



## Your application is failing intermittently. How would you use CloudWatch Logs Insights to troubleshoot?

### Answer:

CloudWatch Logs Insights is great for searching patterns in logs quickly.

Here's how I'd use it:

- Go to CloudWatch Logs Insights
- Select the log group for the application (e.g., /ecs/my-app or /var/log/messages)
- Use **queries like**:

```
sql
```

```
-----
```

```
fields @timestamp, @message
```

```
| filter @message like /error/
```

```
| sort @timestamp desc
```

```
| limit 50
```

- If it's intermittent, I might query over a wider time range (last 6 hours or 12 hours).
- I'd look for patterns: specific exceptions, timeouts, or missing values in request payloads.

### Example:

Once our ECS app had 502 Gateway errors, but only some users saw them. Using Logs Insights, I filtered logs by status=502 and traced them back to requests missing a token. It turned out to be a client-side issue.

## Which AWS service allows you to run queries to analyze and troubleshoot application logs in near real-time?

- A. AWS X-Ray
- B. CloudWatch Logs Insights


- C. AWS Athena
- D. Amazon QuickSight

B. CloudWatch Logs Insights 

---

**If an application fails intermittently, what is the best initial step in CloudWatch Logs Insights?**


- A. Enable VPC Flow Logs
- B. Select the relevant log group and run targeted queries
- C. Create an S3 bucket to store logs
- D. Turn on CloudTrail for the account

B. Select the relevant log group and run targeted queries 

---

**Why might you increase the time range (e.g., last 6 or 12 hours) when troubleshooting intermittent failures in CloudWatch Logs Insights?**


- A. To reduce query costs
- B. To capture more log events and spot patterns over time
- C. To avoid rate-limiting
- D. To improve dashboard refresh speed

B. To capture more log events and spot patterns over time 

---

**In the example where an ECS app had 502 Gateway errors for some users, how was the root cause identified using CloudWatch Logs Insights?**

- A. By enabling debug logging on the ECS service
- B. By filtering logs for status=502 and tracing to requests missing a token
- C. By checking CloudTrail for API failures
- D. By inspecting EC2 CPU usage metrics

B. By filtering logs for status=502 and tracing to requests missing a token 

---

---