**1. What is Amazon CloudWatch?**

**Answer:** Amazon CloudWatch is a **monitoring and observability service** that collects logs, metrics, and events for AWS resources and applications.

* Provides dashboards, alarms, and automated actions.

**2. What are the key features of CloudWatch?**

**Answer:**

* **Metrics Monitoring**
* **Logs Management**
* **Alarms & Notifications**
* **Events (EventBridge)**
* **Dashboards**
* **Automated Responses** (via Lambda, Auto Scaling)

**3. What are CloudWatch Metrics?**

**Answer:** Metrics are **time-ordered data points** (e.g., CPU utilization, network traffic).

* Each metric belongs to a namespace and can have dimensions (e.g., EC2 InstanceId).

**4. What are the default metrics for EC2 monitored by CloudWatch?**

**Answer:**

* CPU Utilization
* Disk Read/Write (for instance store)
* Network In/Out
* Status Checks

**5. What is the difference between CloudWatch Logs and CloudTrail?**

**Answer:**

* **CloudWatch Logs:** Application & system logs (e.g., EC2 logs).
* **CloudTrail:** API activity logs (who did what and when).

**6. What is a CloudWatch Alarm?**

**Answer:** An alarm monitors a metric and performs an **action** (e.g., send SNS notification, trigger Auto Scaling) when a threshold is breached.

**7. What is the default monitoring interval for EC2 in CloudWatch?**

**Answer:**

* **Basic Monitoring:** 5 minutes
* **Detailed Monitoring:** 1 minute (requires enabling)

**8. Can CloudWatch monitor on-premises servers?**

**Answer:** Yes, by installing the **CloudWatch Agent** to push custom metrics and logs.

**9. What is the retention period for CloudWatch Logs?**

**Answer:** By default, logs are kept **indefinitely**, but retention can be configured (1 day to 10 years).

**10. What are CloudWatch Dashboards?**

**Answer:** Customizable dashboards to visualize metrics across AWS resources in one place.

**11. What is the difference between CloudWatch Metrics and Logs?**

**Answer:**

* **Metrics:** Numeric time-series data.
* **Logs:** Raw log data from applications, OS, and services.

**12. What is CloudWatch Events (now EventBridge)?**

**Answer:** Captures **AWS service events** and routes them to targets (e.g., Lambda, SNS) for automated responses.

**13. What are Custom Metrics in CloudWatch?**

**Answer:** Metrics created by users or applications (e.g., application latency).

* Sent via PutMetricData API or CloudWatch Agent.

**14. What is a CloudWatch Log Group?**

**Answer:** A container for logs, where each group holds multiple log streams (e.g., EC2 logs per instance).

**15. How do you create an alarm for an S3 bucket size?**

**Answer:** Enable **S3 Storage Metrics**, then create an alarm based on the metrics.

**16. What are CloudWatch Contributor Insights?**

**Answer:** Analyzes logs to identify **top contributors** to system performance issues.

**17. Can you integrate CloudWatch with third-party tools?**

**Answer:** Yes, using **APIs, SDKs, and AWS Partners** like Splunk, Datadog, etc.

**18. What is the cost model for CloudWatch?**

**Answer:** Charges are based on:

* Metrics (per metric per month)
* Alarms
* Logs ingestion and storage
* API requests

**19. How do you enable detailed monitoring for EC2?**

**Answer:** Enable **Detailed Monitoring** in the EC2 settings or via CLI:

aws ec2 monitor-instances --instance-ids i-1234567890abcdef0

**20. Can CloudWatch trigger Auto Scaling actions?**

**Answer:** Yes. CloudWatch Alarms can trigger **Auto Scaling Policies**.

**21. Scenario: You need to monitor memory utilization on EC2. CloudWatch default metrics don’t show memory usage. What do you do?**

**Answer:** Install the **CloudWatch Agent** and configure it to push memory metrics as custom metrics.

**22. Scenario: You want to trigger a Lambda function when an EC2 instance stops.**

**Answer:** Use **CloudWatch Event Rule (EventBridge)** with EC2 Instance State-change Notification → target Lambda.

**23. Scenario: CloudWatch alarms are flapping due to noisy data. How to fix it?**

**Answer:**

* Use **datapointsToAlarm** parameter.
* Increase evaluation periods.
* Smooth metrics with averaging.

**24. How can you reduce CloudWatch Logs cost?**

**Answer:**

* Set appropriate retention policies.
* Use log filters to store only needed logs.
* Export old logs to S3 Glacier.

**25. Scenario: Need to alert when the number of 5xx errors in an ALB exceeds a threshold.**

**Answer:** Create a CloudWatch Alarm on the **ALB 5XXErrorCount** metric.

**26. Scenario: Detect and stop EC2 instances with high CPU usage automatically.**

**Answer:**

* Create a CloudWatch Alarm (CPU > threshold).
* Trigger an **SNS Topic** → **Lambda** → stop instance.

**27. How do you query logs in CloudWatch?**

**Answer:** Use **CloudWatch Logs Insights**, a SQL-like query engine for log analysis.

**28. Scenario: You want to store all VPC Flow Logs and analyze them for unusual traffic.**

**Answer:** Send VPC Flow Logs to **CloudWatch Logs**, then analyze using **Logs Insights** or stream to **Kinesis**/**S3**.

**29. How do you monitor API Gateway latency?**

**Answer:** Enable CloudWatch metrics for API Gateway and create an alarm on Latency metric.

**30. What is the difference between CloudWatch Logs Metric Filters and Alarms?**

**Answer:**

* **Metric Filter:** Converts log patterns into metrics.
* **Alarm:** Monitors a metric and triggers an action.

**31. Scenario: Application logs need to be archived periodically.**

**Answer:** Set **log retention policy** → export logs to **S3** for long-term storage.

**32. How do you monitor DynamoDB performance using CloudWatch?**

**Answer:** CloudWatch provides metrics like ConsumedReadCapacityUnits, ThrottledRequests, etc. Create alarms accordingly.

**33. Can CloudWatch monitor Lambda cold starts?**

**Answer:** Indirectly, by tracking **Duration** and **Init Duration** metrics for Lambda functions.

**34. Scenario: Detect an EC2 instance stopped unexpectedly at 3 AM.**

**Answer:**

* Use **CloudWatch Event Rule** for EC2 Instance State-change.
* Send notification via **SNS**.

**35. Scenario: You have a multi-account setup and want centralized monitoring.**

**Answer:** Use **CloudWatch Cross-Account Observability** or **CloudWatch Logs Subscription Filters** to send logs to a central account.

**36. What is a CloudWatch Composite Alarm?**

**Answer:** An alarm that **combines multiple alarms** into one for complex conditions (reduces false positives).

**37. Scenario: Detect abnormal user login attempts in AWS.**

**Answer:**

* Send **CloudTrail logs** to CloudWatch Logs.
* Create **Metric Filters** to detect suspicious patterns.
* Trigger an alarm.

**38. What is the difference between CloudWatch Alarms and EventBridge Rules?**

**Answer:**

* **Alarms:** Monitor metrics thresholds.
* **EventBridge (Events):** React to AWS events (state changes, API calls).

**39. Scenario: Monitor custom application running on Kubernetes (EKS).**

**Answer:**

* Install CloudWatch Agent or **Container Insights** to push container metrics and logs.

**40. How to troubleshoot missing CloudWatch metrics?**

**Answer:**

* Check IAM permissions.
* Verify metric namespace and dimensions.
* Ensure data is being pushed correctly (for custom metrics).