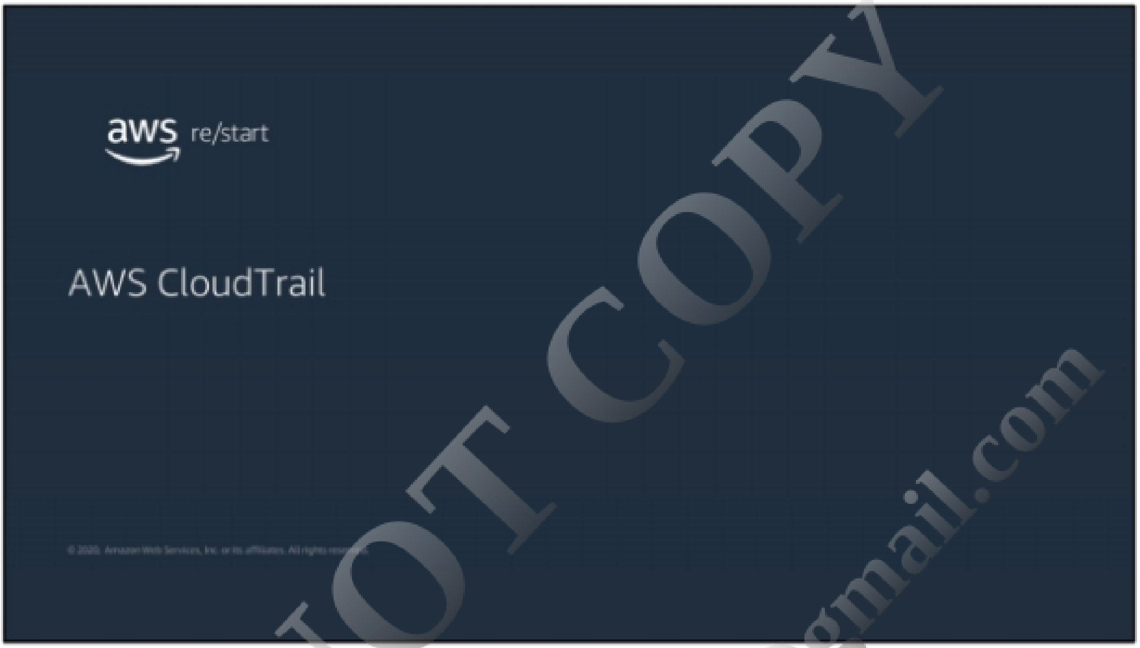
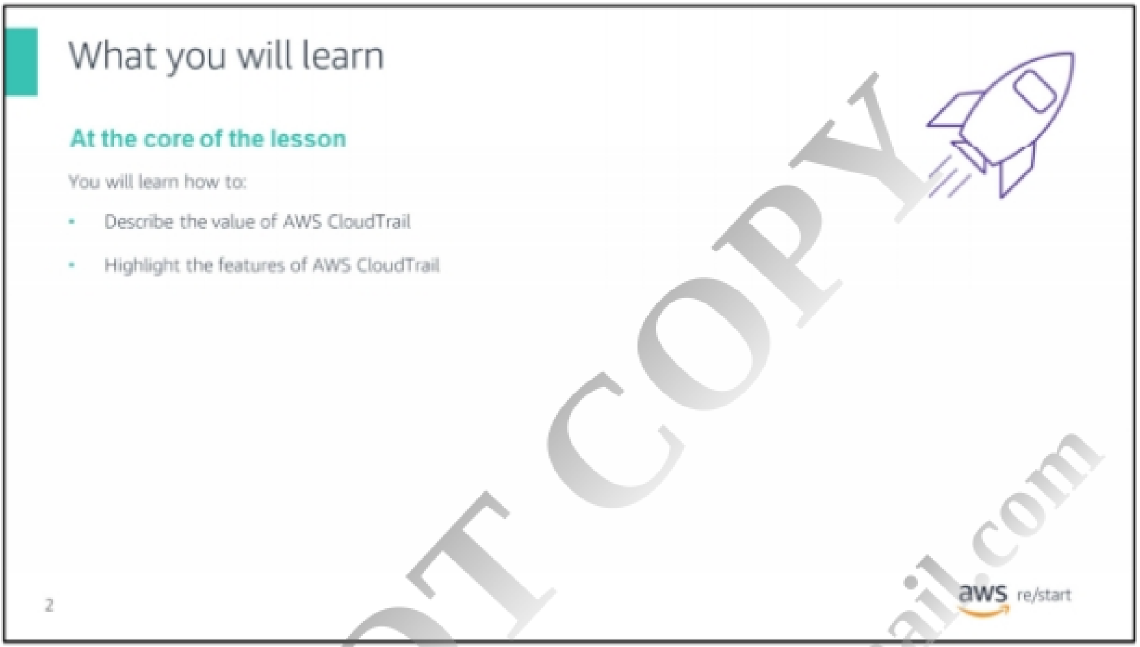


aws re/start

AWS CloudTrail

Welcome to AWS CloudTrail.



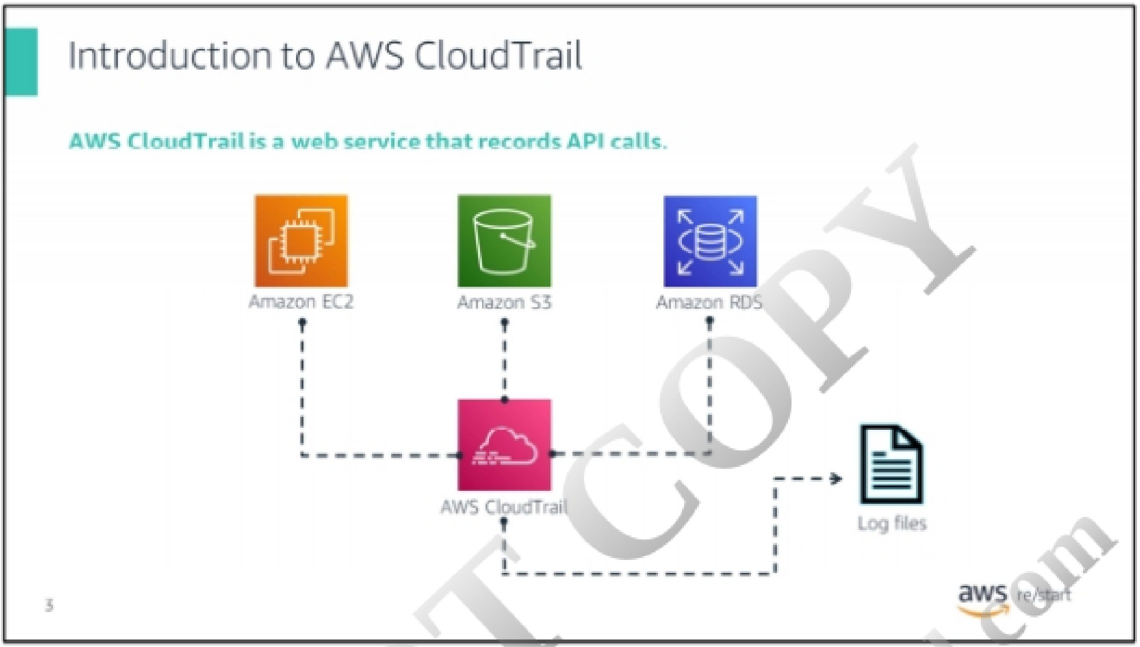
What you will learn

At the core of the lesson

You will learn how to:

- Describe the value of AWS CloudTrail
- Highlight the features of AWS CloudTrail

This module will describe AWS CloudTrail, which is a service that helps you monitor requests to the AWS services that you use.



Introduction to AWS CloudTrail

AWS CloudTrail is a web service that records API calls.

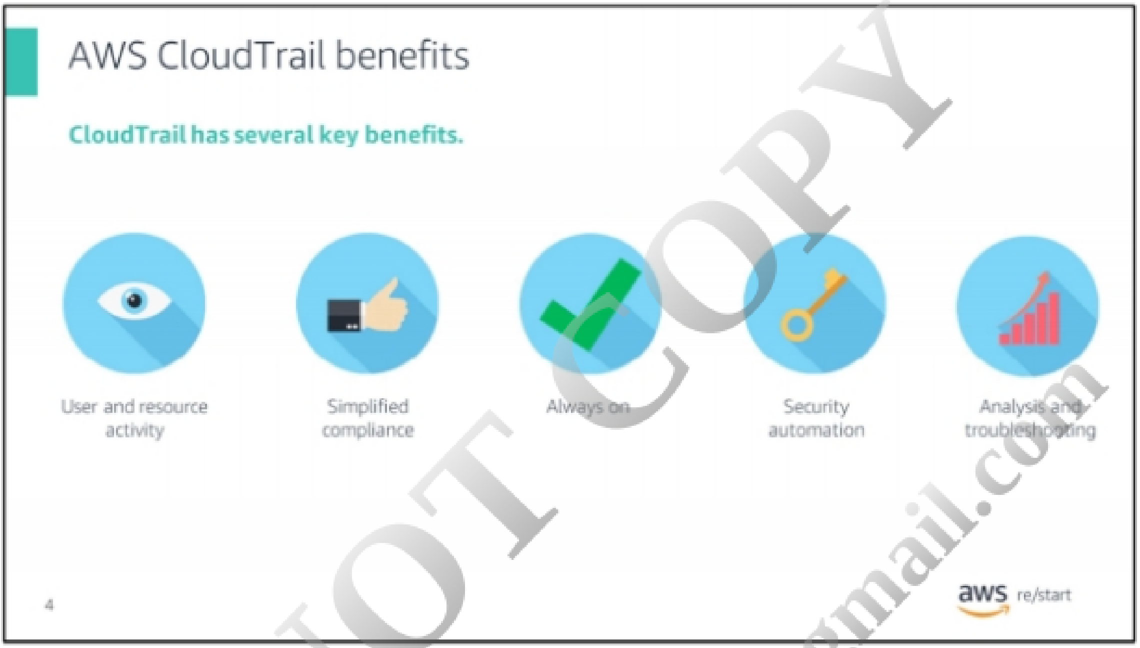
AWS CloudTrail is a web service that records AWS application programming interface (API) calls for your account and delivers log files to you.

CloudTrail is a crucial tool for simplifying governance, compliance, and risk auditing. Everything in AWS is an API call. CloudTrail logs the API calls that are made in an AWS account across AWS Regions. It does so whether that action was performed using the AWS Command Line Interface (AWS CLI), a software development kit (SDK), the console, or directly through an API.

The service logs include actions such as:

- Starting and stopping instances
- Creating or modifying Amazon Relational Database Service (Amazon RDS) databases
- Uploading a file to Amazon Simple Storage Service (Amazon S3)

This logging accelerates analysis of operational and security issues by providing visibility into actions in your AWS account.



AWS CloudTrail benefits

CloudTrail has several key benefits.

User and resource activity

Simplified compliance

Always on

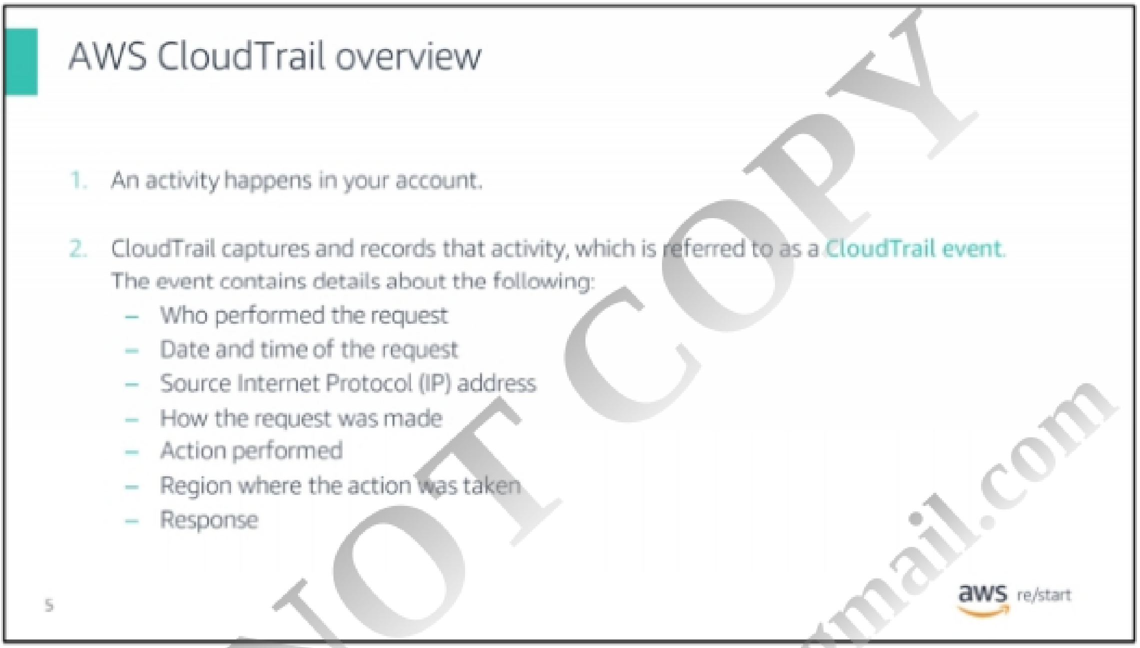
Security automation

Analysis and troubleshooting

aws re/start

CloudTrail has several key benefits:

- It increases your visibility into user and resource activity. With this visibility, you can identify who did what and when in your AWS account.
- Compliance audits are simplified because activities are automatically recorded and stored in event logs. The logging of activities enables you to search through log data, identify actions that are noncompliant, accelerate investigations into incidents, and then expedite a response.
- Because you are able to capture a comprehensive history of changes that are made in your account, you can analyze and troubleshoot operational issues in your account.



AWS CloudTrail overview

1. An activity happens in your account.

2. CloudTrail captures and records that activity, which is referred to as a CloudTrail event.
   The event contains details about the following:
   - Who performed the request
   - Date and time of the request
   - Source Internet Protocol (IP) address
   - How the request was made
   - Action performed
   - Region where the action was taken
   - Response

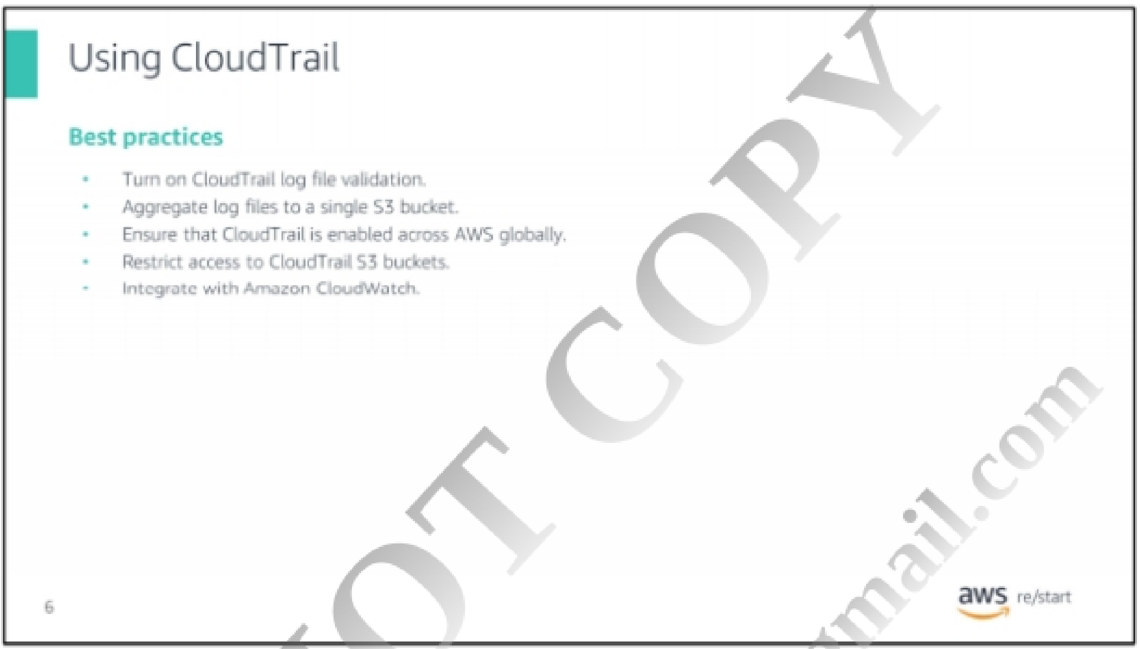
5

How does CloudTrail work?

1. An activity happens in your account.

2. CloudTrail captures and records that activity, which is referred to as a **CloudTrail event**. The event contain details about the following:
   - Who performed the request
   - Date and time of the request
   - Source Internet Protocol (IP) address
   - How the request was made
   - Action performed
   - Region where the action was taken
   - Response

By default, the logs are stored for 7 days. You can send the activity log to other AWS services. Therefore, you can retain the activity history for as long as you want.



Using CloudTrail

Best practices

- Turn on CloudTrail log file validation.
- Aggregate log files to a single S3 bucket.
- Ensure that CloudTrail is enabled across AWS globally.
- Restrict access to CloudTrail S3 buckets.
- Integrate with Amazon CloudWatch.

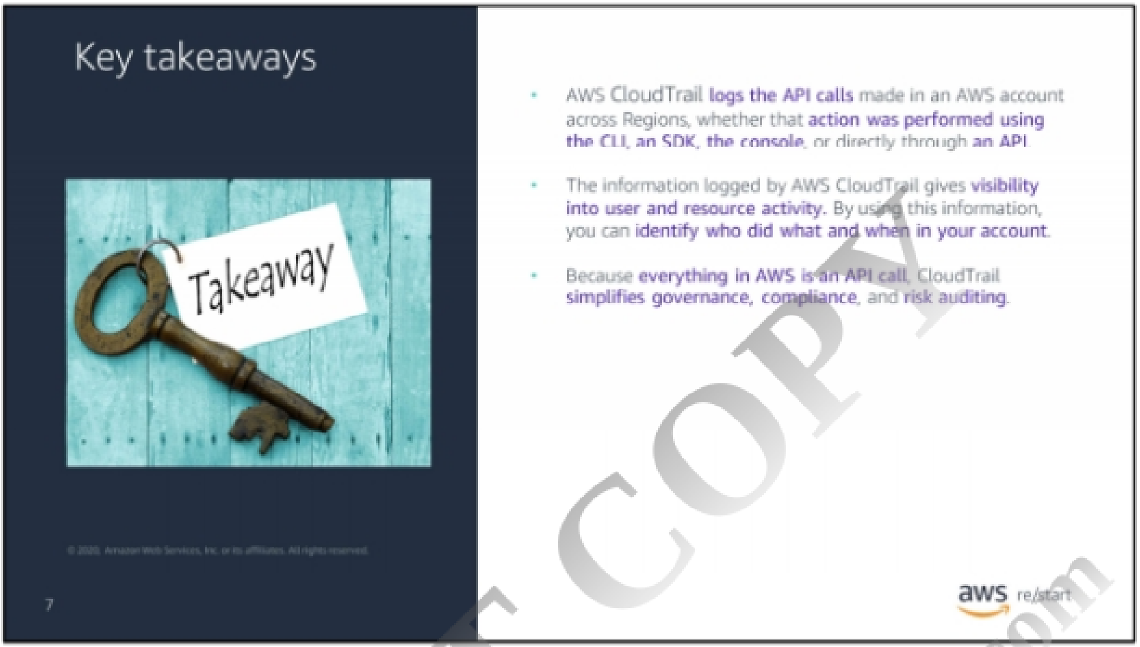
aws re/start

To get the most out of CloudTrail, turn on CloudTrail log file validations. When you configure CloudTrail, you can aggregate all log files to a single S3 bucket.

Additionally, a configuration that applies to all Regions means that your settings are applied consistently across all existing and newly launched Regions.

You can also validate the integrity of log files by detecting whether they were changed or deleted after they were sent to the S3 bucket. It is also good practice to run multi-factor authentication (MFA) to delete a CloudTrail bucket. This can be accomplished by restricting access to where they are stored.

Integrating CloudTrail with Amazon CloudWatch enables you to define actions to run when CloudTrail logs specific events. CloudWatch is a monitoring service for AWS Cloud resources. You can use the service to collect and track metrics, collect and monitor log files, set alarms, and automatically react to AWS resource changes. Integrating CloudTrail with CloudWatch also provides a comprehensive, secure, and searchable event history of activities. These activities can originate from the console, AWS SDKs, command line tools, and other AWS services.



Key takeaways

- AWS CloudTrail **logs the API calls** made in an AWS account across Regions, whether that **action was performed using the CLI, an SDK, the console**, or directly through **an API**.
- The information logged by AWS CloudTrail gives **visibility into user and resource activity**. By using this information, you can **identify who did what and when in your account**.
- Because **everything in AWS is an API call**, CloudTrail **simplifies governance, compliance**, and **risk auditing**.

aws re/start

Key takeaways from this lesson include:

- AWS CloudTrail logs the API calls made in an AWS account across Regions, whether that action was performed using the CLI, an SDK, the console, or directly through an API.
- The information logged by AWS CloudTrail gives visibility into user and resource activity. By using this information, you can identify who did what and when in your account.
- Because everything in AWS is an API call, CloudTrail simplifies governance, compliance, and risk auditing.