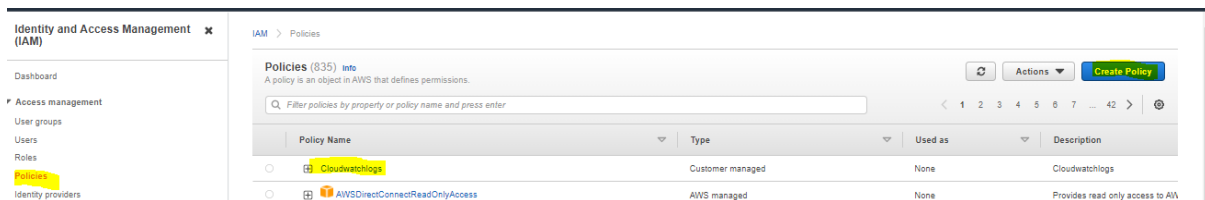


Cloud Watch Logs

Step:1

Create a custom policy using JSON

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



Step:2

Add that custom policy to the role

Create role

1 2 3 4

▼ Attach permissions policies

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

Create policy



Filter policies		Showing 7 results
	Policy name	Used as
<input type="checkbox"/>	AmazonAPIGatewayPushToCloudWatchLogs	None
<input type="checkbox"/>	AmazonDMSCloudWatchLogsRole	None
<input type="checkbox"/>	AWSAppSyncPushToCloudWatchLogs	None
<input type="checkbox"/>	AWSOpsWorksCloudWatchLogs	None
<input checked="" type="checkbox"/>	Cloudwatchlogs	None
<input type="checkbox"/>	CloudWatchLogsFullAccess	None
<input type="checkbox"/>	CloudWatchLogsReadOnlyAccess	None

* Required

Cancel

Previous

Next: Tags

Step:3

Review the role and create it

1234

Review

Provide the required information below and review this role before you create it.

Role name*

cloudlogs

Use alphanumeric and '+', '@', '-' characters. Maximum 64 characters.

Role description

Allows EC2 instances to call AWS services on your behalf.

Maximum 1000 characters. Use alphanumeric and '+', '@', '-' characters.

Trusted entities

AWS service: ec2.amazonaws.com

Policies

Cloudwatchlogs

Permissions boundary

Permissions boundary is not set

The new role will receive the following tag

Key	Value
Cloudlog	Cloudlog

* Required

Cancel

Previous

Create role

Step:4

Create a webserver allow port 80 and attach the IAM role to the particular server.

```
#!/bin/bash
```

```
sudo su
```

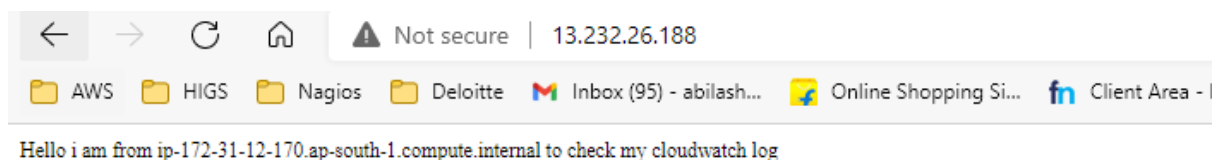
```
yum update -y
```

```
yum install httpd -y #apache
```

```
systemctl start httpd
```

```
systemctl enable httpd #server restart
```

```
echo "Hello i am from $(hostname -f) to check my cloudwatch log" > /var/www/html/index.html
```



Step:5

Login to the server update and Install the awslogs package.

```
sudo yum update -y
```

```
sudo yum install -y awslogs
```

```
Downloading packages:
(1/2): aws-cli-plugin-cloudwatch-logs-1.4.6-1.amzn2.0.1.no | 62 kB 00:00
(2/2): awslogs-1.1.4-3.amzn2.noarch.rpm | 8.2 kB 00:00
-----
Total 534 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-172-31-12-170 ~]$
```

Step:6

- Edit the /etc/awslogs/awslogs.conf file to configure the logs to track.
- By default, the /etc/awslogs/awscli.conf points to the us-east-1 Region. To push your logs to a different Region, edit the awscli.conf file and specify that Region.

```
[/var/log/httpd/access_log]
datetime_format = %b %d %H:%M:%S
file = /var/log/httpd/access_log
buffer_duration = 5000
log_stream_name = Webserver-{instance_id}
initial_position = start_of_file
log_group_name = WEBSERVER
```

```
GNU nano 2.9.8 awscli.conf

[plugins]
cwlogs = cwlogs
[default]
region = ap-south-1
```

Step:7

If you are running Amazon Linux 2, start the awslogs service and enable it on system boot.

```
sudo systemctl start awslogsd
```

```
sudo systemctl enable awslogsd.service
```

```
[ec2-user@ip-172-31-12-170 awslogs]$ sudo systemctl start awslogsd
[ec2-user@ip-172-31-12-170 awslogs]$ sudo systemctl enable awslogsd.service
Created symlink from /etc/systemd/system/multi-user.target.wants/awslogsd.service to /usr/lib/systemd/system/awslogsd.service.
```

Step:8

Access the site and check the logs in the cloud watch logs section you can able to see the logs

The screenshot displays the AWS CloudWatch console interface. On the left, there is a navigation menu with options like Dashboards, Alarms, Logs, and Metrics. The main area shows a list of log groups, with 'WEBSERVER' selected. Below this, the 'Log events' section is visible, showing a list of log entries with timestamps and messages. The messages include HTTP requests and responses, such as 'GET / HTTP/1.1' and '200 OK'.

Timestamp	Message
2021-08-12T13:05:51.871+05:30	223.182.197.20 - - [12/Aug/2021:07:22:39 +0000] "GET / HTTP/1.1" 200 88 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/92.0.4515.159 Safari/537.36"
2021-08-12T13:05:51.871+05:30	223.182.197.20 - - [12/Aug/2021:07:22:39 +0000] "GET /Favicon.ico HTTP/1.1" 404 196 "http://13.232.26.188/" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/92.0.4515.159 Safari/537.36"
2021-08-12T13:06:25.081+05:30	223.182.197.20 - - [12/Aug/2021:07:36:24 +0000] "GET / HTTP/1.1" 304 - "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/92.0.4515.159 Safari/537.36"
2021-08-12T13:06:49.088+05:30	223.182.197.20 - - [12/Aug/2021:07:36:48 +0000] "GET / HTTP/1.1" 200 88 "-" "Mozilla/5.0 (iPhone; CPU iPhone OS 14_1 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/14.0 Mobile/15E148 Safari/604.1"
2021-08-12T13:06:49.089+05:30	223.182.197.20 - - [12/Aug/2021:07:36:48 +0000] "GET /Favicon.ico HTTP/1.1" 404 196 "http://13.232.26.188/" "Mozilla/5.0 (iPhone; CPU iPhone OS 14_1 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/14.0 Mobile/15E148 Safari/604.1"

IT WORKS 😊