

Professional Skills
Agile Fundamentals
Jira
Git
Databases Introduction
Java Beginner
Maven
Testing (Foundation)
Java Intermediate
HTML
CSS
Javascript
Spring Boot
Selenium
Sonarqube
Advanced Testing (Theory)
Cucumber
MongoDB
Express
NodeJS
React
Express-Testing
Networking
Security
Cloud Fundamentals
AWS Foundations
AWS Intermediate
<div><div></div>Virtual Private Cloud (VPC)</div>
<div><div></div>EC2 VPC Security Groups</div>
<div><div></div>EC2 VPC Subnets</div>

# CloudTrail

## Contents

- [Overview](#)
- [Tutorial](#)
- [Exercises](#)

## Overview

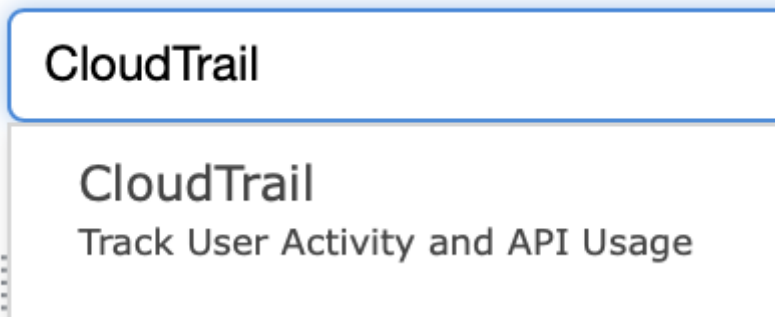
Amazon **CloudTrail** is an AWS service that helps you enable governance, compliance, and operational and risk auditing of your AWS account. Actions taken by a user, role, or an AWS service are recorded as events in CloudTrail. Events include actions taken in the AWS Management Console, AWS Command Line Interface, and AWS SDKs and APIs.

CloudTrail is enabled on your AWS account when you create it. When activity occurs in your AWS account, that activity is recorded in a CloudTrail event. You can easily view recent events in the CloudTrail console by going to Event history.

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

## Tutorial

- Navigate to the AWS Console and sign in [here](#)
- Search for CloudTrail under the services dropdown menu, and click on CloudTrail



- You will be shown the CloudTrail overview, and you should see logs of the root user and their activity.  
This will be your activity if you are logging into your AWS account as the root user.  
By clicking on the activity, it will expand and you will be able to see more details on that specific activity.
- On the left navigation pane click on **Event history**.  
This will show all events that took place, showing the most recent ones at the top.  
Again, by expanding the event, you will be able to see more details on this.
- On the left navigation pane, click on **Trails** and then **Create trail**.

**Note:** You will be charged for using AWS **CloudTrail**

- You will be prompted to configure your CloudTrail.  
In this case, leave everything as it's default value and only provide the **Trail**

<div><div></div><div>EC2 VPC Internet Gateways</div></div> <div><div></div><div>AWS Route Tables</div></div> <div><div></div><div>AWS Network Address Translation (NAT) Gateway</div></div> <div><div></div><div>AWS Network Access Control Lists (NACLs) CLI</div></div> <div><div></div><div>AWS Java SDK</div></div> <div><div></div><div>AWS DynamoDB</div></div> <div><div></div><div>AWS Lambda Functions</div></div> <div><div></div><div>AWS API Gateway</div></div> <div><div></div><div>SQS Introduction</div></div> <div><div></div><div>AWS Serverless CRUD Solution</div></div> <div><div></div><div>AWS Serverless Solution with DynamoDB</div></div> <div><div></div><div>CloudWatch CLI</div></div> <div><div></div><div>CloudTrail</div></div>
Linux
DevOps
Jenkins Introduction
Jenkins Pipeline
Markdown
IDE Cheatsheet

Name and S3 Bucket:

- Trail Name: Example-Management-Tail-Log
- S3 Bucket: example-management-trail-log-bucket

Note: The S3 Bucket name must be unique to the world. Similar to a DNS.

7. You can now navigate to your S3 bucket, and go onto the bucket which you created to store your logs.

This log will follow a pattern where it will be under AWSLogs -> Unique User ID -> CloudTrail -> Regions -> Year -> Month -> Date.

These will contain .json.gz files which can be downloaded and viewed to see all events that took place that specific date.

8. Delete the Trail that you created.

## Exercises

Since all activities are being logged, try to integrate CloudWatch to look at the logs and raise any alarms.