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

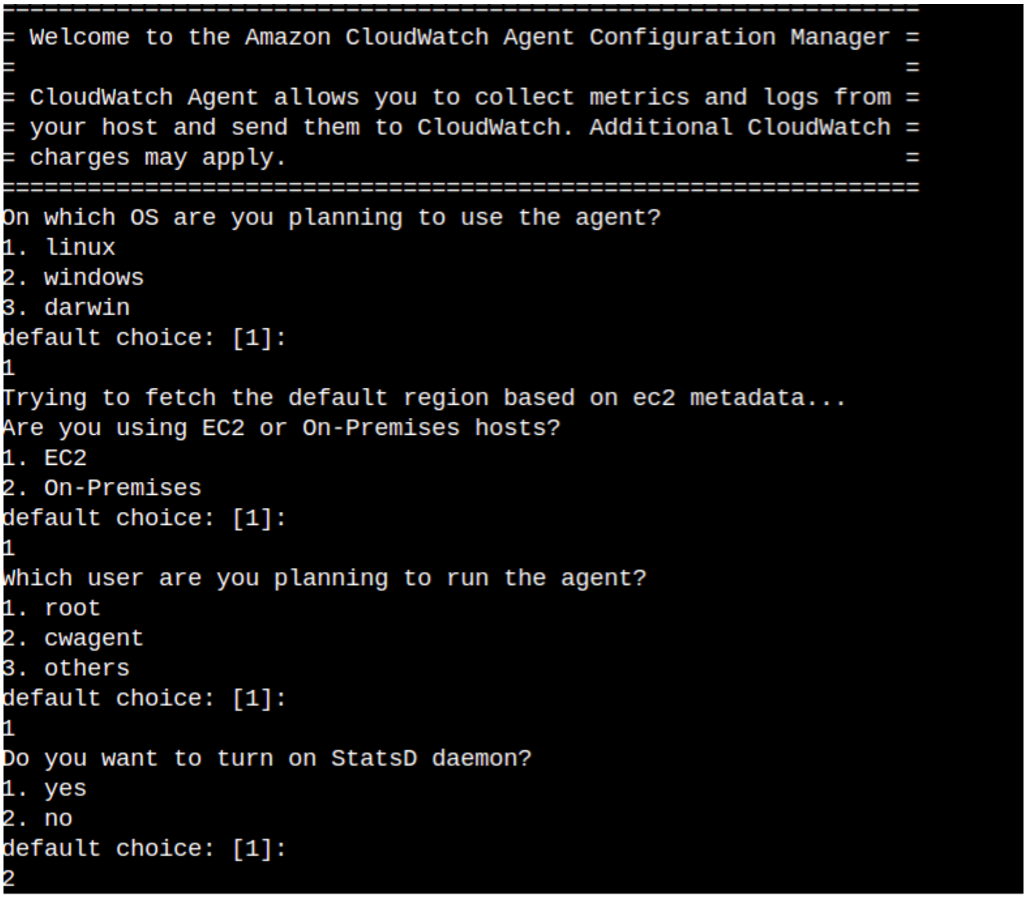
- Install the CloudWatch Agent:

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

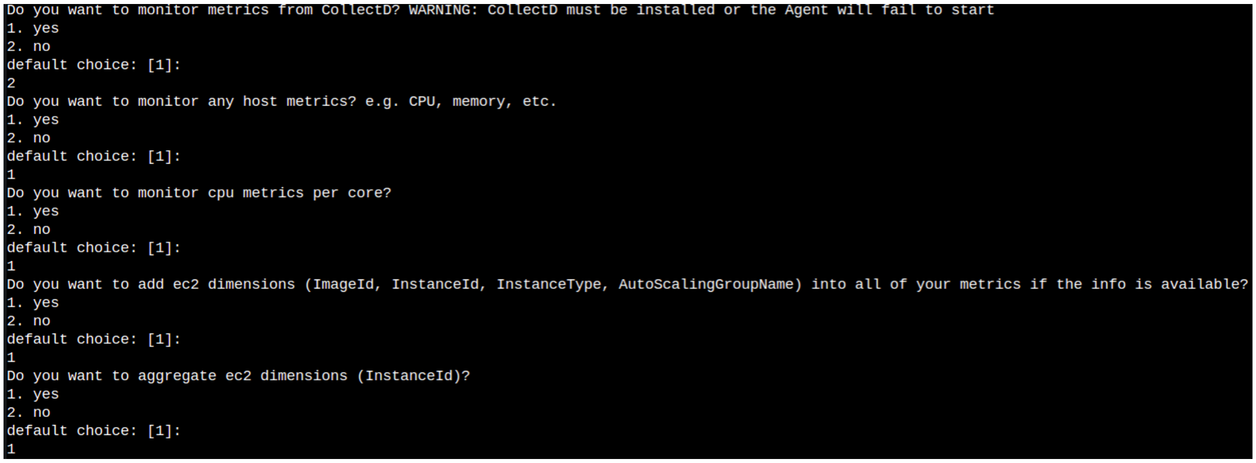
- Run the following command to start the configuration wizard:

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

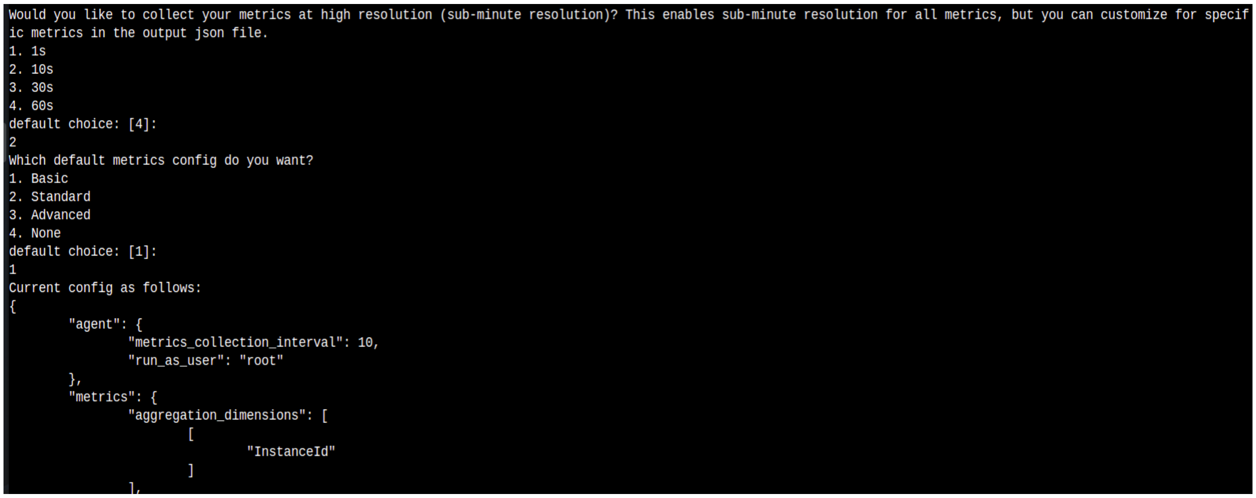
- Follow the instructions from the images given below:



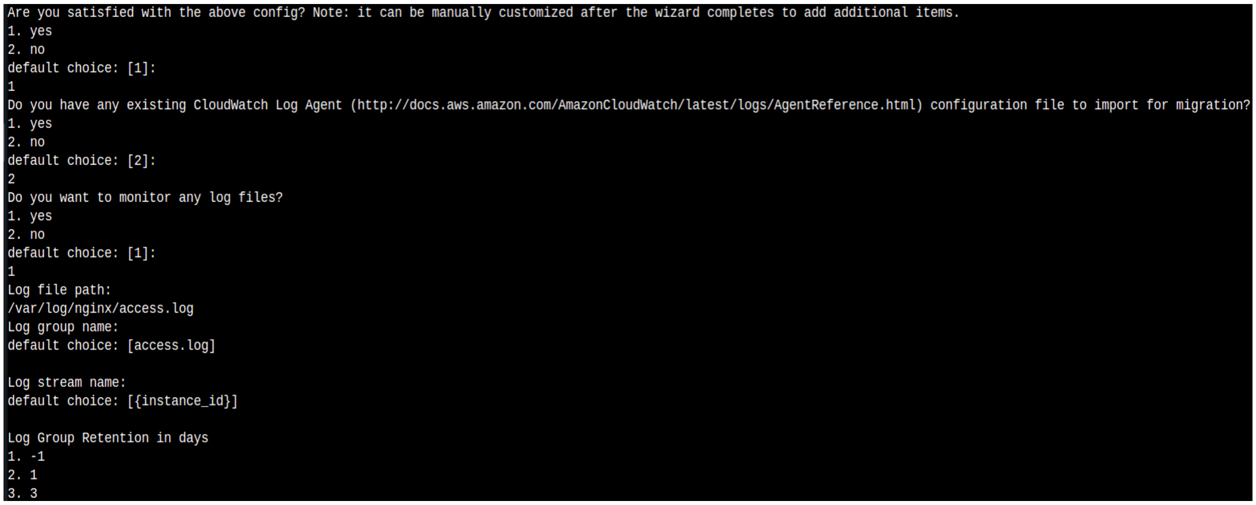
```
==============================================================
= Welcome to the Amazon CloudWatch Agent Configuration Manager =
=                                                            =
= CloudWatch Agent allows you to collect metrics and logs from =
= your host and send them to CloudWatch. Additional CloudWatch =
= charges may apply.                                         =
==============================================================
On which OS are you planning to use the agent?
1. linux
2. windows
3. darwin
default choice: [1]:
1
Trying to fetch the default region based on ec2 metadata...
Are you using EC2 or On-Premises hosts?
1. EC2
2. On-Premises
default choice: [1]:
1
Which user are you planning to run the agent?
1. root
2. cwagent
3. others
default choice: [1]:
1
Do you want to turn on StatsD daemon?
1. yes
2. no
default choice: [1]:
2
```



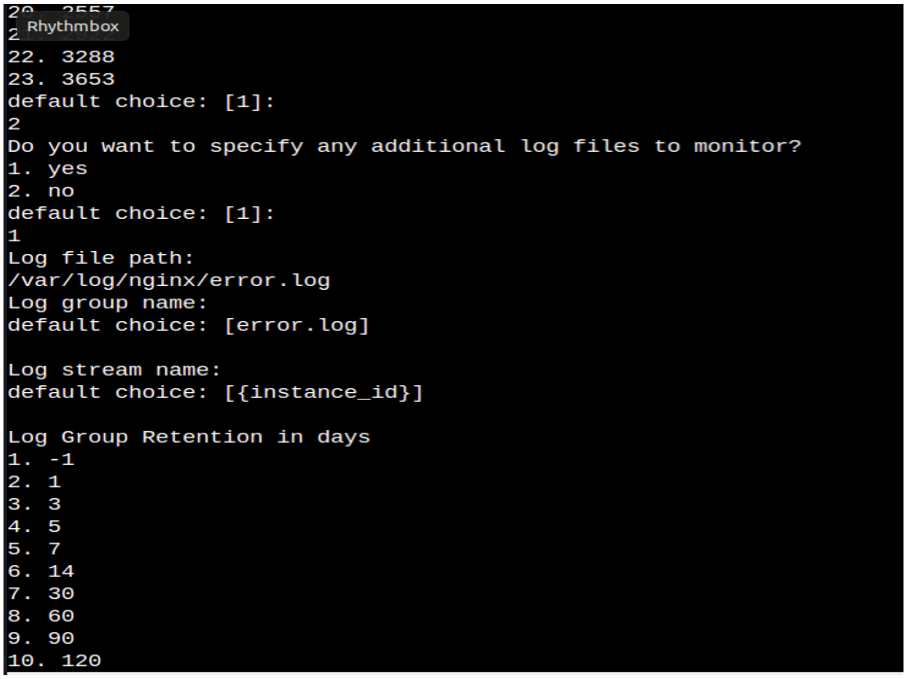
```
Do you want to monitor metrics from CollectD? WARNING: CollectD must be installed or the Agent will fail to start
1. yes
2. no
default choice: [1]:
2
Do you want to monitor any host metrics? e.g. CPU, memory, etc.
1. yes
2. no
default choice: [1]:
1
Do you want to monitor cpu metrics per core?
1. yes
2. no
default choice: [1]:
1
Do you want to add ec2 dimensions (ImageId, InstanceId, InstanceType, AutoScalingGroupName) into all of your metrics if the info is available?
1. yes
2. no
default choice: [1]:
1
Do you want to aggregate ec2 dimensions (InstanceId)?
1. yes
2. no
default choice: [1]:
1
```



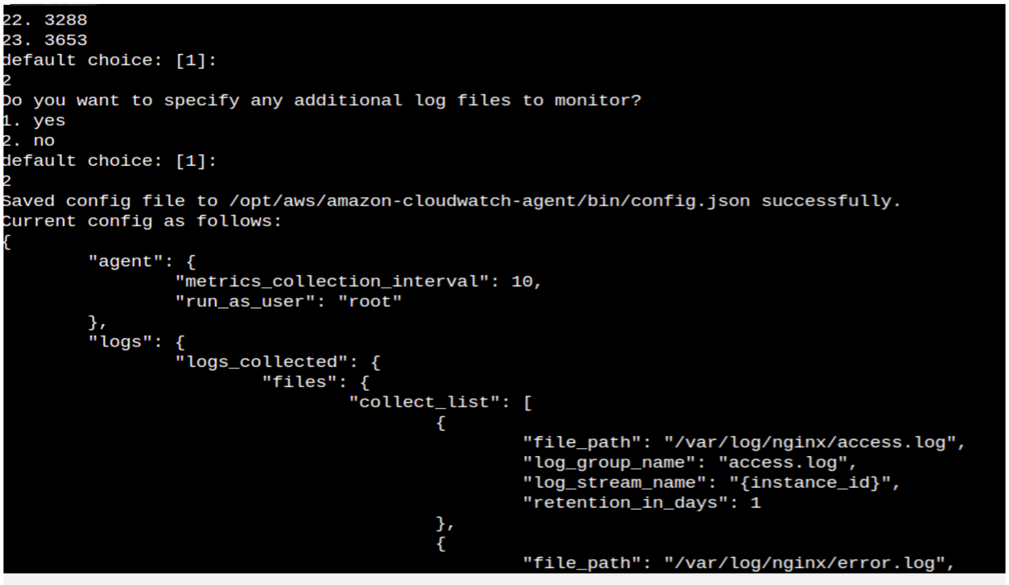
```
Would you like to collect your metrics at high resolution (sub-minute resolution)? This enables sub-minute resolution for all metrics, but you can customize for specif
ic metrics in the output json file.
1. 1s
2. 10s
3. 30s
4. 60s
default choice: [4]:
2
Which default metrics config do you want?
1. Basic
2. Standard
3. Advanced
4. None
default choice: [1]:
1
Current config as follows:
{
        "agent": {
                "metrics_collection_interval": 10,
                "run_as_user": "root"
        },
        "metrics": {
                "aggregation_dimensions": [
                        [
                                "InstanceId"
                        ]
                ],
```



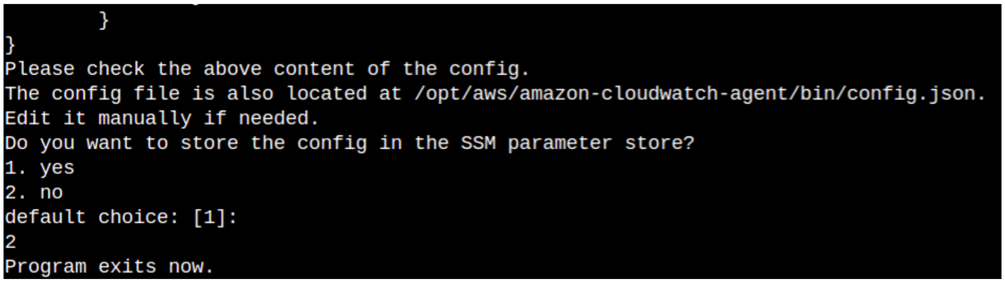
```
Are you satisfied with the above config? Note: it can be manually customized after the wizard completes to add additional items.
1. yes
2. no
default choice: [1]:
1
Do you have any existing CloudWatch Log Agent (http://docs.aws.amazon.com/AmazonCloudWatch/latest/logs/AgentReference.html) configuration file to import for migration?
1. yes
2. no
default choice: [2]:
2
Do you want to monitor any log files?
1. yes
2. no
default choice: [1]:
1
Log file path:
/var/log/nginx/access.log
Log group name:
default choice: [access.log]

Log stream name:
default choice: [{instance_id}]

Log Group Retention in days
1. -1
2. 1
3. 3
```



```
20. 2557
21. 2922
22. 3288
23. 3653
default choice: [1]:
2
Do you want to specify any additional log files to monitor?
1. yes
2. no
default choice: [1]:
1
Log file path:
/var/log/nginx/error.log
Log group name:
default choice: [error.log]

Log stream name:
default choice: [{instance_id}]

Log Group Retention in days
1. -1
2. 1
3. 3
4. 5
5. 7
6. 14
7. 30
8. 60
9. 90
10. 120
```



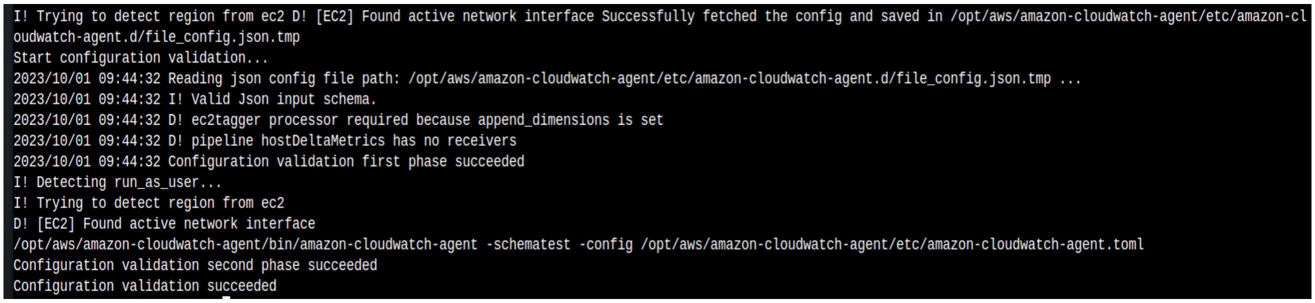
```
22. 3288
23. 3653
default choice: [1]:
2
Do you want to specify any additional log files to monitor?
1. yes
2. no
default choice: [1]:
2
Saved config file to /opt/aws/amazon-cloudwatch-agent/bin/config.json successfully.
Current config as follows:
{
        "agent": {
                "metrics_collection_interval": 10,
                "run_as_user": "root"
        },
        "logs": {
                "logs_collected": {
                        "files": {
                                "collect_list": [
                                        {
                                                "file_path": "/var/log/nginx/access.log",
                                                "log_group_name": "access.log",
                                                "log_stream_name": "{instance_id}",
                                                "retention_in_days": 1
                                        },
                                        {
                                                "file_path": "/var/log/nginx/error.log",
```



```
        }
}
Please check the above content of the config.
The config file is also located at /opt/aws/amazon-cloudwatch-agent/bin/config.json.
Edit it manually if needed.
Do you want to store the config in the SSM parameter store?
1. yes
2. no
default choice: [1]:
2
Program exits now.
```

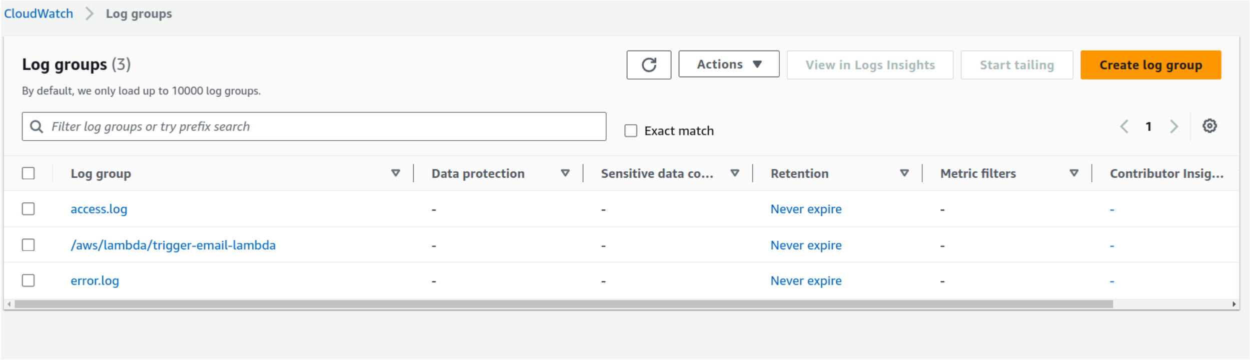
- This configures the cloud watch agent on EC2 instance, important configuration during this, is to provide the path for the log files.

- 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



```
I! Trying to detect region from ec2 D! [EC2] Found active network interface Successfully fetched the config and saved in /opt/aws/amazon-cloudwatch-agent/etc/amazon-cl
oudwatch-agent.d/file_config.json.tmp
Start configuration validation...
2023/10/01 09:44:32 Reading json config file path: /opt/aws/amazon-cloudwatch-agent/etc/amazon-cloudwatch-agent.d/file_config.json.tmp ...
2023/10/01 09:44:32 I! Valid Json input schema.
2023/10/01 09:44:32 D! ec2tagger processor required because append_dimensions is set
2023/10/01 09:44:32 D! pipeline hostDeltaMetrics has no receivers
2023/10/01 09:44:32 Configuration validation first phase succeeded
I! Detecting run_as_user...
I! Trying to detect region from ec2
D! [EC2] Found active network interface
/opt/aws/amazon-cloudwatch-agent/bin/amazon-cloudwatch-agent -schematest -config /opt/aws/amazon-cloudwatch-agent/etc/amazon-cloudwatch-agent.toml
Configuration validation second phase succeeded
Configuration validation succeeded
```

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

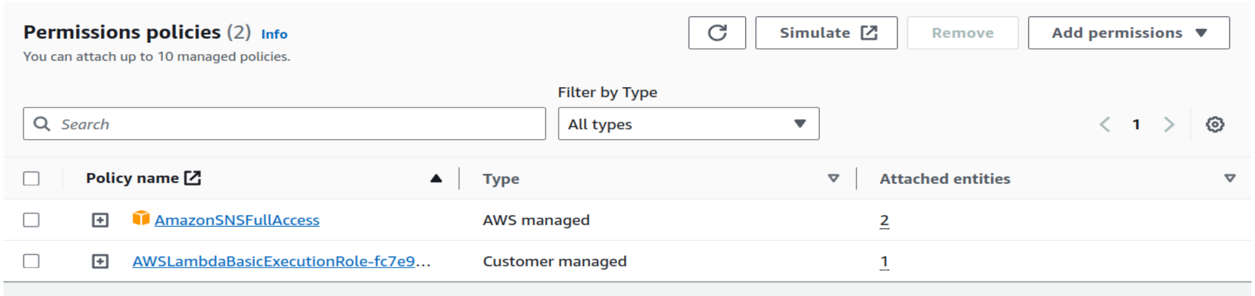


Log group	Data protection	Sensitive data co...	Retention	Metric filters	Contributor Insig...
access.log	-	-	Never expire	-	-
/aws/lambda/trigger-email-lambda	-	-	Never expire	-	-
error.log	-	-	Never expire	-	-

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

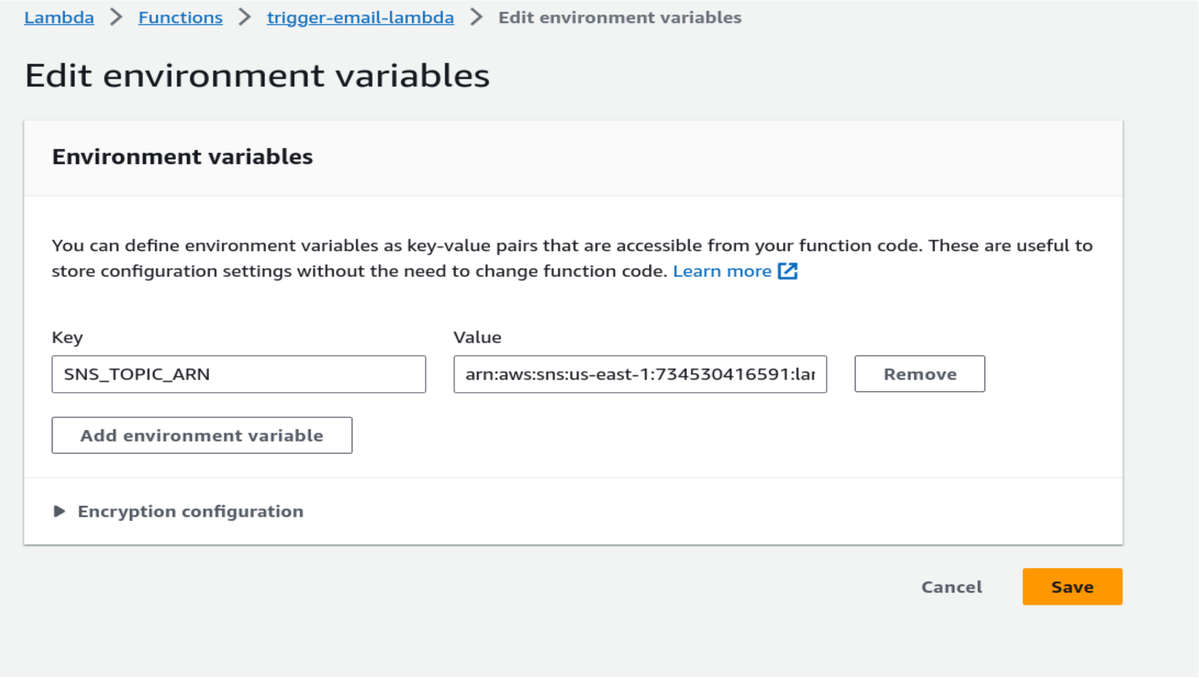

Permissions policies (2) Info
You can attach up to 10 managed policies.
Simulate
Remove
Add permissions
Filter by Type
Search
All types
1

Policy name	Type	Attached entities
AmazonSNSFullAccess	AWS managed	2
AWSLambdaBasicExecutionRole-fc7e9...	Customer managed	1

- ADD ENVIRONMENT VARIABLE OF SNS TOPIC ARN:

  → Click on configuration>Environment Variable

  → Add the Environment variable



Lambda > Functions > trigger-email-lambda > Edit environment variables

Edit environment variables

Environment variables

You can define environment variables as key-value pairs that are accessible from your function code. These are useful to store configuration settings without the need to change function code. Learn more

Key	Value
SNS_TOPIC_ARN	arn:aws:sns:us-east-1:734530416591:lar

Remove
Add environment variable
▶ Encryption configuration
Cancel
Save

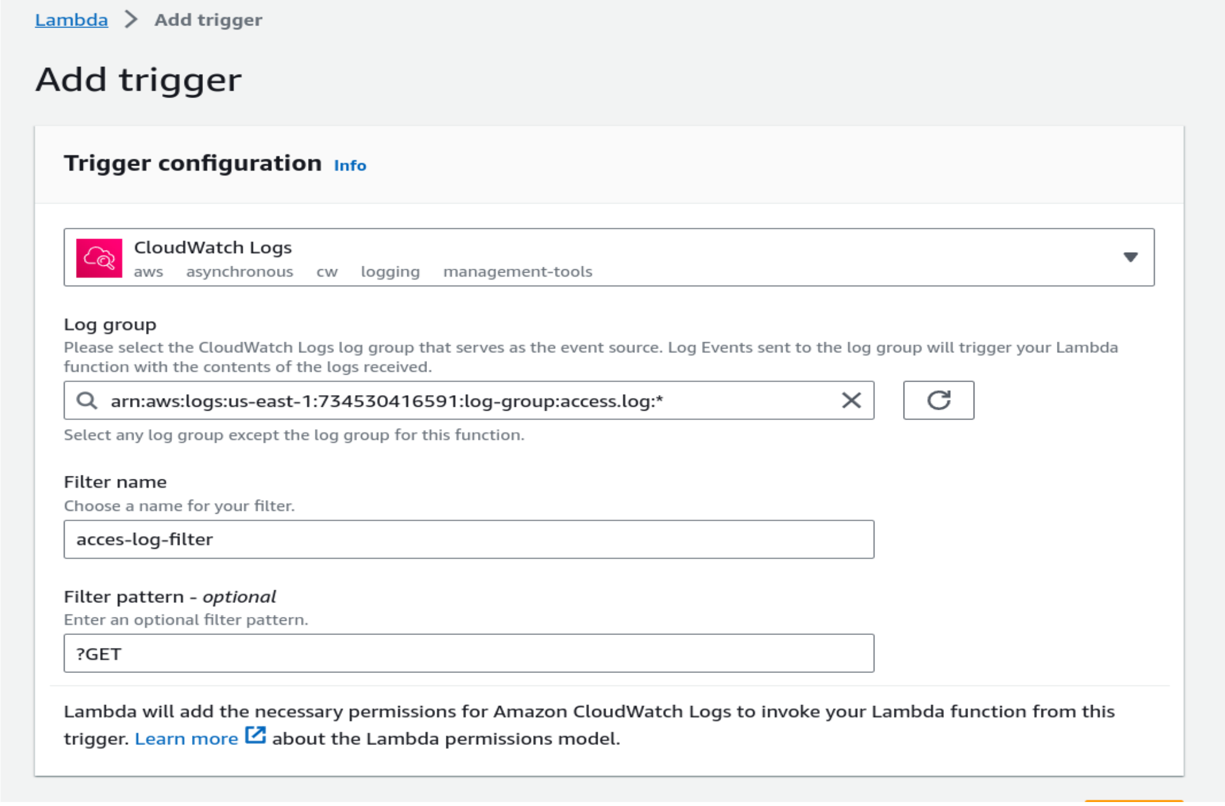
- ADD TRIGGER FOR CLOUD WATCH LOGS:

  →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.



Add trigger

Trigger configuration

CloudWatch Logs
aws asynchronous cw logging management-tools

Log group
Please select the CloudWatch Logs log group that serves as the event source. Log Events sent to the log group will trigger your Lambda function with the contents of the logs received.

arn:aws:logs:us-east-1:734530416591:log-group:access.log:*

Select any log group except the log group for this function.

Filter name
Choose a name for your filter.

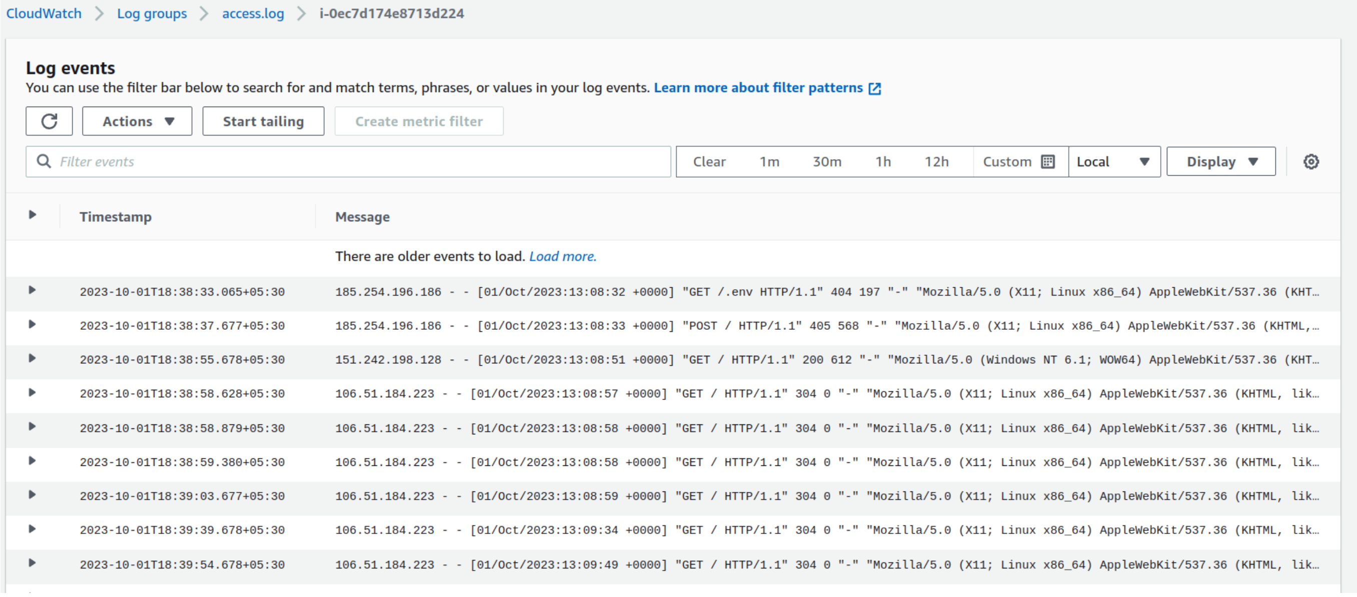
acces-log-filter

Filter pattern - *optional*
Enter an optional filter pattern.

?GET

Lambda will add the necessary permissions for Amazon CloudWatch Logs to invoke your Lambda function from this trigger. Learn more about the Lambda permissions model.

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



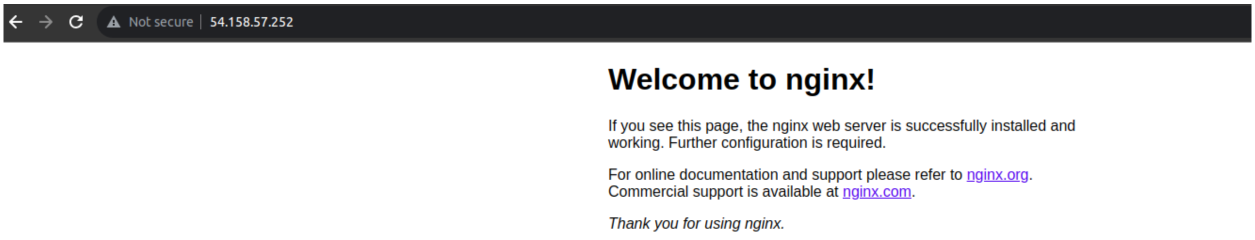
Log events
You can use the filter bar below to search for and match terms, phrases, or values in your log events. Learn more about filter patterns

```
Timestamp                        Message
                                 There are older events to load. Load more.
2023-10-01T18:38:33.065+05:30    185.254.196.186 - - [01/Oct/2023:13:08:32 +0000] "GET /.env HTTP/1.1" 404 197 "-" "Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHT…
2023-10-01T18:38:37.677+05:30    185.254.196.186 - - [01/Oct/2023:13:08:33 +0000] "POST / HTTP/1.1" 405 568 "-" "Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML,…
2023-10-01T18:38:55.678+05:30    151.242.198.128 - - [01/Oct/2023:13:08:51 +0000] "GET / HTTP/1.1" 200 612 "-" "Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHT…
2023-10-01T18:38:58.628+05:30    106.51.184.223 - - [01/Oct/2023:13:08:57 +0000] "GET / HTTP/1.1" 304 0 "-" "Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, lik…
2023-10-01T18:38:58.879+05:30    106.51.184.223 - - [01/Oct/2023:13:08:58 +0000] "GET / HTTP/1.1" 304 0 "-" "Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, lik…
2023-10-01T18:38:59.380+05:30    106.51.184.223 - - [01/Oct/2023:13:08:58 +0000] "GET / HTTP/1.1" 304 0 "-" "Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, lik…
2023-10-01T18:39:03.677+05:30    106.51.184.223 - - [01/Oct/2023:13:08:59 +0000] "GET / HTTP/1.1" 304 0 "-" "Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, lik…
2023-10-01T18:39:39.678+05:30    106.51.184.223 - - [01/Oct/2023:13:09:34 +0000] "GET / HTTP/1.1" 304 0 "-" "Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, lik…
2023-10-01T18:39:54.678+05:30    106.51.184.223 - - [01/Oct/2023:13:09:49 +0000] "GET / HTTP/1.1" 304 0 "-" "Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, lik…
```

- 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.



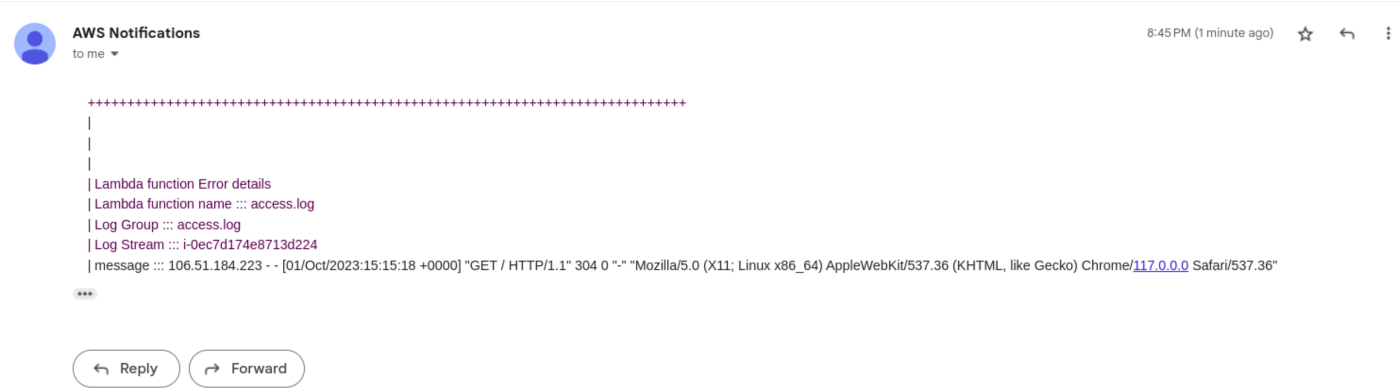
Welcome to nginx!

If you see this page, the nginx web server is successfully installed and working. Further configuration is required.

For online documentation and support please refer to nginx.org.
Commercial support is available at nginx.com.

Thank you for using nginx.

- Open the email and check for notification



```
+++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++
|
|
|
| Lambda function Error details
| Lambda function name ::: access.log
| Log Group ::: access.log
| Log Stream ::: i-0ec7d174e8713d224
| message ::: 106.51.184.223 - - [01/Oct/2023:15:15:18 +0000] "GET / HTTP/1.1" 304 0 "-" "Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/117.0.0.0 Safari/537.36"
```

- 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.