

Amazon-CloudWatch: CloudWatch Logs

Problem Statement:

You work for XYZ Corporation. To maintain the security of the AWS account and the resources you have been asked to implement a solution that can help easily recognize and monitor the different users. Also, you will be monitoring the machines created by these users for any errors or misconfigurations.

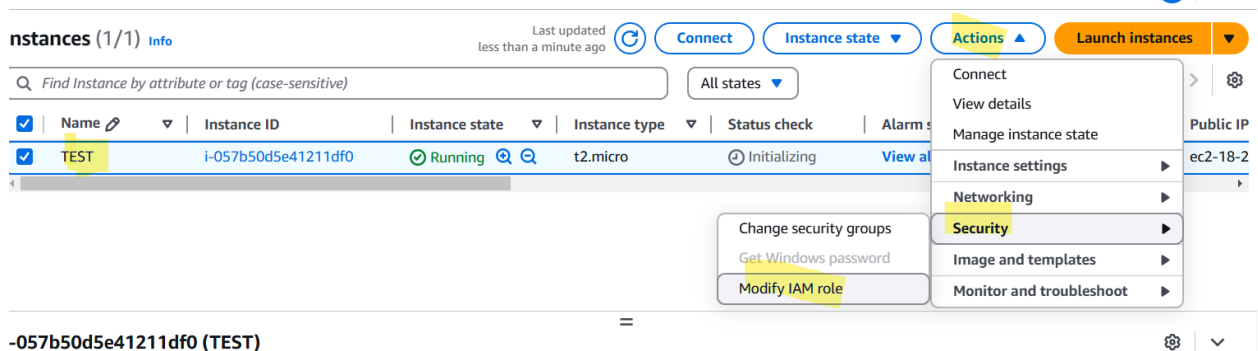
Tasks To Be Performed:

1. Create a EC2 and create logs and monitor on CloudWatch

these logs.


Solution:



- **Create** EC2 instance and attach IAM policy in EC2 to full access for CloudWatch.



Instance ID
i-057b50d5e41211df0 (TEST)

IAM role
Select an IAM role to attach to your instance or create a new role if you haven't created any. The role you select replaces any roles that are currently attached to your instance.

Choose IAM role 

 Create new IAM role 

Q |

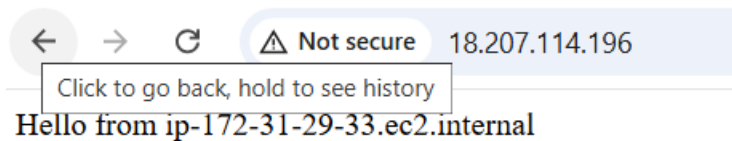
No IAM Role
Choose this option to detach an IAM role

cloudwatchfullaccess
arn:aws:iam:050451395918:instance-profile/cloudwatchfullaccess

cloudwatchfullaccess

Cancel **Update IAM role**

```
root@ip-172-31-29-33 home]#
root@ip-172-31-29-33 home]#
root@ip-172-31-29-33 home]#
root@ip-172-31-29-33 home]# cd /var/log/httpd
root@ip-172-31-29-33 httpd]# ll
total 4
-rw-r--r--. 1 root root 0 Dec 11 15:49 access_log
-rw-r--r--. 1 root root 690 Dec 11 15:49 error_log
root@ip-172-31-29-33 httpd]# tail -f access_log
03.108.5.100 - - [11/Dec/2024:15:55:48 +0000] "GET / HTTP/1.1" 200 40 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/131.0.0.0 Safari/537.36"
03.108.5.100 - - [11/Dec/2024:15:55:48 +0000] "GET /favicon.ico HTTP/1.1" 404 196 "http://18.207.114.196/" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/131.0.0.0 Safari/537.36"
03.108.5.100 - - [11/Dec/2024:15:55:50 +0000] "GET / HTTP/1.1" 304 - "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/131.0.0.0 Safari/537.36"
03.108.5.100 - - [11/Dec/2024:15:55:51 +0000] "GET / HTTP/1.1" 304 - "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/131.0.0.0 Safari/537.36"
03.108.5.100 - - [11/Dec/2024:15:56:00 +0000] "GET /log HTTP/1.1" 404 196 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/131.0.0.0 Safari/537.36"
03.108.5.100 - - [11/Dec/2024:15:56:02 +0000] "GET /log HTTP/1.1" 404 196 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/131.0.0.0 Safari/537.36"
MFC
root@ip-172-31-29-33 httpd]#
```



2. Download and install CloudWatch agent in instance.
3. And configure that agent .

```
[root@ip-172-31-29-33 httpd]# cd /home
[root@ip-172-31-29-33 home]# wget https://amazoncloudwatch-agent-us-east-1.s3.us-east-1.amazonaws.com/amazon_linux/amd64/latest/amazon-cloudwatch-agent.rpm
--2024-12-11 15:58:06-- https://amazoncloudwatch-agent-us-east-1.s3.us-east-1.amazonaws.com/amazon_linux/amd64/latest/amazon-cloudwatch-agent.rpm
Resolving amazoncloudwatch-agent-us-east-1.s3.us-east-1.amazonaws.com (amazoncloudwatch-agent-us-east-1.s3.us-east-1.amazonaws.com)... 52.217.236.218, 52.216.40.138, 52.217.254.2, ...
Connecting to amazoncloudwatch-agent-us-east-1.s3.us-east-1.amazonaws.com (amazoncloudwatch-agent-us-east-1.s3.us-east-1.amazonaws.com)|52.217.236.218|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 113235159 (108M) [application/octet-stream]
Saving to: 'amazon-cloudwatch-agent.rpm'

amazon-cloudwatch-agent.rpm      100%[=====] 107.99M  81.8MB/s   in 1.3s

2024-12-11 15:58:08 (81.8 MB/s) - 'amazon-cloudwatch-agent.rpm' saved [113235159/113235159]

[root@ip-172-31-29-33 home]# ll
total 110584
-rw-r--r--. 1 root root 113235159 Nov 15 20:52 amazon-cloudwatch-agent.rpm
drwx----- 3 ec2-user ec2-user 74 Dec 11 15:49 ec2-user
[root@ip-172-31-29-33 home]# rpm -U amazon-cloudwatch-agent.rpm
create group cwagent, result: 0
create user cwagent, result: 0
[root@ip-172-31-29-33 home]# ll
```

```
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.
[root@ip-172-31-29-33 ~]# sudo /opt/aws/amazon-cloudwatch-agent/bin/amazon-cloudwatch-agent-config-wizard
=====
= 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]:
```

```
2. no
default choice: [1]:
2
Do you want to monitor metrics from CollectD? WARNING: CollectD must be installed on
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]:

Do you want to add ec2 dimensions (ImageId, InstanceId, InstanceType, AutoScalingGroup)?
1. yes
2. no
default choice: [1]:
2
Do you want to aggregate ec2 dimensions (InstanceId)?
1. yes
2. no
default choice: [1]:
```

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": 60,
    "run_as_user": "root"
  },
  "metrics": {
    "aggregation_dimensions": [
      "InstanceId"
    ],
    "metrics_collected": {
      "disk": {
        "measurement": [
          "used_percent"
        ],
        "metrics_collection_interval": 60,
        "resources": [
```

```
}
```

Are you satisfied with the above config? Note: it can be manually customized after the wizard completes to add ac

- 1. yes
- 2. no

default choice: [1]:

Do you have any existing CloudWatch Log Agent (<http://docs.aws.amazon.com/AmazonCloudWatch/latest/logs/AgentRefer>)

- 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/httpd/access_log

Log group name:

default choice: [access_log]

Log group class:

- 1. STANDARD
- 2. INFREQUENT_ACCESS

default choice: [1]:

Log stream name:

default choice: [{instance_id}]

```
Program exits now.
[root@ip-172-31-29-33 home]#
[root@ip-172-31-29-33 home]#
[root@ip-172-31-29-33 ~]# 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 -s
***** processing amazon-cloudwatch-agent *****
I! Trying to detect region from ec2 D! [EC2] Found active network interface I! imds retry client will retry 1 timesSuccessfully fetched the config and saved in /opt/aw
s/amazon-cloudwatch-agent/etc/amazon-cloudwatch-agent.d/file_config.json.tmp
Start configuration validation...
2024/12/11 16:14:47 Reading json config file path: /opt/aws/amazon-cloudwatch-agent/etc/amazon-cloudwatch-agent.d/file_config.json.tmp ...
2024/12/11 16:14:47 I! Valid Json input schema.
2024/12/11 16:14:47 Configuration validation first phase succeeded
I! Detecting run as user...
I! Trying to detect region from ec2
D! [EC2] Found active network interface
I! imds retry client will retry 1 times
```

Log groups

Log groups (1)

By default, we only load up to 10000 log groups.

☐ Exact match < 1 >

<input type="checkbox"/>	Log group	Log class	Anomaly d...	Data pr...	Sensitiv...	Retention	Metric ...
<input type="checkbox"/>	access_log	Standard	Configure	-	-	3 days	-

[view](#) 0

[Log streams](#) | [Tags](#) | [Anomaly detection](#) | [Metric filters](#) | [Subscription filters](#) | [Contributor Insights](#) | [Data protection](#) | [Field](#)

Log streams (1)

☐ Exact match ☐ Show expired [Info](#) < 1 >

<input type="checkbox"/>	Log stream	Last event time
<input type="checkbox"/>	i-057b50d5e41211df0	2024-12-11 16:14:54 (UTC)

[access_log](#) > [i-057b50d5e41211df0](#)

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](#)

<input type="checkbox"/>	Timestamp	Message
		No older events at this moment. Retry
<input type="checkbox"/>	2024-12-11T16:14:54.413Z	103.108.5.100 - - [11/Dec/2024:15:55:48 +0000] "GET / HTTP/1.1" 200 40 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit...
<input type="checkbox"/>	2024-12-11T16:14:54.413Z	103.108.5.100 - - [11/Dec/2024:15:55:48 +0000] "GET /favicon.ico HTTP/1.1" 404 196 "http://18.207.114.196/" "Mozilla/5.0 (Window...
<input type="checkbox"/>	2024-12-11T16:14:54.413Z	103.108.5.100 - - [11/Dec/2024:15:55:50 +0000] "GET / HTTP/1.1" 304 - "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit...
<input type="checkbox"/>	2024-12-11T16:14:54.413Z	103.108.5.100 - - [11/Dec/2024:15:55:51 +0000] "GET / HTTP/1.1" 304 - "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit...
<input type="checkbox"/>	2024-12-11T16:14:54.413Z	103.108.5.100 - - [11/Dec/2024:15:56:00 +0000] "GET /log HTTP/1.1" 404 196 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleW...
<input type="checkbox"/>	2024-12-11T16:14:54.413Z	103.108.5.100 - - [11/Dec/2024:15:56:02 +0000] "GET /log HTTP/1.1" 404 196 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleW...
<input type="checkbox"/>	2024-12-11T16:14:54.413Z	103.108.5.100 - - [11/Dec/2024:15:56:52 +0000] "-" 408 - "-" "-"
<input type="checkbox"/>	2024-12-11T16:14:54.413Z	103.108.5.100 - - [11/Dec/2024:15:57:11 +0000] "GET / HTTP/1.1" 304 - "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit...
<input type="checkbox"/>	2024-12-11T16:14:54.413Z	103.108.5.100 - - [11/Dec/2024:15:58:03 +0000] "-" 408 - "-" "-"
<input type="checkbox"/>	2024-12-11T16:14:54.413Z	152.32.213.86 - - [11/Dec/2024:16:06:27 +0000] "GET / HTTP/1.1" 200 40 "-" "curl/7.29.0"
<input type="checkbox"/>	2024-12-11T16:14:54.413Z	152.32.213.86 - - [11/Dec/2024:16:06:28 +0000] "\x16\x03\x01" 400 226 "-" "-"
<input type="checkbox"/>	2024-12-11T16:14:54.413Z	152.32.213.86 - - [11/Dec/2024:16:06:29 +0000] "t3 12.1.2\n" 400 226 "-" "-"