



AWS Config

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

AWS Config를 시작하겠습니다.

학습 내용

이 강의의 핵심

배울 내용은 다음과 같습니다.

- AWS Config의 가치를 설명합니다.
- AWS Config의 기능을 알아봅니다.



이 모듈에서는 AWS Config를 설명하고 그 기능을 알아봅니다.

AWS Config 소개

AWS Config는 AWS 리소스를 측정하고, 감사하고, 평가할 수 있게 해주는 완전관리형 서비스입니다.

- 거의 지속적인 모니터링
- 거의 지속적인 평가
- 변경 관리
- 운영 문제 해결

AWS Config는 AWS 리소스를 측정하고, 감사하고, 평가할 수 있게 해주는 완전관리형 서비스입니다. AWS Config는 거의 지속적인 모니터링, 거의 지속적인 평가, 변경 관리 및 운영 문제 해결을 제공합니다.

AWS Config

리소스 변경 사항 추적

- AWS 리소스 인벤토리, 구성 기록 및 구성 변경 알림을 제공합니다.
- 모든 구성 변경의 세부 정보를 제공합니다.
- AWS CloudTrail과 결합됩니다.
- 이를 통해 다음을 수행할 수 있습니다.
 - 규정 준수 감사
 - 보안 분석
 - 리소스 변경 사항 추적
 - 문제 해결



AWS Config는 AWS 리소스 인벤토리, 구성 기록 및 구성 변경 사항 알림을 제공하여 보안과 거버넌스를 활성화합니다.

AWS Config를 사용하면 다음을 수행할 수 있습니다.

- 기존 AWS 리소스 검색
- 모든 구성 세부 정보와 함께 AWS 리소스의 전체 인벤토리 내보내기
- 특정 시점의 리소스 구성 방식 확인

이러한 기능 덕분에 규정 준수 감사, 보안 분석, 리소스 변경 추적 및 문제 해결이 가능합니다. AWS Config의 구체적인 가치:

- 탐지
 - 탐지 제어 조치를 만들고 이상 현상을 식별 및 분석합니다.
- 규정 준수
 - 리소스 규정 준수를 평가하는 규칙을 만들고 SOC 인증을 충족하도록 지원합니다.
 - AWS 리소스 간 구성 및 관계 변경 사항을 검토합니다.
- 액세스 제어
 - AWS Config에 S3 버킷과 같은 리소스에 액세스할 권한을

- 부여하는 IAM 역할을 생성합니다.
- 사용자를 대신해서 다른 서비스를 호출하기 위해 Config에서 요구하는 모든 권한을 포함하며 AWS Config에 연결된 서비스-링크 역할을 생성합니다.
- 암호화/저장 데이터
 - AWS Config는 기록 중인 리소스 유형에 대한 변경 사항을 탐지할 때마다 구성 항목을 생성합니다. 구성 항목의 구성 요소에는 메타데이터, 속성, 관계, 현재 구성, 관련 이벤트가 있습니다.

AWS Config를 통해 규정 준수 감사, 보안 분석, 변경 관리 및 운영 문제 해결을 간소화할 수 있습니다.

AWS Config 개요

작동 원리:



이 다이어그램은 AWS Config의 작동 원리를 보여줍니다.

1. AWS 리소스 중 하나에서 변경 사항이 발생합니다.
2. AWS Config 엔진이 해당 변경 사항을 일관된 형식으로 기록하고 정규화합니다.
3. 그런 다음 변경 사항의 레코드가 Amazon Simple Storage Service(Amazon S3) 버킷으로 전송되고, 여기에서 AWS Config 애플리케이션 프로그래밍 인터페이스(API)를 통해 레코드가 액세스됩니다. 변경 사항은 Amazon Simple Notification Service(Amazon SNS)와 같은 알림 서비스를 통해서도 전송될 수 있습니다.
4. 영향을 받은 리소스에 대해 **AWS Config 규칙**이 정의된 경우 AWS Config가 변경 사항이 규칙을 위반하지 않는지 확인합니다. AWS Config가 대시보드에 평가의 결과를 표시합니다. 결과가 Amazon SNS에 전송될 수도 있습니다.

비즈니스 당면 과제

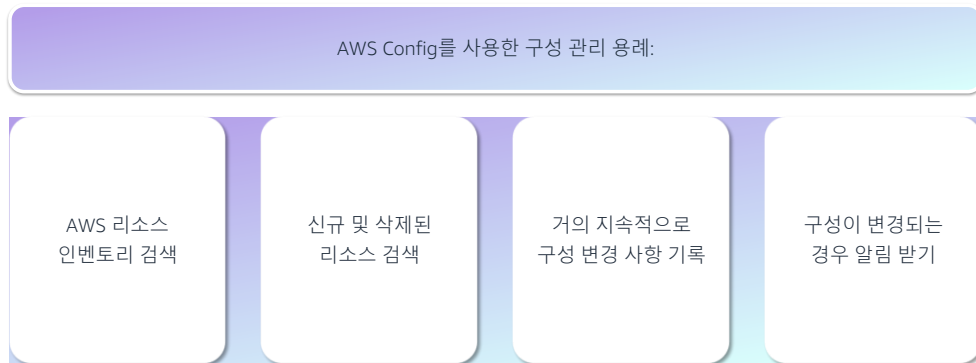
구성 관리



고객은 AWS 계정에서 대개 수백, 수천 개의 Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스를 실행합니다. AWS 계정의 다른 리소스 역시 그 수가 많을 수 있습니다. 이 모든 리소스의 구성을 관리하는 일은 쉽지 않습니다.

배포된 리소스가 현재 어떻게 구성되어 있어야 하는지는 알지도 모르지만 일어날 수도 있는 구성 오류에 대한 가시성도 확보되어 있습니까? 구성 변경 사항을 관리하고 추적할 시스템이 있습니까?

구성 관리에 AWS Config 사용



7

aws re/start

AWS Config는 AWS 리소스 구성을 거의 지속적으로 모니터링하고 기록합니다. 원하는 구성과 비교하여 기록된 구성을 평가하는 작업을 자동화할 수 있습니다.

AWS Config를 사용하면 다음 태스크를 수행할 수 있습니다.

- AWS 리소스 인벤토리 검색
- 신규 및 삭제된 리소스 검색
- 거의 지속적으로 구성 변경 사항 기록 내부 가이드라인에 지정된 구성을 기준으로 전반적인 규정 준수 확인
- 구성이 변경되면 알림을 받고 상세한 리소스 구성 기록 분석

이 모든 기능 덕분에 규정 준수 감사, 보안 분석, 변경 관리, 운영 문제 해결 작업이 간소화됩니다.

AWS Config 규칙

AWS Config 규칙 용례:

기록된 구성 변경
사항 확인을 위한
규칙 설정하기

사전 정의된
관리형 규칙을
사용하거나
사용자 지정 규칙
생성하기

AWS Lambda를
사용하여 사용자
지정 규칙
작성하기

규정 준수를
시각화하고
우려가 될 만한
변경 사항을
식별하기 위해
대시보드 보기

거의 지속적인
평가를 위해
규칙이 자동으로
호출됨

AWS Config는 규칙 시스템을 제공합니다. AWS와 AWS 파트너의 기존 규칙을 사용할 수 있습니다. AWS Lambda를 사용하여 여러분이 직접 규칙을 정의할 수도 있습니다. AWS Lambda는 서버를 프로비저닝하거나 관리할 필요 없이 코드를 실행할 수 있는 웹 서비스입니다.

특정 리소스, 특정 리소스 유형, 특정 방식으로 태그가 지정된 리소스 수준에서 규칙을 타겟팅할 수 있습니다. 규칙은 해당 리소스가 생성되거나 변경될 때 실행되며 주기적으로(매시간, 매일 등) 평가될 수도 있습니다.

구성 변경 사항이 기록되는지 확인하는 규칙을 설정할 수 있습니다. AWS Config를 설정하면 규정 준수가 시각화되는 대시보드가 제공됩니다. 이 대시보드를 사용하여 리소스에서 우려가 될 만한 변경 사항을 식별할 수도 있습니다.

AWS Config는 자동으로 호출되므로 구성이 거의 지속적으로 평가됩니다.

예: AWS Config 규칙

Amazon EBS 볼륨이 암호화됩니다.

인스턴스가 승인된 Amazon Machine Image(AMI)를 사용합니다.

탄력적 IP 주소가 인스턴스에 연결됩니다.

Amazon EC2 인스턴스에 적절한 태그가 지정됩니다.

규칙은 정상 상태나 비정상 상태를 확인합니다.

예를 들면, 상태가 다음과 같은지 확인하는 규칙을 정의할 수 있습니다.

- Amazon Elastic Block Store(Amazon EBS) 볼륨이 암호화됩니다.
- 인스턴스가 승인된 Amazon Machine Image(AMI)에서만 생성됩니다.
- 탄력적 IP 주소가 인스턴스에 연결됩니다.
- Amazon EC2 인스턴스에 적절한 태그가 지정됩니다.

핵심 사항



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

10

- AWS Config를 사용하면 리소스 구성 변경 사항을 추적하고 이에 대한 질문에 답변할 수 있으며, 규정 준수를 입증하고 보안 취약성을 탐지 및 해결할 수 있습니다.
- AWS Config 규칙을 정의하여 리소스 구성의 모범 실무를 구현하고 보안 및 거버넌스 정책을 시행할 수 있습니다.
- AWS Config를 사용하면 리소스가 생성, 수정 또는 삭제될 때마다 알림을 받고 리소스 간의 관계를 볼 수 있습니다.

aws re/start

이 강의에서 다룬 핵심 사항은 다음과 같습니다.

- AWS Config를 사용하면 리소스 구성 변경 사항을 추적하고 이에 대한 질문에 답변할 수 있으며, 규정 준수를 입증하고 보안 취약성을 탐지 및 해결할 수 있습니다.
- AWS Config 규칙을 정의하여 리소스 구성의 모범 실무를 구현하고 보안 및 거버넌스 정책을 시행할 수 있습니다.
- AWS Config를 사용하면 리소스가 생성, 수정 또는 삭제될 때마다 알림을 받고 리소스 간의 관계를 볼 수 있습니다.