

## AWS DevOps Interview Questions (4 Years Experience)

### Monitoring & Logging Interview Questions with Detailed Answers

Q: How do you monitor applications in AWS?

A: In AWS, application monitoring is done using:

- Amazon CloudWatch (metrics, logs, dashboards)
- AWS X-Ray (tracing)
- Third-party tools (Datadog, Prometheus, etc.)

CloudWatch monitors:

- EC2 instance metrics
- Lambda invocations/errors
- Custom metrics

Real-time example: We monitored memory, CPU, disk usage on EC2 using CloudWatch Agent, and visualized metrics in CloudWatch Dashboards.

Q: What are custom metrics in CloudWatch and how do you use them?

A: Custom metrics are user-defined data points sent to CloudWatch.

Usage:

- Use AWS CLI, SDK, or CloudWatch Agent to push metrics
- Visualize using dashboards
- Set alarms for thresholds

## AWS DevOps Interview Questions (4 Years Experience)

Real-time example: We sent app-specific metrics like number of logged-in users per minute from a Python app using `put-metric-data` and triggered alerts based on traffic spikes.

Q: Difference between CloudWatch Logs and CloudTrail?

A: CloudWatch Logs: Collects log data from applications, OS, AWS services.

CloudTrail: Records AWS API calls for governance, compliance, and auditing.

Feature	CloudWatch Logs	CloudTrail
Purpose	Application/system logging	API activity tracking
Data Type	Log streams	Event history
Use Case	Debugging, monitoring	Security auditing, compliance

Real-time example: We used CloudTrail to detect unauthorized IAM access, and CloudWatch Logs to debug Lambda timeouts.

Q: How do you set up alarms and notifications?

- A:
1. Create CloudWatch Alarm on a metric (e.g., CPU > 80%)
  2. Attach alarm to an SNS topic
  3. Subscribe email/SMS endpoints to SNS topic

Real-time example: When EC2 CPU > 85% for 5 mins, a CloudWatch Alarm triggered an SNS notification

## AWS DevOps Interview Questions (4 Years Experience)

sent to Slack via webhook and to on-call engineers via email.

Q: How do you trace issues in serverless (Lambda) architecture?

A: For tracing Lambda:

- Enable active tracing with AWS X-Ray
- Review CloudWatch Logs for error details
- Use structured logging (JSON format)

Real-time example: A payment Lambda function was timing out. X-Ray showed delays in the downstream SQS call. Logs confirmed the queue was overloaded.

Q: How do you visualize logs and metrics effectively?

A: Visualization tools:

- CloudWatch Dashboards (native)
- Kibana (via Elasticsearch)
- Grafana (for Prometheus, CloudWatch)

Real-time example: We pushed logs from EC2 to CloudWatch, and metrics to Prometheus. Grafana dashboards displayed real-time latency, error rate, and request volume for our services.