AWS 인시던트 감지 및 대응 개념 및 절차

AWS 인시던트 감지 및 대응 사용 설명서

버전 November 1, 2024

AWS 인시던트 감지 및 대응 사용 설명서: AWS 인시던트 감지 및 대응 개념 및 절차

Table of Contents

AWS 인시던트 감지 및 대응이란 무엇입니까?

AWS 인시던트 감지 및 대응은 적격 AWS Enterprise Support 고객에게 사전 예방적인 인시던트 참여를 제공하여 장애 가능성을 줄이고 중요한 워크로드의 중단 복구를 가속화합니다. 인시던트 감지 및 대응을 통해 와 협력하여 온보딩된 각 워크로드 AWS 에 맞는 런북 및 대응 계획을 쉽게 개발할 수 있습니다.

인시던트 감지 및 대응은 다음과 같은 주요 기능을 제공합니다.

- 향상된 관찰 가능성: AWS 전문가는 워크로드의 애플리케이션 계층과 인프라 계층 간에 지표와 경보를 정의하고 상호 연관시켜 중단을 조기에 감지하는 데 도움이 되는 지침을 제공합니다.
- 5분 응답 시간: 온보딩된 워크로드를 연중무휴 IMEs 모니터링하여 중요한 인시던트를 탐지합니다. 경보가 트리거된 후 5분 이내에 또는 인시던트 감지 및 IMEs 대응에 제기한 비즈니스 크리티컬 지원 사례에 대한 응답입니다.
- 더 빠른 해결: 워크로드용으로 개발된 사전 정의된 사용자 지정 런북을 IMEs 사용하여 5분 이내에 응답하고, 사용자를 대신하여 지원 사례를 생성하고, 워크로드에서 인시던트를 관리합니다. IMEs 인시던트에 대한 단일 스레드 소유권을 제공하고 인시던트가 해결될 때까지 적절한 AWS 전문가와 계속 소통합니다.
- AWS 이벤트에 대한 인시던트 관리: 중요한 워크로드(예: 계정, 서비스 및 인스턴스)의 컨텍스트를 이해하므로 AWS 서비스 이벤트 중에 워크로드에 미칠 수 있는 잠재적 영향을 감지하고 사전에 알릴 수 있습니다. 요청된 경우 AWS 서비스 이벤트 중에 IMEs 사용자를 참여시키고 이벤트에 대한 업데이트를 제공합니다. 인시던트 감지 및 대응은 서비스 이벤트 중 복구를 위해 우선 순위를 지정할 수 없지만 인시던트 감지 및 대응은 완화 계획을 구현하는 데 도움이 되는 지원 지침을 제공합니다.
- 실패 가능성 감소 : 해결 후 는 인시던트 후 검토(요청 시)를 IMEs 제공합니다. 또한 AWS 전문가는 고객과 협력하여 학습한 교훈을 적용하여 인시던트 대응 계획 및 런북을 개선합니다. 또한 워크로드의 지속적인 복원력 추적을 AWS Resilience Hub 위해 를 활용할 수 있습니다.

주제

인시던트 감지 및 대응 사용 약관

다음 목록은 AWS 인시던트 감지 및 대응을 사용하기 위한 주요 요구 사항 및 제한 사항을 간략하게 설명합니다. 이 정보는 지원 계획 요구 사항, 온보딩 프로세스 및 최소 구독 기간과 같은 측면을 다루기 때문에 서비스를 사용하기 전에 이해하는 것이 중요합니다.

- AWS 인시던트 감지 및 대응은 직접 및 파트너 재판매 엔터프라이즈 지원 계정에서 사용할 수 있습니다.
- AWS 파트너 주도 지원의 계정에서는 인시던트 감지 및 응답을 사용할 수 없습니다.
- 인시던트 감지 및 대응 서비스 기간 동안 항상 AWS 엔터프라이즈 지원을 유지해야 합니다. 자세한 내용은 엔터프라이즈 지원 섹션을 참조하세요. 엔터프라이즈 지원이 종료되면 AWS 인시던트 감지 및 대응 서비스에서 동시에 제거됩니다.
- AWS 인시던트 감지 및 대응의 모든 워크로드는 워크로드 온보딩 프로세스를 거쳐야 합니다.
- 계정을 AWS Incident Detection and Response에 구독하는 최소 기간은 구십(90) 일입니다. 모든 취소 요청은 예정된 취소 발효일 삼십(30) 일 전에 제출해야 합니다.
- AWS 는 AWS 개인정보 보호 고지 에 설명된 대로 정보를 처리합니다.

> **Note**
>
> 인시던트 감지 및 대응 청구 관련 질문은 AWS 청구 관련 도움말 받기를 참조하세요.

인시던트 감지 및 대응 아키텍처

AWS 인시던트 감지 및 대응은 다음 그림과 같이 기존 환경과 통합됩니다. 아키텍처에는 다음 서비스가 포함됩니다.

- Amazon EventBridge: Amazon EventBridge 은 워크로드와 AWS 인시던트 감지 및 대응 간의 유일한 통합 지점 역할을 합니다. 경보는 에서 관리하는 사전 정의된 규칙을 EventBridge 사용하여 Amazon CloudWatch를 통해 Amazon 와 같은 모니터링 도구에서 수집됩니다 AWS. 인시던트 감지 및 대응이 EventBridge 규칙을 빌드하고 관리할 수 있도록 하려면 서비스 연결 역할을 설치합니다. 이러한 서비스에 대한 자세한 내용은 Amazon 및 Amazon 규칙이란 무엇입니까 EventBridge, Amazon이란 무엇입니까, CloudWatch에 대한 서비스 연결 역할 사용을 AWS Health 참조하세요. EventBridge
- AWS Health: 리소스 성능과 AWS 서비스 및 계정의 가용성에 대한 지속적인 가시성을 AWS Health 제공합니다. Incident Detection and Response는 AWS Health 를 사용하여 워크로드에서 AWS 서비

스 사용되는 의 이벤트를 추적하고 워크로드에서 알림을 수신한 시기를 알려줍니다. 에 대한 자세한 내용은 정의 섹션을 AWS Health AWS Health참조하세요.

- AWS Systems Manager: Systems Manager는 AWS 리소스 전반의 자동화 및 작업 관리를 위한 통합 사용자 인터페이스를 제공합니다. AWS Incident Detection and Response는 워크로드 아키텍처 다이어그램, 경보 세부 정보 및 AWS Systems Manager 문서의 해당 인시던트 관리 런북을 포함하여 워크로드에 대한 정보를 호스팅합니다(자세한 내용은 AWS Systems Manager 문서 참조). 에 대한 자세한 내용은 정의 섹션을 AWS Systems Manager AWS Systems Manager참조하세요.
- 특정 런북: 인시던트 관리 런북은 인시던트 관리 중에 AWS 인시던트 감지 및 대응이 수행하는 작업을 정의합니다. 특정 실행서는 AWS Incident Detection and Response에 연락할 사람, 연락 방법, 공유할 정보를 알려줍니다.

인시던트 감지 및 대응의 역할 및 책임

AWS 인시던트 감지 및 대응RACI(책임, 책임, 상담 및 정보 제공) 표에는 인시던트 감지 및 대응과 관련된 다양한 활동에 대한 역할과 책임이 요약되어 있습니다. 이 표는 데이터 수집, 운영 준비 검토, 계정 구성, AWS 인시던트 관리 및 인시던트 후 검토와 같은 작업에 대한 고객 및 인시던트 감지 및 대응 팀의 참여를 정의하는 데 도움이 됩니다.

활동	고객	인시던트 감지 및 대응
데이터 수집		
고객 및 워크로드 소개	상담됨	책임
아키텍처	책임	책임
운영	책임	책임
구성할 CloudWatch 경보 결정	책임	책임
인시던트 대응 계획 정의	책임	책임
온보딩 설문지 작성	책임	책임

활동	고객	인시던트 감지 및 대응
작업 준비 검토		
워크로드에 대해 잘 설계된 검토(WAR) 수행	상담됨	책임
인시던트 응답 검증	상담됨	책임
경보 매트릭스 검증	상담됨	책임
워크로드에서 사용되는 주요 AWS 서비스 식별	책임	책임
계정 구성		
고객 계정에서 IAM 역할 생성	책임	정보 제공
생성된 역할을 사용하여 관리형 EventBridge 규칙 설치	정보 제공	책임
CloudWatch 경보 테스트	책임	책임
고객 경보가 인시던트 감지 및 대응과 관련이 있는지 확인	정보 제공	책임
경보 업데이트	책임	상담됨
런북 업데이트	상담됨	책임
인시던트 관리		
인시던트 감지 및 대응에서 감지된 인시던트에 사전 알림	정보 제공	책임
인시던트 대응 제공	정보 제공	책임
인시던트 해결/인프라 복원 제공	책임	상담됨
사고 후 검토		
사고 후 검토 요청	책임	정보 제공
사고 후 검토 제공	정보 제공	책임

인시던트 감지 및 대응을 위한 리전 가용성

AWS 인시던트 감지 및 대응은 현재 다음 중 하나에서 호스팅되는 영어 및 일본어 for Enterprise Support 계정에서 사용할 수 있습니다 AWS 리전.

명칭	AWS 리전
us-east-1	미국 동부(버지니아)
us-east-2	미국 동부(오하이오)
us-west-1	미국 서부(캘리포니아 북부)
us-west-2	미국 서부(오레곤)
ca-central-1	캐나다(중부)
ca-west-1*	캐나다 서부(캘거리)
sa-east-1	남아메리카(상파울루)
eu-central-1	유럽(프랑크푸르트)
eu-west-1	유럽(아일랜드)
eu-west-2	유럽(런던)
eu-west-3	유럽(파리)
eu-north-1	유럽(스톡홀름)
eu-central-2*	유럽(취리히)
eu-south-1*	유럽(밀라노)
eu-south-2*	유럽(스페인)
ap-south-1	아시아 태평양(뭄바이)
ap-northeast-1	아시아 태평양(도쿄)

명칭	AWS 리전
ap-northeast-2	아시아 태평양(서울)
ap-southeast-1	아시아 태평양(싱가포르)
ap-southeast-2	아시아 태평양(시드니)
ap-east-1*	아시아 태평양(홍콩)
ap-northeast-3*	아시아 태평양(오사카)
ap-south-2*	아시아 태평양(하이데라바드)
ap-southeast-3*	아시아 태평양(자카르타)
ap-southeast-4*	아시아 태평양(멜버른)
ap-southeast-5*	아시아 태평양(말레이시아)
af-south-1*	아프리카(케이프타운)
il-central-1*	이스라엘(텔아비브)
me-central-1*	중동(UAE)
me-south-1*	중동(바레인)

* AWS 리전 이의 데이터는 AWS 인시던트 감지 및 대응으로 전송되기 전에 기본 설정 AWS 리전 과 다른 방식으로 처리됩니다.

인시던트 감지 및 대응 시작하기

워크로드와 경보는 AWS Incident Detection and Response의 핵심입니다. 는 고객과 긴밀하게 AWS 협력하여 비즈니스에 중요한 특정 워크로드를 정의하고 모니터링합니다. 는 중요한 성능 문제 또는 고객 영향을 팀에 빠르게 알리는 경보를 설정하는 데 AWS 도움이 됩니다. 인시던트 감지 및 대응 내에서 사전 예방적 모니터링 및 신속한 인시던트 대응을 위해서는 적절하게 구성된 경보가 필수적입니다.

워크로드

AWS Incident Detection and Response를 사용하여 모니터링 및 중요 인시던트 관리를 위한 특정 워크로드를 선택할 수 있습니다. 워크로드는 비즈니스 가치를 제공하기 위해 함께 작동하는 리소스 및 코드의 모음입니다. 워크로드는 은행 결제 포털 또는 고객 관계 관리(CRM) 시스템을 구성하는 모든 리소스와 코드일 수 있습니다. 단일 AWS 계정 또는 여러 계정에서 워크로드를 호스팅할 수 AWS 있습니다.

예를 들어 단일 계정에 모놀리식 애플리케이션이 호스팅되어 있을 수 있습니다(예: 다음 다이어그램의 직원 성과 앱). 또는 애플리케이션(예: 다이어그램의 Storefront Webapp)이 여러 계정에 걸쳐 확장되는 마이크로서비스로 분할되어 있을 수 있습니다. 워크로드는 다이어그램과 같이 데이터베이스와 같은 리소스를 다른 애플리케이션 또는 워크로드와 공유할 수 있습니다.

워크로드 온보딩을 시작하려면 워크로드 온보딩 및 워크로드 온보딩 설문지 섹션을 참조하세요.

경보

경보는 애플리케이션 및 기본 AWS 인프라의 성능에 대한 가시성을 제공하므로 인시던트 감지 및 대응의 주요 부분 AWS 입니다. 는 사용자와 협력하여 모니터링되는 워크로드에 중요한 영향이 있을 때만 트리거되는 적절한 지표 및 경보 임계값을 정의합니다. 목표는 경보가 지정된 해석기를 참여시키는 것이며, 그러면 지정된 해석기는 인시던트 관리 팀과 협력하여 문제를 신속하게 완화할 수 있습니다. 즉각적인 주의가 필요한 성능 또는 고객 경험이 크게 저하된 경우에만 경보가 경보 상태로 전환되도록 경보를 구성해야 합니다. 일부 주요 경보 유형에는 비즈니스 영향을 나타내는 경보, Amazon CloudWatch canary 및 종속성을 모니터링하는 집계 경보가 포함됩니다.

경보 수집을 시작하려면 경보 수집 및 경보 수집 설문지 를 참조하세요.

> **Note**
>
> 실행서, 워크로드 정보 또는 AWS 인시던트 감지 및 대응에서 모니터링되는 경보를 변경하려면 섹션을 참조하세요인시던트 감지 및 대응에서 온보딩된 워크로드에 대한 변경 요청.

인시던트 감지 및 대응에 온보딩

AWS 는 사용자와 협력하여 워크로드 및 경보를 AWS 인시던트 감지 및 대응에 온보딩합니다. AWS 에서 에 주요 정보를 제공합니다인시던트 감지 및 대응의 워크로드 온보딩 및 경보 수집 설문지. 워크로드를 에 등록하는 것이 가장 좋습니다 AppRegistry. 자세한 내용은 AppRegistry 사용 설명서 섹션을 참조하세요.

다음 다이어그램은 인시던트 감지 및 대응에서 워크로드 온보딩 및 경보 수집의 흐름을 보여줍니다.

워크로드 온보딩

워크로드 온보딩 중에 는 사용자와 AWS 협력하여 워크로드와 인시던트 및 AWS 서비스 이벤트 중에를 지원하는 방법을 파악합니다. 영향 완화를 지원하는 워크로드에 대한 주요 정보를 제공합니다.

키 출력:

- 일반 워크로드 정보
- 다이어그램을 포함한 아키텍처 세부 정보
- 런북 정보
- 고객 주도 인시던트
- AWS 서비스 이벤트

경보 수집

AWS 는 사용자와 협력하여 경보를 온보딩합니다. AWS 인시던트 감지 및 대응은 Amazon 를 통해 Amazon CloudWatch 및 타사 애플리케이션 성능 모니터링(APM) 도구에서 경보를 수집할 수 있습니다 EventBridge. 온보딩 경보를 사용하면 사전 예방적인 인시던트 감지 및 자동 참여를 수행할 수 있습니다. 자세한 내용은 Amazon 와 직접 통합APMs되는 에서 경보 수신 EventBridge을 참조하세요.

키 출력:

- 경보 매트릭스

다음 표에는 워크로드를 AWS 인시던트 감지 및 대응에 온보딩하는 데 필요한 단계가 나열되어 있습니다. 이 표에는 각 작업의 기간이 예제로 나와 있습니다. 각 작업의 실제 날짜는 팀 및 일정의 가용성에 따라 정의됩니다.

인시던트 감지 및 대응의 워크로드 온보딩 및 경보 수집 설문지

이 페이지에서는 워크로드를 AWS 인시던트 감지 및 대응에 온보딩하고 서비스에 수집하도록 경보를 구성할 때 완료해야 하는 설문지를 제공합니다. 워크로드 온보딩 설문지는 워크로드, 아키텍처 세부 정보 및 인시던트 대응 연락에 대한 일반적인 정보를 다룹니다. 경보 수집 설문지에서는 워크로드에 대한 인시던트 감지 및 대응에서 인시던트 생성을 트리거해야 하는 중요한 경보와 누구에게 연락해야 하는지, 어떤 조치를 취해야 하는지에 대한 런북 정보를 지정합니다. 이러한 설문지를 올바르게 작성하는 것은 AWS 워크로드에 대한 모니터링 및 인시던트 대응 프로세스를 설정하는 데 중요한 단계입니다.

워크로드 온보딩 설문지 를 다운로드합니다.

경보 수집 설문지 를 다운로드합니다.

워크로드 온보딩 설문지 - 일반 질문

일반 질문

질문	응답의 예
엔터프라이즈 이름	Amazon Inc.
이 워크로드의 이름(약어 포함)	Amazon Retail Operations(ARO)
기본 최종 사용자 및 이 워크로드의 함수입니다.	이 워크로드는 최종 사용자가 다양한 항목을 구매할 수 있는 전자 상거래 애플리케이션입니다. 이 워크로드는 비즈니스의 주요 수익 창출자입니다.
이 워크로드에 적용되는 규정 준수 및/또는 규제 요구 사항과 인시던트 AWS 후 에서 필요한 모든 작업.	워크로드는 보안 및 기밀을 유지해야 하는 환자 건강 기록을 처리합니다.

워크로드 온보딩 설문지 - 아키텍처 질문

아키텍처 질문

질문	응답의 예
이 워크로드의 일부인 리소스를 정의하는 데 사용되는 AWS 리소스 태그 목록입니다. 는 이러한 태그를 AWS 사용하여 이 워크로드의 리소스를 식별하여 인시던트 발생 시 지원을 신속하게 처리합니다. **Note** 태그는 대/소문자를 구분합니다. 여러 태그를 제공하는 경우 이 워크로드에서 사용하는 모든 리소스에 동일한 태그가 있어야 합니다.	appName: Optimax 환경: 프로덕션
이 워크로드에서 사용하는 AWS 서비스 목록과 해당 워크로드가 속한 AWS 계정 및 리전입니다. **Note** 각 서비스에 대해 새 행을 생성합니다.	Route 53: 인터넷 트래픽을 로 라우팅합니다 ALB. 계정:123456789101 리전: US-EAST-1, US-WEST-2
이 워크로드에서 사용하는 AWS 서비스 목록과 해당 워크로드가 속한 AWS 계정 및 리전입니다. **Note** 각 서비스에 대해 새 행을 생성합니다.	ALB: 수신 트래픽을 대상 ECS 컨테이너 그룹으로 라우팅합니다. 계정: 123456789101 리전: 해당 없음

질문	응답의 예
이 워크로드에서 사용하는 AWS 서비스 목록과 해당 워크로드가 속한 AWS 계정 및 리전입니다. Note 각 서비스에 대해 새 행을 생성합니다.	ECS: 기본 비즈니스 로직 플릿의 컴퓨팅 인프라입니다. 들어오는 사용자 요청을 처리하고 지속성 계층에 쿼리를 수행할 책임이 있습니다. 계정: 123456789101 리전: US-EAST-1
이 워크로드에서 사용하는 AWS 서비스 목록과 해당 워크로드가 속한 AWS 계정 및 리전입니다. Note 각 서비스에 대해 새 행을 생성합니다.	RDS: Amazon Aurora 클러스터는 ECS 비즈니스 로직 계층에서 액세스하는 사용자 데이터를 저장합니다. 계정: 123456789101 리전: US-EAST-1
이 워크로드에서 사용하는 AWS 서비스 목록과 해당 워크로드가 속한 AWS 계정 및 리전입니다. Note 각 서비스에 대해 새 행을 생성합니다.	S3: 웹 사이트 정적 자산을 저장합니다. 계정: 123456789101 리전: 해당 없음
중단이 발생할 경우 이 워크로드에 영향을 미칠 수 있는 온보딩되지 않은 업스트림/다운스트림 구성 요소를 자세히 설명합니다.	인증 마이크로서비스: 사용자가 인증되지 않을 때 상태 레코드를 로드하지 못하게 합니다.
이 워크로드에 온프레미스 또는 비AWS 구성 요소가 있습니까? 그렇다면 어떤 함수가 수행됩니까?	의 모든 인터넷 기반 트래픽 AWS 은 온프레미스 프록시 서비스를 통해 라우팅됩니다.
가용 영역 및 리전 수준에서 수동 또는 자동 장애 조치/재해 복구 계획에 대한 세부 정보를 제공합니다.	웜 스탠바이. 성공률이 지속적으로 저하되는 동안 US-WEST-2로의 자동 장애 조치.

워크로드 온보딩 설문지 - AWS 서비스 이벤트 질문

AWS 서비스 이벤트 질문

질문	응답의 예
회사 내부 주요 인시던트/IT 위기 관리 팀의 연락처 세부 정보(이름/이메일/전화)를 입력합니다.	주요 인시던트 관리 팀 mim@example.com +61 2 3456 7890
회사에서 설정한 정적 인시던트/위기 관리 브리지에 대한 세부 정보를 제공합니다. 비정적 브리지를 사용하는 경우 원하는 애플리케이션을 지정 AWS 하면 인시던트 중에 이러한 세부 정보를 요청합니다. **Note** 제공되지 않으면 AWS 는 인시던트 중에에 연락하여 조인할 Chime 브리지를 제공합니다.	Amazon Chime https://chime.aws/1234567890

경보 수집 설문지

런북 질문

질문	응답의 예
AWS 는 AWS Support 사례를 통해 워크로드 컨택을 참여시킵니다. 이 워크로드에 대해 경보가 트리거될 때 기본 연락처는 누구입니까? 선호하는 회의 애플리케이션을 지정 AWS 하면 인시던트 중에 이러한 세부 정보를 요청합니다.	애플리케이션 팀 app@example.com +61 2 3456 7890

질문	응답의 예
Note 기본 다자간 통화 애플리케이션이 제공되지 않은 경우 AWS 는 인시던트 중에 에 연락하여 조인할 수 있는 Chime 브리지를 제공합니다.	
인시던트 중에 기본 연락처를 사용할 수 없는 경우 선호하는 커뮤니케이션 순서로 에스컬레이션 연락처와 타임라인을 제공하십시오.	1. 10분 후 기본 연락처의 응답이 없는 경우 다음을 수행합니다. John Smith - 애플리케이션 감독자 john.smith@example.com +61 2 3456 7890 2. 10분 후 John Smith의 응답이 없는 경우 다음으로 문의하세요. Jane Smith - 운영 관리자 jane.smith@example.com +61 2 3456 7890
AWS 는 인시던트 전반에 걸쳐 정기적으로 지원 사례를 통해 업데이트를 전달합니다. 이러한 업데이트를 받아야 하는 추가 연락처가 있습니까?	john.smith@example.com, jane.smith@example.com

경보 매트릭스

다음 정보를 제공하여 워크로드를 대신하여 인시던트를 생성하기 위해 AWS 인시던트 감지 및 대응을 사용하는 경보 세트를 식별합니다. AWS 인시던트 감지 및 대응의 엔지니어가 경보를 검토하면 추가 온보딩 단계가 제공됩니다.

AWS 인시던트 감지 및 대응 중요 경보 기준:

- AWS 인시던트 감지 및 대응 경보는 즉각적인 운영자 주의가 필요한 모니터링된 워크로드(수익 손실/고객 경험 저하)에 상당한 비즈니스 영향이 있을 때만 “경보” 상태로 전환되어야 합니다.
- AWS 인시던트 감지 및 대응 경보는 동시에 또는 참여 전에 워크로드에 대한 해석기를 참여시켜야 합니다. AWS 인시던트 관리자는 완화 프로세스에서 해결사와 협력하며, 1차 대응 담당자 역할을 하지 않으며, 대응 담당자는 이를 상부에 보고합니다.
- AWS 사고 감지 및 대응 경보 임계값은 경보가 조사를 시작할 때마다 발생할 수 있도록 적절한 임계값 및 기간으로 설정되어야 합니다. 경보가 “경보”와 “확인” 상태 사이에서 이동하는 경우 작업자의 응답과 주의를 끌기에 충분한 영향이 발생합니다.

AWS 기준 위반에 대한 인시던트 탐지 및 대응 정책:

이러한 기준은 이벤트가 case-by-case 발생할 때만 평가할 수 있습니다. Incident Management 팀은 기술 계정 관리자(TAMs)와 협력하여 경보를 조정하고, 드물게 고객 경보가 이 기준을 준수하지 않는 것으로 의심되고 인시던트 관리 팀을 정기적으로 참여시키는 경우 모니터링을 비활성화합니다.

> **Important**
>
> 연락처 주소를 제공할 때 그룹 배포 이메일 주소를 제공하여 실행서 업데이트 없이 수신자 추가 및 삭제를 제어할 수 있습니다.
> 초기 참여 이메일을 보낸 후 AWS 인시던트 감지 및 대응 팀이 전화를 걸도록 하려면 사이트 신뢰성 엔지니어링(SRE) 팀의 연락 전화번호를 입력합니다.

경보 매트릭스 테이블

지표 이름 / ARN / 임계값	설명	참고	요청된 작업
워크로드 볼륨 / *CW Alarm ARN* / CallCount 5분 이내에 5개의 데이터 포인트에 대해 < 100000, 누락된 데이터를 누락으로 처리	이 지표는 Application Load Balancer 수준에서 측정된 워크로드로 들어오는 수신 요청 수를 나타냅니다. 이 경보는 수신 요청의 상당한 저하가 업스트림 네트워크 연결 문제 또는 사용자가 워크로	지난 주에 경보가 '경보' 상태로 10회 들어갔습니다. 이 경보는 오탐의 위험이 있습니다. 임계값 검토가 계획되어 있습니다. 문제가 있습니까? 아니요 또는 예(아니요인 경우 비워 두세요): 이	에 이메일을 보내 Site Reliability Engineering 팀을 참여시킵니다.*SRE@xyz.com* ELB, 및 Route 53 서비스에 대한 AWS 사전 지원 사례를 생성합니다.

지표 이름 / ARN / 임계값	설명	참고	요청된 작업
	드에 액세스할 수 없게 만드는 DNS 구현 문제를 나타낼 수 있기 때문에 중요합니다.	경보는 특정 배치 작업 실행 중에 자주 뒤집힙니다. 해석기: 사이트 신뢰성 엔지니어	IMMEDIATE 작업이 필요한 경우: EC2 여유 메모리/디스크 공간을 확인하고 *XYZ* 이메일을 통해 팀을 구성하여 인스턴스를 다시 시작하거나 로그 플러시를 실행합니다(즉각적인 작업이 필요하지 않은 경우 비워 둡니다).
워크로드 요청 지연 시간 / *CW Alarm ARN* / 5분 이내에 5개의 데이터 포인트에 대해 p90 지연 시간 > 100ms, 누락된 데이터를 누락으로 처리	이 지표는 워크로드가 수행할 HTTP 요청에 대한 p90 지연 시간을 나타냅니다. 이 경보는 지연 시간을 나타냅니다(웹사이트의 고객 경험에 대한 중요한 측정치).	지난 주에 경보가 '알람' 상태로 0회 들어갔습니다. 문제가 있습니까? 아니요 또는 예(아니요인 경우 비워 두세요): 이 경보는 특정 배치 작업 실행 중에 자주 뒤집힙니다. 해석기: 사이트 신뢰성 엔지니어	에 이메일을 보내 Site Reliability Engineering 팀을 참여시킵니다.*SRE@xyz.com* ECW, 및 RDS 서비스에 대한 AWS 사전 지원 사례를 생성합니다. IMMEDIATE 작업이 필요한 경우: EC2 여유 메모리/디스크 공간을 확인하고 *XYZ* 이메일을 통해 팀을 구성하여 인스턴스를 다시 시작하거나 로그 플러시를 실행합니다(즉각적인 작업이 필요하지 않은 경우 비워 둡니다).

지표 이름 / ARN / 임계값	설명	참고	요청된 작업
워크로드 요청 가용성 / *CW Alarm ARN* / 5분 이내에 5개의 데이터 포인트에 대해 가용성 < 95%인 경우 누락된 데이터를 누락된 것으로 취급합니다.	이 지표는 워크로드에서 수행할 HTTP 요청의 가용성을 나타냅니다(HTTP200개 수/요청 수). 이 경보는 워크로드의 가용성을 나타냅니다.	지난 주에 경보가 '알람' 상태로 0회 들어갔습니다. 문제가 있습니까? 아니요 또는 예(아니요인 경우 비워둠): 이 경보는 특정 배치 작업 실행 중에 자주 뒤집힙니다. 해석기: 사이트 신뢰성 엔지니어	에 이메일을 보내 Site Reliability Engineering 팀을 참여시킵니다.*SRE@xyz.com* ELB, 및 Route 53 서비스에 대한 AWS 사전 지원 사례를 생성합니다. IMMEDIATE 작업이 필요한 경우: EC2 여유 메모리/디스크 공간을 확인하고 *XYZ* 이메일을 통해 팀을 구성하여 인스턴스를 다시 시작하거나 로그 플러시를 실행합니다(즉각적인 작업이 필요하지 않은 경우 비워 둡니다).
새 복제 경보 예제			

지표 이름 / ARN / 임계값	설명	참고	요청된 작업
엔드 투 엔드 통합 테스트 / *CW Alarm ARN* / 3분 동안 1분 지표에 대한 3% 실패율, 누락된 데이터를 누락으로 처리 워크로드 식별자: 엔드 투 엔드 테스트 워크플로, AWS 리전: US-EAST-1, AWS 계정 ID: 012345678910	이 지표는 요청이 워크로드의 각 계층을 통과할 수 있는지 테스트합니다. 이 테스트가 실패하면 비즈니스 트랜잭션을 처리하는 데 심각한 실패를 나타냅니다. 이 경보는 워크로드에 대한 비즈니스 트랜잭션을 처리하는 기능을 나타냅니다.	지난 주에 경보가 '경보' 상태로 0회 들어갔습니다. 문제가 있습니까? 아니요 또는 예(아니요인 경우 비워둠): 이 경보는 특정 배치 작업 실행 중에 자주 뒤집힙니다. 해석기: 사이트 신뢰성 엔지니어	에 이메일을 보내 Site Reliability Engineering 팀을 참여시킵니다.*SRE@xyz.com* ECS, 및 DynamoDB 서비스에 대한 AWS 사전 지원 사례를 생성합니다. IMMEDIATE 작업이 필요한 경우: EC2 여유 메모리/디스크 공간을 확인하고 *XYZ* 이메일을 통해 팀을 구성하여 인스턴스를 다시 시작하거나 로그 플러시를 실행합니다(즉각적인 작업이 필요하지 않은 경우 비워 둡니다).

인시던트 감지 및 대응의 워크로드 검색

AWS 는 사용자와 협력하여 워크로드에 대한 컨텍스트를 최대한 이해합니다. AWS 인시던트 감지 및 대응은 이 정보를 사용하여 인시던트 및 AWS 서비스 이벤트 중에 런북을 생성하여 사용자를 지원합니다. 필수 정보는 에 캡처됩니다인시던트 감지 및 대응의 워크로드 온보딩 및 경보 수집 설문지. 워크로드를 에 등록하는 것이 가장 좋습니다 AppRegistry. 자세한 내용은 AppRegistry 사용 설명서 섹션을 참조하세요.

키 출력:

- 워크로드의 설명, 아키텍처 다이어그램, 연락처 및 에스컬레이션 세부 정보와 같은 워크로드 정보입니다.
- 워크로드가 각 AWS 리전에서 AWS 서비스를 사용하는 방법에 대한 세부 정보입니다.

- 서비스 이벤트 중에 가 사용자를 AWS 지원하는 방법에 대한 특정 정보입니다.
- 중요한 워크로드 영향을 감지하는 팀이 사용하는 경보입니다.

인시던트 감지 및 대응에 워크로드 구독

AWS 인시던트 감지 및 대응에 워크로드를 구독하려면 각 워크로드에 대한 새 지원 사례를 생성합니다. 지원 사례를 생성할 때는 다음 사항에 유의하세요.

- 단일 AWS 계정에 있는 워크로드를 온보딩하려면 워크로드 계정 또는 지불자 계정에서 지원 사례를 생성합니다.
- 여러 AWS 계정에 걸쳐 있는 워크로드를 온보딩하려면 지급자 계정 에서 지원 사례를 생성합니다. 지원 사례 본문에 온보딩IDs할 모든 계정을 나열합니다.

> **Important**
>
> 잘못된 계정에서 인시던트 감지 및 대응에 대한 워크로드를 구독하는 지원 사례를 생성하는 경우 워크로드를 구독하기 전에 지연 및 추가 정보 요청이 발생할 수 있습니다.

워크로드를 구독하려면

1. AWS Support 센터 로 이동한 다음 다음 예제와 같이 사례 생성을 선택합니다. Enterprise Support에 등록된 계정에서만 워크로드를 구독할 수 있습니다.

2. 지원 사례 양식을 작성합니다.
   - 기술 지원 을 선택합니다.
   - 서비스 에서 인시던트 감지 및 응답 을 선택합니다.
   - 범주 에서 온보딩 새 워크로드 를 선택합니다.
   - 심각도 에서 일반 지침 을 선택합니다.
3. 이 변경 사항에 대한 주제를 입력합니다. 예:

   [온보드] AWS 인시던트 감지 및 대응 - *workload_name*
4. 이 변경 사항에 대한 설명을 입력합니다. 예를 들어 '이 요청은 워크로드를 AWS 인시던트 감지 및 대응에 온보딩하기 위한 것입니다'를 입력합니다. 요청에 다음 정보를 포함해야 합니다.

- 워크로드 이름: 워크로드 이름입니다.
- 계정 ID(들): ID1, ID2ID3, 등. 다음은 AWS 인시던트 감지 및 대응에 온보딩하려는 계정입니다.
- 구독 시작 날짜: AWS Incident Detection and Response 구독을 시작하려는 날짜입니다.

5. 추가 연락처 - 선택 사항 섹션에서 이 요청에 대한 서신을 수신IDs하려는 이메일을 입력합니다.

   다음은 추가 연락처 - 선택적 섹션의 예입니다.

> **Important**
>
> 추가 연락처 IDs - 선택 사항 섹션에 이메일을 추가하지 않으면 AWS 인시던트 감지 및 대응 온보딩 프로세스가 지연될 수 있습니다.

6. 제출을 선택합니다.

   요청을 제출한 후 조직의 이메일을 추가할 수 있습니다. 이메일을 추가하려면 사례에 회신한 다음 IDs 추가 연락처 - 선택 사항 섹션에 이메일을 추가합니다.

   다음은 추가 연락처 - 선택적 섹션의 예입니다.

구독 요청에 대한 지원 사례를 생성한 후 워크로드 온보딩 프로세스를 진행할 수 있도록 다음 두 문서를 준비해 둡니다.

- AWS 워크로드 아키텍처 다이어그램.
- 인시던트 감지 및 대응의 워크로드 온보딩 및 경보 수집 설문지: 온보딩 중인 워크로드와 관련된 설문지의 모든 정보를 작성합니다. 온보딩할 워크로드가 여러 개 있는 경우 각 워크로드에 대해 새 온보딩 설문지를 생성합니다. 온보딩 설문지 작성에 대한 질문이 있는 경우 기술 계정 관리자()에게 문의하세요TAM.

> **Note**
>
> 파일 NOT 연결 옵션을 사용하여 이 두 문서를 사례에 연결합니다. AWS 인시던트 감지 및 대응 팀은 문서를 업로드할 수 있도록 Amazon Simple Storage Service Uploader 링크를 사용하여 사례에 회신합니다.

기존 온보딩 워크로드에 대한 변경을 요청하는 AWS 인시던트 감지 및 대응으로 사례를 생성하는 방법에 대한 자세한 내용은 섹션을 참조하세요인시던트 감지 및 대응에서 온보딩된 워크로드에 대한 변경 요청. 워크로드를 오프보드하는 방법에 대한 자세한 내용은 섹션을 참조하세요인시던트 감지 및 대응에서 워크로드 오프보드.

인시던트 감지 및 대응에서 경보 정의 및 구성

AWS 는 사용자와 협력하여 지표 및 경보를 정의하여 애플리케이션 및 기본 AWS 인프라의 성능에 대한 가시성을 제공합니다. 임계값을 정의하고 구성할 때 경보가 다음 기준을 준수하도록 요청합니다.

- 경보는 작업자의 즉각적인 주의가 필요한 모니터링된 워크로드(수익 손실 또는 성능을 크게 저하시키는 고객 경험 저하)에 중대한 영향이 있는 경우에만 “경보” 상태로 전환됩니다.
- 또한 경보는 인시던트 관리 팀을 참여시키기 전에 워크로드에 대해 지정된 해석기를 동시에 참여시켜야 합니다. 인시던트 관리 엔지니어는 완화 프로세스에서 지정된 해결 담당자와 협력해야 하며, 1차 대응 담당자 역할을 하지 않고 에스컬레이션해야 합니다.
- 경보 임계값은 경보가 발생할 때마다 조사가 이루어지도록 적절한 임계값 및 기간으로 설정되어야 합니다. 경보가 “경보”와 “OK” 상태 사이에서 플래핑되는 경우 작업자의 응답과 주의를 끌기에 충분한 영향이 발생합니다.

경보 유형:

- 비즈니스 영향 수준을 표현하고 간단한 장애 감지를 위해 관련 정보를 전달하는 경보입니다.
- Amazon CloudWatch canary. 자세한 내용은 Canaries 및 X-Ray 추적 , X-Ray 를 참조하세요.
- 집계 경보(종속성 모니터링)

다음 표에서는 CloudWatch 모니터링 시스템을 사용하는 경보의 예를 제공합니다.

지표 이름/알람 임계값	경보 ARN 또는 리소스 ID	이 경보가 발사되는 경우	참여하는 경우 이러한 서비스에 대한 프리미엄 지원 사례를 잘라냅니다.
API 오류 / 10개의 데이터 포인트에 대해 오류 수 >= 10	arn:aws:cloudwatch:us-west-2:000000000000:alarm:E2MPmimLambda-Errors	데이터베이스 관리자(DBA) 팀으로 티켓 잘라내기	Lambda, API 게이트웨이
ServiceUnavailable (Http 상태 코드 503) 5분 기간 내 10개의 데이터 포인트(다른 클라이언트)에 대한 오류 수 >=3	arn:aws:cloudwatch:us-west-2:xxxxx:alarm:httperrorcode503	서비스 팀으로 티켓 자르기	Lambda, API 게이트웨이
ThrottlingException (Http 상태 코드 400) 5분 기간 내 10개의 데이터 포인트(다른 클라이언트)에 대한 오류 수 >=3	arn:aws:cloudwatch:us-west-2:xxxxx:alarm:httperrorcode400	서비스 팀으로 티켓 자르기	EC2, Amazon Aurora

자세한 내용은 AWS 인시던트 감지 및 대응 모니터링 및 관찰 가능성를 참조하세요.

키 출력:

- 워크로드에 대한 경보의 정의 및 구성.

- 온보딩 설문지의 경보 세부 정보 작성.

주제

인시던트 감지 및 대응에서 비즈니스 요구 사항에 맞는 CloudWatch 경보 생성

Amazon CloudWatch 경보를 생성할 때 경보가 비즈니스 요구 사항에 가장 잘 맞도록 하기 위해 취할 수 있는 몇 가지 단계가 있습니다.

제안된 CloudWatch 경보 검토

제안된 경보를 검토하여 모니터링되는 워크로드에 중대한 영향(수입 손실 또는 성능 저하를 초래하는 고객 경험 저하)이 있을 때만 '경보' 상태로 전환되는지 확인합니다. 예를 들어 이 경보가 '경보' 상태로 전환되는 경우 즉시 대응해야 할 만큼 이 경보가 중요하다고 생각하십니까?

다음은 애플리케이션에 대한 최종 사용자의 경험에 영향을 미치는 등 중요한 비즈니스 영향을 나타낼 수 있는 권장 지표입니다.

- CloudFront: 자세한 내용은 보기 CloudFront 및 엣지 함수 지표를 참조하세요.
- Application Load Balancer: 가능하면 Application Load Balancer에 대해 다음 경보를 생성하는 것이 좋습니다.
  - HTTPCode_ELB_5XX_카운트
  - HTTPCode_대상_5XX_수

  앞의 경보를 사용하면 Application Load Balancer 또는 다른 리소스 뒤에 있는 대상의 응답을 모니터링할 수 있습니다. 이렇게 하면 5XX 오류의 원인을 더 쉽게 식별할 수 있습니다. 자세한 내용은 CloudWatch Application Load Balancer 의 지표를 참조하세요.
- Amazon API Gateway: Elastic Beanstalk에서 를 사용하는 WebSocket API 경우 다음 지표를 사용하는 것이 좋습니다.
  - 통합 오류율(5XX 오류로 필터링됨)
  - 통합 지연 시간
  - 실행 오류

자세한 내용은 CloudWatch 지표를 사용하여 실행 모니터링을 WebSocket API 참조하세요.

- Amazon Route 53: EndPointUnhealthyENICount 지표를 모니터링합니다. 이 지표는 자동 복구 상태의 탄력적 네트워크 인터페이스 수입니다. 이 상태는 확인자가 엔드포인트와 연결된 Amazon Virtual Private Cloud 네트워크 인터페이스 중 하나 이상을 복구하려고 시도했음을 나타냅니다(에 의해 지정됨EndpointId). 복구 프로세스에서 엔드포인트는 제한된 용량으로 작동합니다. 엔드포인트는 완전히 복구될 때까지 DNS 쿼리를 처리할 수 없습니다. 자세한 내용은 Amazon 을 사용하여 Route 53 Resolver 엔드포인트 모니터링을 CloudWatch 참조하세요.

경보 구성 검증

제안된 경보가 비즈니스 요구 사항에 맞는지 확인한 후 경보의 구성 및 기록을 확인합니다.

- 지표의 임계값을 검증하여 지표의 그래프 추세에 대해 “경보” 상태로 전환합니다.
- 데이터 포인트를 폴링하는 데 사용되는 기간을 확인합니다. 60초에 데이터 포인트를 폴링하면 인시던트를 조기에 감지하는 데 도움이 됩니다.
- DatapointToAlarm 구성을 확인합니다. 대부분의 경우 이를 3/3 또는 5/5로 설정하는 것이 가장 좋습니다. 인시던트에서 경보는 [3/3의 60초 지표 DatapointToAlarm]로 설정하면 3분 후에 트리거되고 [5/5의 60초 지표]로 설정하면 5분 후에 트리거됩니다 DatapointToAlarm. 이 조합을 사용하여 소음 경보를 제거합니다.

> **Note**
>
> 위의 권장 사항은 서비스 사용 방식에 따라 달라질 수 있습니다. 각 AWS 서비스는 워크로드 내에서 다르게 작동합니다. 또한 여러 곳에서 사용할 때 동일한 서비스가 다르게 작동할 수 있습니다. 워크로드가 경보를 공급하는 리소스와 업스트림 및 다운스트림 효과를 어떻게 활용하는지 이해해야 합니다.

경보가 누락된 데이터를 처리하는 방법 검증

일부 지표 소스는 정기적으로 CloudWatch 에 데이터를 전송하지 않습니다. 이러한 지표의 경우 누락된 데이터를 로 처리하는 것이 가장 좋습니다notBreaching. 자세한 내용은 CloudWatch 경보가 누락된 데이터를 처리하는 방법 구성 및 경보 상태로의 조기 전환 방지를 참조하세요.

예를 들어 지표가 오류율을 모니터링하고 오류가 없는 경우 지표는 데이터(nil) 데이터 포인트를 보고하지 않습니다. 누락된 데이터를 누락으로 처리하도록 경보를 구성하면 위반 데이터 포인트가 하나 있고

데이터 없음(nil) 데이터 포인트가 두 개 있으면 지표가 '알람' 상태로 전환됩니다(3개 데이터 포인트 중 3개). 이는 누락된 데이터 구성이 평가 기간의 마지막으로 알려진 데이터 포인트를 평가하기 때문입니다.

지표가 오류율을 모니터링하는 경우 서비스 성능 저하가 없으면 데이터가 좋지 않다고 가정할 수 있습니다. 누락된 데이터를 'OK'로 취급하고 지표가 단일 데이터 포인트에서 '알람' 상태로 들어가지 notBreaching 않도록 하려면 누락된 데이터를 처리하는 것이 가장 좋습니다.

각 경보의 기록 검토

경보의 기록에 자주 “경보” 상태로 전환된 다음 빠르게 복구되는 것으로 표시되면 경보가 문제가 될 수 있습니다. 경보를 조정하여 노이즈 또는 거짓 경보를 방지해야 합니다.

기본 리소스에 대한 지표 검증

지표가 유효한 기본 리소스를 살펴보고 올바른 통계를 사용해야 합니다. 잘못된 리소스 이름을 검토하도록 경보가 구성된 경우 경보가 기본 데이터를 추적하지 못할 수 있습니다. 이로 인해 경보가 “경보” 상태가 될 수 있습니다.

복합 경보 생성

온보딩을 위해 많은 수의 경보가 포함된 인시던트 감지 및 대응 작업을 제공하는 경우 복합 경보를 생성하라는 메시지가 표시될 수 있습니다. 복합 경보는 온보딩해야 하는 총 경보 수를 줄입니다.

CloudFormation 템플릿을 사용하여 인시던트 감지 및 대응에서 CloudWatch 경보 빌드

AWS 인시던트 탐지 및 대응에 대한 온보딩을 가속화하고 경보를 구축하는 데 필요한 노력을 줄이기 위해 는 AWS CloudFormation 템플릿을 AWS 제공합니다. 이러한 템플릿에는 Application Load Balancer , Network Load Balancer 및 Amazon 과 같이 일반적으로 온보딩되는 서비스에 대해 최적화된 경보 설정이 포함되어 있습니다 CloudFront.

CloudFormation 템플릿을 사용하여 CloudWatch 경보 빌드

1. 제공된 링크를 사용하여 템플릿을 다운로드합니다.

NameSpac	지표	Compariso nOperator (임계값)	기간	DatapoinT sToAlarm	TreatMiss ingData	통계	템플릿 링크
Applicati on Elastic Load Balancer	(m1+m2)/ (m1+m2+m m4)*100 m1=HTTP(de_Target _2XX_Cou t m2=HTTP(de_Target _3XX_Cou t m3=HTTP(de_Target _4XX_Cou t m4=HTTP(de_Target _5XX_Cou t	LessThanT hreshold(95)	60	3/3	누락	Sum	템플릿
Amazon CloudFron t	TotalErro rRate	GreaterTh anThresho ld(5)	60	3/3	notBreach ing	평균	템플릿
Applicati on Elastic Load Balancer	UnHealthy HostCount	GreaterTh anOrEqual ToThresho ld(2)	60	3/3	notBreach ing	Maximum	템플릿

NameSpac	지표	Compariso nOperator (임계값)	기간	Datapoint sToAlarm	TreatMiss ingData	통계	템플릿 링크
Network Elastic Load Balancer	UnHealthy HostCount	GreaterTh anOrEqual ToThresho ld(2)	60	3/3	notBreach ing	Maximum	템플릿

2. 다운로드한 JSON 파일을 검토하여 조직의 운영 및 보안 프로세스를 충족하는지 확인합니다.
3. CloudFormation 스택 생성:

> **Note**
>
> 다음 단계에서는 표준 CloudFormation 스택 생성 프로세스를 사용합니다. 자세한 단계는 AWS CloudFormation 콘솔에서 스택 생성을 참조하세요.

a. https://console.aws.amazon.com/cloudformation에서 AWS CloudFormation 콘솔을 엽니다.
b. 스택 생성을 선택합니다.
c. 템플릿 준비 완료 를 선택한 다음 로컬 폴더에서 템플릿 파일을 업로드합니다.

   다음은 스택 생성 화면의 예입니다.

d. Next(다음)를 선택합니다.
e. 다음 필수 정보를 입력합니다.

   - AlarmNameConfig 및 AlarmDescriptionConfig: 경보의 이름과 설명을 입력합니다.
   - ThresholdConfig: 애플리케이션의 요구 사항에 맞게 임계값을 수정합니다.
   - D istributionIDConfig: 배포 ID가 AWS CloudFormation 스택을 생성하려는 계정의 올바른 리소스를 가리키는지 확인합니다.

f. Next(다음)를 선택합니다.

g. PeriodConfig, EvalutionPeriodConfig및 DatapointsToAlarmConfig 필드의 기본값을 검토합니다. 이러한 필드의 기본값을 사용하는 것이 가장 좋습니다. 필요한 경우 애플리케이션의 요구 사항에 맞게 조정할 수 있습니다.

h. 필요에 따라 태그 및 SNS 알림 정보를 선택적으로 입력합니다. 경보가 실수로 삭제되지 않도록 종료 방지 기능을 켜는 것이 가장 좋습니다. 종료 방지 기능을 켜려면 다음 예제와 같이 활성화된 라디오 버튼을 선택합니다.

i. Next(다음)를 선택합니다.

j. 스택 설정을 검토한 다음 스택 생성 을 선택합니다.

k. 스택을 생성한 후 다음 예제와 같이 Amazon 경보 목록에 CloudWatch 경보가 나열됩니다.

4. 올바른 계정 및 AWS 리전에서 모든 경보를 생성한 후 기술 계정 관리자()에게 알립니다TAM. AWS 인시던트 감지 및 대응 팀은 새 경보의 상태를 검토한 다음 온보딩을 계속합니다.

인시던트 감지 및 대응의 CloudWatch 경보 사용 사례 예

다음 사용 사례는 인시던트 감지 및 대응에서 Amazon CloudWatch 경보를 사용하는 방법의 예를 제공합니다. 이 예제에서는 다양한 AWS 서비스에서 주요 지표와 임계값을 모니터링하도록 CloudWatch 경보를 구성하여 애플리케이션 및 워크로드의 가용성과 성능에 영향을 미칠 수 있는 잠재적 문제를 식별하고 대응할 수 있는 방법을 보여줍니다.

예제 사용 사례 A: Application Load Balancer

잠재적 워크로드 영향을 알리는 다음 CloudWatch 경보를 생성할 수 있습니다. 이렇게 하려면 연결 성공이 특정 임계값 아래로 떨어질 때 경보를 울리는 지표 수학을 생성합니다. 사용 가능한 CloudWatch 지표는 CloudWatch Application Load Balancer의 지표를 참조하세요.

지
표:HTTPCode_Target_3XX_Count;HTTPCode_Target_4XX_Count;HTTPCode_Target_5XX_Count.
(m1+m2)/(m1+m2+m3+m4)*100 m1 = HTTP Code 2xx || m2 = HTTP Code 3xx || m3 = HTTP Code 4xx || m4 = HTTP Code 5xx

NameSpace: AWS/애플리케이션ELB

ComparisonOperator(임계값): x 미만(x = 고객의 임계값).

기간: 60초

DatapointsToAlarm: 3/3

누락된 데이터 처리: 누락된 데이터를 위반으로 처리합니다.

통계: Sum

다음 다이어그램은 사용 사례 A의 흐름을 보여줍니다.

예제 사용 사례 B: Amazon API Gateway

잠재적 워크로드 영향을 알리는 다음 CloudWatch 경보를 생성할 수 있습니다. 이렇게 하려면 API Gateway에서 지연 시간이 높거나 평균 4XX개 오류 수가 높을 때 경보를 올리는 복합 지표를 생성합니다. 사용 가능한 지표는 Amazon API Gateway 차원 및 지표를 참조하세요.

지표:`compositeAlarmAPI Gateway (ALARM(error4XXMetricApiGatewayAlarm)) OR (AALARM(latencyMetricApiGatewayAlarm))`

NameSpace: AWS/API 게이트웨이

ComparisonOperator(임계값): 보다 큼(x 또는 y 고객의 임계값)

기간: 60초

DatapointsToAlarm: 1/1

누락된 데이터 처리: 누락된 데이터를 위반하지 않는 것으로 처리합니다.

통계:

다음 다이어그램은 사용 사례 B의 흐름을 보여줍니다.

예제 사용 사례 C: Amazon Route 53

CloudWatch 를 사용하여 원시 데이터를 수집하고 읽기 가능한 실시간에 가까운 지표로 처리하는 Route 53 상태 확인을 생성하여 리소스를 모니터링할 수 있습니다. 잠재적 워크로드 영향을 알리는 다음 CloudWatch 경보를 생성할 수 있습니다. CloudWatch 지표를 사용하여 설정된 임계값을 위반할 때 트리거되는 경보를 생성할 수 있습니다. 사용 가능한 CloudWatch 지표는 CloudWatch Route 53 상태 확인 지표를 참조하세요.

지표:`R53-HC-Success`

NameSpace: AWS/라우팅 53

임계값 HealthCheckStatus: HealthCheckStatus 3분 이내에 3개의 데이터 포인트에 대해 < x(x 고객의 임계값)

기간: 1분

DatapointsToAlarm: 3/3

누락된 데이터 처리: 누락된 데이터를 위반으로 처리합니다.

통계: Minimum

다음 다이어그램은 사용 사례 C의 흐름을 보여줍니다.

예제 사용 사례 D: 사용자 지정 앱을 사용하여 워크로드 모니터링

이 시나리오에서는 시간을 내어 적절한 상태 확인을 정의하는 것이 중요합니다. 애플리케이션의 포트만 열려 있는지 확인하는 경우 애플리케이션이 작동하는지 확인하지 않은 것입니다. 또한 애플리케이션의 홈 페이지에 전화를 거는 것이 앱이 작동하는지 확인하는 올바른 방법은 아닙니다. 예를 들어 애플리케이션이 데이터베이스와 Amazon Simple Storage Service(Amazon S3)에 모두 의존하는 경우 상태 확인을 통해 모든 요소를 검증해야 합니다. 이렇게 하는 한 가지 방법은 /monitor와 같은 모니터링 웹 페이지를 생성하는 것입니다. 모니터링 웹 페이지는 데이터베이스에 전화를 걸어 데이터를 연결하고 가져올 수 있는지 확인합니다. 또한 모니터링 웹 페이지에서 Amazon S3를 호출합니다. 그런 다음 로드 밸런서의 상태 확인을 /monitor 페이지로 가리킵니다.

다음 다이어그램은 사용 사례 D의 흐름을 보여줍니다.

AWS 인시던트 감지 및 대응에 경보 삽입

AWS 인시던트 감지 및 대응은 Amazon EventBridge 를 통한 경보 수집을 지원합니다. 이 섹션에서는 AWS 인시던트 감지 및 대응을 Amazon 을 포함한 다양한 Application Performance Monitoring(APM) 도구와 Amazon 과의 CloudWatch APMs 직접 통합 EventBridge (예: Datadog 및 New Relic)과 Amazon 와의 직접 통합 APMs 없이 통합하는 방법을 설명합니다 EventBridge. Amazon APMs 에 직접 통합되는 의 전체 목록은 Amazon 통합을 EventBridge참조하세요. EventBridge

주제

- 인시던트 감지 및 대응에 대한 경보 수집을 위한 액세스 권한 프로비저닝
- 인시던트 감지 및 대응을 Amazon과 통합 CloudWatch
- Amazon과 직접 통합APMs되는 에서 경보 수신 EventBridge

- 예: Datadog 및 Splunk의 알림 통합
- 웹후크를 사용하여 Amazon과의 직접 통합 APMs 없이 에서 경보 수집 EventBridge

인시던트 감지 및 대응에 대한 경보 수집을 위한 액세스 권한 프로비저닝

계정에서 경보를 수집하기 위한 AWS 인시던트 감지 및 응답을 허용하려면 `AWSServiceRoleForHealth_EventProcessor` 서비스 연결 역할()을 설치합니다SLR. AWS 는 를 가정SLR하여 Amazon EventBridge관리형 규칙을 생성합니다. 관리형 규칙은 계정에서 AWS 인시던트 감지 및 대응으로 알림을 보냅니다. 연결된 AWS 관리형 정책을 SLR포함하여 이 에 대한 자세한 내용은 AWS Health 사용 설명서의 서비스 연결 역할 사용을 참조하세요.

AWS Identity and Access Management 사용 설명서의 서비스 연결 역할 생성의 지침에 따라 계정에 이 서비스 연결 역할을 설치할 수 있습니다. 또는 다음 AWS 명령줄 인터페이스(AWS CLI) 명령을 사용할 수 있습니다.

```
aws iam create-service-linked-role --aws-service-name event-
processor.health.amazonaws.com
```

키 출력

- 계정에 서비스 연결 역할을 성공적으로 설치했습니다.

관련 정보

자세한 정보는 다음 주제를 참조하세요.

- AWS Health에 서비스 연결 역할 사용
- 서비스 연결 역할 생성
- AWS 관리형 정책: AWSHealth_EventProcessorServiceRolePolicy

인시던트 감지 및 대응을 Amazon과 통합 CloudWatch

AWS 인시던트 감지 및 대응은 액세스 프로비저닝 중에 켜진 서비스 연결 역할(SLR)을 사용하여 라는 이름의 AWS 계정에서 Amazon EventBridge관리형 규칙을 생성합니다`AWSHealthEventProcessor-DO-NOT-DELETE`. 인시던트 감지 및 대응은 이 규칙을 사용하여 계정에서 Amazon CloudWatch 경보를 수집합니다. 에서 경보를 수집하는 데 추가 단계가 필요하지 않습니다 CloudWatch.

Amazon과 직접 통합APMs되는 에서 경보 수신 EventBridge

다음 그림은 Datadog 및 Splunk EventBridge와 같이 Amazon 와 직접 통합되는 Application Performance Monitoring(APM) 도구에서 AWS Incident Detection and Response로 알림을 보내는 프로세스를 보여줍니다. 와 직접 통합APMs되는 의 전체 목록은 Amazon 통합을 EventBridge참조하세요. EventBridge

다음 단계에 따라 AWS 인시던트 감지 및 대응과의 통합을 설정합니다. 이 단계를 수행하기 전에 AWS 서비스 연결 역할(SLR)`AWSServiceRoleForHealth_EventProcessor`이 계정에 설치되어 있는지 확인합니다.

AWS 인시던트 감지 및 대응과의 통합 설정

각 AWS 계정 및 AWS 리전에 대해 다음 단계를 완료해야 합니다. 알림은 애플리케이션 리소스가 있는 AWS 계정 및 AWS 리전에서 와야 합니다.

1. 각 를 Amazon EventBridge 파트너 이벤트 소스APMs로 설정합니다(예: `aws.partner/my_apm/integrationName`). 를 이벤트 소스APM로 설정하는 방법에 대한 지침은 Amazon 의 SaaS 파트너로부터 이벤트 수신을 EventBridge 참조하세요. 이렇게 하면 계정에 파트너 이벤트 버스가 생성됩니다.
2. 다음 중 하나를 수행합니다.
   - (권장 방법) 사용자 지정 EventBridge 이벤트 버스를 생성합니다. AWS Incident Detection and Response는 `AWSServiceRoleForHealth_EventProcessor` 를 통해 관리형 규칙(`AWSHealthEventProcessorEventSource-DO-NOT-DELETE`) 버스를 설치합니다SLR. 규칙 소스는 사용자 지정 이벤트 버스입니다. 규칙 대상은 AWS 인시던트 감지 및 응답입니다. 규칙은 타사 APM 이벤트를 수집하기 위한 패턴과 일치합니다.
   - (대체 방법) 사용자 지정 이벤트 버스 대신 기본 이벤트 버스를 사용합니다. 기본 이벤트 버스는 AWS 인시던트 감지 및 대응에 APM 알림을 전송하기 위해 관리형 규칙이 필요합니다.
3. AWS Lambda 함수(예: `My_APM-AWSIncidentDetectionResponse-LambdaFunction`)를 생성하여 파트너 이벤트 버스 이벤트를 변환합니다. 변환된 이벤트는 관리형 규칙 과 일치합니다`AWSHealthEventProcessorEventSource-DO-NOT-DELETE`.
   a. 변환된 이벤트에는 고유한 AWS 인시던트 감지 및 응답 식별자가 포함되며 이벤트의 소스 및 세부 정보 유형을 필요한 값으로 설정합니다. 패턴은 관리형 규칙과 일치합니다.
   b. Lambda 함수의 대상을 2단계(권장 방법)에서 생성된 사용자 지정 이벤트 버스 또는 기본 이벤트 버스로 설정합니다.

4. EventBridge 규칙을 생성하고 AWS 인시던트 감지 및 대응에 푸시하려는 이벤트 목록과 일치하는 이벤트 패턴을 정의합니다. 규칙의 소스는 1단계에서 정의한 파트너 이벤트 버스입니다(예: aws.partner/my_apm/integrationName). 규칙의 대상은 3단계에서 정의한 Lambda 함수입니다(예: `My_APM-AWSIncidentDetectionResponse-LambdaFunction`). EventBridge 규칙 정의에 대한 지침은 Amazon EventBridge 규칙 섹션을 참조하세요.

AWS 인시던트 감지 및 대응과 함께 사용할 파트너 이벤트 버스 통합을 설정하는 방법에 대한 예제는 섹션을 참조하세요예: Datadog 및 Splunk의 알림 통합.

예: Datadog 및 Splunk의 알림 통합

이 예제에서는 Datadog 및 Splunk의 알림을 AWS 인시던트 감지 및 대응에 통합하는 자세한 단계를 제공합니다.

주제

- 1단계: Amazon에서 를 이벤트 소스APM로 설정 EventBridge
- 2단계: 사용자 지정 이벤트 버스 생성
- 3단계: 변환을 위한 AWS Lambda 함수 생성
- 4단계: 사용자 지정 Amazon EventBridge 규칙 생성

1단계: Amazon에서 를 이벤트 소스APM로 설정 EventBridge

각 를 EventBridge AWS 계정의 Amazon에서 이벤트 소스APMs로 설정합니다. 를 이벤트 소스APM로 설정하는 방법에 대한 지침은 Amazon EventBridge 파트너 의 도구에 대한 이벤트 소스 설정 지침을 참조하세요.

를 이벤트 소스APM로 설정하면 에서 AWS 계정의 이벤트 버스APM로 알림을 수집할 수 있습니다. 설정 후 AWS 인시던트 감지 및 대응은 이벤트 버스가 이벤트를 수신할 때 인시던트 관리 프로세스를 시작할 수 있습니다. 이 프로세스는 Amazon EventBridge 을 의 대상으로 추가합니다APM.

2단계: 사용자 지정 이벤트 버스 생성

사용자 지정 이벤트 버스를 사용하는 것이 가장 좋습니다. AWS Incident Detection and Response는 사용자 지정 이벤트 버스를 사용하여 변환된 이벤트를 수집합니다. AWS Lambda 함수는 파트너 이벤트 버스 이벤트를 변환하여 사용자 지정 이벤트 버스로 전송합니다. AWS Incident Detection and Response는 관리형 규칙을 설치하여 사용자 지정 이벤트 버스에서 이벤트를 수집합니다.

사용자 지정 이벤트 버스 대신 기본 이벤트 버스를 사용할 수 있습니다. AWS 인시던트 감지 및 대응은 사용자 지정 규칙 대신 기본 이벤트 버스에서 수집하도록 관리형 규칙을 수정합니다.

AWS 계정에서 사용자 지정 이벤트 버스를 생성합니다.

1. 에서 Amazon EventBridge 콘솔 열기 https://console.aws.amazon.com/events/
2. 버스 , 이벤트 버스 를 선택합니다.
3. 사용자 지정 이벤트 버스 에서 생성을 선택합니다.
4. 이름 아래에 이벤트 버스의 이름을 입력합니다. 권장 형식은 APMName-AWSIncidentDetectionResponse-EventBus입니다.

   예를 들어 Datadog 또는 Splunk를 사용하는 경우 다음 중 하나를 사용합니다.

   - Datadog : Datadog-AWSIncidentDetectionResponse-EventBus
   - Splunk : Splunk-AWSIncidentDetectionResponse-EventBus

3단계: 변환을 위한 AWS Lambda 함수 생성

Lambda 함수는 1단계의 파트너 이벤트 버스와 2단계의 사용자 지정(또는 기본) 이벤트 버스 간의 이벤트를 변환합니다. Lambda 함수 변환은 AWS 인시던트 감지 및 응답 관리형 규칙과 일치합니다.

AWS 계정에서 AWS Lambda 함수 생성

1. AWS Lambda 콘솔에서 함수 페이지를 엽니다.
2. 함수 생성(Create function)을 선택합니다.
3. 처음부터 작성자 탭을 선택합니다.
4. 함수 이름 에 형식을 사용하여 이름을 입력합니다`APMName-AWSIncidentDetectionResponse-LambdaFunction`.

   다음은 Datadog 및 Splunk의 예입니다.

   - Datadog : Datadog-AWSIncidentDetectionResponse-LambdaFunction
   - Splunk : Splunk-AWSIncidentDetectionResponse-LambdaFunction
5. 런타임 에 Python 3.10을 입력합니다.
6. 나머지 필드는 기본값으로 둡니다. 함수 생성(Create function)을 선택합니다.
7. 코드 편집 페이지에서 기본 Lambda 함수 콘텐츠를 다음 코드 예제의 함수로 바꿉니다.

   다음 코드 예제에서 #로 시작하는 주석에 유의하세요. 이러한 주석은 변경할 값을 나타냅니다.

Datadog 변환 코드 템플릿:

```
import logging
import json
import boto3

logger = logging.getLogger()
logger.setLevel(logging.INFO)

# Change the EventBusName to the custom event bus name you created previously or
 use your default event bus which is called 'default'.
# Example 'Datadog-AWSIncidentDetectionResponse-EventBus'
EventBusName = "Datadog-AWSIncidentDetectionResponse-EventBus"

def lambda_handler(event, context):
    # Set the event["detail"]["incident-detection-response-identifier"] value to
 the name of your alert that is coming from your APM. Each APM is different and
 each unique alert will have a different name.
    # Replace the dictionary path, event["detail"]["meta"]["monitor"]["name"], with
 the path to your alert name based on your APM payload.
    # This example is for finding the alert name for Datadog.
    event["detail"]["incident-detection-response-identifier"] = event["detail"]
["meta"]["monitor"]["name"]
    logger.info(f"We got: {json.dumps(event, indent=2)}")

    client = boto3.client('events')
    response = client.put_events(
     Entries=[
              {
               'Detail': json.dumps(event["detail"], indent=2),
               'DetailType': 'ams.monitoring/generic-apm', # Do not modify. This
 DetailType value is required.
               'Source': 'GenericAPMEvent', # Do not modify. This Source value is
 required.
               'EventBusName': EventBusName # Do not modify. This variable is set
 at the top of this code as a global variable. Change the variable value for your
 eventbus name at the top of this code.
             }
     ]
    )
    print(response['Entries'])
```

Splunk 변환 코드 템플릿:

```
import logging
import json
import boto3

logger = logging.getLogger()
logger.setLevel(logging.INFO)

# Change the EventBusName to the custom event bus name you created previously or
 use your default event bus which is called 'default'.
# Example Splunk-AWSIncidentDetectionResponse-EventBus
EventBusName = "Splunk-AWSIncidentDetectionResponse-EventBus"

def lambda_handler(event, context):
    # Set the event["detail"]["incident-detection-response-identifier"] value to
 the name of your alert that is coming from your APM. Each APM is different and
 each unique alert will have a different name.
    # replace the dictionary path event["detail"]["ruleName"] with the path to your
 alert name based on your APM payload.
    # This example is for finding the alert name in Splunk.
    event["detail"]["incident-detection-response-identifier"] = event["detail"]
["ruleName"]
    logger.info(f"We got: {json.dumps(event, indent=2)}")

    client = boto3.client('events')
    response = client.put_events(
    Entries=[
             {
              'Detail': json.dumps(event["detail"], indent=2),
              'DetailType': 'ams.monitoring/generic-apm', # Do not modify. This
 DetailType value is required.
              'Source': 'GenericAPMEvent', # Do not modify. This Source value is
 required.
              'EventBusName': EventBusName # Do not modify. This variable is set
 at the top of this code as a global variable. Change the variable value for your
 eventbus name at the top of this code.
            }
        ]
    )
    print(response['Entries'])
```

8. 배포(Deploy)를 선택합니다.

9. 변환PutEvents된 데이터를 보내는 이벤트 버스의 Lambda 실행 역할에 권한을 추가합니다.

   a. AWS Lambda 콘솔에서 함수 페이지를 엽니다.
   b. 함수를 선택한 다음 구성 탭에서 권한을 선택합니다.
   c. 실행 역할 에서 역할 이름을 선택하여 AWS Identity and Access Management 콘솔에서 실행 역할을 엽니다.
   d. 권한 정책 에서 기존 정책 이름을 선택하여 정책을 엽니다.
   e. 이 정책 에 정의된 권한에서 편집을 선택합니다.
   f. 정책 편집기 페이지에서 새 문 추가를 선택합니다.
   g. 정책 편집기는 다음과 유사한 새 빈 문을 추가합니다.

   h. 새 자동 생성된 문을 다음과 같이 바꿉니다.

```
{
  "Sid": "AWSIncidentDetectionResponseEventBus0",
  "Effect": "Allow",
  "Action": "events:PutEvents",
  "Resource": "arn:aws:events:{region}:{accountId}:event-bus/{custom-eventbus-
name}"
}
```

   i. 리소스는 Lambda 코드ARN에서 기본 이벤트 버스를 사용하는 경우 에서 생성한 사용자 지정 이벤트 버스ARN의 2단계: 사용자 지정 이벤트 버스 생성 또는 기본 이벤트 버스의 입니다.

10. 필요한 권한이 역할에 추가되었는지 검토하고 확인합니다.
11. 이 새 버전을 기본 로 설정을 선택한 다음 변경 사항 저장을 선택합니다.

페이로드 변환에는 무엇이 필요합니까?

AWS 인시던트 감지 및 대응에서 수집되는 이벤트 버스 이벤트에는 다음 JSON 키:값 페어가 필요합니다.

```
{
    "detail-type": "ams.monitoring/generic-apm",
    "source": "GenericAPMEvent"
    "detail" : {
        "incident-detection-response-identifier": "Your alarm name from your APM",
    }
```

```
}
```

다음 예제에서는 변환 전후의 파트너 이벤트 버스에서 발생한 이벤트를 보여줍니다.

```
{
    "version": "0",
    "id": "a6150a80-601d-be41-1a1f-2c5527a99199",
    "detail-type": "Datadog Alert Notification",
    "source": "aws.partner/datadog.com/Datadog-aaa111bbbc",
    "account": "123456789012",
    "time": "2023-10-25T14:42:25Z",
    "region": "us-east-1",
    "resources": [],
    "detail": {
      "alert_type": "error",
      "event_type": "query_alert_monitor",
      "meta": {
        "monitor": {
          "id": 222222,
          "org_id": 3333333333,
          "type": "query alert",
          "name": "UnHealthyHostCount",
          "message": "@awseventbridge-Datadog-aaa111bbbc",
          "query":
 "max(last_5m):avg:aws.applicationelb.un_healthy_host_count{aws_account:123456789012}
 \u003c\u003d 1",
          "created_at": 1686884769000,
          "modified": 1698244915000,
          "options": {
            "thresholds": {
              "critical": 1.0
            }
          },
        },
        "result": {
          "result_id": 7281010972796602670,
          "result_ts": 1698244878,
          "evaluation_ts": 1698244868,
          "scheduled_ts": 1698244938,
          "metadata": {
            "monitor_id": 222222,
            "metric": "aws.applicationelb.un_healthy_host_count"
          }
```

```
        },
        "transition": {
          "trans_name": "Triggered",
          "trans_type": "alert"
        },
        "states": {
          "source_state": "OK",
          "dest_state": "Alert"
        },
        "duration": 0
      },
      "priority": "normal",
      "source_type_name": "Monitor Alert",
      "tags": [
        "aws_account:123456789012",
        "monitor"
      ]
    }
}
```

이벤트가 변환되기 전에 는 알림이 오고, 소스가 파트너 이고APM, `incident-detection-response-identifier` 키가 존재하지 APM 않음을 `detail-type` 나타냅니다.

Lambda 함수는 위의 이벤트를 변환하여 대상 사용자 지정 또는 기본 이벤트 버스에 넣습니다. 변환된 페이로드에는 이제 필요한 키:값 페어가 포함됩니다.

```
{
    "version": "0",
    "id": "7f5e0fc1-e917-2b5d-a299-50f4735f1283",
    "detail-type": "ams.monitoring/generic-apm",
    "source": "GenericAPMEvent",
    "account": "123456789012",
    "time": "2023-10-25T14:42:25Z",
    "region": "us-east-1",
    "resources": [],
    "detail": {
      "incident-detection-response-identifier": "UnHealthyHostCount",
      "alert_type": "error",
      "event_type": "query_alert_monitor",
      "meta": {
        "monitor": {
          "id": 222222,
          "org_id": 3333333333,
```

```
          "type": "query alert",
          "name": "UnHealthyHostCount",
          "message": "@awseventbridge-Datadog-aaa111bbbc",
          "query":
 "max(last_5m):avg:aws.applicationelb.un_healthy_host_count{aws_account:123456789012}
 \u003c\u003d 1",
          "created_at": 1686884769000,
          "modified": 1698244915000,
          "options": {
            "thresholds": {
              "critical": 1.0
            }
          },
        },
        "result": {
          "result_id": 7281010972796602670,
          "result_ts": 1698244878,
          "evaluation_ts": 1698244868,
          "scheduled_ts": 1698244938,
          "metadata": {
            "monitor_id": 222222,
            "metric": "aws.applicationelb.un_healthy_host_count"
          }
        },
        "transition": {
          "trans_name": "Triggered",
          "trans_type": "alert"
        },
        "states": {
          "source_state": "OK",
          "dest_state": "Alert"
        },
        "duration": 0
      },
      "priority": "normal",
      "source_type_name": "Monitor Alert",
      "tags": [
        "aws_account:123456789012",
        "monitor"
      ]
    }
}
```

이제 `detail-type`이고`ams.monitoring/generic-apm`, 소스는 이며`GenericAPMEvent`, 세부 정보 아래에 새 키:값 페어가 있습니다`incident-detection-response-identifier`.

앞의 예에서 `incident-detection-response-identifier` 값은 경로 아래의 알림 이름에서 가져옵니다`$.detail.meta.monitor.name`. APM 알림 이름 경로는 서로 다릅니다APM. Lambda 함수를 수정하여 올바른 파트너 이벤트 JSON 경로에서 경보 이름을 가져와 `incident-detection-response-identifier` 값에 사용해야 합니다.

에 설정된 각 고유 이름은 온보딩 중에 AWS 인시던트 감지 및 대응 팀에 `incident-detection-response-identifier` 제공됩니다. 의 이름을 알 수 없는 이벤트`incident-detection-response-identifier`는 처리되지 않습니다.

4단계: 사용자 지정 Amazon EventBridge 규칙 생성

1단계에서 생성된 파트너 이벤트 버스에는 생성한 EventBridge 규칙이 필요합니다. 규칙은 파트너 이벤트 버스에서 3단계에서 생성된 Lambda 함수로 원하는 이벤트를 전송합니다.

EventBridge 규칙 정의에 대한 지침은 Amazon EventBridge 규칙 섹션을 참조하세요.

1. 에서 Amazon EventBridge 콘솔 열기 https://console.aws.amazon.com/events/
2. 규칙 을 선택한 다음 와 연결된 파트너 이벤트 버스를 선택합니다APM. 다음은 파트너 이벤트 버스의 예제입니다.

   - Datadog: aws.partner/datadog.com/eventbus-name
   - Splunk: aws.partner/signalfx.com/RandomString
3. 규칙 생성을 선택하여 새 EventBridge 규칙을 생성합니다.
4. 규칙 이름에 다음 형식의 이름을 입력한 `APMName-AWS Incident Detection and Response-EventBridgeRule`다음 다음 를 선택합니다. 다음은 예제 이름입니다.

   - Datadog: Datadog-AWSIncidentDetectionResponse-EventBridgeRule
   - Splunk: Splunk-AWSIncidentDetectionResponse-EventBridgeRule
5. 이벤트 소스 에서 AWS 이벤트 또는 EventBridge 파트너 이벤트 를 선택합니다.
6. 샘플 이벤트 및 생성 방법을 기본값으로 둡니다.
7. 이벤트 패턴 에서 다음을 선택합니다.

   a. 이벤트 소스: EventBridge 파트너.

   b. 파트너: APM 파트너를 선택합니다.

   c. 이벤트 유형: 모든 이벤트.

다음은 이벤트 패턴의 예입니다.

예제 Datadog 이벤트 패턴

Splunk 이벤트 패턴 예제

8. 대상 에서 다음을 선택합니다.
   a. 대상 유형: AWS 서비스
   b. 대상 선택: Lambda 함수를 선택합니다.
   c. 함수: 2단계에서 생성한 Lambda 함수의 이름입니다.
9. 다음 , 규칙 저장 을 선택합니다.

웹후크를 사용하여 Amazon과의 직접 통합 APMs 없이 에서 경보 수집 EventBridge

AWS Incident Detection and Response는 Amazon 와 직접 통합되지 APMs 않은 타사의 경보 수집을 위해 웹후크 사용을 지원합니다 EventBridge.

Amazon과의 직접 통합이 APMs 포함된 목록은 Amazon 통합을 EventBridge참조하세요. EventBridge

다음 단계에 따라 AWS 인시던트 감지 및 대응과의 통합을 설정합니다. 이 단계를 수행하기 전에 AWS 관리형 규칙 AWSHealthEventProcessorEventSource-DO-NOT-DELETE가 계정에 설치되어 있는지 확인합니다.

웹후크를 사용하여 이벤트 수집

1. 에서 페이로드를 수락할 Amazon API Gateway를 정의합니다APM.
2. 앞의 그림과 같이 인증 토큰을 사용하여 권한 부여 AWS Lambda 함수를 정의합니다.
3. AWS 인시던트 감지 및 응답 식별자를 변환하고 페이로드에 추가할 두 번째 Lambda 함수를 정의합니다. 또한 이 함수를 사용하여 AWS 인시던트 감지 및 응답에 전송할 이벤트를 필터링할 수 있습니다.
4. API 게이트웨이에서 URL 생성된 에 알림을 보내APM도록 를 설정합니다.

인시던트 감지 및 대응에서 워크로드 관리

효과적인 인시던트 관리의 주요 부분은 모니터링되는 워크로드를 온보딩, 테스트 및 유지하기 위한 올바른 프로세스와 절차를 마련하는 것입니다. 이 섹션에서는 인시던트를 통해 팀을 안내하는 포괄적인 런북 및 대응 계획 개발, 온보딩 전에 새 워크로드의 철저한 테스트 및 검증, 워크로드 모니터링 업데이트 변경 요청, 필요한 경우 워크로드의 적절한 오프보딩을 비롯한 필수 단계를 다룹니다.

주제

인시던트 감지 및 대응에서 인시던트에 대응하기 위한 실행서 및 대응 계획 개발

인시던트 감지 및 대응은 온보딩 설문지에서 캡처한 정보를 사용하여 워크로드에 영향을 미치는 인시던트 관리를 위한 런북 및 대응 계획을 개발합니다. 런북은 인시던트에 대응할 때 인시던트 관리자가 수행하는 단계를 문서화합니다. 응답 계획은 워크로드 중 하나 이상에 매핑됩니다. 인시던트 관리 팀은 워크로드 검색 중에 제공한 정보에서 이러한 템플릿을 생성합니다. 대응 계획은 인시던트를 트리거하는 데 사용되는 AWS Systems Manager (SSM) 문서 템플릿입니다. SSM 문서에 대한 자세한 내용은 AWS Systems Manager 문서 섹션을 참조하세요. Incident Manager에 대한 자세한 내용은 란 무엇입니까 AWS Systems Manager Incident Manager?를 참조하세요.

키 출력:

- AWS 인시던트 감지 및 대응에 대한 워크로드 정의 완료.
- AWS 인시던트 감지 및 대응에 대한 경보, 실행서 및 대응 계획 정의 완료.

AWS 인시던트 감지 및 대응 실행서 예제: aws-idr-runbook-example.zip 을 다운로드할 수도 있습니다.

런북 예제:

```
Runbook template for AWS Incident Detection and Response
# Description
This document is intended for [CustomerName] [WorkloadName].
```

```
[Insert short description of what the workload is intended for].

## Step: Priority
**Priority actions**
1. When a case is created with Incident Detection and Response, lock the case to
 yourself, verify the Customer Stakeholders in the Case from *Engagement Plans -
 Initial Engagement*.
2. Send the first correspondence on the support case to the customer as below. If
 there is no support case or if it is not possible to use the support case then backup
 communication details are listed in the steps that follow.

```
Hello,

This is <<Engineer's name>> from AWS Incident Detection and Response. An alarm has
 triggered for your workload <<application name>>. I am currently investigating and
 will update you in a few minutes after I have finished initial investigation.

Alarm Identifier - <insert CloudWatch Alarm ARN or APM Response Identifier>
```

Compliance and regulatory requirements for the workload
<<e.g. The workload deals with patient health records which must be kept secured and
 confidential. Information not to be shared with any third parties.>>

Actions required from Incident Detection and Response in complying
<<e.g Incident Management Engineers must not shared data with third parties.>>

Step: Information
Review of common information

* This section provides a space for defining common information which may be needed
 through the life of the incident.
* The target user of this information is the Incident Management Engineer and
 Operations Engineer.
* The following steps may reference this information to complete an action (for
 example, execute the "Initial Engagement" plan).

Engagement plans
```

```
Describe the engagement plans applicable to this runbook. This section contains
 only contact details. Engagement plans will be referenced in the step by step
 **Communication Plans**.

* **Initial engagement**

AWS Incident Detection and Response Team will add customer stakeholder addresses below
 to the Support Case. AWS Stakeholders are for additional stakeholders that may need to
 be made aware of any issues.
When updating customer stakeholders details in this plan also update the Backup Mailto
 links.
  * ***Customer Stakeholders***:  customeremail1; customeremail2; etc
  * ***AWS Stakeholders***: aws-idr-oncall@amazon.com; tam-team-email; etc.
  * ***One Time Only Contacts***: [These are email contacts that are included on only
 the first communication. Remove these contacts after the first communication has gone
 out. These could be customer paging email addresses such as pager-duty that must not
 be paged for every correspondence]
  * ***Backup Mailto Impact Template***: <*Insert Impact Template Mailto Link here*>
    * Use the backup Mailto when communication over cases is not possible.
  * ***Backup Mailto No Impact Template***: <*Insert No Impact Mailto Link here*>
    * Use the backup Mailto when communication over cases is not possible.


* **Engagement Escalation**

AWS Incident Detection and Response will reach out to the following contacts when the
 contacts from the **Initial engagement** plan do not respond to incidents.
For each Escalation Contact indicate if they must be added to the support case, phoned
 or both.
  * ***First Escalation Contact***: [escalationEmailAddress#1] / [PhoneNumber] - Wait
 XX Minutes before escalating to this contact.
    * [add Contact to Case / phone] this contact.
  * ***Second Escalation Contact***: [escalationEmailAddress#2] / [PhoneNumber] - Wait
 XX Minutes before escalating to this contact.
    * [add Contact to Case / phone] this contact.
  * Etc;
---
**Communication plans**

Describe how Incident Management Engineer communicates with designated stakeholders
 outside the incident call and communication channels.

* **Impact Communication plan**
```

```
This plan is initiated when Incident Detection and Response have determined from step
 **Triage** that an alert indicates potential impact to a customer.
Incident Detection and Response will request the customer to join the predetermined
 bridge (Chime Bridge/Customer Provided Bridge / Customer Static Bridge) as indicated
 in **Engagement plans - Incident call setup**.
All backup email templates for use when cases can't be used are in **Engagement plans -
 Initial engagement**.
  * 1 – Before sending the impact notification, verify then remove and/or add customer
 contacts from the Support Case CC based on the contacts listed in the **Initial
 engagement** Engagement plan.
  * 2 – Send the engagement notification to the customer based the following Template:

    (choose one and remove the rest)
    ***Impact Template - Chime Bridge***
    ```
    The following alarm has engaged AWS Incident Detection and Response to an Incident
 bridge:
        Alarm Identifier - <insert CloudWatch Alarm ARN or APM Response Identifier>
        Alarm State Change Reason - <insert state change reason>
        Alarm Start Time - <Example: 1 January 2023, 3:30 PM UTC>
    Please join the Chime Bridge below so we can start the steps outlined in your
 Runbook:
        <insert Chime Meeting ID>
        <insert Link to Chime Bridge>
        International dial-in numbers: https://chime.aws/dialinnumbers/
    ```


    ***Impact Template - Customer Provided Bridge***
    ```
    The following alarm has engaged AWS Incident Detection and Response:
        Alarm Identifier - <insert CloudWatch Alarm ARN or APM Response Identifier>
        Alarm State Change Reason - <insert state change reason>
        Alarm Start Time - <Example: 1 January 2023 3:30 PM UTC>
    Please respond with your internal bridge details so we can join and start the steps
 outlined in your Runbook.
    ```
    ***Impact Template - Customer Static Bridge***
    ```
    The following alarm has engaged AWS Incident Detection and Response to an Incident
 bridge:
        Alarm Identifier - <insert CloudWatch Alarm ARN or APM Response Identifier>
        Alarm State Change Reason - <insert state change reason>
        Alarm Start Time - <Example: 1 January 2023, 3:30 PM UTC>
    Please join the Bridge below so we can start the steps outlined in your Runbook:
```
```

```
        Conference Number: <insert conference number>
        Conference URL : <insert bridgeURL>
    ```
  * 3 - Set the Case to Pending Customer Action
  * 4 - Follow **Engagement Escalation** plan as mentioned above.
  * 5 - If the customer does not respond within 30 minutes, disengage and continue to monitor until the alarm recovers.

* **No Impact Communication plan**
This plan is initiated when an alarm recovers before Incident Detection and Response have completed initial **Triage**.
  * 1 - Before sending the no impact notification, verify then remove and/or add customer contacts from the Support Case CC based on the contacts listed in the **Engagement plans - Initial engagement** Engagement plan.
  * 2 - Send a no engagement notification to the customer based on the below template:

  No Impact Template
  ```
  AWS Incident Detection and Response received an alarm that has recovered for your workload.
      Alarm Identifier -  <insert CloudWatch Alarm ARN or APM Response Identifier>
      Alarm State Change Reason -  <insert state change reason>
      Alarm Start Time -  <Example: 1 January 2023, 3:30 PM UTC>
      Alarm End Time -  <Example: 1 January 2023, 3:35 PM UTC>
  This may indicate a brief customer impact that is currently not ongoing.
  If there is an ongoing impact to your workload, please let us know and we will engage to assist.
  ```
  * 3 - Put the case in to Pending Customer Action.
  * 4 - If the customer does not respond within 30 minutes Resolve the case.

* **Updates**
If AWS Incident Detection and Response is expected to provide regular updates to customer stakeholders, list those stakeholders here. Updates must be sent via the same support case.
Remove this section if not needed.
  * Update Cadence: Every XX minutes
  * External Update Stakeholders: customeremailaddress1; customeremailaddress2; etc
  * Internal Update Stakeholders: awsemailaddress1; awsemailaddress2; etc

---
Application architecture overview
```
```

```
This section provides an overview of the application/workload architecture for Incident
 Management Engineer and Operations Engineer awareness.

* **AWS Accounts and Regions with key services** - list of AWS accounts with regions
 supporting this application. Assists Engineers in assessing underlying infrastructure
 supporting the application.
    * 123456789012
      * US-EAST-1 - brief desc as appropriate
        * EC2 - brief desc as appropriate
        * DynamoDB - brief desc as appropriate
        * etc.
      * US-WEST-1 - brief desc as appropriate
      * etc.
    * another-account-etc.

* **Resource identification** - describe how engineers determine resource association
 with application
    * Resource groups: etc.
    * Tag key/value: AppId=123456

* **CloudWatch Dashboards** - list dashboards relevant to key metrics and services
  * 123456789012
    * us-east-1
      * some-dashboard-name
      * etc.
  * some-other-dashboard-name-in-current-acct

## Step: Triage
**Evaluate incident and impact**
This section provides instructions for triaging of the incident to determine correct
 impact, description, and overall correct runbook being executed.

* **Evaluation of initial incident information**
  * 1 - Review Incident Alarm, noting time of first detected impact as well as the
 alarm start time.
  * 2 - Identify which service(s) in the customer application is seeing impact.
  * 3 - Review AWS Service Health for services listed under **AWS Accounts and Regions
 with key services**.
  * 4 - Review any customer provided dashboards listed under **CloudWatch Dashboards**

---
* **Impact**
Impact is determined when either the customer's metrics do not recover, appear to be
 trending worse or if there is indication of AWS Service Impact.
```

```
  * 1 – Start **Communication plans - Impact Communication plan**
  * 2 - Start **Engagement plans - Engagement Escalation** if no response is received
 from the **Initial Engagement** contacts.
  * 3 - Start **Communication plans - Updates** if specified in **Communication plans**

* **No Impact**
No Impact is determined when the customer's alarm recovers before Triage is complete
 and there are no indications of AWS service impact or sustained impact on the
 customer's CloudWatch Dashboards.
  * 1 - Start **Communication plans - No Impact Communication plan**

## Step: Investigate
**Investigation**

  This section describes performing investigation of known and unknown symptoms.

**Known issue**
  * *List all known issues with the application and their standard actions here*

**Unknown issues**
  * Investigate with the customer and AWS Premium Support.
  * Escalate internally as required.

## Step: Mitigation
**Collaborate**
* Communicate any changes or important information from the **Investigate** step to the
 members of the incident call.

**Implement mitigation**
* ***List customer failover plans / Disaster Recovery plans / etc here for implementing
 mitigation.

## Step: Recovery
**Monitor customer impact**
* Review metrics to confirm recovery.
* Ensure recovery is across all Availability Zones / Regions / Services
* Get confirmation from the customer that impact is over and the application has
 recovered.

**Identify action items**
* Record key decisions and actions taken, including temporary mitigation that might
 have been implemented.
* Ensure outstanding action items have assigned owners.
```

```
* Close out any Communication plans that were opened during the incident with a final
 confirmation of recovery notification.
```

인시던트 감지 및 대응에서 온보딩된 워크로드 테스트

> **Note**
>
> 경보 테스트에 사용하는 AWS Identity and Access Management 사용자 또는 역할에 `cloudwatch:SetAlarmState` 권한이 있어야 합니다.

온보딩 프로세스의 마지막 단계는 새 워크로드에 대해 게임데이를 수행하는 것입니다. 경보 수집이 완료되면 AWS 인시던트 감지 및 대응에서 게임데이를 시작하기로 선택한 날짜와 시간을 확인합니다.

게임데이는 두 가지 주요 목적을 제공합니다.

- 기능 검증: AWS 인시던트 감지 및 대응이 경보 이벤트를 올바르게 수신할 수 있는지 확인합니다. 또한 기능 검증을 통해 경보 이벤트가 적절한 실행서와 경보 수집 중에 자동 사례 생성과 같은 기타 원하는 작업을 트리거하는지 확인합니다.
- 시뮬레이션: 게임데이는 실제 인시던트 중에 발생할 수 있는 상황에 대한 엔드 투 엔드 시뮬레이션입니다. AWS 인시던트 감지 및 대응은 규정된 실행서 단계에 따라 실제 인시던트가 어떻게 전개될 수 있는지에 대한 통찰력을 제공합니다. 게임데이는 참여를 개선하기 위해 질문을 하거나 지침을 수정할 수 있는 기회입니다.

경보 테스트 중에 AWS Incident Detection and Response는 사용자와 협력하여 식별된 문제를 해결합니다.

CloudWatch 경보

AWS Incident Detection and Response는 CloudWatch 경보의 상태 변화를 모니터링하여 Amazon 경보를 테스트합니다. 이렇게 하려면 를 사용하여 경보를 경보 상태로 수동으로 변경합니다 AWS Command Line Interface. AWS CLI 에서 에 액세스할 수도 있습니다 AWS CloudShell. AWS Incident Detection and Response는 테스트 중에 사용할 수 있는 AWS CLI 명령 목록을 제공합니다.

경보 상태를 설정하는 AWS CLI 명령의 예:

```
aws cloudwatch set-alarm-state --alarm-name "ExampleAlarm" --state-value ALARM --state-
reason "Testing AWS Incident Detection and Response" --region us-east-1
```

CloudWatch 경보 상태를 수동으로 변경하는 방법에 대한 자세한 내용은 섹션을 참조하세요SetAlarmState.

작업에 필요한 권한에 대한 자세한 내용은 Amazon CloudWatch 권한 참조를 참조하세요 CloudWatch API.

타사 APM 경보

Datadog, Splunk, New Relic 또는 Dynatrace와 같은 타사 Application Performance Monitoring(APM) 도구를 사용하는 워크로드는 경보를 시뮬레이션하기 위해 다른 지침이 필요합니다. 게임데이가 시작될 때 AWS 인시던트 감지 및 대응은 경보 임계값 또는 비교 연산자를 일시적으로 변경하여 경보를 ALARM 상태로 강제로 전환하도록 요청합니다. 이 상태는 AWS 인시던트 감지 및 대응에 대한 페이로드를 트리거합니다.

키 출력

키 출력:

- 경보 수집이 성공했으며 경보 구성이 정확합니다.
- 경보는 AWS 인시던트 감지 및 대응에서 성공적으로 생성되고 수신됩니다.
- 참여에 대한 지원 사례가 생성되고 규정된 연락처에 알림이 전송됩니다.
- AWS 인시던트 감지 및 대응은 규정된 회의 수단을 통해 고객과 소통할 수 있습니다.
- 게임데이의 일부로 생성된 모든 경보 및 지원 사례가 해결됩니다.
- AWS 이제 인시던트 감지 및 대응에서 워크로드를 모니터링하고 있음을 확인하는 Go-Live 이메일이 전송됩니다.

인시던트 감지 및 대응에서 온보딩된 워크로드에 대한 변경 요청

온보딩된 워크로드에 대한 변경을 요청하려면 다음 단계를 완료하여 AWS 인시던트 감지 및 대응으로 지원 사례를 생성합니다.

1. AWS Support 센터 로 이동한 다음 다음 예제와 같이 사례 생성을 선택합니다.

2. 기술 을 선택합니다.
3. 서비스 에서 인시던트 감지 및 대응 을 선택합니다.
4. 범주 에서 워크로드 변경 요청 을 선택합니다.
5. 심각도 에서 일반 지침 을 선택합니다.

6. 이 변경 사항에 대한 제목을 입력합니다. 예:

   AWS 인시던트 감지 및 대응 - *workload_name*

7. 이 변경 사항에 대한 설명을 입력합니다. 예를 들어 '이 요청은 AWS 인시던트 감지 및 대응'에 온보딩된 기존 워크로드에 대한 변경 사항입니다. 요청에 다음 정보를 포함해야 합니다.

   - 워크로드 이름: 워크로드 이름입니다.
   - 계정 ID(들): ID1, ID2ID3, 등.
   - 변경 세부 정보: 요청된 변경에 대한 세부 정보를 입력합니다.

8. 추가 연락처 - 선택 사항 섹션에서 이 변경 사항에 대한 서신을 수신IDs하려는 이메일을 입력합니다.

   다음은 추가 연락처 - 옵션 섹션의 예입니다.

   > **Important**
   >
   > 추가 연락처 IDs - 선택 사항 섹션에 이메일을 추가하지 않으면 변경 프로세스가 지연될 수 있습니다.

9. 제출을 선택합니다.

   변경 요청을 제출한 후 조직의 이메일을 추가할 수 있습니다. 이메일을 추가하려면 다음 예제와 같이 사례 세부 정보에서 회신을 선택합니다.

   그런 다음 IDs 추가 연락처 - 선택 사항 섹션에 이메일을 추가합니다.

   다음은 추가 이메일을 입력할 수 있는 위치를 보여주는 회신 페이지의 예입니다.

인시던트 감지 및 대응에서 워크로드 오프보드

AWS 인시던트 감지 및 대응에서 워크로드를 오프보딩하려면 각 워크로드에 대해 새 지원 사례를 생성합니다. 지원 사례를 생성할 때는 다음 사항에 유의하세요.

- 단일 AWS 계정에 있는 워크로드를 오프보딩하려면 워크로드 계정 또는 지불자 계정에서 지원 사례를 생성합니다.

- 여러 AWS 계정에 걸쳐 있는 워크로드를 오프보딩하려면 지불자 계정 에서 지원 사례를 생성합니다. 지원 사례 본문에 오프보드IDs할 모든 계정을 나열합니다.

> **Important**
>
> 잘못된 계정에서 워크로드를 오프보딩하는 지원 사례를 생성하는 경우 워크로드를 오프로드하기 전에 지연 및 추가 정보 요청이 발생할 수 있습니다.

워크로드 오프보딩 요청

1. AWS Support 센터 로 이동한 다음 사례 생성 을 선택합니다.
2. 기술 을 선택합니다.
3. 서비스 에서 인시던트 감지 및 응답 을 선택합니다.
4. 범주 에서 워크로드 오프보딩 을 선택합니다.
5. 심각도 에서 일반 지침 을 선택합니다.
6. 이 변경 사항에 대한 제목을 입력합니다. 예:

   [오프보드] AWS 인시던트 감지 및 대응 - *workload_name*
7. 이 변경 사항에 대한 설명을 입력합니다. 예를 들어 '이 요청은 AWS 인시던트 감지 및 대응'에 온보딩된 기존 워크로드를 오프보딩하기 위한 것입니다. 요청에 다음 정보를 포함해야 합니다.

   - 워크로드 이름: 워크로드 이름입니다.
   - 계정 ID(들): ID1, ID2ID3, 등.
   - 오프보딩 사유: 워크로드 오프보딩 사유를 입력합니다.
8. 추가 연락처 - 선택 사항 섹션에서 이 오프보딩 요청에 대한 서신을 수신IDs하려는 이메일을 입력합니다.
9. 제출을 선택합니다.

AWS 인시던트 감지 및 대응 모니터링 및 관찰 가능성

AWS Incident Detection and Response는 애플리케이션 계층에서 기본 인프라에 이르기까지 워크로드 전반에 걸쳐 관찰 가능성을 정의하는 전문가 지침을 제공합니다. 모니터링은 문제가 있음을 알려줍니다. 관측성은 데이터 수집을 사용하여 무엇이 잘못되었는지, 왜 발생했는지 알려줍니다.

Incident Detection and Response 시스템은 Amazon 및 Amazon과 같은 네이티브 AWS 서비스를 활용하여 AWS 워크로드 EventBridge 에 영향을 미칠 수 있는 이벤트를 감지하여 워크로드에 장애 CloudWatch 및 성능 저하가 있는지 모니터링합니다. 모니터링은 임박한, 지속적인, 후퇴하는 또는 잠재적 장애 또는 성능 저하에 대한 알림을 제공합니다. 계정을 인시던트 감지 및 대응에 온보딩할 때 인시던트 감지 및 대응 모니터링 시스템에서 모니터링해야 하는 계정의 경보를 선택하고 이러한 경보를 인시던트 관리 중에 사용되는 애플리케이션 및 실행서와 연결합니다.

Incident Detection and Response는 Amazon CloudWatch 및 기타 AWS 서비스 를 사용하여 관찰 가능성 솔루션을 구축합니다. AWS Incident Detection and Response는 두 가지 방법으로 관찰 가능성을 제공합니다.

- 비즈니스 결과 지표 : AWS 인시던트 감지 및 대응에 대한 관찰 가능성은 워크로드 또는 최종 사용자 경험의 결과를 모니터링하는 주요 지표를 정의하는 것으로 시작됩니다. AWS 전문가는 사용자와 협력하여 워크로드의 목표, 사용자 경험에 영향을 미칠 수 있는 주요 출력 또는 요인을 이해하고 이러한 주요 지표의 저하를 캡처하는 지표와 알림을 정의합니다. 예를 들어 모바일 통화 애플리케이션의 주요 비즈니스 지표는 통화 설정 성공률(사용자 통화 시도 성공률 모니터링)이고 웹 사이트의 주요 지표는 페이지 속도입니다. 인시던트 참여는 비즈니스 결과 지표를 기반으로 트리거됩니다.
- 인프라 수준 지표 : 이 단계에서는 애플리케이션을 지원하는 기본 AWS 서비스 및 인프라를 식별하고 지표와 경보를 정의하여 이러한 인프라 서비스의 성능을 추적합니다. 여기에는 Application Load Balancer 인스턴스`ApplicationLoadBalancerErrorCount`와 같은 지표가 포함될 수 있습니다. 이는 워크로드가 온보딩되고 모니터링이 설정된 후 시작됩니다.

AWS 인시던트 감지 및 대응에 대한 관찰 가능성 구현

관찰 가능성은 한 번의 연습 또는 기간 내에 완료할 수 없는 지속적인 프로세스이므로 AWS Incident Detection and Response는 두 단계로 관찰 가능성을 구현합니다.

- 온보딩 단계 : 온보딩 중 관찰 가능성은 애플리케이션의 비즈니스 결과가 손상된 시점을 감지하는 데 중점을 둡니다. 이를 위해 온보딩 단계 동안의 관찰 가능성은 애플리케이션 계층에서 주요 비즈니스 결과 지표를 정의하여 워크로드 AWS 중단을 알리는 데 중점을 둡니다. 이렇게 하면 이러한 중단에 즉시 대응하고 복구에 도움이 될 AWS 수 있습니다.

- 온보딩 후 단계: AWS 인시던트 감지 및 대응은 인프라 수준 지표의 정의, 지표 조정, 고객의 성숙도에 따른 추적 및 로그 설정 등 관찰 가능성을 위한 다양한 사전 예방 서비스를 제공합니다. 이러한 서비스의 구현은 몇 개월에 걸쳐 진행될 수 있으며 여러 팀이 참여할 수 있습니다. AWS Incident Detection and Response는 관찰성 설정에 대한 지침을 제공하며 고객은 워크로드 환경에서 필요한 변경 사항을 구현해야 합니다. 관찰 기능 실습 구현에 도움이 필요하면 기술 계정 관리자()에게 요청을 제기하세요TAMs.

인시던트 감지 및 대응을 통한 인시던트 관리

AWS 인시던트 감지 및 대응은 지정된 인시던트 관리자 팀이 제공하는 연중무휴 사전 예방적 모니터링 및 인시던트 관리를 제공합니다. 다음 다이어그램은 애플리케이션 경보가 경보 생성, Incident Manager 참여, AWS 인시던트 해결 및 인시던트 후 검토를 포함하여 인시던트를 트리거할 때의 표준 인시던트 관리 프로세스를 간략하게 설명합니다.

1. 경보 생성 : 워크로드에서 트리거된 경보는 Amazon을 통해 AWS 인시던트 감지 및 대응 EventBridge 으로 푸시됩니다. AWS Incident Detection and Response는 경보와 연결된 실행서를 자동으로 가져와 인시던트 관리자에게 알립니다. 워크로드에 인시던트 감지 및 대응으로 모니터링되는 경보로 감지되지 않는 중요한 AWS 인시던트가 발생하는 경우 지원 사례를 생성하여 인시던트 대응을 요청할 수 있습니다. 인시던트 대응 요청에 대한 자세한 내용은 섹션을 참조하세요인시던트 응답 요청.
2. AWS Incident Manager 참여 : 인시던트 관리자가 경보에 응답하고 다자간 통화에 참여하거나 달리 실행서에 지정된 대로 참여시킵니다. 인시던트 관리자는 의 상태를 확인하여 경보가 워크로드에서 AWS 서비스 사용하는 의 문제와 관련이 있는지 AWS 서비스 확인하고 기본 서비스의 상태에 대한 조언을 제공합니다. 필요한 경우 인시던트 관리자는 사용자를 대신하여 사례를 생성하고 지원을 위해 적절한 AWS 전문가를 참여시킵니다.

   AWS Incident Detection and Response는 애플리케이션에 대해 AWS 서비스 특별히 모니터링하기 때문에 AWS 인시던트 감지 및 대응은 AWS 서비스 이벤트가 선언되기 전에도 인시던트가 AWS 서비스 문제와 관련이 있다고 판단할 수 있습니다. 이 시나리오에서는 인시던트 관리자가 의 상태를 알리고 AWS 서비스, AWS 서비스 이벤트 인시던트 관리 흐름을 트리거하고, 해결 시 서비스 팀과 후속 조치를 취합니다. 제공된 정보는 AWS 서비스 이벤트의 영향을 완화하기 위해 복구 계획 또는 해결 방법을 조기에 구현할 수 있는 기회를 제공합니다. 자세한 내용은 서비스 이벤트에 대한 인시던트 관리 단원을 참조하십시오.
3. 인시던트 해결 : 인시던트 관리자는 필요한 AWS 팀 전체에서 인시던트를 조정하고 인시던트가 완화되거나 해결될 때까지 적절한 AWS 전문가와 계속 협력해야 합니다.
4. 사후 인시던트 검토(요청된 경우): 인시던트 후 AWS 인시던트 감지 및 대응은 요청 시 사후 인시던트 검토를 수행하고 사후 인시던트 보고서를 생성할 수 있습니다. 인시던트 후 보고서에는 문제에 대한 설명, 영향, 참여 팀, 인시던트를 완화하거나 해결하기 위해 취한 해결 방법 또는 조치가 포함되어 있습니다. 사후 인시던트 보고서에는 인시던트 재발 가능성을 줄이거나 향후 유사한 인시던트 발생 관리를 개선하는 데 사용할 수 있는 정보가 포함될 수 있습니다. 사후 인시던트 보고서는 근본 원인 분석()이 아닙니다RCA. 사후 인시던트 보고서 외에 RCA 를 요청할 수 있습니다. 인시던트 후 보고서의 예는 다음 섹션에 나와 있습니다.

> **Important**
>
> 다음 보고서 템플릿은 예시일 뿐입니다.

Post ** Incident ** Report ** Template
Post Incident Report - 0000000123
Customer: Example Customer
AWS Support case ID(s): 0000000000
Customer internal case ID (if provided): 1234567890
Incident start: 2023-02-04T03:25:00 UTC
Incident resolved: 2023-02-04T04:27:00 UTC
Total Incident time: 1:02:00 s
Source Alarm ARN: arn:aws:cloudwatch:us-east-1:000000000000:alarm:alarm-prod-workload-impaired-useast1-P95

Problem Statement:
Outlines impact to end users and operational infrastructure impact.
Starting at 2023-02-04T03:25:00 UTC, the customer experienced a large scale outage of their workload that lasted one hour and two minutes and spanning across all Availability Zones where the application is deployed. During impact, end users were unable to connect to the workload's Application Load Balancers (ALBs) which service inbound communications to the application.

Incident Summary:

Summary of the incident in chronological order and steps taken by AWS Incident Managers to direct the incident to a path to mitigation.
At 2023-02-04T03:25:00 UTC, the workload impairments alarm triggered a critical incident for the workload. AWS Incident Detection and Response Managers responded to the alarm, checking AWS service health and steps outlined in the workload’s runbook.
At 2023-02-04T03:28:00 UTC, ** per the runbook, the alarm had not recovered and the Incident Management team sent the engagement email to the customer’s Site Reliability Team (SRE) team, created a troubleshooting bridge, and an AWS Support support case on behalf of the customer.
At 2023-02-04T03:32:00 UTC, ** the customer’s SRE team, and AWS Support Engineering joined the bridge. The Incident Manager confirmed there was no on-going AWS impact to services the workload depends on. The investigation shifted to the specific resources in the customer account.
At 2023-02-04T03:45:00 UTC, the Cloud Support Engineer discovered a sudden increase in traffic volume was causing a drop in connections. The customer confirmed this

```
 ALB was newly provisioned to handle an increase in workload traffic for an on-going
 promotional event.
  At 2023-02-04T03:56:00 UTC, the customer instituted back off and retry logic. The
 Incident Manager worked with the Cloud Support Engineer to raise an escalation a
 higher support level to quickly scale the ALB per the runbook.
  At 2023-02-04T04:05:00 UTC, ALB support team initiates scaling activities. The
 back-off/retry logic yields mild recovery but timeouts are still being seen for some
 clients.
 By 2023-02-04T04:15:00 UTC, scaling activities complete and metrics/alarms return to
 pre-incident levels. Connection timeouts subside.
  At 2023-02-04T04:27:00 UTC, per the runbook the call was spun down, after 10 minutes
 of recovery monitoring. Full mitigation is agreed upon between AWS and the customer.

Mitigation:
Describes what was done to mitigate the issue. NOTE: this is not a Root Cause Analysis
 (RCA).
  Back-off and retries yielded mild recovery. Full mitigation happened after escalation
 to ALB support team (per runbook) to scale the newly provisioned ALB.

Follow up action items (if any):
Action items to be reviewed with your Technical Account Manager (TAM), if required.
Review alarm thresholds to engage AWS Incident Detection and Response closer to the
 time of impact.
Work with AWS Support and TAM team to ensure newly created ALBs are pre-scaled to
 accommodate expected spikes in workload traffic.
```

주제

- 애플리케이션 팀을 위한 AWS Support Center에 대한 액세스 권한 프로비저닝
- 서비스 이벤트에 대한 인시던트 관리
- 인시던트 응답 요청
- 를 사용하여 인시던트 감지 및 대응 지원 사례 관리 AWS Support App in Slack

애플리케이션 팀을 위한 AWS Support Center에 대한 액세스 권한 프로비저닝

AWS 인시던트 감지 및 대응은 인시던트 수명 주기 동안 AWS Support 사례를 통해 사용자와 통신합니다. 인시던트 관리자에 대응하려면 팀이 AWS Support 센터에 액세스할 수 있어야 합니다.

액세스 프로비저닝에 대한 자세한 내용은 사용 설명서의 AWS Support 센터에 대한 액세스 관리를 참조하세요. AWS Support

서비스 이벤트에 대한 인시던트 관리

AWS 인시던트 감지 및 대응은 워크로드에 영향을 미치는지 여부에 관계없이 해당 AWS 리전에서 진행 중인 서비스 이벤트를 알립니다. AWS 서비스 이벤트 중에 AWS 인시던트 감지 및 대응은 지원 사례를 생성하고 AWS , 는 다자간 통화 브리지에 참여하여 영향 및 감정에 대한 피드백을 받고, 이벤트 중에 복구 계획을 호출하는 지침을 제공합니다. 이벤트의 세부 정보가 AWS Health 포함된 알림을 받을 수도 있습니다. AWS 소유 서비스 이벤트(예: 다른 AWS 리전에서 운영, 손상된 AWS 서비스 사용 금지 등)의 영향을 받지 않는 고객은 표준 참여의 지원을 계속 받습니다. 에 대한 자세한 내용은 란 무엇입니까 AWS Health?를 AWS Health참조하세요.

다음 다이어그램은 AWS 서비스 이벤트가 발생할 때 따르는 인시던트 흐름 또는 프로세스를 보여 주며, AWS 팀, 인시던트 대응 팀 및 고객이 서비스 중단 또는 문제를 식별, 완화 및 해결하기 위해 취하는 단계를 간략하게 설명합니다.

서비스 이벤트에 대한 사후 인시던트 보고서(요청된 경우): 서비스 이벤트로 인해 인시던트가 발생하는 경우 AWS 인시던트 감지 및 응답을 요청하여 사후 인시던트 검토를 수행하고 사후 인시던트 보고서를 생성할 수 있습니다. 서비스 이벤트에 대한 사후 인시던트 보고서에는 다음이 포함됩니다.

- 문제에 대한 설명
- 인시던트의 영향
- AWS Health 대시보드에서 공유되는 정보
- 인시던트 중에 참여한 팀
- 인시던트를 완화하거나 해결하기 위해 취한 해결 방법 및 조치

서비스 이벤트에 대한 인시던트 후 보고서에는 인시던트 재발 가능성을 줄이거나 향후 유사한 인시던트 발생 관리를 개선하는 데 사용할 수 있는 정보가 포함될 수 있습니다. 서비스 이벤트에 대한 사후 인시던트 보고서는 근본 원인 분석()이 아닙니다RCA. 서비스 이벤트에 대한 사후 인시던트 보고서 외에 RCA 를 요청할 수 있습니다.

다음은 서비스 이벤트에 대한 사후 인시던트 보고서의 예입니다.

> **Note**
>
> 다음 보고서 템플릿은 예시일 뿐입니다.

```
Post Incident Report - LSE000123
Customer: Example Customer
AWS Support Case ID(s): 0000000000
Incident Start: Example: 1 January 2024, 3:30 PM UTC
Incident Resolved: Example: 1 January 2024, 3:30 PM UTC
Incident Duration: 1:02:00
Service(s) Impacted: Lists the impacted services such as EC2, ALB
Region(s): Lists the impacted AWS Regions, such as US-EAST-1
Alarm Identifiers: Lists any customer alarms that triggered during the Service Level
 Event

Problem Statement:
Outlines impact to end users and operational infrastructure impact during the Service
 Level Event.
Starting at 2023-02-04T03:25:00 UTC, the customer experienced a service outage...

Impact Summary for Service Level Event:
(This section is limited to approved messaging available on the AWS Health Dashboard)
Outline approved customer messaging as provided on the AWS Health Dashboard.
Between 1:14 PM and 4:33 PM UTC, we experienced increased error rates for the Amazon
 SNS Publish, Subscribe, Unsubscribe, Create Topic, and Delete Topic APIs in the EU-
WEST-1 Region. The issue has been resolved and the service is operating normally.

Incident Summary:
Summary of the incident in chronological order and steps taken by AWS Incident Managers
 during the Service Level Event to direct the incident to a path to mitigation.
At 2024-01-04T01:25:00 UTC, the workload alarm triggered a critical incident...
At 2024-01-04T01:27:00 UTC, customer was notified via case 000000000 about the
 triggered alarm
At 2024-01-04T01:30:00 UTC, IDR team identified an ongoing service event which was
 related to the customer triggered alarm
At 2024-01-04T01:32:00 UTC, IDR team sent an impact case correspondence requesting for
 the incident bridge details
At 2024-01-04T01:32:00 UTC, customer provided the incident bridge details
At 2024-01-04T01:32:00 UTC, IDR team joined the incident bridge and provided
 information about the ongoing service outage
```

```
By 2024-01-04T02:35:00 UTC, customer failed over to the secondary region (EU-WEST-1) to
 mitigate impact...
At 2024-01-04T03:27:00 UTC, customer confirmed recovery, the call was spun down...

Mitigation:
Describes what was done to mitigate the issue. NOTE: this is not a Root Cause Analysis
 (RCA).
Back-off and retries yielded mild recovery. Full mitigation happened ...

Follow up action items (if any):
Action items to be reviewed with your Technical Account Manager (TAM), if required.
Review alarm thresholds to engage AWS Incident Detection and Response closer ...
Work with AWS Support and TAM team to ensure ...
```

인시던트 응답 요청

워크로드에 인시던트 감지 및 대응으로 모니터링되는 경보로 감지되지 않는 중요한 AWS 인시던트가 발생하는 경우 지원 사례를 생성하여 인시던트 대응을 요청할 수 있습니다. 온보딩, AWS Support Center Console AWS Support API, 또는 를 사용하는 과정에서의 워크로드를 포함하여 Incident Detection and Response를 구독하는 모든 워크로드에 대해 AWS Incident Response를 요청할 수 있습니다 AWS Support App in Slack.

다음 다이어그램은 인시던트 감지 및 대응 팀에서 인시던트 지원을 요청하는 AWS 고객의 워크플로를 보여 end-to-end 주며, 초기 요청부터 조사, 완화 및 해결까지의 단계를 자세히 설명합니다.

워크로드에 적극적으로 영향을 미치는 인시던트에 대한 인시던트 응답을 요청하려면 AWS Support 사례를 생성합니다. 지원 사례가 제기되면 AWS Incident Detection and Response는 워크로드 복구를 가속화하는 데 필요한 AWS 전문가와의 회의 브리지에 참여합니다.

를 사용하여 인시던트 응답 요청 AWS Support Center Console

1. 를 연 AWS Support Center Console다음 사례 생성 을 선택합니다.
2. 기술 을 선택합니다.
3. 서비스 에서 인시던트 감지 및 응답 을 선택합니다.
4. 범주 에서 활성 인시던트 를 선택합니다.
5. 심각도 에서 비즈니스 크리티컬 시스템 다운을 선택합니다.

6. 이 인시던트의 주제를 입력합니다. 예:

   AWS 인시던트 감지 및 대응 - 활성 인시던트 - workload_name
7. 이 인시던트에 대한 문제 설명을 입력합니다. 다음 세부 정보를 추가합니다.
   - 기술 정보:

     영향을 받는 서비스(들):

     영향을 받는 리소스(들):

     영향을 받는 리전(들):

     워크로드 이름:
   - 비즈니스 정보:

     비즈니스에 미치는 영향에 대한 설명:

     [선택 사항] Customer Bridge 세부 정보:
8. 추가 연락처 섹션에서 이 인시던트에 대한 서신을 수신하려는 이메일 주소를 입력합니다.

   다음 그림은 추가 연락처 필드가 강조 표시된 콘솔 화면을 보여줍니다.

9. 제출을 선택합니다.

   Incident Response 요청을 제출한 후 조직의 이메일 주소를 추가할 수 있습니다. 주소를 추가하려면 사례에 회신한 다음 추가 연락처 섹션에 이메일 주소를 추가합니다.

   다음 그림은 회신 버튼이 강조 표시된 사례 세부 정보 화면을 보여줍니다.

   다음 그림은 추가 연락처 필드와 제출 버튼이 강조 표시된 사례 회신을 보여줍니다.

10. AWS 인시던트 감지 및 대응은 5분 이내에 사례를 확인하고 적절한 AWS 전문가와의 다자간 통화 브리지에 참여합니다.

를 사용하여 인시던트 응답 요청 AWS Support API

를 AWS Support API 사용하여 프로그래밍 방식으로 지원 사례를 생성할 수 있습니다. 자세한 내용은 AWS Support 사용 설명서의 정보를 AWS Support API 참조하세요.

를 사용하여 인시던트 응답 요청 AWS Support App in Slack

AWS Support App in Slack 를 사용하여 인시던트 응답을 요청하려면 다음 단계를 완료합니다.

1. 를 구성한 Slack 채널을 엽니다 AWS Support App in Slack .
2. 다음 명령을 입력합니다.

```
/awssupport create
```

3. 이 인시던트의 주제를 입력합니다. 예를 들어AWS, Incident Detection and Response - Active Incident - workload_name 을 입력합니다.
4. 이 인시던트에 대한 문제 설명을 입력합니다. 다음 세부 정보를 추가합니다.

   기술 정보:

   영향을 받는 서비스(들):

   영향을 받는 리소스(들):

   영향을 받는 리전(들):

   워크로드 이름:

   비즈니스 정보:

   비즈니스에 미치는 영향에 대한 설명:

   [선택 사항] Customer Bridge 세부 정보:
5. Next(다음)를 선택합니다.

6. 문제 유형 에서 기술 지원을 선택합니다.
7. 서비스 에서 인시던트 감지 및 대응 을 선택합니다.
8. 범주 에서 활성 인시던트 를 선택합니다.
9. 심각도 에서 비즈니스 크리티컬 시스템 다운을 선택합니다.

10. 필요에 따라 추가 연락처 필드에 쉼표로 구분하여 최대 10개의 추가 연락처를 입력합니다. 이러한 추가 연락처는 이 인시던트에 대한 이메일 서신 사본을 받습니다.

11.검토를 선택합니다.

12.사용자만 볼 수 있는 새 메시지가 Slack 채널에 나타납니다. 사례 세부 정보를 검토한 다음 사례 생성 을 선택합니다.

13.케이스 ID는 의 새 메시지에 제공됩니다 AWS Support App in Slack.

14.인시던트 감지 및 대응은 5분 이내에 사례를 확인하고 적절한 AWS 전문가와의 다자간 통화 브리지에 참여합니다.

15.인시던트 감지 및 응답의 응답은 대/소문자 스레드에서 업데이트됩니다.

를 사용하여 인시던트 감지 및 대응 지원 사례 관리 AWS Support App in Slack

를 사용하면 Slack에서 AWS Support 사례를 관리하고, AWS 인시던트 감지 및 대응 워크로드에서 새 경보 시작 인시던트에 대한 알림을 수신하고, 인시던트 대응 요청을 생성할 AWS Support App in Slack수 있습니다. https://docs.aws.amazon.com/IDR/latest/userguide/inbound-incident-idr.html

를 구성하려면 AWS Support 사용 설명서 에 제공된 지침을 AWS Support App in Slack따릅니다.

> **Important**
>
> - 워크로드의 모든 경보 시작 인시던트에 대한 알림을 Slack에서 받으려면 AWS 인시던트 감지 및 대응에 온보딩된 모든 워크로드 계정에 AWS Support App in Slack 대해 를 구성해야 합니다. 지원 사례는 워크로드 경보가 시작된 계정에 생성됩니다.
> - 인시던트 중에 사용자를 대신하여 여러 고심도 지원 사례를 열어 AWS Support 해석기를 참여시킬 수 있습니다. Slack 채널 에 대한 알림 구성과 일치하는 인시던트 중에 열린 모든 지원 사례에 대한 알림을 Slack에서 수신합니다.
> - 를 통해 수신한 알림은 AWS 인시던트 감지 및 대응을 통해 이메일 또는 전화를 통해 발생하는 워크로드의 초기 및 에스컬레이션 연락처를 대체하지 AWS Support App in Slack 않습니다.

주제

Slack에서 경보 시작 인시던트 알림

Slack 채널 AWS Support App in Slack 에서 를 구성하면 AWS Incident Detection and Response 모니터링 워크로드에서 경보 시작 인시던트에 대한 알림을 받게 됩니다.

다음 예제는 경보 시작 인시던트에 대한 알림이 Slack에 표시되는 방법을 보여줍니다.

알림 예

경보 시작 인시던트가 AWS 인시던트 감지 및 대응에 의해 확인되면 다음과 유사한 알림이 Slack에서 생성됩니다.

AWS Incident Detection and Response에서 추가한 전체 서신을 보려면 세부 정보 참조를 선택합니다.

AWS 인시던트 감지 및 대응의 추가 업데이트는 사례의 스레드에 표시됩니다.

세부 정보 보기를 선택하여 AWS 인시던트 감지 및 대응에 추가된 전체 서신을 봅니다.

Slack에서 인시던트 응답 요청 생성

를 통해 인시던트 응답 요청을 생성하는 방법에 대한 지침은 섹션을 AWS Support App in Slack참조하세요인시던트 응답 요청.

인시던트 감지 및 대응 보고

AWS Incident Detection and Response는 서비스가 구성된 방식, 인시던트 기록, Incident Detection and Response 서비스의 성능을 이해하는 데 도움이 되는 운영 및 성능 데이터를 제공합니다. 이 페이지에서는 구성 데이터, 인시던트 데이터 및 성능 데이터를 포함하여 사용 가능한 데이터 유형을 다룹니다.

구성 데이터

- 온보딩된 모든 계정
- 모든 애플리케이션의 이름
- 각 애플리케이션과 연결된 경보, 실행서 및 지원 프로파일

인시던트 데이터

- 각 애플리케이션의 인시던트 날짜, 수 및 기간
- 특정 경보와 관련된 인시던트의 날짜, 수 및 기간
- 사후 인시던트 보고서

성능 데이터

- 서비스 수준 목표(SLO) 성능

필요한 운영 및 성능 데이터는 기술 계정 관리자에게 문의하세요.

인시던트 탐지 및 대응 보안 및 복원력

책임 AWS 공유 모델은 의 데이터 보호에 적용됩니다 AWS Support. https://aws.amazon.com/compliance/shared-responsibility-model/ 이 모델에 설명된 대로 AWS 는 모든 를 실행하는 글로벌 인프라를 보호할 책임이 있습니다 AWS 클라우드. 사용자는 인프라에서 호스팅되는 콘텐츠를 관리해야 합니다. 이 콘텐츠에는 사용하는 에 대한 보안 구성 및 관리 작업이 포함되어 AWS 서비스 있습니다.

데이터 프라이버시에 대한 자세한 내용은 데이터 프라이버시 섹션을 FAQ참조하세요.

유럽의 데이터 보호에 대한 자세한 내용은 AWS 보안 블로그의 AWS 책임 공유 모델 및 GDPR 블로그 게시물을 참조하세요.

데이터 보호를 위해 AWS 계정 자격 증명을 보호하고 AWS Identity and Access Management ()를 사용하여 개별 사용자 계정을 설정하는 것이 좋습니다IAM. 이러한 방식에서는 각 사용자에게 자신의 직무를 충실히 이행하는 데 필요한 권한만 부여됩니다. 또한 다음과 같은 방법으로 데이터를 보호하는 것이 좋습니다.

- 각 계정에 다단계 인증(MFA)을 사용합니다.
- Secure Sockets Layer/Transport Layer Security(SSL/TLS) 인증서를 사용하여 AWS 리소스와 통신합니다. TLS 1.2 이상을 사용하는 것이 좋습니다. 자세한 내용은 SSL/TLS 인증서란 무엇입니까?를 참조하세요.
- 를 사용하여 API 및 사용자 활동 로깅을 설정합니다 AWS CloudTrail. 자세한 내용은 AWS CloudTrail을 참조하세요.
- AWS 암호화 AWS 솔루션과 서비스 내 모든 기본 보안 제어를 사용합니다. 자세한 내용은 AWS 암호화 서비스 및 도구 를 참조하세요.
- Amazon S3에 저장된 개인 데이터를 검색하고 보호하는 데 도움이 되는 Amazon Macie와 같은 고급 관리형 보안 서비스를 사용합니다. Amazon Macie 에 대한 자세한 내용은 Amazon Macie 참조하세요.
- 명령줄 인터페이스 또는 FIPS 를 AWS 통해 에 액세스할 때 140-2개의 검증된 암호화 모듈이 필요한 경우 FIPS 엔드포인트를 API사용합니다. 사용 가능한 FIPS 엔드포인트에 대한 자세한 내용은 연방 정보 처리 표준(FIPS) 140-2를 참조하세요.

고객의 이메일 주소와 같은 기밀 정보나 중요한 정보는 태그나 이름 필드와 같은 자유 양식 필드에 입력하지 않는 것이 좋습니다. 여기에는 콘솔, API AWS CLI, 또는 를 AWS 서비스 사용하여 AWS Support 또는 다른 로 작업하는 경우가 포함됩니다 AWS SDKs. 이름에 사용되는 태그 또는 자유 형식 필드에 입력하는 모든 데이터는 청구 또는 진단 로그에 사용될 수 있습니다. 외부 서버에 URL를 제공

하는 경우 해당 서버에 대한 요청을 검증URL하기 위해 에 보안 인증 정보를 포함하지 않는 것이 좋습니다.

AWS 계정에 대한 인시던트 감지 및 대응 액세스

AWS Identity and Access Management (IAM)는 리소스에 대한 액세스를 안전하게 제어하는 데 AWS 도움이 되는 웹 서비스입니다. IAM 를 사용하여 리소스를 사용할 수 있는 인증(로그인) 및 권한(권한 보유)을 받은 사용자를 제어할 수 있습니다.

AWS 인시던트 감지 및 대응과 경보 데이터

기본적으로 Incident Detection and Response는 계정의 모든 CloudWatch 경보의 Amazon 리소스 이름(ARN)과 상태를 수신한 다음 온보딩된 경보가 ALARM 상태로 변경될 때 인시던트 감지 및 응답 프로세스를 시작합니다. 계정에서 경보에 대해 인시던트 감지 및 대응이 수신하는 정보를 사용자 지정하려면 기술 계정 관리자에게 문의하세요.

문서 이력

다음 표에서는 IDR 가이드의 마지막 릴리스 이후 문서에 대한 중요한 변경 사항을 설명합니다.

- 최신 설명서 업데이트: 2024년 11월 1일

변경 사항	설명	날짜
추가 AWS 리전 됨	인시던트 감지 및 대응 가용성 섹션에 추가 AWS 리전 정보가 추가되었습니다. 업데이트된 섹션: 인시던트 감지 및 대응을 위한 리전 가용성	2024년 11월 1일
페이지를 사용하여 인시던트 감지 및 대응 지원 사례 관리를 업데이트합니다. AWS Support App in Slack	인시던트 관리 아래의 페이지를 이동하고, 텍스트를 수정하고, 스크린샷을 교체했습니다. 업데이트된 섹션: 를 사용하여 인시던트 감지 및 대응 지원 사례 관리 AWS Support App in Slack	2024년 10월 10일
새 페이지 추가 AWS Support App in Slack 인시던트 감지 및 대응으로 AWS 인시던트 관리 업데이트	에 대한 새 페이지 추가 AWS Support App in Slack 인시던트 감지 및 대응으로 AWS 인시던트 관리를 업데이트하여 새 섹션인 "를 사용하여 인시던트 대응 요청'을 추가했습니다 AWS Support App in Slack.	2024년 9월 10일
업데이트된 계정 구독	계정 구독을 요청할 때 지원 사례를 열 수 있는 위치에 대한 세부 정보를 포함하도록 계정 구독 섹션을 업데이트했습니다. 업데이트된 섹션: 인시던트 감지 및 대응에 워크로드 구독	2024년 6월 12일
이제 서비스 이벤트에 대한 사후 인시던트 보고서를 사용할 수 있습니다.	서비스 이벤트에 대한 인시던트 관리 섹션을 업데이트하여 서비스 이벤트에 대한 사후 인시던트 보고서에 대한 정보를 포함했습니다.	2024년 5월 8일

변경 사항	설명	날짜
	업데이트된 섹션: 서비스 이벤트에 대한 인시던트 관리	
새 섹션 추가: 워크로드 오프보드	오프보딩 워크로드에 대한 정보를 포함하도록 시작하기에 워크로드 오프로드 섹션 추가 자세한 내용은 인시던트 감지 및 대응에서 워크로드 오프보드 단원을 참조하십시오.	2024년 3월 28일
업데이트된 계정 구독	오프보딩 워크로드에 대한 정보를 포함하도록 계정 구독 섹션 업데이트 자세한 내용은 계정 구독을 참조하세요.	2024년 3월 28일
업데이트된 테스트	온보딩 프로세스의 마지막 단계로 게임데이 테스트에 대한 정보를 포함하도록 테스트 섹션을 업데이트했습니다. 업데이트된 섹션: 인시던트 감지 및 대응에서 온보딩된 워크로드 테스트	2024년 2월 29일
AWS 인시던트 탐지 및 대응이란 무엇인가 업데이트	AWS 인시던트 감지 및 대응이란 무엇입니까 섹션을 업데이트했습니다. 업데이트된 섹션: AWS 인시던트 감지 및 대응이란 무엇입니까?	2024년 2월 19일
설문지 섹션 업데이트	워크로드 온보딩 설문지를 업데이트하고 경보 수집 설문지를 추가했습니다. 온보딩 설문지에서 워크로드 온보딩 및 경보 수집 설문지 로 섹션의 이름을 변경했습니다. 업데이트된 섹션: 인시던트 감지 및 대응의 워크로드 온보딩 및 경보 수집 설문지	2024년 2월 2일

변경 사항	설명	날짜
AWS 서비스 이벤트 및 온보딩 정보 업데이트	온보딩을 위한 새로운 정보로 여러 섹션을 업데이트했습니다. 업데이트된 섹션: • 서비스 이벤트에 대한 인시던트 관리 • 인시던트 감지 및 대응의 워크로드 검색 • 인시던트 감지 및 대응에 온보딩 • 인시던트 감지 및 대응에 워크로드 구독 새 섹션 • 애플리케이션 팀을 위한 AWS Support Center에 대한 액세스 권한 프로비저닝	2024년 1월 31일
관련 정보 섹션 추가	액세스 프로비저닝 에 관련 정보 섹션이 추가되었습니다. 업데이트된 섹션: 인시던트 감지 및 대응에 대한 경보 수집을 위한 액세스 권한 프로비저닝	2024년 1월 17일
예제 단계 업데이트	예제: Datadog 및 Splunk 의 알림 통합에서 2, 3 및 4단계 절차를 업데이트했습니다. 업데이트된 섹션: 예: Datadog 및 Splunk의 알림 통합	2023년 12월 21일
소개 그래픽 및 텍스트 업데이트	Amazon 와 직접 통합APMs되는 의 Ingest 경보의 그래픽이 EventBridge 업데이트되었습니다. 업데이트된 섹션: 인시던트 감지 및 대응에서 인시던트에 대응하기 위한 실행서 및 대응 계획 개발	2023년 12월 21일

변경 사항	설명	날짜
런북 템플릿 업데이트	AWS 인시던트 감지 및 대응을 위한 런북 개발의 런북 템플릿을 업데이트했습니다. 업데이트된 섹션: 인시던트 감지 및 대응에서 인시던트에 대응하기 위한 실행서 및 대응 계획 개발	2023년 12월 4일
업데이트된 경보 구성	경보 구성에 대한 자세한 정보로 CloudWatch 경보 구성을 업데이트했습니다. 새 섹션: 인시던트 감지 및 대응에서 비즈니스 요구 사항에 맞는 CloudWatch 경보 생성 새 섹션: CloudFormation 템플릿을 사용하여 인시던트 감지 및 대응에서 CloudWatch 경보 빌드 새 섹션: 인시던트 감지 및 대응의 CloudWatch 경보 사용 사례 예	2023년 9월 28일
시작 업데이트	워크로드 변경 요청에 대한 정보로 시작하기가 업데이트되었습니다. 새 섹션: 인시던트 감지 및 대응에서 온보딩된 워크로드에 대한 변경 요청 업데이트된 섹션: 인시던트 감지 및 대응에 워크로드 구독	2023년 9월 5일
시작하기의 새 섹션	AWS 인시던트 감지 및 대응에 알림 AWS 인시던트 감지 및 대응에 경보 삽입수신이 추가되었습니다.	2023년 6월 30일
원본 문서	AWS 인시던트 감지 및 대응이 처음 게시됨	2023년 3월 15일

기계 번역으로 제공되는 번역입니다. 제공된 번역과 원본 영어의 내용이 상충하는 경우에는 영어 버전이 우선합니다.