AWS사고 탐지 및 대응 개념 및 절차

AWS사고 감지 및 대응 사용자 가이드

버전 July 3, 2024

AWS사고 감지 및 대응 사용자 가이드: AWS사고 탐지 및 대응 개념 및 절차

Table of Contents

AWS 사고 탐지 및 대응이란 무엇입니까?

AWS 사고 탐지 및 대응은 자격을 갖춘 AWS Enterprise Support 고객에게 사전 인시던트 참여를 제공하여 장애 가능성을 줄이고 중요한 워크로드의 장애 복구를 가속화합니다. 사고 탐지 및 대응을 통해 협업하여 각 온보드 워크로드에 맞게 사용자 AWS 지정된 런북 및 대응 계획을 개발할 수 있습니다. 사고 관리 엔지니어 (IME) 팀이 온보드 워크로드를 연중무휴로 모니터링하고 긴급 경보가 발생한 후 5분 이내에 콜 브리지에 연락합니다.

사고 탐지 및 대응은 다음과 같은 주요 기능을 제공합니다.

- 관찰 가능성 개선: AWS 전문가가 워크로드의 애플리케이션과 인프라 계층 간에 지표와 경보를 정의하고 상호 연관시켜 장애를 조기에 감지할 수 있도록 도와주는 지침을 제공합니다.
- 5분 응답 시간: IME는 온보드 워크로드를 연중무휴 모니터링하여 심각한 사고를 감지합니다. IME는 경보가 트리거된 후 5분 이내에 응답하거나 사용자가 사고 탐지 및 대응에 제기한 비즈니스 크리티컬 지원 사례에 응답합니다.
- 더 빠른 해결: IME는 워크로드용으로 개발된 사전 정의된 사용자 지정 런북을 사용하여 5분 이내에 대응하고, 사용자를 대신하여 Support 케이스를 생성하고, 워크로드에서 인시던트를 관리합니다. IME는 사고에 대한 단일 스레드 소유권을 제공하며 사고가 해결될 때까지 적합한 전문가와 계속 소통할 수 있습니다. AWS
- AWS 이벤트에 대한 인시던트 관리: 중요한 워크로드 (예: 계정, 서비스, 인스턴스) 의 컨텍스트를 이해하므로 서비스 이벤트 중에 워크로드에 미칠 수 있는 잠재적 영향을 감지하고 사전에 알릴 수 있습니다. AWS 요청 시 IME는 AWS 서비스 이벤트 기간 동안 사용자를 참여시키고 이벤트에 대한 업데이트를 제공합니다. 사고 탐지 및 대응은 서비스 이벤트 중에 복구 우선 순위를 정할 수는 없지만, 사고 탐지 및 대응은 완화 계획을 구현하는 데 도움이 되는 지원 지침을 제공합니다.
- 실패 가능성 감소: 문제 해결 후 IME는 사고 후 검토 (요청 시) 를 제공합니다. 또한 AWS 전문가가 고객과 협력하여 배운 교훈을 적용하여 사고 대응 계획 및 런북을 개선합니다. 또한 워크로드에 AWS Resilience Hub 대한 지속적인 복원력 추적을 위해 활용할 수 있습니다.

사고 탐지 및 대응 제품 용어

- AWS 사고 탐지 및 대응은 직속 및 파트너가 재판매한 Enterprise Support 계정에서 사용할 수 있습니다.
- AWS 사고 탐지 및 대응은 파트너 주도 Support 계정에서는 사용할 수 없습니다.

- 사고 탐지 및 대응 서비스 기간 동안 항상 AWS Enterprise Support를 유지해야 합니다. 자세한 내용은 기업 지원을 참조하십시오. Enterprise Support가 종료되면 AWS 사고 탐지 및 대응 서비스에서 동시에 제외됩니다.
- AWS 사고 탐지 및 대응의 모든 워크로드는 워크로드 온보딩 프로세스를 거쳐야 합니다.
- AWS 사고 탐지 및 대응 계정을 구독할 수 있는 최소 기간은 90일입니다. 모든 취소 요청은 예정된 취소 발효일로부터 30일 전에 제출해야 합니다.
- AWS AWS 개인 정보 보호 고지에 설명된 대로 정보를 처리합니다.

> **Note**
>
> 사고 감지 및 대응 청구 관련 질문은 AWS 청구 관련 도움 받기를 참조하십시오.

사고 탐지 및 대응 가능 여부

AWS 사고 탐지 및 대응은 현재 AWS 리전다음 중 하나에서 호스팅되는 Enterprise Support 계정에 대해 영어로 제공됩니다.

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)
sa-east-1	남아메리카(상파울루)
eu-central-1	유럽(프랑크푸르트)
eu-west-1	유럽(아일랜드)
eu-west-2	유럽(런던)

명칭	AWS 리전
eu-west-3	유럽(파리)
eu-north-1	유럽(스톡홀름)
ap-south-1	아시아 태평양(뭄바이)
ap-northeast-1	아시아 태평양(도쿄)
ap-northeast-2	아시아 태평양(서울)
ap-southeast-1	아시아 태평양(싱가포르)
ap-southeast-2	아시아 태평양(시드니)

AWS 인시던트 탐지 및 대응 RACI

다음 표에는 AWS 사고 탐지 및 대응에 대한 책임, 상담 및 정보 제공의 RACI가 나와 있습니다.

활동	고객	인시던트 탐지 및 대응
데이터 수집		
고객 및 워크로드 소개	C	R
아키텍처	R	A
운영	R	A
구성할 CloudWatch 알람을 결정합니다.	R	A
사고 대응 계획 정의	R	A
온보딩 설문지 작성	R	A
운영 준비 상태 검토		

활동	고객	인시던트 탐지 및 대응
워크로드에 대한 체계적인 검토 (WAR) 수행	C	R
인시던트 대응 검증	C	R
알람 매트릭스 검증	C	R
워크로드에서 사용 중인 주요 AWS 서비스를 식별하십시오.	A	R
계정 구성		
고객 계정에서 IAM 역할 생성	R	I
생성된 역할을 사용하여 관리형 EventBridge 규칙 설치	I	R
테스트 CloudWatch 알람	R	A
고객 경보가 사고 탐지 및 대응에 관여하는지 확인하십시오.	I	R
알람 업데이트	R	C
런북 업데이트	C	R
인시던트 관리		
사고 탐지 및 대응을 통해 탐지된 사고를 사전에 알립니다.	I	R
사고 대응 제공	I	R
사고 해결/인프라 복원 제공	R	C
인시던트 사후 검토		
사후 검토 요청	R	I
인시던트 사후 검토 제공	I	R

AWS 사고 탐지 및 대응 아키텍처

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

- Amazon EventBridge: EventBridge Amazon은 워크로드와 AWS 사고 탐지 및 대응 간의 유일한 통합 지점 역할을 합니다. 에서 관리하는 사전 정의된 규칙을 EventBridge 사용하여 Amazon과 같은 모니터링 도구에서 CloudWatch Amazon을 통해 경보를 수집합니다. AWS사고 탐지 및 대응이 EventBridge 규칙을 구축하고 관리할 수 있도록 하려면 서비스 연결 역할을 설치해야 합니다. 이러한 서비스에 대해 자세히 알아보려면 Amazon EventBridge 및 Amazon EventBridge 규칙이란?, CloudWatchAmazon이란? 및 서비스 연결 역할 사용을 참조하십시오. AWS Health
- AWS Health: 리소스 성능과 및 계정의 가용성에 대한 지속적인 가시성을 AWS Health 제공합니다. AWS 서비스 인시던트 탐지 및 AWS Health 대응은 워크로드에서 AWS 서비스 사용되는 이벤트를 추적하고 워크로드로부터 경고가 수신되면 이를 알리는 데 사용됩니다. 자세히 알아보려면 AWS Health Whatis를 참조하십시오. AWS Health
- 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 해당 인시던트 관리 런북을 비롯한 워크로드에 대한 정보를 문서에 호스팅합니다 (자세한 내용은 AWS Systems Manager 문서 참조).AWS Systems Manager 자세히 AWS Systems Manager알아보려면 Whatis를 참조하십시오. AWS Systems Manager
- 특정 런북: 인시던트 관리 런북은 AWS 인시던트 탐지 및 대응이 인시던트 관리 중에 수행하는 작업을 정의합니다. 특정 런북에는 AWS 사고 탐지 및 대응 부서에 누구에게 연락해야 하는지, 어떻게 연락해야 하는지, 어떤 정보를 공유해야 하는지 나와 있습니다.

AWS사고 탐지 및 대응 시작하기

사고 탐지 및 대응을 사용하여 모니터링 및 중요 사고 관리에 사용할 AWS 특정 워크로드를 선택할 수 있습니다. 워크로드는 비즈니스 가치를 제공하기 위해 함께 작동하는 리소스와 코드의 모음입니다. 워크로드는 은행 결제 포털 또는 고객 관계 관리 (CRM) 시스템을 구성하는 모든 리소스와 코드일 수 있습니다. 워크로드를 한 곳에서 호스팅할 수 있습니다. AWS 계정 또는 여러 계정 AWS 계정.

예를 들어 단일 계정에서 모놀리식 애플리케이션을 호스팅할 수 있습니다 (예: 그림 1의 직원 성과 앱). 또는 애플리케이션 (예: 그림 1의 Storefront Webapp) 이 여러 계정에 걸쳐 확장되는 마이크로서비스로 분할되어 있을 수 있습니다. 워크로드는 그림 1과 같이 데이터베이스와 같은 리소스를 다른 애플리케이션 또는 워크로드와 공유할 수 있습니다.

> **Note**
>
> AWS인시던트 탐지 및 대응에서 모니터링되는 런북, 워크로드 정보 또는 경보를 변경하려면 를 생성하십시오. 온보드 워크로드 변경 요청

온보딩

AWS 고객과 협력하여 워크로드 및 경보를 AWS 사고 탐지 및 대응에 온보딩합니다. 주요 정보를 다음 주소에 제공합니다. AWS 워크로드 온보딩 및 알람 수집 설문지. 워크로드도 등록하는 것이 가장 좋습니다. AppRegistry 자세한 내용은 AppRegistry 사용 설명서를 참조하십시오.

다음 다이어그램은 사고 감지 및 대응의 워크로드 온보딩 및 경보 수집 흐름을 보여줍니다.

워크로드 온보딩

워크로드 온보딩 중에 AWS 고객과 협력하여 워크로드를 이해하고 사고 발생 시 지원 방법을 파악합니다. AWS 서비스 이벤트. 영향 완화에 도움이 되는 워크로드에 대한 주요 정보를 제공합니다.

주요 결과:

- 일반 워크로드 정보
- 다이어그램을 포함한 아키텍처 세부 정보

- 런북 정보
- 고객이 시작한 사고
- AWS 서비스 이벤트

알람 수집

AWS 사용자와 협력하여 알람을 온보딩합니다. AWS사고 탐지 및 대응은 Amazon을 통해 Amazon CloudWatch 및 타사 애플리케이션 성능 모니터링 (APM) 도구에서 경보를 수집할 수 있습니다. EventBridge 온보딩 알람을 사용하면 사전 예방적 사고 탐지와 자동화된 개입이 가능합니다. 자세한 내용은 Amazon과 직접 APMs 통합되는 Ingest 경보를 참조하십시오. EventBridge

주요 결과:

- 알람 매트릭스

다음 표에는 AWS 사고 탐지 및 대응에 워크로드를 온보딩하는 데 필요한 단계가 나와 있습니다. 이 표에는 각 작업의 예제 기간이 나와 있습니다. 각 작업의 실제 날짜는 팀의 가용성과 일정에 따라 정의됩니다.

계정 구독

워크로드를 AWS 사고 탐지 및 대응에 구독하려면 각 워크로드에 대한 새 지원 사례를 생성하십시오. 지원 사례를 만들 때는 다음 사항을 염두에 두세요.

- 단일 워크로드를 온보딩하려면 AWS 계정에서 워크로드 계정이나 지급인 계정에서 지원 사례를 생성하세요.
- 여러 곳에 걸친 워크로드를 온보딩하려면 AWS 계정에서 지급인 계정에서 지원 사례를 생성하세요. 지원 사례 본문에 IDs 온보딩할 모든 계정을 나열하십시오.

> **Important**
>
> 잘못된 계정에서 인시던트 탐지 및 대응에 워크로드를 구독하는 지원 사례를 생성하면 워크로드를 구독하기 전에 지연이 발생하고 추가 정보 요청이 요청될 수 있습니다.

워크로드를 구독하려면

1. 로 이동 AWS Support센터로 이동한 다음 다음 예와 같이 사례 만들기를 선택합니다. Enterprise Support에 등록된 계정의 워크로드만 구독할 수 있습니다.

2. 지원 사례 양식 작성:

   - 기술 지원을 선택합니다.
   - 서비스에서 사고 탐지 및 대응을 선택합니다.
   - 카테고리에서 새 워크로드 온보드를 선택합니다.
   - 심각도에서는 일반 지침을 선택합니다.

3. 이 변경의 제목을 입력합니다. 예:

   [온보드] AWS 사고 탐지 및 대응 - *workload_name*

4. 이 변경에 대한 설명을 입력합니다. 예를 들어 “이 요청은 AWS 사고 탐지 및 대응에 워크로드를 온보딩하기 위한 요청입니다”라고 입력합니다. 요청에 다음 정보를 포함해야 합니다.

   - 워크로드 이름: 워크로드 이름.
   - 계정 ID: ID1ID2,ID3, 등. AWS사고 탐지 및 대응에 온보딩하려는 계정은 다음과 같습니다.
   - 구독 시작 날짜: AWS 사고 탐지 및 대응 구독을 시작하려는 날짜입니다.

5. 추가 연락처 - 선택 섹션에서 이 요청에 대한 서신을 받고 싶은 이메일을 IDs 입력합니다.

   다음은 추가 연락처 - 선택 섹션의 예입니다.

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

6. 제출을 선택합니다.

   요청을 제출한 후 조직에서 보내는 이메일을 더 추가할 수 있습니다. 이메일을 추가하려면 사례에 회신한 다음 추가 연락처 - 선택 IDs 섹션에 이메일을 추가합니다.

   다음은 추가 연락처 - 선택 섹션의 예입니다.

서브스크립션 요청에 대한 지원 사례를 생성한 후에는 워크로드 온보딩 프로세스를 진행할 수 있도록 다음 두 문서를 준비해 두십시오.

- AWS 워크로드 아키텍처 다이어그램.
- 워크로드 온보딩 및 알람 수집 설문지: 온보딩 중인 워크로드와 관련된 모든 정보를 설문지에 작성하세요. 온보딩해야 할 워크로드가 여러 개 있는 경우 각 워크로드에 대해 새 온보딩 설문지를 만드세요. 온보딩 설문지 작성과 관련하여 질문이 있는 경우 기술 계정 관리자 () 에게 문의하십시오. TAM

> **Note**
>
> 파일 NOT 첨부 옵션을 사용하여 이 두 문서를 케이스에 첨부하십시오. AWS사고 감지 및 대응 팀에서 문서를 업로드할 수 있는 Amazon 심플 스토리지 서비스 업로더 링크를 통해 사례에 답변해 드립니다.

기존 온보드 워크로드에 대한 요청 변경을 위해 AWS 사고 탐지 및 대응을 사용하여 사례를 생성하는 방법에 대한 자세한 내용은 을 참조하십시오. 온보드 워크로드 변경 요청 워크로드를 오프보딩하는 방법에 대한 자세한 내용은 을 참조하십시오. 워크로드 오프보딩

워크로드 검색

AWS 사용자와 협력하여 워크로드에 대한 컨텍스트를 최대한 많이 이해합니다. AWS인시던트 탐지 및 대응은 이 정보를 사용하여 인시던트 발생 시 지원을 위한 런북을 생성합니다. AWS 서비스 이벤트. 필수 정보는 에 캡처되어 워크로드 온보딩 및 알람 수집 설문지 있습니다. 워크로드를 등록하는 것이 가장 좋습니다. AppRegistry 자세한 내용은 AppRegistry 사용 설명서를 참조하십시오.

주요 결과:

- 워크로드 설명, 아키텍처 다이어그램, 연락처, 에스컬레이션 세부 정보와 같은 워크로드 정보
- 워크로드 사용 방식에 대한 세부 정보 AWS 각각의 서비스 AWS 리전.
- 방법에 대한 구체적인 정보 AWS 서비스 이벤트 기간 동안 여러분을 지원합니다.
- 팀에서 중요한 워크로드 영향을 감지하는 데 사용하는 경보입니다.

알람 구성

AWS 사용자와 협력하여 지표와 경보를 정의하여 애플리케이션 및 기본 성능의 가시성을 제공합니다. AWS 인프라. 임계값을 정의하고 구성할 때는 경보가 다음 기준을 준수해 주시기 바랍니다.

- 경보는 모니터링된 워크로드에 즉각적인 운영자의 주의가 필요한 중대한 영향 (수익 손실 또는 성능을 크게 저하시키는 고객 경험 저하) 이 있는 경우에만 “경보” 상태로 전환됩니다.
- 또한 알람은 사고 관리 팀과 협의하는 동시에 또는 그 전에 워크로드에 대해 지정된 해결 담당자를 참여시켜야 합니다. 사고 관리 엔지니어는 1차 대응 역할을 한 다음 사용자에게 에스컬레이션하는 것이 아니라 완화 프로세스에서 지정된 해결 담당자와 협력해야 합니다.
- 경보 임계값을 적절한 임계값 및 기간으로 설정하여 경보가 울릴 때마다 조사가 진행되도록 해야 합니다. 경보가 “경보” 상태와 “정상” 상태 사이에서 펄럭이는 경우 운영자의 대응과 주의를 기울여야 할 만큼 충분한 영향이 발생한 것입니다.

알람 유형:

- 비즈니스에 미치는 영향의 수준을 나타내고 간단한 장애 탐지를 위해 관련 정보를 전달하는 경보.
- 아마존 CloudWatch 카나리아. 자세한 내용은 카나리아 및 X-Ray 추적 및 X-Ray를 참조하십시오.
- 종합 경보 (종속성 모니터링)

알람 예시, 모두 모니터링 시스템 사용 CloudWatch

지표 이름/경보 임계값	알람 ARN 또는 리소스 ID	이 경보가 발생하는 경우	참여한다면 해당 서비스에 대한 Premium Support 케이스를 제출하십시오.
API오류/ 데이터 포인트 10개에 대한 오류 수 >= 10	arn:aws:cloudwatch:us-west- 2:0000000 0000000:alarm:E2 - 오류 MPmimLambda	데이터베이스 관리자 () 팀	API람다, 게이트웨이

지표 이름/경보 임계값	알람 ARN 또는 리소스 ID	이 경보가 발생하는 경우	참여한다면 해당 서비스에 대한 Premium Support 케이스를 제출하십시오.
		입장권 인하 DBA	
ServiceUnavailable (HTTP 상태 코드 503) 5분 동안 10개 데이터 포인트 (다른 클라이언트) 에 대한 오류 수 >=3	arn:aws:cloudwatch:us-west-2:xxxxx:alarm:httperrorcode503	서비스 팀 입장권 인하	API람다, 게이트웨이
ThrottlingException (HTTP 상태 코드 400) 5분 동안 10개 데이터 포인트 (다른 클라이언트) 에 대한 오류 수 >=3	arn:aws:cloudwatch:us-west-2:xxxxx:alarm:httperrorcode400	서비스 팀 입장권 인하	EC2, 아마존 Aurora

자세한 내용은 AWS 사고 탐지 및 대응 모니터링 및 관찰 가능성를 참조하세요.

주요 출력:

- 워크로드에 대한 경보의 정의 및 구성
- 온보딩 설문지의 알람 세부 정보 작성.

사고 탐지 및 대응에서 비즈니스 요구 사항에 맞는 CloudWatch 경보를 생성하십시오.

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

제안된 경보를 검토하십시오. CloudWatch

제안된 경보를 검토하여 모니터링된 워크로드에 중대한 영향 (수익 손실 또는 성능이 크게 저하되는 고객 경험 저하) 이 발생할 때만 경보가 “경보” 상태로 전환되도록 하십시오. 예를 들어, 이 경보가 “경보” 상태가 되면 즉시 대응해야 할 정도로 중요하다고 생각하십니까?

다음은 최종 사용자의 애플리케이션 사용 환경에 미치는 영향 등 비즈니스에 중대한 영향을 미칠 수 있는 권장 지표입니다.

- CloudFront: 자세한 내용은 보기 CloudFront 및 에지 함수 지표를 참조하십시오.
- 애플리케이션 로드 밸런서: 가능하면 애플리케이션 로드 밸런서에 대해 다음과 같은 경보를 생성하는 것이 가장 좋습니다.
  - HTTPCodeELB_ _5xx_count
  - HTTPCode_타겟_5xx_개수

  위의 경보를 사용하면 Application Load Balancer 뒤에 있거나 다른 리소스 뒤에 있는 대상의 응답을 모니터링할 수 있습니다. 이렇게 하면 5XX 오류의 원인을 더 쉽게 식별할 수 있습니다. 자세한 내용은 Application Load Balancer의 CloudWatch 지표를 참조하십시오.
- Amazon API Gateway: Elastic WebSocket API Beanstalk에서 사용하는 경우 다음 측정치를 사용해 보십시오.
  - 통합 오류율 (5XX 오류로 필터링)
  - 통합 레이턴시
  - 실행 오류

  자세한 내용은 CloudWatch 지표를 사용한 WebSocket API 실행 모니터링을 참조하십시오.
- Amazon Route 53: EndPointUnhealthyENICount메트릭을 모니터링합니다. 이 지표는 자동 복구 상태에 있는 엘라스틱 네트워크 인터페이스의 수입니다. 이 상태는 확인자가 엔드포인트와 연결된 하나 이상의 Amazon Virtual Private Cloud 네트워크 인터페이스 (지정) 를 복구하려는 시도를 나타냅니다. EndpointId 복구 프로세스에서 엔드포인트는 제한된 용량으로 작동합니다. 엔드포인트는 완전히 복구될 때까지 DNS 쿼리를 처리할 수 없습니다. 자세한 내용은 Amazon을 통한 Route 53 리졸버 엔드포인트 모니터링을 참조하십시오. CloudWatch

경보 구성을 검증하십시오.

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

- 지표의 임계값을 검증하여 지표의 그래프 추세를 기준으로 “경보” 상태를 입력합니다.
- 데이터 포인트를 폴링하는 데 사용된 기간을 확인합니다. 60초 간격의 폴링 데이터 포인트는 사고를 조기에 감지하는 데 도움이 됩니다.
- DatapointToAlarm구성을 검증하십시오. 대부분의 경우 이 값을 3점 만점에 3점 또는 5점 만점에 5점으로 설정하는 것이 좋습니다. 인시던트에서 [3점 만점에 60초 지표] 로 설정하면 3분 후, [5점 만점에 60초 지표 DatapointToAlarm] 로 설정하면 5분 후에 경보가 트리거됩니다. DatapointToAlarm 이 조합을 사용하면 시끄러운 알람을 제거할 수 있습니다.

> **Note**
>
> 위의 권장 사항은 서비스 사용 방식에 따라 달라질 수 있습니다. 각 AWS 서비스는 워크로드 내에서 다르게 작동합니다. 또한 동일한 서비스를 여러 곳에서 사용할 경우 다르게 작동할 수 있습니다. 워크로드가 경보를 제공하는 리소스를 어떻게 활용하는지와 업스트림 및 다운스트림 효과를 이해해야 합니다.

경보가 누락된 데이터를 처리하는 방법을 검증하십시오.

일부 지표 소스는 일정한 CloudWatch 간격으로 데이터를 전송하지 않습니다. 이러한 지표의 경우 누락된 데이터를 다음과 같이 처리하는 것이 가장 좋습니다 notBreaching. 자세한 내용은 경보가 누락된 데이터를 처리하는 방법 구성 및 CloudWatch 경보 상태로의 조기 전환 방지를 참조하십시오.

예를 들어 지표가 오류율을 모니터링하고 오류가 없는 경우 지표는 데이터 (nil) 데이터 요소를 보고하지 않습니다. 누락된 데이터를 누락으로 처리하도록 경보를 구성한 경우, 단일 침해 데이터 요소 다음에 데이터 없음 (nil) 데이터 지점 두 개가 이어지면 지표가 “경보” 상태로 전환됩니다 (3개 데이터 요소 중 3개). 이는 누락된 데이터 구성이 평가 기간 중 마지막으로 알려진 데이터 포인트를 평가하기 때문입니다.

지표에서 오류율을 모니터링하는 경우 서비스 성능 저하가 없다면 데이터가 없는 것은 좋은 일이라고 생각할 수 있습니다. 누락된 데이터를 “정상”으로 처리하고 지표가 단일 데이터 포인트에서 “경보” 상태로 전환되지 notBreaching않도록 누락된 데이터를 처리하는 것이 가장 좋습니다.

각 경보의 기록을 검토하십시오.

알람 기록에서 자주 “알람” 상태로 전환되었다가 빠르게 복구되는 것으로 나타나는 경우 알람이 문제가 될 수 있습니다. 잡음이나 잘못된 경보를 방지하려면 알람을 조정해야 합니다.

기본 리소스에 대한 메트릭을 검증하십시오.

지표가 유효한 기본 리소스를 기준으로 하고 올바른 통계를 사용하는지 확인하세요. 잘못된 리소스 이름을 검토하도록 경보를 구성한 경우 경보가 기본 데이터를 추적하지 못할 수 있습니다. 이로 인해 경보가 “Alarm” 상태가 될 수 있습니다.

복합 알람 생성

온보딩을 위해 많은 수의 경보가 포함된 사고 탐지 및 대응 작업을 제공하는 경우 복합 경보를 생성하라는 메시지가 표시될 수 있습니다. 복합 경보를 사용하면 온보딩해야 하는 총 경보 수를 줄일 수 있습니다.

사용 AWS CloudFormation 사고 탐지 및 대응에서 CloudWatch 경보를 구축하기 위한 템플릿

AWS사고 탐지 및 대응에 대한 온보딩을 가속화하고 경보 구축에 필요한 노력을 줄이려면 AWS 다음을 제공합니다. AWS CloudFormation 템플릿. 이러한 템플릿에는 Application Load Balancer, Network Load Balancer, Amazon 등 일반적으로 온보딩되는 서비스를 위한 최적화된 경보 설정이 포함되어 있습니다. CloudFront

템플릿으로 경보를 구축하십시오. CloudWatch CloudFormation

1. 제공된 링크를 사용하여 템플릿을 다운로드하세요.

NameSpac	지표	Compariso nOperator (임계값)	기간	Datapoint sToAlarm	TreatMiss ingData	통계	템플릿 링크
애플리케 이션 엘 라스틱 로드 밸 런서	(m1+m2)/ (m1+m2+m m4) *100 m1= _타	LessThanT hreshold(95)	60	3점 만점 에 3점	누락되었 습니다	Sum	템플릿

NameSpac	지표	Compariso nOperator (임계값)	기간	Datapoint sToAlarm	TreatMiss ingData	통계	템플릿 링크
	겟_2xx_c ount m2= _Target_3 xx_count m3= _Target_4 xx_count m4= _Target_5 xx_count HTTPCode HTTPCode HTTPCode HTTPCode						
아마존 CloudFron t	TotalErro rRate	GreaterTh anThresho ld(5)	60	3점 만점에 3점	notBreach ing	평균	템플릿
애플리케 이션 엘 라스틱 로드 밸 런서	UnHealthy HostCount	GreaterTh anOrEqual ToThresho ld(2)	60	3점 만점에 3점	notBreach ing	Maximum	템플릿
네트워크 엘라스틱 로드 밸 런서	UnHealthy HostCount	GreaterTh anOrEqual ToThresho ld(2)	60	3점 만점에 3점	notBreach ing	Maximum	템플릿

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

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

a. 열기 AWS CloudFormation https://console.aws.amazon.com/cloudformation에서 콘솔을 실행하세요.

b. 스택 생성을 선택합니다.

c. 템플릿이 준비되었습니다를 선택한 다음 로컬 폴더에서 템플릿 파일을 업로드합니다.

   다음은 스택 생성 화면의 예입니다.

d. Next(다음)를 선택합니다.

e. 다음 필수 정보를 입력합니다.

   - AlarmNameConfig및 AlarmDescriptionConfig: 알람의 이름과 설명을 입력합니다.
   - ThresholdConfig: 애플리케이션 요구 사항에 맞게 임계값을 수정하십시오.
   - D istributionIDConfig: 배포 ID가 생성하려는 계정의 올바른 리소스를 가리키는지 확인하세요. AWS CloudFormation 겹쳐 쓰세요.

f. Next(다음)를 선택합니다.

g. PeriodConfigEvalutionPeriodConfig, 및 DatapointsToAlarmConfig필드의 기본값을 검토하십시오. 이러한 필드에 기본값을 사용하는 것이 가장 좋습니다. 필요한 경우 애플리케이션 요구 사항에 맞게 조정할 수 있습니다.

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

i. Next(다음)를 선택합니다.

j. 스택 설정을 검토한 다음 스택 생성을 선택합니다.

k. 스택을 생성하면 다음 예와 같이 Amazon CloudWatch Alarm 목록에 경보가 나열됩니다.

4. 알맞은 계정에 모든 알람을 생성한 후 AWS 지역, 기술 계정 관리자 (TAM) 에게 알리십시오. AWS 사고 탐지 및 대응 팀은 새 경보의 상태를 검토한 다음 온보딩을 계속합니다.

사고 탐지 및 대응에서의 CloudWatch 경보 사용 사례 예시

다음 사용 사례를 검토하여 사고 탐지 및 대응에서 Amazon CloudWatch 경보를 사용하는 방법에 대한 예를 확인하십시오.

예제 사용 사례 A: 애플리케이션 로드 밸런서

워크로드에 미칠 수 있는 CloudWatch 영향을 알리는 다음 경보를 생성하십시오. 성공적인 연결이 특정 임계값 아래로 떨어질 때 경보를 표시하는 지표 계산을 만들 수 있습니다. 사용 가능한 CloudWatch 지표는 Application Load Balancer의 CloudWatch 지표를 참조하십시오.

지표: `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/애플리케이션 ELB

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

기간: 60초

DatapointsToAlarm: 3점 만점에 3점

누락된 데이터 처리: 누락된 데이터를 침해로 취급합니다.

통계: Sum

다음 다이어그램은 사용 사례 A의 흐름을 보여줍니다.

사용 사례 B 예시: 아마존 API 게이트웨이

잠재적인 워크로드 영향을 CloudWatch 알려주는 다음 경보를 생성하십시오. 게이트웨이에 지연 시간이 길거나 평균 4XX 오류 수가 많을 때 경보를 울리는 복합 지표를 만들 수 있습니다. API 사용 가능한 지표는 Amazon API Gateway 차원 및 지표를 참조하십시오.

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

NameSpace: AWS/API게이트웨이

ComparisonOperator(임계값): (x 또는 y 고객 임계값) 초과

기간: 60초

DatapointsToAlarm: 1점 만점에 1점

누락된 데이터 처리: 누락된 데이터를 위반이 아닌 것으로 취급합니다.

통계:

다음 다이어그램은 사용 사례 B의 흐름을 보여줍니다.

사용 사례 C 예시: 아마존 루트 53

원시 데이터를 수집하여 읽을 수 있는 거의 실시간 지표로 처리하는 CloudWatch 데 사용하는 Route 53 상태 확인을 생성하여 리소스를 모니터링할 수 있습니다. 잠재적인 워크로드 영향을 알리는 다음과 같은 CloudWatch 경보를 생성할 수 있습니다. CloudWatch 지표를 사용하여 설정된 임계값을 위반할 때 트리거되는 경보를 만들 수 있습니다. 사용 가능한 CloudWatch 지표는 Route 53 상태 확인 CloudWatch 지표를 참조하십시오.

지표: `R53-HC-Success`

NameSpace: AWS/53번 국도

임계값 HealthCheckStatus: 3분 이내 데이터 포인트 3개에 대해 x HealthCheckStatus 미만 (고객 임계값 x)

기간: 1분

DatapointsToAlarm: 3점 만점에 3점

누락된 데이터 처리: 누락된 데이터를 침해로 취급합니다.

통계: Minimum

다음 다이어그램은 사용 사례 C의 흐름을 보여줍니다.

예제 사용 사례 D: 사용자 지정 앱으로 워크로드 모니터링

이 시나리오에서는 시간을 들여 적절한 상태 점검을 정의하는 것이 중요합니다. 애플리케이션의 포트가 열려 있는지만 확인한다면 애플리케이션이 작동하는지 확인하지 못한 것입니다. 또한 응용 프로그램의 홈 페이지에 전화를 거는 것이 반드시 응용 프로그램의 작동 여부를 판단하는 올바른 방법은 아닙니다. 예를 들어, 애플리케이션이 AND Amazon Simple Storage Service 데이터베이스를 사용하는 경우 상태 점검을 통해 모든 요소를 검증해야 합니다. 이를 위한 한 가지 방법은 모니터링 웹 페이지 (예: /monitor) 를 만드는 것입니다. 모니터링 웹 페이지에서는 데이터베이스를 호출하여 데이터베이스에 연결하여 데이터를 가져올 수 있는지 확인합니다. 그리고 모니터링 웹 페이지에서 Amazon S3를 호출합니다. 그런 다음 로드 밸런서의 상태 점검이 /monitor 페이지를 가리키도록 합니다.

다음 다이어그램은 사용 사례 D의 흐름을 보여줍니다.

알림을 AWS 사고 탐지 및 대응에 수집

AWS사고 탐지 및 대응은 Amazon을 통한 경보 수집을 지원합니다. EventBridge 이 섹션에서는 Amazon과 직접 APMs 통합하지 않고 Amazon (예: New RelicAPM) 과 직접 통합하면서 Amazon CloudWatch (예: New Relic) APMs 과 직접 통합하면서 AWS 사고 탐지 DataDog 및 대응을 Amazon 을 비롯한 다양한 애플리케이션 성능 모니터링 EventBridge () 도구와 통합하는 방법을 설명합니다. EventBridge Amazon에 직접 통합되는 전체 목록은 APMs Amazon EventBridge 통합을 참조하십시오 EventBridge.

주제

- 사고 탐지 및 대응에 대한 알림 수집을 위한 액세스를 제공합니다.
- 사고 탐지 및 대응을 Amazon과 통합 CloudWatch
- Amazon과 직접 APMs 통합되는 알람 수집 EventBridge
- 예: Datadog와 Splunk의 알림 통합
- Amazon과 직접 APMs 통합하지 않고도 Webhook을 사용하여 경보를 수집할 수 있습니다. EventBridge

사고 탐지 및 대응에 대한 알림 수집을 위한 액세스를 제공합니다.

AWS인시던트 탐지 및 대응이 계정에서 경보를 수집할 수 있도록 하려면 `AWSServiceRoleForHealth_EventProcessor` 서비스 연결 역할 () 을 설치하십시오. SLR AWS 에서는 Amazon EventBridge 관리 SLR 규칙을 생성한다고 가정합니다. 관리형 규칙은 사용자 계정

의 알림을 AWS 사고 탐지 및 대응으로 보냅니다. 관련 정보를 SLR 포함하여 이에 대한 자세한 내용은 AWS 관리형 정책은 의 서비스 연결 역할 사용을 참조하십시오. AWS Health 사용 설명서.

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

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

주요 출력

- 계정에 서비스 연결 역할이 성공적으로 설치되었습니다.

관련 정보

자세한 정보는 다음 주제를 참조하세요.

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

사고 탐지 및 대응을 Amazon과 통합 CloudWatch

AWS인시던트 탐지 및 대응은 액세스 프로비저닝 중에 설정한 서비스 연결 역할 (SLR) 을 사용하여 Amazon EventBridge 관리 규칙을 생성합니다. AWS 계정 이름. `AWSHealthEventProcessor-DO-NOT-DELETE` 사고 탐지 및 대응은 이 규칙을 사용하여 사용자 계정에서 Amazon CloudWatch 경보를 수집합니다. 에서 경보를 수집하기 위한 추가 단계는 필요하지 않습니다. CloudWatch

Amazon과 직접 APMs 통합되는 알람 수집 EventBridge

다음 그림은 Datadog 및 Splunk와 같이 EventBridge Amazon과 직접 통합된 애플리케이션 성능 모니터링 (APM) 도구에서 AWS 사고 탐지 및 대응으로 알림을 보내는 프로세스를 보여줍니다. 와 EventBridge 직접 APMs 통합되는 전체 목록은 Amazon EventBridge 통합을 참조하십시오.

다음 단계를 사용하여 AWS 사고 탐지 및 대응과의 통합을 설정하십시오. 이 단계를 수행하기 전에 다음을 확인하십시오. AWS 서비스 연결 역할 (SLR) `AWSServiceRoleForHealth_EventProcessor` 이 계정에 설치되어 있습니다.

AWS사고 탐지 및 대응과의 통합 설정

각 단계에 대해 다음 단계를 완료해야 합니다. AWS 계정 및 AWS 리전. 알림은 다음 주소에서 와야 합니다. AWS 계정 및 AWS 애플리케이션 리소스가 있는 지역.

1. Amazon EventBridge 파트너 이벤트 소스를 각각 설정합니다 (예:`aws.partner/my_apm/integrationName`). APMs Y를 이벤트 소스로 설정하는 APM 방법에 대한 지침은 Amazon의 SaaS 파트너로부터 이벤트 수신을 참조하십시오. EventBridge 그러면 계정에 파트너 이벤트 버스가 생성됩니다.
2. 다음 중 하나를 수행합니다.
   - (권장 방법) 커스텀 EventBridge 이벤트 버스를 만드세요. AWS인시던트 탐지 및 대응은 를 통해 관리형 규칙 (`AWSHealthEventProcessorEventSource-DO-NOT-DELETE`) 버스를 설치합니다. `AWSServiceRoleForHealth_EventProcessor` SLR 규칙 소스는 사용자 지정 이벤트 버스입니다. 규칙 대상은 AWS 사고 탐지 및 대응입니다. 규칙은 타사 APM 이벤트 수집 패턴과 일치합니다.
   - (다른 방법) 사용자 지정 이벤트 버스 대신 기본 이벤트 버스를 사용합니다. 기본 이벤트 버스에는 AWS 사고 탐지 및 대응에 APM 경고를 보내는 관리형 규칙이 필요합니다.
3. 생성AWS Lambda기능 (예:`My_APM-AWSIncidentDetectionResponse-LambdaFunction`) 은 파트너 이벤트 버스 이벤트를 변환합니다. 변환된 이벤트는 관리형 규칙과 `AWSHealthEventProcessorEventSource-DO-NOT-DELETE` 일치합니다.
   a. 변환된 이벤트는 고유한 AWS 인시던트 탐지 및 대응 식별자를 포함하며 이벤트의 소스 및 세부 유형을 필수 값으로 설정합니다. 패턴이 관리형 규칙과 일치합니다.
   b. Lambda 함수의 대상을 2단계에서 생성한 사용자 지정 이벤트 버스 (권장 방법) 또는 기본 이벤트 버스로 설정합니다.
4. EventBridge 규칙을 생성하고 AWS 사고 탐지 및 대응으로 푸시하려는 이벤트 목록과 일치하는 이벤트 패턴을 정의합니다. 규칙의 소스는 1단계에서 정의한 파트너 이벤트 버스 (예: integrationName aws.partner/my_apm/) 입니다. 규칙의 대상은 3단계에서 정의한 Lambda 함수 (예:) 입니다. `My_APM-AWSIncidentDetectionResponse-LambdaFunction` 규칙 정의에 대한 지침은 Amazon EventBridge EventBridge 규칙을 참조하십시오.

AWS사고 탐지 및 대응에 사용할 파트너 이벤트 버스 통합을 설정하는 방법에 대한 예는 을 참조하십시오. 예: Datadog와 Splunk의 알림 통합

예: Datadog와 Splunk의 알림 통합

이 예제에서는 Datadog 및 Splunk의 알림을 사고 탐지 및 대응에 통합하기 위한 세부 단계를 제공합니다. AWS

1. AWS계정에서 EventBridge Amazon에서 이벤트 소스로 를 설정하십시오. APM
2. 커스텀 이벤트 버스를 만드세요.
3. 생성하기 AWS Lambda 변환을 위한 함수.
4. 사용자 지정 EventBridge 규칙을 만드세요.

1단계: Amazon에서 이벤트 소스로 설정 APM EventBridge

EventBridge AWS계정에서 Amazon의 이벤트 소스로 각각을 설정하십시오. APMs 를 이벤트 소스로 설정하는 방법에 대한 지침은 Amazon EventBridge 파트너의 도구에 대한 이벤트 소스 설정 지침을 참조하십시오. APM

를 이벤트 소스로 설정하면 사용자 APM AWS 계정에서 이벤트 버스로 전송되는 알림을 APM 수집할 수 있습니다. 설정 후, AWS 인시던트 탐지 및 대응은 이벤트 버스가 이벤트를 수신할 때 인시던트 관리 프로세스를 시작할 수 있습니다. 이 프로세스는 Amazon을 EventBridge 목적지로 추가합니다APM.

2단계: 사용자 지정 이벤트 버스 생성

사용자 지정 이벤트 버스를 사용하는 것이 가장 좋습니다. AWS인시던트 탐지 및 대응은 사용자 지정 이벤트 버스를 사용하여 변환된 이벤트를 수집합니다. 원래 요청 ping에 대한 AWS Lambda 함수는 파트너 이벤트 버스 이벤트를 변환하여 사용자 지정 이벤트 버스로 전송합니다. AWS인시던트 탐지 및 대응은 관리형 규칙을 설치하여 사용자 지정 이벤트 버스에서 이벤트를 수집합니다.

사용자 지정 이벤트 버스 대신 기본 이벤트 버스를 사용할 수 있습니다. AWS인시던트 탐지 및 대응은 사용자 지정 이벤트 버스 대신 기본 이벤트 버스에서 수집하도록 관리형 규칙을 수정합니다.

자체 이벤트 버스를 사용자 지정 이벤트 버스를 생성하십시오. AWS 계정:

1. 다음 위치에서 Amazon EventBridge 콘솔을 엽니다. https://console.aws.amazon.com/events/
2. 버스, 이벤트 버스를 선택합니다.
3. 커스텀 이벤트 버스에서 만들기를 선택합니다.
4. 이름 아래에 이벤트 버스의 이름을 입력합니다. 권장 형식은 APMNameAWSIncidentDetectionResponse- -입니다 EventBus.

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

- 데이터독: 데이터독- - AWSIncidentDetectionResponse EventBus
- 스플렁크: 스플렁크- - AWSIncidentDetectionResponse EventBus

3단계: 생성 AWS Lambda 변환을 위한 함수

Lambda 함수는 1단계의 파트너 이벤트 버스와 2단계의 사용자 지정 (또는 기본) 이벤트 버스 사이에서 이벤트를 변환합니다. Lambda 함수 변환은 사고 탐지 및 대응 관리 규칙과 AWS 일치합니다.

생성: AWS Lambda 내 함수 내 AWS account

1. 에서 함수 페이지를 엽니다. AWS Lambda 콘솔.
2. 함수 생성(Create function)을 선택합니다.
3. 스크래치 탭에서 작성자를 선택합니다.
4. 함수 이름에는 형식을 사용하여 이름을 입력합니다`APMName-AWSIncidentDetectionResponse-LambdaFunction`.

   다음은 데이터독과 스플렁크의 예시입니다.

   - 데이터독: 데이터독- - AWSIncidentDetectionResponse LambdaFunction
   - 스플렁크: 스플렁크- - AWSIncidentDetectionResponse LambdaFunction
5. 런타임에 Python 3.10을 입력합니다.
6. 나머지 필드는 디폴트 값으로 유지합니다. 함수 생성(Create function)을 선택합니다.
7. 코드 편집 페이지에서 기본 Lambda 함수 콘텐츠를 다음 코드 예제의 함수로 교체하십시오.

   다음 코드 예제에서 #로 시작하는 주석을 참고하십시오. 이러한 주석은 변경할 값을 나타냅니다.

   데이터독 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'])
```

스플렁크 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. 변환된 데이터를 보내는 대상 이벤트 버스의 Lambda 실행 역할에 PutEvents권한을 추가합니다.

   a. 에서 함수 페이지를 엽니다. AWS Lambda 콘솔.
   b. 함수를 선택한 다음 구성 탭에서 권한을 선택합니다.
   c. 실행 역할에서 역할 이름을 선택하여 실행 역할을 열고 AWS Identity and Access Management 콘솔.
   d. 권한 정책에서 기존 정책 이름을 선택하여 정책을 엽니다.
   e. 이 정책에 정의된 권한에서 편집을 선택합니다.
   f. 정책 편집기 페이지에서 새 명령문 추가를 선택합니다.
   g. 정책 편집기는 다음과 비슷한 새 빈 설명을 추가합니다.

h. 자동으로 생성된 새 명령문을 다음과 같이 대체합니다.

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

i. 리소스는 생성한 사용자 지정 이벤트 버스 2단계: 사용자 지정 이벤트 버스 생성 또는 Lambda 코드에서 기본 이벤트 버스를 사용하는 경우 기본 이벤트 버스의 리소스입니다. ARN ARN

10. 필요한 권한이 역할에 추가되었는지 검토하고 확인합니다.
11. 새 버전을 기본값으로 설정을 선택한 다음 변경 내용 저장을 선택합니다.

페이로드 변환에 필요한 것은 무엇입니까?

AWS인시던트 탐지 및 대응에서 수집한 이벤트 버스 이벤트에는 다음과 같은 JSON 키:값 쌍이 필요합니다.

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

다음 예는 파트너 이벤트 버스의 이벤트가 변환되기 전과 후의 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"
      ]
    }
}
```

단, 이벤트가 변환되기 전에는 알림의 APM 출처, 파트너의 소스APM, `incident-detection-response-identifier` 키가 존재하지 `detail-type` 않음을 알 수 있습니다.

Lambda 함수는 위 이벤트를 변환하여 대상 사용자 지정 또는 기본 이벤트 버스에 넣습니다. 이제 변환된 페이로드에는 필수 키:값 쌍이 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"
      ]
    }
}
```

참고로 지금은 소스가 되었고 ams.monitoring/generic-apmGenericAPMEvent, 자세히 보면 키:값 쌍이 새로 생겼습니다. detail-type incident-detection-response-identifier

위 예제에서는 경로 아래에 있는 알림 이름에서 incident-detection-response-identifier 값을 가져왔습니다. $.detail.meta.monitor.name APM경고 이름 경로는 서로 APM 다릅니다. 올바른 파트너 JSON 이벤트 경로에서 알람 이름을 가져와 값으로 사용하도록 Lambda 함수를 수정해야 합니다. incident-detection-response-identifier

에 설정된 각 고유 이름은 incident-detection-response-identifier 온보딩 중에 AWS 사고 탐지 및 대응 팀에 제공됩니다. 이름을 알 수 없는 이벤트는 incident-detection-response-identifier 처리되지 않습니다.

4단계: 사용자 지정 Amazon EventBridge 규칙 생성

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

EventBridge 규칙 정의에 대한 지침은 Amazon EventBridge 규칙을 참조하십시오.

1. 다음 위치에서 Amazon EventBridge 콘솔을 엽니다. https://console.aws.amazon.com/events/
2. 규칙을 선택한 다음 해당 규칙과 관련된 파트너 이벤트 버스를 선택합니다APM. 다음은 파트너 이벤트 버스의 예입니다.

   - 데이터독: aws.partner/datadog.com/eventbus-name
   - 스플렁크: aws.partner/signalfx.com/ RandomString
3. 규칙 생성을 선택하여 새 규칙을 생성합니다. EventBridge
4. 규칙 이름에 다음 형식으로 이름을 입력하고 **`APMName-AWS Incident Detection and Response-EventBridgeRule`** 다음을 선택합니다. 예제 이름은 다음과 같습니다.

   - 데이터독: 데이터독- - AWSIncidentDetectionResponse EventBridgeRule
   - 스플렁크: 스플렁크- - AWSIncidentDetectionResponse EventBridgeRule
5. 이벤트 소스의 경우 이벤트 또는 EventBridge 파트너 AWS 이벤트를 선택합니다.
6. 샘플 이벤트 및 생성 방법을 기본값으로 유지합니다.
7. 이벤트 패턴의 경우 다음을 선택합니다.

   a. 이벤트 소스: EventBridge 파트너.

   b. 파트너: APM 파트너를 선택하세요.

   c. 이벤트 유형: 모든 이벤트.

   다음은 예제 이벤트 패턴입니다.

   Datadog 이벤트 패턴 예시

   Splunk 이벤트 패턴 예시

8. 타겠에서 다음을 선택합니다.

   a. 대상 유형: AWS 서비스

b. 대상 선택: Lambda 함수를 선택합니다.

c. 함수: 2단계에서 생성한 Lambda 함수의 이름.

9. 다음, 규칙 저장을 선택합니다.

Amazon과 직접 APMs 통합하지 않고도 Webhook을 사용하여 경보를 수집할 수 있습니다. EventBridge

AWS사고 탐지 및 대응은 Amazon과 직접 통합되지 APMs 않은 타사의 알람 수집을 위한 웹후크 사용을 지원합니다. EventBridge

APMsAmazon과의 직접 통합 목록은 Amazon EventBridge EventBridge 통합을 참조하십시오.

다음 단계를 사용하여 AWS 사고 탐지 및 대응과의 통합을 설정하십시오. 이 단계를 수행하기 전에 계정에 AWS 관리형 DELETE 규칙인 AWSHealthEventProcessorEventSourceNOT---가 설치되어 있는지 확인하십시오.

웹후크를 사용한 이벤트 인제스트

1. Amazon API Gateway를 정의하여 사용자의 APM 페이로드를 수락합니다.
2. 다음을 정의하십시오. AWS Lambda 위 그림에 표시된 대로 인증 토큰을 사용한 권한 부여 함수를 사용합니다.
3. 두 번째 Lambda 함수를 정의하여 인시던트 탐지 및 대응 AWS 식별자를 변환하여 페이로드에 추가합니다. 또한 이 함수를 사용하여 AWS 사고 탐지 및 대응으로 전송하려는 이벤트를 필터링할 수 있습니다.
4. API게이트웨이에서 URL 생성된 알림에 알림을 APM 보내도록 설정합니다.

AWS사고 탐지 및 대응을 위한 런북 개발

예제 인시던트 탐지 및 대응 런북인 .zip을 다운로드할 수 있습니다. aws-idr-runbook-example

인시던트 탐지 및 대응은 온보딩 설문지에서 캡처한 정보를 사용하여 워크로드에 영향을 미치는 인시던트 관리를 위한 런북과 대응 계획을 개발합니다. 런북에는 인시던트 관리자가 인시던트에 대응할 때 취하는 단계가 기록되어 있습니다. 대응 계획은 워크로드 중 하나 이상에 매핑되어 있습니다. 인시던트 관리 팀은 앞서 설명한 것처럼 워크로드 검색 중에 사용자가 제공한 정보를 바탕으로 이러한 템플릿을 만듭니다. 대응 계획은 다음과 같습니다. AWS Systems Manager (SSM) 사고를 유발하는 데 사

용되는 문서 템플릿입니다. SSM문서에 대한 자세한 내용은 을 참조하십시오. AWS Systems Manager 문서, 인시던트 관리자에 대한 자세한 내용은 다음을 참조하십시오. AWS Systems Manager Incident Manager?

주요 결과:

- AWS사고 탐지 및 대응에 대한 워크로드 정의 완료.
- AWS사고 탐지 및 대응에 대한 경보, 런북 및 대응 계획 정의 완료.

또한 AWS 인시던트 탐지 및 대응 런북 예시.zip을 다운로드할 수 있습니다. aws-idr-runbook-example

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.
```

온보드 워크로드 테스트

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

온보딩 프로세스의 마지막 단계는 새 워크로드를 위한 게임데이를 수행하는 것입니다. 알람 수집이 완료되면 AWS 인시던트 탐지 및 대응 팀에서 게임데이를 시작하기로 선택한 날짜와 시간을 확인합니다.

경기일은 크게 두 가지 용도로 사용됩니다.

- 기능 검증: AWS 인시던트 탐지 및 대응이 알람 이벤트를 올바르게 수신할 수 있는지 확인합니다. 또한 기능 검증을 통해 알람 이벤트가 적절한 런북과 기타 원하는 작업 (예: 알람 수집 중에 선택한 경우 자동 케이스 생성) 을 트리거하는지 확인합니다.
- 시뮬레이션: 경기일은 실제 사고 발생 시 발생할 수 있는 상황을 종합적으로 시뮬레이션하는 것입니다. AWS사고 감지 및 대응은 규정된 런북 단계에 따라 실제 사건이 어떻게 전개될 수 있는지에 대한 통찰력을 제공합니다. 게임 데이는 질문을 하거나 지침을 수정하여 참여도를 높일 수 있는 기회입니다.

알람 테스트 중에는 AWS 인시던트 탐지 및 대응이 사용자와 협력하여 식별된 문제를 해결합니다.

CloudWatch 알람

AWS사고 감지 및 대응은 경보 상태 변화를 모니터링하여 Amazon CloudWatch 경보를 테스트합니다. 이렇게 하려면 다음을 사용하여 경보를 알람 상태로 수동으로 변경하십시오. AWS Command Line Interface. 또한 액세스할 수 있습니다. AWS CLI from AWS CloudShell. AWS사고 탐지 및 대응은 다음 목록을 제공합니다. AWS CLI 테스트 중에 사용할 수 있는 명령.

예 AWS CLI 알람 상태를 설정하는 명령:

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

CloudWatch 알람 상태를 수동으로 변경하는 방법에 대한 자세한 내용은 을 참조하십시오 SetAlarmState.

CloudWatch API작업에 필요한 권한에 대해 자세히 알아보려면 Amazon CloudWatch 권한 참조를 참조하십시오.

타사 APM 알람

Splunk 또는 Dynatrace와 같은 DataDog 타사 애플리케이션 성능 모니터링 (APM) 도구를 사용하는 워크로드에는 경보를 시뮬레이션하기 위한 다른 지침이 필요합니다. NewRelic AWS사고 탐지 및 대응 요청을 시작할 때 경보 임계값 또는 비교 연산자를 일시적으로 변경하여 경보를 강제로 상태로 전환합니다. GameDay ALARM 이 상태는 AWS 사고 탐지 및 대응에 대한 페이로드를 트리거합니다.

주요 결과

주요 결과:

- 알람 인제스트가 성공했고 알람 구성이 정확합니다.
- AWS사고 감지 및 대응을 통해 경보가 성공적으로 생성되고 수신됩니다.
- 참여를 위한 지원 사례가 생성되고 지정된 연락처에 알림이 전송됩니다.
- AWS사전 정의된 회의 수단을 통해 사고 탐지 및 대응에 참여할 수 있습니다.
- Gameday의 일환으로 생성된 모든 알람 및 지원 사례가 해결되었습니다.
- AWS사고 탐지 및 대응 팀에서 현재 워크로드를 모니터링하고 있음을 알리는 Go-Live 이메일이 발송됩니다.

워크로드 온보딩 및 알람 수집 설문지

워크로드 온보딩 설문지를 다운로드하십시오.

알람 통합 설문지를 다운로드하십시오.

워크로드 온보딩 설문지 - 일반 질문

일반 질문

질문	응답의 예
기업 이름	아마존 주식회사
이 워크로드의 이름 (약어 포함)	아마존 리테일 오퍼레이션 (ARO)
기본 최종 사용자 및 이 워크로드의 기능	이 워크로드는 최종 사용자가 다양한 품목을 구매할 수 있는 전자 상거래 애플리케이션입니다. 이 워크로드는 우리 비즈니스의 주요 수익 창출원입니다.
이 워크로드에 적용되는 규정 준수 및/또는 규제 요구 사항 및 필요한 조치 AWS 사고 이후.	업무량은 안전하게 기밀로 유지되어야 하는 환자 건강 기록을 다룹니다.

워크로드 온보딩 설문지 - 아키텍처 질문

아키텍처 질문

질문	응답의 예
목록: AWS 이 워크로드의 일부인 리소스를 정의하는 데 사용되는 리소스 태그. AWS 이러한 태그를 사용하여 이 워크로드의 리소스를 식별하여 인시던트 발생 시 지원을 신속하게 처리합니다. **Note** 태그는 대/소문자를 구분합니다. 여러 태그를 제공하는 경우 이 워크로드에 사용	appName: Optimax 환경: 프로덕션

질문	응답의 예
되는 모든 리소스에 동일한 태그가 있어야 합니다.	
목록: AWS 이 워크로드에서 사용하는 서비스 및 AWS 이들이 속해 있는 계정 및 지역 Note 각 서비스에 대해 새 행을 생성하세요.	Route 53: 인터넷 트래픽을 로 라우팅합니다 ALB. 계정: 123456789101 지역: 미국- -1, 미국- -2 EAST WEST
목록: AWS 이 워크로드에서 사용하는 서비스 및 AWS 이들이 속해 있는 계정 및 지역 Note 각 서비스에 대해 새 행을 생성하세요.	ALB: 들어오는 트래픽을 대상 ECS 컨테이너 그룹으로 라우팅합니다. 계정: 123456789101 지역: 해당 없음
목록 AWS 이 워크로드에서 사용하는 서비스 및 AWS 이들이 속해 있는 계정 및 지역 Note 각 서비스에 대해 새 행을 생성하세요.	ECS: 주요 비즈니스 로직 플릿을 위한 컴퓨팅 인프라. 들어오는 사용자 요청을 처리하고 지속성 계층에 쿼리를 만드는 일을 담당합니다. 계정: 123456789101 지역: 미국- -1 EAST
목록 AWS 이 워크로드에서 사용하는 서비스 및 AWS 이들이 속해 있는 계정 및 지역 Note 각 서비스에 대해 새 행을 생성하세요.	RDS: Amazon Aurora 클러스터는 ECS 비즈니스 로직 계층에서 액세스하는 사용자 데이터를 저장합니다. 계정: 123456789101 지역: 미국- -1 EAST

질문	응답의 예
목록 AWS 이 워크로드에서 사용하는 서비스 및 AWS 이들이 속해 있는 계정 및 지역 Note 각 서비스에 대해 새 행을 생성하세요.	S3: 웹 사이트 정적 자산을 저장합니다. 계정: 123456789101 지역: 해당 없음
정전이 발생할 경우 이 워크로드에 영향을 미칠 수 있는 온보딩되지 않은 업스트림/다운스트림 구성 요소를 자세히 설명하십시오.	인증 마이크로서비스: 인증되지 않으므로 사용자가 의료 기록을 로드하지 못하게 합니다.
온프레미스 또는 비프레미스가 있나요?AWS 이 워크로드의 구성 요소는 무엇입니까? 그렇다면 구성 요소는 무엇이며 어떤 기능이 수행됩니까?	들어오고 나가는 모든 인터넷 기반 트래픽 AWS 온프레미스 프록시 서비스를 통해 라우팅됩니다.
가용 영역 및 지역 수준의 수동 또는 자동 페일오버/재해 복구 계획의 세부 정보를 제공하십시오.	웜 스탠바이. 성공률이 지속적으로 떨어지는 동안 WEST US-2로 자동 페일오버를 수행합니다.

워크로드 온보딩 설문지 - AWS 서비스 이벤트 질문

AWS 서비스 이벤트 질문

질문	응답의 예
회사 내부 주요 사고/IT 위기 관리 팀의 연락처 세부 정보 (이름/이메일/전화) 를 제공하십시오.	주요 사고 관리팀 mim@example.com +61 2 3456 7890
회사에서 설치한 정적 사고/위기 관리 브리지의 세부 정보를 제공하십시오. 비정적 브리지를 사용하는 경우 선호하는 애플리케이션을 지정하고 AWS 사고 발생 시 이러한 세부 정보를 요청합니다.	Amazon Chime https://chime.aws/1234567890

질문	응답의 예
Note 정보가 제공되지 않는 경우 AWS 사고 발생 시 연락을 취해 합류할 수 있는 차임 다리를 제공합니다.	

알람 통합 설문지

런북 질문

질문	응답의 예
AWS 다음을 통해 워크로드 담당자를 참여시킬 것입니다. AWS Support 케이스. 이 워크로드에 대해 알람이 트리거될 때 주요 담당자는 누구인가요? 선호하는 회의 애플리케이션을 지정하고 AWS 인시던트 발생 시 이러한 세부 정보를 요청합니다. Note 선호하는 회의 응용 프로그램이 제공되지 않는 경우 AWS 인시던트 발생 시 연락을 취해 참여할 수 있는 Chime 브릿지를 제공합니다.	애플리케이션 팀 app@example.com +61 2 3456 7890
사고 중에 기본 연락처를 이용할 수 없는 경우, 에스컬레이션 연락처와 일정을 선호하는 연락 순서대로 제공하십시오.	1. 10분이 지난 후에도 기본 연락처로부터 응답이 없으면 다음과 같이 연락하십시오. John Smith - 애플리케이션 수퍼바이저 john.smith@example.com +61 2 3456 7890

질문	응답의 예
	2. 10분 후 존 스미스로부터 응답이 없으면 다음 연락처로 연락하십시오. 제인 스미스 - 운영 관리자 jane.smith@example.com +61 2 3456 7890
AWS 인시던트 내내 정기적으로 지원 케이스를 통해 업데이트 내용을 전달합니다. 이러한 업데이트를 받아야 하는 추가 연락처가 있습니까?	john.smith@example.com, jane.smith@example.com

알람 매트릭스

알람 매트릭스

다음 정보를 제공하여 AWS 사고 탐지 및 대응을 통해 워크로드를 대신하여 인시던트를 생성할 경보 세트를 식별하십시오. AWS사고 탐지 및 대응 담당 엔지니어가 경보를 검토한 후 추가 온보딩 단계가 제공됩니다.

AWS사고 감지 및 대응 중요 경보 기준:

- AWS사고 감지 및 대응 경보는 모니터링되는 워크로드에 중대한 비즈니스 영향 (수익 손실/고객 경험 저하) 이 발생하여 운영자의 즉각적인 주의가 필요한 경우에만 “경보” 상태로 전환되어야 합니다.
- AWS또한 사고 감지 및 대응 경보는 동시에 또는 작업 전에 해결 담당자를 워크로드에 참여시켜야 합니다. AWS 사고 관리자는 완화 프로세스에서 해결 담당자와 협력하며, 1차 대응 담당자 역할을 수행하지 않으며, 이후 사용자에게 에스컬레이션하는 역할을 합니다.
- AWS경보가 울릴 때마다 조사가 진행되도록 사고 탐지 및 대응 경보 임계값을 적절한 임계값 및 기간으로 설정해야 합니다. 경보가 “경보” 상태와 “정상” 상태 사이를 오가는 경우 운영자의 대응과 주의를 기울여야 할 만큼 충분한 영향이 발생하고 있는 것입니다.

AWS기준 위반에 대한 사고 감지 및 대응 정책:

이러한 기준은 이벤트 발생 시에만 평가할 수 있습니다. case-by-case 인시던트 관리 팀은 기술 계정 관리자 (TAMs) 와 협력하여 경보를 조정하고, 고객 경보가 이 기준을 준수하지 않고 정기적으로 사고

관리 팀에 불필요하게 개입하는 것으로 의심되는 경우 드문 경우이긴 하지만 모니터링을 비활성화합니다.

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

알람 매트릭스 테이블

지표 이름/ARN/임계값	설명	참고	요청된 조치
워크로드 볼륨/ *CW Alarm ARN* / CallCount 5분 내 5개 데이터 포인트에 대해 100000 미만, 누락된 데이터를 누락된 데이터로 처리	이 지표는 워크로드로 들어오는 요청 수를 나타내며, Application Load Balancer 수준에서 측정됩니다. 수신 요청이 크게 감소하면 업스트림 네트워크 연결에 문제가 있거나 DNS 구현 문제로 인해 사용자가 워크로드에 액세스할 수 없게 될 수 있기 때문에 이 경보는 중요합니다.	지난 주에 알람이 “Alarm” 상태에 10번이나 진입했습니다. 이 알람은 오탐이 발생할 위험이 있습니다. 임계값 검토가 계획되어 있습니다. 문제가 있나요? 아니요 또는 예 (아니오인 경우 비워 두기): 이 경보는 특정 배치 작업 실행 중에 자주 깜박입니다. 해결 담당자: 사이트 신뢰성 엔지니어	다음 주소로 이메일을 보내 사이트 신뢰성 엔지니어링 팀의 참여를 유도하세요.*SRE@xyz.com* 당사 ELB 및 Route 53 서비스에 대한 AWS 프리미엄 지원 사례를 생성하십시오. IMMEDIATE조치가 필요한 경우: 사용 가능한 메모리/디스크 EC2 공간을 확인하고 다음 연락처로 알리십시오.*XYZ* 이메일을 통해 팀을 구성하여 인스턴스를 다시 시작하거나 로그 플러시를 실행하십시오. (즉각적인 조치가 필요하지 않은 경우 공란으로 두세요)

지표 이름/ARN/임계값	설명	참고	요청된 조치
워크로드 요청 지연 시간/ *CW Alarm ARN* / p90 5분 내 5개 데이터 포인트에 대해 100ms 이상의 지연 시간, 누락된 데이터를 누락된 데이터로 처리	이 지표는 워크로드가 HTTP 요청을 처리하기 위한 p90 지연 시간을 나타냅니다. 이 경보는 대기 시간(웹 사이트의 고객 경험을 측정하는 중요한 척도) 을 나타냅니다.	지난 주에 알람이 “알람” 상태에 0번 들어갔습니다. 문제가 있나요? 아니요 또는 예 (아니오인 경우 비워 두기): 이 경보는 특정 배치 작업 실행 중에 자주 깜박입니다. 해결 담당자: 사이트 신뢰성 엔지니어	다음 주소로 이메일을 보내 사이트 신뢰성 엔지니어링 팀의 참여를 유도하세요.*SRE@xyz.com* 당사 ECW 및 RDS 서비스에 대한 AWS Premium Support 사례를 생성하십시오. IMMEDIATE조치가 필요한 경우: EC2 여유 메모리/디스크 공간을 확인하고 다음 연락처로 알리십시오.*XYZ* 이메일을 통해 팀을 구성하여 인스턴스를 다시 시작하거나 로그 플러시를 실행하십시오. (즉각적인 조치가 필요하지 않은 경우 공란으로 두세요)

지표 이름/ARN/임계값	설명	참고	요청된 조치
워크로드 요청 가용성/ *CW Alarm ARN* / 5분 이내에 5개 데이터 포인트의 가용성이 95% 미만이면 누락된 데이터를 누락된 것으로 처리합니다.	이 지표는 워크로드가 처리해야 하는 HTTP 요청의 가용성을 나타냅니다. 기간별 요청 수 (요청 수 HTTP 200 개/요청 수). 이 경보는 워크로드의 가용성을 나타냅니다.	지난 주에 알람이 “알람” 상태에 0번 진입했습니다. 문제가 있나요? 아니요 또는 예 (아니오인 경우 비워 두기): 이 경보는 특정 배치 작업 실행 중에 자주 깜박입니다. 해결 담당자: 사이트 신뢰성 엔지니어	다음 주소로 이메일을 보내 사이트 신뢰성 엔지니어링 팀의 참여를 유도하세요.*SRE@xyz.com* 당사 ELB 및 Route 53 서비스에 대한 AWS 프리미엄 지원 사례를 생성하십시오. IMMEDIATE조치가 필요한 경우: 사용 가능한 메모리/디스크 EC2 공간을 확인하고 다음 연락처로 알리십시오.*XYZ* 이메일을 통해 팀을 구성하여 인스턴스를 다시 시작하거나 로그 플러시를 실행하십시오. (즉각적인 조치가 필요하지 않은 경우 공란으로 두세요)
뉴렐릭 알람 예제			

지표 이름/ARN/임계값	설명	참고	요청된 조치
엔드투엔드 통합 테스트/ *CW Alarm ARN* / 3분 동안 1분 지표의 실패율 3%, 누락된 데이터는 누락된 것으로 처리 워크로드 식별자: 엔드 투 엔드 테스트 워크플로, AWS 지역: 미국 EAST -1, AWS 계정 ID: 012345678910	이 지표는 요청이 워크로드의 각 계층을 통과할 수 있는지 테스트합니다. 이 테스트가 실패하면 비즈니스 트랜잭션 처리에 심각한 장애가 발생한 것입니다. 이 경보는 워크로드에 대한 비즈니스 트랜잭션을 처리할 수 있는 능력을 나타냅니다.	지난 주에 알람이 "알람" 상태에 0번 들어갔습니다. 문제가 있나요? 아니요 또는 예 (아니오인 경우 비워 두기): 이 경보는 특정 배치 작업 실행 중에 자주 깜박입니다. 해결 담당자: 사이트 신뢰성 엔지니어	다음 주소로 이메일을 보내 사이트 신뢰성 엔지니어링 팀의 참여를 유도하세요.*SRE@xyz.com* 당사 ECS 및 DynamoDB 서비스에 대한 AWS 프리미엄 지원 사례를 생성하십시오. IMMEDIATE조치가 필요한 경우: 사용 EC2 가능한 메모리/디스크 공간을 확인하고 다음을 알리십시오.*XYZ* 이메일을 통해 팀을 구성하여 인스턴스를 다시 시작하거나 로그 플러시를 실행하십시오. (즉각적인 조치가 필요하지 않은 경우 공란으로 두세요)

온보드 워크로드 변경 요청

온보드 워크로드에 대한 변경을 요청하려면 다음 단계를 완료하여 AWS 사고 탐지 및 대응에 대한 지원 사례를 생성하십시오.

1. 다음으로 이동 AWS Support센터로 이동한 다음 다음 예와 같이 사례 만들기를 선택합니다.

2. 기술을 선택합니다.
3. [서비스] 에서 사고 탐지 및 대응을 선택합니다.

4. 범주에서 워크로드 변경 요청을 선택합니다.
5. 심각도에서는 일반 지침을 선택합니다.
6. 이 변경의 제목을 입력합니다. 예:

   AWS사고 탐지 및 대응 - *workload_name*
7. 이 변경에 대한 설명을 입력합니다. 예를 들어 “이 요청은 AWS 사고 탐지 및 대응에 온보딩된 기존 워크로드의 변경 사항에 대한 요청입니다”라고 입력합니다. 요청에 다음 정보를 포함해야 합니다.

   - 워크로드 이름: 워크로드 이름.
   - 계정 ID: ID1ID2,ID3, 등.
   - 변경 세부 정보: 요청한 변경 사항의 세부 정보를 입력합니다.
8. 추가 연락처 - 선택 사항 섹션에서 이 변경 사항에 대한 서신을 받고 싶은 이메일을 IDs 입력합니다.

   다음은 추가 연락처 - 선택 섹션의 예입니다.

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

   변경 요청을 제출한 후 조직에서 보내는 이메일을 더 추가할 수 있습니다. 이메일을 추가하려면 다음 예와 같이 케이스 세부 정보에 답장을 선택합니다.

   그런 다음 추가 연락처 - 선택 IDs 섹션에 이메일을 추가합니다.

   다음은 추가 이메일을 입력할 수 있는 회신 페이지의 예입니다.

워크로드 오프보딩

AWS인시던트 탐지 및 대응에서 워크로드를 오프보딩하려면 각 워크로드에 대한 새 지원 사례를 만드세요. 지원 사례를 만들 때는 다음 사항을 염두에 두세요.

- 단일 워크로드를 오프보딩하려면 AWS 계정에서 워크로드 계정이나 지급인 계정에서 지원 사례를 생성하세요.
- 여러 곳에 걸친 워크로드를 오프보딩하려면 AWS 계정을 만든 다음 지급인 계정에서 지원 사례를 생성하세요. 지원 사례 본문에 IDs 오프보딩할 모든 계정을 나열하십시오.

> **Important**
>
> 잘못된 계정에서 워크로드를 오프보딩하기 위해 지원 사례를 생성하면 워크로드를 오프로드하기 전에 지연이 발생하고 추가 정보 요청이 발생할 수 있습니다.

워크로드 오프보딩 요청

1. 다음으로 이동 AWS Support센터로 이동한 다음 사례 만들기를 선택합니다.
2. 테크니컬을 선택합니다.
3. [서비스] 에서 사고 탐지 및 대응을 선택합니다.
4. 카테고리에서는 워크로드 오프보딩을 선택합니다.
5. 심각도에서는 일반 지침을 선택합니다.
6. 이 변경의 제목을 입력합니다. 예:

   [오프보드] AWS 사고 탐지 및 대응 - *workload_name*
7. 이 변경에 대한 설명을 입력합니다. 예를 들어 “이 요청은 AWS 사고 탐지 및 대응에 온보딩된 기존 워크로드를 오프보딩하기 위한 요청입니다”라고 입력합니다. 요청에 다음 정보를 포함해야 합니다.

   - 워크로드 이름: 워크로드 이름.
   - 계정 ID: ID1ID2,ID3, 등.
   - 오프보딩 이유: 워크로드를 오프보딩하는 이유를 제공하십시오.
8. 추가 연락처 - 선택 섹션에서 이 오프보딩 요청에 대한 서신을 받고 싶은 이메일을 IDs 입력합니다.
9. 제출을 선택합니다.

AWS 사고 탐지 및 대응 모니터링 및 관찰 가능성

AWS 사고 탐지 및 대응은 애플리케이션 계층에서 기본 인프라에 이르는 워크로드 전반의 관찰 가능성을 정의하는 데 대한 전문적인 지침을 제공합니다. 모니터링을 통해 무언가 잘못되었음을 알 수 있습니다. Observability는 데이터 수집을 통해 무엇이 잘못되었고 왜 발생했는지 알려줍니다.

사고 탐지 및 대응 시스템은 Amazon, Amazon 등의 네이티브 AWS 서비스를 활용하여 AWS 워크로드에 영향을 줄 수 있는 이벤트를 EventBridge 탐지하여 워크로드의 장애 및 CloudWatch 성능 저하를 모니터링합니다. 모니터링은 임박한 장애, 진행 중인 장애, 지연 또는 잠재적 장애 또는 성능 저하에 대한 알림을 제공합니다. 계정을 인시던트 탐지 및 대응에 온보딩할 때는 인시던트 탐지 및 대응 모니터링 시스템에서 모니터링해야 하는 계정 내 경보를 선택하고 이러한 경보를 사고 관리 시 사용되는 응용 프로그램 및 Runbook과 연결합니다.

사고 탐지 및 대응은 Amazon CloudWatch 및 기타 AWS 서비스 업체를 사용하여 옵저버빌리티 솔루션을 구축합니다. AWS 사고 탐지 및 대응은 다음 두 가지 방식으로 관찰 가능성을 높이는 데 도움이 됩니다.

- 비즈니스 성과 지표: AWS 사고 탐지 및 대응에서의 관찰 가능성은 워크로드 또는 최종 사용자 경험의 결과를 모니터링하는 주요 지표를 정의하는 것으로 시작됩니다. AWS 전문가가 고객과 협력하여 워크로드의 목표, 사용자 경험에 영향을 미칠 수 있는 주요 결과 또는 요인을 이해하고 이러한 주요 지표의 성능 저하를 포착하는 지표와 알림을 정의합니다. 예를 들어 모바일 통화 응용 프로그램의 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 이러한 인프라 서비스의 성능을 추적하기 위한 지표와 경보를 정의합니다. 여기에는 Application Load Balancer `ApplicationLoadBalancerErrorCount` 인스턴스와 같은 지표가 포함될 수 있습니다. 이는 워크로드가 온보딩되고 모니터링이 설정된 후에 시작됩니다.

AWS 사고 탐지 및 대응에 옵저버빌리티 구현

옵저버빌리티는 한 번의 연습 또는 일정 기간으로 완료할 수 없는 지속적인 프로세스이므로 AWS 사고 탐지 및 대응은 두 단계로 옵저버빌리티를 구현합니다.

- 온보딩 단계: 온보딩 중의 옵저버빌리티는 애플리케이션의 비즈니스 성과가 손상되는 시점을 감지하는 데 중점을 둡니다. 이를 위해 온보딩 단계의 옵저버빌리티는 애플리케이션 계층에서 주요 비즈니스 성과 지표를 정의하여 워크로드 중단을 알리는 AWS 데 중점을 둡니다. 이 방법을 AWS 사용하면 이러한 중단에 신속하게 대응하고 복구에 도움을 줄 수 있습니다.

- 온보딩 이후 단계: AWS Incident Detection and Response는 인프라 수준 메트릭의 정의, 메트릭 튜닝, 고객의 성숙도에 따른 추적 및 로그 설정 등 옵저버빌리티를 위한 다양한 사전 예방 서비스를 제공합니다. 이러한 서비스의 구현에는 몇 개월이 걸리며 여러 팀이 참여할 수 있습니다. AWS 사고 탐지 및 대응은 관찰 가능성 설정에 대한 지침을 제공하며 고객은 워크로드 환경에 필요한 변경 사항을 구현해야 합니다. 옵저버빌리티 기능을 직접 구현하는 데 도움이 필요하면 기술 계정 관리자 (TAM)에게 요청하십시오.

사고 탐지 및 대응을 통한 AWS 사고 관리

AWS사고 탐지 및 대응은 지정된 사고 관리자 팀이 제공하는 연중무휴 사전 모니터링 및 사고 관리를 제공합니다.

1. 경보 생성: 워크로드에서 트리거된 경보는 Amazon을 통해 AWS 사고 탐지 및 EventBridge 대응으로 푸시됩니다. AWS사고 탐지 및 대응은 경보와 관련된 실행서를 자동으로 불러와 사고 관리자에게 알립니다. 워크로드에서 사고 탐지 및 대응으로 모니터링되는 경보로 감지되지 않는 중대한 AWS 사고가 발생하는 경우 지원 사례를 생성하여 사고 대응을 요청할 수 있습니다. 인시던트 대응 요청에 대한 자세한 내용은 을 참조하십시오사고 대응 요청.
2. AWS 인시던트 관리자 참여: 인시던트 관리자가 경보에 응답하고 전화 회의 또는 런북에 달리 명시된 대로 사용자를 참여시킵니다. 인시던트 관리자는 사고 현장의 상태를 확인합니다. AWS 서비스 경보가 다음과 같은 문제와 관련이 있는지 확인하기 위해 AWS 서비스 워크로드에 사용되며 기본 서비스의 상태에 대해 조언합니다. 필요한 경우 인시던트 관리자가 사용자를 대신하여 케이스를 생성하고 권한을 부여합니다. AWS 지원을 위한 전문가.

   AWS사고 탐지 및 대응이 모니터링되기 때문입니다. AWS 서비스 특히 응용 프로그램의 경우 AWS 사고 탐지 및 대응에서 사고가 다음과 관련이 있다고 판단할 수 있습니다. AWS 서비스 문제가 발생하기 전에도 AWS 서비스 이벤트가 선언됩니다. 이 시나리오에서는 인시던트 관리자가 이벤트 상태에 대해 조언합니다. AWS 서비스, 트리거를 트리거합니다. AWS 서비스 이벤트 인시던트 관리 흐름을 파악하고 서비스 팀에 후속 조치를 취하여 해결합니다. 제공된 정보를 통해 복구 계획이나 해결 방법을 조기에 구현하여 그로 인한 영향을 완화할 수 있습니다. AWS 서비스 이벤트. 자세한 내용은 서비스 이벤트에 대한 인시던트 관리 단원을 참조하십시오.
3. 인시던트 해결: 인시던트 관리자가 필요한 범위에서 인시던트를 조정합니다. AWS 팀을 이루어 항상 권리를 지키고 있는지 확인합니다. AWS 사고가 완화되거나 해결될 때까지 전문가를 고용하세요.
4. 사후 사고 검토 (요청 시): 사고 발생 후, AWS 사고 탐지 및 대응 부서에서는 사용자의 요청에 따라 사후 사고 검토를 수행하고 사고 후 보고서를 생성할 수 있습니다. 사후 사고 보고서에는 문제에 대한 설명, 영향, 참여한 팀, 사고를 완화 또는 해결하기 위해 취해진 해결 방법 또는 조치가 포함됩니다. 사후 사고 보고서에는 사고 재발 가능성을 줄이거나 유사한 사고의 향후 발생에 대한 관리를 개선하는 데 사용할 수 있는 정보가 포함될 수 있습니다. 사후 사고 보고서는 근본 원인 분석 (RCA) 이 아닙니다. 사후 보고서 RCA 외에 추가로 요청할 수 있습니다. 다음 섹션에는 사후 사고 보고서의 예가 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 a 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 an 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.
```

애플리케이션 팀에 액세스 권한 제공

AWS사고 탐지 및 대응은 다음을 통해 사용자와 소통합니다. AWS Support 인시던트 수명 주기 동안의 사례. 인시던트 관리자와 연락을 취하려면 팀이 다음 연락처에 액세스할 수 있어야 합니다. AWS Support 센터.

프로비저닝 액세스에 대한 자세한 내용은 액세스 관리를 참조하십시오. AWS Support 센터 내 AWS Support 사용자 가이드.

서비스 이벤트에 대한 인시던트 관리

AWS사고 탐지 및 대응은 회사에서 진행 중인 서비스 이벤트를 알려줍니다. AWS 지역 (워크로드가 영향을 받는지 여부) 기간 중 AWS 서비스 이벤트, AWS 사고 탐지 및 대응은 다음을 생성합니다. AWS Support Case: 컨퍼런스 콜 브리지에 참여하여 영향력과 정서에 대한 피드백을 받고, 이벤트 기간 동안 복구 계획을 실행하기 위한 지침을 제공합니다. 다음을 통해서도 알림을 받게 됩니다. AWS Health 이벤트 세부 정보가 들어 있습니다. 영향을 받지 않는 고객 AWS 자체 서비스 이벤트 (예: 다른 지역에

서 운영 중) AWS 지역, 사용하지 마세요. AWS 장애가 발생한 서비스 등) 에 대해서는 표준 계약을 통해 계속 지원됩니다. 에 대한 자세한 내용은 AWS Health무엇입니까를 참조하십시오. AWS Health?.

서비스 이벤트에 대한 사후 사고 보고서 (요청된 경우): 서비스 이벤트로 인해 사고가 발생한 경우 AWS 사고 탐지 및 대응을 요청하여 사후 검토를 수행하고 사후 사고 보고서를 생성할 수 있습니다. 서비스 이벤트에 대한 사고 후 보고서에는 다음이 포함됩니다.

- 문제에 대한 설명
- 사고의 영향
- 에서 공유된 정보 AWS Health 대시보드
- 사고 발생 당시 참여했던 팀들
- 사고를 완화 또는 해결하기 위해 취한 해결 방법 및 조치

서비스 이벤트에 대한 사후 사고 보고서에는 사고 재발 가능성을 줄이거나 유사한 사고의 향후 발생에 대한 관리를 개선하는 데 사용할 수 있는 정보가 포함될 수 있습니다. 서비스 이벤트에 대한 사후 사고 보고서는 근본 원인 분석 (RCA) 이 아닙니다. 서비스 이벤트에 대한 사후 사고 보고서 RCA 외에 추가로 요청할 수 있습니다.

다음은 서비스 이벤트에 대한 사후 사고 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 an 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 ...
```

사고 대응 요청

워크로드에서 사고 탐지 및 대응으로 모니터링되는 경보로 감지되지 않는 중대한 AWS 사고가 발생하는 경우 지원 사례를 생성하여 사고 대응을 요청할 수 있습니다. 온보딩 프로세스 중인 워크로드를 포함하여 AWS 인시던트 탐지 및 대응에 구독된 모든 워크로드에 대해 인시던트 대응을 요청할 수 있습니다.

워크로드에 적극적으로 영향을 미치는 인시던트에 대한 인시던트 대응을 요청하려면 다음을 생성하십시오. AWS Support 사례. 지원 케이스가 제기되면 AWS 인시던트 탐지 및 대응 담당자가 컨퍼런스 브리지로 안내해 드립니다. AWS 워크로드 복구를 가속화하려면 전문가가 필요합니다.

를 사용하여 사고 대응을 요청하십시오. AWS Support Center Console

1. AWS Support Center Console그런 다음 사례 만들기를 선택합니다.
2. 테크니컬을 선택합니다.
3. [서비스] 에서 사고 탐지 및 대응을 선택합니다.
4. 카테고리에서는 활성 인시던트를 선택합니다.
5. 심각도에서는 비즈니스 크리티컬 시스템 다운을 선택합니다.
6. 이 사고의 제목을 입력합니다. 예:

   AWS사고 탐지 및 대응 - 진행 중인 사고 - workload_name
7. 이 사고에 대한 문제 설명을 입력합니다. 다음 세부 정보를 추가합니다.
   - 기술 정보:

     영향을 받는 서비스:

     영향을 받는 리소스:

     영향을 받는 지역:

     워크로드 이름:
   - 비즈니스 정보:

     비즈니스에 미치는 영향에 대한 설명:

     [선택 사항] 고객 브리지 세부 정보:
8. 추가 연락처 섹션에 이 사고와 관련된 서신을 받을 이메일 주소를 입력합니다.

다음 그림은 추가 연락처 필드가 강조 표시된 콘솔 화면을 보여줍니다.

9. 제출을 선택합니다.

   인시던트 대응 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 케이스 세부 정보 화면을 보여줍니다.

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

10AWS사고 탐지 및 대응 담당자가 5분 이내에 사례를 확인하고 적절한 담당자와 함께 컨퍼런스 브리지로 안내합니다. AWS 전문가.

다음을 사용하여 사고 대응을 요청하십시오. AWS Support API

지원 사례는 다음을 사용하여 프로그래밍 방식으로 만들 수 있습니다. AWS Support API.

를 사용하여 사고 대응을 요청하십시오. AWS Support App in Slack

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

```
/awssupport create
```

3. 이 인시던트의 제목을 입력합니다. 예를 들어 AWS사고 탐지 및 대응 - 활성 사고 - workload_name을 입력합니다.
4. 이 사고에 대한 문제 설명을 입력합니다. 다음 세부 정보를 추가합니다.

   기술 정보:

   영향을 받는 서비스:

   영향을 받는 리소스:

   영향을 받는 지역:

워크로드 이름:

비즈니스 정보:

비즈니스에 미치는 영향에 대한 설명:

[선택 사항] 고객 브리지 세부 정보:

5. Next(다음)를 선택합니다.

6. 문제 유형에서 기술 지원을 선택합니다.
7. [서비스] 에서 사고 탐지 및 대응을 선택합니다.
8. 카테고리에서는 활성 인시던트를 선택합니다.
9. 심각도에서는 비즈니스 크리티컬 시스템 다운을 선택합니다.

10. 연락 방법에서 이메일 및 Slack 알림을 선택합니다.

> **Note**
>
> AWS사고 탐지 및 대응은 Slack의 실시간 채팅을 지원하지 않습니다. 이 옵션을 선택하면 사고 대응 요청에 대한 응답이 지연될 수 있습니다.

11. 이 사고에 대한 이메일 서신 사본을 받고자 하는 추가 연락처를 구성할 수 있습니다.

12. 검토를 선택합니다.
13. 본인만 볼 수 있는 새 메시지가 Slack 채널에 표시됩니다. 사례 세부 정보를 검토한 다음 사례 만들기를 선택합니다.

14. 케이스 ID는 새 메시지로 제공됩니다. AWS Support App in Slack.
15. 사고 탐지 및 대응은 5분 이내에 케이스를 확인하고 해당 담당자와 함께 컨퍼런스 브리지로 연결해 드립니다. AWS 전문가.
16. 사고 탐지 및 대응의 서신은 사례 스레드에서 업데이트됩니다.

AWS슬랙의 Support 앱

AWS 고객은 다음을 사용할 수 있습니다. AWS Support App in Slack관리하기 위해 AWS Support 슬랙의 케이스.

AWS 사고 탐지 및 대응 고객은 다음을 사용할 수 있습니다. AWS Support App in Slack 워크로드에서 새로 발생한 경보 발생 사고에 대한 알림을 받거나 사고 대응 요청을 생성할 수 있습니다.

구성하려면 AWS Support App in Slack에 제공된 지침을 따르십시오. AWS Support 사용자 가이드.

Important

- Support 사례를 업데이트하거나 생성하는 경우 AWS 를 통한 사고 탐지 및 대응 AWS Support App in Slack, 이메일 및 슬랙 알림 연락 방법을 선택해야 합니다.

  AWS 사고 탐지 및 대응은 Support 사례에 대한 이메일 서신만 지원합니다. 실시간 채팅은 지원되지 않습니다.

- 워크로드에서 경보가 시작된 모든 인시던트에 대해 Slack에서 알림을 받을 수 있도록 하려면 다음을 구성해야 합니다. AWS Support App in Slack 온보딩된 모든 워크로드 계정에 대해 AWS 사고 탐지 및 대응. 지원 사례는 워크로드 경보가 발생한 계정에서 생성됩니다.
- 인시던트 중에 귀사를 대신하여 심각도가 높은 Support 케이스를 여러 개 개설하여 참여할 수 있습니다. AWS Support 리졸버. Slack 채널의 알림 구성과 일치하는 인시던트 중에 접수된 모든 지원 사례에 대해 Slack에서 알림을 받게 됩니다.
- 를 통해 수신하는 알림 AWS Support App in Slack 이메일이나 전화로 문의하는 워크로드의 초기 및 에스컬레이션 연락처를 다음과 같이 교체하지 마세요. AWS 사고 발생 중 사고 감지 및 대응.

Slack에서 경보로 시작된 사고 알림

Slack의 AWS Support 앱을 Slack 채널에 구성하면 AWS 인시던트 탐지 및 대응 모니터링 워크로드에서 경보가 시작된 인시던트에 대한 알림을 받게 됩니다.

다음 예시는 Slack에서 알람 발생 인시던트에 대한 알림이 어떻게 나타나는지 보여줍니다.

알림 예시

경보로 시작된 사고가 AWS 사고 탐지 및 대응에서 확인되면 Slack에 다음과 유사한 알림이 생성됩니다.

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

AWS사고 탐지 및 대응의 추가 업데이트는 사례 스레드에 표시됩니다.

AWS사고 탐지 및 대응에서 추가한 전체 서신을 보려면 세부 정보 보기를 선택하십시오.

Slack의 사고 대응 요청

Slack의 AWS Support 앱을 통해 사고 대응 요청을 생성하는 방법에 대한 지침은 사고 대응 요청을 참조하십시오.

AWS 사고 탐지 및 대응 보고

사고 탐지 및 대응은 서비스 구성 방식, 사고 기록, 사고 탐지 및 대응 서비스의 성능을 이해하는 데 도움이 되는 운영 및 성능 데이터를 제공합니다.

구성 데이터

- 모든 계정이 온보딩되었습니다.
- 모든 애플리케이션의 이름
- 각 애플리케이션과 관련된 알람, 런북 및 지원 프로필

인시던트 데이터

- 각 애플리케이션의 사고 날짜, 횟수 및 기간
- 특정 경보와 관련된 사고의 날짜, 횟수 및 기간
- 사후 사고 보고서

성능 데이터

- 서비스 수준 목표 (SLO) 성능

필요한 운영 및 성능 데이터는 기술 계정 관리자에게 문의하세요.

사고 감지 및 대응 보안 및 복원력

AWS 공동 책임 모델은 의 데이터 보호에 적용됩니다 AWS Support. 이 모델에 설명된 대로, AWS 는 모든 모델을 실행하는 글로벌 인프라를 보호할 책임이 AWS 클라우드있습니다. 사용자는 인프라에서 호스팅되는 콘텐츠를 관리해야 합니다. 이 콘텐츠에는 AWS 서비스 사용하는 보안 구성 및 관리 작업이 포함됩니다.

데이터 프라이버시에 대한 자세한 내용은 데이터 프라이버시 FAQ를 참조하세요.

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

데이터 보호를 위해 AWS 계정 자격 증명을 보호하고 AWS Identity and Access Management (IAM) 을 사용하여 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 멀티 팩터 인증 설정(MFA)을 사용하세요.
- 보안 소켓 계층/전송 계층 보안 (SSL/TLS) 인증서를 사용하여 리소스와 통신할 수 있습니다. AWS TLS 1.2 이상을 권장합니다. 자세한 내용은 SSL/TLS 인증서란 무엇입니까? 를 참조하십시오. .
- 를 사용하여 API 및 사용자 활동 로깅을 설정합니다 AWS CloudTrail. 자세한 내용은 AWS CloudTrail을 참조하세요.
- AWS 서비스 내의 모든 기본 보안 제어와 함께 AWS 암호화 솔루션을 사용하십시오. 자세한 내용은 AWS 암호화 서비스 및 도구를 참조하십시오.
- 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 참조하십시오.
- 명령줄 인터페이스 또는 API를 AWS 통해 액세스할 때 FIPS 140-2의 검증을 거친 암호화 모듈이 필요한 경우 FIPS 엔드포인트를 사용하십시오. 사용 가능한 FIPS 엔드포인트에 대한 자세한 내용은 연방 정보 처리 표준 (FIPS) 140-2를 참조하십시오.

고객의 이메일 주소와 같은 기밀 정보나 중요한 정보는 태그나 이름 필드와 같은 자유 양식 필드에 입력하지 않는 것이 좋습니다. 여기에는 콘솔, API, AWS CLI AWS Support 또는 AWS 서비스 SDK를 사용하거나 다른 방법을 사용하는 경우가 포함됩니다. AWS 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 제어하는 데 도움이 되는 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 감지 및 대응은 계정 내 모든 CloudWatch 경보의 Amazon 리소스 이름 (ARN) 과 상태를 수신한 다음 온보드 경보가 ALARM 상태로 변경될 때 사고 탐지 및 대응 프로세스를 시작합니다. 인시던트 탐지 및 대응이 계정으로부터 경보에 대해 수신하는 정보를 사용자 지정하려면 기술 계정 관리자에게 문의하십시오.

문서 이력

다음 표에는 IDR 가이드의 마지막 릴리스 이후 이 설명서의 중요한 변경 사항이 설명되어 있습니다.

- 최신 설명서 업데이트: 2024년 6월 12일

변경 사항	설명	날짜
새 페이지 추가 AWS Support App in Slack 사고 탐지 및 대응을 통한 AWS 사고 관리 업데이트	에 대한 새 페이지 추가 AWS Support App in Slack 사고 탐지 및 대응으로 AWS 사고 관리를 업데이트하여 “다음을 사용하여 사고 대응 요청”이라는 새 섹션을 추가했습니다. AWS Support App in Slack".	2024년 9월 10일
계정 구독 업데이트	계정 구독 요청 시 지원 케이스를 열 수 있는 위치에 대한 세부 정보를 포함하도록 계정 구독 섹션을 업데이트했습니다. 업데이트된 섹션: 계정 구독	2024년 6월 12일
서비스 이벤트에 대한 사후 사고 보고서를 현재 이용할 수 있습니다.	서비스 이벤트에 대한 인시던트 관리 섹션이 서비스 이벤트에 대한 사후 인시던트 보고서에 대한 정보를 포함하도록 업데이트되었습니다. 업데이트된 섹션: 서비스 이벤트에 대한 인시던트 관리	2024년 5월 8일
새 섹션 추가: 워크로드 오프보딩	시작하기에 워크로드 오프로드 섹션이 추가되어 오프보딩 워크로드에 대한 정보가 포함됩니다. 자세한 내용은 워크로드 오프보딩을 참조하십시오.	2024년 3월 28일
업데이트된 계정 구독	오프보딩 워크로드에 대한 정보를 포함하도록 계정 구독 섹션을 업데이트했습니다.	2024년 3월 28일

변경 사항	설명	날짜
	자세한 내용은 계정 구독을 참조하십시오.	
업데이트된 테스트	온보딩 프로세스의 마지막 단계로 게임데이 테스트에 대한 정보를 포함하도록 테스트 섹션을 업데이트했습니다. 업데이트된 섹션: 온보드 워크로드 테스트	2024년 2월 29일
업데이트: AWS 사고 탐지 및 대응이란 무엇입니까?	AWS사고 탐지 및 대응이란? 섹션을 업데이트했습니다. 업데이트된 섹션: AWS 사고 탐지 및 대응이란 무엇입니까?	2024년 2월 19일
설문지 섹션 업데이트	워크로드 온보딩 설문지를 업데이트하고 알람 통합 설문지를 추가했습니다. 섹션 이름을 온보딩 설문지에서 워크로드 온보딩 및 알람 통합 설문지로 변경했습니다. 업데이트된 섹션: 워크로드 온보딩 및 알람 수집 설문지	2024년 2월 2일
Updated AWS 서비스 이벤트 및 온보딩 정보	온보딩에 대한 새로운 정보로 여러 섹션을 업데이트했습니다. 업데이트된 섹션: • 서비스 이벤트에 대한 인시던트 관리 • 워크로드 검색 • 온보딩 • 계정 구독 새 섹션 • 애플리케이션 팀에 액세스 권한 제공	2024년 1월 31일

변경 사항	설명	날짜
관련 정보 섹션 추가	액세스 프로비저닝에 관련 정보 섹션이 추가되었습니다. 업데이트된 섹션: 사고 탐지 및 대응에 대한 알림 수집을 위한 액세스를 제공합니다.	2024년 1월 17일
업데이트된 예제 단계	예제: Datadog와 Splunk의 알림 통합에서 2, 3, 4단계에 대한 절차를 업데이트했습니다. 업데이트된 섹션: 예: Datadog와 Splunk의 알림 통합	2023년 12월 21일
소개 그래픽 및 텍스트 업데이트	Amazon과 직접 APMs 통합되는 Ingest 경보의 그래픽이 업데이트되었습니다. EventBridge 업데이트된 섹션: AWS사고 탐지 및 대응을 위한 런북 개발	2023년 12월 21일
업데이트된 런북 템플릿	AWS사고 탐지 및 대응을 위한 런북 개발의 런북 템플릿을 업데이트했습니다. 업데이트된 섹션: AWS사고 탐지 및 대응을 위한 런북 개발	2023년 12월 4일
업데이트된 알람 구성	알람 구성에 대한 자세한 정보가 포함된 CloudWatch 알람 구성을 업데이트했습니다. 새 섹션: 사고 탐지 및 대응에서 비즈니스 요구 사항에 맞는 CloudWatch 경보를 생성하십시오. 새 섹션: 사용 AWS CloudFormation 사고 탐지 및 대응에서 CloudWatch 경보를 구축하기 위한 템플릿 새 섹션: 사고 탐지 및 대응에서의 CloudWatch 경보 사용 사례 예시	2023년 9월 28일

변경 사항	설명	날짜
업데이트됨 시작하기	시작하기에 워크로드 변경 요청에 대한 정보가 업데이트되었습니다. 새 섹션: 온보드 워크로드 변경 요청 업데이트된 섹션: 계정 구독	2023년 9월 5일
시작하기의 새 섹션	알림을 AWS 사고 탐지 및 대응에 수집AWS인시던트 탐지 및 대응에 인제스팅 알림을 추가했습니다.	2023년 6월 30일
원본 문서	AWS사고 탐지 및 대응 최초 공개	2023년 3월 15일

AWS 용어집

최신 AWS 용어는 참조의 AWS 용어집을 참조하십시오.AWS 용어집

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