Logging and Monitoring

LOGGING VS MONITORING · CLOUDTRAIL · BUILT-IN LOGS · CLOUDWATCH · BEST PRACTICES · CONFIG · EVENTBRIDGE · SECURITY HUB

STUDY & REVIEW

01 MUST KNOW

if you remember five things, remember these

01 **Logging vs. monitoring: logging** is the collection and recording of activity and event data — a record of events captured at a point in time. **Monitoring** is the *continuous* verification of the security and performance of your resources, applications, and data. Together they let you identify, mitigate, and remediate threats.

02 **CloudTrail = actions, CloudWatch = performance: AWS CloudTrail** records **who** performed **what** action and **when** (user, role, and service events). **Amazon CloudWatch** monitors resource and application **performance**, detects anomalies, and **alerts** you that an issue occurred — but it does not tell you who caused it.

03 **CloudTrail records every API call:** each event captures the **name of the API**, **identity of the caller**, **time in UTC**, **originating location**, **request parameters**, and **response elements**. Events cover actions in the Console, AWS CLI, SDKs, and APIs — used to track resource changes, troubleshoot, and prove compliance.

04 **Some services log themselves:** logging is provided either by a **secondary service** (CloudTrail) or by the **service itself** — **S3 server access logs**, **VPC Flow Logs**, and **ELB access logs** are built-in features. Built-in logs publish to **CloudWatch Logs** or **Amazon S3**.

05 **Logs are a compliance requirement:** logs demonstrate compliance with regulations such as **HIPAA**, **GDPR**, and **LGPD**, and are a primary focus in **incident response** — their time-stamped records support troubleshooting, auditing, recordkeeping, and remediation.

02 KEY TERMS

TERM	DEFINITION
Logging	The collection and recording of activity and event data; provided by the service itself or by a secondary service
Monitoring	The continuous verification of the security and performance of your resources, applications, and data
AWS CloudTrail	Records actions taken by a user, role, or AWS service as events, for governance, compliance, operational and risk auditing
Event (CloudTrail)	A record of an action taken in the AWS Management Console, AWS CLI, or an SDK or API call
Amazon CloudWatch	Monitoring and observability service that collects logs, metrics, and events for a unified view of operational health
CloudWatch Logs	Centralizes, stores, searches, and queries log files from EC2, CloudTrail, Route 53, and other sources as a single time-ordered flow
VPC Flow Logs	Built-in feature that captures inbound and outbound IP traffic at the VPC, subnet, or network-interface level
S3 server access logging	Built-in Amazon S3 feature that records detailed access requests made to a bucket
ELB access logs	Detailed records of requests to a load balancer; captured, compressed, and stored in a specified S3 bucket
AWS Config	Continuously records AWS resource configurations and evaluates them against desired configurations
Amazon EventBridge	Serverless event bus (formerly Amazon CloudWatch Events) that routes real-time events to targets such as AWS Lambda

TERM	DEFINITION
AWS Security Hub	Aggregates security findings from AWS services and partner products in a standardized format with a consolidated security score

03 CLOUDTRAIL VS. CLOUDWATCH

the module's central distinction

AWS CLOUDTRAIL	AMAZON CLOUDWATCH
WHO did WHAT, and WHEN	*performance, anomalies, alarms*
— Logs user, group, role activity as **events**	— Monitors resource & application **performance**
— Records actions in Console, CLI, SDKs, APIs	— Detects anomalies; sets alarms; finds insights
— Names **who** performed an unauthorized action	— **Alerts** you an issue occurred — not who

04 SERVICES WITH BUILT-IN LOGS

logging built into the service itself

SERVICE	WHAT IT CAPTURES	WHERE LOGS GO
Amazon S3	Detailed access requests to a bucket (server access logging)	Amazon S3
VPC Flow Logs	Inbound/outbound IP traffic at VPC, subnet, or interface level	CloudWatch Logs or S3
Elastic Load Balancing	Requests to the load balancer: client IP, latencies, paths, responses	S3 (compressed)

05 ADDITIONAL LOGGING & MONITORING SERVICES

know the one-line job of each

SERVICE	ONE-LINE ROLE
AWS Config	Records resource configurations and evaluates them against a desired state; streams changes to Amazon SNS
Amazon EventBridge	Serverless event bus (formerly CloudWatch Events); routes real-time events to Lambda and other targets
AWS Security Hub	Aggregates findings in a standard format; consolidated security score across accounts; integrates with EventBridge
AWS Trusted Advisor	Best-practice checks in 5 categories: cost optimization, security, fault tolerance, service limits, performance

06 MONITORING & ALERTING PIPELINE (THE LAB)

detect → alert → respond

01 **CloudTrail** trail delivers API events to **CloudWatch Logs** → 02 A **metric filter** matches a pattern (e.g., a security-group change) → 03 A **CloudWatch alarm** fires when the metric crosses its threshold → 04 The alarm publishes to an **Amazon SNS** topic → subscribers notified → 05 Query the raw events anytime with **CloudWatch Logs Insights**

07 EXAM TRAPS

where the knowledge check gets you

- × “CloudWatch tells you who deleted the resource.” — No. CloudWatch **alerts** you that an anomalous action occurred; only **CloudTrail** provides the identity of the user, role, or service that performed it.
- × “AWS Config identifies who made a change.” — Config records the **configuration** state and history, not the caller. To find who changed a resource, use **CloudTrail**.
- × “Trusted Advisor alerts you about attacks and anomalies.” — Trusted Advisor **recommends** best-practice improvements across five categories; it does not monitor or alert on real-time anomalous activity.
- × “Enabling VPC Flow Logs slows the network.” — Flow log data is collected **outside** the path of your network traffic — no impact on throughput, latency, or overall performance.
- × “CloudTrail and CloudWatch are two names for the same thing.” — CloudTrail records **actions** (user/role/service events); CloudWatch monitors **performance** (metrics, alarms). Actions vs. performance.
- × “EventBridge is a brand-new service unrelated to CloudWatch.” — EventBridge is the **renamed** Amazon CloudWatch Events; it uses the **same API**, and new features are added only to EventBridge.
- × “Every log needs a separate service like CloudTrail.” — Many services log **themselves**: S3 server access logs, VPC Flow Logs, and ELB access logs are built-in features; CloudTrail is the secondary-service example.
- × “Security Hub generates all of its own findings from scratch.” — Security Hub **aggregates and standardizes** findings from AWS services and partner products and runs best-practice checks, producing a consolidated score — it centralizes the sources.

08 SELF-QUIZ

answers are upside-down below

Q1 A user deleted an S3 bucket without authorization; which AWS service reveals the identity of the user who did it?

Q2 In one word each, what does CloudTrail monitor and what does CloudWatch monitor?

Q3 Name the six pieces of information CloudTrail records about each API call.

Q4 Which built-in feature captures inbound and outbound IP traffic at the VPC, subnet, or network-interface level?

Q5 To which two destinations can VPC Flow Logs publish their data?

Q6 Which service continuously records resource configurations and evaluates them against a desired state?

Q7 What was Amazon EventBridge formerly known as?

Q8 Which service aggregates security findings in a standardized format and produces a consolidated security score across accounts?

Q9 List the five best-practice categories that AWS Trusted Advisor checks.

Q10 Which three regulations does the module name as requiring logs to demonstrate compliance?

ANSWER KEY (rotate the page)

Q1 AWS CloudTrail **Q2** CloudTrail → actions; CloudWatch → performance **Q3** name of the API, identity of the caller, time in UTC, originating location of the request, request parameters, response elements **Q4** VPC Flow Logs **Q5** Amazon CloudWatch Logs or Amazon S3 **Q6** AWS Config **Q7** Amazon CloudWatch Events **Q8** AWS Security Hub **Q9** cost optimization, security, fault tolerance, service limits, and performance improvement **Q10** HIPAA, GDPR, and LGPD