AWS 결정 가이드

AWS CloudTrail 또는 Amazon CloudWatch?

AWS CloudTrail 또는 Amazon CloudWatch?: AWS 결정 가이드

Table of Contents

AWS CloudTrail 또는 Amazon CloudWatch?

차이점을 이해하고 자신에게 적합한 것을 선택하세요.

용도	AWS CloudTrail 또는 Amazon CloudWatch가 클라우드 환경의 가시성, 보안 및 운영 효율성을 유지하는 데 적합한 선택인지 여부를 결정하는 데 도움이 됩니다.
최종 업데이트 날짜	2024년 9월 20일
적용 대상 서비스	• AWS CloudTrail • Amazon CloudWatch

소개

에 중요한 비즈니스 워크로드를 배포할 때는 클라우드 환경에서 가시성, 보안 및 운영 효율성을 유지하는 AWS 클라우드것이 중요합니다. 해결해야 할 주요 영역은 다음과 같습니다.

- 운영 투명성 - 클라우드 환경에서 누가 무엇을 하고 있는지 추적하고 리소스의 성능을 모니터링합니다.
- 보안 보증 - 보안 위협을 나타낼 수 있는 비정상적인 API 호출 또는 리소스 사용률을 감지합니다.
- 규정 준수 - 감사를 위해 사용자 활동 및 인프라 변경에 대한 세부 로그를 유지합니다.
- 성능 관리 - 리소스 사용률 및 애플리케이션 성능 지표를 모니터링합니다.
- 인시던트 대응 - 운영 문제를 신속하게 식별하고 대응할 수 있는 데이터 및 알림입니다.
- 비용 제어 - 클라우드 지출을 관리하는 데 도움이 되는 리소스 사용량에 대한 인사이트입니다.
- 자동화 - 특정 이벤트 또는 성능 임계값에 대한 자동 응답입니다.

AWS 는 이러한 문제를 해결하는 데 도움이 되는 두 가지 주요 서비스를 제공합니다.

- AWS CloudTrail는 주로 거버넌스, 규정 준수 및 운영 감사에 중점을 둡니다. AWS 환경 내에서 이루어진 모든 API 호출을 로깅합니다. 주요 기능:
  - API 호출, , AWS Management Console AWS SDKs, 명령줄 도구 및 기타 AWS 서비스에서 수행된 작업을 포함한 모든 AWS 계정 활동을 추적합니다.

  - 호출한 사람, 사용한 서비스, 영향을 받은 리소스 등 모든 작업에 대한 자세한 로그를 제공합니다.
  - 보안 감사, 사용자 활동 추적 및 잠재적으로 악의적인 작업 식별에 유용합니다.
- Amazon CloudWatch는 AWS온프레미스 및 하이브리드 애플리케이션과 인프라에 대한 데이터와 실행 가능한 인사이트를 제공하는 모니터링 및 관찰성 서비스입니다. 이 기능은 다음과 같습니다.
  - 지표, 로그 및 경보를 포함하여 AWS 에서 실행되는 AWS 리소스와 애플리케이션을 실시간으로 모니터링합니다.
  - 시스템 성능, 오류율, 리소스 사용률 등에 대한 자세한 인사이트를 제공합니다.
  - 특정 조건에 따라 작업(예: 조정 리소스)을 트리거하도록 경보를 설정할 수 있습니다.

두 서비스 모두 강력하고 안전한 클라우드 환경에 중요하지만 사용 사례와 제공하는 기능이 다릅니다.

다음은 시작하기 위한 이러한 서비스 간의 주요 차이점에 대한 개괄적인 보기입니다.

카테고리	CloudTrail	CloudWatch
기본 용도	API 활동 추적 및 감사	실시간 모니터링 및 성능 관리
수집된 데이터	호출한 사람, 시기 및 영향을 받은 리소스를 포함한 API 호출 로그	리소스 성능 및 애플리케이션 동작과 관련된 지표, 로그 및 이벤트
사용 사례	환경의 보안 감사, 규정 준수 및 변경 사항 추적	리소스 사용률 모니터링, 경보 설정 및 성능 관리
보안 및 규정 준수	자세한 활동 로그를 제공하여 보안 및 규정 준수 요구 사항을 충족하는 데 도움이 됩니다.	시스템 성능에서 보안 이상을 모니터링하고 운영 무결성을 유지하는 데 도움이 됩니다.
로그 보존	지난 90일간의 이벤트 기록. 추적 및 이벤트 데이터 스토어(CloudTrail Lake 사용)를 생성하여 90일 이상 활동 기록을 유지할 수 있습니다.	실시간 모니터링 및 문제 해결을 위한 단기 데이터 보존
경보 및 알림	주로 경보에 사용되지 않지만 API 활동에 따라 작업을 트리거할 수 있습니다.	자동 응답을 사용하여 특정 지표 또는 로그 이벤트에 대한 경보 설정 활성화

카테고리	CloudTrail	CloudWatch
통합	보안 관리를 강화하기 위해 AWS Config 및 IAM과 같은 보안 서비스와 함께 자주 사용됩니다.	포괄적인 모니터링 및 자동화를 위해 다양한 AWS 서비스와 통합
비용 고려 사항	생성 및 저장된 로그의 양에 따른 비용	모니터링되는 지표, 로그 및 경보 수를 기준으로 한 비용
데이터 세분화	세분화된 정보와 함께 모든 API 호출에 대한 세부 로그를 제공합니다.	실시간 모니터링을 위한 집계된 지표 및 로그 데이터 제공
액세스 제어	사용자 권한의 액세스 패턴 및 변경 사항을 추적할 수 있습니다.	성능 지표를 기반으로 리소스에 대한 액세스를 모니터링하고 최적화하는 데 도움이 됩니다.
리소스 범위	AWS 계정-wide	개별 AWS 리소스
실시간 추적	거의 실시간(5분 이내)	실시간 또는 거의 실시간
시각화	제한적, 다른 도구와 함께 자주 사용됨	기본 제공 대시보드 및 그래프

CloudTrail과 CloudWatch의 차이점

여러 주요 영역에서 CloudTrail과 CloudWatch의 차이점을 살펴봅니다.

Primary purpose

AWS CloudTrail

- 내의 모든 API 활동에 대한 포괄적인 감사 추적을 제공합니다 AWS 계정. 누가 무엇을 언제 어디서 했는지 기록하는 데 중점을 둡니다. 여기에는 AWS Management Console, AWS SDKs, 명령줄 도구 및 기타 AWS 서비스를 통해 수행된 작업이 포함됩니다. CloudTrail은 "이 EC2 인스턴스를 종료한 사람은 누구입니까?"와 같은 질문에 답합니다. 또는 "이 IAM 정책은 어떻게 변경되었나요?"

Amazon CloudWatch

- 리소스 및 애플리케이션의 운영 상태 및 성능을 AWS 모니터링합니다. CloudWatch는 지표를 수집 및 추적하고, 로그 파일을 수집 및 모니터링하고, 경보를 설정합니다. 이를 통해 애플리케이션이 어떻게 실행되고 있는지 이해하고 시스템 전체의 성능 변화에 대응할 수 있습니다. CloudWatch는 "Amazon EC2 인스턴스의 CPU 사용률이 너무 높습니까?"와 같은 질문에 답합니다. 또는 "Lambda 함수가 생성하는 오류는 몇 개입니까?"

요약

CloudTrail은 보안 및 규정 준수에 대한 사용자 활동을 추적하고 감사하는 데 도움이 되며, CloudWatch는 시스템 성능 및 운영 상태를 모니터링하고 최적화하는 데 중점을 둡니다. 두 도구 모두 클라우드 환경을 관리하는 데 있어 고유하지만 보완적인 역할을 합니다.

Data collected

AWS CloudTrail

- AWS 환경 내 모든 API 활동의 세부 로그를 캡처하는 데 중점을 둡니다. 여기에는 API 호출을 수행한 사람, 호출이 수행된 시간, 수행된 작업 및 관련된 리소스에 대한 정보가 포함됩니다. CloudTrail의 로그는 변경 사항을 추적하고 규정 준수를 보장하며 보안 인시던트를 조사하는 데 필수적인 포괄적인 감사 추적을 제공합니다.

Amazon CloudWatch

- AWS 리소스 및 애플리케이션에서 성능 및 운영 데이터를 수집합니다. 여기에는 CPU 사용량, 메모리 사용률, 네트워크 트래픽 및 애플리케이션 로그와 같은 지표와 정의할 수 있는 사용자 지정 지표가 포함됩니다. CloudWatch에서 수집하는 데이터는 실시간 모니터링, 성능 최적화 및 경보 설정에 사용되어 특정 조건에 따라 자동화된 작업을 트리거합니다.

요약

CloudTrail은 감사 및 보안 목적으로 사용자 활동 및 API 사용과 관련된 데이터를 수집하는 반면, CloudWatch는 지표 및 로그를 수집하여 시스템 성능 및 운영 상태를 모니터링, 관리 및 최적화합니다. 둘 다 중요한 인사이트를 제공하지만 클라우드 관리의 다양한 측면을 제공합니다.

Use cases

AWS CloudTrail

- 보안 감사, 규정 준수 및 운영 감사에 주로 사용됩니다. CloudTrail은 AWS 환경 내 API 호출 및 사용자 활동에 대한 자세한 레코드를 제공하므로 변경 사항을 추적하고, 보안 인시던트를 조사하고, 조직이 규제 요구 사항을 충족하는 데 필수적입니다. 예를 들어 CloudTrail은 특정 리소스에 액세스한 사용자를 모니터링하거나 구성에 대한 변경 사항을 추적하거나 여러에서 활동을 감사해야 하는 시나리오에서 유용합니다 AWS 계정.

Amazon CloudWatch

- 실시간 모니터링, 성능 관리 및 운영 효율성을 위해 설계되었습니다. CloudWatch는 지표, 로그 및 이벤트를 수집하고 추적하여 AWS 리소스 및 애플리케이션의 상태를 모니터링하는 데 사용됩니다. CloudWatch를 사용하면 특정 임계값이 충족될 때 리소스 조정 또는 알림 전송과 같은 자동화된 작업을 트리거하는 경보를 설정할 수 있습니다. CloudWatch 사용 사례에는 애플리케이션 성능 모니터링, 리소스 사용률 관리, 이상 탐지, 가동 중지를 방지하기 위한 시스템 최적의 실행 여부 확인이 포함됩니다.

Security and compliance

AWS CloudTrail

- AWS 환경에서 보안 및 규정 준수를 유지하기 위한 필수 요소입니다. CloudTrail은 호출한 사람, 호출한 시간, 수행한 작업을 포함하여 모든 API 호출에 대한 포괄적인 감사 추적을 제공합니다. 이 세부 로깅은 규정 준수 표준을 충족하고, 보안 감사를 수행하고, 인시던트를 조사하는 데 필수적입니다. CloudTrail은 사용자 활동 및 리소스 변경 사항을 추적하여 많은 규제 프레임워크의 주요 요구 사항인 책임과 투명성을 보장하는 데 도움이 됩니다.

Amazon CloudWatch

- 운영 이상 탐지를 활성화하여 보안에서 역할을 수행합니다. 예를 들어 CloudWatch를 사용하여 네트워크 트래픽 또는 CPU 사용량의 비정상적인 급증과 같은 잠재적 보안 문제를 나타내는 지표를 모니터링할 수 있습니다. 또한 CloudWatch는 특정 임계값이 충족되면 경보와 자동 응답을 트리거하여 사전 인시던트 관리를 가능하게 할 수 있습니다. CloudWatch에 캡처된 로그를 사용하여 운영 이벤트를 추적할 수도 있으며, 이는 보안 인시던트의 컨텍스트를 이해하는 데 중요할 수 있습니다.

요약

CloudTrail은 함께 규정 준수에 필요한 감사 로그를 제공하는 반면, CloudWatch는 보안 위협을 탐지하고 이에 대응하는 데 도움이 되는 실시간 모니터링을 제공하여 안전하고 규정을 준수하는 클라우드 환경에 기여합니다.

Log retention

AWS CloudTrail

- 기본적으로 CloudTrail 이벤트 기록은 계정에 대한 지난 90일간의 관리 이벤트를 기록합니다.
- 사용자는 S3 버킷에 로그를 무기한 저장하는 추적을 생성할 수 있습니다.
- Amazon S3에 저장된 로그는 자동으로 삭제되지 않으므로 장기 보존이 가능합니다.
- 사용자는 S3 버킷에 수명 주기 정책을 구현하여 장기 스토리지 비용을 관리할 수 있습니다.
- CloudTrail은 보다 유연한 보존 옵션을 위해 CloudWatch Logs로 로그를 보내도록 구성할 수 있습니다.

Amazon CloudWatch

- CloudWatch Logs의 로그 보존은 더 유연하고 구성 가능합니다.
- 기본 보존 기간은 로그 그룹에 따라 다르며, 일반적으로 "만료되지 않음"으로 설정됩니다.
- 사용자는 1일에서 10년까지의 사용자 지정 보존 기간을 설정하거나 무기한 보존을 선택할 수 있습니다.
- 로그 그룹마다 보존 기간이 다를 수 있습니다.
- 보존 기간이 지나면 로그가 자동으로 삭제되어 스토리지 비용을 관리합니다.
- CloudWatch Logs는 필요한 경우 장기 스토리지를 위해 Amazon S3로 내보낼 수 있습니다.

Alarms and notifications

AWS CloudTrail

- 주로 API 활동 로깅에 중점을 두며 경보 또는 알림 기능이 내장되어 있지 않습니다. 그러나 CloudWatch Logs 및 CloudWatch 경보와 통합하여 CloudTrail 이벤트에 대한 경보를 구성할 수 있습니다. 이 설정은 일반적으로 무단 액세스 시도 또는 중요 리소스 변경과 같은 보안 관련 이벤트를 알리는 데 사용됩니다.

Amazon CloudWatch

- 실시간 모니터링을 위해 특별히 설계되었으며 강력한 경보 및 알림 기능이 포함되어 있습니다. CloudWatch를 사용하면 지표, 로그 데이터 또는 사용자 지정 정의 임계값을 기반으로 경보를 설정할 수 있습니다. 이러한 임계값이 위반되면 CloudWatch는 Amazon SNS(Amazon Simple Notification Service)를 통해 알림을 보내거나, 인스턴스 조정과 같은 자동화된 작업을 트리거하거나,를 사용하여 사용자 지정 문제 해결 단계를 수행할 수 있습니다 AWS Lambda. 따라서 CloudWatch는 선제적 시스템 관리를 위한 필수 도구로, 성능 문제 또는 운영 이상이 발생할 때 이를 알려줍니다.

Integration

CloudTrail 및 CloudWatch는 다른 AWS 서비스 및 외부 도구와의 광범위한 통합 옵션을 제공하여 기능과 유틸리티를 개선합니다.

CloudTrail 통합

- Amazon S3: 보관 및 분석을 위한 장기 로그 저장
- CloudWatch Logs: 실시간 로그 분석 및 알림 활성화
- Amazon EventBridge: API 이벤트를 기반으로 자동화된 작업 트리거
- AWS Config: 구성 추적 및 규정 준수를 위한 입력 제공
- AWS Security Hub CSPM: 중앙 집중식 보안 태세 관리에 기여
- AWS Lake Formation: CloudTrail 로그의 데이터 레이크 거버넌스 활성화
- Amazon Athena: Amazon S3에 저장된 CloudTrail 로그에서 SQL 쿼리 수행

CloudWatch 통합

- Amazon SNS: 경보 및 이벤트에 대한 알림 전송
- AWS Lambda: 지표 또는 로그를 기반으로 서버리스 함수 트리거
- Amazon EC2 Auto Scaling: 성능 지표를 기반으로 용량 조정
- AWS Systems Manager: CloudWatch 데이터를 기반으로 운영 작업 자동화
- AWS X-Ray: 추적 데이터와 결합하여 심층적인 애플리케이션 인사이트 확보
- 컨테이너 서비스(Amazon ECS, Amazon EKS): 컨테이너화된 애플리케이션 모니터링
- 타사 도구: 지표 및 로그를 외부 모니터링 플랫폼으로 내보내기

Cost considerations

AWS CloudTrail

- CloudTrail은 주로 로깅되고 저장된 이벤트 수를 기준으로 가격이 책정됩니다. 기본적으로 CloudTrail 이벤트 기록는 계정에 대한 지난 90일간의 관리 이벤트를 무료로 기록하고 저장합니다. 그러나 데이터 이벤트(예: S3 객체 수준 작업)를 활성화하거나 여러 추적을 생성하는 경우 Amazon S3에 필요한 이벤트 볼륨과 스토리지에 따라 요금이 발생합니다. 비정상적인 API 활동에 대한 심층 분석을 제공하는 CloudTrail Insights와 같은 고급 기능을 사용하는 경우 추가 비용이 발생할 수 있습니다.

Amazon CloudWatch

- CloudWatch는 모니터링하는 사용자 지정 지표 수, 수집 및 저장된 로그 이벤트 수, 경보 및 대시보드 사용 등 여러 요인을 기반으로 보다 복잡한 요금 구조를 제공합니다. AWS 서비스에 대한 기본 모니터링은 무료이지만 세부 모니터링 및 사용자 지정 지표에는 요금이 부과됩니다. 로그 스토리지는 수집 및 보존되는 데이터의 양을 기준으로 요금이 책정되며, 경보를 설정 및 유지 관리하거나 고급 로그 분석에 CloudWatch Logs Insights를 사용하는 데 드는 추가 비용이 발생합니다.

Data granularity

AWS CloudTrail

- CloudTrail은 AWS 환경 내에서 이루어진 모든 개별 API 직접 호출을 로깅하여 높은 세부 수준을 제공합니다. 각 로그 항목에는 요청한 사람, 수행된 작업, 영향을 받는 리소스, 작업 시간과 같은 세부 정보가 포함됩니다. 이러한 세부 정보는 특정 사용자 작업과 변경 사항을 정확한 API 직접 호출까지 추적할 수 있으므로 감사, 보안 모니터링 및 규정 준수에 매우 중요합니다.

Amazon CloudWatch

- CloudWatch는 모니터링 및 성능 관리를 위해 집계된 데이터에 중점을 둡니다. 정기적으로(일반적으로 1분 또는 5분마다) 지표를 수집하고 AWS 리소스에서 운영 데이터를 로깅합니다. CloudWatch는 시스템 성능 및 애플리케이션 동작에 대한 자세한 인사이트를 제공하지만 CloudTrail에 비해 데이터가 더 집계됩니다. 예를 들어 개별 요청이나 작업이 아닌 시간 경과에 따른 평균 CPU 사용량을 모니터링할 수 있습니다. 그러나 CloudWatch Logs는 CloudTrail과 유사한 보다 세분화된 데이터를 제공할 수 있지만 API 호출을 추적하는 대신 운영 로그를 분석하는 데 자주 사용됩니다.

Real-time tracking

AWS CloudTrail

- CloudTrail은 기본적으로 실시간 추적을 위해 설계되지 않았지만 near-real-time 알림을 제공하도록 구성할 수 있습니다. 기본적으로 CloudTrail은 API 활동을 기록하지만 로그 전송이 약간 지연됩니다. 보다 즉각적인 추적을 위해 CloudTrail AWS Lambda 을 Amazon CloudWatch Events와 통합하거나 로깅되는 즉시 특정 API 호출 또는 활동을 기반으로 작업을 트리거할 수 있습니다. 이 설정을 사용하면 중요한 보안 이벤트 또는 구성 변경 사항을 near-real-time 있습니다.

Amazon CloudWatch

- 반면 CloudWatch는 시스템 및 애플리케이션 성능을 실시간으로 추적하도록 구축되었습니다. AWS 리소스의 지표를 지속적으로 모니터링하고 사전 정의된 임계값을 초과하면 경보 또는 알림을 즉시 트리거할 수 있습니다. 또한 CloudWatch는 로그 데이터를 실시간으로 수집 및 분석하여 애플리케이션 로그를 모니터링하고, 이상을 감지하고, 운영 문제가 발생할 때 이에 대응할 수 있습니다. 따라서 CloudWatch는 AWS 환경의 상태와 성능을 실시간으로 유지하기 위한 필수 도구입니다.

사용

이제 AWS CloudTrail 와 Amazon CloudWatch 중에서 선택하는 기준에 대해 읽었으므로 필요에 맞는 서비스를 선택하고 다음 정보를 사용하여 각 서비스 사용을 시작할 수 있습니다.

AWS CloudTrail

- 시작하기 AWS CloudTrail

  AWS CloudTrail 는 운영 및 위험 감사, 거버넌스 및 규정 준수를 지원하는 AWS 서비스입니다 AWS 계정. 시작하는 방법은 다음과 같습니다.

  가이드 살펴보기
- AWS 계정 활동 검토

  CloudTrail의 이벤트 기록 기능을 AWS 계정 사용하여에서 최근 AWS API 활동을 검토하는 방법을 알아봅니다.

  자습서 사용
- 추적 생성

데이터 및 Insights 이벤트를 포함하여 모든 리전에서 AWS API 활동을 로깅하는 추적을 생성하는 방법을 알아봅니다.

자습서 사용

- 의 보안 모범 사례 AWS CloudTrail

  이 가이드는 AWS CloudTrail 조직에서를 사용하기 위한 탐지 및 예방 보안 모범 사례를 제공합니다.

  가이드 살펴보기

Amazon CloudWatch

- Amazon CloudWatch 시작하기

  Amazon CloudWatch를 사용하여 AWS 에서 실행하는 AWS 리소스와 애플리케이션을 실시간으로 모니터링합니다. CloudWatch를 사용하여 리소스 및 애플리케이션에 대해 측정할 수 있는 변수인 지표를 수집하고 추적할 수 있습니다.

  가이드 살펴보기

- Amazon CloudWatch 지표 시작하기

  이 가이드에서는 기본 모니터링 및 세부 모니터링, 지표를 그래프로 표시하는 방법, CloudWatch 이상 탐지를 사용하는 방법을 설명합니다.

  가이드 살펴보기

- Amazon EKS 및 Kubernetes에서 Container Insights 설정

  EKS 클러스터에서 Amazon CloudWatch Observability ESK 추가 기능 및 ADTO를 설정하여 지표를 CloudWatch로 전송합니다. 또한 CloudWatch Logs로 로그를 전송하도록 Fluent Bit 또는 Fluentd를 설정하는 방법도 알아봅니다.

  가이드 살펴보기

- Amazon CloudWatch Application Insights 시작하기

  콘솔을 사용하여 CloudWatch Application Insights가 모니터링을 위해 애플리케이션을 관리할 수 있도록 하는 방법을 알아봅니다.

  가이드 살펴보기

- Container Insights 사용

  CloudWatch Container Insights가 컨테이너화된 애플리케이션 및 마이크로서비스에서 지표와 로그를 수집, 집계 및 요약하는 방법을 알아봅니다.

  가이드 살펴보기

- Amazon ECS에서 Container Insights 설정

  클러스터 및 서비스 수준 지표를 구성하고, ADOT를 배포하여 EC2 인스턴스 수준 지표를 수집하고, FireLens를 설정하여 CloudWatch Logs로 로그를 전송하는 방법을 알아봅니다.

  가이드 살펴보기

AWS CloudTrail 또는 Amazon CloudWatch의 문서 기록

다음 표에서는이 결정 가이드의 중요한 변경 사항에 대해 설명합니다. 이 가이드 업데이트에 대한 알림을 받으려면 RSS 피드를 구독하면 됩니다.

변경 사항	설명	날짜
최초 릴리스	결정 가이드의 최초 릴리스입니다.	2024년 9월 20일