Mock Interview Guide

Amazon CloudWatch

Instructions for Interviewer:

- You are playing the role of **interviewer**. Use this guide as a script.
- Ask each question one at a time. Follow the steps: **Definition → Details → Scenario → Follow-up.**
- If the interviewee struggles, use the **hint**.
- The goal is to keep it conversational and practical. Help the interviewee think and express their learning.
- **colors assigned:** Questions Answers Hint

Freshers - Level

Amazon CloudWatch

(10 Easy Interview Questions)

---

1. "What is Amazon CloudWatch?"

Expected Answer: CloudWatch is a monitoring and observability service provided by AWS to track metrics, logs, and events.

Hint: Think AWS monitoring for everything — servers, apps, logs.

2. "What types of data can CloudWatch collect?"

Expected Answer: Metrics, logs, events, and alarms from AWS services or custom sources.

Hint: Logs + metrics + events = full monitoring.

3. “What is a CloudWatch metric?”

Expected Answer: A metric is a time-ordered set of data points that represent the performance of a resource.

Hint: CPU usage, memory, or request count are examples.

4. “What are CloudWatch Alarms?”

Expected Answer: Alarms monitor a metric and trigger actions if it crosses a threshold.

Hint: Set thresholds to get notified or take action.

5. “How does CloudWatch get data from EC2 instances?”

Expected Answer: CloudWatch automatically collects some metrics, but you can also install the CloudWatch agent for detailed stats.

Hint: Default vs custom metrics.

6. “What is the retention period for CloudWatch logs?”

Expected Answer: By default, logs are kept indefinitely, but you can change the retention settings.

Hint: You control how long logs are kept.

7. “Can CloudWatch monitor non-AWS servers?”

Expected Answer: Yes, using the CloudWatch Agent and custom metrics, even on-prem servers can be monitored.

Hint: Install agent and send data manually.

8. “How do you view metrics in CloudWatch?”

Expected Answer: Through the CloudWatch Console > Metrics section.

Hint: Visual dashboards show everything.

9. “What is the default interval for basic EC2 metrics in CloudWatch?”

Expected Answer: 5 minutes.

Hint: Detailed monitoring brings it down to 1 minute.

10. “Can you use CloudWatch to trigger automated actions?”

Expected Answer: Yes, alarms can trigger SNS, Lambda, Auto Scaling, or EC2 actions.

Hint: Monitoring + Automation = Power.

SCENARIO-BASED INTERVIEW QUESTIONS

1. **You receive no metrics from your EC2 instance in CloudWatch. What could be the issue?**

   Expected Answer: The instance may not have CloudWatch agent installed or IAM permissions may be missing.

   Hint: Check agent and IAM role.

2. **You want to monitor memory usage, but it's not showing in metrics. Why?**

   Expected Answer: Memory is not part of basic EC2 metrics — CloudWatch Agent is needed for custom metrics.

   Hint: Install and configure the agent.

3. **An alarm keeps triggering unexpectedly. What might be wrong?**

   Expected Answer: The threshold may be incorrectly set, or the evaluation period is too short.

   Hint: Review threshold logic.

4. **You're asked to send a custom app metric to CloudWatch. How do you do it?**

   Expected Answer: Use the AWS CLI or SDK with PutMetricData API.

Hint: Custom metrics must be pushed manually.

5. **You want to monitor CPU across multiple EC2 instances. What's the best way?**

Expected Answer: Use metric math or dashboards to group and analyze metrics.

Hint: Combine metrics for better visibility.

PROJECT-BASED INTERVIEW QUESTIONS

---

1. **How would you set up basic monitoring for an EC2 instance in CloudWatch?**

Expected Answer:

- **Ensure EC2 instance has appropriate IAM role**
- **Use basic metrics (CPU, disk, network)**
- **Set alarms for thresholds**

Hint: Start with default metrics.

2. You want to notify your team when CPU usage exceeds 80%. How would you do it?

Expected Answer:

- **Create a CloudWatch alarm**
- **Set threshold and add SNS topic**
- **Subscribe team email to SNS**

Hint: Alarm → SNS → Email.

3. How would you collect and view application logs in CloudWatch?

Expected Answer:

- **Install CloudWatch Agent**
- **Configure log file paths**
- **View logs under CloudWatch Logs**

Hint: Push logs using agent.

4. You want to monitor a scheduled job’s success/failure. How do you track this in CloudWatch?

Expected Answer:

- **Log output to CloudWatch Logs**
- **Create metric filters for "Success"/"Failure" keywords**
- **Trigger alarms on failures**

Hint: Logs → filter → alarm.

Medium - Level

Amazon CloudWatch

(Interview Questions- 1 to 2 Years Experience)

1. **“What is CloudWatch Agent and when do you use it?”**

    Expected Answer: It's a software agent that collects system-level metrics and logs from EC2 or on-prem servers.

    Hint: Use when default metrics aren’t enough.

2. **“How does metric math work in CloudWatch?”**

    Expected Answer: Metric math lets you perform calculations (sum, average, rate, etc.) on one or more metrics.

    Hint: Visual calculations with formulas.

3. **“What are Composite Alarms?”**

    Expected Answer: Alarms based on the state of multiple other alarms using logic operators (AND, OR).

    Hint: Combine multiple checks into one.

4. **“What is the difference between standard and detailed monitoring?”**

Expected Answer: Standard provides 5-minute intervals, while detailed gives 1-minute metrics.

Hint: More granularity = better alerting.

5. “What is a metric filter in CloudWatch Logs?”

Expected Answer: It extracts numerical values or keywords from log entries to create custom metrics.

Hint: Turn logs into triggerable metrics.

6. “Can CloudWatch trigger Lambda functions?”

Expected Answer: Yes, alarms or scheduled events can invoke Lambda directly.

Hint: Automation using Lambda + CloudWatch.

7. “What is the default retention for CloudWatch metrics?”

Expected Answer: 15 months, with decreasing resolution over time.

Hint: Old metrics stay — but lose precision.

8. “How does cross-account log monitoring work?”

Expected Answer: Use resource policies and centralized log collection via subscription filters.

Hint: Share logs securely across accounts.

9. **“What is the role of CloudWatch Events?”**

Expected Answer: It responds to AWS resource state changes and schedules actions.

Hint: It’s AWS's event-based trigger system.

10. **“Can you send metrics from a non-AWS app to CloudWatch?”**

Expected Answer: Yes, by using the PutMetricData API or CLI.

Hint: Push metrics programmatically.

SCENARIO-BASED INTERVIEW QUESTIONS

---

1. **You receive CPU alarms daily, but performance is unaffected. What should you do?**

Expected Answer: Check threshold levels and evaluation windows; optimize or suppress noisy alarms.

Hint: Tune your alert sensitivity.

2. **You want to monitor error rates in app logs. What’s your approach?**

Expected Answer: Use metric filters to search for “ERROR” strings and create a custom metric.

Hint: Keywords in logs → metric.

3. **You need to track multiple alarms and notify only if all are triggered. How?**

Expected Answer: Use a composite alarm with AND condition across all individual alarms.

Hint: Combine for smarter alerting.

4. **A new EC2 instance doesn’t appear in your dashboard. What could be missing?**

Expected Answer: It may lack proper IAM roles, or metrics aren't enabled/configured.

Hint: Check permissions + agent config.

5. **You want to analyze historical CPU trends. How do you do it in CloudWatch?**

Expected Answer: Use the CloudWatch console or GetMetricData API with time ranges and visualization.

Hint: Graph it over time.

PROJECT-BASED INTERVIEW QUESTIONS

---

1. **Design a CloudWatch-based alerting system for a multi-tier web app**

Expected Answer:

- **Alarms for EC2, RDS, ELB, and app logs**
- **Group alerts via SNS**
- **Use dashboards to monitor all layers**

Hint: End-to-end visibility.

2. **How would you automatically restart a service if an error is found in logs?**

Expected Answer:

- **Create a metric filter → alarm → Lambda function to restart the service**

Hint: Logs → metric → Lambda.

3. You want to send CloudWatch logs to a SIEM tool. How?

Expected Answer:

- **Use subscription filters → send to Kinesis or Lambda → forward to SIEM endpoint**

Hint: Logs out via stream.

4. Monitor and visualize memory usage across 10 EC2 instances.

Expected Answer:

- **Use CloudWatch Agent to collect memory metrics**
- **Aggregate using dashboards**

Hint: Agent + dashboard.

Hard - Level

Amazon CloudWatch

(Interview Questions - 3+ Years Experience)

1. **“How does CloudWatch Logs Insights differ from regular log viewing?”**

   Expected Answer: Logs Insights allows powerful queries and aggregation over logs for fast analysis.

   Hint: SQL-like log analysis.

2. **“Explain how you’d monitor a serverless app end-to-end using CloudWatch.”**

   Expected Answer: Use metrics and logs from Lambda, API Gateway, and DynamoDB, and create dashboards/alarms for each layer.

   Hint: Monitor every service involved.

3. **“How do you reduce CloudWatch log ingestion costs?”**

   Expected Answer: Use filters to ingest only needed logs, reduce retention, and avoid verbose debug logs.

   Hint: Log less, log smart.

4. **“How do you prevent alarm fatigue in large-scale monitoring?”**

Expected Answer: Use composite alarms, suppression rules, and logical groupings to reduce false positives.

Hint: Smarter alerting = less noise.

5. **“What’s the difference between PutMetricData and Embedded Metric Format?”**

Expected Answer: PutMetricData sends raw metrics; EMF embeds structured metrics in logs for better context.

Hint: EMF gives more dimensions inside logs.

6. **“What are anomaly detection alarms in CloudWatch?”**

Expected Answer: They use machine learning to detect metric patterns and deviations instead of fixed thresholds.

Hint: Dynamic alerts using ML.

7. **“Explain high-resolution metrics and their use cases.”**

Expected Answer: High-res metrics offer sub-minute granularity (down to 1-second) for detailed monitoring.

Hint: Needed for real-time apps.

8. **“How do you architect cross-region monitoring in AWS?”**

Expected Answer: Use centralized dashboards, cross-account sharing, or CloudWatch cross-region data aggregation.

Hint: Think centralized visibility.

9. **"What is metric stream and when do you use it?"**

Expected Answer: It streams CloudWatch metrics to services like Kinesis for real-time analytics.

Hint: Real-time pipeline for metrics.

10. **"How would you detect and alert on log-based security anomalies?"**

Expected Answer: Use metric filters, anomaly detection, and trigger alarms or Lambda responses.

Hint: Logs + filters + intelligence.

SCENARIO-BASED INTERVIEW QUESTIONS

---

1. **You want to correlate spikes in latency with log events. How would you do it?**

Expected Answer: Use Logs Insights to query logs and align with metric timelines.

Hint: Analyze logs + metrics together.

2. **Your app performs fine but CloudWatch shows high error rates. Why?**

   Expected Answer: Logs may include handled exceptions or retries not impacting user experience.

   Hint: Not all errors are critical.

3. **A deployment causes memory leaks visible only in log patterns. How do you detect this automatically?**

   Expected Answer: Create metric filters for memory warnings and set anomaly-based alarms.

   Hint: Watch for repeating memory logs.

4. **You're required to build a real-time dashboard across 5 regions. What's your approach?**

   Expected Answer: Use cross-region metric data and CloudWatch dashboards with widgets per region.

Hint: Build one pane of glass view.

5. How do you automate alert enrichment with log context?

Expected Answer: Trigger Lambda on alarms, fetch log context, and include it in alerts.

Hint: Smarter alerts = faster debugging.

PROJECT-BASED INTERVIEW QUESTIONS

---

1. Design a security alerting system using CloudWatch for an AWS environment.

Expected Answer:

- **Use CloudTrail + CloudWatch Logs**
- **Create metric filters for unauthorized access**
- **Trigger alarms or Lambda for response**

Hint: Compliance & security pipeline.

2. Build a custom CloudWatch dashboard for a multi-service architecture.

Expected Answer:

- **Aggregate metrics across services**
- **Add alarms and visual indicators**
- **Use log widgets and graphs**

Hint: Metrics, alarms, logs — all in one view.

3. Stream CloudWatch logs in real-time to Elasticsearch.

Expected Answer:

- **Use subscription filters → Kinesis → Lambda → Elasticsearch**

Hint: Real-time searchable logging.

4. Create a cost-optimized monitoring strategy for 100+ servers.

Expected Answer:

- **Use standard metrics where possible**
- **Aggregate low-priority alarms**
- **Use log filters and reduced retention**

Hint: Balance cost with visibility.