Project in AWS
Practice Lab

Implement Advanced CloudWatch Monitoring for a Web Server

Andra-Diana Popescu

2025

ABOUT THIS LAB

CloudWatch Logs centralizes the logs from all of your systems, applications, and AWS services that you use, in a single, highly scalable service. In this lab, you will configure an EC2 instance to stream its Apache web server error logs to CloudWatch Logs. You will configure the agent and then log in to the CloudWatch Logs console to make sure the logs are streamed correctly. By the end of this lab, you will understand how to install the CloudWatch Logs agent and configure it to stream a log to the service.

LEARNING OBJECTIVES

- Download and Run the CloudWatch Logs Installer
- Configure CloudWatch Logs
- Log In to the CloudWatch Logs Website

AWS Documentation about CloudWatch:

https://aws.amazon.com/cloudwatch/faqs/#topic-0

https://docs.aws.amazon.com/AmazonCloudWatch/latest/monitoring/cloudwatch_concepts.html

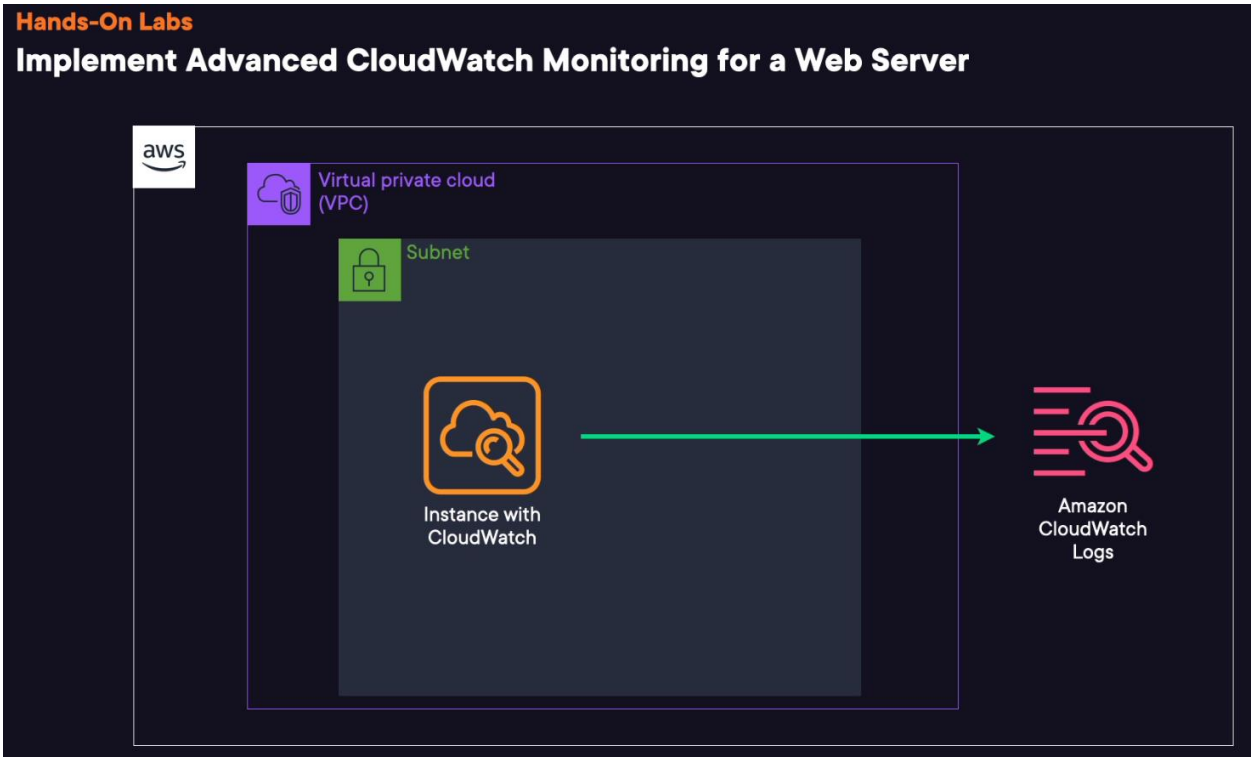
https://docs.aws.amazon.com/AmazonCloudWatch/latest/monitoring/CloudWatch-Agent-Configuration-File-Details.html

https://docs.aws.amazon.com/AmazonCloudWatch/latest/monitoring/create-cloudwatch-agent-configuration-file-wizard.html

Source: https://learn.acloud.guru/course/certified-solutions-architect-associate/

Table of Contents

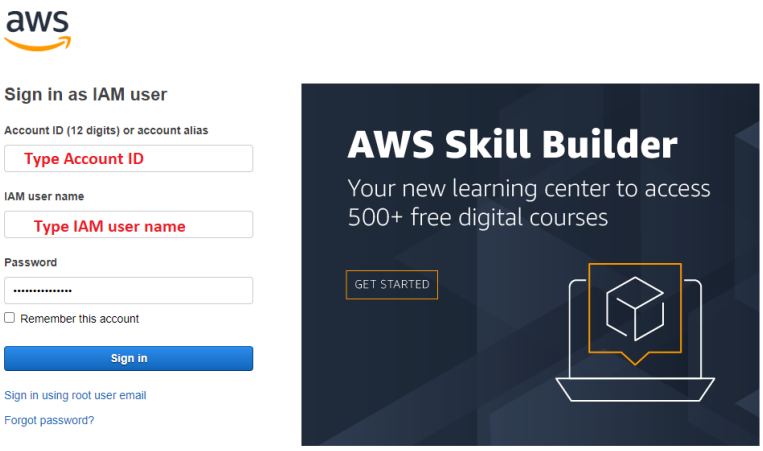
Lab Diagrams



We have the AWS account in **us-east-1** Region. In this lab, you're setting up a new web server for a company which will host a critical application. You've been asked to store the Apache Web logs in an Amazon CloudWatch log group in case any problems occur on the server.

You'll be logging into the EC2 instance and installing the CloudWatch Logs agent. Once installed, you'll be configuring the CloudWatch logs agent to send copies of the Apache Web logs to the CloudWatch Logs group.

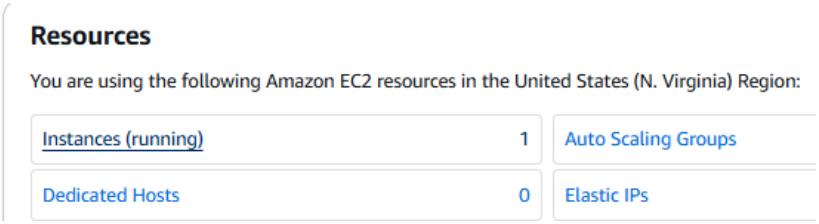
Log in to your AWS account



1. Download and Run the CloudWatch Logs Installer

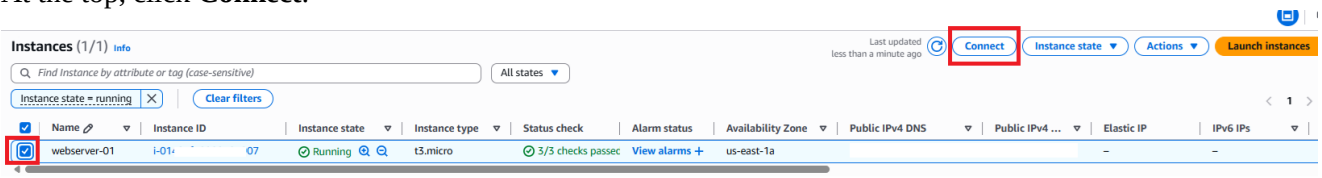
1. Once you are logged in to the AWS Management Console, navigate to **EC2**.

2. Click **Instances (running).**

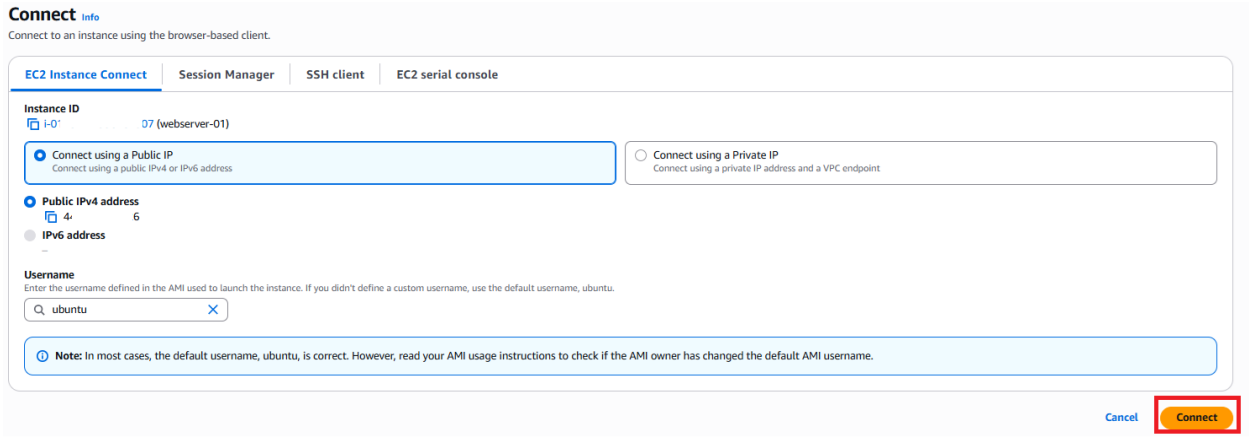


3. Click the checkbox next to ***webserver-01***. Please give the lab an extra few minutes before connecting to ***webserver-01***.

4. At the top, click **Connect**.



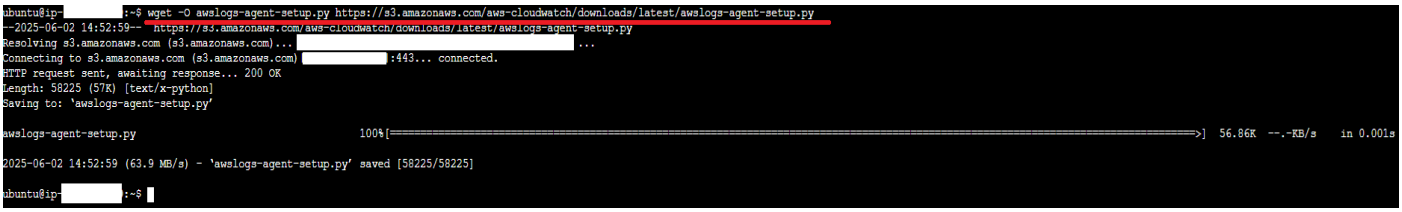
5. At the bottom of the page, click **Connect** to access the CLI.



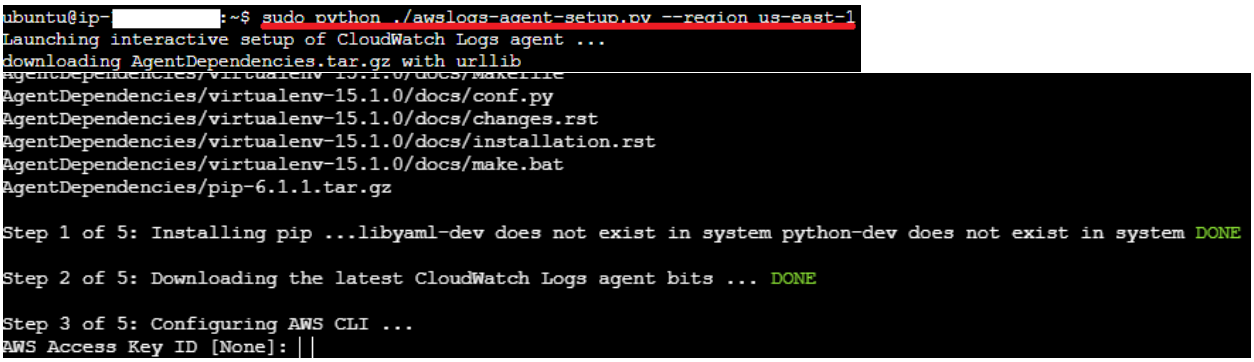
6. Run the following commands to install the CloudWatch Logs agent:

wget -O awslogs-agent-setup.py https://s3.amazonaws.com/aws-cloudwatch/downloads/latest/awslogs-agent-setup.py

Note: This command fetches the aws-logs-agent-setup file from the S3 bucket where it's stored.



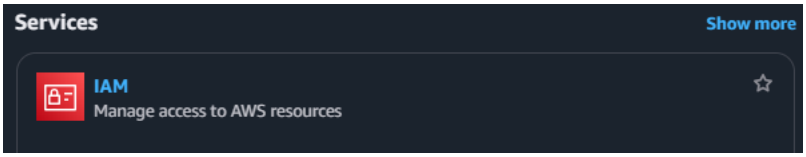
sudo python ./awslogs-agent-setup.py --region us-east-1



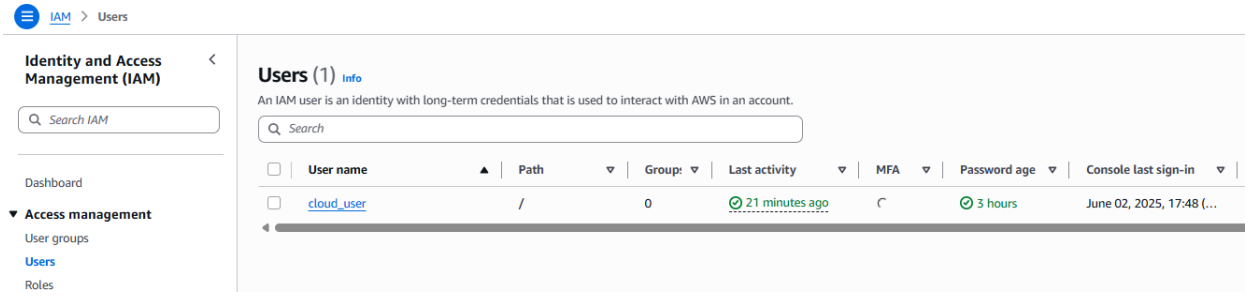
Note: This command executes the setup.py file and targets the server to the default region of us-east-1. Once a CloudWatch Logs agent has finished downloading, you'll move on to **step 3 of 5**, which is where you'll need an AWS access key and a secret access key to complete the configuration. Our cloud user account currently does not have an access key we can use.

2. Configure CloudWatch Logs

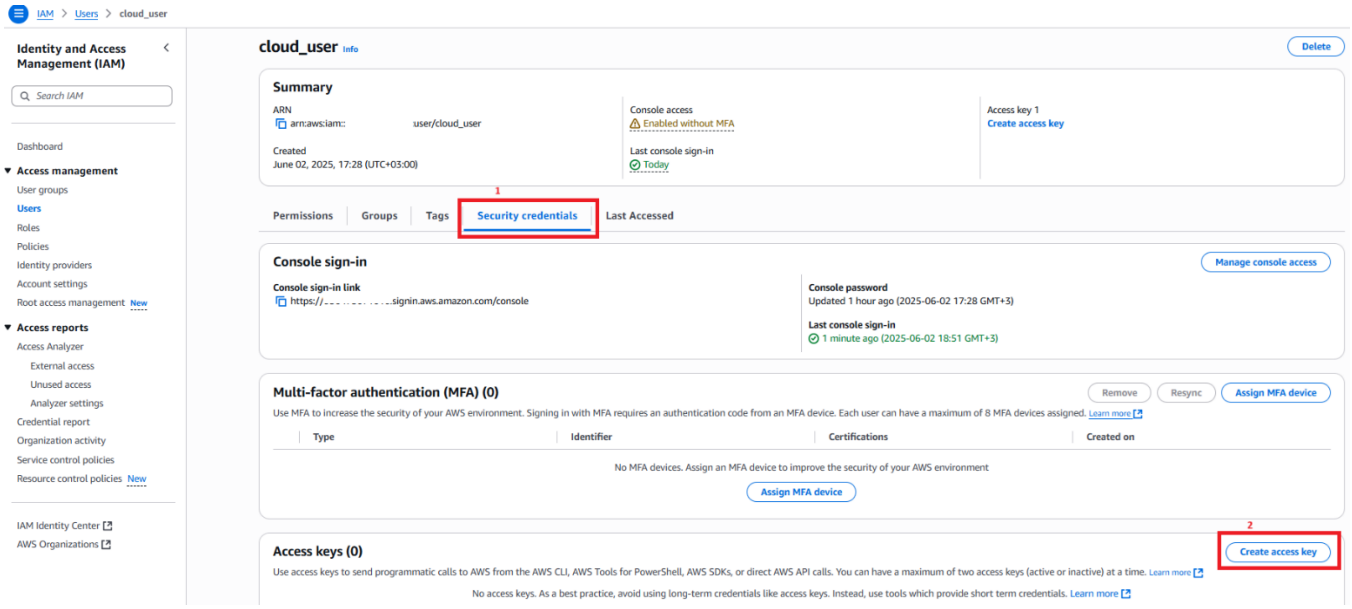
1. Go back to the AWS Management Console, and open **IAM** in a separate tab.



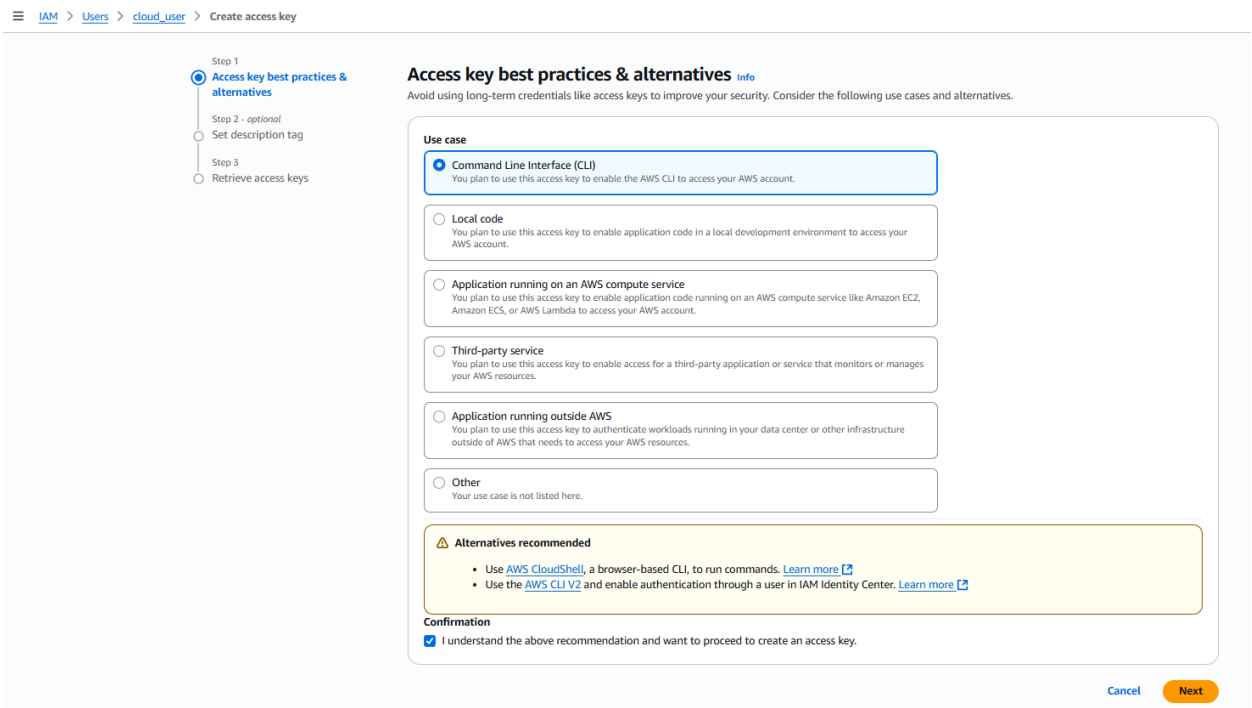
2. Click **Users**.
3. Click **cloud_user**.



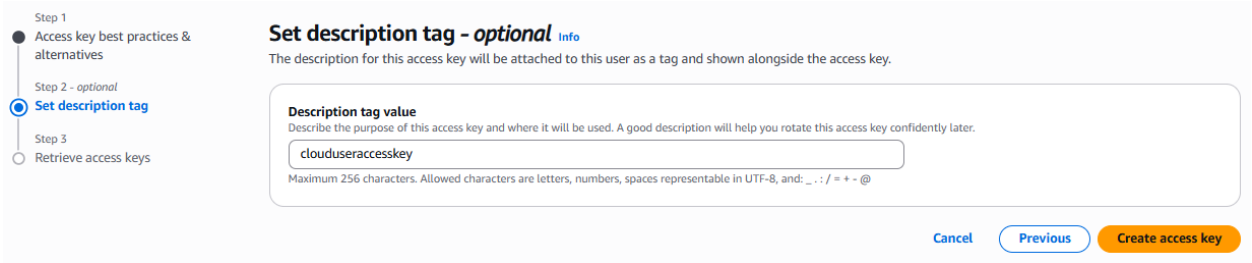
4. Select the **Security credentials** tab.
5. Click **Create access key**.



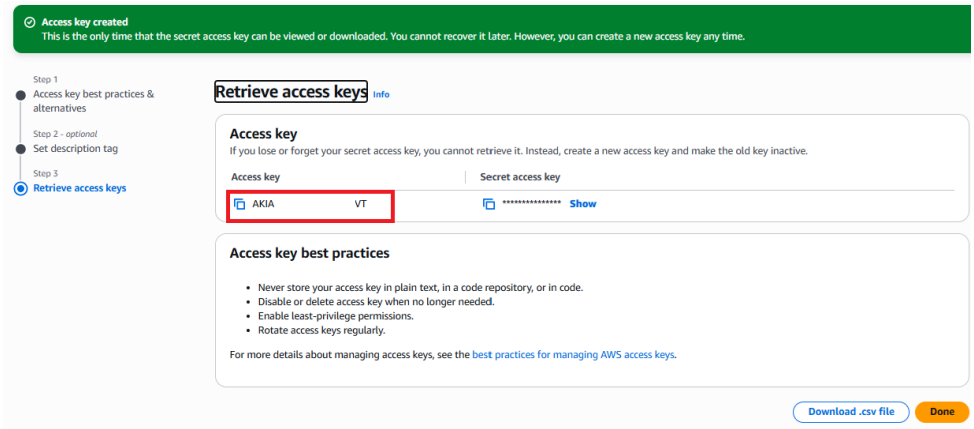
6. Select **Command Line Interface (CLI)**.
7. Check the acknowledgment checkbox at the bottom of the page and click **Next**.



8. For **Description tag value**, enter ***clouduseraccesskey***.
9. Click **Create access key**.



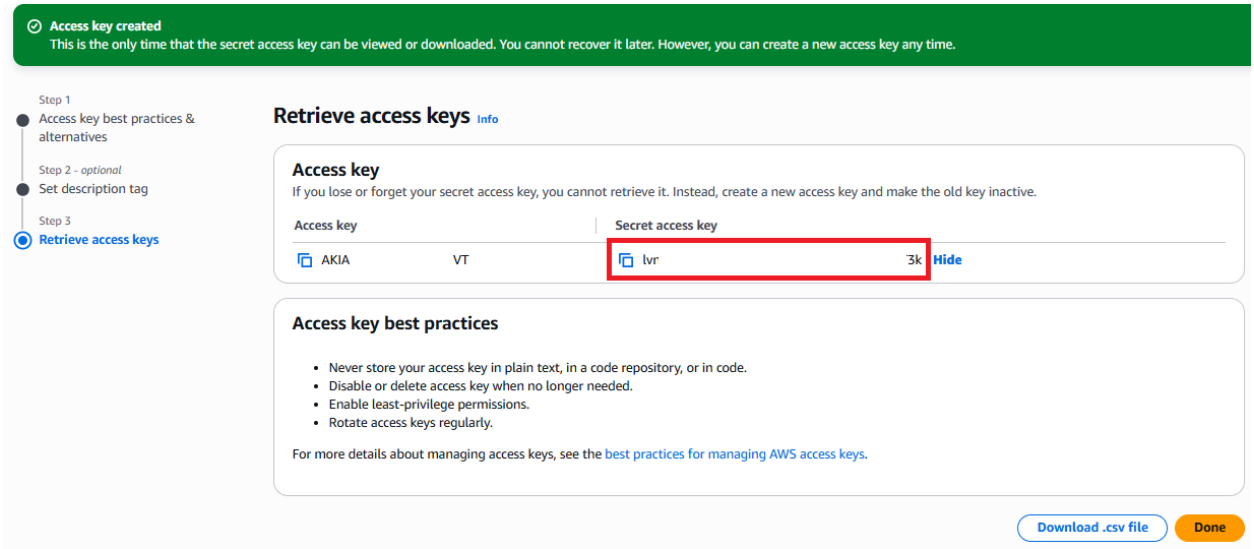
10. Copy the **Access key**.



11. Go back to the CLI (keep IAM open in the other tab), paste the **Access key ID**, and press **Enter**.

```
Step 3 of 5: Configuring AWS CLI ...
AWS Access Key ID [None]: AKIA                    VT
```

12. Go back to IAM and, in the **Secret access key** on the right, click **Show**. Then, copy the **Secret access key**.



13. Go back to the CLI, paste the **Secret access key**, and press **Enter**.

```
AWS Secret Access Key [None]: lvn                    3k
Default region name [us-east-1]:
```

14. Press **Enter** twice to accept the default region name and output format.

```
Default region name [us-east-1]:
Default output format [None]:

Step 4 of 5: Configuring the CloudWatch Logs Agent ...
Path of log file to upload [/var/log/syslog]:
```

15. Copy and paste the below path for the log file to upload:

    /var/log/apache2/error.log

```
Step 4 of 5: Configuring the CloudWatch Logs Agent ...
Path of log file to upload [/var/log/syslog]: /var/log/apache2/error.log
Destination Log Group name [/var/log/apache2/error.log]:
```

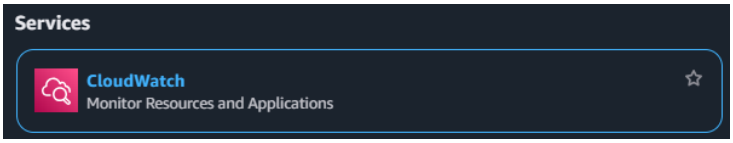
16. Press **Enter** to keep the current Destination Log Group name.
17. Press **Enter** to accept the default Log Stream name.
18. Press **Enter** to keep the default Log Event timestamp format.
19. Press **1** to select **From start of file as** the initial position of upload.
20. Type **N** to complete the configuration.

```
Destination Log Group name [/var/log/apache2/error.log]:

Choose Log Stream name:
  1. Use EC2 instance id.
  2. Use hostname.
  3. Custom.
Enter choice [1]:

Choose Log Event timestamp format:
  1. %b %d %H:%M:%S    (Dec 31 23:59:59)
  2. %d/%b/%Y:%H:%M:%S (10/Oct/2000:13:55:36)
  3. %Y-%m-%d %H:%M:%S (2008-09-08 11:52:54)
  4. Custom
Enter choice [1]:

Choose initial position of upload:
  1. From start of file.
  2. From end of file.
Enter choice [1]: 1
More log files to configure? [Y]: n

Step 5 of 5: Setting up agent as a daemon ...DONE


- Configuration file successfully saved at: /var/awslogs/etc/awslogs.conf
- You can begin accessing new log events after a few moments at https://console.aws.amazon.com/cloudwatch/home?region=us-east-1#logs:
- You can use 'sudo service awslogs start|stop|status|restart' to control the daemon.
- To see diagnostic information for the CloudWatch Logs Agent, see /var/log/awslogs.log
- You can rerun interactive setup using 'sudo python ./awslogs-agent-setup.py --region us-east-1 --only-generate-config'
------------------------------------------------------
ubuntu@ip-          :~$
```

Note: The agent's been configured, you can access the log events through the URL provided or type CloudWatch in the search bar.

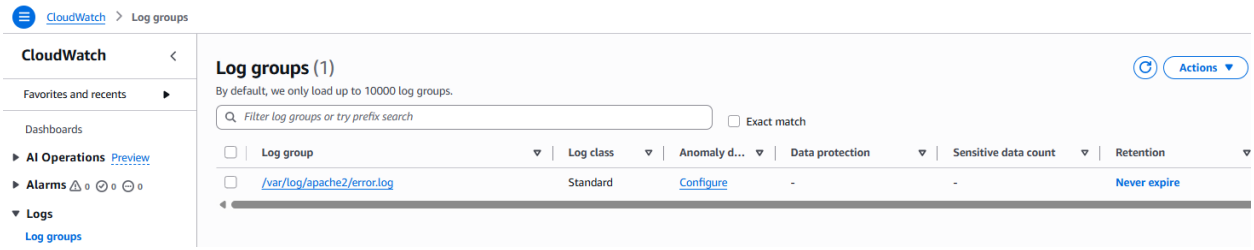
3. Log In to the CloudWatch Logs Website

1. In the search bar, enter **CloudWatch**, and right-click to open it in a new tab.

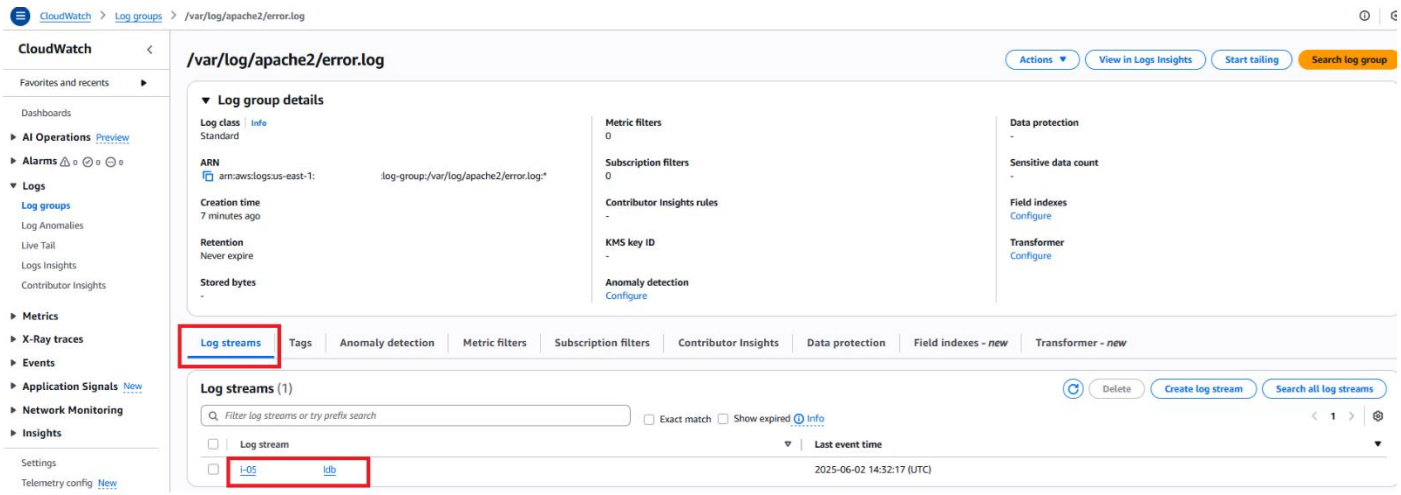


2. Click **Log groups**.

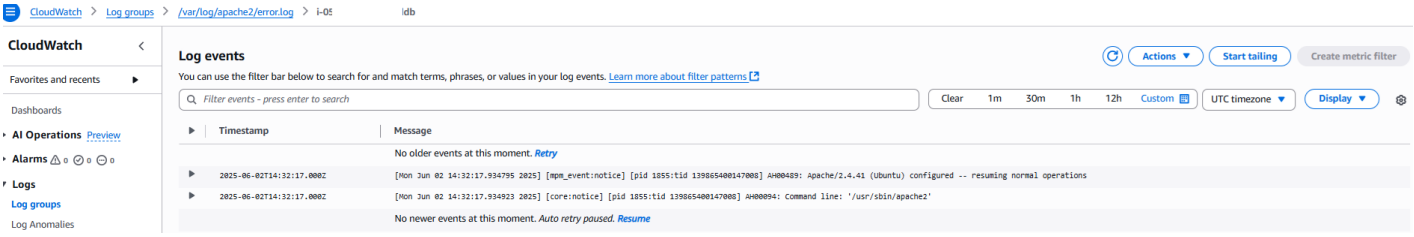
3. Click **/var/log/apache2/error.log**; if you don't see it yet, click the **Refresh** button.



4. Under **Log streams**, click the link for the instance identifier. You will see the contents of your error log with two events logged.



As you can see, we already have two log file entries already uploaded to our log stream. We can confirm these are the only lines already in our log file.



5. You can also view the contents of the error log in the CLI by running the following command:

sudo cat /var/log/apache2/error.log

```
ubuntu@ip-          :~$ sudo cat /var/log/apache2/error.log
[Mon Jun 02 14:32:17.934795 2025] [mpm_event:notice] [pid 1855:tid 139865400147008] AH00489: Apache/2.4.41 (Ubuntu) configured -- resuming normal operations
[Mon Jun 02 14:32:17.934923 2025] [core:notice] [pid 1855:tid 139865400147008] AH00094: Command line: '/usr/sbin/apache2'
ubuntu@ip-          :~$
```

We can see here we have the same two log file lines as we've already been displayed in our log stream.