# **TRIGGER LAMBDA FUNCTION BASED ON CLOUD-WATCH FILTER PATTERN**

**OVERVIEW:**

* Create an EC2 instance and install a cloud watch agent to access logs of the application.
* Create SNS topic and subscription , then confirm subscription through email provided.
* Create a lambda function and add an IAM role to it.
* Provide the code to lambda and run it.

**STEP 1: LAUNCH EC2 AND INSTALL CLOUD WATCH AGENT USING CLOUD WATCH AGENT WIZARD**

In this case,we are using default nginx page, and monitor logs based on the number of times the page is visited and access a specific keyword from the log.

* Launch an EC2 instance and connect to it.
* Update the instance:

→Sudo apt update

* Install Nginx :

→sudo apt install nginx -y

* Download the CloudWatch Agent installer:

→ wget <https://s3.amazonaws.com/amazoncloudwatch-agent/ubuntu/amd64/latest/amazon-cloudwatch-agent.deb>

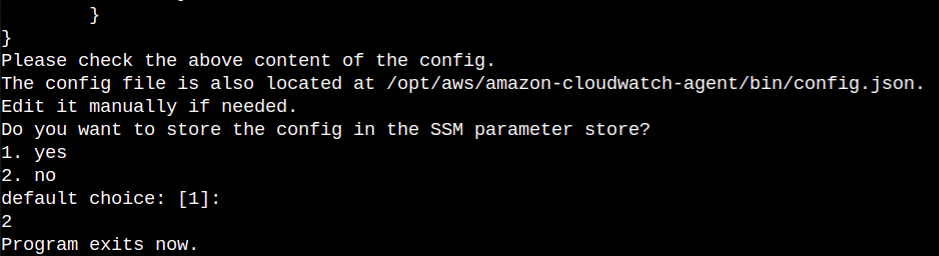
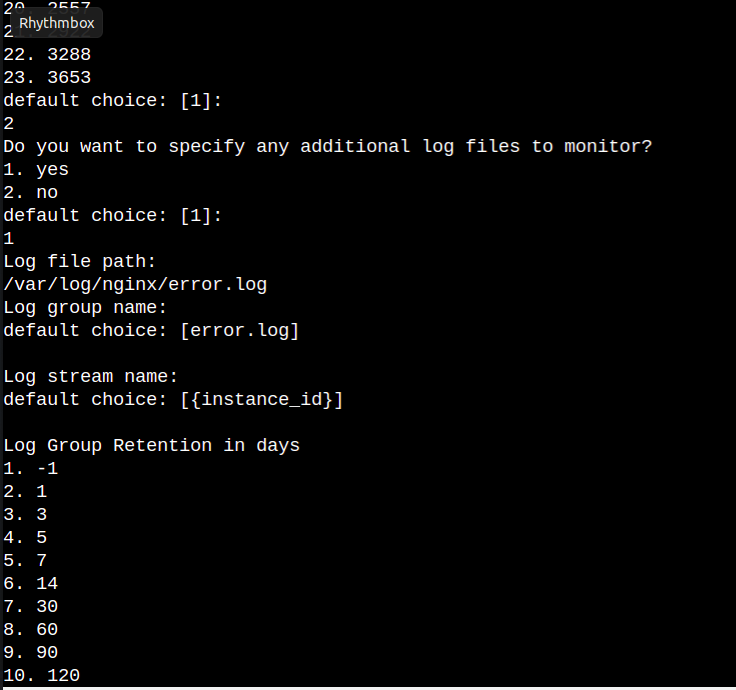
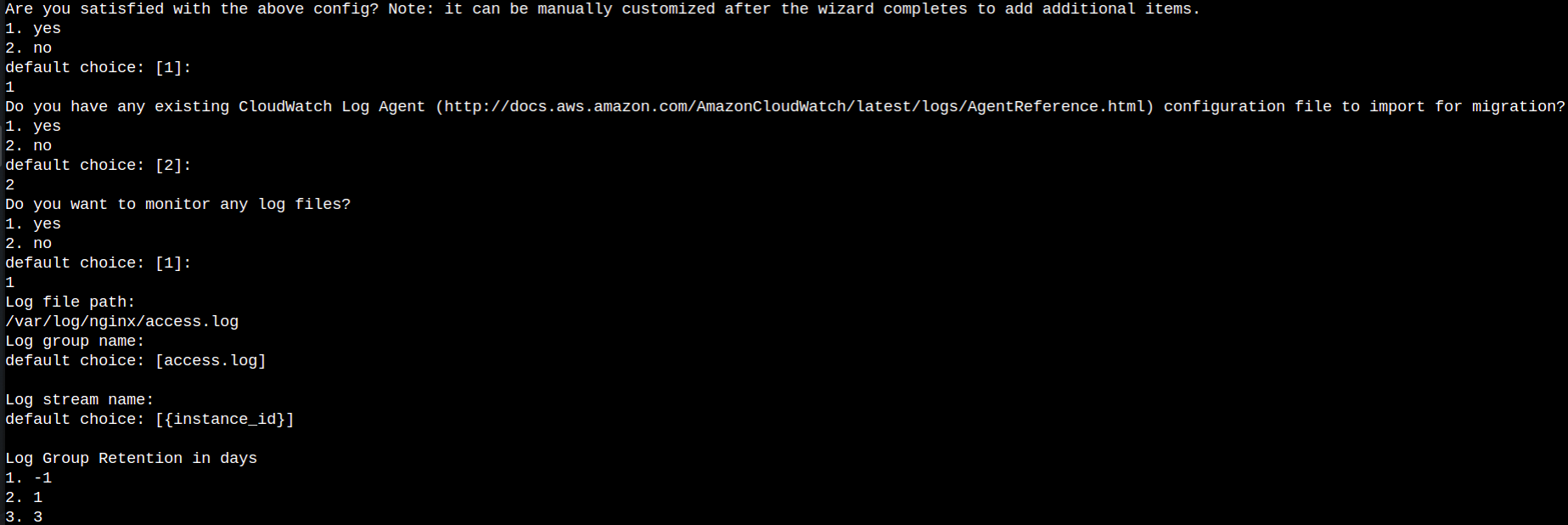
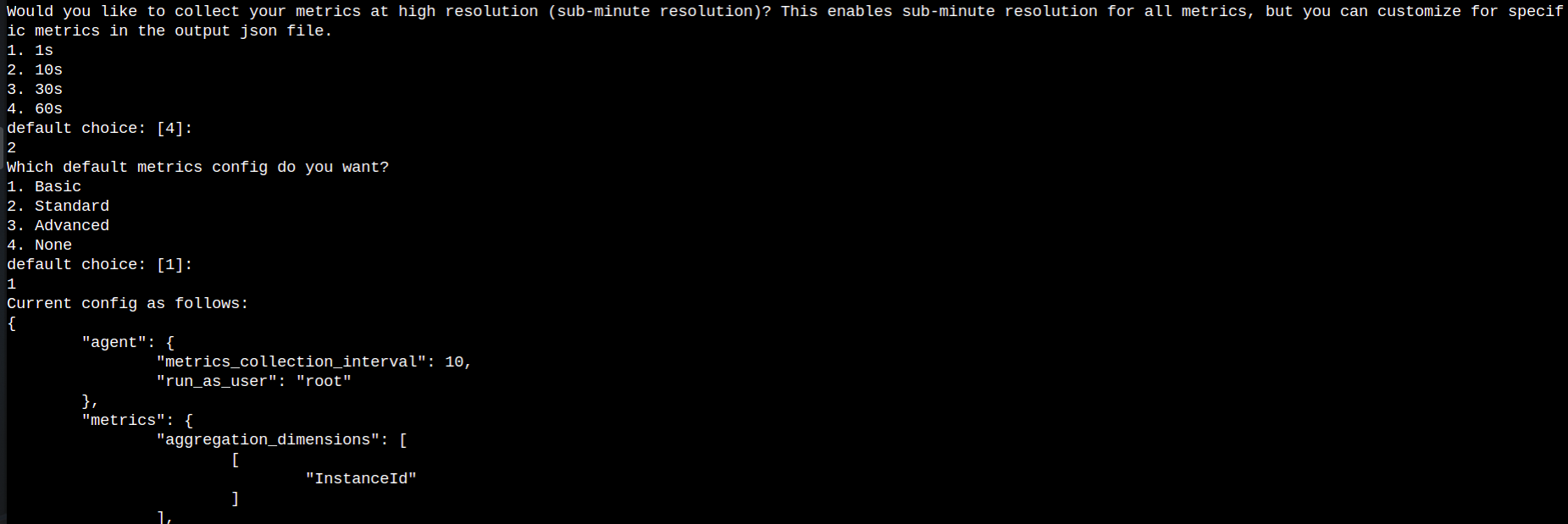
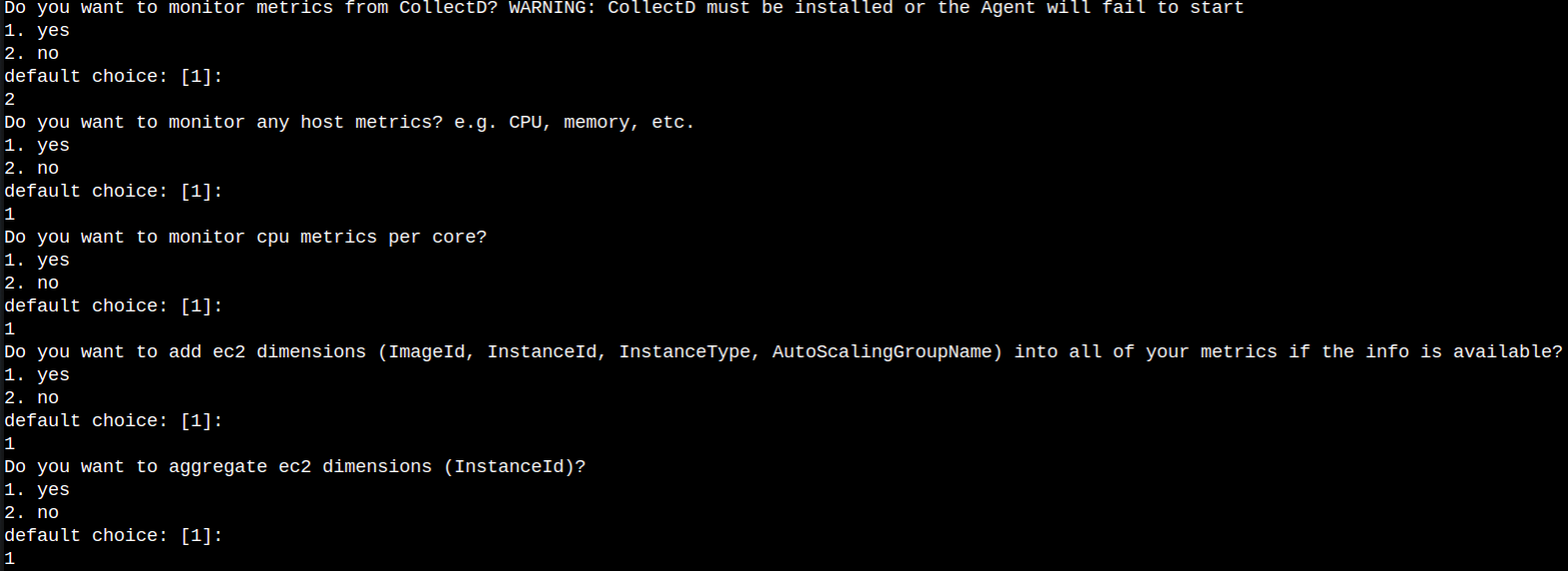
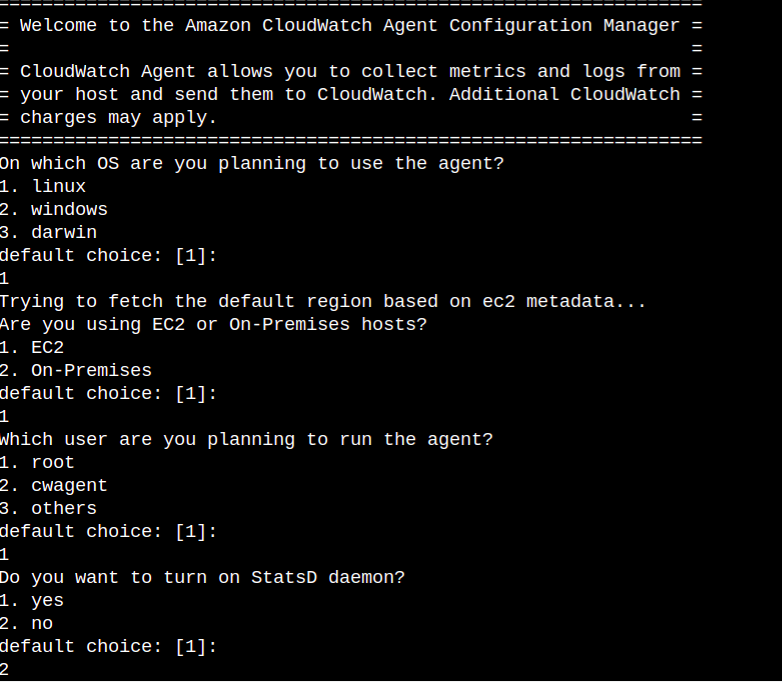
* Install the CloudWatch Agent:

→sudo dpkg -i amazon-cloudwatch-agent.deb

* Run the following command to start the configuration wizard:

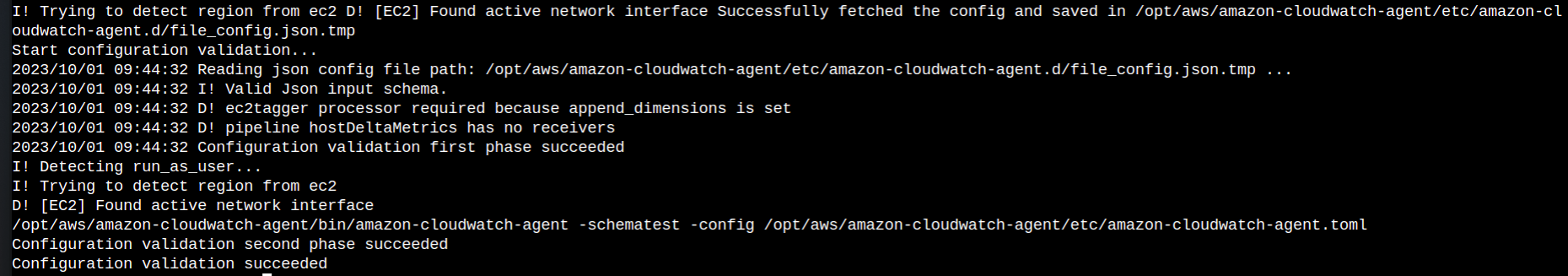
→ sudo /opt/aws/amazon-cloudwatch-agent/bin/amazon-cloudwatch-agent-config-wizard

* Follow the instructions from the images given below:

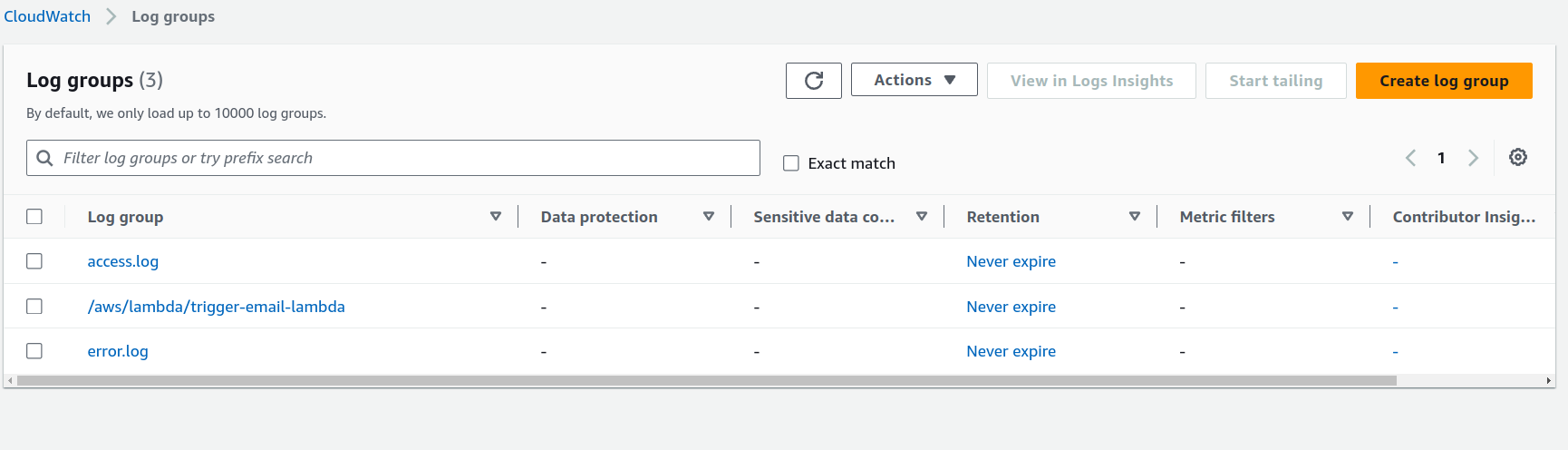


* This configures the cloud watch agent on EC2 instance, important configuration during this, is to provide the path for the log files.
* This command is used by the Cloud watch agent to fetch the log files and provide it to cloud watch log group:

→ sudo /opt/aws/amazon-cloudwatch-agent/bin/amazon-cloudwatch-agent-ctl -a fetch-config -m ec2 -c file:/opt/aws/amazon-cloudwatch-agent/bin/config.json -sfile:/opt/aws/amazon-cloudwatch-agent/bin/config.json -s



* Check the cloud watch log group,we should have both **access.log** and **error.log** of nginx inside the **Log groups** of cloud watch.



**STEP 2: CREATE LAMBDA FUNCTION AND ADD CLOUD-WATCH TRIGGER TO IT**

* Create a lambda function with **python 3.10** or any latest python runtime.
* Copy and paste the code inside code section of lambda:

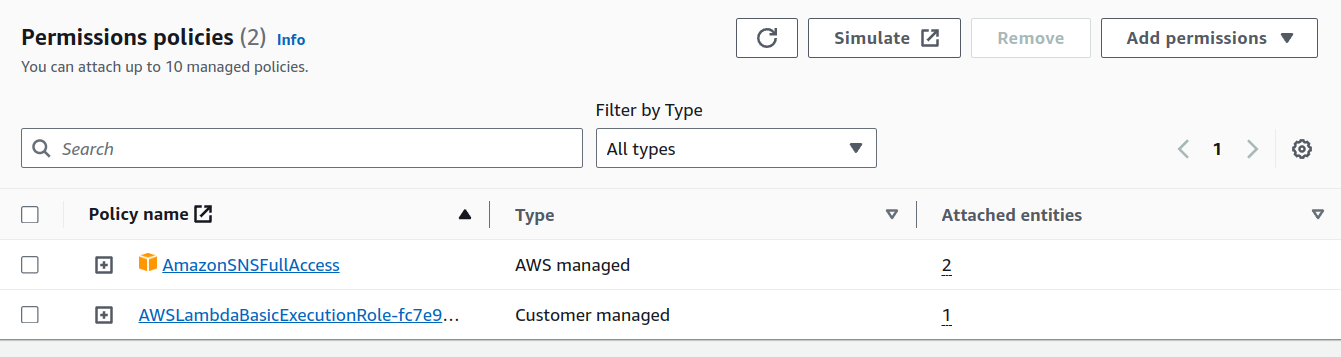
<https://github.com/srcecde/aws-tutorial-code/blob/master/lambda/lambda_proces_cw_error_notification.py>

* ADD THE IAM ROLE TO LAMBDA :

→ Click on configuration>Permissions

→ Under **role name,** click on the role link

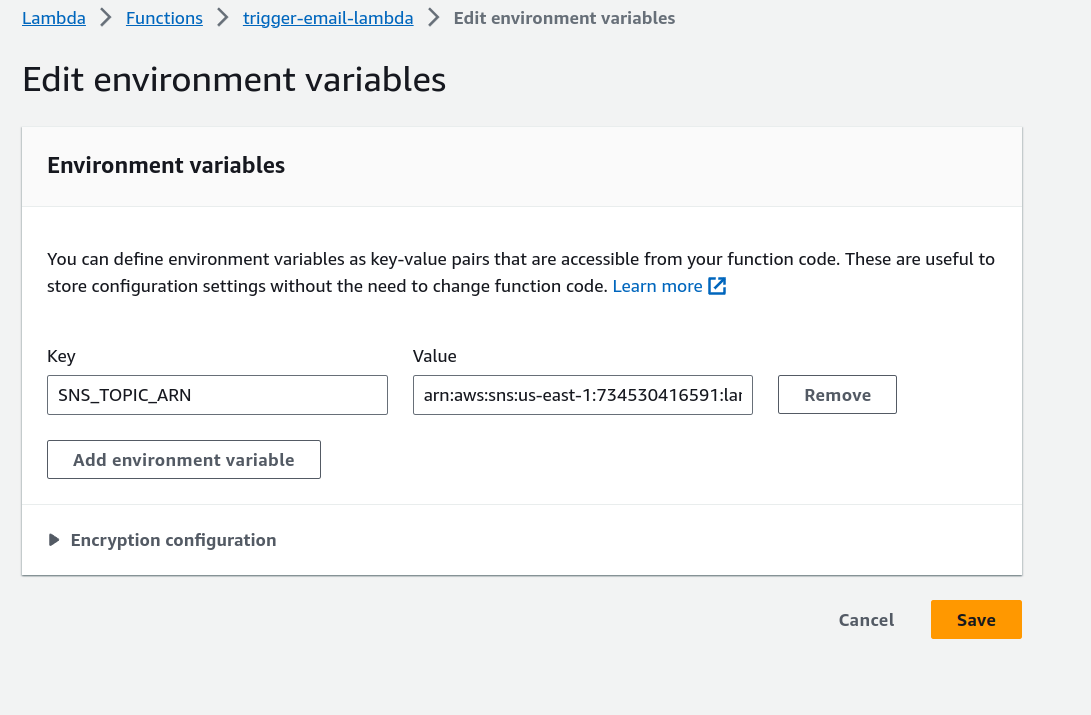
→ Add SNSFullAccess Permission role to lambda



* ADD ENVIRONMENT VARIABLE OF SNS TOPIC ARN:

→ Click on configuration>Environment Variable

→ Add the Environment variable



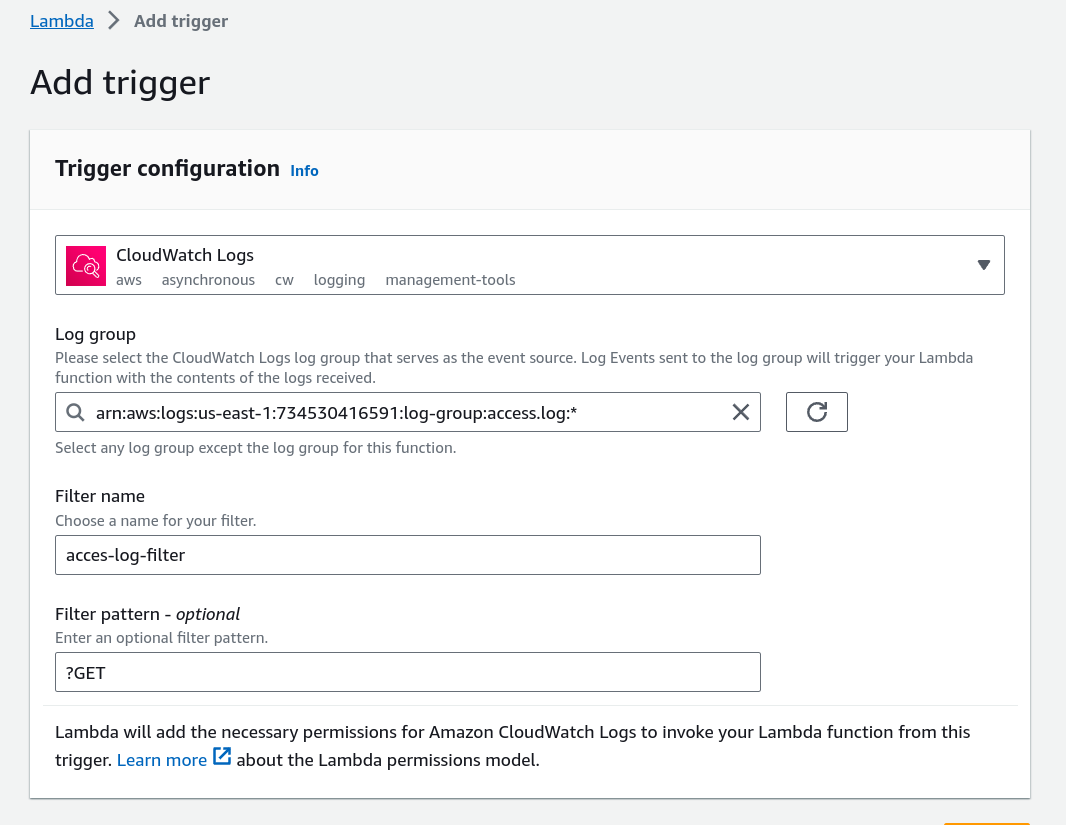
* ADD TRIGGER FOR CLOUD WATCH LOGS:

→Click on **Add Trigger** inside the lambda function created.

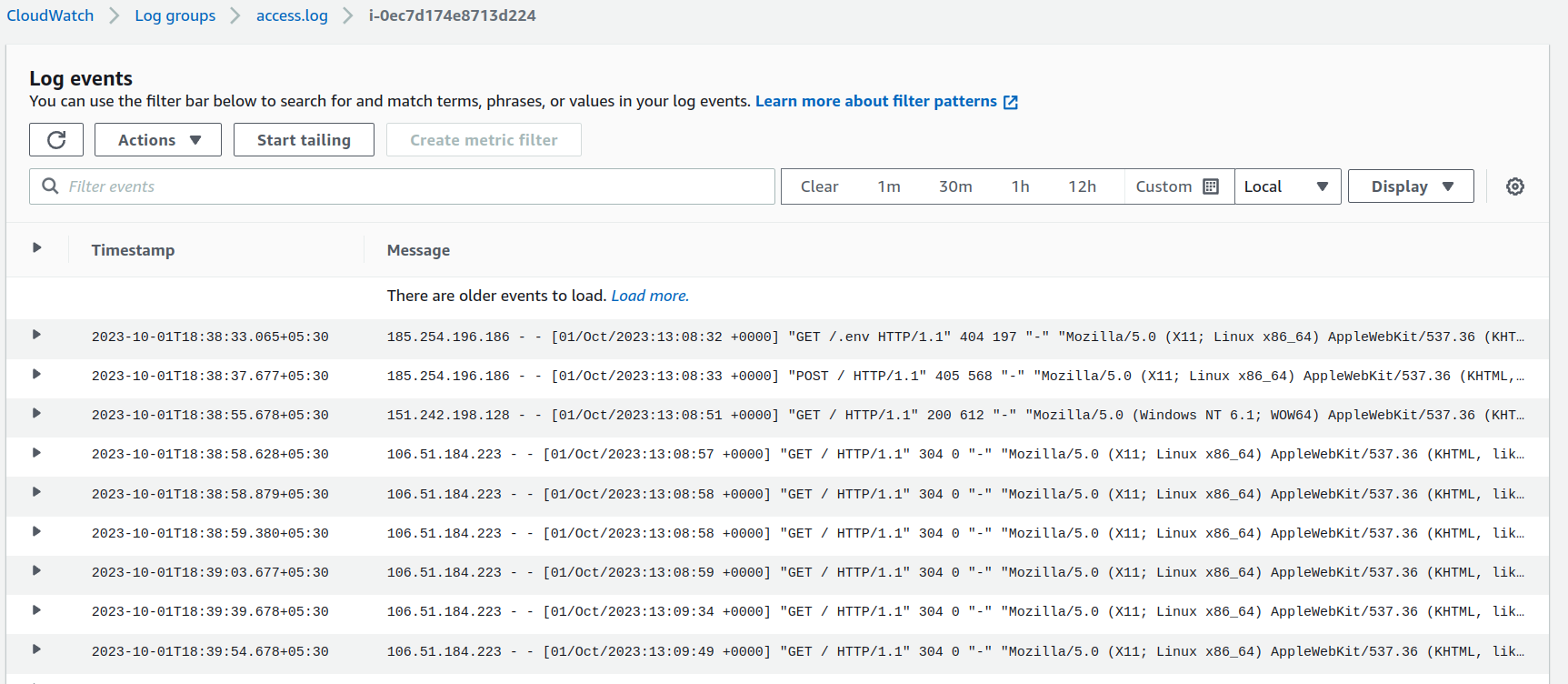
→ Choose the selected options from the below image.

→ Select the **log group** and set the **Filter Pattern.**

**→** In this case,we use “ **?GET** ” because it is the word which will occur when we refresh the nginx default page using the ip-address of the instance.



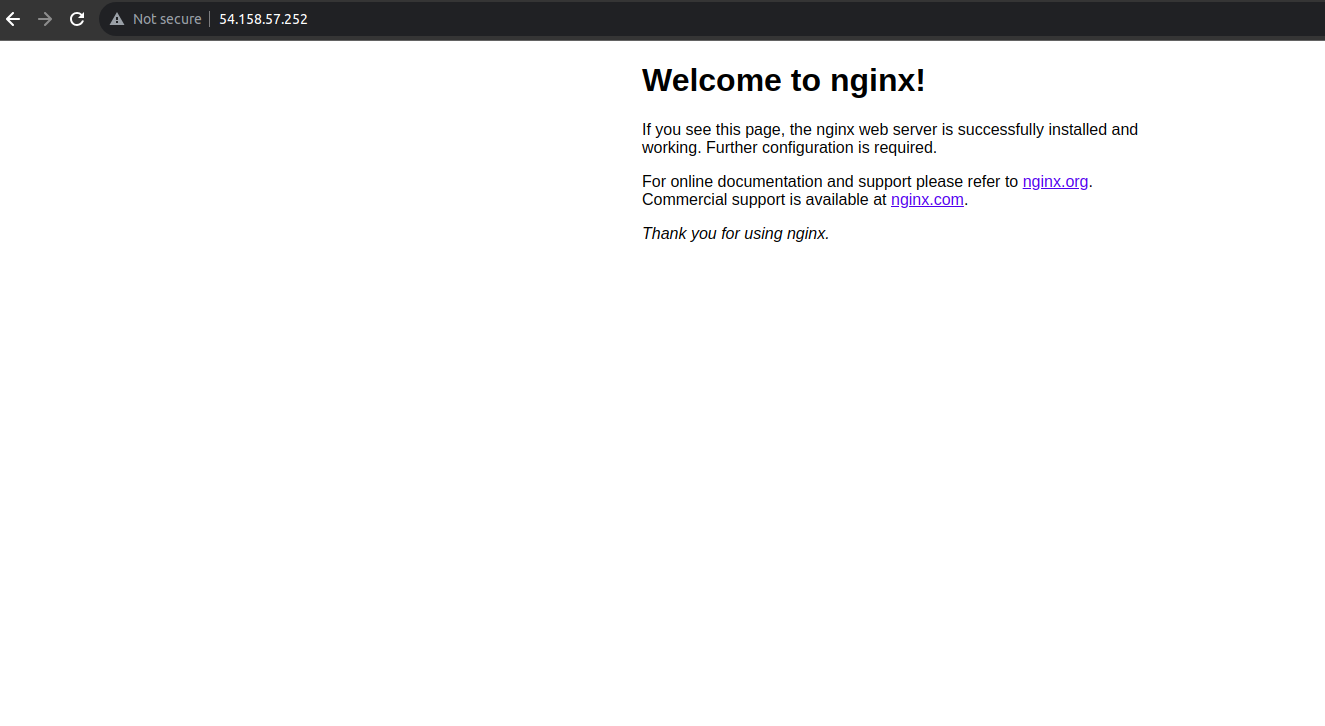
* This image shows the logs from **access.log.**



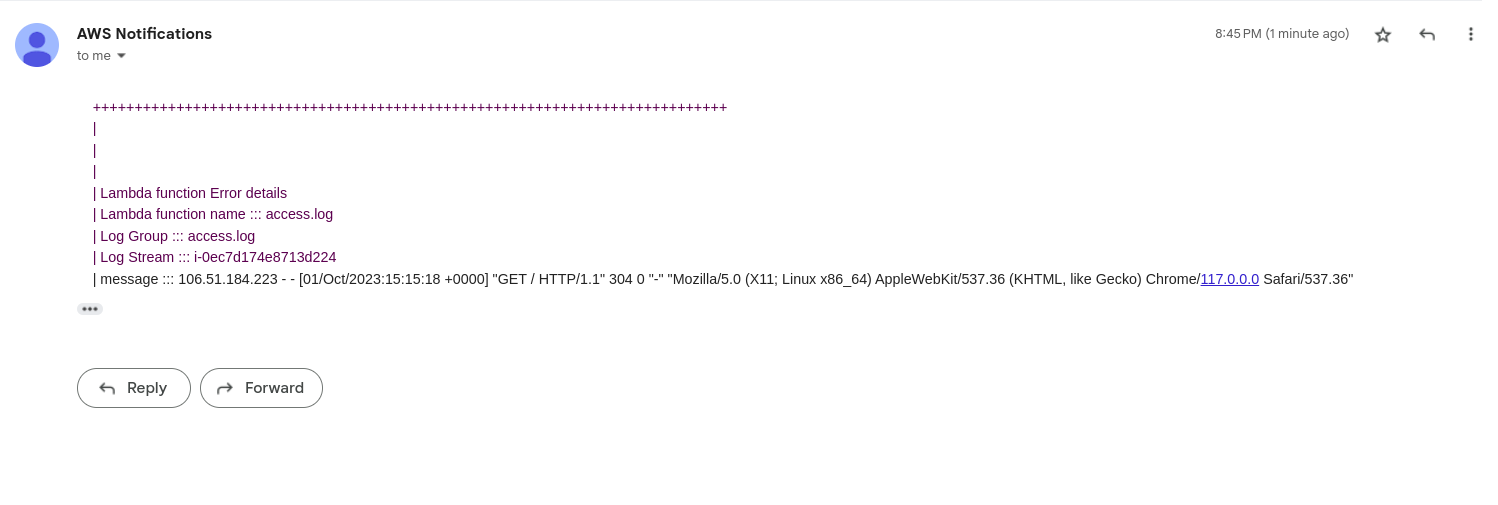
* Go back to the **Code** section and Click on **Deploy** code.

**STEP 3:**

* Now copy the ip-address of EC2 instance and paste it in browser.



* Open the email and check for notification



* We will get the email and also the log line which triggered the email.
* Check the access log and also the lambda log group to check if the triggered log is available.