MODULE 6 · STUDY NOTES

Logging and Monitoring

How AWS logging and monitoring services — CloudTrail, CloudWatch, VPC Flow Logs, Config, EventBridge, Security Hub, and Trusted Advisor — help you identify, mitigate, and remediate security threats

After securing every tier of a cloud application, the next job is watching it — knowing what happened, who did it, and whether anything looks wrong. This module maps the AWS tools that provide that visibility. **Logging** is the collection and recording of activity and event data; **monitoring** is the continuous verification of your resources' security and performance. The two headline services are **AWS CloudTrail**, which records the actions taken in your account, and **Amazon CloudWatch**, which monitors performance and raises alarms — and a recurring exam theme is knowing which to reach for. Around them sit services that log themselves (S3 server access logs, VPC Flow Logs, ELB access logs) and a supporting cast that extends the picture: AWS Config for configuration history, Amazon EventBridge for event-driven responses, AWS Security Hub for aggregated findings, and AWS Trusted Advisor for best-practice checks. In the bank scenario, an insider-threat story prompts María to align each of these services with the threat it helps identify, mitigate, and remediate.

LEARNING OBJECTIVES

- Log and monitor access and control to help identify security threats
- Read and interpret log reports to identify security threats
- Monitor and report on your Amazon Web Services (AWS) resources and applications
- Recognize when to use Amazon CloudWatch and when to use AWS CloudTrail

6.1 Importance of logging and monitoring

Logging is the collection and recording of activity and event data. It can be provided by the **service itself** — as with Amazon VPC Flow Logs and Amazon S3 server access logs — or by a **secondary service** such as AWS CloudTrail. The exact information logged varies by the service doing the logging, but some elements are common to nearly all logs: the **date and time** of the event, the **originating location** of the request, and the **identity of the resources accessed**. A log provides a record of events captured at a specific point in time. Common log files include access logs, application logs, system logs, event logs, API call logs, and database logs.

A comprehensive logging methodology helps in every phase of an incident-response strategy, and log files are a **primary focus point in incident response** because of their ability to provide detailed, time-stamped records to investigators and responders. Logs assist in troubleshooting performance issues in the cloud and on premises, and they are necessary for security audits and recordkeeping to demonstrate compliance with regulatory measures — the **Health Insurance Portability and Accountability Act (HIPAA)** in the United States, the European Union's **General Data Protection Regulation (GDPR)**, and Brazil's **General Data Protection Law (LGPD)**. Finally, logs help you remediate issues by showing the point in time when a problem arose.

WHY LOGS MATTER

- **Troubleshooting** — trace performance issues across cloud and on-premises environments.
- **Auditing** — support security audits with detailed, time-stamped records.
- **Recordkeeping and compliance** — required to demonstrate adherence to HIPAA, GDPR, LGPD, and similar regulations.
- **Incident response and remediation** — a primary focus in investigations; logs pinpoint when an issue arose.

Monitoring is the continuous verification of the security and performance of your resources, applications, and data. AWS provides several services that give you the visibility to spot issues before they impact operations — **AWS CloudTrail**, **Amazon CloudWatch**, **Amazon EventBridge**, and **AWS X-Ray** — but this module focuses on the two most central. **CloudTrail** provides a record of the actions taken within your environment, including the action type, identity of the user, and the date and time of the action, so you can monitor who is doing what and when. **CloudWatch** monitors your resources and applications in real time, giving system-wide visibility into resource utilization, application performance, and operational health. Paired with a solid incident-response plan, monitoring can mitigate the effects of an outage or malicious actor — and often spot an issue before it has operational impact.

KEY TERMS

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.

COMMON PITFALL

Logging and monitoring are not the same activity. **Logging** captures a record of events at a specific point in time; **monitoring** is the *continuous* verification of security and performance. You log so that you have something to monitor, audit, and investigate later.

6.2 Capture and collect: AWS CloudTrail

AWS CloudTrail helps you enable governance and compliance, as well as operational and risk auditing of your AWS account. Actions taken by a **user, role, or an AWS service** are recorded as **events** in CloudTrail. Events include actions taken in the **AWS Management Console**, the **AWS CLI**, and the **AWS SDKs and APIs**. In the CloudTrail console you can **view, search, download, archive, analyze, and respond** to these recorded events. You can also integrate CloudTrail into applications through the API, automate trail creation for your organization, check the status of the trails you create, and control how users view CloudTrail events.

CloudTrail records important information about **each API call**. That information helps you track changes made to your AWS resources — including the **creation, modification, and deletion** of resources such as Amazon EC2 instances and Amazon VPC security groups — troubleshoot operational issues, and ensure compliance with internal policies and regulatory standards.

WHAT CLOUDTRAIL RECORDS ABOUT EVERY API CALL

- **Name of the API** — the action that was requested.
- **Identity of the caller** — the user, role, or service that made the call.
- **Time of the API call** — captured in Coordinated Universal Time (**UTC**).
- **Originating location** — where the request came from.
- **Request parameters** — the inputs supplied to the action.
- **Response elements** — what the AWS service returned.

WORKED EXAMPLE – READING A CLOUDTRAIL LOG

In the activity, an IAM user named **Jane** runs `ec2-stop-instances` in the AWS CLI, which calls the Amazon EC2 **StopInstances** action. The log tells the whole story field by field. **Who:** `userIdentity` shows `type: IAMUser` and `arn: arn:aws:iam::111122223333:user/Jane` — Jane, in account 111122223333. **When:** `eventTime: 2021-07-06T21:01:59Z` — the `Z` marks UTC. **What:** `eventSource: ec2.amazonaws.com` with `eventName: StopInstances` — the EC2 service and the stop action. **Where and how:** `sourceIPAddress: 203.0.113.176`, `awsRegion: us-east-2`, and `userAgent: ec2-api-tools` — the call came through the CLI/tools, not the console. **Result:** `requestParameters` name `instanceId: i-ebeaf9e2` with `force: false`; `responseElements` show `previousState: running` (code 16) transitioning to `currentState: stopping` (code 64).

TABLE 6.1 Mapping CloudTrail log fields to the questions they answer

LOG FIELD(S)	WHAT IT TELLS YOU
userIdentity / arn	Identity of the caller — IAM user Jane in account 111122223333
eventTime	When the action occurred, in UTC (the trailing Z)
eventSource / eventName	Which service and which action — EC2 StopInstances
awsRegion / sourceIPAddress	Where the request originated
userAgent	How the call was made — AWS CLI/tools versus the console
requestParameters / responseElements	The target resource and the resulting state change

COMMON PITFALL

If a scenario asks you to determine the **identity** of the user who performed an action, the answer is almost always **CloudTrail**. Its ability to record the caller's identity, the action, and the UTC time of every API call is its defining exam superpower.

6.3 AWS services with built-in logs

Not every log requires a secondary service. Several AWS services provide logging as a **built-in feature** that you simply enable. Three appear in this module — Amazon S3, Amazon VPC, and Elastic Load Balancing — and knowing what each captures and where the logs land is enough to answer most questions about them.

TABLE 6.2 Built-in logging features compared

SERVICE	BUILT-IN LOG	CAPTURES	DESTINATION
Amazon S3	Server access logging	Detailed records of requests made to a bucket	Amazon S3
Amazon VPC	VPC Flow Logs	Inbound/outbound IP traffic at the VPC, subnet, or interface level	CloudWatch Logs or S3
Elastic Load Balancing	ELB access logs	Requests to the load balancer: request time, client IP, latencies, paths, responses	S3 (compressed)

DETAILS WORTH REMEMBERING

- **S3 server access logs** are useful for security and access audits, provide insight into your customer base, and help you understand your Amazon S3 bill and storage usage.
- **VPC Flow Logs** capture traffic from the VPC, subnets, or individual network interfaces, and can publish to **CloudWatch Logs or Amazon S3**; the data is collected **outside the path of your network traffic**, so there is no impact on throughput, latency, or overall performance.
- **ELB access logs** contain the time of request receipt, client IP address, latencies, request paths, and server responses; ELB **captures, compresses, and stores** them in a specified S3 bucket for traffic analysis and troubleshooting.

COMMON PITFALL

Do not assume that turning on VPC Flow Logs adds latency to your traffic. Because flow log data is collected **outside** the network path, enabling it has **no impact on throughput, latency, or overall performance** — a common distractor on exam questions.

6.4 Monitor and report: Amazon CloudWatch

Amazon CloudWatch is a monitoring and observability service built for DevOps engineers, developers, site reliability engineers (SREs), IT managers, and product owners. It collects monitoring and operational data as **logs, metrics, and events**, giving you a **unified view** of your AWS resources, applications, and services running on AWS and on-premises servers. With CloudWatch you can detect anomalous behavior, **set alarms**, visualize logs and metrics side by side, take automated actions, troubleshoot issues, and discover insights — breaking down data silos to gain system-wide visibility and resolve issues quickly.

THE PIECES OF CLOUDWATCH

- **CloudWatch Logs** — monitor, store, and access log files from EC2 instances, CloudTrail, Amazon Route 53, and other sources; centralize them as a single, time-ordered flow; search for error codes or patterns, filter by fields, archive securely, query with a powerful query language, and visualize in dashboards.
- **Metrics** — data on resource utilization and application performance that drives visualizations and alarms.
- **CloudWatch Events** — a near-real-time stream of system events describing changes in AWS resources, able to take corrective action; it is **being replaced by Amazon EventBridge**.

AWS CLOUDTRAIL	AMAZON CLOUDWATCH
logs user activity — WHO, WHAT, WHEN	*monitors performance — anomalies and alarms*
▪ Continuously monitors and logs the activity of users, groups, and roles ▪ Useful for compliance auditing, security analysis, and troubleshooting ▪ If an EC2 instance is deleted without permission, gives the **identity** of the user, group, or role that did it	▪ Continuously monitors the performance of resources and applications ▪ Useful for detecting anomalous service behavior, setting alarms, and discovering insights ▪ **Alerts** you that an anomalous action — such as that instance deletion — has occurred

The two are strongest **together**. You can create custom CloudWatch **dashboards, alarms, and notifications** for key metrics and for specific CloudTrail events — so a particular action recorded by CloudTrail can trigger a CloudWatch alarm that notifies your team, helping you respond quickly to key operational and security issues.

WORKED EXAMPLE – THE LAB PIPELINE

The module lab wires these services into a working detect-and-alert flow. You create a **CloudTrail trail with CloudWatch Logs enabled** so API events stream into Logs; create an **Amazon SNS topic** and subscribe to it; add a **CloudWatch alarm based on a metric filter** that matches an event pattern; and create an **EventBridge rule to monitor security groups**. When a matching change occurs, the alarm publishes to the SNS topic and subscribers are notified — and you can query the raw events at any time using **CloudWatch Logs Insights**.

COMMON PITFALL

CloudWatch can tell you **that** an anomalous action happened and can alarm on it, but it does **not** identify who performed it. Pair it with CloudTrail — CloudWatch raises the alert, CloudTrail names the caller.

6.5 Best practices for logging and monitoring

Putting AWS logging and monitoring to work starts with **defining your requirements**. Identify the resources, applications, and services you want to maintain logs for, and determine your organizational, legal, and compliance requirements — these can vary widely — before evaluating which AWS resources can help. When you then collect metrics and define baselines, you gain insight into potential security threats, and you can decide **who should receive alerts** and **what they should do** with them.

THREE BEST PRACTICES

- **Define your organizational requirements** for logs, alerts, and metrics — including who receives alerts and how they respond.
- **Configure service and application logging throughout your workload** — application logs, AWS service logs, and resource logs.
- **Analyze your logs centrally** — collect logs in one place and use automation from services such as CloudWatch to detect anomalies or indicators of malicious activity or compromise.

6.6 Additional AWS services for logging and monitoring

Beyond CloudTrail and CloudWatch, four more services round out the logging and monitoring toolkit. **AWS Trusted Advisor** provides recommendations that help you follow AWS best practices, evaluating your account with checks

across five categories — **cost optimization, security, fault tolerance, service limits (service quotas), and performance improvement**. It is accessible through the AWS Management Console and available in all AWS Support plans: Basic and Developer Support customers can access core **security** checks and all **service-quota** checks, while Business and Enterprise Support customers can access **all** checks.

Amazon EventBridge is a serverless **event bus** service that connects your applications with data from a variety of sources, providing a stream of real-time data to targets such as **AWS Lambda** or other event buses. Events are signals that a system's state has changed; EventBridge needs no servers to provision, patch, or manage, scales automatically, and has built-in fault tolerance. For monitoring and auditing, it can respond to operational changes in real time — for example, when resources are accessed by cross-account or public principals, an **Access Analyzer** event can be sent through EventBridge to a Lambda function that removes the unintended permissions. EventBridge was **formerly Amazon CloudWatch Events**; the two share the same API, but new features are added only to EventBridge.

AWS Security Hub helps you monitor your cloud security posture through automated, continuous best-practice checks against your resources. It **aggregates security alerts** from various AWS services and third-party partner products and presents them in a **standardized format**, and it produces a **security score** for each enabled standard plus a **consolidated total** across all accounts associated with your administrator account. Through its integration with EventBridge, Security Hub supports automated response, remediation, and enrichment workflows, helping central security and DevSecOps teams prioritize by searching, correlating, and aggregating findings by account and resource.

AWS Config lets you assess, audit, and evaluate the configurations of your AWS resources. It **continuously monitors and records** resource configurations and can **automatically evaluate** them against desired configurations. Because it keeps historical configurations, you can view the **IAM policies** assigned to a user, group, or role at any time Config was recording — determining what permissions belonged to whom at a specific moment. For change management, Config streams configuration changes to **Amazon SNS** so you are notified of every change, and it represents the **relationships between resources** so you can assess how a change to one resource may affect others.

TABLE 6.3 Additional services at a glance

SERVICE	WHAT IT DOES
AWS Trusted Advisor	Best-practice recommendations across five categories: cost optimization, security, fault tolerance, service limits, and performance improvement
Amazon EventBridge	Serverless event bus (formerly CloudWatch Events) that routes real-time events to targets such as Lambda; enables automated responses
AWS Security Hub	Aggregates findings from AWS and partner products in a standard format; consolidated security score; integrates with EventBridge
AWS Config	Continuously records resource configurations, evaluates them against desired state, and streams changes to Amazon SNS

WORKED EXAMPLE – THE SAMPLE EXAM QUESTION

*A system administrator discovers that a user has deleted an Amazon S3 bucket without authorization, triggering an incident response. Which AWS service can they use to determine the **identity** of the **user** who committed the incident?* The keywords are **identity** and **user** — so the answer is **AWS CloudTrail**, which records the action type, the identity of the user, and the date and time. **CloudWatch** is wrong: it can alert that an anomalous action occurred but does not identify the user. **AWS Config** is wrong: it gives a record of configurations but not the identity of who made a change. **Trusted Advisor** is wrong: it assesses your security posture but does not alert on anomalous behavior.

COMMON PITFALL

Keep Config and CloudTrail straight: **AWS Config** answers *what the configuration was and how it changed*; **AWS CloudTrail** answers *who made the change and when*. Config tracks state and relationships; CloudTrail tracks the caller and the action.

Module summary

- Logging is the collection and recording of activity and event data (a point-in-time record); monitoring is the continuous verification of the security and performance of your resources, applications, and data. Together they help you identify, mitigate, and remediate threats and prove compliance with HIPAA, GDPR, and LGPD.
- Logging is provided either by a secondary service (AWS 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.
- CloudTrail records actions by users, roles, and services as events across the Console, CLI, SDKs, and APIs; each API-call record includes the API name, caller identity, UTC time, originating location, request parameters, and response elements — the WHO, WHAT, and WHEN.
- Reading a CloudTrail log: userIdentity/arn = who, eventTime = when (UTC), eventSource/eventName = which action, sourceIPAddress = where, userAgent = how the call was made.
- Amazon CloudWatch is a monitoring and observability service that collects logs, metrics, and events for a unified operational view; it detects anomalies, sets alarms, and — paired with CloudTrail — drives custom dashboards and notifications. CloudTrail = actions; CloudWatch = performance.
- Best practices: define your organizational requirements for logs, alerts, and metrics; configure service and application logging throughout the workload; and analyze logs centrally, using automation to detect anomalies or indicators of compromise.
- Additional services: AWS Config (records and evaluates configurations, streams changes to SNS), Amazon EventBridge (serverless event bus, formerly CloudWatch Events, routes events to Lambda), AWS Security Hub (aggregates findings with a consolidated security score), and AWS Trusted Advisor (five-category best-practice checks).
- Exam rule of thumb: to find WHO performed an action use CloudTrail; to be alerted THAT an anomaly happened use CloudWatch; to see WHAT a configuration was use Config; for best-practice recommendations use Trusted Advisor.

Review questions

1. **Distinguish logging from monitoring.**

   Answer: Logging is the collection and recording of activity and event data — a record of events captured at a specific point in time. Monitoring is the continuous verification of the security and performance of your resources, applications, and data.

2. When should you reach for CloudTrail versus CloudWatch?

Answer: Use CloudTrail to determine who performed what action and when — user, role, and service events and API history, for compliance auditing, security analysis, and troubleshooting. Use CloudWatch to monitor resource and application performance, detect anomalies, and set alarms. Actions versus performance.

3. What information does CloudTrail capture about each API call, and why is it useful?

Answer: The name of the API, the identity of the caller, the time in UTC, the originating location, the request parameters, and the response elements — used to track changes to resources (creation, modification, deletion), troubleshoot operational issues, and ensure compliance.

4. Which services log themselves, what do they capture, and where do the logs go?

Answer: Amazon S3 server access logging records bucket access requests (to S3); VPC Flow Logs capture inbound/outbound IP traffic at the VPC, subnet, or interface level (to CloudWatch Logs or S3); ELB access logs record requests to the load balancer (captured, compressed, and stored in an S3 bucket).

5. Why does enabling VPC Flow Logs not degrade network performance?

Answer: Flow log data is collected outside the path of your network traffic, so there is no impact on throughput, latency, or overall performance.

6. A user deleted an S3 bucket without authorization. Which service identifies the user, and why not CloudWatch, Config, or Trusted Advisor?

Answer: AWS CloudTrail, because it records the identity of the caller. CloudWatch only alerts that an anomalous action occurred; AWS Config records configurations, not the identity of who made a change; Trusted Advisor assesses security posture but does not alert on anomalous behavior.

7. What are the three best practices for logging and monitoring?

Answer: Define your organizational requirements for logs, alerts, and metrics; configure service and application logging throughout your workload; and analyze your logs centrally, using automation from services such as CloudWatch to detect anomalies.

8. How do EventBridge, Security Hub, and Config each contribute?

Answer: Amazon EventBridge is a serverless event bus (formerly CloudWatch Events) that routes real-time events to targets such as Lambda for automated responses; AWS Security Hub aggregates findings from AWS and partner products in a standardized format with a consolidated security score; AWS Config continuously records resource configurations, evaluates them against desired configurations, and streams changes to Amazon SNS.