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

**Go to the CloudTrail Console**: <https://console.aws.amazon.com/cloudtrail/>

Click **"Create trail"**.

**Trail name**: Provide a unique name.

**Storage location**:

* **Create a new S3 bucket** or use an existing one.

**CloudWatch Logs (Optional)**:

* Check **"Send to CloudWatch Logs"**.
* Create or use an existing **CloudWatch Logs group**.
* Specify or create an **IAM role** with appropriate permissions.

Click **Next**, then **Create trail**.

A screenshot of a computer

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.

**✅ Verification**

* Go to **S3**, navigate to your bucket, and check if logs are being created.
* Go to **CloudWatch Logs**, check under the log group if log streams are being populated.

A screenshot of a computer

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.

1. Enable SNS for cloudtrial to send alert on email.

**🔹 Step 1: Create an SNS Topic**

1. Go to the **SNS Console**:  
   👉 <https://console.aws.amazon.com/sns/>
2. Click **"Create topic"**
   * Type: Standard
   * Name: CloudTrailAlerts
3. Click **"Create topic"**

A screenshot of a computer

AI-generated content may be incorrect.

**🔹 Step 2: Subscribe an Email to the Topic**

1. Open the SNS topic you just created.
2. Click **“Create subscription”**
   * Protocol: Email
   * Endpoint: your email address (nithinreddy8811@gmail.com)
3. Click **“Create subscription”**
4. Check your email inbox and **confirm the subscription**

A screenshot of a computer

AI-generated content may be incorrect.

**🔹 Step 4: Send Alerts to SNS**

1. Under **Target**, select:
   * Target type: SNS topic
   * Topic: CloudTrailAlerts (your topic)
2. Click **"Next" → "Create rule"**

A screenshot of a computer

AI-generated content may be incorrect.

A screenshot of a computer error

AI-generated content may be incorrect.

You’ll now receive **email alerts** for any CloudTrail events that match your rule (like EC2 terminations, S3 deletions, etc.).

A screenshot of a computer

AI-generated content may be incorrect.

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

**Enable Detailed Monitoring (1-minute granularity)**

If you want **1-minute resolution**:

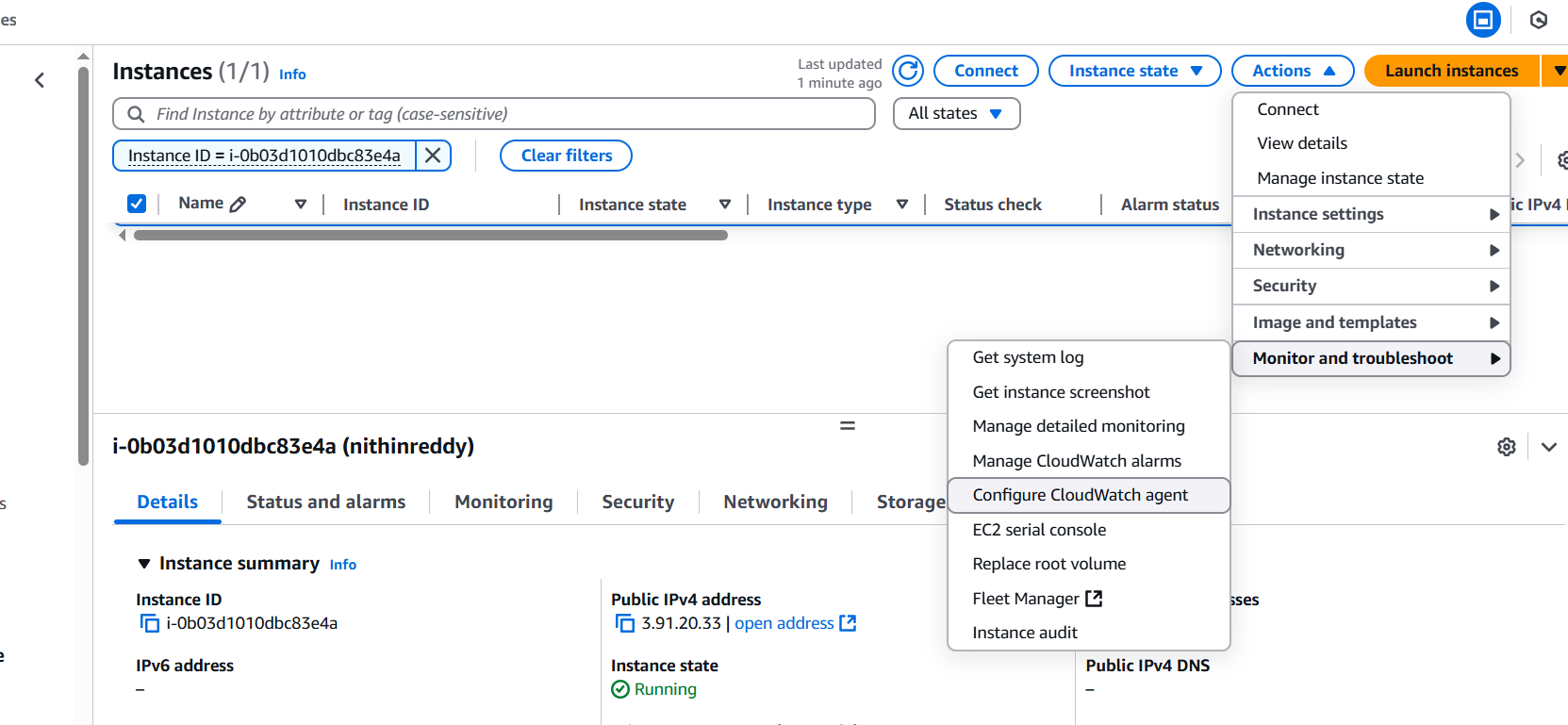
**Using AWS Console:**

Go to the **EC2 Console**.

Select your **EC2 instance**.

Click **Actions > Monitor and troubleshoot > Enable detailed monitoring**.

Confirm and save.



A screenshot of a computer

AI-generated content may be incorrect.

**View Metrics in CloudWatch**

**Using Console:**

1. Go to **CloudWatch Console** → Metrics.
2. Choose **EC2**.
3. Select **Per-Instance Metrics** or **Across Instances**.
4. View metrics like:
   * CPUUtilization
   * DiskReadBytes, DiskWriteBytes
   * NetworkIn, NetworkOut
   * StatusCheckFailed

A screenshot of a computer

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.

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

**Create the Alarm for High CPU**

1. Go to the **CloudWatch Console**  
   👉 <https://console.aws.amazon.com/cloudwatch/>
2. In the sidebar, click **“Alarms” > “Create alarm”**
3. Click **“Select metric”**
   * Choose: EC2 → Per-Instance Metrics
   * Select CPUUtilization
   * Choose the **InstanceId** you want to monitor
   * Click **“Select metric”**

A screenshot of a computer

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.

A screen shot of a graph

AI-generated content may be incorrect.

 Set the condition:

* **Threshold type**: Static
* **Whenever CPUUtilization is...** Greater than
* **Threshold value**: 70
* **For...** 1 out of 1 datapoints

 Click **Next**

A screenshot of a computer

AI-generated content may be incorrect.

**Attach the SNS Notification**

1. Under **Notification**, select:
   * **Send a notification to**: CPUAlerts (your SNS topic)
   * If it's not listed, click **“Create new topic”**, or use the ARN directly.
2. Click **Next**, name your alarm (e.g., HighCPU-Instance1), then **Create alarm**

A screenshot of a computer

AI-generated content may be incorrect.

**That’s It — Now You're Protected**

* You’ll receive an **email** any time CPU usage is over 70%.
* The alarm status will show:
  + OK: Normal
  + ALARM: Threshold breached
  + INSUFFICIENT\_DATA: Not enough recent data

A screenshot of a computer

AI-generated content may be incorrect.

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

**🔹 Step 1: Install and Configure CloudWatch Agent**

**Install the CloudWatch Agent (if not already installed)**

sudo yum install amazon-cloudwatch-agent -y

A screenshot of a computer

AI-generated content may be incorrect.

**Create CloudWatch Agent configuration file:**  
Save this file as /opt/aws/amazon-cloudwatch-agent/etc/amazon-cloudwatch-agent.json

{

"metrics": {

"append\_dimensions": {

"InstanceId": "${aws:InstanceId}"

},

"metrics\_collected": {

"procstat": [

{

"exe": "java",

"measurement": [

"cpu\_usage",

"memory\_rss"

],

"metrics\_collection\_interval": 60,

"custom\_dimensions": {

"Application": "Tomcat"

}

}

]

}

}

}

Apply and start the agent:

sudo /opt/aws/amazon-cloudwatch-agent/bin/amazon-cloudwatch-agent-ctl \

-a fetch-config \

-m ec2 \

-c file:/opt/aws/amazon-cloudwatch-agent/etc/amazon-cloudwatch-agent.json \

-s

A black background with white lines

AI-generated content may be incorrect.

🔹 **Step 2: Install and Start Apache Tomcat**

Download and extract the latest Tomcat:

wget https://downloads.apache.org/tomcat/tomcat-9/v9.0.105/bin/apache-tomcat-9.0.105.tar.gz

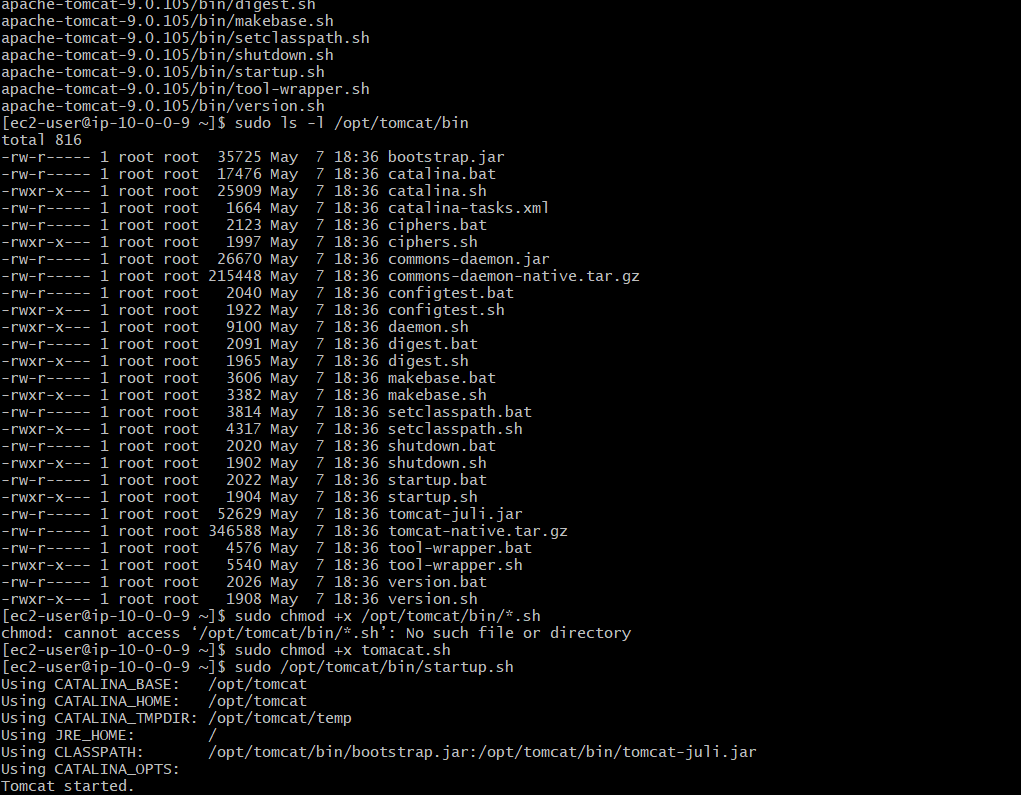
sudo mkdir -p /opt/tomcat

sudo tar -xvzf apache-tomcat-9.0.105.tar.gz -C /opt/tomcat --strip-components=1

sudo chmod +x /opt/tomcat/bin/\*.sh

sudo /opt/tomcat/bin/startup.sh

ps aux | grep tomcat



🔹 **Step 3: Push Custom Metric "TomcatStatus"**

**Create health check script:**  
Create /usr/local/bin/check\_tomcat.sh:

#!/bin/bash

if pgrep -f tomcat > /dev/null

then

/opt/aws/amazon-cloudwatch-agent/bin/amazon-cloudwatch-agent-ctl \

-a put-metric-data \

-n "Custom/Tomcat" \

-m "TomcatStatus" \

--value 1

else

/opt/aws/amazon-cloudwatch-agent/bin/amazon-cloudwatch-agent-ctl \

-a put-metric-data \

-n "Custom/Tomcat" \

-m "TomcatStatus" \

--value 0

Fi

sudo chmod +x /usr/local/bin/check\_tomcat.sh

Add it to crontab to run every minute:

crontab -e

\* \* \* \* \* /usr/local/bin/check\_tomcat.sh

A black screen with white text

AI-generated content may be incorrect.

**🔹 Step 4: Create IAM Role (If Not Already Done)**

1. Go to **IAM → Roles → Create Role**
2. Select **EC2** as trusted entity
3. Attach **CloudWatchAgentServerPolicy**
4. Attach the role to the EC2 instance

A screenshot of a computer

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.

A long line of colorful objects

AI-generated content may be incorrect.

**🔹 Step 5: View Custom Metric in CloudWatch**

1. Go to **CloudWatch Console**
2. Navigate to **Metrics → Custom → Custom/Tomcat**

A screenshot of a computer

AI-generated content may be incorrect.

**🔹 Step 6: Create CloudWatch Alarm**

1. Go to **CloudWatch → Alarms → Create Alarm**
2. Choose **Custom → Custom/Tomcat**
3. Select **TomcatStatus**
4. Set condition:
   * Whenever **TomcatStatus < 1** for **2 datapoints within 2 minutes**
5. Set **notification** to an **SNS Topic** (Email)
   * Confirm the subscription email if not done before
6. Name and create the alarm

A screenshot of a computer

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.

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

**🔹 Step 1: Install and Configure CloudWatch Agent**

1. **Install CloudWatch Agent (if not already installed):**

sudo yum install amazon-cloudwatch-agent -y

**Create CloudWatch Agent config file:**

sudo nano /opt/aws/amazon-cloudwatch-agent/etc/amazon-cloudwatch-agent.json

{

"metrics": {

"append\_dimensions": {

"InstanceId": "${aws:InstanceId}"

},

"metrics\_collected": {

"procstat": [

{

"exe": "nginx",

"measurement": [

"cpu\_usage",

"memory\_rss"

],

"metrics\_collection\_interval": 60,

"custom\_dimensions": {

"Application": "NGINX"

}

}

]

}

}

}

Start CloudWatch Agent with the config:

sudo /opt/aws/amazon-cloudwatch-agent/bin/amazon-cloudwatch-agent-ctl \

-a fetch-config \

-m ec2 \

-c file:/opt/aws/amazon-cloudwatch-agent/etc/amazon-cloudwatch-agent.json \

-s

🔹 **Step 2: Push NGINX Status Custom Metric**

**sudo nano /usr/local/bin/check\_nginx.sh**

**#!/bin/bash**

**if pgrep nginx > /dev/null**

**then**

**/usr/bin/aws cloudwatch put-metric-data \**

**--metric-name NGINXStatus \**

**--namespace Custom/NGINX \**

**--value 1 \**

**--dimensions InstanceID=$(curl -s http://169.254.169.254/latest/meta-data/instance-id)**

**else**

**/usr/bin/aws cloudwatch put-metric-data \**

**--metric-name NGINXStatus \**

**--namespace Custom/NGINX \**

**--value 0 \**

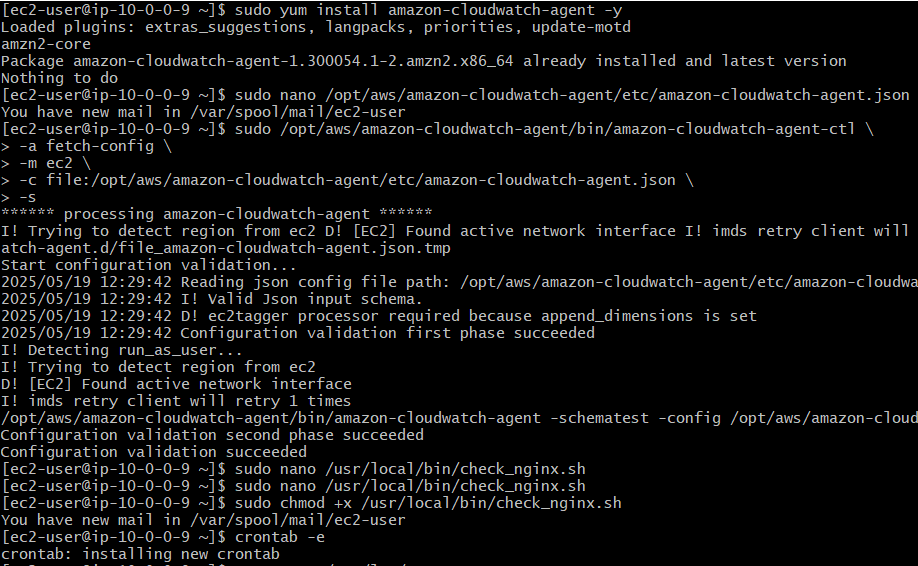
**--dimensions InstanceID=$(curl -s http://169.254.169.254/latest/meta-data/instance-id)**

**Fi**

**sudo chmod +x /usr/local/bin/check\_nginx.sh**

**crontab -e**

**\* \* \* \* \* /usr/local/bin/check\_nginx.sh**



A computer screen with text on it

AI-generated content may be incorrect.

**🔹 Step 3: Create IAM Role (if needed)**

1. **Go to IAM → Roles → Create Role**
2. **Select EC2**
3. **Attach policies:**
   * **CloudWatchAgentServerPolicy**
   * **CloudWatchFullAccess**
4. **Attach the role to your EC2 instance**

A screenshot of a computer

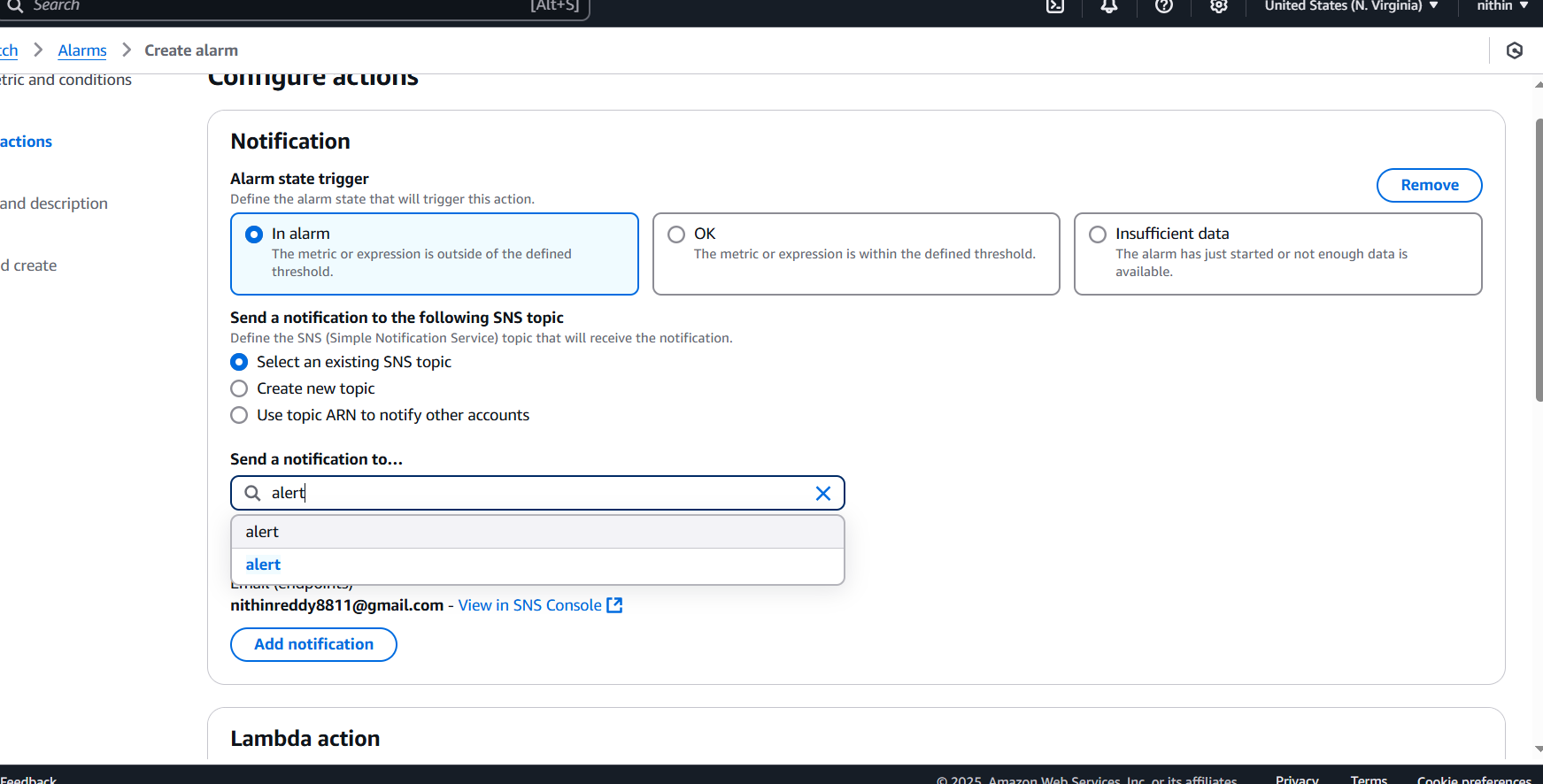
AI-generated content may be incorrect.

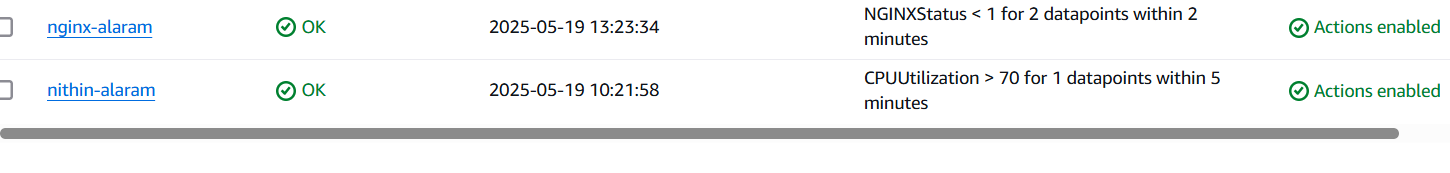
**🔹 Step 4: Create CloudWatch Alarm for NGINXStatus**

1. **Go to CloudWatch → Alarms → Create alarm**
2. **Choose Custom → Custom/NGINX**
3. **Select NGINXStatus**
4. **Condition:**
   * **Whenever NGINXStatus < 1 for 2 out of 2 datapoints**
5. **Set action:**
   * **Send notification to SNS topic**
   * **(Create topic and subscribe email if not already done)**
6. **Name and create the alarm**

A screenshot of a computer

AI-generated content may be incorrect.





**🔹 Step 5: Create CloudWatch Dashboard**

1. Go to **CloudWatch → Dashboards → Create dashboard**
2. Name it e.g. NGINX-Monitor
3. Add a widget:
   * Type: **Line graph**
   * Source: **Custom/NGINX**
   * Metric: **NGINXStatus**
   * Dimension: **InstanceID**
4. Customize widget title and layout
5. Save the dashboard

A screenshot of a login box

AI-generated content may be incorrect.