Assignment 9 – DynamoDB & CloudWatch

Today's tasks:

1. Create a DynamoDB table for the Course API.
2. Configure the Lambda's execution role so that it can store data in the DB.
3. Update the Course Lambda that should do the CRUD operations below.
4. The most tricky part in this assignment is query on the index. There must be the index table ARN in the IAM policy.
5. Console log out "system error" and "validation error" then count it using CloudWatch insights.

Bonus task:

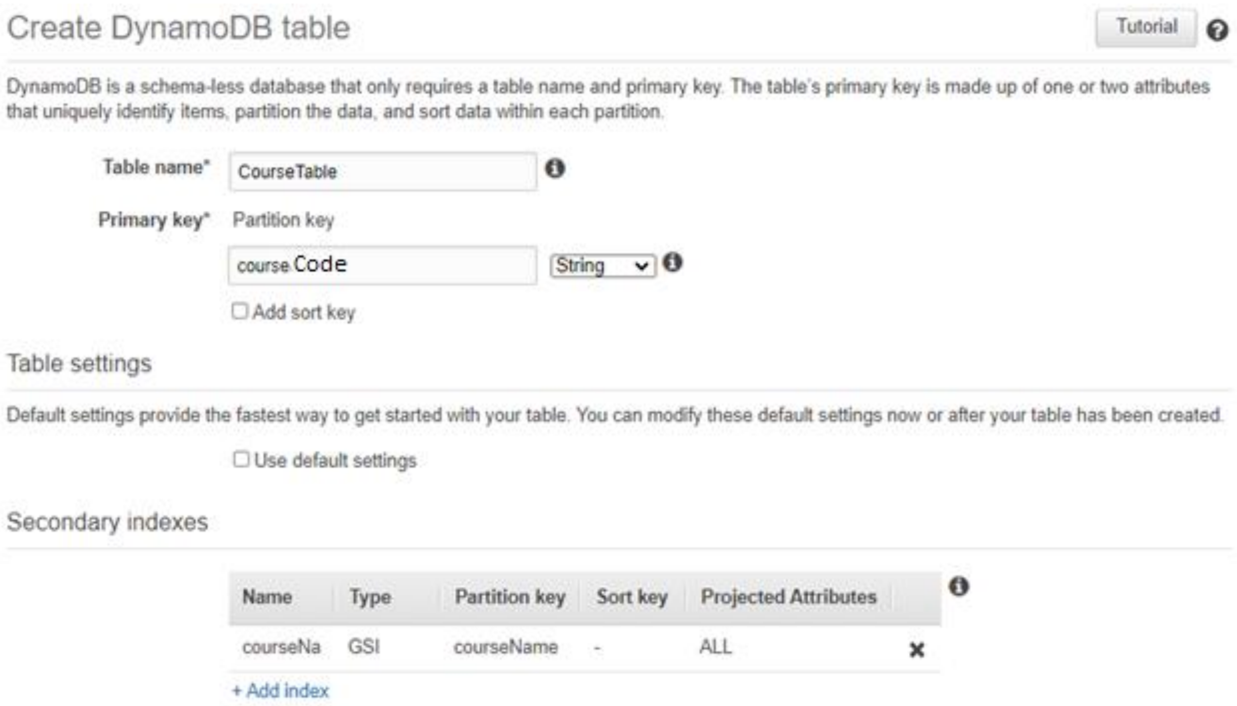
- Publish CloudWatch logs using the agent from EC2. Refer: https://www.youtube.com/watch?v=F4IE69V-iuw
    a. Publish a custom log to CloudWatch from EC2 via CloudWatch agent
    b. Create a filter on the log group that will create a metric
    c. Set an alarm on the metric that sends email to you and me.

Submit items below in one pdf file:

1. Screenshots of logs and DynamoDB table.
2. Screenshot of CloudWatch insight query result.
3. Submit your code.

Instruction 1 – DynamoDB

1. Create a DynamoDB table for the Course API
    a. Go to DynamoDB console and click on Create Table.
    b. The table name is **CourseTable**
    c. The primary key is **courseCode**
    d. Uncheck **Use default settings**
    e. Click on **add index.** Notice that the price got doubled as you added an index. If you add another index, it costs three times higher. The reason is, the index creates a hidden table that boosts querying. The trade-off is that you are losing the write speed as it now inserts data into the actual tables and indexes.
    f. On the popup, partition key or primary key is **courseName.** Click add index.



Create DynamoDB table

DynamoDB is a schema-less database that only requires a table name and primary key. The table's primary key is made up of one or two attributes that uniquely identify items, partition the data, and sort data within each partition.

Table name* CourseTable

Primary key* Partition key

courseCode String

□ Add sort key

Table settings

Default settings provide the fastest way to get started with your table. You can modify these default settings now or after your table has been created.

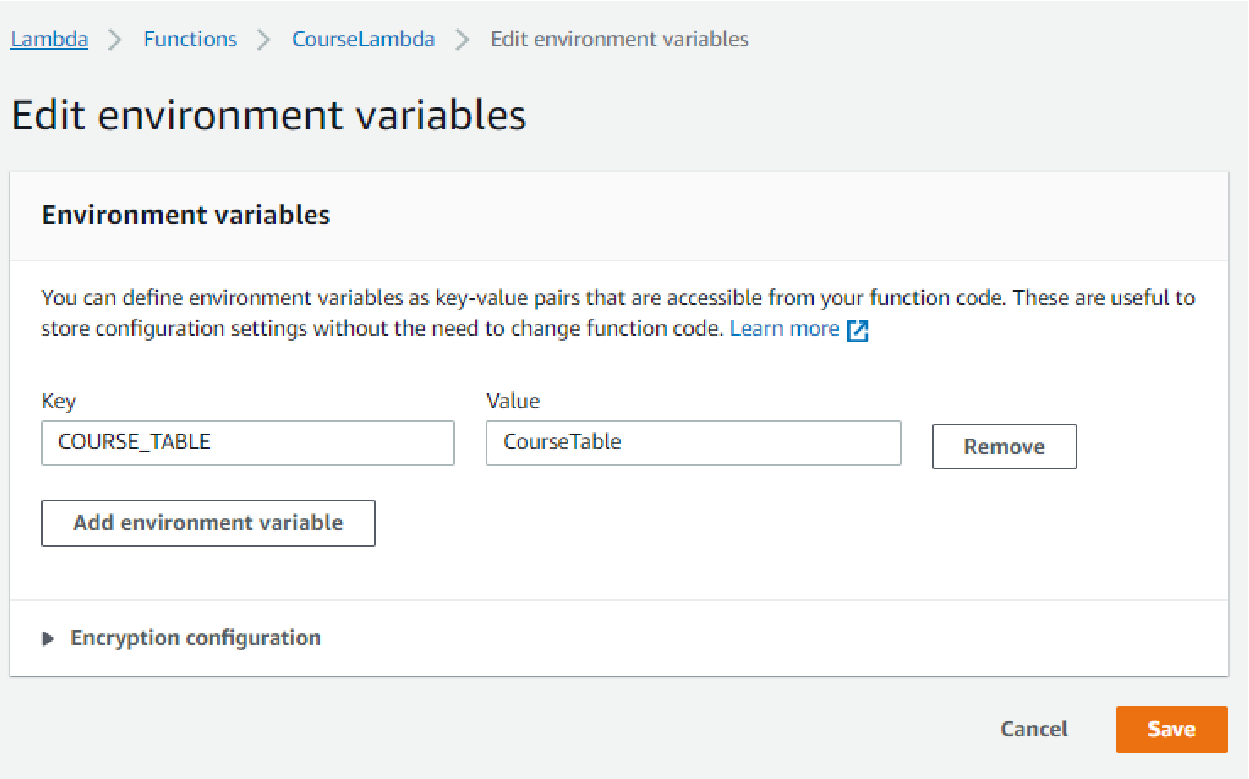
□ Use default settings

Secondary indexes

Name	Type	Partition key	Sort key	Projected Attributes
courseNa	GSI	courseName	-	ALL

g. In Read/write capacity mode, change the **maximum provisioned capacity** to 5.
h. Hit create. You might have an error because of the AWS starter account limitation. But it should be created.

2. Update the IAM role of the Lambda and give it access to the DynamoDB table that you created in step 1.
    a. Click on the **Configuration** tab
    b. Select **Permissions**
    c. In the execution role section, there is Role name, click on that. It will open up the role in AWS IAM.
    d. Click on the blue **Add inline policy.**
    e. Click on the **JSON** tab. Copy and paste the policy below. Don't forget to **replace** the <<account-id>> with your account id.
    f. Give it a name and click on **Create policy** button.
3. Update the Lambda. Use the code below.
    a. Add an environment variable **COURSE_TABLE** with the value **CourseTable**.
        i. Configuration -> Environment Variables -> Edit -> Add environment variable -> hit save.



Lambda > Functions > CourseLambda > 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: COURSE_TABLE

Value: CourseTable

   b. Copy and paste the code below.

4. Implement the following and submit your code along with screenshots that show it works.
   a. **GetItem**
   b. **Scan**
   c. **Query** (on courseName)

References

Inline policy for the lambda that gives it DynamoDB table access on the CourseTable.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "PolicyToGiveLambdaAccessCourseTable",
            "Effect": "Allow",
            "Action": [
                "dynamodb:PutItem",
                "dynamodb:GetItem",
                "dynamodb:Scan",
                "dynamodb:Query"
            ],
            "Resource": "arn:aws:dynamodb:us-east-1:<<account-id>>:table/CourseTable"
        }
    ]
  }
```

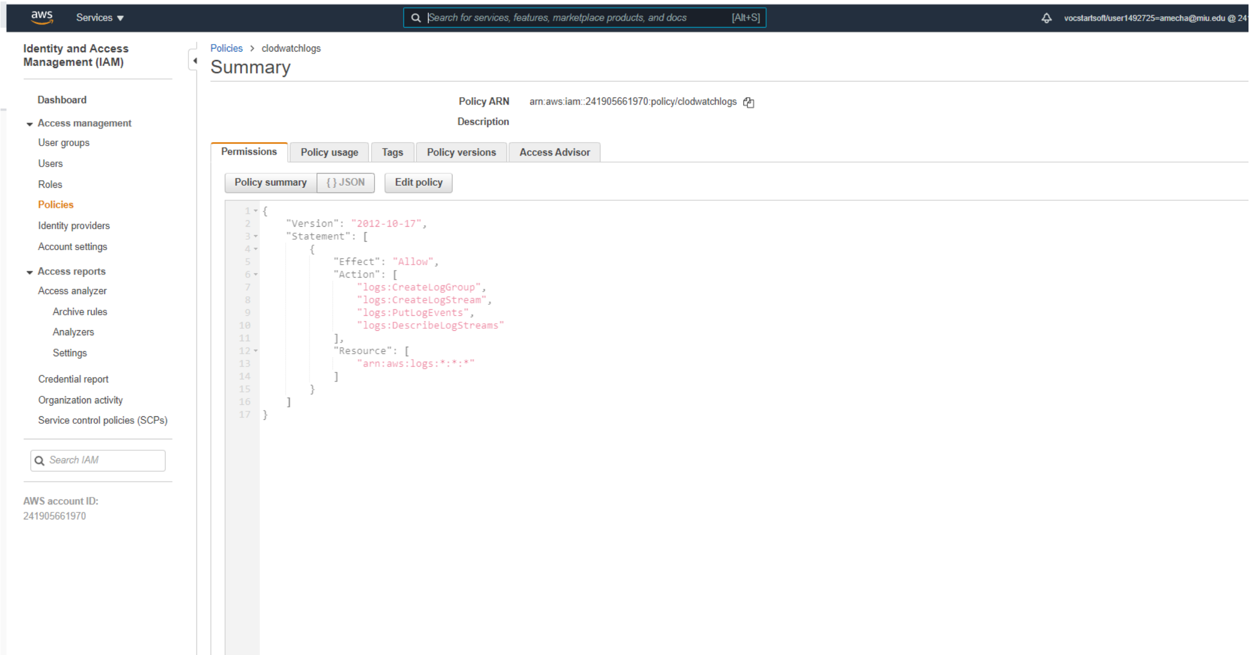
The lambda code for the CourseLambda

```
const AWS = require("aws-sdk");
const dynamodb = new AWS.DynamoDB({ apiVersion: "2012-08-10" });
const tableName = process.env.COURSE_TABLE;

exports.handler = async (event) => {
    console.log("Request received: " + JSON.stringify(event));

    const saveParams = {
        TableName: tableName,
        Item: {
            "courseCode": {
                S: "CS516"
            },
            "courseName": {
                S: "Cloud Computing"
            },
            "teacherName": {
                S: "Unubold"
            },
            "students": {
                SS: [
                    "Bipin",
                    "Ryan",
                    "Michael"
                ]
            },
            "monthYear": {
                S: "July, 2021"
            }
        }
    };

    await dynamodb.putItem(saveParams).promise();

    const response = {
        statusCode: 200,
        body: JSON.stringify('An item is saved.'),
    };
    return response;
};
```

Instruction 2 – CloudWatch Agent

First create IAM policy

```
{

  "Version":"2012-10-17",

  "Statement":[

    {
      "Effect":"Allow",
      "Action":[
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:PutLogEvents",
        "logs:DescribeLogStreams"
        ],
        "Resource":[
          "arn:aws:logs:*:*:*"]
    }]
}
```



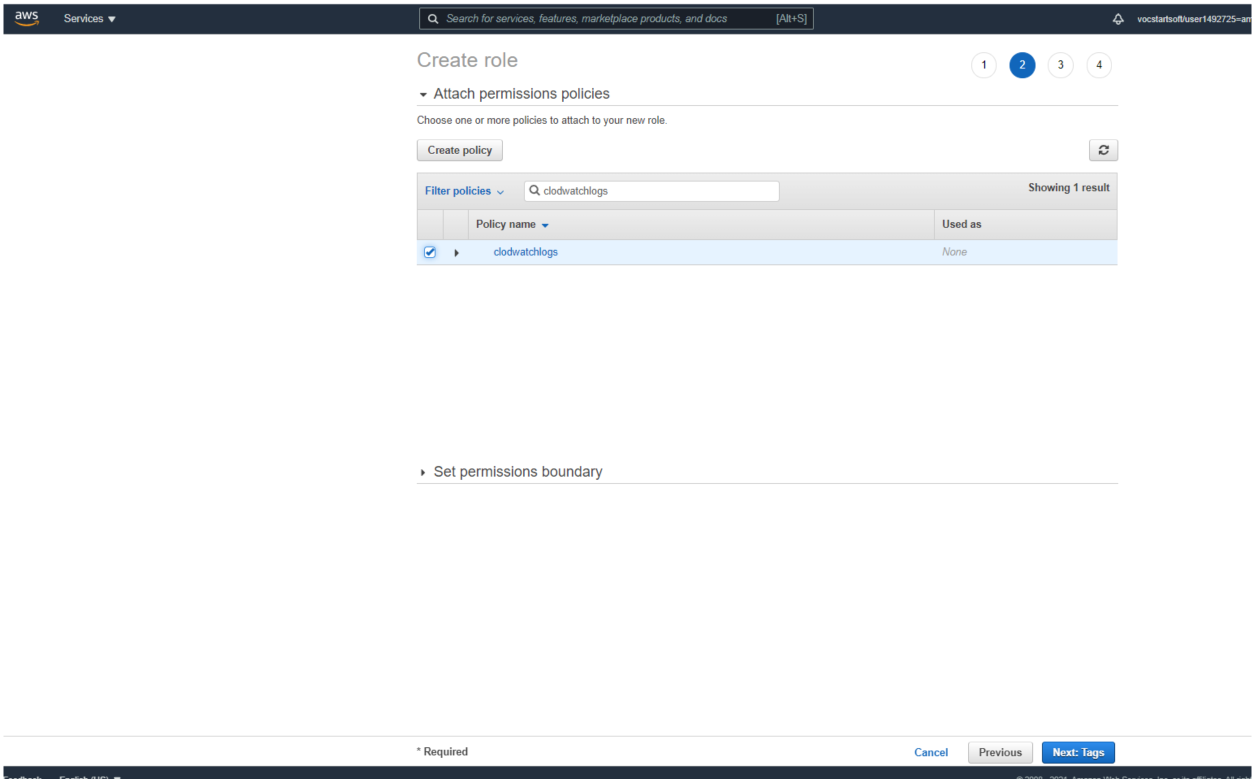
AWS account ID: 241905661970

Policy ARN arn:aws:iam::241905661970:policy/clodwatchlogs

Description

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "logs:CreateLogGroup",
                "logs:CreateLogStream",
                "logs:PutLogEvents",
                "logs:DescribeLogStreams"
            ],
            "Resource": [
                "arn:aws:logs:*:*:*"
            ]
        }
    ]
}
```

Create new role for EC2 instance


aws
Services ▼
Search for services, features, marketplace products, and docs [Alt+S]
vocstartsoft/user1492725=am

Create role

Attach permissions policies

Choose one or more policies to attach to your new role.

Create policy
Filter policies

clodwatchlogs

Showing 1 result

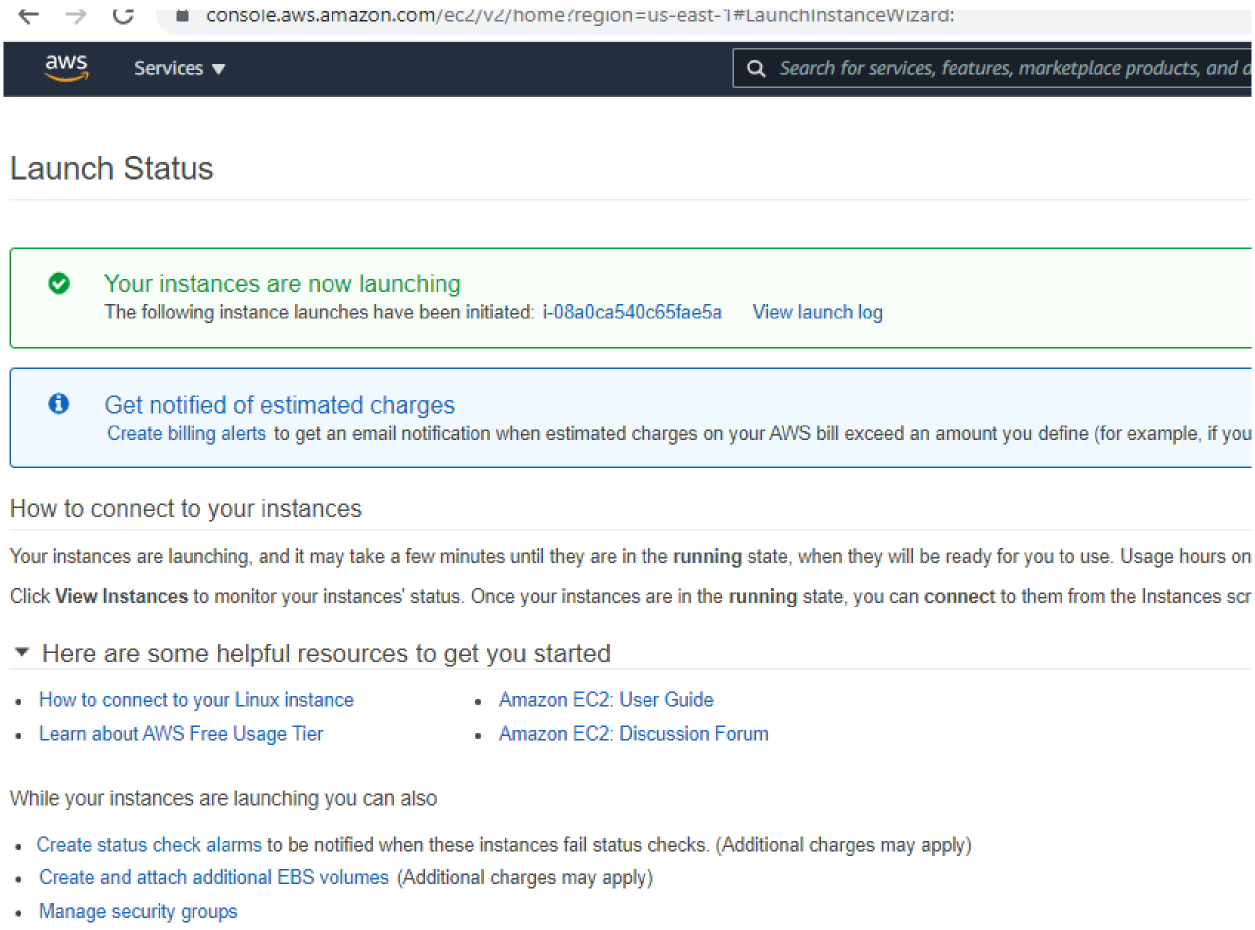
		Policy name	Used as
☑	▸	clodwatchlogs	None

Set permissions boundary

* Required

Cancel
Previous
Next: Tags

EC2 instance launch


console.aws.amazon.com/ec2/v2/home?region=us-east-1#LaunchInstanceWizard:
aws
Services ▼
Search for services, features, marketplace products, and d

Launch Status

Your instances are now launching

The following instance launches have been initiated: i-08a0ca540c65fae5a View launch log

Get notified of estimated charges

Create billing alerts to get an email notification when estimated charges on your AWS bill exceed an amount you define (for example, if you

How to connect to your instances

Your instances are launching, and it may take a few minutes until they are in the **running** state, when they will be ready for you to use. Usage hours on

Click **View Instances** to monitor your instances' status. Once your instances are in the **running** state, you can **connect** to them from the Instances scr

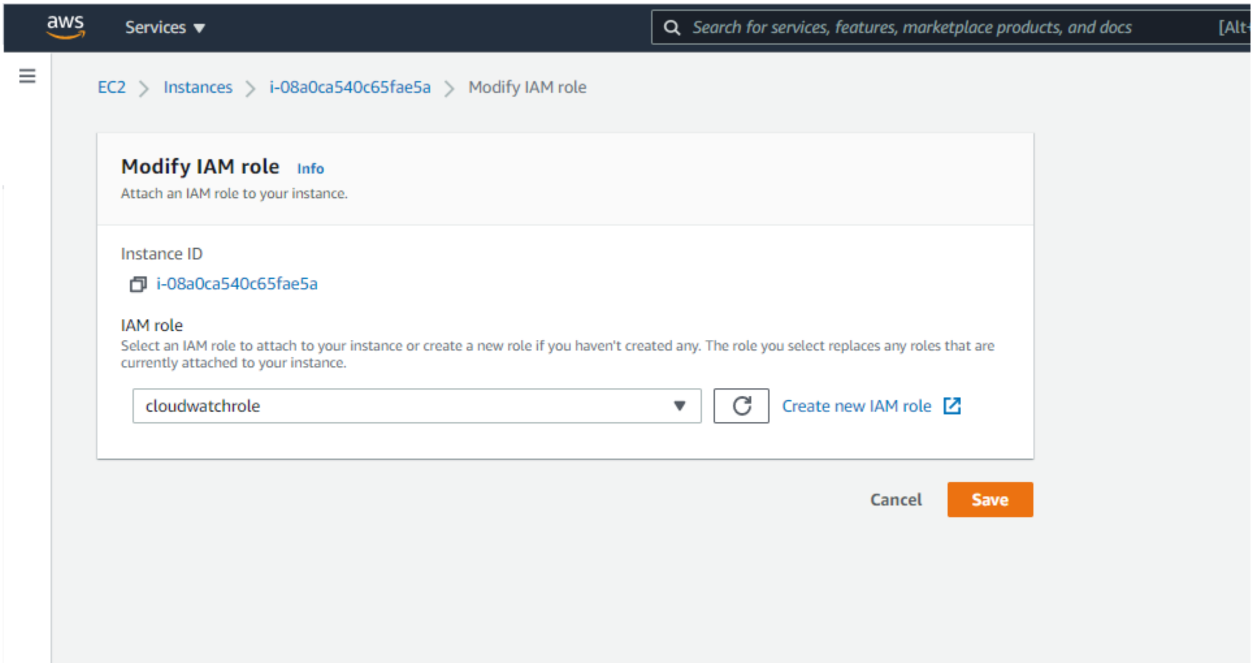
▼ Here are some helpful resources to get you started

- How to connect to your Linux instance
- Learn about AWS Free Usage Tier
- Amazon EC2: User Guide
- Amazon EC2: Discussion Forum

While your instances are launching you can also

- Create status check alarms to be notified when these instances fail status checks. (Additional charges may apply)
- Create and attach additional EBS volumes (Additional charges may apply)
- Manage security groups

Attach instance to IAM role


aws
Services ▼
Search for services, features, marketplace products, and docs
[Alt
EC2 > Instances > i-08a0ca540c65fae5a > Modify IAM role
Info
Create new IAM role
Cancel
Save

Modify IAM role

Attach an IAM role to your instance.

Instance ID

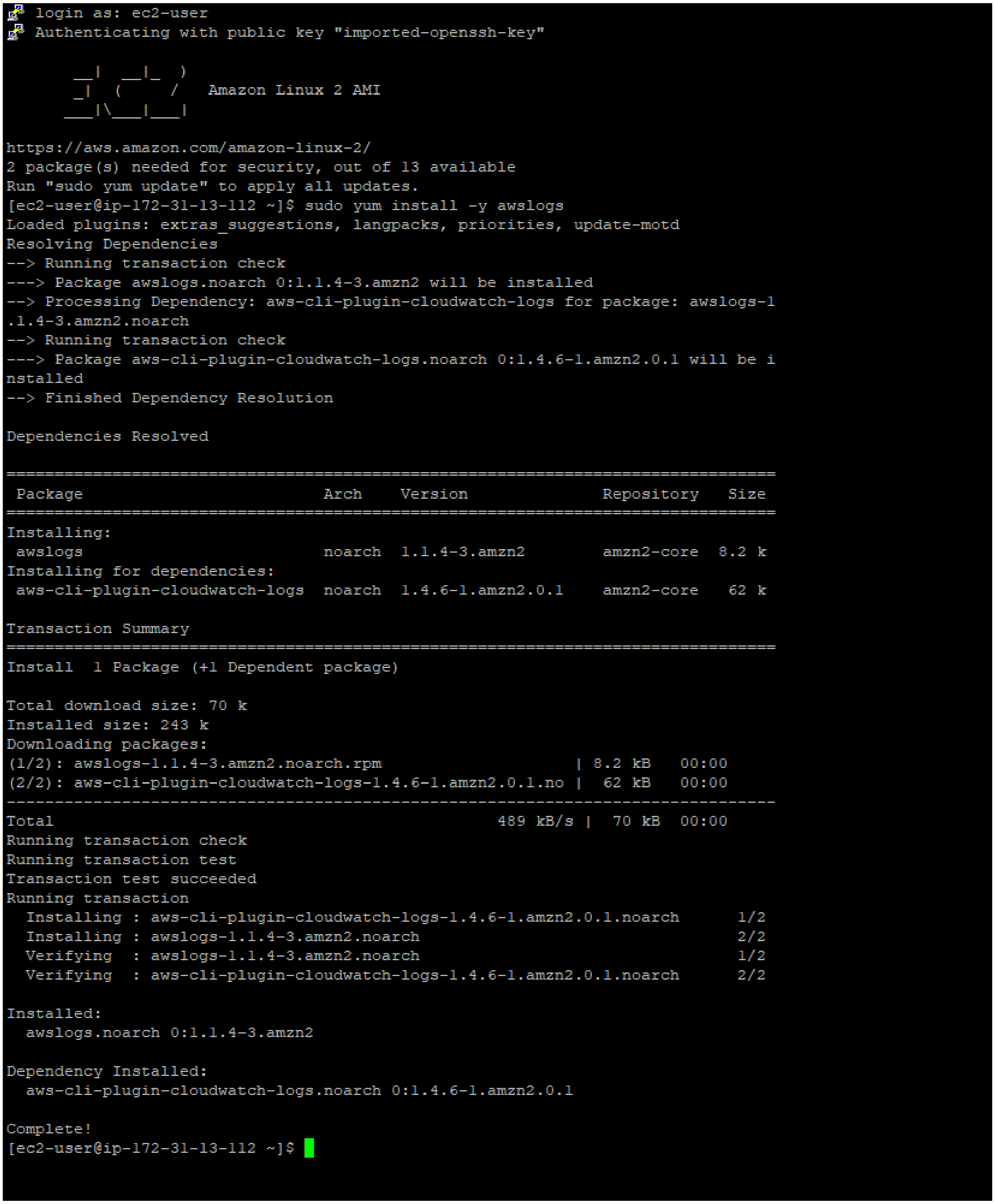
i-08a0ca540c65fae5a

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.

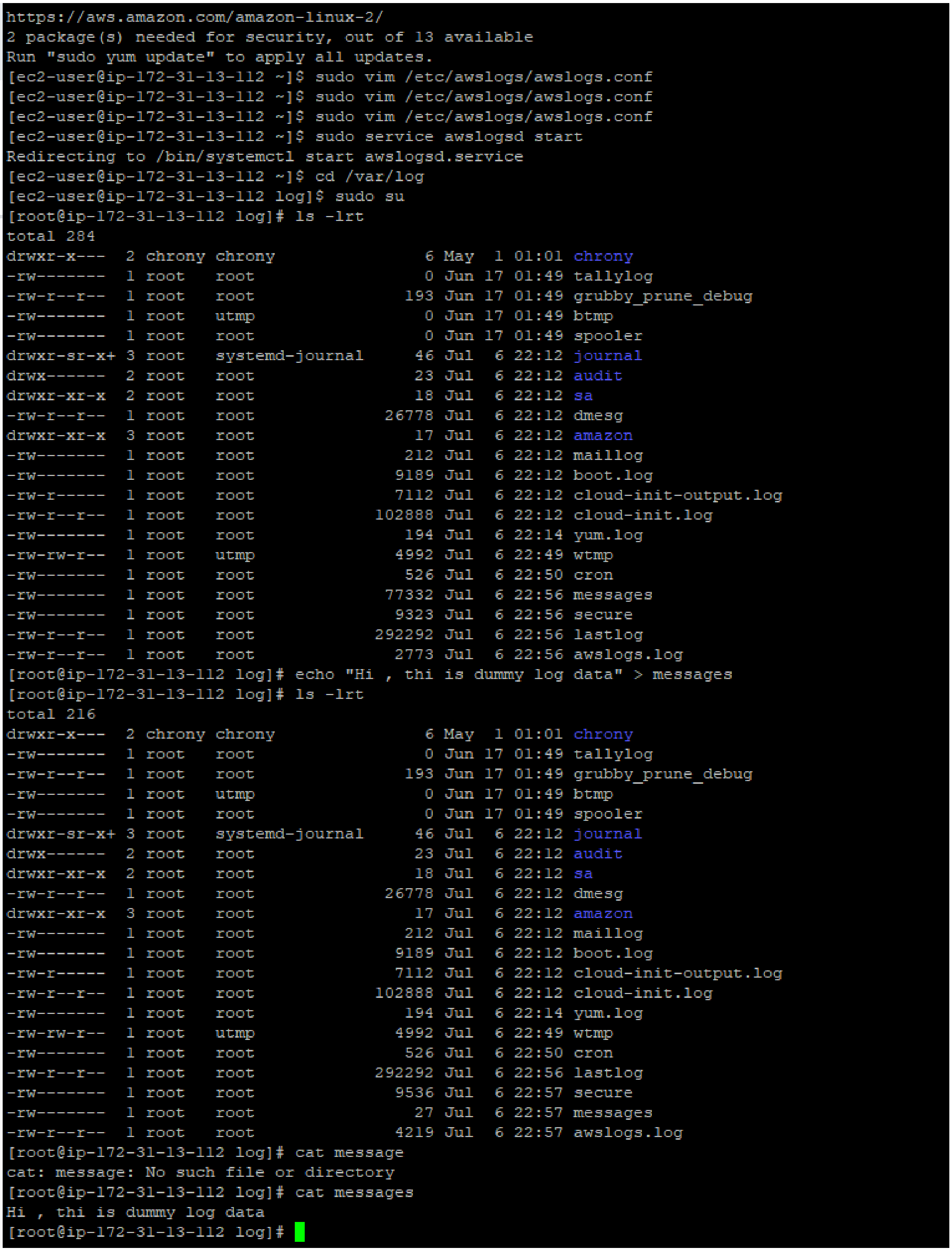
cloudwatchrole ▼

Install Cloudwatch agent into EC2 instance



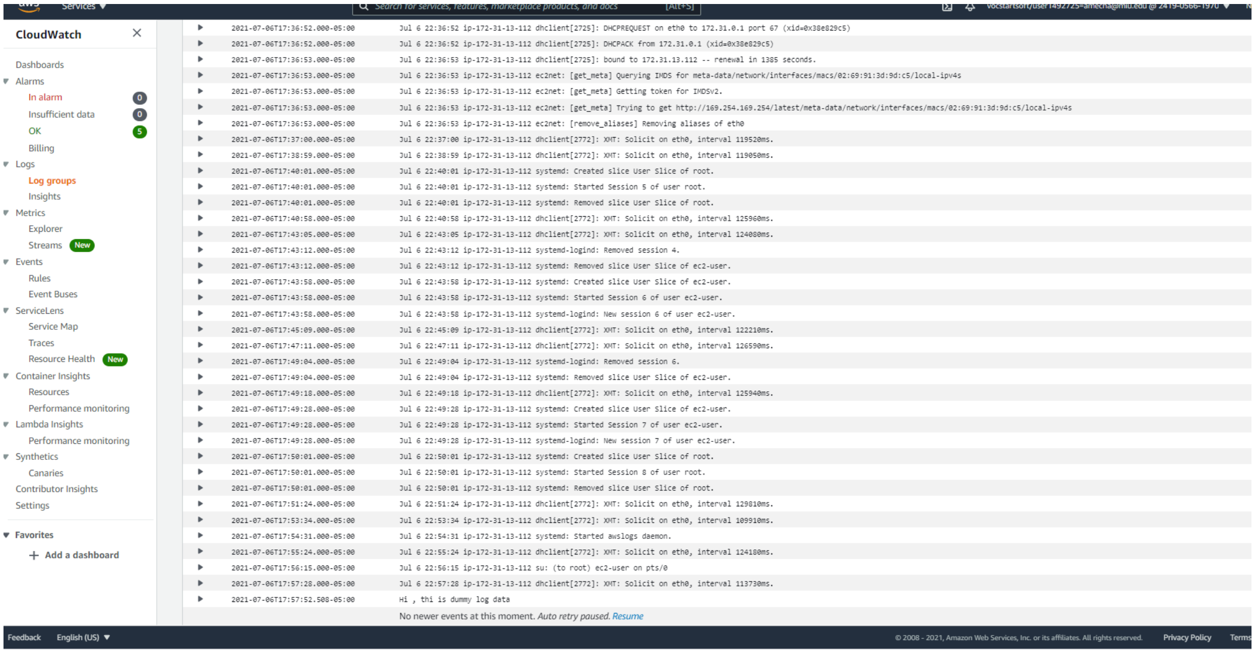
```
 login as: ec2-user
 Authenticating with public key "imported-openssh-key"

       __|  __|_  )
       _|  (     /   Amazon Linux 2 AMI
      ___|\___|___|

https://aws.amazon.com/amazon-linux-2/
2 package(s) needed for security, out of 13 available
Run "sudo yum update" to apply all updates.
[ec2-user@ip-172-31-13-112 ~]$ sudo yum install -y awslogs
Loaded plugins: extras_suggestions, langpacks, priorities, update-motd
Resolving Dependencies
--> Running transaction check
---> Package awslogs.noarch 0:1.1.4-3.amzn2 will be installed
--> Processing Dependency: aws-cli-plugin-cloudwatch-logs for package: awslogs-1
.1.4-3.amzn2.noarch
--> Running transaction check
---> Package aws-cli-plugin-cloudwatch-logs.noarch 0:1.4.6-1.amzn2.0.1 will be i
nstalled
--> Finished Dependency Resolution

Dependencies Resolved

================================================================================
 Package                         Arch    Version             Repository   Size
================================================================================
Installing:
 awslogs                         noarch  1.1.4-3.amzn2       amzn2-core  8.2 k
Installing for dependencies:
 aws-cli-plugin-cloudwatch-logs  noarch  1.4.6-1.amzn2.0.1   amzn2-core   62 k

Transaction Summary
================================================================================
Install  1 Package (+1 Dependent package)

Total download size: 70 k
Installed size: 243 k
Downloading packages:
(1/2): awslogs-1.1.4-3.amzn2.noarch.rpm                    | 8.2 kB   00:00
(2/2): aws-cli-plugin-cloudwatch-logs-1.4.6-1.amzn2.0.1.no |  62 kB   00:00
--------------------------------------------------------------------------------
Total                                              489 kB/s |  70 kB  00:00
Running transaction check
Running transaction test
Transaction test succeeded
Running transaction
  Installing : aws-cli-plugin-cloudwatch-logs-1.4.6-1.amzn2.0.1.noarch      1/2
  Installing : awslogs-1.1.4-3.amzn2.noarch                                 2/2
  Verifying  : awslogs-1.1.4-3.amzn2.noarch                                 1/2
  Verifying  : aws-cli-plugin-cloudwatch-logs-1.4.6-1.amzn2.0.1.noarch      2/2

Installed:
  awslogs.noarch 0:1.1.4-3.amzn2

Dependency Installed:
  aws-cli-plugin-cloudwatch-logs.noarch 0:1.4.6-1.amzn2.0.1

Complete!
[ec2-user@ip-172-31-13-112 ~]$
```

Insert dummy data



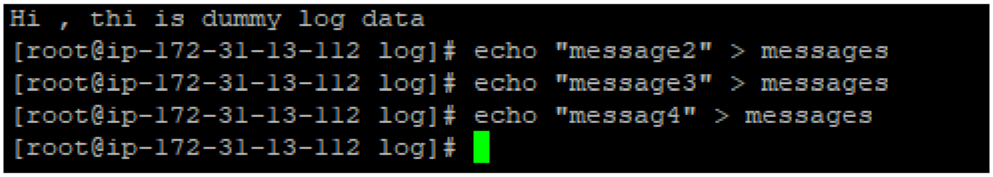
```
https://aws.amazon.com/amazon-linux-2/
2 package(s) needed for security, out of 13 available
Run "sudo yum update" to apply all updates.
[ec2-user@ip-172-31-13-112 ~]$ sudo vim /etc/awslogs/awslogs.conf
[ec2-user@ip-172-31-13-112 ~]$ sudo vim /etc/awslogs/awslogs.conf
[ec2-user@ip-172-31-13-112 ~]$ sudo vim /etc/awslogs/awslogs.conf
[ec2-user@ip-172-31-13-112 ~]$ sudo service awslogsd start
Redirecting to /bin/systemctl start awslogsd.service
[ec2-user@ip-172-31-13-112 ~]$ cd /var/log
[ec2-user@ip-172-31-13-112 log]$ sudo su
[root@ip-172-31-13-112 log]# ls -lrt
total 284
drwxr-x---  2 chrony chrony               6 May  1 01:01 chrony
-rw-------  1 root   root                 0 Jun 17 01:49 tallylog
-rw-r--r--  1 root   root               193 Jun 17 01:49 grubby_prune_debug
-rw-------  1 root   utmp                 0 Jun 17 01:49 btmp
-rw-------  1 root   root                 0 Jun 17 01:49 spooler
drwxr-sr-x+ 3 root   systemd-journal     46 Jul  6 22:12 journal
drwx------  2 root   root                23 Jul  6 22:12 audit
drwxr-xr-x  2 root   root                18 Jul  6 22:12 sa
-rw-r--r--  1 root   root             26778 Jul  6 22:12 dmesg
drwxr-xr-x  3 root   root                17 Jul  6 22:12 amazon
-rw-------  1 root   root               212 Jul  6 22:12 maillog
-rw-------  1 root   root              9189 Jul  6 22:12 boot.log
-rw-r-----  1 root   root              7112 Jul  6 22:12 cloud-init-output.log
-rw-r--r--  1 root   root            102888 Jul  6 22:12 cloud-init.log
-rw-------  1 root   root               194 Jul  6 22:14 yum.log
-rw-rw-r--  1 root   utmp              4992 Jul  6 22:49 wtmp
-rw-------  1 root   root               526 Jul  6 22:50 cron
-rw-------  1 root   root             77332 Jul  6 22:56 messages
-rw-------  1 root   root              9323 Jul  6 22:56 secure
-rw-r--r--  1 root   root            292292 Jul  6 22:56 lastlog
-rw-r--r--  1 root   root              2773 Jul  6 22:56 awslogs.log
[root@ip-172-31-13-112 log]# echo "Hi , thi is dummy log data" > messages
[root@ip-172-31-13-112 log]# ls -lrt
total 216
drwxr-x---  2 chrony chrony               6 May  1 01:01 chrony
-rw-------  1 root   root                 0 Jun 17 01:49 tallylog
-rw-r--r--  1 root   root               193 Jun 17 01:49 grubby_prune_debug
-rw-------  1 root   utmp                 0 Jun 17 01:49 btmp
-rw-------  1 root   root                 0 Jun 17 01:49 spooler
drwxr-sr-x+ 3 root   systemd-journal     46 Jul  6 22:12 journal
drwx------  2 root   root                23 Jul  6 22:12 audit
drwxr-xr-x  2 root   root                18 Jul  6 22:12 sa
-rw-r--r--  1 root   root             26778 Jul  6 22:12 dmesg
drwxr-xr-x  3 root   root                17 Jul  6 22:12 amazon
-rw-------  1 root   root               212 Jul  6 22:12 maillog
-rw-------  1 root   root              9189 Jul  6 22:12 boot.log
-rw-r-----  1 root   root              7112 Jul  6 22:12 cloud-init-output.log
-rw-r--r--  1 root   root            102888 Jul  6 22:12 cloud-init.log
-rw-------  1 root   root               194 Jul  6 22:14 yum.log
-rw-rw-r--  1 root   utmp              4992 Jul  6 22:49 wtmp
-rw-------  1 root   root               526 Jul  6 22:50 cron
-rw-r--r--  1 root   root            292292 Jul  6 22:56 lastlog
-rw-------  1 root   root              9536 Jul  6 22:57 secure
-rw-------  1 root   root                27 Jul  6 22:57 messages
-rw-r--r--  1 root   root              4219 Jul  6 22:57 awslogs.log
[root@ip-172-31-13-112 log]# cat message
cat: message: No such file or directory
[root@ip-172-31-13-112 log]# cat messages
Hi , thi is dummy log data
[root@ip-172-31-13-112 log]#
```

Check on cloudwatch



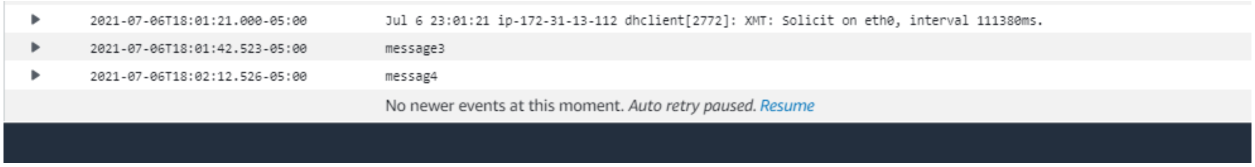
```
2021-07-06T17:36:52.000-05:00    Jul 6 22:36:52 ip-172-31-13-112 dhclient[2725]: DHCPREQUEST on eth0 to 172.31.0.1 port 67 (xid=0x38e829c5)
2021-07-06T17:36:52.000-05:00    Jul 6 22:36:52 ip-172-31-13-112 dhclient[2725]: DHCPACK from 172.31.0.1 (xid=0x38e829c5)
2021-07-06T17:36:53.000-05:00    Jul 6 22:36:53 ip-172-31-13-112 dhclient[2725]: bound to 172.31.13.112 -- renewal in 1385 seconds.
2021-07-06T17:36:53.000-05:00    Jul 6 22:36:53 ip-172-31-13-112 ec2net: [get_meta] Querying IMDS for meta-data/network/interfaces/macs/02:69:91:3d:9d:c5/local-ipv4s
2021-07-06T17:36:53.000-05:00    Jul 6 22:36:53 ip-172-31-13-112 ec2net: [get_meta] Getting token for IMDSv2.
2021-07-06T17:36:53.000-05:00    Jul 6 22:36:53 ip-172-31-13-112 ec2net: [get_meta] Trying to get http://169.254.169.254/latest/meta-data/network/interfaces/macs/02:69:91:3d:9d:c5/local-ipv4s
2021-07-06T17:36:53.000-05:00    Jul 6 22:36:53 ip-172-31-13-112 ec2net: [remove_aliases] Removing aliases of eth0
2021-07-06T17:37:00.000-05:00    Jul 6 22:37:00 ip-172-31-13-112 dhclient[2772]: XMT: Solicit on eth0, interval 119520ms.
2021-07-06T17:38:59.000-05:00    Jul 6 22:38:59 ip-172-31-13-112 dhclient[2772]: XMT: Solicit on eth0, interval 119050ms.
2021-07-06T17:40:01.000-05:00    Jul 6 22:40:01 ip-172-31-13-112 systemd: Created slice User Slice of root.
2021-07-06T17:40:01.000-05:00    Jul 6 22:40:01 ip-172-31-13-112 systemd: Started Session 5 of user root.
2021-07-06T17:40:01.000-05:00    Jul 6 22:40:01 ip-172-31-13-112 systemd: Removed slice User Slice of root.
2021-07-06T17:40:58.000-05:00    Jul 6 22:40:58 ip-172-31-13-112 dhclient[2772]: XMT: Solicit on eth0, interval 125960ms.
2021-07-06T17:43:05.000-05:00    Jul 6 22:43:05 ip-172-31-13-112 dhclient[2772]: XMT: Solicit on eth0, interval 124080ms.
2021-07-06T17:43:12.000-05:00    Jul 6 22:43:12 ip-172-31-13-112 systemd-logind: Removed session 4.
2021-07-06T17:43:12.000-05:00    Jul 6 22:43:12 ip-172-31-13-112 systemd: Removed slice User Slice of ec2-user.
2021-07-06T17:43:58.000-05:00    Jul 6 22:43:58 ip-172-31-13-112 systemd: Created slice User Slice of ec2-user.
2021-07-06T17:43:58.000-05:00    Jul 6 22:43:58 ip-172-31-13-112 systemd: Started Session 6 of user ec2-user.
2021-07-06T17:43:58.000-05:00    Jul 6 22:43:58 ip-172-31-13-112 systemd-logind: New session 6 of user ec2-user.
2021-07-06T17:45:09.000-05:00    Jul 6 22:45:09 ip-172-31-13-112 dhclient[2772]: XMT: Solicit on eth0, interval 122210ms.
2021-07-06T17:47:11.000-05:00    Jul 6 22:47:11 ip-172-31-13-112 dhclient[2772]: XMT: Solicit on eth0, interval 126590ms.
2021-07-06T17:49:04.000-05:00    Jul 6 22:49:04 ip-172-31-13-112 systemd-logind: Removed session 6.
2021-07-06T17:49:04.000-05:00    Jul 6 22:49:04 ip-172-31-13-112 systemd: Removed slice User Slice of ec2-user.
2021-07-06T17:49:18.000-05:00    Jul 6 22:49:18 ip-172-31-13-112 dhclient[2772]: XMT: Solicit on eth0, interval 125940ms.
2021-07-06T17:49:28.000-05:00    Jul 6 22:49:28 ip-172-31-13-112 systemd: Created slice User Slice of ec2-user.
2021-07-06T17:49:28.000-05:00    Jul 6 22:49:28 ip-172-31-13-112 systemd: Started Session 7 of user ec2-user.
2021-07-06T17:49:28.000-05:00    Jul 6 22:49:28 ip-172-31-13-112 systemd-logind: New session 7 of user ec2-user.
2021-07-06T17:50:01.000-05:00    Jul 6 22:50:01 ip-172-31-13-112 systemd: Created slice User Slice of root.
2021-07-06T17:50:01.000-05:00    Jul 6 22:50:01 ip-172-31-13-112 systemd: Started Session 8 of user root.
2021-07-06T17:50:01.000-05:00    Jul 6 22:50:01 ip-172-31-13-112 systemd: Removed slice User Slice of root.
2021-07-06T17:51:24.000-05:00    Jul 6 22:51:24 ip-172-31-13-112 dhclient[2772]: XMT: Solicit on eth0, interval 129810ms.
2021-07-06T17:53:34.000-05:00    Jul 6 22:53:34 ip-172-31-13-112 dhclient[2772]: XMT: Solicit on eth0, interval 109910ms.
2021-07-06T17:54:31.000-05:00    Jul 6 22:54:31 ip-172-31-13-112 systemd: Started awslogs daemon.
2021-07-06T17:55:24.000-05:00    Jul 6 22:55:24 ip-172-31-13-112 dhclient[2772]: XMT: Solicit on eth0, interval 124180ms.
2021-07-06T17:56:15.000-05:00    Jul 6 22:56:15 ip-172-31-13-112 su: (to root) ec2-user on pts/0
2021-07-06T17:57:28.000-05:00    Jul 6 22:57:28 ip-172-31-13-112 dhclient[2772]: XMT: Solicit on eth0, interval 113730ms.
2021-07-06T17:57:52.508-05:00    Hi , thi is dummy log data
                                 No newer events at this moment. Auto retry paused. Resume
```

Adding more data



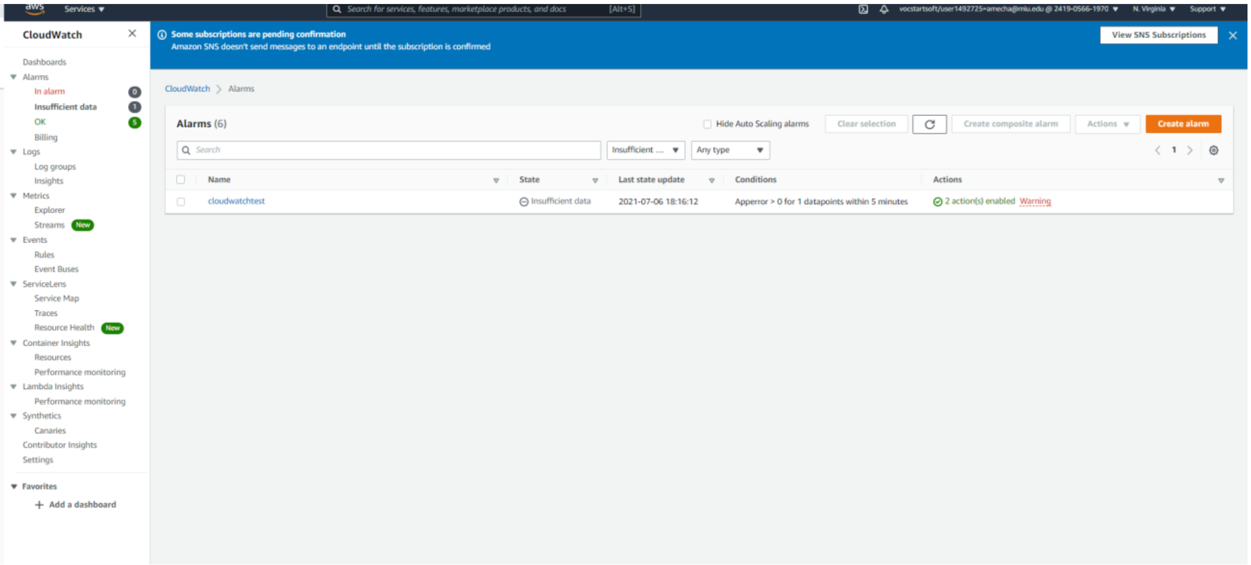
```
Hi , thi is dummy log data
[root@ip-172-31-13-112 log]# echo "message2" > messages
[root@ip-172-31-13-112 log]# echo "message3" > messages
[root@ip-172-31-13-112 log]# echo "messag4" > messages
[root@ip-172-31-13-112 log]#
```

On cloudwatch



```
2021-07-06T18:01:21.000-05:00    Jul 6 23:01:21 ip-172-31-13-112 dhclient[2772]: XMT: Solicit on eth0, interval 111380ms.
2021-07-06T18:01:42.523-05:00    message3
2021-07-06T18:02:12.526-05:00    messag4
                                 No newer events at this moment. Auto retry paused. Resume
```

Create alarm

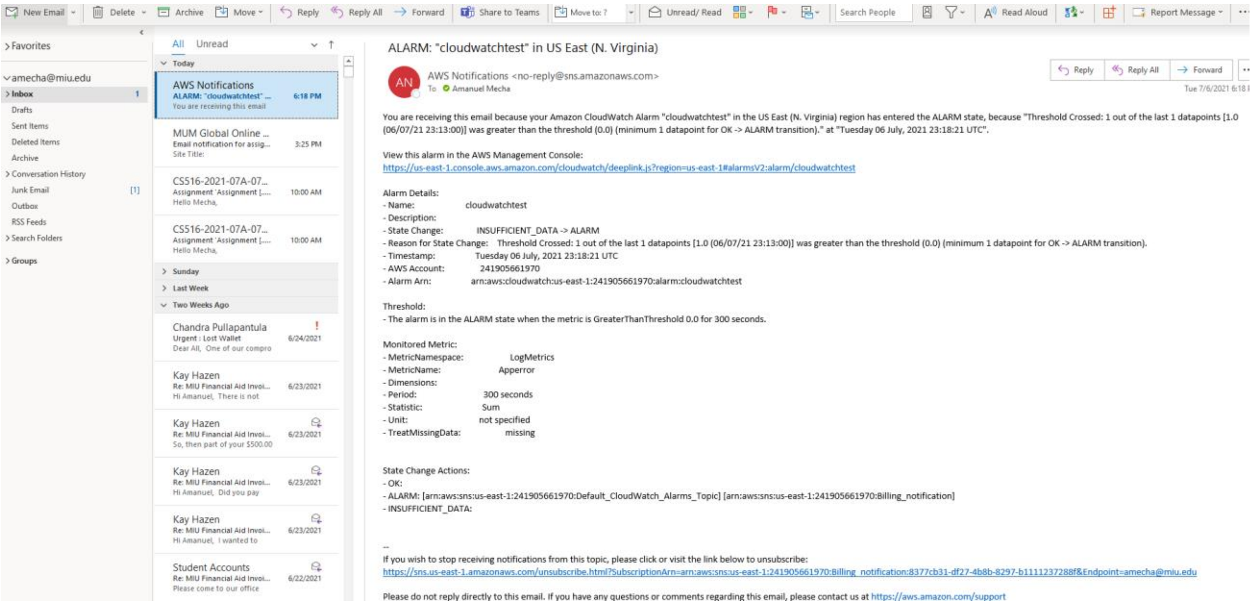


Some subscriptions are pending confirmation
Amazon SNS doesn't send messages to an endpoint until the subscription is confirmed

Alarms (6)

Name	State	Last state update	Conditions	Actions
cloudwatchtest	Insufficient data	2021-07-06 18:16:12	Apperror > 0 for 1 datapoints within 5 minutes	2 action(s) enabled Warning

Finally I notified through an email



ALARM: "cloudwatchtest" in US East (N. Virginia)

AWS Notifications <no-reply@sns.amazonaws.com>
To Amanuel Mecha

You are receiving this email because your Amazon CloudWatch Alarm "cloudwatchtest" in the US East (N. Virginia) region has entered the ALARM state, because "Threshold Crossed: 1 out of the last 1 datapoints [1.0 (06/07/21 23:13:00)] was greater than the threshold (0.0) (minimum 1 datapoint for OK -> ALARM transition)." at "Tuesday 06 July, 2021 23:18:21 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/cloudwatchtest

Alarm Details:
- Name: cloudwatchtest
- Description:
- State Change: INSUFFICIENT_DATA -> ALARM
- Reason for State Change: Threshold Crossed: 1 out of the last 1 datapoints [1.0 (06/07/21 23:13:00)] was greater than the threshold (0.0) (minimum 1 datapoint for OK -> ALARM transition).
- Timestamp: Tuesday 06 July, 2021 23:18:21 UTC
- AWS Account: 241905661970
- Alarm Arn: arn:aws:cloudwatch:us-east-1:241905661970:alarm:cloudwatchtest

Threshold:
- The alarm is in the ALARM state when the metric is GreaterThanThreshold 0.0 for 300 seconds.

Monitored Metric:
- MetricNamespace: LogMetrics
- MetricName: Apperror
- Dimensions:
- Period: 300 seconds
- Statistic: Sum
- Unit: not specified
- TreatMissingData: missing

State Change Actions:
- OK:
- ALARM: [arn:aws:sns:us-east-1:241905661970:Default_CloudWatch_Alarms_Topic] [arn:aws:sns:us-east-1:241905661970:Billing_notification]
- INSUFFICIENT_DATA:

--
If you wish to stop receiving notifications from this topic, please click or visit the link below to unsubscribe:
https://sns.us-east-1.amazonaws.com/unsubscribe.html?SubscriptionArn=arn:aws:sns:us-east-1:241905661970:Billing_notification:8377cb31-df27-4b8b-8297-b1111237288f&Endpoint=amecha@miu.edu

Please do not reply directly to this email. If you have any questions or comments regarding this email, please contact us at https://aws.amazon.com/support