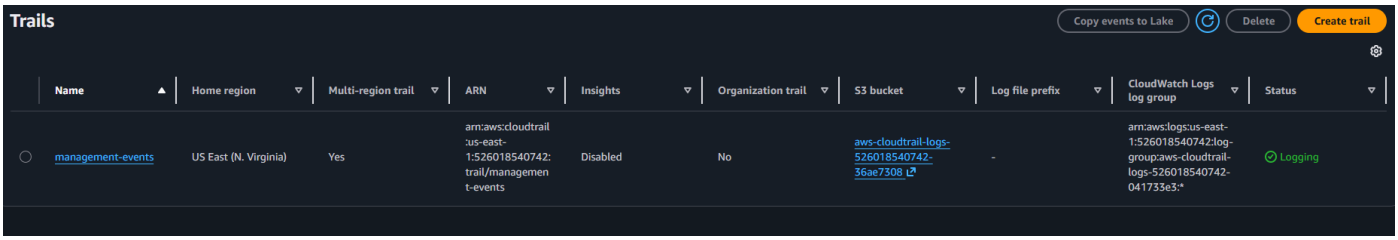
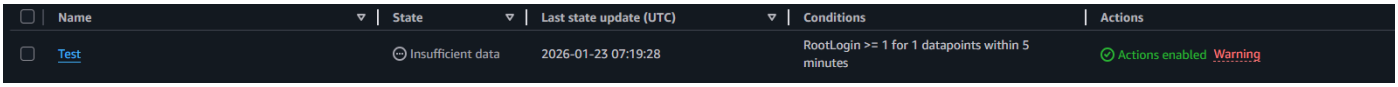
CloudTrail & CloudWatch – Tasks 01

- Enable CloudTrail monitoring and store the events in S3 and CloudWatch log events.

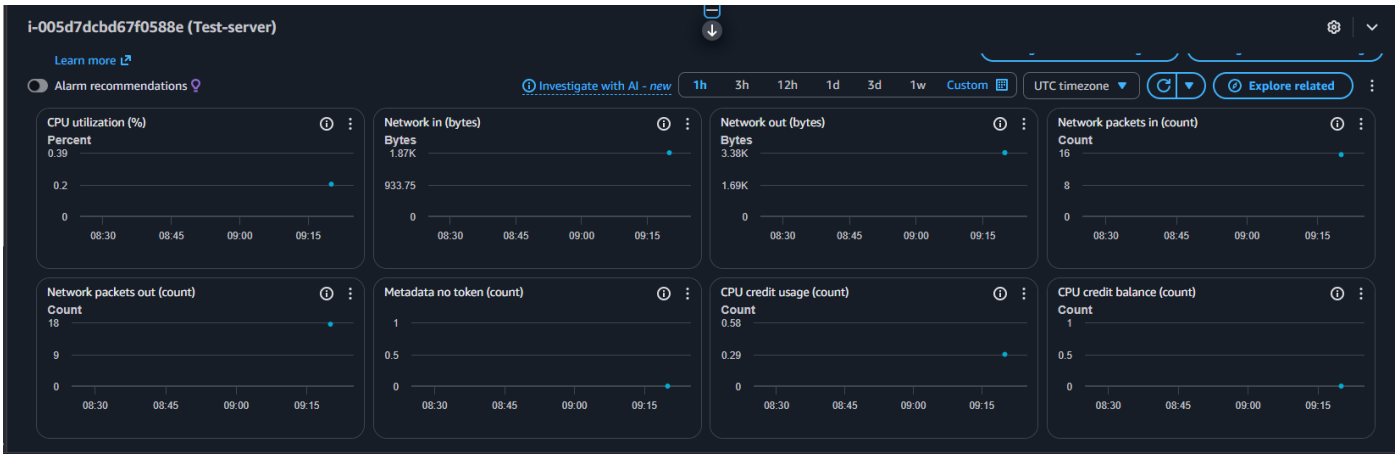


- Enable SNS for CloudTrail to send alerts via email.

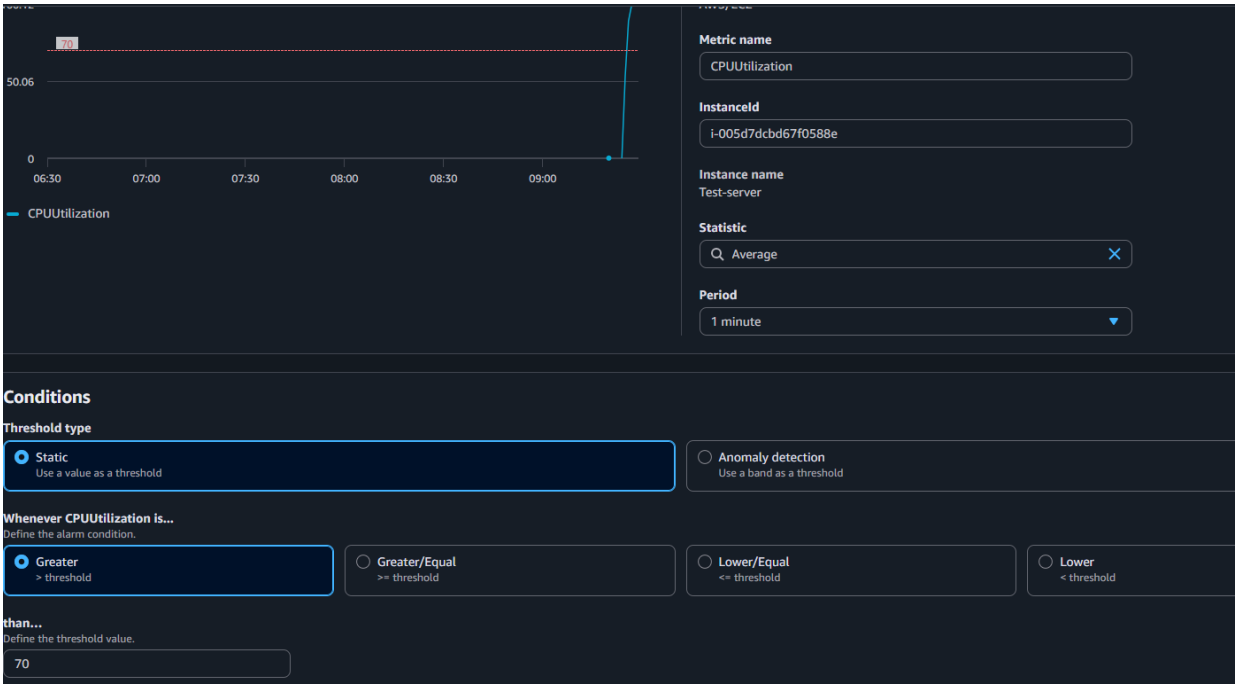
  The following alarm was created to track any changes done by root user.



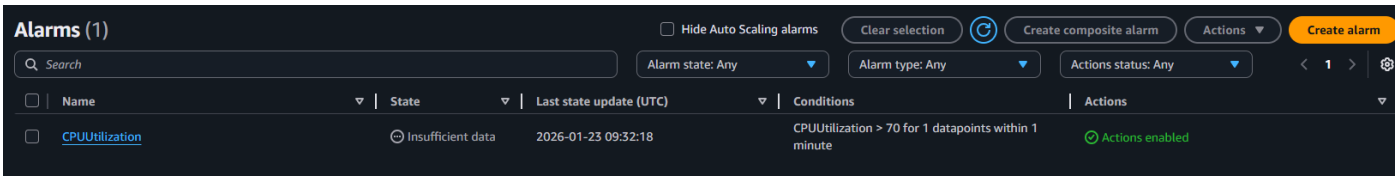
- Configure CloudWatch monitoring and record the CPU utilization and other metrics of EC2



- Create one alarm to send an alert to email if the CPU utilization is more than 70 percent.



CloudTrail & CloudWatch – Tasks 01



ALARM: "CPUUtilization" in US East (N. Virginia) Inbox ×

AWS Notifications <no-reply@sns.amazonaws.com> 3:03 PM (0 minutes ago)
to me

You are receiving this email because your Amazon CloudWatch Alarm "CPUUtilization" in the US East (N. Virginia) region has entered the ALARM state, because "Threshold Crossed: 1 out of the last 1 datapoints [82.18778152213807 (2 greater than the threshold (70.0) (minimum 1 datapoint for OK -> ALARM transition)." at "Friday 23 January, 2026 09:33:02 UTC".

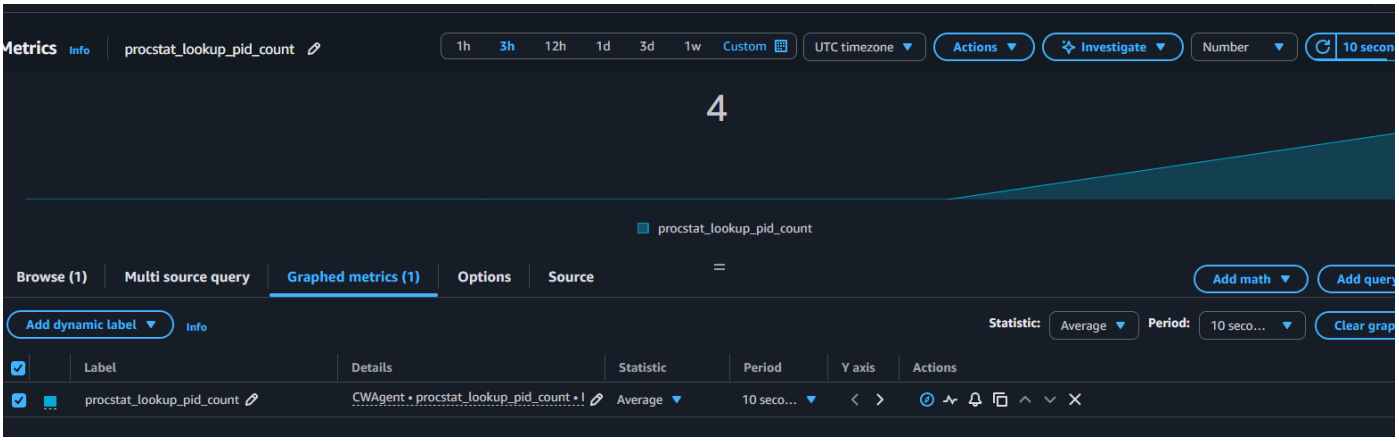
View this alarm in the AWS Management Console:
https://us-east-1.console.aws.amazon.com/cloudwatch/deeplink.js?region=us-east-1#alarmsV2:alarm/CPUUtilization

Alarm Details:
- Name: CPUUtilization
- Description: When load is >- 70%
- State Change: INSUFFICIENT_DATA -> ALARM
- Reason for State Change: Threshold Crossed: 1 out of the last 1 datapoints [82.18778152213807 (23/01/26 09:31:00)] was greater than the threshold (70.0) (minimum 1 datapoint for OK -> ALARM transition).
- Timestamp: Friday 23 January, 2026 09:33:02 UTC
- AWS Account: 526018540742
- Alarm Arn: arn:aws:cloudwatch:us-east-1:526018540742:alarm:CPUUtilization

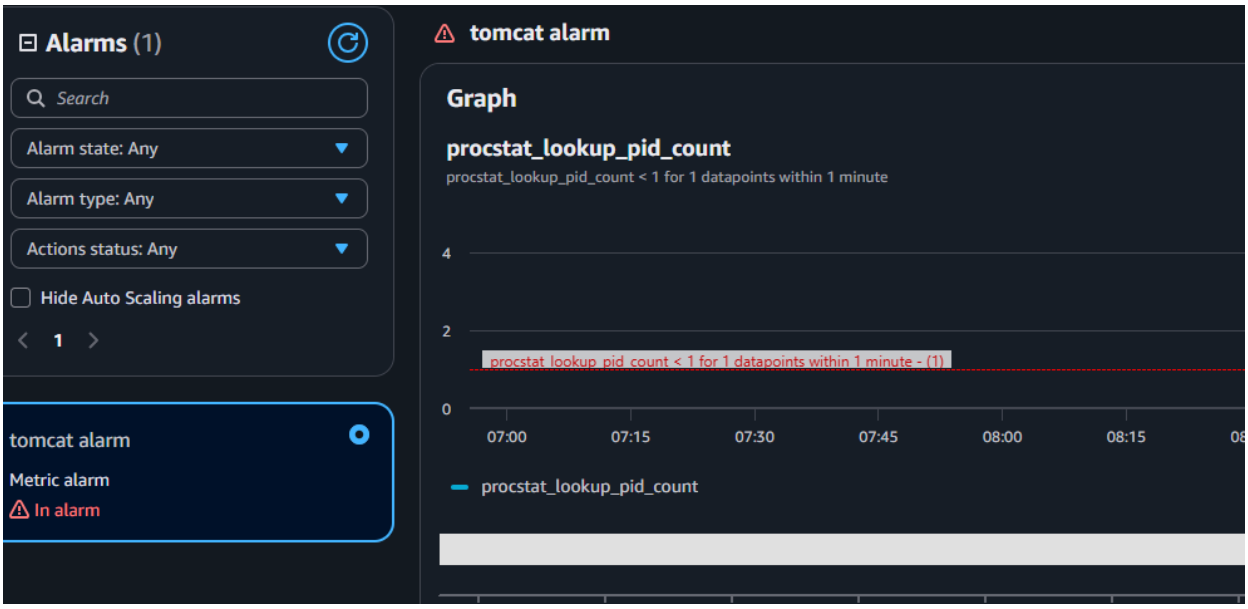
Threshold:
- The alarm is in the ALARM state when the metric is GreaterThanThreshold 70.0 for at least 1 of the last 1 period(s) of 60 seconds.

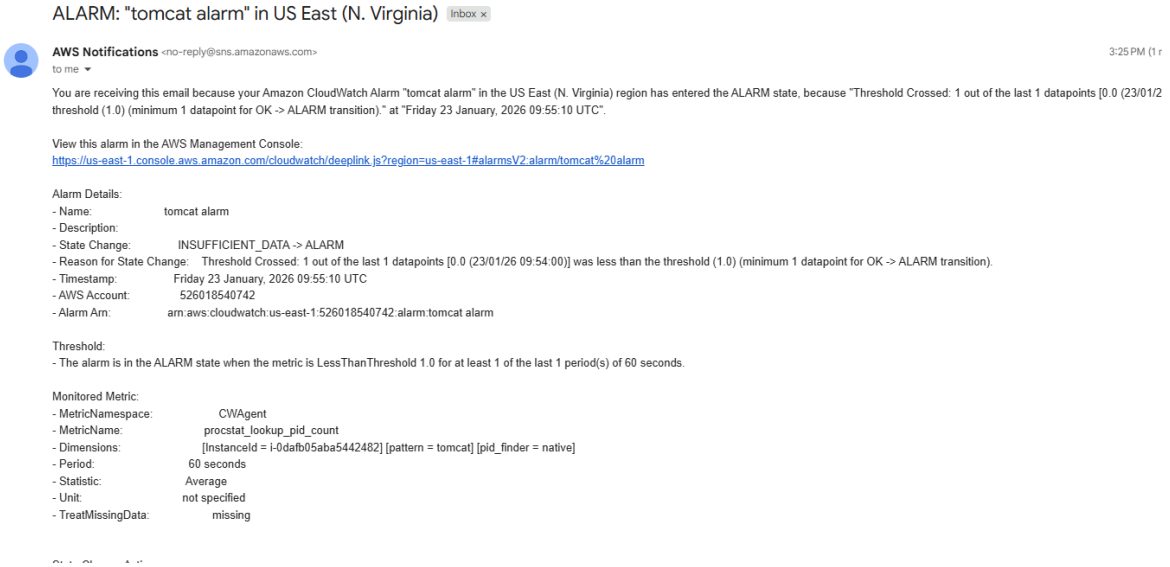
Monitored Metric:
- MetricNamespace: AWS/EC2
- MetricName: CPUUtilization
- Dimensions: [InstanceId = i-005d7dcbd67f0588e]
- Period: 60 seconds
- Statistic: Average
- Unit: not specified
- TreatMissingData: missing

- Create a Dashboard and monitor the Tomcat service whether it is running or not and send the alert.



CloudTrail & CloudWatch – Tasks 01





ALARM: "tomcat alarm" in US East (N. Virginia) Inbox ×

AWS Notifications <no-reply@sns.amazonaws.com> 3:25 PM (1 r
to me

You are receiving this email because your Amazon CloudWatch Alarm "tomcat alarm" in the US East (N. Virginia) region has entered the ALARM state, because "Threshold Crossed: 1 out of the last 1 datapoints [0.0 (23/01/2 threshold (1.0) (minimum 1 datapoint for OK -> ALARM transition)." at "Friday 23 January, 2026 09:55:10 UTC".

View this alarm in the AWS Management Console:
https://us-east-1.console.aws.amazon.com/cloudwatch/deeplink.js?region=us-east-1#alarmsV2:alarm/tomcat%20alarm

Alarm Details:
- Name: tomcat alarm
- Description:
- State Change: INSUFFICIENT_DATA -> ALARM
- Reason for State Change: Threshold Crossed: 1 out of the last 1 datapoints [0.0 (23/01/26 09:54:00)] was less than the threshold (1.0) (minimum 1 datapoint for OK -> ALARM transition).
- Timestamp: Friday 23 January, 2026 09:55:10 UTC
- AWS Account: 526018540742
- Alarm Arn: arn:aws:cloudwatch:us-east-1:526018540742:alarm:tomcat alarm

Threshold:
- The alarm is in the ALARM state when the metric is LessThanThreshold 1.0 for at least 1 of the last 1 period(s) of 60 seconds.

Monitored Metric:
- MetricNamespace: CWAgent
- MetricName: procstat_lookup_pid_count
- Dimensions: [InstanceId = i-0dafb05aba5442482] [pattern = tomcat] [pid_finder = native]
- Period: 60 seconds
- Statistic: Average
- Unit: not specified
- TreatMissingData: missing

CloudWatch cannot see OS processes by default

We use CloudWatch Agent + procstat

Create IAM Role and attach CloudWatchAgentServerPolicy, then attach the role to ec2.

Install CloudWatch Agent on your instance.

Create CloudWatch Agent Config (procstat)

Start CloudWatch Agent

Verify Tomcat Is Running

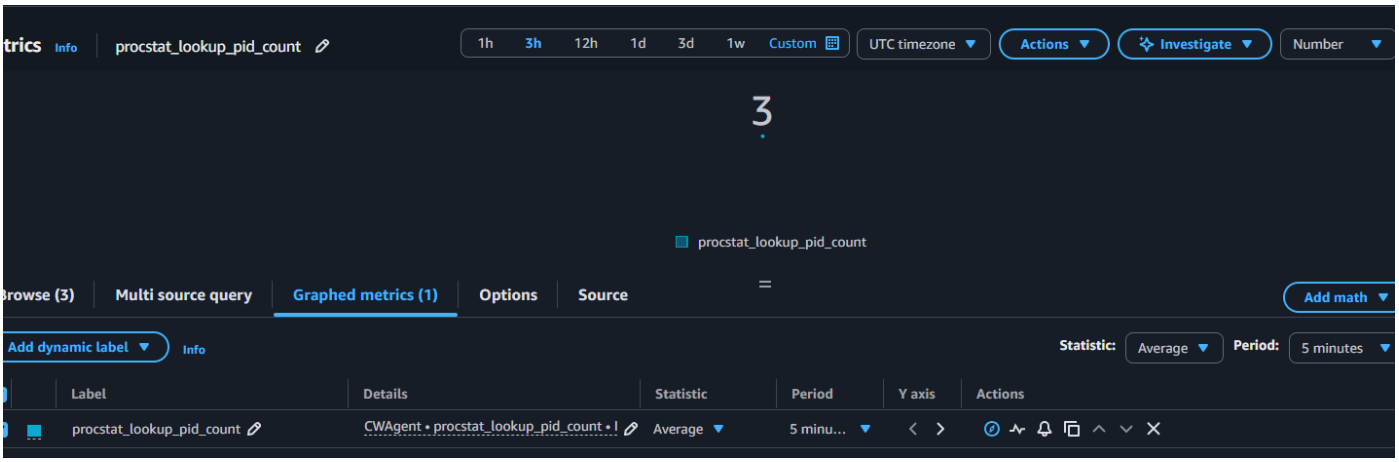
Verify Metrics in CloudWatch

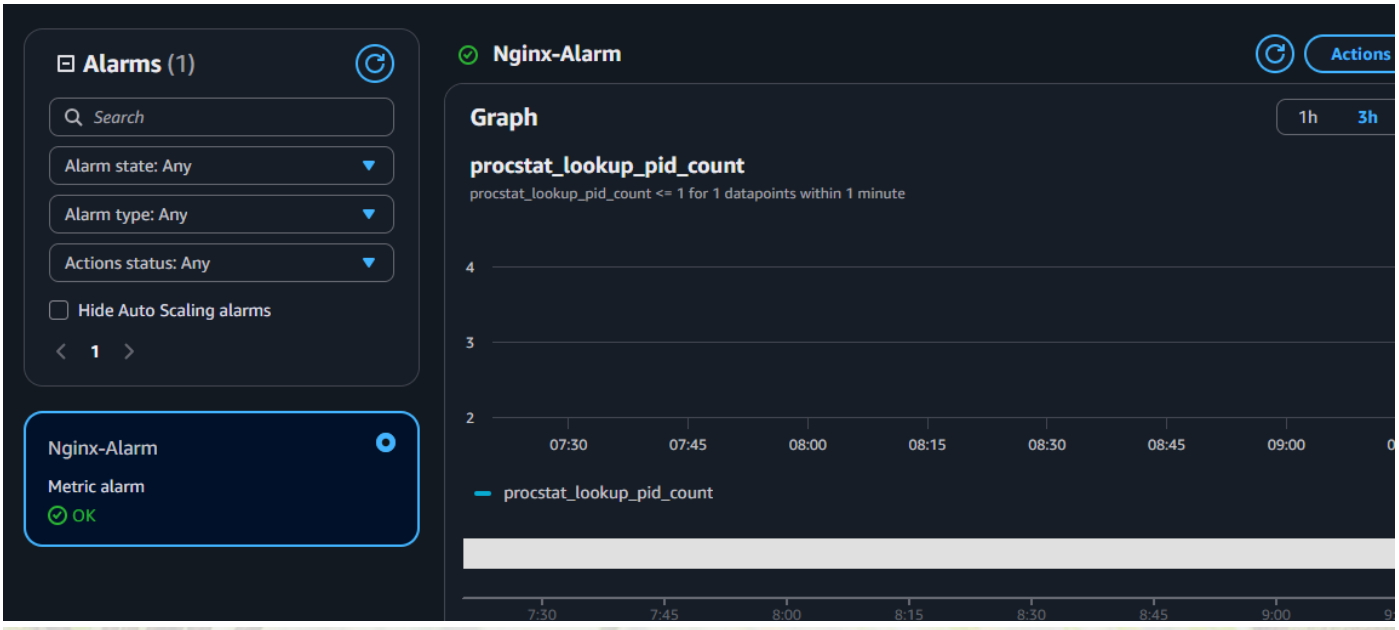
1 → Tomcat running

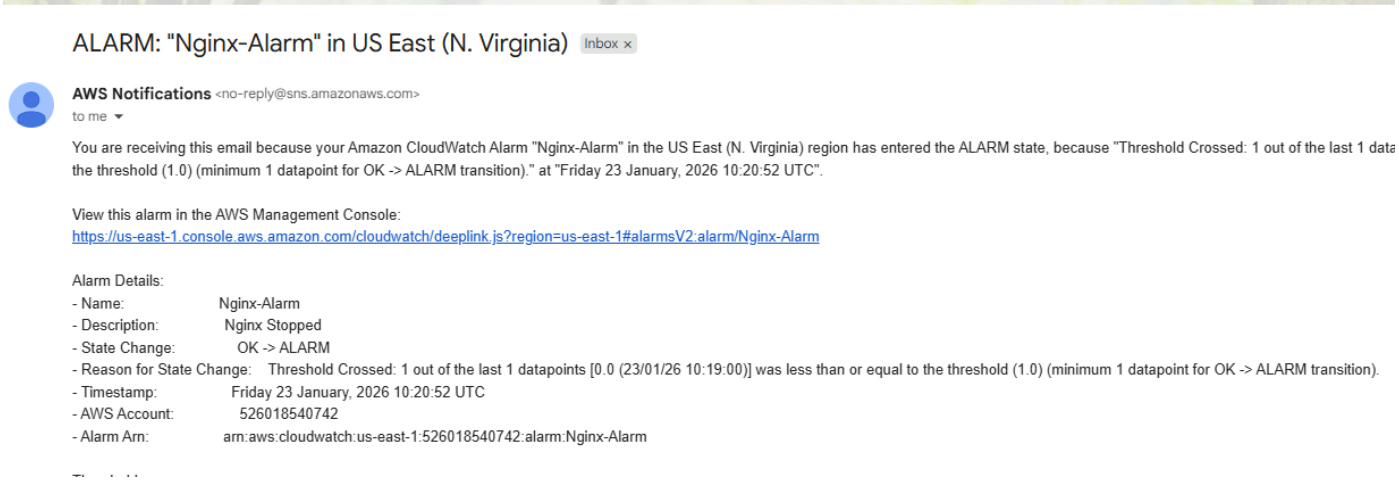
0 → Tomcat stopped

CloudTrail & CloudWatch – Tasks 01

- Create a Dashboard and monitor the Nginx service to send the alert if Nginx is not running.







ALARM: "Nginx-Alarm" in US East (N. Virginia) Inbox ×

AWS Notifications <no-reply@sns.amazonaws.com>
to me

You are receiving this email because your Amazon CloudWatch Alarm "Nginx-Alarm" in the US East (N. Virginia) region has entered the ALARM state, because "Threshold Crossed: 1 out of the last 1 data the threshold (1.0) (minimum 1 datapoint for OK -> ALARM transition)." at "Friday 23 January, 2026 10:20:52 UTC".

View this alarm in the AWS Management Console:
https://us-east-1.console.aws.amazon.com/cloudwatch/deeplink.js?region=us-east-1#alarmsV2:alarm/Nginx-Alarm

Alarm Details:
- Name: Nginx-Alarm
- Description: Nginx Stopped
- State Change: OK -> ALARM
- Reason for State Change: Threshold Crossed: 1 out of the last 1 datapoints [0.0 (23/01/26 10:19:00)] was less than or equal to the threshold (1.0) (minimum 1 datapoint for OK -> ALARM transition).
- Timestamp: Friday 23 January, 2026 10:20:52 UTC
- AWS Account: 526018540742
- Alarm Arn: arn:aws:cloudwatch:us-east-1:526018540742:alarm:Nginx-Alarm