AWS CloudTrail 을 시작하겠습니다.

교육 내용

이 강의의 핵심

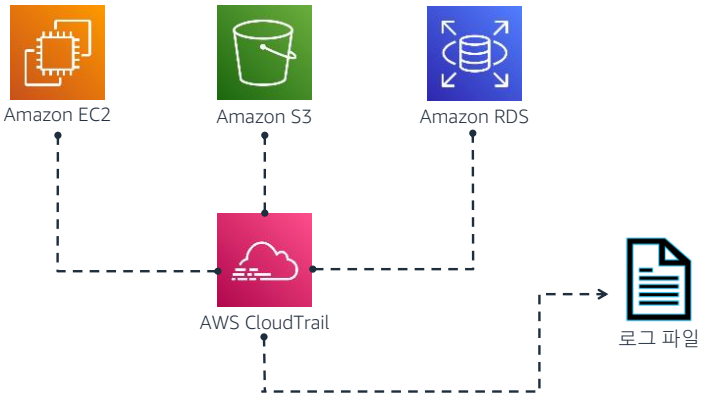
배울 내용은 다음과 같습니다.

- AWS CloudTrail의 가치를 설명합니다.
- AWS CloudTrail의 기능을 알아봅니다.

이 모듈에서는 여러분이 사용하는 AWS 서비스에 대한 요청을 모니터링하는 데 도움이 되는 서비스인 AWS CloudTrail을 설명합니다.

AWS CloudTrail 소개

AWS CloudTrail은 API 호출을 기록하는 웹 서비스입니다.



3

aws re/start

AWS CloudTrail은 여러분의 계정에 대한 AWS 애플리케이션 프로그래밍 인터페이스(API) 호출을 기록하고 로그 파일을 여러분에게 전달하는 웹 서비스입니다.

CloudTrail은 거버넌스, 규정 준수 및 위험 감사를 간소화하는 데 중요한 도구입니다. AWS에서 일어나는 모든 일은 API 호출입니다. CloudTrail은 AWS 리전 전체를 통틀어 AWS 계정에서 발생한 API 호출을 로깅합니다. 그 액션이 AWS Command Line Interface(AWS CLI)나 소프트웨어 개발 키트(SDK), 콘솔을 사용해서 수행되었는지, 아니면 API를 통해 직접 수행되었는지와는 상관없이 로깅합니다.

CloudTrail 서비스는 다음과 같은 액션을 로깅합니다.

- 인스턴스 시작 및 중지
- Amazon Relational Database Service(Amazon RDS) 데이터베이스 생성 또는 수정
- Amazon Simple Storage Service(Amazon S3)에 파일 업로드

이 로깅은 AWS 계정 내 활동에 대한 가시성을 제공함으로써 운영 및 보안 문제에 대한 분석을 가속화합니다.

CloudTrail에는 여러 가지 주요 이점이 있습니다.

- 사용자 및 리소스 활동에 대한 가시성을 높입니다. 이 가시성을 통해 여러분의 AWS 계정에서 누가, 무엇을, 언제 했는지 파악할 수 있습니다.
- 이벤트 로그에 활동이 자동으로 기록되고 저장되기 때문에 규정 준수 감사가 간편합니다. 활동 로깅을 통해 로그 데이터를 검색하고, 규정을 위반한 액션을 식별하며, 인시던트 조사를 가속화한 다음, 신속하게 대응할 수 있습니다.
- 계정 내에서 발생한 변경 사항에 대한 종합적인 기록을 캡처할 수 있으므로 계정의 운영 문제를 분석하고 문제를 해결할 수 있습니다.

AWS CloudTrail 개요

1. 계정에서 활동이 발생합니다.

2. CloudTrail이 이 활동을 캡처하여 기록하며, 이를 CloudTrail 이벤트라고 합니다.
   이벤트에는 다음 항목의 세부 정보가 포함됩니다.
   - 요청을 수행한 사용자
   - 요청의 날짜와 시간
   - 소스 인터넷 프로토콜(IP) 주소
   - 요청 방법
   - 수행한 액션
   - 액션을 수행한 리전
   - 대응

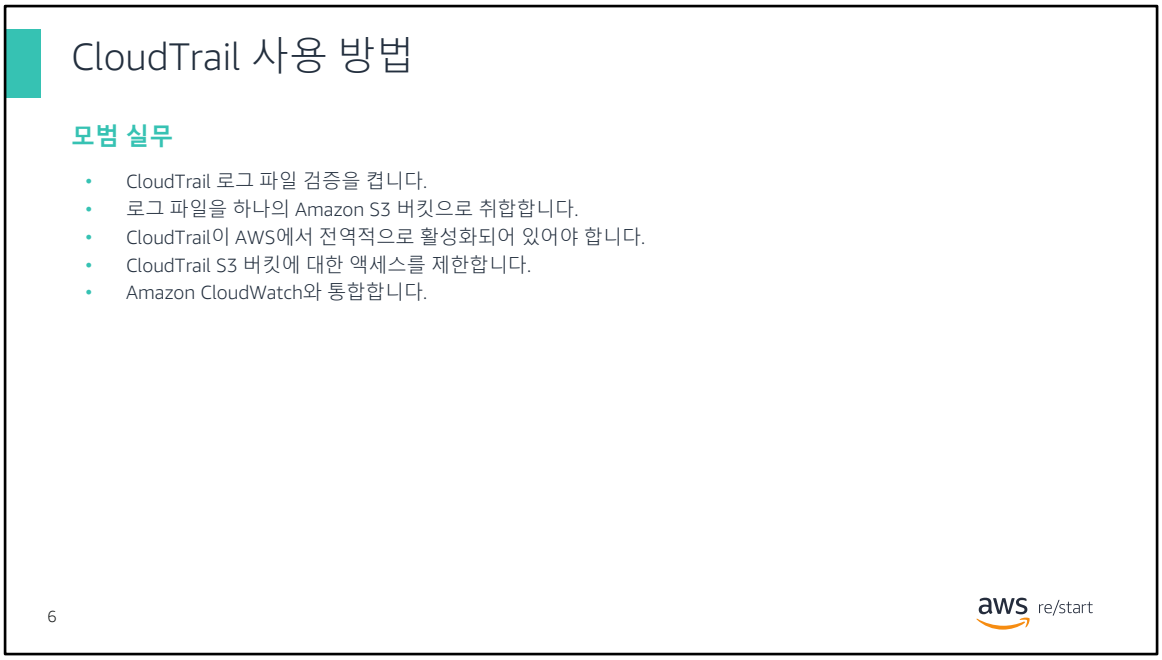
aws re/start

CloudTrail의 작동 방식입니다.

1. 계정에서 활동이 발생합니다.

2. CloudTrail이 이 활동을 캡처하여 기록하며, 이를 **CloudTrail 이벤트**라고 합니다. 이벤트에는 다음 항목의 세부 정보가 포함됩니다.
   - 요청을 수행한 사용자
   - 요청의 날짜와 시간
   - 소스 인터넷 프로토콜(IP) 주소
   - 요청 방법
   - 수행한 액션
   - 액션을 수행한 리전
   - 대응

기본적으로 로그는 7일간 저장됩니다. 활동 로그를 다른 AWS 서비스에 전송할 수 있으므로 원하는 기간 동안 활동 기록을 유지할 수 있습니다.



CloudTrail을 최대한 활용하려면 CloudTrail 로그 파일 검증을 켭니다. CloudTrail을 구성할 때 모든 로그 파일을 하나의 S3 버킷으로 취합할 수 있습니다.

또한 모든 리전에 적용되는 구성을 통해 설정이 모든 기존 및 새로 시작된 리전 전체에 일관되게 적용됩니다.

또한 로그 파일이 S3 버킷에 전송된 후 변경되었거나 삭제되었는지 탐지하여 로그 파일의 무결성을 확인할 수 있습니다. 다중 인증(MFA)을 실행하여 CloudTrail 버킷을 삭제하는 것도 좋습니다. 저장된 위치에 대한 액세스를 제한하면 됩니다.

CloudTrail을 Amazon CloudWatch와 통합하면 CloudTrail에서 특정 이벤트를 로깅할 때 수행할 액션을 정의할 수 있습니다. CloudWatch는 AWS 클라우드 리소스에 대한 모니터링 서비스입니다. CloudWatch 서비스를 사용하여 지표를 수집 및 추적하고, 로그 파일을 수집 및 모니터링하며, 경보를 설정하고, AWS 리소스 변경 사항에 자동으로 대응할 수 있습니다. 또한 CloudTrail을 CloudWatch와 통합하면 종합적이고 안전하며 검색 가능한 활동 이벤트 기록을 확보할 수 있습니다. 이 활동은 콘솔, AWS SDK, 명령줄 도구, 기타 AWS 서비스에서 발생한 것일 수 있습니다.

핵심 사항

- AWS CloudTrail은 **CLI, SDK, 콘솔을 사용하여 액션을 수행**했는지, **API**를 통해 직접 액션을 수행했는지와 상관없이 AWS 계정에서 리전 간에 수행된 **API 호출을 로깅**합니다.
- AWS CloudTrail에서 로깅한 정보는 **사용자와 리소스 활동에 대한 가시성**을 제공합니다. 이 정보를 사용하면 **여러분의 계정에서 누가, 무엇을, 언제 했는지 파악**할 수 있습니다.
- **AWS에서 일어나는 모든 일이 API 호출**이기 때문에 CloudTrail은 **거버넌스, 규정 준수, 위험 감사를 간소화**해 줍니다.

aws re/start

이 강의에서 다룬 핵심 사항은 다음과 같습니다.

- AWS CloudTrail은 CLI, SDK, 콘솔을 사용하여 액션을 수행했는지, API를 통해 직접 액션을 수행했는지와 상관없이 AWS 계정에서 리전 간에 수행된 API 호출을 로깅합니다.
- AWS CloudTrail에서 로깅한 정보는 사용자와 리소스 활동에 대한 가시성을 제공합니다. 이 정보를 사용하면 여러분의 계정에서 누가, 무엇을, 언제 했는지 파악할 수 있습니다.
- AWS에서 일어나는 모든 일이 API 호출이기 때문에 CloudTrail은 거버넌스, 규정 준수, 위험 감사를 간소화해 줍니다.