

# Lab 8: Logging to CloudWatch via CLI and OpenSearch

---

## Objective

This lab teaches students how to manually send logs to AWS CloudWatch Logs using AWS CLI, understand log group/stream mechanics, and optionally stream to OpenSearch for visualization. This version avoids the complexity and pitfalls of the CloudWatch Agent setup.

## Prerequisites

- AWS Free Tier account with CloudWatch and IAM access
- EC2 instance (Amazon Linux 2) with an IAM role that has the following permissions:
  - logs:CreateLogGroup
  - logs:CreateLogStream
  - logs:PutLogEvents
- AWS CLI preinstalled (comes with CloudShell and Amazon Linux)
- Region set with `aws configure set region <your-region>`

## Lab Steps

### Step 1: Create a CloudWatch Log Group

Run the following command to create a log group:

```
aws logs create-log-group --log-group-name /ec2/manual-log
```

---

### Step 2: Create a Log Stream

```
aws logs create-log-stream --log-group-name /ec2/manual-log --  
log-stream-name manual-stream
```

---

### Step 3: Send a Log Event

Create a timestamp and send a basic log message:

```
timestamp=$(date +%s%3N)
```

---

```
aws logs put-log-events --log-group-name /ec2/manual-log --log-stream-name manual-stream --log-events timestamp=$timestamp,message="Test log message from CLI"
```

---

#### **Step 4: Verify in Console**

Go to CloudWatch → Log Groups → /ec2/manual-log → manual-stream and verify your message.

#### **Optional Extension: Streaming to OpenSearch**

Configure a Lambda or Kinesis Firehose to stream CloudWatch logs to OpenSearch.

#### **Summary**

This lab demonstrated how to interact with CloudWatch Logs using CLI for better control and visibility.

It avoids complexities of agent configuration and gives students direct insight into AWS logging APIs.