aws

사용자 가이드

Incident Manager

Incident Manager: 사용자 가이드

Table of Contents

란 무엇인가요 AWS Systems Manager Incident Manager?

의 도구인 Incident Manager AWS Systems Manager는 호스팅되는 애플리케이션에 영향을 미치는 인시던트를 완화하고 복구하는 데 도움이 되도록 설계되었습니다 AWS.

의 맥락에서 AWS인시던트는 비즈니스 운영에 상당한 영향을 미칠 수 있는 서비스 품질의 예상치 못한 중단 또는 저하입니다. 따라서 조직은 인시던트를 효율적으로 완화 및 복구하기 위한 대응 전략을 수립하고 향후 인시던트를 예방하기 위한 조치를 취하는 것이 중요합니다.

Incident Manager는 다음과 같은 방법으로 인시던트 해결 시간을 줄이는 데 도움이 됩니다.

- 인시던트 대응 책임자를 효율적으로 참여시키기 위한 자동화된 계획을 제공합니다.
- 관련 문제 해결 데이터를 제공합니다.
- 사전 정의된 자동화 런북을 사용하여 자동 대응 조치를 가능하게 합니다.
- 모든 이해 관계자와 협업하고 소통할 수 있는 방법을 제공합니다.

Incident Manager에 내장된 기능 및 워크플로는 Amazon이 거의 설립 초기부터 개발해 온 인시던트 대응을 위한 모범 사례를 기반으로 합니다. Incident Manager는 Amazon CloudWatch, AWS CloudTrail AWS Systems Manager, 및 Amazon EventBridge와 AWS 서비스 같은와 통합됩니다.

기본 구성 요소 및 기능

이 섹션에서는 인시던트 대응 계획을 설정하는 데 사용하는 Incident Manager의 기능에 대해 설명합니다.

대응 계획

대응 계획은 인시던트 발생 시 마련해야 할 사항을 정의하는 템플릿의 역할을 합니다. 여기에는 다음과 같은 정보가 포함됩니다.

- 인시던트 발생 시 대응해야 하는 담당자.
- 인시던트를 완화하기 위해 확립된 자동 대응.
- 대응 담당자가 인시던트에 대해 통신하고 자동 알림을 수신하는 데 사용해야 하는 협업 도구.

인시던트 탐지

AWS 리소스에 영향을 미치는 조건 또는 변경 사항이 감지되면 인시던트를 생성하도록 Amazon CloudWatch 경보 및 Amazon EventBridge 이벤트를 구성할 수 있습니다.

자동화 런북 지원

Incident Manager 내에서 자동화 런북을 시작하여 인시던트에 대한 중요한 대응을 자동화하고 최초 대응 담당자에게 세부 단계를 제공할 수 있습니다.

참여 및 에스컬레이션

참여 계획에는 각 개별 인시던트에 대해 모든 사람에게 알리도록 명시되어 있습니다. Incident Manager에 추가한 개별 연락처를 지정하거나 Incident Manager에서 만든 대기 일정을 지정할 수 있습니다. 또한 참여 계획에는 에스컬레이션 경로가 지정되어 있어 이해 관계자가 상황을 파악하고 인시던트 대응 프로세스에 적극적으로 참여할 수 있습니다.

대기 일정

Incident Manager의 대기 일정은 해당 일정에 대해 생성한 하나 이상의 교대로 구성됩니다. 각 교대에 최대 30명의 연락처를 포함할 수 있습니다. 에스컬레이션 계획이나 대응 계획에 추가할 경우, 대기 일정은 대응 담당자의 개입이 필요한 인시던트 발생 시 알림을 받는 사람을 정의합니다. 대기 일정을 통해 인시던트 대응에 필요한 만큼 완전하고 중복된 연중무휴 지원을 받을 수 있습니다.

적극적인 협업

인시던트 대응 담당자는 채팅 애플리케이션 클라이언트에서 Amazon Q Developer와의 통합을 통해 인시던트에 적극적으로 대응합니다. 채팅 애플리케이션의 Amazon Q Developer는 Slack, Microsoft Teams또는 Amazon Chime을 사용하는 Incident Manager에 대한 채팅 채널 생성을 지원합니다. 대응 담당자는 서로 직접 통신하고, 인시던트에 대한 자동 알림을 수신하고, Slack 및 Microsoft Teams에서 일부 Incident Manager CLI(명령줄 인터페이스) 작업을 직접 실행할 수 있습니다.

인시던트 진단

대응 담당자는 인시던트 발생 중에 Incident Manager 콘솔에서 최신 정보를 볼 수 있습니다. 정보 변경에 따라 대응 담당자는 후속 조치를 만들고 자동화 런북을 사용하여 문제를 해결할 수 있습니다.

다른 서비스의 조사 결과

대응 담당자의 인시던트 진단을 지원하기 위해 Incident Manager에서 조사 결과 기능을 활성화할 수 있습니다. 조사 결과는 인시던트 발생 당시에 발생했고 인시던트와 관련이 있을 가능성이 있는 하나 이상의 리소스와 관련된 AWS CodeDeploy 배포 및 AWS CloudFormation 스택 업데이트에 대한 정보입니다. 이 정보가 있으면 잠재적 원인을 평가하는 데 필요한 시간이 줄어들어 인시던트의 평균 복구 시간(MTTR)을 줄일 수 있습니다.

인시던트 사후 분석

인시던트가 해결된 후 인시던트는 인시던트 사후 분석을 사용하여 탐지 시간 및 완화를 포함한 인시던트 대응에 대한 개선 사항을 식별합니다. 분석을 통해 인시던트의 근본 원인을 이해하는 데도 도움이 될 수 있습니다. Incident Manager는 인시던트 대응을 개선하는 데 사용할 수 있는 권장 후속 조치 항목을 생성합니다.

Incident Manager 사용의 이점

인시던트 탐지 및 대응 작업에서 Incident Manager를 사용하는 경우 얻을 수 있는 이점에 대해 알아봅니다.

이 섹션에서는 Incident Manager 대응 계획을 구현할 때 조직이 얻을 수 있는 이점에 대해 설명합니다.

문제를 효율적이고 즉각적으로 진단합니다.

구성한 Amazon CloudWatch 경보 및 Amazon EventBridge 이벤트는 예상치 못한 중단이나 서비스 품질 저하가 발생할 경우 자동으로 인시던트를 생성할 수 있습니다.

CloudWatch 경보는 여러 기간 동안 임계값과 지표 또는 표현식 값이 변경되는 경우 이를 감지하고 보고합니다. EventBridge 이벤트는 EventBridge 규칙에 지정한 환경, 애플리케이션 또는 서비스가 변경되면 생성됩니다. 경보 또는 이벤트를 생성할 때 Incident Manager에서 생성할 인시던트에 대한 조치와 적절한 대응 계획을 지정하여 인시던트의 참여, 에스컬레이션 및 완화를 촉진할 수 있습니다.

Incident Manager는 CloudWatch 지표를 사용하여 인시던트와 관련된 지표를 자동으로 수집하고 추적하는 기능을 제공합니다. CloudWatch 경보를 통해 인시던트를 생성할 때 인시던트에 대해 생성된 자동 지표 외에도 실시간으로 지표를 수동으로 추가하여 인시던트 대응 담당자에게 추가 컨텍스트와 데이터를 제공할 수 있습니다.

Incident Manager 인시던트 타임라인을 사용하여 관심 지점을 시간순으로 표시할 수 있습니다. 또한 대응 담당자는 타임라인을 사용하여 자신이 무엇을 했는지 또는 무슨 일이 일어났는지 설명하는 사용자 지정 이벤트를 추가할 수 있습니다. 자동화된 관심 지점에는 다음이 포함됩니다.

- CloudWatch 경보 또는 EventBridge 규칙이 인시던트를 생성합니다.
- 인시던트 지표는 Incident Manager에게 보고됩니다.
- 대응 담당자들이 참여하고 있습니다.
- 런북 단계가 성공적으로 완료되었습니다.

효과적인 참여

Incident Manager는 연락처, 대기 일정, 에스컬레이션 계획 및 채팅 채널을 사용하여 인시던트 대응 담당자를 하나로 모읍니다. Incident Manager에서 직접 개별 연락처를 정의하고 연락처 기본 설정(이메일, SMS 또는 음성)을 지정합니다. 대기 일정 교대에 연락처를 추가하여 지정된 기간 동안 인시던트 처리에 관여하는 사람을 결정할 수 있습니다. 정의된 연락처와 대기 일정을 사용하여 에스컬레이션 계획을 세워 인시던트 발생 시 필요한 대응 인력을 적시에 배치할 수 있습니다.

실시간 공동 작업

인시던트 발생 시 커뮤니케이션은 신속한 해결의 핵심입니다. Slack, Microsoft Teams또는 Amazon Chime을 사용하도록 설정된 채팅 애플리케이션 클라이언트에서 Amazon Q Developer를 사용하면 선호하는 연결 채팅 채널에서 대응 담당자가 인시던트 및 서로 직접 상호 작용할 수 있습니다. 또한 Incident Manager는 채팅 채널에 인시던트 대응 담당자의 실시간 작업을 표시하여 다른 사람에게 컨텍스트를 제공합니다.

서비스 복원 자동화

Incident Manager를 사용하면 대응 담당자가 자동화 런북을 사용하여 인시던트를 해결하는 데 필요한 주요 작업에 집중할 수 있습니다. Incident Manager에서 런북은 인시던트를 해결하기 위해 취해진 사전 정의된 일련의 조치입니다. 자동화된 작업의 기능과 필요에 따른 수동 단계를 결합하여 대응 담당자가 영향을 분석하고 이에 대응할 수 있는 역량을 강화할 수 있습니다.

향후 인시던트 예방

Incident Manager를 사용하여 인시던트 분석을 게시하면 팀에서 보다 강력한 대응 계획을 개발하고 애플리케이션 전반에 변경 사항을 적용하여 향후 인시던트 및 가동 중지 시간을 방지할 수 있습니다. 또한 인시던트 사후 분석을 통해 런북, 대응 계획 및 지표를 반복적으로 학습하고 개선할 수 있습니다.

관련 서비스

Incident Manager는 여러 다른 AWS 서비스 및 타사 서비스 및 도구와 통합되어 인시던트를 감지 및 해결하고 API 작업과 간접적으로 상호 작용하고 인프라를 관리하는 데 도움이 됩니다. 자세한 내용은 Incident Manager와 제품 및 서비스 통합을 참조하세요.

Incident Manager 액세스

다음 방법 중 하나를 사용하여 Incident Manager에 액세스할 수 있습니다.

- Incident Manager 콘솔

- AWS CLI – 자세한 내용은 AWS Command Line Interface 사용 설명서에서 AWS CLI시작하기를 참조하세요. Incident Manager의 CLI 명령에 대한 자세한 내용은 AWS CLI 명령 참조서의 ssm-incidents 및 ssm-contacts를 참조하세요.
- Incident Manager API – 자세한 내용은 AWS Systems Manager Incident Manager API 참조서를 참조하세요.
- AWS SDKs- 자세한 내용은 빌드 기반 도구를 AWS 참조하세요.

Incident Manager 리전 및 할당량

Incident Manager는 Systems Manager에서 지원하는 모든에서 AWS 리전 지원되지 않습니다.

Incident Manager 리전 및 할당량에 대한 자세한 내용은 Amazon Web Services 일반 참조의 AWS Systems Manager Incident Manager 엔드포인트 및 할당량을 참조하세요.

Incident Manager 요금

Incident Manager를 사용하면 사용료가 부과됩니다. 자세한 내용은 AWS Systems Manager 가격을 참조하세요.

> **Note**
>
> 이 서비스와 관련하여 제공되는 기타 콘텐츠, AWS 서비스 AWS 콘텐츠 및 타사 콘텐츠에는 별도의 요금이 부과될 수 있으며 추가 약관이 적용될 수 있습니다.

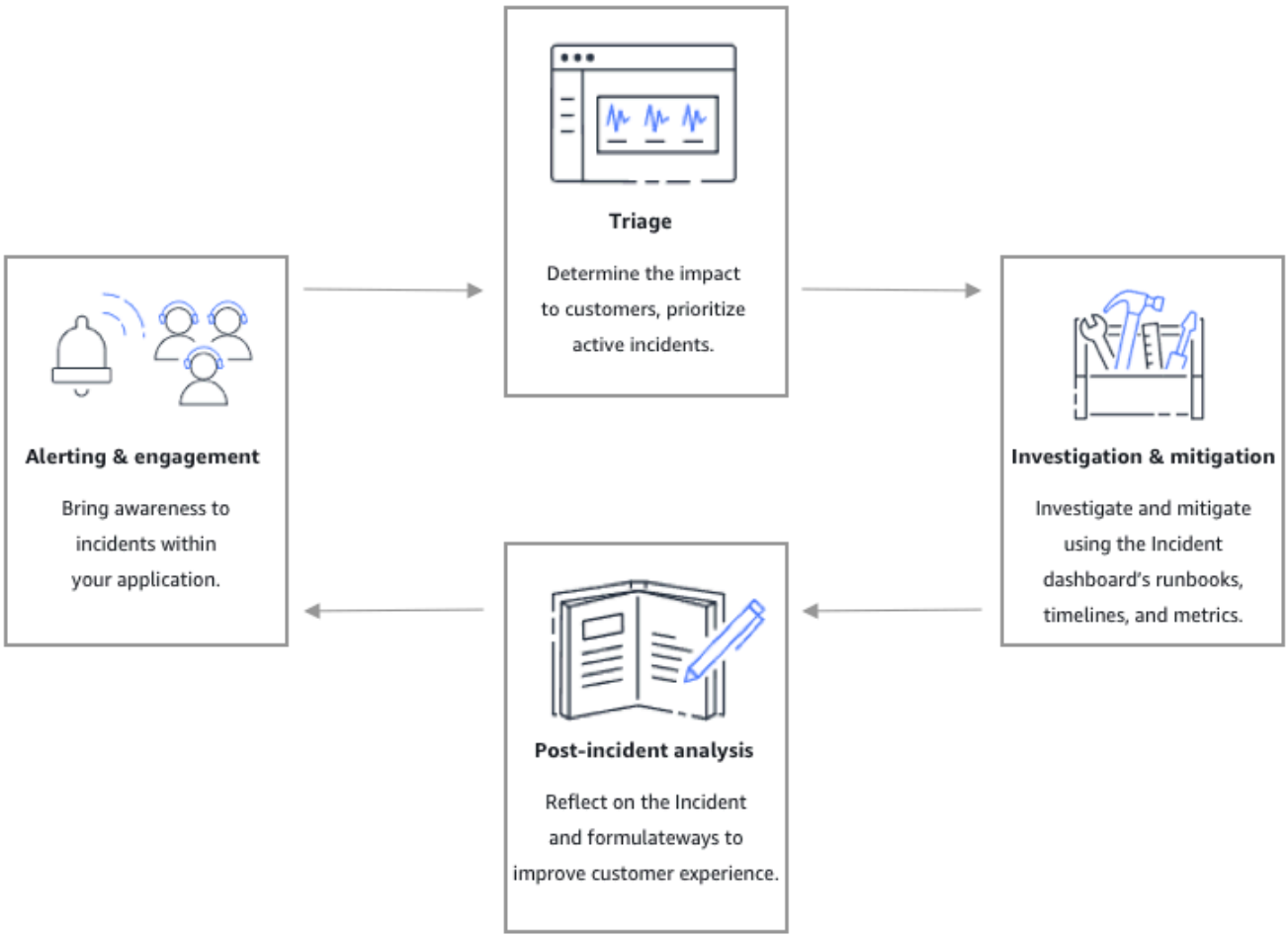
AWS 환경의 비용 Trusted Advisor, 보안 및 성능을 최적화하는 데 도움이 되는 서비스에 대한 개요는 AWS Support 사용 설명서AWS Trusted Advisor의 섹션을 참조하세요.

Incident Manager의 인시던트 수명 주기

AWS Systems Manager Incident Manager 는 서비스 중단 또는 보안 위협과 같은 인시던트를 식별하고 이에 대응하기 위한 모범 사례를 기반으로 step-by-step 프레임워크를 제공합니다. Insident Manager의 주요 초점은 완전한 인시던트 라이프사이클 관리 솔루션을 통해 영향을 받는 서비스 또는 애플리케이션을 최대한 빨리 정상 상태로 복원할 수 있도록 지원하는 것입니다.

다음 그림과 같이 Incident Manager는 인시던트 수명 주기의 모든 단계에 대한 도구와 모범 사례를 제공합니다.

- 알림 및 참여
- 심사
- 조사 및 완화
- 인시던트 사후 분석



알림 및 참여

인시던트 라이프사이클의 알림 및 참여 단계는 애플리케이션 및 서비스 내에서 인시던트를 인지하는 데 중점을 둡니다. 이 단계는 인시던트가 감지되기 전에 시작되며 애플리케이션에 대한 깊은 이해가 필요합니다. Amazon CloudWatch 지표를 사용하여 애플리케이션의 성능에 대한 데이터를 모니터링하거나 Amazon EventBridge를 사용하여 다양한 소스, 애플리케이션 및 서비스의 알림을 집계할 수 있습니

다. 애플리케이션에 대한 모니터링을 설정한 후에는 과거 기준을 벗어나는 지표에 대해 경고를 보낼 수 있습니다. 모니터링 모범 사례에 대한 자세한 내용은 모니터링을 참조하세요.

대응 담당자의 인시던트 진단을 지원하기 위해 Incident Manager에서 조사 결과 기능을 활성화 할 수 있습니다. 조사 결과는 인시던트 발생 시점 즈음에 발생한 AWS CodeDeploy 배포 및 AWS CloudFormation 스택 업데이트에 대한 정보입니다. 이 정보가 있으면 잠재적 원인을 평가하는 데 필요한 시간이 줄어들어 인시던트의 평균 복구 시간(MTTR)을 줄일 수 있습니다.

이제 애플리케이션에서 인시던트를 모니터링하고 있으므로 인시던트 중에 사용할 인시던트 대응 계획을 정의할 수 있습니다. 대응 계획 생성에 대한 자세한 내용은 Incident Manager에서 대응 계획 생성 및 구성 섹션을 참조하세요. Amazon EventBridge 이벤트 또는 CloudWatch 경보는 대응 계획을 템플릿으로 사용하여 자동으로 인시던트를 생성할 수 있습니다. 인시던트 생성에 대한 자세한 내용은 Incident Manager에서 자동으로 또는 수동으로 인시던트 생성을 참조하세요.

대응 계획은 관련 에스컬레이션 계획 및 참여 계획을 수립하여 최초 대응 인력을 인시던트에 투입합니다. 에스컬레이션 계획 설정에 대한 자세한 내용은 에스컬레이션 계획 만들기 섹션을 참조하세요. 동시에 채팅 애플리케이션의 Amazon Q Developer는 채팅 채널을 사용하여 대응자에게 인시던트 세부 정보 페이지로 안내하는 알림을 보냅니다. 팀은 채팅 채널과 인시던트 세부 정보를 사용하여 의견을 교환하고 인시던트를 분류할 수 있습니다. Incident Manager의 채팅 채널 설정에 대한 자세한 내용은 작업 2: 채팅 애플리케이션에서 Amazon Q Developer에 채팅 채널 생성 섹션을 참조하세요.

심사

심사는 최초 대응 담당자가 고객에게 미치는 영향을 파악하는 것을 말합니다. Incident Manager 콘솔의 인시던트 세부 정보 보기는 대응 담당자가 인시던트를 평가하는 데 도움이 되는 타임라인과 지표를 제공합니다. 또한 인시던트의 영향을 평가하면 인시던트에 대한 대응 시간, 해결 및 커뮤니케이션을 위한 토대를 마련할 수 있습니다. 대응 담당자는 1(중요)에서 5(영향 없음)까지의 영향 등급을 사용하여 인시던트의 우선 순위를 정합니다.

조직은 원하는 대로 각 영향 등급의 정확한 범위를 정의할 수 있습니다. 다음 표에는 각 영향 수준이 일반적으로 정의되는 방법의 예가 나와 있습니다.

영향 코드	영향 이름	샘플 정의 범위
1	Critical	대부분의 고객에게 영향을 미치는 전체 애플리케이션 장애
2	High	일부 고객에게 영향을 미치는 전체 애플리케이션 장애

영향 코드	영향 이름	샘플 정의 범위
3	Medium	고객에게 발생하는 부분적인 애플리케이션 장애
4	Low	고객에게 제한적인 영향을 미치는 간헐적인 장애
5	No Impact	고객은 현재 영향을 받지 않지만 영향을 피하기 위해 긴급 조치가 필요합니다.

조사 및 완화

인시던트 세부 정보 보기는 팀에 런북, 타임라인 및 지표를 제공합니다. 인시던트 처리 방법을 알아보려면 콘솔에서 인시던트 세부 정보 보기 섹션을 참조하세요.

런북은 일반적으로 조사 단계를 제공하며 자동으로 데이터를 가져오거나 일반적으로 사용되는 솔루션을 시도할 수 있습니다. 또한 런북은 팀에서 인시던트를 완화하는 데 유용하다고 판단한 명확하고 반복 가능한 단계를 제공합니다. 런북 탭은 현재 런북 단계에 초점을 맞추고 과거 및 미래 단계를 보여줍니다.

Incident Manager는 Systems Manager 자동화와 통합되어 런북을 구축합니다. 런북을 사용하여 다음을 수행하십시오.

- 인스턴스 및 AWS 리소스 관리
- 스크립트 자동 실행
- AWS CloudFormation 리소스 관리

지원되는 작업 유형에 대한 자세한 내용은 AWS Systems Manager 사용 설명서의 Systems Manager 자동화 작업 참조를 참조하세요.

타임라인 탭에는 수행된 조치가 표시됩니다. 타임라인은 타임스탬프와 자동으로 생성된 세부 정보와 함께 각각을 기록합니다. 타임라인에 사용자 지정 이벤트를 추가하려면 이 사용 설명서의 인시던트 세부 정보 페이지에 있는 타임라인 섹션을 참조하세요.

진단 탭에는 자동으로 채워진 지표와 수동으로 추가한 지표가 표시됩니다. 이 뷰는 인시던트 발생 시 애플리케이션 활동에 대한 중요한 정보를 제공합니다.

참여 탭에서는 인시던트에 연락처를 추가할 수 있으며, 인시던트에 연루된 담당자가 신속하게 조치를 취할 수 있도록 리소스를 제공할 수 있습니다. 연락처는 정의된 에스컬레이션 계획 또는 개인 참여 계획을 통해 참여합니다.

채팅 채널을 사용하면 인시던트 및 팀의 다른 대응 담당자와 직접 대화할 수 있습니다. 채팅 애플리케이션에서 Amazon Q Developer를 사용하면 , Slack Microsoft Teams및 Amazon Chime에서 채팅 채널을 구성할 수 있습니다. Slack 및 Microsoft Teams 채널에서 대응 담당자는 여러 `ssm-incidents` 명령을 사용하여 채팅 채널에서 직접 인시던트와 상호 작용할 수 있습니다. 자세한 내용은 채팅 채널을 통한 상호작용 단원을 참조하십시오.

인시던트 사후 분석

Insident Manager는 인시던트를 반영하고, 향후 인시던트가 다시 발생하지 않도록 방지하는 데 필요한 조치를 취하고, 인시던트 대응 활동을 전반적으로 개선하기 위한 프레임워크를 제공합니다. 개선 사항에는 다음이 포함됩니다.

- 인시던트와 관련된 애플리케이션 변경. 팀은 이 시간을 활용하여 시스템을 개선하고 내결함성을 높일 수 있습니다.
- 인시던트 대응 계획 변경. 시간을 내어 학습한 교훈을 통합하십시오.
- 런북에 대한 변경. 팀에서 해결에 필요한 단계와 자동화할 수 있는 단계를 자세히 알아볼 수 있습니다.
- 알림 변경. 인시던트가 발생한 후 팀에 인시던트를 더 빨리 알리는 데 사용할 수 있는 지표에서 중요한 포인트를 발견했을 수도 있습니다.

Insident Manager는 인시던트 타임라인과 함께 일련의 인시던트 사후 분석 질문 및 조치 항목을 사용하여 이러한 잠재적 개선을 촉진합니다. 분석을 통한 개선에 대해 자세히 알아보려면 Incident Manager에서 인시던트 사후 분석 수행 섹션을 참조하세요.

AWS Systems Manager Incident Manager 설정

작업을 관리하는 데 사용하는 계정에서 AWS Systems Manager Incident Manager를 설정하는 것이 좋습니다. Incident Manager를 처음 사용한다면 먼저 다음 작업을 완료해야 합니다.

주제

에 가입 AWS 계정

이 없는 경우 다음 단계를 AWS 계정완료하여 생성합니다.

에 가입하려면 AWS 계정

1. https://portal.aws.amazon.com/billing/signup을 엽니다.
2. 온라인 지시 사항을 따릅니다.

   가입 절차의 일부로는 전화 또는 문자 메시지를 수신하고 전화 키패드에 확인 코드를 입력하는 것이 포함됩니다.

   에 가입하면 AWS 계정AWS 계정 루트 사용자이 생성됩니다. 루트 사용자에게는 계정의 모든 AWS 서비스 및 리소스에 액세스할 권한이 있습니다. 보안 모범 사례는 사용자에게 관리 액세스 권한을 할당하고, 루트 사용자만 사용하여 루트 사용자 액세스 권한이 필요한 작업을 수행하는 것입니다.

AWS 는 가입 프로세스가 완료된 후 확인 이메일을 보냅니다. 언제든지 https://aws.amazon.com/으로 이동하고 내 계정을 선택하여 현재 계정 활동을 보고 계정을 관리할 수 있습니다.

관리자 액세스 권한이 있는 사용자 생성

에 가입한 후 일상적인 작업에 루트 사용자를 사용하지 않도록 관리 사용자를 AWS 계정보호 AWS IAM Identity Center, AWS 계정 루트 사용자활성화 및 생성합니다.

보안 AWS 계정 루트 사용자

1. 루트 사용자를 선택하고 AWS 계정 이메일 주소를 입력하여 계정 소유자AWS Management Console로에 로그인합니다. 다음 페이지에서 비밀번호를 입력합니다.

   루트 사용자를 사용하여 로그인하는 데 도움이 필요하면 AWS 로그인 User Guide의 루트 사용자로 로그인을 참조하세요.
2. 루트 사용자의 다중 인증(MFA)을 활성화합니다.

   지침은 IAM 사용 설명서의 AWS 계정 루트 사용자(콘솔)에 대한 가상 MFA 디바이스 활성화를 참조하세요.

관리자 액세스 권한이 있는 사용자 생성

1. IAM Identity Center를 활성화합니다.

   지침은 AWS IAM Identity Center 사용 설명서의 AWS IAM Identity Center설정을 참조하세요.
2. IAM Identity Center에서 사용자에게 관리 액세스 권한을 부여합니다.

   를 자격 증명 소스 IAM Identity Center 디렉터리 로 사용하는 방법에 대한 자습서는 사용 AWS IAM Identity Center 설명서의 기본값으로 사용자 액세스 구성을 IAM Identity Center 디렉터리 참조하세요.

관리 액세스 권한이 있는 사용자로 로그인

- IAM IDentity Center 사용자로 로그인하려면 IAM Identity Center 사용자를 생성할 때 이메일 주소로 전송된 로그인 URL을 사용합니다.

  IAM Identity Center 사용자를 사용하여 로그인하는 데 도움이 필요하면 AWS 로그인 사용 설명서의 AWS 액세스 포털에 로그인을 참조하세요.

추가 사용자에게 액세스 권한 할당

1. IAM Identity Center에서 최소 권한 적용 모범 사례를 따르는 권한 세트를 생성합니다.

   지침은AWS IAM Identity Center 사용 설명서의 Create a permission set를 참조하세요.
2. 사용자를 그룹에 할당하고, 그룹에 Single Sign-On 액세스 권한을 할당합니다.

   지침은 AWS IAM Identity Center 사용 설명서의 Add groups를 참조하세요.

프로그래밍 방식 액세스 권한 부여

사용자는 AWS 외부에서와 상호 작용하려는 경우 프로그래밍 방식으로 액세스해야 합니다 AWS Management Console. 프로그래밍 방식 액세스를 부여하는 방법은에 액세스하는 사용자 유형에 따라 다릅니다 AWS.

사용자에게 프로그래밍 방식 액세스 권한을 부여하려면 다음 옵션 중 하나를 선택합니다.

프로그래밍 방식 액세스가 필요한 사용자는 누구인가요?	To	액세스 권한을 부여하는 사용자
작업 인력 ID (IAM Identity Center가 관리하는 사용자)	임시 자격 증명을 사용하여 AWS CLI, AWS SDKs 또는 AWS APIs.	사용하고자 하는 인터페이스에 대한 지침을 따릅니다. • 자세한 AWS CLI내용은 AWS Command Line Interface 사용 설명서의 AWS CLI 를 사용하도록 구성을 AWS IAM Identity Center 참조하세요. • AWS SDKs, 도구 및 AWS APIs의 경우 SDK 및 도구 참조 안내서의 IAM Identity Center 인증을 참조하세요. AWS SDKs
IAM	임시 자격 증명을 사용하여 AWS CLI, AWS SDKs 또는 AWS APIs.	IAM 사용 설명서의 AWS 리소스에서 임시 자격 증명 사용의 지침을 따릅니다.
IAM	(권장되지 않음) 장기 자격 증명을 사용하여 AWS CLI, AWS SDKs 또는 AWS APIs.	사용하고자 하는 인터페이스에 대한 지침을 따릅니다. • 자세한 AWS CLI내용은 AWS Command Line Interface 사용 설명서의 IAM 사용자 자격 증명을 사용하여 인증을 참조하세요.

프로그래밍 방식 액세스가 필요한 사용자는 누구인가요?	To	액세스 권한을 부여하는 사용자
		• AWS SDKs 및 도구의 경우 SDK 및 도구 참조 안내서의 장기 자격 증명을 사용하여 인증을 참조하세요. AWS SDKs • AWS APIs 경우 IAM 사용 설명서의 IAM 사용자의 액세스 키 관리를 참조하세요.

Incident Manager 설정에 필요한 역할

시작에 앞서 계정에 IAM 권한 `iam:CreateServiceLinkedRole`이 있어야 합니다. Incident Manager는 이 권한을 사용하여 계정에 `AWSServiceRoleforIncidentManager`를 생성합니다. 자세한 내용은 Incident Manager의 서비스 연결 역할 단원을 참조하십시오.

Incident Manager 시작하기

이 섹션에서는 Incident Manager 콘솔에서 준비하는 과정을 안내합니다. 인시던트 관리에 사용하려면 먼저 콘솔에서 준비하기를 완료해야 합니다. 마법사는 복제 세트, 최소 하나의 연락처 및 하나의 에스컬레이션 계획, 첫 번째 대응 계획을 설정하는 과정을 안내합니다. 다음 설명서는 Incident Manager와 인시던트 라이프사이클을 이해하는 데 도움이 됩니다.

- 란 무엇인가요 AWS Systems Manager Incident Manager?
- Incident Manager의 인시던트 수명 주기

사전 조건

Incident Manager를 처음 사용하는 경우 AWS Systems Manager Incident Manager 설정을 참조하세요. 작업을 관리하는 데 사용하는 계정에서 Incident Manager를 설정하는 것이 좋습니다.

Incident Manager 준비 마법사를 시작하기 전에 Systems Manager 빠른 설치를 완료하는 것이 좋습니다. 을 사용하여 권장되는 모범 사례에 따라 자주 사용하는 서비스 및 기능을 구성합니다. Incident Manager는 Systems Manager 기능을 사용하여와 관련된 인시던트 AWS 계정 를 관리하고 Systems Manager를 먼저 구성하면 얻을 수 있는 이점을 제공합니다.

준비하기 마법사

Incident Manager를 처음 사용하는 경우 Incident Manager 서비스 홈 페이지에서 준비 마법사에 액세스할 수 있습니다. 설정을 처음 완료한 후 준비 마법사에 액세스하려면 인시던트 목록 페이지에서 준비를 선택합니다.

1. Incident Manager 콘솔을 엽니다.
2. Incident Manager 서비스 홈페이지에서 준비를 선택합니다.

일반 설정

1. 일반 설정에서 파일을 선택합니다.
2. Terms and Conditions(이용 약관)를 모두 읽어보세요. Incident Manager의 이용 약관에 동의하는 경우, Incident Manager 이용 약관을 읽었으며 이에 동의합니다를 선택한 후 다음을 선택합니다.
3. 리전 영역에서 현재는 복제 세트의 첫 번째 리전으로 AWS 리전 표시됩니다. 복제 세트에 더 많은 리전을 추가하려면 리전 목록에서 리전을 선택합니다.

두 개 이상의 리전을 포함하는 것이 좋습니다. 한 리전을 일시적으로 사용할 수 없는 경우에도 인시던트 관련 활동을 다른 리전으로 라우팅할 수 있습니다.

> **Note**
>
> 복제 세트를 생성하면 사용자 계정에서 `AWSServiceRoleforIncidentManager` 서비스 연결 역할이 생성됩니다. 이 역할에 대한 자세한 내용은 Incident Manager의 서비스 연결 역할 섹션을 참조하세요.

4. 복제 세트에 대해 암호화를 설정하려면 다음 중 하나를 수행합니다.

> **Note**
>
> 모든 Incident Manager 리소스는 암호화됩니다. 데이터 암호화 방법에 대해 자세히 알아보려면 Incident Manager의 데이터 보호 섹션을 참조하세요. Incident Manager 복제 세트에 대한 자세한 내용은 Incident Manager 복제 세트 구성 섹션을 참조하세요.

- AWS 소유 키를 사용하려면 AWS 소유 키 사용을 선택합니다.
- 자체 AWS KMS 키를 사용하려면 기존 선택을 선택합니다 AWS KMS key. 3단계에서 선택한 각 리전에 대해 AWS KMS 키를 선택하거나 AWS KMS Amazon 리소스 이름(ARN)을 입력합니다.

> **Tip**
>
> 사용 가능한이 없는 경우 생성을 AWS KMS key AWS KMS key선택합니다.

5. (선택 사항) 태그 영역에서 복제 세트에 대해 하나 이상의 태그를 추가합니다. 태그에는 키가 포함되고, 필요한 경우 값도 포함됩니다.

   태그는 리소스에 할당하는 선택적 메타데이터입니다. 태그를 사용하면 용도, 소유자 또는 환경을 기준으로 하는 등 리소스를 다양한 방식으로 분류할 수 있습니다. 자세한 내용은 Incident Manager의 리소스 태깅 단원을 참조하십시오.

6. (선택 사항) 서비스 액세스 영역의 조사 결과 기능을 활성화하려면 이 계정의 조사 결과에 대한 서비스 역할 생성 확인란을 선택합니다.

   조사 결과는 인시던트가 생성된 시기와 거의 같은 시기에 발생한 코드 배포 또는 인프라 변경에 대한 정보입니다. 조사 결과를 인시던트의 잠재적 원인으로 조사할 수 있습니다. 이러한 잠재적 원인

에 대한 정보는 해당 인시던트의 인시던트 세부 정보 페이지에 추가됩니다. 이러한 배포 및 변경 사항에 대한 정보를 쉽게 확인할 수 있으므로 대응 담당자가 이 정보를 수동으로 검색할 필요가 없습니다.

> **Tip**
>
> 생성할 역할에 대한 정보를 보려면 권한 세부 정보 보기를 선택합니다.

7. 생성(Create)을 선택합니다.

   복제 세트 및 복원력에 대한 자세한 내용은 의 복원력 AWS Systems Manager Incident Manager 섹션을 참조하세요.

연락처(준비 중 선택 사항)

인시던트 중 Incident Manager가 연락처를 참여시킵니다. 연락처에 대한 자세한 내용은 Incident Manager에서 연락처 생성 및 구성 섹션을 참조하세요.

1. 연락처 생성을 선택합니다.
2. 이름에 연락처 이름을 입력합니다.
3. 고유 별칭에 이 연락처를 식별하는 별칭을 입력합니다.
4. 연락처 채널 섹션에서 다음을 수행하여 인시던트 발생 시 연락처가 참여하는 방식을 정의하십시오.

   a. 유형에서 이메일, SMS 또는 음성을 선택합니다.
   b. 채널 이름에서 채널을 식별하는 데 도움이 되는 고유한 이름을 입력합니다.
   c. 세부 정보에서 연락처의 이메일 주소 또는 전화 번호를 입력합니다.

      전화번호는 9~15자여야 하고 +로 시작하고 그 뒤에 국가 코드와 가입자 번호가 와야 합니다.

   d. 다른 고객 응대 채널을 생성하려면 고객 응대 채널 추가를 선택합니다. 각 연락처에 대해 채널을 두 개 이상 정의하는 것이 좋습니다.
5. 참여 계획 영역에서 다음을 수행하여 연락처에 알릴 채널과 각 채널을 통해 확인을 기다리는 시간을 정의하십시오.

> **Note**
>
> 참여 계획에서 채널을 두 개 이상 정의하는 것이 좋습니다.

a. 연락처 채널 이름에 대해 연락처 채널 영역에서 지정한 채널을 선택합니다.

b. 참여 시간(분)에는 연락처 채널을 참여시키기 전에 대기할 시간(분)을 입력합니다.

   참여 시작 시 참여할 디바이스를 하나 이상 선택하고 대기 시간을 **0**(0)분으로 지정하는 것이 좋습니다.

c. 참여 계획에 연락처 채널을 더 추가하려면 참여 추가를 선택합니다.

6. (선택 사항) 태그 영역에서 연락처에 대해 하나 이상의 태그를 추가합니다. 태그에는 키가 포함되고, 필요한 경우 값도 포함됩니다.

   태그는 리소스에 할당하는 선택적 메타데이터입니다. 태그를 사용하면 용도, 소유자 또는 환경을 기준으로 하는 등 리소스를 다양한 방식으로 분류할 수 있습니다. 자세한 내용은 Incident Manager의 리소스 태깅 단원을 참조하십시오.

7. 고객 응대 레코드를 생성하고 정의된 고객 응대 채널로 활성화 코드를 보내려면 생성을 선택합니다.

8. (선택 사항) 연락처 채널 활성화 페이지에서 각 채널로 전송된 활성화 코드를 입력합니다.

   지금 코드를 입력할 수 없는 경우 나중에 새 활성화 코드를 생성할 수 있습니다.

9. 연락처를 추가하려면 연락처 생성을 선택하고 이전 단계를 반복합니다.

(준비 중 선택 사항) 에스컬레이션 계획

1. 에스컬레이션 계획 생성을 선택합니다.

   에스컬레이션 계획은 인시던트 발생 시 연락처를 통해 에스컬레이션되므로 Incident Manager가 인시던트 발생 시 올바른 대응 담당자를 참여시킬 수 있습니다. 에스컬레이션 계획에 대한 자세한 내용은 Incident Manager에서 대응자 참여를 위한 에스컬레이션 계획 생성 섹션을 참조하세요.

2. 이름에 에스컬레이션 계획의 고유한 이름을 입력합니다.

3. 별칭에 에스컬레이션 계획을 식별하는 데 도움이 되는 고유한 별칭을 입력합니다.

4. 1단계 영역에서 다음을 수행합니다.

   a. 에스컬레이션 채널에서 참여할 연락 채널을 선택합니다.

   b. 담당자가 에스컬레이션 계획 단계의 진행을 중단할 수 있게 하려면 승인이 계획 진행 중지를 선택합니다.

   c. 단계에 채널을 더 추가하려면 에스컬레이션 채널 추가를 선택합니다.

5. 에스컬레이션 계획에 새 단계를 만들려면 단계 추가를 선택하고 단계 세부 정보를 추가합니다.
6. (선택 사항) 태그 영역에서 에스컬레이션 계획에 대해 하나 이상의 태그를 추가합니다. 태그에는 키가 포함되고, 필요한 경우 값도 포함됩니다.

   태그는 리소스에 할당하는 선택적 메타데이터입니다. 태그를 사용하면 용도, 소유자 또는 환경을 기준으로 하는 등 리소스를 다양한 방식으로 분류할 수 있습니다. 자세한 내용은 Incident Manager의 리소스 태깅 단원을 참조하십시오.
7. 에스컬레이션 계획 생성을 선택합니다.

대응 계획

> **Note**
>
> Incident Manager 시작 페이지로 돌아가서 준비를 선택하여 계속해야 할 수 있습니다.

1. 대응 계획 생성을 선택합니다.

   대응 계획을 사용하여 만들어둔 연락처와 에스컬레이션 계획을 통합합니다.

   특히 대응 계획을 처음 설정하는 경우에는 이 시작하기 마법사의 다음 섹션은 선택 사항입니다.

   - 채팅 채널
   - 런북
   - 참여
   - 서드 파티 통합

   나중에 이러한 요소를 대응 계획에 추가하는 방법에 대한 자세한 내용은 Incident Manager에서 인시던트 준비 섹션을 참조하세요.
2. 이름에 대응 계획의 고유한 이름을 입력합니다. 이름은 대응 계획 ARN을 생성하는데 사용되거나 표시 이름이 없는 대응 계획에 사용됩니다.
3. (선택 사항) 표시 이름에는 인시던트를 생성할 때 이 대응 계획을 식별하는 데 도움이 되는 이름을 입력합니다.
4. 제목에는 이 대응 계획과 관련된 인시던트 유형을 식별하는 데 도움이 되는 제목을 입력합니다.

지정하는 값은 각 인시던트의 제목에 포함됩니다. 인시던트를 시작한 경보 또는 이벤트도 제목에 추가됩니다.

5. 영향에서 이 대응 계획과 관련된 인시던트에 대해 예상하는 영향 수준(예: **Critical** 또는 **Low**)을 선택합니다.
6. (선택 사항) 요약에는 인시던트의 개요를 제공하는 데 사용되는 간략한 설명을 입력합니다. Incident Manager는 인시던트 중에 관련 정보를 요약에 자동으로 채웁니다.
7. (선택 사항) 중복 제거 문자열에는 중복 제거 문자열을 입력합니다. Incident Manager는 이 문자열을 사용하여 동일한 계정에서 동일한 근본 원인으로 인해 여러 인시던트가 생성되는 것을 방지합니다.

   중복 제거 문자열은 시스템에서 중복 인시던트를 확인하는 데 사용하는 용어 또는 문구입니다. 중복 제거 문자열을 지정하는 경우 Incident Manager는 인시던트를 생성할 때 `dedupeString` 필드에 동일한 문자열이 포함된 미해결 인시던트를 검색합니다. 중복이 감지되면 Incident Manager는 새 인시던트의 중복을 기존 인시던트에서 제거합니다.

   > **Note**
   >
   > 기본적으로 Incident Manager는 동일한 Amazon CloudWatch 경보 또는 Amazon EventBridge 이벤트로 생성된 여러 인시던트의 중복을 자동으로 제거합니다. 이러한 리소스 유형의 중복을 방지하기 위해 중복 제거 문자열을 직접 입력할 필요는 없습니다.

8. (선택 사항) 인시던트 태그 영역에서 대응 계획에 하나 이상의 태그를 추가합니다. 태그에는 키가 포함되고, 필요한 경우 값도 포함됩니다.

   태그는 리소스에 할당하는 선택적 메타데이터입니다. 태그를 사용하면 용도, 소유자 또는 환경을 기준으로 하는 등 리소스를 다양한 방식으로 분류할 수 있습니다. 자세한 내용은 Incident Manager의 리소스 태깅 단원을 참조하십시오.
9. 참여 드롭다운에서 인시던트에 적용할 연락처 및 에스컬레이션 계획을 선택합니다.
10. 대응 계획 생성을 선택합니다.

대응 계획을 생성한 후 Amazon CloudWatch 경보 또는 Amazon EventBridge 이벤트를 대응 계획과 연결할 수 있습니다. 이렇게 하면 경보 또는 이벤트를 기반으로 인시던트가 자동으로 생성됩니다. 자세한 내용은 Incident Manager에서 자동으로 또는 수동으로 인시던트 생성 단원을 참조하십시오.

Incident Manager에서 AWS 계정 및 리전 간 인시던트 관리

의 도구인 Incident Manager가 여러 AWS 리전 및 계정에서 작동 AWS Systems Manager하도록 구성할 수 있습니다. 이 섹션에서는 크로스 리전 및 크로스 계정 모범 사례, 설정 단계, 알려진 제한 사항에 대해 설명합니다.

주제

크로스 리전 인시던트 관리

Incident Manager는 여러 AWS 리전에서 자동 및 수동 인시던트 생성을 지원합니다. 준비하기 마법사를 사용하여 Incident Manager에 처음 온보딩할 때는 복제 세트에 최대 3개까지 AWS 리전 을 지정할 수 있습니다. Amazon CloudWatch 경보 또는 Amazon EventBridge 이벤트에 의해 자동으로 생성된 인시던트의 경우 Incident Manager는 이벤트 규칙 또는 경보 AWS 리전 와 동일한에서 인시던트를 생성하려고 시도합니다. Incident Manager가 해당 리전에서 중단되는 경우 CloudWatch 또는 EventBridge는 데이터가 복제되는 다른 리전에 인시던트를 자동으로 생성합니다.

> **Important**
>
> 다음과 같은 중요 세부 정보에 주의합니다.
>
> - 복제 세트 AWS 리전 에 2개 이상을 지정하는 것이 좋습니다. 리전을 두 개 이상 지정하지 않으면 Incident Manager를 사용할 수 없는 기간 동안 시스템에서 인시던트를 생성하지 못합니다.
> - 크로스 리전 장애 조치로 생성된 인시던트는 대응 계획에 지정된 런북을 호출하지 않습니다.

Incident Manager 온보딩 및 추가 리전 지정에 대한 자세한 내용은 Incident Manager 시작하기를 참조하세요.

크로스 계정 인시던트 관리

Incident Manager는 AWS Resource Access Manager (AWS RAM)를 사용하여 관리 및 애플리케이션 계정 간에 Incident Manager 리소스를 공유합니다. 이 섹션에서는 크로스 계정 모범 사례, Incident

Manager의 크로스 계정 기능을 설정하는 방법, Incident Manager의 크로스 계정 기능에 대한 알려진 제한 사항에 대해 설명합니다.

관리 계정은 운영 관리를 수행하는 데 사용하는 계정입니다. 조직 설정에서 관리 계정은 대응 계획, 연락처, 에스컬레이션 계획, 실행서 및 기타 AWS Systems Manager 리소스를 소유합니다.

애플리케이션 계정은 애플리케이션을 구성하는 리소스를 소유하고 있는 계정입니다. 이러한 리소스는 Amazon EC2 인스턴스, Amazon DynamoDB 테이블 또는 AWS 클라우드에서 애플리케이션을 구축하는 데 사용하는 기타 리소스일 수 있습니다. 또한 애플리케이션 계정은 Incident Manager에서 인시던트를 생성하는 Amazon CloudWatch 경보 및 Amazon EventBridge 이벤트를 소유합니다.

AWS RAM 는 리소스 공유를 사용하여 계정 간에 리소스를 공유합니다. AWS RAM에서 계정 간에 대응 계획 및 연락처 리소스를 공유할 수 있습니다. 이러한 리소스를 공유하면 애플리케이션 계정과 관리 계정이 참여 및 인시던트와 상호 작용할 수 있습니다. 대응 계획을 공유하면 해당 대응 계획을 사용하여 생성된 모든 과거 및 미래 인시던트를 공유할 수 있습니다. 연락처를 공유하면 연락처 또는 대응 계획의 모든 과거 및 미래 참여가 공유됩니다.

모범 사례

여러 계정에서 Incident Manager 리소스를 공유할 때는 다음 모범 사례를 따르십시오.

- 대응 계획 및 연락처와 함께 리소스 공유를 정기적으로 업데이트하세요.
- 리소스 공유 보안 주체를 정기적으로 검토하세요.
- 관리 계정에서 Incident Manager, 런북, 채팅 채널을 설정하세요.

크로스 계정 인시던트 관리를 설정 및 구성합니다.

다음 단계에서는 Incident Manager 리소스를 설정 및 구성하고 이를 크로스 계정 기능에 사용하는 방법을 설명합니다. 과거에 크로스 계정 기능을 위해 일부 서비스와 리소스를 구성했을 수 있습니다. 크로스 계정 리소스를 사용하여 첫 번째 인시던트를 시작하기 전에 다음 단계를 요구 사항 체크리스트로 활용하세요.

1. (선택 사항)를 사용하여 조직 및 조직 단위를 생성합니다 AWS Organizations. AWS Organizations 사용 설명서의 자습서: 조직 생성 및 구성의 단계를 수행합니다.
2. (선택 사항)의 도구인 빠른 설정을 사용하여 교차 계정 런북을 구성할 때 사용할 올바른 AWS Identity and Access Management 역할을 AWS Systems Manager설정합니다. 자세한 내용은 AWS Systems Manager 사용 설명서의 빠른 설정을 참조하세요.

3. AWS Systems Manager 사용 설명서의 여러 AWS 리전 및 계정에서 자동화 실행에 나열된 단계에 따라 Systems Manager 자동화 문서에서 런북을 생성합니다. 런북은 관리 계정 또는 애플리케이션 계정 중 하나로 실행할 수 있습니다. 사용 사례에 따라 인시던트 중에 런북을 생성하고 보는 데 필요한 역할에 적합한 AWS CloudFormation 템플릿을 설치해야 합니다.

   - 관리 계정에서 런북 실행 관리 계정은 AWS-SystemsManager-AutomationReadOnlyRole CloudFormation 템플릿을 다운로드하고 설치해야 합니다. AWS-SystemsManager-AutomationReadOnlyRole 설치 시 모든 애플리케이션 계정의 계정 ID를 지정하십시오. 이 역할을 통해 애플리케이션 계정은 인시던트 세부 정보 페이지에서 런북의 상태를 읽을 수 있습니다. 애플리케이션 계정이 AWS-SystemsManager-AutomationAdministrationReadOnlyRole CloudFormation 템플릿을 설치해야 합니다. 인시던트 세부 정보 페이지는 이 역할을 사용하여 관리 계정으로부터 자동화 상태를 가져옵니다.
   - 애플리케이션 계정에서 런북 실행. 관리 계정은 AWS-SystemsManager-AutomationAdministrationReadOnlyRole CloudFormation 템플릿을 다운로드하고 설치해야 합니다. 이 역할을 통해 관리 계정은 애플리케이션 계정의 런북 상태를 읽을 수 있습니다. 애플리케이션 계정이 AWS-SystemsManager-AutomationReadOnlyRole CloudFormation 템플릿을 다운로드하고 설치해야 합니다. `AWS-SystemsManager-AutomationReadOnlyRole` 설치 시 관리 계정 및 다른 애플리케이션 계정의 계정 ID를 사용해야 합니다. 관리 계정과 다른 애플리케이션 계정이 이 역할을 수임하여 런북의 상태를 읽습니다.

4. (선택 사항) 조직의 각 애플리케이션 계정에서 AWS-SystemsManager-IncidentManagerIncidentAccessServiceRole CloudFormation 템플릿을 다운로드하고 설치합니다. AWS-SystemsManager-IncidentManagerIncidentAccessServiceRole 설치 시 관리 계정의 계정 ID를 지정합니다. 이 역할은 Incident Manager가 배포 및 AWS CloudFormation 스택 업데이트에 대한 AWS CodeDeploy 정보에 액세스하는 데 필요한 권한을 제공합니다. 조사 결과 기능이 활성화된 경우 이 정보가 인시던트에 대한 조사 결과로 보고됩니다. 자세한 내용은 Incident Manager에서 다른 서비스의 잠재적 인시던트 원인을 "결과"로 식별 단원을 참조하십시오.

5. 연락처, 에스컬레이션 계획, 채팅 채널, 대응 계획을 설정하고 생성하려면 Incident Manager에서 인시던트 준비에 설명된 단계를 따르세요.

6. AWS RAM에서 연락처 및 대응 계획 리소스를 기존 리소스 공유 또는 새 리소스 공유에 추가합니다. 자세한 내용은 AWS RAM 사용 설명서의 AWS RAM시작하기를 참조하세요. 에 대응 계획을 추가 AWS RAM 하면 애플리케이션 계정이 대응 계획을 사용하여 생성된 인시던트 및 인시던트 대시보드에 액세스할 수 있습니다. 또한 애플리케이션 계정은 CloudWatch 경보 및 EventBridge 이벤트를 대응 계획에 연결할 수 있게 됩니다. 고객 응대 및 에스컬레이션 계획을 추가하여 애플리케이션 계정이 인시던트 대시보드에서 참여를 보고 고객 응대를 참여할 수 AWS RAM 있도록 합니다.

7. CloudWatch 콘솔에 크로스 계정 크로스 리전 기능을 추가합니다. 단계 및 자세한 내용은 Amazon CloudWatch 사용 설명서의 크로스 계정 크로스 리전 CloudWatch 콘솔을 참조하세요. 이 기능을 추가하면 생성한 애플리케이션 계정과 관리 계정이 인시던트 및 분석 대시보드에서 지표를 보고 편집할 수 있습니다.
8. 크로스 계정 Amazon EventBridge 이벤트 버스를 생성합니다. 단계 및 정보는 AWS 계정 간 Amazon EventBridge 이벤트 전송 및 수신을 참조하세요. 그런 다음 이 이벤트 버스를 사용하여 애플리케이션 계정에서 인시던트를 탐지하고 관리 계정에서 인시던트를 생성하는 이벤트 규칙을 생성할 수 있습니다.

제한 사항

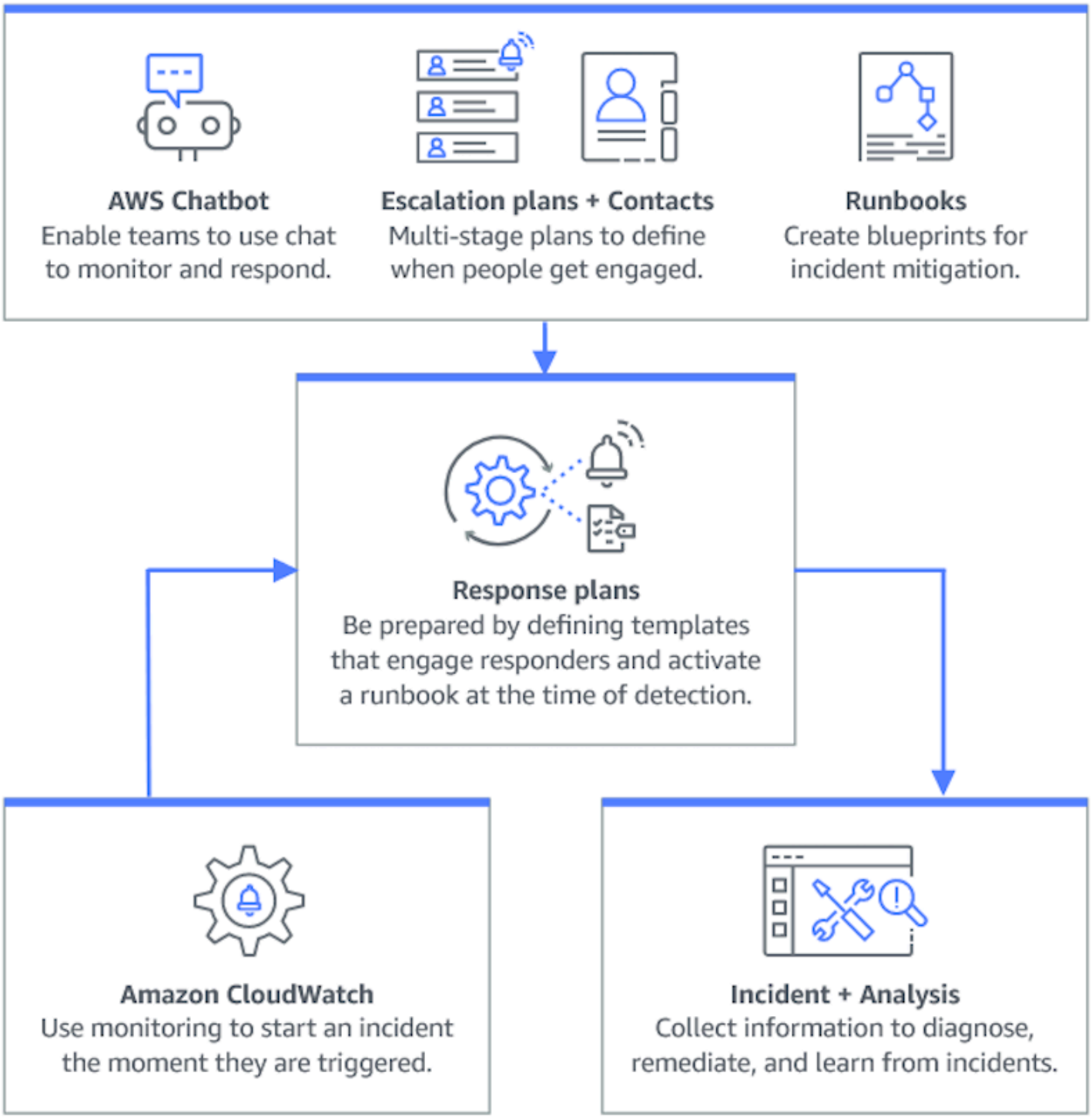
다음은 Incident Manager의 크로스 계정 기능에 대한 알려진 제한 사항입니다.

- 인시던트 사후 분석을 생성하는 계정은 분석을 보고 변경할 수 있는 유일한 계정입니다. 애플리케이션 계정을 사용하여 인시던트 사후 분석을 만드는 경우 해당 계정의 구성원만 분석을 보고 변경할 수 있습니다. 관리 계정을 사용하여 인시던트 사후 분석을 만드는 경우에도 동일합니다.
- 애플리케이션 계정에서 실행되는 자동화 문서에는 타임라인 이벤트가 채워지지 않습니다. 애플리케이션 계정에서 실행되는 자동화 문서의 업데이트는 인시던트의 Runbook 탭에서 확인할 수 있습니다.

- Amazon CloudWatch 리전 및 Amazon EventBridge 이벤트 Amazon SNS 주제는 해당 주제가 사용되는 응답 계획과 동일한 리전 및 계정에서 생성되어야 합니다. 관리 계정을 사용하여 모든 SNS 주제 및 대응 계획을 생성하는 것이 좋습니다.
- 에스컬레이션 계획은 동일한 계정의 연락처를 사용해서만 생성할 수 있습니다. 공유된 연락처는 계정의 에스컬레이션 플랜에 추가할 수 없습니다.
- 대응 계획, 인시던트 기록 및 연락처에 적용된 태그는 자원 소유자 계정에서만 보고 수정할 수 있습니다.

Incident Manager에서 인시던트 준비

인시던트 계획은 인시던트 라이프사이클 한참 전부터 시작됩니다. 다음 그림에서 볼 수 있듯이 인시던트 대응을 시작하기 전에 채팅 채널을 설정하고, 에스컬레이션 계획을 생성하고, 연락처를 지정하고, 인시던트 대응에 사용할 Automation 런북을 결정하여 준비합니다. 그런 다음 모니터링 수행 방식과 응답 자동화 여부를 지정하는 응답 계획을 사용합니다. 문제 해결이 완료되면 인시던트 및 인시던트 대응을 분석하여 향후 인시던트에 대한 대응 계획을 더욱 구체화할 수 있습니다.



주제

- 모니터링
- Incident Manager에서 복제 세트 및 결과 구성
- Incident Manager에서 연락처 생성 및 구성

- Incident Manager에서 대기 일정으로 응답기 교체 관리
- Incident Manager에서 대응자 참여를 위한 에스컬레이션 계획 생성
- Incident Manager에서 대응 담당자를 위한 채팅 채널 생성 및 통합
- 인시던트 해결을 위해 Incident Manager에 Systems Manager Automation 런북 통합
- Incident Manager에서 대응 계획 생성 및 구성
- Incident Manager에서 다른 서비스의 잠재적 인시던트 원인을 "결과"로 식별

모니터링

AWS 호스팅 애플리케이션의 상태를 모니터링하는 것은 애플리케이션 가동 시간과 성능을 보장하는 데 중요합니다. 모니터링 솔루션을 결정할 때 다음 항목을 고려해야 합니다.

- 기능의 중요성 — 시스템에 장애가 발생할 경우 다운스트림 사용자에게 미치는 영향은 얼마나 심각할까요?
- 장애의 공통성 — 시스템 장애는 얼마나 자주 발생합니까? 잦은 개입이 필요한 시스템은 면밀히 모니터링해야 합니다.
- 지연 시간 증가 — 작업을 완료하는 데 걸리는 시간이 늘어나거나 줄어드는 정도입니다.
- 클라이언트측 지표와 서버측 지표 비교 — 클라이언트 및 서버의 관련 지표 간에 불일치가 있는 경우입니다.
- 종속성 장애 — 팀에서 대비할 수 있고 또 대비해야 하는 장애입니다.

대응 계획을 수립한 후에는 모니터링 솔루션을 사용하여 환경에서 인시던트가 발생하는 즉시 인시던트를 자동으로 추적할 수 있습니다. 인시던트 추적 및 생성에 대한 자세한 내용은 Incident Manager 콘솔에서 인시던트 세부 정보 보기 섹션을 참조하세요.

안전하고 성능이 뛰어나며 복원력이 뛰어나고 효율적인 인프라 애플리케이션 및 워크로드 설계에 대한 자세한 내용은 AWS Well-Architected를 참조하세요.

Incident Manager에서 복제 세트 및 결과 구성

Incident Manager 준비 마법사를 완료한 후 설정 페이지에서 특정 옵션을 관리할 수 있습니다. 이러한 옵션에는 복제 세트, 복제 세트에 적용된 태그 및 조사 결과 기능이 포함됩니다.

주제

- Incident Manager 복제 세트 구성

- 복제 세트의 태그 관리
- 조사 결과 기능 관리

Incident Manager 복제 세트 구성

Incident Manager 복제 세트는 다음을 수행하기 AWS 리전 위해 많은에 데이터를 복제합니다.

- 교차 리전 중복성 증가
- Incident Manager가 서로 다른 리전의 리소스에 액세스하고 사용자의 지연 시간을 줄일 수 있도록 허용합니다.
- AWS 관리형 키 또는 자체 고객 관리형 키를 사용하여 데이터를 암호화합니다.

  모든 Incident Manager 리소스는 기본적으로 암호화됩니다. 리소스 암호화 방법에 대해 자세히 알아보려면 Incident Manager의 데이터 보호 섹션을 참조하세요.

Incident Manager를 시작하려면 먼저 준비 완료 마법사를 사용하여 복제 세트를 생성하십시오. Incident Manager에서 준비하는 방법에 대해 자세히 알아보려면 준비하기 마법사 섹션을 참조하세요.

복제 세트 편집

Incident Manager 설정 페이지를 사용하여 복제 세트를 편집할 수 있습니다. 리전을 추가 또는 삭제하거나, 복제 세트 삭제 보호를 활성화하거나 비활성화할 수 있습니다. 데이터를 암호화하는 데 사용되는 키를 편집할 수 없습니다. 키를 변경하려면 복제 세트를 삭제하고 다시 생성하십시오.

리전 추가

1. Incident Manager 콘솔을 열고 왼쪽 탐색 창에서 설정을 선택합니다.
2. 리전 추가를 선택합니다.
3. 리전을 선택합니다.
4. 추가를 선택합니다.

리전 삭제

1. Incident Manager 콘솔을 열고 왼쪽 탐색 창에서 설정을 선택합니다.
2. 삭제할 리전을 선택합니다.
3. 삭제를 선택합니다.

4. 상자에 delete를 입력하고 삭제를 선택합니다.

복제 세트 삭제

복제 세트의 마지막 리전을 삭제하면 전체 복제 세트가 삭제됩니다. 마지막 리전을 삭제하려면 설정 페이지에서 삭제 방지를 꺼서 삭제 방지를 비활성화합니다. 복제 세트를 삭제한 후 준비 마법사를 사용하여 새 복제 세트를 생성할 수 있습니다.

복제 세트에서 리전을 삭제하려면 생성 후 24시간을 기다리십시오. 생성 후 24시간이 지나지 않아 복제 세트에서 리전을 삭제하려고 하면 삭제에 실패합니다.

복제 세트를 삭제하면 모든 Incident Manager 데이터가 삭제됩니다.

복제 세트를 삭제합니다.

1. Incident Manager 콘솔을 열고 왼쪽 탐색 창에서 설정을 선택합니다.
2. 복제 세트의 마지막 리전을 선택합니다.
3. 삭제를 선택합니다.
4. 상자에 delete를 입력하고 삭제를 선택합니다.

복제 세트의 태그 관리

태그는 리소스에 할당하는 선택적 메타데이터입니다. 태그를 사용하면 용도, 소유자 또는 환경을 기준으로 하는 등 리소스를 다양한 방식으로 분류할 수 있습니다.

복제 세트의 태그를 관리하려면

1. Incident Manager 콘솔을 열고 왼쪽 탐색 창에서 설정을 선택합니다.
2. 태그 영역에서 편집을 선택합니다.
3. 태그를 추가하려면 다음을 수행합니다.
    a. 새로운 태그 추가를 선택합니다.
    b. 키를 입력하고, 원한다면 태그 값도 입력합니다.
    c. 저장을 선택합니다.
4. 태그를 삭제하려면 다음을 수행합니다.
    a. 삭제할 태그 아래에서 제거를 선택합니다.

b. 저장을 선택합니다.

조사 결과 기능 관리

조사 결과 기능은 조직의 대응 담당자가 인시던트가 시작된 직후 인시던트의 잠재적 근본 원인을 식별하는 데 도움이 됩니다. 현재 Incident Manager는 AWS CodeDeploy 배포 및 AWS CloudFormation 스택 업데이트에 대한 조사 결과를 제공합니다.

조사 결과에 대한 크로스 계정 지원을 받으려면 기능을 활성화한 후 조직의 각 애플리케이션 계정에서 추가 설정 단계를 완료해야 합니다.

이 기능을 사용하려면 Incident Manager에서 사용자 대신 데이터에 액세스하는 데 필요한 권한이 포함된 서비스 역할을 생성하도록 합니다.

조사 결과 기능을 활성화하려면

1. Incident Manager 콘솔을 열고 왼쪽 탐색 창에서 설정을 선택합니다.
2. 조사 결과 영역에서 서비스 역할 생성을 선택합니다.
3. 생성할 서비스 역할에 대한 정보를 검토한 후 생성을 선택합니다.

조사 결과 기능을 비활성화하려면

조사 결과 기능 사용을 중단하려면 `IncidentManagerIncidentAccessServiceRole` 역할이 생성된 각 계정에서 역할을 삭제하십시오.

1. https://console.aws.amazon.com/iam/에서 IAM 콘솔을 엽니다.
2. 왼쪽 탐색 창에서 역할을 선택합니다.
3. 검색 상자에 **`IncidentManagerIncidentAccessServiceRole`**을(를) 입력합니다.
4. 역할의 이름을 선택하고 나서 삭제를 선택합니다.
5. 대화 상자에 역할 이름을 입력하여 역할 삭제 의도를 확인한 다음 삭제를 선택합니다.

Incident Manager에서 연락처 생성 및 구성

AWS Systems Manager Incident Manager 고객 응대는 인시던트에 대한 대응 담당자입니다. 연락처는 Incident Manager가 인시던트 중에 참여할 수 있는 여러 채널을 가질 수 있습니다. 연락처의 참여 계획을 정의하여 Incident Manager가 해당 연락을 취하는 방법과 시기를 설명할 수 있습니다.

주제

연락처 채널

연락 채널은 Incident Manager가 연락처를 참여시키기 위해 사용하는 다양한 방법입니다.

Incident Manager는 다음 연락처 채널을 지원합니다.

- 이메일
- 모바일 문자 메시지(SMS)
- Voice

연락처 채널 활성화

개인 정보 및 보안을 보호하기 위해 연락처를 만들 때 Incident Manager에서 디바이스 활성화 코드를 사용자에게 보냅니다. 인시던트 중에 디바이스를 작동시키려면 먼저 디바이스를 활성화해야 합니다. 이렇게 하려면 연락처 생성 페이지에 디바이스 활성화 코드를 입력합니다.

Incident Manager의 특정 기능에는 연락처 채널에 알림을 보내는 기능이 포함됩니다. 이러한 기능을 사용하면 이 서비스가 지정된 워크플로에 포함된 연락처 채널에 서비스 중단 또는 기타 이벤트에 대한 알림을 보내는 데 동의하는 것으로 간주됩니다. 여기에는 대기 일정 교대 중에 연락처에게 전송된 알림이 포함됩니다. 연락처 세부 정보에 지정된 대로 이메일, SMS 메시지 또는 음성 통화를 통해 알림을 보낼 수 있습니다. 이러한 기능을 사용하여 Incident Manager에게 제공하는 연락처 채널을 추가할 권한이 부여되었음을 확인합니다.

옵트아웃

연락처 채널에서 모바일 디바이스를 제거하여 언제든지 이러한 알림을 취소할 수 있습니다. 개별 알림 수신자는 연락처에서 디바이스를 제거하여 언제든지 알림을 취소할 수 있습니다.

연락처에서 연락처 채널을 제거하려면

1. Incident Manager 콘솔로 이동한 다음 왼쪽 탐색 메뉴에서 연락처를 선택합니다.

2. 제거하려는 연락처 채널의 연락처를 선택하고 편집을 선택합니다.
3. 제거하려는 연락처 채널 옆의 제거를 선택합니다.
4. 업데이트를 선택합니다.

연락처 채널 활성화

디바이스를 비활성화하려면 구독 취소라고 회신하세요. 구독 취소라고 회신하면 Incident Manager가 사용자 디바이스의 참여를 막습니다.

연락처 채널 재활성화

1. Incident Manager가 보낸 메시지에 시작이라고 회신하세요.
2. Incident Manager 콘솔로 이동한 다음 왼쪽 탐색 메뉴에서 연락처를 선택합니다.
3. 제거하려는 연락처 채널의 연락처를 선택하고 편집을 선택합니다.
4. 디바이스 활성화를 선택합니다.
5. Incident Manager가 디바이스로 보낸 활성화 코드를 입력합니다.
6. 활성화를 선택합니다.

참여 계획

참여 계획은 Incident Manager가 연락처 채널을 참여시키는 시기를 정의합니다. 참여 시작 시점부터 여러 단계에서 연락 채널을 여러 번 참여시킬 수 있습니다. 에스컬레이션 계획 또는 대응 계획에서 참여 계획을 사용할 수 있습니다. 에스컬레이션 계획에 대한 자세한 내용은 Incident Manager에서 대응자 참여를 위한 에스컬레이션 계획 생성 섹션을 참조하세요.

연락처 만들기

다음 단계에 따라 연락처를 만듭니다.

1. Incident Manager 콘솔을 열고 왼쪽 탐색 메뉴에서 연락처를 선택합니다.
2. 연락처 생성을 선택합니다.
3. 연락처의 전체 이름을 입력하고 고유하고 식별 가능한 별칭을 제공하십시오.
4. 연락처 채널을 정의합니다. 두 개 이상의 다른 유형의 연락처 채널을 사용하는 것이 좋습니다.
    a. 이메일, SMS 또는 음성 중에서 유형을 선택합니다.

b. 연락처 채널의 식별할 수 있는 이름을 입력합니다.

c. 연락처 채널 세부 정보(예: 이메일: arosalez@example.com)를 제공하십시오.

5. 연락처 채널을 두 개 이상 정의하려면 연락처 채널 추가를 선택합니다. 새로 추가된 각 연락처 채널에 대해 4단계를 반복합니다.

6. 참여 계획을 정의합니다.

> **Important**
>
> 연락처를 참여시키려면 참여 계획을 정의해야 합니다.

a. 연락처 채널 이름을 선택합니다.

b. Incident Manager가 이 연락처 채널을 참여시킬 때까지 참여 시작을 기다려야 하는 시간을 정의하십시오.

c. 다른 연락처 채널을 추가하려면 참여 추가를 선택합니다.

7. 참여 계획을 정의한 후 생성을 선택합니다. Incident Manager가 정의된 각 연락처 채널에 활성화 코드를 보냅니다.

8. (선택 사항) 연락처 채널을 활성화하려면 Incident Manager가 정의된 각 연락처 채널에 보낸 활성화 코드를 입력합니다.

9. (선택 사항) 새 활성화 코드를 보내려면 새 코드 보내기를 선택합니다.

10. 마침을 클릭합니다.

연락처를 정의하고 연락처 채널을 활성화한 후 에스컬레이션 계획에 연락처를 추가하여 일련의 에스컬레이션을 구성할 수 있습니다. 에스컬레이션 계획에 대한 자세한 내용은 Incident Manager에서 대응자 참여를 위한 에스컬레이션 계획 생성 섹션을 참조하세요. 직접 참여를 위한 대응 계획에 연락처를 추가할 수 있습니다. 대응 계획 생성에 대한 자세한 내용은 Incident Manager에서 대응 계획 생성 및 구성 섹션을 참조하세요.

연락처 세부 정보를 주소록으로 가져오기

인시던트가 생성되면 Incident Manager는 음성 또는 SMS 알림을 사용하여 대응 담당자에게 알릴 수 있습니다. 대응 담당자가 Incident Manager가 보낸 전화 또는 SMS 알림을 확인할 수 있도록 하려면 모든 대응 담당자가 Incident Manager 가상 카드 형식(.vcf) 파일을 모바일 디바이스의 주소록에 다운로드하는 것이 좋습니다. 파일은 Amazon CloudFront에서 호스팅되며 AWS 상용 파티션에서 사용할 수 있습니다.

Incident Manager .vcf 파일을 다운로드하려면

1. 모바일 디바이스에서 다음 URL을 선택하거나 입력하십시오. https://d26vhuvd5b89k2.cloudfront.net/aws-incident-manager.vcf.
2. 모바일 디바이스의 주소록에 파일을 저장하거나 해당 주소록으로 파일을 가져옵니다.

Incident Manager에서 대기 일정으로 응답기 교체 관리

Incident Manager의 대기 일정은 운영자 개입이 필요한 인시던트 발생 시 알림을 받는 사람을 정의합니다. 대기 일정은 해당 일정에 대해 생성한 하나 이상의 교대로 구성됩니다. 각 교대에 최대 30명의 연락처를 포함할 수 있습니다.

대기 일정을 만든 후 에스컬레이션 계획에 에스컬레이션으로 포함시킬 수 있습니다. 해당 에스컬레이션 계획과 관련된 인시던트가 발생하면 Incident Manager는 일정에 따라 대기 중인 운영자에게 알립니다. 그러면 이 연락처가 참여 사실을 확인할 수 있습니다. 에스컬레이션 계획에서는 여러 에스컬레이션 단계에 걸쳐 하나 이상의 대기 일정과 한 명 이상의 개별 연락처를 지정할 수 있습니다. 자세한 내용은 Incident Manager에서 대응자 참여를 위한 에스컬레이션 계획 생성 단원을 참조하십시오.

> **Tip**
>
> 모범 사례로 에스컬레이션 계획에서 에스컬레이션 채널로 연락처 및 대기 일정을 추가할 것을 권장합니다. 에스컬레이션 계획을 대응 계획의 참여로 선택해야 합니다. 이 접근 방식은 조직의 인시던트 대응을 위한 최대한의 범위를 제공합니다.

각 대기 일정은 최대 8개의 교대를 지원합니다. 교대가 겹치거나 동시에 실행될 수 있습니다. 이로 인해 인시던트 발생 시 대응하라는 통지를 받는 작업자 수가 늘어납니다. 연속적으로 실행되는 교대를 생성할 수도 있습니다. 이는 전 세계에 동일한 서비스를 지원하는 그룹이 있는 “Follow the Sun” 인시던트 관리와 같은 시나리오를 지원합니다.

이 섹션의 주제를 참고하여 인시던트 대응 작업을 위한 대기 일정을 생성하고 관리할 수 있습니다.

주제

- Incident Manager에서 대기 일정과 교대 만들기
- Incident Manager에서 기존 대기 일정 관리

Incident Manager에서 대기 일정과 교대 만들기

연락처를 한 번 이상 교대하여 대기 일정을 만들어 교대 근무 중 인시던트에 대응할 수 있도록 하세요.

시작하기 전 준비 사항

대기 일정을 만들기 전에 일정에 추가할 연락처를 미리 생성했는지 확인하세요. 자세한 내용은 Incident Manager에서 연락처 생성 및 구성 섹션을 참조하세요.

일광 절약 시간(DST) 변경 사항 고려

교대 근무를 생성할 때는 해당 교대에 대해 지정한 교대 적용 범위 시간 및 날짜의 기준이 되는 글로벌 시간대를 지정합니다. IANA(Internet Assigned Numbers Authority)에서 정의한 모든 시간대를 사용할 수 있습니다. 예를 들어, `America/Los_Angeles`, `UTC` 및 `Asia/Seoul`입니다. 대기 일정에 교대 근무를 두 번 이상 추가할 수 있습니다. 그러나 각 교대의 대응 담당자가 지리적으로 서로 다른 시간대에 있는 경우 각 교대에 영향을 미칠 수 있는 DST 변경 사항을 염두에 두십시오.

예를 들어, `America/Los_Angeles` 및 `Europe/Dublin`은 다른 DST 일정을 준수합니다 따라서 두 지역 간의 시차는 연중 시기에 따라 6시간에서 8시간까지 달라질 수 있습니다. 예를 들어, follow-the-Sun 대기 일정의 경우 `America/Los_Angeles` 시간대에서 한 번 교대가 있고 `Europe/Dublin`에서 한 번 교대가 있습니다. 이 예제의 일정에는 DST 변경으로 인한 1시간 교대 간격 또는 1시간 교대 중복이 포함될 수 있습니다.

이러한 상황을 방지하려면 다음 작업을 수행하는 것이 좋습니다.

1. 대기 일정의 모든 교대에 대해 단일 시간대를 사용합니다.
2. 특정 시간대 이외의 시간에 대응 담당자를 지정할 때는 현지 시간을 계산하세요.

각 교대를 현지 시간대로 지정하기로 결정했다면 DST 전에 일정을 검토하십시오. 그런 다음 DST 변경 사항이 적용되기 전에 대기 적용 범위에 의도하지 않은 간격이나 중복이 발생하지 않도록 필요에 따라 교대 근무 시간을 조정하십시오.

대기 일정을 만들려면

1. Incident Manager 콘솔을 엽니다.
2. 왼쪽 탐색 창에서 대기 일정을 선택합니다.
3. 대기 일정 만들기를 선택합니다.
4. 일정 이름에 일정을 식별하는 데 도움이 되는 이름(예**`MyApp Primary On-call Schedule`**:)을 입력합니다.

5. 일정 별칭에 AWS 리전와 같이 현재에서 고유한이 일정의 별칭을 입력합니다**my-app-primary-on-call-schedule**.
6. (선택 사항) 태그 영역에서 하나 이상의 태그 키 이름 및 값 쌍을 대기 일정에 적용합니다.

   태그는 리소스에 할당하는 선택적 메타데이터입니다. 태그를 사용하면 용도, 소유자 또는 환경을 기준으로 하는 등 리소스를 다양한 방식으로 분류할 수 있습니다. 예를 들어 일정에 태그를 지정하여 실행 기간, 일정에 포함된 운영자 유형 또는 지원하는 에스컬레이션 계획을 식별할 수 있습니다. Incident Manager 리소스 태그 지정에 대한 자세한 내용은 Incident Manager의 리소스 태깅 섹션을 참조하세요.
7. 대기 일정에 교대를 하나 이상 추가하여 계속하십시오.

Incident Manager에서 대기 일정에 대한 교대 생성

대기 일정의 교대에서 교대가 적용되는 시점을 지정합니다. 또한 교대하는 연락처도 지정합니다. 단일 대기 일정에 최대 8회의 교대를 포함할 수 있습니다.

Incident Manager에서 연락처로 생성한 모든 개인을 교대에 추가할 수 있습니다. 연락처 관리에 대한 자세한 내용은 Incident Manager에서 연락처 생성 및 구성 섹션을 참조하세요.

교대를 구성하면 페이지 오른쪽에 있는 미리 보기 달력에서 전체 일정이 어떤지 확인할 수 있습니다.

대기 일정의 교대를 생성하려면

1. 대기 일정 만들기 페이지의 교대 1 섹션에서 교대 이름에 교대를 식별하는 이름(예**00:00 - 7:59 Support**: 또는 **Dublin Support Group**)을 입력합니다.
2. 시작 날짜에는 이 교대가 활성화되는 날짜를 2023/07/14 같이 YYYY/MM/DD 형식으로 입력합니다.
3. 시간대에서 이 교대에 대해 지정한 교대 적용 범위 시간 및 날짜의 기준이 되는 글로벌 시간대를 선택합니다.

   IANA(Internet Assigned Numbers Authority)에서 정의한 모든 시간대를 사용할 수 있습니다. 예를 들어 "America/Los_Angeles", "UTC" 또는 "Asia/Seoul"입니다. 자세한 내용은 IANA 웹 사이트에서 표준 시간대 데이터베이스를 참조하세요.

> **Warning**
>
> 각 교대는 자체 시간대를 기준으로 할 수 있습니다. 하지만 선택한 시간대의 일광 절약 시간제 변경은 의도한 적용 범위에 영향을 미칠 수 있습니다. 자세한 내용은 이 항목의 앞부분에 있는 일광 절약 시간(DST) 변경 사항 고려를 참조하세요.

4. 교대 시작 시간에 이 교대 순환이 시작되는 시간을 `16:00` 같이 24시간 `hh:mm` 형식으로 입력합니다.

   지정한 시간대와 다른 시간대 내 연락처의 현지 시간 차이를 주의하십시오. 예를 들어 시간대로 `America/Los_Angeles`를 선택하고 교대 시작 시간으로 `00:00`을 선택한 경우 이 시간은 아일랜드 더블린에서는 08:00, 인도 뭄바이에서는 13:30이 됩니다.

5. 교대 종료 시간에 이 교대 순환이 종료되는 시간을 `23:59` 같이 24시간 `hh:mm` 형식으로 입력합니다.

   > **Note**
   >
   > 교대 시작과 종료 사이의 시간 간격은 30분 이상이어야 합니다.

6. (선택 사항) 교대 기간을 24시간으로 설정하려면 24시간 적용 범위를 선택하고 교대 시작 시간 필드에 이 교대의 시작 시간을 입력합니다. 교대 종료 시간 값이 자동으로 업데이트됩니다.

   예를 들어, 오전 11시에 교대가 바뀌는 24시간 적용 범위의 대기 일정을 원할 경우 24시간 적용 범위를 선택하고 시작 시간으로 **`11:00`**을 입력합니다.

7. 활성 요일의 경우 이 교대가 활성화되는 요일을 선택합니다. 예를 들어 대기 계획에서 주말 적용 범위를 제외할 경우 일요일과 토요일을 제외한 모든 요일을 선택하십시오.

8. 교대에 연락처를 추가하여 계속하십시오.

Incident Manager에서 대기 일정의 교대에 연락처 추가

대기 일정의 각 교대에 대해 하나 이상의 연락처를 추가할 수 있으며, 최대 30개까지 추가할 수 있습니다. Incident Manager 구성에 설정된 연락처 중에서 선택할 수 있습니다.

연락처를 교대에 추가하면 해당 연락처는 대기 업무 중에 알림을 받을 수 있습니다. 연락처 세부 정보에 명시된 대로 이메일, SMS 또는 음성 통화를 통해 알림을 보낼 수 있습니다.

연락처 관리 및 연락처 알림 옵션에 대한 자세한 내용은 Incident Manager에서 연락처 생성 및 구성 섹션을 참조하세요.

대기 일정의 교대에 연락처를 추가하려면

1. 대기 일정 만들기 페이지의 교대에 대한 연락처 섹션에서 연락처 추가 또는 제거를 선택합니다.
2. 연락처 추가 또는 제거 대화 상자에서 교대에 포함할 연락처의 별칭을 선택합니다.

   연락처를 선택하는 순서는 교대 일정에 해당 연락처가 처음 나열되는 순서입니다. 연락처를 추가한 후 순서를 변경할 수 있습니다.
3. 확인을 선택합니다.
4. 순서에서 연락처 위치를 변경하려면 해당 사용자의 라디오 버튼을 선택하고
   Up( )
   및
   Down( )
   버튼을 사용하여 연락처 순서를 업데이트하십시오.
5. 교대에 대한 개별 교대 반복 및 기간을 지정하여 계속하십시오.

Incident Manager에서 교대 반복 및 기간을 지정하고 교대에 태그 추가

교대 반복은 교대의 연락처가 대기에 들어오고 나가는 빈도를 지정합니다. 반복 기간은 일, 주 또는 월 단위로 지정할 수 있습니다.

교대 반복 및 기간을 지정하고 교대에 태그를 추가하려면

1. 대기 일정 만들기 페이지의 교대에 대한 반복 설정 섹션에서 다음과 같이 하십시오.

   - 교대 반복 유형에서 `Daily`, `Weekly` 및 `Monthly` 중에서 선택하여 각 대기 일정의 교대가 일 단위, 주 단위 또는 월 단위로 지속되는지 여부를 지정합니다.
   - 교대 기간에는 교대가 지속되는 일, 주 또는 개월 수를 입력합니다.

     예를 들어, `Daily`를 선택하고 **1**을 입력하면 각 연락처의 대기 교대 기간은 1일입니다.
     `Weekly`를 선택하고 **3**을 입력하면 각 연락처의 대기 교대 기간은 3주입니다.
2. (선택 사항) 태그 영역에서 하나 이상의 태그 키 이름/값 쌍을 교대에 적용합니다.

   태그는 리소스에 할당하는 선택적 메타데이터입니다. 태그를 사용하면 용도, 소유자 또는 환경을 기준으로 하는 등 리소스를 다양한 방식으로 분류할 수 있습니다. 예를 들어, 교대에 태그를 지정하여 교대에 지정된 연락처의 위치, 제공하려는 적용 범위 유형, 지원되는 에스클레이션 계획을 식

별할 수 있습니다. Incident Manager 리소스 태그 지정에 대한 자세한 내용은 Incident Manager의 리소스 태깅 섹션을 참조하세요.

3. (권장) 달력 미리 보기를 사용하여 대기 일정의 적용 범위에 의도치 않은 간격이 없는지 확인하세요.
4. 생성(Create)을 선택합니다.

이제 에스컬레이션 계획에서 에스컬레이션 채널로 대기 일정을 추가할 수 있습니다. 자세한 내용은 에스컬레이션 계획 만들기을 참조하세요.

Incident Manager에서 기존 대기 일정 관리

이 섹션의 내용은 이미 생성한 대기 일정에 대해 작업하는 데 도움이 됩니다.

주제

- 대기 일정 세부 정보 보기
- 대기 일정 편집
- 대기 일정 복사
- 대기 일정 교대에 대한 재정의 만들기
- 대기 일정 삭제

대기 일정 세부 정보 보기

대기 일정 세부 정보 보기 페이지에서 대기 일정을 한 눈에 볼 수 있습니다. 이 페이지에는 현재 대기에 있는 사람과 다음 대기에 있는 사람에 대한 정보도 포함되어 있습니다. 이 페이지에는 특정 시간에 대기에 있는 연락처를 보여주는 달력 보기가 포함되어 있습니다.

대기 일정 세부 정보를 보려면

1. Incident Manager 콘솔을 엽니다.
2. 왼쪽 탐색 창에서 대기 일정을 선택합니다.
3. 세부 정보를 보려는 대기 일정의 행에서 다음 중 하나를 수행합니다.

   - 달력의 요약 보기를 열려면 일정 별칭을 선택합니다.

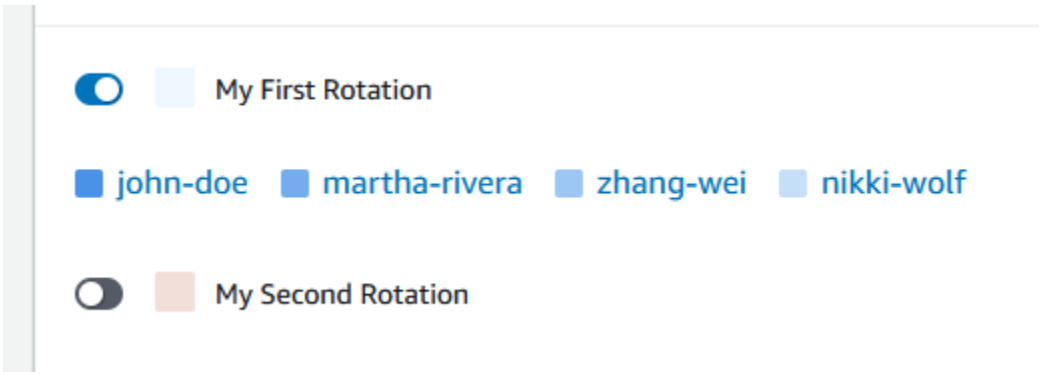
     -또는-

     행에 대한 라디오 버튼을 선택한 후 보기를 선택합니다.

- 일정의 달력 보기를 열려면 달력 보기를 선택합니다.

  달력 보기에서 일정의 특정 날짜의 연락처 이름을 선택하여 배정된 교대에 대한 세부 정보를 보거나 재정의를 생성하십시오.
- 일정에서 특정 교체 표시를 켜거나 끄려면 교체 이름 옆에 있는 토글을 선택합니다.



대기 일정 편집

다음 세부 정보를 제외하고 대기 일정 및 교대에 대한 구성을 업데이트할 수 있습니다.

- 스케줄 별칭
- 교대 이름
- 교대 시작 날짜

이러한 값을 변경할 수 있는 기능을 사용하여 기존 달력을 새 달력의 기반으로 사용하려면 대신 달력을 복사하면 됩니다. 자세한 내용은 대기 일정 복사을 참조하세요.

대기 일정을 편집하려면

1. Incident Manager 콘솔을 엽니다.
2. 왼쪽 탐색 창에서 대기 일정을 선택합니다.
3. 다음 중 하나를 수행합니다.
   - 편집하려는 대기 일정의 행에서 라디오 버튼을 선택한 다음 편집을 선택합니다.
   - 대기 일정의 일정 별칭을 선택하여 대기 일정 세부 정보 보기 페이지를 연 다음 편집을 선택합니다.

4. 대기 일정 및 교대에서 필요한 수정을 하십시오. 시작 및 종료 시간, 연락처, 반복 등의 교대 구성 옵션을 변경할 수 있습니다. 필요에 따라 일정에서 교대를 추가하거나 제거할 수 있습니다. 달력 미리 보기에 변경 내용이 반영됩니다.

   페이지의 옵션 작업에 대한 자세한 내용은 Incident Manager에서 대기 일정과 교대 만들기 섹션을 참조하세요.
5. 업데이트를 선택합니다.

> **Important**
>
> 재정의가 포함된 일정을 편집하는 경우 변경 사항이 재정의에 영향을 미칠 수 있습니다. 재정의가 예상대로 구성된 상태를 유지하도록 하려면 일정을 업데이트한 후 교대 재정의를 면밀히 검토하는 것이 좋습니다.

대기 일정 복사

기존 대기 일정 구성을 새 일정의 시작 지점으로 사용하려면 달력 사본을 만들어 필요에 따라 수정하면 됩니다.

대기 일정을 복사하려면

1. Incident Manager 콘솔을 엽니다.
2. 왼쪽 탐색 창에서 대기 일정을 선택합니다.
3. 복사하려는 대기 일정의 행에서 라디오 버튼을 선택합니다.
4. 복사를 선택합니다.
5. 달력 및 교대에서 필요한 수정을 하십시오. 필요에 따라 교대를 변경, 추가 또는 제거할 수 있습니다.

   > **Note**
   >
   > 기존 일정을 복사할 때는 각 교대에 대해 새 시작 날짜를 지정해야 합니다. 복사된 일정은 시작 날짜가 과거인 교대를 지원하지 않습니다.

   페이지의 옵션 작업에 대한 자세한 내용은 Incident Manager에서 대기 일정과 교대 만들기 섹션을 참조하세요.

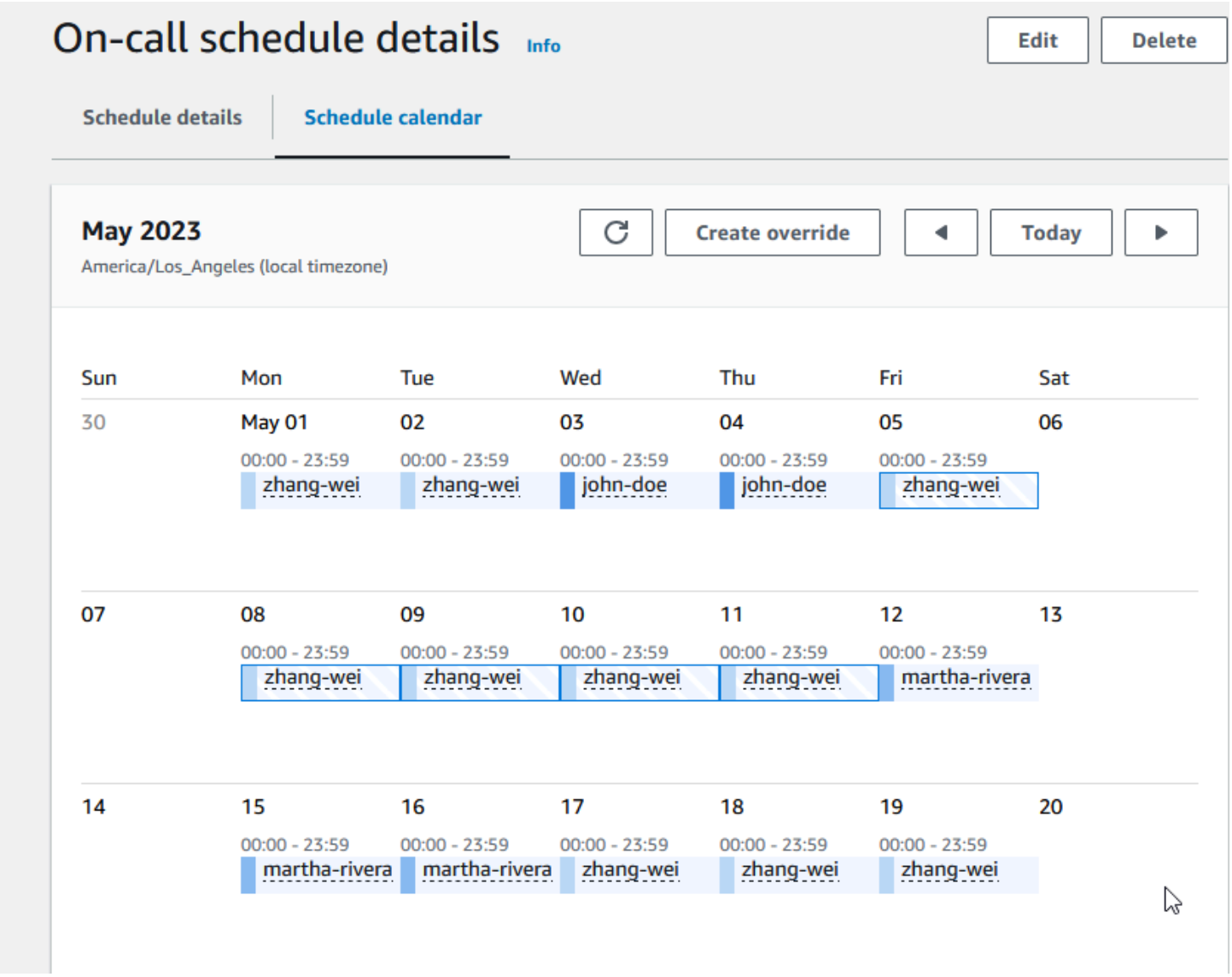
6. 사본 생성을 선택합니다.

대기 일정 교대에 대한 재정의 만들기

기존 교대 일정에 대해 한 번의 해제 변경을 해야 하는 경우 재정의를 생성할 수 있습니다. 재정의를 사용하면 연락처의 교대 전체 또는 일부를 다른 연락처로 바꿀 수 있습니다. 여러 교대에 걸친 재정의를 만들 수도 있습니다.

이미 교대에 지정된 연락처만 재정의에 지정할 수 있습니다.

달력 미리 보기에서 재정의된 교대는 단색 배경 대신 줄무늬 배경으로 표시됩니다. 다음 이미지는 Zhang Wei라는 연락처가 재정의를 통해 통화 중임을 보여줍니다. 재정의에는 5월 5일부터 5월 11일까지 John Doe 및 Martha Rivera에 대한 교대 근무의 일부가 포함됩니다.



대기 일정에 대한 재정의를 생성하려면

1. Incident Manager 콘솔을 엽니다.
2. 왼쪽 탐색 창에서 대기 일정을 선택합니다.
3. 세부 정보를 보려는 대기 일정의 행에서 다음 중 하나를 수행합니다.
   - 일정 별칭을 선택한 다음 일정 달력 탭을 선택합니다.
   - 달력 보기
     
     를 선택합니다.
4. 다음 중 하나를 수행합니다.
   - 재정의 생성을 선택합니다.
   - 달력 미리보기에서 연락처 이름을 선택한 다음 교대 재정의를 선택합니다.
5. 교대 재정의 생성 대화 상자에서 다음을 수행합니다.

   > **Note**
   >
   > 재정의 기간은 30분 이상이어야 합니다. 향후 6개월 이내에 발생하는 교대 근무에 대해서만 재정의를 지정할 수 있습니다.

   a. 교대 선택에서 재정의를 생성할 교대 이름을 선택합니다.
   b. 시작 날의에서 재정의가 시작되는 날짜를 선택하거나 입력합니다.
   c. 시작 시간에서 재정의가 시작되는 시간을 `hh:mm` 형식으로 입력합니다.
   d. 종료 날짜에서 재정의가 종료되는 날짜를 선택하거나 입력합니다.
   e. 종료 시간에서 재정의가 종료되는 시간을 `hh:mm` 형식으로 입력합니다.
   f. 재정의 연락처 선택에서 재정의 기간 중에 대기에 있는 교대 연락처 이름을 선택합니다.
6. 재정의 생성을 선택합니다.

재정의를 만든 후에는 줄무늬 배경으로 해당 재정의를 식별할 수 있습니다. 재정의된 교대의 연락처 이름을 선택하면 정보 상자에 해당 교대가 재정의된 교대로 표시됩니다. 재정의 삭제를 선택하여 재정의를 제거하고 원래의 대기 지정을 복원할 수 있습니다.

대기 일정 삭제

대기 일정이 더 이상 필요하지 않다면 Incident Manager에서 이를 삭제할 수 있습니다.

에스컬레이션 계획이나 대응 계획이 현재 대기 일정을 에스컬레이션 채널로 사용하고 있는 경우 일정을 삭제하기 전에 해당 계획에서 제거해야 합니다.

대기 일정을 삭제하려면

1. Incident Manager 콘솔을 엽니다.
2. 왼쪽 탐색 창에서 대기 일정을 선택합니다.
3. 삭제하려는 대기 일정의 행에서 라디오 버튼을 선택합니다.
4. Delete(삭제)를 선택합니다.
5. 대기 일정 삭제? 대화 상자의 입력란에 **`confirm`**을 입력합니다.
6. Delete(삭제)를 선택합니다.

Incident Manager에서 대응자 참여를 위한 에스컬레이션 계획 생성

AWS Systems Manager Incident Manager 는 정의된 고객 응대 또는 대기 일정을 통해 에스컬레이션 경로를 총칭하여 에스컬레이션 채널이라고 합니다. 동시에 여러 에스컬레이션 채널을 인시던트로 가져올 수 있습니다. 에스컬레이션 채널의 지정된 연락처가 응답하지 않는 경우, Incident Manager는 다음 연락처 세트로 에스컬레이션합니다. 사용자가 참여를 확인한 후 계획에서 에스컬레이션을 중단할지 여부를 선택할 수도 있습니다. 대응 계획에 에스컬레이션 계획을 추가하여 인시던트가 시작될 때 에스컬레이션이 자동으로 시작되도록 할 수 있습니다. 진행 중인 인시던트에 에스컬레이션 계획을 추가할 수도 있습니다.

주제

- Stages
- 에스컬레이션 계획 만들기

Stages

에스컬레이션 계획은 각 단계가 정해진 시간(분) 동안 지속되는 단계를 사용합니다. 각 단계에는 다음과 같은 정보가 있습니다.

- 기간 — 계획이 다음 단계를 시작할 때까지 기다리는 시간입니다. 에스컬레이션 계획의 첫 단계는 참여가 시작되면 시작됩니다.
- 에스컬레이션 채널 — 에스컬레이션 채널은 단일 연락처 또는 정의된 일정에 따라 책임을 교대하는 여러 연락처로 구성된 대기 일정입니다. 에스컬레이션 계획은 정의된 참여 계획을 사용하여 각 채널

을 참여시킵니다. 각 에스컬레이션 채널을 설정하여 다음 단계로 진행하기 전에 에스컬레이션 계획의 진행을 중단할 수 있습니다. 각 단계에는 여러 에스컬레이션 채널이 있을 수 있습니다.

개별 연락처 설정에 대한 자세한 내용은 Incident Manager에서 연락처 생성 및 구성 섹션을 참조하세요. 대기 일정 만들기에 대한 자세한 내용은 Incident Manager에서 대기 일정으로 응답기 교체 관리 섹션을 참조하세요.

에스컬레이션 계획 만들기

1. Incident Manager 콘솔 열고 왼쪽 탐색 메뉴에서 에스컬레이션 계획을 선택합니다.
2. 에스컬레이션 계획 생성을 선택합니다.
3. 이름에 에스컬레이션 계획의 고유한 이름(예: **`My Escalation Plan`**)을 입력합니다.
4. 별칭에 계획을 식별하는 데 도움이 되는 별칭 (예: **`my-escalation-plan`**)을 입력합니다.
5. 단계 기간에는 Incident Manager가 다음 단계로 넘어갈 때까지 대기할 시간(분)을 입력합니다.
6. 에스컬레이션 채널에서이 단계에서 참여할 연락 또는 대기 일정을 하나 이상 선택합니다.
7. (선택 사항) 연락처가 참여를 확인한 후 에스컬레이션 계획을 중단하도록 하려면 승인이 계획 진행 중지를 선택합니다.
8. 단계에 채널을 더 추가하려면 에스컬레이션 채널 추가를 선택합니다.
9. 에스컬레이션 계획에 다른 단계를 추가하려면 단계 추가를 선택합니다.
10. 이 에스컬레이션 계획에 사용할 에스컬레이션 채널과 단계를 모두 추가할 때까지 5~9단계를 반복합니다.
11. (선택 사항) 태그 영역에서 하나 이상의 태그 키 이름/값 쌍을 스택에 적용합니다.

    태그는 리소스에 할당하는 선택적 메타데이터입니다. 태그를 사용하면 용도, 소유자 또는 환경을 기준으로 하는 등 리소스를 다양한 방식으로 분류할 수 있습니다. 예를 들어 에스컬레이션 계획에 태그를 지정하여 사용할 인시던트 유형, 포함된 에스컬레이션 채널 유형 또는 지원하는 에스컬레이션 계획을 식별할 수 있습니다. Incident Manager 리소스 태그 지정에 대한 자세한 내용은 Incident Manager의 리소스 태깅 섹션을 참조하세요.
12. 에스컬레이션 계획 생성을 선택합니다.

Incident Manager에서 대응 담당자를 위한 채팅 채널 생성 및 통합

의 도구인 Incident Manager는 인시던트 대응 담당자가 인시던트 중에 채팅 채널을 통해 직접 통신할 수 있는 기능을 AWS Systems Manager제공합니다. 채팅 채널은 채팅 애플리케이션의 Amazon Q

Developer에서 설정한 채팅룸입니다. 그런 다음 이 채널을 Incident Manager의 대응 계획에 연결합니다.

인시던트 발생 시 대응 담당자는 채팅 채널을 사용하여 인시던트에 대해 서로 소통합니다. 또한 Incident Manager는 인시던트에 대한 모든 업데이트 및 알림을 채팅 채널에 직접 푸시합니다. 채팅방 구성에 지정하는 하나 이상의 Amazon Simple Notification Service(Amazon SNS) 주제를 사용하여 이러한 알림을 보냅니다.

채팅 애플리케이션의 Amazon Q Developer 및 Incident Manager는 다음 애플리케이션에서 채팅 채널을 지원합니다.

- Slack
- Microsoft Teams
- Amazon Chime

인시던트에 사용할 채팅 채널을 설정하는 프로세스는 세 가지 Amazon Web Services 서비스의 작업으로 구성됩니다.

업무

- 작업 1: 채팅 채널용 Amazon SNS 주제 생성 또는 업데이트
- 작업 2: 채팅 애플리케이션에서 Amazon Q Developer에 채팅 채널 생성
- 작업 3: Incident Manager의 대응 계획에 채팅 채널 추가
- 채팅 채널을 통한 상호작용

작업 1: 채팅 채널용 Amazon SNS 주제 생성 또는 업데이트

Amazon SNS는 게시자에서 구독자(생산자 및 소비자라고도 함)로 메시지를 전송하는 관리형 서비스입니다. 게시자는 논리적 액세스 지점 및 커뮤니케이션 채널인 주제에 메시지를 전송하여 구독자와 비동기식으로 통신합니다. Incident Manager는 사용자가 대응 계획과 연계한 하나 이상의 주제를 사용하여 인시던트 대응 담당자에게 인시던트에 대한 알림을 보냅니다.

대응 계획에서 하나 이상의 Amazon SNS 주제를 인시던트 알림에 포함할 수 있습니다. 복제 세트에 추가 AWS 리전 한 각에 SNS 주제를 생성하는 것이 가장 좋습니다.

> **Tip**
>
> 보다 선형적인 설정 워크플로를 위해서는 먼저 Amazon SNS 주제를 Incident Manager와 함께 사용할 수 있도록 구성하는 것이 좋습니다. 구성한 후에는 채팅 채널을 생성할 수 있습니다.

채팅 채널용 Amazon SNS 주제를 생성 또는 업데이트하려면

1. Amazon Simple Notification Service 개발자 안내서에서 Amazon SNS 주제 생성의 단계를 수행하십시오.

   > **Note**
   >
   > 주제를 생성한 후 편집하여 액세스 정책을 업데이트합니다.

2. 생성한 주제를 선택하고 주제의 Amazon 리소스 이름(ARN)을 `arn:aws:sns:us-east-2:111122223333:My_SNS_topic` 같은 형식으로 메모하거나 복사하십시오.
3. 편집을 선택한 다음, 기본값 이외의 추가 액세스 권한을 구성하려면 액세스 정책 섹션을 확장합니다.
4. 다음 명령문을 정책의 문 배열에 추가합니다.

```
{
    "Sid": "IncidentManagerSNSPublishingPermissions",
    "Effect": "Allow",
    "Principal": {
        "Service": "ssm-incidents.amazonaws.com"
    },
    "Action": "SNS:Publish",
    "Resource": "sns-topic-arn",
    "Condition": {
        "StringEqualsIfExists": {
            "AWS:SourceAccount": "account-id"
        }
    }
}
```

`######` # 다음과 같이 바꿉니다.

- *sns-topic-arn*은 이 리전에 대해 `arn:aws:sns:us-east-2:111122223333:My_SNS_topic` 형식으로 생성한 주제의 Amazon 리소스 이름(ARN)입니다.
- *account-id*는와 같이 작업 AWS 계정 중인의 ID입니다`111122223333`.

5. Save changes(변경 사항 저장)를 선택합니다.
6. 복제 세트에 포함된 각 리전에서 이 프로세스를 반복합니다.

작업 2: 채팅 애플리케이션에서 Amazon Q Developer에 채팅 채널 생성

Slack, Microsoft Teams또는 Amazon Chime에서 채팅 채널을 생성할 수 있습니다. 각 대응 계획에는 채팅 채널이 하나만 필요합니다.

채팅 채널의 경우 최소 권한의 보안 주체를 따르는 것이 좋습니다(사용자에게 작업을 완료하는 데 필요한 것보다 더 많은 권한을 제공하지 않음). 또한 채팅 애플리케이션 채팅 채널에서 Amazon Q Developer의 멤버십을 정기적으로 검토해야 합니다. 검토를 통해 적절한 대응 담당자와 기타 이해 관계자만 채팅 채널에 액세스할 수 있는지 확인할 수 있습니다.

채팅 애플리케이션의 Amazon Q Developer에서 생성된 Slack 채널 및 Microsoft Teams 채널에서 인시던트 대응 담당자는 Slack 또는 Microsoft Teams 애플리케이션에서 직접 여러 Incident Manager CLI 명령을 실행할 수 있습니다. 자세한 내용은 채팅 채널을 통한 상호작용 단원을 참조하십시오.

> **Important**
>
> 채팅 채널에 추가하는 사용자는 에스컬레이션 또는 대응 계획에 나열된 연락처와 동일해야 합니다. 이해 관계자 및 인시던트 관찰자와 같은 사용자를 채팅 채널에 추가할 수도 있습니다.

채팅 애플리케이션의 Amazon Q Developer에 대한 일반적인 내용은 채팅 애플리케이션의 Amazon Q Developer 관리자 안내서의 채팅 애플리케이션의 Amazon Q Developer란 무엇입니까?를 참조하세요.

다음 애플리케이션 중에서 선택하여 채널을 만들 수 있습니다.

Slack

이 절차의 단계는 모든 채널 사용자가 Incident Manager에서 채팅 명령을 사용할 수 있도록 하는 권장 권한 설정을 제공합니다. 지원되는 채팅 명령을 사용하면 인시던트 대응 담당자가 Slack 채팅 채널에서 인시던트를 직접 업데이트하고 상호 작용할 수 있습니다. 자세한 내용은 채팅 채널을 통한 상호작용을 참조하세요.

에서 채팅 채널을 생성하려면 Slack

- 자습서: 채팅 애플리케이션의 Amazon Q Developer 관리자 안내서의를 시작하고 Slack 구성에 다음을 포함하세요.
  - 10단계의 역할 설정에서 채널 역할을 선택합니다.
  - 10d단계의 정책 템플릿에서 Incident Manager 권한을 선택합니다.
  - 11단계의 채널 가드레일 정책에서 정책 이름에 대해 AWSIncidentManagerResolverAccess를 선택합니다.
  - 12단계의 SNS 주제 섹션에서 다음을 수행하십시오.
    - 리전 1에서 복제 세트에 포함된 AWS 리전 를 선택합니다.
    - 주제 1에서 채팅 채널에 인시던트 알림을 보내는 데 사용하기 위해 해당 리전에서 생성한 SNS 주제를 선택합니다.
    - 복제 세트의 각 추가 리전에 대해 다른 리전 추가를 선택하고 리전 및 SNS 주제를 추가합니다.

Microsoft Teams

이 절차의 단계는 모든 채널 사용자가 Incident Manager에서 채팅 명령을 사용할 수 있도록 하는 권장 권한 설정을 제공합니다. 지원되는 채팅 명령을 사용하면 인시던트 대응 담당자가 Microsoft Teams 채팅 채널에서 인시던트를 직접 업데이트하고 상호 작용할 수 있습니다. 자세한 내용은 채팅 채널을 통한 상호작용을 참조하세요.

에서 채팅 채널을 생성하려면 Microsoft Teams

- 자습서: 채팅 애플리케이션의 Amazon Q Developer 관리자 안내서Microsoft Teams의를 시작하고 구성에 다음을 포함하세요.
  - 10단계의 역할 설정에서 채널 역할을 선택합니다.
  - 10d단계의 정책 템플릿에서 Incident Manager 권한을 선택합니다.
  - 11단계의 채널 가드레일 정책에서 정책 이름에 대해 AWSIncidentManagerResolverAccess를 선택합니다.
  - 12단계의 SNS 주제 섹션에서 다음을 수행하십시오.
    - 리전 1에서 복제 세트에 포함된 AWS 리전 를 선택합니다.
    - 주제 1에서 채팅 채널에 인시던트 알림을 보내는 데 사용하기 위해 해당 리전에서 생성한 SNS 주제를 선택합니다.

- 복제 세트의 각 추가 리전에 대해 다른 리전 추가를 선택하고 리전 및 SNS 주제를 추가합니다.

Amazon Chime

Amazon Chime에서 채팅 채널을 만들려면

- 자습서: 채팅 애플리케이션의 Amazon Q Developer 관리자 안내서에서 Amazon Chime 시작하기의 단계를 따르고 구성에 다음을 포함합니다.
  - 11단계에서 정책 템플릿의 경우 Incident Manager 권한을 선택합니다.
  - 12단계의 SNS 주제 섹션에서 Amazon Chime 웹훅으로 알림을 전송할 SNS 주제를 선택합니다.
    - 리전 1에서 복제 세트에 포함된 AWS 리전 를 선택합니다.
    - 주제 1에서 채팅 채널에 인시던트 알림을 보내는 데 사용하기 위해 해당 리전에서 생성한 SNS 주제를 선택합니다.
    - 복제 세트의 각 추가 리전에 대해 다른 리전 추가를 선택하고 리전 및 SNS 주제를 추가합니다.

> **Note**
>
> 인시던트 대응 담당자가 Slack 및 채팅 채널에서 사용할 수 있는 Microsoft Teams 채팅 명령은 Amazon Chime에서 지원되지 않습니다.

작업 3: Incident Manager의 대응 계획에 채팅 채널 추가

대응 계획을 만들거나 업데이트할 때 대응 담당자가 의사소통하고 업데이트를 받을 수 있는 채팅 채널을 추가할 수 있습니다.

대응 계획 생성의 단계를 따를 때 (선택 사항) 인시던트 대응 채팅 채널 지정 섹션에서 이 대응 계획과 관련된 인시던트에 사용할 채널을 선택하십시오.

채팅 채널을 통한 상호작용

Slack 및의 채널의 경우 Microsoft TeamsIncident Manager를 사용하면 대응 담당자가 다음 `ssm-incidents` 명령을 사용하여 채팅 채널에서 직접 인시던트와 상호 작용할 수 있습니다.

- start-incident
- list-response-plan
- get-response-plan
- create-timeline-event
- delete-timeline-event
- get-incident-record
- get-timeline-event
- list-incident-records
- list-timeline-events
- list-related-items
- update-related-items
- update-incident-record
- update-timeline-event

진행 중인 인시던트의 채팅 채널에서 명령을 실행하려면 다음 형식을 사용하십시오. *cli-options*를 명령에 포함할 모든 옵션으로 바꾸십시오.

```
@aws ssm-incidents cli-options
```

예시:

```
@aws ssm-incidents start-incident --response-plan-arn arn:aws:ssm-
incidents::111122223333:response-plan/test-response-plan-chat --region us-east-2
```

```
@aws ssm-incidents create-timeline-event --event-data "\"example timeline event"\" --
event-time 2023-03-31 T20:30:00.000  --event-type Custom Event --incident-record-arn
 arn:aws:ssm-incidents::111122223333:incident-record/MyResponsePlanChat/98c397e6-7c10-
aa10-9b86-f199aEXAMPLE
```

```
@aws ssm-incidents list-incident-records
```

인시던트 해결을 위해 Incident Manager에 Systems Manager Automation 런북 통합

의 도구인 AWS Systems Manager Automation의 런북 AWS Systems Manager을 사용하여 AWS 클라우드 환경의 일반적인 애플리케이션 및 인프라 작업을 자동화할 수 있습니다.

각 런북은 관리형 노드 또는 기타 AWS 리소스 유형에서 Systems Manager가 수행하는 작업으로 구성된 런북 워크플로를 정의합니다. 런북을 사용하여 AWS 리소스의 유지 관리, 배포 및 문제 해결을 자동화할 수 있습니다.

Incident Manager에서는 런북이 인시던트 대응 및 완화를 주도하므로 대응 계획의 일부로 사용할 런북을 지정합니다.

대응 계획에서 일반적으로 자동화된 작업을 위해 미리 구성된 수십 개의 런북 중에서 선택하거나 사용자 지정 런북을 만들 수 있습니다. 대응 계획 정의에 런북을 지정하면 인시던트가 시작될 때 시스템에서 Runbook을 자동으로 시작할 수 있습니다.

> **Important**
>
> 크로스 리전 장애 조치로 생성된 인시던트는 대응 계획에 지정된 런북을 호출하지 않습니다.

Systems Manager Automation, 런북 및 Incident Manager를 통한 런북 사용에 대한 자세한 내용은 다음 주제를 참조하세요.

- 대응 계획에 런북을 추가하려면 Incident Manager에서 대응 계획 생성 및 구성 섹션을 참조하세요.
- 런북에 대해 자세히 알아보려면 AWS Systems Manager 사용 설명서의 AWS Systems Manager 자동화 및 AWS Systems Manager 자동화 런북 참조를 참조하세요.
- 런북 사용 비용에 대한 자세한 내용은 Systems Manager 요금을 참조하세요.
- Amazon CloudWatch 경보 또는 Amazon EventBridge 이벤트로 인시던트가 생성될 때 런북을 자동으로 호출하는 방법에 대한 자세한 내용은 자습서: Incident Manager를 통한 Systems Manager 자동화 런북 사용을 참조하세요.

주제

- 런북 정의
- Incident Manager 런북 템플릿

런북 워크플로를 시작하고 실행하는 데 필요한 IAM 권한

Incident Manager에는 인시던트 대응의 일환으로 런북을 실행할 권한이 필요합니다. 이러한 권한을 제공하려면 AWS Identity and Access Management (IAM) 역할, 런북 서비스 역할 및 자동화 *AssumeRole*를 사용합니다.

런북 서비스 역할은 필수 서비스 역할입니다. 이 역할은 Incident Manager에게 런북에 대한 워크플로에 액세스하고 시작하는 데 필요한 권한을 제공합니다.

자동화 AssumeRole은 런북에 지정된 개별 명령을 실행하는 데 필요한 권한을 제공합니다.

> **Note**
>
> AssumeRole을 지정하지 않으면 Systems Manager Automation은 개별 명령에 대해 런북 서비스 역할을 사용하려고 시도합니다. AssumeRole을 지정하지 않는 경우 런북 서비스 역할에 필요한 권한을 추가해야 합니다. 그렇지 않으면 런북이 해당 명령을 실행하지 못합니다. 하지만 최상의 보안을 위해 별도의 AssumeRole을 사용하는 것이 좋습니다. 별도의 AssumeRole을 사용하면 각 역할에 추가해야 하는 필수 권한을 제한할 수 있습니다.

자동화 AssumeRole에 대한 자세한 내용은 AWS Systems Manager 사용 설명서의 자동화를 위한 서비스 역할 (역할 수임) 액세스 구성을 참조하세요.

IAM 콘솔에서 두 가지 유형의 역할 중 하나를 직접 만들 수 있습니다. 대응 계획을 만들거나 업데이트할 때 Incident Manager에서 둘 중 하나를 대신 생성하도록 할 수도 있습니다.

런북 서비스 역할 권한

런북 서비스 역할 권한은 다음과 유사한 정책을 통해 제공됩니다.

첫 번째 명령문을 사용하면 Incident Manager가 Systems Manager StartAutomationExecution 작업을 시작할 수 있습니다. 그런 다음 이 작업은 세 가지 Amazon 리소스 이름(ARN) 형식으로 표시되는 리소스에 대해 실행됩니다.

두 번째 명령문은 해당 런북이 영향을 받는 계정에서 실행될 때 런북 서비스 역할이 다른 계정에서 역할을 맡도록 허용합니다. 자세한 내용은 AWS Systems Manager 사용 설명서의 여러 AWS 리전 및 계정에서 자동화 실행을 참조하세요.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "ssm:StartAutomationExecution",
      "Resource": [
        "arn:aws:ssm:*:{{DocumentAccountId}}:automation-definition/{{DocumentName}}:*",
        "arn:aws:ssm:*:{{DocumentAccountId}}:document/{{DocumentName}}:*",
        "arn:aws:ssm:*::automation-definition/{{DocumentName}}:*"
      ]
    },
    {
      "Effect": "Allow",
      "Action": "sts:AssumeRole",
      "Resource": "arn:aws:iam::*:role/AWS-SystemsManager-AutomationExecutionRole",
      "Condition": {
        "StringEquals": {
          "aws:CalledViaLast": "ssm.amazonaws.com"
        }
      }
    }
  ]
}
```

Automation AssumeRole 권한

대응 계획을 생성하거나 업데이트할 때 여러 AWS 관리형 정책 중에서 선택하여 Incident Manager가 생성하는 AssumeRole에 연결할 수 있습니다. 이러한 정책은 Incident Manager 런북 시나리오에서 사용되는 여러 가지 일반적인 작업을 실행할 수 있는 권한을 제공합니다. 이러한 관리형 정책 중 하나 이상을 선택하여 `AssumeRole` 정책에 대한 권한을 제공할 수 있습니다. 다음 표에는 Incident Manager 콘솔에서 `AssumeRole`을 생성할 때 선택할 수 있는 정책이 설명되어 있습니다.

AWS IAM 관리형 정책 이름	정책 설명
`AmazonSSMAutomationRole`	Systems Manager Automation 서비스에 런북 내에 정의된 활동을 실행할 수 있는 권한을 부여합니다. 관리자 및 신뢰할 수 있는 고급 사용자에게 이 정책을 할당합니다.

AWS IAM 관리형 정책 이름	정책 설명
AWSIncidentManagerResolverAccess	사용자에게 인시던트를 시작하고, 보고, 업데이트할 수 있는 권한을 부여합니다. 또한 이를 사용하여 인시던트 대시보드에서 고객 타임라인 이벤트 및 관련 항목을 만들 수 있습니다.

이러한 관리형 정책을 사용하여 여러 일반적인 인시던트 대응 시나리오에 대한 권한을 부여할 수 있습니다. 하지만 특정 작업에 필요한 권한은 다를 수 있습니다. 이러한 경우에는 사용자의 AssumeRole을 위한 추가 정책 권한을 제공해야 합니다. 자세한 내용은 AWS Systems Manager Automation 런북 참조를 참조하세요.

런북 파라미터 작업

대응 계획에 런북을 추가할 때 런북이 런타임에 사용해야 하는 파라미터를 지정할 수 있습니다. 대응 계획은 정적 값과 동적 값이 모두 있는 파라미터를 지원합니다. 정적 값의 경우 대응 계획에서 파라미터를 정의할 때 값을 입력합니다. 동적 값의 경우 시스템은 인시던트에서 정보를 수집하여 올바른 파라미터 값을 결정합니다. Incident Manager는 다음과 같은 동적 파라미터를 지원합니다.

`Incident ARN`

Incident Manager가 인시던트를 생성할 때 시스템은 해당 인시던트 레코드의 Amazon 리소스 이름(ARN)을 캡처하고 런북의 이 파라미터에 대해 입력합니다.

> **Note**
>
> 이 값은 String 유형의 파라미터에만 할당할 수 있습니다. 다른 유형의 파라미터에 할당하면 런북이 실행되지 않습니다.

`Involved resources`

Incident Manager가 인시던트를 생성하면 시스템은 인시던트와 관련된 리소스의 ARN을 캡처합니다. 그런 다음 이러한 리소스 ARN은 런북의 이 파라미터에 할당됩니다.

관련 리소스 정보

Incident Manager는 CloudWatch 경보, EventBridge 이벤트 및 수동으로 생성된 인시던트에 지정된 AWS 리소스의 ARNs으로 런북 파라미터 값을 채울 수 있습니다. 이 섹션에서는 Incident Manager가 이 파라미터를 채울 때 ARN을 캡처할 수 있는 다양한 유형의 리소스에 대해 설명합니다.

CloudWatch 경보

CloudWatch 경보 작업에서 인시던트가 생성되면 Incident Manager는 관련 지표에서 다음 유형의 리소스를 자동으로 추출합니다. 그런 다음 선택한 파라미터를 다음과 같은 관련 리소스로 채웁니다.

AWS 서비스	리소스 유형
Amazon DynamoDB	글로벌 보조 인덱스 스트림 표
Amazon EC2	이미지 인스턴스
AWS Lambda	함수 별칭 함수 버전 함수
Amazon Relational Database Service(Amazon RDS)	클러스터 데이터베이스 인스턴스
Amazon Simple Storage Service(S3)	버킷

EventBridge 규칙

시스템이 EventBridge 이벤트에서 인시던트를 생성하면 Incident Manager는 선택한 파라미터를 이벤트의 `Resources` 속성으로 채웁니다. 자세한 내용은 Amazon EventBridge 사용 설명서의 Amazon EventBridge 이벤트를 참조하세요.

수동으로 생성된 인시던트

StartIncient API 작업을 사용하여 인시던트를 생성하면 Incident Manager가 API 직접 호출의 정보를 사용하여 선택한 파라미터를 채웁니다. 특히, `relatedItems` 파라미터에 전달된 `INVOLVED_RESOURCE` 유형의 항목을 사용하여 파라미터를 채웁니다.

> **Note**
>
> `INVOLVED_RESOURCES` 값은 `StringList` 유형의 파라미터에만 할당할 수 있습니다. 다른 유형의 파라미터에 할당하면 런북이 실행되지 않습니다.

런북 정의

런북을 생성할 때 여기에 제공된 단계를 따르거나 Systems Manager 사용 설명서의 런북 작업 섹션에 제공된 자세한 안내서를 따를 수 있습니다. 다중 계정, 다중 리전 런북을 생성하는 경우 Systems Manager 사용 설명서의 여러 AWS 리전 및 계정에서 자동화 실행을 참조하세요.

런북 정의

1. https://console.aws.amazon.com/systems-manager/ Systems Manager 콘솔을 엽니다.
2. 탐색 창에서 Documents를 선택합니다.
3. Create automation(자동화 생성)을 선택합니다.
4. 고유하고 식별 가능한 런북 이름을 입력합니다.
5. 작업에 대한 설명을 입력합니다.
6. 자동화 문서가 수행할 IAM 역할을 제공합니다. 이렇게 하면 런북에서 명령을 자동으로 실행할 수 있습니다. 자세한 내용은 자동화 워크플로를 위한 서비스 역할 액세스 구성을 참조하세요.
7. (선택 사항) 런북에서 시작하는 입력 파라미터를 모두 추가합니다. 런북을 시작할 때 동적 또는 정적 파라미터를 사용할 수 있습니다. 동적 파라미터는 런북이 시작된 인시던트의 값을 사용합니다. 정적 파라미터는 사용자가 제공한 값을 사용합니다.
8. (선택 사항) 대상 유형을 추가합니다.
9. (선택 사항) 태그를 추가합니다.
10. 런북이 실행될 때 수행할 단계를 입력합니다. 각 단계에는 다음이 필요합니다.
    - 이름.
    - 단계의 용도에 대한 설명.

- 단계 중에 실행할 작업. 런북은 일시 중지 작업 유형을 사용하여 수동 단계를 설명합니다.
- (선택 사항) 명령 속성.

11. 필요한 모든 런북 단계를 추가한 후 자동화 생성을 선택합니다.

크로스 계정 기능을 활성화하려면 관리 계정의 런북을 인시던트 중에 해당 런북을 사용하는 모든 애플리케이션 계정과 공유하십시오.

런북 공유

1. https://console.aws.amazon.com/systems-manager/ Systems Manager 콘솔을 엽니다.
2. 탐색 창에서 Documents를 선택합니다.
3. 문서 목록에서 공유하고자 하는 문서를 선택한 후 세부 정보 보기를 선택합니다. [권한(Permissions)] 탭에서 자신이 문서의 소유자인지 확인합니다. 문서 소유자만이 문서를 공유할 수 있습니다.
4. 편집을 선택합니다.
5. 명령을 공개적으로 공유하려면 퍼블릭을 선택한 후, 저장을 선택합니다. 명령을 비공개로 공유하려면 비공개를 선택하고 AWS 계정 ID를 입력한 다음 권한 추가를 선택한 다음 저장을 선택합니다.

Incident Manager 런북 템플릿

Incident Manager는 팀이 Systems Manager 자동화에서 런북 작성을 시작하는 데 도움이 되는 다음과 같은 런북 템플릿을 제공합니다. 이 템플릿을 그대로 사용하거나 애플리케이션 및 리소스에 대한 세부 정보를 포함하도록 편집할 수 있습니다.

Incident Manager 런북 템플릿을 찾아보세요.

1. https://console.aws.amazon.com/systems-manager/ Systems Manager 콘솔을 엽니다.
2. 탐색 창에서 Documents를 선택합니다.
3. 문서 영역에서 검색 필드에 **`AWSIncidents-`**를 입력하여 모든 Incident Manager 런북을 표시합니다.

> **Tip**
>
> 문서 이름 접두사 필터 옵션을 사용하는 대신 **AWSIncidents-**를 자유 텍스트로 입력하십시오.

템플릿 사용

1. https://console.aws.amazon.com/systems-manager/ Systems Manager 콘솔을 엽니다.
2. 탐색 창에서 Documents를 선택합니다.
3. 문서 목록에서 업데이트하려는 템플릿을 선택합니다.
4. 내용 탭을 선택한 다음 문서의 내용을 복사합니다.
5. 탐색 창에서 Documents를 선택합니다.
6. Create automation(자동화 생성)을 선택합니다.
7. 고유하고 식별 가능한 이름을 입력합니다.
8. 편집기 탭을 선택합니다.
9. 편집을 선택합니다.
10. 복사한 세부 정보를 문서 편집기 영역에 붙여넣거나 입력합니다.
11. Create automation(자동화 생성)을 선택합니다.

AWSIncidents-CriticalIncidentRunbookTemplate

AWSIncidents-CriticalIncidentRunbookTemplate은 Incident Manager 인시던트 라이프사이클을 수동 단계로 제공하는 템플릿입니다. 이러한 단계는 대부분의 애플리케이션에서 사용할 수 있을 정도로 일반적이지만 대응 담당자가 인시던트 해결을 시작할 수 있을 만큼 상세합니다.

Incident Manager에서 대응 계획 생성 및 구성

대응 계획을 통해 사용자에게 영향을 미치는 인시던트에 대응하는 방법을 계획할 수 있습니다. 대응 계획은 참여 대상, 이벤트의 예상 심각도, 시작할 자동 런북, 모니터링할 지표에 대한 정보가 포함된 템플릿으로 작동합니다.

모범 사례

인시던트를 미리 계획하면 인시던트가 팀에 미치는 영향을 줄일 수 있습니다. 팀은 대응 계획을 설계할 때 다음 모범 사례를 고려해야 합니다.

- 간소화된 참여 — 인시던트에 가장 적합한 팀을 찾아내십시오. 배포 목록을 너무 광범위하게 구성하거나 잘못된 팀을 참여시키면 혼란을 야기하고 인시던트 발생 중 대응 시간을 낭비할 수 있습니다.
- 신뢰할 수 있는 에스컬레이션 — 대응 계획에 참여하려면 연락처나 대기 일정 대신 참여 계획을 선택하는 것이 좋습니다. 참여 계획에는 인시던트 발생 시 참여할 개별 연락처 또는 대기 일정(여러 명의 교대 연락처 포함)을 명시해야 합니다. 참여 계획에 지정된 대응 담당자에게 연락이 닿지 않는 경우가 있기 때문에 이러한 시나리오를 처리할 수 있도록 대응 계획에 백업 대응 담당자를 구성해야 합니다. 백업 연락처를 사용하면 1차 및 2차 연락처를 이용할 수 없거나 서비스 제공 시 예상치 못한 다른 간격이 있는 경우에도 Incident Manager는 연락처에게 인시던트에 대해 알립니다.
- 런북 — 런북을 사용하여 인시던트 중에 대응 담당자가 겪는 스트레스를 줄이는 반복 가능하고 이해하기 쉬운 단계를 제공합니다.
- 협업 — 채팅 채널을 사용하여 인시던트 발생 시 커뮤니케이션을 간소화합니다. 채팅 채널은 대응 담당자가 정보를 최신 상태로 유지하는 데 도움이 됩니다. 또한 이러한 채널을 통해 다른 대응 담당자와 정보를 공유할 수 있습니다.

대응 계획 생성

다음 절차를 사용하여 대응 계획을 만들고 인시던트 대응을 자동화하세요.

대응 계획을 생성하려면

1. Incident Manager 콘솔을 열고 탐색 창에서 대응 계획을 선택합니다.
2. 대응 계획 생성을 선택합니다.
3. 이름에는 Amazon 리소스 이름(ARN)에서 대응 계획에 사용할 고유하고 식별 가능한 대응 계획 이름을 입력합니다.
4. (선택 사항) 표시 이름에는 인시던트를 생성할 때 대응 계획을 식별하는 데 도움이 되도록 더 쉽게 이해할 수 있는 이름을 입력합니다.
5. 인시던트 기록의 기본값을 지정하여 계속하십시오.

인시던트 기본값 지정

인시던트를 보다 효과적으로 관리하는 데 도움이 되도록 기본값을 지정할 수 있습니다. Incident Manager는 이러한 값을 대응 계획과 관련된 모든 인시던트에 적용합니다.

인시던트 기본값을 지정하려면

1. 제목에는 Incident Manager 홈 페이지에서 쉽게 식별할 수 있도록 이 인시던트의 제목을 입력합니다.
2. 영향에서 이 대응 계획에서 생성된 인시던트의 잠재적 범위를 나타내는 영향 수준(예: 심각 또는 낮음)을 선택합니다. Incident Manager의 영향 등급에 대한 자세한 내용은 심사 섹션을 참조하세요
3. (선택 사항) 요약에는 이 대응 계획에서 생성된 인시던트 유형을 간략하게 요약하여 입력합니다.
4. (선택 사항) 중복 제거 문자열에는 중복 제거 문자열을 입력합니다. Incident Manager는 이 문자열을 사용하여 동일한 계정에서 동일한 근본 원인으로 인해 여러 인시던트가 생성되는 것을 방지합니다.

   중복 제거 문자열은 시스템에서 중복 인시던트를 확인하는 데 사용하는 용어 또는 문구입니다. 중복 제거 문자열을 지정하는 경우 Incident Manager는 인시던트를 생성할 때 `dedupeString` 필드에 동일한 문자열이 포함된 미해결 인시던트를 검색합니다. 중복이 감지되면 Incident Manager는 새 인시던트의 중복을 기존 인시던트에서 제거합니다.

   > **Note**
   >
   > 기본적으로 Incident Manager는 동일한 Amazon CloudWatch 경보 또는 Amazon EventBridge 이벤트로 생성된 여러 인시던트의 중복을 자동으로 제거합니다. 이러한 리소스 유형의 중복을 방지하기 위해 중복 제거 문자열을 직접 입력할 필요는 없습니다.

5. (선택 사항) 인시던트 태그에 이 대응 계획에서 생성된 인시던트에 할당할 태그 키와 값을 추가합니다.

   대응 계획 내에서 인시던트 태그를 설정하려면 인시던트 기록 리소스에 대한 `TagResource` 권한이 있어야 합니다.
6. 해결 담당자들이 인시던트에 대해 서로 소통할 수 있는 선택적 채팅 채널을 지정하여 계속하세요.

(선택 사항) 인시던트 대응 채팅 채널 지정

대응 계획에 채팅 채널을 포함하면 대응 담당자가 채널을 통해 인시던트 업데이트를 받게 됩니다. 채팅 명령을 사용하여 채팅 채널에서 직접 인시던트와 상호 작용할 수 있습니다.

채팅 애플리케이션에서 Amazon Q Developer를 사용하면 , Slack Microsoft Teams또는 Amazon Chime이 대응 계획에 사용할 채널을 생성할 수 있습니다. 채팅 애플리케이션에서 Amazon Q

Developer에서 채팅 채널을 생성하는 방법에 대한 자세한 내용은 채팅 애플리케이션의 Amazon Q Developer 관리자 안내서를 참조하세요.

> **Important**
>
> Incident Manager는 채팅 채널의 Amazon Simple Notification Service(Amazon SNS) 주제에 게시할 수 있는 권한이 있어야 합니다. 해당 SNS 주제에 게시할 권한이 없으면 해당 주제를 대응 계획에 추가할 수 없습니다. Incident Manager는 권한을 확인하기 위해 SNS 주제에 테스트 알림을 게시합니다.

채팅 채널에 대한 자세한 내용은 Incident Manager에서 대응 담당자를 위한 채팅 채널 생성 및 통합 섹션을 참조하세요.

인시던트 대응 채팅 채널을 지정하려면

1. 채팅 채널의 경우 채팅 애플리케이션 채팅 채널에서 대응 담당자가 인시던트 발생 시 통신할 수 있는 Amazon Q Developer를 선택합니다.

   > **Tip**
   >
   > 채팅 애플리케이션의 Amazon Q Developer에서 새 채팅 채널을 생성하려면 새 Chatbot 클라이언트 구성을 선택합니다.

2. 채팅 채널 SNS 주제에서 인시던트 중에 게시할 추가 SNS 주제를 선택합니다. SNS 주제를 여러 에 추가하면 인시던트 발생 시 리전이 중단될 경우 중복성이 AWS 리전 높아집니다.
3. 인시던트 중에 참여할 연락처, 대기 일정 및 에스컬레이션 계획을 선택하여 계속하십시오.

(선택 사항) 인시던트 대응에 참여할 리소스를 선택합니다.

인시던트 발생 시 가장 적절한 대응 담당자를 찾는 것이 중요합니다. 다음 모범 사례를 따르는 것이 좋습니다.

1. 에스컬레이션 계획에서 에스컬레이션 채널로 연락처 및 대기 일정을 추가하세요.

   > **Note**
   >
   > 현재 다른 계정에서 공유된 연락처를 대응 계획에 추가하는 기능은 지원되지 않습니다.

2. 에스컬레이션 계획을 대응 계획의 참여로 선택하십시오.

연락처 및 에스컬레이션 계획에 대한 자세한 내용은 Incident Manager에서 연락처 생성 및 구성 및 Incident Manager에서 대응자 참여를 위한 에스컬레이션 계획 생성 섹션을 참조하세요.

인시던트 대응에 참여할 리소스를 선택하려면

1. 참여에서 에스컬레이션 계획, 대기 일정 및 개별 연락처를 원하는 수만큼 선택할 수 있습니다.
2. 인시던트 완화의 일환으로 실행할 런북을 선택적으로 지정하여 계속하세요.

(선택 사항) 인시던트 완화를 위한 런북 지정

의 도구인 AWS Systems Manager Automation의 런북 AWS Systems Manager을 사용하여 AWS 클라우드 환경에서 일반적인 애플리케이션 및 인프라 작업을 자동화할 수 있습니다.

각 런북은 런북 워크플로를 정의합니다. 실행서 워크플로에는 Systems Manager가 관리형 노드 또는 기타 AWS 리소스 유형에서 수행하는 작업이 포함됩니다. Incident Manager에서 런북은 인시던트 대응 및 완화를 주도합니다.

대응 계획에 런북을 사용하는 방법에 대해 자세히 알아보려면 인시던트 해결을 위해 Incident Manager에 Systems Manager Automation 런북 통합을 참조하세요.

인시던트 완화를 위한 런북을 지정하려면

1. 런북에 대해 다음 중 하나를 수행합니다.
   - 템플릿에서 런북 복제를 선택하여 기본 Incident Manager 런북의 복사본을 만드십시오. 이름에 새로운 런북을 설명하는 이름을 입력합니다.
   - 기존 런북 선택을 선택합니다. 사용할 소유자, 런북, 버전을 선택합니다.

   > **Tip**
   >
   > 런북을 처음부터 새로 만들려면 새 런북 구성을 선택합니다.
   > 실행서 생성에 대한 자세한 내용은 인시던트 해결을 위해 Incident Manager에 Systems Manager Automation 런북 통합 섹션을 참조하세요.

2. 파라미터 영역에서 선택한 런북에 대해 요청된 파라미터를 입력합니다.

사용 가능한 파라미터는 런북에서 지정한 파라미터입니다. 런북마다 다른 파라미터가 필요할 수 있습니다. 일부 파라미터는 필수이고 다른 파라미터는 선택 사항일 수 있습니다.

대부분의 경우 Amazon EC2 인스턴스 ID 목록과 같은 파라미터의 정적 값을 수동으로 입력할 수 있습니다. 또한 Incident Manager가 인시던트에 의해 동적으로 생성된 파라미터 값을 제공하도록 할 수 있습니다.

3. (선택 사항) AutomationSummerole에서 사용할 AWS Identity and Access Management (IAM) 역할을 지정합니다. 이 역할에는 런북에 지정된 개별 명령을 실행하는 데 필요한 권한이 있어야 합니다.

> **Note**
>
> `AssumeRole`을 지정하지 않으면 Incident Manager는 Runbook 서비스 역할을 사용하여 런북 내에 지정된 개별 명령을 실행하려고 합니다.

다음 중에서 선택합니다.

- ARN 값 입력 - AssumeRole의 Amazon 리소스 이름(ARN)을 `arn:aws:iam::account-id:role/assume-role-name` 형식으로 수동으로 입력합니다. 예를 들어 **`arn:aws:iam::123456789012:role/MyAssumeRole`**입니다.
- 기존 서비스 역할 사용 — 계정의 기존 역할 목록에서 필요한 권한이 있는 역할을 선택합니다.
- 새 서비스 역할 생성 - AWS 관리형 정책 중에서 선택하여 AssumeRole에 연결합니다. 이 옵션을 선택한 후 AWS 관리형 정책의 경우 목록에서 정책을 하나 이상 선택합니다.

  새 역할에 제안된 기본 이름을 그대로 사용하거나 선택한 이름을 입력할 수 있습니다.

> **Note**
>
> 이 새 런북 서비스 역할은 선택한 특정 런북과 연결됩니다. 다른 런북과 함께 사용할 수 없습니다. 이는 정책의 리소스 섹션이 다른 런북을 지원하지 않기 때문입니다.

4. 런북 서비스 역할의 경우 런북 자체에 액세스하고 워크플로를 시작하는 데 필요한 권한을 제공하는 데 사용할 IAM 역할을 지정하십시오.

최소한 역할은 특정 런북에 대한 `ssm:StartAutomationExecution` 작업을 허용해야 합니다. 런북이 여러 계정에서 작동하려면 역할이 Incident Manager에서 AWS 계정 및 리전 간 인시

던트 관리 도중에 만든 AWS-SystemsManager-AutomationExecutionRole 역할에 대한 sts:AssumeRole 작업도 허용해야 합니다.

다음 중에서 선택합니다.

- 새 서비스 역할 생성 - Incident Manager가 런북 워크플로를 시작하는 데 필요한 최소 권한이 포함된 런북 서비스 역할을 자동으로 생성합니다.

  역할 이름의 경우 제안된 기본 이름을 그대로 사용하거나 선택한 이름을 입력할 수 있습니다. 제안된 이름을 사용하거나 이름에 런북 이름을 유지하는 것이 좋습니다. 이는 새 Assumerole이 선택한 특정 런북과 연결되며 다른 런북에 필요한 권한을 포함하지 않을 수 있기 때문입니다.

- 기존 서비스 역할 사용 - 사용자 또는 Incident Manager가 이전에 생성한 IAM 역할이 필요한 권한을 부여합니다.

  역할 이름에서 사용할 기존 역할의 이름을 선택합니다.

5. 추가 옵션을 확장하고 다음 중 하나를 선택하여 실행서 워크플로를 실행할 AWS 계정 를 지정합니다.

   - 대응 계획 소유자의 계정 - 실행서를 생성한에서 실행서 워크플로 AWS 계정 를 시작합니다.
   - 영향을 받은 계정 - 인시던트를 시작하거나 보고한 계정에서 런북 워크플로를 시작합니다.

     크로스 계정 시나리오에 Incident Manager를 사용하고 런북이 문제를 해결하기 위해 영향을 받는 계정의 리소스에 액세스해야 하는 경우 영향을 받는 계정을 선택하십시오.

6. 선택적으로 PagerDuty 서비스를 응답 계획에 통합하여 계속하십시오.

(선택 사항) PagerDuty 서비스를 응답 계획에 통합

PagerDuty 서비스를 응답 계획에 통합하려면

Incident Manager를 PagerDuty와 통합하면 PagerDuty는 Incident Manager가 인시던트를 생성할 때마다 해당 인시던트를 생성합니다. PagerDuty의 인시던트는 Incident Manager의 페이징 워크플로 및 에스컬레이션 정책 외에도 사용자가 정의한 페이징 워크플로 및 에스컬레이션 정책을 사용합니다. PagerDuty는 Incident Manager의 타임라인 이벤트를 인시던트에 대한 메모로 첨부합니다.

1. 타사 통합을 확장한 다음 PagerDuty 통합 활성화 확인란을 선택합니다.

2. 암호 선택에서 PagerDuty 계정에 액세스하기 위한 자격 증명을 저장하는 AWS Secrets Manager에서 암호를 선택합니다.

   Secrets Manager 암호에 PagerDuty 자격 증명을 저장하는 방법에 대한 자세한 내용은 AWS Secrets Manager 보안 암호에 PagerDuty 액세스 자격 증명 저장 섹션을 참조하세요.

3. PagerDuty 서비스의 경우 PagerDuty 인시던트를 생성하려는 PagerDuty 계정에서 서비스를 선택합니다.

4. 선택적 태그를 추가하고 대응 계획을 생성하여 계속하십시오.

태그 추가 및 대응 계획 생성

태그를 추가하고 대응 계획을 생성하려면

1. (선택 사항) 태그 영역에서 하나 이상의 태그 키 이름/값 쌍을 대응 계획에 적용합니다.

   태그는 리소스에 할당하는 선택적 메타데이터입니다. 태그를 사용하여 용도, 소유자 또는 환경을 기준으로 하는 등 리소스를 다양한 방식으로 분류할 수 있습니다. 예를 들어 대응 계획에 태그를 지정하여 완화 대상 인시던트 유형, 포함된 에스컬레이션 채널 유형 또는 관련된 에스컬레이션 계획을 식별할 수 있습니다. Incident Manager 리소스 태그 지정에 대한 자세한 내용은 Incident Manager의 리소스 태깅 섹션을 참조하세요.

2. 대응 계획 생성을 선택합니다.

Incident Manager에서 다른 서비스의 잠재적 인시던트 원인을 "결과"로 식별

Incident Manager에서 조사 결과는 인시던트 발생 시점 즈음에 발생했고 인시던트와 관련이 있을 가능성이 있는 하나 이상의 리소스와 관련된 AWS CodeDeploy 배포 또는 AWS CloudFormation 스택 업데이트에 대한 정보입니다. 각 발견을 인시던트의 잠재적 원인으로 조사할 수 있습니다. 이러한 잠재적 원인에 대한 정보는 인시던트의 인시던트 세부 정보 페이지에 추가됩니다. 이러한 배포 및 변경 사항에 대한 정보를 쉽게 확인할 수 있으므로 대응 담당자가 이 정보를 수동으로 검색할 필요가 없습니다. 이렇게 하면 잠재적 원인을 평가하는 데 필요한 시간이 줄어들어 인시던트의 평균 복구 시간 (MTTR) 을 줄일 수 있습니다.

현재 Incident Manager는 AWS 서비스AWS CodeDeploy 및의 두 가지 조사 결과 수집을 지원합니다AWS CloudFormation.

조사 결과는 옵트인 기능입니다. Incident Manager에 처음 온보딩할 때 준비 완료 마법사에서 활성화하거나 나중에 설정 페이지에서 활성화할 수 있습니다.

조사 결과 기능을 활성화하면 Incident Manager가 사용자를 대신하여 서비스 역할을 생성합니다. 이 서비스 역할에는 CodeDeploy 및 CloudFormation에서 결과를 검색하는 데 필요한 권한이 포함됩니다.

크로스 계정 시나리오에서 결과를 처리하려면 관리 계정에서 해당 기능을 활성화하세요. 그런 다음 AWS Resource Access Manager (AWS RAM) 조직의 각 애플리케이션 계정은 해당 서비스 역할을 생성해야 합니다.

조사 결과 기능을 사용하는 데 도움이 되는 다음 주제를 참조하세요.

주제

- 조사 결과에 대한 서비스 역할을 활성화하고 생성합니다.
- 크로스 계정 조사 결과 지원에 대한 권한 구성

조사 결과에 대한 서비스 역할을 활성화하고 생성합니다.

조사 결과 기능을 활성화하면 Incident Manager가 사용자를 대신하여 `IncidentManagerIncidentAccessServiceRole`이라는 서비스 역할을 생성합니다. 이 서비스 역할은 Incident Manager가 인시던트 생성 시기에 발생한 CodeDeploy 배포 및 CloudFormation 스택 업데이트에 대한 정보를 수집하는 데 필요한 권한을 제공합니다.

> **Note**
>
> 조직에서 Incident Manager를 사용하는 경우 관리 계정에 서비스 역할이 생성됩니다. 조직의 다른 계정에서 조사 결과를 처리하려면 각 애플리케이션 계정에서 서비스 역할을 만들어야 합니다. CloudFormation 템플릿을 사용하여 애플리케이션 계정에서 이 역할을 생성하는 방법에 대한 자세한 내용은 의 4단계를 참조하세요. 크로스 계정 인시던트 관리를 설정 및 구성합니다.

이 서비스 역할은 AWS 관리형 정책과 연결됩니다. 필요한 권한에 관한 자세한 내용은 이 안내서의 단원을 참조하세요.

Incident Manager 온보딩 프로세스 중에 조사 결과를 활성화하는 방법에 대한 자세한 내용은 Incident Manager 시작하기를 참조하세요.

온보딩 프로세스를 완료한 후 조사 결과를 활성화하는 방법에 대한 자세한 내용은 을 참조하세요. 조사 결과 기능 관리

크로스 계정 조사 결과 지원에 대한 권한 구성

에 설정된 조직이 있는 계정에서 조사 결과 기능을 사용하려면 AWS RAM각 애플리케이션 계정이 Incident Manager가 관리 계정의 서비스 역할을 대신 맡을 수 있는 권한을 구성해야 합니다.

이러한 권한은 역할을 AWS생성하는에서 제공하는 템플릿을 배포 AWS CloudFormation 하여 애플리케이션 계정에서 구성할 수 있습니다`IncidentManagerIncidentAccessServiceRole`.

애플리케이션 계정에서 이 템플릿을 다운로드하고 배포하는 방법에 대한 자세한 내용은 의 4단계를 참조하세요. Incident Manager에서 AWS 계정 및 리전 간 인시던트 관리

Incident Manager에서 자동으로 또는 수동으로 인시던트 생성

의 도구인 Incident Manager를 AWS Systems Manager사용하면 인시던트를 관리하고 신속하게 대응할 수 있습니다. CloudWatch 경보 및 EventBridge 이벤트에 따라 인시던트를 자동으로 생성하도록 Amazon CloudWatch 및 Amazon EventBridge를 구성할 수 있습니다. 인시던트 목록 페이지에서 수동으로 또는 AWS CLI 또는 AWS SDK의 StartIncident API 작업을 사용하여 인시던트를 생성할 수도 있습니다. Incident Manager는 동일한 CloudWatch 경보 또는 EventBridge 이벤트에서 생성된 인시던트를 동일한 인시던트로 중복 제거합니다.

CloudWatch 경보 또는 EventBridge 이벤트에 의해 자동으로 생성된 인시던트의 경우 Incident Manager는 이벤트 규칙 또는 경보 AWS 리전 와 동일한에서 인시던트를 생성하려고 시도합니다. 에서 Incident Manager를 사용할 수 없는 경우 AWS 리전 CloudWatch 또는 EventBridge는 복제 세트에 지정된 사용 가능한 리전 중 하나에 인시던트를 자동으로 생성합니다. 자세한 내용은 Incident Manager에서 AWS 계정 및 리전 간 인시던트 관리 단원을 참조하십시오.

시스템에서 인시던트를 생성하면 Incident Manager는 인시던트와 관련된 AWS 리소스에 대한 정보를 자동으로 수집하고이 정보를 관련 항목 탭에 추가합니다. 대응 계획에 런북을 지정한 경우 시스템에서 인시던트를 생성하면 Incident Manager가 인시던트와 관련된 AWS 리소스에 대한 정보를 런북으로 보낼 수 있습니다. 그러면 시스템에서 런북을 시작하고 문제를 해결하려고 시도할 때 해당 리소스를 대상으로 지정할 수 있습니다.

시스템이 인시던트를 생성하면 Systems Manager의 구성 요소인 OpsCenter에도 OpsItem이 생성되고 인시던트에 관련 항목으로 연결됩니다. 이 OpsItem을 사용하여 관련 작업과 향후 인시던트 분석을 추적할 수 있습니다. OpsCenter로 전화를 걸면 비용이 발생합니다. OpsCenter 요금에 대한 자세한 내용은 Systems Manager 가격을 참조하세요.

Important

다음과 같은 중요 세부 정보에 주의합니다.

- Incident Manager를 사용할 수 없는 경우 복제 세트에 두 개 이상의 리전을 지정한 AWS 리전 경우에만 시스템이 장애 조치하고 다른에서 인시던트를 생성할 수 있습니다. 복제 세트 구성에 대한 자세한 내용은 Incident Manager 시작하기 섹션을 참조하세요.
- 크로스 리전 장애 조치로 생성된 인시던트는 대응 계획에 지정된 런북을 호출하지 않습니다.

CloudWatch 경보를 사용하여 자동으로 인시던트 생성

CloudWatch는 CloudWatch 지표를 사용하여 환경 변화에 대해 경고하고 인시던트 시작 작업을 자동으로 수행합니다. CloudWatch는 Systems Manager 및 Incident Manager와 협력하여 경보가 경보 상태로 전환되면 대응 계획 템플릿에서 인시던트를 생성합니다. 이 자습서의 사전 요구 사항은 다음과 같습니다.

- Incident Manager가 구성되고 복제 세트가 생성되어 있습니다. 이 단계에서는 계정에 Incident Manager 서비스 연결 역할을 생성하여 필요한 권한을 제공합니다.
- 구성된 Incident Manager 대응 계획 Incident Manager 대응 계획을 구성하는 방법을 알아보려면 이 설명서의 인시던트 준비 섹션에서 Incident Manager에서 대응 계획 생성 및 구성을 참조하세요.
- 애플리케이션을 모니터링하는 CloudWatch 지표가 구성되어 있습니다. 모니터링 모범 사례는 이 설명서의 인시던트 준비 섹션에서 모니터링을 참조하세요.

인시던트 시작 작업으로 경보를 만들려면

1. CloudWatch에서 경보를 생성합니다. 자세한 내용은 Amazon CloudWatch 사용 설명서의 Amazon CloudWatch 경보 사용을 참조하세요.
2. 수행할 경보에 대한 작업을 선택할 때는 Systems Manager 작업 추가를 선택합니다.
3. 인시던트 생성을 선택하고 이 인시던트에 대한 대응 계획을 선택합니다.
4. 선택한 경보 유형 설명서의 나머지 단계를 완료하여 설치하세요.

> **Tip**
>
> 기존 경보에 인시던트 생성 작업을 추가할 수도 있습니다.

EventBridge 이벤트를 사용하여 자동으로 인시던트 생성

EventBridge 규칙은 이벤트 패턴을 감시합니다. 이벤트가 정의된 패턴과 일치하는 경우 Incident Manager는 선택한 대응 계획을 사용하여 인시던트를 생성합니다.

SaaS 파트너 이벤트를 사용하여 인시던트 생성

SaaS(Software as a Service) 파트너 애플리케이션 및 서비스로부터 이벤트를 수신하도록 EventBridge를 구성하여 타사 통합이 가능하도록 할 수 있습니다. 타사 파트너로부터 이벤트를 수신하

도록 EventBridge를 구성한 후 파트너 이벤트와 일치하는 규칙을 생성하여 인시던트를 생성할 수 있습니다. 타사 통합 목록을 보려면 SaaS 파트너로부터 이벤트 수신을 참조하세요.

SaaS 통합에서 이벤트를 수신하도록 EventBridge 구성

1. Amazon EventBridge 콘솔(https://console.aws.amazon.com/events/)을 엽니다.
2. 탐색 창에서 Partner event sources(파트너 이벤트 소스)를 선택하십시오.
3. 검색 막대를 사용하여 원하는 파트너를 찾고 해당 파트너에 대해 설정을 선택합니다.
4. 계정 ID를 클립보드에 복사하려면 복사를 선택하십시오.

> **Note**
>
> Salesforce와 통합하려면 Amazon AppFlow 사용 설명서에 설명된 단계를 사용하십시오.

5. 파트너 웹사이트로 이동하여 지침에 따라 파트너 이벤트 소스를 생성하십시오. 이를 위해 계정 ID를 사용하십시오. 생성한 이벤트 소스는 본인 계정에서만 사용할 수 있습니다.
6. EventBridge 콘솔로 돌아가서 탐색 창에서 파트너 이벤트 소스를 선택하세요.
7. 파트너 이벤트 소스 옆에 있는 버튼을 선택하고 Associate with event bus(이벤트 버스와 연결)를 선택하십시오.

SaaS 파트너의 이벤트에서 트리거되는 규칙 생성

1. https://console.aws.amazon.com/events/에서 Amazon EventBridge 콘솔을 엽니다.
2. 탐색 창에서 규칙을 선택합니다.
3. 규칙 생성을 선택합니다.
4. 규칙에 대해 이름과 설명을 입력하세요.

   규칙은 동일한 지역과 동일한 이벤트 버스의 다른 규칙과 동일한 이름을 가질 수 없습니다.
5. 이벤트 버스의 경우 이 파트너에 해당하는 이벤트 버스를 선택하십시오.
6. 규칙 유형(Rule type)에서 이벤트 패턴이 있는 규칙(Rule with an event pattern)을 생성합니다.
7. 다음을 선택합니다.
8. 이벤트 소스(Event source)에서 AWS 이벤트 또는 EventBridge 파트너 이벤트(Events or EventBridge partner events)를 선택합니다.
9. 이벤트 패턴에서 이벤트 패턴 양식을 선택합니다.

10. 이벤트 소스에서 EventBridge 파트너를 선택합니다.
11. 파트너에서 파트너 이름을 선택합니다.
12. 이벤트 유형(Event type)에 모든 이벤트(All Events)를 선택하거나 이 규칙에 사용할 이벤트 유형을 선택합니다. 모든 이벤트를 선택하면 이 파트너 이벤트 소스가 출력한 모든 이벤트가 규칙과 일치합니다.

    이벤트 패턴을 사용자 지정하려면 편집을 선택하고 변경한 후 저장을 선택하십시오.
13. 다음을 선택합니다.
14. 대상 선택에서 Incident Manager 대응 계획을 선택한 다음 대응 계획을 선택합니다.

> **Note**
>
> 대응 계획을 선택하면 소유하고 있고 계정과 공유된 모든 대응 계획이 대응 계획 드롭다운 목록에 나타납니다.

15. EventBridge는 규칙 실행에 필요한 IAM 역할을 생성할 수 있습니다.
    - IAM 역할을 자동으로 생성하려면 이 특정 리소스에 대해 새 역할 생성을 선택합니다.
    - 이전에 생성한 IAM 역할을 사용하려면 기존 역할 사용을 선택합니다.
16. 다음을 선택합니다.
17. (선택 사항)규칙에 대해 하나 이상의 태그를 입력하세요. 자세한 정보는 Amazon EventBridge 사용 설명서의 Amazon EventBridge 태그를 참조하세요.
18. 다음을 선택합니다.
19. 규칙을 검토한 다음 규칙 생성을 선택합니다.

AWS 서비스 이벤트를 사용하여 인시던트 생성

또한 EventBridge는 지원되는 AWS 서비스의 이벤트에 나열된 AWS 서비스로부터 이벤트를 수신합니다. SaaS 파트너에 대한 규칙을 구성하는 방법과 마찬가지로 AWS 서비스에 대한 규칙을 구성할 수 있습니다.

AWS 서비스의 이벤트에 대해 트리거되는 규칙 생성

1. https://console.aws.amazon.com/events/에서 Amazon EventBridge 콘솔을 엽니다.
2. 탐색 창에서 규칙을 선택합니다.

3. 규칙 생성을 선택합니다.
4. 규칙에 대해 이름과 설명을 입력하세요.

   규칙은 동일한 지역과 동일한 이벤트 버스의 다른 규칙과 동일한 이름을 가질 수 없습니다.
5. 이벤트 버스에서 기본값을 선택합니다.
6. 규칙 유형에서 이벤트 패턴이 있는 규칙을 선택합니다.
7. 다음을 선택합니다.
8. 이벤트 소스(Event source)에서 AWS 이벤트 또는 EventBridge 파트너 이벤트(Events or EventBridge partner events)를 선택합니다.
9. 이벤트 패턴에서 이벤트 패턴 양식을 선택합니다.
10. 이벤트 소스에서 AWS 서비스를 선택합니다.
11. 서비스 이름에서 인시던트를 모니터링하는 서비스를 선택합니다.
12. 이벤트 유형(Event type)에 모든 이벤트(All Events)를 선택하거나 이 규칙에 사용할 이벤트 유형을 선택합니다. 모든 이벤트를 선택하면 이 파트너 이벤트 소스가 출력한 모든 이벤트가 규칙과 일치합니다.

    이벤트 패턴을 사용자 지정하려면 편집을 선택하고 변경한 후 저장을 선택하십시오.
13. 다음을 선택합니다.
14. 대상 선택에서 Incident Manager 대응 계획을 선택한 다음 대응 계획을 선택합니다.

    > **Note**
    >
    > 대응 계획을 선택하면 소유하고 있고 계정과 공유된 모든 대응 계획이 대응 계획 드롭다운 목록에 나타납니다.
15. EventBridge는 규칙 실행에 필요한 IAM 역할을 생성할 수 있습니다.

    - IAM 역할을 자동으로 생성하려면 이 특정 리소스에 대해 새 역할 생성을 선택합니다.
    - 이전에 생성한 IAM 역할을 사용하려면 기존 역할 사용을 선택합니다.
16. 다음을 선택합니다.
17. (선택 사항)규칙에 대해 하나 이상의 태그를 입력하세요. 자세한 정보는 Amazon EventBridge 사용 설명서의 Amazon EventBridge 태그를 참조하세요.
18. 다음을 선택합니다.
19. 규칙을 검토한 다음 규칙 생성을 선택합니다.

인시던트 수동 생성

대응 담당자는 사전 정의된 대응 계획을 사용하여 Incident Manager 콘솔을 사용하여 인시던트를 수동으로 추적할 수 있습니다. 다음 단계에 따라 인시던트를 생성합니다.

1. Incident Manager 콘솔을 엽니다.
2. 인시던트 시작을 선택합니다.
3. 대응 계획의 경우 목록에서 대응 계획을 선택합니다.
4. (선택 사항) 정의된 대응 계획에서 제공하는 제목을 재정의하려면 인시던트 제목을 입력합니다.
5. (선택 사항) 정의된 대응 계획에서 제공하는 영향을 재정의하려면 인시던트의 영향을 입력합니다.

인시던트를 수동으로 시작하는 데 필요한 IAM 권한

인시던트를 수동으로 시작하려면 사용자가 Incident Manager 콘솔에 액세스하고, 대응 계획을 보고, 인시던트를 시작할 수 있는 권한이 필요합니다. 사용자가 인시던트를 시작하면 Incident Manager는 전달 액세스 세션(FAS)을 사용하여의 일부로 `StartEngagement` 호출합니다`StartIncident`.

다음 IAM 정책은 인시던트를 수동으로 시작하고, 인시던트를 생성할 수 있는 대응 계획을 보고, 인시던트가 생성된 후 인시던트를 보고 편집하는 데 필요한 권한을 제공합니다.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ssm-incidents:StartIncident",
                "ssm-incidents:GetResponsePlan",
                "ssm-incidents:ListResponsePlans",
                "ssm-incidents:TagResource",
                "ssm-incidents:GetIncidentRecord",
                "ssm-incidents:ListIncidentRecords",
                "ssm-incidents:UpdateIncidentRecord"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "ssm-contacts:StartEngagement"
```

```
            ],
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "aws:CalledViaFirst": "ssm-incidents.amazonaws.com"
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": [
                "ssm:CreateOpsItem"
            ],
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "aws:CalledViaFirst": "ssm-incidents.amazonaws.com"
                }
            }
        }
    ]
}
```

이 정책에는 다음 권한이 포함되어 있습니다.

- ssm-incidents:StartIncident - 사용자가 콘솔 또는 API를 사용하여 인시던트를 수동으로 시작할 수 있습니다. 이렇게 하면 대응 계획에서 새 인시던트 레코드가 생성됩니다.
- ssm-incidents:GetResponsePlan - 사용자가 특정 대응 계획에 대한 정보를 검색할 수 있습니다.
- ssm-incidents:ListResponsePlans - 사용자가 계정의 모든 대응 계획을 나열할 수 있도록 허용합니다.
- ssm-incidents:TagResource - 인시던트 및 대응 계획을 포함하여 Incident Manager 리소스에 태그를 추가할 수 있습니다.
- ssm-incidents:GetIncidentRecord - 사용자가 특정 인시던트에 대한 세부 정보를 검색할 수 있습니다.
- ssm-incidents:ListIncidentRecords - 사용자가 계정의 모든 인시던트를 나열할 수 있습니다.
- ssm-incidents:UpdateIncidentRecord - 사용자가 기존 인시던트의 세부 정보를 업데이트할 수 있도록 허용합니다.
- ssm-contacts:StartEngagement(조건 포함) - Incident Manager가 연락처와의 참여를 시작하도록 허용합니다. 이 조건은 Incident Manager를 통해서만 호출할 수 있도록 합니다.

- ssm:CreateOpsItem(조건 포함) - Incident Manager가 OpsCenter에서 OpsItem을 생성할 수 있도록 허용합니다. OpsCenter 이 조건은 Incident Manager를 통해서만 호출할 수 있도록 합니다.

aws:CalledViaFirst 조건 키는 요청이 Incident Manager 서비스를 통해 오는 경우에만 특정 권한(예: `StartEngagement`)을 사용할 수 있도록 합니다. 이 접근 방식은 서비스 연결 역할 대신 FAS를 사용하여 보안 위험을 초래할 수 있는 잠재적 교차 계정 호출을 방지합니다.

Incident Manager 콘솔에서 인시던트 세부 정보 보기

AWS Systems Manager Incident Manager는 인시던트가 감지된 순간부터 해결 및 인시던트 후 분석을 통해 인시던트를 추적합니다. 모든 인시던트는 Incident Manager 콘솔의 인시던트 목록 페이지에서 찾을 수 있으며, 여기에는 인시던트 세부 정보로 바로 연결되는 링크가 있습니다.

주제

콘솔에서 인시던트 목록 보기

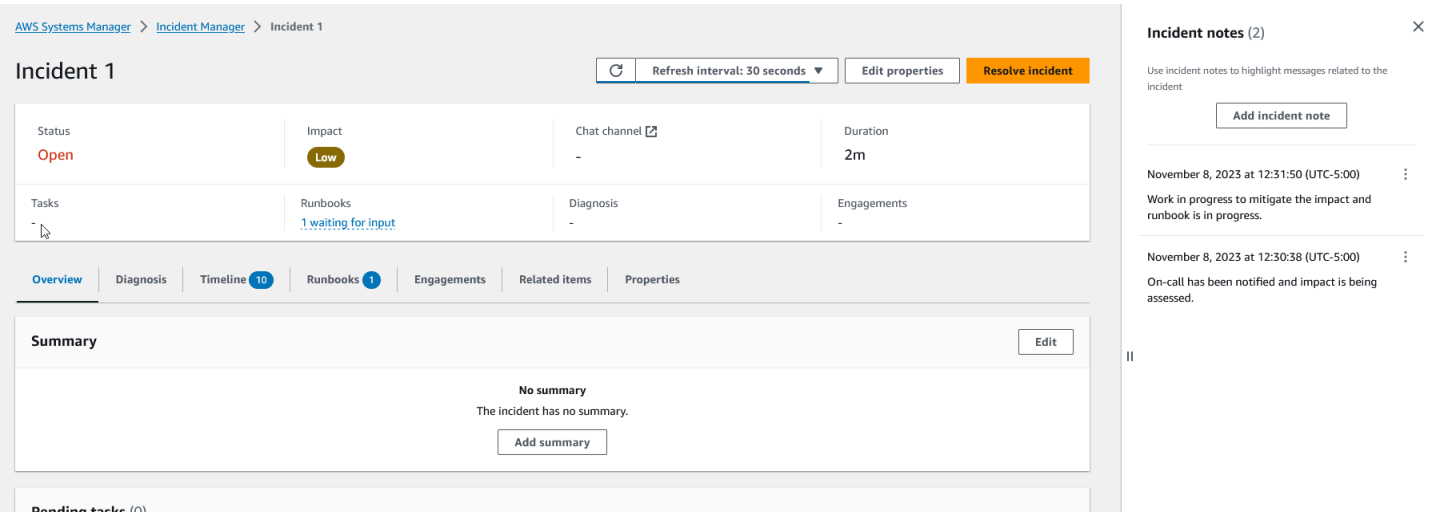
인시던트 목록 페이지에는 미해결 인시던트, 해결된 인시던트 및 분석이라는 세 개의 섹션이 있습니다. 이 페이지에서 새 인시던트를 수동으로 추적하고 분석을 생성할 수 있습니다. 인시던트를 수동으로 추적하는 방법에 대해 자세히 알아보려면 이 설명서의 인시던트 생성 섹션에서 인시던트 수동 생성을 참조하세요. 인시던트 사후 분석에 대해 알아보려면 이 설명서의 Incident Manager에서 인시던트 사후 분석 수행 섹션을 참조하세요.

인시던트 세부 정보에는 미해결 인시던트가 해당 인시던트의 제목, 영향, 기간 및 채팅 채널과 함께 타일로 표시됩니다. 인시던트를 해결하면 해당 인시던트는 해결된 인시던트 목록으로 이동합니다. 분석은 두 번째 탭에 있습니다.

콘솔에서 인시던트 세부 정보 보기

인시던트 세부 정보 페이지는 인시던트를 관리하는 데 사용할 수 있는 세부 정보와 도구를 제공합니다. 이 페이지에서 런북을 시작하여 인시던트를 완화하고, 인시던트 노트를 추가하고, 다른 해결 담당자를 참여시키고, 타임라인, 지표, 속성 및 관련 리소스와 같은 인시던트 세부 정보를 볼 수 있습니다.

다음 이미지와 같이 인시던트 세부 정보 페이지에는 상위 배너, 인시던트 메모, 추가 정보와 리소스가 포함된 7개의 탭 등 여러 섹션이 포함되어 있습니다. 기본적으로 상위 배너 및 인시던트 정보 섹션은 모든 인시던트 세부 정보 페이지에 표시됩니다.



이 항목에서는 인시던트 세부 정보 페이지의 요소와 이 페이지에서 수행할 수 있는 작업에 대해 설명합니다.

상단 배너

모든 인시던트 세부 정보 페이지의 상단 배너에는 다음 정보가 포함됩니다.

- 상태 — 인시던트의 현재 상태는 미결 또는 해결일 수 있습니다.
- 영향 — 인시던트가 환경에 미치는 영향. 높음, 중간, 낮음일 수 있습니다. 인시던트의 영향을 변경하려면 속성 편집을 선택합니다.
- 채팅 채널 - 인시던트 업데이트 및 알림을 볼 수 있는 채팅 채널에 액세스할 수 있는 링크입니다.
- 기간 — 대응 담당자가 인시던트를 해결하기까지 경과한 시간입니다.
- 런북 — 이 인시던트와 관련된 런북의 상태입니다. 상태는 입력 대기 중, 성공 또는 실패일 수 있습니다. 런북의 상태가 입력 대기 상태인 경우 해당 런북을 선택하여 작업 세부 정보를 볼 수 있습니다. 실패를 선택하여 시간 초과, 실패 또는 취소된 런북을 볼 수 있습니다.
- 참여 — 총 참여수와 각 참여의 상태입니다. 참여를 생성하면 참여 상태가 참여로 표시됩니다. 참여를 확인하면 상태가 참여됨에서 승인됨으로 바뀝니다. Incident Manager는 타사 참여 승인을 지원하지 않습니다. 이러한 참여는 참여 상태로 유지됩니다.

배너 오른쪽 상단의 편집을 선택하여 인시던트 제목, 영향 및 채팅 채널을 편집할 수 있습니다.

Incident Manager

화면 오른쪽에는 인시던트 메모 섹션이 표시됩니다. 메모를 사용하면 인시던트를 처리하는 다른 사용자와 협업하고 소통할 수 있습니다. 적용한 완화 조치, 식별한 잠재적 근본 원인 또는 인시던트의 현재

상태를 설명할 수 있습니다. 가장 좋은 방법은 인시던트 메모 섹션을 사용하여 상태 업데이트 및 본인 또는 다른 사람이 인시던트에 대해 취하는 조치를 게시하는 것입니다. 다른 해결 담당자와 실시간으로 소통해야 하는 경우 Incident Manager에서 사용할 수 있는 채팅 채널을 사용하세요.

메모를 추가하려면 인시던트 메모 추가 버튼을 선택한 다음 메모를 입력합니다. 메모에는 인시던트 상태에 대한 업데이트 또는 다른 사용자에게 정보를 제공하는 기타 관련 정보가 포함될 수 있습니다. 필요한 경우 인시던트 메모를 편집하거나 삭제할 수도 있습니다.

> **Note**
>
> `ssm-incidents:UpdateTimelineEvent` 및 `ssm-incidents:DeleteTimelineEvent` 작업을 실행할 수 있는 IAM 권한을 가진 모든 사용자는 메모를 편집하고 삭제할 수 있습니다. 하지만 다른 계정과 인시던트를 공유하는 경우 리소스 정책에는 해당 `ssm-incidents:DeleteTimelineEvent` 작업이 포함되지 않습니다. 이렇게 하면 인시던트를 공유하는 사용자가 메모를 삭제할 수 없습니다. AWS CloudTrail 콘솔에서 Incident Manager 이벤트의 메모에 대한 감사 기록을 볼 수 있습니다.

탭

인시던트 세부 정보 페이지에는 7개의 탭이 있어 대응 담당자가 인시던트 중에 정보를 쉽게 찾고 볼 수 있습니다. 탭 이름에는 탭의 업데이트 수를 나타내는 카운터가 표시됩니다. 각 탭의 내용 및 사용 가능한 작업에 대한 자세한 내용은 해당 섹션을 참조하세요.

개요

개요 탭은 대응 담당자를 위한 시작 페이지입니다. 여기에는 인시던트 요약, 최근 타임라인 이벤트 목록, 현재 런북 단계가 포함됩니다.

대응 담당자는 요약을 사용하여 취해진 조치, 변경 결과, 가능한 다음 단계 및 인시던트의 영향에 대한 정보를 파악합니다. 요약을 업데이트하려면 요약 섹션의 오른쪽 상단에서 편집을 선택합니다.

> **Important**
>
> 여러 대응 담당자가 요약 필드를 동시에 편집하는 경우 편집 내용을 제출한 대응 담당자가 마지막으로 다른 모든 입력을 덮어씁니다.

최근 타임라인 이벤트 섹션에는 Incident Manager가 가장 최근 이벤트 5개로 채운 타임라인이 있습니다. 이 섹션을 사용하여 인시던트 상태와 최근에 발생한 상황을 파악할 수 있습니다. 전체 타임라인을 보려면 타임라인 탭으로 이동하십시오.

개요 페이지에는 현재 런북 단계도 표시됩니다. 이 단계는 AWS 환경에서 실행되는 자동 단계이거나 대응 담당자를 위한 수동 지침 세트일 수 있습니다. 이전 단계와 다음 단계를 포함한 전체 런북을 보려면 런북 탭을 선택하십시오.

진단

진단 탭에는 지표에 대한 정보와 활성화된 경우 조사 결과에 대한 정보를 포함하여 호스트된 AWS 애플리케이션 및 시스템에 대한 중요한 정보가 들어 있습니다.

지표 작업

Incident Manager는 Amazon CloudWatch를 사용하여 이 탭에 있는 지표와 경보 그래프를 채웁니다. 경보 및 지표 정의를 위한 인시던트 관리 모범 사례에 대해 자세히 알아보려면 이 사용 설명서의 인시던트 계획 섹션에서 모니터링을 참조하세요.

지표를 추가하려면

- 이 탭의 오른쪽 위 모서리에서 추가를 선택합니다.
  - 기존 CloudWatch 대시보드의 지표를 추가하려면 기존 CloudWatch 대시보드에서를 선택합니다.

    a. 대시보드를 선택합니다. 그러면 선택한 대시보드에 속하는 모든 지표와 경보가 추가됩니다.

    b. (선택 사항) 대시보드에서 지표를 선택하여 특정 지표를 볼 수도 있습니다.
  - CloudWatch에서를 선택하고 지표 소스를 붙여넣어 단일 지표를 추가합니다. 지표 소스를 복사하려면:

    a. https://console.aws.amazon.com/cloudwatch/에서 CloudWatch 콘솔을 엽니다.

    b. 탐색 창에서 지표를 선택합니다.

    c. 모든 지표 탭의 검색 필드에 검색어(예: 지표 이름 또는 리소스 이름)를 입력하고 입력을 선택합니다.

    예를 들어, `CPUUtilization` 지표를 검색하면 이 지표와 함께 네임스페이스와 차원이 표시됩니다.

    d. 지표 검색을 위해 결과 중 하나를 선택합니다.

e. 소스 탭을 선택하고 소스를 복사합니다.

지표 경보 그래프는 관련 대응 계획을 통해 또는 지표를 추가할 때 기존 CloudWatch 대시보드에서를 선택해야만 인시던트 세부 정보에 추가할 수 있습니다.

지표를 제거하려면 제거를 선택한 다음 제공된 지표 드롭다운에서 제거하려는 지표를 선택합니다.

AWS CodeDeploy 및에서 결과 보기 AWS CloudFormation

조사 결과를 활성화하고 필요한 모든 권한을 구성하면 특정 인시던트와 관련이 있을 수 있는 모든 조사 결과가 인시던트에 연결됩니다. 대응 담당자는 인시던트 세부 정보 페이지에서 이러한 조사 결과에 대한 정보를 볼 수 있습니다.

CodeDeploy 및 CloudFormation의 조사 결과를 보려면

1. Incident Manager 콘솔을 엽니다.
2. 조사할 인시던트의 이름을 선택합니다.
3. 진단 탭의 조사 결과 영역에서 보고된 모든 조사 결과의 시작 시간을 인시던트 시작 시간과 비교합니다.
4. 조사 결과에 대한 자세한 내용을 보려면 참조 열에서 CodeDeploy 또는 CloudFormation 조사 결과에 대한 링크를 선택합니다.

타임라인

타임라인 탭을 사용하여 인시던트 중에 발생하는 이벤트를 추적할 수 있습니다. Incident Manager는 타임라인 이벤트를 자동으로 채워 인시던트 중에 발생한 중요한 사건을 식별합니다. 대응 담당자는 수동으로 탐지된 사건을 기반으로 사용자 지정 이벤트를 추가할 수 있습니다. 인시던트 사후 분석 중에 타임라인 탭은 향후 인시던트에 더 잘 대비하고 대응하는 방법에 대한 귀중한 통찰력을 제공합니다. 인시던트 사후 분석에 대한 자세한 내용은 Incident Manager에서 인시던트 사후 분석 수행 섹션을 참조하세요.

사용자 지정 타임라인 이벤트를 추가하려면 추가를 선택합니다. 달력을 사용하여 날짜를 선택한 다음 시간을 입력합니다. 모든 시간은 현지 시간대로 표시됩니다. 타임라인에 나타나는 이벤트에 대한 간략한 설명을 입력합니다.

기존 사용자 지정 이벤트를 편집하려면 타임라인에서 이벤트를 선택하고 편집을 선택합니다. 사용자 지정 이벤트의 시간, 날짜 및 설명을 변경할 수 있습니다. 사용자 지정 이벤트만 편집할 수 있습니다.

런북

인시던트 세부 정보 페이지의 런북 탭에서는 대응 담당자가 런북 단계를 보고 새 런북을 시작할 수 있습니다.

새 런북을 시작하려면 런북 섹션에서 런북 시작을 선택합니다. 검색 필드를 사용하여 시작하려는 런북을 찾습니다. 필요한 파라미터와 런북을 시작할 때 사용할 런북의 버전을 모두 입력합니다. 런북 탭에서 인시던트 중에 시작된 런북은 현재 로그인한 계정의 권한을 사용합니다.

Systems Manager에서 런북 정의로 이동하려면 런북에서 해당 런북 제목을 선택합니다. Systems Manager에서 실행 중인 런북 인스턴스로 이동하려면 실행 세부 정보에서 실행 세부 정보를 선택합니다. 이 페이지에는 런북을 시작하는 데 사용된 템플릿과 현재 실행 중인 자동화 문서 인스턴스의 특정 세부 정보가 표시됩니다.

런북 단계 섹션에는 선택한 런북이 자동으로 수행하거나 대응 담당자가 수동으로 수행하는 단계 목록이 표시됩니다. 단계가 현재 단계가 되면 단계가 확장되어 단계를 완료하는 데 필요한 정보나 단계가 수행하는 작업에 대한 세부 정보가 표시됩니다. 자동 런북 단계는 자동화가 완료된 후에 해결됩니다. 수동 단계를 수행하려면 대응 담당자가 각 단계 하단에서 다음 단계를 선택해야 합니다. 단계가 완료되면 단계 출력이 드롭다운으로 표시됩니다.

런북 실행을 취소하려면 런북 취소를 선택합니다. 이렇게 하면 런북 실행이 중지되고 런북의 추가 단계가 완료되지 않습니다.

참여

인시던트 세부 정보의 참여 탭은 대응 담당자와 팀의 참여를 유도합니다. 이 탭에서는 누가 참여했는지, 누가 대응했는지, 에스컬레이션 계획의 일환으로 참여할 대응 담당자를 확인할 수 있습니다. 대응 담당자는 이 탭에서 직접 다른 담당자를 참여시킬 수 있습니다. 연락처 및 에스컬레이션 계획을 만드는 방법에 대해 자세히 알아보려면 이 설명서의 Incident Manager에서 연락처 생성 및 구성 및 Incident Manager에서 대응자 참여를 위한 에스컬레이션 계획 생성 섹션을 참조하세요.

연락처 및 에스컬레이션 계획을 포함한 대응 계획을 구성하여 인시던트 초기에 자동으로 참여를 시작할 수 있습니다. 대응 계획 구성에 대한 자세한 내용은 이 설명서의 Incident Manager에서 대응 계획 생성 및 구성 섹션을 참조하세요.

표에서 각 연락처 정보를 확인할 수 있습니다. 이 표에는 다음 정보가 포함되어 있습니다.

- 이름 - 연락 방법 및 참여 계획이 표시된 연락처 세부 정보 페이지로 연결되는 링크입니다.
- 에스컬레이션 계획 — 해당 연락처를 참여시킨 에스컬레이션 계획으로 연결되는 링크입니다.

- 고객 응대 소스 - AWS Systems Manager 또는 PagerDuty와 같이이 고객 응대와 관련된 서비스를 식별합니다.
- 참여됨 — 계획에서 연락처를 참여시킨 시점 또는 에스컬레이션 계획의 일환으로 연락처를 참여시켜야 하는 시점을 표시합니다.
- 승인됨 — 연락처가 참여를 승인했는지 여부를 표시합니다.

참여를 승인하기 위해 대응 담당자는 다음 중 하나를 수행할 수 있습니다.

- 전화 통화 - 메시지가 표시되면 **1**을 입력합니다.
- SMS — 제공된 코드를 사용하여 메시지에 회신하거나 인시던트의 참여 탭에 제공된 코드를 입력합니다.
- 이메일 — 인시던트의 참여 탭에 제공된 코드를 입력합니다.

관련 항목

관련 항목 탭은 인시던트 완화와 관련된 리소스를 수집하는 데 사용됩니다. 이러한 리소스는 ARN, 외부 리소스에 대한 링크 또는 Amazon S3 버킷에 업로드된 파일일 수 있습니다. 표에는 설명이 포함된 제목과 ARN, 링크 또는 버킷 세부 정보가 표시됩니다. S3 버킷을 사용하기 전에 Amazon S3 사용 설명서에서 Amazon S3의 보안 모범 사례를 검토하십시오.

파일을 Amazon S3 버킷에 업로드하면 해당 버킷에서 버전 관리가 활성화되거나 일시 중단됩니다. 버킷에서 버전 관리를 활성화하면 기존 파일과 같은 이름으로 업로드된 파일이 새 버전의 파일로 추가됩니다. 버전 관리가 일시 중단되면 기존 파일과 같은 이름으로 업로드된 파일이 기존 파일을 덮어씁니다. 버전 관리에 대해 자세히 알아보려면 Amazon S3 사용 설명서의 S3 버킷에서의 버전 관리 사용을 참조하세요.

파일 관련 항목을 제거하면 파일이 인시던트에서 제거되지만 Amazon S3 버킷에서는 제거되지 않습니다. Amazon S3 버킷에서 객체를 제거하는 방법에 대한 자세한 내용은 Amazon S3 사용 설명서의 Amazon S3 객체 삭제를 참조하세요.

속성

속성 탭은 인시던트에 대한 다음 세부 정보를 제공합니다.

인시던트 속성 섹션에서 다음을 확인할 수 있습니다.

- 상태 - 인시던트의 현재 상태를 설명합니다. 인시던트는 미해결 상태이거나 해결되었을 수 있습니다.

- 시작 시간 - Incident Manager에서 인시던트가 생성된 시간입니다.
- 해결 시간 - Incident Manager에서 인시던트가 해결된 시간입니다.
- Amazon 리소스 이름(ARN) — 인시던트의 ARN입니다. 채팅 또는 AWS Command Line Interface (AWS CLI) 명령에서 인시던트를 참조할 때는 ARN을 사용하십시오.
- 대응 계획 - 선택한 인시던트에 대한 대응 계획을 식별합니다. 대응 계획을 선택하면 대응 계획의 세부 정보 페이지가 열립니다.
- 상위 OpsItem — 인시던트의 상위 항목으로 생성된 OpsItem을 식별합니다. 상위 OpsItem에는 여러 관련 인시던트 및 후속 조치 항목이 있을 수 있습니다. 상위 OpsItem을 선택하면 OpsCenter에서 OpsItem 세부 정보 페이지가 열립니다.
- 분석 — 이 인시던트에서 생성된 분석을 식별합니다. 해결된 인시던트를 바탕으로 분석을 생성하여 인시던트 대응 프로세스를 개선하십시오. 분석을 선택하여 분석 세부 정보 페이지를 엽니다.
- 소유자 - 인시던트가 생성된 계정입니다.

태그 섹션에서 인시던트 기록과 관련된 태그 키와 값을 보고 편집할 수 있습니다. Incident Manager의 태그에 대한 자세한 내용은 Incident Manager의 리소스 태깅 섹션을 참조하세요.

Incident Manager에서 인시던트 사후 분석 수행

인시던트 사후 분석은 탐지 및 완화 시간을 포함하여 인시던트 대응에 대한 개선 사항을 식별하는 과정을 안내합니다. 분석을 통해 인시던트의 근본 원인을 이해하는 데도 도움이 될 수 있습니다. Incident Manager는 인시던트 대응을 개선하기 위한 권장 조치 항목을 생성합니다.

인시던트 사후 분석의 이점

- 인시던트 대응 개선
- 문제의 근본 원인 파악
- 실행 가능한 조치 항목으로 근본 원인 해결
- 인시던트의 영향 분석
- 조직 내에서 학습한 내용을 캡처 및 공유

분석을 사용하지 말아야 할 경우

분석에는 비난하는 내용이 없고 사람의 이름을 언급하지 않습니다.

“우리가 발견한 내용이 무엇이든, 우리는 모든 사람이 당시에 자신이 알고 있는 것, 자신의 기술과 능력, 가용한 자원, 당면한 상황을 고려하여 최선을 다했다는 것을 알고 있고 진심으로 그렇게 믿고 있습니다.” - Norm Kerth, 프로젝트 회고 조사: 팀 검토를 위한 핸드북

분석 세부 정보

분석 세부 정보 페이지는 정보 수집, 개선 사항 평가, 조치 항목 생성 과정을 안내합니다. 분석 세부 정보 페이지는 과거 지표, 편집 가능한 타임라인, 향후 인시던트를 개선하기 위한 질문 등 몇 가지 주요 차이점을 제외하고 인시던트 세부 정보와 유사합니다.

개요

개요는 인시던트를 요약한 것입니다. 이 요약에는 배경, 발생 항목, 발생 원인, 완화 방법, 기간, 인시던트 재발을 방지하기 위한 주요 조치 항목이 포함됩니다. 개요는 개략적인 내용입니다. 분석의 질문 탭에서 자세한 내용을 살펴볼 수 있습니다.

Metrics

지표 탭을 사용하면 인시던트 기간 동안 애플리케이션의 주요 지표를 시각화할 수 있습니다. 동일한 그래프에 하나 이상의 지표가 표시된 지표 그래프를 여기에 추가할 수 있습니다. 인시던트 중에 사용된

지표는 이 탭에 자동으로 채워집니다. 인시던트 발생 중 주요 시점에 대한 설명, 제목 및 주석을 추가하는 것이 좋습니다.

지표 그래프를 분석할 때 고려할 수 있는 몇 가지 주요 시점은 다음과 같습니다.

- 배포 변경
- 구성 변경
- 인시던트 시작 시간
- 경보 이름
- 참여 시간
- 완화 시작 시간
- 인시던트 해결 시간

제한 사항

- CloudWatch 경보 및 지표 표현식은 인시던트에서 가져오지 않습니다.
- Incident Manager가 지원하지 않는 리전에 있는 지표는 인시던트에서 가져오지 않습니다.
- 분석을 생성하기 전에 애플리케이션 계정의 지표에 `CloudWatch-CrossAccountSharingRole`의 구성이 필요합니다. 자세한 내용은 Amazon CloudWatch 사용 설명서의 크로스 계정 크로스 리전 CloudWatch 콘솔을 참조하세요.

타임라인

인시던트에 대한 심도 있는 이해를 위해 타임라인의 주요 시점을 설명합니다. 이 탭에서 인시던트 타임라인이 자동으로 채워집니다. 분석과 관련이 없는 시점을 삭제할 수 있습니다. 또한 시점을 추가하고 편집하여 인시던트와 그 영향을 더 정확하게 설명할 수 있습니다.

타임라인 탭을 사용하면 질문 탭에 있는 인시던트 대응에 대한 질문에 답할 수 있습니다.

Questions

Incident Manager 질문을 사용하면 애플리케이션에서 인시던트를 해결하는 데 걸리는 시간을 단축하고 인시던트 발생을 줄일 수 있습니다. 질문에 답할 때 지표 및 타임라인 탭을 업데이트하여 정확성을 높이십시오. 질문은 인시던트 대응의 다음과 같은 주요 측면에 초점을 맞춥니다.

- 탐지 — 탐지 시간을 단축할 수 있습니까? 인시던트를 더 빨리 감지할 수 있는 지표 및 경보 업데이트가 있습니까?

- 진단 — 진단 시간을 단축할 수 있습니까? 대응 계획이나 에스컬레이션 계획에 올바른 대응 담당자를 더 빨리 투입할 수 있는 업데이트가 있습니까?
- 완화 — 완화 시간을 단축할 수 있습니까? 추가하거나 개선할 수 있는 런북 단계가 있습니까?
- 예방 — 미래의 인시던트 발생을 예방할 수 있습니까? 인시던트의 근본 원인을 파악하기 위해 Amazon은 문제 조사에 5-Whys 접근 방식을 사용합니다.

작업

Incident Manager는 사용자가 질문을 완료하면서 검토할 수 있도록 권장 조치 항목을 생성합니다. 이 탭에서 이러한 작업을 수락하고 완료하거나 취소할 수 있습니다. 취소된 조치 항목을 선택하여 취소된 조치 항목을 검토할 수 있습니다. 조치 항목은 OpsCenter의 분석 및 인시던트와 연결된 일종의 OpsItem입니다.

체크리스트

분석을 종료하기 전에 체크리스트를 사용하여 대응 담당자가 취해야 할 조치를 검토하십시오. 대응 담당자가 체크리스트의 작업을 완료하면 작업 옆의 아이콘이 타원에서 확인 표시로 변경되어 작업이 완료되었음을 나타냅니다. 체크리스트 항목을 완료하지 않은 경우 Incident Manager는 대응 담당자가 분석을 완료하지 않고 분석을 종료하기를 원하는지 확인하는 메시지를 표시합니다.

분석 템플릿

분석 템플릿은 인시던트의 근본 원인을 자세히 설명하는 일련의 질문을 제공합니다. 이러한 질문에 대한 답을 바탕으로 애플리케이션 성능과 인시던트 대응을 개선할 수 있습니다.

AWS 표준 템플릿

Incident Manager는 AWS 인시던트 대응 및 문제 분석 모범 사례를 기반으로 라는 제목의 표준 질문 템플릿을 제공합니다`AWSIncidents-PostIncidentAnalysisTemplate`.

분석 템플릿 생성

기본 `AWSIncidents-PostIncidentAnalysisTemplate` 템플릿을 사용하고 사용 사례에 적합한 질문이나 섹션을 추가하는 것이 좋습니다. 기본 템플릿을 기반으로 분석 템플릿 생성 이 템플릿을 시작점으로 사용하여 관리 계정에서 분석 템플릿을 생성할 수 있습니다. 그런 다음 Incident Manager를 활성화한 각 리전에 분석 템플릿을 복제할 수 있습니다.

분석 템플릿 생성

1. GetDocument 조치를 직접적으로 호출하고 해당 Name 파라미터를 사용하여 AWSIncidents-PostIncidentAnalysisTemplate을 다운로드합니다. GetDocument 구문에 대한 자세한 내용은 Systems Manager API 참조를 참조하세요.
2. 응답 내용에는 분석을 위한 JSON 구성 블록이 포함되어 있습니다. 질문 구성 블록을 사용하여 분석에 추가 질문을 삽입할 수 있습니다. Incident questions 섹션에 질문이나 섹션을 추가하는 것이 좋습니다.
3. 새 템플릿을 만들려면 이전 단계에서 업데이트된 JSON을 사용한 CreateDocument 작업을 사용하십시오. 다음을 포함해야 합니다. 여기서 *Analysis_Template_Name*은 템플릿 이름입니다.
   - DocumentFormat: "JSON"
   - DocumentType: "ProblemAnalysisTemplate"
   - Name: "*Analysis_Template_Name*"

분석 만들기

1. 분석을 만들려면 종료된 인시던트의 인시던트 세부 정보 페이지에서 분석 만들기를 선택합니다.
2. 이 분석을 만들 때 사용할 분석 템플릿을 선택하고 분석을 설명하는 이름을 입력합니다.
3. 생성(Create)을 선택합니다.

형식이 지정된 인시던트 분석을 인쇄하십시오.

인쇄용으로 형식이 지정된 완전하거나 불완전한 분석의 사본을 생성할 수 있습니다. 이 사본을 PDF로 저장할 수도 있습니다. 한 번에 하나의 분석을 인쇄할 수 있습니다. 다중 분석의 배치 인쇄는 현재 지원되지 않습니다.

형식이 지정된 분석을 인쇄하려면

1. Incident Manager 콘솔을 엽니다.
2. 분석 탭을 선택합니다.
3. 인쇄하려는 분석 제목을 선택합니다.
4. 분석 세부 정보 페이지의 오른쪽 상단에서 인쇄를 선택합니다.

5. 인시던트 분석 인쇄 대화 상자에서 인쇄된 버전에 포함하지 않으려는 분석 섹션을 지웁니다. 기본적으로 모든 섹션이 선택됩니다.
6. 인쇄를 선택하여 디바이스의 로컬 인쇄 제어를 엽니다.
7. 인쇄 대상 또는 형식을 선택합니다. 로컬 또는 네트워크 프린터를 선택하거나 분석을 PDF로 저장할 수 있습니다. 필요한 경우 나머지 인쇄 옵션을 변경한 다음 인쇄를 선택합니다.

> **Note**
>
> 로컬 인쇄 제어는 웹 브라우저 및 디바이스에서 제공하는 사용자 인터페이스를 말합니다. 인쇄 대상은 디바이스에 맞게 구성되어 있고 디바이스에서 액세스할 수 있는 대상입니다.

Incident Manager 자습서

이러한 AWS Systems Manager Incident Manager 자습서는 보다 강력한 인시던트 관리 시스템을 구축하는 데 도움이 됩니다. 이 자습서는 인시던트 중에 발생하는 일반적인 활동을 다루거나 인시던트 대응을 지원합니다.

주제

- 자습서: Incident Manager에서 Systems Manager Automation 런북 사용
- 자습서: Incident Manager에서 보안 인시던트 관리

자습서: Incident Manager에서 Systems Manager Automation 런북 사용

AWS Systems Manager Automation 런북을 사용하여 AWS 서비스에 대한 일반적인 유지 관리, 배포 및 문제 해결 작업을 간소화할 수 있습니다. 이 자습서에서는 Incident Manager에서 인시던트 대응을 자동화하는 사용자 지정 런북을 만들어 보겠습니다. 이 자습서의 시나리오에는 Amazon EC2 지표에 할당된 Amazon CloudWatch 경보가 포함됩니다. 인스턴스가 경보를 트리거하는 상태에 들어가면 Incident Manager가 자동으로 다음 작업을 수행합니다.

1. Incident Manager에서 인시던트를 생성합니다.
2. 문제 해결을 시도하는 런북을 시작합니다.
3. 런북 결과를 Incident Manager의 인시던트 세부 정보 페이지에 게시합니다.

이 자습서에 설명된 프로세스는 Amazon EventBridge 이벤트 및 기타 유형의 AWS 리소스에도 사용할 수 있습니다. 경보 및 이벤트에 대한 해결 대응을 자동화하면 인시던트가 조직 및 리소스에 미치는 영향을 줄일 수 있습니다.

이 자습서에서는 Incident Manager 대응 계획을 위해 Amazon EC2 인스턴스에 할당된 CloudWatch 경보를 편집하는 방법을 설명합니다. 경보, 인스턴스 또는 대응 계획이 구성되어 있지 않은 경우 시작하기 전에 해당 리소스를 구성하는 것이 좋습니다. 자세한 정보는 다음의 주제를 참조하세요.

- Amazon CloudWatch 사용 설명서의 Amazon CloudWatch 경보 사용
- Amazon EC2 사용 설명서의 Amazon EC2 인스턴스 Amazon EC2
- Amazon EC2 사용 설명서의 Amazon EC2 인스턴스 Amazon EC2
- Incident Manager에서 대응 계획 생성 및 구성

> **Important**
>
> AWS 리소스를 생성하고 런북 자동화 단계를 사용하면 비용이 발생합니다. 자세한 내용은 AWS 요금을 참조하세요.

주제

작업 1: 런북 생성

Systems Manager 콘솔에서 런북을 생성하려면 다음 절차를 따릅니다. Incident Manager 인시던트에서 호출되면 런북은 Amazon EC2 인스턴스를 재시작하고 런북 실행에 대한 정보로 인시던트를 업데이트합니다. 시작하기 전에 런북을 생성할 권한이 있는지 확인합니다. 자세한 내용은 AWS Systems Manager 사용 설명서에서 자동화 설정을 참조하세요.

> **Important**
>
> 이 자습서의 런북을 생성하는 방법에 대한 다음과 같은 중요 세부 정보를 검토합니다.
>
> - 런북은 CloudWatch 경보 소스에서 생성된 인시던트를 대상으로 합니다. 이 런북을 다른 유형의 인시던트(예: 수동으로 생성한 인시던트)에 사용할 경우 첫 번째 런북 단계의 타임라인 이벤트를 찾을 수 없으며 시스템에서 오류를 반환합니다.
> - 런북에는 CloudWatch 경보에 `InstanceId`라는 차원이 포함되어 있어야 합니다. Amazon EC2 인스턴스 지표에 대한 경보는 이 차원을 가집니다. 이 런북을 다른 지표(또는 EventBridge와 같은 다른 인시던트 소스)와 함께 사용하는 경우 시나리오에서 캡처된 데이터와 일치하도록 `JsonDecode2` 단계를 변경해야 합니다.
> - 런북은 Amazon EC2 인스턴스를 재시작하여 경보를 유발한 문제를 해결하려고 시도합니다. 실제 인시던트의 경우 인스턴스를 다시 시작하고 싶지 않을 수도 있습니다. 시스템에서 수행하고자 하는 특정 수정 조치로 런북을 업데이트하십시오.

런북 생성에 대한 자세한 내용은AWS Systems Manager 사용 설명서의 런북 작업을 참조하세요.

런북을 생성하려면

1. https://console.aws.amazon.com/systems-manager/ AWS Systems Manager 콘솔을 엽니다.
2. 탐색 창에서 Documents를 선택합니다.
3. 자동화를 선택합니다.
4. 이름에 런북을 설명하는 이름을 입력합니다(예: **IncidentResponseRunbook**).
5. 편집기 탭을 선택하고 편집을 선택합니다.
6. 다음 콘텐츠를 편집기에 붙여 넣습니다.

```
description: This runbook attempts to restart an Amazon EC2 instance that caused an
 incident.
schemaVersion: '0.3'
parameters:
  IncidentRecordArn:
    type: String
    description: The incident
mainSteps:
  - name: ListTimelineEvents
    action: 'aws:executeAwsApi'
    outputs:
      - Selector: '$.eventSummaries[0].eventId'
        Name: eventId
        Type: String
    inputs:
      Service: ssm-incidents
      Api: ListTimelineEvents
      incidentRecordArn: '{{IncidentRecordArn}}'
      filters:
        - key: eventType
          condition:
            equals:
              stringValues:
                - SSM Incident Trigger
    description: This step retrieves the ID of the first timeline event with the
 CloudWatch alarm details.
  - name: GetTimelineEvent
    action: 'aws:executeAwsApi'
    inputs:
      Service: ssm-incidents
```

```
      Api: GetTimelineEvent
      incidentRecordArn: '{{IncidentRecordArn}}'
      eventId: '{{ListTimelineEvents.eventId}}'
    outputs:
      - Name: eventData
        Selector: $.event.eventData
        Type: String
    description: This step retrieves the timeline event itself.
  - name: JsonDecode
    action: 'aws:executeScript'
    inputs:
      Runtime: python3.8
      Handler: script_handler
      Script: |-
        import json

        def script_handler(events, context):
          data = json.loads(events["eventData"])
          return data
      InputPayload:
        eventData: '{{GetTimelineEvent.eventData}}'
    outputs:
      - Name: rawData
        Selector: $.Payload.rawData
        Type: String
    description: This step parses the timeline event data.
  - name: JsonDecode2
    action: 'aws:executeScript'
    inputs:
      Runtime: python3.8
      Handler: script_handler
      Script: |-
        import json

        def script_handler(events, context):
          data = json.loads(events["rawData"])
          return data
      InputPayload:
        rawData: '{{JsonDecode.rawData}}'
    outputs:
      - Name: InstanceId
        Selector:
'$.Payload.detail.configuration.metrics[0].metricStat.metric.dimensions.InstanceId'
        Type: String
```

```
    description: This step parses the CloudWatch event data.
  - name: RestartInstance
    action: 'aws:executeAutomation'
    inputs:
      DocumentName: AWS-RestartEC2Instance
      DocumentVersion: $DEFAULT
      RuntimeParameters:
        InstanceId: '{{JsonDecode2.InstanceId}}'
    description: This step restarts the Amazon EC2 instance
```

7. Create automation(자동화 생성)을 선택합니다.

작업 2: IAM 역할 생성

다음 자습서를 사용하여 Incident Manager에 대응 계획에 지정된 실행서를 시작할 수 있는 권한을 부여하는 AWS Identity and Access Management (IAM) 역할을 생성합니다. 이 자습서의 런북은 Amazon EC2 인스턴스를 재시작합니다. 런북을 대응 계획에 연결할 때 다음 작업에서 이 IAM 역할을 지정하게 됩니다.

대응 계획에서 런북을 시작하는 IAM 역할을 생성하십시오.

1. https://console.aws.amazon.com/iam/에서 IAM 콘솔을 엽니다.
2. 탐색 창에서 역할(Roles)을 선택한 후 역할 생성(Create role)을 선택합니다.
3. 신뢰할 수 있는 엔터티 유형에서 AWS 서비스를 선택해야 합니다.
4. 사용 사례의 기타 AWS 서비스 사용 사례 필드에 **`Incident Manager`**를 입력합니다.
5. Incident Manager를 선택하고 다음을 선택합니다.
6. 권한 정책 연결 페이지에서 정책 생성을 선택합니다. 권한 편집기가 새 브라우저 창이나 탭에서 열립니다.
7. 정책 편집기에서 JSON 탭을 선택합니다.
8. 다음 권한 정책을 복사해 JSON 편집기에 붙여 넣습니다. *`account_ID`*를 AWS 계정 ID로 바꿉니다.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Resource": [
```

```
                "arn:aws:ssm:*:account_ID:automation-definition/
IncidentResponseRunbook:*",
                "arn:aws:ssm:*::automation-definition/AWS-RestartEC2Instance:*"
            ],
            "Action": "ssm:StartAutomationExecution"
        },
        {
            "Effect": "Allow",
            "Resource": "arn:aws:ssm:*:*:automation-execution/*",
            "Action": "ssm:GetAutomationExecution"
        },
        {
            "Effect": "Allow",
            "Resource": "arn:aws:ssm-incidents:*:*:*",
            "Action": "ssm-incidents:*"
        },
        {
            "Effect": "Allow",
            "Resource": "arn:aws:iam::*:role/AWS-SystemsManager-
AutomationExecutionRole",
            "Action": "sts:AssumeRole"
        },
        {
            "Effect": "Allow",
            "Resource": "*",
            "Action": [
                "ec2:StopInstances",
                "ec2:DescribeInstanceStatus",
                "ec2:StartInstances"
            ]
        }
    ]
}
```

9. 다음: 태그를 선택합니다.
10. (선택 사항) 필요한 경우 정책에 태그를 추가합니다.
11. 다음: 검토를 선택합니다.
12. 이름 필드에 이 자습서에서 사용되는 역할을 식별하는 데 도움이 되는 이름을 입력합니다.
13. (선택 사항) 설명 필드에 설명을 입력합니다.
14. 정책 생성을 선택합니다.
15. 생성하려는 역할의 브라우저 창이나 탭으로 다시 이동합니다. 권한 추가 페이지가 표시됩니다.

16. 새로 고침 버튼(정책 생성 버튼 옆에 있음)을 선택한 다음 생성한 권한 정책의 이름을 필터 상자에 입력합니다.
17. 생성한 권한 정책을 선택한 후 다음을 선택합니다.
18. 이름, 검토 및 생성 페이지에서 역할 이름에 이 자습서에서 사용할 역할을 식별하는 데 도움이 되는 이름을 입력합니다.
19. (선택 사항) 설명 필드에 설명을 입력합니다.
20. 역할 세부 정보를 검토하고, 필요하면 태그를 추가하고 역할 생성을 선택합니다.

작업 3: 런북을 대응 계획에 연결

런북을 Incident Manager 대응 계획에 연결하면 일관되고 반복 가능하며 시기적절한 완화 프로세스를 보장할 수 있습니다. 또한 런북은 해결 담당자가 다음 조치 방침을 결정하는 출발점 역할을 합니다.

런북을 대응 계획에 할당하려면 다음과 같이 하세요.

1. Incident Manager 콘솔을 엽니다.
2. 대응 계획을 선택합니다.
3. 대응 계획의 경우 기존 대응 계획을 선택하고 편집을 선택합니다. 기존 대응 계획이 없는 경우, 대응 계획 생성을 선택하여 새 계획을 생성하십시오.

   다음 작업을 완료합니다.

   a. 런북 섹션에서 기존 런북 선택을 선택합니다.
   b. 소유자에서 내 소유가 선택되어 있는지 확인합니다.
   c. 런북의 경우 작업 1: 런북 생성에서 생성한 런북을 선택합니다.
   d. 버전의 경우 실행 시 기본값을 선택합니다.
   e. 입력 섹션에서 IncidentRecordArn 파라미터에 대해 인시던트 ARN을 선택합니다.
   f. 실행 권한 섹션에서 작업 2: IAM 역할 생성에서 생성한 IAM 역할을 선택합니다.
4. 변경 내용을 저장합니다.

작업 4: 대응 계획에 CloudWatch 경보 할당

다음 절차를 사용하여 Amazon EC2 인스턴스에 대한 CloudWatch 경보를 대응 계획에 할당하십시오.

대응 계획에 CloudWatch 경보를 할당하려면

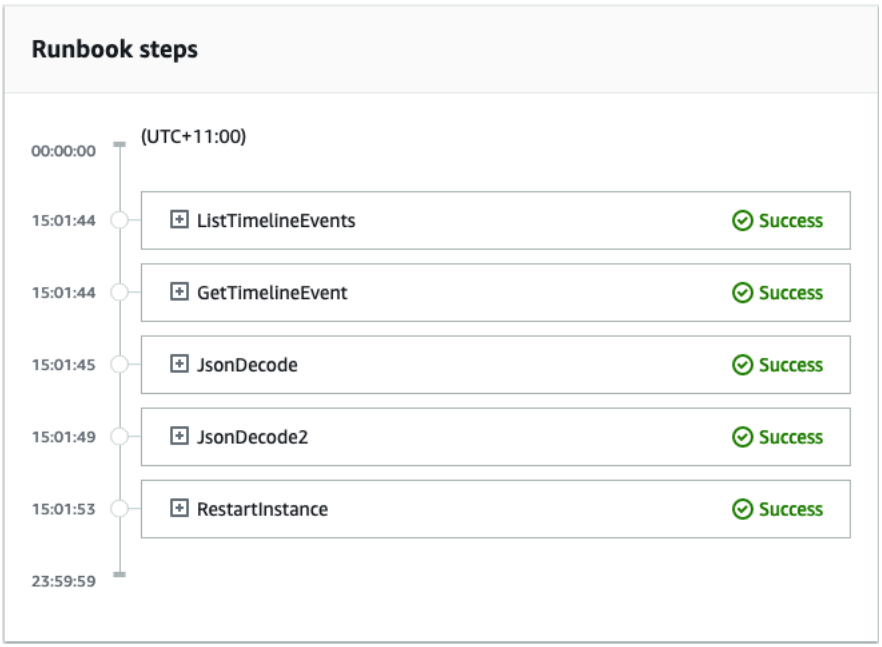
1. https://console.aws.amazon.com/cloudwatch/에서 CloudWatch 콘솔을 엽니다.
2. 탐색 창에서 경보 아래의 모든 경보를 선택합니다.
3. 대응 계획에 연결하려는 Amazon EC2 인스턴스에 대한 경보를 선택합니다.
4. 작업을 선택한 후 편집을 선택합니다. 지표에 `InstanceId`라는 차원이 있는지 확인하십시오.
5. Next(다음)를 선택합니다.
6. 작업 구성 마법사에서 Systems Manager 작업 추가를 선택합니다.
7. 인시던트 생성을 선택합니다.
8. 작업 3: 런북을 대응 계획에 연결에서 만든 대응 계획을 선택합니다.
9. 경보 업데이트(Update alarm)을 선택합니다.

작업 5: 결과 확인

CloudWatch 경보가 인시던트를 생성한 다음 대응 계획에 지정된 런북을 처리하는지 확인하려면 경보를 트리거해야 합니다. 경보를 트리거하고 런북의 처리가 완료되면 다음 절차를 사용하여 런북의 결과를 확인할 수 있습니다. 경보 트리거에 대한 자세한 내용은 AWS CLI 명령 참조의 set-alarm-state를 참조하세요.

1. Incident Manager 콘솔을 엽니다.
2. CloudWatch 경보로 생성된 인시던트를 선택합니다.
3. 런북 탭을 선택합니다.
4. 런북 단계 섹션에서 Amazon EC2 인스턴스에서 수행된 작업을 확인하십시오.

   다음 이미지는이 자습서에서 생성한 실행서에서 수행한 단계가 콘솔에 보고되는 방법을 보여줍니다. 각 단계는 타임스탬프 및 상태 메시지와 함께 나열됩니다.



CloudWatch 경보의 모든 세부 정보를 보려면 JSONDecode2 단계를 확장한 다음 출력을 확장하십시오.

Important

이 자습서에서 구현한 리소스 변경 사항 중 유지하지 않을 리소스는 모두 정리해야 합니다. 여기에는 리소스 계획 및 인시던트, CloudWatch 경보에 대한 변경 사항, 이 자습서에서 생성한 IAM 역할 등 Incident Manager 리소스에 대한 변경 사항이 포함됩니다.

자습서: Incident Manager에서 보안 인시던트 관리

AWS Security Hub Amazon EventBridge와 Incident Manager를 함께 사용하여 AWS 호스팅 애플리케이션에서 보안 인시던트를 식별하고 관리할 수 있습니다. 이 자습서에서는 Security Hub가 자동으로 전송한 조사 결과를 기반으로 인시던트를 생성하는 EventBridge 규칙을 구성하는 방법을 안내합니다.

Note

이 자습서에서는 EventBridge Security Hub를 사용합니다. 이러한 서비스를 사용하면 비용이 발생할 수 있습니다.

사전 조건

- Security Hub를 설정합니다. 자세한 내용은 설정 AWS Security Hub을 참조하세요.
- Security Hub에서 조사 결과를 생성하거나 업데이트합니다. 자세한 내용은 AWS Security Hub의 조사 결과를 참조하세요.
- Incident Manager가 보안 인시던트를 생성할 때 템플릿으로 사용할 대응 계획을 구성하십시오. 자세한 내용은 Incident Manager에서 인시던트 준비 단원을 참조하십시오.

이 자습서에서는 사전 정의된 패턴을 사용하여 EventBridge 규칙을 생성합니다. 사용자 지정 패턴을 사용하여 규칙을 생성하려면 AWS Security Hub 사용 설명서의 사용자 지정 패턴을 사용하여 규칙 생성을 참조하세요.

EventBridge 규칙 생성

1. https://console.aws.amazon.com/events/에서 Amazon EventBridge 콘솔을 엽니다.
2. 탐색 창에서 규칙을 선택합니다.
3. 규칙 생성을 선택합니다.
4. 규칙에 대해 이름과 설명을 입력합니다.

   규칙은 동일한 지역과 동일한 이벤트 버스의 다른 규칙과 동일한 이름을 가질 수 없습니다.
5. 이벤트 버스에서 기본값을 선택합니다.
6. 규칙 유형에서 이벤트 패턴이 있는 규칙을 선택합니다.
7. Next(다음)를 선택합니다.
8. 이벤트 소스(Event source)에서 AWS 이벤트 또는 EventBridge 파트너 이벤트(Events or EventBridge partner events)를 선택합니다.
9. 이벤트 패턴에서 이벤트 패턴 양식을 선택합니다.
10. 이벤트 소스에서 AWS 서비스를 선택합니다.
11. AWS 서비스에 대해 Security Hub를 선택합니다.
12. 이벤트 유형에서 Security Hub 조사 결과 - 가져오기를 선택합니다.
13. 기본적으로 EventBridge는 필터 값 없이 이벤트 패턴을 구성합니다. 각 속성에 대해 모든 **## ##** 옵션이 선택됩니다. 이러한 필터를 업데이트하여 환경에 가장 큰 영향을 미치는 보안 결과를 기반으로 인시던트를 생성하십시오.
14. 다음을 클릭합니다.
15. 대상 유형에서 AWS 서비스를 선택합니다.

16. 대상 선택에서 Incident Manager 대응 계획을 선택합니다.
17. 대응 계획의 경우 생성된 인시던트의 템플릿으로 사용할 대응 계획을 선택합니다.
18. EventBridge는 규칙 실행에 필요한 IAM 역할을 생성할 수 있습니다.
    - IAM 역할을 자동으로 생성하려면 이 특정 리소스에 대해 새 역할 생성을 선택합니다.
    - 계정에 이미 있는 IAM 역할을 사용하려면 기존 역할 사용을 선택합니다.
19. (선택 사항)규칙에 대해 하나 이상의 태그를 입력하세요.
20. Next(다음)를 선택합니다.
21. 규칙의 세부 정보를 검토하고 규칙 생성을 선택합니다.

이제 이 EventBridge 규칙을 만들었으므로 정의한 속성 값과 일치하는 보안 결과가 Incident Manager에 인시던트를 생성합니다. 이러한 인시던트를 분류, 관리, 모니터링하고, 인시던트 사후 분석을 생성할 수 있습니다.

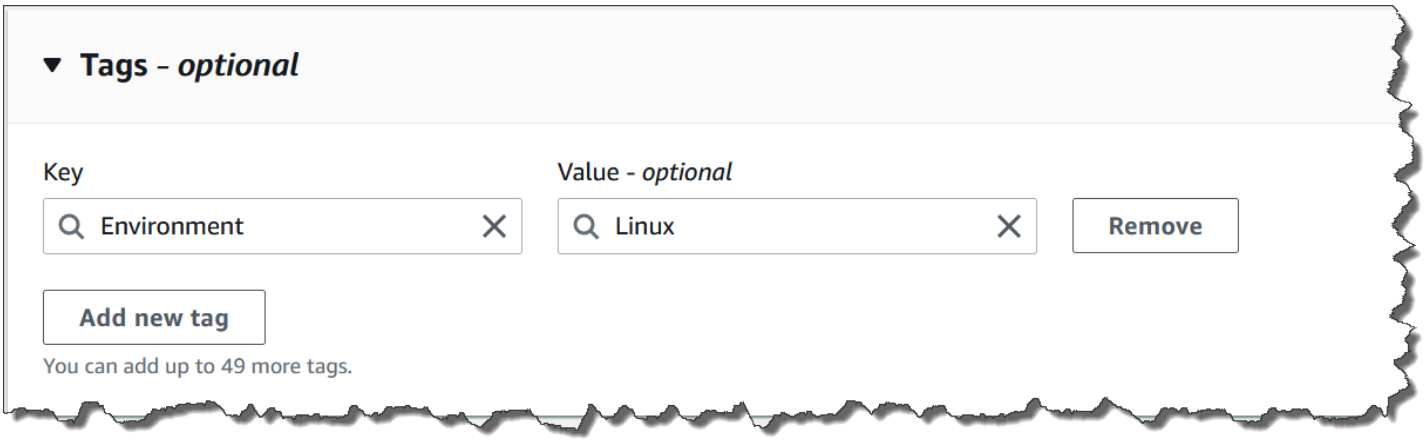
Incident Manager의 리소스 태깅

태그는 복제 세트에 AWS 리전 지정된의 Incident Manager 리소스에 할당할 수 있는 선택적 메타데이터입니다. 대응 계획, 인시던트 기록 및 연락처에 태그를 할당할 수 있습니다. 대기 일정 및 교대에도 태그를 추가할 수 있습니다. 복제 세트 자체에 태그를 추가할 수도 있습니다. 태그를 사용하면 다양한 방식으로 이 리소스를 분류하고 해당 액세스를 제어할 수 있습니다. 각 태그는 사용자가 정의하는 키와 선택적 값으로 구성됩니다. 각 Incident Manager 리소스 유형에 대한 요건을 충족하는 태그 키 세트를 고안하는 것이 좋습니다. 일관된 태그 키 세트를 사용하면 이 리소스 및 해당 액세스를 보다 쉽게 관리할 수 있습니다. 태그에 따라 리소스를 검색하고 필터링할 수 있습니다. 태그를 사용하여 리소스에 대한 액세스를 제어하는 방법에 대한 자세한 내용은 IAM 사용 설명서의 태그를 사용하여 AWS 리소스에 대한 액세스 제어를 참조하세요.

대응 계획을 만들 때 인시던트 기본 섹션에서 태그를 지정할 수 있습니다. 이러한 태그는 대응 계획을 사용하여 인시던트를 만들 때 인시던트 기록에 적용됩니다.

> **Note**
>
> 태그에는 의미론적 의미가 없습니다. 태그는 엄격히 문자열로 해석됩니다.

Incident Manager 콘솔을 사용하여 태그를 추가하거나 제거할 수 있습니다. 다음 스크린샷은 태그 키 및 값을 추가하기 위한 필드와 태그를 추가 및 제거하기 위한 버튼이 있는 콘솔 페이지의 태그 영역을 표시합니다.



태그를 프로그래밍 방식으로 사용하려면 다음 API 작업을 사용합니다.

- TagResource
- UntagResource

- ListTagsForResource

> **Important**
>
> 대응 계획, 인시던트 기록, 연락처, 대기 일정 및 교대, 복제 세트에 적용된 태그는 리소스 소유자 계정에서만 보고 수정할 수 있습니다.

의 보안 AWS Systems Manager Incident Manager

의 클라우드 보안 AWS 이 최우선 순위입니다. AWS 고객은 보안에 가장 민감한 조직의 요구 사항을 충족하도록 구축된 데이터 센터 및 네트워크 아키텍처의 이점을 누릴 수 있습니다.

보안은 AWS 와 사용자 간의 공동 책임입니다. 공동 책임 모델은 이 사항을 클라우드의 보안 및 클라우드 내 보안으로 설명합니다.

- 클라우드 보안 - AWS 는 AWS 서비스 에서 실행되는 인프라를 보호할 책임이 있습니다 AWS 클라우드. AWS 또한는 안전하게 사용할 수 있는 서비스를 제공합니다. 타사 감사자는 AWS 규정 준수 프로그램 일환으로 보안의 효과를 정기적으로 테스트하고 확인합니다. 에 적용되는 규정 준수 프로그램에 대한 자세한 내용은 규정 준수 프로그램 AWS 제공 범위 내 서비스규정 준수 프로그램 제공 범위 내 서비스를 AWS Systems Manager Incident Manager참조하세요.
- 클라우드의 보안 - 사용자의 책임은 사용하는 AWS 서비스에 따라 결정됩니다. 또한 귀하는 귀사의 데이터 민감도, 귀사의 요구 사항, 관련 법률 및 규정을 비롯한 기타 요소에 대해서도 책임이 있습니다.

이 설명서는 Incident Manager 사용 시 책임 분담 모델을 적용하는 방법을 이해하는 데 도움이 됩니다. 다음 주제에서는 보안 및 규정 준수 목표를 충족하도록 Incident Manager를 구성하는 방법을 보여줍니다. 또한 Incident Manager 리소스를 모니터링하고 보호하는 데 도움이 AWS 서비스 되는 다른를 사용하는 방법을 알아봅니다.

주제

- Incident Manager의 데이터 보호
- 에 대한 자격 증명 및 액세스 관리 AWS Systems Manager Incident Manager
- Incident Manager에서 공유 연락처 및 대응 계획 사용
- 에 대한 규정 준수 검증 AWS Systems Manager Incident Manager
- 의 복원력 AWS Systems Manager Incident Manager
- 의 인프라 보안 AWS Systems Manager Incident Manager
- AWS Systems Manager Incident Manager 및 인터페이스 VPC 엔드포인트 작업(AWS PrivateLink)
- Incident Manager의 구성 및 취약성 분석
- 의 보안 모범 사례 AWS Systems Manager Incident Manager

Incident Manager의 데이터 보호

AWS 공동 책임 모델의 데이터 보호에 적용됩니다 AWS Systems Manager Incident Manager. 이 모델에 설명된 대로 AWS 는 모든를 실행하는 글로벌 인프라를 보호할 책임이 있습니다 AWS 클라우드. 사용자는 인프라에서 호스팅되는 콘텐츠를 관리해야 합니다. 사용하는 AWS 서비스 의 보안 구성과 관리 태스크에 대한 책임도 사용자에게 있습니다. 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 참조하세요.

데이터 보호를 위해 자격 증명을 보호하고 AWS 계정 AWS IAM Identity Center 또는 AWS Identity and Access Management (IAM)를 사용하여 개별 사용자를 설정하는 것이 좋습니다. 이렇게 하면 개별 사용자에게 자신의 직무를 충실히 이행하는 데 필요한 권한만 부여됩니다. 또한 다음과 같은 방법으로 데이터를 보호하는 것이 좋습니다.

- 각 계정에 다중 인증(MFA)을 사용하세요.
- SSL/TLS를 사용하여 AWS 리소스와 통신합니다. TLS 1.2는 필수이며 TLS 1.3을 권장합니다.
- 를 사용하여 API 및 사용자 활동 로깅을 설정합니다 AWS CloudTrail. CloudTrail 추적을 사용하여 AWS 활동을 캡처하는 방법에 대한 자세한 내용은 AWS CloudTrail 사용 설명서의 CloudTrail 추적 작업을 참조하세요.
- 내부의 모든 기본 보안 제어와 함께 AWS 암호화 솔루션을 사용합니다 AWS 서비스.
- Amazon S3에 저장된 민감한 데이터를 검색하고 보호하는 데 도움이 되는 Amazon Macie와 같은 고급 관리형 보안 서비스를 사용하세요.
- 명령줄 인터페이스 또는 API를 AWS 통해에 액세스할 때 FIPS 140-3 검증 암호화 모듈이 필요한 경우 FIPS 엔드포인트를 사용합니다. 사용 가능한 FIPS 엔드포인트에 대한 자세한 내용은 Federal Information Processing Standard(FIPS) 140-3을 참조하세요.

고객의 이메일 주소와 같은 기밀 정보나 중요한 정보는 태그나 이름 필드와 같은 자유 형식 텍스트 필드에 입력하지 않는 것이 좋습니다. 여기에는 Incident Manager 또는 기타 AWS 서비스 에서 콘솔 AWS CLI, API 또는 AWS SDKs를 사용하여 작업하는 경우가 포함됩니다. 이름에 사용되는 태그 또는 자유 형식 텍스트 필드에 입력하는 모든 데이터는 청구 또는 진단 로그에 사용될 수 있습니다. 외부 서버에 URL을 제공할 때 해당 서버에 대한 요청을 검증하기 위해 자격 증명을 URL에 포함해서는 안 됩니다.

기본적으로 Incident Manager는 SSL/TLS를 사용하여 전송 중인 데이터를 암호화합니다.

데이터 암호화

Incident Manager는 AWS Key Management Service (AWS KMS) 키를 사용하여 Incident Manager 리소스를 암호화합니다. 에 대한 자세한 내용은 AWS KMS 개발자 안내서를 AWS KMS참조하세요. AWS KMS 는 안전하고 가용성이 높은 하드웨어와 소프트웨어를 결합하여 클라우드에 맞게 확장된 키 관리 시스템을 제공합니다. Incident Manager는 지정된 키를 사용하여 데이터를 암호화하고 AWS 소유 키를 사용하여 메타데이터를 암호화합니다. Incident Manager를 사용하려면 암호화 설정을 포함한 복제 세트를 설정해야 합니다. Incident Manager를 사용하려면 데이터 암호화가 필요합니다.

AWS 소유 키를 사용하여 복제 세트를 암호화하거나에서 생성한 자체 고객 관리형 키를 사용하여 복제 세트의 리전을 암호화 AWS KMS 할 수 있습니다. Incident Manager는 내부에 생성된 데이터를 암호화하기 위한 대칭 암호화 AWS KMS 키만 지원합니다 AWS KMS. Incident Manager는 가져온 AWS KMS 키 구성 요소, 사용자 지정 키 스토어, 해시 기반 메시지 인증 코드(HMAC) 또는 기타 유형의 키가 있는 키를 지원하지 않습니다. 고객 관리 키를 사용하는 경우 AWS KMS 콘솔 또는 AWS KMS API를 사용하여 고객 관리 키를 중앙에서 생성하고 Incident Manager가 고객 관리 키를 사용하는 방법을 제어하는 키 정책을 정의합니다. Incident Manager를 사용한 암호화에 고객 관리형 키를 사용하는 경우 AWS KMS 고객 관리형 키는 리소스와 동일한 리전에 있어야 합니다. Incident Manager에서 데이터 암호화를 설정하는 방법에 대한 자세한 내용은 준비하기 마법사를 참조하세요.

AWS KMS 고객 관리형 키 사용에는 추가 요금이 부과됩니다. 자세한 내용은 AWS Key Management Service 개발자 설명서의 AWS KMS 개념 - KMS 키 및 AWS KMS 요금을 참조하세요.

> **Important**
>
> AWS KMS key (KMS 키)를 사용하여 복제 세트와 Incident Manager 데이터를 암호화했지만 나중에 복제 세트를 삭제하기로 결정한 경우 KMS 키를 비활성화하거나 삭제하기 전에 복제 세트를 삭제해야 합니다.

Incident Manager가 고객 관리 키를 사용하여 데이터를 암호화하도록 허용하려면 고객 관리 키의 키 정책에 다음 정책 문을 추가해야 합니다. 계정에서 키 정책을 설정하고 변경하는 방법에 대해 자세히 알아보려면 AWS Key Management Service 개발자 안내서의 AWS KMS에서 키 정책 사용을 참조하세요. 정책에서 다음 권한을 제공합니다.

- Incident Manager가 읽기 전용 작업을 수행하여 계정에서 Incident Manager AWS KMS key 용를 찾을 수 있도록 허용합니다.
- Incident Manager가 KMS 키를 사용하여 권한 부여를 생성하고 키를 설명할 수 있도록 허용합니다. 단, Incident Manager를 사용할 권한이 있는 계정의 보안 주체를 대신하여 행동하는 경우에만 가

능합니다. 정책 문에 지정된 보안 주체가 KMS 키 및 Incident Manager를 사용할 권한이 없는 경우 Incident Manager 서비스에서 오는 경우에도 호출이 실패합니다.

```
    {
    "Sid": "Allow CreateGrant through AWS Systems Manager Incident Manager",
    "Effect": "Allow",
    "Principal": {
      "AWS": "arn:aws:iam::111122223333:user/ssm-lead"
    },
    "Action": [
      "kms:CreateGrant",
      "kms:DescribeKey"
    ],
    "Resource": "*",
    "Condition": {
      "StringLike": {
        "kms:ViaService": [
          "ssm-incidents.amazonaws.com",
          "ssm-contacts.amazonaws.com"
        ]
      }
    }
   }
```

`Principal` 값을 복제 세트를 생성한 IAM 보안 주체로 바꾸십시오.

Incident Manager는 암호화 작업을 위해에 AWS KMS 대한 모든 요청에서 암호화 컨텍스트를 사용합니다. 이 암호화 컨텍스트를 사용하여 Incident Manager가 KMS 키를 사용하는 CloudTrail 로그 이벤트를 식별할 수 있습니다. Incident Manager는 다음과 같은 암호화 컨텍스트를 사용합니다.

- `contactArn=`*`ARN of the contact or escalation plan`*

에 대한 자격 증명 및 액세스 관리 AWS Systems Manager Incident Manager

AWS Identity and Access Management (IAM)는 관리자가 AWS 리소스에 대한 액세스를 안전하게 제어할 수 AWS 서비스 있도록 도와주는 입니다. IAM 관리자는 누가 Incident Manager 리소스를 사용하

도록 인증되고(로그인됨) 권한이 부여되는지(권한 있음)를 제어합니다. IAM은 추가 비용 없이 사용할 수 AWS 서비스 있는 입니다.

주제

대상

AWS Identity and Access Management (IAM)를 사용하는 방법은 Incident Manager에서 수행하는 작업에 따라 다릅니다.

서비스 사용자 - Incident Manager 서비스를 사용하여 작업을 수행하는 경우 필요한 자격 증명과 권한을 관리자가 제공합니다. 더 많은 Incident Manager 기능을 사용하여 작업을 수행하게 되면 추가 권한이 필요할 수 있습니다. 액세스 권한 관리 방법을 이해하면 관리자에게 올바른 권한을 요청하는 데 도움이 됩니다. Incident Manager의 기능에 액세스할 수 없는 경우 AWS Systems Manager Incident Manager 자격 증명 및 액세스 문제 해결 섹션을 참조하세요.

서비스 관리자 - 회사에서 Incident Manager 리소스를 책임지고 있는 경우 Incident Manager에 대한 전체 액세스 권한을 가지고 있을 것입니다. 서비스 관리자는 서비스 사용자가 액세스해야 하는 Incident Manager 기능과 리소스를 결정합니다. 그런 다음 IAM 관리자에게 요청을 제출하여 서비스 사용자의 권한을 변경해야 합니다. 이 페이지의 정보를 검토하여 IAM의 기본 개념을 이해하세요. 회사가 Incident Manager에서 IAM을 사용하는 방법에 대해 자세히 알아보려면 AWS Systems Manager Incident Manager 에서 IAM을 사용하는 방법 섹션을 참조하세요.

IAM 관리자 - IAM 관리자라면 Incident Manager에 대한 액세스 권한 관리 정책 작성 방법을 자세히 알고 싶을 것입니다. IAM에서 사용할 수 있는 Incident Manager 자격 증명 기반 정책 예제를 보려면 AWS Systems Manager Incident Manager에 대한 자격 증명 기반 정책 예시 섹션을 참조하세요.

ID를 통한 인증

인증은 자격 증명 자격 증명을 AWS 사용하여에 로그인하는 방법입니다. IAM 사용자 또는 AWS 계정 루트 사용자 IAM 역할을 수임하여 로 인증(로그인 AWS)되어야 합니다.

자격 증명 소스를 통해 제공된 자격 증명을 사용하여 페더레이션 자격 증명 AWS 으로에 로그인할 수 있습니다. AWS IAM Identity Center (IAM Identity Center) 사용자, 회사의 Single Sign-On 인증 및 Google 또는 Facebook 자격 증명은 페더레이션 자격 증명의 예입니다. 페더레이션형 ID로 로그인할 때 관리자가 이전에 IAM 역할을 사용하여 ID 페더레이션을 설정했습니다. 페더레이션을 사용하여 AWS 에 액세스하면 간접적으로 역할을 수임하게 됩니다.

사용자 유형에 따라 AWS Management Console 또는 AWS 액세스 포털에 로그인할 수 있습니다. 로그인에 대한 자세한 내용은 AWS 로그인 사용 설명서의에 로그인하는 방법을 AWS참조하세요. AWS 계정

AWS 프로그래밍 방식으로에 액세스하는 경우는 자격 증명을 사용하여 요청에 암호화 방식으로 서명할 수 있는 소프트웨어 개발 키트(SDK)와 명령줄 인터페이스(CLI)를 AWS 제공합니다. AWS 도구를 사용하지 않는 경우 요청에 직접 서명해야 합니다. 권장 방법을 사용하여 요청에 직접 서명하는 자세한 방법은 IAM 사용 설명서에서 API 요청용AWS Signature Version 4를 참조하세요.

사용하는 인증 방법에 상관없이 추가 보안 정보를 제공해야 할 수도 있습니다. 예를 들어는 멀티 팩터 인증(MFA)을 사용하여 계정의 보안을 강화할 것을 AWS 권장합니다. 자세한 내용은 AWS IAM Identity Center 사용 설명서에서 다중 인증 및 IAM 사용 설명서에서 IAM의AWS 다중 인증을 참조하세요.

AWS 계정 루트 사용자

를 생성할 때 계정의 모든 AWS 서비스 및 리소스에 대한 완전한 액세스 권한이 있는 하나의 로그인 자격 증명으로 AWS 계정시작합니다. 이 자격 증명을 AWS 계정 루트 사용자라고 하며 계정을 생성하는 데 사용한 이메일 주소와 암호로 로그인하여 액세스합니다. 일상적인 작업에 루트 사용자를 사용하지 않을 것을 강력히 권장합니다. 루트 사용자 자격 증명을 보호하고 루트 사용자만 수행할 수 있는 작업을 수행하는 데 사용합니다. 루트 사용자로 로그인해야 하는 전체 작업 목록은 IAM 사용 설명서의 루트 사용자 보안 인증이 필요한 작업을 참조하세요.

페더레이션 자격 증명

가장 좋은 방법은 관리자 액세스가 필요한 사용자를 포함한 인간 사용자에게 자격 증명 공급자와의 페더레이션을 사용하여 임시 자격 증명을 사용하여 AWS 서비스 에 액세스하도록 요구하는 것입니다.

페더레이션 자격 증명은 엔터프라이즈 사용자 디렉터리, 웹 자격 증명 공급자, AWS Directory Service, Identity Center 디렉터리 또는 자격 증명 소스를 통해 제공된 자격 증명을 사용하여 AWS 서비스 에 액

세스하는 모든 사용자의 사용자입니다. 페더레이션 자격 증명에 액세스할 때 역할을 AWS 계정수임하고 역할은 임시 자격 증명을 제공합니다.

중앙 집중식 액세스 관리를 위해 AWS IAM Identity Center을(를) 사용하는 것이 좋습니다. IAM Identity Center에서 사용자 및 그룹을 생성하거나 모든 및 애플리케이션에서 사용할 수 있도록 자체 ID 소스의 사용자 AWS 계정 및 그룹 집합에 연결하고 동기화할 수 있습니다. IAM Identity Center에 대한 자세한 내용은 AWS IAM Identity Center 사용 설명서에서 IAM Identity Center란 무엇인가요?를 참조하세요.

IAM 사용자 및 그룹

IAM 사용자는 단일 사용자 또는 애플리케이션에 대한 특정 권한이 AWS 계정 있는 내의 자격 증명입니다. 가능하면 암호 및 액세스 키와 같은 장기 자격 증명이 있는 IAM 사용자를 생성하는 대신 임시 자격 증명을 사용하는 것이 좋습니다. 하지만 IAM 사용자의 장기 자격 증명이 필요한 특정 사용 사례가 있는 경우, 액세스 키를 교체하는 것이 좋습니다. 자세한 내용은 IAM 사용 설명서의 장기 보안 인증이 필요한 사용 사례의 경우, 정기적으로 액세스 키 교체를 참조하세요.

IAM 그룹은 IAM 사용자 컬렉션을 지정하는 자격 증명입니다. 사용자는 그룹으로 로그인할 수 없습니다. 그룹을 사용하여 여러 사용자의 권한을 한 번에 지정할 수 있습니다. 그룹을 사용하면 대규모 사용자 집합의 권한을 더 쉽게 관리할 수 있습니다. 예를 들어, IAMAdmins라는 그룹이 있고 이 그룹에 IAM 리소스를 관리할 권한을 부여할 수 있습니다.

사용자는 역할과 다릅니다. 사용자는 한 사람 또는 애플리케이션과 고유하게 연결되지만, 역할은 해당 역할이 필요한 사람이라면 누구나 수임할 수 있습니다. 사용자는 영구적인 장기 자격 증명을 가지고 있지만, 역할은 임시 보안 인증만 제공합니다. 자세한 내용은 IAM 사용 설명서에서 IAM 사용자 사용 사례를 참조하세요.

IAM 역할

IAM 역할은 특정 권한이 AWS 계정 있는 내의 자격 증명입니다. IAM 사용자와 유사하지만, 특정 개인과 연결되지 않습니다. 에서 IAM 역할을 일시적으로 수임하려면 사용자에서 IAM 역할(콘솔)로 전환할 AWS Management Console수 있습니다. https://docs.aws.amazon.com/IAM/latest/UserGuide/id_roles_use_switch-role-console.html 또는 AWS API 작업을 호출하거나 사용자 지정 URL을 AWS CLI 사용하여 역할을 수임할 수 있습니다. 역할 사용 방법에 대한 자세한 내용은 IAM 사용 설명서의 역할 수임 방법을 참조하세요.

임시 보안 인증이 있는 IAM 역할은 다음과 같은 상황에서 유용합니다.

- 페더레이션 사용자 액세스 - 페더레이션 ID에 권한을 부여하려면 역할을 생성하고 해당 역할의 권한을 정의합니다. 페더레이션 ID가 인증되면 역할이 연결되고 역할에 정의된 권한이 부여됩니다. 페

더레이션 관련 역할에 대한 자세한 내용은 IAM 사용 설명서의 Create a role for a third-party identity provider (federation)를 참조하세요. IAM Identity Center를 사용하는 경우, 권한 집합을 구성합니다. 인증 후 ID가 액세스할 수 있는 항목을 제어하기 위해 IAM Identity Center는 권한 집합을 IAM의 역할과 연관짓습니다. 권한 집합에 대한 자세한 내용은 AWS IAM Identity Center 사용 설명서의 권한 집합을 참조하세요.

- 임시 IAM 사용자 권한 - IAM 사용자 또는 역할은 IAM 역할을 수임하여 특정 작업에 대한 다양한 권한을 임시로 받을 수 있습니다.
- 교차 계정 액세스 - IAM 역할을 사용하여 다른 계정의 사용자(신뢰할 수 있는 보안 주체)가 내 계정의 리소스에 액세스하도록 허용할 수 있습니다. 역할은 계정 간 액세스를 부여하는 기본적인 방법입니다. 그러나 일부 에서는 정책을 리소스에 직접 연결할 AWS 서비스수 있습니다(역할을 프록시로 사용하는 대신). 교차 계정 액세스에 대한 역할과 리소스 기반 정책의 차이점을 알아보려면 IAM 사용 설명서의 IAM의 교차 계정 리소스 액세스를 참조하세요.
- 교차 서비스 액세스 - 일부는 다른에서 기능을 AWS 서비스 사용합니다 AWS 서비스. 예를 들어, 서비스에서 호출하면 일반적으로 해당 서비스는 Amazon EC2에서 애플리케이션을 실행하거나 Amazon S3에 객체를 저장합니다. 서비스는 직접적으로 호출하는 위탁자의 권한을 사용하거나, 서비스 역할을 사용하거나, 또는 서비스 연결 역할을 사용하여 이 작업을 수행할 수 있습니다.
  - 전달 액세스 세션(FAS) - IAM 사용자 또는 역할을 사용하여에서 작업을 수행하는 경우 AWS보안 주체로 간주됩니다. 일부 서비스를 사용하는 경우, 다른 서비스에서 다른 작업을 시작하는 작업을 수행할 수 있습니다. FAS는를 호출하는 보안 주체의 권한을 다운스트림 서비스에 AWS 서비스 대한 요청과 AWS 서비스함께 사용합니다. FAS 요청은 서비스가 완료하기 위해 다른 AWS 서비스 또는 리소스와의 상호 작용이 필요한 요청을 수신할 때만 이루어집니다. 이 경우, 두 작업을 모두 수행할 수 있는 권한이 있어야 합니다. FAS 요청 시 정책 세부 정보는 전달 액세스 세션을 참조하세요.
  - 서비스 역할 - 서비스 역할은 서비스가 사용자를 대신하여 작업을 수행하기 위해 맡는 IAM 역할입니다. IAM 관리자는 IAM 내에서 서비스 역할을 생성, 수정 및 삭제할 수 있습니다. 자세한 정보는 IAM 사용 설명서의 Create a role to delegate permissions to an AWS 서비스를 참조하세요.
  - 서비스 연결 역할 - 서비스 연결 역할은에 연결된 서비스 역할의 한 유형입니다 AWS 서비스. 서비스는 사용자를 대신하여 작업을 수행하기 위해 역할을 수임할 수 있습니다. 서비스 연결 역할은에 표시 AWS 계정 되며 서비스가 소유합니다. IAM 관리자는 서비스 링크 역할의 권한을 볼 수 있지만 편집은 할 수 없습니다.
- Amazon EC2에서 실행되는 애플리케이션 - IAM 역할을 사용하여 EC2 인스턴스에서 실행되고 AWS CLI 또는 AWS API 요청을 수행하는 애플리케이션의 임시 자격 증명을 관리할 수 있습니다. 이는 EC2 인스턴스 내에 액세스 키를 저장할 때 권장되는 방법입니다. EC2 인스턴스에 AWS 역할을 할당하고 모든 애플리케이션에서 사용할 수 있도록 하려면 인스턴스에 연결된 인스턴스 프로파일을 생성합니다. 인스턴스 프로필에는 역할이 포함되어 있으며 EC2 인스턴스에서 실행되는 프로그

램이 임시 보안 인증을 얻을 수 있습니다. 자세한 정보는 IAM 사용 설명서의 IAM 역할을 사용하여 Amazon EC2 인스턴스에서 실행되는 애플리케이션에 권한 부여를 참조하세요.

정책을 사용하여 액세스 관리

정책을 AWS 생성하고 자격 증명 또는 리소스에 연결하여 AWS 에서 액세스를 제어합니다. 정책은 자격 증명 또는 리소스와 연결 AWS 될 때 권한을 정의하는의 객체입니다.는 보안 주체(사용자, 루트 사용자 또는 역할 세션)가 요청할 때 이러한 정책을 AWS 평가합니다. 정책에서 권한은 요청이 허용되거나 거부되는 지를 결정합니다. 대부분의 정책은에 JSON 문서 AWS 로 저장됩니다. JSON 정책 문서의 구조와 콘텐츠에 대한 자세한 정보는 IAM 사용 설명서의 JSON 정책 개요를 참조하세요.

관리자는 AWS JSON 정책을 사용하여 누가 무엇에 액세스할 수 있는지 지정할 수 있습니다. 즉, 어떤 보안 주체가 어떤 리소스와 어떤 조건에서 작업을 수행할 수 있는지를 지정할 수 있습니다.

기본적으로, 사용자 및 역할에는 어떠한 권한도 없습니다. 사용자에게 사용자가 필요한 리소스에서 작업을 수행할 권한을 부여하려면 IAM 관리자가 IAM 정책을 생성하면 됩니다. 그런 다음 관리자가 IAM 정책을 역할에 추가하고, 사용자가 역할을 수임할 수 있습니다.

IAM 정책은 작업을 수행하기 위해 사용하는 방법과 상관없이 작업에 대한 권한을 정의합니다. 예를 들어, `iam:GetRole` 작업을 허용하는 정책이 있다고 가정합니다. 해당 정책이 있는 사용자는 AWS Management Console AWS CLI, 또는 API에서 역할 정보를 가져올 수 있습니다 AWS .

ID 기반 정책

ID 기반 정책은 IAM 사용자, 사용자 그룹 또는 역할과 같은 ID에 연결할 수 있는 JSON 권한 정책 문서입니다. 이러한 정책은 사용자 및 역할이 어떤 리소스와 어떤 조건에서 어떤 작업을 수행할 수 있는지를 제어합니다. 자격 증명 기반 정책을 생성하는 방법을 알아보려면 IAM 사용 설명서에서 고객 관리형 정책으로 사용자 지정 IAM 권한 정의를 참조하세요.

ID 기반 정책은 인라인 정책 또는 관리형 정책으로 한층 더 분류할 수 있습니다. 인라인 정책은 단일 사용자, 그룹 또는 역할에 직접 포함됩니다. 관리형 정책은의 여러 사용자, 그룹 및 역할에 연결할 수 있는 독립 실행형 정책입니다 AWS 계정. 관리형 정책에는 AWS 관리형 정책 및 고객 관리형 정책이 포함됩니다. 관리형 정책 또는 인라인 정책을 선택하는 방법을 알아보려면 IAM 사용 설명서의 관리형 정책 및 인라인 정책 중에서 선택을 참조하세요.

리소스 기반 정책

리소스 기반 정책은 리소스에 연결하는 JSON 정책 설명서입니다. 리소스 기반 정책의 예제는 IAM 역할 신뢰 정책과 Amazon S3 버킷 정책입니다. 리소스 기반 정책을 지원하는 서비스에서 서비스 관리자

는 이러한 정책을 사용하여 특정 리소스에 대한 액세스를 통제할 수 있습니다. 정책이 연결된 리소스의 경우 정책은 지정된 위탁자가 해당 리소스와 어떤 조건에서 어떤 작업을 수행할 수 있는지를 정의합니다. 리소스 기반 정책에서 위탁자를 지정해야 합니다. 보안 주체에는 계정, 사용자, 역할, 페더레이션 사용자 또는이 포함될 수 있습니다 AWS 서비스.

리소스 기반 정책은 해당 서비스에 있는 인라인 정책입니다. 리소스 기반 정책에서는 IAM의 AWS 관리형 정책을 사용할 수 없습니다.

액세스 제어 목록(ACL)

액세스 제어 목록(ACL)은 어떤 보안 주체(계정 멤버, 사용자 또는 역할)가 리소스에 액세스할 수 있는 권한을 가지고 있는지를 제어합니다. ACL은 JSON 정책 문서 형식을 사용하지 않지만 리소스 기반 정책과 유사합니다.

Amazon S3 AWS WAF및 Amazon VPC는 ACLs. ACL에 관한 자세한 내용은 Amazon Simple Storage Service 개발자 가이드의 액세스 제어 목록(ACL) 개요를 참조하세요.

기타 정책 타입

AWS 는 덜 일반적인 추가 정책 유형을 지원합니다. 이러한 정책 타입은 더 일반적인 정책 유형에 따라 사용자에게 부여되는 최대 권한을 설정할 수 있습니다.

- 권한 경계 – 권한 경계는 ID 기반 정책에 따라 IAM 엔터티(IAM 사용자 또는 역할)에 부여할 수 있는 최대 권한을 설정하는 고급 기능입니다. 개체에 대한 권한 경계를 설정할 수 있습니다. 그 결과로 얻는 권한은 객체의 ID 기반 정책과 그 권한 경계의 교집합입니다. `Principal` 필드에서 사용자나 역할을 지정하는 리소스 기반 정책은 권한 경계를 통해 제한되지 않습니다. 이러한 정책 중 하나에 포함된 명시적 거부는 허용을 재정의합니다. 권한 경계에 대한 자세한 정보는 IAM 사용 설명서의 IAM 엔티티에 대한 권한 경계를 참조하세요.
- 서비스 제어 정책(SCPs) - SCPs는의 조직 또는 조직 단위(OU)에 대한 최대 권한을 지정하는 JSON 정책입니다 AWS Organizations. AWS Organizations 는 AWS 계정 기업이 소유한 여러을 그룹화하고 중앙에서 관리하기 위한 서비스입니다. 조직에서 모든 기능을 활성화할 경우, 서비스 제어 정책(SCP)을 임의의 또는 모든 계정에 적용할 수 있습니다. SCP는 각각을 포함하여 멤버 계정의 엔터티에 대한 권한을 제한합니다 AWS 계정 루트 사용자. 조직 및 SCP에 대한 자세한 내용은 AWS Organizations 사용 설명서에서 Service control policies을 참조하세요.
- 리소스 제어 정책(RCP) - RCP는 소유한 각 리소스에 연결된 IAM 정책을 업데이트하지 않고 계정의 리소스에 대해 사용 가능한 최대 권한을 설정하는 데 사용할 수 있는 JSON 정책입니다. RCP는 멤버 계정의 리소스에 대한 권한을 제한하며 조직에 속하는지 여부에 AWS 계정 루트 사용자관계없이를 포함한 자격 증명에 대한 유효 권한에 영향을 미칠 수 있습니다. RCP를 AWS 서비스 지원하는 목록

을 포함하여 조직 및 RCPs에 대한 자세한 내용은 AWS Organizations 사용 설명서의 리소스 제어 정책(RCPs)을 참조하세요.

- 세션 정책 – 세션 정책은 역할 또는 페더레이션 사용자에 대해 임시 세션을 프로그래밍 방식으로 생성할 때 파라미터로 전달하는 고급 정책입니다. 결과적으로 얻는 세션의 권한은 사용자 또는 역할의 ID 기반 정책의 교차와 세션 정책입니다. 또한 권한을 리소스 기반 정책에서 가져올 수도 있습니다. 이러한 정책 중 하나에 포함된 명시적 거부는 허용을 재정의합니다. 자세한 정보는 IAM 사용 설명서의 세션 정책을 참조하세요.

여러 정책 유형

여러 정책 유형이 요청에 적용되는 경우, 결과 권한은 이해하기가 더 복잡합니다. 에서 여러 정책 유형이 관련될 때 요청을 허용할지 여부를 AWS 결정하는 방법을 알아보려면 IAM 사용 설명서의 정책 평가 로직을 참조하세요.

AWS Systems Manager Incident Manager 에서 IAM을 사용하는 방법

IAM을 사용하여 Incident Manager에 대한 액세스를 관리하기 전에 Incident Manager와 함께 사용할 수 있는 IAM 기능을 알아보세요.

에서 사용할 수 있는 IAM 기능 AWS Systems Manager Incident Manager

IAM 기능	Incident Manager 지원
ID 기반 정책	예
리소스 기반 정책	예
정책 작업	예
정책 리소스	예
정책 조건 키	아니요
ACL	아니요
ABAC(정책 내 태그)	아니요
임시 보안 인증	예

IAM 기능	Incident Manager 지원
보안 주체 권한	예
서비스 역할	예
서비스 연결 역할	예

Incident Manager 및 기타 AWS 서비스가 대부분의 IAM 기능과 작동하는 방식을 전체적으로 알아보려면 IAM 사용 설명서의 AWS IAM으로 작업하는 서비스를 참조하세요.

Incident Manager는 AWS RAM를 사용하여 공유하는 리소스에 대한 액세스를 거부하는 정책을 지원하지 않습니다.

Incident Manager 자격 증명 기반 정책

ID 기반 정책 지원: 예

ID 기반 정책은 IAM 사용자, 사용자 그룹 또는 역할과 같은 ID에 연결할 수 있는 JSON 권한 정책 문서입니다. 이러한 정책은 사용자 및 역할이 어떤 리소스와 어떤 조건에서 어떤 작업을 수행할 수 있는지를 제어합니다. 자격 증명 기반 정책을 생성하는 방법을 알아보려면 IAM 사용 설명서에서 고객 관리형 정책으로 사용자 지정 IAM 권한 정의를 참조하세요.

IAM ID 기반 정책을 사용하면 허용되거나 거부되는 작업과 리소스뿐 아니라 작업이 허용되거나 거부되는 조건을 지정할 수 있습니다. ID 기반 정책에서는 위탁자가 연결된 사용자 또는 역할에 적용되므로 위탁자를 지정할 수 없습니다. JSON 정책에서 사용하는 모든 요소에 대해 알아보려면 IAM 사용 설명서의 IAM JSON 정책 요소 참조를 참조하세요.

Incident Manager 자격 증명 기반 정책 예제

Incident Manager 자격 증명 기반 정책의 예제를 보려면 AWS Systems Manager Incident Manager에 대한 자격 증명 기반 정책 예시 섹션을 참조하세요.

Incident Manager 내 리소스 기반 정책

리소스 기반 정책 지원: 예

리소스 기반 정책은 리소스에 연결하는 JSON 정책 설명서입니다. 리소스 기반 정책의 예제는 IAM 역할 신뢰 정책과 Amazon S3 버킷 정책입니다. 리소스 기반 정책을 지원하는 서비스에서 서비스 관리자

는 이러한 정책을 사용하여 특정 리소스에 대한 액세스를 통제할 수 있습니다. 정책이 연결된 리소스의 경우 정책은 지정된 위탁자가 해당 리소스와 어떤 조건에서 어떤 작업을 수행할 수 있는지를 정의합니다. 리소스 기반 정책에서 위탁자를 지정해야 합니다. 보안 주체에는 계정, 사용자, 역할, 페더레이션 사용자 또는이 포함될 수 있습니다 AWS 서비스.

교차 계정 액세스를 활성화하려는 경우, 전체 계정이나 다른 계정의 IAM 개체를 리소스 기반 정책의 위탁자로 지정할 수 있습니다. 리소스 기반 정책에 크로스 계정 보안 주체를 추가하는 것은 트러스트 관계 설정의 절반밖에 되지 않는다는 것을 유념하세요. 보안 주체와 리소스가 다른 경우 신뢰할 수 AWS 계정있는 계정의 IAM 관리자는 보안 주체 엔터티(사용자 또는 역할)에게 리소스에 액세스할 수 있는 권한도 부여해야 합니다. 엔터티에 ID 기반 정책을 연결하여 권한을 부여합니다. 하지만 리소스 기반 정책이 동일 계정의 위탁자에 액세스를 부여하는 경우, 추가 자격 증명 기반 정책이 필요하지 않습니다. 자세한 내용은 IAM 사용 설명서의 교차 계정 리소스 액세스를 참조하세요.

Incident Manager 서비스는 대응 계획 또는 연락처에 연결된 AWS RAM 콘솔 또는 PutResourcePolicy 작업을 사용하여 라는 두 가지 유형의 리소스 기반 정책만 지원합니다. 이 정책은 대응 계획, 연락처, 에스컬레이션 계획 및 인시던트에 대해 조치를 취할 수 있는 보안 주체를 정의합니다. Incident Manager는 리소스 기반 정책을 사용하여 계정 간에 리소스를 공유합니다.

Incident Manager는 AWS RAM를 사용하여 공유하는 리소스에 대한 액세스를 거부하는 정책을 지원하지 않습니다.

대응 계획이나 연락처에 리소스 기반 정책을 연결하는 방법은 Incident Manager에서 AWS 계정 및 리전 간 인시던트 관리 섹션을 참조하세요.

Incident Manager 내 리소스 기반 정책 예제

Incident Manager 리소스 기반 정책의 예제를 보려면 에 대한 리소스 기반 정책 예제 AWS Systems Manager Incident Manager 섹션을 참조하세요.

Incident Manager를 위한 정책 작업

정책 작업 지원: 예

관리자는 AWS JSON 정책을 사용하여 누가 무엇에 액세스할 수 있는지 지정할 수 있습니다. 즉, 어떤 위탁자가 어떤 리소스와 어떤 조건에서 작업을 수행할 수 있는지를 지정할 수 있습니다.

JSON 정책의 `Action` 요소는 정책에서 액세스를 허용하거나 거부하는 데 사용할 수 있는 작업을 설명합니다. 정책 작업은 일반적으로 연결된 AWS API 작업과 이름이 동일합니다. 일치하는 API 작업이 없는 권한 전용 작업 같은 몇 가지 예외도 있습니다. 정책에서 여러 작업이 필요한 몇 가지 작업도 있습니다. 이러한 추가 작업을 일컬어 종속 작업이라고 합니다.

연결된 작업을 수행할 수 있는 권한을 부여하기 위한 정책에 작업을 포함하세요.

Incident Manager 작업 목록을 보려면 서비스 승인 참조의 AWS Systems Manager Incident Manager에서 정의한 작업을 참조하세요.

Incident Manager의 정책 작업은 작업 앞에 다음 접두사를 사용합니다.

```
ssm-incidents
ssm-contacts
```

단일 문에서 여러 작업을 지정하려면 다음과 같이 쉼표로 구분합니다.

```
"Action": [
      "ssm-incidents:GetResponsePlan",
      "ssm-contacts:GetContact"
         ]
```

와일드카드(*)를 사용하여 여러 작업을 지정할 수 있습니다. 예를 들어, Get라는 단어로 시작하는 모든 태스크를 지정하려면 다음 태스크를 포함합니다.

```
"Action": "ssm-incidents:Get*"
```

Incident Manager 자격 증명 기반 정책의 예제를 보려면 AWS Systems Manager Incident Manager에 대한 자격 증명 기반 정책 예시 섹션을 참조하세요.

Incident Manager는 ssm-인시던트와 ssm-연락처라는 두 개의 서로 다른 네임스페이스에서 작업을 사용합니다. Incident Manager에 대한 정책을 만들 때는 작업에 맞는 네임스페이스를 사용해야 합니다. SSM-인시던트는 대응 계획 및 인시던트 관련 작업에 사용됩니다. SSM-연락처는 연락처 및 연락처 참여와 관련된 작업에 사용됩니다. 예시:

- `ssm-contacts:GetContact`
- `ssm-incidents:GetResponsePlan`

Incident Manager를 위한 정책 리소스

정책 리소스 지원: 예

관리자는 AWS JSON 정책을 사용하여 누가 무엇에 액세스할 수 있는지 지정할 수 있습니다. 즉, 어떤 보안 주체가 어떤 리소스와 어떤 조건에서 작업을 수행할 수 있는지를 지정할 수 있습니다.

`Resource` JSON 정책 요소는 작업이 적용되는 하나 이상의 객체를 지정합니다. 문에는 `Resource`또는 `NotResource`요소가 반드시 추가되어야 합니다. 모범 사례에 따라 Amazon 리소스 이름(ARN)을 사용하여 리소스를 지정합니다. 리소스 수준 권한이라고 하는 특정 리소스 유형을 지원하는 작업에 대해 이를 수행할 수 있습니다.

작업 나열과 같이 리소스 수준 권한을 지원하지 않는 작업의 경우, 와일드카드(*)를 사용하여 해당 문이 모든 리소스에 적용됨을 나타냅니다.

```
"Resource": "*"
```

Incident Manager 리소스 유형 및 해당 ARN의 목록을 보려면 서비스 권한 부여 참조에서 AWS Systems Manager Incident Manager에서 정의한 리소스를 참조하세요. 각 리소스의 ARN을 지정할 수 있는 작업을 알아보려면 AWS Systems Manager Incident Manager가 정의한 작업을 참조하십시오.

Incident Manager 자격 증명 기반 정책의 예제를 보려면 AWS Systems Manager Incident Manager에 대한 자격 증명 기반 정책 예시 섹션을 참조하세요.

Incident Manager 리소스는 인시던트를 생성하고, 채팅 채널에서 협업하고, 인시던트를 해결하고, 대응 담당자를 참여시키는 데 사용됩니다. 사용자가 대응 계획에 액세스할 수 있는 경우 해당 계획을 기반으로 생성된 모든 인시던트에 액세스할 수 있습니다. 연락처 또는 에스컬레이션 계획에 액세스할 수 있는 사용자는 해당 연락처를 에스컬레이션 계획에 참여시킬 수 있습니다.

Incident Manager에 대한 정책 조건 키

서비스별 정책 조건 키 지원: 아니요

관리자는 AWS JSON 정책을 사용하여 누가 무엇에 액세스할 수 있는지 지정할 수 있습니다. 즉, 어떤 보안 주체가 어떤 리소스와 어떤 조건에서 작업을 수행할 수 있는지를 지정할 수 있습니다.

`Condition` 요소(또는 `Condition` 블록)를 사용하면 정책이 발효되는 조건을 지정할 수 있습니다. `Condition` 요소는 옵션입니다. 같거나 작음과 같은 조건 연산자를 사용하여 정책의 조건을 요청의 값과 일치시키는 조건식을 생성할 수 있습니다.

한 문에서 여러 `Condition` 요소를 지정하거나 단일 `Condition` 요소에서 여러 키를 지정하는 경우, AWS 는 논리적 `AND` 작업을 사용하여 평가합니다. 단일 조건 키에 여러 값을 지정하는 경우는 논리적

0R 작업을 사용하여 조건을 AWS 평가합니다. 문의 권한을 부여하기 전에 모든 조건을 충족해야 합니다.

조건을 지정할 때 자리 표시자 변수를 사용할 수도 있습니다. 예를 들어, IAM 사용자에게 IAM 사용자 이름으로 태그가 지정된 경우에만 리소스에 액세스할 수 있는 권한을 부여할 수 있습니다. 자세한 내용은 IAM 사용 설명서의 IAM 정책 요소: 변수 및 태그를 참조하세요.

AWS 는 전역 조건 키와 서비스별 조건 키를 지원합니다. 모든 AWS 전역 조건 키를 보려면 IAM 사용 설명서의 AWS 전역 조건 컨텍스트 키를 참조하세요.

Incident Manager 액세스 제어 목록(ACL)

ACL 지원: 아니요

액세스 제어 목록(ACL)은 어떤 위탁자(계정 멤버, 사용자 또는 역할)가 리소스에 액세스할 수 있는 권한을 가지고 있는지를 제어합니다. ACL은 JSON 정책 문서 형식을 사용하지 않지만 리소스 기반 정책과 유사합니다.

Incident Manager에서 속성 기반 액세스 제어(ABAC)

ABAC 지원(정책의 태그): 아니요

속성 기반 액세스 제어(ABAC)는 속성에 근거하여 권한을 정의하는 권한 부여 전략입니다. 에서는 AWS이러한 속성을 태그라고 합니다. IAM 엔터티(사용자 또는 역할) 및 많은 AWS 리소스에 태그를 연결할 수 있습니다. ABAC의 첫 번째 단계로 개체 및 리소스에 태그를 지정합니다. 그런 다음 위탁자의 태그가 액세스하려는 리소스의 태그와 일치할 때 작업을 허용하도록 ABAC 정책을 설계합니다.

ABAC는 빠르게 성장하는 환경에서 유용하며 정책 관리가 번거로운 상황에 도움이 됩니다.

태그에 근거하여 액세스를 제어하려면 `aws:ResourceTag/key-name`, `aws:RequestTag/key-name` 또는 `aws:TagKeys` 조건 키를 사용하여 정책의 조건 요소에 태그 정보를 제공합니다.

서비스가 모든 리소스 유형에 대해 세 가지 조건 키를 모두 지원하는 경우, 값은 서비스에 대해 예입니다. 서비스가 일부 리소스 유형에 대해서만 세 가지 조건 키를 모두 지원하는 경우, 값은 부분적입니다.

ABAC에 대한 자세한 내용은 IAM 사용 설명서의 ABAC 권한 부여를 통한 권한 정의를 참조하세요. ABAC 설정 단계가 포함된 자습서를 보려면 IAM 사용 설명서의 속성 기반 액세스 제어(ABAC) 사용을 참조하세요.

Incident Manager에서 임시 자격 증명 사용

임시 자격 증명 지원: 예

일부 AWS 서비스 는 임시 자격 증명을 사용하여 로그인할 때 작동하지 않습니다. 임시 자격 증명으로 AWS 서비스 작업하는를 비롯한 추가 정보는 AWS 서비스 IAM 사용 설명서의 IAM으로 작업하는 섹션을 참조하세요.

사용자 이름과 암호를 제외한 방법을 AWS Management Console 사용하여에 로그인하는 경우 임시 자격 증명을 사용합니다. 예를 들어 회사의 SSO(Single Sign-On) 링크를 AWS 사용하여에 액세스하면 해당 프로세스가 임시 자격 증명을 자동으로 생성합니다. 또한 콘솔에 사용자로 로그인한 다음 역할을 전환할 때 임시 자격 증명을 자동으로 생성합니다. 역할 전환에 대한 자세한 내용은 IAM 사용 설명서의 사용자에서 IAM 역할로 전환(콘솔)을 참조하세요.

AWS CLI 또는 AWS API를 사용하여 임시 자격 증명을 수동으로 생성할 수 있습니다. 그런 다음 이러한 임시 자격 증명을 사용하여 장기 액세스 키를 사용하는 대신 임시 자격 증명을 동적으로 생성하는 access AWS. AWS recommds에 액세스할 수 있습니다. 자세한 정보는 IAM의 임시 보안 자격 증명 섹션을 참조하세요.

Incident Manager의 교차 서비스 보안 주체 권한

전달 액세스 세션(FAS) 지원: 예

IAM 사용자 또는 역할을 사용하여에서 작업을 수행하는 경우 AWS보안 주체로 간주됩니다. 일부 서비스를 사용하는 경우, 다른 서비스에서 다른 작업을 시작하는 작업을 수행할 수 있습니다. FAS는를 호출하는 보안 주체의 권한을 다운스트림 서비스에 AWS 서비스 대한 요청과 AWS 서비스함께 사용합니다. FAS 요청은 서비스가 완료하기 위해 다른 AWS 서비스 또는 리소스와의 상호 작용이 필요한 요청을 수신할 때만 이루어집니다. 이 경우, 두 작업을 모두 수행할 수 있는 권한이 있어야 합니다. FAS 요청 시 정책 세부 정보는 전달 액세스 세션을 참조하세요.

Incident Manager의 서비스 역할

서비스 역할 지원: 예

서비스 역할은 서비스가 사용자를 대신하여 작업을 수행하는 것으로 가정하는 IAM 역할입니다. IAM 관리자는 IAM 내에서 서비스 역할을 생성, 수정 및 삭제할 수 있습니다. 자세한 정보는 IAM 사용 설명서의 Create a role to delegate permissions to an AWS 서비스를 참조하세요.

> **Warning**
>
> 서비스 역할에 대한 권한을 변경하면 Incident Manager 기능이 중단될 수 있습니다. Incident Manager가 관련 지침을 제공하는 경우에만 서비스 역할을 편집합니다.

Incident Manager에서 IAM 역할 선택하기

Incident Manager에서 대응 계획 리소스를 생성할 경우 Incident Manager가 사용자를 대신하여 Systems Manager 자동화 문서를 실행할 수 있는 역할을 선택해야 합니다. 이전에 서비스 역할 또는 서비스 연결 역할을 생성한 경우 Incident Manager는 선택할 수 있는 역할 목록을 제공합니다. 자동화 문서 인스턴스를 실행할 수 있도록 허용하는 역할을 선택하는 것이 중요합니다. 자세한 내용은 인시던트 해결을 위해 Incident Manager에 Systems Manager Automation 런북 통합 단원을 참조하십시오. 인시던트 중에 사용할 채팅 애플리케이션 채팅 채널에서 Amazon Q Developer를 생성할 때 채팅에서 직접 명령을 사용할 수 있는 서비스 역할을 선택할 수 있습니다. 인시던트 협업에 대한 채팅 채널 생성에 대한 자세한 내용은 Incident Manager에서 대응 담당자를 위한 채팅 채널 생성 및 통합 섹션을 참조하세요. 채팅 애플리케이션의 Amazon Q Developer에서 IAM 정책에 대해 자세히 알아보려면 채팅 애플리케이션의 Amazon Q Developer 관리자 안내서의 채팅 애플리케이션에서 Amazon Q Developer를 사용하여 명령을 실행할 수 있는 권한 관리를 참조하세요.

Incident Manager의 서비스 연결 역할

서비스 링크 역할 지원: 예

서비스 연결 역할은에 연결된 서비스 역할의 한 유형입니다 AWS 서비스. 서비스는 사용자를 대신하여 작업을 수행하기 위해 역할을 수임할 수 있습니다. 서비스 연결 역할은에 나타나 AWS 계정 며 서비스가 소유합니다. IAM 관리자는 서비스 링크 역할의 권한을 볼 수 있지만 편집은 할 수 없습니다.

Incident Manager 서비스 연결 역할을 생성하거나 관리하는 방법에 대한 자세한 내용은 Incident Manager의 서비스 연결 역할 섹션을 참조하세요.

AWS Systems Manager Incident Manager에 대한 자격 증명 기반 정책 예시

기본적으로 사용자 및 역할에는 Incident Manager 리소스를 생성하거나 수정할 수 있는 권한이 없습니다. 또한 AWS Management Console, AWS Command Line Interface (AWS CLI) 또는 AWS API를 사용하여 작업을 수행할 수 없습니다. 사용자에게 사용자가 필요한 리소스에서 작업을 수행할 권한을 부여하려면 IAM 관리자가 IAM 정책을 생성하면 됩니다. 그런 다음 관리자가 IAM 정책을 역할에 추가하고, 사용자가 역할을 맡을 수 있습니다.

이러한 예제 JSON 정책 문서를 사용하여 IAM 자격 증명 기반 정책을 생성하는 방법을 알아보려면 IAM 사용 설명서의 IAM 정책 생성(콘솔)을 참조하세요.

각 리소스 유형에 대한 ARN 형식을 포함하여 Incident Manager에서 정의한 작업 및 리소스 유형에 대한 자세한 내용은 서비스 권한 부여 참조의 AWS Systems Manager Incident Manager에 대한 작업, 리소스 및 조건 키를 참조하세요.

주제

- 정책 모범 사례
- Incident Manager 콘솔 사용
- 사용자가 자신의 고유한 권한을 볼 수 있도록 허용
- 대응 계획에 액세스

정책 모범 사례

ID 기반 정책에 따라 계정에서 사용자가 Incident Manager 리소스를 생성, 액세스 또는 삭제할 수 있는지 여부가 결정됩니다. 이 작업으로 인해 AWS 계정에 비용이 발생할 수 있습니다. ID 기반 정책을 생성하거나 편집할 때는 다음 지침과 권장 사항을 따릅니다.

- AWS 관리형 정책을 시작하고 최소 권한으로 전환 - 사용자 및 워크로드에 권한 부여를 시작하려면 많은 일반적인 사용 사례에 대한 권한을 부여하는 AWS 관리형 정책을 사용합니다. 에서 사용할 수 있습니다 AWS 계정. 사용 사례에 맞는 AWS 고객 관리형 정책을 정의하여 권한을 추가로 줄이는 것이 좋습니다. 자세한 정보는 IAM 사용 설명서의 AWS 관리형 정책 또는 AWS 직무에 대한 관리형 정책을 참조하세요.
- 최소 권한 적용 – IAM 정책을 사용하여 권한을 설정하는 경우, 작업을 수행하는 데 필요한 권한만 부여합니다. 이렇게 하려면 최소 권한으로 알려진 특정 조건에서 특정 리소스에 대해 수행할 수 있는 작업을 정의합니다. IAM을 사용하여 권한을 적용하는 방법에 대한 자세한 정보는 IAM 사용 설명서에 있는 IAM의 정책 및 권한을 참조하세요.
- IAM 정책의 조건을 사용하여 액세스 추가 제한 – 정책에 조건을 추가하여 작업 및 리소스에 대한 액세스를 제한할 수 있습니다. 예를 들어, SSL을 사용하여 모든 요청을 전송해야 한다고 지정하는 정책 조건을 작성할 수 있습니다. AWS 서비스와 같은 특정를 통해 사용되는 경우 조건을 사용하여 서비스 작업에 대한 액세스 권한을 부여할 수도 있습니다 AWS CloudFormation. 자세한 정보는 IAM 사용 설명서의 IAM JSON 정책 요소: 조건을 참조하세요.
- IAM Access Analyzer를 통해 IAM 정책을 확인하여 안전하고 기능적인 권한 보장 - IAM Access Analyzer에서는 IAM 정책 언어(JSON)와 모범 사례가 정책에서 준수되도록 새로운 및 기존 정책을 확인합니다. IAM Access Analyzer는 100개 이상의 정책 확인 항목과 실행 가능한 추천을 제공하여 안전하고 기능적인 정책을 작성하도록 돕습니다. 자세한 내용은 IAM 사용 설명서의 IAM Access Analyzer에서 정책 검증을 참조하세요.
- 다중 인증(MFA) 필요 -에서 IAM 사용자 또는 루트 사용자가 필요한 시나리오가 있는 경우 추가 보안을 위해 MFA를 AWS 계정켭니다. API 작업을 직접 호출할 때 MFA가 필요하면 정책에 MFA 조건을 추가합니다. 자세한 내용은 IAM 사용 설명서의 MFA를 통한 보안 API 액세스를 참조하세요.

IAM의 모범 사례에 대한 자세한 내용은 IAM 사용 설명서의 IAM의 보안 모범 사례를 참조하세요.

Incident Manager 콘솔 사용

AWS Systems Manager Incident Manager 콘솔에 액세스하려면 최소 권한 집합이 있어야 합니다. 이러한 권한은 AWS 계정에서 Incident Manager 리소스에 대한 세부 정보를 나열하고 볼 수 있도록 허용해야 합니다. 최소 필수 권한보다 더 제한적인 ID 기반 정책을 생성하는 경우, 콘솔이 해당 정책에 연결된 엔티티(사용자 또는 역할)에 대해 의도대로 작동하지 않습니다.

AWS CLI 또는 AWS API만 호출하는 사용자에게는 최소 콘솔 권한을 허용할 필요가 없습니다. 대신 수행하려는 API 작업과 일치하는 작업에만 액세스할 수 있도록 합니다.

사용자와 역할이 Incident Manager 콘솔을 사용하여 인시던트를 해결할 수 있도록 하려면 Incident Manager `IncidentManagerResolverAccess` AWS 관리형 정책도 엔터티에 연결합니다. 자세한 내용은 IAM 사용 설명서의 사용자에게 권한 추가를 참조하세요.

```
IncidentManagerResolverAccess
```

사용자가 자신의 고유한 권한을 볼 수 있도록 허용

이 예제는 IAM 사용자가 자신의 사용자 ID에 연결된 인라인 및 관리형 정책을 볼 수 있도록 허용하는 정책을 생성하는 방법을 보여줍니다. 이 정책에는 콘솔에서 또는 AWS CLI 또는 AWS API를 사용하여 프로그래밍 방식으로이 작업을 완료할 수 있는 권한이 포함됩니다.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ViewOwnUserInfo",
            "Effect": "Allow",
            "Action": [
                "iam:GetUserPolicy",
                "iam:ListGroupsForUser",
                "iam:ListAttachedUserPolicies",
                "iam:ListUserPolicies",
                "iam:GetUser"
            ],
            "Resource": ["arn:aws:iam::*:user/${aws:username}"]
        },
        {
            "Sid": "NavigateInConsole",
            "Effect": "Allow",
            "Action": [
                "iam:GetGroupPolicy",
```

```
                "iam:GetPolicyVersion",
                "iam:GetPolicy",
                "iam:ListAttachedGroupPolicies",
                "iam:ListGroupPolicies",
                "iam:ListPolicyVersions",
                "iam:ListPolicies",
                "iam:ListUsers"
            ],
            "Resource": "*"
        }
    ]
}
```

대응 계획에 액세스

이 예에서는 Amazon Web Services 계정의 IAM 사용자에게 Incident Manager 대응 계획 중 하나인 `exampleplan`에 대한 액세스 권한을 부여하려고 합니다. 또한 사용자가 대응 계획을 추가, 업데이트 및 삭제하도록 허용하려고 합니다.

이 정책은 `ssm-incidents:ListResponsePlans`, `ssm-incidents:GetResponsePlan`, `ssm-incidents:UpdateResponsePlan` 및 `ssm-incident:ListResponsePlan` 권한을 사용자에게 부여합니다.

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Sid":"ListResponsePlans",
         "Effect":"Allow",
         "Action":[
            "ssm-incidents:ListResponsePlans"
         ],
         "Resource":"arn:aws:ssm-incidents:::*"
      },
      {
         "Sid":"ViewSpecificResponsePlanInfo",
         "Effect":"Allow",
         "Action":[
            "ssm-incidents:GetResponsePlan"
         ],
         "Resource":"arn:aws:ssm-incidents:*:111122223333:response-plan/exampleplan"
      },
      {
```

```
         "Sid":"ManageResponsePlan",
         "Effect":"Allow",
         "Action":[
            "ssm-incidents:UpdateResponsePlan"
         ],
         "Resource":"arn:aws:ssm-incidents:*:111122223333:response-plan/exampleplan/*"
      }
   ]
}
```

에 대한 리소스 기반 정책 예제 AWS Systems Manager Incident Manager

AWS Systems Manager Incident Manager 는 Incident Manager 대응 계획 및 연락처에 대한 리소스 기반 권한 정책을 지원합니다.

Incident Manager는를 사용하여 공유된 리소스에 대한 액세스를 거부하는 리소스 기반 정책을 지원하지 않습니다 AWS RAM.

대응 계획이나 연락처를 만드는 방법을 알아보려면 Incident Manager에서 대응 계획 생성 및 구성 및 Incident Manager에서 연락처 생성 및 구성 섹션을 참조하세요.

조직의 Incident Manager 대응 계획 액세스 제한

다음 예에서는 `o-abc123def45` 조직 ID를 가진 조직 내 사용자에게 `myplan` 대응 계획을 사용하여 생성된 인시던트에 대응할 수 있는 권한을 부여합니다.

`Condition` 블록은 `StringEquals` 조건과 AWS Organizations 특정 `aws:PrincipalOrgID` 조건 키인 조건 키를 사용합니다. 이러한 조건 키에 대한 자세한 내용은 정책의 조건 지정을 참조합니다.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "OrganizationAccess",
      "Effect": "Allow",
      "Principal": “*”,
      "Condition": {
         "StringEquals": {"aws:PrincipalOrgID":"o-abc123def45"}
      },
      "Action": [
```

```
        "ssm-incidents:GetResponsePlan",
        "ssm-incidents:StartIncident",
        "ssm-incidents:UpdateIncidentRecord",
        "ssm-incidents:GetIncidentRecord",
        "ssm-incidents:CreateTimelineEvent",
        "ssm-incidents:UpdateTimelineEvent",
        "ssm-incidents:GetTimelineEvent",
        "ssm-incidents:ListTimelineEvents",
        "ssm-incidents:UpdateRelatedItems",
        "ssm-incidents:ListRelatedItems"
      ],
      "Resource": [
        "arn:aws:ssm-incidents:*:111122223333:response-plan/myplan",
        "arn:aws:ssm-incidents:*:111122223333:incident-record/myplan/*"
      ]
    }
  ]
}
```

보안 주체에게 Incident Manager 연락처 액세스 권한 제공

다음 예시에서는 ARN `arn:aws:iam::999988887777:root`를 보유한 보안 주체에게 연락처 `mycontact`에 대한 참여를 생성할 수 있는 권한을 부여합니다.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "PrincipalAccess",
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws:iam::999988887777:root"
            },
            "Action": [
                "ssm-contacts:GetContact",
                "ssm-contacts:StartEngagement",
                "ssm-contacts:DescribeEngagement",
                "ssm-contacts:ListPagesByContact"
            ],
            "Resource": [
                "arn:aws:ssm-contacts:*:111122223333:contact/mycontact"
                "arn:aws:ssm-contacts:*:111122223333:engagement/mycontact/*"
            ]
```

```
        }
    ]
}
```

Incident Manager에서 교차 서비스 혼동된 대리자 예방

혼동된 대리자 문제는 작업을 수행할 권한이 없는 엔터티가 권한이 더 많은 엔터티를 호출하여 작업을 수행하도록 하는 경우에 발생합니다. 이를 통해 악의적인 공격자는 실행 또는 액세스할 수 있는 권한이 없는 명령을 실행하거나 리소스를 수정할 수 있습니다.

에서 AWS교차 서비스 가장은 혼동된 대리자 시나리오로 이어질 수 있습니다. 교차 서비스 가장은 한 서비스(직접적으로 호출하는 서비스)가 다른 서비스(직접적으로 호출되는 서비스)를 직접적으로 호출하는 경우입니다. 악의적인 공격자는 호출 서비스를 활용해 평소에는 없는 권한을 사용하여 다른 서비스의 리소스를 변경할 수 있습니다.

AWS 는 서비스 보안 주체에게 계정의 리소스에 대한 관리형 액세스 권한을 제공하여 리소스의 보안을 보호합니다. 리소스 정책에는 `aws:SourceArn` 및 `aws:SourceAccount` 전역 조건 컨텍스트 키를 사용하는 것이 좋습니다. 이러한 키는 해당 리소스에 다른 서비스를 AWS Systems Manager Incident Manager 제공하는 권한을 제한합니다. 두 글로벌 조건 컨텍스트 키를 모두 사용하는 경우 `aws:SourceAccount` 값과 `aws:SourceArn` 값에서 참조된 계정은 동일한 정책 문에서 사용할 경우 동일한 계정 ID를 사용해야 합니다.

`aws:SourceArn`의 값은 영향을 받은 인시던트 레코드의 ARN이어야 합니다. 리소스의 전체 ARN을 모를 경우 또는 여러 리소스를 지정하는 경우, ARN의 알 수 없는 부분에 대해 와일드카드(*)를 포함한 `aws:SourceArn` 글로벌 조건 컨텍스트 키를 사용합니다. 예를 들어, `aws:SourceArn~arn:aws:ssm-incidents::`*`111122223333`*`:*`을 설정할 수 있습니다.

다음 신뢰 정책 예에서는 `aws:SourceArn` 조건 키를 사용하여 인시던트 레코드의 ARN을 기반으로 서비스 역할에 대한 액세스를 제한합니다. 대응 계획 `myresponseplan`에서 생성된 인시던트 레코드만이 이 역할을 사용할 수 있습니다.

```
{
  "Version": "2012-10-17",
  "Statement": {
    "Effect": "Allow",
    "Principal": { "Service": "ssm-incidents.amazonaws.com" },
    "Action": "sts:AssumeRole",
    "Condition": {
      "ArnLike": {
        "aws:SourceArn": "arn:aws:ssm-incidents:*:111122223333:incident-record/
myresponseplan/*"
```

```
      }
    }
  }
}
```

Incident Manager의 서비스 연결 역할

AWS Systems Manager Incident Manager 는 AWS Identity and Access Management (IAM) 서비스 연결 역할을 사용합니다. 서비스 연결 역할은 Incident Manager에 직접 연결된 고유한 유형의 IAM 역할입니다. 서비스 연결 역할은 Incident Manager에서 사전 정의하며 서비스가 사용자를 대신하여 다른 AWS 서비스를 호출하는 데 필요한 모든 권한을 포함합니다.

서비스 연결 역할을 사용하면 필요한 권한을 수동으로 추가할 필요가 없으므로 Incident Manager를 더 쉽게 설정할 수 있습니다. Incident Manager에서 서비스 연결 역할의 권한을 정의하므로 다르게 정의되지 않은 한, Incident Manager만 해당 역할을 수임할 수 있습니다. 정의된 권한에는 신뢰 정책과 권한 정책이 포함되며 이 권한 정책은 다른 IAM 엔티티에 연결할 수 없습니다.

먼저 관련 리소스를 삭제한 후에만 서비스 연결 역할을 삭제할 수 있습니다. 이렇게 하면 리소스에 대한 액세스 권한을 부주의로 삭제할 수 없기 때문에 Incident Manager 리소스가 보호됩니다.

서비스 연결 역할을 지원하는 기타 서비스에 대한 자세한 내용은 IAM으로 작업하는AWS 서비스를 참조하고 서비스 연결 역할 열에 예가 있는 서비스를 찾습니다. 해당 서비스에 대한 서비스 연결 역할 설명서를 보려면 링크가 있는 예를 선택합니다.

Incident Manager에 대한 서비스 연결 역할 권한

Incident Manager는 AWSServiceRoleforIncidentManager라는 서비스 연결 역할을 사용합니다. 이 역할을 통해 Incident Manager는 사용자를 대신하여 Incident Manager 인시던트 레코드 및 관련 리소스를 관리할 수 있습니다.

AWSServiceRoleforIncidentManager 서비스 연결 역할은 역할을 수임하기 위해 다음 서비스를 신뢰합니다.

- `ssm-incidents.amazonaws.com`

역할 권한 정책 `AWSIncidentManagerServiceRolePolicy`는 Incident Manager가 지정된 리소스에서 다음 작업을 완료하도록 허용합니다.

- 작업: 작업과 관련된 모든 리소스에 대한 `ssm-incidents:ListIncidentRecords`

- 작업: 작업과 관련된 모든 리소스에 대한 `ssm-incidents:CreateTimelineEvent`
- 작업: 작업과 관련된 모든 리소스에 대한 `ssm:CreateOpsItem`
- 작업: `all resources related to the action.`에 대한 `ssm:AssociateOpsItemRelatedItem`
- 작업: 작업과 관련된 모든 리소스에 대한 `ssm-contacts:StartEngagement`
- 작업: `AWS/IncidentManager` 및 `AWS/Usage` 네임스페이스 내의 `cloudwatch:PutMetricData` CloudWatch 지표

IAM 엔터티(사용자, 그룹, 역할 등)가 서비스 링크 역할을 생성하고 편집하거나 삭제할 수 있도록 권한을 구성할 수 있습니다. 자세한 내용은 IAM 사용 설명서의 서비스 연결 역할 권한 섹션을 참조하세요.

Incident Manager용 서비스 연결 역할 생성

서비스 링크 역할은 수동으로 생성할 필요가 없습니다. AWS Management Console AWS CLI, 또는 AWS API에서 복제 세트를 생성하면 Incident Manager가 서비스 연결 역할을 생성합니다.

이 서비스 연결 역할을 삭제했다가 다시 생성해야 하는 경우 동일한 프로세스를 사용하여 계정에서 역할을 다시 생성할 수 있습니다. 복제 세트를 생성하면 Incident Manager에서 서비스 연결 역할이 자동으로 생성됩니다.

Incident Manager용 서비스 연결 역할 편집

Incident Manager에서는 AWSServiceRoleforIncidentManage 서비스 연결 역할을 편집할 수 없습니다. 서비스 연결 역할을 생성한 후에는 다양한 엔터티가 역할을 참조할 수 있기 때문에 역할 이름을 변경할 수 없습니다. 하지만 IAM을 사용하여 역할의 설명을 편집할 수 있습니다. 자세한 내용은 IAM 사용 설명서의 서비스 연결 역할 편집을 참조하세요.

Incident Manager용 서비스 연결 역할 삭제

서비스 연결 역할이 필요한 기능 또는 서비스가 더 이상 필요 없는 경우에는 해당 역할을 삭제하는 것이 좋습니다. 이렇게 하면 적극적으로 모니터링하거나 유지 관리하지 않는 미사용 엔터티가 없게 됩니다. 단, 서비스 링크 역할에 대한 리소스를 먼저 정리해야 수동으로 삭제할 수 있습니다.

서비스 연결 역할을 삭제하려면 먼저 복제 세트를 삭제해야 합니다. 복제 세트를 삭제하면 대응 계획, 연락처 및 에스컬레이션 계획을 포함하여 Incident Manager에서 생성되고 저장된 모든 데이터가 삭제됩니다. 또한 이전에 생성한 인시던트도 모두 손실됩니다. 삭제된 대응 계획을 가리키는 모든 경보 및 EventBridge 규칙으로 인해 더 이상 경보 또는 규칙 일치에 따른 인시던트가 생성되지 않습니다. 복제 세트를 삭제하려면 세트의 모든 리전을 삭제해야 합니다.

> **Note**
>
> 리소스를 삭제하려 할 때 Incident Manager 서비스가 역할을 사용 중이면 삭제에 실패할 수 있습니다. 이 문제가 발생하면 몇 분 기다렸다가 작업을 다시 시도하세요.

AWSServiceRoleforIncidentManager가 사용하는 복제 세트의 리전을 삭제하려면

1. Incident Manager 콘솔을 열고 왼쪽 탐색 메뉴에서 설정을 선택합니다.
2. 복제 세트의 리전을 선택합니다.
3. 삭제를 선택합니다.
4. 리전 삭제를 확인하려면 리전 이름을 입력하고 삭제를 선택합니다.
5. 복제 세트의 모든 리전을 삭제할 때까지 이 단계를 반복합니다. 최종 리전을 삭제하면 해당 리전이 있는 복제 세트도 삭제된다는 메시지가 콘솔에 표시됩니다.

IAM을 사용하여 수동으로 서비스 연결 역할을 삭제하려면 다음을 수행하세요.

IAM 콘솔 AWS CLI, 또는 AWS API를 사용하여 AWSServiceRoleforIncidentManager 서비스 연결 역할을 삭제합니다. 자세한 내용은 IAM 사용 설명서의 서비스 연결 역할 삭제를 참조하세요.

Incident Manager 서비스 연결 역할에 대해 지원되는 리전

Incident Manager는 서비스가 제공되는 모든 리전에서 서비스 연결 역할을 사용하도록 지원합니다. 자세한 내용은 AWS 리전 및 엔드포인트 섹션을 참조하세요.

AWS 에 대한 관리형 정책 AWS Systems Manager Incident Manager

AWS 관리형 정책은에서 생성하고 관리하는 독립 실행형 정책입니다 AWS. AWS 관리형 정책은 사용자, 그룹 및 역할에 권한 할당을 시작할 수 있도록 많은 일반적인 사용 사례에 대한 권한을 제공하도록 설계되었습니다.

AWS 관리형 정책은 모든 AWS 고객이 사용할 수 있으므로 특정 사용 사례에 대해 최소 권한을 부여하지 않을 수 있습니다. 사용 사례에 고유한 고객 관리형 정책을 정의하여 권한을 줄이는 것이 좋습니다.

AWS 관리형 정책에 정의된 권한은 변경할 수 없습니다. 가 관리형 정책에 정의된 권한을 AWS 업데이트하는 AWS 경우 업데이트는 정책이 연결된 모든 보안 주체 자격 증명(사용자, 그룹 및 역할)에 영향을 미칩니다. AWS AWS 서비스 는 새가 시작되거나 기존 서비스에 새 API 작업을 사용할 수 있게 될 때 AWS 관리형 정책을 업데이트할 가능성이 높습니다.

자세한 내용은 IAM 사용 설명서의 AWS 관리형 정책을 참조하세요.

AWS 관리형 정책: AWSIncidentManagerIncidentAccessServiceRolePolicy

`AWSIncidentManagerIncidentAccessServiceRolePolicy`을(를) IAM 엔티티에 연결할 수 있습니다. Incident Manager 는 Incident Manager 역할에 이 정책을 추가합니다. 그러면 Incident Manager가 사용자를 대신해 작업을 수행할 수 있도록 허용합니다.

이 정책은 Incident Manager가 특정 다른의 리소스를 읽고 해당 서비스의 인시던트와 관련된 조사 결과를 AWS 서비스 식별할 수 있는 읽기 전용 권한을 부여합니다.

권한 세부 정보

이 정책에는 다음 권한이 포함되어 있습니다.

- `cloudformation` - 보안 주체가 AWS CloudFormation 스택을 설명할 수 있도록 허용합니다. 이는 Incident Manager가 인시던트와 관련된 CloudFormation 이벤트 및 리소스를 식별하는 데 필요합니다.
- `codedeploy` - 보안 주체가 AWS CodeDeploy 배포를 읽을 수 있도록 허용합니다. 이는 Incident Manager가 인시던트와 관련된 CodeDeploy 배포 및 대상을 식별하는 데 필요합니다.
- `autoscaling` - 보안 주체가 Amazon Elastic Compute Cloud(EC2) 인스턴스가 Auto Scaling 그룹의 일부인지 확인할 수 있습니다. 이는 Incident Manager가 Auto Scaling 그룹의 일부인 EC2 인스턴스에 대한 조사 결과를 제공할 수 있도록 하기 위해 필요합니다.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "IncidentAccessPermissions",
            "Effect": "Allow",
            "Action": [
```

```
                "cloudformation:DescribeStackEvents",
                "cloudformation:DescribeStackResources",
                "codedeploy:BatchGetDeployments",
                "codedeploy:ListDeployments",
                "codedeploy:ListDeploymentTargets",
                "autoscaling:DescribeAutoScalingInstances"
            ],
            "Resource": "*"
        }
    ]
}
```

최신 버전의 JSON 정책 문서를 포함하여 정책에 대한 추가 세부 정보를 보려면 AWS 관리형 정책 참조 안내서의 AWSIncidentManagerIncidentAccessServiceRolePolicy를 참조하세요.

AWS 관리형 정책: **AWSIncidentManagerServiceRolePolicy**

AWSIncidentManagerServiceRolePolicy를 IAM 엔티티에 연결할 수 없습니다. 이 정책은 Incident Manager에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 자세한 내용은 Incident Manager의 서비스 연결 역할 단원을 참조하십시오.

이 정책은 Incident Manager에게 인시던트 나열, 타임라인 이벤트 생성, OpsItem 생성, 관련 항목을 OpsItem에 연결, 참여 시작, 인시던트와 관련된 CloudWatch 지표 게시를 수행할 수 있는 권한을 부여합니다.

권한 세부 정보

이 정책에는 다음 권한이 포함되어 있습니다.

- ssm-incidents – 보안 주체가 인시던트를 나열하고 타임라인 이벤트를 생성할 수 있도록 허용합니다. 이는 인시던트 발생 중에 대응 담당자가 인시던트 대시보드에서 협업할 수 있도록 하기 위해 필요합니다.
- ssm – 보안 주체가 OpsItems를 생성하고 관련 항목을 연결할 수 있도록 허용합니다. 이는 인시던트가 시작될 때 상위 OpsItem을 생성하는 데 필요합니다.
- ssm-contacts – 보안 주체가 참여를 시작할 수 있도록 허용합니다. 이는 Incident Manager가 인시던트 발생 시 연락처를 참여시키는 데 필요합니다.

- `cloudwatch` – 보안 주체가 CloudWatch 지표를 게시할 수 있도록 허용합니다. 이는 Incident Manager가 인시던트 및 사용량 지표와 관련된 지표를 게시하는 데 필요합니다.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "UpdateIncidentRecordPermissions",
            "Effect": "Allow",
            "Action": [
                "ssm-incidents:ListIncidentRecords",
                "ssm-incidents:CreateTimelineEvent"
            ],
            "Resource": "*"
        },
        {
            "Sid": "RelatedOpsItemPermissions",
            "Effect": "Allow",
            "Action": [
                "ssm:CreateOpsItem",
                "ssm:AssociateOpsItemRelatedItem"
            ],
            "Resource": "*"
        },
        {
            "Sid": "IncidentEngagementPermissions",
            "Effect": "Allow",
            "Action": "ssm-contacts:StartEngagement",
            "Resource": "*"
        },
        {
            "Sid": "PutCloudWatchMetricPermission",
            "Effect": "Allow",
            "Action": [
                "cloudwatch:PutMetricData"
            ],
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "cloudwatch:namespace": [
                         "AWS/IncidentManager",
                         "AWS/Usage"
```

```
                    ]
                }
            }
        }
    ]
}
```

최신 버전의 JSON 정책 문서를 포함하여 정책에 대한 추가 세부 정보를 보려면 AWS 관리형 정책 참조 안내서의 AWSIncidentManagerServiceRolePolicy를 참조하세요.

AWS 관리형 정책: **AWSIncidentManagerResolverAccess**

AWSIncidentManagerResolverAccess를 IAM 엔티티에 연결하여 인시던트를 시작하고, 보고, 업데이트하도록 허용할 수 있습니다. 또한 이를 사용하여 인시던트 대시보드에서 고객 타임라인 이벤트 및 관련 항목을 만들 수 있습니다. 또한이 정책을 채팅 애플리케이션 서비스 역할의 Amazon Q Developer에 연결하거나 인시던트 협업에 사용되는 채팅 채널과 연결된 고객 관리형 역할에 직접 연결할 수 있습니다. 채팅 애플리케이션의 Amazon Q Developer에서 IAM 정책에 대해 자세히 알아보려면 채팅 애플리케이션의 Amazon Q Developer 관리자 안내서의 채팅 애플리케이션에서 Amazon Q Developer를 사용하여 명령을 실행하는 권한 관리를 참조하세요.

권한 세부 정보

이 정책에는 다음 권한이 포함되어 있습니다.

- ssm-incidents— 인시던트 시작, 대응 계획 나열, 인시던트 나열, 인시던트 업데이트, 타임라인 이벤트 나열, 사용자 지정 타임라인 이벤트 생성, 사용자 지정 타임라인 이벤트 업데이트, 사용자 지정 타임라인 이벤트 삭제, 관련 항목 나열, 관련 항목 생성, 관련 항목 업데이트 등을 수행할 수 있습니다.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "StartIncidentPermissions",
            "Effect": "Allow",
            "Action": [
                "ssm-incidents:StartIncident"
```

```
            ],
            "Resource": "*"
        },
        {
            "Sid": "ResponsePlanReadOnlyPermissions",
            "Effect": "Allow",
            "Action": [
                "ssm-incidents:ListResponsePlans",
                "ssm-incidents:GetResponsePlan"
            ],
            "Resource": "*"
        },
        {
            "Sid": "IncidentRecordResolverPermissions",
            "Effect": "Allow",
            "Action": [
                "ssm-incidents:ListIncidentRecords",
                "ssm-incidents:GetIncidentRecord",
                "ssm-incidents:UpdateIncidentRecord",
                "ssm-incidents:ListTimelineEvents",
                "ssm-incidents:CreateTimelineEvent",
                "ssm-incidents:GetTimelineEvent",
                "ssm-incidents:UpdateTimelineEvent",
                "ssm-incidents:DeleteTimelineEvent",
                "ssm-incidents:ListRelatedItems",
                "ssm-incidents:UpdateRelatedItems"
            ],
            "Resource": "*"
        }
    ]
}
```

최신 버전의 JSON 정책 문서를 포함하여 정책에 대한 추가 세부 정보를 보려면 AWS 관리형 정책 참조 안내서의 AWSIncidentManagerResolverAccess를 참조하세요.

AWS 관리형 정책에 대한 Incident Manager 업데이트

이 서비스가 이러한 변경 사항을 추적하기 시작한 이후부터 Incident Manager의 AWS 관리형 정책 업데이트에 대한 세부 정보를 봅니다. 이 페이지의 변경 사항에 대한 자동 알림을 받아보려면 Incident Manager 문서 기록 페이지에서 RSS 피드를 구독하세요.

변경 사항	설명	날짜
AWSIncidentManagerServiceRolePolicy - 정책 업데이트	Incident Manager는 Incident Manager가 AWS/Usage 네임스페이스 내의 지표를 계정에 게시할 수 있는 새 권한을 추가했습니다.	2025년 1월 27일
AWSIncidentManagerIncidentAccessServiceRolePolicy - 정책 업데이트	Incident Manager는 조사 결과 기능을 AWSIncidentManagerIncidentAccessServiceRolePolicy 지원하기 위해 EC2 인스턴스가 Auto Scaling 그룹의 일부인지 확인할 수 있는 새 권한을에 추가했습니다.	2024년 2월 20일
AWSIncidentManagerIncidentAccessServiceRolePolicy - 새 정책	Incident Manager는 인시던트 관리의 일환으로 다른를 호출할 수 있는 권한을 Incident Manager AWS 서비스 에 부여하는 새 정책을 추가했습니다.	2023년 11월 17일
AWSIncidentManagerServiceRolePolicy - 정책 업데이트	Incident Manager는 Incident Manager가 계정에 지표를 게시할 수 있는 새 권한을 추가했습니다.	2022년 12월 16일
AWSIncidentManagerResolverAccess - 새 정책	Incident Manager는 인시던트 시작, 대응 계획 나열, 인시던트 나열, 인시던트 업데이트, 타임라인 이벤트 나열, 사용자 지정 타임라인 이벤트 생성, 사용자 지정 타임라인 이벤트 업데이트, 사용자 지정 타임라인 이벤트 삭제, 관련 항목 나열, 관련 항목 생성, 관련 항목 업데이트	2021년 4월 26일

변경 사항	설명	날짜
	등을 허용하는 새 정책을 추가했습니다.	
AWSIncidentManagerServiceRolePolicy - 새 정책	Incident Manager는 Incident Manager에게 인시던트를 나열하고, 타임라인 이벤트를 생성하고, OpSiteM을 생성하고, 관련 항목을 OpSiteMS에 연결하고, 인시던트와 관련된 참여를 시작할 수 있는 권한을 부여하는 새 정책을 추가했습니다.	2021년 4월 26일
Incident Manager가 변경 사항 추적을 시작함	Incident Manager가 AWS 관리형 정책에 대한 변경 사항 추적을 시작했습니다.	2021년 4월 26일

AWS Systems Manager Incident Manager 자격 증명 및 액세스 문제 해결

다음 정보를 사용하여 Incident Manager 및 IAM에서 발생할 수 있는 공통적인 문제를 진단하고 수정할 수 있습니다.

주제

- Incident Manager에서 작업을 수행할 권한이 없음
- iam:PassRole을 수행하도록 인증되지 않음
- 내 Amazon Web Services 계정 외부의 사람이 내 Incident Manager 리소스에 액세스하도록 허용하려고 함

Incident Manager에서 작업을 수행할 권한이 없음

작업을 수행할 권한이 없다는 오류가 수신되면, 작업을 수행할 수 있도록 정책을 업데이트해야 합니다.

다음의 예제 오류는 `mateojackson` IAM 사용자가 콘솔을 사용하여 가상 *`my-example-widget`* 리소스에 대한 세부 정보를 보려고 하지만 가상 `ssm-incidents:`*`GetWidget`* 권한이 없을 때 발생합니다.

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform: ssm-incidents:GetWidget on resource: my-example-widget
```

이 경우, `ssm-incidents:GetWidget` 작업을 사용하여 *my-example-widget* 리소스에 액세스할 수 있도록 `mateojackson` 사용자 정책을 업데이트해야 합니다.

도움이 필요한 경우 AWS 관리자에게 문의하세요. 관리자는 로그인 자격 증명을 제공한 사람입니다.

iam:PassRole을 수행하도록 인증되지 않음

`iam:PassRole` 작업을 수행할 수 있는 권한이 없다는 오류가 수신되면 Incident Manager에 역할을 전달할 수 있도록 정책을 업데이트해야 합니다.

일부 AWS 서비스 에서는 새 서비스 역할 또는 서비스 연결 역할을 생성하는 대신 기존 역할을 해당 서비스에 전달할 수 있습니다. 이렇게 하려면 사용자가 서비스에 역할을 전달할 수 있는 권한을 가지고 있어야 합니다.

다음 예제 오류는 `marymajor`라는 IAM 사용자가 콘솔을 사용하여 Incident Manager에서 작업을 수행하려고 하는 경우에 발생합니다. 하지만 작업을 수행하려면 서비스 역할이 부여한 권한이 서비스에 있어야 합니다. Mary는 서비스에 역할을 전달할 수 있는 권한을 가지고 있지 않습니다.

```
User: arn:aws:iam::123456789012:user/marymajor is not authorized to perform:
 iam:PassRole
```

이 경우, Mary가 `iam:PassRole` 작업을 수행할 수 있도록 Mary의 정책을 업데이트해야 합니다.

도움이 필요한 경우 AWS 관리자에게 문의하세요. 관리자는 로그인 자격 증명을 제공한 사람입니다.

내 Amazon Web Services 계정 외부의 사람이 내 Incident Manager 리소스에 액세스하도록 허용하려고 함

다른 계정의 사용자 또는 조직 외부의 사람이 리소스에 액세스할 때 사용할 수 있는 역할을 생성할 수 있습니다. 역할을 수임할 신뢰할 수 있는 사람을 지정할 수 있습니다. 리소스 기반 정책 또는 액세스 제어 목록(ACL)을 지원하는 서비스의 경우, 이러한 정책을 사용하여 다른 사람에게 리소스에 대한 액세스 권한을 부여할 수 있습니다.

자세히 알아보려면 다음을 참조하세요.

- Incident Manager에서 이러한 기능을 지원하는지 여부를 알아보려면 AWS Systems Manager Incident Manager 에서 IAM을 사용하는 방법 섹션을 참조하세요.

- 소유 AWS 계정 한의 리소스에 대한 액세스 권한을 제공하는 방법을 알아보려면 IAM 사용 설명서의 소유한 다른의 IAM 사용자에게 액세스 권한 제공을 참조 AWS 계정 하세요.
- 타사에 리소스에 대한 액세스 권한을 제공하는 방법을 알아보려면 IAM 사용 설명서의 타사가 AWS 계정 소유한에 대한 액세스 권한 제공을 AWS 계정참조하세요.
- ID 페더레이션을 통해 액세스 권한을 제공하는 방법을 알아보려면 IAM 사용 설명서의 외부에서 인증된 사용자에게 액세스 권한 제공(ID 페더레이션)을 참조하세요.
- 크로스 계정 액세스에 대한 역할과 리소스 기반 정책 사용의 차이점을 알아보려면 IAM 사용 설명서의 IAM의 크로스 계정 리소스 액세스를 참조하세요.

Incident Manager에서 공유 연락처 및 대응 계획 사용

연락처 공유를 사용하면 연락처 소유자로서 연락처 정보, 에스컬레이션 계획 및 참여를 다른 AWS 계정 또는 조직 내에서 공유할 수 있습니다 AWS .

대응 계획 공유를 사용하면 대응 계획 소유자는 대응 계획 및 관련 인시던트를 다른 AWS 계정 또는 AWS 조직 내에서 공유할 수 있습니다.

연락처 또는 대응 계획 소유자는 연락처 및 대응 계획을 다음과 공유할 수 있습니다.

- 에서 조직 AWS 계정 내부 또는 외부에 특정 AWS Organizations
- 의 조직 내 조직 단위 AWS Organizations
- 의 전체 조직 AWS Organizations

내용

연락처 및 대응 계획을 공유하기 위한 사전 요구 사항

연락처 또는 대응 계획을 AWS Organizations의 조직 또는 조직 단위와 공유하려면

- 에서 리소스를 소유해야 합니다 AWS 계정. 자신과 공유된 리소스 또는 대응 계획을 공유할 수 없습니다.
- 와의 공유를 활성화해야 합니다 AWS Organizations. 자세한 내용은 AWS RAM 사용 설명서의 AWS Organizations를 사용하여 공유 사용을 참조하세요.

관련 서비스

고객 응대 및 대응 계획 공유는 AWS Resource Access Manager ()와 통합됩니다AWS RAM. 를 사용하면 AWS 계정 또는를 통해 AWS 리소스를 공유할 AWS RAM수 있습니다 AWS Organizations. 리소스 공유를 생성하여 소유한 리소스를 공유할 수 있습니다. 리소스 공유는 공유할 리소스와 공유 대상 소비자를 지정합니다. 소비자는의 개인, AWS 계정조직 단위 또는 전체 조직일 수 있습니다 AWS Organizations.

에 대한 자세한 내용은 AWS RAM 사용 설명서를 AWS RAM참조하세요.

연락처 또는 대응 계획 공유

대응 계획을 공유하면 소비자는 해당 대응 계획을 사용하여 생성된 과거, 현재 및 미래의 모든 인시던트에 액세스할 수 있습니다.

연락처를 공유하면 소비자는 연락처 정보, 참여 계획, 에스컬레이션 계획, 인시던트 중에 발생하는 참여 등에 액세스할 수 있습니다. 또한 소비자는 인시던트 발생 시 연락처 또는 에스컬레이션 계획을 참여시킬 수 있습니다.

의 조직에 속 AWS Organizations 해 있고 조직 내 공유가 활성화된 경우 조직의 소비자에게 공유 연락처 또는 대응 계획에 대한 액세스 권한이 자동으로 부여됩니다. 그렇지 않으면 소비자는 리소스 공유에 가입하라는 초대장을 받고 초대를 수락한 후 공유된 연락처 또는 대응 계획의 액세스 권한을 받습니다.

AWS RAM 콘솔 또는를 사용하여 소유한 연락처 또는 대응 계획을 공유할 수 있습니다 AWS CLI.

> **Note**
>
> 현재 다른 계정에서 공유된 연락처를 대응 계획에 추가하는 기능은 지원되지 않습니다.

AWS RAM 콘솔을 사용하여 소유한 연락처 또는 대응 계획을 공유하려면

AWS RAM 사용 설명서의 리소스 공유 생성을 참조하세요.

를 사용하여 소유하고 있는 연락처 또는 대응 계획을 공유하려면 AWS CLI

create-resource-share 명령을 사용합니다.

고유한 연락처 또는 대응 계획 공유 중지

리소스 소유자가 소비자와의 연락처 또는 대응 계획 공유를 중단하면 연락처, 대응 계획, 에스컬레이션 계획, 참여 및 인시던트가 더 이상 소비자 콘솔에 표시되지 않습니다.

> **Note**
>
> 소비자가 콘솔에서 연락처, 대응 계획, 에스컬레이션 계획, 참여 또는 사건을 볼 수 있는 경우 페이지를 새로 고치거나 페이지를 벗어나기 전까지는 업데이트 없이도 계속 볼 수 있습니다.

소유하고 있는 공유 연락처 또는 대응 계획의 공유를 중지하려면 리소스 공유에서 제거해야 합니다. AWS RAM 콘솔 또는를 사용하여이 작업을 수행할 수 있습니다 AWS CLI.

AWS RAM 콘솔을 사용하여 자신이 소유한 연락처 또는 대응 계획의 공유를 중지하려면

AWS RAM 사용 설명서에서 리소스 공유 업데이트를 참조하세요.

AWS CLI를 사용하여 자신이 소유한 연락처 또는 대응 계획의 공유를 중지하려면

disassociate-resource-share 명령을 사용합니다.

공유 연락처 또는 대응 계획 식별

소유자와 소비자는 Incident Manager 콘솔 및 AWS CLI를 사용하여 공유 연락처 및 대응 계획을 식별할 수 있습니다.

Incident Manager 콘솔을 사용하여 공유 연락처 또는 대응 계획을 식별하려면

> **Note**
>
> 연락처, 대응 계획, 에스컬레이션 계획, 참여, 인시던트는 일반적으로 Incident Manager 콘솔에서 공유 리소스로 식별할 수 없습니다. Amazon 리소스 이름(ARN) 이 표시되는 곳에서는 ARN에 소유자의 계정 ID가 포함됩니다.

를 사용하여 공유 연락처 또는 대응 계획을 식별하려면 AWS CLI

ListResponsePlans 또는 ListContacts 명령을 사용합니다. 이 명령은 소유한 연락처 및 대응 계획과 공유된 연락처 및 대응 계획을 반환합니다. ARN에는 연락처 또는 대응 계획 소유자의 AWS 계정 ID가 표시됩니다.

공유 연락처 및 대응 계획 권한

소유자에 대한 권한

소유자는 연락처 및 대응 계획을 업데이트하고, 보고, 공유하고, 공유를 중단하고, 사용할 수 있습니다. 연락처 및 대응 계획에는 관련 참여 및 인시던트가 포함됩니다.

소비자에 대한 권한

소비자는 대응 계획과 연락처만 사용하고 볼 수 있습니다. 연락처 및 대응 계획에는 관련 참여 및 인시던트가 포함됩니다.

결제 및 측정

리소스 소유자에게 리소스 요금이 청구됩니다. 소비자에게 공유된 리소스에 대한 요금은 청구되지 않습니다. 리소스 공유와 관련된 추가 비용은 없습니다.

인스턴스 제한

리소스를 공유해도 소유자 또는 소비자 계정의 리소스 한도에는 영향을 미치지 않습니다. 소유자 계정만 리소스 한도를 계산하는 데 사용됩니다.

에 대한 규정 준수 검증 AWS Systems Manager Incident Manager

타사 감사자는 여러 규정 준수 프로그램의 AWS Systems Manager Incident Manager 일환으로의 보안 및 AWS 규정 준수를 평가합니다. 여기에는 SOC, PCI, FedRAMP, HIPAA 등이 포함됩니다.

AWS 서비스 가 특정 규정 준수 프로그램의 범위 내에 있는지 알아보려면 AWS 서비스 규정 준수 프로그램 제공 범위 섹션을 참조하고 관심 있는 규정 준수 프로그램을 선택합니다. 일반 정보는 AWS 규정 준수 프로그램.

를 사용하여 타사 감사 보고서를 다운로드할 수 있습니다 AWS Artifact. 자세한 내용은 Downloading Reports inDownloading AWS Artifact을 참조하세요.

사용 시 규정 준수 책임은 데이터의 민감도, 회사의 규정 준수 목표 및 관련 법률과 규정에 따라 AWS 서비스 결정됩니다.는 규정 준수를 지원하기 위해 다음 리소스를 AWS 제공합니다.

- 보안 규정 준수 및 거버넌스 - 이러한 솔루션 구현 가이드에서는 아키텍처 고려 사항을 설명하고 보안 및 규정 준수 기능을 배포하는 단계를 제공합니다.
- HIPAA 적격 서비스 참조 - HIPAA 적격 서비스가 나열되어 있습니다. 모두 HIPAA 자격이 AWS 서비스 있는 것은 아닙니다.
- AWS 규정 준수 리소스 -이 워크북 및 가이드 모음은 산업 및 위치에 적용될 수 있습니다.
- AWS 고객 규정 준수 가이드 - 규정 준수의 관점에서 공동 책임 모델을 이해합니다. 이 가이드에는 여러 프레임워크(미국 국립표준기술연구소(NIST), 결제 카드 산업 보안 표준 위원회(PCI), 국제표준화기구(ISO) 포함)의 보안 제어에 대한 지침을 보호하고 AWS 서비스 매핑하는 모범 사례가 요약되어 있습니다.
- AWS Config 개발자 안내서의 규칙을 사용하여 리소스 평가 -이 AWS Config 서비스는 리소스 구성이 내부 관행, 업계 지침 및 규정을 얼마나 잘 준수하는지 평가합니다.
- AWS Security Hub - 내 보안 상태에 대한 포괄적인 보기를 AWS 서비스 제공합니다 AWS. Security Hub는 보안 컨트롤을 사용하여 AWS 리소스를 평가하고 보안 업계 표준 및 모범 사례에 대한 규정 준수를 확인합니다. 지원되는 서비스 및 제어 목록은 Security Hub 제어 참조를 참조하세요.
- Amazon GuardDuty - 의심스러운 활동과 악의적인 활동이 있는지 환경을 모니터링하여 사용자, AWS 계정워크로드, 컨테이너 및 데이터에 대한 잠재적 위협을 AWS 서비스 탐지합니다. GuardDuty는 특정 규정 준수 프레임워크에서 요구하는 침입 탐지 요구 사항을 충족하여 PCI DSS와 같은 다양한 규정 준수 요구 사항을 따르는 데 도움을 줄 수 있습니다.
- AWS Audit Manager - 이를 AWS 서비스 통해 AWS 사용량을 지속적으로 감사하여 위험과 규정 및 업계 표준 준수를 관리하는 방법을 간소화할 수 있습니다.

의 복원력 AWS Systems Manager Incident Manager

AWS 글로벌 인프라는 AWS 리전 및 가용 영역을 중심으로 구축됩니다. AWS 리전은 물리적으로 분리되고 격리된 여러 가용 영역을 제공하며,이 가용 영역은 지연 시간이 짧고 처리량이 높으며 중복성이 높은 네트워킹과 연결됩니다. 가용 영역을 사용하면 중단 없이 영역 간에 자동으로 장애 극복 조치가 이루어지는 애플리케이션 및 데이터베이스를 설계하고 운영할 수 있습니다. 가용 영역은 기존의 단일 또는 다중 데이터 센터 인프라보다 가용성, 내결함성, 확장성이 뛰어납니다.

AWS 리전 및 가용 영역에 대한 자세한 내용은 AWS 글로벌 인프라를 참조하세요.

Incident Manager는 글로벌 지역 서비스이며 현재 가용 영역을 지원하지 않습니다.

AWS 글로벌 인프라 외에도 Incident Manager는 데이터 복원력 및 백업 요구 사항을 지원하는 데 도움이 되는 여러 기능을 제공합니다. 준비하기 마법사를 실행하는 동안 복제 세트를 설정하라는 메시지가 표시됩니다. 이 리전 복제 세트를 사용하면 여러 리전에서 데이터와 리소스에 액세스할 수 있으므로 클라우드 네트워크 전반의 인시던트 관리를 보다 쉽게 수행할 수 있습니다. 또한 이 복제를 통해 리전 중 하나에 장애가 발생하더라도 데이터를 안전하게 보호하고 액세스할 수 있습니다.

Incident Manager 복제 세트 사용에 대한 자세한 내용은 Incident Manager 복제 세트 구성 섹션을 참조하세요.

의 인프라 보안 AWS Systems Manager Incident Manager

관리형 서비스인는 AWS 글로벌 네트워크 보안으로 보호 AWS Systems Manager Incident Manager 됩니다. AWS 보안 서비스 및가 인프라를 AWS 보호하는 방법에 대한 자세한 내용은 AWS 클라우드 보안을 참조하세요. 인프라 보안 모범 사례를 사용하여 AWS 환경을 설계하려면 보안 원칙 AWS Well-Architected Framework의 인프라 보호를 참조하세요.

AWS 에서 게시한 API 호출을 사용하여 네트워크를 통해 Incident Manager에 액세스합니다. 고객은 다음을 지원해야 합니다.

- Transport Layer Security(TLS) TLS 1.2는 필수이며 TLS 1.3을 권장합니다.
- DHE(Ephemeral Diffie-Hellman) 또는 ECDHE(Elliptic Curve Ephemeral Diffie-Hellman)와 같은 완전 전송 보안(PFS)이 포함된 암호 제품군 Java 7 이상의 최신 시스템은 대부분 이러한 모드를 지원합니다.

또한 요청은 액세스 키 ID 및 IAM 위탁자와 관련된 보안 암호 액세스 키를 사용하여 서명해야 합니다. 또는 AWS Security Token Service(AWS STS)를 사용하여 임시 자격 증명을 생성하여 요청에 서명할 수 있습니다.

AWS Systems Manager Incident Manager 및 인터페이스 VPC 엔드포인트 작업(AWS PrivateLink)

인터페이스 VPC 엔드포인트를 생성 AWS Systems Manager Incident Manager 하여 VPC와 간에 프라이빗 연결을 설정할 수 있습니다. 인터페이스 엔드포인트는 로 구동됩니다 AWS PrivateLink를 사용하면 인터넷 게이트웨이 AWS PrivateLink, NAT 디바이스, VPN 연결 또는 AWS Direct Connect 연결 없이 Incident Manager API 작업에 비공개로 액세스할 수 있습니다. VPC의 인스턴스는 Incident Manager API 작업과 통신하는 데 퍼블릭 IP 주소를 필요로 하지 않습니다. VPC와 Incident Manager 간의 트래픽은 Amazon 네트워크 내에서 유지됩니다.

각 인터페이스 엔드포인트는 서브넷에서 하나 이상의 탄력적 네트워크 인터페이스로 표현됩니다.

자세한 내용은 Amazon VPC 사용 설명서의 인터페이스 VPC 엔드포인트(AWS PrivateLink)를 참조하세요.

Incident Manager VPC 엔드포인트에 대한 고려 사항

Incident Manager에 대한 인터페이스 VPC 엔드포인트를 설정하기 전에 Amazon VPC 사용 설명서에서 인터페이스 엔드포인트 속성 및 제한 사항과 AWS PrivateLink 할당량을 검토해야 합니다.

Incident Manager는 VPC에서 모든 API 작업에 대한 직접 호출 수행을 지원합니다. Incident Manager를 모두 사용하려면 두 개의 VPC 엔드포인트를 생성해야 합니다. 하나는 `ssm-incidents`용, 다른 하나는 `ssm-contacts`용입니다.

Incident Manager에 대한 인터페이스 VPC 엔드포인트 생성

Amazon VPC 콘솔이나 AWS Command Line Interface (AWS CLI)를 사용하여 Incident Manager에 대한 VPC 엔드포인트를 생성할 수 있습니다. 자세한 내용은 Amazon VPC 사용 설명서의 인터페이스 엔드포인트 생성을 참조하세요.

에서 Incident Manager에 대해 지원되는 서비스 이름을 사용하여 Incident Manager용 VPC 엔드포인트를 생성합니다 AWS 리전. 다음 예제에서는 IPv4 및 듀얼 스택 엔드포인트의 인터페이스 엔드포인트 형식을 보여줍니다.

IPv4 엔드포인트 형식

- `com.amazonaws.region.ssm-incidents`
- `com.amazonaws.region.ssm-contacts`

듀얼 스택(IPv4 및 IPv6) 엔드포인트 형식

- `aws.api.region.ssm-incidents`
- `aws.api.region.ssm-contacts`

모든 리전에서 지원되는 엔드포인트 목록은 AWS 일반 참조 안내서의 AWS Systems Manager Incident Manager 엔드포인트 및 할당량을 참조하세요.

인터페이스 엔드포인트에 대해 프라이빗 DNS를 활성화하면 형식의 기본 리전 DNS 이름을 사용하여 Incident Manager에 API 요청을 할 수 있습니다. 다음 예제에서는 기본 리전 DNS 이름 형식을 보여줍니다.

- ssm-incidents.*region*.amazonaws.com
- ssm-contacts.*region*.amazonaws.com

자세한 내용은 Amazon VPC 사용 설명서의 인터페이스 엔드포인트를 통해 서비스 액세스를 참조하세요.

Incident Manager에 대한 VPC 엔드포인트 정책 생성

Incident Manager에 대한 액세스를 제어하는 VPC 엔드포인트에 엔드포인트 정책을 연결할 수 있습니다. 이 정책은 다음 정보를 지정합니다.

- 작업을 수행할 수 있는 위탁자.
- 수행할 수 있는 작업.
- 이러한 작업을 수행할 수 있는 리소스입니다.

자세한 정보는 Amazon VPC 사용 설명서의 VPC 엔드포인트를 통해 서비스에 대한 액세스 제어를 참조하세요.

예제: Incident Manager 작업에 대한 VPC 엔드포인트 정책

다음은 Incident Manager에 대한 엔드포인트 정책의 예입니다. 이 정책은 엔드포인트에 연결될 때 모든 리소스의 모든 보안 주체에 대해 나열된 Incident Manager 조치에 액세스할 수 있는 권한을 부여합니다.

```
{
   "Statement":[
      {
         "Principal":"*",
         "Effect":"Allow",
         "Action":[
            "ssm-contacts:ListContacts",
            "ssm-incidents:ListResponsePlans",
            "ssm-incidents:StartIncident"
         ],
         "Resource":"*"
      }
   ]
}
```

Incident Manager의 구성 및 취약성 분석

구성 및 IT 제어는 AWS 와 고객 간의 공동 책임입니다. 자세한 내용은 AWS 공동 책임 모델을 참조하세요.

의 보안 모범 사례 AWS Systems Manager Incident Manager

AWS Systems Manager Incident Manager 는 자체 보안 정책을 개발하고 구현할 때 고려해야 할 여러 보안 기능을 제공합니다. 다음 모범 사례는 일반적인 지침이며 완벽한 보안 솔루션을 나타내지는 않습니다. 이러한 모범 사례는 환경에 적절하지 않거나 충분하지 않을 수 있으므로 참고용으로만 사용하세요.

주제

- Incident Manager 예방 보안 모범 사례
- Incident Manager 예방 보안 모범 사례

Incident Manager 예방 보안 모범 사례

최소 권한 액세스 구현

권한을 부여할 때 누가 어떤 Incident Manager 리소스에 대해 어떤 권한을 갖는지 결정합니다. 해당 리소스에서 허용할 작업을 사용 설정합니다. 따라서 작업을 수행하는 데 필요한 권한만 부여해야 합니다. 최소 권한 액세스를 구현하는 것이 오류 또는 악의적인 의도로 인해 발생할 수 있는 보안 위험과 영향을 최소화할 수 있는 근본적인 방법입니다.

다음과 같은 도구를 사용하여 최소 권한 액세스를 구현할 수 있습니다.

- IAM 엔터티에 대한 정책 및 권한 경계를 사용하여 AWS 리소스에 대한 액세스 제어 https://docs.aws.amazon.com/IAM/latest/UserGuide/access_policies_boundaries.html
- 서비스 제어 정책

연락처 생성 및 관리

연락처를 활성화하면 Incident Manager가 디바이스에 연락하여 활성화를 확인합니다. 디바이스를 활성화하기 전에 디바이스 정보가 정확한지 확인하십시오. 이렇게 하면 활성화 중에 Incident Manager가 잘못된 디바이스나 사람에게 연락할 가능성이 줄어듭니다.

연락처와 에스컬레이션 계획을 정기적으로 검토하여 인시던트 발생 시 연락이 필요한 연락처만 연락을 취하도록 하십시오. 연락처를 정기적으로 검토하여 오래되었거나 잘못된 정보를 제거하세요. 인시던트 발생 시 담당자에게 더 이상 알리지 말아야 할 경우 관련 에스컬레이션 계획에서 삭제하거나 Incident Manager에서 삭제하세요.

채팅 채널을 비공개로 설정

인시던트 채팅 채널을 비공개로 설정하여 최소 권한 액세스를 구현할 수 있습니다. 각 대응 계획 템플릿에 대해 범위를 좁힌 사용자 목록을 포함하는 다른 채팅 채널을 사용하는 것을 고려해 보세요. 이렇게 하면 민감한 정보가 포함될 수 있는 채팅 채널에 올바른 대응 담당자만 참여하도록 할 수 있습니다.

Slack 채팅 애플리케이션의 Amazon Q Developer에서 생성된 채널은 채팅 애플리케이션에서 Amazon Q Developer를 구성하는 데 사용되는 IAM 역할의 권한을 상속합니다. 이를 통해 채팅 애플리케이션의 Amazon Q Developer에서 대응 담당자가 Slack 채널을 활성화하여 Incident Manager APIs 및 지표 그래프 검색과 같은 허용 목록에 있는 작업을 호출할 수 있습니다.

AWS 도구를 최신 상태로 유지

AWS 는 AWS 작업에 사용할 수 있는 업데이트된 버전의 도구 및 플러그인을 정기적으로 릴리스합니다. 이러한 리소스를 최신 상태로 유지하면 해당 계정의 사용자와 인스턴스가 이러한 도구의 최신 기능과 보안 기능에 액세스할 수 있습니다.

- AWS CLI – AWS Command Line Interface (AWS CLI)는 명령줄 셸의 명령을 사용하여 AWS 서비스와 상호 작용할 수 있는 오픈 소스 도구입니다. AWS CLI를 업데이트하려면 AWS CLI를 설치하는 데 사용한 것과 동일한 명령을 실행합니다. 로컬 컴퓨터에서 예약된 작업을 생성하여 운영 체제에 적합한 명령을 최소한 2주에 한 번씩 실행하는 것이 좋습니다. 설치 명령에 대한 자세한 내용은 AWS 명령줄 인터페이스 사용 설명서의 명령줄 인터페이스 설치를 참조하세요. AWS
- AWS Tools for Windows PowerShell – Tools for Windows PowerShell은 .NET용 AWS SDK에서 제공하는 기능을 기반으로 구축된 PowerShell 모듈 세트입니다. Tools for Windows PowerShell을 사용하면 PowerShell 명령줄에서 AWS 리소스에 대한 작업을 스크립팅할 수 있습니다. 정기적으로 Tools for Windows PowerShell의 업데이트된 버전이 릴리스될 때 로컬로 실행 중인 버전을 업데이트해야 합니다. 자세한 내용은 Windows AWS Tools for Windows PowerShell 에서 업데이트 또는 Linux 또는 macOS AWS Tools for Windows PowerShell 에서 업데이트를 참조하세요.

관련 콘텐츠

Systems Manager 보안 모범 사례

Incident Manager 예방 보안 모범 사례

모든 Incident Manager 리소스 식별 및 감사

IT 자산 식별은 거버넌스와 보안의 중요한 측면입니다. Systems Manager 리소스를 식별하여 보안 상태를 평가하고 잠재적 취약 영역에 대해 조치를 취해야 합니다. Incident Manager 리소스의 리소스 그룹을 만드십시오. Resource Groups에 대한 자세한 내용은 AWS Resource Groups 사용 설명서의 Resource Groups란 무엇인가요?를 참조하십시오.

사용 AWS CloudTrail

AWS CloudTrail 는 Incident Manager에서 사용자, 역할 또는 AWS 서비스가 수행한 작업의 레코드를 제공합니다. 에서 수집한 정보를 사용하여 Incident Manager에 수행된 요청 AWS CloudTrail, 요청이 수행된 IP 주소, 요청을 수행한 사람, 요청이 수행된 시간 및 추가 세부 정보를 확인할 수 있습니다. 자세한 내용은 를 사용하여 AWS Systems Manager Incident Manager API 호출 로깅 AWS CloudTrail 단원을 참조하십시오.

AWS 보안 권고 모니터링

Trusted Advisor 에 게시된 보안 권고 사항을 정기적으로 확인합니다 AWS 계정. 이는 describe-trusted-advisor-checks를 사용하여 프로그래밍 방식으로 수행하면 됩니다.

또한 각에 등록된 기본 이메일 주소를 적극적으로 모니터링합니다 AWS 계정. AWS 는이 이메일 주소를 사용하여 사용자에게 영향을 미칠 수 있는 새로운 보안 문제에 대해 연락을 드릴 것입니다.

AWS 광범위한 영향을 미치는 운영 문제는 AWS 서비스 상태 대시보드에 게시됩니다. AWS Health Dashboard를 통해 개별 계정에도 운영 문제가 게시됩니다. 자세한 내용은 AWS Health 설명서를 참조하십시오.

관련 콘텐츠

Amazon Web Services: 보안 프로세스의 개요(백서)

시작하기: 리소스를 구성할 AWS 때 보안 모범 사례 준수(AWS 보안 블로그)

IAM 모범 사례

의 보안 모범 사례 AWS CloudTrail

Incident Manager에서 모니터링

AWS Systems Manager Incident Manager는 모니터링 및 로깅 기능을 제공하는 다음 서비스와 통합됩니다.

CloudWatch 지표

CloudWatch 지표를 사용하면 AWS Systems Manager Incident Manager 작업의 데이터 요소에 대한 통계를 지표라고 하는 정렬된 시계열 데이터 세트로 검색할 수 있습니다. 이러한 지표를 사용하여 시스템이 예상대로 수행되고 있는지 확인할 수 있습니다. 자세한 내용은 Amazon CloudWatch를 사용하여 Incident Manager에서 지표 모니터링 단원을 참조하십시오.

CloudTrail 로그

AWS CloudTrail 를 사용하여 API 호출 AWS 에 대한 자세한 정보를 캡처합니다. APIs Amazon Simple Storage Service에 이러한 호출을 로그 파일로 저장할 수 있습니다. 이러한 CloudTrail 로그를 사용하면 어떤 호출이 이루어졌는지, 호출한 소스 IP 주소, 호출한 사람, 호출한 시기 등의 정보를 확인할 수 있습니다. CloudTrail 로그에는 Incident Manager의 API 작업 호출에 대한 정보가 포함됩니다. 자세한 내용은 를 사용하여 AWS Systems Manager Incident Manager API 호출 로깅 AWS CloudTrail 섹션을 참조하세요.

Trusted Advisor

AWS Trusted Advisor 는 AWS 리소스를 모니터링하여 성능, 안정성, 보안 및 비용 효율성을 개선하는 데 도움이 됩니다. 모든 사용자는 4개의 Trusted Advisor 검사를 사용할 수 있습니다. 비즈니스 또는 엔터프라이즈 지원 플랜을 보유한 사용자는 50개 이상의 검사를 사용할 수 있습니다. Incident Manager의 경우 복제 세트의 구성이 둘 이상의를 사용하여 리전 장애 조치 및 응답을 지원하는 AWS 리전 지 Trusted Advisor 확인합니다. 자세한 내용은AWS Support 사용 설명서의 AWS Trusted Advisor를 참조하십시오.

Amazon CloudWatch를 사용하여 Incident Manager에서 지표 모니터링

Incident Manager는 Amazon CloudWatch에서 모니터링할 수 있는 집계 지표를 제공합니다. 이러한 지표를 사용하여 인시던트 및 대응 계획 추세를 식별할 수 있습니다.

이러한 지표에는 다음이 포함됩니다.

- 일정 기간 동안 발생한 인시던트 수

- 해당 인시던트에 대응하고 해결하는 데 걸리는 시간
- 해결된 인시던트 수

Incident Manager 지표를 모니터링하여 운영 상태를 더 잘 이해하고 의미 있는 조치를 취하여 인시던트 대응의 운영 효율성을 높일 수 있습니다. Incident Manager 지표는 모든 Incident Manager 리전에서 사용할 수 있습니다. Incident Manager로 온보딩할 때 복제 세트에 지정한 모든 리전의 지표를 Amazon CloudWatch에서 볼 수 있습니다. 해당 인시던트에 대한 조치가 취해진 리전에 게시된 지표를 볼 수 있습니다. 이러한 지표에 대한 추가 요금은 없습니다.

CloudWatch 콘솔에서 이러한 지표를 사용하여 대시보드를 빌드할 수 있습니다.

- 기존 인시던트 부하를 측정하고 검토하십시오.
- 인시던트 부하가 증가하고 있는지, 감소하고 있는지 또는 동일하게 유지되는지 추적하십시오.
- Incident Manager를 더 효과적으로 사용하여 인시던트의 빈도, 기간 및 영향을 줄이십시오.

이 페이지에서는 CloudWatch 콘솔에서 사용할 수 있는 Incident Manager 지표를 설명합니다.

> **Important**
>
> 고객 생성 이벤트의 경우 ASCII가 아닌 문자를 사용하여 `TriggerDetails`의 source 값 이름을 지정한 경우, 비 ASCII 텍스트를 지원하지 않는 Amazon CloudWatch 지표에서 해당 이벤트의 지표가 보고되지 않습니다. `source`는 SDK 또는 AWS CLI를 사용하는 등 프로그래밍 방식으로만 제공될 수 있습니다.

Systems Manager는 다음 지표를 CloudWatch로 전송합니다.

지표	설명
`NumberOfCreateIncidents`	생성된 인시던트 수. 유효한 차원: [](빈 차원), [`ResponsePlan `], [`Impact`], [`Source`], [`ResponsePlan , Impact`], [`ResponsePlan , Source`] 단위: 수

지표	설명
NumberOfResolveIncidents	해결된 인시던트 수. 유효한 차원: [](빈 차원), [ResponsePlan], [Impact], [Source], [ResponsePlan , Impact], [ResponsePlan , Source] 단위: 수
TimeToFirstAcknowledgement	인시던트 생성 시간과 인시던트에 대한 최초 승인 시점 간의 시차. 유효한 차원: [](빈 차원), [ResponsePlan], [Impact], [Source], [ResponsePlan , Impact], [ResponsePlan , Source] 단위: 초
TimeToResolveIncident	인시던트가 생성된 시점과 해결된 시점 사이의 시차. 유효한 차원: [](빈 차원), [ResponsePlan], [Impact], [Source], [ResponsePlan , Impact], [ResponsePlan , Source] 단위: 초

CloudWatch 콘솔에서 Incident Manager 지표 보기

CloudWatch 콘솔에서 Incident Manager 지표를 보려면

1. https://console.aws.amazon.com/cloudwatch/에서 CloudWatch 콘솔을 엽니다.
2. 탐색 창에서 지표를 선택합니다.
3. IncidentManager 네임스페이스를 선택합니다.
4. 지표 탭에서 차원을 선택한 다음 지표를 선택합니다.

CloudWatch 지표 작업에 대한 자세한 내용은 Amazon CloudWatch User Guide의 다음 주제를 참조하세요.

- Metrics
- Amazon CloudWatch 지표 사용

지표 차원

Incident Manager 지표는 `IncidentManager` 네임스페이스를 사용하며 다음 차원에게 지표를 제공합니다.

차원	설명
`By Response Plan`	응답 계획별 집계 지표 보기.
`By Impact Level`	심각도 수준별로 집계된 지표를 볼 수 있습니다.
`By Source`	CloudWatch 경보 또는 EventBridge 이벤트를 통해 수동으로 생성한 인시던트의 지표를 볼 수 있습니다.
`Across All Incidents`	현재 AWS 리전의 모든 인시던트에 대한 집계 지표를 볼 수 있습니다.
`Response Plan name and Source`	대응 계획과 소스의 각 조합에 대한 집계 지표를 볼 수 있습니다.
`Response Plan Name and Impact Level`	대응 계획과 심각도 수준의 각 조합에 대한 집계 지표를 볼 수 있습니다.

를 사용하여 AWS Systems Manager Incident Manager API 호출 로깅 AWS CloudTrail

AWS Systems Manager Incident Manager 는 사용자AWS CloudTrail, 역할 또는가 수행한 작업에 대한 레코드를 제공하는 서비스인와 통합됩니다 AWS 서비스. CloudTrail은 Network Manager에 대한 모든 API 호출을 이벤트로 캡처합니다. 캡처되는 호출에는 Audit Manager 콘솔에서 수행한 호출과 Audit Manager API 작업에 대한 코드 호출이 포함됩니다. CloudTrail에서 수집한 정보를 사용하여 Incident Manager에 수행된 요청, 요청이 수행된 IP 주소, 요청이 수행된 시간 및 추가 세부 정보를 확인할 수 있습니다.

모든 이벤트 또는 로그 항목에는 요청을 생성했던 사용자에 대한 정보가 포함됩니다. 자격 증명을 이용하면 다음을 쉽게 판단할 수 있습니다.

- 요청을 루트 사용자로 했는지 사용자 보안 인증으로 했는지 여부.
- IAM Identity Center 사용자를 대신하여 요청이 이루어졌는지 여부입니다.
- 역할 또는 페더레이션 사용자에 대한 임시 자격 증명을 사용하여 요청이 생성되었는지 여부.
- 다른 AWS 서비스에서 요청했는지 여부.

CloudTrail은 계정을 생성할 AWS 계정 때에서 활성화되며 CloudTrail 이벤트 기록에 자동으로 액세스할 수 있습니다. CloudTrail 이벤트 기록은 지난 90일 간 AWS 리전의 관리 이벤트에 대해 보기, 검색 및 다운로드가 가능하고, 수정이 불가능한 레코드를 제공합니다. 자세한 설명은 AWS CloudTrail 사용 설명서의 CloudTrail 이벤트 기록 작업을 참조하세요. Event history(이벤트 기록) 보기는 CloudTrail 요금이 부과되지 않습니다.

AWS 계정 지난 90일 동안의 이벤트를 지속적으로 기록하려면 추적 또는 CloudTrail Lake 이벤트 데이터 스토어를 생성합니다.

CloudTrail 추적

CloudTrail은 추적을 사용하여 Amazon S3 버킷으로 로그 파일을 전송할 수 있습니다. 를 사용하여 생성된 모든 추적 AWS Management Console 은 다중 리전입니다. AWS CLI를 사용하여 단일 리전 또는 다중 리전 추적을 생성할 수 있습니다. 계정 AWS 리전 의 모든에서 활동을 캡처하므로 다중 리전 추적을 생성하는 것이 좋습니다. 단일 리전 추적을 생성하는 경우 추적의 AWS 리전에 로깅된 이벤트만 볼 수 있습니다. 추적에 대한 자세한 내용은 AWS CloudTrail 사용 설명서의 Creating a trail for your AWS 계정 및 Creating a trail for an organization을 참조하세요.

CloudTrail에서 추적을 생성하여 진행 중인 관리 이벤트의 사본 하나를 Amazon S3 버킷으로 무료로 전송할 수는 있지만, Amazon S3 스토리지 요금이 부과됩니다. CloudTrail 요금에 대한 자세한 내용은 AWS CloudTrail 요금을 참조하세요. Amazon S3 요금에 대한 자세한 내용은 Amazon S3 요금을 참조하세요.

CloudTrail Lake 이벤트 데이터 스토어

CloudTrail Lake를 사용하면 이벤트에 대해 SQL 기반 쿼리를 실행할 수 있습니다. CloudTrail Lake는 행 기반 JSON 형식의 기존 이벤트를 Apache ORC 형식으로 변환합니다. ORC는 빠른 데이터 검색에 최적화된 열 기반 스토리지 형식입니다. 이벤트는 이벤트 데이터 스토어로 집계되며, 이벤트 데이터 스토어는 고급 이벤트 선택기를 적용하여 선택한 기준을 기반으로 하는 변경 불가능한 이벤트 컬렉션입니다. 이벤트 데이터 스토어에 적용하는 선택기는 어떤 이벤트가 지속되고 쿼리할

수 있는지 제어합니다. CloudTrail Lake에 대한 자세한 내용은 AWS CloudTrail 사용 설명서의 AWS CloudTrail Lake 작업을 참조하세요.

CloudTrail Lake 이벤트 데이터 스토어 및 쿼리에는 비용이 발생합니다. 이벤트 데이터 스토어를 생성할 때 이벤트 데이터 스토어에 사용할 요금 옵션을 선택합니다. 요금 옵션에 따라 이벤트 모으기 및 저장 비용과 이벤트 데이터 스토어의 기본 및 최대 보존 기간이 결정됩니다. CloudTrail 요금에 대한 자세한 내용은 AWS CloudTrail 요금을 참조하세요.

CloudTrail의 Incident Manager 관리 이벤트

관리 이벤트는의 리소스에서 수행되는 관리 작업에 대한 정보를 제공합니다 AWS 계정. 이를 컨트롤 플레인 작업이라고도 합니다. 기본적으로 CloudTrail은 관리 이벤트를 로깅합니다.

AWS Systems Manager Incident Manager 는 모든 Incident Manager 컨트롤 플레인 작업을 관리 이벤트로 기록합니다. Incident Manager가 CloudTrail에 로깅하는 AWS Systems Manager Incident Manager 컨트롤 플레인 작업 목록은 AWS Systems Manager Incident Manager API 참조를 참조하세요.

Incident Manager 이벤트 예제

이벤트는 모든 소스로부터의 단일 요청을 나타내며 요청된 API 작업, 작업 날짜와 시간, 요청 파라미터 등에 대한 정보가 들어 있습니다. CloudTrail 로그 파일은 퍼블릭 API 직접 호출의 주문 스택 추적이 아니므로 이벤트가 특정 순서로 표시되지 않습니다.

다음은 `StartIncident` 작업을 설명하는 CloudTrail 로그 항목을 보여 주는 예시입니다.


```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "IAMUser",
        "principalId": "1234567890abcdef0",
        "arn": "arn:aws:iam::246873129580111122223333:user/nikki_wolf",
        "accountId": "abcdef01234567890",
        "accessKeyId": "021345abcdef6789",
        "userName": "nikki_wolf"
    },
    "eventTime": "2024-04-22T23:20:10Z",
    "eventSource": "ssm-incidents.amazonaws.com",
    "eventName": "StartIncident",
    "awsRegion": "us-east-2",
```

```
    "sourceIPAddress": "192.0.2.0",
    "userAgent": "aws-cli/2.0.58 Python/3.7.4 Darwin/19.6.0 exe/x86_64 command/
ssmincidents.start-incident",
    "requestParameters": {
        "responsePlanArn": "arn:aws:ssm-incidents::555555555555:response-plan/security-
test-response-plan-non-dedupe-v1",
        "clientToken": "12345678-1111-2222-3333-abcdefghijkl"
    },
    "responseElements": {
        "incidentRecordArn": "arn:aws:ssm-incidents::444455556666:incident-record/
security-test-response-plan-non-dedupe-v1/abcdefgh-abcd-1234-1234-1234567890"
    },
    "requestID": "abcdefgh-1234-abcd-1234-1234567abcdef",
    "eventID": "12345678-1234-1234-abcd-abcdef1234567",
    "readOnly": false,
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "eventCategory": "Management",
    "recipientAccountId": "12345678901234567"
}
```

다음은 DeleteContactChannel 작업을 설명하는 CloudTrail 로그 항목을 보여 주는 예시입니다.

```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "IAMUser",
        "principalId": "1234567890abcdef0",
        "arn": "arn:aws:iam::246873129580111122223333:user/nikki_wolf",
        "accountId": "abcdef01234567890",
        "accessKeyId": "021345abcdef6789",
        "userName": "nikki_wolf"
    },
    "eventTime": "2024-04-08T02:27:21Z",
    "eventSource": "ssm-contacts.amazonaws.com",
    "eventName": "DeleteContactChannel",
    "awsRegion": "us-east-2",
    "sourceIPAddress": "192.0.2.0",
    "userAgent": "Apache-HttpClient/UNAVAILABLE (Java/1.8.0_282)",
    "requestParameters": {
        "contactChannelId": "arn:aws:ssm-contacts:us-west-2:555555555555:device/
bnuomysohc/abcdefgh-abcd-1234-1234-1234567890"
    },
```

```
    "responseElements": null,
    "requestID": "abcdefgh-1234-abcd-1234-1234567abcdef",
    "eventID": "12345678-1234-1234-abcd-abcdef1234567",
    "readOnly": true,
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "eventCategory": "Management",
    "recipientAccountId": "12345678901234567"
}
```

CloudTrail 레코드 콘텐츠에 대한 자세한 내용은 AWS CloudTrail 사용 설명서의 CloudTrail record contents를 참조하세요.

Incident Manager와 제품 및 서비스 통합

의 도구인 Incident Manager는 다음 제품, 서비스 및 도구와 AWS Systems Manager통합됩니다.

와 통합 AWS 서비스

Incident Manager는 다음 표에 설명된 AWS 서비스 및 도구와 통합됩니다.

AWS CDK	AWS CDK 는 코드를 사용하여 클라우드 인프라를 정의하고를 프로비저닝에 사용하기 AWS CloudFormation 위한 개발 프레임워크입니다. 는 TypeScript, JavaScript, , Python Java및 C#/를 포함한 여러 프로그래밍 언어를 AWS CDK 지원합니다.Net. Incident Manager AWS CDK 에서를 사용하는 방법에 대한 자세한 내용은 AWS CDK API 참조의 다음 섹션을 참조하세요. • @aws-cdk/aws-ssmincidents 모듈 • @aws-cdk/aws-ssmcontacts 모듈
채팅 애플리케이션의 Amazon Q Developer	채팅 애플리케이션의 Amazon Q Developer를 사용하면 DevOps 및 소프트웨어 개발 팀이 메시징 프로그램 채팅룸을 사용하여의 운영 이벤트를 모니터링하고 대응할 수 있습니다 AWS 클라우드. Incident Manager를 사용하는 채팅 애플리케이션에서 Amazon Q Developer를 사용하면 대응 담당자가 인시던트를 모니터링하고 대응하는 데 사용할 수 있는 채팅 채널을 생성할 수 있습니다. 채팅 애플리케이션의 Amazon Q Developer는 Slack 채팅룸, Microsoft Teams 채널 및 Amazon Chime 채팅룸을 채팅 채널로 지원합니다.

	Amazon Simple Notification Service(Amazon SNS)에서 주제를 생성하여 채팅 채널을 생성할 수도 있습니다. Amazon SNS는 게시자의 메시지를 구독자에게 전달하는 관리형 서비스입니다. 인시던트 대응 계획에서는 생성한 채팅 채널을 계획에 연결할 때 채팅 채널과 연결한 주제를 하나 이상 선택합니다. 이러한 SNS 주제는 인시던트 대응 담당자에게 인시던트에 대한 알림을 보내는 데 사용됩니다. 자세한 내용은 Incident Manager에서 대응 담당자를 위한 채팅 채널 생성 및 통합 단원을 참조하십시오.
AWS CloudFormation	AWS CloudFormation 는 애플리케이션에 필요한 모든 리소스가 포함된 템플릿을 생성한 다음 리소스를 구성하고 프로비저닝하는 데 사용할 수 있는 서비스입니다. 또한 모든 종속성을 구성하므로 리소스 관리보다는 애플리케이션에 더 집중할 수 있습니다. Incident Manager와 AWS CloudFormation 함께를 사용하는 방법에 대한 자세한 내용은 AWS CloudFormation 사용 설명서의 다음 주제를 참조하세요. • Incident Manager 리소스 유형 참조 • 연락처 리소스 유형 참조 리소스 유형 참조

Amazon CloudWatch	CloudWatch는 AWS 리소스와 실행 중인 애플리케이션을 AWS 실시간으로 모니터링합니다. CloudWatch를 사용하여 리소스 및 애플리케이션에 대해 측정할 수 있는 변수인 지표를 수집하고 추적할 수 있습니다. Incident Manager에서 인시던트를 생성하도록 CloudWatch 경보를 구성할 수 있습니다. CloudWatch는 Systems Manager 및 Incident Manager와 협력하여 경보가 경보 상태로 전환되면 대응 계획 템플릿에서 인시던트를 생성합니다. 자세한 내용은 CloudWatch 경보를 사용하여 자동으로 인시던트 생성 단원을 참조하십시오.
Amazon Chime	Amazon Chime은 회의, 채팅 및 비즈니스 통화를 결합한 온라인 작업 공간입니다. Amazon Chime을 사용하여 조직 내부 및 외부에서 회의, 채팅 및 비즈니스 통화를 수행할 수 있습니다. 채팅 애플리케이션에서 Amazon Q Developer에 Amazon Chime용 채팅 채널을 생성한 다음 해당 채널을 대응 계획에 추가하여 Amazon Chime 룸을 Incident Manager 작업에 통합할 수 있습니다. 자세한 내용은 Incident Manager에서 대응 담당자를 위한 채팅 채널 생성 및 통합 단원을 참조하십시오.

Amazon EventBridge	EventBridge는 이벤트를 사용하여 애플리케이션 구성 요소를 연결하는 서버리스 서비스로, 이를 통해 확장 가능한 이벤트 기반 애플리케이션을 보다 쉽게 구축할 수 있습니다. 이벤트가 정의한 패턴과 일치할 때 AWS 리소스의 이벤트 패턴을 감시하고 Incident Manager에서 인시던트를 생성하도록 EventBridge 규칙을 구성할 수 있습니다. 규칙은 수십 개의 AWS 서비스 및 타사 애플리케이션 및 서비스의 이벤트 패턴을 모니터링할 수 있습니다. 자세한 내용은 EventBridge 이벤트를 사용하여 자동으로 인시던트 생성 단원을 참조하십시오.
AWS Secrets Manager	Secrets Manager를 사용하면 수명 주기 동안 데이터베이스 보안 인증, 애플리케이션 보안 인증, OAuth 토큰, API 키 및 기타 암호를 관리, 검색, 교체할 수 있습니다. Incident Manager를 PagerDuty 서비스와 통합하면 PagerDuty 자격 증명이 포함된 시크릿이 Secrets Manager에 생성됩니다. 자세한 내용은 AWS Secrets Manager 보안 암호에 PagerDuty 액세스 자격 증명 저장 단원을 참조하십시오.

AWS Systems Manager	Systems Manager는 애플리케이션 인프라를 보고 제어하는 데 사용할 수 있는 운영 허브이자 클라우드 환경을 위한 안전한 엔드 투 엔드 관리 솔루션입니다. 다음 Systems Manager 도구는 Incident Manager와 직접 통합됩니다. • Automation – Automation 런북에서는 Systems Manager가 AWS 리소스에 대해 수행하는 작업을 정의합니다. Incident Manager의 런북은 인시던트를 해결하는 데 사용할 일련의 자동 및 수동 단계를 정의합니다. Incident Manager와 사용하기 위한 자동화 런북 생성에 대한 자세한 내용은 인시던트 해결을 위해 Incident Manager에 Systems Manager Automation 런북 통합 섹션을 참조하세요. • OpsCenter – OpsCenter는 운영 엔지니어와 IT 전문가가 AWS 리소스와 관련된 OpsItems라는 운영 작업 항목을 관리할 수 있는 중앙 위치를 제공합니다. 인시던트 사후 분석을 통해 직접 OpsItems를 생성하여 관련 작업에 대한 후속 조치를 취할 수 있습니다. 자세한 내용은 Incident Manager에서 인시던트 사후 분석 수행 단원을 참조하십시오.

AWS Trusted Advisor	Trusted Advisor는 기본 또는 개발자 지원 플랜을 보유한 AWS 고객이 사용할 수 있는 도구입니다.는 AWS 환경을 Trusted Advisor 검사한 다음 비용을 절감하거나, 시스템 가용성 및 성능을 개선하거나, 보안 격차를 좁힐 수 있는 기회가 있을 때 권장 사항을 제공합니다. Incident Manager의 경우 복제 세트의 구성이 둘 이상의를 사용하여 리전 장애 조치 및 응답을 지원하는 AWS 리전 지 Trusted Advisor 확인합니다.

다른 제품 및 서비스와 통합

Incident Manager를 다음 표에 설명된 타사 서비스와 통합하거나 사용할 수 있습니다.

Jira Cloud	를 사용하여 Incident Manager를 타사 클라우드 기반 워크플로 플랫폼인 Jira Cloud(Atlassian)와 통합할 AWS Service Management Connector수 있습니다. Jira Cloud와의 통합을 구성한 후 Incident Manager에서 새 인시던트를 만들면 통합을 통해 Jira Cloud에도 인시던트가 생성됩니다. Incident Manager에서 인시던트를 업데이트하면 Jira Cloud의 해당 인시던트가 업데이트됩니다. Incident Manager 또는 Jira Cloud에서 인시던트를 해결하는 경우 통합은 사용자가 구성한 기본 설정에 따라 두 서비스 모두에서 인시던트를 해결합니다. 자세한 내용은 AWS Service Management Connector 관리자 안내서의 Integrating AWS Systems Manager Incident Manager (Jira Cloud)을 참조하세요.

Jira Service Management	를 사용하여 Incident Manager를 타사 클라우드 기반 워크플로 플랫폼인 Jira Service Management와 통합할 AWS Service Management Connector수 있습니다. Jira Service Management와의 통합을 구성한 후 Incident Manager에서 새 인시던트를 만들면 통합을 통해 Jira Service Management에도 인시던트가 생성됩니다. Incident Manager에서 인시던트를 업데이트하면 Jira Service Managemen t의 해당 인시던트가 업데이트됩니다. Incident Manager 또는 Jira Service Management에서 인시던트를 해결하는 경우 사용자가 구성한 기본 설정에 따라 통합을 통해 두 서비스 모두에서 인시던트가 해결됩니다. 자세한 정보는 AWS Service Managemen t Connector 관리자 설명서의 Jira Service Management 구성을 참조하세요.
Microsoft Teams	Microsoft Teams는 팀 메시징, 오디오 및 비디오 회의, 파일 공유를 위한 클라우드 기반 협업 도구를 제공합니다. 채팅 애플리케이션에서 Microsoft Team Amazon Q DeveloperMicrosoft Teams의에 대한 채팅 채널을 생성한 다음 해당 채널을 대응 계획에 추가하여 채널을 Incident Manager 작업에 통합할 수 있습니다. https://docs.aws.amazon.com/chatbot/latest/adminguide/ 자세한 내용은 Incident Manager에서 대응 담당자를 위한 채팅 채널 생성 및 통합 단원을 참조하십시오.

PagerDuty	PagerDuty는 페이징 워크플로 및 에스컬레이션 정책을 지원하는 인시던트 대응 도구입니다. Incident Manager를 PagerDuty와 통합하면 대응 계획에 PagerDuty 서비스를 추가할 수 있습니다. 이후 Incident Manager에서 인시던트가 생성될 때마다 PagerDuty에 해당 인시던트가 생성됩니다. PagerDuty의 인시던트는 Incident Manager의 페이징 워크플로 및 에스컬레이션 정책 외에도 사용자가 정의한 페이징 워크플로 및 에스컬레이션 정책을 사용합니다. PagerDuty는 Incident Manager의 타임라인 이벤트를 인시던트에 대한 메모로 첨부합니다. Incident Manager를 PagerDuty와 통합하려면 먼저 AWS Secrets Manager 에서 PagerDuty 자격 증명이 포함된 시크릿을 만들어야 합니다. 의 보안 암호에 PagerDuty REST API 키 및 기타 필수 세부 정보를 추가하는 방법에 대한 자세한 내용은 섹션을 AWS Secrets Manager참조하세요AWS Secrets Manager 보안 암호에 PagerDuty 액세스 자격 증명 저장. PagerDuty 계정의 PagerDuty 서비스를 Incident Manager의 대응 계획에 추가하는 방법에 대한 자세한 내용은 대응 계획 생성 항목의 PagerDuty 서비스를 대응 계획에 통합하는 단계를 참조하세요.

ServiceNow	를 사용하여 Incident Manager를 타사 클라우드 기반 워크플로 플랫폼인 ServiceNow와 통합할 AWS Service Management Connector수 있습니다. ServiceNow와의 통합을 구성한 후 Incident Manager에서 새 인시던트를 만들면 통합을 통해 ServiceNow에도 인시던트가 생성됩니다. Incident Manager에서 인시던트를 업데이트하면 ServiceNow의 해당 인시던트가 업데이트됩니다. Incident Manager 또는 ServiceNow에서 인시던트를 해결하는 경우 사용자가 구성한 기본 설정에 따라 통합을 통해 두 서비스의 인시던트가 해결됩니다. 자세한 내용은 AWS Service Management Connector 관리자 안내서의 ServiceNow AWS Systems Manager Incident Manager 에서 통합을 참조하세요.
Slack	Slack는 팀 메시징, 오디오 및 비디오 회의, 파일 공유를 위한 클라우드 기반 협업 도구를 제공합니다. 채팅 애플리케이션에서 Slack Amazon Q DeveloperSlack의에 대한 채팅 채널을 생성한 다음 해당 채널을 대응 계획에 추가하여 채널을 Incident Manager 작업에 통합할 수 있습니다. https://docs.aws.amazon.com/chatbot/latest/adminguide/ 자세한 내용은 Incident Manager에서 대응 담당자를 위한 채팅 채널 생성 및 통합 단원을 참조하십시오.

Terraform	HashiCorp Terraform은 다양한 클라우드 서비스를 관리하기 위한 명령줄 인터페이스(CLI) 워크플로를 제공하는 오픈 소스 코드형 인프라(IaC) 소프트웨어 도구입니다. Incident Manager의 경우 Terraform을 사용하여 다음을 관리하거나 제공할 수 있습니다. SSM Incident Manager 연락처 리소스 • aws_ssmcontacts_contact • aws_ssmcontacts_contact_channel • aws_ssmcontacts_plan • aws_ssmcontacts_rotation SSM 연락처 데이터 소스 • aws_ssmcontacts_contact • aws_ssmcontacts_contact_channel • aws_ssmcontacts_plan • aws_ssmcontacts_rotation SSM Incident Manager 리소스 • aws_ssmincidents_replication_set • aws_ssmincidents_response_plan SSM Incident Manager 데이터 소스 • aws_ssmincidents_replication_set • aws_ssmincidents_response_plan

AWS Secrets Manager 보안 암호에 PagerDuty 액세스 자격 증명 저장

대응 계획을 위해 PagerDuty와의 통합을 활성화한 후 Incident Manager는 다음과 같은 방식으로 PagerDuty를 사용합니다.

- Incident Manager에서 새 인시던트를 만들면 Incident Manager가 PagerDuty에 해당 인시던트를 생성합니다.
- PagerDuty에서 만든 페이징 워크플로 및 에스컬레이션 정책은 PagerDuty 환경에서 사용됩니다. 하지만 Incident Manager는 PagerDuty 구성을 가져오지 않습니다.
- Incident Manager는 타임라인 이벤트를 PagerDuty에 인시던트에 대한 메모로 최대 2,000개의 메모까지 게시합니다.
- Incident Manager에서 관련 인시던트를 해결할 때 PagerDuty 인시던트를 자동으로 해결하도록 선택할 수 있습니다.

Incident Manager를 PagerDuty와 통합하려면 먼저 PagerDuty 보안 인증 AWS Secrets Manager 정보가 포함된 보안 암호를에 생성해야 합니다. 이를 통해 Incident Manager는 PagerDuty 서비스와 통신할 수 있습니다. 그런 다음 Incident Manager에서 생성하는 대응 계획에 PagerDuty 서비스를 포함시킬 수 있습니다.

Secrets Manager에서 생성하는 이 암호에는 적절한 JSON 형식으로 다음이 포함되어야 합니다.

- PagerDuty 계정의 API 키. 일반 액세스 REST API 키 또는 사용자 토큰 REST API 키 중 하나를 사용할 수 있습니다.
- PagerDuty 하위 도메인의 유효한 사용자 이메일 주소입니다.
- 하위 도메인을 배포한 PagerDuty 서비스 리전.

> **Note**
>
> PagerDuty 하위 도메인의 모든 서비스는 동일한 서비스 리전에 배포됩니다.

사전 조건

Secrets Manager에서 암호를 생성하기 전에 다음 요구 사항을 충족해야 합니다.

KMS 키

생성한 보안 암호는 AWS Key Management Service ()에서 생성한 고객 관리형 키로 암호화해야 합니다AWS KMS. PagerDuty 자격 증명을 저장하는 암호를 만들 때 이 키를 지정합니다.

> **Important**
>
> Secrets Manager는 로 보안 암호를 암호화하는 옵션을 제공 AWS 관리형 키하지만이 암호화 모드는 지원되지 않습니다.

고객 관리 키는 다음 요구 사항을 충족해야 합니다.

- 키 유형: 대칭을 선택합니다.
- 키 사용: 암호화 및 암호 해독을 선택합니다.
- 리전성: 응답 계획을 여러에 복제하려면 다중 리전 키를 선택해야 AWS 리전합니다.

키 정책

대응 계획을 구성하는 사용자는 키의 리소스 기반 정책에 대한 `kms:GenerateDataKey` 및 `kms:Decrypt` 권한이 있어야 합니다. `ssm-incidents.amazonaws.com` 서비스 보안 주체는 키의 리소스 기반 정책에 대한 `kms:GenerateDataKey` 및 `kms:Decrypt` 권한을 가지고 있어야 합니다.

다음 정책은 이러한 권한을 보여줍니다. *`user input placeholder`*를 사용자의 정보로 바꿉니다.

```
{
    "Version": "2012-10-17",
    "Id": "key-consolepolicy-3",
    "Statement": [
        {
            "Sid": "Enable IAM user permissions",
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws:iam::account-id:root"
            },
            "Action": "kms:*",
            "Resource": "*"
```

```
        },
        {
            "Sid": "Allow creator of response plan to use the key",
            "Effect": "Allow",
            "Principal": {
                "AWS": "IAM_ARN_of_principal_creating_response_plan"
            },
            "Action": [
                "kms:Decrypt",
                "kms:GenerateDataKey*"
            ],
            "Resource": "*"
        },
        {
            "Sid": "Allow Incident Manager to use the key",
            "Effect": "Allow",
            "Principal": {
                "Service": "ssm-incidents.amazonaws.com"
            },
            "Action": [
                "kms:Decrypt",
                "kms:GenerateDataKey*"
            ],
            "Resource": "*"
        }
    ]
}
```

고객 관리형 키 생성에 대한 자세한 내용은 AWS Key Management Service 개발자 안내서에서 대칭 암호화 KMS 키 생성을 참조하세요. AWS KMS 키에 대한 자세한 내용은 AWS KMS 개념을 참조하세요.

기존 고객 관리형 키가 이전 요구 사항을 모두 충족하는 경우 정책을 편집하여 이러한 권한을 추가할 수 있습니다. 고객 관리형 키의 정책 업데이트에 대한 자세한 내용은 AWS Key Management Service 개발자 안내서의 키 정책 변경을 참조하세요.

> **Tip**
>
> 조건 키를 지정하여 액세스를 더 제한할 수 있습니다. 예를 들어 다음 정책은 미국 동부(오하이오) 리전 (us-east-2) 에서 Secrets Manager를 통한 액세스만 허용합니다.
>
> ```
> {
> ```

```
    "Sid": "Enable IM Permissions",
    "Effect": "Allow",
    "Principal": {
        "Service": "ssm-incidents.amazonaws.com"
    },
    "Action": ["kms:Decrypt", "kms:GenerateDataKey*"],
    "Resource": "*",
    "Condition": {
        "StringEquals": {
            "kms:ViaService": "secretsmanager.us-east-2.amazonaws.com"
        }
    }
}
```

`GetSecretValue` 권한

대응 계획을 생성하는 IAM ID(사용자, 역할 또는 그룹)에 IAM 권한 `secretsmanager:GetSecretValue`가 있어야 합니다.

AWS Secrets Manager 보안 암호에 PagerDuty 액세스 자격 증명을 저장하려면

1. AWS Secrets Manager 사용 설명서의 AWS Secrets Manager 보안 암호 생성에서 3a단계의 단계를 따릅니다.
2. 3b단계에서 키/값 쌍에 대해 다음을 수행하십시오.
   - 일반 텍스트 탭을 선택합니다.
   - 상자의 기본 내용을 다음 JSON 구조로 바꿉니다.

     ```
     {
         "pagerDutyToken": "pagerduty-token",
         "pagerDutyServiceRegion": "pagerduty-region",
         "pagerDutyFromEmail": "pagerduty-email"
     }
     ```

   - 붙여넣은 JSON 샘플에서 `###### #` 값을 다음과 같이 바꿉니다.
     - *`pagerduty-token`*: PagerDuty 계정의 일반 액세스 REST API 키 또는 사용자 토큰 REST API 키 값입니다.

       관련 정보는 PagerDuty 기술 자료의 API 액세스 키를 참조하세요.

- *pagerduty-region*: PagerDuty 하위 도메인을 호스팅하는 PagerDuty 데이터 센터의 서비스 리전입니다.

  관련 정보는 PagerDuty 기술 자료의 서비스 리전을 참조하세요.

- *pagerduty-email*: PagerDuty 하위 도메인에 속하는 사용자의 유효한 이메일 주소입니다.

  관련 정보는 PagerDuty 기술 자료의 사용자 관리를 참조하세요.

다음 예제는 필수 PagerDuty 자격 증명이 포함된 완성된 JSON 암호를 보여줍니다.

```
{
    "pagerDutyToken": "y_NbAkKc66ryYEXAMPLE",
    "pagerDutyServiceRegion": "US",
    "pagerDutyFromEmail": "JohnDoe@example.com"
}
```

3. 3c단계에서 암호화 키의 경우 사전 요구 사항 섹션에 나열된 요구 사항을 충족하는 생성된 고객 관리형 키를 선택합니다.
4. 4c단계에서 리소스 권한에 대해 다음을 수행하십시오.
   - 리소스 권한을 확장합니다.
   - 권한 편집을 선택합니다.
   - 정책 상자의 기본 내용을 다음 JSON 구조로 바꿉니다.

```
{
    "Effect": "Allow",
    "Principal": {
        "Service": "ssm-incidents.amazonaws.com"
    },
    "Action": "secretsmanager:GetSecretValue",
    "Resource": "*"
}
```

   - 저장(Save)을 선택합니다.
5. 응답 계획을 두 개 이상의 AWS 리전으로 복제했다면 4d단계에서 암호 복제에 대해 다음을 수행하십시오.
   - 암호 복제를 확장합니다.
   - AWS 리전에서 응답 계획을 복제했던 리전을 선택합니다.

- 암호화 키의 경우 사전 요구 사항 섹션에 나열된 요구 사항을 충족하는 이 리전에서 생성했거나 해당 리전에 복제된 고객 관리 키를 선택합니다.
- 각 추가에 대해 리전 AWS 리전추가를 선택하고 리전 이름과 고객 관리형 키를 선택합니다.

6. AWS Secrets Manager 사용 설명서의 AWS Secrets Manager 보안 암호 생성의 나머지 단계를 완료합니다.

PagerDuty 서비스를 Incident Manager 인시던트 워크플로에 추가하는 방법에 대한 자세한 내용은 대응 계획 생성 항목의 PagerDuty 서비스를 대응 계획에 통합을 참조하세요.

관련 정보

PagerDuty 및 AWS Systems Manager Incident Manager를 사용하여 인시던트 대응을 자동화하는 방법(AWS 클라우드 운영 및 마이그레이션 블로그)

AWS Secrets Manager 사용 설명서의 AWS Secrets Manager에서 암호 암호화

AWS Systems Manager Incident Manager 문제 해결

AWS Systems Manager Incident Manager를 사용하는 동안 문제가 발생하면 다음 정보를 사용하여 모범 사례에 따라 문제를 해결할 수 있습니다. 발생한 문제가 다음 정보의 범위를 벗어나거나 해결을 시도한 후에도 문제가 지속되는 경우 AWS Support에 문의하세요.

주제

오류 메시지: `ValidationException – We were unable to validate the AWS Secrets Manager secret`

문제 1: 대응 계획을 생성하는 AWS Identity and Access Management (IAM) 자격 증명(사용자, 역할 또는 그룹)에 `secretsmanager:GetSecretValue` IAM 권한이 없습니다. Secrets Manager 암호를 검증하려면 IAM ID에 이 권한이 있어야 합니다.

- 해결 방법: 응답 계획을 생성하는 IAM ID에 대한 IAM 정책에 누락된 `secretsmanager:GetSecretValue` 권한을 추가하세요. 자세한 내용은 IAM 사용 설명서의 IAM ID 권한 추가(콘솔) 또는 IAM 정책 추가(AWS CLI)를 참조하세요.

문제 2: 암호에 IAM ID로 `GetSecretValue`작업을 실행할 수 있도록 허용하는 리소스 기반 정책이 연결되어 있지 않거나 리소스 기반 정책이 ID에 대한 권한을 거부합니다.

- 해결 방법: IAM ID에 대한 `secrets:GetSecretValue` 권한을 부여하는 `Allow` 문을 암호의 리소스 기반 정책에 만들거나 추가하십시오. 또는 IAM 자격 증명이 포함된 `Deny` 명령문을 사용하는 경우 자격 증명이 작업을 실행할 수 있도록 정책을 업데이트하세요. 자세한 내용은 AWS Secrets Manager 사용 설명서의 AWS Secrets Manager 보안 암호에 권한 정책 연결을 참조하세요.

문제 3: 암호에 Incident Manager 서비스 보안 주체, `ssm-incidents.amazonaws.com`에 대한 액세스를 허용하는 리소스 기반 정책이 첨부되어 있지 않습니다.

- 해결 방법: 암호에 대한 리소스 기반 정책을 만들거나 업데이트하고 다음 권한을 포함하세요.

```
{
```

```
    "Effect": "Allow",
    "Principal": {
        "Service": ["ssm-incidents.amazonaws.com"]
    },
    "Action": "secretsmanager:GetSecretValue",
    "Resource": "*"
}
```

문제 4: 보안 암호를 암호화하기 위해 AWS KMS key 선택한이 고객 관리형 키가 아니거나, 선택한 고객 관리형 키가 Incident Manager 서비스 보안 주체`kms:GenerateDataKey*`에게 IAM 권한 `kms:Decrypt` 및를 제공하지 않습니다. 또는 대응 계획을 생성하는 IAM 자격 증명에 `GetSecretValue` IAM 권한이 없을 수도 있습니다.

- 해결 방법: AWS Secrets Manager 보안 암호에 PagerDuty 액세스 자격 증명 저장 주제의 사전 요구 사항에 설명된 요구 사항을 충족하는지 확인하세요.

문제 5: General Access REST API Key 키 또는 User Token REST API 키가 포함된 암호의 ID가 올바르지 않습니다.

- 해결 방법: Secrets Manager 암호의 ID를 뒤에 공백 없이 정확하게 입력했는지 확인하십시오. 사용하려는 보안 암호를 AWS 리전 저장하는 동일한에서 작업해야 합니다. 삭제된 암호는 사용할 수 없습니다.

문제 6: 드문 경우이긴 하지만 Secrets Manager 서비스에 문제가 발생하거나 Incident Manager가 해당 서비스와 통신하는 데 문제가 있을 수 있습니다.

- 해결 방법: 몇 분 기다린 후 다시 시도합니다. AWS Health Dashboard에 영향을 미칠 수 있는 문제가 있는지 확인하십시오.

기타 문제 해결

이전 단계로도 문제가 해결되지 않은 경우 다음 리소스에서 추가 지원을 찾을 수 있습니다.

- Incident Manager 콘솔에 액세스할 때 Incident Manager와 관련된 IAM 문제에 대해서는 AWS Systems Manager Incident Manager 자격 증명 및 액세스 문제 해결 섹션을 참조하세요.

- 에 액세스할 때 발생하는 일반적인 인증 및 권한 부여 문제는 IAM 사용 설명서의 IAM 문제 해결을 AWS Management Console참조하세요. https://docs.aws.amazon.com/IAM/latest/UserGuide/troubleshoot.html

Incident Manager 문서 기록

변경 사항	설명	날짜
인시던트를 수동으로 생성하기 위한 권한 요구 사항으로 변경	사용자가 인시던트를 수동으로 생성하는 데 필요한 IAM 권한이 변경되어 더 이상 서비스 연결 역할을 사용하지 않습니다. 대신 Incident Manager는 이제 전달 액세스 세션(FAS)을 사용하여의 `ssm-contacts:StartEngagement` 일부로를 호출합니다`ssm-incidents:StartIncident`. 자세한 내용은 인시던트를 수동으로 시작하는 데 필요한 IAM 권한을 참조하세요.	2025년 6월 10일
관리형 정책 업데이트 `AWSServiceRoleforIncidentManagerPolicy`	Incident Manager는 Incident Manager가 `AWS/Usage` 네임스페이스 내의 지표를 계정에 게시할 수 `AWSServiceRoleforIncidentManagerPolicy` 있는 새 권한을에 추가했습니다. 자세한 내용은 AWS 관리형 정책에 대한 Incident Manager 업데이트를 참조하세요.	2025년 1월 28일
관리형 정책 업데이트 `AWSIncidentManagerIncidentAccessServiceRolePolicy`	Incident Manager는 조사 결과 기능을 `AWSIncidentManagerIncidentAccessServiceRolePolicy` 지원하기 위해 EC2 인스턴스가 Auto Scaling 그룹의	2024년 2월 20일

	일부인지 확인할 수 있는 새 권한을에 추가했습니다. 자세한 내용은 AWS 관리형 정책에 대한 Incident Manager 업데이트를 참조하세요.	
추가 HashiCorp Terraform 지원: 대기 교체	Terraform은 Incident Manager에 대한 지원에를 추가했습니다. 이제 Terraform을 사용하여 Incident Manager 대기 리소스를 프로비저닝하거나 관리할 수 있습니다. 이 통합 및 Incident Manager와의 기타 타사 통합에 대한 자세한 내용은 다른 제품 및 서비스와의 통합을 참조하세요.	2024년 2월 2일

새로운 기능: 다른의 결과 AWS 서비스	조사 결과는 Incident Manager에서 인시던트가 생성된 시점에 발생한 AWS CloudFormation 스택 및 AWS CodeDeploy 배포와 관련된 변경 사항에 대한 정보를 제공합니다. Incident Manager 콘솔에서 이러한 변경 사항에 대한 요약 정보를 볼 수 있으며, 대부분의 경우 CloudFormation 또는 CodeDeploy 콘솔 링크에 액세스하여 변경 사항에 대한 전체 세부 정보를 확인할 수 있습니다. 조사 결과는 인시던트의 잠재적 원인을 평가하는 데 필요한 시간을 줄여줍니다. 또한 인시던트 원인을 조사하기 위해 대응 담당자가 잘못된 계정이나 콘솔에 액세스할 가능성도 줄어듭니다. 또한이 기능은 Incident Manager가 다른의 리소스를 읽고 인시던트와 관련된 조사 결과를 AWS 서비스 식별할 수 있도록 하는 새로운 관리형 정책`AWSIncidentManagerIncidentAccessServiceRolePolicy` 인를 도입합니다. 자세한 정보는 다음의 주제를 참조하세요. • 조사 결과 작업 • AWS 관리형 정책: AWSIncidentManagerIncidentAccessServiceRolePolicy	2023년 11월 15일

Incident Manager와의 통합 목록이 업데이트되었습니다.	Incident Manager와의 제품 및 서비스 통합 항목이 확장되어 Incident Manager와 함께 인시던트 탐지 및 대응 작업에 통합할 수 있는 모든 AWS 서비스 및 타사 도구를 나열하고 설명합니다.	2023년 6월 9일
와 통합 AWS Trusted Advisor	Trusted Advisor 이제는 복제 세트의 구성이 둘 이상의를 사용하여 리전 장애 조치 및 응답을 지원하는 AWS 리전 지 확인합니다. CloudWatch 경보 또는 EventBridge 이벤트에 의해 생성된 인시던트의 경우 Incident Manager는 경보 또는 이벤트 규칙 AWS 리전 과 동일한에 인시던트를 생성합니다. 해당 리전에서 Incident Manager를 일시적으로 사용할 수 없는 경우 시스템은 복제 세트의 다른 리전에 인시던트를 생성하려고 시도합니다. 복제 세트에 리전이 하나만 포함된 경우 Incident Manager를 사용할 수 없는 동안에는 시스템이 인시던트 레코드를 만들지 못합니다. 이러한 상황을 방지하기 위해는 복제 세트가 하나의 리전에 대해서만 구성된 경우를 Trusted Advisor 보고합니다. Trusted Advisor사용에 대한 자세한 정보는 AWS Support 사용 설명서의 AWS Trusted Advisor를 참조하세요.	2023년 4월 28일

대응 계획에서 채팅 채널 Microsoft Teams로 사용	채팅 애플리케이션의 Microsoft Teams 및 Amazon Q Developer와의 통합을 통해 이제 대응 계획에서 채팅 채널에 Microsoft Teams를 사용할 수 있습니다. 이는 Slack 및 Amazon Chime 채팅 채널에 대한 지원에 추가됩니다. 인시던트 발생 시 Incident Manager는 채팅 채널로 상태 알림을 직접 전송하여 모든 대응 담당자에게 계속 정보를 제공합니다. 또한 대응 담당자는 Microsoft Teams 애플리케이션의 인시던트 관련 AWS CLI 명령 및 서로 통신하여 인시던트를 업데이트하고 상호 작용할 수 있습니다. 자세한 내용은 Incident Manager의 채팅 채널 사용을 참조하세요.	2023년 4월 4일

새 기능: 대기 일정	Incident Manager의 대기 일정은 운영자 개입이 필요한 인시던트 발생 시 알림을 받는 사람을 정의합니다. 대기 일정은 해당 일정에 대해 생성한 하나 이상의 교대로 구성됩니다. 각 교대에 최대 30명의 연락처를 포함할 수 있습니다. 대기 일정을 만든 후 에스컬레이션 계획에 에스컬레이션으로 포함시킬 수 있습니다. 해당 에스컬레이션 계획과 관련된 인시던트가 발생하면 Incident Manager는 일정에 따라 대기 중인 운영자에게 알립니다. 자세한 내용은 Incident Manager의 대기 일정 사용을 참조하세요.	2023년 3월 28일
형식이 지정된 인시던트 분석을 인쇄하거나 PDF로 저장	이제 인시던트 분석 페이지에 인쇄용으로 포맷된 분석 버전을 생성할 수 있는 인쇄 버튼이 포함되어 있습니다. 디바이스용으로 구성된 프린터 대상을 사용하여 인시던트 분석을 PDF로 저장하거나 로컬 또는 네트워크 프린터로 보낼 수 있습니다. 자세한 내용은 서식이 지정된 인시던트 분석 인쇄를 참조하세요.	2023년 1월 17일

PagerDuty 통합: Incident Manager가 이제 인시던트 타임라인 이벤트를 PagerDuty 인시던트에 복사합니다.	대응 계획에서 PagerDuty와의 통합을 켜면 Incident Manager가 해당 계획에서 만든 타임라인 이벤트를 PagerDuty의 해당 인시던트 레코드에 추가합니다. PagerDuty는 타임라인 이벤트를 PagerDuty에 인시던트에 대한 메모로 최대 2,000개의 메모까지 게시합니다. 이 변경 사항에 대한 자세한 내용은 다음 주제를 참조하세요. • AWS Secrets Manager 보안 암호에 PagerDuty 액세스 자격 증명 저장 • PagerDuty 서비스를 대응 계획에 통합	2022년 12월 15일
Incident Manager와 CloudWatch 지표의 통합	이제 CloudWatch에 인시던트 관련 지표를 게시할 수 있습니다. 자세한 내용은 CloudWatch 지표를 참조하세요. AWSIncidentManagerServiceRolePolicy에는 AWS 서비스가 사용자를 대신하여 지표를 게시할 수 있는 추가 권한이 포함되어 있습니다.	2022년 12월 15일
인시던트 메모를 시작하고 인시던트 세부 정보 화면을 업데이트했습니다.	인시던트 메모를 사용하면 인시던트를 처리하는 다른 사용자와 협업하고 소통할 수 있습니다. 또한 인시던트 세부 정보 화면에서 런북 및 참여 상태를 볼 수 있습니다. 자세한 내용은 인시던트 세부 정보를 참조하세요.	2022년 11월 16일

PagerDuty 에스컬레이션 계획 및 페이징 워크플로를 Incident Manager 대응 계획에 통합	이제 Incident Manager를 PagerDuty와 통합하고 PagerDuty 서비스를 대응 계획에 추가할 수 있습니다. 통합을 구성한 후 Incident Manager는 Incident Manager에서 생성된 각 새 인시던트에 대해 PagerDuty에서 해당 인시던트를 생성할 수 있습니다. PagerDuty 환경에서 정의한 페이징 워크플로 및 에스컬레이션 정책을 PagerDuty에서 사용합니다. 자세한 정보는 다음의 주제를 참조하세요. • Incident Manager와 제품 및 서비스 통합 • AWS Secrets Manager 보안 암호에 PagerDuty 액세스 자격 증명 저장 • PagerDuty 서비스를 대응 계획 생성 주제의 응답 계획에 통합 • 문제 해결	2022년 11월 16일
인시던트 메모를 시작하고 인시던트 세부 정보 화면을 업데이트했습니다.	인시던트 메모를 사용하면 인시던트를 처리하는 다른 사용자와 협업하고 소통할 수 있습니다. 또한 인시던트 세부 정보 화면에서 런북 및 참여 상태를 볼 수 있습니다. 자세한 내용은 인시던트 세부 정보를 참조하세요.	2022년 11월 16일

복제 세트에 대한 태그 지정 지원	이제 AWS Systems Manager Incident Manager에서 설정한 복제 세트에 태그를 지정할 수 있습니다. 이렇게 하면 복제 세트에 AWS 리전 지정된의 대응 계획, 인시던트 레코드 및 연락처에 태그를 할당하는 기존 지원이 추가됩니다. 자세한 내용은 다음 주제를 참조하세요. • 준비 완료 마법사 • Incident Manager 리소스 태그 지정	2022년 11월 2일
Incident Manager와 Atlassian Jira Service Management 통합	Jira 서비스 관리용 AWS 서비스 관리 커넥터를 사용하여 Incident Manager를 Jira 서비스 관리와 통합할 수 있습니다. 통합을 구성한 후 Incident Manager에서 만든 새 인시던트는 Jira에 해당하는 인시던트를 생성합니다. Incident Manager에서 인시던트를 업데이트하면 업데이트가 Jira의 해당 인시던트에 추가됩니다. Incident Manager 또는 Jira에서 인시던트를 해결하는 경우 구성된 기본 설정에 따라 해당 인시던트도 해결됩니다. 자세한 내용은 AWS Service Management Connector 관리자 안내서의 Jira Service Management 구성을 참조하세요.	2022년 10월 6일

향상된 태그 지정 지원	Incident Manager는 복제 세트에 AWS 리전 지정된의 대응 계획, 인시던트 레코드 및 연락처에 태그 할당을 지원합니다. 또한 Incident Manager는 대응 계획에서 생성된 인시던트에 태그를 자동으로 할당할 수 있도록 지원합니다. 자세한 내용은 Incident Manager 리소스 태그 지정을 참조하세요.	2022년 6월 28일
Incident Manager와 ServiceNow의 통합	AWS ServiceNow 관리 커넥터를 사용하여 Incident Manager를 ServiceNow와 통합할 수 있습니다. 통합을 구성한 후 Incident Manager에서 만든 새 인시던트는 ServiceNow에서 해당 인시던트를 생성합니다. Incident Manager에서 인시던트를 업데이트하면 ServiceNow의 해당 인시던트에 업데이트가 추가됩니다. Incident Manager 또는 ServiceNow에서 인시던트를 해결하는 경우 구성된 기본 설정에 따라 해당 인시던트도 해결됩니다. 자세한 내용은 ServiceNow에서 AWS Systems Manager Incident Manager 통합을 참조하세요.	2022년 6월 9일

연락처 세부 정보 가져오기	인시던트가 생성되면 Incident Manager는 음성 또는 SMS 알림을 사용하여 대응 담당자에게 알릴 수 있습니다. 대응 담당자가 Incident Manager가 보낸 전화 또는 SMS 알림을 확인할 수 있도록 하려면 모든 대응담당자가 Incident Manager 가상 카드 형식 (.vcf) 파일을 모바일 디바이스의 주소록에 다운로드하는 것이 좋습니다. 자세한 내용은 주소록으로 연락처 세부 정보 가져오기를 참조하세요.	2022년 5월 18일

인시던트 생성 및 해결을 개선하기 위한 여러 기능의 개선 사항	Incident Manager는 인시던트 생성 및 해결을 개선하기 위해 다음과 같은 기능 개선 사항을 출시했습니다. • 다른 AWS 리전에서 인시던트 자동 생성: Amazon CloudWatch 또는 Amazon EventBridge가 인시던트를 생성할 때 AWS 리전 에서 Incident Manager를 사용할 수 없는 경우, 이제 이러한 서비스는 복제 세트에 지정된 가용 리전 중 하나에 인시던트를 자동으로 생성합니다. 자세한 내용은 크로스 리전 인시던트 관리를 참조하세요. • 런북 파라미터를 인시던트 메타데이터로 자동 채우기: 이제 인시던트에서 AWS 리소스에 대한 정보를 수집하도록 Incident Manager를 구성할 수 있습니다. 그러면 Incident Manager가 수집된 정보로 런북 파라미터를 채울 수 있습니다. 자세한 내용은 자습서: Incident Manager를 통한 Systems Manager 자동화 런북 사용을 참조하세요. • AWS 리소스 정보 자동 수집: 시스템에서 인시던트를 생성하면 이제 Incident Manager가 인시던트와 관련된 AWS 리소스에 대한 정보를 자동	2022년 5월 17일

	으로 수집합니다. 그러면 Incident Manager가 이 정보를 관련 항목 탭에 추가합니다.	
다중 런북 지원	Incident Manager는 이제 인시던트 세부 정보 페이지에서 인시던트 중에 여러 개의 런북을 실행할 수 있도록 지원합니다.	2022년 1월 14일
에서 Incident Manager 출시 AWS 리전	Incident Manager는 이제 새로운 리전 us-west-1, sa-east-1, ap-northeast-2, ap-south-1, ca-central-1, eu-west-2 및 eu-west-3에서 사용할 수 있습니다. Incident Manager 리전 및 할당량에 대한 자세한 내용은 AWS 일반 참조 참조 설명서를 참조하세요.	2021년 11월 8일
콘솔 참여 확인	이제 Incident Manager 콘솔에서 직접 참여를 확인할 수 있습니다.	2021년 8월 5일
속성 탭	Incident Manager는 인시던트 세부 정보 페이지에 속성 탭을 도입하여 인시던트, 상위 OpsItem 및 관련 인시던트 사후 분석에 대한 자세한 정보를 제공합니다.	2021년 8월 3일
Incident Manager 시작	Incident Manager는 사용자가 AWS 호스팅 애플리케이션에 영향을 미치는 인시던트를 완화하고 복구할 수 있도록 설계된 인시던트 관리 콘솔입니다.	2021년 5월 10일

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