aws re/start

AWS CloudTrail

© 2020, Amazon Web Services, Inc. 또는 계열사. All rights reserved.

학습 내용

강의의 핵심

배울 내용은 다음과 같습니다.

- AWS CloudTrail의 목적 및 기능 설명하기

주제:

- AWS CloudTrail

주요 용어:

- 로그 항목
- requestParameters
- responseElements

aws re/start

AWS CloudTrail

AWS CloudTrail은 다음을 수행하는 서비스입니다.

- AWS 인프라 전반의 작업과 관련된 계정 활동을 기록, 지속적으로 모니터링 및 유지합니다.
- 대부분의 AWS 서비스에 대한 애플리케이션 프로그램 인터페이스(API) 호출을 기록합니다.
  - AWS Management Console 및 AWS Command Line Interface(AWS CLI) 활동도 기록됩니다.
- 늘어나는 AWS 서비스에 대해 지원됩니다.
- 구성된 후 Amazon Simple Storage Service(Amazon S3)에 로그를 자동으로 푸시합니다.
- Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스 내에서 이벤트를 추적하지 않습니다.
  - 예제: 인스턴스의 수동 종료

AWS CloudTrail

aws re/start

CloudTrail 예제

CloudTrail은 세부 분석을 필요로 하는 질문에 답하도록 도와줄 수 있습니다.

누가 특정 인스턴스를 종료했습니까?

누가 보안 그룹 구성을 변경했습니까?

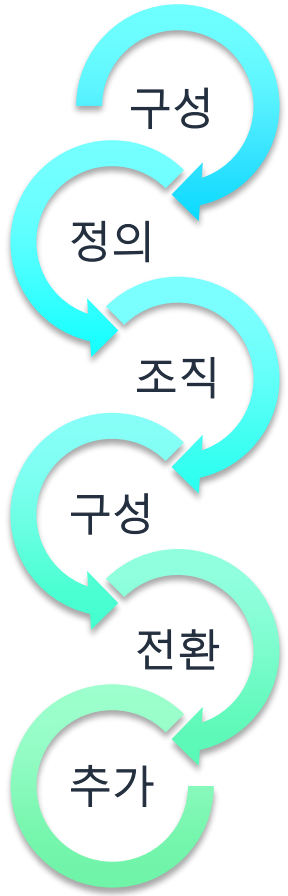
알 수 없는 IP 주소 범위에서 나온 작업이 있습니까?

권한 부족으로 인해 거부된 활동은 무엇입니까?

추적 구성

추적을 구성하는 단계는 다음과 같습니다.

1. 로그 파일을 업로드하기 위해 신규 또는 기존 Amazon Simple Storage Service(Amazon S3) 버킷을 구성합니다.
2. 원하는 이벤트를 기록할 추적을 정의합니다(모든 관리 이벤트는 기본적으로 기록됨).
3. 알림을 받을 Amazon Simple Notification Service(Amazon SNS) 주제를 생성합니다.
4. CloudTrail로부터 로그를 수신하도록 Amazon CloudWatch Logs를 구성합니다(선택 사항).
5. 로그 파일에 대해 로그 파일 암호화 및 무결성 검증을 켭니다(선택 사항).
6. 추적에 태그를 추가합니다(선택 사항).



aws re/start

CloudTrail 로그 항목: requestParameters

이 예제는 로그 항목의 requestParameters 섹션을 보여줍니다. 여기에는 다음과 같은 파라미터가 포함됩니다.

- userIdentity – 조치를 취한 사람(또는 애플리케이션)
- eventTime – 작업이 발생한 날짜 및 시간
- eventSource – 작업이 콘솔, AWS CLI 또는 API 호출을 통해 수행되었는지 여부


```
{   "eventVersion" : "1.01",
    "userIdentity" : {
        "type" : "IAMUser",
        "principalId" : "AIDAyyyyyyyyyyyyyyyy",
        "arn" : "arn:aws:iam::xxxxxxxxxxxx:user/tests3user",
        "accountId" : "xxxxxxxxxxxx",
        "userName" : "tests3user"
    },
    "eventTime" : "2018-09-23T22:41:38Z",
    "eventSource" : "signin.amazonaws.com",
    "eventName" : "ConsoleLogin",
    "awsRegion" : "us-east-1",
    "sourceIPAddress" : "54.240.217.10",
    "userAgent" : "Mozilla/5.0 (Windows NT 6.1; WOW64; rv:31.0)
Gecko/20100101 Firefox/31.0",
```


aws re/start

CloudTrail 로그 항목: responseElements(성공 예제)

이 예제는 동일한 샘플 로그 항목의 responseElements 섹션을 보여줍니다.

```
"responseElements" : {
                "ConsoleLogin" : "Success"
            },
            "additionalEventData" : {
                "MobileVersion" : "No",
                "LoginTo" :
"https://console.aws.amazon.com/console/home?state\u003dhas
hArgs%23\u0026isauthcode\u003dtrue",
                "MFAUsed" : "No"
            },
            "eventID" : "b31716e9-13e5-4fb5-9c60-
1c723c59f5a6"
        }
```


aws re/start

CloudTrail 로그 항목: responseElements(실패 예제)

이 예제는 다른 샘플 로그 항목에 대한 로그인 시도의 responseElements 섹션입니다.


```
        "errorMessage" : "Failed authentication",
            "requestParameters" : null,
            "responseElements" : {
                "ConsoleLogin" : "Failure"
            },
            "additionalEventData" : {
                "MobileVersion" : "No",
                "LoginTo" :
"https://console.aws.amazon.com/console/home?state
\u003dhashArgs%23\u0026isauthcode\u003dtrue",
                "MFAUsed" : "No"
            },
            "eventID" : "99dc0ee0-ec1d-4a14-bb74-
10407b3b8ab1"
        },
```


aws re/start

모니터링 및 보안

CloudWatch Logs 및 CloudTrail을 검사하여 잠재적인 무단 사용을 탐지합니다.

예제:

- 실패한 AWS 관리 콘솔 로그인 시도 또는 의심스러운 IP 주소에서의 로그인 시도
- API를 사용하여 서비스에 무단 액세스
- 의심스러운 리소스 시작

핵심 사항

- AWS CloudTrail을 사용하면 계정 활동을 지속적으로 기록하여 AWS 계정을 감사할 수 있습니다.
- CloudTrail이 캡처하는 정보는 Amazon S3와 같은 스토리지 서비스 또는 비즈니스 보고 도구로 보낼 수 있습니다.
- 로그 모니터링은 전문 보안 태세의 필수적인 부분입니다.

© 2020, Amazon Web Services, Inc. 또는 계열사. All rights reserved.

aws re/start