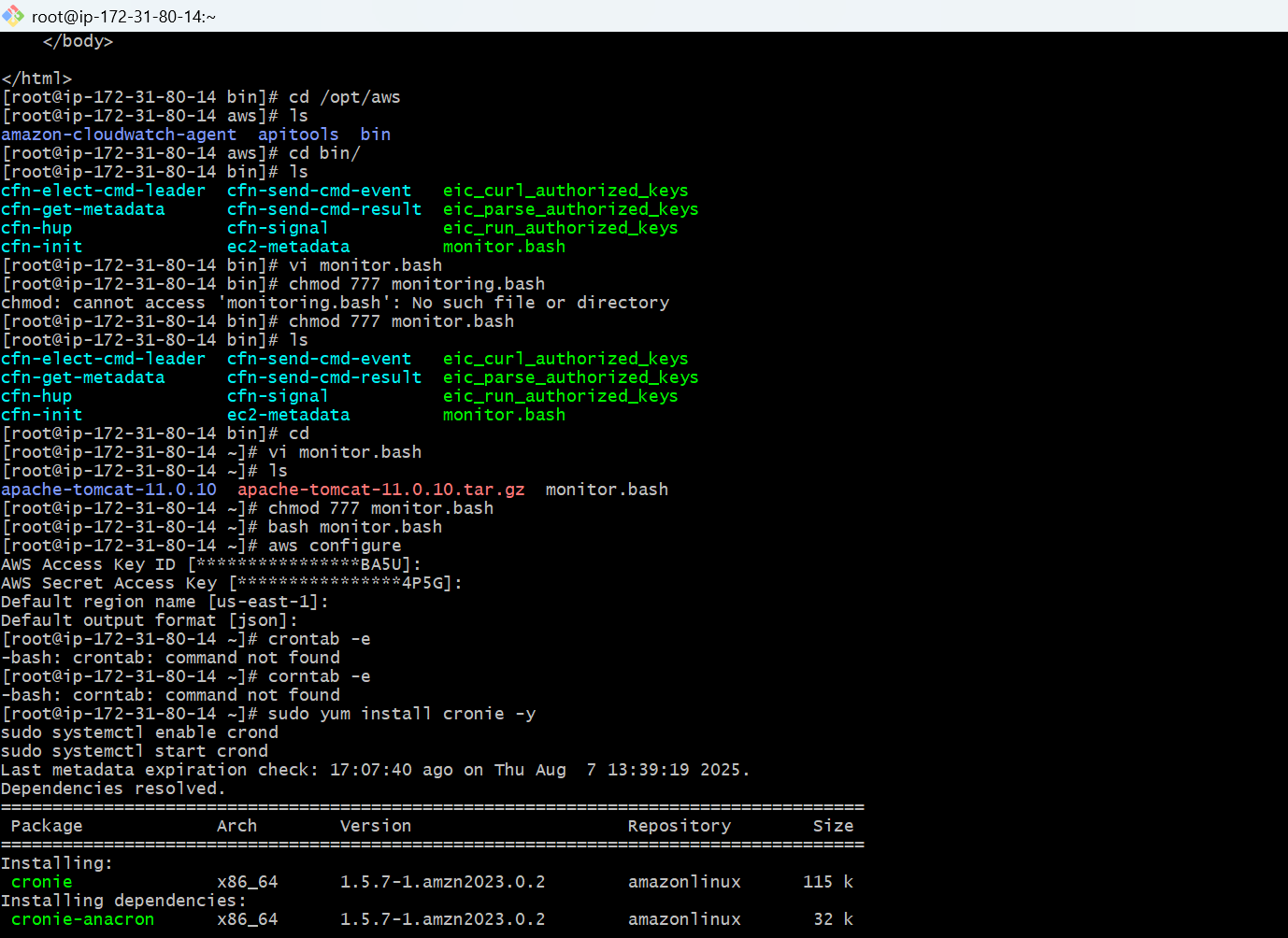
5) Create Dashboard and monitor tomcat service weather it is running or not and send the alert.

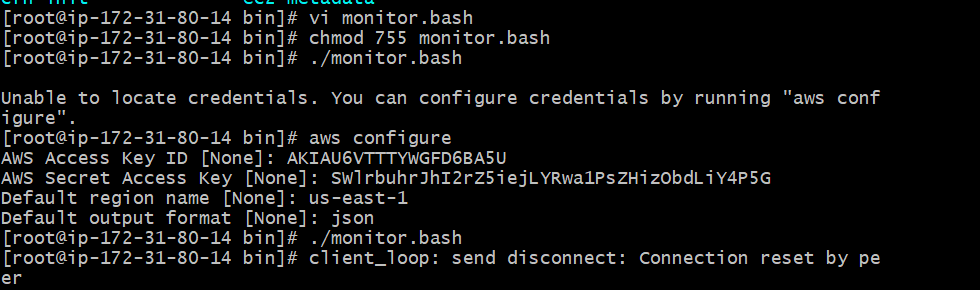


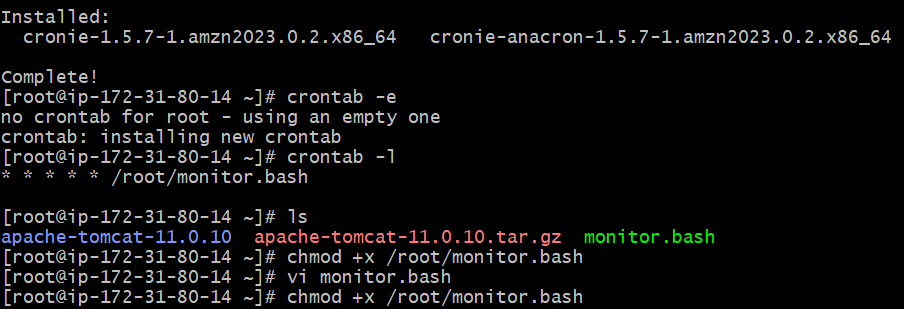


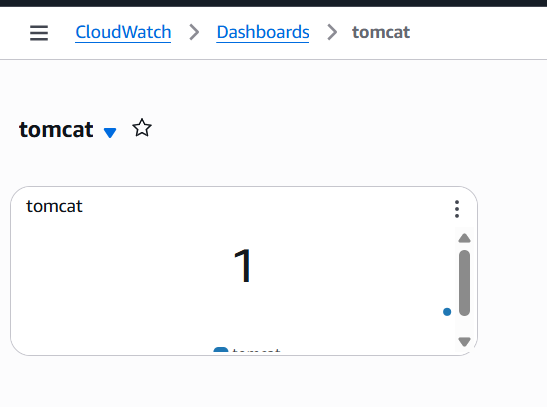


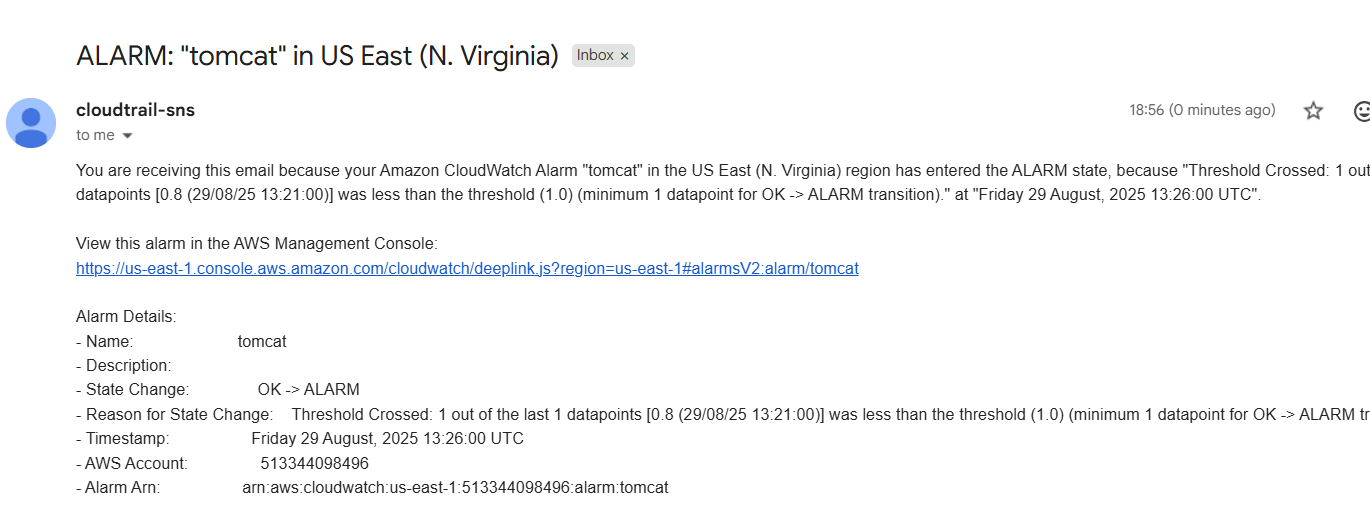












6) Create Dashboard and monitor nginx service to send the alert if nginx is not running.

