Monitoring and Security

CLOUDWATCH · METRICS & ALARMS · LOGS · EVENTS · CLOUDTRAIL · ATHENA · AWS CONFIG

STUDY & REVIEW

01 MUST KNOW

if you remember five things, remember these

01 **CloudWatch is the monitoring hub:** a monitoring and management service that collects **metrics, logs, and events** into a unified view of your AWS resources, applications, and services. It integrates with **70+ AWS services** that publish standard metrics automatically, and it spans three functional areas — **CloudWatch monitoring** (metrics + alarms), **CloudWatch Logs**, and **CloudWatch Events**.

02 **Know the metric anatomy:** a **metric** is a time-ordered set of data points, uniquely defined by a **name**, a **namespace** (`AWS/<service>`, e.g. `AWS/EC2`), and up to **10 dimensions** (name-value pairs). A **period** is 1 second to 1 day (`86,400` s). Metrics are **Regional**, cannot be deleted, and expire after **15 months** with no new data.

03 **Standard vs. custom, basic vs. detailed: standard metrics** publish automatically and are **free**; **custom metrics** (your own data via CLI, API, or the **CloudWatch agent**) and **detailed monitoring** cost extra. **Basic** monitoring reports every **5 minutes**; **detailed** monitoring every **1 minute**.

04 **Alarms watch a threshold:** an alarm tests a metric (or a math expression) against a threshold over one or more periods and holds one of three states — **OK**, **ALARM**, or **INSUFFICIENT_DATA**. **ALARM is not an emergency** — it only means the metric crossed the threshold. Alarms notify through **Amazon SNS/SQS** or trigger automated actions.

05 **The security trio: CloudWatch Logs** monitors your log content; **AWS CloudTrail** audits **API calls** (Console, CLI, SDK) and pushes logs to **Amazon S3**; **AWS Config** assesses and evaluates **resource configuration** against rules. Use **CloudWatch + CloudTrail together** to detect unauthorized use — and remember CloudTrail does **not** record actions taken *inside* an EC2 instance.

02 KEY TERMS

TERM	DEFINITION
Amazon CloudWatch	Monitoring and management service that provides data and actionable insights for AWS resources; collects logs, metrics, and events
Metric	A time-ordered set of data points published to CloudWatch — a variable to monitor over time (e.g. an instance's CPU utilization)
Namespace	A container that isolates metrics so unrelated ones are not aggregated together; AWS uses `AWS/<service>`, such as `AWS/EC2`
Dimension	A name-value pair that uniquely identifies a metric; up to 10 per metric, used to filter results (e.g. `InstanceId`)
Period	The length of time associated with a CloudWatch statistic, in seconds — from 1 second up to 1 day (86,400 seconds)
CloudWatch alarm	Watches a single metric or a math expression against a threshold over periods; states are OK, ALARM, and INSUFFICIENT_DATA
CloudWatch agent	Collects system-level metrics (and logs) from Amazon EC2 instances or from on-premises servers not managed by AWS
CloudWatch Events	Near-real-time stream of system events describing changes in AWS resources; rules match events and route them to targets
Amazon CloudWatch Logs	Collects, stores, and monitors log files; aggregates them into log groups, applies metric filters, and queries with Logs Insights
AWS CloudTrail	Logs, continuously monitors, and retains account activity by recording API calls; automatically pushes audit logs to Amazon S3

TERM	DEFINITION
AWS Config	Assesses, audits, and evaluates the configuration of AWS resources; records changes and checks compliance against rules
Amazon Athena	Serverless, interactive query service that analyzes data in Amazon S3 (including AWS logs) using standard SQL

03 THE THREE SERVICES — CLOUDWATCH VS. CLOUDTRAIL VS. AWS CONFIG

the exam turns on which one answers the question

SERVICE	ANSWERS	CAPTURES	WHERE DATA GOES
Amazon CloudWatch	How are my resources performing?	Metrics, logs, and events — performance and operational health	Dashboards and alarms → SNS/ SQS, automated actions
AWS CloudTrail	Who did what, and when?	API calls across AWS (Console, CLI, SDK) — account activity	Log files pushed to an Amazon S3 bucket
AWS Config	Are my resources configured correctly?	Resource configurations and how they change over time	Config dashboard — compliance vs. rules, plus history

04 STANDARD METRICS VS. CUSTOM METRICS

know source, grouping, and cost

STANDARD METRICS

published automatically by AWS services

- Grouped by service name (70+ services)
- Display graphically so selected metrics can be compared
- Appear only if the service was used in the past **15 months**
- Reachable programmatically through the AWS CLI or API
- **Free** — no extra charge

CUSTOM METRICS

your own application data

- Grouped by a **user-defined namespace**
- Published via AWS CLI, API, or the **CloudWatch agent**
- Example: memory usage of the `httpd` service on EC2
- The agent also gathers metrics from **on-premises servers**
- **Paid** feature

05 FROM LOG LINE TO ALERT

the CloudWatch Logs metric-filter pipeline

01 CloudWatch agent ships logs from EC2 instances → **02** Data aggregates into a **log group** (e.g. `HttpAccessLog`) → **03** A **metric filter** matches a pattern (e.g. `404`) → **04** Each match increments a **custom metric** (`404Count`) → **05** A **CloudWatch alarm** trips over the threshold → **06** **Amazon SNS** notifies the IT support team

06 EXAM TRAPS

where the knowledge check gets you

- × "CloudTrail tracks everything that happens on my instances." — No. CloudTrail records **API calls**; it does not track events *inside* an EC2 instance, such as a manual `sudo shutdown -h now` over SSH.
- × "The ALARM state means something is broken." — ALARM is only a name for a state — the metric crossed its threshold. It can be a normal, expected condition you handle programmatically (e.g. a low T2 `CPUCreditBalance`).
- × "CloudWatch metrics are global and can be deleted." — Metrics exist **only in the Region** where they are created, and they **cannot be deleted** — they expire after 15 months of no new data.
- × "All CloudWatch monitoring is free." — **Standard metrics** are free, but **custom metrics** and **detailed monitoring** cost extra. Basic monitoring is 5-minute; detailed is 1-minute.
- × "Billing alerts work out of the box." — You must first **enable billing alerts** in your account preferences before you can set a CloudWatch alarm on estimated charges.
- × "CloudTrail keeps my full history forever by default." — Event history shows only the **last 90 days** of management events. For a complete record (all management and data events), you must **create a trail** that delivers logs to S3.
- × "CloudWatch Logs and CloudTrail are redundant — pick one." — They are **complementary**: Logs monitors your application/system log content; CloudTrail audits API activity. Using both is the security best practice.
- × "AWS Config reports performance metrics." — No. Config evaluates **resource configuration and compliance**; performance metrics and alarms are CloudWatch's job.

07 SELF-QUIZ

answers are upside-down below

Q1 CloudWatch collects which three kinds of monitoring data to build a unified view?

Q2 A CloudWatch metric is uniquely identified by which three attributes?

Q3 What is the shortest and the longest a CloudWatch period can be?

Q4 What are the three possible states of a CloudWatch alarm?

Q5 How often does basic monitoring publish EC2 metrics, and how often does detailed monitoring?

Q6 Before you can alarm on estimated monthly charges, what must you turn on?

Q7 What do you create on a log group so each match of a string pattern increments a custom metric?

Q8 Which service continuously logs account API activity and automatically pushes the logs to Amazon S3?

Q9 Give one example of activity that CloudTrail does not record.

Q10 Which serverless service queries logs stored in Amazon S3 (CloudTrail, ALB, VPC Flow Logs) using standard SQL?

ANSWER KEY (rotate the page)

Q1 logs, metrics, and events **Q2** its name, its namespace, and its dimensions **Q3** 1 second to 1 day (86,400 seconds) **Q4** OK, ALARM, and INSUFFICIENT_DATA **Q5** every 5 minutes; every 1 minute **Q6** billing alerts in the account (billing) preferences **Q7** a metric filter **Q8** AWS CloudTrail **Q9** actions taken inside an EC2 instance, such as a manual shutdown over SSH **Q10** Amazon Athena