AWS Academy Cloud Security Foundations
Logging and Monitoring Student Guide
Version 1.0.0

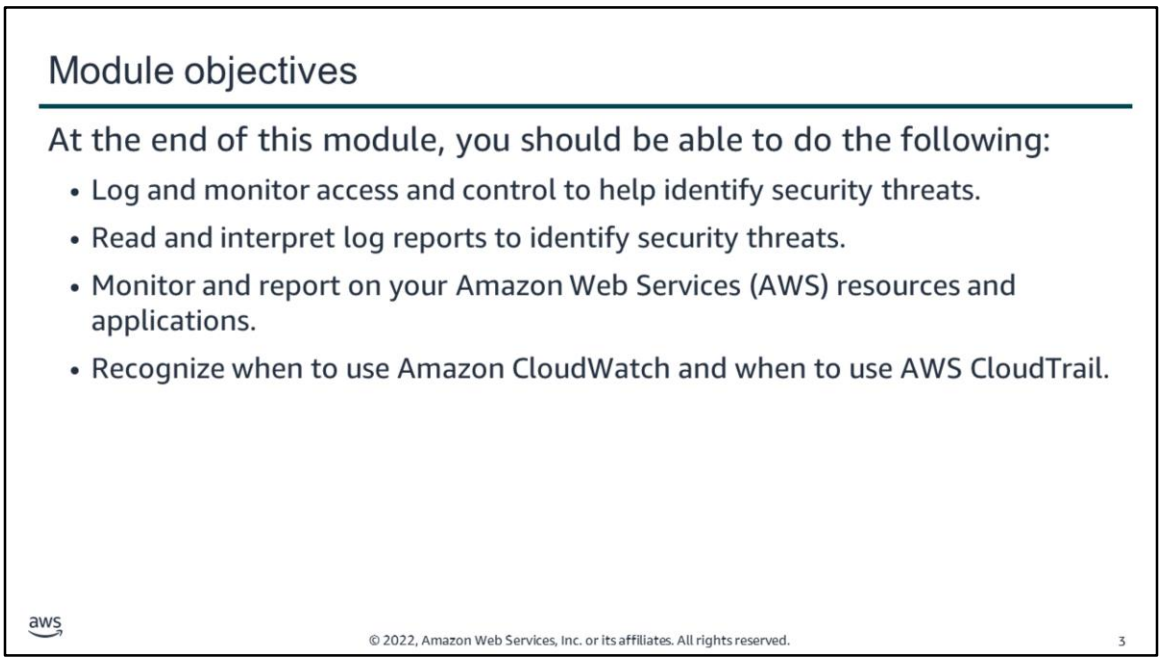
100-ACSECF-10-EN-SG

AWS Academy Cloud Security Foundations

Contents

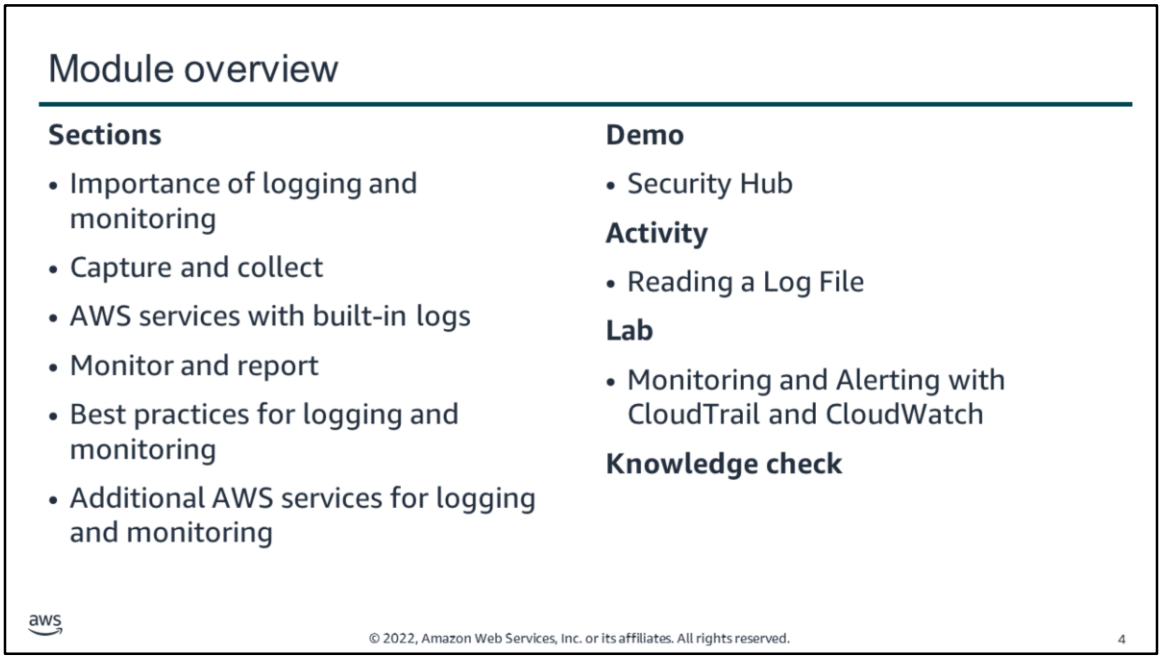
Welcome to the Logging and Monitoring module.

Introduction



At the end of this module, you should be able to do the following:

- 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.



This module includes the following sections:

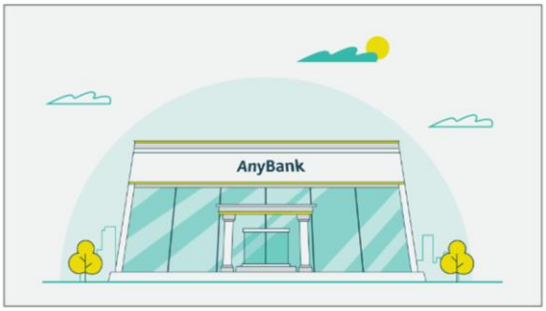
- Importance of logging and monitoring
- Capture and collect
- AWS services with built-in logs
- Monitor and report
- Best practices for logging and monitoring
- Additional AWS services for logging and monitoring

This module also includes the following:

- A demonstration to introduce you to AWS Security Hub
- An activity that walks you through an AWS CloudTrail log file
- A lab where you will configure monitoring and alerting with AWS CloudTrail and Amazon CloudWatch

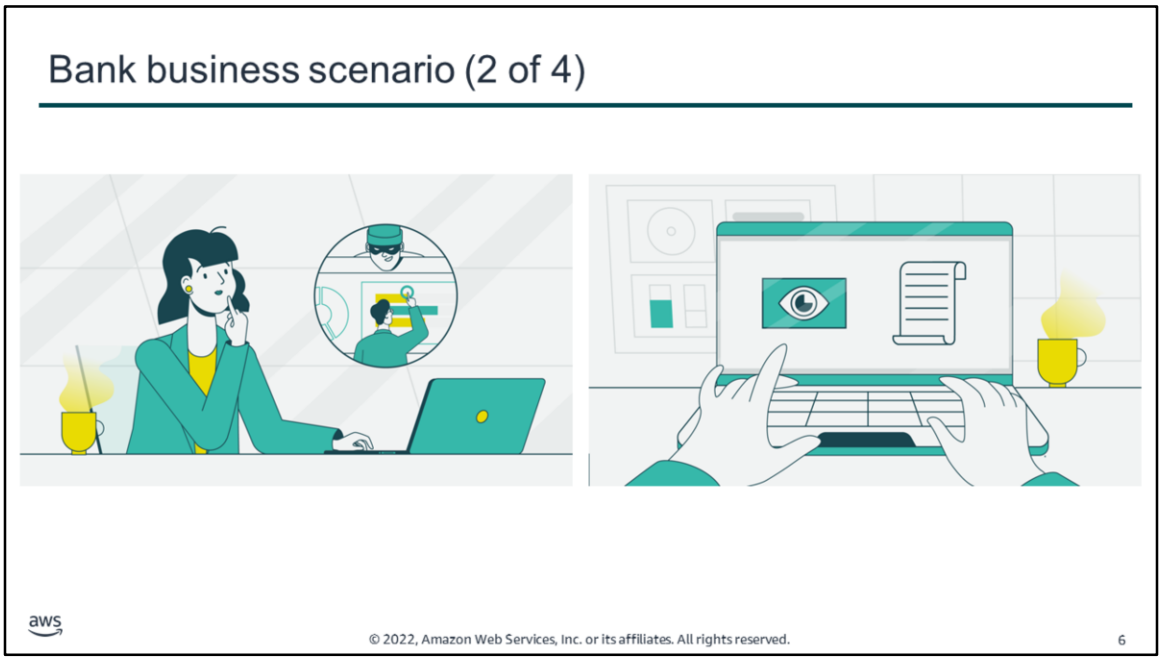
Finally, you will be asked to complete a knowledge check that will test your understanding of key concepts covered in this module.

Bank business scenario (1 of 4)



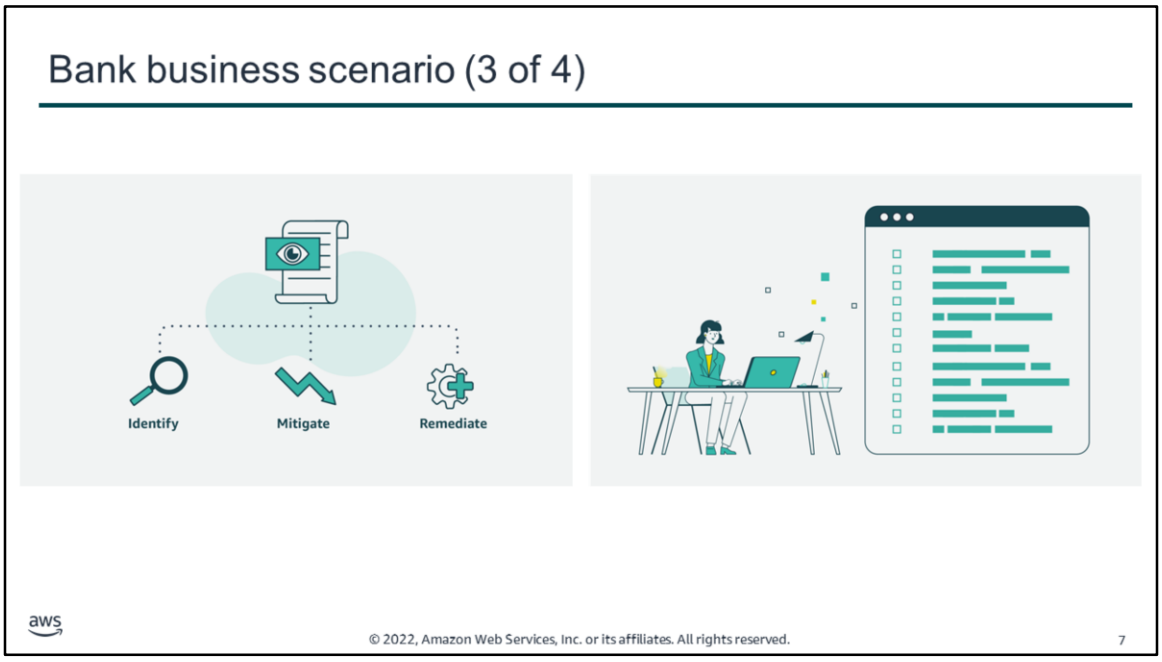
5

Let’s discuss how the concepts in this module are applicable to the bank business scenario.



John’s story of an insider threat at his previous employer gave María an idea.

At their next meeting, María plans to discuss how to use the logging and monitoring capabilities that AWS provides.

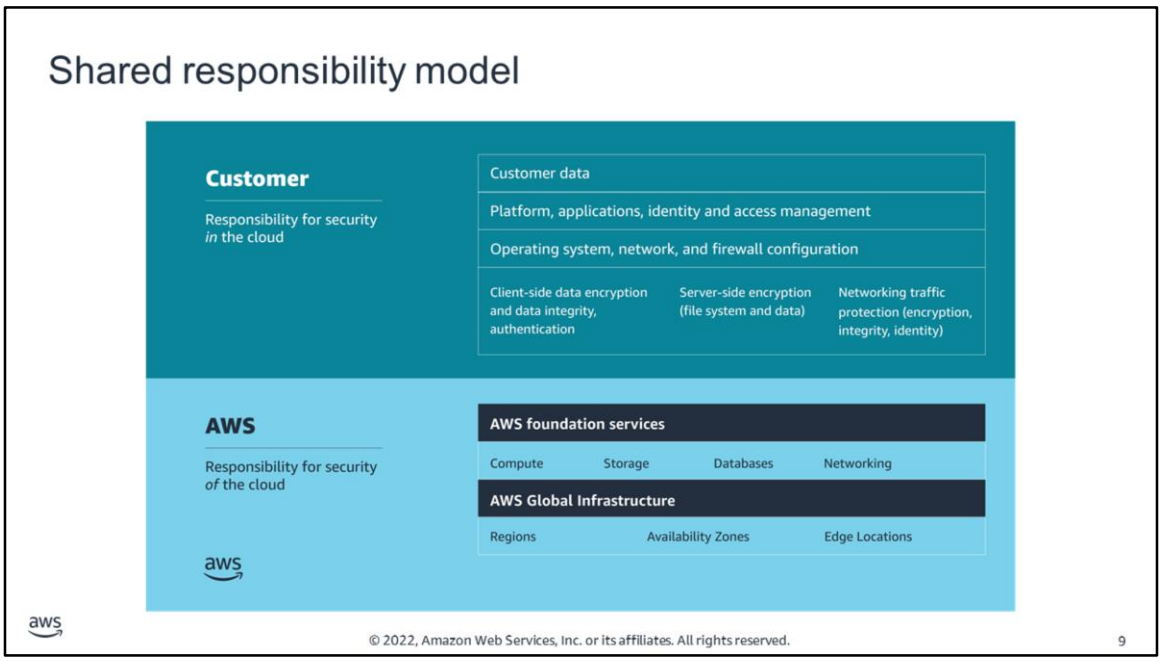


These capabilities can help an organization to identify, mitigate, and remediate security threats.

María creates a list of AWS logging and monitoring services.

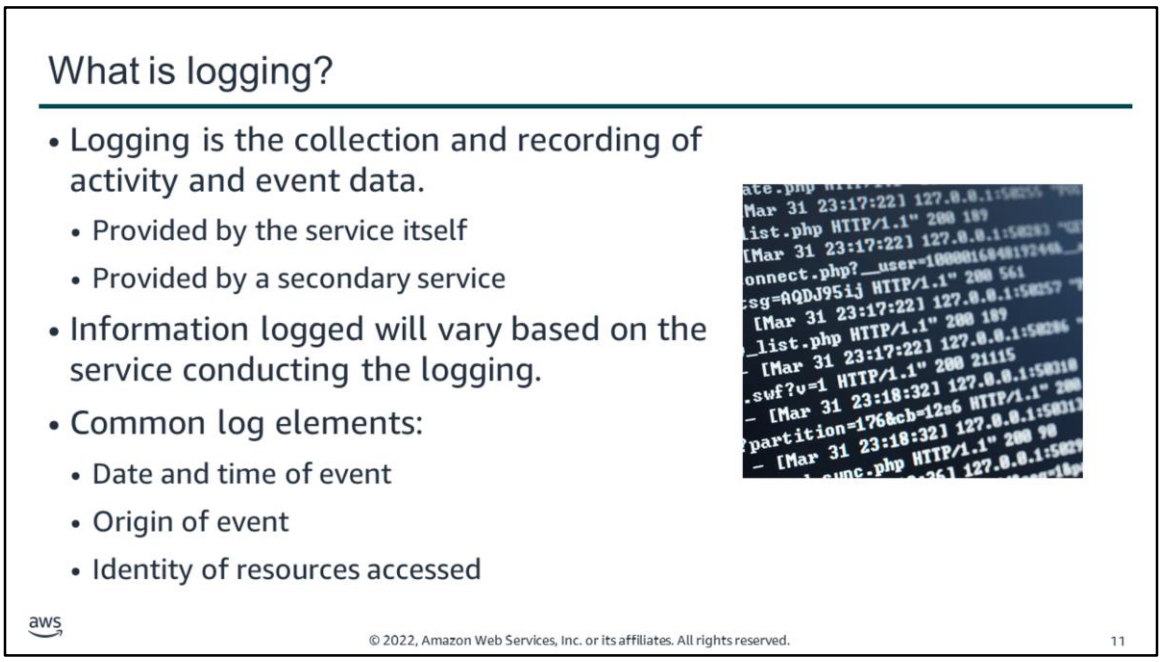
She will discuss these AWS offerings with John and explain the potential benefits and, if necessary, the potential costs.

María wants to align each service with the threat it could help mitigate so she's prepared for questions or scenarios that John might bring up.



Now that we've secured all of the tiers of a cloud application, let's look at the tools that AWS provides that help you log and monitor access to your resources to help you identify and react to anomalous behavior.

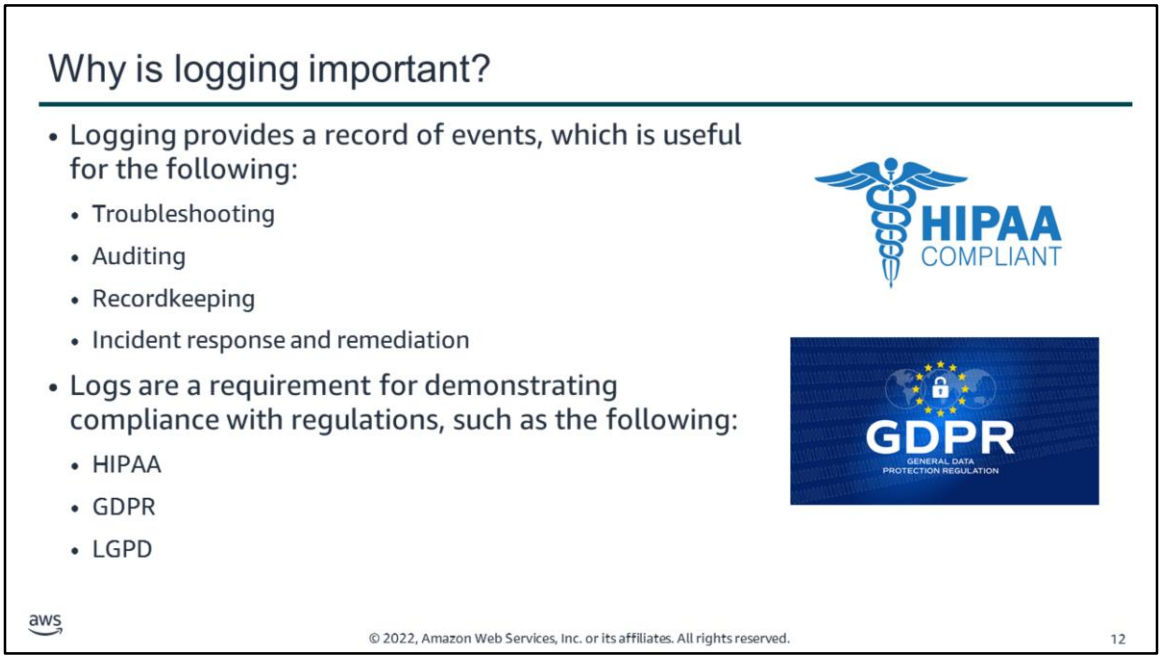
This section covers the importance of logging and monitoring.



Logging is the collection and recording of activity and event data. The service itself can provide logging capabilities, as with Amazon Virtual Private Cloud (Amazon VPC) Flow Logs and Amazon Simple Storage Service (Amazon S3) server access logs. Or a secondary service, such as AWS CloudTrail, might provide logging.

The type of information logged will vary based on the service that is conducting the logging, but some common elements are logged:

- Date and time of event
- Originating location of request
- Identity of resources accessed



A comprehensive logging methodology can help you in every phase of your incident response strategy. Log files are also a primary focus point in incident response. This is because of their ability to provide detailed, time-stamped records to investigators and incident responders. Logging 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.

Log files can assist in troubleshooting performance issues within your AWS Cloud and on-premises environment. Logs are also necessary to perform security audits and adhere to recordkeeping requirements to demonstrate compliance with a number of regulatory measures. Examples of regulatory measures include the Health Insurance Portability and Accountability Act (HIPAA) in the United States, the European Union General Data Protection Regulation (GDPR), and Brazil's General Data Protection Law (LGPD). Finally, log files can assist you to remediate issues that arise organically or through audits. Logs provide you with insights on the point in time when an issue arose.

What is monitoring?

- 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
  - AWS X-Ray

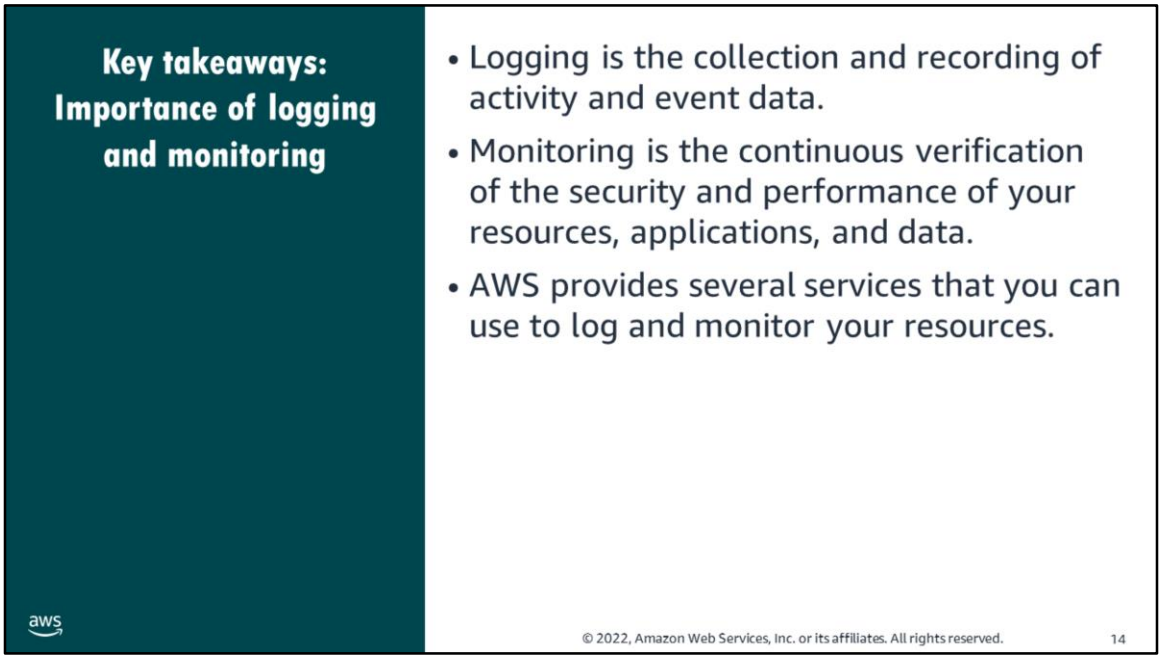
13

Monitoring is the practice of continuously verifying the security and performance of your resources and data. AWS provides several services that you can use to monitor your resources, but this module will focus on two: AWS CloudTrail and Amazon CloudWatch.

CloudTrail provides a record of actions taken within your environment. CloudTrail logs include information such as the action type, identity of the user, and time and date of the action. With this information, you can monitor who is doing what and when they are doing it.

With CloudWatch, you can monitor your resources and applications in real time. CloudWatch provides you with system-wide visibility into resource utilization, application performance, and operational health.

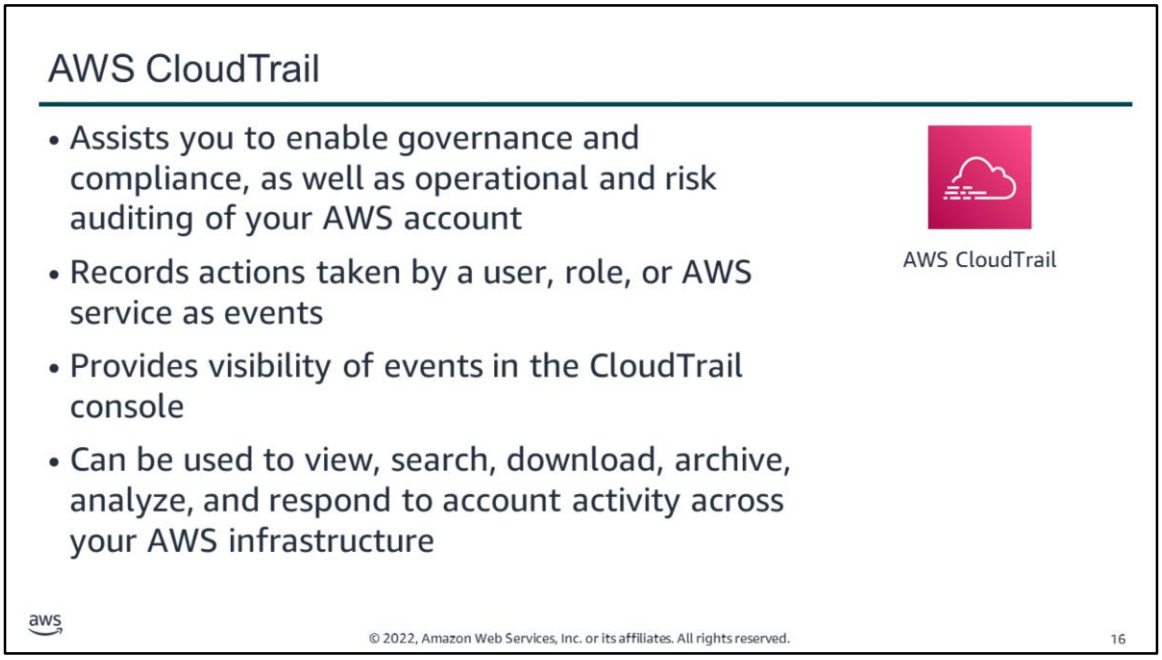
Monitoring services and tools, along with a solid incident response plan, can help you mitigate the effects of a system outage or malicious actor. In many cases, monitoring can help you to spot an issue before it has operational impact.



Key takeaways from this section of the module include the following:

- Logging is the collection and recording of activity and event data.
- Monitoring is the continuous verification of the security and performance of your resources, applications, and data.
- AWS provides several services that you can use to log and monitor your resources.

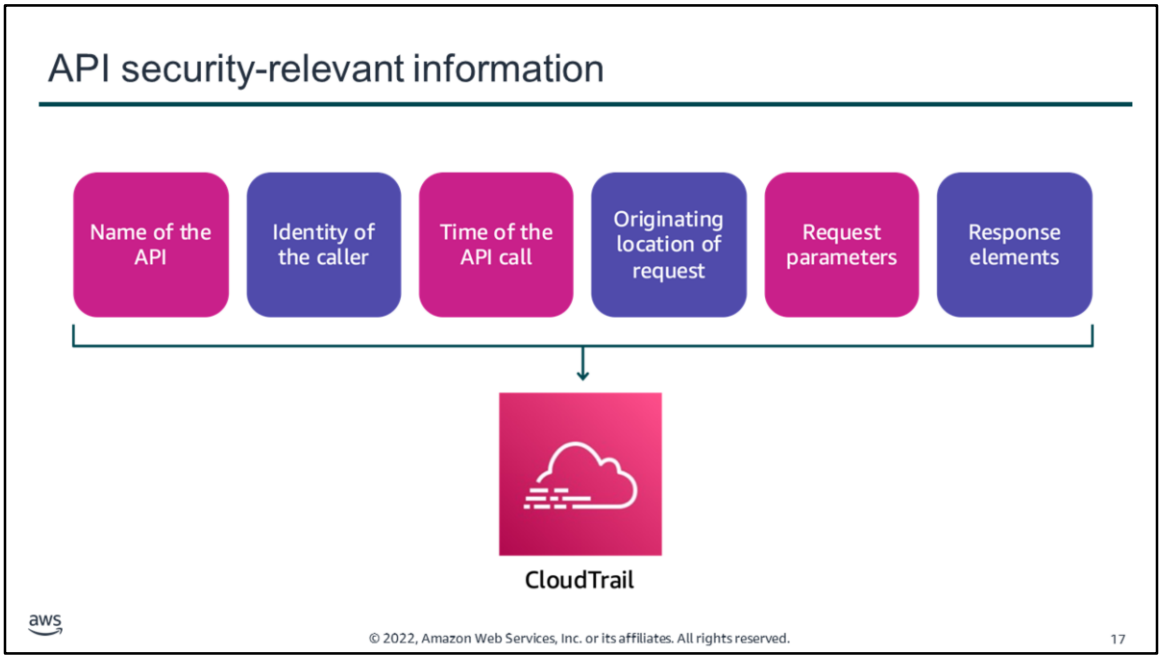
This section covers how to capture and collect logs.



AWS CloudTrail is an AWS service that 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, AWS Command Line Interface (AWS CLI), and AWS Software Development Kits (SDKs) and APIs. You can view, search, download, archive, analyze, and respond to these recorded events in the CloudTrail console.

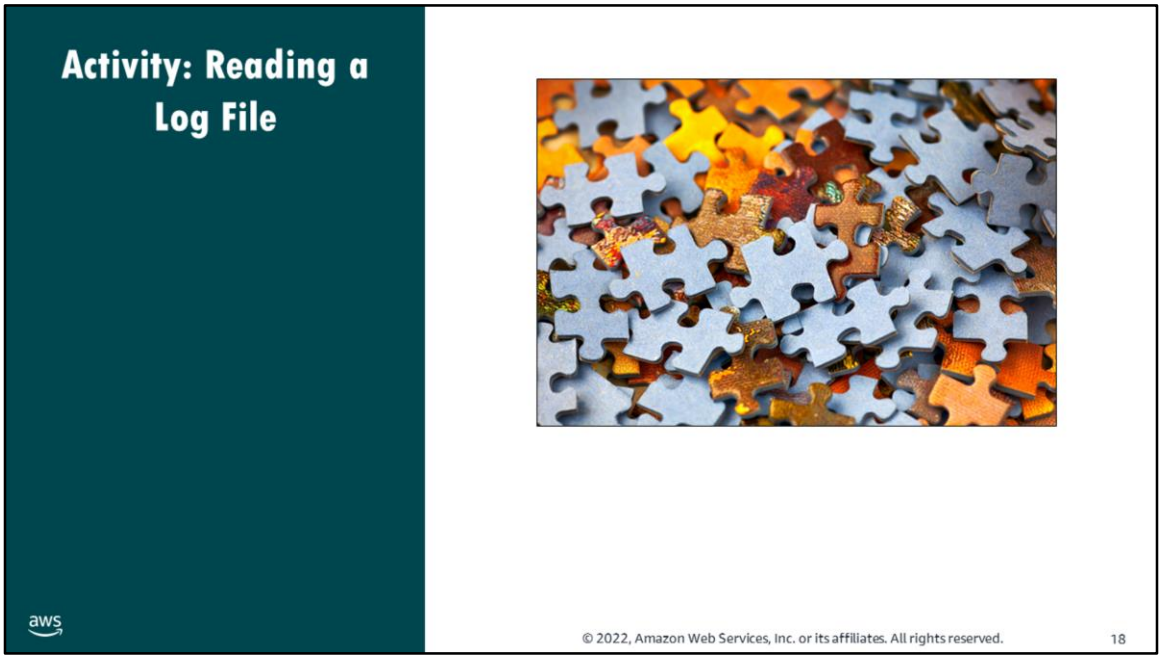
You can integrate CloudTrail into applications by using the API, automate trail creation for your organization, check the status of trails you create, and control how users view CloudTrail events.

For more information, see AWS CloudTrail at https://aws.amazon.com/cloudtrail.

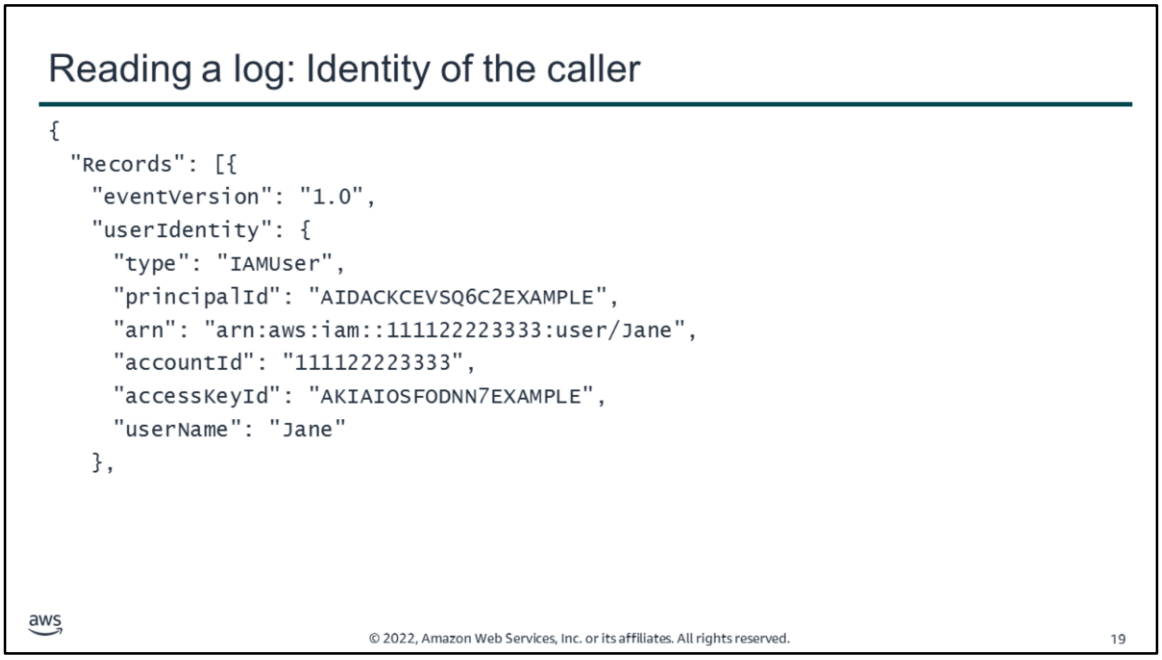


CloudTrail records important information about each API call. Information includes the name of the API, identity of the caller, time of the API call (captured in Universal Time Coordinated, or UTC), location that the call originated from, request parameters, and response elements returned by the AWS service. This information helps you to track changes made to your AWS resources, troubleshoot operational issues, and ensure compliance with internal policies and regulatory standards.

You can use the AWS API call history that CloudTrail produces to track changes to AWS resources. Changes include creation, modification, and deletion of AWS resources, such as Amazon Elastic Compute Cloud (Amazon EC2) instances and Amazon VPC security groups. The log file record example on the next few slides shows actions from an AWS Identity and Access Management (IAM) user named Jane. Jane used the ec2-stop-instances command in the AWS CLI to call the Amazon EC2 StopInstances action.



In this educator-led activity, you will read a CloudTrail log file.

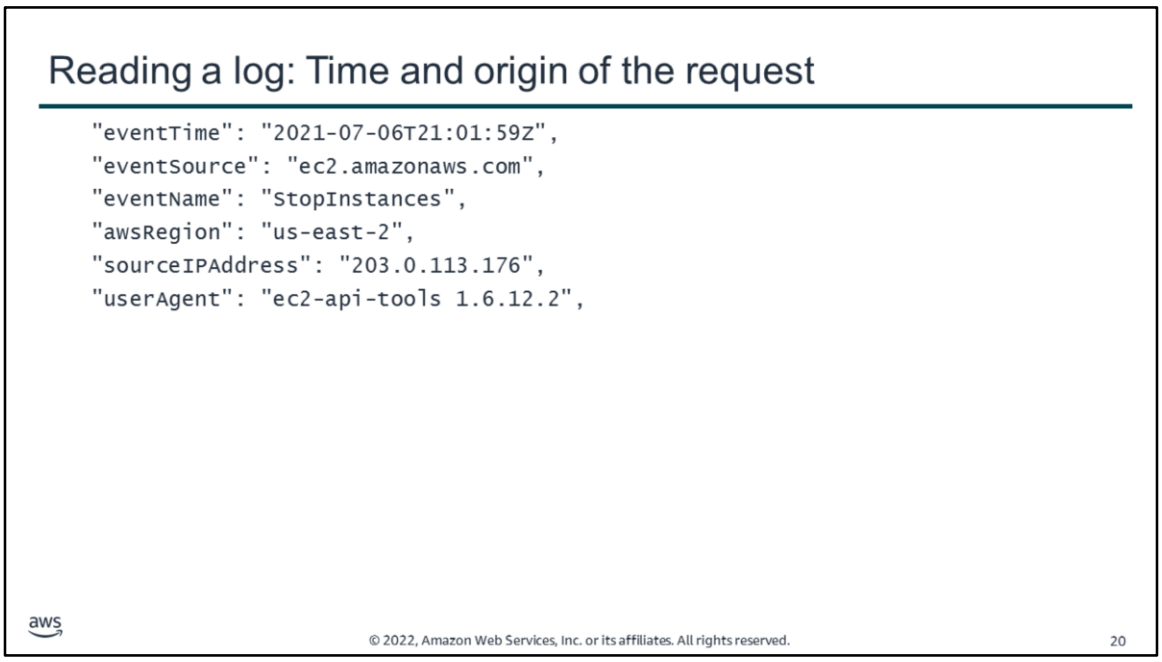


This log file was generated when someone or something performed some kind of action.

Take a moment to review this log file snippet, and then answer the following questions individually or as a group:

1. What type of account did the log collect information about?
2. What can you determine from the **arn** element?

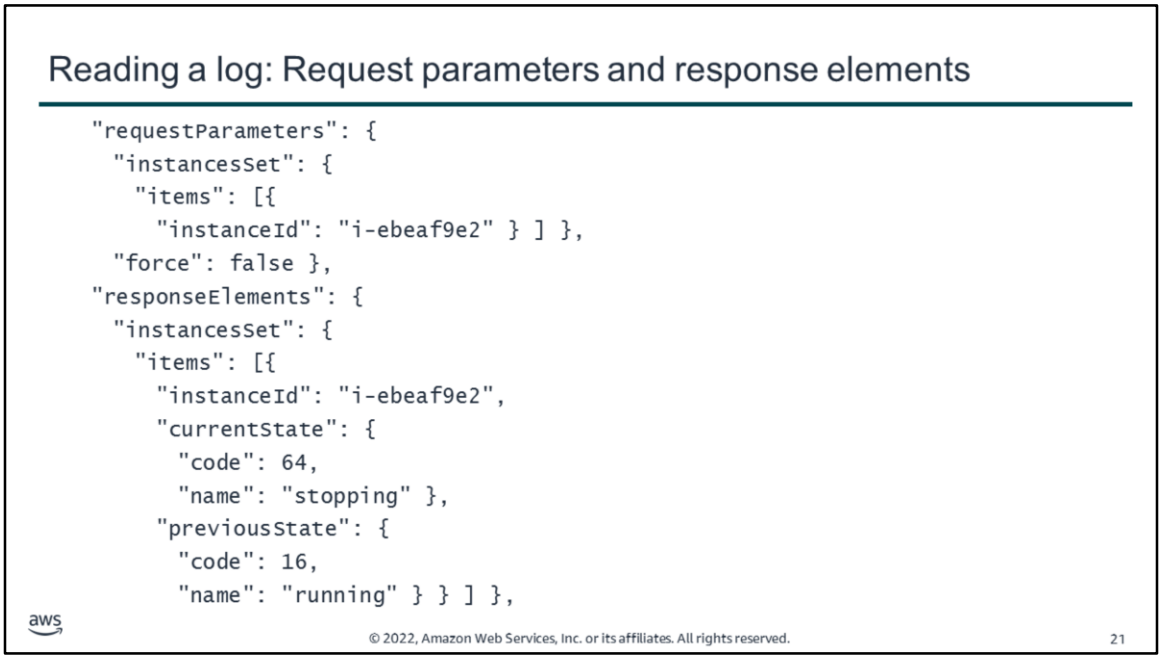
On the next slide, you will be able to see when this call was made.



Take a moment to review this log file snippet, and then answer the following questions individually or as a group:

1. What does the **eventSource** field give you information about?
2. In the **eventName** field, what does the **StopInstances** value indicate?
3. What method was used to perform this action? (Console, AWS CLI, or other)

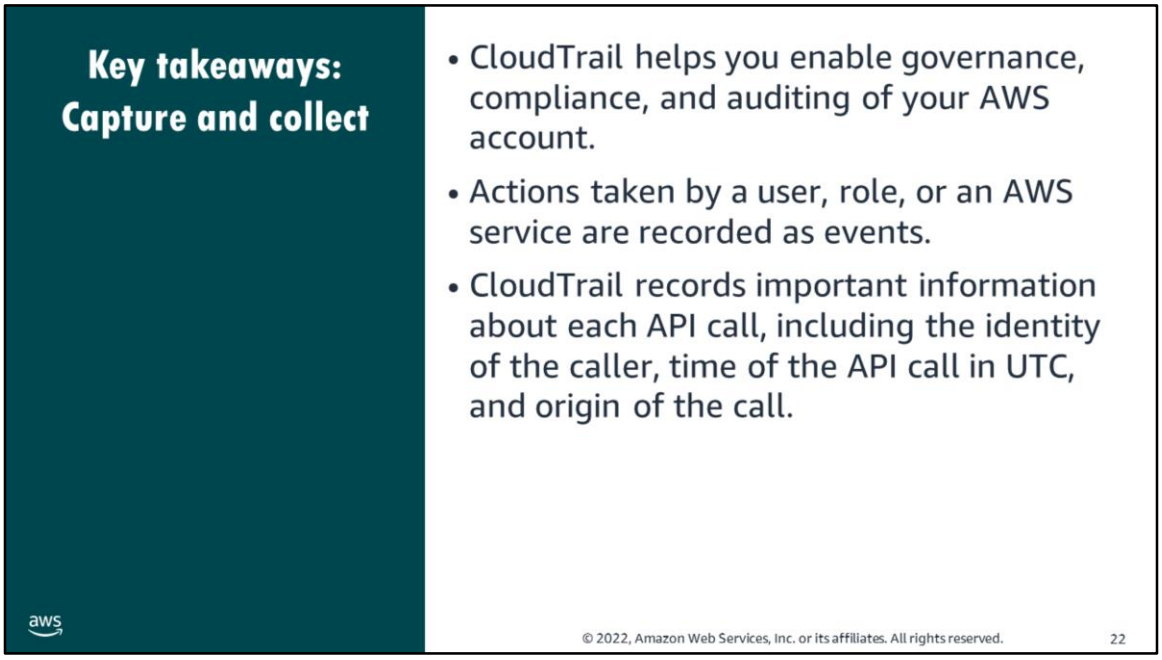
Now let's see what was involved in this request.



Take a moment to review this log file snippet, and then answer the following questions individually or as a group:

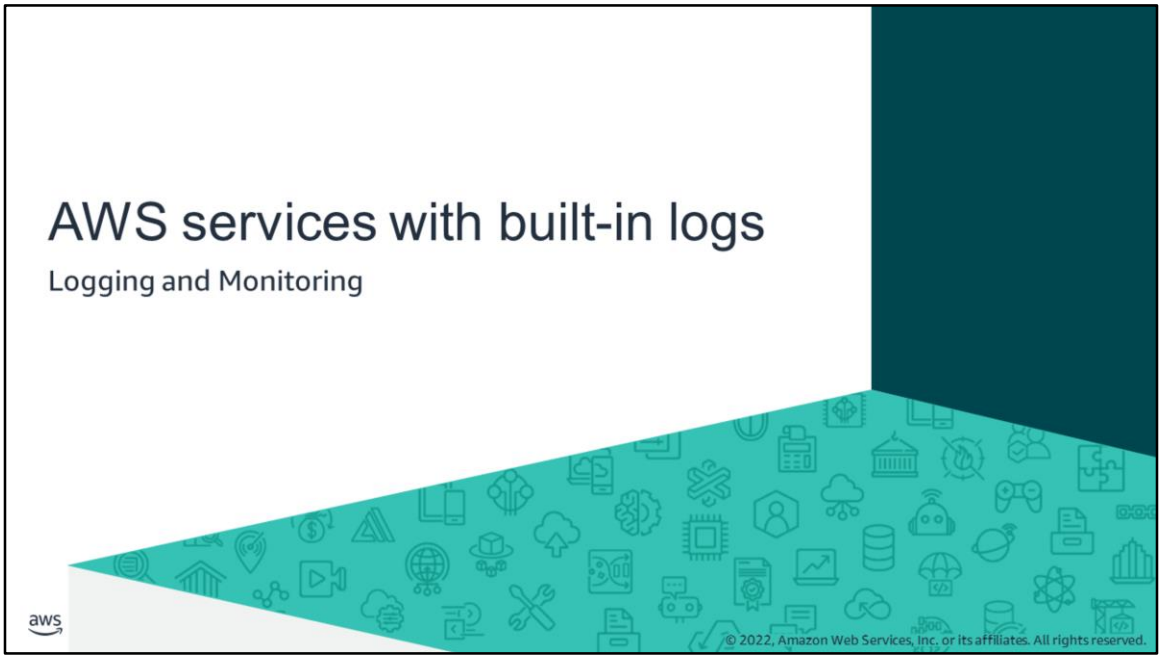
1. In the **instanceId** field, what does the **i-ebeaf9e2** value indicate?
2. What was the action that was performed?

If you need to track changes to such resources, answer questions about user activity, demonstrate compliance, troubleshoot, or perform security analysis, you can use CloudTrail to detect threats and provide security.

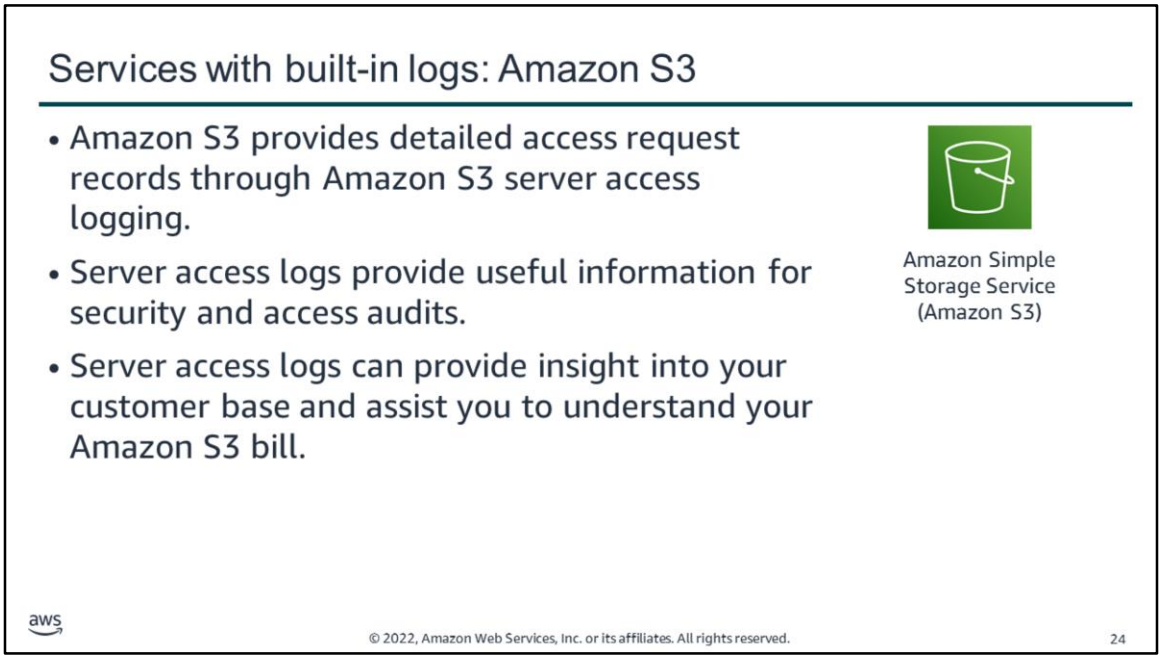


Key takeaways from this section of the module include the following:

- CloudTrail helps you enable governance, compliance, and auditing of your AWS account.
- Actions taken by a user, role, or an AWS service are recorded as events.
- CloudTrail records important information about each API call, including the identity of the caller, time of the API call in UTC, and origin of the call.

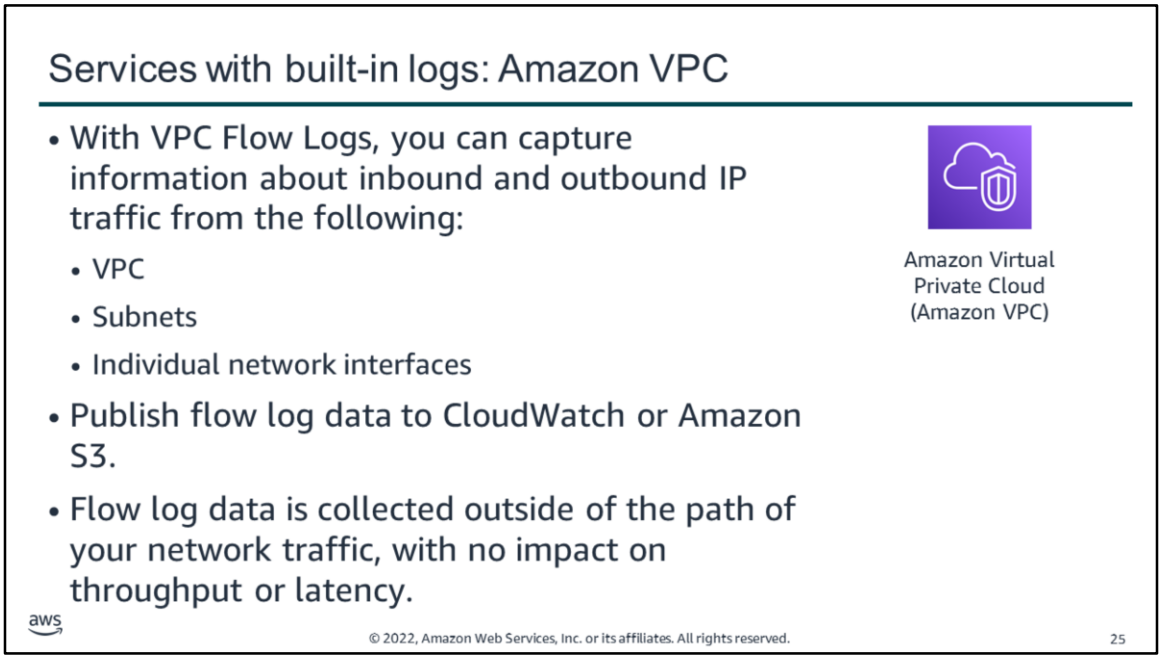


This section describes AWS services that have built-in logging.



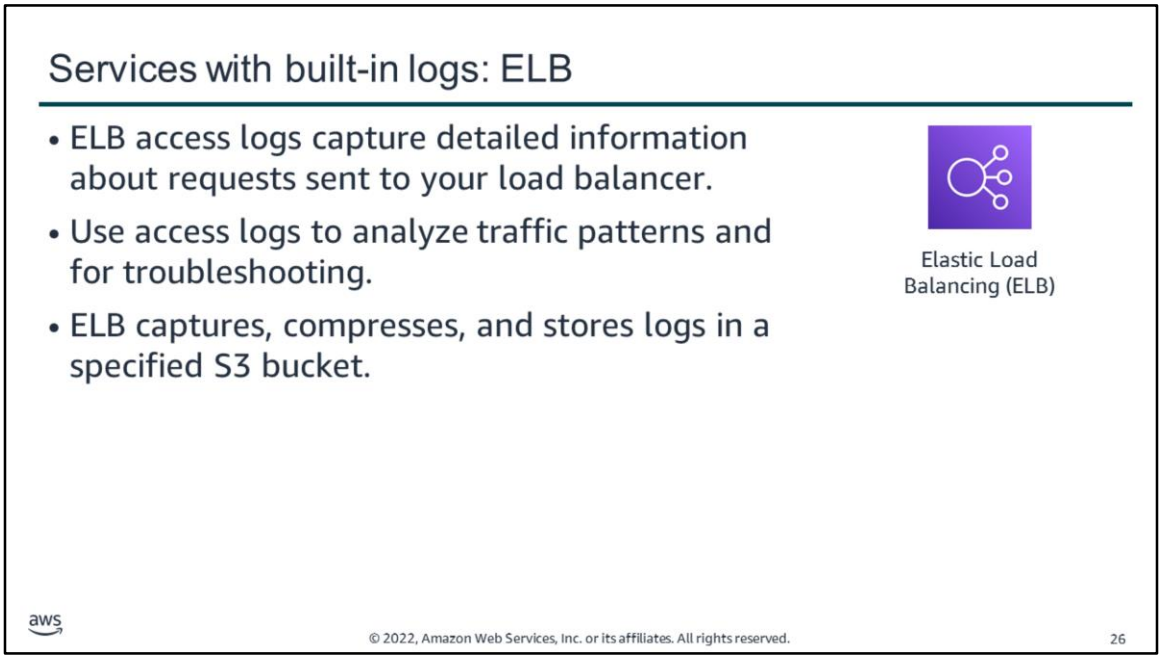
Server access logging is a built-in feature of Amazon S3. Enable the feature for detailed records of requests that are made to an S3 bucket. These logs are useful in a number of ways—from providing information during a security and access audit to providing insights about your customer base. Server access logs can also provide insights into your storage usage, which can help you to better understand your Amazon S3 bill.

For more information, see Logging Requests Using Server Access Logging in the *Amazon S3 User Guide* at https://docs.aws.amazon.com/AmazonS3/latest/userguide/ServerLogs.html.



VPC Flow Logs is a built-in feature of Amazon VPC. Flow logs capture information about inbound and outbound IP traffic from your VPC network interfaces. Flow logs can be captured at the VPC level, the subnet level, or for each individual network interface. You can publish flow log data to the Amazon CloudWatch Logs service or Amazon S3. Flow logs are helpful to troubleshoot, monitor, and analyze the flow of IP traffic within your VPC. Because flow log data is collected outside of the path of your network traffic, there is no impact on throughput, latency, or overall performance.

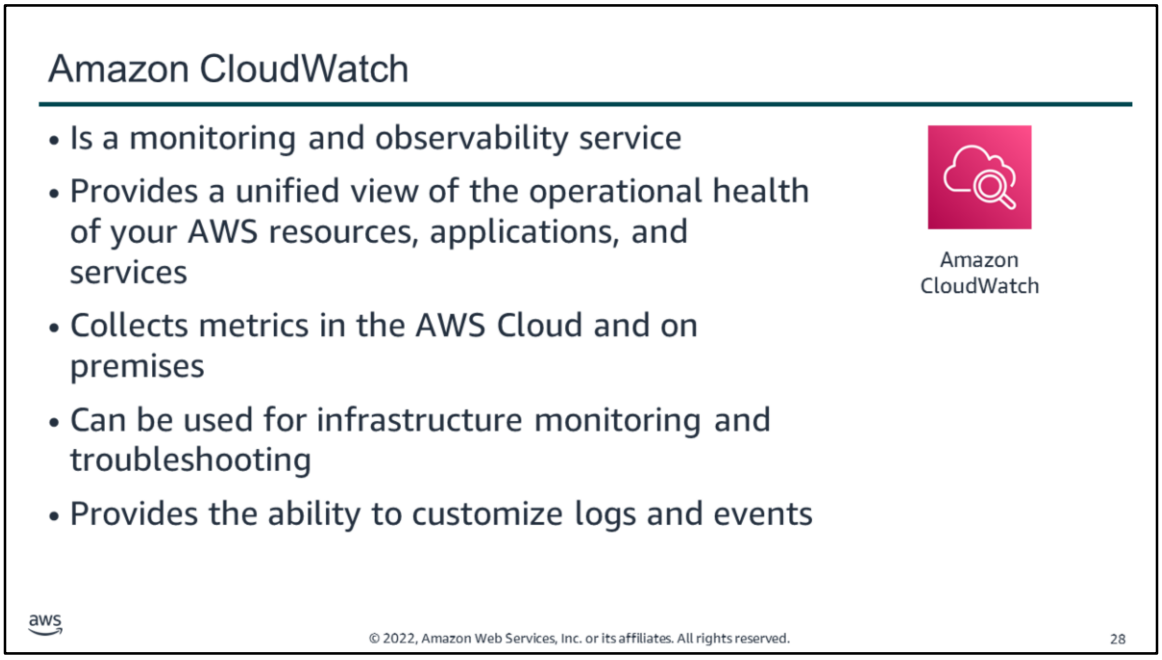
For more information, see Logging IP Traffic with VPC Flow Logs in the *Amazon VPC User Guide* at https://docs.aws.amazon.com/vpc/latest/userguide/flow-logs.html.



Elastic Load Balancing (ELB) access logs capture detailed information about requests sent to your load balancer. Logs contain information about the time of request receipt, IP address of the client, latencies, request paths, and server responses. The information contained in these logs can assist you to troubleshoot issues and analyze traffic on your network.

For more information, see Access Logs for Your Application Load Balancer in the *User Guide for Application Load Balancers* at https://docs.aws.amazon.com/elasticloadbalancing/latest/application/load-balancer-access-logs.html.

This section covers monitoring and reporting.

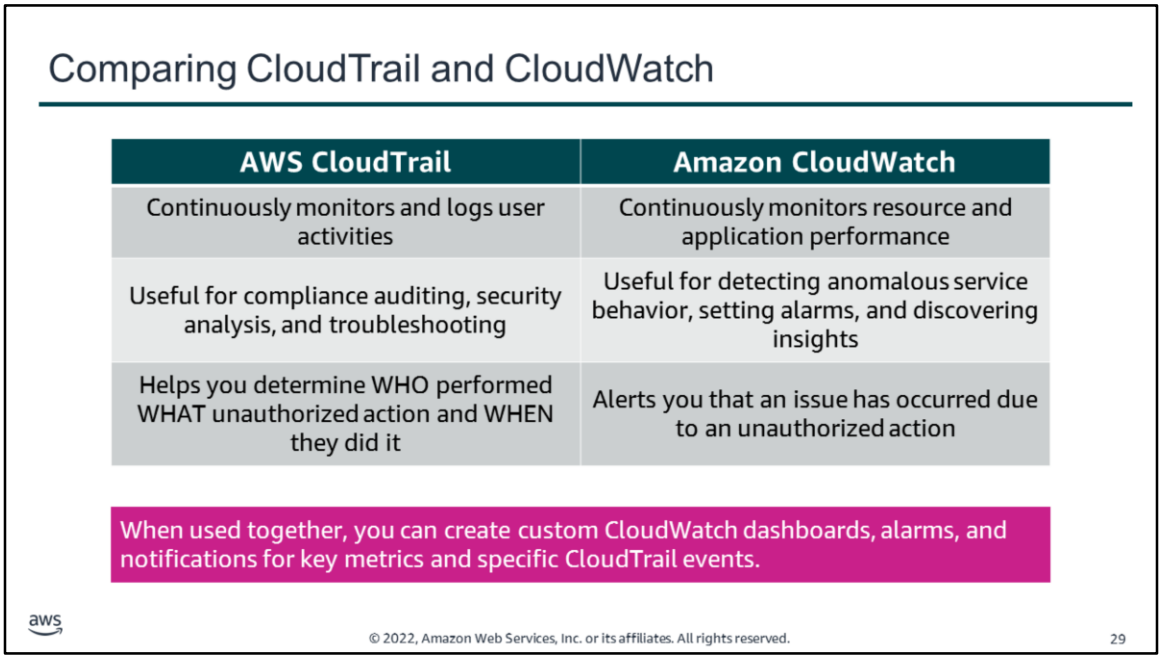


Amazon CloudWatch is a monitoring and observability service built for DevOps engineers, developers, site reliability engineers (SREs), IT managers, and product owners. CloudWatch collects monitoring and operational data as logs, metrics, and events. This information gives you a unified view of your AWS resources, applications, and services that run on AWS and on-premises servers. You can use CloudWatch to detect anomalous behavior in your environments, set alarms, visualize logs and metrics side by side, take automated actions, troubleshoot issues, and discover insights to keep your applications running smoothly. With CloudWatch, you can collect, access, and correlate information from all your AWS resources, applications, and services running on AWS and on premises. This capability helps you break down data silos to gain system-wide visibility and quickly resolve issues.

You can use CloudWatch Events to deliver a near-real-time stream of system events that describe changes in AWS resources. CloudWatch Events becomes aware of operational changes as they occur and responds to them. CloudWatch Events takes corrective action as necessary by sending messages to respond to the environment, activating functions, making changes, and capturing state information. CloudWatch Events is currently being replaced by Amazon EventBridge.

With CloudWatch Logs, you can monitor, store, and access your log files from EC2 instances, CloudTrail, Amazon Route 53, and other sources. You can centralize the logs from all of your systems, applications, and AWS services in a single, highly scalable service. You can then easily view the logs, search them for specific error codes or patterns, filter them based on specific fields, or archive them securely for future analysis. With CloudWatch Logs, you can see all of your logs, regardless of their source, as a single and consistent flow of events ordered by time. You can query the logs and sort them based on other dimensions, group them by specific fields, create custom computations with a powerful query language, and visualize log data in dashboards.

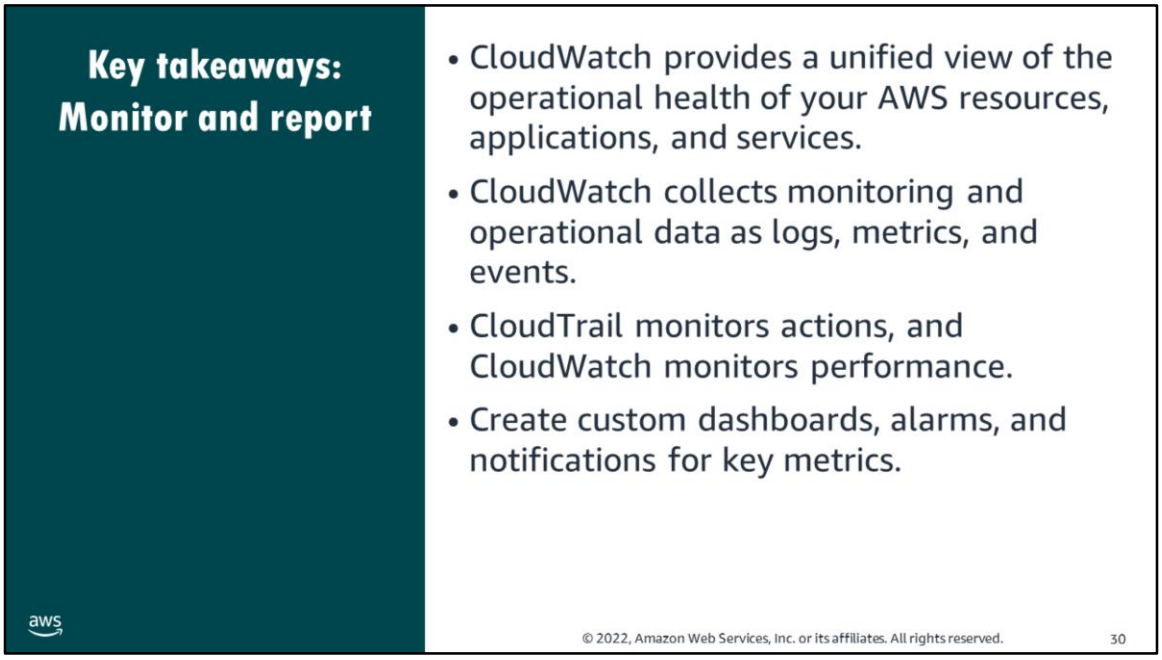
For more information, see Amazon CloudWatch at https://aws.amazon.com/cloudwatch.



The AWS CloudTrail service provides the ability to continuously monitor and log the activity of users, groups, and roles within your AWS environment. These log files are useful for compliance auditing, security analysis, and troubleshooting. Assume that an EC2 instance was deleted without permission. CloudTrail could provide a log that gives you the identity of the user, group, or role that performed the unauthorized action.

Amazon CloudWatch provides the ability to continuously monitor the performance of your AWS resources and applications. CloudWatch can help detect and notify you of anomalous service behavior, such as an EC2 instance deletion. Whether coupled with CloudTrail or on its own, CloudWatch provides you with increased oversight of your AWS environment.

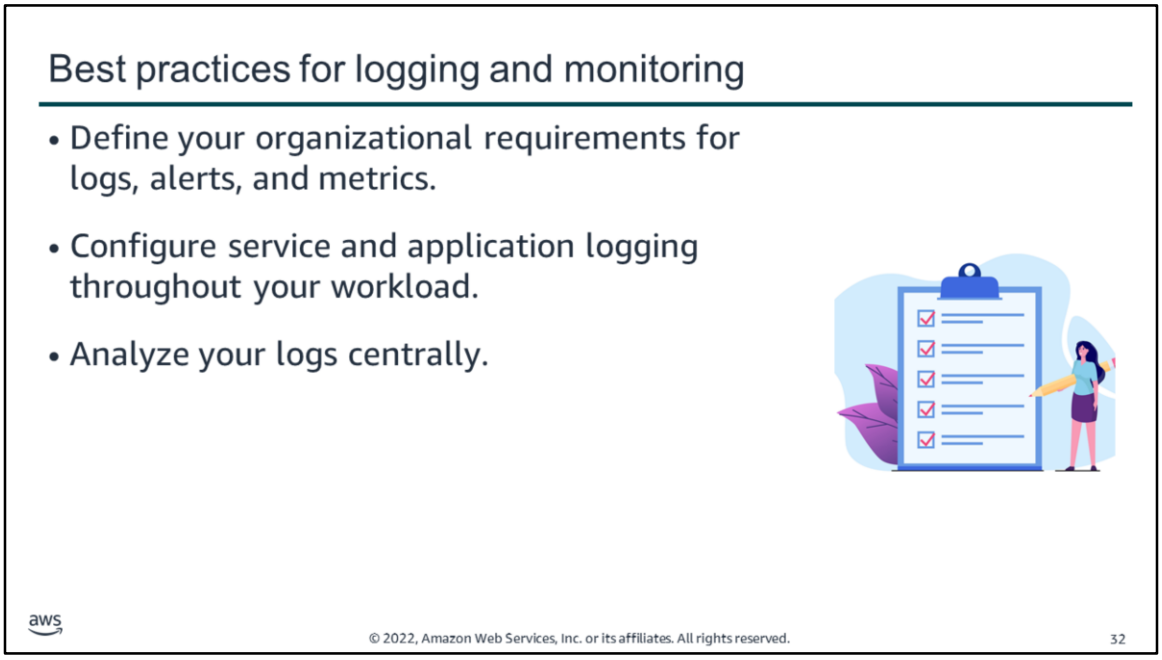
When used together, you can create custom CloudWatch alarms and notifications for specific CloudTrail events. This helps you to respond quickly to key operational issues.



Key takeaways from this section of the module include the following:

- CloudWatch provides a unified view of the operational health of your AWS resources, applications, and services.
- CloudWatch collects monitoring and operational data as logs, metrics, and events.
- CloudTrail monitors actions, and CloudWatch monitors performance.
- Create custom dashboards, alarms, and notifications for key metrics.

This section describes best practices for logging and monitoring.

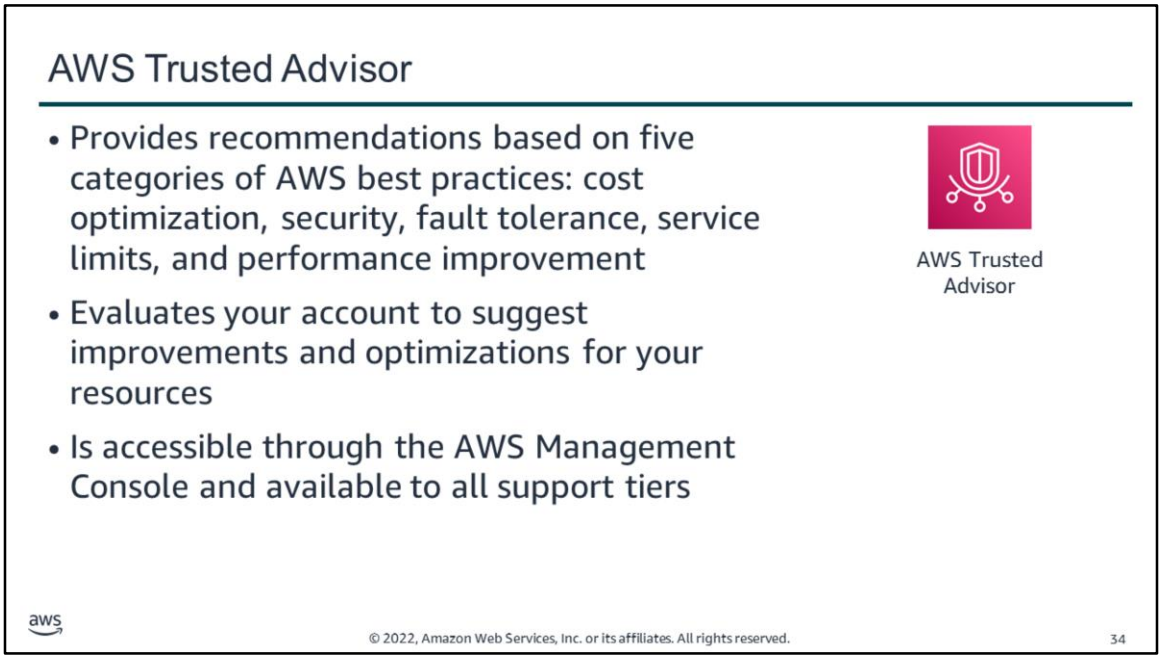


The first step to use the logging and monitoring capabilities that AWS provides is to define your requirements. Identify the resources, applications, and services that you want to maintain logs for. Logging and monitoring requirements can vary widely, so you must determine what the organizational, legal, and compliance requirements for your workloads are. Then, evaluate and identify the resources that AWS has available to assist.

When you collect metrics and define baselines, you can gain insights to potential security threats. Define who should receive alerts and what they should do with the alerts that they receive. Configure logging throughout the workload, including application logs, AWS services logs, and resource logs.

Collect your logs centrally. Use automation from services such as CloudWatch to analyze logs to detect any anomalies or indicators of malicious activity or compromise.

This section covers additional AWS services for logging and monitoring.

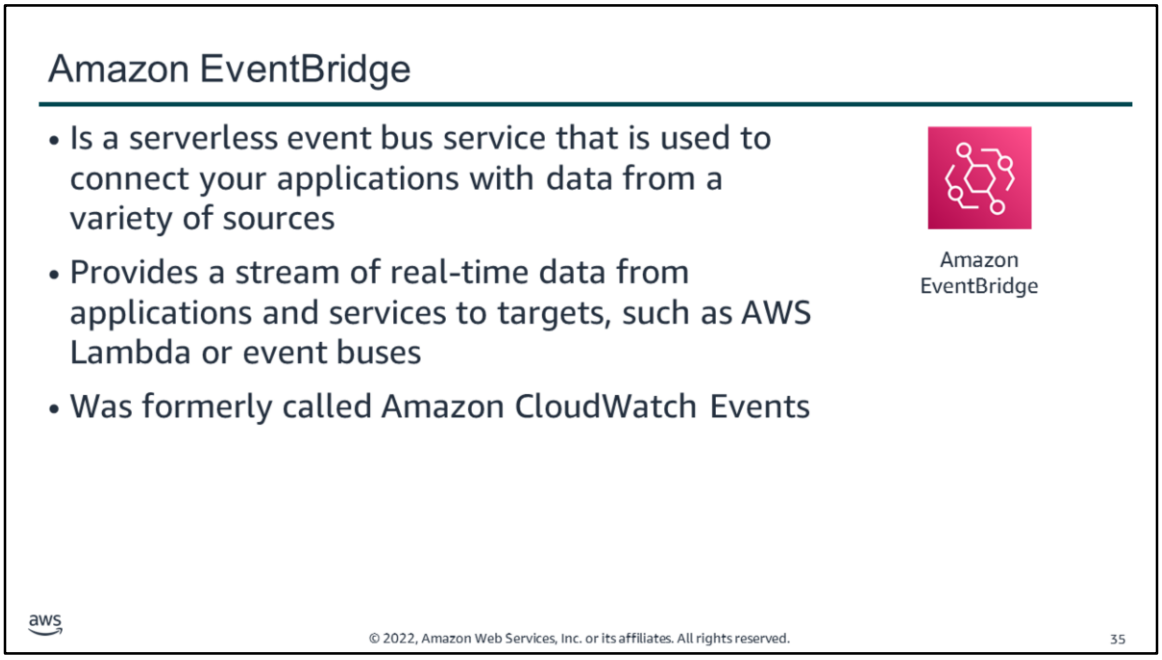


AWS Trusted Advisor provides recommendations that help you follow AWS best practices, which have been learned from serving hundreds of thousands of AWS customers. Trusted Advisor evaluates your account by using checks based on five categories of AWS best practices. The checks identify ways to optimize your AWS infrastructure, improve security and performance, reduce costs, and monitor service quotas.

Assume you're the administrator of your organization's AWS account. You're looking for ways to optimize your account resources and improve your overall security posture, but the time it would take to do so manually would be prohibitive. AWS Trusted Advisor can automate this process for you, providing you with recommendations for actions you can take to improve these areas. You can then follow the recommendations to optimize your resources and security posture.

Trusted Advisor is available in all AWS Support plans. AWS Basic Support and AWS Developer Support customers can access core security checks and all checks for service quotas. AWS Business Support and AWS Enterprise Support customers can access all checks, including cost optimization, security, fault tolerance, performance, and service quotas.

For more information, see AWS Trusted Advisor in the *AWS Support User Guide* at https://docs.aws.amazon.com/awssupport/latest/user/trusted-advisor.html.

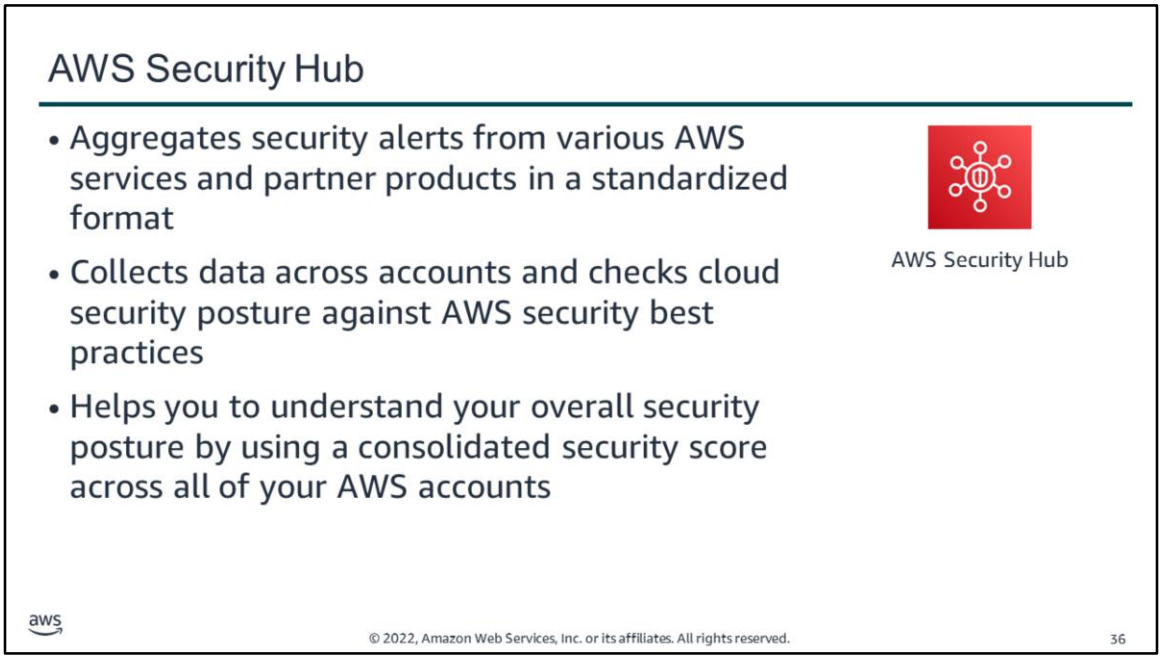


Amazon EventBridge is a serverless event bus service that makes it easier for you to build event-driven applications by connecting those applications with data from a variety of sources. The service connects applications by using *events*, which are signals that a system's state has changed. To use the service, you don't need to provision, patch, or manage any servers, and you don't need to install or maintain any software. EventBridge automatically scales based on the number of events ingested and has built-in fault tolerance.

Let's look at how can EventBridge be used to help you with your monitoring and auditing. You can monitor and audit your AWS environments and respond to operational changes in your applications in real-time to prevent infrastructure vulnerabilities. For example, when your resources are accessed by cross-accounts or public accounts, you can configure an Amazon Access Analyzer event to be generated and sent to an AWS Lambda Function using EventBridge to remove the unintended permissions.

EventBridge was formerly known as Amazon CloudWatch Events. CloudWatch Events and EventBridge use the same API, so any code that you were previously using with CloudWatch Events stays the same. Although both services are still supported, new features are only added to EventBridge.

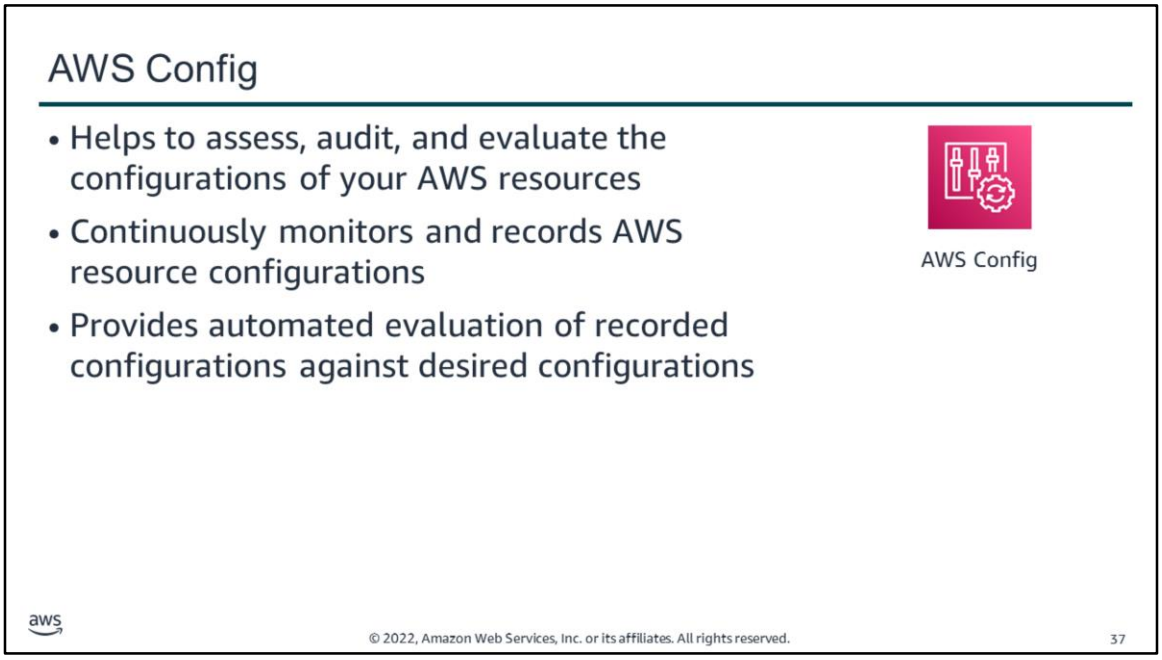
For more information, see the *Amazon EventBridge User Guide* at https://docs.aws.amazon.com/eventbridge/latest/userguide/eb-what-is.html.



AWS Security Hub is a service that assists you to monitor your cloud security posture through the use of automated, continuous security best practice checks against your AWS resources. Security Hub aggregates security alerts from various AWS services and third-party partner products, and presents them in a standardized format, making it easier for you to act on the alerts. You can also use Security Hub to create automated response, remediation, and enrichment workflows by taking advantage of Security Hub's integration with EventBridge. Security Hub provides a security score for each enabled standard and a total score for all accounts associated with your administrator account. This information can assist you to monitor your overall security posture.

One example of how AWS Security Hub can help is by assisting you in prioritizing the response and remediation efforts of your central security teams and DevSecOps teams by searching, correlating, and aggregating diverse security findings by accounts and resources.

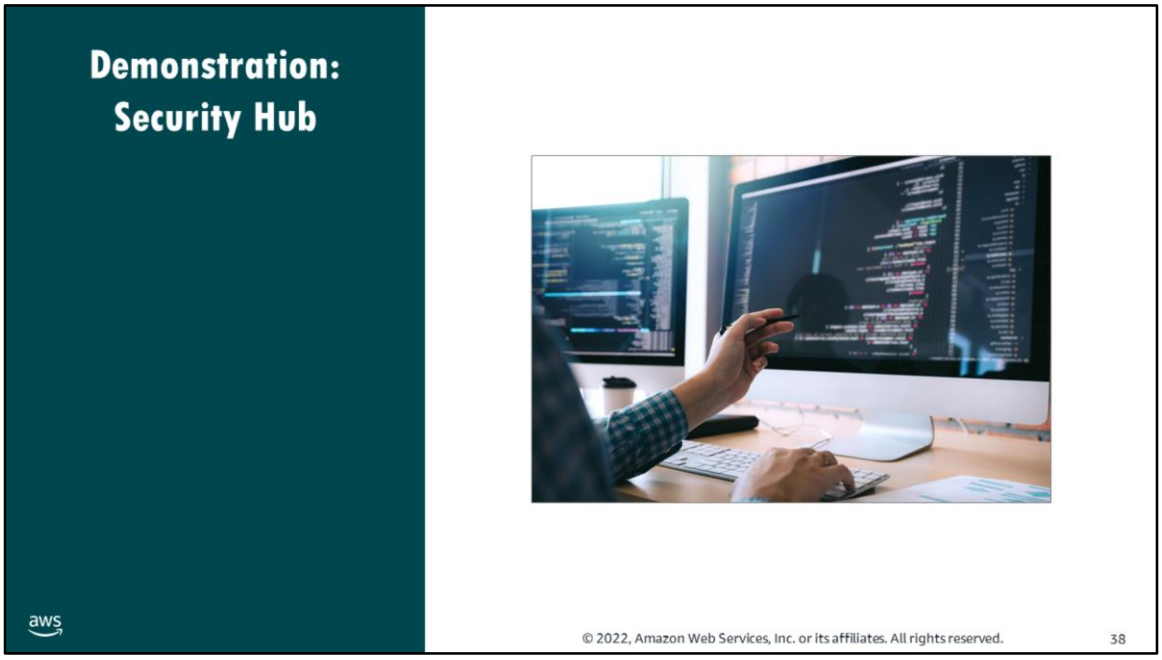
For more information, see AWS Security Hub at https://aws.amazon.com/security-hub.



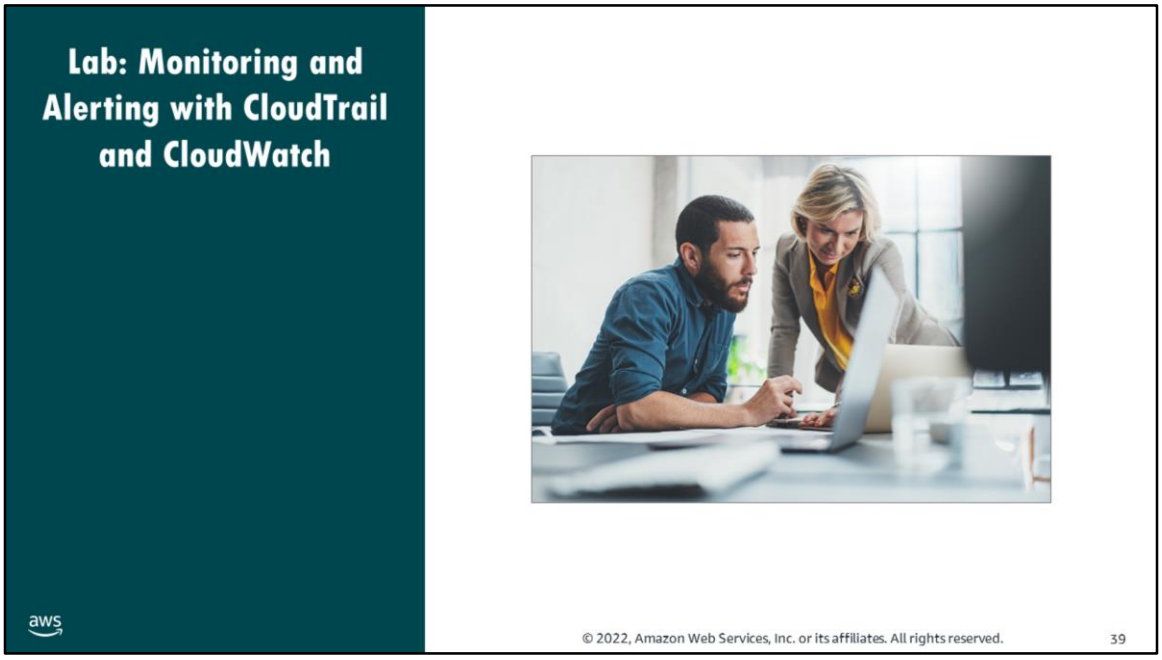
With the AWS Config service, you can assess, audit, and evaluate the configurations of your AWS resources. AWS Config continuously monitors and records your AWS resource configurations, which provides you with the ability to automate the evaluation of those configurations against desired configurations. You can also use AWS Config to view IAM policies that are assigned to IAM users, groups, or roles at any time that AWS Config was recording. This capability can aid you in determining what permissions belonged to what user at that specific time. AWS Config can assist you to maintain auditing and compliance by providing historical resource configurations. With the wide range of AWS Config capabilities, you can simplify compliance auditing, security analysis, change management, and operational troubleshooting in your AWS environment.

An example of an area where AWS Config is a valuable asset is change management. When your resources are created, updated, or deleted, AWS Config streams these configuration changes to Amazon Simple Notification Service (SNS), so that you are notified of all the configuration changes. AWS Config represents relationships between resources so that you can assess how a change to one resource may impact other resources.

For more information, see AWS Config at https://aws.amazon.com/config.

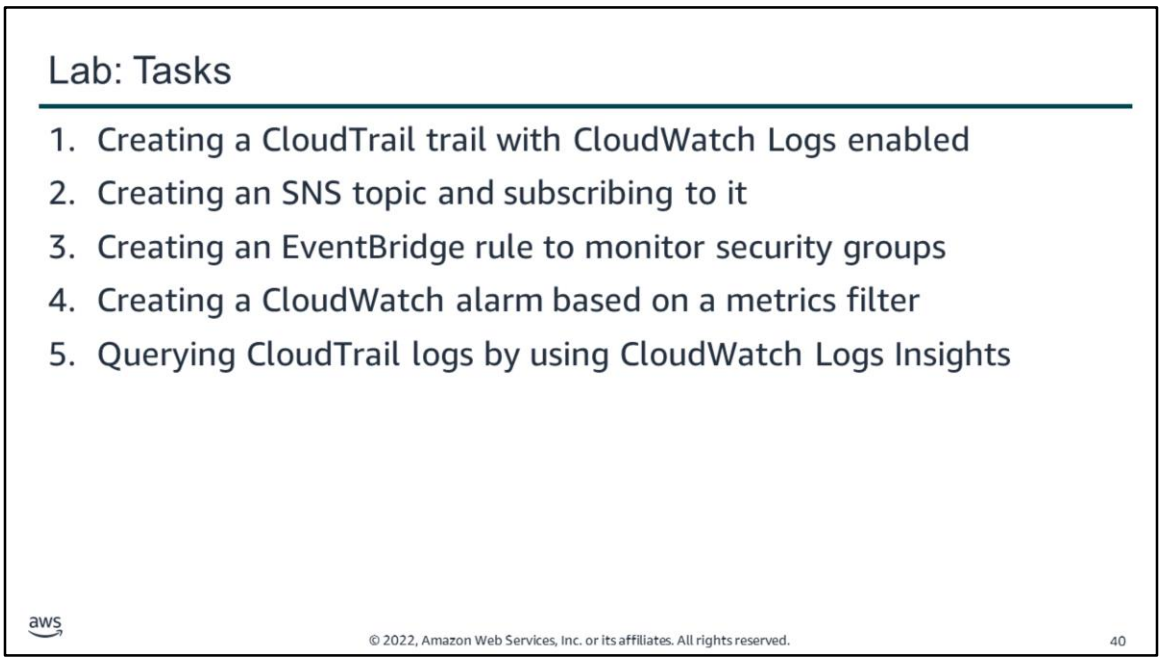


You will now view a recorded demonstration of AWS Security Hub.



You will now complete the Monitoring and Alerting with CloudTrail and CloudWatch lab.

In this lab, you will configure logging and monitoring in an AWS account.

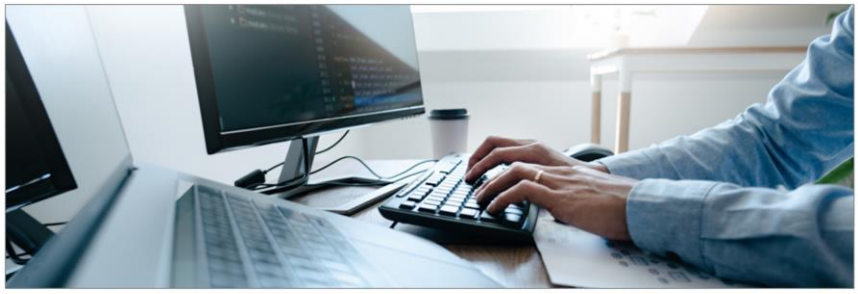


In this lab, you will complete the following tasks:

1. Creating a CloudTrail trail with CloudWatch Logs enabled
2. Creating an SNS topic and subscribing to it
3. Creating an EventBridge rule to monitor security groups
4. Creating a CloudWatch alarm based on a metrics filter
5. Querying CloudTrail logs by using CloudWatch Logs Insights

Begin Lab: Monitoring and Alerting with CloudTrail and CloudWatch

Duration: 60 minutes



aws

41

It's now time to start the lab.

After you complete the lab, your educator might choose to lead a conversation about the key takeaways from the lab.

It’s now time to review the module, and wrap up with a knowledge check and discussion of a practice certification exam question.

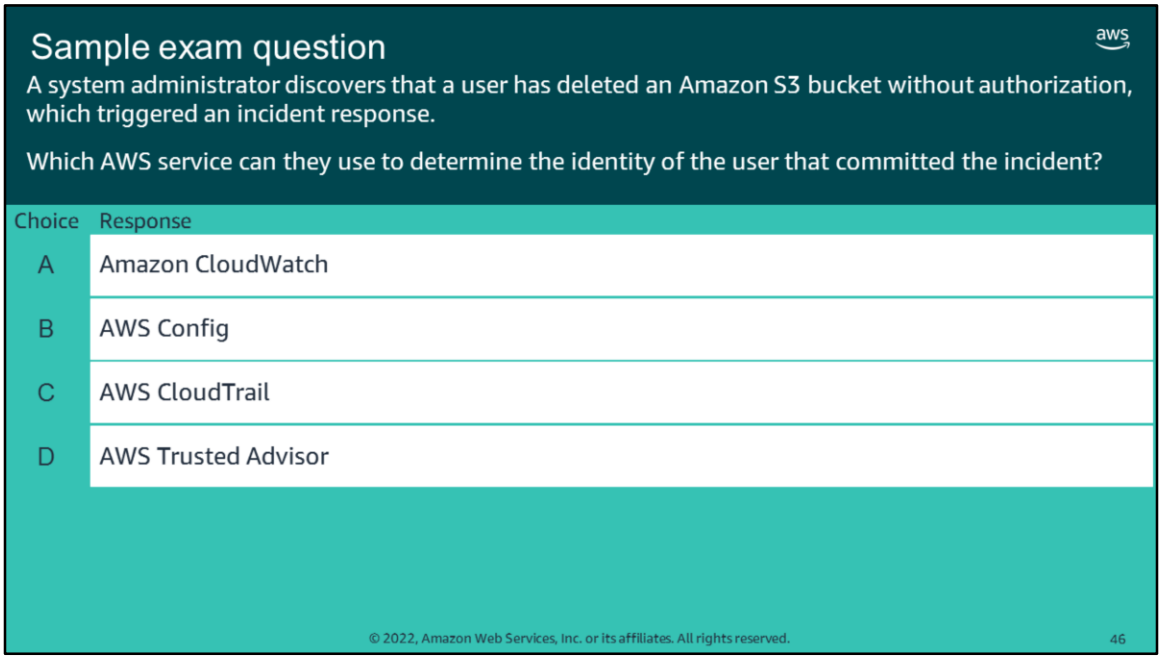
In this module you learned how to do the following:

- 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 AWS resources and applications.
- Recognize when to use CloudWatch and when to use CloudTrail.

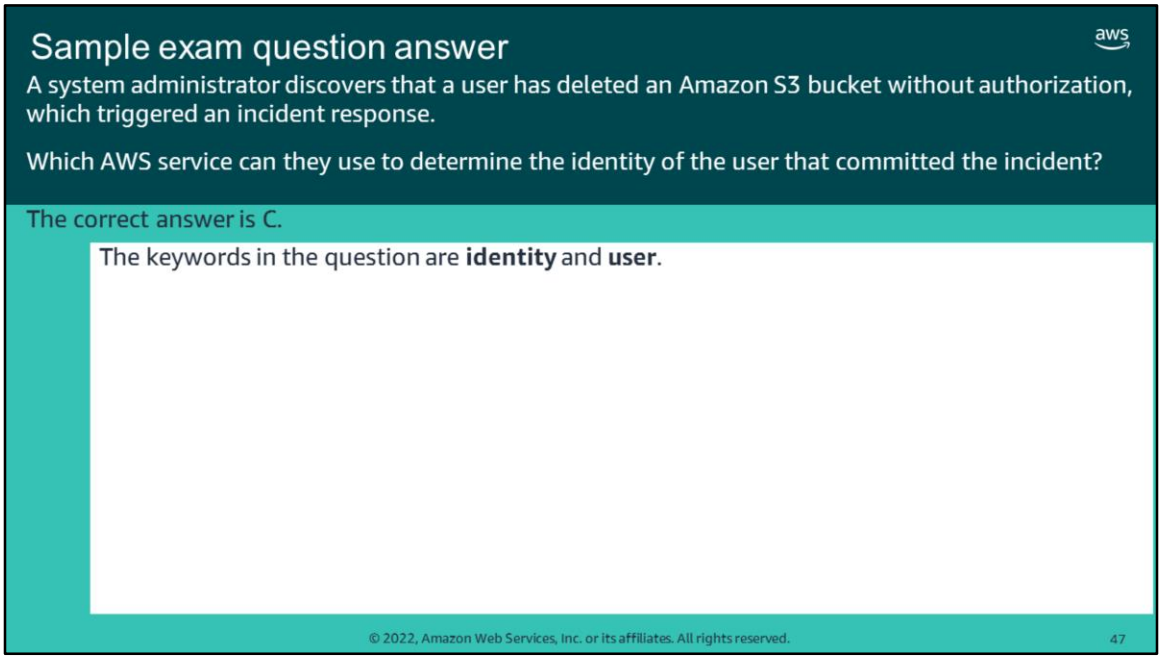
Complete the knowledge check

45

It is now time to complete the knowledge check for this module.



Look at the answer choices, and rule them out based on the keywords.

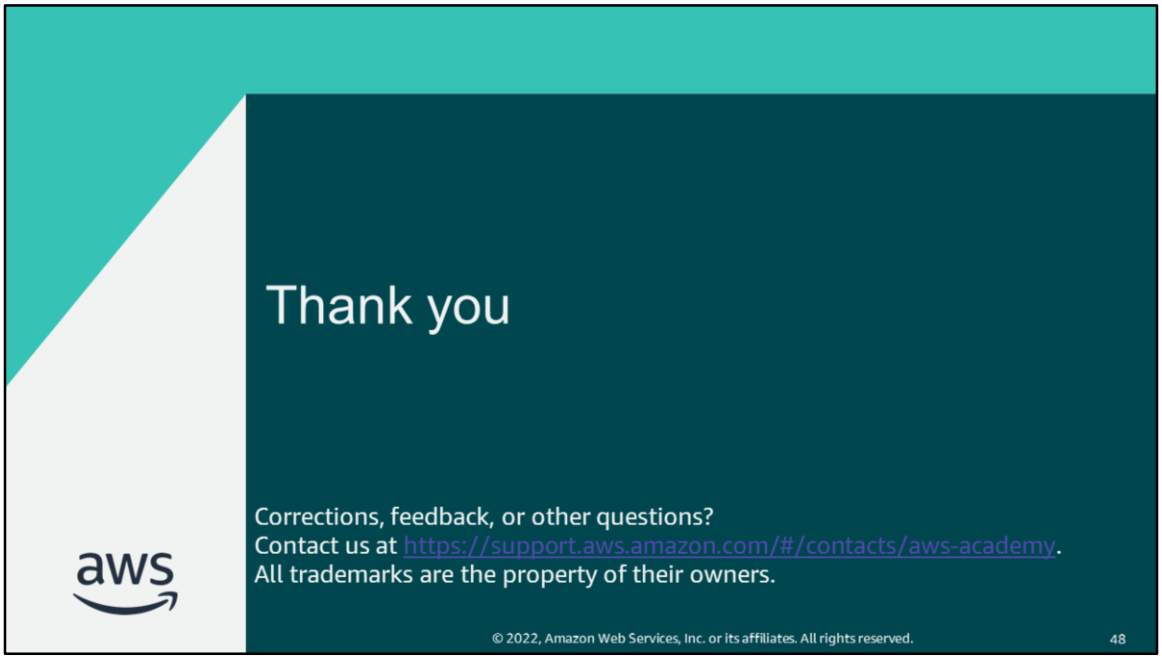


The correct answer is C. CloudTrail can provide a record of actions taken within your environment. CloudTrail logs include information such as the action type, identity of user, and time and date of the action.

Answer A is incorrect. CloudWatch can alert you that an anomalous action has taken place, but it does not tell you the identity of the user who took the action.

Answer B is incorrect. AWS Config can give you a record of configurations, but it cannot tell you the identity of the user who made a change.

Answer D is incorrect. Trusted Advisor can help you to assess the security posture of your AWS environment but does not alert on anomalous behavior.



Thank you for completing this module.