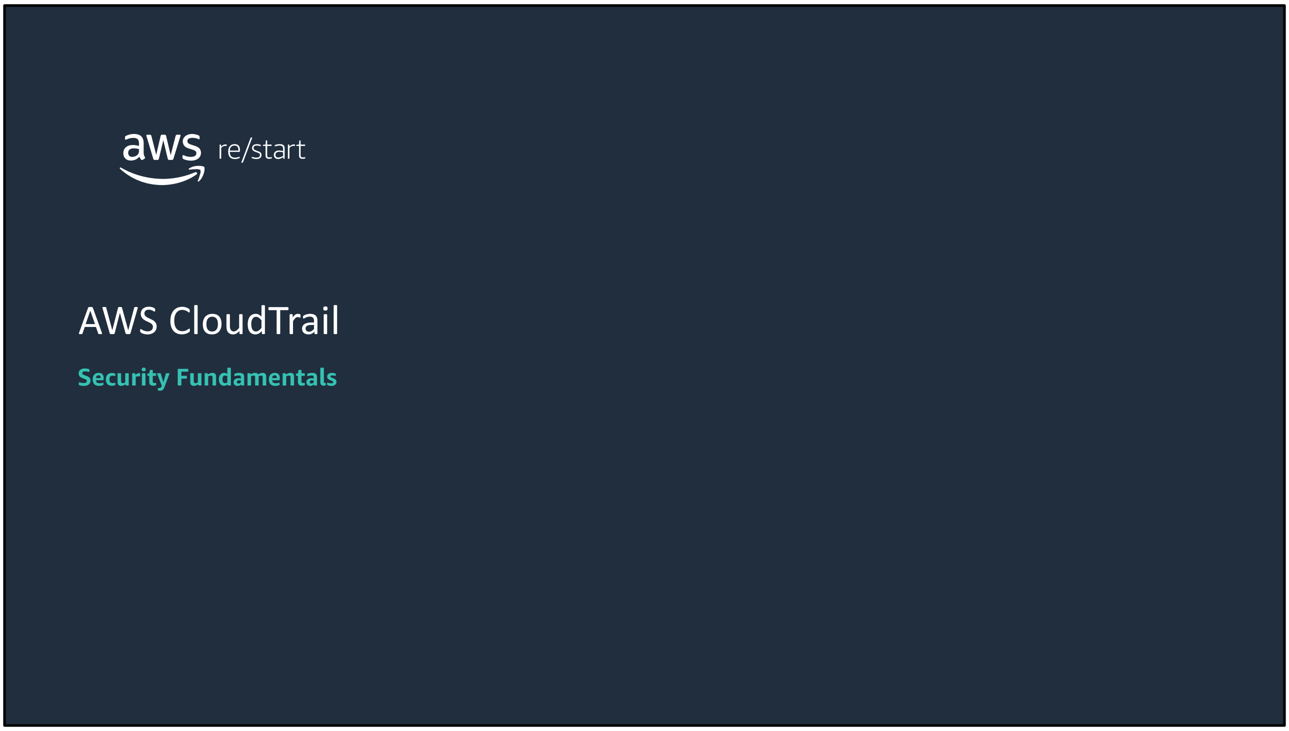
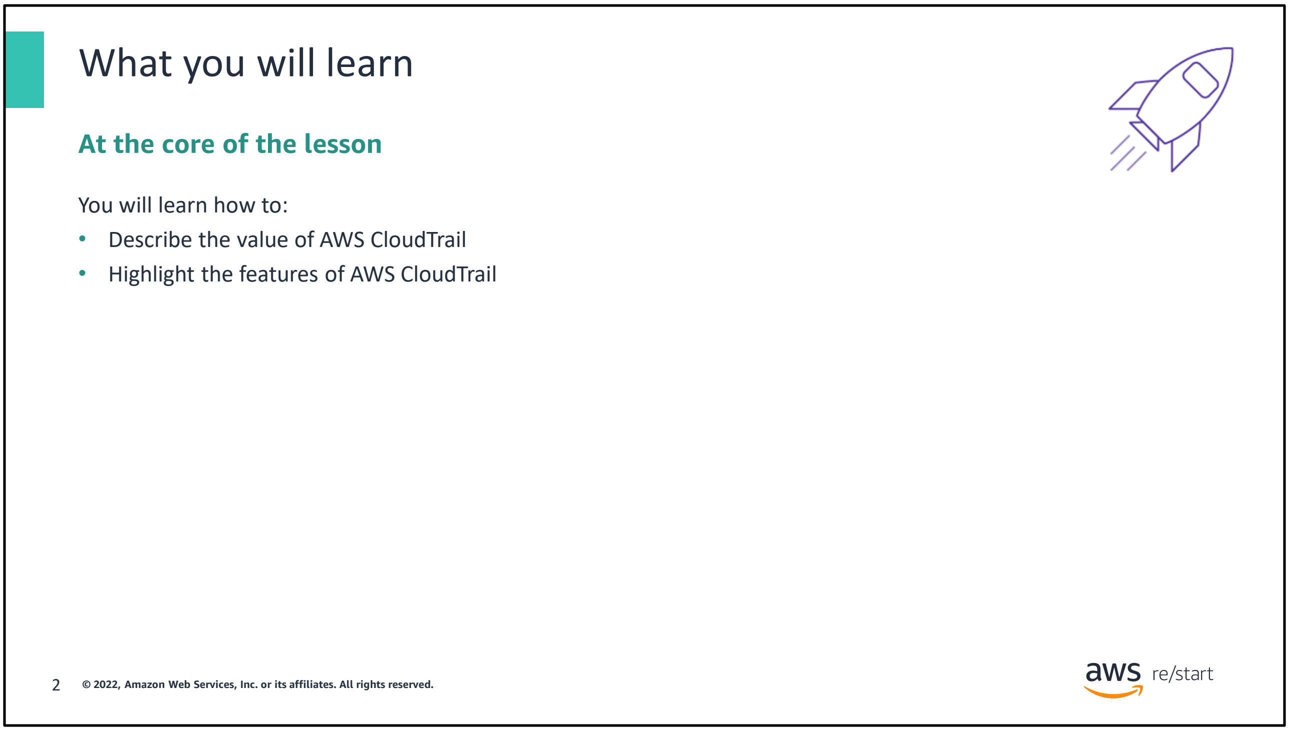


aws re/start

AWS CloudTrail

Security Fundamentals

Welcome to AWS CloudTrail.



What you will learn

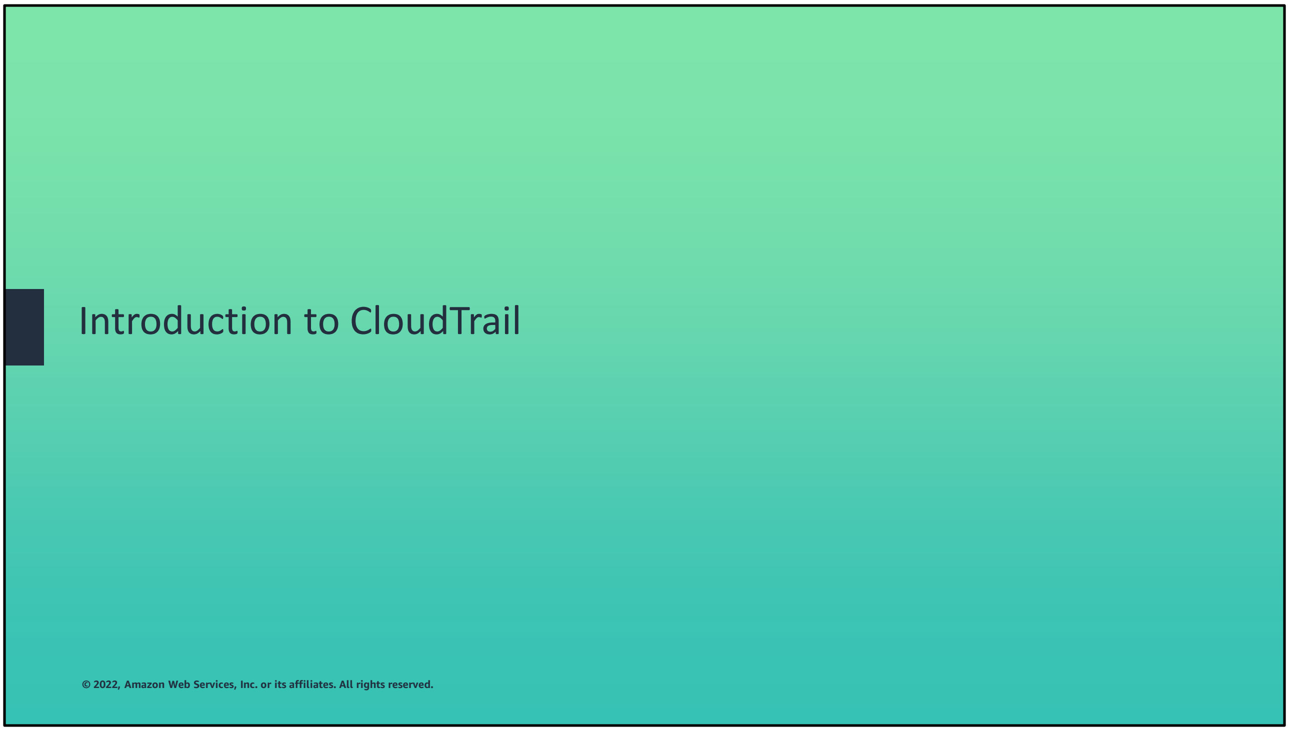
At the core of the lesson

You will learn how to:

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

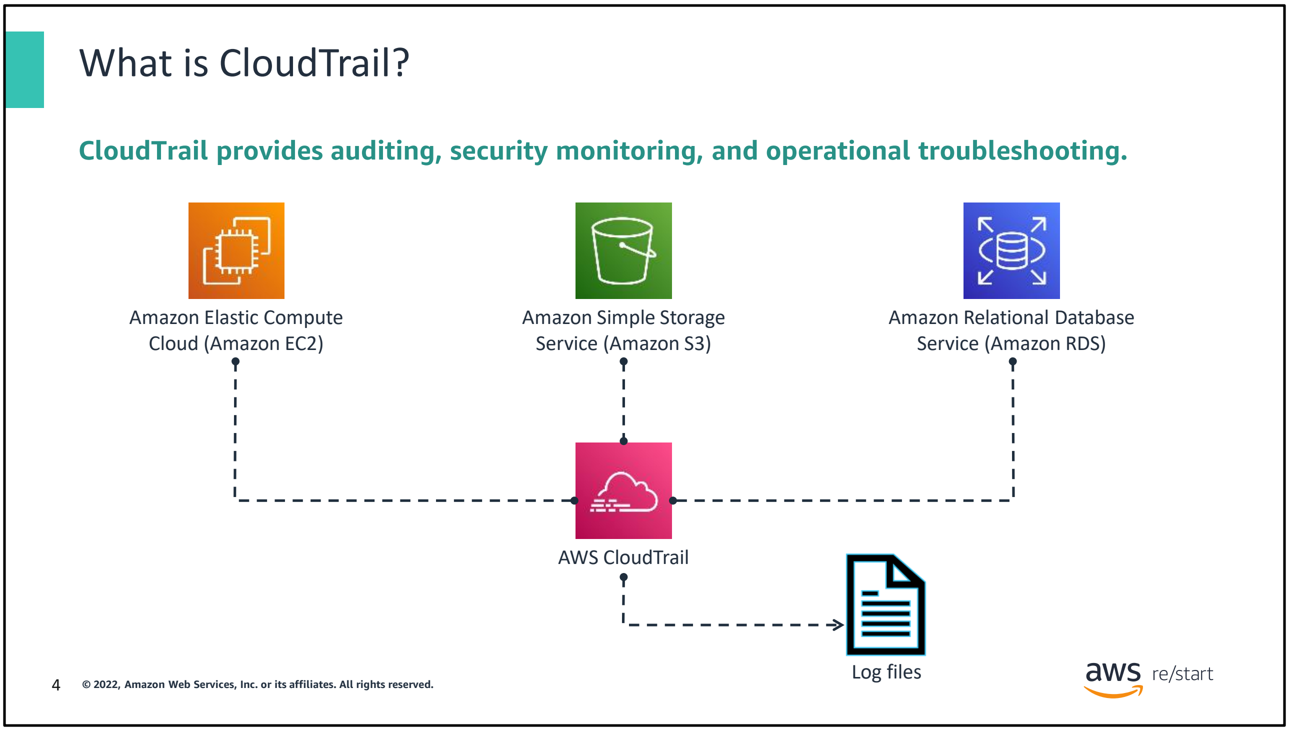
aws re/start

This module will describe AWS CloudTrail, a service that helps you monitor requests to the Amazon Web Services (AWS) services that you use.



Introduction to CloudTrail

You’ll begin with an overview of CloudTrail.



What is CloudTrail?

CloudTrail provides auditing, security monitoring, and operational troubleshooting.

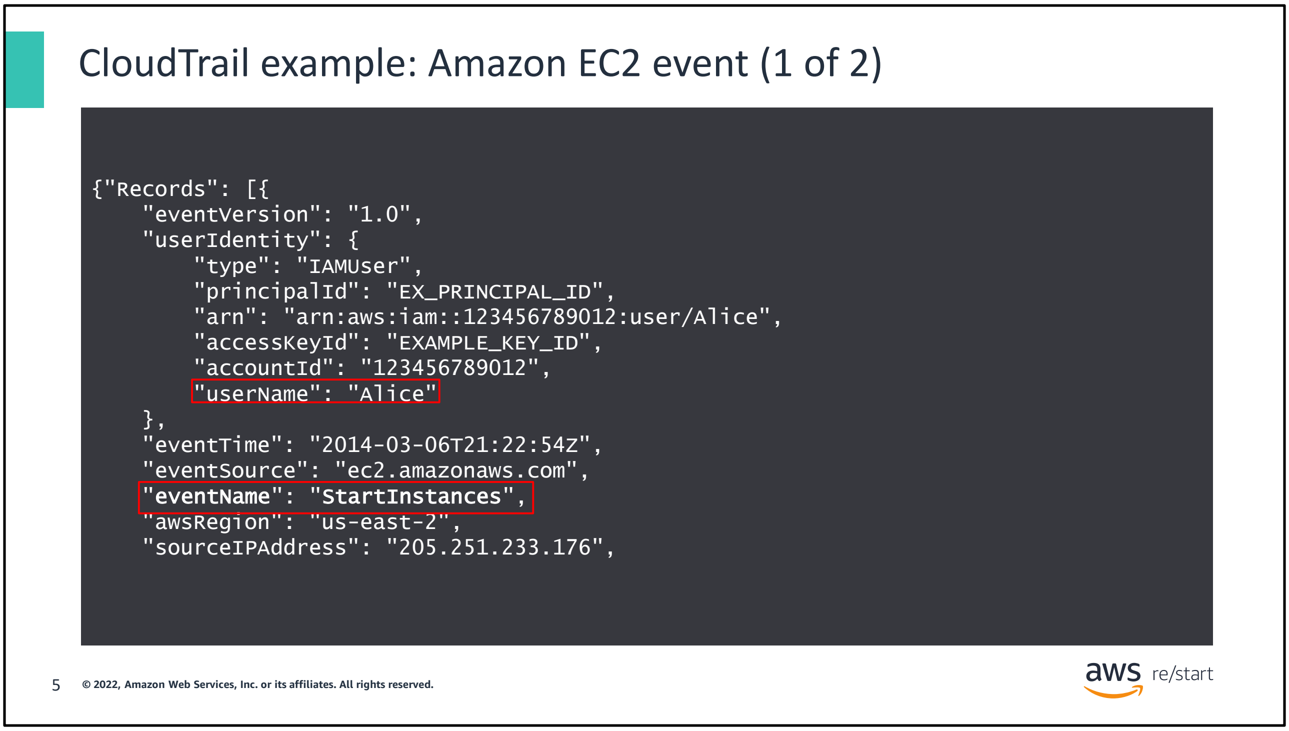
Amazon Elastic Compute Cloud (Amazon EC2)
Amazon Simple Storage Service (Amazon S3)
Amazon Relational Database Service (Amazon RDS)
AWS CloudTrail
Log files
aws re/start

By definition, CloudTrail is an auditing, compliance monitoring, and governance tool from AWS. It is classified as a Management and Governance tool in the AWS Management Console.

CloudTrail logs, continuously monitors, and retains account activity related to actions across your AWS infrastructure, which gives you control over storage, analysis, and remediation actions.

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 contains details about the following:
    - Who performed the request
    - When the event occurred (that is, the date and time of the request)
    - What the source Internet Protocol (IP) address was
    - How the request was made
    - Which actions were performed
    - Where the action occurred (that is, in which Region)
    - What the response was

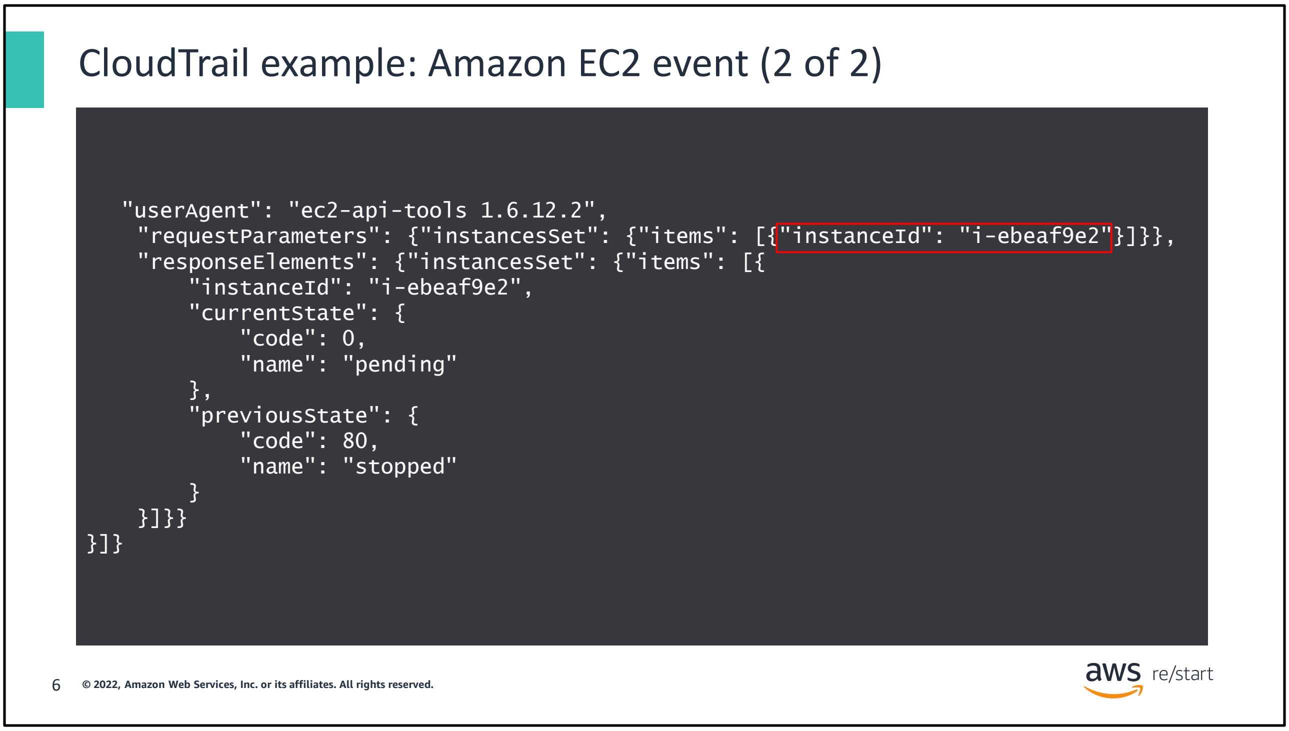


CloudTrail example: Amazon EC2 event (1 of 2)

```
{"Records": [{
    "eventVersion": "1.0",
    "userIdentity": {
        "type": "IAMUser",
        "principalId": "EX_PRINCIPAL_ID",
        "arn": "arn:aws:iam::123456789012:user/Alice",
        "accessKeyId": "EXAMPLE_KEY_ID",
        "accountId": "123456789012",
        "userName": "Alice"
    },
    "eventTime": "2014-03-06T21:22:54Z",
    "eventSource": "ec2.amazonaws.com",
    "eventName": "StartInstances",
    "awsRegion": "us-east-2",
    "sourceIPAddress": "205.251.233.176",
```

The log file contains one or more records. This slide includes an example of a CloudTrail log entry that shows the records for an action that started an EC2 instance.

The example shows that an AWS Identity and Access Management (IAM) user named Alice used the AWS Command Line Interface (AWS CLI). Alice used the AWS CLI to call the Amazon EC2 *StartInstances* action to start the instance with an instanceID of *i-ebeaf9e2*.



CloudTrail example: Amazon EC2 event (2 of 2)

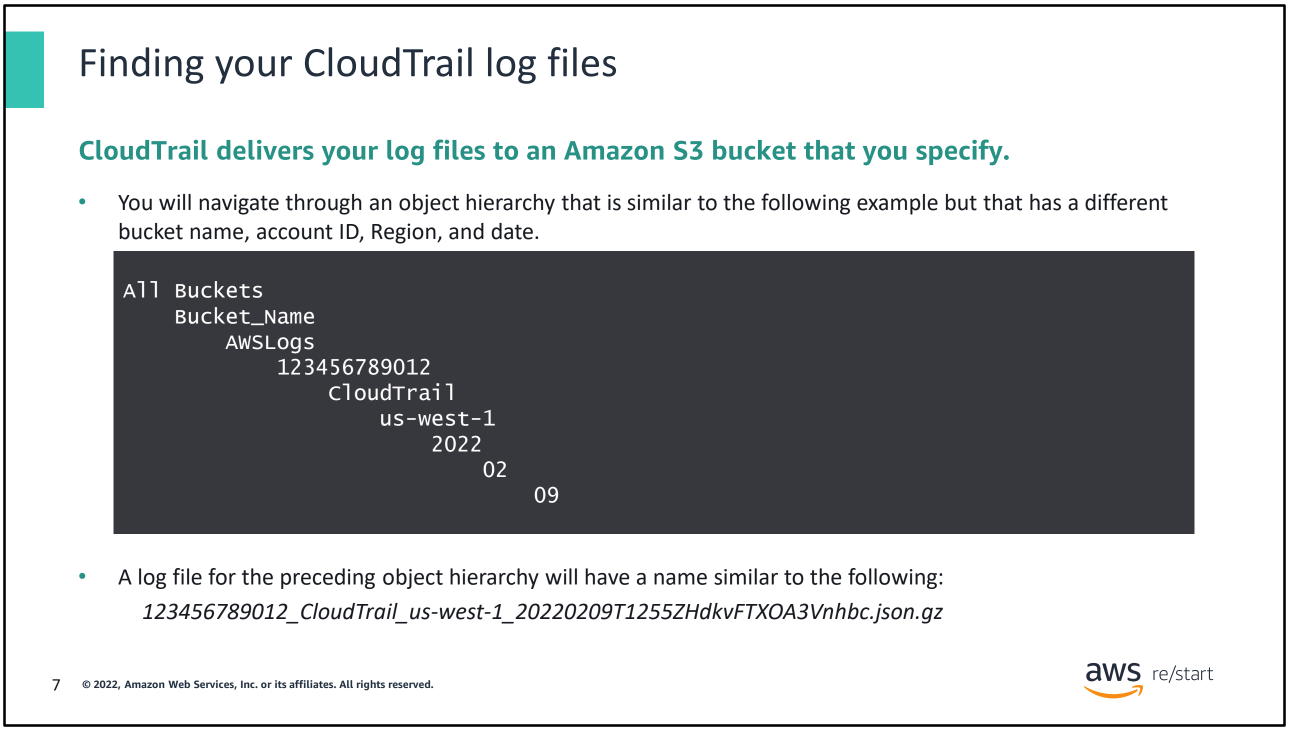
```
   "userAgent": "ec2-api-tools 1.6.12.2",
    "requestParameters": {"instancesSet": {"items": [{"instanceId": "i-ebeaf9e2"}]}},
    "responseElements": {"instancesSet": {"items": [{
        "instanceId": "i-ebeaf9e2",
        "currentState": {
            "code": 0,
            "name": "pending"
        },
        "previousState": {
            "code": 80,
            "name": "stopped"
        }
    }]}}
}]}
```

6

aws re/start

The log file contains one or more records. This slide includes an example of a CloudTrail log entry that shows the records for an action that started an EC2 instance.

The example shows that an AWS Identity and Access Management (IAM) user named Alice used the AWS Command Line Interface (AWS CLI). Alice used the AWS CLI to call the Amazon EC2 *StartInstances* action to start the instance with an instanceID of *i-ebeaf9e2*.



Finding your CloudTrail log files

CloudTrail delivers your log files to an Amazon S3 bucket that you specify.

- You will navigate through an object hierarchy that is similar to the following example but that has a different bucket name, account ID, Region, and date.

```
All Buckets
    Bucket_Name
        AWSLogs
            123456789012
                CloudTrail
                    us-west-1
                        2022
                            02
                                09
```

- A log file for the preceding object hierarchy will have a name similar to the following:
  123456789012_CloudTrail_us-west-1_20220209T1255ZHdkvFTXOA3Vnhbc.json.gz

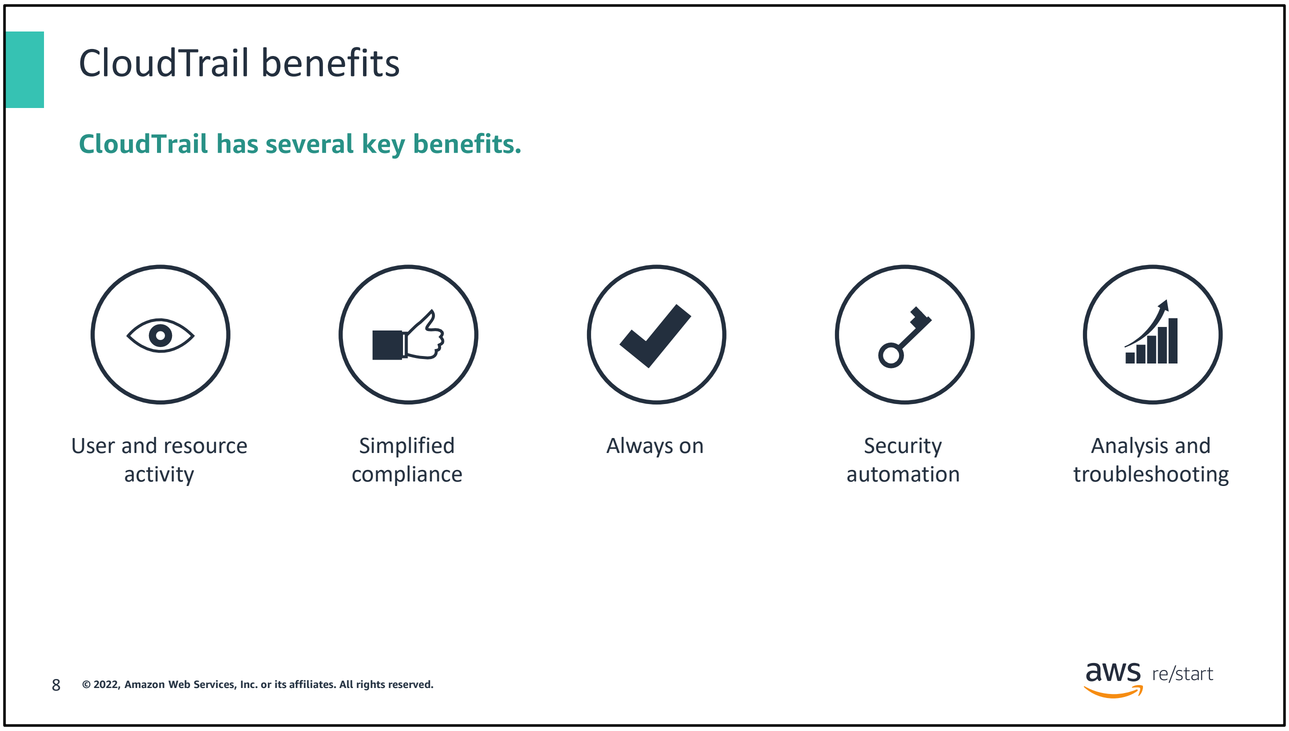
7

Follow these steps to find your log files:

1. Open the Amazon S3 console.
2. Choose the bucket that you specified when you created the trail.
3. Navigate through the object hierarchy until you find the log file that you want.

All log files are stored as compressed files with a .gz extension.

CloudTrail typically delivers logs within an average of about 15 minutes of an event.



CloudTrail benefits

CloudTrail has several key benefits.

User and resource activity

Simplified compliance

Always on

Security automation

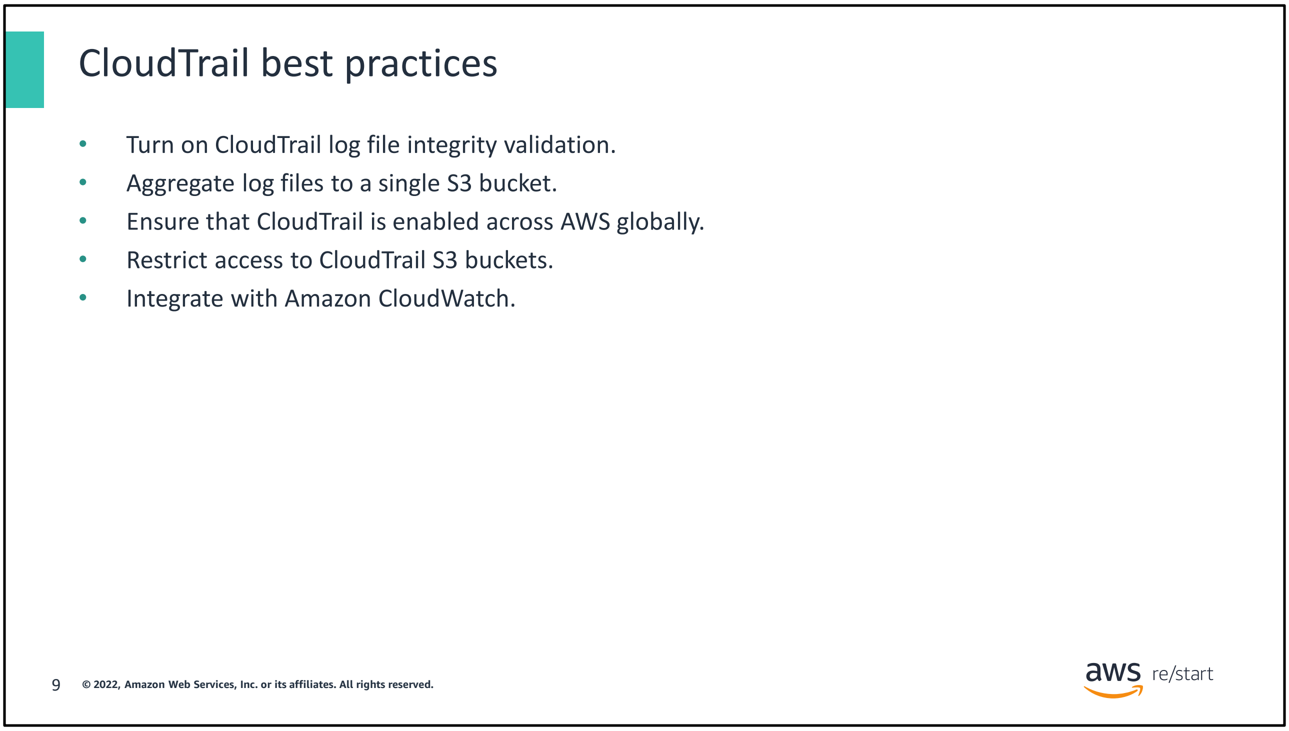
Analysis and troubleshooting

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. Because CloudTrail logs activities, you can 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.
- CloudTrail helps discover changes made to an AWS account that have the potential of putting the data or the account at heightened security risk. At the same time, it expedites AWS audit request fulfillment. This action helps to simplify auditing requirements, troubleshooting, and compliance.

The body of the CloudTrail record contains fields that help you determine the requested action and also when and where the request was made. For example, by using the field awsRegion, you can keep a close watch if adverse behavior occurs in a Region that you don't normally use. You can create alerts for your common Regions and alerts for anything that is happening outside your primary Region. Be sure to enable CloudTrail in all of your Regions.



CloudTrail best practices

- Turn on CloudTrail log file integrity 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.

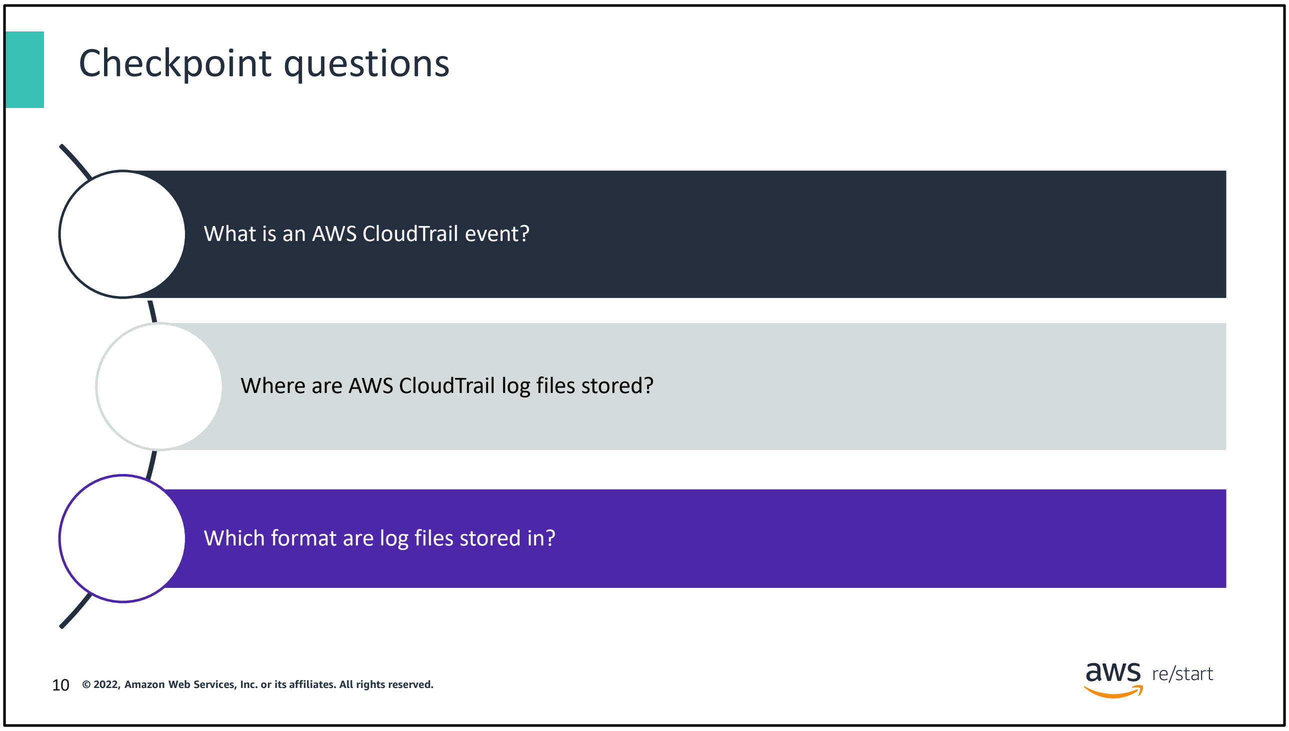
To harden your security and auditing processes, turn on CloudTrail log file integrity validation. This feature helps you to determine whether a CloudTrail log file was unchanged, deleted, or modified since CloudTrail delivered it to the specified S3 bucket.

When you configure CloudTrail, you can aggregate all log files to a single S3 bucket. By aggregating all files to a single bucket, you can store the files in a single location and define permissions to protect their access. It is also good practice to run multi-factor authentication (MFA) to delete a CloudTrail 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 integrate CloudTrail with Amazon CloudWatch 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 Software Development Kits (SDKs), command line tools, and other AWS services.

Ensure that CloudTrail is enabled for all AWS Regions to increase the visibility into the activities in your AWS account for security and management purposes.



Checkpoint questions

What is an AWS CloudTrail event?

Where are AWS CloudTrail log files stored?

Which format are log files stored in?

1. Q1: What is an AWS CloudTrail event?

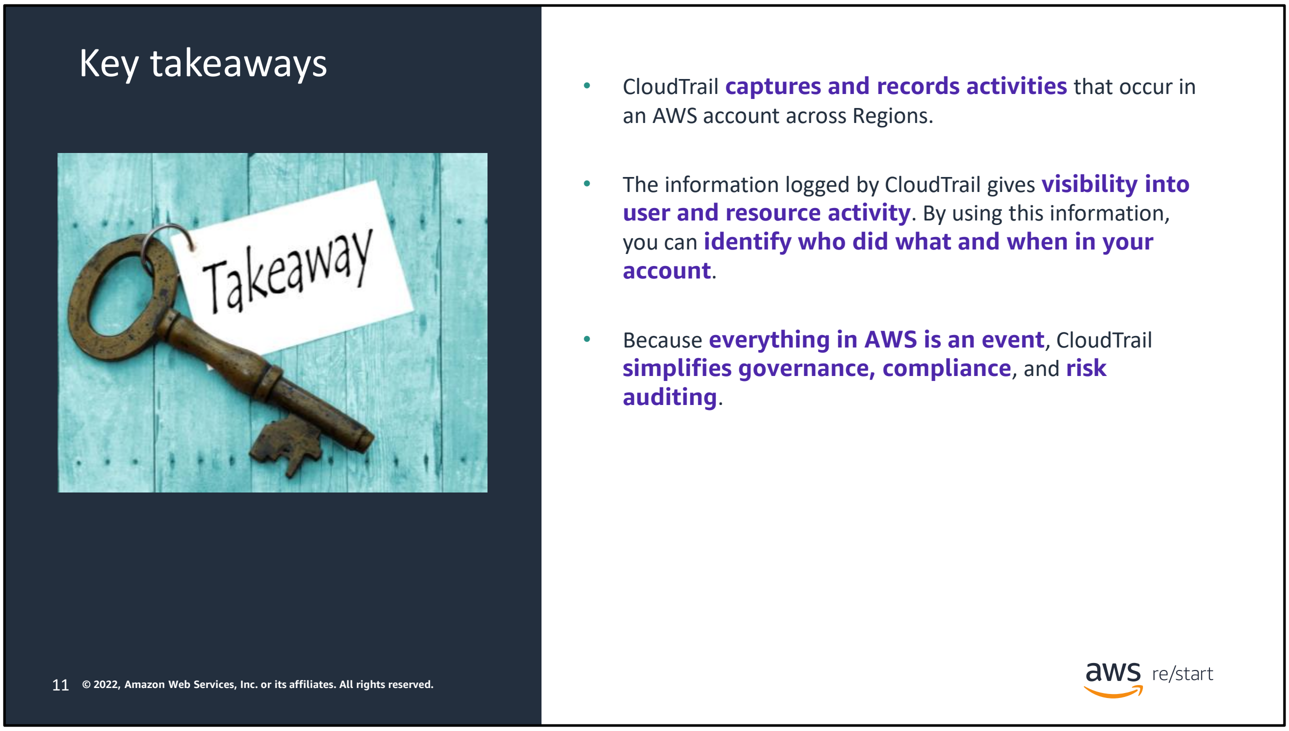
   An AWS CloudTrail event is an activity that occurs in an AWS account. Technically, events are triggered by application programming interface (API) calls that are made to services and resources in an AWS account.

2. Q2: Where are AWS CloudTrail log files stored?

   AWS CloudTrail log files are stored in Amazon S3.

3. Q3: Which format are log files stored in?

   Log files are stored in a compressed format with a .gz extension.



Key takeaways

- CloudTrail **captures and records activities** that occur in an AWS account across Regions.
- The information logged by 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 event**, CloudTrail **simplifies governance, compliance**, and **risk auditing**.

This lesson includes the following key takeaways:

- CloudTrail captures and records activities in an AWS account across Regions.
- The information logged by 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 event, CloudTrail simplifies governance, compliance, and risk auditing.

Thank you

aws re/start

Thank you for completing this module.