AWS 사고 탐지 및 대응 개념 및 절차

AWS 사고 탐지 및 대응 사용 설명서

버전 May 12, 2026

AWS 사고 탐지 및 대응 사용 설명서: AWS 사고 탐지 및 대응 개념 및 절차

Table of Contents

AWS 사고 탐지 및 대응이란 무엇인가요? 1
이용 약관 1
아키텍처 2
역할 및 책임 3
리전 가용성 5
시작하기 8
워크로드 정보 8
경보 정보 8
워크로드 온보딩 8
IDR CLI를 통한 온보딩 9
경보 수집 10
경보 수집 단계 10
경보 수집을 위한 대체 옵션 10
액세스 프로비저닝 10
경보 정의 11
경보 최적화 31
경보 검토 31
경보 테스트 31
경보 가동 33
온보딩 설문지(예외 경로) 33
워크로드 온보딩 설문지 - 일반 질문 34
워크로드 온보딩 설문지 - 아키텍처 질문 34
경보 수집 설문지 - 개요 36
경보 수집 설문지 - 런북 질문 37
경보 매트릭스 38
워크로드 관리 43
런북 및 대응 계획 개발 43
온보딩된 워크로드 테스트 50
CloudWatch 경보 32
타사 APM 경보 32
핵심 결과물 32
워크로드 변경 요청 51
경보 억제 52
경보 소스에서 경보 억제 53

경보를 억제하기 위한 워크로드 변경 요청 제출 58
자습서: 지표 수학 함수를 사용하여 경보 억제 58
자습서: 지표 수학 함수를 제거하여 경보 억제 해제 60
워크로드 오프보딩 61
모니터링 및 관찰성 62
관찰성 구현 62
인시던트 관리 64
애플리케이션 팀의 액세스 권한 프로비저닝 66
인시던트 대응 요청 67
AWS Support Center Console을 통한 요청 67
AWS Support API를 통한 요청 68
AWS Support App in Slack을 통한 요청 68
AWS Support App in Slack을 사용하여 사고 탐지 및 대응 지원 사례 관리 69
Slack에서 경보 시작 인시던트 알림 70
Slack에서 인시던트 대응 요청 생성 71
보고 72
보안 및 복원력 73
계정에 액세스 74
경보 데이터 74
문서 이력 75

AWS 사고 탐지 및 대응이란 무엇인가요?

AWS 사고 탐지 및 대응은 적격 AWS Enterprise Support 고객에게 선제적 인시던트 참여를 제공하여 장애 발생 가능성을 줄이고 중단 발생 시 중요한 워크로드의 복구를 가속화합니다. 사고 탐지 및 대응을 통해 AWS와 협력하여 온보딩된 각 워크로드에 맞게 사용자 지정된 런북 및 대응 계획을 개발할 수 있습니다.

사고 탐지 및 대응은 다음과 같은 주요 기능을 제공합니다.

- 향상된 관찰성: AWS 전문가는 워크로드의 애플리케이션 계층과 인프라 계층 간에 지표와 경보를 정의하고 상호 연관시켜 중단을 조기에 탐지하는 데 도움이 되는 지침을 제공합니다.
- 5분 응답 시간: 인시던트 관리 엔지니어는 경보 발생 후 5분 이내에, 워크로드에서 또는 사용자가 제출하는 중요한 사례에 대응하여 사전에 고객 응대를 제공합니다.
- 더 빠른 해결: IME는 사용자의 워크로드에 맞춰 개발된 사전 정의된 및 사용자 지정 런북을 사용하고, 사용자를 대신하여 지원 사례를 생성하며, 워크로드 관련 문제를 관리합니다. IME가 인시던트에 대한 단일 스레드 소유권을 제공하고 인시던트가 해결될 때까지 적절한 AWS 전문가와 계속 소통합니다.
- 장애 가능성 감소: 해결 후 IME는 인시던트 후 검토(요청 시)를 제공합니다. 또한 AWS 전문가는 고객과 협력해 학습한 교훈을 적용하여 인시던트 대응 계획 및 런북을 개선합니다. 워크로드에 대한 지속적인 복원력 추적을 위해 AWS Resilience Hub를 활용할 수도 있습니다.

주제

- 사고 탐지 및 대응 이용 약관
- 사고 탐지 및 대응 아키텍처
- 인시던트 탐지 및 대응의 역할 및 책임
- 사고 탐지 및 대응의 리전 가용성

사고 탐지 및 대응 이용 약관

다음 목록은 AWS 사고 탐지 및 대응 사용에 대한 주요 요구 사항과 제한 사항을 간략하게 설명합니다. 이 정보는 지원 플랜 요구 사항, 온보딩 프로세스 및 최소 구독 기간과 같은 측면을 다루므로 서비스를 사용하기 전에 이해하는 데 중요합니다.

- AWS 사고 탐지 및 대응은 직접 및 파트너 재판매 Enterprise Support 계정에서 사용할 수 있습니다.

- AWS 사고 탐지 및 대응은 파트너 주도 지원 계정에서는 사용할 수 없습니다.
- 사고 탐지 및 대응 서비스 기간 동안 항상 AWS Enterprise Support를 유지해야 합니다. 자세한 내용은 엔터프라이즈 지원을 참조하세요. Enterprise Support가 종료되면 AWS 사고 탐지 및 대응 서비스에서 동시에 제거됩니다.
- AWS 사고 탐지 및 대응의 모든 워크로드는 워크로드 온보딩 프로세스를 거쳐야 합니다.
- AWS 사고 탐지 및 대응을 구독하는 최소 기간은 구십(90)일입니다. 모든 취소 요청은 의도한 취소 발효일 삼십(30)일 전에 제출해야 합니다.
- AWS에서는 AWS 개인정보 처리방침에 설명된 대로 정보를 처리합니다.

> **Note**
>
> 사고 탐지 및 대응 결제 관련 질문은 AWS 결제 관련 도움말 받기를 참조하세요.

사고 탐지 및 대응 아키텍처

AWS 사고 탐지 및 대응은 다음 그림과 같이 기존 환경과 통합됩니다. 이 아키텍처에는 다음 서비스가 포함됩니다.

- Amazon EventBridge: Amazon EventBridge는 워크로드와 AWS 사고 탐지 및 대응 간의 유일한 통합 지점 역할을 합니다. 경보는 AWS에서 관리하는 사전 정의된 규칙을 사용하여 Amazon EventBridge를 통해 Amazon CloudWatch와 같은 모니터링 도구에서 수집됩니다. 사고 탐지 및 대응이 EventBridge 규칙을 빌드하고 관리할 수 있도록 하려면 서비스 연결 역할을 설치합니다. 이러한 서비스에 대한 자세한 내용은 Amazon EventBridge란 무엇인가요? 및 Amazon EventBridge 규칙, Amazon CloudWatch란 무엇인가요?, AWS Health에 서비스 연결 역할 사용을 참조하세요.
- AWS Health: AWS Health는 리소스 성능과 사용자 AWS 서비스 및 계정의 가용성에 대한 지속적인 가시성을 제공합니다. 사고 탐지 및 대응은 AWS Health를 사용하여 워크로드에서 사용하는 AWS 서비스에 대한 이벤트를 추적하고 워크로드에서 알림이 수신되면 알려줍니다. AWS Health에 대한 자세한 내용은 AWS Health란을 참조하십시오.
- AWS Systems Manager: Systems Manager는 AWS 리소스 전반의 자동화 및 작업 관리를 위한 통합 사용자 인터페이스를 제공합니다. AWS 사고 탐지 및 대응은 워크로드 아키텍처 세부 정보, 경보 세부 정보 및 AWS Systems Manager 문서의 해당 인시던트 관리 런북을 포함하여 워크로드에 대한 정보를 호스팅합니다(자세한 내용은 AWS Systems Manager 문서 참조). AWS Systems Manager에 대한 자세한 내용은 AWS Systems Manager란을 참조하십시오.

- 특정 런북: 인시던트 관리 런북은 인시던트 관리 중에 AWS 사고 탐지 및 대응이 수행하는 작업을 정의합니다. 특정 런북은 연락 대상, 연락 방법 및 공유할 정보를 AWS 사고 탐지 및 대응에 알려줍니다.

인시던트 탐지 및 대응의 역할 및 책임

AWS 사고 탐지 및 대응 RACI(실무 담당자, 최종 책임자, 조언자 및 결과 통보 대상자) 테이블에는 사고 탐지 및 대응과 관련된 다양한 활동의 역할과 책임이 요약되어 있습니다. 이 표는 데이터 수집, 운영 준비 상태 검토, 계정 구성, 인시던트 관리, 인시던트 사후 검토와 같은 작업에 대한 고객 및 AWS 사고 탐지 및 대응 팀의 참여를 정의하는 데 도움이 됩니다.

활동	Customer	Incident Detection and Response
데이터 수집		
고객 및 워크로드 소개	조언자	실무 담당자
아키텍처	실무 담당자	최종 책임자
작업	실무 담당자	최종 책임자
구성할 CloudWatch 경보 결정	실무 담당자	최종 책임자
인시던트 대응 계획 정의	실무 담당자	최종 책임자
운영 준비 상태 검토		

활동	Customer	Incident Detection and Response
워크로드에 대해 Well Architected 리뷰(WAR) 수행	조언자	실무 담당자
인시던트 대응 검증	조언자	실무 담당자
경보 매트릭스 검증	조언자	실무 담당자
워크로드에서 사용 중인 주요 AWS 서비스 식별	최종 책임자	실무 담당자
계정 구성		
고객 계정에서 IAM 역할 생성	실무 담당자	결과 통보 대상자
생성된 역할을 사용하여 관리형 EventBridge 규칙 설치	결과 통보 대상자	실무 담당자
CloudWatch 경보 테스트	실무 담당자	최종 책임자
고객 경보가 사고 탐지 및 대응과 관련이 있는지 확인	결과 통보 대상자	실무 담당자
경보 업데이트	실무 담당자	조언자
런북 업데이트	조언자	실무 담당자
인시던트 관리		

활동	Customer	Incident Detection and Response
사고 탐지 및 대응에서 탐지된 인시던트를 사전 예방적으로 알림	결과 통보 대상자	실무 담당자
인시던트 대응 제공	결과 통보 대상자	실무 담당자
인시던트 해결/인프라 복원 제공	실무 담당자	조언자
인시던트 사후 보고서		
인시던트 후 검토 요청	실무 담당자	결과 통보 대상자
인시던트 후 검토 제공	결과 통보 대상자	실무 담당자

사고 탐지 및 대응의 리전 가용성

AWS 사고 탐지 및 대응은 현재 다음 AWS 리전 중 하나에서 호스팅되는 AWS Enterprise Support 계정에 대해 영어, 일본어, 표준 중국어 및 한국어로 제공됩니다.

AWS 리전	이름
미국 동부(버지니아 북부) 리전	us-east-1
미국 동부(오하이오) 리전	us-east-2
미국 서부(캘리포니아 북부) 리전	us-west-1
미국 서부(오리곤) 리전	us-west-2
캐나다(중부) 리전	ca-central-1

AWS 리전	이름
캐나다 서부(캘거리) 리전	ca-west-1
남아메리카(상파울루) 리전	sa-east-1
유럽(프랑크푸르트) 리전	eu-central-1
유럽(아일랜드) 리전	eu-west-1
유럽(런던) 리전	eu-west-2
유럽(파리) 리전	eu-west-3
유럽(스톡홀름) 리전	eu-north-1
유럽(취리히) 리전	eu-central-2
유럽(밀라노) 리전	eu-south-1
유럽(스페인) 리전	eu-south-2
아시아 태평양(뭄바이)	ap-south-1
아시아 태평양(도쿄)	ap-northeast-1
아시아 태평양(서울)	ap-northeast-2
아시아 태평양(싱가포르)	ap-southeast-1
아시아 태평양(시드니)	ap-southeast-2
아시아 태평양(홍콩)	ap-east-1
아시아 태평양(오사카)	ap-northeast-3
아시아 태평양(하이데라바드)	ap-south-2
아시아 태평양(자카르타)	ap-southeast-3
아시아 태평양(멜버른)	ap-southeast-4

AWS 리전	이름
아시아 태평양(말레이시아)	ap-southeast-5
아프리카(케이프타운)	af-south-1
이스라엘(텔아비브)	il-central-1
중동(UAE)	me-central-1
중동(바레인)	me-south-1
AWS GovCloud (US-East)	us-gov-east-1
AWS GovCloud(미국 서부)	us-gov-west-1

사고 탐지 및 대응 시작하기

워크로드 및 경보는 AWS 사고 탐지 및 대응의 핵심입니다. AWS는 고객과 긴밀하게 협력하여 비즈니스에 중요한 특정 워크로드를 정의하고 모니터링합니다. AWS는 중요한 성능 문제 또는 고객에게 미치는 영향을 팀에 알리는 경보를 설정하는 데 도움이 됩니다. 적절하게 구성된 경보는 사고 탐지 및 대응 내에서 선제적 모니터링 및 신속한 인시던트 대응에 필수적입니다.

사고 탐지 및 대응의 워크로드 정보

AWS 사고 탐지 및 대응을 사용하여 모니터링 및 중요한 인시던트 관리를 위한 특정 워크로드를 선택할 수 있습니다. 워크로드는 비즈니스 가치를 제공하기 위해 함께 작동하는 리소스 및 코드 모음입니다. 워크로드는 은행 결제 포털 또는 고객 관계 관리(CRM) 시스템을 구성하는 모든 리소스와 코드일 수 있습니다. 단일 AWS 계정 또는 여러 AWS 계정에서 워크로드를 호스팅할 수 있습니다.

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

워크로드 온보딩을 시작하려면 사고 탐지 및 대응에 워크로드 온보딩 섹션을 참조하세요.

사고 탐지 및 대응의 경보 정보

경보는 사고 탐지 및 대응의 핵심 부분입니다. 경보는 애플리케이션 및 기본 AWS 인프라의 성능에 대한 가시성을 제공합니다. AWS는 적절한 지표와 경보 임계값을 정의하여 모니터링 대상 워크로드에 심각한 영향이 발생할 때만 경보가 트리거되도록 지원합니다. 목표는 경보가 지정된 담당자에게 전달되어, 담당자가 인시던트 관리 팀과 협력하여 문제를 신속하게 해결하는 것입니다. 성능이나 고객 경험에 심각한 저하가 발생하여 즉각적인 조치가 필요한 경우에만 경보 상태가 되도록 경보 시스템을 구성합니다. 일부 주요 경보 유형에는 비즈니스 영향을 나타내는 경보, Amazon CloudWatch 카나리 및 종속성을 모니터링하는 집계 경보가 포함됩니다.

경보 수집을 시작하려면 경보 수집 섹션을 참조하세요.

사고 탐지 및 대응에 워크로드 온보딩

AWS 사고 탐지 및 대응은 선택한 워크로드에 대한 모니터링 및 중요 인시던트 관리를 지원합니다. 워크로드는 결제 포털 또는 고객 관계 관리(CRM) 시스템과 같이 비즈니스 가치를 제공하기 위해 함께 작

동하는 리소스 모음입니다. 아키텍처에 따라 이러한 워크로드를 단일 AWS 계정 또는 여러 계정에 분산하여 호스팅할 수 있습니다.

목차

- IDR CLI를 사용하여 사고 탐지 및 대응에 온보딩
  - IDR CLI에 대한 언어 지원
  - 워크로드 온보딩을 위한 대체 옵션

IDR CLI를 사용하여 사고 탐지 및 대응에 온보딩

AWS 사고 탐지 및 대응 고객 명령줄 인터페이스(IDR CLI)는 AWS 사고 탐지 및 대응에 대한 온보딩 프로세스를 간소화하는 명령줄 인터페이스 도구입니다.

IDR CLI는 AWS CloudShell에서 실행되어 다음 기능을 수행합니다.

- 온보딩 정보 수집
- AWS Resource Groups Tagging API를 통해 리소스 데이터 수집
- AWS Support 사례 관리
- 새 Amazon CloudWatch 경보 생성 또는 기존 경보 수집
- AWS CloudFormation을 통해 인프라를 배포하고 테스트하여 타사 도구가 사고 탐지 및 대응에 알림을 보낼 수 있도록 합니다.

IDR CLI는 온보딩 단계를 안내하는 대화형 모드나 대량 또는 DevOps 사용 사례를 위한 오프라인 모드로 실행할 수 있습니다.

설치, 사전 조건 및 종합 예제를 포함하여 IDR CLI를 사용하는 방법에 대한 자세한 내용은 AWS 사고 탐지 및 대응을 위한 CLI를 참조하세요.

IDR CLI에 대한 언어 지원

AWS 사고 탐지 및 대응은 영어, 일본어, 표준 중국어 및 한국어로 제공됩니다. 일본어, 표준 중국어 또는 한국어 지원이 필요한 경우 IDR CLI에서 생성한 AWS Support 사례를 통해 AWS에 문의하거나 기술 계정 관리자(TAM)에게 문의하세요.

워크로드 온보딩을 위한 대체 옵션

온보딩에 IDR CLI를 사용할 수 없는 경우 기술 계정 관리자(TAM)에게 대체 옵션을 문의하세요. 자세한 내용은 사고 탐지 및 대응(예외 경로)에서의 워크로드 온보딩 및 경보 수집 설문지 섹션을 참조하세요.

경보 수집

AWS 사고 탐지 및 대응 고객 명령줄 인터페이스(IDR CLI)를 사용하면 새로운 Amazon CloudWatch 경보를 생성하거나 기존 경보를 수집할 수 있으며, 타사 도구가 AWS 사고 탐지 및 대응으로 경고를 보낼 수 있도록 AWS CloudFormation을 통해 인프라를 배포하고 테스트할 수 있습니다.

AWS 사고 탐지 및 대응은 Amazon EventBridge를 통해 Amazon CloudWatch 및 타사 애플리케이션 성능 모니터링(APM) 도구에서 경보를 수집할 수 있습니다.

- CloudWatch 경보 수집
- 타사 애플리케이션 성능 모니터링 경보 수집

경보 수집 단계

경보 수집을 위해 다음 단계를 완료해야 합니다.

- 경보 정의
- IDR CLI를 사용한 경보 수집
- 경보 검토 및 피드백
- 사고 탐지 및 대응에 대한 경보 수집을 위한 액세스 권한 프로비저닝
- 경보 테스트(게임데이)
- 경보는 이전 단계가 완료된 후 AWS 사고 탐지 및 대응에서 활성 모니터링을 위해 활성화됩니다.

경보 수집을 위한 대체 옵션

경보 수집에 IDR CLI를 사용할 수 없는 경우 기술 계정 관리자(TAM)에게 대체 옵션을 문의하세요. 자세한 내용은 사고 탐지 및 대응(예외 경로)에서의 워크로드 온보딩 및 경보 수집 설문지 섹션을 참조하세요.

사고 탐지 및 대응에 대한 경보 수집을 위한 액세스 권한 프로비저닝

> **Note**
>
> IDR CLI 온보딩 중에 서비스 연결 역할(SLR)을 생성하지 않은 경우 아래 단계에 따라 액세스를 수동으로 프로비저닝합니다.

AWS 사고 탐지 및 대응에서 계정의 경보를 수집할 수 있도록 하려면 `AWSServiceRoleForHealth_EventProcessor` SLR을 생성해야 합니다. AWS는 계정에 관리형 EventBridge 규칙을 생성하기 위해 SLR이 필요하다고 가정합니다. 관리형 EventBridge 규칙은 사용자 계정에서 AWS 사고 탐지 및 대응 시스템으로 알림을 전송합니다. 연결된 AWS 관리형 정책을 포함하여 이 SLR에 대한 자세한 내용은 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 만들 수 있습니다. 다음 AWS Command Line Interface(AWS CLI) 명령을 사용할 수 있습니다.

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

핵심 결과물

- 계정에 서비스 연결 역할을 성공적으로 만들었습니다.

> **Note**
>
> 서비스 연결 역할 - AWS 사고 탐지 및 대응에 경보를 보내는 데 사용할 각 계정에서 AWSServiceRoleForHealth_EventProcessor를 생성해야 합니다.

관련 정보

자세한 내용은 다음 항목을 참조하세요.

- 에 서비스 연결 역할 사용
- 서비스 연결 역할 만들기
- AWS 관리형 정책: AWSHealth_EventProcessorServiceRolePolicy

경보 정의

경보를 AWS 사고 탐지 및 대응에 온보딩할 때 애플리케이션의 성능에 대한 가시성을 제공하는 지표 및 경보 구성을 정의하는 것은 사용자의 책임입니다. 이 프로세스의 일환으로 이러한 경보에 대응할 책임이 있는 조직 내 팀도 식별해야 합니다.

경보를 준비할 때는 다음 모범 사례를 따르는 것이 좋습니다.

- 경보는 모니터링되는 워크로드에 지속적으로 중요한 영향을 미치고 팀 및 AWS의 즉각적인 주의가 필요한 경우에만 '경보' 상태로 전환됩니다. 트리거되고 자동으로 복구되지 않는 경보는 팀이 AWS 사고 탐지 및 대응과 인시던트 브리지에 조인해야 합니다.
- 제공한 연락처 정보를 통해 AWS 사고 탐지 및 대응이 조직 내 적절한 팀을 인시던트 브리지에 연중무휴 안정적으로 참여시킬 수 있는지 확인합니다.

핵심 결과물

- IDR CLI를 사용하여 AWS 사고 탐지 및 대응에 제공하는 경보 및 연락처 세부 정보 목록입니다.

Amazon CloudWatch 경보를 정의하고 수집하는 방법에 대한 자세한 내용은 CloudWatch 경보 수집 섹션을 참조하세요.

타사 애플리케이션 성능 모니터링 경보 수집에 대한 자세한 내용은 타사 애플리케이션 성능 모니터링 경보 수집 섹션을 참조하세요.

CloudWatch 경보 수집

AWS 사고 탐지 및 대응은 Amazon CloudWatch 경보를 수집하여 중요한 워크로드에 대한 사전 모니터링을 제공할 수 있습니다. AWS 사고 탐지 및 대응은 모니터링을 위해 Amazon CloudWatch 경보를 수집하여 다음을 수행할 수 있습니다.

- 경보가 '경보' 상태가 되면 자동으로 감지합니다.
- 팀을 참여시켜 공동으로 대응하고 인시던트를 해결합니다.

온보딩하는 경보의 효과를 보장하기 위해 AWS 사고 탐지 및 대응은 다음 모범 사례를 권장합니다.

- 지표 수학 표현식으로 경보를 구성하여 정기적인 유지 관리 또는 배치 작업 실행 기간 동안 경보를 억제함으로써 오탐지 경보 개입을 방지합니다.
- 예상 데이터 포인트 전송 빈도를 기반으로 경보에 대한 누락 데이터 처리를 설정합니다. 예를 들어 데이터 포인트의 연속 스트림을 생성하는 경보 모니터링 지표는 누락된 데이터를 '위반'(잘못됨)으로 처리해야 합니다. 누락된 데이터 포인트는 모니터링되는 기본 리소스에 문제가 있음을 나타낼 수 있기 때문입니다. 반대로 실패 또는 오류가 발생할 때 데이터 포인트만 기록하는 경보 모니터링 지표와 같이 데이터 포인트를 자주 보고하지 않는 경보 모니터링 지표는 누락된 데이터를 '위반이 아님'(양호)으로 처리해야 합니다.

- 워크로드에 심각하고 지속적인 영향이 있을 때 '경보' 상태가 되는 경보를 정의합니다. 예를 들어 비정상 리소스를 처음 감지하는 대신 비정상 리소스를 자동으로 교체하는 데 필요한 예상 시간 이후에 트리거되도록 경보를 구성합니다.
- 워크로드의 고객 경험을 직접 나타내는 사용자 지정 지표에 대한 경보를 식별하고 생성합니다.

일반적인 AWS 서비스에 권장되는 Amazon CloudWatch 경보 목록은 AWS re:Post의 사고 탐지 및 대응 경보 모범 사례를 참조하세요.

타사 애플리케이션 성능 모니터링 경보 수집

AWS 사고 탐지 및 대응은 Amazon EventBridge를 통해 타사 애플리케이션 성능 모니터링(APM) 도구의 경보 수집을 지원합니다. 이 통합은 APM 알림을 수집하여 유연성을 제공하므로 다양한 AWS 서비스를 통해 계정의 Amazon EventBridge 이벤트 버스로 APM 이벤트를 라우팅할 수 있습니다.

통합 경로 예제:

- 소스(APM) → AWS 서비스(예: Amazon API Gateway 또는 Amazon SNS) → Lambda 함수 변환 → 사용자 지정 Amazon EventBridge 이벤트 버스 → AWS 사고 탐지 및 대응
- 소스(APM) → 파트너 Amazon EventBridge 이벤트 버스 → Lambda 함수 변환 → 사용자 지정 Amazon EventBridge 이벤트 버스 → AWS 사고 탐지 및 대응

AWS 사고 탐지 및 대응은 사용자 지정 이벤트 버스에 관리형 규칙을 설치하여 Lambda 함수 변환에서 전송한 알림을 수집합니다. SaaS Amazon EventBridge 통합의 경우 파트너 이벤트 버스는 관리형 규칙이 설치된 이벤트 버스가 아닙니다. Amazon EventBridge와 파트너 통합을 지원하는 APM의 전체 목록은 Amazon EventBridge 통합을 참조하세요.

파트너 이벤트 버스 또는 기타 AWS 이벤트 버스 소스를 사용한 통합 예제

다음 다이어그램은 파트너 이벤트 버스 또는 기타 AWS 이벤트 버스 소스를 사용한 통합의 예를 보여 줍니다.

Amazon EventBridge와 파트너 통합을 지원하는 APM의 전체 목록은 Amazon EventBridge 통합을 참조하세요.

Amazon API Gateway를 사용한 통합 예제

다음 다이어그램은 API 게이트웨이를 사용한 통합 예시를 보여 줍니다.

Amazon Simple Notification Service를 사용한 통합 예제

다음 다이어그램은 Amazon SNS를 사용한 통합 예시를 보여 줍니다.

통합 프로세스를 간소화하기 위해 AWS 사고 탐지 및 대응은 가장 일반적으로 사용되는 통합 유형에 대한 CloudFormation 템플릿을 제공합니다. 이러한 템플릿은 AWS 리소스 및 필요한 IAM 역할 설정을 자동화합니다.

다양한 통합 유형을 수동으로 생성하는 CloudFormation 템플릿과 지침은 아래 해당 통합 설명서에서 확인할 수 있습니다.

- 직접 EventBridge 통합으로 APM에서 경보 수집
- EventBridge와 직접 통합하지 않고도 APM에서 경보 수집
- Amazon SNS와 직접 연동하여 APM에서 경보 수집

> **Note**
>
> CloudFormation 템플릿은 수정해야 합니다. 이러한 수정 사항은 이전 주제에서 설명합니다. AWS 사고 탐지 및 대응에 APM 알림을 보내는 데 필요한 페이로드 형식에 대한 자세한 내용은 EventBridge를 사용하여 APM 알림을 수집하기 위한 페이로드 요구 사항 섹션을 참조하세요.

EventBridge를 사용하여 APM 알림을 수집하기 위한 페이로드 요구 사항

사고 탐지 및 대응은 어디에서 APM 알림을 수집하나요?

AWS 사고 탐지 및 대응은 최종 변환된 페이로드를 보내는 이벤트 버스에 관리형 규칙을 설치합니다. 이를 위해 사용자 지정 이벤트 버스를 생성하는 것이 가장 좋습니다.

페이로드는 어떤 형식이어야 하나요?

AWS 사고 탐지 및 대응에서 수집하는 이벤트 버스 이벤트에는 다음과 같은 최소 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 예제는 변환 전과 후에 파트너 이벤트 버스의 이벤트를 보여줍니다.

변환 전:

```
{
    "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}
 <= 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 `detail-type` 및 `source`는 알림이 발생한 APM 세부 정보를 나타냅니다. 수집 전에 수정해야 합니다. `incident-detection-response-identifier` 키가 아직 없으며 수집 전에 추가해야 합니다.

Lambda 함수는 위의 이벤트를 변환하여 대상 사용자 지정 또는 기본 이벤트 버스에 넣습니다. 변환된 페이로드에는 필수 키:값 페어가 포함되어야 합니다.

변환 후:

```
{
    "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}
<= 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`이 `ams.monitoring/generic-apm`이고, 소스가 `GenericAPMEvent`이며, 세부 사항에 새 키:값 페어 `incident-detection-response-identifier`가 있습니다.

`incident-detection-response-identifier` 값은 APM이 전송하는 페이로드를 기반으로 알림 이름에서 가져옵니다. APM 알림 이름 경로는 한 APM에서 다른 APM으로 다릅니다. Lambda 함수는 Lambda가 수신한 APM JSON 페이로드의 올바른 경로에서 경보 이름을 가져와 `incident-detection-response-identifier` 값에 사용하도록 설정해야 합니다.

`incident-detection-response-identifier` 값은 AWS 사고 탐지 및 대응으로 전송되는 경보 유형별로 고유해야 합니다. `incident-detection-response-identifier`에 설정된 각 고유 이름은 온보딩 중에 AWS 사고 탐지 및 대응 팀에 제공되어야 합니다. `incident-detection-response-identifier` 키에 대해 알 수 없거나 누락된 값이 있는 이벤트는 처리되지 않습니다.

직접 EventBridge 통합으로 APM에서 경보 수집

다음 항목에서는 Amazon EventBridge와 직접 통합된 애플리케이션 성능 모니터링(APM) 도구에서 AWS 사고 탐지 및 대응으로 경보를 전송하는 프로세스를 보여 줍니다. Amazon EventBridge와 직접 통합되는 전체 APM 목록은 Amazon EventBridge 통합을 참조하세요.

제공된 CloudFormation 템플릿을 배포하거나 이 통합을 수동으로 설정할 수 있습니다. 통합을 설정하기 전에 AWS 서비스 연결 역할(SLR) `AWSServiceRoleForHealth_EventProcessor`가 계정에 생성되었는지 확인합니다.

옵션 1: 사용CloudFormation

CloudFormation 템플릿을 사용하면 Amazon EventBridge 통합을 통해 APM에서 AWS 사고 탐지 및 대응에 경보를 수집하는 데 필요한 통합 인프라를 생성하는 프로세스를 간소화할 수 있습니다.

> **Note**
>
> - 이 CloudFormation 템플릿을 통해 배포된 리소스(예: Lambda 및 EventBridge)에 대해 추가 비용이 발생합니다. 이러한 서비스의 가격에 대한 자세한 내용은 AWS 가격을 참조하세요.
> - AWS 사고 탐지 및 대응에서 경보를 수집해야 하는 모든 AWS 계정 및 리전에 이 CloudFormation 템플릿을 배포합니다. 인시던트 및 지원 사례는 APM 알림을 받은 AWS 계정에서 열립니다.

- 이 문서에서는 New Relic을 예로 사용하지만, CloudFormation 템플릿은 Amazon EventBridge와 SaaS 통합이 있는 모든 APM에 사용할 수 있습니다.
- 통합을 테스트한 후 `TransformLambdaFunction`에서 logger.info() 문을 제거하여 Amazon CloudWatch Logs에 페이로드가 표시되지 않도록 합니다.

이 CloudFormation 템플릿을 배포하기 위한 사전 조건:

- 파트너 이벤트 소스는 Amazon EventBridge에서 설정해야 합니다. APM을 이벤트 소스로 설정하는 방법에 대한 자세한 내용은 Amazon EventBridge 사용 설명서의 Amazon EventBridge를 사용하여 SaaS 파트너로부터 이벤트 수신을 참조하세요.
- 템플릿의 `TransformLambdaFunction`(Lambda 함수)을 수정하여 APM 페이로드에서 알림 이름의 JSON 경로를 기반으로 `["detail"]["incident-detection-response-identifier"]`를 원하는 값으로 설정해야 합니다.

사전 요구 사항 단계:

1. EventBridge 콘솔을 엽니다. 통합 메뉴에서 파트너 이벤트 소스를 선택합니다.
   - Amazon EventBridge 파트너 상자에서 APM을 검색합니다.
   - 설정을 선택한 다음 제공된 지침을 따릅니다.
     - 참고: 마지막 단계는 파트너 이벤트 소스에 대해 콘솔에서 이벤트 버스와 연결을 선택하는 것입니다. 이 옵션을 선택하면 파트너 이벤트 소스와 이름이 동일한 파트너 이벤트 버스가 자동으로 생성됩니다(이름이 일치해야 함).
   - 파트너 이벤트 버스 또는 소스의 이름을 복사합니다. 이벤트 버스 또는 소스는 CloudFormation 템플릿을 배포할 때 `PartnerEventBusNameParameter`라는 파라미터로 사용됩니다.
     - New Relic의 예제: `aws.partner/newrelic.com/1234567/source_name`
   - CloudFormation 템플릿을 배포할 때 `PartnerEventBusPrefixParameter`에 입력할 파트너 이벤트 버스 또는 소스의 첫 번째 부분을 복사합니다.
     - New Relic의 예제는 `aws.partner/newrelic.com`입니다.
2. CloudFormation 템플릿을 다운로드하고 편집합니다.
   - 템플릿에서 `TransformLambdaFunction`을 찾습니다.
   - `def lambda_handler(event, context)`에서 경보 이름이 APM 경보의 JSON 페이로드에 표시되는 json 경로로 `event["detail"]["incident-detection-response-`

identifier"]를 설정합니다. 모든 APM의 경로는 다릅니다. 아래에서 몇 가지 예를 볼 수 있지만 특정 페이로드는 다를 수 있습니다.

- New Relic 예제: `event["detail"]["incident-detection-response-identifier"] = event["detail"]["workflowName"]`.
- Datadog 예제: `event["detail"]["incident-detection-response-identifier"] = event["detail"]["meta"]["monitor"]["name"]`
- Splunk 예제: `event["detail"]["incident-detection-response-identifier"] = event["detail"]["ruleName"]`

- CloudFormation 템플릿을 저장합니다.

CloudFormation 템플릿 배포:

1. 대상 계정 및 리전에서 CloudFormation 콘솔을 엽니다.
2. 스택 생성, 새 리소스 사용(표준)을 선택합니다.
   - 기존 템플릿 선택, 템플릿 파일 업로드, 파일 선택을 선택한 다음 로컬로 저장한 CloudFormation 템플릿을 업로드합니다.
3. 다음과 같이 스택 세부 정보를 지정합니다.
   - 스택 이름을 입력합니다(예: `NewRelicIntegrationForIDR`).
   - 사전 조건 완료 중에 얻은 파라미터 값을 지정합니다.
     - APMNameParameter(예: `NewRelic`)
     - PartnerEventBusNameParameter(예: `aws.partner/newrelic.com/1234567/source_name`)
     - PartnerEventBusPrefixParameter(예: `aws.partner/newrelic.com`)
   - 다음을 선택합니다.
4. 다음과 같이 스택 옵션을 구성합니다.
   - 페이지 하단으로 스크롤하고 확인란을 선택하여 CloudFormation이 사용자 지정 이름으로 IAM 리소스를 생성하도록 허용합니다.
5. 검토 및 생성
   - 파라미터 값이 올바르게 구성되었는지 확인하고 제출을 선택합니다.
6. CloudFormation 스택은 APM 이벤트를 AWS 사고 탐지 및 대응에 통합하는 데 필요한 리소스를 배포합니다. 스택 상태에 `CREATE_COMPLETE`가 표시될 때까지 기다립니다.
7. CloudFormation 스택은 예제 값이 New Relic의 파라미터에 입력되었고 US-EAST-1 리전에서 실행되었다고 가정하여 다음 리소스를 생성합니다.

- CustomEventBus: NewRelic-AWSIncidentDetectionResponse-EventBus
- EventBridgeRule: aws.partner/newrelic.com/1234567/source_name|NewRelic-AWSIncidentDetectionResponse-EventBridgeRule
- TransformLambdaExecutionRole: IDR-TransformLambdaExecutionRole-us-east-1
- TransformLambdaFunction: NewRelic-AWSIncidentDetectionResponse-Lambda-Transform
- TransformLambdaPermission: NewRelicIntegrationForIDR-TransformLambdaPermission-[random_string]

통합 테스트하기

스택을 배포한 후 APM에서 테스트 페이로드를 전송하여 통합을 테스트합니다.

1. Lambda 콘솔로 이동하여 `APMNameParameter-AWSIncidentDetectionResponse-Lambda-Transform` 함수를 선택합니다. 모니터링 탭을 선택합니다.
2. 지표 그래프에서 성공적인 간접 호출을 찾습니다.
3. Amazon CloudWatch Logs 보기를 선택하여 테스트 페이로드 또는 오류가 있는지 로그 스트림을 확인합니다.

이벤트 버스 ARN을 AWS 사고 탐지 및 대응과 공유

1. Amazon EventBridge 콘솔을 엽니다. 이벤트 버스를 선택합니다.
2. CloudFormation 스택의 일부로 생성된 사용자 지정 이벤트 버스의 ARN을 복사합니다(예: *`arn:aws:events:us-east-1:123456789123:event-bus/NewRelic-AWSIncidentDetectionResponse-EventBus`*).
   - 경보 수집 설문지 - 개요의 '타사 APM 경보' 섹션에 있는 'EventBridge 이벤트 버스 ARN' 필드에 이 ARN을 추가합니다.
3. 온보딩 프로세스 중에 AWS 사고 탐지 및 대응은 이 사용자 지정 이벤트 버스에 관리형 EventBridge 규칙을 생성하여 APM 경보를 수집합니다.

옵션 2: 수동 통합

AWS 사고 탐지 및 대응이 경보를 수집해야 하는 각 AWS 계정 및 AWS 리전에 대해 다음 단계를 완료합니다. AWS 사고 탐지 및 대응은 영향을 받는 리소스를 더 빠르게 식별하고 조사할 수 있도록 애플리

케이션 리소스와 동일한 AWS 계정 및 리전에 경보를 설정할 것을 권장합니다. 인시던트 및 지원 사례는 APM 알림을 받은 AWS 계정에서 열립니다.

1. APM을 Amazon EventBridge 파트너 이벤트 소스(예: `aws.partner/apm_name/integrationName`)로 설정하여 EventBridge 파트너 이벤트 버스를 생성합니다. APM을 이벤트 소스로 설정하는 방법에 대한 지침은 Amazon EventBridge를 사용하여 SaaS 파트너로부터 이벤트 수신을 참조하세요.
2. 다음 중 하나를 수행합니다.
   - (권장 방법) 이름이 `$YourApmName-AWSIncidentDetectionResponse-EventBus`인 EventBridge 사용자 지정 이벤트 버스를 만듭니다.
   - (대체 방법) 사용자 지정 이벤트 버스 대신 기본 EventBridge 이벤트 버스를 사용합니다.

   AWS 사고 탐지 및 대응은 `AWSHealthEventProcessorEventSource-DO-NOT-DELETE` SLR을 통해 사용자 지정 또는 기본 이벤트 버스에 관리형 규칙(`AWSServiceRoleForHealth_EventProcessor`)을 설치합니다. 규칙 소스는 사용자 지정 또는 기본 이벤트 버스이고, 규칙 대상은 AWS 사고 탐지 및 대응이며, 규칙은 타사 APM 이벤트 수집 패턴과 일치합니다.
3. 이름이 `$YourApmName-AWSIncidentDetectionResponse-LambdaFunction`인 Lambda 함수를 만들어 파트너 이벤트 버스 이벤트를 변환합니다. 변환된 이벤트는 관리형 규칙 `AWSHealthEventProcessorEventSource-DO-NOT-DELETE`와 일치합니다.
   - 변환된 이벤트에는 고유한 AWS 사고 탐지 및 대응 식별자가 포함되며 이벤트의 소스 및 세부 정보 유형을 필요한 값으로 설정합니다. 이렇게 하면 변환된 JSON 페이로드 구조가 관리형 규칙 패턴과 일치할 수 있습니다.
   - Lambda 함수의 대상을 2단계에서 생성한 사용자 지정 이벤트 버스(권장) 또는 기본 이벤트 버스로 설정합니다.
4. EventBridge 규칙을 생성하고 AWS 사고 탐지 및 대응에 푸시하려는 이벤트 목록과 일치하는 이벤트 패턴을 정의합니다. 규칙의 소스는 1단계에서 생성한 파트너 이벤트 버스(`aws.partner/apm_name/integrationName`)입니다. 규칙의 대상은 3단계에서 생성한 Lambda 함수(`[apm_name]-AWSIncidentDetectionResponse-LambdaFunction`)입니다. EventBridge 규칙 정의에 대한 지침은 Amazon EventBridge 규칙을 참조하세요.

AWS 사고 탐지 및 대응과 파트너 이벤트 버스 통합을 수동으로 설정하는 방법에 대한 단계별 예제는 Datadog 및 Splunk의 알림 통합을 참조하세요.

EventBridge와 직접 통합하지 않고도 APM에서 경보 수집

AWS 사고 탐지 및 대응은 Amazon EventBridge와 직접 통합되지 않은 타사 APM에서 경보 수집을 위해 웹후크 사용을 지원합니다.

CloudFormation 템플릿을 배포하거나 통합을 수동으로 설정할 수 있습니다. 통합을 설정하기 전에 AWS 서비스 연결 역할(SLR) `AWSServiceRoleForHealth_EventProcessor`가 계정에 생성되었는지 확인합니다.

옵션 1: CloudFormation 템플릿 사용

CloudFormation 템플릿은 직접 Amazon EventBridge 통합이 없는 APM에서 AWS 사고 탐지 및 대응에 경보를 수집하는 데 필요한 통합 인프라를 생성하는 프로세스를 간소화하는 데 사용할 수 있습니다.

이 CloudFormation 템플릿을 배포하기 전 고려 사항

- 이 솔루션은 API Gateway Lambda 권한 부여자를 사용하여 페이로드에서 전달된 보안 토큰을 AWS Secrets Manager의 토큰과 비교합니다. 토큰이 일치하지 않으면 명시적 거부가 있는 정책이 반환됩니다. 자세한 내용은 Lambda 권한 부여자를 참조하세요.
- AWS 공동 책임 모델에 따라 조직의 보안 요구 사항을 충족하는 인증 접근 방식을 사용하는 것은 사용자의 책임입니다. API 키 또는 권한 부여 토큰과 같은 민감한 정보를 하드 코딩된 변수로 저장하는 대신 AWS Secrets Manager 또는 유사한 서비스를 사용하는 것이 좋습니다. 자세한 내용은 AWS Secrets Manager로 암호 생성 및 관리를 참조하세요.
- 해시 기반 메시지 인증 코드(HMAC)를 구현하는 추가 예제는 aws-samples Github 페이지의 receive-webhooks를 참조하세요. 토큰 권한 부여 구현에 대한 자세한 내용은 API Gateway 설명서의 예제 토큰 권한 부여자 Lambda 함수를 참조하세요.
- 이 솔루션은 API Gateway에서 RateLimit, BurstLimit 및 Quota를 사용하여 요청 볼륨을 제어합니다. 이러한 도구는 설정된 시간에 처리할 수 있는 요청 수를 제한합니다. 이렇게 하면 시스템 과부하를 방지하고 서비스를 안정적으로 유지할 수 있습니다. 스로틀링에 대한 자세한 내용은 API 게이트웨이 개발자 안내서를 참조하세요.
- AWS 웹 애플리케이션 방화벽(WAF)을 사용하여 알려진 잘못된 IP 주소로부터 API Gateway를 보호하는 것이 좋습니다. 이렇게 하면 공격자가 실제 로그 이벤트를 차단할 수 있는 가짜 요청으로 API를 플러딩할 위험이 줄어듭니다.
- AWS Secrets Manager 토큰 값은 애플리케이션 성능 모니터링(APM) 도구에 HTTP 헤더로 저장해야 합니다. 보안 모범 사례로 토큰을 정기적으로 교체해야 합니다.
- 이 CloudFormation 템플릿을 통해 배포된 리소스(예: Lambda 및 EventBridge)에 대해 추가 비용이 발생합니다. 이러한 서비스의 가격에 대한 자세한 내용은 AWS 가격을 참조하세요.

- 통합을 테스트한 후 `TransformLambdaFunction`(Lambda 함수)에서 logger.info() 문을 제거하여 Amazon CloudWatch Logs에 페이로드가 표시되지 않도록 합니다.
- AWS 사고 탐지 및 대응이 경보를 수집해야 하는 모든 AWS 계정 및 리전에 이 CloudFormation 템플릿을 배포합니다.

CloudFormation 템플릿 준비:

참고: 통합 단계에서는 Dynatrace를 예로 사용하지만 이 템플릿은 API Gateway로 페이로드를 전송할 수 있는 모든 APM에 사용할 수 있습니다.

1. CloudFormation 템플릿을 다운로드하여 엽니다.
2. 템플릿에서 `APIGWUsagePlan`을 찾습니다. 기본적으로 20, 50 및 2,000으로 설정된 `RateLimit`, `BurstLimit` 및 `Quota Limit`에 대해 구성된 값을 검토합니다. 요구 사항에 따라 값을 조정합니다.
3. 템플릿에서 `AuthorizerLambdaFunction`을 찾습니다. 이 Lambda 함수는 인증 메커니즘의 예제 역할을 합니다. APM에서 전달되는 `authorizationToken`이라는 헤더에서 토큰 값을 추출합니다. 조직의 보안 정책 및 APM 요구 사항에 맞게 이 코드를 수정할 수 있습니다.
4. 템플릿에서 `TransformLambdaFunction`을 찾습니다. 사전 경로인 `raw_json["detail"]["ProblemTitle"]`을 APM의 JSON 페이로드에서 전송되는 경보 이름의 경로로 바꿉니다. Dynatrace의 경우 그대로 둡니다.

CloudFormation 템플릿 배포:

1. 대상 계정 및 AWS 리전에서 CloudFormation 콘솔을 엽니다.
2. 스택 생성, 새 리소스 사용(표준)을 선택하세요.
   - 기존 템플릿 선택, 템플릿 파일 업로드, 파일 선택을 선택한 다음 로컬로 저장한 CloudFormation 템플릿을 업로드합니다.
3. 다음과 같이 스택 세부 정보를 지정합니다.
   - 스택 이름을 입력합니다(예: *`DynatraceIntegrationForIDR`*).
   - APMNameParameter(예: *`Dynatrace`*)
   - 다음을 선택합니다.
4. 다음과 같이 스택 옵션을 구성합니다.
   - 페이지 하단으로 스크롤하고 확인란을 선택하여 CloudFormation이 사용자 지정 이름으로 IAM 리소스를 생성하도록 허용합니다.

5. 검토 및 생성
   - 파라미터 값이 올바르게 구성되었는지 확인하고 제출을 선택합니다.
6. CloudFormation 스택은 APM 이벤트를 AWS 사고 탐지 및 대응에 통합하는 데 필요한 리소스를 배포합니다. CloudFormation 스택 상태가 CREATE_COMPLETE가 될 때까지 기다립니다.
7. CloudFormation 스택은 예시 값 `Dynatrace`가 파라미터에 입력되고 US-EAST-1 리전에서 실행되었다고 가정할 때 아래와 같은 리소스를 생성합니다.
   - 보안 암호 이름: DynatraceMySecretTokenName(보안 암호 키 APMSecureToken에 대해 임의의 보안 암호 값이 생성됨)
   - API 게이트웨이 리소스:
     - API 이름: Dynatrace-AWSIncidentDetectionResponse-APIGW
     - 스테이지 이름: Dynatrace-Stage-Prod
     - 권한 부여자: Dynatrace-APIGW-Authorizer
     - 사용 계획: APIGW_Throttling_Plan
   - Lambda 함수:
     - 권한 부여 함수: Dynatrace-AWSIncidentDetectionResponse-Lambda-Authorizer
     - 변환 함수: Dynatrace-AWSIncidentDetectionResponse-Lambda-Transform
   - 사용자 지정 EventBus 이름: Dynatrace-AWSIncidentDetectionResponse-EventBus
   - IAM 역할:
     - TransformLambdaExecutionRole: IDR-TransformLambdaExecutionRole-us-east-1
     - AuthorizerLambdaExecutionRole: IDR-AuthorizerLambdaExecutionRole-us-east-1
8. 다음과 같이 웹후크 URL 및 토큰 값을 기록합니다.
   - API Gateway 콘솔을 열고 CloudFormation 스택의 일부로 생성된 API 이름을 선택합니다.
   - 왼쪽 탐색에서 스테이지를 선택하고 + 기호를 사용하여 스테이지 이름을 확장한 다음 POST를 선택합니다. 간접 호출 URL을 기록합니다. 경보 이벤트에 대한 웹후크를 전송할 대상으로 APM에서 이 URL을 구성합니다.
   - AWS Secrets Manager 콘솔을 열고 CloudFormation 스택의 일부로 생성된 보안 암호 이름을 선택합니다. (예: DynatraceMySecretTokenName.)
     - 보안 암호 값 탭에서 보안 암호 값 검색을 선택합니다. 보안 키가 APMSecureToken으로 표시됩니다. 보안 암호 값을 기록합니다. 이 보안 암호 값을 다른 사람과 공유하지 마세요.

통합 테스트하기

스택을 배포한 후 APM에서 테스트 페이로드를 전송하여 통합을 테스트합니다.

1. Lambda 콘솔로 이동하여 `APMNameParameter-AWSIncidentDetectionResponse-Lambda-Transform` 함수를 선택합니다. 모니터링 탭을 선택합니다.
2. 지표 그래프에서 성공적인 간접 호출을 찾습니다.
3. Amazon CloudWatch Logs 보기를 선택하여 테스트 페이로드 또는 오류가 있는지 로그 스트림을 확인합니다.

이벤트 버스 ARN을 AWS 사고 탐지 및 대응과 공유

1. Amazon EventBridge 콘솔을 엽니다. 이벤트 버스를 선택합니다.
2. CloudFormation 스택의 일부로 생성된 사용자 지정 이벤트 버스의 ARN을 복사합니다(예: *`arn:aws:events:us-east-1:123456789123:event-bus/Dynatrace-AWSIncidentDetectionResponse-EventBus`*).
   - 경보 수집 설문지 - 개요의 '타사 APM 경보' 섹션에 있는 'EventBridge 이벤트 버스 ARN' 필드에 이 ARN을 추가합니다.
3. 온보딩 프로세스 중에 AWS 사고 탐지 및 대응은 이 사용자 지정 이벤트 버스에 관리형 EventBridge 규칙을 생성하여 APM 경보를 수집합니다.

옵션 2: 수동 통합

다음 단계에 따라 AWS 사고 탐지 및 대응과의 통합을 설정합니다.

1. Amazon API Gateway를 생성하여 APM의 페이로드를 수락합니다.
2. 인증 토큰을 사용하여 권한 부여를 위한 Lambda 함수를 정의합니다.
3. 다음 중 하나를 수행합니다.
   - (권장 방법) 이름이 `$YourApmName-AWSIncidentDetectionResponse-EventBus`인 EventBridge 사용자 지정 이벤트 버스를 만듭니다.
   - (대체 방법) 사용자 지정 이벤트 버스 대신 기본 EventBridge 이벤트 버스를 사용합니다.
4. AWS 사고 탐지 및 대응 식별자를 페이로드에 추가하는 Lambda 함수 변환을 정의합니다. 이 함수를 사용하여 AWS 사고 탐지 및 대응으로 보내려는 이벤트를 필터링할 수도 있습니다.
   - API Gateway는 API Gateway에서 전달하는 페이로드를 변환하는 Lambda 함수 변환을 간접적으로 호출해야 합니다.
   - Lambda 함수 변환은 위의 포인트 3에 정의된 이벤트 버스에 변환된 이벤트를 작성해야 합니다.

5. API Gateway에서 생성된 URL로 알림을 보내도록 APM을 설정합니다.

Amazon SNS와 직접 연동하여 APM에서 경보 수집

APM이 Amazon SNS 주제로 경보 전송을 지원하는 경우 이 가이드에 따라 AWS 사고 탐지 및 대응에 APM 경보를 수집할 수 있습니다.

제공된 CloudFormation 템플릿을 배포하거나 이 통합을 수동으로 설정할 수 있습니다. 통합을 설정하기 전에 AWS 서비스 연결 역할(SLR) `AWSServiceRoleForHealth_EventProcessor`가 계정에 생성되었는지 확인합니다.

옵션 1: 사용CloudFormation

CloudFormation 템플릿을 사용하면 Amazon SNS 통합을 통해 APM에서 AWS 사고 탐지 및 대응에 경보를 수집하는 데 필요한 통합 인프라를 생성하는 프로세스를 간소화할 수 있습니다.

> **Note**
>
> - 이 CloudFormation 템플릿을 통해 배포된 리소스(예: Lambda 및 EventBridge)에 대해 추가 비용이 발생합니다. 이러한 서비스의 가격에 대한 자세한 내용은 AWS 가격을 참조하세요.
> - 이 CloudFormation 템플릿은 AWS 사고 탐지 및 대응에서 경보를 수집해야 하는 모든 AWS 계정 및 리전에 배포되어야 합니다.
> - 이 문서에 제공된 예제는 Grafana용이지만 이 템플릿은 Amazon Simple Notification Service와 직접 통합되는 모든 APM에 사용할 수 있습니다.
> - 보안상의 이유로 AWS는 페이로드가 Amazon CloudWatch Logs에 로깅되지 않도록 `TransformLambdaFunction`에서 `logger.info()` 문을 제거할 것을 권장합니다.

이 CloudFormation 템플릿을 배포하기 위한 사전 조건:

- APM에서 경보 이벤트를 수신하려면 Amazon Simple Notification Service 주제를 생성해야 합니다. Amazon Simple Notification Service 콘솔에서 SNS 주제를 생성합니다.
- 템플릿의 `TransformLambdaFunction`을 수정하여 사용 중인 APM에 따라 원하는 값으로 `["detail"]["incident-detection-response-identifier"]`를 설정해야 합니다.

사전 조건 완료:

1. Amazon SNS 콘솔을 열고 주제를 선택합니다. APM에서 경보 이벤트를 수신하도록 생성된 SNS 주제의 ARN을 복사합니다.
   - 예시: `arn:aws:sns:eu-west-1:012345678912:<your-apm-name>-sns`
2. CloudFormation 템플릿 다운로드 및 열기
   - 템플릿에서 `TransformLambdaFunction`을 찾습니다.
     - `def lambda_handler(event, context)`에서 SNS 레코드의 JSON 페이로드에 경보 이름이 표시되는 json 경로로 `event["detail"]["incident-detection-response-identifier"]`를 설정합니다.
       - SNS를 통해 `TransformLambdaFunction`으로 전송되는 모든 이벤트는 `event["Records"][n]["Sns"]["Message"]`의 상위 페이로드 구조를 갖습니다. 소스(APM)의 실제 페이로드 오리진은 상위 구조 내에 래핑됩니다.
       - Grafana의 예: `event["Records"][n]["Sns"]["Message"]["alerts"][n]["labels"]["alertname"]`

CloudFormation 템플릿 배포:

1. 통합을 설정해야 하는 계정 및 리전의 CloudFormation 콘솔로 이동합니다.
2. CloudFormation로 이동합니다.
   - 스택 생성, 새 리소스 사용(표준)을 선택합니다.
     - 기존 템플릿 선택, 템플릿 파일 업로드, 파일 선택을 선택한 다음 로컬로 저장한 CloudFormation 템플릿을 업로드합니다.
3. 다음과 같이 스택 세부 정보를 지정합니다.
   - 스택 이름 입력 예: `<your-apm-name>IntegrationForIDR`
   - 사전 조건 완료 중에 얻은 파라미터 값 지정
     - APMNameParameter 예: `Grafana`
     - TriggerSNSParameter 예: `arn:aws:sns:eu-west-1:012345678912:<your-apm-name>-sns`
   - [Next]를 선택합니다.
4. 다음과 같이 스택 옵션을 구성합니다.
   - 페이지 하단으로 스크롤하고 확인란을 선택하여 CloudFormation이 사용자 지정 이름으로 IAM 리소스를 생성하도록 허용합니다.
5. 검토 및 생성
   - 파라미터 값이 올바르게 구성되었는지 확인한 다음 제출을 선택합니다.

6. CloudFormation 스택은 APM 이벤트를 AWS 사고 탐지 및 대응에 통합하는 데 필요한 리소스를 배포합니다. CloudFormation 스택 상태가 CREATE_COMPLETE가 될 때까지 기다립니다.
7. CloudFormation 스택은 예제 값이 Grafana의 파라미터에 입력되었고 EU-WEST-1 리전에서 실행되었다고 가정하여 아래 리소스를 생성합니다.
   - CustomEventBus: Grafana-AWSIncidentDetectionResponse-EventBus
   - SNSSubscription: arn:aws:sns:eu-west-1:012345678912:grafana-sns:[random_string]
   - TransformLambdaExecutionRole: IDR-TransformLambdaExecutionRole-eu-west-1
   - TransformLambdaFunction: Grafana-AWSIncidentDetectionResponse-Lambda-Transform
   - TransformLambdaPermission: GrafanaIntegrationForIDR-TransformLambdaPermission-[random_string]

통합 테스트하기

CloudFormation 스택이 성공적으로 배포되면 APM에서 테스트 페이로드를 전송하여 통합을 검증할 수 있습니다. 테스트 페이로드가 APM에서 전송된 후 다음을 수행합니다.

1. Lambda 콘솔로 이동하여 `APMNameParameter-AWSIncidentDetectionResponse-Lambda-Transform` 함수를 선택합니다. 그러고 나서 모니터링 탭을 선택합니다.
2. 지표 그래프에서 성공적인 간접 호출을 관찰해야 합니다.
3. Amazon CloudWatch Logs 보기를 선택합니다. 로그 스트림의 로그 이벤트를 통해 APM에서 전송된 테스트 페이로드가 있는지 또는 오류가 발생했는지 확인할 수 있습니다.

이벤트 버스 ARN을 AWS 사고 탐지 및 대응과 공유

1. Amazon EventBridge 콘솔로 이동합니다. 이벤트 버스를 선택합니다.
2. CloudFormation 스택의 일부로 배포된 사용자 지정 이벤트 버스의 ARN을 기록합니다(예: `arn:aws:events:eu-west-1:012345678912:event-bus/Grafana-AWSIncidentDetectionResponse-EventBus`).
   - AWS 사고 탐지 및 대응에 이 사용자 지정 이벤트 버스의 ARN을 경보 수집 설문지 - 개요의 '타사 APM 경보' 섹션에 있는 'EventBridge 이벤트 버스 ARN' 필드에 제공합니다.
3. 온보딩 프로세스 중에 AWS 사고 탐지 및 대응은 이 사용자 지정 이벤트 버스에 관리형 EventBridge 규칙을 생성하여 APM 경보를 수집합니다.

옵션 2: 수동 통합

1. Amazon SNS 콘솔을 열고 Amazon Simple Notification Service 콘솔에서 APM으로부터 경보 이벤트를 수신할 이름이 [apm_name]-sns인 SNS 토픽을 생성합니다. 생성된 SNS 주제의 ARN을 기록해 둡니다.
2. 다음 중 하나를 수행합니다.
   - (권장 방법) 이름이 [apm_name]-AWSIncidentDetectionResponse-EventBus인 EventBridge 사용자 지정 이벤트 버스를 만듭니다.
   - (대체 방법) 사용자 지정 이벤트 버스 대신 기본 EventBridge 이벤트 버스를 사용합니다.

   AWS 사고 탐지 및 대응은 AWSHealthEventProcessorEventSource-DO-NOT-DELETE SLR을 통해 사용자 지정 또는 기본 이벤트 버스에 관리형 규칙(AWSServiceRoleForHealth_EventProcessor)을 설치합니다. 규칙 소스는 사용자 지정 또는 기본 이벤트 버스이고, 규칙 대상은 AWS 사고 탐지 및 대응이며, 규칙은 타사 APM 이벤트 수집 패턴과 일치합니다.
3. $YourApmName-AWSIncidentDetectionResponse-LambdaFunction이라는 Lambda 함수를 생성하여 SNS 페이로드를 변환합니다.
   - 변환된 이벤트는 EventBridge를 사용하여 APM 알림을 수집하기 위한 페이로드 요구 사항에 명시된 페이로드 요구 사항을 충족해야 합니다.
   - Lambda 함수의 대상을 2단계에서 생성한 사용자 지정 이벤트 버스(권장) 또는 기본 이벤트 버스로 설정합니다.
4. SNS 주제를 Lambda 함수 $YourApmName-AWSIncidentDetectionResponse-LambdaFunction의 트리거로 설정합니다.
   - '트리거 추가' 페이지에서 'SNS'를 검색합니다.
   - 1단계에서 생성한 전용 SNS 주제의 ARN을 추가합니다.
   - '추가'를 선택합니다.
5. APM 설명서에 따라 AWS 사고 탐지 및 대응에서 수집해야 하는 APM 페이로드의 SNS 대상을 설정합니다.

AWS 사고 탐지 및 대응은 AWSHealthEventProcessorEventSource-DO-NOT-DELETE SLR을 통해 사용자 지정 또는 기본 이벤트 버스에 관리형 규칙(AWSServiceRoleForHealth_EventProcessor)을 설치합니다. 규칙 소스는 사용자 지정 또는 기본 이벤트 버스이고, 규칙 대상은 AWS 사고 탐지 및 대응이며, 규칙은 타사 APM 이벤트 수집 패턴과 일치합니다.

경보 최적화 및 모니터링 조정

최적의 사고 탐지 정확도를 보장하기 위해 인시던트 관리 엔지니어는 중요한 워크로드에 대해 경보 성능을 지속적으로 평가합니다. 필요한 권장 경보 구성 변경 사항을 제공하고 사용자 및 기술 계정 관리자(TAM)와 사전에 협력하여 이러한 설정을 구체화합니다.

데이터 모니터링에서 해당 고객 영향 없이 경보가 트리거되거나 경보 상태가 자주 변동하는 경우와 같이 경보가 비즈니스 크리티컬 운영과 일치하지 않을 수 있는 것으로 나타나는 경우, 중요하지 않은 경보를 오프보딩하고 중요한 워크로드 영향을 더 잘 반영하는 경보를 온보딩하는 것이 좋습니다. 이를 통해 사고 대응 적용 범위의 전반적인 효과를 유지할 수 있습니다.

경보 검토 및 피드백

AWS 사고 탐지 및 대응은 모니터링을 위해 경보를 온보딩하기 전에 경보에 대한 포괄적인 검토를 수행합니다. 경보는 구성 파라미터, 데이터 품질 및 알림 효과를 포함한 기술적 수락 기준에 따라 평가됩니다.

이 검토를 기반으로 두 가지 유형의 피드백이 제공됩니다.

- 필수 구성 요구 사항 - 경보 수락을 위해 이러한 변경 사항을 구현해야 합니다.
- 선택적 개선 권장 사항 - 이러한 변경 사항은 경보 효과를 개선하지만 경보 수락에 필수는 아닙니다.

이 피드백을 받은 후 필수 구성 요구 사항이 있는 경보에 대한 구성 변경을 동시에 수행하면서 수락된 경보와 선택적 개선이 필요한 경보만 온보딩하도록 결정할 수 있습니다.

또는 가동하기 전에 모든 변경 사항을 구현할 수 있습니다. 이 접근 방식은 조정이 필요한 경보 수에 따라 온보딩 타임라인을 확장합니다.

경보 테스트(게임데이)

AWS 사고 탐지 및 대응 온보딩 프로세스의 마지막 단계는 새 워크로드에 대한 게임데이를 수행하는 것입니다. 경보 수집 단계를 완료하면 AWS 사고 탐지 및 대응에서 사용자가 선택한 게임데이 시작 날짜와 시간을 확인합니다.

게임데이는 다음의 두 가지 주요 목적을 위한 것입니다.

- 기능 검증: AWS 사고 탐지 및 대응이 경보 이벤트를 올바르게 수신할 수 있는지 확인합니다. 또한 기능 검증을 통해 경보 이벤트가 원하는 작업(예: 경보 수집 시 선택한 경우 자동 지원 사례 생성)을 트리거하는지 확인할 수 있습니다.

- 시뮬레이션: 게임데이는 실제 인시던트 중에 발생할 수 있는 상황을 전체적으로 다루는 시뮬레이션입니다. AWS 사고 탐지 및 대응은 실제 사고가 어떻게 전개될 수 있는지에 대한 통찰력을 제공합니다. 게임데이는 질문을 하거나 지침을 구체화하여 참여도를 개선할 수 있는 기회입니다.

경보 테스트 중에 AWS 사고 탐지 및 대응은 사용자와 협력하여 식별된 문제를 해결합니다.

CloudWatch 경보 테스트

게임데이 중에는 AWS Command Line Interface를 사용하여 경보를 경보 상태로 수동으로 변경하여 Amazon CloudWatch 경보를 테스트합니다. AWS CloudShell에서 AWS CLI에 액세스할 수 있습니다. AWS 사고 탐지 및 대응은 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
```

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

CloudWatch 경보의 상태를 수동으로 변경하는 방법에 대한 자세한 내용은 SetAlarmState를 참조하세요.

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

타사 APM 경보 테스트

Datadog, Splunk, New Relic 또는 Dynatrace와 같은 타사 애플리케이션 성능 모니터링(APM) 도구를 사용하는 워크로드로 경보를 시뮬레이션하려면 다른 지침이 필요합니다. 게임데이가 시작될 때 AWS 사고 탐지 및 대응은 경보 임곗값 또는 비교 연산자를 일시적으로 변경하여 경보를 경보 상태로 강제 전환하도록 요청합니다. 이 상태는 AWS 사고 탐지 및 대응에 대한 페이로드를 트리거합니다.

게임데이는 다음 사항을 검증합니다.

- 경보 수집에 성공하고 경보 구성이 정확합니다.

- 경보가 AWS 사고 탐지 및 대응에서 성공적으로 생성 및 수신되었습니다.
- 해당 문제에 대한 지원 사례가 생성되고, 지정된 런북 연락처로 알림이 전송됩니다.
- AWS 사고 탐지 및 대응은 사용자가 정의한 회의 브리지 방식을 통해 사용자와 소통할 수 있습니다.

경보 가동

게임데이가 성공적으로 완료되면 AWS 사고 탐지 및 대응은 온보딩 지원 사례를 통해 실시간 통신을 전송합니다. 이 시점부터 온보딩된 경보가 모니터링되고 온보딩된 경보가 경보 상태가 되면 워크로드의 연락처 세부 정보에 따라 AWS 사고 탐지 및 대응이 사용자를 참여시킵니다.

핵심 결과물

- AWS 사고 탐지 및 대응 시스템에서 워크로드를 모니터링하기 시작했음을 확인하는 가동 안내가 발송됩니다.

게임데이 중에 식별된 모든 필수 변경 사항, AWS 사고 탐지 및 대응은 사고 탐지 및 대응에서 온보딩된 워크로드에 대한 변경 요청를 사용하여 이를 이행합니다.

사고 탐지 및 대응(예외 경로)에서의 워크로드 온보딩 및 경보 수집 설문지

> **Note**
>
> AWS 사고 탐지 및 대응 고객 명령줄 인터페이스를 사용하여 워크로드를 온보딩할 수 없는 경우 워크로드 및 경보 온보딩에 대해 다음 설문지를 사용합니다.

이 페이지에서는 AWS 사고 탐지 및 대응에 워크로드를 온보딩하고 서비스에 수집하도록 경보를 구성할 때 완료해야 하는 설문지를 제공합니다. 워크로드 온보딩 설문은 워크로드, 아키텍처 세부 정보 및 인시던트 대응을 위한 연락처에 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 주요 단계입니다.

다음 워크로드 온보딩 설문지를 다운로드합니다.

- 영어 버전

- 일본어 버전

다음 경보 수집 설문지를 다운로드합니다.

- 영어 버전
- 일본어 버전

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 창출기입니다.
이 워크로드에 적용되는 규정 준수 및/또는 규제 요구 사항과 인시던트 발생 후 AWS에 필요한 모든 조치.	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. AWS는 이러한 태그를 사용하여 이 워크로드의 리소스를 식별하여 인시던트 발생 시 지원을 신속하게 처리합니다.	appName: Optimax 환경: 프로덕션

질문	응답의 예
Note 태그는 대/소문자를 구분합니다. 여러 태그를 제공하는 경우 이 워크로드에서 사용하는 모든 리소스에 동일한 태그가 있어야 합니다.	
이 워크로드와 해당 워크로드가 속한 AWS 계정 및 리전에서 사용하는 AWS 서비스 목록입니다. Note 각 서비스에 대해 새 행을 생성합니다.	Route 53: 인터넷 트래픽을 ALB로 라우팅합니다. 계정: 123456789101 리전: US-EAST-1, US-WEST-2
이 워크로드와 해당 워크로드가 속한 AWS 계정 및 리전에서 사용하는 AWS 서비스 목록입니다. Note 각 서비스에 대해 새 행을 생성합니다.	ALB: 수신 트래픽을 ECS 컨테이너의 대상 그룹으로 라우팅합니다. 계정: 123456789101 리전: 해당 사항 없음
이 워크로드와 해당 워크로드가 속한 AWS 계정 및 리전에서 사용하는 AWS 서비스 목록입니다. Note 각 서비스에 대해 새 행을 생성합니다.	ECS: 주요 비즈니스 로직 플릿을 위한 컴퓨팅 인프라입니다. 수신 사용자 요청을 처리하고 지속성 계층에 대한 쿼리를 수행할 책임이 있습니다. 계정: 123456789101 리전: US-EAST-1

질문	응답의 예
이 워크로드와 해당 워크로드가 속한 AWS 계정 및 리전에서 사용하는 AWS 서비스 목록입니다. 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 워크로드와 해당 워크로드가 속한 AWS 계정 및 리전에서 사용하는 AWS 서비스 목록입니다. Note 각 서비스에 대해 새 행을 생성합니다.	S3: 웹 사이트 정적 자산을 저장합니다. 계정: 123456789101 리전: 해당 사항 없음
중단이 발생할 경우 이 워크로드에 영향을 미칠 수 있는 온보딩되지 않은 업스트림/다운스트림 구성 요소를 자세히 설명합니다.	인증 마이크로서비스: 사용자가 인증되지 않은 상태 레코드를 로드하지 못하도록 합니다.
이 워크로드에 온프레미스 또는 비AWS 구성 요소가 있나요? 그렇다면 무엇이고 어떤 함수가 수행되나요?	AWS의 모든 인터넷 기반 트래픽은 온프레미스 프록시 서비스를 통해 라우팅됩니다.
가용 영역 및 리전 수준에서 수동 또는 자동 장애 조치/재해 복구 계획에 대한 세부 정보를 제공합니다.	예열 대기 방식입니다. 성공률이 지속적으로 저하되는 동안 US-WEST-2로의 자동 장애 조치입니다.

경보 수집 설문지 - 개요

경보 수집 설문지에서 AWS 사고 탐지 및 대응에 참여하려는 워크로드에 대한 중요한 경보와 이러한 경보가 트리거될 때 인시던트 관리 엔지니어가 참여시키려는 연락처를 지정합니다.

경보 수집 설문지는 다음 섹션으로 나뉩니다.

- 연락처 섹션: 먼저 경보가 트리거될 때 AWS 사고 탐지 및 대응으로 생성된 지원 사례에 포함할 기본 연락처와 인시던트 브리지를 위한 선호하는 회의 애플리케이션을 지정합니다. 브리지 기본 설정이

제공되지 않은 경우 AWS 사고 탐지 및 대응은 인시던트 중에 인시던트 브리지를 생성합니다. 다음으로, 기본 연락처에 연결할 수 없는 경우 참여시키기 위한 에스컬레이션 연락처 및 시간 간격을 지정합니다. 마지막으로 인시던트 기간 동안 지원 사례를 통해 정기적인 인시던트 상태 업데이트를 받아야 하는 연락처를 나열합니다.

- 경보 매트릭스: 트리거될 때 AWS 사고 탐지 및 대응과 관련된 경보 세트를 나열합니다. 온보딩을 위한 경보를 선택할 때 AWS 사고 탐지 및 대응에서 정의한 '중요 경보 기준'을 참조하세요. 자세한 내용은 경보 정의 섹션을 참조하세요.
  - Amazon CloudWatch 경보(Amazon CloudWatch 경보가 없는 경우 이 섹션을 비워 둡니다.)
  - 타사 APM 경보(타사 APM 경보가 없는 경우 이 섹션을 비워둡니다.)
    - EventBridge EventBus ARN: 직접 EventBridge 통합으로 APM에서 경보 수집 또는 EventBridge와 직접 통합하지 않고도 APM에서 경보 수집에서 생성한 사용자 지정 EventBus ARN의 ARN입니다.
    - 경보 식별자: APM 경보의 계정 번호, 리전 및 이름을 공유합니다.

경보 수집 설문지 - 런북 질문

런북 질문

질문	응답의 예
AWS는 지원 사례를 통해 워크로드 연락처를 참여시킵니다. 이 워크로드에 대해 경보가 트리거될 때 기본 연락처는 누구인가요? 선호하는 회의 애플리케이션을 지정하면 인시던트 발생 시 AWS가 세부 정보를 요청합니다. **Note** 선호하는 회의 애플리케이션이 제공되지 않은 경우 AWS는 인시던트 발생 시 연락하여 조인할 수 있는 Chime 브리지를 제공합니다.	애플리케이션 팀 app@example.com +61 2 3456 7890

질문	응답의 예
인시던트 발생 시 기본 연락처를 사용할 수 없는 경우 선호하는 커뮤니케이션 순서로 에스컬레이션 연락처와 타임라인을 제공하세요.	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
AWS는 인시던트 전반에 걸쳐 정기적으로 지원 사례를 통해 업데이트를 전달합니다. 이러한 업데이트를 받아야 하는 추가 연락처가 있나요?	john.smith@example.com, jane.smith@example.com

경보 매트릭스

다음 정보를 제공하여 워크로드를 대신하여 인시던트를 생성하기 위해 AWS 사고 탐지 및 대응과 관련된 경보 세트를 식별합니다. AWS 사고 탐지 및 대응의 엔지니어가 경보를 검토하면 추가 온보딩 단계가 제공됩니다.

AWS 사고 탐지 및 대응 중요 경보 기준:

- AWS 사고 탐지 및 대응 경보는 즉각적인 운영자 주의가 필요한 모니터링되는 워크로드에 상당한 비즈니스 영향(수익 손실/고객 경험 저하)이 있을 때만 '경보' 상태로 전환되어야 합니다.
- AWS 사고 탐지 및 대응 경보는 동시에 또는 참여 전에 워크로드에 대한 해석기를 참여시켜야 합니다. AWS 인시던트 관리자는 완화 프로세스에서 해석기와 협업하며, 1차 대응 담당자 역할을 하지 않습니다. 대응 담당자는 사용자에게 에스컬레이션합니다.

- AWS 사고 탐지 및 대응 경보 임곗값은 경보가 조사를 실행할 때마다 적절한 임곗값 및 기간으로 설정해야 합니다. 경보가 '경보' 상태와 '정상' 상태 사이에서 이동하는 경우 운영자의 응답과 주의를 끌기에 충분한 영향이 발생합니다.

기준 위반에 대한 AWS 사고 탐지 및 대응 정책:

이러한 기준은 이벤트가 발생할 때 사례별로만 평가할 수 있습니다. 인시던트 관리 팀은 기술 계정 관리자(TAM)와 협력하여 경보를 조정하고 드물게 고객 경보가 이 기준을 준수하지 않는 것으로 의심되고 인시던트 관리 팀을 정기적으로 참여시키는 경우 모니터링을 비활성화합니다.

> **Important**
>
> 런북 업데이트 없이 수신자 추가 및 삭제를 제어할 수 있도록 연락처 주소를 제공할 때 그룹 배포 이메일 주소를 제공합니다.
> 초기 참여 이메일을 보낸 후 AWS 사고 탐지 및 대응 팀이 전화를 걸도록 하려면 사이트 신뢰성 엔지니어링(SRE) 팀의 연락처 전화번호를 제공합니다.

경보 매트릭스 테이블

지표 이름/ARN/임곗값	설명	참고	요청된 작업
워크로드 볼륨 / *CW ## ARN* / 5분 이내에 5개의 데이터 포인트에 대해 CallCount < 100000, 누락된 데이터를 누락으로 처리	이 지표는 Application Load Balancer 수준에서 측정된 워크로드로 들어오는 수신 요청 수를 나타냅니다. 이 경보는 수신 요청이 크게 감소하면 업스트림 네트워크 연결 문제 또는 사용자가 워크로드에 액세스할 수 없게 되는 DNS 구현 문제를 나타낼 수 있으므로 중요합니다.	경보가 지난주에 '경보' 상태로 10회 전환되었습니다. 이 경보는 거짓 긍정의 위험이 있습니다. 임곗값 검토가 계획되어 있습니다. 문제가 있나요? 아니요 또는 예(아니요인 경우 비워 둠):이 경보는 특정 배치 작업 실행 중에 자주 뒤집힙니다. 해석기: 사이트 신뢰성 엔지니어	*SRE@example.com* 으로 이메일을 보내 사이트 신뢰성 엔지니어링 팀을 참여시킵니다. ELB 및 Amazon Route 53 서비스에 대한 AWS Support 사례를 생성합니다. 즉각적인 작업이 필요한 경우: EC2 여유 메모리/디스크 공간을 확인하고 ## 팀에 이메일을 통해 인스턴스를 다시 시작하거나 로그

지표 이름/ARN/임곗값	설명	참고	요청된 작업
			플러시를 실행합니다(즉각적인 작업이 필요하지 않은 경우 비워 둠).
워크로드 요청 지연 시간 / *CW ## ARN* / 5분 이내에 5개의 데이터 포인트에 대해 p90 지연 시간 > 100ms, 누락된 데이터를 누락으로 처리	이 지표는 워크로드가 이행할 HTTP 요청의 p90 지연 시간을 나타냅니다. 이 경보는 웹 사이트에 대한 고객 경험의 중요한 척도인 지연 시간을 나타냅니다.	경보가 지난주에 '경보' 상태로 0회 전환되었습니다. 문제가 있나요? 아니요 또는 예(아니요인 경우 비워 둠):이 경보는 특정 배치 작업 실행 중에 자주 뒤집힙니다. 해석기: 사이트 신뢰성 엔지니어	*SRE@example.com* 으로 이메일을 보내 사이트 신뢰성 엔지니어링 팀을 참여시킵니다. ECW 및 RDS 서비스에 대한 AWS Support 사례를 생성합니다. 즉각적인 작업이 필요한 경우: EC2 여유 메모리/디스크 공간을 확인하고 *##* 팀에 이메일을 통해 인스턴스를 다시 시작하거나 로그 플러시를 실행합니다(즉각적인 작업이 필요하지 않은 경우 비워 둠).

지표 이름/ARN/임곗값	설명	참고	요청된 작업
워크로드 요청 가용성 / *CW ## ARN* / 5분 이내에 5개의 데이터 포인트에 대해 가용성 < 95%인 경우 누락된 데이터를 누락으로 처리합니다.	이 지표는 워크로드가 이행할 HTTP 요청의 가용성을 나타냅니다(HTTP 200 수/요청 수). 이 경보는 워크로드의 가용성을 나타냅니다.	경보가 지난주에 '경보' 상태로 0회 전환되었습니다. 문제가 있나요? 아니요 또는 예(아니요인 경우 비워 둠):이 경보는 특정 배치 작업 실행 중에 자주 뒤집힙니다. 해석기: 사이트 신뢰성 엔지니어	*SRE@example.com* 으로 이메일을 보내 사이트 신뢰성 엔지니어링 팀을 참여시킵니다. ELB 및 Amazon Route 53 서비스에 대한 AWS Support 사례를 생성합니다. 즉각적인 작업이 필요한 경우: EC2 여유 메모리/디스크 공간을 확인하고 *##* 팀에 이메일을 통해 인스턴스를 다시 시작하거나 로그 플러시를 실행합니다(즉각적인 작업이 필요하지 않은 경우 비워 둠).
New Relic 경보 예제			

지표 이름/ARN/임곗값	설명	참고	요청된 작업
엔드 투 엔드 통합 테스트 / *CW ## ARN* / 3분 동안 1분 지표의 실패율 3%, 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.	경보가 지난주에 '경보' 상태로 0회 전환되었습니다. 문제가 있나요? 아니요 또는 예(아니요인 경우 비워 둠):이 경보는 특정 배치 작업 실행 중에 자주 뒤집힙니다. 해석기: 사이트 신뢰성 엔지니어	*SRE@example.com* 으로 이메일을 보내 사이트 신뢰성 엔지니어링 팀을 참여시킵니다. Amazon Elastic Container Service 및 Amazon DynamoDB 서비스에 대한 AWS Support 사례를 생성합니다. 즉각적인 작업이 필요한 경우: EC2 여유 메모리/디스크 공간을 확인하고 *##* 팀에 이메일을 통해 인스턴스를 다시 시작하거나 로그 플러시를 실행합니다(즉각적인 작업이 필요하지 않은 경우 비워 둠).

사고 탐지 및 대응에서 워크로드 관리

효과적인 인시던트 관리의 핵심은 모니터링되는 워크로드를 온보딩, 테스트 및 유지하기 위한 올바른 프로세스와 절차를 마련하는 것입니다. 이 섹션에서는 팀에 인시던트를 안내하기 위한 포괄적인 런북 및 대응 계획 개발, 온보딩 전 새 워크로드에 대한 철저한 테스트 및 검증, 변경 요청을 통한 워크로드 모니터링 업데이트, 필요에 따른 적절한 워크로드 오프보딩을 비롯한 필수 단계를 다룹니다.

주제

- 사고 탐지 및 대응에서 인시던트에 대응하기 위한 런북 및 대응 계획 개발
- 사고 탐지 및 대응에서 온보딩된 워크로드 테스트
- 사고 탐지 및 대응에서 온보딩된 워크로드에 대한 변경 요청
- 사고 탐지 및 대응과 관련된 경보 억제
- 사고 탐지 및 대응에서 워크로드 오프보딩

사고 탐지 및 대응에서 인시던트에 대응하기 위한 런북 및 대응 계획 개발

사고 탐지 및 대응은 AWS 사고 탐지 및 대응 고객 명령줄 인터페이스 온보딩에서 수집한 정보를 사용하여 워크로드에 영향을 미치는 인시던트 관리를 위한 런북 및 대응 계획을 개발합니다. Incident Manager가 인시던트에 대응할 때 수행하는 런북 문서 단계입니다. 응답 계획은 하나 이상의 워크로드에 매핑됩니다. 인시던트 관리 팀은 워크로드 온보딩 중에 사용자가 제공한 정보를 바탕으로 이러한 템플릿을 생성합니다. 대응 계획은 인시던트를 트리거하는 데 사용되는 AWS Systems Manager(SSM) 문서 템플릿입니다. SSM 문서에 대한 자세한 내용은 AWS Systems Manager 문서를 참조하세요. Incident Manager에 대한 자세한 내용은 AWS Systems Manager Incident Manager란 무엇인가요?를 참조하세요.

핵심 결과물:

- AWS 사고 탐지 및 대응에 대한 워크로드 정의를 완료합니다.
- AWS 사고 탐지 및 대응에 대한 경보, 런북 및 대응 계획 정의를 완료합니다.

AWS 사고 탐지 및 대응 런북 예제 aws-idr-runbook-example.zip을 다운로드할 수도 있습니다.

예제 런북:

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.
```

사고 탐지 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 게임데이를 수행하는 것입니다. 경보 수집이 완료되면 AWS 사고 탐지 및 대응은 게임데이를 시작하기로 선택한 날짜와 시간을 확인합니다.

게임데이는 다음의 두 가지 주요 목적을 위한 것입니다.

- 기능 검증: AWS 사고 탐지 및 대응이 경보 이벤트를 올바르게 수신할 수 있는지 확인합니다. 또한 기능 검증은 경보 이벤트가 적절한 런북과 자동 사례 생성(경보 수집 시 선택한 경우)과 같은 기타 원하는 작업을 트리거하는지 확인합니다.
- 시뮬레이션: 게임데이는 실제 인시던트 중에 발생할 수 있는 상황을 전체적으로 다루는 시뮬레이션입니다. AWS 사고 탐지 및 대응은 규정된 런북 단계에 따라 실제 인시던트가 어떻게 전개될 수 있는지에 대한 인사이트를 제공합니다. 게임데이는 질문을 하거나 지침을 구체화하여 참여도를 개선할 수 있는 기회입니다.

경보 테스트 중에 AWS 사고 탐지 및 대응은 사용자와 협력하여 식별된 문제를 해결합니다.

CloudWatch 경보

AWS 사고 탐지 및 대응은 경보의 상태 변경을 모니터링하여 Amazon CloudWatch 경보를 테스트합니다. 이렇게 하려면 AWS Command Line Interface를 사용하여 경보를 경보 상태로 수동으로 변경합니다. AWS CloudShell에서 AWS CLI에 액세스할 수 있습니다. AWS 사고 탐지 및 대응은 테스트 중에 사용할 수 있는 AWS CLI 명령 목록을 제공합니다.

Amazon EC2 인스턴스 재시작과 같은 원치 않는 작업을 방지하려면 경보 상태를 변경하기 전에 CloudWatch 경보 작업을 비활성화하세요. 테스트가 완료된 후 CloudWatch 경보 작업을 다시 활성화할 수 있습니다. 경보 작업 비활성화 또는 활성화에 대한 자세한 내용은 Amazon CloudWatch API 참조의 DisableAlarmActions 및 EnableAlarmActions를 참조하세요.

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 경보의 상태를 수동으로 변경하는 방법에 대한 자세한 내용은 SetAlarmState를 참조하세요.

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

타사 APM 경보

Datadog, Splunk, New Relic 또는 Dynatrace와 같은 타사 애플리케이션 성능 모니터링(APM) 도구를 사용하는 워크로드로 경보를 시뮬레이션하려면 다른 지침이 필요합니다. 게임데이가 시작될 때 AWS 사고 탐지 및 대응은 경보 임곗값 또는 비교 연산자를 일시적으로 변경하여 경보를 경보 상태로 강제 전환하도록 요청합니다. 이 상태는 AWS 사고 탐지 및 대응에 대한 페이로드를 트리거합니다.

핵심 결과물

핵심 결과물:

- 경보 수집에 성공하고 경보 구성이 정확합니다.
- 경보가 AWS 사고 탐지 및 대응에서 성공적으로 생성 및 수신되었습니다.
- 참여에 대한 지원 사례가 생성되고 규정된 연락처에 알림이 전송됩니다.
- AWS 사고 탐지 및 대응은 미리 정해진 회의 수단을 통해 고객과 소통할 수 있습니다.
- 게임데이의 일부로 생성된 모든 경보 및 지원 사례가 해결됩니다.
- AWS 사고 탐지 및 대응에서 워크로드를 모니터링 중임을 확인하는 Go-Live 이메일이 전송됩니다.

사고 탐지 및 대응에서 온보딩된 워크로드에 대한 변경 요청

온보딩된 워크로드에 대한 변경을 요청하려면 다음 단계를 완료하여 AWS 사고 탐지 및 대응으로 지원 사례를 생성합니다.

1. 다음 예와 같이 AWS Support Center로 이동한 다음 사례 생성을 선택합니다.

2. 기술을 선택합니다.

3. 서비스에서 사고 탐지 및 대응을 선택합니다.
4. 범주에서 워크로드 변경 요청을 선택합니다.
5. 심각도에서 일반 지침을 선택합니다.
6. 이 변경 사항의 제목을 입력합니다. 예제:

   AWS 사고 탐지 및 대응 - *workload_name*
7. 이 변경 사항의 설명을 입력합니다. 예를 들어 "이 요청은 AWS 사고 탐지 및 대응에 온보딩된 기존 워크로드에 대한 변경 사항입니다"라고 입력합니다. 요청에 다음 정보를 포함해야 합니다.

   - 워크로드 이름: 워크로드 이름입니다.
   - 계정 ID: ID1, ID2, ID3 등.
   - 변경 세부 정보: 요청된 변경에 대한 세부 정보를 입력합니다.
8. 추가 연락처 - 선택 사항 섹션에서 이 변경 사항에 대한 서신을 받을 이메일 ID를 입력합니다.

   다음은 추가 연락처 - 선택 사항 섹션의 예입니다.

   > **Important**
   >
   > 추가 연락처 - 선택 사항 섹션에 이메일 ID를 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 추가 연락처 - 선택 사항 섹션에 이메일 ID를 추가합니다.

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

사고 탐지 및 대응과 관련된 경보 억제

온보딩된 워크로드 경보 중 AWS 사고 탐지 및 대응 모니터링과 관련된 경보를 일시적으로 또는 일정에 따라 억제하여 지정합니다. 예를 들어 계획된 유지 관리 중에 워크로드 경보를 일시적으로 억제하여

경보가 사고 탐지 및 대응과 연관되지 않도록 할 수 있습니다. 또는 일일 재부팅 활동이 있는 경우 일정에 따라 경보를 억제할 수 있습니다. Amazon CloudWatch와 같은 경보 소스에서 경보를 억제하거나 워크로드 변경 요청을 제출할 수 있습니다.

주제

- 경보 소스에서 경보 억제
- 경보를 억제하기 위한 워크로드 변경 요청 제출
- 자습서: 지표 수학 함수를 사용하여 경보 억제
- 자습서: 지표 수학 함수를 제거하여 경보 억제 해제

경보 소스에서 경보 억제

경보 소스에서 경보를 억제하여 사고 탐지 및 대응과 관련된 경보와 관련되는 시기를 지정합니다.

주제

- 지표 수학 함수를 사용하여 CloudWatch 경보 억제
- 지표 수학 함수를 제거하여 CloudWatch 경보 억제 해제
- 예제 지표 수학 함수 및 관련 사용 사례
- 타사 APM에서 경보 억제

지표 수학 함수를 사용하여 CloudWatch 경보 억제

Amazon CloudWatch 경보의 사고 탐지 및 대응 모니터링을 억제하려면 지표 수학 함수를 사용하여 지정된 기간 동안 CloudWatch 경보가 `ALARM` 상태로 전환되지 않도록 합니다.

> **Note**
>
> CloudWatch 경보에서 경보 작업을 비활성화해도 사고 탐지 및 대응을 통한 경보 모니터링이 억제되지 않습니다. 경보 상태 변경은 CloudWatch 경보 작업이 아닌 Amazon EventBridge를 통해 수집됩니다.

지표 수학 함수를 사용하여 CloudWatch 경보를 억제하려면 다음 단계를 완료합니다.

1. AWS Management Console에 로그인하고 https://console.aws.amazon.com/cloudwatch/에서 CloudWatch 콘솔을 엽니다.

2. 경보를 선택한 다음 지표 수학 함수를 추가할 경보를 찾습니다.
3. 작업 및 편집을 차례로 선택하여 경보를 변경합니다.
4. 지표 편집을 선택하여 경보에 대한 지표를 수정합니다.
5. 수학 추가, 빈 표현식으로 시작을 선택합니다.
6. 수학 표현식을 입력한 다음 적용을 선택합니다.
7. 경보가 모니터링한 기존 지표를 선택 취소합니다.
8. 생성한 표현식을 선택한 후 지표 선택을 선택합니다.
9. 검토 및 생성 건너뛰기를 선택합니다.
10. 변경 사항을 검토하여 지표 수학 함수가 정상적으로 적용되었는지 확인한 다음 경보 업데이트를 선택합니다.

지표 수학 함수를 사용하여 CloudWatch 경보를 억제하는 단계별 예제는 자습서: 지표 수학 함수를 사용하여 경보 억제 섹션을 참조하세요.

구문 및 사용 가능한 함수에 대해 자세히 알아보려면 Amazon CloudWatch 사용 설명서의 지표 수학 구문 및 함수를 참조하세요.

지표 수학 함수를 제거하여 CloudWatch 경보 억제 해제

지표 수학 함수를 제거하여 CloudWatch 경보의 억제를 해제합니다. 경보에서 지표 수학 함수를 제거하려면 다음 단계를 완료합니다.

1. AWS Management Console에 로그인하고 https://console.aws.amazon.com/cloudwatch/에서 CloudWatch 콘솔을 엽니다.
2. 경보를 선택한 다음 지표 수학 표현식을 제거할 경보를 찾습니다.
3. 지표 수학 섹션에서 편집을 선택합니다.
4. 경보에서 지표를 제거하려면 지표에서 편집을 선택한 다음 지표 수학 표현식 옆에 있는 x 버튼을 선택합니다.
5. 원래 지표를 선택한 다음 지표 선택을 선택합니다.
6. 검토 및 생성 건너뛰기를 선택합니다.
7. 변경 사항을 검토하여 지표 수학 함수가 정상적으로 적용되었는지 확인한 다음 경보 업데이트를 선택합니다.

예제 지표 수학 함수 및 관련 사용 사례

다음 표에는 관련 사용 사례 및 각 지표 구성 요소에 대한 설명과 함께 지표 수학 함수 예제가 포함되어 있습니다.

지표 수학 함수	사용 사례	설명
`IF((DAY(m1) == 2 && HOUR(m1) >= 1 && HOUR(m1) < 3), 0, m1)`	이 기간 동안 실제 데이터 포인트를 0으로 대체하여 UTC 기준 매주 화요일 오전 1시~3시 사이에 경보를 억제합니다.	• DAY(m1) == 2: 화요일인지 확인합니다(월요일 = 1, 일요일 = 7). • HOUR(m1) >= 1 && HOUR(m1) > 3: UTC 기준 오전 1시~오전 3시의 시간 범위를 지정합니다. • IF(condition, value_if_true, value_if_false): 조건이 true인 경우 지표 값을 0으로 바꿉니다. 그렇지 않으면 원래 값(m1)을 반환합니다.
`IF((HOUR(m1) >= 23 || HOUR(m1) < 4), 0, m1)`	이 기간 동안 실제 데이터 포인트를 0으로 대체하여 UTC 기준 매일 오후 11시~오전 4시 사이에 경보를 억제합니다.	• HOUR(m1) >= 23: UTC 기준 23:00부터 시간을 캡처합니다. • HOUR(m1) < 4: UTC 기준 04:00(포함되지 않음)까지의 시간을 캡처합니다. • ||: 논리적 OR은 조건이 늦은 밤 시간과 이른 아침 시간이라는 두 가지 범위에 걸쳐 적용되도록 합니다. • IF(condition, value_if_true, value_if_false): 지정된 시간 범위 동안 0을 반환합니다. 원래 지표 값 m1을 해당 범위 밖으로 유지합니다.

지표 수학 함수	사용 사례	설명
`IF((HOUR(m1) >= 11 && HOUR(m1) < 13), 0, m1)`	이 기간 동안 실제 데이터 포인트를 0으로 대체하여 UTC 기준 매일 오전 11시~오후 1시 사이에 경보를 억제합니다.	• HOUR(m1) >= 11 && HOUR(m1) < 13: UTC 기준 11:00~13:00의 시간 범위를 캡처합니다. • IF(condition, value_if_true, value_if_false): 조건이 true인 경우(예: 시간이 UTC 기준 11:00~13:00인 경우), 0을 반환하고 조건이 false인 경우 원래 지표 값(m1)을 유지합니다.
`IF((DAY(m1) == 2 && HOUR(m1) >= 1 && HOUR(m1) < 3), 99, m1)`	이 기간 동안 실제 데이터 포인트를 99로 대체하여 UTC 기준 매주 화요일 오전 1시~3시 사이에 경보를 억제합니다.	• DAY(m1) == 2:: 화요일인지 확인합니다(월요일 = 1, 일요일 = 7). • HOUR(m1) >= 1 && HOUR(m1) < 3: UTC 기준 오전 1시~오전 3시의 시간 범위를 지정합니다. • IF(condition, value_if_true, value_if_false): 조건이 true인 경우 지표 값을 99로 바꿉니다. 그렇지 않으면 원래 값(m1)을 반환합니다.

지표 수학 함수	사용 사례	설명
`IF((HOUR(m1) >= 23 || HOUR(m1) < 4), 100, m1)`	이 기간 동안 실제 데이터 포인트를 100으로 대체하여 UTC 기준 매일 오후 11시~오전 4시 사이에 경보를 억제합니다.	• HOUR(m1) >= 23: UTC 기준 23:00부터 시간을 캡처합니다. • HOUR(m1) < 4: UTC 기준 04:00(포함되지 않음)까지의 시간을 캡처합니다. • ||: 논리적 OR은 조건이 늦은 밤 시간과 이른 아침 시간이라는 두 가지 범위에 걸쳐 적용되도록 합니다. • IF(condition, value_if_true, value_if_false): 지정된 시간 범위 동안 100을 반환합니다. 원래 지표 값 m1을 해당 범위 밖으로 유지합니다.
`IF((HOUR(m1) >= 11 && HOUR(m1) < 13), 99, m1)`	이 기간 동안 실제 데이터 포인트를 99로 대체하여 UTC 기준 매일 오전 11시~오후 1시 사이에 경보를 억제합니다.	• HOUR(m1) >= 11 && HOUR(m1) < 13: UTC 기준 11:00~13:00의 시간 범위를 캡처합니다. • IF(condition, value_if_true, value_if_false): 조건이 true인 경우(예: 시간이 UTC 기준 11:00~13:00인 경우), 99를 반환합니다. 조건이 false인 경우 원래 지표 값(m1)을 유지합니다.

타사 APM에서 경보 억제

경보를 억제하는 방법에 대한 지침은 타사 APM 공급업체의 설명서를 참조하세요. 타사 APM 공급업체의 예로는 New Relic, Splunk, Dynatrace, Datadog 및 SumoLogic이 있습니다.

경보를 억제하기 위한 워크로드 변경 요청 제출

이전 섹션에 설명된 대로 소스에서 경보를 억제할 수 없는 경우, 워크로드 변경 요청을 제출하여 워크로드 경보의 일부 또는 전부에 대한 모니터링을 수동으로 억제하도록 사고 탐지 및 대응을 지시합니다.

워크로드 변경 요청을 생성하는 방법에 대한 자세한 지침은 사고 탐지 및 대응의 온보딩된 워크로드에 대한 변경 요청을 참조하세요. 워크로드 변경 요청을 제기하여 경보 억제를 요청할 때 다음 필수 정보를 제공해야 합니다.

- 워크로드 이름: 워크로드 이름입니다.
- 계정 ID: ID1, ID2, ID3 등.
- 변경 세부 정보: 경보 억제
- 억제 시작 시간: 날짜, 시간 및 시간대.
- 억제 종료 시간: 날짜, 시간 및 시간대.
- 억제할 경보: 억제할 CloudWatch 경보 ARN 또는 타사 APM 이벤트 식별자 목록입니다.

경보 억제 워크로드 변경 요청을 생성하면 사고 탐지 및 대응으로부터 다음 알림을 받게 됩니다.

- 워크로드 변경 요청 승인.
- 경보가 억제될 때의 알림입니다.
- 모니터링을 위해 경보를 다시 활성화할 때의 알림입니다.

자습서: 지표 수학 함수를 사용하여 경보 억제

다음 자습서에서는 지표 수학을 사용하여 CloudWatch 경보를 억제하는 방법을 안내합니다.

예제 시나리오

UTC 기준 오는 화요일 오전 1시부터 오전 3시까지 예정된 활동이 있습니다. 이 시간 동안 실제 데이터 포인트를 0(설정된 임곗값보다 낮은 데이터 포인트)으로 대체하는 CloudWatch 지표 수학 함수를 생성하려고 합니다.

1. 경보가 트리거되는 기준을 평가합니다. 다음 스크린샷은 경보 기준의 예를 제공합니다.

   이전 스크린샷에 표시된 경보는 Application Load Balancer 대상 그룹의 `UnHealthyHostCount` 지표를 모니터링합니다. 이 경보는 `UnHealthyHostCount` 지표가 5개의 데이터 포인트 중 5개에

대해 3보다 크거나 같을 때 ALARM 상태로 전환됩니다. 경보는 누락된 데이터를 불량으로 처리합니다(구성된 임곗값 위반).

2. 지표 수학 함수를 생성합니다.

   이 예제에서는 UTC 기준 오는 화요일 오전 1시부터 오전 3시까지 예정된 활동이 있습니다. 따라서 이 시간 동안 실제 데이터 포인트를 0(설정된 임곗값보다 낮은 데이터 포인트)으로 대체하는 CloudWatch 지표 수학 함수를 생성하려고 합니다.

   구성해야 하는 대체 데이터 포인트는 경보 구성에 따라 다릅니다. 예를 들어 임곗값이 98 미만인 HTTP 성공률을 모니터링하는 경보가 있는 경우, 계획된 활동 중 실제 데이터 포인트를 구성된 임곗값인 100보다 큰 값으로 바꿉니다. 다음은 이 시나리오에 대한 지표 수학 함수의 예입니다.

   ```
   IF((DAY(m1) == 2 && HOUR(m1) >= 1 && HOUR(m1) < 3), 0, m1)
   ```

   이전 지표 수학 함수에는 다음 요소가 포함되어 있습니다.

   - DAY(m1) == 2: 화요일인지 확인합니다(월요일 = 1, 일요일 = 7).
   - HOUR(m1) >= 1 && HOUR(m1) < 3: UTC 기준 오전 1시~오전 3시의 시간 범위를 지정합니다.
   - IF(condition, value_if_true, value_if_false): 조건이 true인 경우 함수는 지표 값을 0으로 바꿉니다. 그렇지 않으면 원래 값(m1)이 반환됩니다.

   구문 및 사용 가능한 함수에 대한 자세한 정보는 Amazon CloudWatch 사용 설명서의 지표 수학 구문 및 함수를 참조하세요.

3. AWS Management Console에 로그인하고 https://console.aws.amazon.com/cloudwatch/에서 CloudWatch 콘솔을 엽니다.
4. 경보를 선택한 다음 지표 수학 함수를 추가할 경보를 찾습니다.
5. 지표 수학 섹션에서 편집을 선택합니다.
6. 수학 추가, 빈 표현식으로 시작을 선택합니다.
7. 수학 표현식을 입력한 다음 적용을 선택합니다.

   다음 예제와 같이 경보가 자동으로 모니터링하는 기존 지표는 m1이 되고 수학 표현식은 e1이 됩니다.

8. (선택 사항) 다음 예와 같이 지표 수학 표현식의 레이블을 편집하여 다른 사용자가 함수와 생성된 이유를 이해하는 데 도움을 줍니다.

9. m1을 선택 취소하고 e1을 선택한 다음 지표 선택을 선택합니다. 이렇게 하면 기본 지표 대신 수학 표현식을 직접 모니터링하도록 경보가 설정됩니다.
10. 검토 및 생성 건너뛰기를 선택합니다.
11. 경보가 정상적으로 구성되어 있는지 확인한 다음 경보 업데이트를 선택하여 변경 사항을 저장합니다.

앞의 예에서 지표 수학 함수를 적용하지 않으면 계획된 활동 중에 실제 `UnHealthyHostCount` 지표가 보고되었을 것입니다. 이렇게 하면 다음 예제와 같이 CloudWatch 경보가 `ALARM` 상태로 전환되고 사고 탐지 및 대응이 개입됩니다.

지표 수학 함수를 사용하면 활동 중에 실제 데이터 포인트가 0으로 대체되고 경보는 `OK` 상태로 유지되어 사고 탐지 및 대응 참여를 억제합니다.

자습서: 지표 수학 함수를 제거하여 경보 억제 해제

일회성 활동에 대해 CloudWatch 경보를 억제한 경우, 활동이 완료된 후 경보에서 지표 수학 함수를 제거하여 경보의 정기적인 모니터링을 재개합니다. 예를 들어 매주 같은 요일과 시간에 인스턴스를 재부팅하는 예약된 주간 패치 루틴이 있는 경우 정기적으로 경보를 억제하려면 지표 수학 함수를 그대로 둡니다.

다음 자습서에서는 CloudWatch 경보의 억제를 해제하기 위해 지표 수학 함수를 제거하는 방법을 안내합니다.

1. AWS Management Console에 로그인하고 https://console.aws.amazon.com/cloudwatch/에서 CloudWatch 콘솔을 엽니다.
2. 경보를 선택한 다음 지표 수학 함수를 추가할 경보를 찾습니다.
3. 지표 수학 섹션에서 편집을 선택합니다.
4. 경보에서 억제를 제거하려면 지표 수학 표현식 옆에 있는 x 버튼을 선택합니다.
5. 지표를 선택하여 실제 지표의 모니터링을 재개한 다음 지표 선택을 선택합니다.
6. 검토 및 생성 건너뛰기를 선택합니다.
7. 경보가 정상적으로 구성되어 있는지 확인한 다음 경보 업데이트를 선택하여 변경 사항을 저장합니다.

사고 탐지 및 대응에서 워크로드 오프보딩

AWS 사고 탐지 및 대응에서 워크로드를 오프보딩하려면 각 워크로드에 대한 새 지원 사례를 생성합니다. 지원 사례를 생성할 때 다음 사항을 염두에 두어야 합니다.

- 단일 AWS 계정에 있는 워크로드를 오프보딩하려면 워크로드의 계정 또는 지급인 계정에서 지원 사례를 생성합니다.
- 여러 AWS 계정에 걸쳐 있는 워크로드를 오프보딩하려면 지급인 계정에서 지원 사례를 생성합니다. 지원 사례 본문에 오프보딩할 모든 계정 ID를 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 Center로 이동한 다음 사례 생성을 선택합니다.
2. 기술을 선택합니다.
3. 서비스에서 사고 탐지 및 대응을 선택합니다.
4. 범주에서 워크로드 오프보딩을 선택합니다.
5. 심각도에서 일반 지침을 선택합니다.
6. 이 변경 사항의 제목을 입력합니다. 예제:

   [오프보딩] AWS 사고 탐지 및 대응 - *workload_name*
7. 이 변경 사항의 설명을 입력합니다. 예를 들어 "이 요청은 AWS 사고 탐지 및 대응에 온보딩된 기존 워크로드에 대한 오프보딩입니다"라고 입력합니다. 요청에 다음 정보를 포함해야 합니다.

   - 워크로드 이름: 워크로드 이름입니다.
   - 계정 ID: ID1, ID2, ID3 등.
   - 오프보딩 이유: 워크로드를 오프보딩하는 이유를 제공합니다.
8. 추가 연락처 - 선택 사항 섹션에서 이 오프보딩 요청에 대한 서신을 받을 이메일 ID를 입력합니다.
9. 제출을 선택합니다.

AWS 사고 탐지 및 대응 모니터링 및 관찰성

AWS 사고 탐지 및 대응은 애플리케이션 계층에서 기본 인프라에 이르기까지 워크로드 전반의 관찰성을 정의하는 방법에 대한 전문가 지침을 제공합니다. 모니터링은 문제가 있음을 알려줍니다. 관찰성은 데이터 수집을 사용하여 무엇이 왜 발생했는지 알려줍니다.

사고 탐지 및 대응 시스템은 Amazon CloudWatch 및 Amazon EventBridge와 같은 네이티브 AWS 서비스를 활용하여 AWS 워크로드에 영향을 미칠 수 있는 이벤트를 감지하여 워크로드에 장애 및 성능 저하가 있는지 모니터링합니다. 모니터링을 통해 임박한 장애, 진행 중인 장애, 완화되는 장애 또는 잠재적 장애 또는 성능 저하에 대한 알림을 받을 수 있습니다. 계정을 사고 탐지 및 대응에 온보딩할 때 사고 탐지 및 대응 모니터링 시스템에서 모니터링해야 하는 계정의 경보를 선택하고 이러한 경보를 인시던트 관리 중에 사용되는 애플리케이션 및 런북과 연결합니다.

사고 탐지 및 대응은 Amazon CloudWatch 및 기타 AWS 서비스를 사용하여 관찰성 솔루션을 구축합니다. AWS 사고 탐지 및 대응은 다음 두 가지 방법으로 관찰성을 지원합니다.

- 비즈니스 성과 지표: AWS 사고 탐지 및 대응에 대한 관찰성은 워크로드 또는 최종 사용자 경험의 결과를 모니터링하는 주요 지표를 정의하는 것으로 시작됩니다. AWS 전문가는 고객과 협력하여 워크로드의 목표, 사용자 경험에 영향을 미칠 수 있는 핵심 결과물 또는 요소를 이해하고 이러한 주요 지표의 성능 저하를 파악하는 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 성과 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 인스턴스의 `ApplicationLoadBalancerErrorCount`와 같은 지표가 포함될 수 있습니다. 이는 워크로드가 온보딩되고 모니터링이 설정된 후에 시작됩니다.

AWS 사고 탐지 및 대응에 대한 관찰성 구현

관찰성은 한 가지 연습 또는 기간으로 완료할 수 없는 지속적인 프로세스이므로 AWS 사고 탐지 및 대응은 두 단계로 관찰성을 구현합니다.

- 온보딩 단계: 온보딩 중 관찰성은 애플리케이션의 비즈니스 성과가 저하되는 시점을 감지하는 데 중점을 둡니다. 이를 위해 온보딩 단계 중 관찰성은 애플리케이션 계층에서 주요 비즈니스 성과 지표를 정의하여 워크로드에 AWS 중단을 알리는 데 중점을 둡니다. 이렇게 하면 AWS가 이러한 중단에 즉시 대응할 수 있으며 복구에 도움이 될 수 있습니다. AWS 사고 탐지 및 대응 고객 명령줄 인터페이스

(CLI)를 사용하여 이러한 단계를 자동화하는 방법에 대한 자세한 내용은 AWS 사고 탐지 및 대응용 CLI를 참조하세요.

- 온보딩 후 단계: AWS 사고 탐지 및 대응은 인프라 수준 지표 정의, 지표 튜닝, 고객의 성숙도 수준에 따른 추적 및 로그 설정 등 관찰성을 위한 다양한 사전 예방 서비스를 제공합니다. 이러한 서비스의 구현은 몇 개월에 걸쳐 진행되며 여러 팀이 참여할 수 있습니다. AWS 사고 탐지 및 대응은 관찰성 설정에 대한 지침을 제공하며 고객은 워크로드 환경에서 필요한 변경 사항을 구현해야 합니다. 관찰성 기능의 실습 구현에 도움이 필요하면 기술 계정 관리자(TAM)에게 요청을 제출하세요.

사고 탐지 및 대응을 통한 인시던트 관리

AWS 사고 탐지 및 대응은 지정된 인시던트 관리자 팀이 제공하는 사전 모니터링 및 인시던트 관리를 하루 24시간, 주 7일 제공합니다. 다음 다이어그램은 애플리케이션 경보가 경보 생성, AWS Incident Manager 참여, 인시던트 해결 및 인시던트 사후 검토를 포함하여 인시던트를 트리거할 때의 표준 인시던트 관리 프로세스를 간략하게 설명합니다.

1. 경보 생성: 워크로드에서 트리거된 경보는 Amazon EventBridge를 통해 AWS 사고 탐지 및 대응으로 푸시됩니다. AWS 사고 탐지 및 대응은 경보와 연결된 런북을 자동으로 가져와 인시던트 관리자에게 알립니다. AWS 사고 탐지 및 대응에서 모니터링하는 경보로 감지되지 않는 중요한 인시던트가 워크로드에서 발생하는 경우, 지원 사례를 생성하여 인시던트 대응을 요청할 수 있습니다. 인시던트 대응 요청에 대한 자세한 내용은 인시던트 대응 요청 섹션을 참조하세요.
2. AWS Incident Manager 참여: 인시던트 관리자가 경보에 응답하고 회의 통화에 참여하거나 런북에 달리 지정된 대로 참여합니다. 인시던트 관리자는 AWS 서비스의 상태를 확인하여 경보가 워크로드에서 사용하는 AWS 서비스의 문제와 관련이 있는지 확인하고 기본 서비스의 상태에 대해 조언합니다. 필요한 경우 인시던트 관리자는 사용자를 대신하여 사례를 생성하고 지원을 위해 적절한 AWS 전문가를 참여시킵니다. AWS 사고 탐지 및 대응은 애플리케이션에 대해 AWS 서비스를 특별히 모니터링하므로 AWS 사고 탐지 및 대응은 AWS 서비스 이벤트가 선언되기 전에 인시던트가 AWS 서비스 문제와 관련이 있다고 판단할 수 있습니다. 이 시나리오에서 인시던트 관리자는 AWS 서비스의 상태를 알리고, AWS 서비스 이벤트 인시던트 관리 워크플로를 트리거하고, 해결 시 서비스 팀과 후속 조치를 취합니다. 제공된 정보를 통해 복구 계획 또는 해결 방법을 조기에 구현하여 AWS 서비스 이벤트의 영향을 완화할 수 있습니다.

   때때로 경보가 트리거되고 빠르게 복구됩니다. 이 시나리오에서 인시던트 관리자는 경보가 복구되었다는 내용의 사례 관련 서신을 보내지만, 사용자에게 연락하지는 않습니다. 그러나 경보가 15분 이내에 두 번 이상 트리거되면 경보가 복구되더라도 인시던트 관리자는 런북 지침에 따라 사용자에게 연락합니다.
3. 인시던트 해결: 인시던트 관리자는 필요한 AWS 팀 전체에서 인시던트를 조정하고 인시던트가 완화되거나 해결될 때까지 적절한 AWS 전문가와 계속 소통해야 합니다.
4. 인시던트 사후 검토(요청된 경우): 인시던트 후 AWS 사고 탐지 및 대응은 요청 시 인시던트 사후 검토를 수행하고 인시던트 사후 보고서를 생성할 수 있습니다. 인시던트 사후 보고서에는 문제에 대한 설명, 영향, 참여한 팀, 인시던트를 완화하거나 해결하기 위해 취한 해결 방법 또는 조치가 포함되어 있습니다. 인시던트 사후 보고서에는 인시던트 재발 가능성을 줄이거나 향후 유사한 인시던트 발생 관리를 개선하는 데 사용할 수 있는 정보가 포함될 수 있습니다. 인시던트 사후 보고서는 근본 원인

분석(RCA)이 아닙니다. 인시던트 사후 보고서 외에도 RCA를 요청할 수 있습니다. 인시던트 사후 보고서의 예는 다음 섹션에 나와 있습니다.

> **Important**
>
> 다음 보고서 템플릿은 단순 예시입니다.

```
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 ## support case on behalf of
 the customer.
  At 2023-02-04T03:32:00 UTC, ** the customer’s SRE team, and ## 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 팀의 AWS Support Center Console에 대한 액세스 권한 프로비저닝
- 인시던트 대응 요청
- AWS Support App in Slack을 사용하여 사고 탐지 및 대응 지원 사례 관리

애플리케이션 팀의 AWS Support Center Console에 대한 액세스 권한 프로비저닝

AWS 사고 탐지 및 대응은 인시던트의 수명 주기 동안 지원 사례를 통해 사용자와 통신합니다. 인시던트 관리자에 대응하려면 팀이 지원 센터에 액세스할 수 있어야 합니다.

액세스 프로비저닝에 대한 자세한 내용은 지원 사용 설명서의 지원 센터에 대한 액세스 관리를 참조하세요.

인시던트 대응 요청

AWS 사고 탐지 및 대응에서 모니터링하는 경보로 감지되지 않는 중요한 인시던트가 워크로드에서 발생하는 경우, 지원 사례를 생성하여 인시던트 대응을 요청할 수 있습니다. AWS Support Center Console, AWS Support API 또는 AWS Support App in Slack을 사용하여 온보딩 과정에서 워크로드를 포함하여 AWS 사고 탐지 및 대응을 구독하는 모든 워크로드에 대해 인시던트 대응을 요청할 수 있습니다.

다음 다이어그램은 사고 탐지 및 대응 팀에 인시던트 지원을 요청하는 AWS 고객을 위한 엔드 투 엔드 워크플로를 보여 주며, 초기 요청부터 조사, 완화 및 해결까지의 단계를 자세히 설명합니다.

워크로드에 적극적으로 영향을 미치는 인시던트에 대한 인시던트 대응을 요청하려면 지원 사례를 생성합니다. 지원 사례가 제기되면 AWS 사고 탐지 및 대응은 워크로드 복구를 가속화하는 데 필요한 AWS 전문가와의 회의 브리지에 참여합니다.

AWS Support Center Console을 사용하여 인시던트 대응 요청

사고 대응을 요청하려면 다음 단계를 완료합니다.

1. AWS Support Center Console을 열어 새 지원 사례를 생성합니다.
2. 제목에 인시던트에 대한 간략한 요약을 입력합니다. 예를 들어 `AWS Incident Detection and Response - Active Incident - workload_name`입니다.
3. 설명에 인시던트의 세부 정보를 입력합니다. 지원 사례에 다음 세부 정보를 포함하는 것이 좋습니다.
   - 영향을 받는 AWS 리소스 ARN, 워크로드 이름 및 해당 함수
   - 비즈니스에 미치는 영향에 대한 설명
   - (선택 사항) 선호하는 회의 브리지 URL. 브리지 세부 정보를 제공하지 않으면 AWS 사고 탐지 및 대응이 AWS 회의 브리지를 생성하고 브리지 URL이 포함된 초대를 보냅니다.
4. (선택 사항) 스크린샷 또는 로그 발췌문과 같이 인시던트를 설명하는 데 도움이 되는 파일을 첨부합니다.
5. 다음 사례 분류 필드를 구성합니다.
   - 사례 유형: 기술

- 서비스: 사고 탐지 및 대응
- 범주: 활성 인시던트
- 심각도: 비즈니스 크리티컬 시스템 중단

6. 영향을 받는 AWS 서비스, 영향을 받는 AWS 리전, 비즈니스 영향, 영향 시작 시간 및 영향을 받는 리소스 등 AWS 사고 탐지 및 대응이 AWS 전문가를 더 빠르게 참여시키는 데 도움이 되는 추가 컨텍스트를 제공합니다.
7. 제출을 선택합니다.
8. AWS 사고 탐지 및 대응은 5분 이내에 사례를 확인하고 적절한 AWS 전문가와의 회의 브리지에 참여합니다.

AWS Support API를 사용하여 인시던트 대응 요청

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

AWS Support App in Slack을 사용하여 인시던트 대응 요청

AWS Support App in Slack을 사용하여 인시던트 대응을 요청하려면 다음 단계를 완료합니다.

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

```
/awssupport create
```

3. 이 인시던트의 주제를 입력합니다. 예를 들어, AWS 사고 탐지 및 대응 - 활성 인시던트 - workload_name을 입력합니다.
4. 이 인시던트에 대한 문제 설명을 입력합니다. 다음의 세부 정보를 추가합니다.

   기술 정보:

   영향을 받는 서비스:

   영향을 받는 리소스:

   영향을 받는 리전:

워크로드 이름:

비즈니스 정보:

비즈니스에 미치는 영향에 대한 설명:

[선택 사항] Customer Bridge 세부 정보:

5. 다음을 선택합니다.

6. 문제 유형에서 기술 지원을 선택합니다.
7. 서비스에서 사고 탐지 및 대응을 선택합니다.
8. 범주에서 활성 인시던트를 선택합니다.
9. 심각도에서 비즈니스 크리티컬 시스템 중단을 선택합니다.

10. 선택적으로 알림을 보낼 추가 연락처 필드에 최대 10개의 추가 연락처를 쉼표로 구분하여 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 생성을 선택합니다.

13. 사례 ID는 AWS Support App in Slack의 새 메시지에 제공됩니다.
14. 사고 탐지 및 대응은 5분 이내에 사례를 확인하고 적절한 AWS 전문가와의 회의 브리지에 참여합니다.
15. 사례 스레드에서 사고 탐지 및 대응의 서신이 업데이트되었습니다.

AWS Support App in Slack을 사용하여 사고 탐지 및 대응 지원 사례 관리

AWS Support App in Slack을 사용하면 Slack에서 지원 사례를 관리하고, AWS 사고 탐지 및 대응 워크로드에서 새 경보 시작 인시던트에 대한 알림을 수신하고, 인시던트 대응 요청을 생성할 수 있습니다.

AWS Support App in Slack을 구성하려면 지원 사용 설명서에 제공된 지침을 따릅니다.

Important

- 워크로드에서 경보가 시작된 모든 인시던트에 대한 알림을 Slack에서 받으려면 AWS 사고 탐지 및 대응에 온보딩된 모든 워크로드 계정에 AWS Support App in Slack을 구성해야 합니다. 지원 사례는 워크로드 경보가 시작된 계정에 생성됩니다.
- 인시던트 발생 시 사용자를 대신하여 심각도가 높은 여러 지원 사례를 열어 지원 해석기를 참여시킬 수 있습니다. Slack 채널의 알림 구성과 일치하는 인시던트 중에 열린 모든 지원 사례에 대해 Slack에서 알림을 받습니다.
- AWS Support App in Slack을 통해 수신하는 알림은 인시던트 발생 시 AWS 사고 탐지 및 대응에서 이메일 또는 전화를 통해 참여하는 워크로드의 초기 및 에스컬레이션 연락처를 대체하지 않습니다.

주제

- Slack에서 경보 시작 인시던트 알림
- Slack에서 인시던트 대응 요청 생성

Slack에서 경보 시작 인시던트 알림

Slack 채널에서 AWS Support App in Slack을 구성하면 AWS 사고 탐지 및 대응 모니터링 워크로드에서 경보 시작 인시던트에 대한 알림을 받게 됩니다.

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

알림 예제:

AWS 사고 탐지 및 대응에서 경보 시작 인시던트를 승인하면 다음과 유사한 알림이 Slack에서 생성됩니다.

AWS 사고 탐지 및 대응에서 추가한 전체 서신을 보려면 세부 정보 보기를 선택합니다.

AWS 사고 탐지 및 대응의 추가 업데이트는 사례 스레드에 표시됩니다.

AWS 사고 탐지 및 대응에서 추가한 전체 서신을 보려면 세부 정보 보기를 선택합니다.

Slack에서 인시던트 대응 요청 생성

AWS Support App in Slack을 통해 인시던트 대응 요청을 생성하는 방법에 대한 지침은 인시던트 대응 요청 섹션을 참조하세요.

사고 탐지 및 대응 보고

AWS 사고 탐지 및 대응은 서비스가 구성된 방식, 인시던트 기록, 인시던트 감지 및 대응 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, 런북 및 지원 프로필

인시던트 데이터

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

성능 데이터

- 서비스 수준 목표(SLO) 성능

필요한 운영 및 성능 데이터는 기술 담당 계정 관리자에게 문의하세요.

사고 탐지 및 대응 보안 및 복원력

AWS 공동 책임 모델은 지원의 데이터 보호에 적용됩니다. 이 모델에서 설명하는 것처럼 AWS는 모든 AWS 클라우드를 실행하는 글로벌 인프라를 보호할 책임이 있습니다. 사용자는 인프라에서 호스팅되는 콘텐츠를 관리해야 합니다. 이 콘텐츠에는 사용하는 AWS 서비스 서비스의 보안 구성과 관리 작업이 포함되어 있습니다.

데이터 프라이버시에 대한 자세한 내용은 데이터 프라이버시 FAQ를 참조하세요.

유럽의 데이터 보호에 대한 자세한 내용은 AWS 보안 블로그에서 AWS 공동 책임 모델과 GDPR 블로그 게시물을 참조하세요.

데이터를 보호하려면 AWS 계정 보안 인증을 보호하고 AWS Identity and Access Management(IAM)을 사용해 개별 사용자 계정을 설정하는 것이 좋습니다. 이러한 방식에서는 각 사용자에게 자신의 직무를 충실히 이행하는 데 필요한 권한만 부여됩니다. 또한 다음과 같은 방법으로 데이터를 보호하는 것이 좋습니다.

- 각 계정에 다중 인증(MFA)을 사용합니다.
- 보안 소켓 계층/전송 계층 보안(SSL/TLS) 인증서를 사용하여 AWS 리소스와 통신합니다. TLS 1.2 이상을 권장합니다. 자세한 내용은 SSL/TLS 인증서란 무엇인가요?를 참조하세요.
- AWS CloudTrail으로 API 및 사용자 활동 로깅을 설정하세요. 자세한 내용은 AWS CloudTrail 섹션을 참조하세요.
- AWS 암호화 솔루션을 AWS 서비스내의 모든 기본 보안 컨트롤과 함께 사용하세요.
- Amazon S3에 저장된 개인 데이터를 검색하고 보호하는 데 도움이 되는 Amazon Macie와 같은 고급 관리형 보안 서비스를 사용합니다. Amazon Macie에 대한 자세한 내용은 Amazon Macie를 참조하세요.
- 명령행 인터페이스 또는 API를 통해 AWS에 액세스할 때 FIPS 140-2 검증된 암호화 모듈이 필요한 경우, FIPS 엔드포인트를 사용합니다. 사용 가능한 FIPS 엔드포인트에 대한 자세한 내용은 Federal Information Processing Standard(FIPS) 140-2를 참조하세요.

고객의 이메일 주소와 같은 기밀 정보나 중요한 정보는 태그나 이름 필드와 같은 자유 양식 필드에 입력하지 않는 것이 좋습니다. 여기에는 지원 또는 기타 AWS 서비스에서 콘솔, API, AWS CLI 또는 AWS SDK를 사용하여 작업하는 경우가 포함됩니다. 이름에 사용되는 태그 또는 자유 형식 필드에 입력하는 모든 데이터는 청구 또는 진단 로그에 사용될 수 있습니다. 외부 서버에 URL을 제공할 때 해당 서버에 대한 요청을 검증하기 위해 자격 증명 정보를 URL에 포함시켜서는 안됩니다.

계정에 대한 AWS 사고 탐지 및 대응 액세스

AWS Identity and Access Management(IAM)은 AWS 리소스에 대한 액세스를 안전하게 제어할 수 있는 웹 서비스입니다. IAM을 사용하여 리소스를 사용하도록 인증(로그인) 및 권한 부여(권한 있음)된 대상을 제어합니다.

AWS 사고 탐지 및 대응과 경보 데이터

기본적으로 사고 탐지 및 대응은 계정의 모든 CloudWatch 경보의 Amazon 리소스 이름(ARN)과 상태를 수신한 후 온보딩된 경보가 ALARM 상태로 변경될 때 인시던트 감지 및 대응 프로세스를 시작합니다. 계정에서 경보에 대해 사고 탐지 및 대응이 수신하는 정보를 사용자 지정하려면 기술 계정 관리자에게 문의하세요.

문서 이력

다음 표에서는 IDR 가이드의 최신 릴리스가 발표된 이후 이 설명서에서 변경된 중요 사항에 대해 설명합니다.

변경	설명	날짜
사고 대응 요청 절차 업데이트	현재 AWS Support Center Console UI와 일치하도록 사고 대응 요청 절차를 업데이트하고, 브리지 URL 지침을 추가하고, 오래된 스크린샷을 제거했습니다. 자세한 내용은 AWS Support Center Console을 사용하여 인시던트 대응 요청 섹션을 참조하세요.	2026년 5월 12일
CLI 우선 접근 방식으로 온보딩 업데이트	시작하기 장을 업데이트하여 AWS 사고 탐지 및 대응 고객 명령줄 인터페이스를 주요 온보딩 방법으로 권장하고, 워크로드 온보딩 설문지와 경보 수집 설문지를 기본 온보딩 경로에서 제외했습니다. IDR CLI를 사용할 수 없는 고객은 설문지를 예외 전용 옵션으로 계속 사용할 수 있습니다. 자세한 내용은 사고 탐지 및 대응에 워크로드 온보딩 및 경보 수집(을)를 참조하세요.	2026년 5월 12일
일본어 설문지 링크 추가	워크로드 온보딩 설문지 및 경보 수집 설문지에 일본어 다운로드 링크가 추가되었습니다. 자세한 내용은 사고 탐지 및 대응(예외 경로)에서의 워크로드 온보딩 및 경보 수집 설문지 섹션을 참조하세요.	2026년 4월 20일
업데이트된 아키텍처 참조	아키텍처 다이어그램에 대한 참조를 제거하고 아키텍처 세부 정보로 대체했습니다.	2026년 3월 31일

변경	설명	날짜
	자세한 내용은 사고 탐지 및 대응 아키텍처 및 사고 탐지 및 대응의 워크로드 정보(을)를 참조하세요.	
사고 탐지 및 대응에서 온보딩된 워크로드 테스트 업데이트	테스트 중 경보 상태를 변경하기 전에 CloudWatch 경보 작업을 비활성화하는 방법에 대한 정보가 추가되었습니다. 자세한 내용은 사고 탐지 및 대응에서 온보딩된 워크로드 테스트 섹션을 참조하세요.	2026년 3월 2일
사고 탐지 및 대응으로 인시던트 관리 업데이트	반복 경보 동작 및 인시던트 관리자 연락에 대한 정보가 추가되었습니다. 자세한 내용은 사고 탐지 및 대응을 통한 인시던트 관리 섹션을 참조하세요.	2026년 3월 2일
지표 수학 함수를 사용하여 CloudWatch 경보 억제 섹션의 단계 업데이트	지표 수학 함수를 사용하여 CloudWatch 경보 억제 섹션의 단계를 업데이트했습니다. 자세한 내용은 경보 소스에서 경보 억제 섹션을 참조하세요.	2026년 2월 3일
한국어를 지원되는 언어로 추가	한국어를 지원되는 언어로 추가했습니다. 자세한 내용은 사고 탐지 및 대응의 리전 가용성 섹션을 참조하세요.	2026년 1월 22일
표준 중국어를 지원되는 언어로 추가	표준 중국어를 지원되는 언어로 추가했습니다. 자세한 내용은 사고 탐지 및 대응의 리전 가용성 섹션을 참조하세요.	2026년 1월 13일

변경	설명	날짜
새 섹션 추가: AWS 사고 탐지 및 대응 고객 명령줄 인터페이스	IDR CLI 섹션을 추가하고 시작하기 장을 업데이트하여 AWS 사고 탐지 및 대응 고객 명령줄 인터페이스(IDR CLI)에 대한 정보를 포함했습니다. 자세한 내용은 AWS 사고 탐지 및 대응을 위한 CLI를 참조하세요.	2025년 12월 8일
여러 섹션 업데이트: 사고 탐지 및 대응의 워크로드 온보딩 및 경보 수집 설문지 및 사고 탐지 및 대응 시작하기	AWS 서비스 이벤트 처리 프로세스는 더 이상 AWS 사고 탐지 및 대응의 일부가 아닙니다. 이 프로세스에 대한 참조를 제거하도록 이 사용 설명서의 섹션이 업데이트되었습니다. AWS 서비스 상태 대시보드를 통해 서비스 이벤트 알림을 계속 받게 됩니다. AWS 사고 탐지 및 대응 고객은 인시던트 대응 요청을 사용하여 필요에 따라 서비스 이벤트 중에 도움을 받을 수 있습니다. 자세한 내용은 인시던트 대응 요청 섹션을 참조하세요.	2025년 10월 14일
삭제된 섹션: 서비스 이벤트에 대한 인시던트 관리	AWS 서비스 이벤트 처리 프로세스는 더 이상 AWS 사고 탐지 및 대응의 일부가 아닙니다. 이 변경 사항을 반영하기 위해 사용 설명서의 이 섹션이 제거되었습니다. AWS 서비스 상태 대시보드를 통해 서비스 이벤트 알림을 계속 받게 됩니다. AWS 사고 탐지 및 대응 고객은 인시던트 대응 요청을 사용하여 필요에 따라 서비스 이벤트 중에 도움을 받을 수 있습니다. 자세한 내용은 인시던트 대응 요청 섹션을 참조하세요.	2025년 10월 14일
섹션 업데이트: 사고 탐지 및 대응의 리전 가용성	이제 AWS GovCloud(미국 동부) 및 AWS GovCloud(미국 서부)에서 AWS 사고 탐지 및 대응을 사용할 수 있습니다. 자세한 내용은 사고 탐지 및 대응의 리전 가용성 섹션을 참조하세요.	2025년 10월 5일

변경	설명	날짜
섹션 업데이트: 사고 탐지 및 대응의 워크로드 온보딩 및 경보 수집 설문지	경보 매트릭스 테이블의 예제 이메일 주소를 업데이트했습니다.	2025년 8월 26일
섹션 업데이트: AWS 사고 탐지 및 대응을 위한 워크로드 구독	사례 생성 창의 설명 섹션에서 구독 시작 날짜 필드에 대한 참조를 제거했습니다. 섹션 업데이트: AWS 사고 탐지 및 대응을 위한 워크로드 구독	2025년 8월 4일
새 함수: 사고 탐지 및 대응과 관련된 경보 억제	일시적으로 또는 일정에 따라 경보를 억제하는 방법에 대한 정보를 제공하는 새 섹션을 관리형 워크로드에 추가했습니다. 새로운 섹션: 사고 탐지 및 대응과 관련된 경보 억제	2025년 4월 9일
AWS Support Center Console을 사용하여 인시던트 대응 요청에 대한 지침을 업데이트했습니다.	문제 설명 필드에 입력할 정보에 대한 세부 정보가 추가되었습니다. 섹션 업데이트: 인시던트 대응 요청	2025년 2월 6일
추가 AWS 리전 추가됨	사고 탐지 및 대응 가용성 섹션에 추가 AWS 리전이 추가되었습니다. 섹션 업데이트: 사고 탐지 및 대응의 리전 가용성	2024년 11월 1일
AWS Support App in Slack을 사용하여 사고 탐지 및 대응 지원 사례 관리 페이지 업데이트	인시던트 관리 아래의 페이지를 이동하고, 텍스트를 수정하고, 스크린샷을 대체했습니다. 섹션 업데이트: AWS Support App in Slack을 사용하여 사고 탐지 및 대응 지원 사례 관리	2024년 10월 10일

변경	설명	날짜
새 페이지 AWS Support App in Slack 추가 AWS 사고 탐지 및 대응으로 인시던트 관리 업데이트	AWS Support App in Slack에 대한 새 페이지 추가 AWS 사고 탐지 및 대응으로 인시던트 관리에서 새 섹션 'AWS Support App in Slack을 사용하여 인시던트 대응 요청'을 추가로 업데이트했습니다.	2024년 9월 10일
계정 구독 업데이트	계정 구독을 요청할 때 지원 사례를 개설할 위치에 대한 세부 정보를 포함하도록 계정 구독 섹션을 업데이트했습니다. 섹션 업데이트: AWS 사고 탐지 및 대응을 위한 워크로드 구독	2024년 6월 12일
새 섹션 추가: 워크로드 오프보딩	워크로드 오프보딩에 대한 정보를 포함하도록 시작하기에 워크로드 오프로드 섹션 추가 자세한 내용은 사고 탐지 및 대응에서 워크로드 오프보딩 섹션을 참조하세요.	2024년 3월 28일
계정 구독 업데이트	워크로드 오프보딩에 대한 정보를 포함하도록 계정 구독 섹션 업데이트 자세한 내용은 AWS 사고 탐지 및 대응에 대한 워크로드 구독을 참조하세요.	2024년 3월 28일
테스트 업데이트	온보딩 프로세스의 마지막 단계로 게임데이 테스트에 대한 정보를 포함하도록 테스트 섹션을 업데이트했습니다. 섹션 업데이트: 사고 탐지 및 대응에서 온보딩된 워크로드 테스트	2024년 2월 29일

변경	설명	날짜
AWS 사고 탐지 및 대응이란 무엇인가요 업데이트	AWS 사고 탐지 및 대응이란 무엇인가요 섹션을 업데이트했습니다. 섹션 업데이트: AWS 사고 탐지 및 대응이란 무엇인가요?	2024년 2월 19일
설문지 섹션 업데이트	워크로드 온보딩 설문지를 업데이트하고 경보 수집 설문지를 추가했습니다. 섹션의 이름을 온보딩 설문지에서 워크로드 온보딩 및 경보 수집 설문지로 변경했습니다.	2024년 2월 2일
AWS 서비스 이벤트 및 온보딩 정보 업데이트	온보딩을 위한 새로운 정보로 여러 섹션을 업데이트했습니다. 섹션 업데이트: • 사고 탐지 및 대응에 워크로드 온보딩 • AWS 사고 탐지 및 대응을 위한 워크로드 구독 새로운 섹션 • 애플리케이션 팀의 AWS Support Center Console에 대한 액세스 권한 프로비저닝	2024년 1월 31일
관련 정보 섹션 추가	액세스 프로비저닝에 관련 정보 섹션이 추가되었습니다. 섹션 업데이트: 사고 탐지 및 대응에 대한 경보 수집을 위한 액세스 권한 프로비저닝	2024년 1월 17일
예제 단계 업데이트	예제: Datadog 및 Splunk의 알림 통합의 2, 3 및 4단계 절차를 업데이트했습니다. 업데이트된 섹션: 예: Datadog 및 Splunk의 알림 통합	2023년 12월 21일

변경	설명	날짜
소개 그래픽 및 텍스트 업데이트	Amazon EventBridge와 직접 통합되는 APM에서 경보 수집에서 그래픽이 업데이트되었습니다. 섹션 업데이트: 사고 탐지 및 대응에서 인시던트에 대응하기 위한 런북 및 대응 계획 개발	2023년 12월 21일
런북 템플릿 업데이트	AWS 사고 탐지 및 대응을 위한 런북 개발의 런북 템플릿을 업데이트했습니다. 섹션 업데이트: 사고 탐지 및 대응에서 인시던트에 대응하기 위한 런북 및 대응 계획 개발	2023년 12월 4일
경보 구성 업데이트	CloudWatch 경보 구성에 대한 자세한 정보로 경보 구성을 업데이트했습니다. 새 섹션: 사고 탐지 및 대응에서 비즈니스 요구 사항에 맞는 CloudWatch 경보 생성 새 섹션: CloudFormation 템플릿을 사용하여 사고 탐지 및 대응에서 CloudWatch 경보 구축 새 섹션: 사고 탐지 및 대응의 CloudWatch 경보 예제 사용 사례	2023년 9월 28일
시작하기 업데이트	워크로드 변경 요청에 대한 시작하기 정보가 업데이트되었습니다. 새로운 섹션: 사고 탐지 및 대응에서 온보딩된 워크로드에 대한 변경 요청 섹션 업데이트: AWS 사고 탐지 및 대응을 위한 워크로드 구독	2023년 9월 5일
시작하기의 새 섹션	AWS 사고 탐지 및 대응에 알림 수집을 추가했습니다.	2023년 6월 30일

변경	설명	날짜
원본 문서	AWS 사고 탐지 및 대응이 처음 게시됨	2023년 3월 15일