사용자 가이드

AWS Audit Manager

AWS Audit Manager: 사용자 가이드

Table of Contents

AWS Audit Manager란 무엇인가요?

AWS Audit Manager 사용 설명서를 시작합니다.

AWS Audit Manager은 귀하가 위험을 관리하고 규정 및 업계 표준을 준수하는 방법을 간소화하기 위해 자신의 AWS 사용을 지속해서 감사할 수 있도록 지원합니다. Audit Manager는 증거 수집을 자동화하여 정책, 절차 및 활동(제어라고도 함)이 효과적으로 운영되는지 더욱 쉽게 평가할 수 있도록 합니다. 감사 시기에 Audit Manager는 귀하의 제어에 대한 이해 관계자들의 검토를 관리할 수 있습니다. 즉, 훨씬 적은 수작업으로 감사에 바로 사용할 수 있는 보고서를 작성할 수 있습니다.

Audit Manager는 지정된 규정 준수 표준 또는 규정에 대한 평가를 구조화하고 자동화하는 사전 구축된 프레임워크를 제공합니다. 프레임워크에는 설명 및 테스트 절차가 포함된 사전 구축된 제어 컬렉션이 포함됩니다. 이러한 제어는 지정된 규정 준수 표준 또는 규정의 요구 사항에 따라 그룹화됩니다. 또한 특정 요구 사항에 따라 내부 감사를 지원하도록 프레임워크와 제어를 사용자 지정할 수 있습니다.

모든 프레임워크에서 평가를 생성할 수 있습니다. 평가를 생성하면 Audit Manager가 자동으로 리소스 평가를 실행합니다. 이러한 평가는 감사 범위로 귀하가 정의한 AWS 계정 및 서비스 모두에 대한 데이터를 수집합니다. 수집된 데이터는 감사에 적합한 증거로 자동 변환됩니다. 그런 다음 보안, 변경 관리, 비즈니스 연속성 및 소프트웨어 라이선싱의 규정 준수를 입증하는 데 도움이 되도록 관련 제어에 첨부됩니다. 이 증거 수집 프로세스는 진행 중이며 평가를 작성할 때부터 시작됩니다. 감사를 완료하고 증거를 수집하는 데 Audit Manager가 더 이상 필요하지 않은 경우 증거 수집을 중단할 수 있습니다. 이렇게 하려면 평가 상태를 비활성으로 변경하세요.

Audit Manager 기능

AWS Audit Manager을 사용하여 다음 작업을 할 수 있습니다.

- 빠르게 시작 — 다양한 규정 준수 표준 및 규정을 지원하는 사전 구축된 프레임워크 갤러리에서 선택하여 첫 번째 평가를 작성하세요. 그런 다음 자동 증거 수집을 시작하여 귀하의 AWS 서비스 사용량을 감사하세요.
- 하이브리드 또는 멀티클라우드 환경에서 증거 업로드 및 관리 — Audit Manager가 귀하의 AWS 환경에서 수집하는 증거 외에도 온프레미스 또는 멀티클라우드 환경으로부터 취득한 증거를 업로드하고 중앙에서 관리할 수 있습니다.
- 공통 규정 준수 표준 및 규정 지원 — AWS Audit Manager표준 프레임워크 중 하나를 선택합니다. 이러한 프레임워크는 공통 규정 준수 표준 및 규정에 대한 사전 구축된 제어 매핑을 제공합니다. 여기에는 CIS 재단 벤치마크, PCI DSS, GDPR, HIPAA, SOC2, GxP 및 AWS 운영 모범 사례가 포함됩니다.

- 진행 중인 평가 모니터링 — Audit Manager 대시보드를 사용하여 귀하의 능동적 평가에 대한 분석 데이터를 보고 수정이 필요한 규정을 준수하지 않는 증거를 신속하게 식별할 수 있습니다.
- 증거 검색 — 증거 찾기 기능을 사용하여 검색 쿼리와 관련된 증거를 빠르게 찾을 수 있습니다. 검색 결과에서 평가 보고서를 생성하거나 검색 결과를 CSV 형식으로 내보낼 수 있습니다.
- 사용자 지정 제어 생성— 처음부터 직접 제어를 만들거나 필요에 맞게 기존 제어를 사용자 지정할 수 있습니다. 또한 사용자 지정 제어 기능을 사용하여 위험 평가 질문을 만들고 해당 질문에 대한 응답을 수동 증거로 저장할 수 있습니다.
- 프레임워크 사용자 지정 — 내부 감사에 대한 귀하의 특정 요구 사항에 따라 표준 또는 사용자 지정 제어를 사용하여 귀하 자신의 프레임워크를 생성할 수 있습니다.
- 사용자 지정 프레임워크 공유 — 사용자 지정 Audit Manager 프레임워크를 다른 AWS 계정과 공유하거나 귀하 자신의 AWS 리전 계정에 있는 다른 프레임워크에 복제할 수 있습니다.
- 팀 간 협업 지원 — 관련 증거를 검토하고, 의견을 추가하고, 각 제어의 상태를 업데이트할 수 있는 주제 전문가에게 제어 세트를 위임합니다.
- 감사자용 보고서 작성 — 감사를 위해 수집된 관련 증거를 요약하는 평가 보고서를 생성하고 자세한 증거가 포함된 폴더에 연결합니다.
- 증거 무결성 보장 — 증거를 변경하지 않고 안전한 장소에 보관하세요.

> **Note**
>
> AWS Audit Manager은 특정 규정 준수 표준 및 규정의 준수 여부를 확인하는 데 필요한 증거를 수집하는 데 도움이 됩니다. 하지만, 규정 준수 자체를 평가하지는 않습니다. 따라서, AWS Audit Manager를 통해 수집되는 증거에는 감사에 필요한 AWS 사용량에 대한 모든 정보가 포함되어 있지 않을 수 있습니다. AWS Audit Manager가 법률 고문이나 규정 준수 전문가를 대신하지는 못합니다.

Audit Manager 요금

요금에 대한 자세한 내용은 AWS Audit Manager 요금을 참조하세요.

Audit Manager를 처음 사용하나요?

Audit Manager 를 처음 사용하는 경우 아래 설명하는 페이지부터 시작하는 것이 좋습니다.

1. AWS Audit Manager 개념 및 용어 — 평가, 프레임워크, 제어 등 Audit Manager에서 사용되는 주요 개념 및 용어에 대해 알아봅니다.
2. AWS Audit Manager 증거 수집 방법 — Audit Manager가 리소스 평가를 위한 증거를 수집하는 방법에 대해 알아봅니다.
3. 설정 — Audit Manager의 설정 요구 사항에 대해 알아봅니다.
4. 시작하기 — 자습서를 따라 첫 번째 Audit Manager 평가를 작성하세요.
5. AWS Audit Manager API 참조 — Audit Manager API 작업 및 데이터 유형을 숙지하세요.

Audit Manager 리소스 추가

다음 리소스를 탐색하여 Audit Manager에 대해 더욱 자세히 알아봅니다.

- AWS Audit Manager를 사용하여 증거 수집 및 감사 데이터를 관리합니다.
- AWS워크샵에서 사용자 지정 Audit Manager 평가를 수동으로 구성하세요.
- AWS 관리 및 거버넌스 블로그에서 세 줄 모델 통합(2부): AWS Config 적합성 팩을 AWS Audit Manager 평가로 변환

AWS Audit Manager 개념 및 용어

시작하는 데 도움이 되도록 이 페이지에서는 AWS Audit Manager의 몇 가지 핵심 개념을 정의합니다.

A

A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z

평가

Audit Manager 평가를 사용하여 감사와 관련된 증거를 자동으로 수집할 수 있습니다.

평가는 감사와 관련된 제어 체계를 그룹화한 프레임워크를 기반으로 합니다. 비즈니스 요구 사항에 따라 표준 프레임워크 또는 사용자 지정 프레임워크에서 평가를 생성할 수 있습니다. 표준 프레임워크에는 특정 규정 준수 표준 또는 규정을 지원하는 사전 구축된 컨트롤 세트가 포함되어 있습니다. 반면, 사용자 지정 프레임워크에는 내부 감사 요구 사항에 따라 사용자 지정하고 그룹화할 수 있는 컨트롤 항목이 포함되어 있습니다. 프레임워크를 출발점으로 사용하여 귀하가 감사 범위에 포함하고자 하는 AWS 계정 및 서비스를 지정하는 평가를 작성할 수 있습니다.

평가를 작성하면 Audit Manager는 프레임워크에 정의된 제어를 기반으로 귀하의 AWS 계정의 리소스 및 서비스를 자동으로 평가하기 시작합니다. 그런 다음 관련 증거를 수집하여 감사자 친화적인 형식으로 변환합니다. 이를 수행한 이후, 평가 내 제어에 증거를 첨부합니다. 감사 시기가 되면 사용자 또는 사용자가 선택한 대리인이 수집한 증거를 검토한 다음 평가 보고서에 추가할 수 있습니다. 이 평가 보고서는 제어가 의도한 대로 작동하고 있음을 입증하는 데 도움이 됩니다.

증거 수집은 평가를 생성할 때 시작되는 지속적인 프로세스입니다. 귀하는 평가 상태를 비활성으로 변경하여 증거 수집을 중지할 수 있습니다. 또는 제어 수준에서 증거 수집을 중지할 수 있습니다. 평가 내의 특정 제어 상태를 비활성으로 변경하여 이 작업을 수행할 수 있습니다.

평가 생성 및 관리 방법에 대한 지침은 AWS Audit Manager에서의 평가 섹션을 참조하세요.

평가 보고서

평가 보고서는 Audit Manager 평가를 통해 생성된 최종 문서입니다. 이 보고서에는 감사를 위해 수집된 관련 증거가 요약되어 있습니다. 이 보고서는 관련 증거 폴더로 연결됩니다. 귀하의 평가에 지정된 제어 항목에 따라 폴더의 이름과 구성이 지정됩니다. 각 평가에 대해 귀하는 Audit Manager가 수집하는 증거를 검토하고 평가 보고서에 포함할 증거를 결정할 수 있습니다.

평가 보고서에 대한 보다 상세한 내용은 평가 보고서 섹션을 참조하세요. 평가 보고서를 생성하는 방법을 알아보려면 평가 보고서 생성 섹션을 참조하세요.

평가 보고서 대상

평가 보고서 대상은 Audit Manager가 평가 보고서를 저장하는 기본 S3 버킷입니다. 자세한 내용은 평가 보고서 목적지(선택 사항) 섹션을 참조하세요.

감사

감사는 조직의 자산, 운영 또는 비즈니스 무결성을 독립적으로 검사하는 것입니다. 정보 기술 (IT) 감사는 특히 조직의 정보 시스템 내에 있는 제어를 검사합니다. IT 감사의 목표는 정보 시스템이 자산을 보호하고, 효과적으로 운영되며, 데이터 무결성을 유지하는지 확인하는 것입니다. 이러한 모든 사항은 규정 준수 표준 또는 규정에서 요구하는 규제 요구 사항을 충족하는 데 중요합니다.

감사 소유자

감사 소유자라는 용어는 상황에 따라 두 가지 다른 의미를 갖습니다.

Audit Manager의 맥락에서 감사 소유자는 평가 및 관련 리소스를 관리하는 사용자 또는 역할입니다. 이 Audit Manager 인격체의 책임에는 평가 작성, 증거 검토 및 평가 보고서 생성이 포함됩니다. Audit Manager는 협업 서비스이며, 다른 이해 관계자가 평가에 참여하면 감사 소유자가 혜택을 누릴 수 있습니다. 예를 들어 평가에 다른 감사 소유자를 추가하여 관리 작업을 공유할 수 있습니다.

또는 감사 담당자로서 제어를 위해 수집된 증거를 해석하는 데 도움이 필요한 경우 해당 분야에 대한 주제 전문 지식을 갖춘 이해 관계자에게 제어 세트를 위임할 수 있습니다. 이러한 사람을 대리인 인격체라고 합니다.

비즈니스 측면에서 감사 소유자는 회사의 감사 준비 노력을 조정 및 감독하고 감사자에게 증거를 제시하는 사람입니다. 일반적으로 이들은 규정 준수 책임자 또는 GDPR 데이터 보호 책임자와 같은 GRC(거버넌스, 위험 및 규정 준수) 전문가입니다. GRC 전문가는 감사 준비를 관리할 수 있는 전문 지식과 권한을 보유하고 있습니다. 보다 구체적으로 말하자면, 이들은 규정 준수 요구 사항을 이해하고 보고 데이터를 분석, 해석 및 준비할 수 있습니다. 그러나 다른 비즈니스 역할도 감사 소유자인 Audit Manager 인격체를 맡을 수 있습니다. GRC 전문가만이 이 역할을 맡는 것이 아닙니다. 예를 들어, 아래 나열한 팀 중 한 곳의 기술 전문가가 Audit Manager 평가를 설정하고 관리하도록 선택할 수 있습니다.

- SecOps
- IT/DevOps
- 보안 운영 센터/사고 대응팀
- 클라우드 자산을 소유, 개발, 개선 및 배포하고 조직의 클라우드 인프라를 이해하는 유사한 팀

Audit Manager 평가에서 누구를 감사 소유자로 선택하여 지정할 것인지는 귀하의 조직에 따라 크게 달라집니다. 또한 보안 운영 구조 및 감사 세부 사항에 따라서도 달라집니다. Audit Manager에서는 동일한 개인이 한 평가에서는 감사 소유자 인격체를, 다른 평가에서는 대리인 인격체를 떠맡을 수 있습니다.

Audit Manager로 이용할 사람을 어떻게 선택하든 감사 소유자/대리인 인격체를 사용하고 각 사용자에게 특정 IAM 정책을 부여함으로써 귀하의 조직 전체에 걸쳐 업무 분리를 관리할 수 있습니다. Audit Manager는 이 2단계 접근 방식을 통해 귀하가 개별 평가의 모든 세부 사항을 완벽하게 제어할 수 있도록 합니다. 자세한 내용은 AWS Audit Manager에서의 사용자 페르소나에 대한 권장 정책을 참조하세요.

C

A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z

Changelog

Audit Manager는 평가의 각 제어에 대해 변경 로그를 캡처하여 해당 제어에 대한 사용자 활동을 추적합니다. 그런 다음 특정 제어와 관련된 활동의 감사 기록을 검토할 수 있습니다. 변경 로그에 캡처되는 사용자 활동에 대한 자세한 내용은 Changelog 탭 섹션을 참조하세요.

클라우드 규정 준수

클라우드 규정 준수는 클라우드 제공 시스템이 클라우드 고객이 직면한 표준을 준수해야 한다는 일반 원칙입니다.

규정 준수 규정

규정 준수 규정은 일반적으로 행위를 규제하기 위해 기관에서 규정하는 법률, 규칙 또는 기타 명령입니다. 한 가지 예는 GDPR입니다.

규정 준수 표준

규정 준수 표준은 확립된 규정, 사양 또는 법률에 따라 조직을 유지하기 위한 조직의 프로세스를 자세히 설명하는 일련의 구조화된 지침입니다. PCI DSS 및 HIPAA를 예로 들 수 있습니다.

제어

제어는 정보 시스템 또는 조직을 위해 규정된 보호 장치 또는 대응책입니다. 제어는 정보의 기밀성, 무결성 및 가용성을 보호하고 정의된 일련의 보안 요구 사항을 충족하도록 설계되었습니다. 이를 통해 리소스가 의도한 대로 운영되고, 데이터가 신뢰할 수 있으며, 조직이 관련 법률 및 규정을 준수하고 있음을 확인할 수 있습니다.

Audit Manager에서 제어는 공급업체 위험 평가 설문지의 질문을 나타낼 수도 있습니다. 이 경우 제어는 조직의 보안 및 규정 준수 태세에 대한 정보를 묻는 특정 질문입니다.

제어는 Audit Manager 평가에서 활성화될 때 지속적으로 증거를 수집합니다. 모든 제어에 증거를 수동으로 추가할 수도 있습니다. 각 증거는 귀하가 제어 요건 준수를 입증하는 데 도움이 되는 기록이 됩니다.

Audit Manager에는 두 가지 유형의 제어가 있습니다.

- 표준 제어 — Audit Manager의 특정 프레임워크와 연결된 사전 확립된 제어입니다. 표준 제어를 사용하면 다양한 규정 준수 표준 및 규정에 대한 감사 준비를 지원할 수 있습니다.
- 사용자 지정 제어 — Audit Manager 사용자로 정의하는 사용자 지정 제어입니다. 사용자 지정 제어를 사용하면 내부 감사 또는 공급업체 위험 평가를 위한 특정 규정 준수 요구 사항을 충족하는 데 도움이 됩니다.

자세한 내용은 AWS Audit Manager 제어 예제를 참조하세요. 제어를 생성하고 관리하는 방법에 관한 지침은 컨트롤 라이브러리 섹션을 참조하세요.

제어 도메인

제어 도메인은 특정 프레임워크에만 국한되지 않는 일반적인 제어 범주로 생각할 수 있습니다. 제어 도메인 그룹화는 Audit Manager 대시보드의 가장 강력한 기능 중 하나입니다. Audit Manager는

평가에서 규정을 준수하지 않는 증거가 있는 제어 항목을 강조 표시하고 제어 도메인별로 그룹화합니다. 이를 통해 귀하는 감사를 준비하면서 특정 주제 영역에 대응 노력을 집중할 수 있습니다.

> **Note**
>
> 제어 도메인은 제어 세트와 다릅니다. 제어 세트는 일반적으로 규제 기관에서 정의하는 프레임워크별 제어 그룹입니다. 예를 들어, PCI DSS 프레임워크에는 요구 사항 8: 시스템 구성 요소에 대한 액세스 식별 및 인증이라는 제어 세트가 있습니다. 이 제어 세트는 ID 및 액세스 관리의 제어 도메인에 속합니다.

Audit Manager는 제어를 다음과 같은 제어 도메인에 따라 분류합니다.

제어 도메인 이름	이러한 제어가 규제하는 내용에 대한 설명
비즈니스 연속성 및 비상 계획	주요 시스템 및 네트워크 중단의 영향으로부터 중요한 비즈니스 운영을 보호하는 프로세스를 수립하는 방법
변경 관리	클라우드 인프라의 변경 사항을 테스트, 승인, 구현 및 문서화하는 방법
데이터 보안 및 개인정보 보호	데이터의 프라이버시, 가용성, 무결성을 보호하는 방법.
개발 및 구성 관리	클라우드 인프라를 바람직하고 일관된 상태로 유지하는 방법.
거버넌스 및 감독	클라우드 컴퓨팅 사용을 법률, 규제 및 윤리적 의무에 맞추는 방법.
ID 및 액세스 관리	적합한 사용자가 귀하의 기술 리소스에 적절하게 액세스할 수 있도록 하는 방법
인시던트 관리	보안 인시던트에 신속하고 효과적으로 대응할 수 있는 책임과 절차를 설정하는 방법
로깅 및 모니터링	사용자 활동을 검토하여 무단 활동이 시도되거나 수행되었다는 징후가 있는지 확인하는 방법
네트워크 관리	네트워크 관리 시스템을 사용하여 데이터 네트워크를 관리하고 운영하는 방법.
인사 관리	조직 수준에서 직원 보안 위험을 평가하고 관리하는 방법.

제어 도메인 이름	이러한 제어가 규제하는 내용에 대한 설명
물리적 보안	시설의 물리적 보안 문제를 감지하고 예방하는 방법.
위험 관리	잠재적 위험과 손실을 평가하는 방법, 그리고 그러한 위협을 줄이거나 없애는 방법
공급망 관리	IT 제품, 공급업체 및 공급망과 관련된 위험을 식별, 평가 및 완화하는 방법.
사용자 장치 관리	직원의 IT 하드웨어가 분실, 손상 또는 손상될 위험을 줄이는 방법.
취약성 관리	귀하의 클라우드 인프라 내 자산에 대해 알려진 모든 취약성을 정의, 평가 및 해결하는 방법

D

A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z

데이터 소스

Audit Manager는 데이터 소스를 사용하여 제어에 대한 증거를 수집합니다. 다음 용어는 데이터 소스의 정의 및 작동 방식을 설명합니다.

- 데이터 소스 유형은 Audit Manager가 제어에 대한 증거를 수집하는 위치를 정의합니다. 사용자만의 고유 증거를 업로드하는 경우, 데이터 소스 유형은 수동입니다. Audit Manager가 사용자를 대신하여 증거를 수집하는 경우 데이터 소스 유형은 AWS Security Hub, AWS Config, AWS CloudTrail, 또는 AWS API 직접 호출 중 하나입니다. Audit Manager API는 데이터 소스 유형을 sourceType(단수) 또는 controlSources(복수)라고 합니다.
- 매핑은 데이터 소스 유형과 관련된 특정 키워드입니다. 예를 들어 CloudTrail 이벤트 이름 또는 AWS Config 이름일 수 있습니다. Audit Manager API에서는 이를 sourceKeyword(단수) 또는 controlMappingSources(복수형)라고 합니다.
- 데이터 소스 이름은 데이터 소스에 부여되는 이름입니다. 즉, 데이터 소스 이름은 데이터 소스 유형과 매핑의 조합에 라벨을 지정합니다. 표준 제어의 경우 Audit Manager는 기본 데이터 소스 이름 (예: 데이터 소스 1 및 데이터 소스 2) 을 제공합니다. 사용자 지정 제어의 경우 고유한 데이터 소스 이름을 제공할 수 있습니다. 이렇게 하면 동일한 데이터 소스 유형에 속하는 여러 매핑을 구별하는 데 도움이 될 수 있습니다. Audit Manager API는 데이터 소스 이름을 sourceName이라고 합니다.

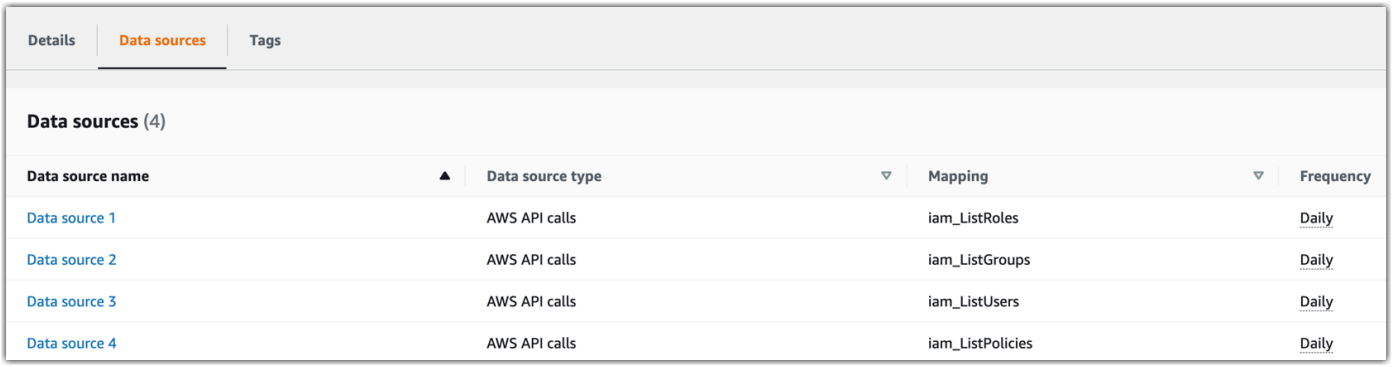
단일 제어에 여러 데이터 소스 유형과 여러 매핑이 있을 수 있습니다. 예를 들어 하나의 제어가 여러 데이터 소스 유형 (예: AWS Config 및 Security Hub) 에서 증거를 수집할 수 있습니다. 또 다른 제어는 여러 AWS Config 규칙을 매핑으로 사용하는 유일한 데이터 소스 유형으로서 AWS Config을 가질 수 있습니다.

다음 표에는 자동화된 데이터 소스 유형이 나열되어 있으며 일부 해당 매핑의 예가 나와 있습니다.

데이터 소스 유형	설명	매핑 예제
AWS Security Hub	이 데이터 소스 유형을 사용하여 리소스 보안 상태의 스냅샷을 캡처할 수 있습니다. Audit Manager는 Security Hub 제어의 이름을 매핑 키워드로 사용하고 해당 보안 검사의 결과를 Security Hub에서 직접 보고합니다.	`1.1 – Avoid the use of the "root" account`
AWS Config	이 데이터 소스 유형을 사용하여 리소스 보안 상태의 스냅샷을 캡처할 수 있습니다. Audit Manager는 AWS Config 규칙 이름을 매핑 키워드로 사용하고 해당 규칙 검사 결과를 AWS Config에서 직접 보고합니다.	`EC2_INSTANCE_MANAGED_BY_SSM`
AWS CloudTrail	이 데이터 소스 유형을 사용하면 감사에 필요한 특정 사용자 활동을 추적할 수 있습니다. Audit Manager는 CloudTrail 이벤트 이름을 매핑 키워드로 사용하고 CloudTrail 로그에서 관련 사용자 활동을 수집합니다.	`CreateAccessKey`
AWS API 직접 호출	이 데이터 소스 유형을 사용하면 특정 AWS 서비스에 대한	`ec2_DescribeSecurityGroups`

데이터 소스 유형	설명	매핑 예제
	API 직접 호출을 통해 리소스 구성의 스냅샷을 찍을 수 있습니다. Audit Manager는 API 직접 호출 이름을 매핑 키워드로 사용하고 API 응답을 수집합니다.	

다음 이미지는 Audit Manager 콘솔에 표시된 다양한 데이터 소스의 예를 보여줍니다.



> **Note**
>
> 일부 데이터 소스 유형이 AWS 서비스이긴 하지만, 데이터 소스 유형은 서비스 범위마다 다릅니다. 자세한 내용은 본 안내서의 문제 해결 섹션에서 서비스 범위와 데이터 소스 유형의 차이는 무엇인가요?를 참조하세요.

위임

대리인은 권한이 제한된 AWS Audit Manager 사용자입니다. 대리인은 일반적으로 전문적인 비즈니스 또는 기술 전문 지식을 갖추고 있습니다. 예를 들어, 이러한 전문 지식은 데이터 보존 정책, 교육 계획, 네트워크 인프라 또는 ID 관리 등에 관한 것일 수 있습니다. 대리인은 감사 담당자가 수집된 증거를 검토하여 자신의 전문 분야에 적용되는 규제 항목을 검토할 수 있도록 지원합니다. 대리인은 제어 세트 및 관련 증거를 검토하고, 의견을 추가하고, 추가 증거를 업로드하고, 검토를 위해 할당한 각 규제 항목의 상태를 업데이트할 수 있습니다.

감사 소유자는 전체 평가가 아닌 특정 제어 세트를 대리인에게 할당합니다. 따라서 대리인은 평가에 대한 제한된 액세스 권한을 가집니다. 제어 세트를 위임하는 방법에 대한 지침은 AWS Audit Manager에서의 위임 섹션을 참조하세요.

E

A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z

Evidence

증거는 제어 요건 준수를 입증하는 데 필요한 정보가 들어 있는 기록입니다. 증거의 예로는 사용자가 호출한 변경 활동, 시스템 구성 스냅샷 등이 있습니다.

Audit Manager에는 자동 증거와 수동 증거의 두 가지 주요 유형이 있습니다.

- 자동 증거 — Audit Manager가 자동으로 수집하는 증거입니다. 여기에는 다음과 같은 세 가지 범주의 자동 증명이 포함됩니다.
  - 규정 준수 검사 — 규정 준수 검사 결과는 AWS Security Hub, AWS Config, 또는 두 가지 모두에서 포착됩니다. 규정 준수 검사의 예로는 PCI DSS 제어에 대한 Security Hub의 보안 검사 결과, HIPAA 제어에 대한 AWS Config 규칙 평가 등이 있습니다. 자세한 내용은 AWS Audit Manager에 의해 지원되는 AWS Config 규칙 및 AWS Audit Manager에 의해 지원되는 AWS Security Hub제어를 참조하세요.
  - 사용자 활동 — 리소스 구성을 변경하는 사용자 활동은 해당 활동이 발생하는 즉시 CloudTrail 로그에서 포착됩니다. 사용자 활동의 예로는 라우팅 테이블 업데이트, Amazon RDS 인스턴스 백업 설정 변경, S3 버킷 암호화 정책 변경 등이 있습니다. 자세한 내용은 AWS Audit Manager에 의해 지원되는 AWS CloudTrail 이벤트 이름을 참조하세요.
  - 구성 데이터 - 리소스 구성의 스냅샷은 일별, 주별 또는 월별로 AWS 서비스로부터 직접 캡처됩니다. 구성 스냅샷의 예로는 VPC 라우팅 테이블의 경로 목록, Amazon RDS 인스턴스 백업 설정, S3 버킷 암호화 정책 등이 있습니다. 자세한 내용은 AWS Audit Manager이 지원하는 API 직접 호출을 참조하세요.
- 수동 증거 — Audit Manager에 직접 추가하는 증거입니다. 다음과 같은 세 가지 방법으로 증거를 추가할 수 있습니다.
  - Amazon S3에서 파일 가져오기
  - 브라우저에서 파일 업로드
  - 위험 평가 질문에 대한 텍스트 응답 입력

  자세한 내용은 AWS Audit Manager에서 수동 증거 추가 섹션을 참조하세요.

평가를 생성하면 자동 증거 수집이 시작됩니다. 이는 진행 중인 프로세스이며, Audit Manager는 증거 유형 및 기본 데이터 소스에 따라 다양한 빈도로 증거를 수집합니다. 증거 모음에 대한 자세한 내용은 AWS Audit Manager 증거 수집 방법 섹션을 참조하세요. 평가에서 증거를 검토하는 방법에 대한 지침은 평가에서 증거 검토하기 섹션을 참조하세요.

증거 수집 방법

제어가 증거를 수집할 수 있는 두 가지 방법이 있습니다.

- 자동화된 제어는 AWS 데이터 소스에서 증거를 자동으로 수집합니다. 이 자동화된 증거는 제어 기능의 전체 또는 부분 준수를 입증하는 데 도움이 될 수 있습니다.
- 수동 제어를 위해서는 제어 준수를 입증할 수 있는 귀하 자신의 증거를 업로드해야 합니다.

> **Note**
>
> 모든 자동 제어에 수동 증거를 첨부할 수 있습니다. 대부분의 경우 제어 기능의 완전한 준수를 입증하려면 자동 증거의 조합과 수동 증거의 조합이 필요합니다. Audit Manager는 유용하고 관련성이 높은 자동 증거를 제공할 수 있지만 일부 자동 증거는 부분적인 규정 준수만 입증할 수 있습니다. 이 경우 Audit Manager에서 제공하는 자동 증거를 귀하 자신의 증거로 보완할 수 있습니다.
>
> 예:
>
> - AWS 생성형 AI 모범 사례 프레임워크는 `Error analysis`이라는 제어를 포함합니다. 이 제어를 사용하려면 모델 사용에서 부정확성이 감지되는 시점을 식별해야 합니다. 또한 귀하는 철저한 오류 분석을 수행하여 근본 원인을 파악하고 수정 조치를 취해야 합니다.
> - 이러한 제어를 지원하기 위해 Audit Manager는 평가가 실행되는 AWS 계정을 위해 CloudWatch 경보가 활성화되었는지 여부를 보여주는 자동 증거를 수집합니다. 이 증거를 사용하여 경고 및 확인이 올바르게 구성되었음을 증명함으로써 제어 기능의 부분적 준수를 입증할 수 있습니다.
> - 완전한 규정 준수를 입증하기 위해 자동 증거를 수동 증거로 보완할 수 있습니다. 예를 들어 오류 분석 프로세스, 에스컬레이션 및 보고 임계값, 근본 원인 분석 결과를 보여주는 정책 또는 절차를 업로드할 수 있습니다. 이 수동 증거를 사용하여 기존의 확립된 정책이 시행되고 있으며 시정 조치가 취해졌음을 입증할 수 있습니다.
>
> 자세한 예는 혼합 데이터 소스를 사용한 제어를 참조하세요.

내보내기 대상

내보내기 대상은 증거 찾기에서 귀하가 내보낸 파일을 Audit Manager가 저장하는 기본 S3 버킷입니다. 자세한 내용은 내보내기 대상(선택 사항) 섹션을 참조하세요.

F

A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z

프레임워크

Audit Manager 프레임워크는 특정 표준 또는 위험 거버넌스 원칙에 대한 평가를 구조화하고 자동화하는 데 사용되는 파일입니다. 이러한 프레임워크를 통해 AWS 리소스를 제어 요건에 맞게 매핑할 수 있습니다. 여기에는 사전 구축된 제어 또는 고객이 정의한 제어 컬렉션이 포함됩니다. 컬렉션에는 각 제어에 대한 설명과 테스트 절차가 있습니다. 이러한 제어는 지정된 규정 준수 표준 또는 규정의 요구 사항에 따라 구성 및 그룹화됩니다. 예로는 PCI, DSS, GDPR 등이 있습니다.

Audit Manager 에는 두 가지 유형의 프레임워크가 있습니다.

- 표준 프레임워크 — 다양한 규정 준수 표준 및 규정의 AWS 모범 사례를 기반으로 사전 구축된 프레임워크입니다. 이러한 프레임워크를 사용하여 감사 준비를 지원할 수 있습니다.
- 사용자 지정 프레임워크 - Audit Manager 사용자로 귀하가 정의하는 사용자 지정 프레임워크입니다. 이러한 프레임워크를 사용하여 특정 규정 준수 또는 위험 관리 요구 사항에 따른 감사 준비를 지원할 수 있습니다.

프레임워크 생성 설치 및 관리 방법에 대한 지침은 프레임워크 라이브러리 섹션을 참조하세요.

> **Note**
>
> AWS Audit Manager은 특정 규정 준수 표준 및 규정의 준수 여부를 확인하는 데 필요한 증거를 수집하는 데 도움이 됩니다. 하지만, 규정 준수 자체를 평가하지는 않습니다. 따라서, AWS Audit Manager를 통해 수집되는 증거에는 감사에 필요한 AWS 사용량에 대한 모든 정보가 포함되어 있지 않을 수 있습니다. AWS Audit Manager가 법률 고문이나 규정 준수 전문가를 대신하지는 못합니다.

프레임워크 공유

Audit Manager의 사용자 지정 프레임워크 공유 기능을 사용하여 여러 AWS 계정 지역 간에 사용자 지정 프레임워크를 빠르게 공유할 수 있습니다. 사용자 지정 프레임워크를 공유하려면 공유 요청을 생성합니다. 그러면 공유 요청 수신자는 120일 이내에 요청을 수락하거나 거부해야 합니다. 승인하면 Audit Manager는 공유된 사용자 지정 프레임워크를 해당 프레임워크 라이브러리에 복제합니다. Audit Manager는 사용자 지정 프레임워크를 복제하는 것 외에도 해당 프레임워크에 포함된 모든 사용자 지정 제어 집합 및 제어를 복제합니다. 이러한 사용자 지정 제어는 수신자의 제어 라이브러

리에 추가됩니다. Audit Manager는 표준 프레임워크 또는 컨트롤을 복제하지 않습니다. 이러한 리소스는 기본적으로 각 계정 및 지역에서 이미 사용 가능하기 때문입니다.

R

A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z

리소스

리소스는 감사를 통해 평가되는 물리적 또는 정보 자산입니다. AWS 리소스의 예로는 Amazon EC2 인스턴스, Amazon RDS 인스턴스, Amazon S3 버킷, Amazon VPC 서브넷 등이 포함됩니다.

리소스 평가

자원 평가는 개별 자원을 평가하는 프로세스입니다. 이 평가는 제어 요구 사항을 기반으로 합니다. 평가가 활성화되어 있는 동안 Audit Manager는 평가 범위 내의 각 개별 자원에 대해 자원 평가를 실행합니다. 리소스 평가는 다음과 같은 과업 세트를 실행합니다.

1. 리소스 구성, 이벤트 로그, 조사 결과를 포함한 증거를 수집합니다.
2. 증거를 변환하여 제어 시스템에 매핑합니다.
3. 증거의 계보를 저장 및 추적하여 무결성을 확보합니다.

리소스 규정 준수

리소스 규정 준수란 규정 준수 확인 증거를 수집할 때 평가된 리소스의 평가 상태를 말합니다.

Audit Manager는 데이터 소스 유형으로 AWS Config와 Security Hub를 사용하는 제어의 규정 준수 검사 증거를 수집합니다. 이 증거 수집 과정에서 여러 리소스가 평가될 수 있습니다. 따라서 단일 규정 준수 검사 증거에는 하나 이상의 리소스가 포함될 수 있습니다.

증거 찾기의 리소스 규정 준수 필터를 사용하여 리소스 수준에서 규정 준수 상태를 탐색할 수 있습니다. 검색이 완료되면 검색 쿼리와 일치하는 리소스를 미리 볼 수 있습니다.

증거 찾기에서 리소스 규정 준수에 사용할 수 있는 값은 세 가지입니다.

- 비준수 — 규정 준수 검사와 관련된 문제가 있는 리소스를 말합니다. 이는 Security Hub가 리소스에 대한 실패 결과를 보고하거나 비준수 결과를 AWS Config 보고하는 경우에 발생합니다.
- 규정 준수 — 규정 준수 검사 문제가 없는 리소스를 말합니다. 이는 Security Hub가 리소스에 대한 합격 결과를 보고하거나 규정 준수 결과를 AWS Config 보고하는 경우에 발생합니다.
- 결정 유보 — 규정 준수 검사를 사용할 수 없거나 적용할 수 없는 리소스를 말합니다. 이는 AWS Config 또는 Security Hub가 기저의 데이터 소스 유형이지만 해당 서비스가 활성화되지 않은 경

우 발생합니다. 이는 기저의 데이터 소스 유형이 규정 준수 검사 (예: 수동 증거, AWS API 직접 호출 또는 CloudTrail) 를 지원하지 않는 경우에도 발생합니다.

S

A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z

서비스 범위 내 서비스

귀하의 평가 범위에 포함된 AWS 서비스입니다. 서비스를 평가 범위에 포함하도록 지정하면 Audit Manager가 해당 서비스의 리소스를 평가합니다. Audit Manager는 범위 내에서 서비스의 다양한 리소스를 평가할 수 있습니다. 리소스의 예로서는 다음과 같은 항목들이 있습니다.

- Amazon EC2 인스턴스
- S3 버킷
- 사용자 또는 역할
- DynamoDB 테이블
- Amazon Virtual Private Cloud(VPC), 보안 그룹 또는 네트워크 액세스 제어 목록(ACL) 테이블과 같은 네트워크 구성 요소

Audit Manager 콘솔을 사용하여 표준 프레임워크에서 평가를 만들거나 업데이트하는 경우 기본적으로 범위 내 AWS 서비스 목록이 미리 선택됩니다. 이 목록은 편집할 수 없습니다. 이는 Audit Manager가 자동으로 데이터 소스 및 서비스를 매핑하고 선택하기 때문입니다. 이 선택은 표준 프레임워크의 요구 사항에 따라 이루어집니다. 표준 프레임워크가 수동 제어만 포함하는 경우, AWS 서비스는 평가 범위에 포함되지 않으며, 귀하는 평가에 어떤 서비스도 추가할 수 없습니다.

이 프레임워크의 범위 내에서 서비스 목록을 편집해야 하는 경우 CreateAssessment 또는 UpdateAssessment API 작업을 사용하여 편집할 수 있습니다. 또는 표준 프레임워크를 사용자 지정한 다음 사용자 지정 프레임워크에서 평가를 생성할 수도 있습니다.

> **Note**
>
> 범위 내 서비스는 데이터 소스 유형과는 다르며, 데이터 소스 유형 역시 AWS 서비스이거나 아니면 다른 것일 수도 있습니다. 자세한 내용은 본 안내서의 문제 해결 섹션에서 서비스 범위와 데이터 소스 유형의 차이는 무엇인가요?를 참조하세요.

AWS Audit Manager 증거 수집 방법

AWS Audit Manager에서의 각 활성 평가는 다양한 데이터 소스에서 증거를 자동으로 수집합니다. 모든 평가에는 Audit Manager가 데이터를 수집하는 AWS 서비스 및 계정을 지정하는 정의된 범위가 있습니다. 범위 내에 정의된 서비스 및 계정 각각에는 여러 리소스가 포함되며 각 리소스는 귀하가 소유한 시스템 자산 인벤토리입니다. Audit Manager의 증거 수집에는 각 범위 내 리소스에 대한 평가가 포함됩니다. 이를 리소스 평가라고 합니다.

다음 단계는 Audit Manager가 각 자원 평가에 대한 증거를 수집하는 방법을 설명합니다.

1. 데이터 소스에서 리소스 평가

증거 수집을 시작하기 위해 Audit Manager는 데이터 소스에서 범위 내 리소스를 평가합니다. 구성 스냅샷, 관련 규정 준수 검사 결과 및 모든 사용자 활동을 캡처하여 이를 수행합니다. 그런 다음 분석을 실행하여 이 데이터가 지원하는 제어를 결정합니다. 그런 다음 리소스 평가 결과를 저장하고 증거로 변환합니다. 다양한 증거 유형에 대한 자세한 내용은 이 안내서의 AWS Audit Manager 개념 및 용어 섹션에 있는 증거를 참조하세요.

2. 평가 결과를 증거로 전환

리소스 평가 결과에는 해당 리소스에서 캡처한 원본 데이터와 데이터가 지원하는 제어를 나타내는 메타데이터가 모두 포함됩니다. AWS Audit Manager은 원본 데이터를 감사자가 쉽게 이해할 수 있는 형식으로 변환합니다. 그런 다음 변환된 데이터와 메타데이터는 제어에 첨부되기 전에 Audit Manager 증거로 저장됩니다.

3. 관련 제어에 증거 첨부

Audit Manager는 증거 메타데이터를 읽습니다. 그런 다음 저장된 증거를 평가 내 관련 제어에 첨부합니다. 첨부된 증거는 Audit Manager에서 확인할 수 있습니다. 이로써 리소스 평가 주기가 완료됩니다.

> **Note**
>
> 제어 구성에 따라 경우에 따라 여러 Audit Manager 평가를 통해 여러 제어 항목에 동일한 증거를 첨부할 수 있습니다. 여러 제어 항목에 동일한 증거가 첨부되면 Audit Manager는 리소스 평가를 정확히 한 번 측정합니다. 이는 동일한 증거가 정확히 한 번만 수집되기 때문입니다. 그러나 Audit Manager 평가 내 하나의 제어에 여러 데이터 소스의 여러 증거가 포함될 수 있습니다.

증거 수집 빈도

증거 수집은 평가를 생성할 때 시작되는 지속적인 프로세스입니다. AWS Audit Manager는 다양한 빈도로 여러 데이터 소스에서 증거를 수집합니다. 그 결과, 증거 수집 빈도에 대해 모든 경우에 통용되는 한 가지 답을 제시할 수는 없습니다. 증거 수집 빈도는 아래에 설명된 대로 증거 유형과 데이터 출처를 기반으로 합니다.

- 규정 준수 검사 — Audit Manager는 AWS Security Hub 및 AWS Config에서 이 증거 유형을 수집합니다.
  - AWS Security Hub은 증거 수집 빈도는 Security Hub 검사 일정을 따릅니다. Security Hub 검사 일정에 대한 자세한 내용은 AWS Security Hub 사용 안내서의 보안 검사 실행 일정을 참조하세요. Audit Manager 에서 지원하는 Security Hub 검사에 대한 자세한 내용은 AWS Security Hub 에서 지원하는 제어 AWS Audit Manager 섹션을 참조하세요.
  - AWS Config는 증거 수집 빈도는 귀하의 AWS Config 규칙에 정의된 트리거를 따릅니다. AWS Config 규칙 트리거에 대한 자세한 내용은 AWS Config 사용 설명서의 트리거 유형을 참조하세요. Audit Manager가 지원하는 AWS Config 규칙에 대한 자세한 내용은 AWS Config 규칙 에서 지원됩니다. AWS Audit Manager 섹션을 참조하세요.
- 사용자 활동 — Audit Manager는 이러한 증거 유형을 AWS CloudTrail로부터 지속적으로 수집합니다. 사용자 활동은 하루 중 언제라도 발생할 수 있으므로 이 빈도는 계속됩니다. 자세한 내용은 AWS CloudTrail 에서 지원하는 이벤트 이름 AWS Audit Manager 섹션을 참조하세요.
- 구성 데이터 — Audit Manager는 Amazon EC2, Amazon S3 또는 IAM과 AWS 서비스 같은 다른 API에 대한 설명 API 직접 호출을 사용하여 이 증거 유형을 수집합니다. 호출할 API 작업을 선택할 수 있습니다. 또한 Audit Manager에서 빈도를 일별, 주별 또는 월별로 설정할 수 있습니다. 제어 라이브러리에서 제어를 만들거나 편집할 때 이 빈도를 지정할 수 있습니다. 제어를 편집 혹은 생성하는 방법에 대한 지침은 컨트롤 라이브러리 섹션을 참조하세요. Audit Manager가 API 직접 호출을 사용하여 증거를 생성하는 방법에 대한 자세한 내용은 에서 지원하는 API 호출 AWS Audit Manager 섹션을 참조하세요.

데이터 소스의 증거 수집 빈도에 관계없이 제어 및 평가가 활성화되어 있는 한 새로운 증거가 자동으로 수집됩니다.

AWS Audit Manager 제어의 예

이 페이지의 예제를 검토하여 AWS Audit Manager에서 제어가 작동하는 방식에 대해 자세히 알아볼 수 있습니다. 이 예제에서는 제어 수단의 형태, Audit Manager가 해당 제어에 대한 증거를 생성하는 방법, 규정 준수를 입증하기 위해 취할 수 있는 다음 단계를 설명합니다.

> **Tip**
>
> Audit Manager에서의 최적의 경험을 위해 AWS Config 및 AWS Security Hub를 활성화할 것이 권장됩니다. 이러한 서비스를 활성화하면 Audit Manager 평가에서 제어를 위한 데이터 소스 유형으로 사용할 수 있습니다. 즉, Audit Manager는 Security Hub 조사 결과를 사용하고 AWS Config 규칙 자동화된 증거를 생성할 수 있습니다.
>
> - AWS Security Hub활성화한 후에는 모든 보안 표준을 사용하도록 활성화하고 통합 제어 결과 설정을 켜야 합니다. 이 단계를 통해 Audit Manager는 지원되는 모든 규정 준수 표준에 대한 결과를 가져올 수 있습니다.
> - AWS Config활성화한 후에는 또한 관련 AWS Config 규칙을 활성화하거나 감사와 관련된 규정 준수 표준을 위한 적합성 팩을 배포해야 합니다. 이 단계를 통해 Audit Manager는 활성화한 모든 지원되는 AWS Config 규칙에 대한 결과를 들여올 수 있습니다.

다음 각 제어 유형에 대한 예를 사용할 수 있습니다.

주제

데이터 소스 유형으로 AWS Security Hub을 사용하는 자동화된 제어

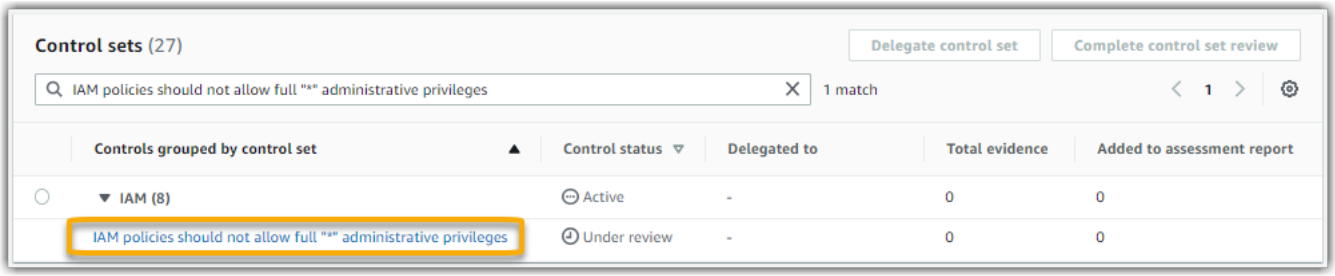
이 예제에서는 데이터 소스 AWS Security Hub 유형으로 사용하는 제어를 보여줍니다. 이는 AWS 기본 보안 모범 사례 (FSBP) 프레임워크에서 가져온 표준 제어입니다. Audit Manager는 이 제어 기능을 사용하여 AWS 환경을 FSBP 요구 사항에 맞추는 데 도움이 될 수 있는 증거를 생성합니다.

제어 세부 정보의 예

- 제어 이름 — `IAM policies should not allow full "*" administrative privileges`

- 제어 세트 — 이 제어는 IAM 제어 세트에 속합니다. ID 및 액세스 관리와 관련된 제어를 그룹화한 것입니다.
- 데이터 소스 유형 – AWS Security Hub
- 증거 유형 — 규정 준수 검사

다음 예제에서 이 제어는 FSBP 프레임워크에서 생성된 Audit Manager 평가 내에 있습니다.



평가에는 제어 상태가 표시됩니다. 또한 지금까지 이 제어에 대해 수집된 증거의 양과 평가 보고서에 포함된 증거의 양을 보여줍니다. 여기에서 제어 세트를 검토하도록 위임하거나 직접 검토를 완료할 수 있습니다. 제어 이름을 선택하면 해당 제어의 증거를 비롯한 자세한 정보가 포함된 세부 정보 페이지가 열립니다.

이 제어의 기능

Audit Manager는 이 제어 기능을 사용하여 IAM 정책이 너무 광범위해서 FSBP 요구 사항을 충족할 수 없는지 확인할 수 있습니다. 보다 구체적으로 말하자면, 고객 관리형 IAM 정책에 다음과 같은 와일드카드 명령문(`"Effect": "Allow"`with `"Action": "*"`over `"Resource": "*"`)이 포함된 관리자 액세스 권한이 있는지 확인할 수 있습니다.

Audit Manager가 이러한 제어에 대한 증거를 수집하는 방법

Audit Manager는 다음 단계를 수행하여 이 제어에 대한 증거를 수집합니다.

1. Audit Manager는 각 제어에 대해 범위 내 리소스를 평가합니다. 제어 설정에 지정된 데이터 소스를 사용하여 이 작업을 수행합니다. 이 예제에서 귀하의 IAM 정책은 리소스이며, Security Hub와 AWS Config는 데이터 소스 유형입니다. Audit Manager는 특정 Security Hub 검사([IAM.1])의 결과를 구하고, 그 다음 AWS Config 규칙을 사용하여 귀하의 IAM 정책(iam-policy-no-statements-with-admin-access)을 평가합니다.
2. 리소스 평가 결과는 저장되고 감사자 친화적인 증거로 변환됩니다. Audit Manager는 Security Hub를 데이터 소스 유형으로 사용하는 제어에 대한 규정 준수 검사 증거를 생성합니다. 이 증거에는 Security Hub에서 직접 보고한 규정 준수 검사 결과가 포함되어 있습니다.

3. Audit Manager는 저장된 증거를 `IAM policies should not allow full "*" administrative privileges`이라고 이름이 지정된 귀하의 평가 내 제어에 첨부합니다.

Audit Manager를 사용하여 이 제어 기능의 규정 준수를 입증하는 방법

증거가 제어 항목에 첨부되면 귀하 본인 또는 대리인이 증거를 검토하여 수정이 필요한지 확인할 수 있습니다.

이 예제에서 Audit Manager는 Security Hub의 실패 결정을 표시할 수 있습니다. 이는 IAM 정책에 와일드카드(*)가 포함되어 있고 너무 광범위해서 제어를 충족하지 못할 경우 발생할 수 있습니다. 이 경우 전체 관리자 권한을 허용하지 않도록 IAM 정책을 업데이트할 수 있습니다. 이를 위해 귀하는 사용자들이 수행해야 하는 작업을 파악한 후 사용자들이 해당 작업만 수행하도록 사용자에 대한 정책을 작성합니다. 이 수정 조치는 귀하의 AWS 환경을 FSBP 요구 사항에 맞추는 데 도움이 됩니다.

귀하의 IAM 정책이 제어에 부합하면 해당 제어를 검토됨으로 표시하고 평가 보고서에 증거를 추가하세요. 그런 다음 이 보고서를 감사자와 공유하여 제어가 의도한 대로 작동하고 있음을 입증할 수 있습니다.

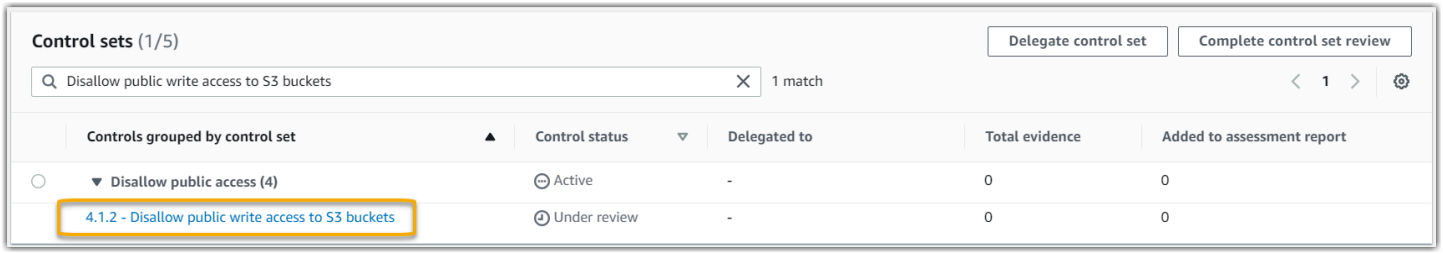
데이터 소스 유형으로 AWS Config을 사용하는 자동화된 제어

이 예제에서는 데이터 소스 유형으로 AWS Config을 사용하는 제어를 보여줍니다. 이는 AWS Control Tower 가드레일 프레임워크에서 가져온 표준 제어입니다. Audit Manager는 이 제어 기능을 사용하여 AWS 환경을 AWS Control Tower Guardrails와 일치시키는 데 도움이 되는 증거를 생성합니다.

제어 세부 정보의 예

- 제어 이름 — `4.1.2 - Disallow public write access to S3 buckets`
- 제어 세트 — 이 제어는 `Disallow public access` 제어 세트에 속합니다. 액세스 관리와 관련된 제어 그룹입니다.
- 데이터 소스 유형 – AWS Config
- 증거 유형 — 규정 준수 검사

다음 예제에서 이 제어는 AWS Control Tower 가드레일 프레임워크에서 생성된 Audit Manager 평가 내에 있습니다.



평가에는 제어 상태, 지금까지 이 제어에 대해 수집된 증거의 양, 평가 보고서에 포함된 증거의 양 등이 표시됩니다. 여기에서 제어 세트를 검토하도록 위임하거나 직접 검토를 완료할 수 있습니다. 제어 이름을 선택하면 해당 제어의 증거를 비롯한 자세한 정보가 포함된 세부 정보 페이지가 열립니다.

이 제어의 기능

Audit Manager는 이 제어를 사용하여 S3 버킷 정책의 액세스 수준이 AWS Control Tower 요구 사항을 충족하기에 너무 관대한지 확인할 수 있습니다. 보다 구체적으로 말하자면, 퍼블릭 액세스 차단 설정, 버킷 정책 및 버킷 액세스 제어 목록(ACL)을 확인하여 버킷이 퍼블릭 쓰기 액세스를 허용하지 않는지 확인할 수 있습니다.

Audit Manager가 이러한 제어에 대한 증거를 수집하는 방법

Audit Manager는 다음 단계를 수행하여 이 제어에 대한 증거를 수집합니다.

1. 각 제어에 대해 Audit Manager는 제어 설정에 지정된 데이터 소스를 사용하여 범위 내 리소스를 평가합니다. 이 경우 S3 버킷은 리소스이며 AWS Config은 데이터 소스 유형입니다. Audit Manager는 평가 범위에 속하는 각 S3 버킷의 설정, 정책 및 ACL을 평가하기 위해 특정 AWS Config 규칙(s3-bucket-public-write-prohibited)의 결과를 구합니다.
2. 리소스 평가 결과는 저장되고 감사자 친화적인 증거로 변환됩니다. Audit Manager는 AWS Config를 데이터 소스 유형으로 사용되는 제어에 대한 규정 준수 검사 증거를 생성합니다. 이 증거에는 AWS Config에서 직접 보고한 규정 준수 검사 결과가 포함됩니다.
3. Audit Manager는 저장된 증거를 `4.1.2 - Disallow public write access to S3 buckets`이라고 이름이 지정된 귀하의 평가 내 제어에 첨부합니다.

Audit Manager를 사용하여 이 제어 기능의 규정 준수를 입증하는 방법

증거가 제어 항목에 첨부되면 귀하 본인 또는 대리인이 증거를 검토하여 수정이 필요한지 확인할 수 있습니다.

이 예제에서 Audit Manager는 S3 버킷이 규정을 준수하지 않는다는 AWS Config의 결정을 표시할 수 있습니다. 이는 귀하의 S3 버킷 중 하나에 공개 정책을 제한하지 않는 공개 액세스 차단 설정이 있고 사

용 중인 정책이 공개 쓰기 액세스를 허용하는 경우 발생할 수 있습니다. 이 문제를 해결하려면 공개 액세스 차단 설정을 업데이트하여 공개 정책을 제한할 수 있습니다. 또는 공개쓰기 액세스를 허용하지 않는 다른 버킷 정책을 사용할 수도 있습니다. 이 수정 조치는 귀하의 AWS 환경을 AWS Control Tower 요구 사항에 맞게 만드는 데 도움이 됩니다.

S3 버킷 액세스 수준이 제어와 일치한다고 판단되면 제어를 검토됨으로 표시하고 귀하의 평가 보고서에 증거를 추가할 수 있습니다. 그런 다음 이 보고서를 감사자와 공유하여 제어가 의도한 대로 작동하고 있음을 입증할 수 있습니다.

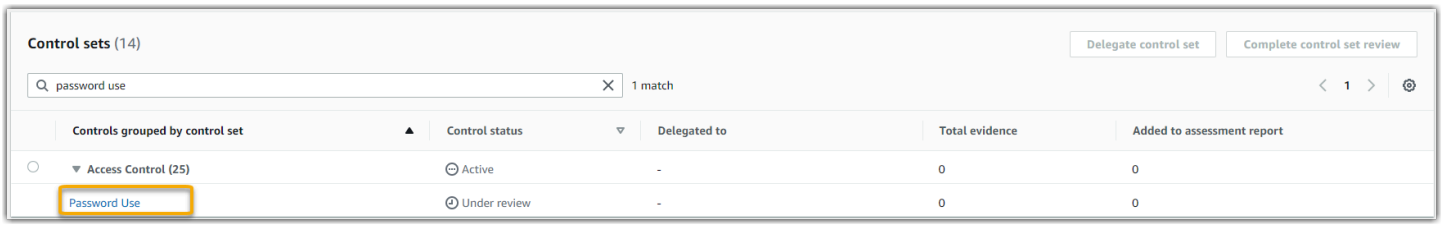
데이터 소스 유형으로 AWS API 직접 호출을 사용하는 자동화된 제어

이 예제에서는 AWS API 직접 호출을 데이터 소스 유형으로 사용하는 사용자 지정 제어를 보여줍니다. Audit Manager는 이 제어 기능을 사용하여 귀하의 AWS 환경을 특정 요구 사항에 맞추는 데 도움이 될 수 있는 증거를 생성합니다.

제어 세부 정보의 예

- 제어 이름 — `Password Use`
- 제어 세트 - 이 제어는 `Access Control`이라고 하는 제어 세트에 속합니다. ID 및 액세스 관리와 관련된 제어를 그룹화한 것입니다.
- 데이터 소스 유형 - AWS API 직접 호출
- 증거 유형 — 구성 데이터

다음 예제에서 이 제어는 사용자 지정 프레임워크에서 생성된 Audit Manager 평가 내에 있습니다.



평가에는 제어 상태가 표시됩니다. 또한 지금까지 이 제어에 대해 수집된 증거의 양과 평가 보고서에 포함된 증거의 양을 보여줍니다. 여기에서 제어 세트를 검토하도록 위임하거나 직접 검토를 완료할 수 있습니다. 제어 이름을 선택하면 해당 제어의 증거를 비롯한 자세한 정보가 포함된 세부 정보 페이지가 열립니다.

이 제어의 기능

Audit Manager는 이 사용자 지정 제어를 사용하여 귀하가 충분한 액세스 제어 정책을 가질 수 있도록 도울 수 있습니다. 이 제어를 위해서는 암호를 선택하고 사용할 때 적절한 보안 관행을 따라야 합니다.

Audit Manager는 평가 범위에 속하는 IAM 주체에 대한 모든 암호 정책 목록을 검색하여 이를 검증하는 데 도움을 줄 수 있습니다.

Audit Manager가 이러한 제어에 대한 증거를 수집하는 방법

Audit Manager는 다음 단계를 수행하여 이 사용자 지정 제어에 대한 증거를 수집합니다.

1. 각 제어에 대해 Audit Manager는 제어 설정에 지정된 데이터 소스를 사용하여 범위 내 리소스를 평가합니다. 이 경우 IAM 주체는 리소스이고 AWS API 직접 호출은 데이터 소스 유형입니다. Audit Manager는 특정 IAM API 직접 호출(GetAccountPasswordPolicy)의 결과를 구합니다. 그런 다음 평가 범위에 해당하는 AWS 계정을 위한 암호 정책을 제공합니다.
2. 리소스 평가 결과는 저장되고 감사자 친화적인 증거로 변환됩니다. Audit Manager는 API 직접 호출을 데이터 소스로 사용하는 제어에 대한 구성 데이터 증거를 생성합니다. 이 증거에는 API 응답에서 캡처한 원본 데이터와 데이터가 지원하는 제어 항목을 나타내는 추가 메타데이터가 포함됩니다.
3. Audit Manager는 저장된 증거를 `Password Use`이라는 이름이 지정된 귀하의 평가 내 사용자 지정 제어에 첨부합니다.

Audit Manager를 사용하여 이 제어 기능의 규정 준수를 입증하는 방법

증거가 제어 항목에 첨부되면 귀하 본인 또는 대리인이 증거를 검토하여 증거가 충분한지 또는 수정이 필요한지 확인할 수 있습니다.

이 예시에서는 증거를 검토하여 API 직접 호출의 응답을 확인할 수 있습니다. GetAccountPasswordPolicy 응답은 계정의 사용자 암호에 대한 복잡성 요구 사항과 필수 순환 기간을 기술합니다. 이 API 응답을 평가 범위에 있는 AWS 계정에 대해 충분한 암호 액세스 제어 정책이 마련되어 있음을 보여주는 증거로 사용할 수 있습니다. 원하는 경우 제어에 설명을 추가하여 이러한 정책에 대한 추가 설명을 제공할 수도 있습니다.

IAM 주체의 암호 정책이 사용자 지정 제어와 일치한다고 판단되면 제어를 검토됨으로 표시하고 귀하의 평가 보고서에 증거를 추가할 수 있습니다. 그런 다음 이 보고서를 감사자와 공유하여 제어가 의도한 대로 작동하고 있음을 입증할 수 있습니다.

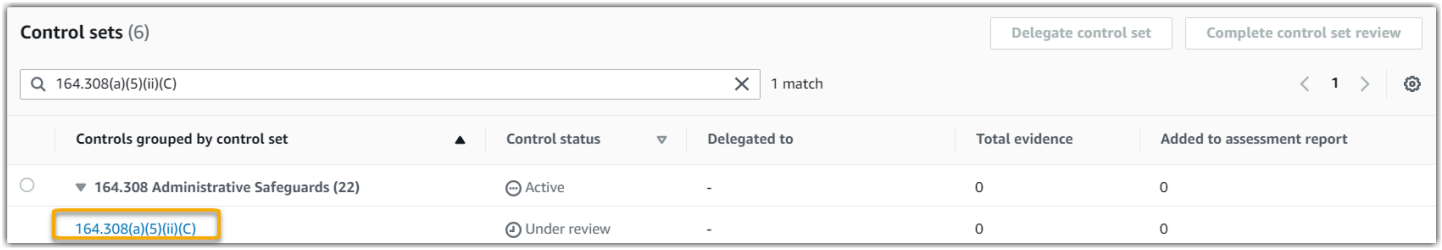
데이터 소스 유형으로 AWS CloudTrail을 사용하는 자동화된 제어

이 예제에서는 AWS CloudTrail을 데이터 소스 유형으로 사용하는 제어를 보여줍니다. HIPAA 프레임워크에서 가져온 표준 제어입니다. Audit Manager는 이 제어 기능을 사용하여 귀하의AWS 환경을 HIPAA 요구 사항에 맞추는 데 도움이 될 수 있는 증거를 생성합니다.

제어 세부 정보의 예

- 제어 이름 — 164.308(a)(5)(ii)(C)
- 제어 세트 - 이 제어는 164.308 Administrative Safeguards라고 하는 제어 세트에 속합니다.
- 데이터 소스 유형 – AWS CloudTrail
- 증거 유형 — 사용자 활동

HIPAA 프레임워크에서 생성된 Audit Manager 평가에 표시된 이러한 제어 기능은 다음과 같습니다.



평가에는 제어 상태가 표시됩니다. 또한 지금까지 이 제어에 대해 수집된 증거의 양과 평가 보고서에 포함된 증거의 양을 보여줍니다. 여기에서 제어 세트를 검토하도록 위임하거나 직접 검토를 완료할 수 있습니다. 제어 이름을 선택하면 해당 제어의 증거를 비롯한 자세한 정보가 포함된 세부 정보 페이지가 열립니다.

이 제어의 기능

이 제어에는 부적절한 로그인을 탐지하기 위한 모니터링 절차가 필요합니다. 부적절한 로그인의 예로는 누군가가 사용자 이름이나 암호를 여러 개 조합하여 입력하여 정보 시스템에 액세스하려고 시도하는 경우를 들 수 있습니다. Audit Manager는 평가 범위에 속하는 리소스에 대해 탐지된 모든 로그인 시도 목록을 제공하여 이러한 제어를 검증할 수 있도록 도와줍니다.

Audit Manager가 이러한 제어에 대한 증거를 수집하는 방법

Audit Manager는 다음 단계를 수행하여 이 제어에 대한 증거를 수집합니다.

1. 각 제어에 대해 Audit Manager는 제어 설정에 지정된 데이터 소스를 사용하여 범위 내 리소스를 평가합니다. 이 경우 사용자가 리소스이고 CloudTrail이 데이터 소스 유형입니다. Audit Manager는 CloudTrail에서 기록하는 모든 AWS Management Console 로그인 이벤트의 결과를 구합니다. 그런 다음 평가 범위 내에 있는 관련 이벤트의 로그를 제공합니다.
2. 리소스 평가 결과는 저장되고 감사자 친화적인 증거로 변환됩니다. Audit Manager는 CloudTrail을 데이터 소스 유형으로 사용하는 제어 기능에 대한 사용자 활동 증거를 생성합니다. 이 증거에는 사용자로부터 캡처한 원본 데이터와 데이터가 지원하는 제어 항목을 나타내는 추가 메타데이터가 포함됩니다.

3. Audit Manager는 저장된 증거를 `164.308(a)(5)(ii)(C)`이라고 이름이 지정된 귀하의 평가 내 제어에 첨부합니다.

Audit Manager를 사용하여 이 제어 기능의 규정 준수를 입증하는 방법

증거가 제어 항목에 첨부되면 귀하 본인 또는 대리인이 증거를 검토하여 수정이 필요한지 확인할 수 있습니다.

이 예시에서는 증거를 검토하여 CloudTrail에서 기록한 로그인 이벤트를 확인할 수 있습니다. 이 로그는 다음 정보를 포함하여 사용자의 콘솔 로그인 활동을 설명합니다.

- 모든 성공적인 로그인
- 실패한 모든 로그인 시도
- 다중 인증(MFA) 적용 시기 확인
- 모든 로그인 이벤트의 IP 주소

이 로그를 평가 범위에 해당하는 충분한 모니터링 절차를 갖추고 있는 AWS 계정을 보여주는 증거로 사용할 수 있습니다. 원하는 경우 제어에 설명을 추가하여 추가 설명을 제공할 수도 있습니다. 예를 들어 로그에 로그인 시도가 여러 번 실패하는 등 불일치가 표시되는 경우 문제를 해결한 방법을 설명하는 설명을 추가할 수 있습니다. 콘솔 로그인을 정기적으로 모니터링하면 불일치 및 부적절한 로그인 시도로 인해 발생할 수 있는 보안 문제를 예방할 수 있습니다. 결과적으로 이 모범 사례는 귀하의 AWS 환경을 HIPAA 요구 사항에 맞추는 데 도움이 됩니다.

모니터링 절차가 제어 기준에 부합한다고 판단되면 해당 제어를 검토됨으로 표시하고 평가 보고서에 증거를 추가할 수 있습니다. 그런 다음 이 보고서를 감사자와 공유하여 제어가 의도한 대로 작동하고 있음을 입증할 수 있습니다.

수동 제어

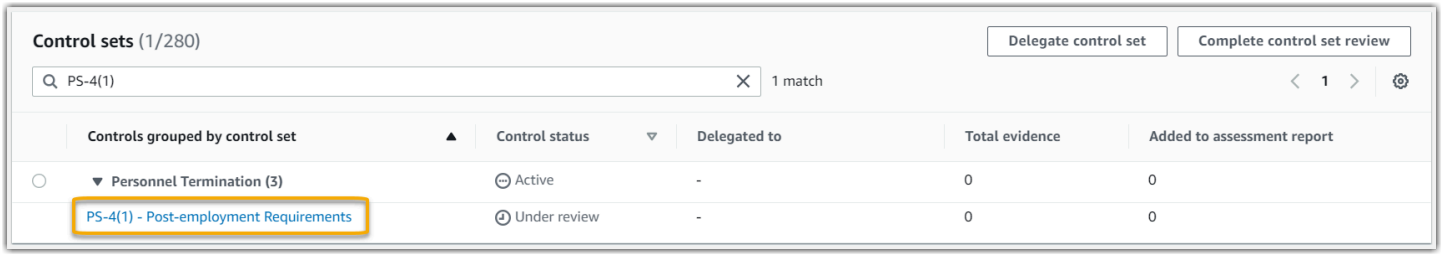
일부 제어는 자동 증거 수집을 지원하지 않습니다. 여기에는 클라우드에서 생성되지 않는 관찰, 인터뷰 및 기타 이벤트 외에도 물리적 기록 및 서명의 제공에 의존하는 제어가 포함됩니다. 이러한 경우 제어 요구 사항을 충족하고 있음을 입증하는 증거를 수동으로 업로드할 수 있습니다.

이 예는 Audit Manager가 자동 증거를 수집하지 않는 수동 제어를 보여줍니다. 이는 NIST 800-53(개정본 5) 프레임워크에서 가져온 표준 제어입니다. Audit Manager를 사용하여 이 제어의 규정 준수를 입증하는 증거를 업로드하고 저장할 수 있습니다.

제어 세부 정보의 예

- 제어 이름 — `PS-4(1) - Post-employment Requirements`
- 제어 세트 — 이 제어는 `Personnel Termination` 제어 세트에 속합니다. 이는 고용 해지 절차의 맥락에서 정보 보안과 관련된 제어들을 그룹화한 것입니다.
- 데이터 소스 유형 — 수동
- 증거 유형 — 수동

다음은 NIST 800-53(개정본 5) 낮음-보통-높음 프레임워크에서 생성된 Audit Manager 평가에서 나타난 제어 기능입니다.



평가에는 제어 상태가 표시됩니다. 또한 지금까지 이 제어에 대해 수집된 증거의 양과 평가 보고서에 포함된 증거의 양을 보여줍니다. 여기에서 제어 세트를 검토하도록 위임하거나 직접 검토를 완료할 수 있습니다. 제어 이름을 선택하면 해당 제어의 증거를 비롯한 자세한 정보가 포함된 세부 정보 페이지가 열립니다.

이 제어의 기능

이 제어를 사용하여 직원이 고용 해지되는 경우 조직의 정보를 보호하고 있는지 확인할 수 있습니다. 특히, 조직 정보 보호를 위한 적용 가능하고 법적 구속력이 있는 고용 후 요구 사항을 고용 해지된 개인에게 지속적으로 통보한다는 점을 입증할 수 있습니다. 또한 조직의 해고 절차의 일환으로 고용 해지된 모든 개인이 취업 후 의무 인정서에 서명했음을 입증할 수 있습니다.

이 제어에 대한 증거를 수동으로 업로드하는 방법

다음 단계에 따라 이 제어를 뒷받침하는 수동 증거를 업로드할 수 있습니다.

1. Amazon Simple Storage Service(S3) 버킷에 배포 패키지를 귀하가 수동으로 업로드하려는 증거 패키지를 Amazon Simple Storage Service(S3) 버킷에 배치하고 S3 URI를 기록합니다.
2. 귀하의 Audit Manager 평가에서 제어를 열고 증거 폴더 탭으로 이동한 다음 S3 URI를 입력하여 증거를 업로드합니다. 지침은 AWS Audit Manager의 수동 증거 업로드를 참조하세요.

3. Audit Manager는 증거를 업로드한 날짜의 이름을 따른 증거 폴더를 만듭니다. 그런 다음 업로드된 증거를 `PS-4(1) - Post-employment Requirements`이라는 이름이 지정된 평가의 제어 항목에 첨부합니다.

Audit Manager를 사용하여 이 제어 기능의 규정 준수를 입증하는 방법

이 제어를 지원하는 문서가 있는 경우 이를 수동 증거로 업로드할 수 있습니다. 예를 들어 인사부에서 퇴직 사원에게 발급하는 법적 구속력이 있는 채용 후 의무의 최신 사본을 업로드할 수 있습니다. 감사 기간 중에 고용 해지된 개인이 있는 경우, 해지된 개인에게 보내는 날짜가 기입된 사본을 업로드할 수도 있습니다.

자동 제어를 사용하는 경우와 마찬가지로, 증거 검토(이 경우에는 제공)를 도와줄 이해관계자에게 수동 제어를 위임할 수 있습니다. 예를 들어, 이 규제 항목을 검토하면 의무를 부분적으로만 충족한다는 사실을 알게 될 수 있습니다. 고용 해지된 개인이 서명한 확인서가 없는 경우가 이에 해당할 수 있습니다. HR 이해 관계자에게 제어를 위임하면 서명된 문서의 사본을 업로드할 수 있습니다. 또는 감사 기간 동안 고용해지된 직원이 없는 경우 관리 항목에 서명된 서신이 첨부되지 않은 이유를 설명하는 의견을 남길 수 있습니다.

제어 기준에 부합한다고 판단되면 검토됨으로 표시하고 귀하의 평가 보고서에 증거를 추가할 수 있습니다. 그런 다음 이 보고서를 감사자와 공유하여 제어가 의도한 대로 작동하고 있음을 입증할 수 있습니다.

데이터 소스 유형이 혼합된 제어(자동 및 수동)

대부분의 경우 제어를 충족시키기 위해서는 자동 증거의 조합과 수동 증거의 조합이 필요합니다. Audit Manager는 제어와 관련된 자동 증거를 제공할 수 있지만, 직접 식별하고 업로드한 수동 증거로 이 데이터를 보완해야 할 수도 있습니다.

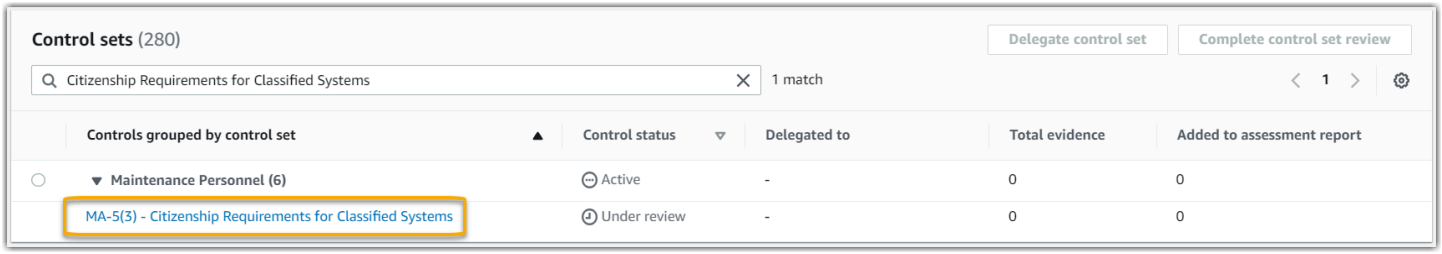
이 예제는 수동 증거와 AWS API 직접 호출을 통해 제공되는 자동 증거를 조합하여 사용하는 제어를 보여줍니다. 이는 NIST 800-53(개정본 5) 프레임워크에서 가져온 표준 제어입니다. Audit Manager는 이 제어 기능을 사용하여 AWS 환경을 NIST 요구 사항에 맞추는 데 도움이 될 수 있는 증거를 생성합니다.

제어 세부 정보의 예

- 제어 이름 — `MA-5(3) - Citizenship Requirements for Classified Systems`
- 제어 세트 — 이 제어는 `Maintenance Personnel` 제어 세트에 속합니다. 조직 시스템에서 하드웨어 또는 소프트웨어 유지 관리를 수행하는 개인과 관련된 제어 그룹입니다.
- 데이터 소스 유형 — AWS API 직접 호출 및 추가 매뉴얼 증거

- 증거 유형 — 구성 데이터

다음은 NIST 800-53(개정본 5) 프레임워크에서 생성된 Audit Manager 평가에서 나타난 제어 기능입니다.



평가에는 제어 상태가 표시됩니다. 또한 지금까지 이 제어에 대해 수집된 증거의 양과 평가 보고서에 포함된 증거의 양을 보여줍니다. 여기에서 제어 세트를 검토하도록 위임하거나 직접 검토를 완료할 수 있습니다. 제어 이름을 선택하면 해당 제어의 증거를 비롯한 자세한 정보가 포함된 세부 정보 페이지가 열립니다.

이 제어의 기능

Audit Manager는 이 제어 기능을 사용하여 유지 관리 및 진단 활동을 수행하는 직원이 필요한 국적을 보유하고 있는지 여부를 귀하가 확인하는데 도움을 줄 수 있습니다. 시스템에서 기밀 정보를 처리, 저장 또는 전송하는 경우 유지 관리 담당자가 미국 시민임을 입증해야 합니다. Audit Manager는 이를 검증하는 데 도움을 줍니다. 평가 범위에 속하는 모든 IAM 정책 및 주체의 전체 목록을 제공하여 이를 수행합니다. 그런 다음 귀하는 이 사용자 목록에 필요한 시민권 요건이 있는지 확인하고 입증할 수 있습니다. 귀하는 국적에 대한 추가 증거를 수동으로 업로드하여 이를 수행할 수 있습니다.

Audit Manager가 이러한 제어에 대한 증거를 수집하는 방법

Audit Manager는 다음 단계를 수행하여 이 제어에 대한 증거를 수집합니다.

1. 각 제어에 대해 Audit Manager는 제어 설정에 지정된 데이터 소스를 사용하여 범위 내 리소스를 평가합니다. 이 경우 IAM 정책 및 주체는 리소스이고 AWS API 직접 호출은 데이터 소스입니다. Audit Manager는 4가지 특정 IAM API 직접 호출(ListUsers/ListRoles/ListGroups/ListPolicies)의 결과를 찾아 평가 범위에 속하는 IAM 정책 및 주체 목록을 제공합니다.
2. 리소스 평가 결과는 저장되고 감사자 친화적인 증거로 변환됩니다. Audit Manager는 API 직접 호출을 데이터 소스 유형으로 사용하는 제어에 대한 구성 데이터 증거를 생성합니다. 이 증거에는 API 응답에서 캡처한 원본 데이터와 데이터가 지원하는 제어 항목을 나타내는 추가 메타데이터가 포함됩니다.
3. Audit Manager는 저장된 증거를 `MA-5(3) - Citizenship Requirements for Classified Systems`이라고 이름이 지정된 귀하의 평가 내 제어에 첨부합니다.

이 제어에 대한 증거를 수동으로 업로드하는 방법

다음 단계에 따라 자동 증거를 보완하는 수동 증거를 업로드할 수 있습니다.

1. Amazon Simple S3 버킷에 시민권 증빙 서류를 넣고 Simple S3 버킷에 Simple S3 URI를 기록합니다.
2. Audit Manager 평가에서 제어 항목을 열고 증거 폴더 탭으로 이동하여 증거를 업로드하세요. S3 URI를 입력하여 이 작업을 수행할 수 있습니다. 지침은 AWS Audit Manager의 수동 증거 추가를 참조하세요.
3. Audit Manager는 업로드된 증거를 `MA-5(3) - Citizenship Requirements for Classified Systems`이라는 이름이 지정된 평가의 제어 항목에 첨부합니다.

Audit Manager를 사용하여 이 제어 기능의 규정 준수를 입증하는 방법

증거가 제어 항목에 첨부되면 귀하 본인 또는 대리인이 증거를 검토하여 증거가 충분한지 또는 수정이 필요한지 확인할 수 있습니다.

이 예시에서는 증거를 검토하여 20명의 사용자 목록을 확인할 수 있습니다. 어떤 사용자가 유지 관리 담당자인지 또는 해당 사용자의 시민권을 식별할 수 있는지 확신이 들지 않으면 주제 전문가에게 제어를 위임하여 검증을 받을 수 있습니다. 대리인은 유지 관리 담당자 명단을 확인하고 추가 증거를 시민권 상태를 증명하는 문서로 직접 업로드할 수 있습니다. 목록에 있는 모든 관련 사용자의 시민권을 확인하면 귀하의 AWS 환경을 NIST 요구 사항에 맞추는 데 도움이 됩니다. 또는 시스템이 기밀 정보를 처리, 저장 또는 전송하지 않는 경우 이 제어가 적용되지 않는 이유를 설명하는 설명을 남길 수 있습니다.

제어 기준에 부합한다고 판단되면 해당 제어를 검토됨으로 표시하고 평가 보고서에 증거를 추가하세요. 그런 다음 이 보고서를 감사자와 공유하여 제어가 의도한 대로 작동하고 있음을 입증할 수 있습니다.

AWS 서비스 관련 항목과의 통합

AWS Audit Manager은 여러 AWS 서비스와 통합하여 평가 보고서에 포함할 수 있는 증거를 자동으로 수집합니다.

AWS Security Hub

AWS Security Hub은 AWS모범 사례 및 업계 표준을 기반으로 하는 자동 보안 검사를 사용하여 환경을 모니터링합니다. Audit Manager는 Security Hub에서 직접 보안 검사 결과를 보고하여 리소스 보안 상태의 스냅샷을 캡처합니다. Security Hub에 대한 자세한 내용은 AWS Security Hub 사용 안내서에서 AWS Security Hub이란 무엇인가요?를 참조하세요.

AWS CloudTrail

AWS CloudTrail은 귀하의 계정 내 AWS 리소스에 대한 호출을 모니터링하는 데 도움이 됩니다. 여기에는 AWS 관리 콘솔, AWS CLI 및 기타AWS 서비스에서 이루어진 호출이 포함됩니다. Audit Manager는 CloudTrail에서 직접 로그 데이터를 수집하고 처리된 로그를 사용자 활동 증거로 변환합니다. CloudTrail에 대한 자세한 내용은 AWS CloudTrail 사용 설명서의 AWS CloudTrail이란 무엇인가요?를 참조하세요.

AWS Config

AWS Config은 귀하의 AWS 계정에 있는 AWS 리소스의 구성을 자세히 보여줍니다. 여기에는 리소스가 서로 관련되는 방식과 리소스가 과거에 구성되었던 방식이 포함됩니다. Audit Manager는 AWS Config로부터 조사 결과를 직접 보고하여 리소스 보안 상태의 스냅샷을 캡처합니다. AWS Config에 대한 자세한 내용은 AWS Config 사용 설명서의 AWS Config이란 무엇인가요?를 참조하세요.

AWS License Manager

AWS License Manager는 소프트웨어 공급업체 라이선스를 클라우드로 가져오는 프로세스를 간소화합니다. AWS에서 클라우드 인프라를 구축할 때 기존 라이선스 인벤토리를 클라우드 리소스와 함께 사용할 목적으로 용도 변경하면 비용을 절감할 수 있습니다. Audit Manager는 감사 준비를 지원하는 라이선스 관리자 프레임워크를 제공합니다. 이 프레임워크는 License Manager와 통합되어 고객이 정의한 라이선스 규칙을 기반으로 라이선스 사용 정보를 집계합니다. License Manager에 대한 자세한 내용은 AWS License Manager 사용 설명서의 AWS License Manager이란 무엇인가요?를 참조하세요.

AWS Control Tower

AWS Control Tower은 클라우드 인프라에 예방 및 탐지 가드레일을 적용합니다. Audit Manager는 귀하의 감사 준비를 지원하는 AWS Control Tower 가드레일 프레임워크를 제공합니다. 이 프레임워크에는 AWS Control Tower로부터의 가드레일을 기반으로 하는 모든 AWS Config 규칙이 포함되어 있습니다. AWS Control Tower에 대한 자세한 내용은 AWS Control Tower 사용 설명서의 AWS Control Tower이란 무엇인가요?를 참조하세요.

AWS Artifact

AWS Artifact은 AWS 인프라에 대한 규정 준수 문서 및 인증에 대한 온디맨드 액세스를 제공하는 셀프 서비스 감사 아티팩트 검색 포털입니다. AWS Artifact은 AWS 클라우드 인프라가 규정 준수 요구 사항을 충족한다는 것을 입증하는 증거를 제공합니다. 반면, AWS Audit Manager는 귀하의 AWS 서비스 사용이 규정을 준수하고 있음을 입증하는 증거를 수집, 검토 및 관리하는 데 도움이 됩니다. AWS Artifact에 대한 자세한 내용은 AWS Artifact 사용 설명서의 AWS Artifact이란 무엇인가요?를 참조하세요. AWS Management Console에서 AWS 보고서 목록을 다운로드할 수 있습니다.

특정 규정 준수 프로그램 범위에 속하는 AWS 서비스의 목록은 범위 내 AWS 서비스 규정 준수 프로그램을 참조하세요. 추가적인 일반 정보는 AWS 규정 준수 프로그램을 참조하세요.

제3자 GRC 제품과의 통합

AWS Audit Manager은 이 페이지에 나열된 제3자 파트너 GRC 제품과의 통합을 지원합니다.

회사에서 하이브리드 클라우드 모델 또는 멀티클라우드 모델을 사용하는 경우 GRC 제품을 사용하여 이러한 환경의 증거를 관리할 가능성이 높습니다. 해당 제품이 Audit Manager와 통합되면 귀하의 AWS 사용 현황에 대한 증거를 GRC 환경으로 직접 가져올 수 있습니다. 이를 통해 감사를 준비하면서 증거를 검토하고 수정할 수 있는 중앙 집중식 장소를 제공함으로써 규정 준수를 관리하는 방법이 간소화됩니다.

Audit Manager로부터 증거를 수집할 수 있는 제3자 GRC 제품에 대한 개요를 보려면 이 페이지를 읽어보세요. 또한 해당 제품 내에서 직접 수행할 수 있는 Audit Manager API 작업에 대한 참조도 볼 수 있습니다.

주제

- 제3자 통합이 Audit Manager와 함께 작동하는 방식 이해하기
- Audit Manager와 통합되는 제3자 GRC 파트너 제품

제3자 통합이 Audit Manager와 함께 작동하는 방식 이해하기

GRC 파트너는 Audit Manager 공개 API를 사용하여 그들의 제품을 Audit Manager와 통합할 수 있습니다. 이러한 통합을 확립함으로써 GRC 환경의 엔터프라이즈 제어를 Audit Manager가 제공하는 제어에 매핑할 수 있습니다.

이 일회성 제어 매핑 예제를 완료한 후에는 GRC 제품에서 직접 Audit Manager 평가를 생성할 수 있습니다. 이 작업을 수행하면 귀하의 AWS 사용에 대한 증거 수집이 시작됩니다. 그러면 하이브리드 환경에서 수집된 다른 증거와 함께 엔터프라이즈 제어의 동일한 맥락 내에서 이 AWS 증거를 확인할 수 있습니다.

Audit Manager 통합을 제3자 GRC 제품과 사용할 때는 다음 사항을 유의해야 합니다.

- Audit Manager가 지원되는 모든 AWS 리전에서 통합이 가능합니다.
- GRC 파트너 제품에서 생성한 모든 Audit Manager 리소스는 Audit Manager에도 반영됩니다.
- 제3자 GRC 제품의 AWS Audit Manager 요금 외에도 요금이 귀하에게 부과됩니다.

- Audit Manager가 수집하는 증거는 변경할 수 없습니다. 증거는 Audit Manager 콘솔에서와 정확히 동일한 방식으로 제3자 GRC 제품에서 제공됩니다. 하지만 제3자 통합을 사용하는 경우 보고에 추가 컨텍스트를 제공하여 이러한 증거를 강화할 수 있습니다.
- Audit Manager에 적용되는 것과 할당량이 동일하게 제3자 GRC 제품에도 적용됩니다. 예를 들어, 각각의 AWS 계정은 최대 100개의 활성 Audit Manager 평가를 포함할 수 있습니다. 이 계정 수준 할당량은 Audit Manager 콘솔에서 평가를 생성하든 제3자 GRC 제품에서 생성하든 상관없이 적용됩니다. 전부는 아니지만 Audit Manager 할당량의 대부분은 Service Quotas 콘솔의 AWS Audit Manager 네임스페이스 아래에 나열됩니다. 할당량 증가를 요청하는 방법에 대해서는 Audit Manager 할당량 관리 섹션을 참조하세요.

규정 준수 솔루션이 있고 Audit Manager와의 통합에 관심이 있다면 `auditmanager-partners@amazon.com`으로 이메일을 보내세요.

Audit Manager와 통합되는 제3자 GRC 파트너 제품

다음 제3자 GRC 제품은 Audit Manager로부터 증거를 수집할 수 있습니다.

메트릭 스트림

이 통합을 사용하려면 MetricStream에 연락하여 MetricStream GRC 소프트웨어의 액세스 및 구매를 요청하세요.

MetricStream 플랫폼을 기반으로 구축된 MetricStream 엔터프라이즈 GRC 솔루션을 사용하면 전사적 GRC 활동 및 프로세스에 대한 포괄적이고 협력적인 접근 방식을 사용할 수 있습니다. Audit Manager의 증거를 MetricStream으로 수집하면 귀하의 AWS 환경에서 규정을 준수하지 않는 증거를 사전에 식별하고 온프레미스 데이터 소스 또는 기타 클라우드 파트너의 증거와 함께 검토할 수 있습니다. 이를 통해 감사를 준비하면서 클라우드 보안 및 규정 준수 상태를 검토하고 개선할 수 있는 편리하고 중앙 집중적인 방법을 제공합니다.

MetricStream과 Audit Manager 통합을 통해 다음과 같은 API 작업을 수행할 수 있습니다.

작업	API 연산
Audit Manager 통합 설정	• GetAccountStatus • GetOrganizationAdminAccount • GetSettings

작업	API 연산
Audit Manager 리소스 검토	• GetAssessment • GetAssessmentFramework • GetControl • ListAssessmentFrameworks • ListControls
Audit Manager 리소스 생성	• CreateAssessment • CreateAssessmentFramework
Audit Manager 리소스 업데이트	• UpdateAssessment • UpdateAssessmentControl • UpdateAssessmentStatus
증거 관리	• 스타트쿼리 (AWS CloudTrail API) • 쿼리 결과 가져오기 (AWS CloudTrail API)
Audit Manager 리소스 삭제	• DeleteAssessmentFramework

관련 MetricStream 링크

- AWS Marketplace 링크
- 제품 링크
- 제품 요금

Audit Manager를 AWS SDK와 함께 사용하기

다양한 프로그래밍 언어에 대해 AWS 소프트웨어 개발 키트(SDK)를 사용할 수 있습니다. 각 SDK는 개발자가 자신이 선호하는 언어로 애플리케이션을 구축하는데 사용할 수 있는 API, 코드 예제 및 설명서를 제공합니다.

SDK 설명서	Audit Manager 관련 문서	코드 예제
AWS SDK for C++	Audit Manager용 AWS SDK for C++ API 참조	AWS SDK for C++ 코드 예제
AWS SDK for Go	Audit Manager용 AWS SDK for Go API 참조	AWS SDK for Go 코드 예제
AWS SDK for Java	Audit Manager용 AWS SDK for Java 2.x API 참조	AWS SDK for Java 코드 예제
AWS SDK for JavaScript	Audit Manager용 AWS SDK for JavaScript API 참조	AWS SDK for JavaScript 코드 예제
AWS SDK for .NET	Audit Manager용 AWS SDK for .NET API 참조	AWS SDK for .NET 코드 예제
AWS SDK for PHP	Audit Manager용 AWS SDK for PHP API 참조	AWS SDK for PHP 코드 예제
AWS SDK for Python (Boto3)	Audit Manager용 AWS SDK for Python (Boto) API 참조	AWS SDK for Python (Boto3) 코드 예제
AWS SDK for Ruby	Audit Manager용 AWS SDK for Ruby API 참조	AWS SDK for Ruby 코드 예제

Audit Manager에만 해당하는 예제는 AWS Audit Manager을 위한 코드 예제를 참조하세요.

> **Note**
>
> Audit Manager는 AWS SDK for Python (Boto3)에 대해 보토코어 버전 1.19.32 및 그 이상 버전에서 사용에 제공됩니다. SDK 사용을 시작하기 전에 귀하가 적절한 botocore 버전을 사용하고 있는지 확인하세요.

AWS Audit Manager 설정

Audit Manager를 사용하기 전에 다음 설정 태스크를 완료했는지 확인하세요.

주제

- 사전 조건: AWS 계정 생성 및 권한 설정
- Audit Manager 활성화: 콘솔, AWS CLI 또는 API를 사용하여 Audit Manager를 활성화합니다.
- 권장 사항: 다른 AWS 서비스와 권장 통합을 설정합니다

사전 조건

다음 단계에 따라 Audit Manager 설정 권한을 가진 AWS 계정와 관리 사용자를 생성할 수 있습니다.

단계

- AWS 계정에 등록
- 관리 사용자 생성
- Audit Manager에 액세스하고 활성화하는 데 필요한 권한을 추가합니다.

> **Important**
>
> AWS와 IAM을 사용하여 이미 설정한 경우, 1단계와 2단계를 건너뛸 수 있습니다. 하지만 Audit Manager를 설정하는 데 필요한 권한이 있는지 확인하려면 3단계를 완료해야 합니다.

AWS 계정에 등록

AWS 계정가 없는 경우 다음 절차에 따라 계정을 생성합니다.

AWS 계정에 가입하려면

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

   가입 절차 중 전화를 받고 전화 키패드로 확인 코드를 입력하는 과정이 있습니다.

AWS 계정에 가입하면 AWS 계정 루트 사용자 항목이 생성됩니다. 루트 사용자에게 계정의 모든 AWS 서비스 및 리소스에 대한 액세스 권한이 있습니다. 보안 모범 사례는 관리 사용자에게 관리자 액세스 권한을 할당하고, 루트 사용자만 루트 사용자 액세스 권한이 필요한 작업을 수행하는 것입니다.

가입 프로세스가 완료되면 AWS가 확인 이메일을 전송합니다. 언제든지 https://aws.amazon.com/으로 이동하고 내 계정을 선택하여 현재 계정 활동을 보고 계정을 관리할 수 있습니다.

관리 사용자 생성

AWS 계정에 가입하고 AWS 계정 루트 사용자에 보안 조치를 한 다음, AWS IAM Identity Center을 활성화하고 일상적인 작업에 루트 사용자를 사용하지 않도록 관리 사용자를 생성합니다.

귀하의 AWS 계정 루트 사용자 보호

1. 루트 사용자를 선택하고 AWS 계정 이메일 주소를 입력하여 AWS Management Console에 계정 소유자로 로그인합니다. 다음 페이지에서 암호를 입력합니다.

   루트 사용자를 사용하여 로그인하는 데 도움이 필요하면 AWS 로그인 사용 설명서의 루트 사용자로 로그인을 참조하세요.
2. 루트 사용자에 대해 다중 인증(MFA)을 활성화합니다.

   지침은 IAM 사용 설명서의 AWS 계정 루트 사용자용 가상 MFA 디바이스 활성화(콘솔) 섹션을 참조하세요.

관리 사용자 생성

1. IAM Identity Center를 활성화합니다.

   지침은 AWS IAM Identity Center 사용 설명서에서 Enabling AWS IAM Identity Center를 참조하세요.
2. IAM ID 센터에서 관리 사용자에게 관리 액세스 권한을 부여합니다.

   IAM Identity Center 디렉터리를 ID 소스로 사용하는 방법에 대한 자습서는 AWS IAM Identity Center 사용 설명서에서 Configure user access with the default IAM Identity Center 디렉터리를 참조하세요.

관리 사용자로 로그인

- IAM 자격 증명 센터 사용자로 로그인하려면 IAM 자격 증명 센터 사용자를 생성할 때 이메일 주소로 전송된 로그인 URL을 사용합니다.

  IAM Identity Center 사용자로 로그인하는 데 도움이 필요한 경우 AWS 로그인 사용 설명서의 AWS 액세스 포털에 로그인을 참조하세요.

Audit Manager에 액세스하고 활성화하는 데 필요한 권한을 추가합니다.

Audit Manager를 활성화하려면 필요한 권한을 사용자에게 부여해야 합니다. Audit Manager에 대한 전체 액세스 권한이 필요한 사용자는 AWSAuditManagerAdministratorAccess 관리형 정책을 사용해야 합니다. 이 정책은 AWS 계정에서 사용할 수 있는 AWS 관리형 정책으로, Audit Manager 관리자에게 권장되는 정책입니다.

> **Tip**
>
> 보안의 모범 사례로서 AWS 관리형 정책을 시작한 다음 최소 권한 권한으로 전환하는 것이 좋습니다. AWS 관리형 정책은 여러 가지 일반적인 사용 사례에 대한 권한을 부여합니다. 하지만 AWS 관리형 정책은 모든 AWS 고객이 사용할 수 있기 때문에 특정 사용 사례에 대해 최소 권한을 부여하지 않을 수 있습니다. 따라서 사용 사례에 고유한 고객 관리형 정책을 정의하여 권한을 줄이는 것이 좋습니다. 자세한 내용은 AWS Identity and Access Management사용 설명서의 AWS 관리형 정책을 참조하세요.

액세스 권한을 제공하려면 사용자, 그룹 또는 역할에 권한을 추가하십시오:

- AWS IAM Identity Center의 사용자 및 그룹:

  권한 세트를 생성합니다. AWS IAM Identity Center 사용 설명서의 권한 세트 생성의 지침을 따르세요.
- ID 공급자를 통해 IAM에서 관리되는 사용자:

  ID 페더레이션을 위한 역할을 생성합니다. IAM 사용 설명서의 서드 파티 자격 증명 공급자의 역할 만들기(연합)의 지침을 따르세요.
- IAM 사용자:
  - 사용자가 맡을 수 있는 역할을 생성합니다. IAM 사용 설명서에서 IAM 사용자의 역할 생성의 지침을 따르세요.

- (권장되지 않음)정책을 사용자에게 직접 연결하거나 사용자를 사용자 그룹에 추가합니다. IAM 사용 설명서에서 사용자(콘솔)에 권한 추가의 지침을 따르세요.

AWS Audit Manager 활성화

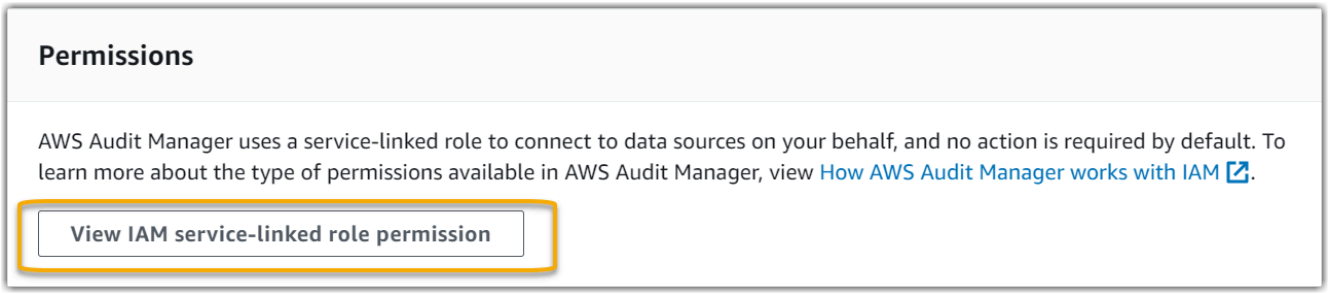
AWS Management Console, Audit Manager API 또는 AWS Command Line Interface(AWS CLI)를 사용하여 Audit Manager를 활성화할 수 있습니다.

Audit Manager console

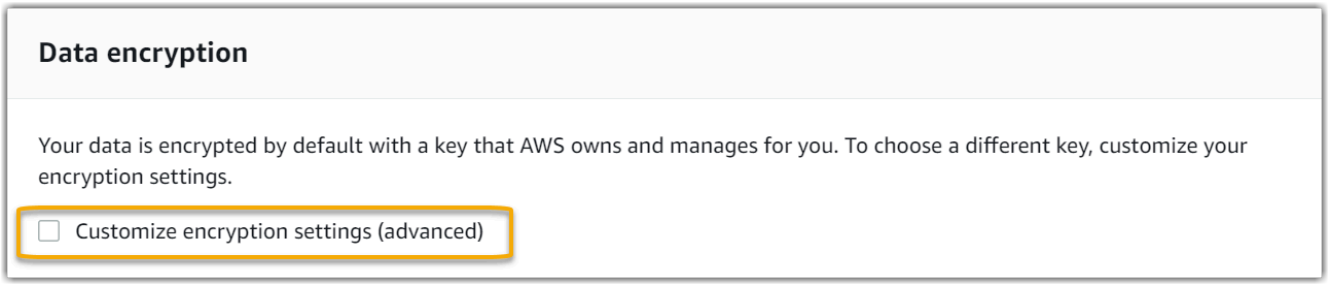
콘솔을 사용하여 Audit Manager를 활성화하려면

1. https://console.aws.amazon.com/auditmanager/home에서 AWS Audit Manager 콘솔을 엽니다.
2. IAM 자격 증명의 보안 인증 정보를 사용하여 로그인합니다.
3. 설정AWS Audit Manager을 선택합니다.

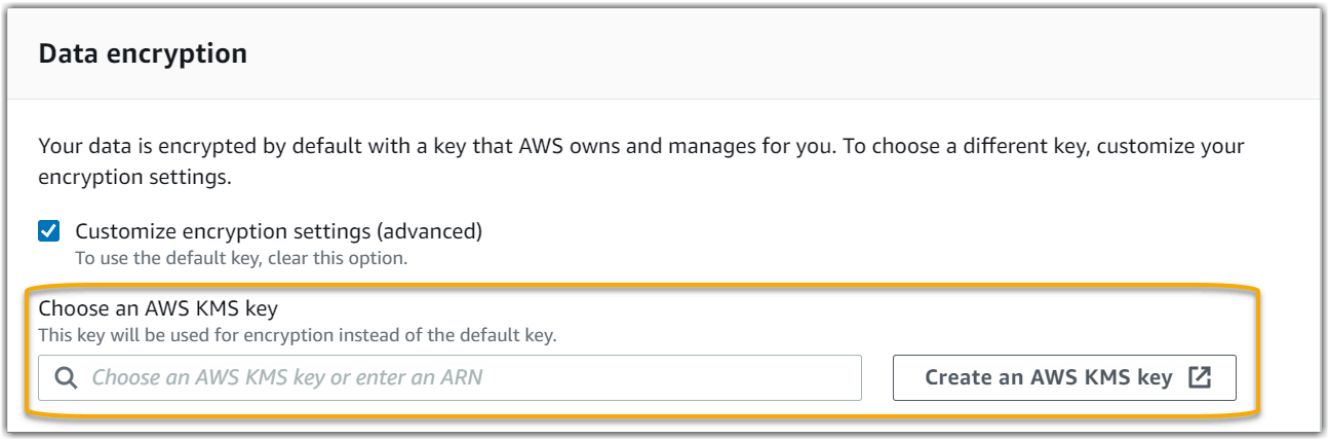
4. 권한에서는 별도의 작업이 필요하지 않습니다. 이는 Audit Manager가 사용자를 대신하여 서비스 연결 역할을 사용하여 데이터 소스에 연결하기 때문입니다. IAM 서비스 연결 역할 권한 보기를 선택하여 서비스 연결 역할을 검토할 수 있습니다.



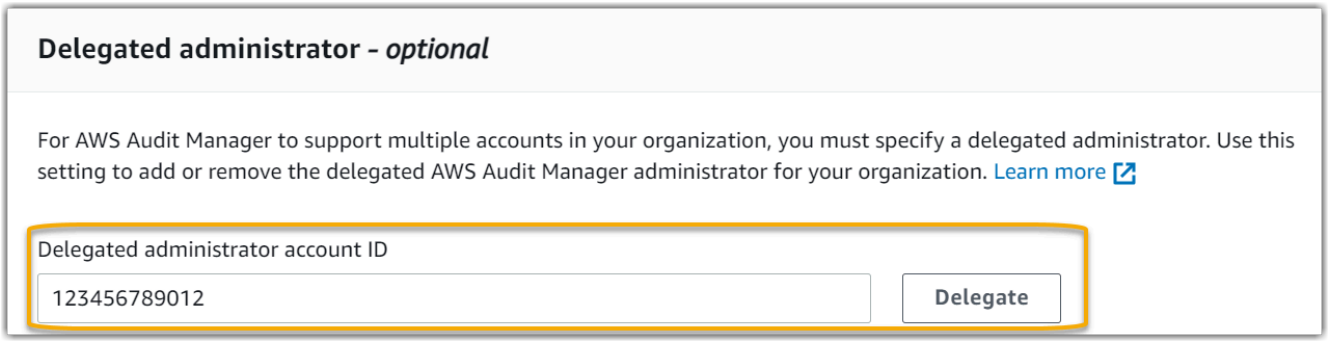
5. 데이터 암호화에서 기본 옵션은 Audit Manager가 데이터를 안전하게 저장하기 위한 AWS KMS key를 만들고 관리하는 것입니다.



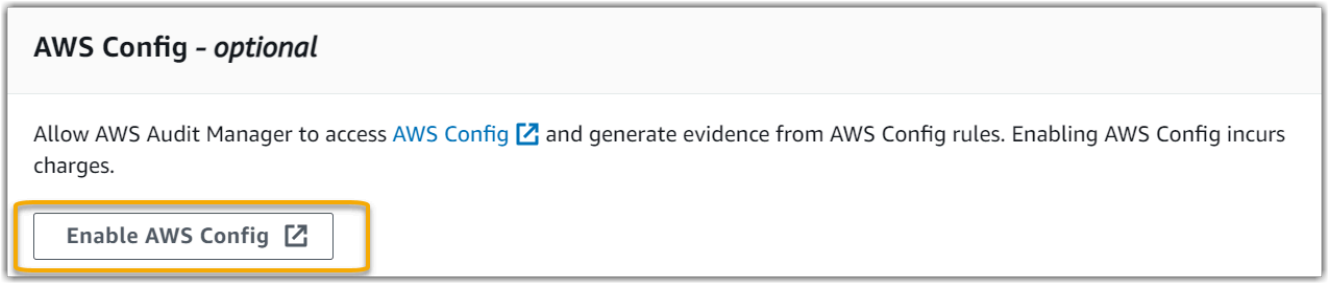
Audit Manager에서 자체 고객 관리형 키를 사용하여 데이터를 암호화하려면 암호화 설정 사용자 지정 (고급) 옆의 확인란을 선택합니다. 기존 KMS 키를 선택하거나 새로 만들 수 있습니다.



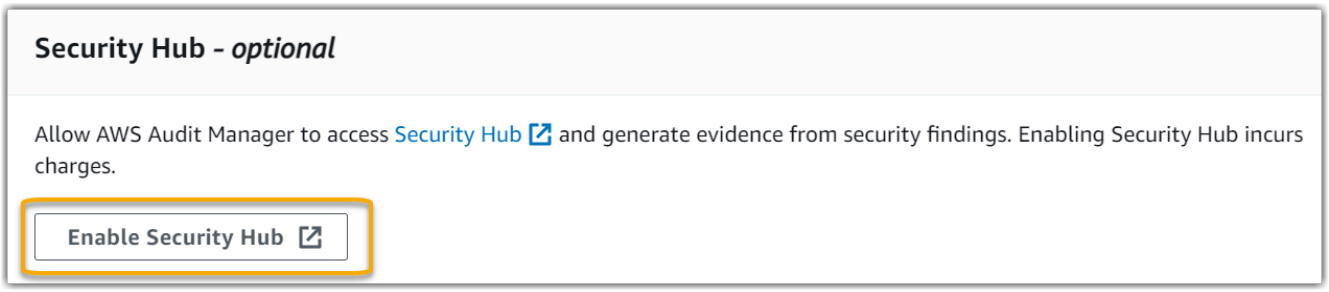
6. (선택 사항) 위임된 관리자 - 선택 사항에서 Audit Manager가 여러 계정에 대한 평가를 실행하도록 하려면 위임된 관리자 계정을 지정할 수 있습니다. 자세한 내용 및 권장 사항은 Audit Manager 사용을 위한 AWS Organizations 활성화 및 설정 섹션을 참조하세요.



7. (선택 사항) AWS Config – 선택 사항에서 최적의 환경을 위해 AWS Config를 활성화하는 것이 좋습니다. 이를 통해 Audit Manager는 AWS Config 규칙을 사용하여 증거를 생성할 수 있습니다. 지침 및 권장 설정은 Audit Manager 사용을 위한 AWS Config 활성화 및 설정 섹션을 참조하세요.



8. (선택 사항) Security Hub - 선택 사항에서 최적의 환경을 위해 Security Hub를 활성화하는 것이 좋습니다. 이를 통해 Audit Manager는 Security Hub 검사를 사용하여 증거를 생성할 수 있습니다. 지침 및 권장 설정은 Audit Manager 사용을 위한 AWS Security Hub 활성화 및 설정 섹션을 참조하세요.



9. 설정 완료를 선택하여 설정 프로세스를 마칩니다.

AWS CLI

AWS CLI를 사용하여 Audit Manager를 활성화하려면

명령줄에서 다음 설정 파라미터를 사용하는 register-account 명령을 실행합니다.

- `--kms-key` (선택 사항) - 이 파라미터를 사용하여 고객 관리형 키를 사용하는 Audit Manager 데이터를 암호화할 수 있습니다. 여기서 옵션을 지정하지 않으면 Audit Manager가 데이터의 안전한 저장을 위해 사용자를 대신하여 AWS KMS key를 생성하고 관리합니다.
- `--delegated-admin-account` (선택 사항) - 이 파라미터를 사용하여 Audit Manager에 대한 조직의 위임된 관리자 계정을 지정합니다. 여기에 옵션을 지정하지 않으면 위임된 관리자가 등록되지 않습니다.

입력 예제(`#####  ###`를 자신의 정보로 대체):

```
aws auditmanager register-account \
--kms-key arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab \
--delegated-admin-account 111122224444
```

출력 예제:

```
{
    "status": "ACTIVE"
}
```

AWS CLI에 대한 자세한 내용과 AWS CLI 도구 설치에 대한 지침은 AWS Command Line Interface 사용 설명서에서 다음을 참조하십시오.

- AWS 명령줄 인터페이스 사용 설명서
- AWS Command Line Interface를 이용한 설정

Audit Manager API

Audit Manager API를 사용하여 Audit Manager를 활성화하려면

다음 설정 파라미터와 함께 RegisterAccount 작업을 사용합니다.

- kmsKey(선택 사항) - 이 파라미터를 사용하면 고객 관리형 키를 사용하여 Audit Manager 데이터를 암호화할 수 있습니다. 여기서 옵션을 지정하지 않으면 Audit Manager가 데이터의 안전한 저장을 위해 사용자를 대신하여 AWS KMS key를 생성하고 관리합니다.
- delegatedAdminAccount (선택 사항) - 이 파라미터를 사용하여 Audit Manager에 대한 조직의 위임된 관리자 계정을 지정합니다. 지정하지 않으면 위임된 관리자가 등록되지 않습니다.

입력 예제(##### ###를 자신의 정보로 대체):

```
{
    "kmsKey":"arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab",
    "delegatedAdminAccount":"111122224444"
}
```

출력 예제:

```
{
  "status": "ACTIVE"
}
```

추천

Audit Manager의 최적의 환경을 위해 다음 AWS 서비스를 설정하고 를 활성화하는 것이 좋습니다.

주제

- 권장 Audit Manager 기능 설정
- 다른 AWS 서비스와의 권장 통합 설정

권장 Audit Manager 기능 설정

Audit Manager를 활성화한 후 증거 찾기 기능을 활성화하는 것이 좋습니다.

증거 찾기는 Audit Manager에서 증거를 검색할 수 있는 강력한 방법을 제공합니다. 찾고 있는 내용을 찾기 위해 깊이 중첩된 증거 폴더를 탐색하는 대신 증거 찾기를 사용하여 증거를 빠르게 쿼리할 수 있습니다. 증거 찾기를 위임 관리자로 사용하면 조직의 모든 멤버 계정에서 증거를 검색할 수 있습니다. 필터와 그룹화를 조합하여 이용하면 검색 쿼리의 범위를 점진적으로 좁힐 수 있습니다. 예를 들어 시스템 상태를 높은 수준으로 보려면 광범위한 검색을 수행하고 평가, 날짜 범위 및 리소스 규정 준수별로 필터링합니다. 특정 리소스를 개선하는 것이 목표인 경우 특정 컨트롤 또는 리소스 ID에 대한 증거를 찾기 위해 좁은 검색을 수행할 수 있습니다. 필터를 정의한 후에는 일치하는 검색 결과를 그룹화하여 미리 본 다음에 평가 보고서를 생성할 수 있습니다.

증거 찾기를 이용하려면 Audit Manager 설정에서 이 기능을 활성화해야 합니다. 지침은 증거 찾기 설정 섹션을 참조하세요.

다른 AWS 서비스와의 권장 통합 설정

Audit Manager의 최적의 환경을 위해 다음 AWS 서비스를 활성화하는 것이 좋습니다.

- AWS Organizations- Organizations를 사용하여 여러 계정에서 Audit Manager 평가를 실행하고 증거를 위임된 관리자 계정으로 통합할 수 있습니다.
- AWS Security Hub 및 AWS Config - 이러한 AWS 서비스를 활성화하면 Audit Manager 평가에서 컨트롤을 위한 데이터 소스 유형으로 사용할 수 있습니다. 그러면 Audit Manager는 이러한 서비스에서 직접 규정 준수 검사 결과를 보고할 수 있습니다.

주제

AWS Config 활성화 및 설정(선택 사항)

Audit Manager의 많은 컨트롤은 AWS Config를 데이터 소스 유형으로 사용합니다. 이러한 컨트롤을 지원하려면 Audit Manager가 활성화된 각 AWS 리전의 모든 계정에서 AWS Config를 활성화해야 합니다. Audit Manager가 AWS Config를 데이터 소스 유형으로 사용하는 컨트롤에 대한 증거를 수집하려고 시도하는데 관련 AWS Config 규칙이 활성화되지 않은 경우, 해당 컨트롤에 대한 증거가 수집되지 않습니다.

Audit Manager는 사용자를 위해 AWS Config를 관리하지 않습니다. 다음 단계에 따라 AWS Config를 활성화하고 해당 설정을 구성할 수 있습니다.

AWS Config를 Audit Manager와 통합하는 태스크

- 1단계: AWS Config 활성화
- 2단계: Audit Manager 사용을 위한 AWS Config 설정 구성

1단계: AWS Config 활성화

AWS Config 콘솔 또는 API를 사용하여 AWS Config를 활성화할 수 있습니다. 지침을 보려면 AWS Config 개발자 안내서의 AWS Config 시작하기를 참조하세요.

2단계: Audit Manager 사용을 위한 AWS Config 설정 구성

> **Important**
>
> AWS Config 활성화는 선택적 권장 사항입니다. 하지만 AWS Config를 활성화하는 경우 다음 설정이 필요합니다.

AWS Config를 활성화한 후에는 AWS Config 규칙을 활성화하거나 감사와 관련된 규정 준수 표준에 대한 규정 준수 팩을 배포해야 합니다. 이 단계를 통해 Audit Manager는 활성화한 AWS Config 규칙에 대한 결과를 가져올 수 있습니다.

AWS Config 규칙을 활성화한 후 해당 규칙의 파라미터를 검토하는 것이 좋습니다. 그런 다음 선택한 규정 준수 프레임워크의 요구 사항을 기준으로 해당 파라미터를 검증해야 합니다. 필요한 경우 AWS Config에 있는 규칙의 파라미터를 업데이트하여 프레임워크 요구 사항과 일치하는지 확인할 수 있습니다. 이렇게 하면 평가를 통해 주어진 프레임워크에 대한 올바른 규정 준수 검사 증거를 수집할 수 있습니다.

예를 들어, CIS v1.2.0에 대한 평가를 생성한다고 가정해 보겠습니다. 이 프레임워크에는 1.4 – 90일이 되기 전에 액세스 키가 교체되는지 여부를 확인합니다라는 컨트롤이 있습니다. AWS Config의 access-keys-rotated 규칙에는 기본값이 90일인 `maxAccessKeyAge` 파라미터가 있습니다. 결과적으로, 규칙은 컨트롤 요구 사항에 맞게 조정됩니다. 기본값을 사용하지 않는 경우 사용하는 값이 CIS v1.2.0의 90일 요구 사항 이상인지 확인하세요.

AWS Config 설명서에서 각 관리형 규칙에 대한 기본 파라미터 세부 정보를 찾을 수 있습니다. 규칙을 구성하는 방법에 대한 지침은 AWS Config 관리형 규칙 작업 섹션을 참조하세요.

AWS Security Hub 활성화 및 설정(선택 사항)

Audit Manager의 많은 컨트롤은 Security Hub를 데이터 소스 유형으로 사용합니다. 이러한 컨트롤을 지원하려면 Audit Manager가 활성화된 각 리전의 모든 계정에서 Security Hub를 활성화해야 합니다. Audit Manager가 Security Hub를 데이터 소스 유형으로 사용하는 컨트롤 기능에 대한 증거를 수집하려고 하는데 관련 Security Hub 표준이 활성화되지 않은 경우, 해당 컨트롤에 대한 증거는 수집되지 않습니다.

Audit Manager는 사용자를 위해 Security Hub를 관리하지 않습니다. 다음 단계에 따라 Security Hub를 활성화하고 해당 설정을 구성할 수 있습니다.

AWS Security Hub를 Audit Manager와 통합하는 태스크

- 1단계: AWS Security Hub 활성화
- 2단계: Audit Manager 사용을 위한 Security Hub 설정 구성

1단계: AWS Security Hub 활성화

콘솔 또는 API를 사용하여 Security Hub를 활성화할 수 있습니다. 지침은 AWS Security Hub 사용 설명서의 AWS Security Hub 설정을 참조하세요.

2단계: Audit Manager 사용을 위한 Security Hub 설정 구성

> **Important**
>
> Security Hub 활성화는 선택적 권장 사항입니다. 하지만 Security Hub를 활성화하는 경우 다음 설정이 필요합니다.

Security Hub를 활성화하면 다음 작업도 수행해야 합니다.

- AWS Config 활성화 및 리소스 기록 구성 - Security Hub는 서비스 연결 AWS Config 규칙을 사용하여 컨트롤에 대한 대부분의 보안 검사를 수행합니다. 이러한 컨트롤을 지원하려면 AWS Config를 활성화하고, 활성화된 각 표준에서 활성화한 컨트롤에 필요한 리소스를 기록하도록 구성해야 합니다.
- 모든 보안 표준 활성화 - 이 단계를 통해 Audit Manager는 지원되는 모든 규정 준수 표준에 대한 결과를 가져올 수 있습니다.
- Security Hub에서 통합 컨트롤 결과 설정 활성화 - 이 설정은 2023년 2월 23일 또는 그 이후에 Security Hub를 사용하도록 설정하는 경우 기본적으로 켜집니다.

> **Note**
>
> 통합 결과를 활성화하면 Security Hub는 각 보안 검사에 대해 단일 검색 결과를 생성합니다(여러 표준에서 동일한 검사를 사용하는 경우에도 해당). 각 Security Hub 검사 결과는 Audit Manager에서 하나의 고유한 리소스 평가로 수집됩니다. 결과적으로 통합된 조사 결과를 사용하면 Audit Manager가 Security Hub 조사 결과에 대해 수행하는 총 고유 리소스 평가 건수가 줄어듭니다. 이러한 이유로, 통합된 결과를 이용하면 Audit Manager 사용 비용을 줄일 수 있는 경우가 많습니다. Security Hub를 데이터 소스 유형으로 사용하는 방법에 대한 자세한 내용은 AWS Security Hub 에서 지원하는 제어 AWS Audit Manager 섹션을 참조하세요. Audit Manager 요금에 대한 자세한 정보는 AWS Audit Manager 요금을 참조하십시오.

AWS Organizations를 사용하고 멤버 계정에서 Security Hub 증거를 수집하려는 경우 Security Hub에서 다음 단계도 수행해야 합니다.

조직의 Security Hub 설정을 지정하려면

1. AWS Management Console에 로그인하고 https://console.aws.amazon.com/securityhub/에서 AWS Security Hub 콘솔을 엽니다.

2. AWS Organizations 관리 계정을 사용하여 계정을 Security Hub의 위임된 관리자로 지정합니다. 자세한 내용은 AWS Security Hub 사용 설명서의 Security Hub 관리자 계정 지정을 참조하세요.

> **Note**
>
> Security Hub에서 지정하는 위임된 관리자 계정이 Audit Manager에서 사용하는 것과 동일한지 확인하세요.

3. Organizations 위임된 관리자 계정을 사용하여 설정, 계정으로 이동하여 모든 계정을 선택한 다음 자동 등록을 선택하여 멤버로 추가합니다. 자세한 내용은 AWS Security Hub 사용 설명서의 조직에서 멤버 계정 활성화를 참조하세요.
4. 조직의 모든 멤버 계정에 대해 AWS Config를 활성화합니다. 자세한 내용은 AWS Security Hub 사용 설명서의 조직에서 멤버 계정 활성화를 참조하세요.
5. 조직의 모든 멤버 계정에 대해 PCI DSS 보안 표준을 활성화합니다. AWS CIS Foundations Benchmark 표준과 AWS Foundational Best Practices는 이미 기본적으로 활성화되어 있습니다. 자세한 내용은 AWS Security Hub 사용 설명서의 보안 표준 활성화 섹션을 참조하세요.

AWS Organizations 활성화(선택 사항)

Audit Manager는 AWS Organizations과의 통합을 통해 여러 계정을 지원합니다. Audit Manager는 여러 계정에서 평가를 실행하고 증거를 위임된 관리자 계정으로 통합할 수 있습니다. 위임된 관리자에게는 조직을 신뢰 영역으로 하여 Audit Manager 리소스를 만들고 관리할 수 있는 권한이 있습니다. 관리 계정만 위임된 관리자를 지정할 수 있습니다.

AWS Organizations를 Audit Manager와 통합하는 태스크

- 1단계: 조직 생성 또는 조직 가입
- 2단계: 조직 내에서 모든 기능을 활성화합니다.
- 3단계: Audit Manager에 위임된 관리자 지정

1단계: 조직 생성 또는 조직 가입

AWS 계정이 조직에 속해 있지 않은 경우 조직을 만들거나 조직에 가입할 수 있습니다. 지침은 AWS Organizations 사용 설명서의 조직 생성 및 관리를 참조하세요.

2단계: 조직 내에서 모든 기능을 활성화합니다.

다음으로, 조직 내에서 모든 기능을 활성화해야 합니다. 지침은 AWS Organizations 사용 설명서의 조직 내 모든 기능 활성화를 참조하세요.

3단계: Audit Manager에 위임된 관리자 지정

Organizations 관리 계정을 사용하여 Audit Manager를 활성화한 다음 위임된 관리자를 지정하는 것이 좋습니다. 그런 다음 위임된 관리자 계정을 사용하여 로그인하고 평가를 실행할 수 있습니다. 가장 좋은 방법은 관리 계정 대신 위임된 관리자 계정으로만 평가를 생성하는 것입니다.

> **Warning**
>
> Organizations 관리 계정을 사용하여 위임된 관리자를 지정한 후에는 관리 계정이 더 이상 Audit Manager에서 추가 평가를 생성할 수 없습니다. 또한 관리 계정에서 생성한 기존 평가에 대한 증거 수집도 중지됩니다. 대신 Audit Manager는 조직의 평가를 관리하는 기본 계정인 위임된 관리자에게 증거를 수집하여 첨부합니다.

Audit Manager를 활성화한 후 위임된 관리자를 추가하거나 변경하려면 AWS Audit Manager 설정, 위임된 관리자를 참조하세요.

고려해야 할 문제:

- Audit Manager에서는 관리 계정을 위임된 관리자로 사용할 수 없습니다.
- 둘 이상의 AWS 리전에서 Audit Manager를 활성화하려면 각 리전에서 위임된 관리자 계정을 별도로 지정해야 합니다. Audit Manager 설정에서 모든 리전에 대해 동일한 위임 관리자 계정을 지정해야 합니다.
- Audit Manager를 활성화할 때 고객 관리형 키를 제공한 경우 위임된 관리자 계정에 해당 KMS 키에 대한 액세스 권한이 있는지 확인합니다. Audit Manager 암호화 설정을 검토 및 변경하려면 데이터 암호화 섹션을 참조하세요.
- Audit Manager의 일반적인 조직 및 위임된 관리자 문제에 대한 해결 방법은 위임된 관리자 및 AWS Organizations 문제 해결 섹션을 참조하세요.

다음으로 무엇을 할까요?

이제 Audit Manager를 설정했으므로 서비스 사용을 시작할 준비가 되었습니다. 콘솔의 설정 페이지를 방문하여 Audit Manager를 설정할 때 선택한 설정을 업데이트할 수도 있습니다.

Audit Manager 시작하기

첫 번째 평가를 생성하는 방법을 안내하는 자습서를 따라 Audit Manager에서 시작할 수 있습니다. 자세한 내용은 Tutorial for Audit Owners: Creating an assessment 섹션을 참조하세요.

Audit Manager 설정 업데이트

설정은 언제든지 업데이트할 수 있습니다. 자세한 내용은 AWS Audit Manager 설정 섹션을 참조하세요.

AWS Audit Manager 시작하기

이 단원의 단계별 자습서를 통해 AWS Audit Manager를 사용하여 작업을 수행하는 방법을 알아봅니다.

> **Tip**
>
> 다음 자습서는 대상 사용자별로 분류되어 있습니다. 감사 소유자 또는 대리인으로서의 역할에 따라 적합한 자습서를 선택하십시오.
>
> - 감사 소유자는 평가 생성 및 관리를 담당하는 Audit Manager 사용자입니다. 비즈니스 세계에서 감사 소유자는 일반적으로 거버넌스, 위험 관리 및 규정 준수(GRC) 전문가입니다. 그러나 Audit Manager의 경우 SecOps 또는 DevOps 팀의 개인도 감사 담당자의 사용자 페르소나를 가정할 수 있습니다. 감사 소유자는 특정 통제 항목을 검토하고 증거를 검증하기 위해 주제 전문가(대리인이라고도 함)에게 지원을 요청할 수 있습니다. Audit Manager는 평가를 관리하는 데 필요한 권한이 있어야 합니다.
> - 대리인은 전문 기술 또는 비즈니스 전문 지식을 갖춘 주제 전문가입니다. Audit Manager 평가를 소유하거나 관리하지는 않지만 여전히 평가에 기여할 수 있습니다. 대리인은 감사 담당자가 자신의 전문 분야에 해당하는 통제 항목에 대한 증거를 검증하는 등의 작업을 수행하도록 지원합니다. 대리인은 Audit Manager에서 제한된 권한을 가집니다. 이는 감사 소유자가 전체 평가가 아닌 특정 통제 세트를 검토용으로 위임하기 때문입니다.
>
> 이러한 페르소나 및 기타 Audit Manager 개념에 대한 자세한 내용은 이 가이드 AWS Audit Manager 개념 및 용어 섹션의 감사 소유자 및 대리인을 참조하십시오. 각 페르소나의 권장 IAM 권한에 대한 자세한 내용은 사용자 페르소나에 대한 권장 정책은 다음과 같습니다. AWS Audit Manager 단원을 참조하십시오.

Audit Manager 자습서

평가 생성

대상: 감사 소유자

개요: 단계별 지침에 따라 첫 번째 평가를 작성하고 빠르게 시작하고 실행하세요. 이 자습서는 하나의 표준 프레임워크를 사용하여 평가를 생성하고 증거의 자동 수집을 시작하는 방법을 안내합니다.

통제 세트 검토

대상: 대리자

개요: 자신의 전문 분야에 속하는 통제 항목에 대한 증거를 검토하여 감사 소유자를 지원하십시오. 통제 세트 및 관련 증거를 검토하고, 의견을 추가하고, 추가 증거를 업로드하고, 통제 상태를 업데이트하는 방법을 알아보십시오.

감사 소유자를 위한 자습서: 평가 생성

이 자습서에서는 AWS Audit Manager에 대해 소개합니다. 이 자습서에서는 AWS Audit Manager 샘플 프레임워크를 사용하여 평가를 생성합니다. 평가를 생성하면 해당 프레임워크의 통제 항목에 대한 자동 증거 수집의 지속적인 프로세스를 시작할 수 있습니다.

이 자습서에서는 다음을 수행하는 방법을 보여줍니다.

- 표준 프레임워크를 선택하여 평가를 생성할 수 있습니다.
- 평가에 포함할 AWS 계정을 지정하십시오.
- 평가에 포함할 AWS 서비스를 지정하십시오.
- 평가의 감사 소유자를 지정하십시오.
- 평가 검토 및 생성

이 자습서를 시작하기 전에 다음 조건을 충족하는지 확인하십시오.

- AWS Audit Manager 설정에 설명된 모든 사전 요구 사항을 완료했습니다. 이 자습서를 완료하려면 AWS 계정과 AWS Audit Manager 콘솔을 사용해야 합니다.
- IAM ID에는 AWS Audit Manager에서 평가를 생성하고 관리할 수 있는 적절한 권한이 부여됩니다. 이러한 권한을 부여하는 두 가지 권장 정책은 예 2: 전체 관리자 액세스 허용과 예 3: 관리 액세스 허용입니다.
- Audit Manager의 용어 및 기능에 대해 잘 알고 계실 것입니다. 일반 개요는 AWS Audit Manager란 무엇인가요? 및 AWS Audit Manager 개념 및 용어를 참조하십시오.

> **Note**
>
> AWS Audit Manager은 특정 규정 준수 프레임워크 및 규정의 준수 여부를 확인하는 것과 관련된 증거를 수집하는 데 도움이 됩니다. 하지만, 규정 준수 자체를 평가하지는 않습니다. 따라서,

AWS Audit Manager를 통해 수집되는 증거에는 감사에 필요한 AWS 사용량에 대한 모든 정보가 포함되어 있지 않을 수 있습니다. AWS Audit Manager가 법률 고문이나 규정 준수 전문가를 대신하지는 못합니다.

1단계: 평가 세부 정보 지정

첫 번째 단계에서는 프레임워크를 선택하고 평가를 위한 기본 정보를 제공합니다.

평가 세부 정보를 지정하려면

1. https://console.aws.amazon.com/auditmanager/home 에서 AWS Audit Manager 콘솔을 엽니다.
2. AWS Audit Manager 시작을 선택합니다.
3. 탐색 창에서 시작하기를 선택한 후 프레임워크로 시작을 선택합니다.
4. 원하는 프레임워크를 선택한 다음 프레임워크에서 평가 생성을 선택합니다. 이 예에서는 AWS Audit Manager 샘플 프레임워크를 사용합니다.
5. 평가 이름에서, 평가에 대한 이름을 입력합니다.
6. (선택 사항) 평가 설명에 평가에 대한 설명을 입력합니다.
7. 평가 보고서 대상에서 평가 보고서를 저장할 Amazon S3 버킷을 선택합니다.
8. 프레임워크에서 AWS Audit Manager 샘플 프레임워크(또는 선택한 프레임워크)가 선택되었는지 확인합니다.
9. 태그에서, 새 태그 추가를 선택하여 태그를 평가에 연결합니다. 각 태그에 대한 키 및 값을 지정할 수 있습니다. 태그 키는 필수이며 이 평가를 검색할 때 검색 기준으로 사용할 수 있습니다. AWS Audit Manager의 태그에 대한 자세한 내용은 AWS Audit Manager 리소스에 태그 지정 단원을 참조하십시오.
10. 다음(Next)을 선택합니다.

2단계: 범위 내 AWS 계정 지정

다음으로 평가 범위에 포함하려는 AWS 계정을 지정합니다.

AWS Audit Manager이 AWS Organizations와 통합되므로 여러 계정에서 Audit Manager 평가를 실행하고 증거를 위임된 관리자 계정으로 통합할 수 있습니다. Audit Manager에서 조직을 활성화하려면(아직 활성화하지 않은 경우) 이 가이드 설정 페이지의 AWS Organizations 활성화(선택 사항)를 참조하십시오.

> **Note**
>
> Audit Manager는 평가 범위 내에서 최대 약 150개의 계정을 지원할 수 있습니다. 150개가 넘는 계정을 포함하려고 하면 평가 생성이 실패할 수 있습니다.

범위 내 계정 지정하기

1. AWS 계정에서 평가 범위에 포함하려는 AWS 계정을 선택합니다.
   - AWS Audit Manager에서 조직을 활성화한 경우 여러 계정이 나열됩니다.
   - Audit Manager에서 조직을 활성화하지 않은 경우 현재 계정만 나열됩니다.
2. 다음(Next)을 선택합니다.

3단계: 범위 내 AWS 서비스 지정

앞서 선택한 프레임워크는 Audit Manager가 모니터링하고 증거를 수집하는 AWS 서비스를 정의합니다.

Audit Manager 콘솔을 사용하여 표준 프레임워크에서 평가를 생성하면 범위 내 서비스 목록이 미리 선택되며 편집할 수 없습니다. 이는 Audit Manager가 자동으로 데이터 소스 및 서비스를 매핑하고 선택하기 때문입니다. 이 선택은 표준 프레임워크의 요구 사항에 따라 이루어집니다. 나열된 AWS 서비스가 선택되지 않은 경우 Audit Manager는 해당 서비스와 관련된 리소스에서 증거를 수집하지 않습니다. 서비스를 선택했지만 해당 환경에서 구독하지 않은 경우에도 마찬가지입니다.

자습서의 이 단계에서는 프레임워크 정의를 기반으로 평가 범위에 속하는 AWS 서비스를 검토할 수 있습니다. 프레임워크와 프레임워크에 액세스하고 검토하는 방법에 대해 자세히 알아보려면 이 가이드의 프레임워크 라이브러리 섹션을 참조하십시오.

범위 내 AWS 서비스 지정하기

1. AWS 서비스에서 이 평가의 범위에 속하는 서비스 목록을 검토하십시오.
2. 다음(Next)을 선택합니다.

> **Tip**
>
> 범위 내에서 서비스 목록을 편집해야 하는 경우 Audit Manager에서 제공하는 CreateAssessment API를 사용하여 편집할 수 있습니다.

또는 표준 프레임워크를 사용자 지정한 다음 사용자 지정 프레임워크에서 평가를 생성할 수도 있습니다.

4단계: 감사 소유자 지정

이 단계에서는 평가의 감사 소유자를 지정합니다. 감사 소유자는 일반적으로 GRC, SecOps 또는 DevOps 팀 소속으로, Audit Manager 평가를 관리하는 직장의 개인입니다. AWSAuditManagerAdministratorAccess 정책을 사용하는 것이 좋습니다.

감사 소유자를 지정하려면

1. 감사 소유자에서 평가에 사용할 감사 소유자를 선택합니다. 추가 감사 소유자를 찾으려면 검색 창을 사용하여 이름 또는 AWS 계정별로 검색하십시오.
2. 다음(Next)을 선택합니다.

5단계: 검토 및 생성

평가를 위한 정보를 검토합니다. 단계 정보를 변경하려면 편집을 선택합니다. 완료되면 평가 만들기를 선택하여 첫 번째 평가를 시작하고 지속적인 증거 수집을 시작합니다.

평가를 생성한 후에는 평가 상태를 비활성으로 변경할 때까지 증거 수집이 계속됩니다. 또는 통제 상태를 비활성으로 변경하여 특정 통제에 대한 증거 수집을 중지할 수 있습니다.

Note

자동 증거는 평가를 생성한 지 24시간 후에 사용할 수 있습니다. AWS Audit Manager은 여러 데이터 소스에서 증거를 자동으로 수집하며, 증거 수집 빈도는 증거 유형에 따라 달라집니다. 자세한 내용은 이 가이드의 증거 수집 빈도을 참조하세요.

추가 정보

이 자습서에 소개된 개념 및 도구에 대해 계속 자세히 알아보는 것이 좋습니다. 다음 리소스를 검토하여 그렇게 할 수 있습니다.

- 평가 검토 — 평가의 다양한 구성 요소를 탐색할 수 있는 평가 페이지를 소개합니다.

- AWS Audit Manager에서의 평가 — 이 자습서를 기반으로 하며 평가 관리의 개념 및 태스크에 대해 깊이 있게 소개합니다. 이 문서에서는 특히 다음 항목을 확인하는 것이 좋습니다.
  - 다른 프레임워크에서 평가를 생성하는 방법
  - 평가에서 증거를 검토하고 평가 보고서를 생성하는 방법
  - 평가 상태를 변경하거나 평가를 삭제하는 방법
- 프레임워크 라이브러리 — 프레임워크 라이브러리를 소개하고 고유한 규정 준수 요구 사항에 맞는 사용자 지정 프레임워크를 만드는 방법을 설명합니다.
- 컨트롤 라이브러리 — 통제 라이브러리를 소개하고 사용자 지정 프레임워크에서 사용할 사용자 지정 통제를 만드는 방법을 설명합니다.
- AWS Audit Manager 개념 및 용어 — Audit Manager에서 사용되는 개념 및 용어에 대한 정의를 제공합니다.
- [비디오] AWS Audit Manager을 사용하여 증거 수집 및 감사 데이터 관리 — 이 자습서에서 설명하는 평가 작성 프로세스와 통제 검토 및 평가 보고서 생성과 같은 기타 작업을 보여줍니다.

대리인을 위한 자습서: 통제 집합 검토

이 자습서에서는 AWS Audit Manager에서 감사 소유자가 공유한 통제 세트를 검토하는 방법을 설명합니다.

감사 소유자는 Audit Manager를 사용하여 평가를 작성하고 해당 평가에 나열된 통제 항목에 대한 증거를 수집합니다. 감사 담당자가 컨트롤 세트에 대한 증거를 검증할 때 질문이 있거나 도움이 필요한 경우가 있습니다. 이 경우 감사 담당자는 주제 전문가에게 검토를 위해 컨트롤 세트를 위임할 수 있습니다.

대리인은 감사 소유자가 수집된 증거를 검토하여 자신의 전문 분야에 해당하는 통제 항목이 있는지 검토할 수 있도록 도와줍니다.

이 자습서에서는 다음을 수행하는 방법을 보여줍니다.

- 감사 소유자가 보낸 액세스 알림
- 통제 집합 및 관련 증거 검토
- 통제를 뒷받침하는 수동 증거 업로드
- 검토 중인 통제에 의견 추가
- 통제 상태 업데이트
- 검토가 완료되면 검토된 통제 세트를 감사 소유자에게 제출

이 자습서를 시작하기 전에 다음 조건을 충족하는지 확인하십시오.

- AWS 계정이 설정되었습니다. 이 자습서를 완료하려면 AWS 계정과 AWS Audit Manager 콘솔을 모두 사용해야 합니다. 자세한 내용은 AWS Audit Manager 설정 섹션을 참조하세요.
- Audit Manager의 용어 및 기능에 대해 잘 알고 계실 것입니다. Audit Manager에 대한 일반적인 개요는 AWS Audit Manager란 무엇인가요? 및 AWS Audit Manager 개념 및 용어을 참조하십시오.

1단계: 알림 액세스

먼저 AWS Audit Manager에 로그인해 알림에 액세스하여 검토를 위해 위임된 통제 세트를 확인할 수 있습니다.

알림에 액세스하려면

1. https://console.aws.amazon.com/auditmanager/home에서 AWS Audit Manager 콘솔을 엽니다.
2. 왼쪽 탐색 창에서 알림을 선택합니다. 또는 페이지 상단의 파란색 플래시 막대에서 알림 보기를 선택하여 알림 페이지를 엽니다.
3. 알림 페이지에서는 자신에게 위임된 통제 집합 목록을 검토할 수 있습니다. 이 알림 표에는 다음 정보가 포함됩니다.
   - 날짜 - 컨트롤 세트를 위임한 날짜.
   - 평가 — 통제 세트와 연결된 평가의 이름입니다. 평가 이름을 선택하여 평가 세부 정보 페이지를 열 수 있습니다.
   - 통제 세트 — 검토를 위해 사용자에게 위임된 통제 세트의 이름입니다.
   - 소스 - 컨트롤 세트를 위임한 사용자 또는 역할.
   - 설명 - 감사 소유자가 제공한 검토 지침입니다.

> **Tip**
>
> 또한 SNS 주제를 구독하여 검토를 위해 통제 세트가 할당되면 이메일 알림을 받을 수 있습니다. 자세한 내용은 AWS Audit Manager의 알림을 참조하십시오.

2단계: 통제 세트 및 관련 증거 검토

다음 단계는 감사 소유자가 위임한 통제 세트를 검토하는 것입니다. 통제 수단과 그 증거를 검토하여 통제를 위한 추가 조치가 필요한지 판단할 수 있습니다. 추가 조치에는 규정 준수를 입증하기 위해 추가 증거를 수동으로 업로드하거나 해당 통제에 대한 의견을 남기는 것이 포함될 수 있습니다.

컨트롤 세트를 검토하려면

1. 알림 페이지에서 자신에게 위임된 통제 세트 목록을 검토하십시오. 그런 다음 검토할 평가를 식별하고 관련 평가의 이름을 선택하십시오.
2. 평가 세부 정보 페이지의 컨트롤 탭에서 컨트롤 세트 테이블까지 아래로 스크롤합니다.
3. 컨트롤 세트별로 그룹화된 컨트롤 열에서 컨트롤 세트의 이름을 확장하여 해당 컨트롤을 표시합니다. 그런 다음 통제 이름을 선택하여 통제 세부 정보 페이지를 엽니다.
4. (선택 사항) 통제 상태 업데이트를 선택하여 통제 상태를 변경합니다. 검토를 진행하는 동안 상태를 검토 중으로 표시할 수 있습니다.
5. 증거 폴더, 데이터 소스, 의견 및 변경 로그 탭에서 통제 에 대한 정보를 검토하십시오. 각 탭에 대한 자세한 내용과 탭에 포함된 데이터를 해석하는 방법은 평가에서 통제 항목 검토를 참조하십시오.

통제에 대한 증거 검토하기

1. 컨트롤 세부 정보 페이지에서 증거 폴더 탭을 선택합니다.
2. 증거 폴더 테이블로 이동합니다. 이 테이블에는 해당 통제에 대한 증거가 들어 있는 폴더 목록이 표시됩니다. 이러한 폴더는 해당 폴더 내의 증거가 수집된 날짜를 기준으로 구성되고 이름이 지정됩니다.
3. 증거 폴더의 이름을 선택하여 엽니다. 여기에서 해당 날짜에 수집된 모든 증거의 요약을 검토할 수 있습니다. 이 요약에는 AWS Security Hub, AWS Config 또는 둘 다에서 직접 보고된 규정 준수 확인 문제의 총 수도 포함됩니다. 이 페이지의 데이터를 해석하는 방법에 대한 지침은 증거 폴더 검토를 참조하십시오.
4. 증거 폴더 요약 페이지에서 증거 테이블로 이동합니다. 시간 열에서 라인 항목을 선택하여 해당 시점에 수집된 증거의 세부 정보를 열고 검토하십시오. 증거 세부 정보 페이지의 데이터를 해석하는 방법에 대한 지침은 개별 증거 검토를 참조하세요.

3단계. 수동 증거 업로드(선택 사항)

AWS Audit Manager이 여러 통제 항목에 대한 증거를 자동으로 수집하지만 경우에 따라 추가 증거를 제공해야 할 수도 있습니다. 이러한 경우 해당 통제 준수를 입증하는 데 도움이 되는 증거를 수동으로 업로드할 수 있습니다.

수동 증거를 평가에 업로드하려면 먼저 증거를 S3 버킷에 배치해야 합니다. 지침을 보려면 Amazon Simple Storage Service 사용 설명서의 버킷 생성 및 객체 업로드를 참조하세요.

Important

각 AWS는 하나의 제어에 매일 최대 100개의 증거 파일만 수동으로 제어에 업로드할 수 있습니다. 이 일일 할당량을 초과하면 해당 제어에 대한 추가 수동 업로드가 실패합니다. 대량의 수동 증거를 단일 컨트롤에 업로드해야 하는 경우, 며칠에 걸쳐 일괄적으로 증거를 업로드하세요.

수동 증거를 통제에 업로드하려면

1. https://console.aws.amazon.com/auditmanager/home에서 AWS Audit Manager 콘솔을 엽니다.
2. 알림 페이지에서 자신에게 위임된 통제 세트 목록을 볼 수 있습니다. 근거를 추가하려는 통제 세트를 식별하고 관련 평가 이름을 선택하여 평가 세부 정보 페이지를 여십시오.
3. 통제 탭을 선택하고 통제 세트까지 아래로 스크롤한 다음 통제 이름을 선택하여 엽니다.
4. 증거 폴더 탭을 선택한 다음 수동 증거 업로드를 선택합니다.
5. 다음 페이지에서 증거의 S3 URI를 입력합니다. Amazon S3 콘솔에서 객체로 이동한 다음 S3 URI 복사를 선택하면 S3 URI를 찾을 수 있습니다.
6. 업로드를 선택하여 수동 증거를 업로드하십시오.

Note

통제가 비활성 상태인 경우 해당 통제에 대한 수동 증거를 업로드할 수 없습니다. 수동 증거를 업로드하려면 먼저 통제 상태를 검토 중 또는 검토 완료 로 변경해야 합니다. 통제 상태를 변경하는 방법에 대한 지침은 단원 5단계: 통제를 검토된 것으로 표시(선택 사항)을 참조하십시오.

4단계. 통제에 의견을 추가합니다(선택 사항).

검토하는 모든 통제에 의견을 추가할 수 있습니다. 이러한 설명은 감사 소유자가 볼 수 있습니다. 예를 들어 의견을 남겨 상태 업데이트를 제공하고 해당 통제와 관련된 문제를 해결했는지 확인할 수 있습니다.

통제에 의견을 추가하려면

1. 알림 페이지에서 자신에게 위임된 통제 세트 목록을 검토하세요. 의견을 남기고 싶은 통제 세트를 찾아 관련 평가의 이름을 선택하십시오.
2. 통제 탭을 선택하고 통제 세트 테이블까지 아래로 스크롤한 다음 통제 이름을 선택하여 엽니다.
3. 의견 탭을 선택합니다.
4. 의견 보내기에서 텍스트 상자에 의견을 입력합니다.
5. 의견 제출을 선택하여 의견을 추가합니다. 이제 의견이 통제와 관련된 다른 의견과 함께 페이지의 이전 의견 섹션 아래에 표시됩니다.

5단계: 통제를 검토된 것으로 표시(선택 사항)

통제 상태 변경은 선택 사항입니다. 그러나 통제에 대한 검토를 완료한 후 각 통제의 상태를 검토됨으로 변경하는 것이 좋습니다. 각 개별 통제의 상태에 관계없이 여전히 감사 소유자에게 통제를 제출할 수 있습니다.

통제를 검토된 것으로 표시하려면

1. 알림 페이지에서 자신에게 위임된 통제 세트 목록을 검토하십시오. 검토한 것으로 표시하려는 통제가 들어 있는 통제 세트를 찾으십시오. 그런 다음 관련 평가의 이름을 선택하여 평가 세부 정보 페이지를 엽니다.
2. 평가 세부 정보 페이지의 컨트롤 탭에서 컨트롤 세트 테이블까지 아래로 스크롤합니다.
3. 컨트롤 세트별로 그룹화된 컨트롤 열에서 컨트롤 세트의 이름을 확장하여 해당 컨트롤을 표시합니다. 통제 이름을 선택하여 통제 세부 정보 페이지를 엽니다.
4. 통제 상태 업데이트를 선택하고 상태를 검토됨으로 변경합니다.
5. 표시되는 팝업 창에서 통제 상태 업데이트를 선택하여 통제 검토를 마쳤는지 확인합니다.

6단계. 검토된 통제 세트를 감사 소유자에게 다시 제출하십시오.

모든 통제 항목 검토를 완료하면 감사 소유자에게 통제 세트를 다시 제출하여 검토가 완료되었음을 알리세요.

검토된 통제 세트를 소유자에게 다시 제출하려면

1. 알림 페이지에서 자신에게 할당된 통제 세트 목록을 검토하십시오. 감사 소유자에게 제출하고자 하는 관리 세트를 찾고 관련 평가의 이름을 선택하십시오.
2. 통제 세트 테이블까지 아래로 스크롤하여 감사 소유자에게 다시 제출할 통제 세트를 선택한 다음 검토를 위해 제출을 선택합니다.
3. 표시되는 팝업 창에서 검토를 위해 제출을 선택하기 전에 해당 통제 세트에 대한 상위 수준의 설명을 추가할 수 있습니다.

통제 기능을 감사 소유자에게 제출하면 감사 소유자는 사용자가 남긴 모든 의견을 볼 수 있습니다.

추가 정보

이 자습서에 소개된 개념에 대해 계속 자세히 알아볼 수 있습니다. 다음은 몇 가지 권장 리소스입니다.

- 평가 검토 - AWS Audit Manager에서 평가의 다양한 구성 요소를 탐색할 수 있는 평가 페이지를 소개합니다.
- 평가의 통제 항목 검토 및 평가의 증거 검토 - 각 평가의 통제 항목 및 증거를 해석하는 데 도움이 되는 데이터 정의를 제공합니다.
- AWS Audit Manager 개념 및 용어 - Audit Manager에서 사용되는 개념 및 용어에 대한 정의를 제공합니다.

Audit Manager 대시보드 사용

Audit Manager 대시보드를 사용하면 진행 중인 평가에서 규정을 준수하지 않는 증거를 시각화할 수 있습니다. 평가를 모니터링하고, 최신 정보를 얻고, 문제를 사전에 해결할 수 있는 편리하고 빠른 방법입니다. 기본적으로 대시보드는 모든 활성 평가를 하향식으로 집계하여 보여줍니다. 이 보기를 사용하면 방대한 양의 개별 증거를 먼저 살펴볼 필요 없이 평가의 문제를 시각적으로 식별할 수 있습니다.

대시보드는 Audit Manager 콘솔에 로그인할 때 나타나는 첫 번째 화면입니다. 여기에는 가장 관련성이 높은 데이터 및 핵심 성과 지표(KPI)를 보여주는 두 개의 위젯이 있습니다. 평가 필터를 사용하면 특정 평가의 KPI에 초점을 맞추도록 이 데이터를 세분화할 수 있습니다. 여기에서 제어 도메인 그룹을 검토하여 가장 규정을 준수하지 않는 증거가 있는 규제 항목을 식별할 수 있습니다. 그런 다음 기본 제어를 탐색하여 문제를 검사하고 해결할 수 있습니다.

> **Note**
>
> Audit Manager를 처음 사용하거나 진행 중인 평가가 없는 경우 대시보드에 데이터가 표시되지 않습니다. 시작하려면 평가를 생성하세요. 이로써 지속적인 증거 수집이 시작됩니다. 24시간이 지나면 집계된 증거 데이터가 대시보드에 표시되기 시작합니다. 다음 섹션을 읽으면 이 데이터를 이해하고 해석하는 방법을 파악할 수 있습니다.

이 섹션은 다음 주제를 다룹니다.

주제

대시보드 개념 및 용어

이 섹션에서는 Audit Manager 대시보드 사용을 시작하기 전에 알아두어야 할 중요한 사항을 다룹니다.

권한 및 가시성

감사 소유자와 대리인 모두 대시보드에 액세스할 수 있습니다. 즉, 이 두 페르소나 모두 AWS 계정의 모든 활성 평가에 대한 지표와 집계를 볼 수 있습니다. 동일한 정보에 액세스하면 모든 팀이 동일한 KPI와 목표에 집중할 수 있습니다.

필터

Audit Manager는 대시보드의 모든 위젯에 적용할 수 있는 페이지 수준 the section called “평가 필터”을 제공합니다.

규정을 준수하지 않는 증거

대시보드는 규정 준수 확인 증거와 비준수 결론이 있는 평가 제어 항목을 강조 표시합니다. 규정 준수 검사 증거는 AWS Config 또는 AWS Security Hub를 데이터 소스 유형으로 사용하는 컨트롤과 관련이 있습니다. 이 증거 유형의 경우 Audit Manager는 해당 서비스에서 직접 규정 준수 점검 결과를 보고합니다. Security Hub가 실패 결과를 보고하거나 AWS Config가 비준수 결과를 보고하는 경우 Audit Manager는 증거를 비준수로 분류합니다.

결정적이지 않은 증거

규정 준수 검사가 가능하지 않거나 적용 가능하지 않은 경우 증거는 결정적이지 않습니다. 따라서 규정 준수 평가를 수행할 수 없습니다. 컨트롤에서 AWS Config 또는 AWS Security Hub를 데이터 원본 유형으로 사용하지만 해당 서비스를 사용하지 않은 경우가 이에 해당합니다. 컨트롤이 수동 증거, AWS API 호출 또는 AWS CloudTrail와 같이 규정 준수 검사를 지원하지 않는 데이터 원본 유형을 사용하는 경우에도 마찬가지입니다.

콘솔에서 규정 준수 검사 상태가 해당 없음으로 표시되어 있는 증거는 대시보드에서 결정적이지 않은 것으로 분류됩니다.

규정 준수 증거

규정 준수 검사에서 문제가 보고되지 않은 경우 증거가 규정을 준수하는 것입니다. Security Hub가 합격 결과를 보고하거나 AWS Config가 규정 준수 결과를 보고하는 경우가 이에 해당합니다.

제어 도메인

대시보드에는 제어 도메인의 개념이 도입되었습니다. 제어 도메인은 특정 프레임워크에만 국한되지 않는 일반적인 제어 범주로 생각할 수 있습니다. 제어 도메인 그룹화는 대시보드의 가장 강력한 기능 중 하나입니다. Audit Manager는 평가에서 규정을 준수하지 않는 증거가 있는 제어 항목을 강조 표시하고 제어 도메인별로 그룹화합니다. 이 기능을 사용하면 감사를 준비하면서 특정 주제 도메인에 수정 노력을 집중할 수 있습니다.

> **Note**
>
> 제어 도메인은 제어 세트와 다릅니다. 제어 세트는 일반적으로 규제 기관에서 정의하는 프레임워크별 제어 그룹입니다. 예를 들어, PCI DSS 프레임워크에는 요구 사항 8: 시스템 구성 요소에 대한 액세스 식별 및 인증이라는 제어 세트가 있습니다. 이 제어 세트는 ID 및 액세스 관리의 제어 도메인에 속합니다.

Audit Manager는 제어를 다음과 같은 제어 도메인에 따라 분류합니다.

제어 도메인 이름	이러한 제어가 규제하는 내용에 대한 설명
비즈니스 연속성 및 비상 계획	주요 시스템 및 네트워크 중단의 영향으로부터 중요한 비즈니스 운영을 보호하는 프로세스를 수립하는 방법
변경 관리	클라우드 인프라의 변경 사항을 테스트, 승인, 구현 및 문서화하는 방법
데이터 보안 및 개인정보 보호	데이터의 프라이버시, 가용성, 무결성을 보호하는 방법.
개발 및 구성 관리	클라우드 인프라를 바람직하고 일관된 상태로 유지하는 방법.
거버넌스 및 감독	클라우드 컴퓨팅 사용을 법률, 규제 및 윤리적 의무에 맞추는 방법.
ID 및 액세스 관리	적합한 사용자가 귀하의 기술 리소스에 적절하게 액세스할 수 있도록 하는 방법
인시던트 관리	보안 인시던트에 신속하고 효과적으로 대응할 수 있는 책임과 절차를 설정하는 방법
로깅 및 모니터링	사용자 활동을 검토하여 무단 활동이 시도되거나 수행되었다는 징후가 있는지 확인하는 방법
Network 관리	네트워크 관리 시스템을 사용하여 데이터 네트워크를 관리하고 운영하는 방법.
인사 관리	조직 수준에서 직원 보안 위험을 평가하고 관리하는 방법.
물리적 보안	시설의 물리적 보안 문제를 감지하고 예방하는 방법.

제어 도메인 이름	이러한 제어가 규제하는 내용에 대한 설명
위험 관리	잠재적 위험과 손실을 평가하는 방법, 그리고 그러한 위협을 줄이거나 없애는 방법
공급망 관리	IT 제품, 공급업체 및 공급망과 관련된 위험을 식별, 평가 및 완화하는 방법.
사용자 장치 관리	직원의 IT 하드웨어가 분실, 손상 또는 손상될 위험을 줄이는 방법.
취약성 관리	귀하의 클라우드 인프라 내 자산에 대해 알려진 모든 취약성을 정의, 평가 및 해결하는 방법

데이터의 최종 일관성

대시보드 데이터는 결국 일관성을 유지합니다. 즉, 대시보드에서 데이터를 읽을 때 최근 완료된 쓰기 또는 업데이트 작업의 결과가 즉시 반영되지 않을 수 있습니다. 몇 시간 후에 다시 확인하면 대시보드에 최신 데이터가 반영될 것입니다.

삭제된 평가 및 비활성 평가의 데이터

대시보드에는 활성 평가의 데이터가 표시됩니다. 대시보드를 본 당일에 평가를 삭제하거나 상태를 비활성으로 변경하면 다음과 같이 해당 평가에 대한 데이터가 포함됩니다.

- 비활성 평가 — 평가를 비활성으로 변경하기 전에 Audit Manager가 평가에 대한 증거를 수집한 경우 해당 증거 데이터가 해당 날짜의 대시보드 수에 포함됩니다.
- 삭제된 평가 — 삭제하기 전에 Audit Manager가 평가에 대한 증거를 수집한 경우 해당 증거 데이터는 해당 날짜의 대시보드 수에 포함되지 않습니다.

대시보드 요소

다음 섹션에서는 대시보드의 다양한 구성 요소에 대해 설명합니다.

주제

- 평가 필터
- 일일 스냅샷
- 미준수 증거가 있는 규제 항목은 제어 도메인별로 그룹화됩니다.

평가 필터

평가 필터를 사용하여 특정 활성 평가에 집중할 수 있습니다.

기본적으로 대시보드에는 모든 활성 평가에 대한 집계 데이터가 표시됩니다. 특정 평가에 대한 데이터를 보려면 평가 필터를 적용합니다. 대시보드의 모든 위젯에 적용되는 페이지 수준 필터입니다.

평가 필터를 적용하려면 대시보드 상단의 드롭다운 목록에서 평가를 선택하세요. 이 목록에는 활성 평가 중 최대 10개가 표시됩니다. 가장 최근에 생성한 평가가 먼저 표시됩니다. 활성 평가가 많은 경우 평가 이름을 입력하여 빠르게 찾을 수 있습니다. 평가를 선택하면 대시보드에 해당 평가에 대한 데이터만 표시됩니다.

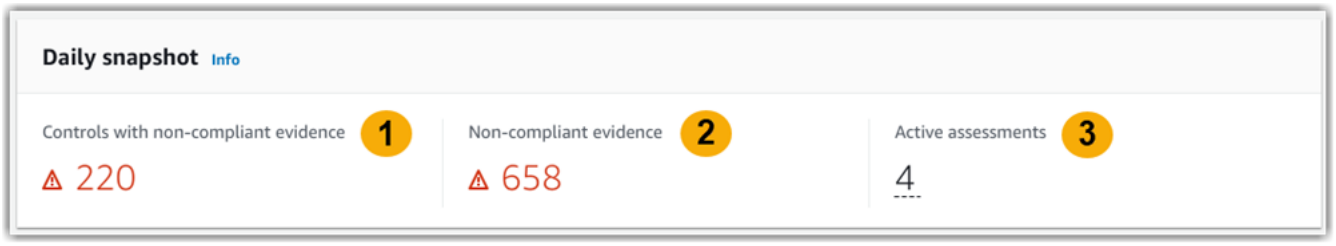
일일 스냅샷

이 위젯은 활성 평가의 현재 규정 준수 상태를 한눈에 보여줍니다.

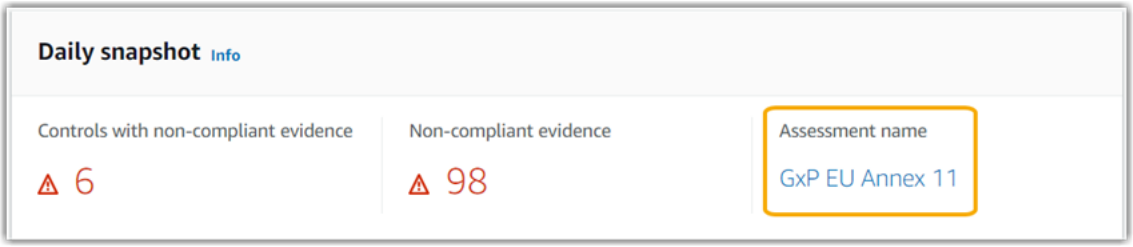
일별 스냅샷은 대시보드 상단의 해당 날짜에 수집된 최신 데이터를 반영합니다. 대시보드의 날짜 및 시간이 협정 세계시(UTC)로 표시됩니다. 이 수치는 이 타임스탬프를 기반으로 한 일일 집계라는 점을 이해하는 것이 중요합니다. 현재까지의 총액은 아닙니다.

기본적으로 일일 스냅샷에는 모든 활성 평가에 대한 다음 데이터가 표시됩니다.

1. 미준수 증거가 있는 규제 항목 - 규정 미준수 증거와 관련된 규제 항목의 총 수입니다.
2. 미준수 증거 - 규정을 준수하지 않은 결론을 포함한 규정 준수 확인 증거의 총량.
3. 활성 평가 - 활성 평가의 총 수입니다. 이 숫자를 선택하면 이러한 평가로 연결되는 링크를 볼 수 있습니다.



일일 스냅샷 데이터는 적용한 the section called “평가 필터”에 따라 달라집니다. 평가를 지정하는 경우 데이터에는 해당 평가의 일일 수만 반영됩니다. 이 경우 일별 스냅샷에는 지정한 평가 이름이 표시됩니다. 평가 이름을 선택하여 열 수 있습니다.

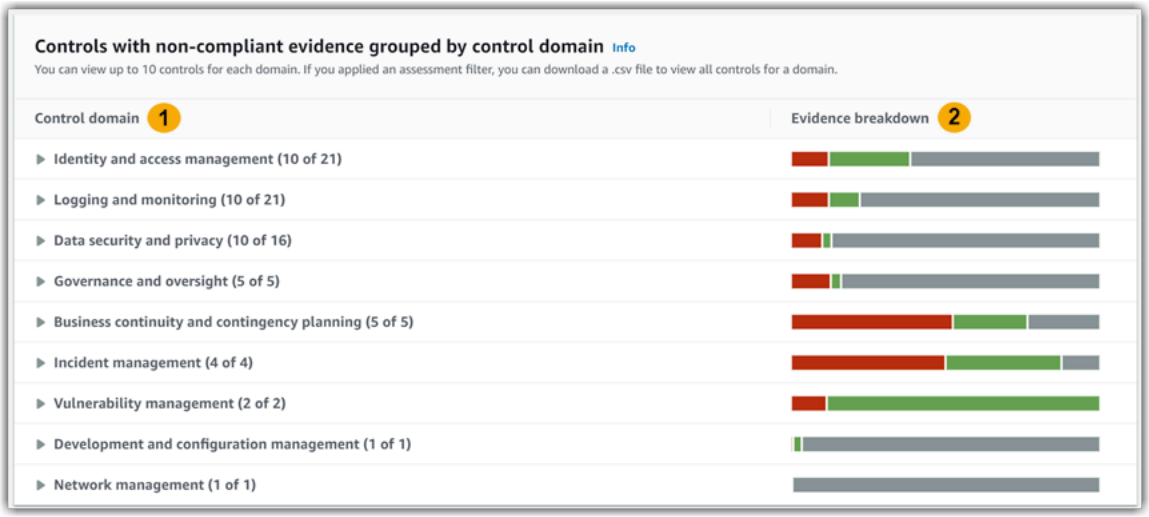


미준수 증거가 있는 규제 항목은 제어 도메인별로 그룹화됩니다.

이 위젯을 사용하여 가장 미준수 증거가 있는 컨트롤을 식별할 수 있습니다.

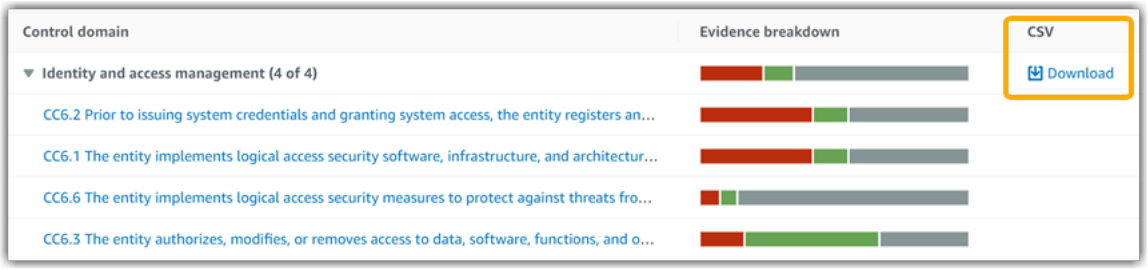
기본적으로 위젯에는 모든 활성 평가에 대한 다음 데이터가 표시됩니다.

1. 제어 도메인 — 활성 평가와 관련된 control domains의 목록입니다.
2. 증거 분석 — 증거 준수 상태를 분류하여 보여주는 막대형 차트입니다.



제어 도메인을 확장하려면 이름 옆에 있는 화살표를 선택합니다. 콘솔을 확장하면 각 도메인에 대해 최대 10개의 컨트롤이 표시됩니다. 이러한 컨트롤은 비준수 증거의 총 개수가 가장 높은 것에 따라 순위가 매겨집니다.

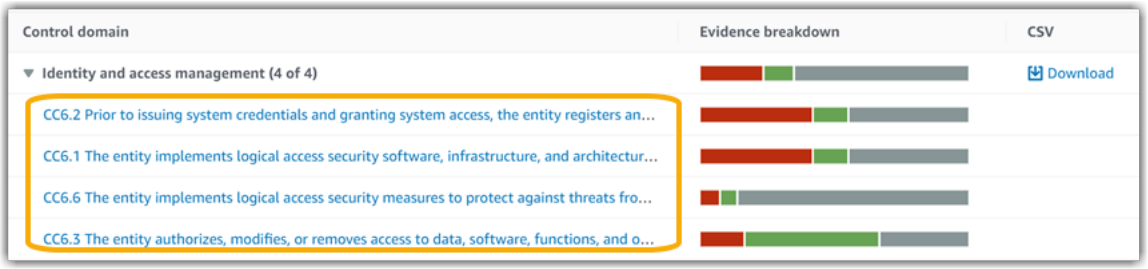
이 위젯의 데이터는 적용한 the section called “평가 필터”에 따라 달라집니다. 평가를 지정하면 해당 평가에 대한 데이터만 볼 수 있습니다. 또한 평가에서 사용 가능한 각 제어 도메인에 대한.csv 파일을 다운로드할 수도 있습니다.



.csv 파일에는 비준수 증거와 관련된 도메인 내 컨트롤의 전체 목록이 포함되어 있습니다. 다음 예제에서는 가상 값이 있는.csv 데이터 열을 보여 줍니다.

	A	B	C	D	E	F	G
1	Date and Time	AssessmentID	AsessmentName	ControlId	ControlName	ControlDescription	DataSource
2	Thu Oct 21 2021 21:31:05 GMT-0700	12345678-abcd-2345-bcde-345678901234	My assessment	abcdefgh-1234-bcde-5678-cdefghijklmn	Control 1	Description of control 1	Manual
3	Thu Oct 21 2021 21:31:05 GMT-0700	12345678-abcd-2345-bcde-345678901234	My assessment	12345678-abcd-9012-bcde-345678901234	Control 2	Description of control 2	Manual
4	Thu Oct 21 2021 21:31:05 GMT-0700	12345678-abcd-2345-bcde-345678901234	My assessment	bcdefghi-2345-cdef-3456-defghijklmno	Control 3	Description of control 3	AWS Config, AWS Security Hub
5	Thu Oct 21 2021 21:31:05 GMT-0700	12345678-abcd-2345-bcde-345678901234	My assessment	23456789-bcde-0123-cdef-456789012345	Control 4	Description of control 4	Manual
6	Thu Oct 21 2021 21:31:05 GMT-0700	12345678-abcd-2345-bcde-345678901234	My assessment	cdefghij-3456-defg-4567-efghijklmnop	Control 5	Description of control 5	AWS Config
7	Thu Oct 21 2021 21:31:05 GMT-0700	12345678-abcd-2345-bcde-345678901234	My assessment	34567890-cdef-1234-defg-567890123456	Control 6	Description of control 6	Manual
8	Thu Oct 21 2021 21:31:05 GMT-0700	12345678-abcd-2345-bcde-345678901234	My assessment	defghijk-4567-efgh-5678-fghijklmnopq	Control 7	Description of control 7	AWS Config
9	Thu Oct 21 2021 21:31:05 GMT-0700	12345678-abcd-2345-bcde-345678901234	My assessment	45678901-defg-2345-efgh-678901234567	Control 8	Description of control 8	AWS Security Hub
10	Thu Oct 21 2021 21:31:05 GMT-0700	12345678-abcd-2345-bcde-345678901234	My assessment	efghijkl-5678-fghi-6789-ghijklmnopqr	Control 9	Description of control 9	Manual
11	Thu Oct 21 2021 21:31:05 GMT-0700	12345678-abcd-2345-bcde-345678901234	My assessment	56789012-efgh-3456-fghi-789012345678	Control 10	Description of control 10	Manual
12	Thu Oct 21 2021 21:31:05 GMT-0700	12345678-abcd-2345-bcde-345678901234	My assessment	fghijklm-6789-ghij-7890-hijklmnopqrs	Control 11	Description of control 11	Manual
13	Thu Oct 21 2021 21:31:05 GMT-0700	12345678-abcd-2345-bcde-345678901234	My assessment	67890123-fghi-4567-ghij-890123456789	Control 12	Description of control 12	Manual
14	Thu Oct 21 2021 21:31:05 GMT-0700	12345678-abcd-2345-bcde-345678901234	My assessment	ghijklmn-7890-hijk-8901-ijklmnopqrst	Control 13	Description of control 13	AWS Config, AWS Security Hub
15	Thu Oct 21 2021 21:31:05 GMT-0700	12345678-abcd-2345-bcde-345678901234	My assessment	78901234-ghij-5678-hijk-901234567890	Control 14	Description of control 14	Manual
16							

마지막으로 평가 필터를 적용하면 각 도메인의 컨트롤 이름이 하이퍼링크로 연결됩니다. 원하는 컨트롤을 선택하면 지정된 평가에서 컨트롤 세부 정보 페이지가 열립니다.



Tip

제어 세부 정보 페이지를 출발점으로 사용하여 한 세부 수준에서 다음 세부 수준으로 이동할 수 있습니다.

1. 통제 세부 정보 페이지 - 이 페이지의 증거 폴더 탭에는 Audit Manager가 해당 통제를 위해 수집한 증거의 일일 폴더가 나열됩니다. 폴더를 선택하면 자세한 내용을 확인할 수 있습니다.
2. 증거 폴더 - 다음으로 폴더 요약과 해당 폴더에 있는 증거 목록을 검토할 수 있습니다. 자세한 내용은 개별 증거 항목을 선택하세요.

3. 개별 증거 - 마지막으로 개별 증거 세부 정보를 탐색할 수 있습니다. 여기에는 증거의 적용 가능한 모든 속성 및 리소스 데이터가 포함됩니다. 이는 가장 세분화된 수준의 증거 데이터입니다.

다음으로 무엇을 할까요?

대시보드를 검토한 후 취할 수 있는 몇 가지 다음 단계는 다음과 같습니다.

- .csv 파일 다운로드 — 집중하려는 평가 및 통제 도메인을 찾고 비준수 증거가 있는 관련 규제 항목의 전체 목록을 다운로드하십시오.
- 규제 항목 검토 — 수정이 필요한 규제 항목을 식별한 후 해당 규제 항목을 검토할 수 있습니다.
- 검토를 위해 통제 위임 — 통제 항목을 검토하는 데 도움이 필요한 경우 검토를 위해 통제 세트를 위임할 수 있습니다.
- 평가 편집 - 활성 평가의 범위를 변경하려면 평가를 편집할 수 있습니다.
- 평가 상태 업데이트 - 평가를 위한 증거 수집을 중단하려면 평가를 비활성화로 변경할 수 있습니다.

문제 해결

일반적인 질문 및 문제에 대한 답변을 찾으려면 이 가이드의 문제 해결 섹션에서 대시보드 문제 해결을 참조하십시오.

AWS Audit Manager에서의 평가

Audit Manager 평가는 그룹화된 컨트롤 항목들인 프레임워크를 기반으로 합니다. 프레임워크를 출발점으로 사용하여 해당 프레임워크의 컨트롤 항목에 대한 증거를 수집하는 평가를 생성할 수 있습니다. 사용자의 평가에서, 감사 범위를 정의할 수도 있습니다. 여기에는 증거를 수집하려는 대상 AWS 계정 및 서비스를 지정하는 것도 포함됩니다.

모든 프레임워크에서 평가를 생성할 수 있습니다. 어느 쪽에서든, Audit Manager에서 제공하는 표준 프레임워크를 사용할 수 있습니다. 또는 직접 구축한 사용자 지정 프레임워크에서 평가를 생성할 수 있습니다. 표준 프레임워크에는 특정 규정 준수 표준 또는 규정을 지원하는 사전 구축된 컨트롤 세트가 포함되어 있습니다. 반면, 사용자 지정 프레임워크에는 내부 감사 요구 사항에 따라 사용자 지정하고 그룹화할 수 있는 컨트롤 항목이 포함되어 있습니다. 표준 프레임워크와 사용자 지정 프레임워크 간의 차이점에 대한 자세한 내용은 이 안내서의 개념 및 용어 섹션에 있는 프레임워크를 참조하세요.

평가를 생성하면, 이를 통해 지속적인 증거 수집이 시작됩니다. 감사 시기가 되면, 사용자 또는 대리인이 이 증거를 검토한 다음, 평가 보고서에 해당 내용을 추가할 수 있습니다.

> **Note**
>
> AWS Audit Manager은 특정 규정 준수 표준 및 규정의 준수 여부를 확인하는 데 필요한 증거를 수집하는 데 도움이 됩니다. 하지만, 규정 준수 자체를 평가하지는 않습니다. 따라서, AWS Audit Manager를 통해 수집되는 증거에는 감사에 필요한 AWS 사용량에 대한 모든 정보가 포함되어 있지 않을 수 있습니다. AWS Audit Manager가 법률 고문이나 규정 준수 전문가를 대신하지는 못합니다.

주제

- 평가 삭제

평가 생성

이 항목은 시작하기: 평가 만들기 자습서를 기반으로 합니다. 여기에는 프레임워크에서 평가를 생성하는 방법에 대한 자세한 지침이 포함되어 있습니다. 다음 단계에 따라 평가를 생성하고 지속적인 증거 수집을 시작하세요.

Tasks

- 1단계: 평가 세부 정보 지정
- 2단계: 범위 내 AWS 계정 지정
- 3단계: 범위 내 AWS 서비스 지정
- 4단계: 감사 소유자 지정
- 5단계: 검토 및 생성
- 다음으로 무엇을 할 수 있습니까?

1단계: 평가 세부 정보 지정

프레임워크를 선택하고 평가를 위한 기본 정보를 제공함으로써 시작하세요.

평가 세부 정보를 지정하려면

1. https://console.aws.amazon.com/auditmanager/home에서 AWS Audit Manager 콘솔을 엽니다.
2. 탐색 창에서 평가를 선택한 후 평가 생성을 선택합니다.
   - 또는 탐색 창에서 시작하기를 선택한 다음 평가 생성을 선택합니다.
3. 평가 이름에서, 평가에 대한 이름을 입력합니다.
4. (선택 사항) 평가 설명에서, 평가에 대한 설명을 입력합니다.
5. 평가 보고서 대상에서, 평가 보고서를 저장할 기존 Amazon S3 버킷을 선택합니다.

> **Tip**
>
> 기본 평가 보고서 대상은 Audit Manager 설정을 기반으로 합니다. 자세한 내용은 AWS Audit Manager 설정, 평가 보고서 대상을 참조하세요. 원하는 경우, 여러 S3 버킷을 생성하고 사용하여 평가 보고서를 구성할 수 있습니다.

6. 프레임워크에서 평가를 생성할 때 사용할 프레임워크를 선택합니다. 검색 창을 사용하여 이름이나 규정 준수 표준 또는 규정별로 프레임워크를 검색할 수도 있습니다.

> **Tip**
>
> 프레임워크에 대해 자세히 알아보려면 프레임워크 이름을 선택하세요. 이렇게 하면 프레임워크 요약 페이지가 열립니다. 이 페이지에서 해당 프레임워크의 내용을 검토할 수 있습니다. 여기에는 프레임워크의 컨트롤과 데이터 소스가 포함됩니다.

7. 태그에서, 새 태그 추가를 선택하여 태그를 평가에 연결합니다. 각 태그에 대한 키 및 값을 지정할 수 있습니다. 태그 키는 필수이며 이 평가를 검색할 때 검색 기준으로 사용할 수 있습니다. Audit Manager의 태그에 대한 자세한 내용은 AWS Audit Manager 리소스에 태그 지정(을)를 참조하세요.
8. 다음을 선택합니다.

> **Note**
>
> 평가가 주어진 프레임워크에 대한 올바른 증거를 수집하는지 확인하는 것이 중요합니다. 증거 수집을 시작하기 전에 선택한 프레임워크의 요구 사항을 검토하는 것이 좋습니다. 그런 다음, 이러한 요구 사항을 현재 AWS Config 규칙 파라미터와 비교하여 검증하세요. 규칙 파라미터가 프레임워크 요구 사항에 맞는지 확인하기 위해 AWS Config에서 규칙을 업데이트할 수 있습니다.
>
> 예를 들어, CIS v1.2.0에 대한 평가를 생성한다고 가정해 보겠습니다. 이 프레임워크에는 1.9라는 컨트롤이 있습니다. IAM 암호 정책에 최소 길이 14 이상이 필요한지 확인하십시오. AWS Config에서, iam-password-policy 규칙에는 암호 길이를 확인하는 `MinimumPasswordLength` 파라미터가 있습니다. 이 파라미터의 기본값은 문자 14개입니다. 결과적으로, 규칙은 컨트롤 요구 사항에 맞게 조정됩니다. 기본 파라미터 값을 사용하지 않는 경우, 사용하는 값이 CIS v1.2.0의 14자 요구 사항과 같거나 더 큰지 확인하세요. AWS Config 설명서에서 각 관리형 규칙에 대한 기본 파라미터 세부 정보를 찾을 수 있습니다.

2단계: 범위 내 AWS 계정 지정

평가 범위에 여러 AWS 계정를 포함하도록 지정할 수 있습니다. Audit Manager는 AWS Organizations와의 통합을 통해 여러 계정을 지원합니다. 즉, 수집된 증거를 위임된 관리자 계정으로 통합하여 여러 계정을 대상으로 Audit Manager 평가를 실행할 수 있습니다. Audit Manager에서 조직을 활성화하려면 AWS Organizations 활성화(선택 사항)(을)를 참조하세요.

> **Note**
>
> Audit Manager는 평가 범위 내에서 최대 약 150개의 계정을 지원할 수 있습니다. 150개가 넘는 계정을 포함하려고 하면 평가 생성이 실패할 수 있습니다.

범위 내에서 AWS 계정를 지정하려면

1. AWS 계정에서, 평가 범위 내에 포함하려는 AWS 계정를 선택합니다.
   - Audit Manager에서 조직을 활성화한 경우 여러 계정이 표시됩니다. 목록에서 계정을 하나 이상 선택할 수 있습니다. 또는 계정 이름, ID 또는 이메일로 계정을 검색할 수도 있습니다.
   - Audit Manager에서 조직을 활성화하지 않은 경우, 현재 AWS 계정만 나열됩니다.
2. 다음을 선택합니다.

> **Note**
>
> 범위 내 계정이 귀하의 조직에서 제거되면 Audit Manager는 더 이상 해당 계정에 대한 증거를 수집하지 않습니다. 하지만 해당 계정은 AWS 계정 탭 아래 귀하의 평가에 계속 표시됩니다. 범위 내 계정 목록에서 계정을 제거하려면 평가를 편집하면 됩니다. 제거된 계정은 편집하는 동안 목록에 더 이상 표시되지 않으므로 해당 계정이 범위에 포함되지 않은 상태에서 변경 내용을 저장할 수 있습니다.

3단계: 범위 내 AWS 서비스 지정

앞서 선택한 프레임워크는 Audit Manager가 모니터링하고 증거를 수집하는 AWS 서비스를 정의합니다. 나열된 AWS 서비스가 선택되지 않았거나 선택되었지만 사용자 환경에서 활성화하지 않은 경우, Audit Manager는 해당 서비스와 관련된 리소스에서 증거를 수집하지 않습니다.

다음과 같이 범위 내에 AWS 서비스를 지정할 수 있습니다.

표준 프레임워크에서 생성된 평가의 경우

Audit Manager 콘솔을 사용하여 표준 프레임워크에서 평가를 생성하는 경우, 범위 내 AWS 서비스 목록이 기본적으로 선택됩니다. 이 목록은 편집할 수 없습니다. 이는 Audit Manager가 자동으로 데이터 소스 및 서비스를 매핑하고 선택하기 때문입니다. 이 선택은 표준 프레임워크의 요구 사항에 따라 이루어집니다. 선택한 표준 프레임워크에 수동 컨트롤만 포함된 경우, AWS 서비스는 평가 범위에 포함되지 않으며 평가에 서비스를 추가할 수 없습니다.

계속하려면 목록을 검토하고 다음을 선택합니다.

> **Tip**
>
> 범위 내에서 서비스 목록을 편집해야 하는 경우, Audit Manager에서 제공하는 CreateAssessment API를 사용하여 편집할 수 있습니다.
> 또는 표준 프레임워크를 사용자 지정한 다음 사용자 지정 프레임워크에서 평가를 생성할 수 있습니다.

사용자 지정 프레임워크에서 생성된 평가의 경우

1단계에서 사용자 지정 프레임워크를 선택한 경우, 평가 범위에 있는 AWS 서비스 목록을 검토하고 수정할 수 있습니다. 선택한 사용자 지정 프레임워크에 수동 컨트롤만 포함된 경우, 모든 AWS 서비스가 표시되지만 선택된 항목은 없습니다. 평가 범위 내에 포함시킬 서비스를 0개 이상 선택할 수 있습니다.

범위 내에서 AWS 서비스를 지정하려면(사용자 지정 프레임워크에서 생성한 평가에만 해당)

1. AWS 서비스에서, 평가에 포함하려는 서비스를 선택합니다. 검색 창을 사용하여 서비스, 범주 또는 설명별로 검색하면 추가 서비스를 찾을 수 있습니다. 서비스를 추가하려면 서비스 이름 옆의 확인란을 선택합니다. 서비스를 제거하려면 확인란의 선택을 취소합니다.
2. 마쳤으면, AWS 서비스를 선택하고 다음을 선택합니다.

4단계: 감사 소유자 지정

이 단계에서는 평가의 감사 소유자를 지정합니다. 감사 소유자는 일반적으로 GRC, SecOps 또는 DevOps 팀 소속으로, Audit Manager 평가를 관리하는 직장의 개인입니다. AWSAuditManagerAdministratorAccess 정책을 사용하는 것이 좋습니다.

감사 소유자를 지정하려면

1. 감사 소유자에서 현재 감사 소유자 목록을 검토하세요. 감사 소유자 열에는 사용자 ID와 역할이 표시됩니다. AWS 계정 열에는 해당 감사 소유자와 관련된 AWS 계정가 표시됩니다.
2. 확인란을 선택한 감사 소유자는 평가에 포함됩니다. 감사 소유자를 평가에서 제거하려면 해당 감사 소유자의 확인란의 선택을 취소하세요. 검색 창을 사용하여 이름이나 AWS 계정로 검색하면 추가 감사 소유자를 찾을 수 있습니다.
3. 마쳤으면, 다음을 선택합니다.

5단계: 검토 및 생성

평가를 위한 정보를 검토합니다. 단계 정보를 변경하려면 편집을 선택합니다. 작업을 마쳤으면 평가 생성을 선택합니다.

이 작업을 통해 평가를 위한 지속적인 증거 수집이 시작됩니다. 평가를 생성한 후에는 평가 상태를 비활성으로 변경할 때까지 증거 수집이 계속됩니다. 또는 컨트롤 상태를 비활성으로 변경하여 특정 컨트롤에 대한 증거 수집을 중지할 수 있습니다.

> **Note**
>
> 자동 증거는 평가가 생성된 후 24시간 후에 사용할 수 있습니다. Audit Manager는 여러 데이터 소스에서 증거를 자동으로 수집하며, 증거 수집 빈도는 증거 유형에 따라 다릅니다. 자세히 알아보려면, 이 안내서의 증거 수집 빈도를 참조하세요.

다음으로 무엇을 할 수 있습니까?

평가를 생성한 후 다음에 대한 자세한 정보를 알아볼 수 있습니다.

- 평가에 액세스
- 평가 검토
- 평가 편집
- 평가에서 컨트롤 검토하기
- 평가에서 증거 검토하기
- 수동 증거를 평가에 업로드
- AWS Audit Manager에서의 위임
- 평가 보고서 생성
- 평가 상태 변경
- 평가 삭제
- 평가 및 증거 수집 문제 해결

AWS Audit Manager에서 평가에 액세스

Audit Manager 콘솔의 평가 페이지에서 모든 평가를 볼 수 있습니다. 여기에서, 평가를 편집하거나, 평가를 삭제하거나, 평가를 생성할 수도 있습니다.

Audit Manager API 또는 AWS Command Line Interface(AWS CLI)를 사용하여 평가를 볼 수도 있습니다.

Audit Manager console

평가를 보려면(콘솔)

1. https://console.aws.amazon.com/auditmanager/home에서 AWS Audit Manager 콘솔을 엽니다.
2. 왼쪽 탐색 창에서, 평가를 선택하여 활성 평가 및 이전 평가 목록을 확인합니다. 검색 창을 사용하여 평가를 검색할 수도 있습니다.
3. 평가 이름을 선택하면 해당 평가의 세부 정보를 볼 수 있는 요약 페이지가 열립니다.

AWS CLI

평가를 보려면(CLI)

Audit Manager에서 평가를 보려면 list-assessments 명령을 실행합니다. `--status` 하위 명령을 사용하여 활성 또는 비활성 상태인 평가를 볼 수 있습니다.

```
aws auditmanager list-assessments --status ACTIVE
```

```
aws auditmanager list-assessments --status INACTIVE
```

Audit Manager API

평가를 보려면(API)

Audit Manager에서 평가를 보려면 평가 목록 작성 작업을 사용하세요. 상태 속성을 사용하여 활성 또는 비활성 상태인 평가를 볼 수 있습니다.

자세한 내용은 이전 링크 중 하나를 선택하여 AWS Audit Manager API 참조에서 자세한 내용을 읽어보세요. 여기에는 언어별 AWS SDK 중 하나로 `ListAssessments` 작업 및 파라미터를 사용하는 방법에 대한 정보가 포함됩니다.

평가 편집

Audit Manager에서 활성 평가를 편집하여 설명, 범위, 감사 소유자, 평가 보고서 대상 등의 정보를 변경할 수 있습니다.

Tasks

- 1단계: 평가 세부 정보 편집
- 2단계: 범위 내 AWS 계정 편집
- 3단계: 범위 내 AWS 서비스 편집
- 4단계: 감사 소유자 편집
- 5단계: 검토 및 저장

1단계: 평가 세부 정보 편집

평가 세부 정보를 편집하려면 다음 단계를 따르세요.

평가를 편집하려면

1. https://console.aws.amazon.com/auditmanager/home에서 AWS Audit Manager 콘솔을 엽니다.
2. 탐색 창에서, 평가를 선택하여 현재 평가 목록을 봅니다.
3. 평가를 선택하고 편집을 선택합니다.
   - 또는, 평가를 연 다음, 페이지 오른쪽 상단에서 편집을 선택할 수도 있습니다.
4. 평가 세부 정보 편집에서, 평가 이름, 설명 및 평가 보고서 대상을 수정합니다.
5. 다음을 선택합니다.

> **Tip**
>
> 평가에 대한 태그를 편집하려면, 평가를 열고 태그 탭를 선택합니다. 그곳에서, 평가에 연결된 태그를 보고 편집할 수 있습니다.

2단계: 범위 내 AWS 계정 편집

이 단계에서는 평가 범위에 포함된 계정의 목록을 변경할 수 있습니다.

Audit Manager는 AWS Organizations와의 통합을 통해 여러 계정을 지원합니다. 즉, 수집된 증거를 위임된 관리자 계정으로 통합하여 여러 계정을 대상으로 Audit Manager 평가를 실행할 수 있습니다. Audit Manager에 대해 위임된 관리자를 추가하거나 변경하려면, AWS Audit Manager 설정, 위임된 관리자를 참조하세요.

> **Note**
>
> Audit Manager는 평가 범위 내에서 최대 약 150개의 계정을 지원할 수 있습니다. 150개가 넘는 계정을 포함하려고 하면 평가 생성이 실패할 수 있습니다.

범위 내에서 AWS 계정를 편집하려면

1. 범위 내 AWS 계정 편집에서, 추가 AWS 계정을 선택합니다. 목록에서 계정을 삭제하여 계정을 제거할 수도 있습니다.
2. 다음을 선택합니다.

3단계: 범위 내 AWS 서비스 편집

이 단계는 Audit Manager가 어떤 AWS 서비스를 모니터링하고 이에 대한 증거를 수집하는지를 지정합니다. 나열된 AWS 서비스가 선택되지 않았거나 선택되었지만 사용자 환경에서 활성화하지 않은 경우, Audit Manager는 해당 서비스와 관련된 리소스에서 증거를 수집하지 않습니다.

다음과 같이 범위 내 AWS 서비스를 검토하고 편집할 수 있습니다.

표준 프레임워크에서 생성된 평가의 경우

Audit Manager 콘솔을 사용하여 표준 프레임워크에서 생성된 평가를 편집할 경우, 범위 내 AWS 서비스 목록을 검토할 수 있지만 이 목록을 편집할 수는 없습니다. 이는 Audit Manager가 표준 프레임워크의 설계에 따라 자동으로 데이터 소스 및 서비스를 매핑하고 선택하기 때문입니다. 수동 컨트롤만 포함된 프레임워크를 사용하여 평가를 생성한 경우에는 AWS 서비스가 평가 범위 내에 포함되지 않으며 서비스를 추가할 수 없습니다.

계속하려면 목록을 검토하고 다음을 선택합니다.

> **Tip**
>
> 기존 평가의 범위 내에서 서비스 목록을 편집해야 하는 경우, Audit Manager에서 제공하는 UpdateAssessment API를 사용하여 편집할 수 있습니다.

사용자 지정 프레임워크에서 생성된 평가의 경우

사용자 지정 프레임워크에서 평가를 생성한 경우, 평가 범위 내에 있는 AWS 서비스를 편집할 수 있습니다. 평가 범위 내에 포함시킬 서비스를 0개 이상 선택할 수 있습니다.

범위 내에서 AWS 서비스를 편집하려면(사용자 지정 프레임워크에서 만든 평가만 해당)

1. 범위 내 AWS 서비스 편집에서, 필요에 따라 추가 AWS 서비스를 선택합니다. 목록에서 서비스를 삭제하여 서비스를 제거할 수도 있습니다.
2. 다음을 선택합니다.

4단계: 감사 소유자 편집

평가에 대한 감사 소유자를 변경할 수도 있습니다. 감사 소유자는 일반적으로 GRC, SecOps 또는 DevOps 팀 소속으로, Audit Manager 평가를 관리하는 직장의 개인입니다. 이들의 임무에는 검토를 위한 컨트롤 세트를 위임하고 평가 보고서를 생성하는 작업이 포함됩니다. AWSAuditManagerAdministratorAccess 정책을 사용하는 것이 좋습니다.

감사 소유자를 편집하려면

1. 평가에 추가할 새 감사 소유자를 선택합니다. 감사 소유자를 제거하려면 목록에서 감사 소유자를 삭제합니다.
2. 다음을 선택합니다.

5단계: 검토 및 저장

평가를 위한 정보를 검토합니다. 단계 정보를 변경하려면 편집을 선택합니다. 마쳤으면, 편집내용을 확인하기 위해 변경 사항 저장을 선택합니다.

> **Note**
>
> 편집내용을 작성한 후, 평가 변경 사항은 다음 날 00:00 UTC에 적용됩니다.

평가 검토

Audit Manager에서 평가를 생성한 후, 언제든지 평가를 열고 검토할 수 있습니다.

평가를 열고 검토하려면

1. https://console.aws.amazon.com/auditmanager/home에서 AWS Audit Manager 콘솔을 엽니다.
2. 왼쪽 탐색 창에서, 평가를 선택하여 평가 목록을 봅니다.
3. 평가에 대한 이름을 선택하여 해당 내용을 엽니다.

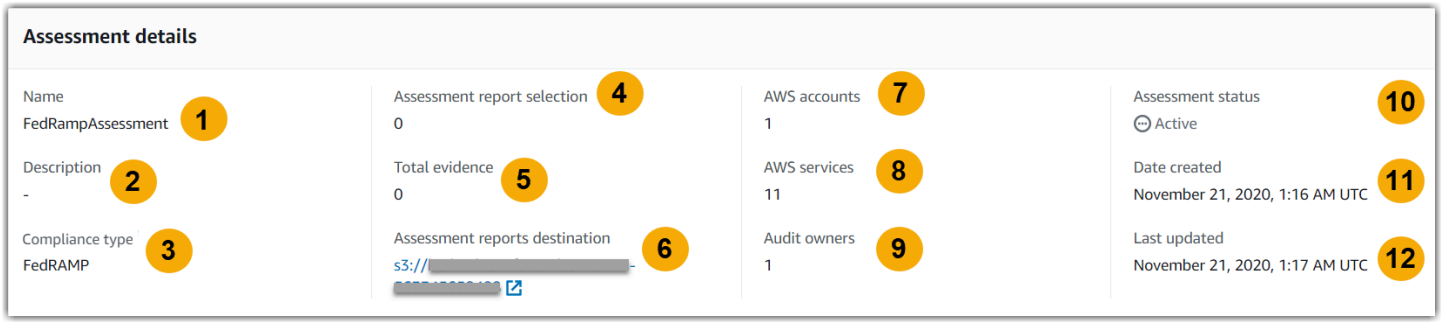
평가를 열면 여러 섹션이 포함된 요약 페이지가 표시됩니다. 이 페이지의 섹션 및 내용은 다음과 같습니다.

평가 페이지 섹션

- 평가 세부 정보
- 컨트롤 탭
- 평가 보고서 선택 탭
- AWS 계정 탭
- AWS 서비스 탭
- 감사 소유자 탭
- 태그 탭
- Changelog 탭

평가 세부 정보

평가 세부 정보 섹션에서는 평가 개요를 제공합니다.



여기에는 다음 정보가 포함됩니다.

1. 이름 - 평가를 위해 제공한 이름입니다.
2. 설명 - 평가를 위해 제공한 선택적 설명입니다.
3. 규정 준수 유형 - 평가에서 지원하는 규정 준수 표준 또는 규정입니다.

4. 평가 보고서 선택 - 평가 보고서에 포함하기로 선택한 증거 항목의 수입니다.
5. 전체 증거 - 이 평가를 위해 수집된 증거 항목의 총 수입니다.
6. 평가 보고서 대상 - Audit Manager가 평가 보고서를 저장하는 Amazon S3 버킷입니다.
7. AWS 계정 - 이 평가 범위에 포함되는 AWS 계정의 개수입니다.
8. AWS 서비스 - 이 평가 범위에 포함되는 AWS 서비스의 개수입니다.
9. 감사 소유자 - 이 평가에 대한 감사 소유자 수입니다.
10. 평가 상태 - 평가 상태입니다.
    - 활성 - 평가에서 현재 증거를 수집 중임을 나타냅니다. 새로 만든 평가의 상태는 다음과 같습니다.
    - 비활성 - 평가에서 더 이상 증거를 수집하지 않음을 나타냅니다. 비활성 평가에 대한 자세한 내용은 평가 상태를 비활성으로 변경(을)를 참조하세요.
11. 생성 날짜 - 평가가 생성된 날짜입니다.
12. 최종 업데이트 - 이 평가를 마지막으로 수정한 날짜입니다.

컨트롤 탭

컨트롤 탭에는 평가에 포함된 컨트롤 요약과 해당 컨트롤의 전체 목록이 표시됩니다. 각 평가에는 여러 컨트롤 세트가 포함될 수 있으며 각 컨트롤 세트에는 여러 컨트롤 항목이 포함될 수 있습니다. 컨트롤 및 컨트롤 세트는 관련 규정 준수 표준 또는 규정에 정의된 레이아웃과 일치하도록 구성됩니다.

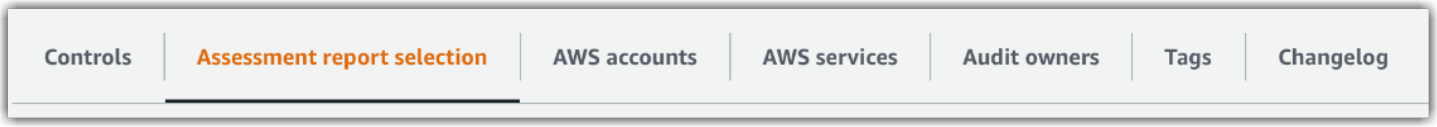
컨트롤 상태 요약에서 이 평가를 위한 컨트롤 요약을 검토할 수 있습니다. 요약에는 다음 정보가 포함됩니다.

- 전체 컨트롤 - 이 평가에 포함된 총 컨트롤 수입니다.
- 검토됨 - 감사 소유자 또는 대리인이 검토한 컨트롤의 수입니다.
- 검토 중 - 현재 검토 중인 컨트롤의 수입니다.
- 비활성 - 더 이상 적극적으로 증거를 수집하지 않는 컨트롤의 수입니다.

컨트롤 세트 표 아래에는 컨트롤 목록이 표시되고 컨트롤 세트별로 그룹화되어 있습니다. 각 컨트롤 세트의 컨트롤을 확장하거나 축소할 수 있습니다. 특정 컨트롤을 찾으려면 컨트롤 이름을 기준으로 검색할 수도 있습니다. 컨트롤 세트별로 그룹화된 컨트롤 표에는 다음과 같은 데이터 열이 표시됩니다.

- 컨트롤 세트별로 그룹화된 컨트롤 - 컨트롤 세트의 이름입니다.
- 컨트롤 상태 - 컨트롤 상태입니다.
  - 검토 중은 이 컨트롤이 아직 검토되지 않았음을 나타냅니다. 이 컨트롤에 대한 증거는 아직 수집 중이므로 수동 증거를 업로드할 수 있습니다. 이것이 기본 상태입니다.
  - 검토됨은 이 컨트롤에 대한 증거가 검토되었음을 나타냅니다. 그러나, 증거는 아직 수집 중이므로 수동 증거를 업로드할 수 있습니다.
  - 비활성은 이 컨트롤에 대한 자동 증거 수집이 중지되었음을 나타냅니다. 더 이상 수동 증거를 업로드할 수 없습니다.
- 위임 대상 - 이 컨트롤의 검토자(검토를 위해 대리인에게 배정된 경우).
- 전체 증거 - 이 컨트롤을 위해 수집된 증거 항목의 수입니다.

평가 보고서 선택 탭



이 탭에는 평가 보고서에 포함할 증거 목록이 증거 폴더별로 그룹화되어 표시됩니다. 이러한 증거 폴더는 생성된 날짜를 기준으로 구성 및 이름이 지정됩니다. 이러한 폴더를 찾아보고 평가 보고서에 포함할 증거를 선택할 수 있습니다. 검색 창을 사용하여 증거 폴더 이름 또는 컨트롤 이름을 기준으로 검색할 수도 있습니다. 평가 보고서에 추가된 총 증거 항목 수는 페이지 상단의 평가 세부 정보 섹션에 요약되어 있습니다.

평가 보고서 선택 표에는 다음 데이터가 포함된 증거 폴더 목록이 표시됩니다.

- 증거 폴더 - 증거 폴더의 이름입니다. 폴더 이름은 증거가 수집된 날짜를 기준으로 합니다.
- 선택된 증거 - 평가 보고서에 포함된 폴더 내 증거 항목의 수입니다.
- 규제 이름 - 이 증거 폴더와 관련된 컨트롤의 이름입니다.

평가 보고서에 증거를 추가하는 방법에 대한 자세한 내용은 평가 보고서 생성(을)를 참조하세요.

AWS 계정 탭

이 탭에는 평가 범위에 포함된 AWS 계정 목록이 표시됩니다. 총 계정 수는 페이지 상단의 평가 세부 정보 섹션에 요약되어 있습니다.

이 AWS 계정 표에는 다음 데이터가 포함된 계정 목록이 나와 있습니다.

- 계정 ID – AWS 계정의 ID입니다.
- 계정 이름 – AWS 계정의 이름입니다.
- 이메일 – AWS 계정와 연결된 이메일 주소입니다.

AWS 서비스 탭

이 탭에는 평가 범위에 포함된 AWS 서비스 목록이 표시됩니다. 즉, 이는 평가에서 증거를 수집하는 AWS 서비스입니다.

총 서비스 수는 페이지 상단의 평가 세부 정보 섹션에 요약되어 있습니다.

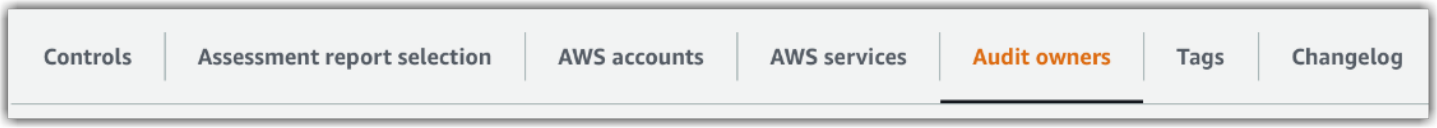
이 AWS 서비스 표에는 다음과 같은 데이터가 포함된 서비스 목록이 나와 있습니다.

- AWS 서비스 – AWS 서비스의 이름입니다.
- 범주 - 서비스 범주(예: 컴퓨팅 또는 데이터베이스)입니다.

Audit Manager는 이 표에 있는 서비스에 대한 리소스 평가를 수행합니다. 예를 들어, Amazon S3가 목록에 있는 경우 Audit Manager는 S3 버킷에 대한 증거를 수집할 수 있습니다. 수집되는 정확한 증거는 컨트롤의 데이터 소스에 의해 결정됩니다. 예를 들어, 데이터 소스 유형이 AWS Config이고 데이터 소스 매핑이 AWS Config 규칙(예:`s3-bucket-public-write-prohibited`)인 경우, Audit Manager는 해당 규칙 평가 결과를 증거로 수집합니다. 자세한 내용은 이 안내서의 범위 내 서비스와 데이터 소스 유형의 차이는 무엇인가요?를 참조하세요.

> **Note**
>
> 콘솔에서 표준 프레임워크를 기반으로 평가를 생성한 경우, Audit Manager는 해당 서비스를 선택하고 프레임워크의 요구 사항에 따라 해당 데이터 소스를 매핑했습니다. 표준 프레임워크에 수동 컨트롤만 포함된 경우에는 범위에 AWS 서비스가 없습니다. 범위 내에서 서비스 목록을 편집해야 하는 경우 UpdateAssessment API를 사용할 수 있습니다.

감사 소유자 탭

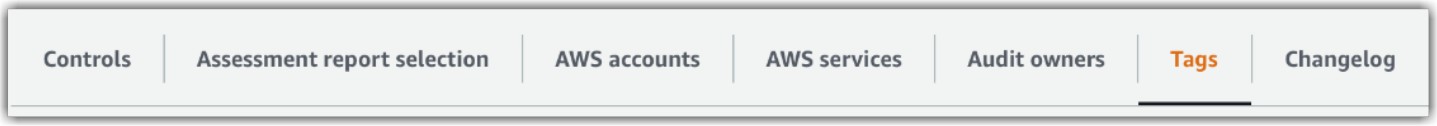


이 탭에는 평가의 감사 소유자가 표시됩니다. 총 감사 소유자 수는 페이지 상단의 평가 세부 정보 섹션에도 요약되어 있습니다.

감사 소유자 표에는 다음 데이터가 포함된 계정 목록이 표시됩니다.

- 감사 소유자 - 감사 소유자 이름입니다.
- AWS 계정 – 감사 소유자와 연결된 이메일 주소입니다.

태그 탭



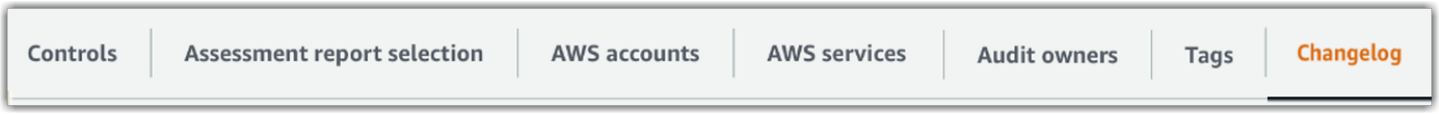
이 탭에는 프레임워크에서 상속된 태그가 이 평가를 생성하는 데 사용된 태그 목록이 표시됩니다. 총 태그 수는 페이지 상단의 평가 세부 정보에 요약되어 있습니다.

태그 표에는 다음 데이터가 포함된 태그 목록이 표시됩니다.

- 키 - 규정 준수 표준, 규정 또는 카테고리와 같은 태그의 키입니다.
- 값 - 태그의 값입니다.

Audit Manager의 태그에 대한 자세한 내용은 AWS Audit Manager 리소스에 태그 지정(을)를 참조하세요.

Changelog 탭



이 탭에는 평가와 관련된 사용자 활동 목록이 표시됩니다.

Changelog 표에는 다음 데이터가 포함된 계정 목록이 표시됩니다.

- 날짜 - 활동 날짜입니다.
- 사용자 - 작업을 수행한 사용자입니다.
- 작업 - 발생한 작업(예: 평가 생성 중)입니다.
- 유형 - 변경된 객체 유형(예: 평가)입니다.
- 리소스 - 변경의 영향을 받은 리소스(예: 평가를 생성한 프레임워크)입니다.

평가에서 컨트롤 검토하기

Audit Manager의 컨트롤 항목을 통해 감사 시 일반적이고 고유한 규정 준수 표준 및 규정을 모두 충족할 수 있습니다. 언제든지 Audit Manager 평가에서 컨트롤 항목을 열고 검토할 수 있습니다.

컨트롤 요약 페이지를 열려면

1. https://console.aws.amazon.com/auditmanager/home에서 AWS Audit Manager 콘솔을 엽니다.
2. 탐색 창에서 평가를 선택한 다음 평가 이름을 선택하여 평가를 엽니다.
3. 평가 페이지에서 컨트롤 탭을 선택하고 컨트롤 세트 표까지 아래로 스크롤한 다음 컨트롤 이름을 선택하여 엽니다.

컨트롤을 열면 여러 섹션이 포함된 요약 페이지가 표시됩니다. 이 페이지의 섹션과 내용은 다음 단원에 설명되어 있습니다.

컨트롤 페이지의 섹션

- 컨트롤 세부 정보
- 컨트롤 상태 업데이트
- 증거 폴더 탭
- 데이터 소스 탭
- 의견 탭
- Changelog 탭

컨트롤 세부 정보

컨트롤 세부 정보 섹션은 컨트롤에 대한 개요를 제공합니다.

여기에는 다음 정보가 포함됩니다.

1. 컨트롤 이름 - 이 컨트롤에 부여되는 이름입니다.
2. 컨트롤 설명 - 이 컨트롤에 대해 제공되는 설명입니다.
3. 테스트 정보 — 이통제에 권장되는 테스트 절차.
4. 작업 계획 - 컨트롤이 이행되지 않을 경우 수행할 권장 조치.

컨트롤 상태 업데이트

페이지의 컨트롤 상태 업데이트 섹션에서 평가 컨트롤의 상태를 검토하고 업데이트할 수 있습니다.

사용 가능한 상태는 다음과 같습니다.

- 검토 중 - 이 컨트롤이 아직 검토되지 않았음을 나타냅니다. 이 컨트롤에 대한 증거는 아직 수집 중이므로 수동 증거를 업로드할 수 있습니다. 이것이 기본 상태입니다.
- 검토됨 - 이 컨트롤에 대한 증거를 검토했음을 나타냅니다. 증거는 아직 수집 중이므로 수동 증거를 업로드할 수 있습니다.
- 비활성 - 이 컨트롤에 대한 자동 증거 수집이 중지되었음을 나타냅니다. 더 이상 수동 증거를 업로드할 수 없습니다.

> **Note**
>
> 컨트롤 상태를 검토됨으로 변경하는 것은 최종적입니다. 컨트롤 상태를 검토됨으로 설정한 후에는 더 이상 해당 컨트롤의 상태를 변경하거나 이전 상태로 되돌릴 수 없습니다.

증거 폴더 탭

증거 폴더 탭에는 이 컨트롤에 대해 자동으로 수집되는 증거가 나열됩니다. 매일 폴더로 구성되어 있습니다.

증거 폴더 표에는 다음 데이터가 포함된 폴더 목록이 표시됩니다.

- 증거 폴더 - 증거 폴더의 이름입니다. 이름은 증거가 수집되거나 수동으로 추가된 날짜를 기준으로 합니다.
- 규정 준수 검사 - 증거 폴더에서 발견된 문제의 수입니다. 이 숫자는 직접 AWS Security Hub 또는 AWS Config, 둘 다에서 보고된 보안 문제의 총 수를 나타냅니다. 해당 없음으로 표시되는 경우 AWS

Security Hub가 없거나 AWS Config이 비활성화되었거나 다른 데이터 소스 유형에서 나온 증거임을 나타냅니다.

- 전체 증거 - 폴더 내 증거 항목의 총 수입니다.
- 평가 보고서 선택 - 평가 보고서에 포함된 폴더 내 증거 항목의 수입니다.

증거 폴더 탭에서 다음과 같은 조치를 취할 수 있습니다.

- 개별 증거 검토 - 증거 폴더를 선택하여 엽니다. 그런 다음, 증거 폴더 요약 페이지에서 검토하려는 개별 증거를 선택할 수 있습니다.
- 수동 증거 추가 - 자세한 내용은 AWS Audit Manager에서 수동 증거 추가(을)를 참조하세요.
- 평가 보고서에 증거 추가 - 자세한 내용은 평가 보고서 생성(을)를 참조하세요.

데이터 소스 탭

이 탭에는 컨트롤의 데이터 소스에 대한 정보가 표시됩니다. 여기에는 다음 정보가 포함됩니다.

- 데이터 소스 이름 - 사용자 지정 컨트롤에만 적용됩니다. 각 데이터 소스에 부여한 설명형 이름을 나타냅니다. 이 이름을 사용하여 동일한 데이터 소스 유형에 속하는 여러 데이터 소스를 구별할 수 있습니다.
- 데이터 소스 유형 - 증거 데이터의 출처를 표시해 줍니다.
  - Audit Manager에서 증거를 수집하는 경우, 데이터 소스는 AWS Security Hub, AWS Config, AWS CloudTrail 또는 AWS API 호출의 네 가지 유형 중 하나일 수 있습니다.
  - 사용자만의 고유 증거를 업로드하는 경우, 데이터 소스 유형은 수동입니다. 설명란은 필요한 수동 증거가 파일 업로드인지 또는 텍스트 응답인지를 나타냅니다.
- 매핑 - 자동화된 데이터 소스에서 데이터를 식별하고 검색하는 데 사용되는 매핑 속성입니다.
  - 데이터 소스 유형이 AWS Config인 경우 매핑은 특정 AWS Config 규칙의 이름입니다(예:`EC2_INSTANCE_MANAGED_BY_SSM`). Audit Manager는 이 매핑을 이용하여 해당 규칙 검사의 결과를 AWS Config으로부터 직접 보고합니다.
  - 데이터 소스 유형이 AWS Security Hub인 경우의 매핑은 특정 Security Hub 컨트롤(예:`1.1 – Avoid the use of the "root" account`)의 이름을 나타냅니다. Audit Manager는 이 매핑을 이용하여 해당 보안 검사의 결과를 Security Hub으로부터 직접 보고합니다..
  - 데이터 소스 유형이 AWS API 직접 호출인 경우의 매핑은 특정 API 직접 호출(예:`ec2_DescribeSecurityGroups`)의 이름을 나타냅니다. Audit Manager는 이 매핑을 이용하여 API 응답을 수집합니다.

  - 데이터 소스 유형이 AWS CloudTrail인 경우 매핑은 특정 CloudTrail 이벤트(예: `CreateAccessKey`)의 이름입니다. Audit Manager는 이 매핑을 사용하여 CloudTrail 로그에서 관련 사용자 활동을 수집합니다.
- 빈도 - 이 데이터 소스에서 증거를 수집하는 빈도입니다. 빈도는 데이터 소스에 따라 다릅니다. 자세한 내용은 열에서 값을 선택하거나 증거 수집 빈도 부분을 참조하세요.

의견 탭

의견 탭에서 컨트롤 및 해당 증거에 대한 설명을 추가할 수 있습니다. 이전 의견 목록도 표시됩니다.

의견 보내기에서 텍스트를 입력한 다음 의견 제출을 선택하여 콘트롤에 설명을 추가할 수 있습니다.

이전 의견에서 의견을 작성한 날짜 및 관련 사용자 ID와 함께 이전 의견 목록을 볼 수 있습니다.

Changelog 탭

changelog 탭에는 컨트롤과 관련된 사용자 활동 목록이 표시됩니다. 동일한 정보를 AWS CloudTrail의 감사 추적 로그로 이용할 수 있습니다. Audit Manager에서 직접 캡처한 사용자 활동을 통해 특정 컨트롤에 대한 감사 활동 내역을 쉽게 검토할 수 있습니다.

Changelog 표에는 다음과 같은 데이터 열이 표시됩니다.

- 날짜 - 활동의 날짜 및 시간이며 협정 세계시(UTC)로 표시됩니다.
- 사용자 - 활동을 수행한 사용자 또는 역할.
- 작업 - 활동에 대한 설명입니다.
- 유형 - 활동을 자세히 설명하는 관련 속성입니다.
- 리소스 - 관련 리소스(해당하는 경우)입니다.

Audit Manager는 Changelog에서 다음과 같은 사용자 활동을 추적합니다.

- 평가 생성
- 평가 편집
- 평가 완료
- 평가 삭제
- 검토를 위한 컨트롤 세트 위임
- 검토된 컨트롤 세트를 감사 소유자에게 다시 제출

- 수동 증거 업로드
- 컨트롤 상태 업데이트
- 평가 보고서 생성

평가에서 증거 검토하기

Audit Manager의 활성 평가는 다양한 데이터 소스에서 증거를 자동으로 수집합니다. 자세한 내용은 AWS Audit Manager 증거 수집 방법(을)를 참조하세요. 언제든지 평가에서 컨트롤에 대한 증거를 열고 검토할 수 있습니다.

컨트롤에 대한 증거를 열려면

1. https://console.aws.amazon.com/auditmanager/home에서 AWS Audit Manager 콘솔을 엽니다.
2. 탐색 창에서 평가를 선택한 다음 평가 이름을 선택하여 평가를 엽니다.
3. 평가 페이지에서 컨트롤 탭을 선택하고 컨트롤 표까지 아래로 스크롤한 다음 컨트롤 이름을 선택하여 엽니다.
4. 컨트롤 페이지에서 증거 폴더 탭을 선택합니다. 증거 폴더 표 아래에 해당 컨트롤의 모든 증거 폴더 목록이 표시됩니다. 이러한 폴더는 폴더 내의 증거가 수집된 날짜를 기준으로 구성되고 이름이 지정됩니다.
5. 증거 폴더의 이름을 선택하여 엽니다.

이제 여기에서 해당 컨트롤의 증거 폴더를 검토하고 필요에 따라 더 자세히 분석하여 개별 증거를 검토할 수 있습니다.

주제

- 증거 폴더 검토
- 개별 증거 검토

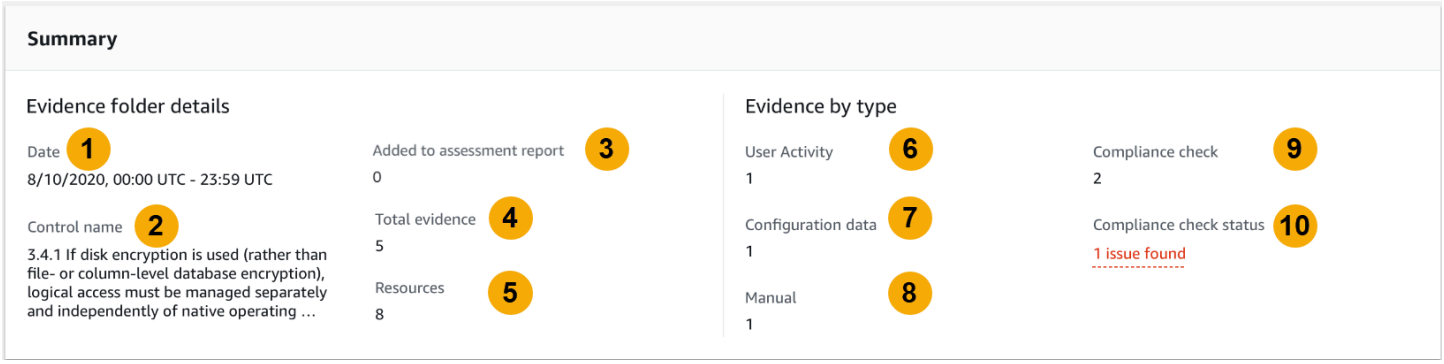
증거 폴더 검토

증거 폴더를 열면 요약 섹션과 증거 표라는 두 섹션이 포함된 증거 폴더 요약 페이지가 표시됩니다. 이러한 섹션과 해당 내용은 다음과 같이 설명됩니다.

- 증거 폴더 요약
- 증거 표

증거 폴더 요약

이 페이지의 요약 섹션은 증거 폴더에 있는 증거에 대한 높은 수준의 개요를 제공합니다.



여기에는 다음 정보가 포함됩니다.

1. 날짜 - 증거 폴더가 생성된 날짜 및 시간이며 협정 세계시(UTC)로 표시됩니다.
2. 컨트롤 이름 - 증거 폴더와 관련된 컨트롤의 이름입니다.
3. 평가 보고서에 추가됨 - 평가 보고서에 포함하기 위해 수동으로 선택한 증거 항목의 수입니다.
4. 전체 증거 - 증거 폴더에 있는 증거 항목의 총 수입니다.
5. 리소스 - 이 폴더에서 증거를 생성할 때 평가된 총 AWS 리소스 수입니다.
6. 사용자 활동 - 사용자 활동 범주에 속하는 증거 항목의 수입니다. 이 증거는 AWS CloudTrail 로그에서 수집됩니다.
7. 구성 데이터 - 구성 데이터 범주에 속하는 증거 항목의 수입니다. 이 증거는 Amazon EC2, Amazon S3 또는 IAM과 같은 다른 AWS 서비스의 구성 스냅샷에서 수집됩니다.
8. 수동 - 수동 범주에 속하는 증거 항목의 수입니다. 이 증거는 수동으로 업로드됩니다.
9. 규정 준수 검사 - 규정 준수 검사 범주에 속하는 증거 항목 수입니다. 이 증거는 AWS Config 또는 AWS Security Hub에서 수집됩니다.
10. 규정 준수 검사 상태 - AWS Security Hub, AWS Config 또는 둘 다에서 직접 보고된 문제의 총 수입니다.

> **Tip**
>
> 다양한 증거 유형(사용자 활동, 구성 데이터, 규정 준수 검사 및 매뉴얼)에 대한 자세한 내용은 증거를 참조하세요.

증거 표

증거 표에는 증거 폴더에 포함된 개별 증거가 나열됩니다.

여기에는 다음 정보가 포함됩니다.

1. 시간 - 증거가 수집된 시기를 지정하며 증거의 이름으로도 사용됩니다. 시간은 협정 세계시(UTC)로 표시됩니다. 이 열에서 시간을 선택하면 증거 세부 정보 페이지가 열립니다. 이 페이지에 대해서는 다음 섹션에서 설명합니다.
2. 유형별 증거 - 증거의 범주.
   - 규정 준수 확인 증거는 AWS Config 또는 AWS Security Hub에서 수집됩니다.
   - 사용자 활동 증거는 AWS CloudTrail 로그에서 수집됩니다.
   - 구성 데이터 증거는 Amazon EC2, Amazon S3 또는 IAM과 같은 다른 서비스의 스냅샷에서 수집됩니다.
   - 수동 증거는 수동으로 업로드한 증거입니다.
3. 규정 준수 검사 - 규정 준수 검사 범주에 속하는 증거의 평가 상태입니다.
   - AWS Security Hub에서 수집된 증거의 경우, 합격 또는 불합격 결과는 AWS Security Hub에서 직접 보고됩니다.
   - AWS Config에서 수집된 증거의 경우, 규정 준수 또는 규정 미준수 결과는 AWS Config에서 직접 보고됩니다.
   - 해당 사항 없음이 표시되면, AWS Security Hub가 없거나 AWS Config이 비활성화되어 있거나 다른 데이터 소스 유형에서 나온 증거임을 나타냅니다.
4. 데이터 소스 - 증거가 수집되는 데이터 소스입니다.
5. 사건 이름 - 증거에 포함된 사건의 이름입니다.
6. 리소스 - 증거를 생성하기 위해 평가된 리소스의 수입니다.
7. 평가 보고서 선택 - 해당 증거를 평가 보고서에 포함하기 위해 수동으로 선택했는지 여부를 나타냅니다.
   - 증거를 포함하려면 증거를 선택하고 평가 보고서에 추가를 선택합니다.
   - 증거를 제외하려면 증거를 선택하고 평가 보고서에서 제거를 선택합니다.

증거 폴더에 수동 증거를 업로드하려면 수동 증거 업로드를 선택하고 증거의 S3 URI를 입력한 다음 업로드를 선택합니다. 자세한 내용은 AWS Audit Manager에 수동 증거 업로드를 참조하세요.

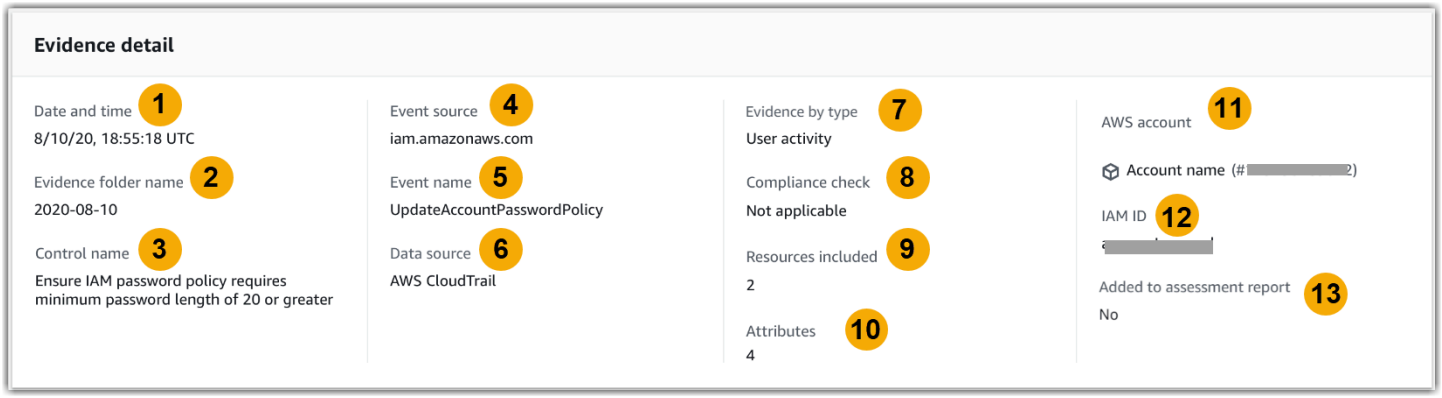
개별 증거의 세부 정보를 보려면, 시간 열에서 하이퍼링크된 증거 이름을 선택하세요. 이렇게 하, 다음 섹션에 설명된 증거 세부 정보 페이지가 열립니다.

개별 증거 검토

개별 증거를 열면 증거 세부 정보 섹션, 속성 표 및 포함된 리소스 표의 세 섹션으로 구성된 증거 세부 정보 페이지가 표시됩니다. 이러한 섹션과 해당 내용은 다음과 같이 설명됩니다.

증거 세부 정보

페이지의 증거 세부 정보 섹션에는 증거의 개요가 표시됩니다.



여기에는 다음 정보가 포함됩니다.

1. 날짜 및 시간 - 증거가 수집된 날짜 및 시간이며 협정 세계시(UTC)로 표시됩니다.
2. 증거 폴더 이름 - 증거가 들어 있는 증거 폴더의 이름입니다.
3. 컨트롤 이름 - 증거와 관련된 컨트롤의 이름입니다.
4. 이벤트 소스 - 증거 이벤트를 만든 리소스의 이름입니다.
5. 이벤트 이름 - 증거 이벤트의 이름입니다.
6. 데이터 소스 - 증거가 수집된 데이터 소스입니다.
7. 유형별 증거 - 증거의 유형입니다.
   - 규정 준수 확인 증거는 AWS Config 또는 AWS Security Hub에서 수집됩니다.
   - 사용자 활동 증거는 AWS CloudTrail 로그에서 수집됩니다.
   - 구성 데이터 증거는 Amazon EC2, Amazon S3 또는 IAM과 같은 다른 AWS 서비스의 스냅샷에서 수집됩니다.
   - 수동 증거는 수동으로 업로드한 증거입니다.

8. 규정 준수 검사 - 규정 준수 검사 범주에 속하는 증거의 평가 상태입니다.
   - AWS Security Hub에서 수집된 증거의 경우, 합격 또는 불합격 결과는 AWS Security Hub에서 직접 보고됩니다.
   - AWS Config에서 수집된 증거의 경우, 규정 준수 또는 규정 미준수 결과는 AWS Config에서 직접 보고됩니다.
   - 해당 사항 없음이 표시되면 AWS Security Hub가 없거나 AWS Config이 비활성화되어 있거나 다른 데이터 소스에서 나온 증거임을 나타냅니다.
9. 포함된 리소스 - 증거를 생성하기 위해 평가된 리소스의 수입니다.
10. 속성 - 사건이 증거에서 사용한 속성의 총 수입니다.
11. AWS 계정 - 증거가 수집된 AWS 계정입니다.
12. IAM ID - 관련 사용자 또는 역할(해당하는 경우)입니다.
13. 평가 보고서에 추가 - 평가 보고서에 증거를 포함하기로 선택했는지 여부를 나타냅니다.

속성

속성 표에는 이 증거에서 이벤트가 사용한 이름과 값이 표시됩니다. 여기에는 다음 정보가 포함됩니다.

- 속성 이름 - 증거의 요구 사항(예: 사용자의 암호 변경 허용)입니다.
- 값 - 속성의 값(예: 참 또는 거짓)입니다.

포함된 리소스

포함된 리소스 표에는 이러한 증거를 생성하기 위해 평가된 리소스 목록이 표시됩니다. 다음과 같은 필드 중 하나 이상을 포함합니다.

- ARN - 리소스의 Amazon 리소스 이름(ARN)입니다. 모든 증거 유형에 ARN을 사용할 수 있는 것은 아닙니다.
- 값 - 해당 리소스의 값(해당하는 경우).
- JSON - 해당 리소스의 JSON 파일을 볼 수 있는 링크입니다.

AWS Audit Manager에서 수동 증거 추가

Audit Manager는 다양한 컨트롤 기능에 대한 증거를 자동으로 수집할 수 있습니다. 하지만, 일부 컨트롤 기능에서는 증거를 직접 추가해야 합니다.

다음 예제를 고려하세요.

- 일부 컨트롤 기능은 물리적 기록(예: 서명) 또는 클라우드에서 생성되지 않은 이벤트(예: 관찰 및 인터뷰)의 제공과 관련이 있습니다. 이러한 경우에는 증거로 파일을 수동으로 업로드할 수 있습니다. 예를 들어, 컨트롤 항목에 조직 구조에 대한 정보가 필요한 경우, 회사 조직도 사본을 수동 증거로 업로드할 수 있습니다.
- 일부 컨트롤은 공급업체 위험 평가 질문을 나타냅니다. 위험 평가 질문에는 증거로 사용할 수 있는 문서(예: 조직도)가 필요할 수 있습니다. 또는 간단한 텍스트 응답(예: 직책 목록)만 있으면 될 수도 있습니다. 후자의 경우 질문에 답변하고 답변을 수동 증거로 저장할 수 있습니다.

또한 수동 업로드 기능을 사용하여 여러 환경의 증거를 관리할 수 있습니다. 회사에서 하이브리드 클라우드 모델 또는 멀티클라우드 모델을 사용하는 경우, 온프레미스 환경, 클라우드에서 호스팅되는 환경 또는 SaaS 애플리케이션에서 증거를 업로드할 수 있습니다. 이를 통해 각 증거가 특정 컨트롤에 매핑되는 Audit Manager 평가 구조 내에 저장하여 출처에 관계없이 증거를 정리할 수 있습니다.

Audit Manager의 다양한 증거 유형에 대해 자세히 알아보려면, 이 안내서의 개념 및 용어 섹션에 있는 증거를 참조하세요.

수동 증거 추가 방법

다음과 같은 방법을 사용하여 자체 수동 증거를 평가 관리에 추가할 수 있습니다.

다음 사항에 유의하세요.

- 한 번에 한 가지 방법만 사용하여 수동 증거를 추가할 수 있습니다.
- 수동 증거 파일 하나에 지원되는 최대 크기는 100MB입니다.
- 수동 증명을 위해 지원되는 파일 형식은 이 페이지 아래에 나열되어 있습니다.
- 각 AWS 계정는 하나의 제어에 매일 최대 100개의 증거 파일만 수동으로 제어에 업로드할 수 있습니다. 이 일일 할당량을 초과하면 해당 제어에 대한 추가 수동 업로드가 실패합니다. 대량의 수동 증거를 단일 컨트롤에 업로드해야 하는 경우, 며칠에 걸쳐 일괄적으로 증거를 업로드하세요.
- 컨트롤이 비활성화된 경우 해당 컨트롤에 수동 증거를 추가할 수 없습니다. 수동 증거를 추가하려면 먼저 컨트롤 상태를 검토 중 또는 검토됨으로 변경해야 합니다. 지침은 컨트롤 상태 업데이트(을)를 참조하세요.

Amazon S3에서 파일 가져오기

다음 단계에 따라 S3 버킷에서 수동 증거를 가져옵니다.

AWS console

S3에서 파일을 가져오려면(콘솔)

1. https://console.aws.amazon.com/auditmanager/home에서 AWS Audit Manager 콘솔을 엽니다.
2. 왼쪽 탐색 창에서 평가를 선택한 다음 평가 이름을 선택하여 엽니다.
3. 컨트롤 탭을 선택하고 컨트롤 세트까지 아래로 스크롤한 다음 컨트롤 이름을 선택하여 엽니다.
4. 증거 폴더 탭에서 수동 증거 추가를 선택한 다음 S3에서 파일 가져오기를 선택합니다.
   - 또는 증거 폴더 탭에서 증거 폴더 이름을 선택하여 증거 폴더 요약을 검토한 다음, 수동 증거 추가, S3에서 파일 가져오기를 선택합니다.
5. 다음 페이지에서 증거의 S3 URI를 입력합니다. Amazon S3 콘솔에서 객체로 이동한 다음 S3 URI 복사를 선택하면 S3 URI를 찾을 수 있습니다.
6. 업로드를 선택합니다.

AWS CLI

다음 절차에서는 *## ### ###*를 자신의 정보로 바꿉니다.

S3에서 파일을 가져오려면(CLI)

1. `list-assessments` 명령을 실행하여 평가 목록을 확인합니다.

```
aws auditmanager list-assessments
```

   응답에서 증거를 업로드하려는 평가를 찾아 평가 ID를 기록해 두세요.

2. `get-assessment` 명령을 실행하고 1단계의 평가 ID를 지정합니다.

```
aws auditmanager get-assessment --assessment-
id 1a2b3c4d-5e6f-7g8h-9i0j-0k1l2m3n4o5p
```

   응답에서 증거를 업로드하려는 컨트롤 세트와 컨트롤을 찾아 ID를 기록해 두세요.

3. `batch-import-evidence-to-assessment-control` 명령을 다음 파라미터와 함께 실행합니다.

   - `--assessment-id` - 1단계의 평가 ID를 사용하세요.
   - `--control-set-id` - 2단계의 컨트롤 세트 ID를 사용합니다.

- `--control-id` - 2단계의 컨트롤 ID를 사용합니다.
- `--manual-evidence` - `s3ResourcePath`를 수동 증거 유형으로 사용하고 증거의 S3 URI를 지정하세요. Amazon S3 콘솔에서 객체로 이동한 다음 S3 URI 복사를 선택하면 S3 URI를 찾을 수 있습니다.

```
aws auditmanager batch-import-evidence-to-assessment-control --assessment-
id 1a2b3c4d-5e6f-7g8h-9i0j-0k1l2m3n4o5p --control-set-id ControlSet --control-
id a1b2c3d4-e5f6-g7h8-i9j0-k1l2m3n4o5p6 --manual-evidence s3ResourcePath=s3://
example-bucket/example-file.extension
```

Audit Manager API

S3에서 파일을 가져오려면(API)

1. `ListAssessments` 작업을 호출하여 평가 목록을 확인하세요. 응답에서 증거를 업로드하려는 평가를 찾아 평가 ID를 기록해 두세요.
2. `GetAssessment` 작업을 호출하고 1단계의 평가 ID를 지정하세요. 응답에서 증거를 업로드하려는 컨트롤 세트와 컨트롤을 찾아 ID를 기록해 두세요.
3. 다음 파라미터와 함께 `BatchImportEvidenceToAssessmentControl` 작업을 호출합니다.
   - `assessmentId` - 1단계의 평가 ID를 사용하세요.
   - `controlSetId` - 2단계의 컨트롤 세트 ID를 사용합니다.
   - `controlId` - 2단계의 컨트롤 ID를 사용합니다.
   - `manualEvidence` - `s3ResourcePath`를 수동 증거 유형으로 사용하고 증거의 S3 URI를 지정하세요. Amazon S3 콘솔에서 객체로 이동한 다음 S3 URI 복사를 선택하면 S3 URI를 찾을 수 있습니다.

자세한 내용은 이전 링크 중 하나를 선택하여 AWS Audit Manager API 참조에서 자세한 내용을 읽어보세요. 여기에는 이러한 작업 및 파라미터를 언어별 AWS SDK 중 하나로 사용하는 방법에 대한 정보가 포함됩니다.

브라우저에서 파일 업로드

다음 단계에 따라 브라우저에서 수동 증거를 업로드하세요.

AWS console

브라우저에서 파일을 업로드하려면(콘솔)

1. https://console.aws.amazon.com/auditmanager/home에서 AWS Audit Manager 콘솔을 엽니다.
2. 왼쪽 탐색 창에서 평가를 선택한 다음 평가 이름을 선택하여 엽니다.
3. 컨트롤 탭에서 컨트롤 세트까지 아래로 스크롤한 다음 컨트롤 이름을 선택하여 엽니다.

   여기에서 세 가지 방법으로 파일을 업로드할 수 있습니다.

   - (선택 사항 1) 파란색 알림 배너에서 수동 증거 업로드를 선택합니다.
   - (선택 사항 2) 증거 폴더 탭에서 수동 증거 추가를 선택한 다음 브라우저에서 파일 업로드를 선택합니다.
   - (선택 사항 3) 해당 폴더의 요약을 검토할 증거 폴더 이름을 선택하고 수동 증거 추가를 선택한 다음 브라우저에서 파일 업로드를 선택합니다.
4. 업로드할 파일을 선택합니다.
5. 업로드를 선택합니다.

AWS CLI

다음 절차에서는 *## ### ###*를 자신의 정보로 바꿉니다.

브라우저에서 파일을 업로드하려면(CLI)

1. list-assessments 명령을 실행하여 평가 목록을 확인합니다.

   ```
   aws auditmanager list-assessments
   ```

   응답에서 증거를 업로드하려는 평가를 찾아 평가 ID를 기록해 두세요.
2. get-assessment 명령을 실행하고 1단계의 평가 ID를 지정합니다.

   ```
   aws auditmanager get-assessment --assessment-
   id 1a2b3c4d-5e6f-7g8h-9i0j-0k1l2m3n4o5p
   ```

   응답에서 증거를 업로드하려는 컨트롤 세트와 컨트롤을 찾아 ID를 기록해 두세요.
3. get-evidence-file-upload-url 명령을 실행하고 업로드할 파일을 지정합니다.

```
aws auditmanager get-evidence-file-upload-url --file-name fileName.extension
```

응답에 표시된 미리 서명된 URL과 `evidenceFileName`를 메모해 둡니다.

4. 3단계의 미리 서명된 URL을 사용하여 브라우저에서 파일을 업로드합니다. 이 작업을 수행하면 파일이 Amazon S3에 업로드되고, 평가 컨트롤에 첨부할 수 있는 객체로 저장됩니다. 다음 단계에서는 `evidenceFileName` 파라미터를 사용하여 새로 생성된 객체를 참조합니다.

> **Note**
>
> 미리 서명된 URL을 사용하여 파일을 업로드하는 경우 Audit Manager는 AWS Key Management Service와 함께 서버 측 암호화를 사용하여 데이터를 보호하고 저장합니다. 이를 지원하려면 미리 서명된 URL을 사용하여 파일을 업로드할 때 요청에 `x-amz-server-side-encryption` 헤더를 사용해야 합니다.
> Audit Manager 데이터 암호화 설정에서 고객 관리형 AWS KMS key를 사용하는 경우 요청에 `x-amz-server-side-encryption-aws-kms-key-id` 헤더도 포함해야 합니다. 요청에 `x-amz-server-side-encryption-aws-kms-key-id` 헤더가 없는 경우 Amazon S3는 AWS 관리형 키를 사용하려 한다고 가정합니다.
> 자세한 내용은 Amazon Simple Storage Service 사용 설명서의 AWS Key Management Service 키(SSE-KMS)로 서버 측 암호화를 사용하여 데이터 보호를 참조하세요.

5. `batch-import-evidence-to-assessment-control` 명령을 다음 파라미터와 함께 실행합니다.

- `--assessment-id` - 1단계의 평가 ID를 사용하세요.
- `--control-set-id` - 2단계의 컨트롤 세트 ID를 사용합니다.
- `--control-id` - 2단계의 컨트롤 ID를 사용합니다.
- `--manual-evidence` - 수동 증거 유형으로 `evidenceFileName`를 사용하고 3단계의 증거 파일 이름을 지정합니다.

```
aws auditmanager batch-import-evidence-to-assessment-control --assessment-
id 1a2b3c4d-5e6f-7g8h-9i0j-0k1l2m3n4o5p --control-set-id ControlSet
 --control-id a1b2c3d4-e5f6-g7h8-i9j0-k1l2m3n4o5p6 --manual-evidence
 evidenceFileName=fileName.extension
```

Audit Manager API

브라우저에서 파일을 업로드하려면(API)

1. `ListAssessments` 작업을 호출합니다. 응답에서 증거를 업로드하려는 평가를 찾아 평가 ID를 기록해 두세요.
2. `GetAssessment` 작업을 호출하고 1단계의 `assessmentId`를 지정하세요. 응답에서 증거를 업로드하려는 컨트롤 세트와 컨트롤을 찾아 ID를 기록해 두세요.
3. `GetEvidenceFileUploadUrl` 작업을 호출하고 업로드할 `fileName`를 지정하세요. 응답에 표시된 미리 서명된 URL과 `evidenceFileName`를 메모해 둡니다.
4. 3단계의 미리 서명된 URL을 사용하여 브라우저에서 파일을 업로드합니다. 이 작업을 수행하면 파일이 Amazon S3에 업로드되고, 평가 컨트롤에 첨부할 수 있는 객체로 저장됩니다. 다음 단계에서는 `evidenceFileName` 파라미터를 사용하여 새로 생성된 객체를 참조합니다.

   > **Note**
   >
   > 미리 서명된 URL을 사용하여 파일을 업로드하는 경우 Audit Manager는 AWS Key Management Service와 함께 서버 측 암호화를 사용하여 데이터를 보호하고 저장합니다. 이를 지원하려면 미리 서명된 URL을 사용하여 파일을 업로드할 때 요청에 `x-amz-server-side-encryption` 헤더를 사용해야 합니다.
   > Audit Manager 데이터 암호화 설정에서 고객 관리형 AWS KMS key를 사용하는 경우 요청에 `x-amz-server-side-encryption-aws-kms-key-id` 헤더도 포함해야 합니다. 요청에 `x-amz-server-side-encryption-aws-kms-key-id` 헤더가 없는 경우 Amazon S3는 AWS 관리형 키를 사용하려 한다고 가정합니다.
   > 자세한 내용은 Amazon Simple Storage Service 사용 설명서의 AWS Key Management Service 키(SSE-KMS)로 서버 측 암호화를 사용하여 데이터 보호를 참조하세요.

5. 다음 파라미터와 함께 `BatchImportEvidenceToAssessmentControl` 작업을 호출합니다.

   - `assessmentId` - 1단계의 평가 ID를 사용하세요.
   - `controlSetId` - 2단계의 컨트롤 세트 ID를 사용합니다.
   - `controlId` - 2단계의 컨트롤 ID를 사용합니다.
   - `manualEvidence` - 수동 증거 유형으로 `evidenceFileName`를 사용하고 3단계의 증거 파일 이름을 지정합니다.

자세한 내용은 이전 링크 중 하나를 선택하여 AWS Audit Manager API 참조에서 자세한 내용을 읽어보세요. 여기에는 이러한 작업 및 파라미터를 언어별 AWS SDK 중 하나로 사용하는 방법에 대한 정보가 포함됩니다.

텍스트 응답을 입력합니다.

다음 단계에 따라 위험 평가 질문에 대한 응답을 입력하고 응답을 수동 증거로 저장하세요.

AWS console

텍스트 응답을 입력하려면(콘솔)

1. https://console.aws.amazon.com/auditmanager/home에서 AWS Audit Manager 콘솔을 엽니다.
2. 왼쪽 탐색 창에서 평가를 선택한 다음 평가 이름을 선택하여 엽니다.
3. 컨트롤 탭을 선택하고 컨트롤 세트까지 아래로 스크롤한 다음 컨트롤 이름을 선택하여 엽니다.

   여기에서 텍스트 응답을 입력하는 세 가지 방법이 있습니다.

   - (선택 사항 1) 파란색 알림 배너에서 응답 입력을 선택합니다.
   - (선택 사항 2) 증거 폴더 탭에서 수동 증거 추가를 선택한 다음 텍스트 응답 입력을 선택합니다.
   - (선택 사항 3) 해당 폴더의 요약을 검토할 증거 폴더를 선택하고 수동 증거 추가를 선택한 다음 텍스트 응답 입력을 선택합니다.
4. 표시되는 팝업 창에서 응답을 일반 텍스트 형식으로 입력합니다.
5. 확인을 선택합니다.

AWS CLI

다음 절차에서는 *## ### ###*를 자신의 정보로 바꿉니다.

텍스트 응답을 입력하려면(CLI)

1. `list-assessments` 명령을 실행합니다.

   ```
   aws auditmanager list-assessments
   ```

   응답에서 증거를 업로드하려는 평가를 찾아 평가 ID를 기록해 두세요.

2. get-assessment 명령을 실행하고 1단계의 평가 ID를 지정합니다.

```
aws auditmanager get-assessment --assessment-
id 1a2b3c4d-5e6f-7g8h-9i0j-0k1l2m3n4o5p
```

응답에서 증거를 업로드하려는 컨트롤 세트 및 컨트롤을 찾고 해당 ID를 기록해 두세요.

3. batch-import-evidence-to-assessment-control 명령을 다음 파라미터와 함께 실행합니다.

- --assessment-id - 1단계의 평가 ID를 사용하세요.
- --control-set-id - 2단계의 컨트롤 세트 ID를 사용합니다.
- --control-id - 2단계의 컨트롤 ID를 사용합니다.
- --manual-evidence - 수동 증거 유형으로 textResponse를 사용하고 수동 증거로 저장하려는 텍스트를 입력합니다.

```
aws auditmanager batch-import-evidence-to-assessment-control --assessment-
id 1a2b3c4d-5e6f-7g8h-9i0j-0k1l2m3n4o5p --control-set-id ControlSet --control-
id a1b2c3d4-e5f6-g7h8-i9j0-k1l2m3n4o5p6 --manual-evidence textResponse="enter
 text here"
```

Audit Manager API

텍스트 응답(API)을 입력하려면

1. ListAssessments 작업을 호출합니다. 응답에서 증거를 업로드하려는 평가를 찾아 평가 ID를 기록해 두세요.
2. GetAssessment 작업을 호출하고 1단계의 assessmentId를 지정하세요. 응답에서 증거를 업로드하려는 컨트롤 세트 및 컨트롤을 찾고 해당 ID를 기록해 두세요.
3. 다음 파라미터와 함께 BatchImportEvidenceToAssessmentControl 작업을 호출합니다.

- assessmentId - 1단계의 평가 ID를 사용하세요.
- controlSetId - 2단계의 컨트롤 세트 ID를 사용합니다.
- controlId - 2단계의 컨트롤 ID를 사용합니다.
- manualEvidence - 수동 증거 유형으로 textResponse를 사용하고 수동 증거로 저장하려는 텍스트를 입력합니다.

자세한 내용은 이전 링크 중 하나를 선택하여 AWS Audit Manager API 참조에서 자세한 내용을 읽어보세요. 여기에는 이러한 작업 및 파라미터를 언어별 AWS SDK 중 하나로 사용하는 방법에 대한 정보가 포함됩니다.

수동 증명을 위해 지원되는 파일 형식

다음 표는 수동 증거로 업로드할 수 있는 파일 유형을 나열하고 설명합니다. 각 파일 유형에 대해 지원되는 파일 확장자도 표에 나열되어 있습니다.

파일 유형	Description	지원되는 파일 확장자
압축 또는 아카이브	GNU Zip 압축 아카이브 및 ZIP 압축 아카이브	`.gz`, `.zip`
문서	PDF 및 Microsoft Office 파일과 같은 일반 문서 파일	`.doc`, `.docx`, `.pdf`, `.ppt`, `.pptx`, `.xls`, `.xlsx`
이미지	이미지 및 그래픽 파일	`.jpeg`, `.jpg`, `.png`, `.svg`
텍스트	기타 비바이너리 텍스트 파일(예: 일반 텍스트 문서 및 마크업 언어 파일)	`.cer`, `.csv`, `.html`, `.jmx`, `.json`, `.md`, `.out`, `.rtf`, `.txt`, `.xml`, `.yaml`, `.yml`

평가 보고서 생성

평가 보고서는 평가를 요약하고 관련 증거가 포함된 체계적인 폴더 세트로 연결되는 링크를 제공합니다. 자세한 내용은 평가 보고서(을)를 참조하세요.

평가 보고서를 생성하기 전에 평가 보고서에 포함할 증거를 선택할 수 있습니다. 새로 수집된 증거는 평가 보고서에 자동으로 포함되지 않습니다.

Tasks

- 평가 보고서에 증거 추가
- 평가 보고서에서 증거 제거
- 평가 보고서 생성
- 다음으로 무엇을 할 수 있습니까?

평가 보고서에 증거 추가

평가 보고서를 생성하려면 먼저 평가 보고서에 증거를 하나 이상 추가해야 합니다. 전체 증거 폴더를 추가하거나 폴더 내에서 개별 증거 항목을 추가할 수 있습니다.

평가 보고서에 증거를 추가하려면

1. https://console.aws.amazon.com/auditmanager/home에서 AWS Audit Manager 콘솔을 엽니다.
2. 탐색 창에서 평가를 선택한 다음 평가 이름을 선택하여 평가를 엽니다.
3. 컨트롤 탭에서 컨트롤 세트 표까지 아래로 스크롤한 다음 컨트롤 이름을 선택하여 엽니다.
4. 평가 보고서에 증거를 추가할 방법을 선택합니다.

   a. 증거 폴더 전체를 추가하려면 증거 폴더로 스크롤하여 추가하려는 폴더를 선택한 다음 평가 보고서에 추가를 선택합니다.

      - 찾고 있는 폴더가 보이지 않으면 드롭다운 필터를 전체 시간으로 변경하세요. 그렇지 않으면, 기본적으로 지난 7일간의 폴더가 표시됩니다.
      - 평가 보고서에 추가가 회색으로 표시되면 증거 폴더가 평가 보고서에 이미 추가된 것입니다.

   b. 특정 증거를 추가하려면 증거 폴더를 선택하여 해당 내용을 여세요. 목록에서 하나 이상의 항목을 선택한 다음 평가 보고서에 추가를 선택합니다.

      - 평가 보고서에 추가가 회색으로 표시된 경우 증거 옆의 확인란을 선택했는지 확인한 다음 다시 시도하세요.

5. 평가 보고서에 증거를 추가하면 녹색 성공 배너가 나타납니다. 평가 보고서에 포함할 증거를 보려면 평가 보고서의 증거 보기를 선택합니다.
   - 또는 평가로 돌아가서 평가 보고서 선택 탭을 선택하여 평가 보고서에 포함될 증거를 확인할 수도 있습니다.

평가 보고서에서 증거 제거

평가 보고서에서 증거를 제거해야 하는 경우 다음 단계를 따르세요. 증거 폴더 전체를 제거하거나 폴더 내에서 특정 증거 항목을 제거할 수 있습니다.

평가 보고서에서 증거를 제거하려면

1. https://console.aws.amazon.com/auditmanager/home에서 AWS Audit Manager 콘솔을 엽니다.

2. 탐색 창에서 평가를 선택한 다음 평가 이름을 선택하여 평가를 엽니다.
3. 컨트롤 탭에서 컨트롤 세트 표까지 아래로 스크롤한 다음 컨트롤 이름을 선택하여 엽니다.
4. 평가 보고서에서 증거를 제거하는 방법을 선택합니다.

   a. 증거 폴더 전체를 제거하려면 증거 폴더로 스크롤하여 추가하려는 폴더를 선택한 다음 평가 보고서에서 제거를 선택합니다.

      - 찾고 있는 폴더가 보이지 않으면 드롭다운 필터를 전체 시간으로 변경하세요. 그렇지 않으면, 기본적으로 지난 7일간의 폴더가 표시됩니다.
      - 평가 보고서에서 제거가 회색으로 표시되면 증거 폴더가 평가 보고서에 이미 제거된 것입니다.

   b. 특정 증거를 제거하려면 증거 폴더를 선택하여 내용을 여십시오. 목록에서 하나 이상의 항목을 선택한 다음 평가 보고서에서 제거를 선택합니다.

      - 평가 보고서에서 제거가 회색으로 표시된 경우, 증거 옆의 확인란을 선택했는지 확인한 다음 다시 시도하세요.

5. 평가 보고서에 증거를 추가하면 녹색 성공 배너가 나타납니다. 평가 보고서에 포함할 증거를 보려면 평가 보고서의 증거 보기를 선택합니다.

   - 또는 평가로 돌아가서 평가 보고서 선택 탭을 선택하여 평가 보고서에 포함될 증거를 확인할 수도 있습니다.

평가 보고서 생성

평가 보고서에 증거를 추가한 후 최종 평가 보고서를 생성하여 심사자와 공유할 수 있습니다. 평가 보고서를 생성하면 평가 보고서 목적지로 선택한 S3 버킷에 저장됩니다.

> **Tip**
>
> 평가 보고서가 성공적으로 생성되었는지 확인하려면 평가 보고서 목적지의 구성 팁를 검토하세요.

평가 보고서를 생성하려면

1. https://console.aws.amazon.com/auditmanager/home에서 AWS Audit Manager 콘솔을 엽니다.
2. 왼쪽 탐색 창에서 평가를 선택합니다.

3. 평가 보고서를 생성하려는 평가 이름을 선택합니다.
4. 평가 보고서 선택 탭을 선택한 다음 평가 보고서 생성을 선택합니다.
   - 평가 보고서 생성이 회색으로 표시되면 평가 보고서에 아직 증거가 추가되지 않았음을 의미합니다.
5. 팝업 창에서 평가 보고서의 이름과 설명을 입력하고 평가 보고서 세부 정보를 검토하세요.
6. 평가 보고서 생성을 선택하고 평가 보고서가 생성되는 동안 몇 분 정도 기다려 주세요.
7. Audit Manager 콘솔의 다운로드 센터 페이지에서 평가 보고서를 찾아 다운로드하세요.
   - 또는 평가 보고서 대상 S3 버킷으로 이동하여 평가 보고서를 다운로드할 수도 있습니다.

평가 보고서에는 평가 보고서의 무결성을 보장하기 위한 파일 체크섬이 있습니다. Audit Manager에서 제공하는 ValidateAssessmentReportIntegrity API 작업을 사용하여 이를 검증할 수 있습니다.

다음으로 무엇을 할 수 있습니까?

평가 보고서를 생성한 후 다음에 대한 자세한 정보를 알아볼 수 있습니다.

- 평가 보고서 검색 및 다운로드 - 다운로드 센터 또는 Amazon S3에서 평가 보고서를 다운로드하는 방법을 알아봅니다.
- 평가 보고서 살펴보기 - 평가 보고서를 탐색하고 내용을 탐색하는 방법을 알아봅니다.
- 평가 보고서 검증 - ValidateAssessmentReportIntegrity API 작업을 사용하여 평가 보고서를 검증하는 방법을 알아봅니다.
- 불필요한 평가 보고서 삭제 - 다운로드 센터 또는 Amazon S3에서 불필요한 보고서를 삭제하는 방법을 알아봅니다.

평가 상태를 비활성으로 변경

더 이상 평가를 위한 증거를 수집하지 않아도 되는 경우 평가 상태를 비활성으로 변경할 수 있습니다. 평가 상태가 비활성으로 변경되면 평가에서는 증거 수집을 중지합니다. 그러면 해당 평가에 대해 더 이상 요금이 부과되지 않습니다.

증거 수집을 중지하는 것 외에도 Audit Manager는 비활성 평가 내의 컨트롤 항목을 다음과 같이 변경합니다.

- 모든 컨트롤 세트가 검토됨 상태로 변경됩니다.

- 검토 중인 모든 컨트롤이 검토됨 상태로 변경됩니다.
- 비활성 평가의 대리인은 더 이상 해당 컨트롤 및 컨트롤 세트를 보거나 편집할 수 없습니다.

> **Warning**
>
> 이 작업은 되돌릴 수 없습니다. 주의해서 진행하고 평가를 비활성 상태로 표시하는 것이 좋습니다. 평가가 비활성 상태인 경우 평가 콘텐츠에 대한 읽기 전용 액세스 권한이 있습니다. 즉, 이전에 수집한 증거를 계속 검토하고 평가 보고서를 생성할 수 있습니다. 하지만 비활성 평가를 편집하거나 설명을 추가하거나 수동 증거를 업로드할 수 없습니다.

Audit Manager console

평가 상태를 비활성으로 변경하려면(콘솔)

1. https://console.aws.amazon.com/auditmanager/home에서 AWS Audit Manager 콘솔을 엽니다.
2. 탐색 창에서 평가를 선택합니다.
3. 평가에 대한 이름을 선택하여 해당 내용을 엽니다.
4. 페이지의 오른쪽 위 모서리에서 평가 상태 업데이트를 선택한 다음 비활성을 선택합니다.
5. 팝업 창에서 업데이트 상태를 선택하여 상태를 비활성으로 변경할지 확인합니다.

평가 및 해당 컨트롤에 대한 변경 사항은 약 1분 후에 적용됩니다.

AWS CLI

평가 상태를 비활성으로 변경하려면(AWS CLI)

1. 먼저 업데이트하려는 평가를 식별합니다. 이렇게 하려면 list-assessments 명령을 실행하세요.

   ```
   aws auditmanager list-assessments
   ```

   응답은 평가 목록을 반환합니다. 비활성화하려는 평가를 찾아 평가 ID를 기록해 둡니다.
2. 그런 다음, update-assessment-status 명령을 실행하고 다음 파라미터를 지정합니다.
   - `--assessment-id` - 이 파라미터를 사용하여 비활성화하려는 평가를 지정합니다.
   - `--status` 이 값을 `INACTIVE`로 설정하세요.

다음 예에서는 각 *## ### ###*를 자신의 정보로 바꿉니다.

```
aws auditmanager update-assessment-status --assessment-id a1b2c3d4-5678-90ab-cdef-EXAMPLE11111 --status INACTIVE
```

평가 및 해당 컨트롤에 대한 변경 사항은 약 1분 후에 적용됩니다.

Audit Manager API

평가 상태를 비활성(API)으로 변경하려면

1. ListAssessments 작업을 사용하여 비활성화하려는 평가를 찾고 평가 ID를 기록해 둡니다.
2. UpdateAssessmentStatus 작업을 사용하고 다음 파라미터를 지정하세요.
   - assessmentId - 이 파라미터를 사용하여 비활성화하려는 평가를 지정합니다.
   - status - 이 값을 `INACTIVE`로 설정합니다.

평가 및 해당 컨트롤에 대한 변경 사항은 약 1분 후에 적용됩니다.

이러한 API 작업에 대한 자세한 내용은 이전 링크 중 하나를 선택하여 AWS Audit Manager API 참조에서 자세한 내용을 읽어보세요. 여기에는 이러한 작업 및 파라미터를 언어별 AWS SDK 중 하나로 사용하는 방법에 대한 정보가 포함됩니다.

평가 삭제

더 이상 필요하지 않은 Audit Manager 평가를 삭제할 수 있습니다. 감사 관리자 콘솔, 감사 관리자 API 또는 AWS Command Line Interface(AWS CLI)를 사용하여 평가를 삭제할 수 있습니다.

> **Warning**
>
> 이 작업을 수행하면 평가 및 평가에서 수집한 모든 증거가 영구적으로 삭제됩니다. 이 데이터는 복구할 수 없습니다. 따라서 주의해서 진행하고 평가를 삭제할 것인지 확인하는 것이 좋습니다.

Audit Manager console

평가를 삭제하려면(콘솔)

1. https://console.aws.amazon.com/auditmanager/home에서 AWS Audit Manager 콘솔을 엽니다.
2. 탐색 창에서 평가를 선택합니다.
3. 삭제하려는 평가를 선택하고 삭제를 선택합니다.
   - 또는 평가를 연 다음 페이지 오른쪽 상단에서 삭제를 선택할 수도 있습니다.

AWS CLI

평가를 삭제하려면(AWS CLI)

1. 먼저 삭제하려는 평가를 식별합니다. 이렇게 하려면 list-assessments 명령을 실행하세요.

   ```
   aws auditmanager list-assessments
   ```

   응답은 평가 목록을 반환합니다. 삭제하려는 평가를 찾고 평가 ID를 기록해 둡니다.
2. 그런 다음, delete-assessment 명령을 사용하여 삭제하려는 평가 `--assessment-id`를 지정합니다.

   다음 예에서는 각 *## ### ###*를 자신의 정보로 바꿉니다.

   ```
   aws auditmanager delete-assessment --assessment-id a1b2c3d4-5678-90ab-cdef-EXAMPLE11111
   ```

Audit Manager API

평가를 삭제하려면(API)

1. ListAssessments 작업을 사용하여 삭제하려는 평가를 찾을 수 있습니다.

   응답에 표시된 평가 ID를 메모해 둡니다.
2. DeleteAssessment 작업을 사용하고 삭제하려는 평가의 assessmentId를 지정합니다.

이러한 API 작업에 대한 자세한 내용은 이전 링크 중 하나를 선택하여 AWS Audit Manager API 참조에서 자세한 내용을 읽어보세요. 여기에는 이러한 작업 및 파라미터를 언어별 AWS SDK 중 하나로 사용하는 방법에 대한 정보가 포함됩니다.

> **Tip**
>
> 비용 절감이 목적이라면 삭제하는 대신, 평가 상태를 비활성으로 변경하는 방법을 고려합니다. 그러면 증거 수집이 중지되고 이전에 수집한 증거를 검토할 수 있는 읽기 전용 상태로 평가가 전환됩니다. 비활성 평가에는 요금이 부과되지 않습니다.

AWS Audit Manager에서의 위임

감사 소유자는 AWS Audit Manager를 사용하여 평가를 작성하고 해당 평가에 나열된 컨트롤에 대한 증거를 수집합니다. 감사 담당자가 컨트롤 세트에 대한 증거를 검증할 때 질문이 있거나 도움이 필요한 경우가 있습니다. 이 경우 감사 담당자는 주제 전문가에게 검토를 위해 컨트롤 세트를 위임할 수 있습니다.

상위 수준에서 위임 프로세스는 다음과 같습니다.

1. 감사 담당자는 평가에서 컨트롤 세트를 선택하고 검토를 위해 위임합니다.
2. 대리인은 이러한 컨트롤과 해당 증거를 검토하고, 완료 시 컨트롤 세트를 감사 소유자에게 다시 제출합니다.
3. 감사 소유자는 검토가 완료되었다는 알림을 받고 검토된 컨트롤에 위임자의 의견이 있는지 확인합니다.

AWS Audit Manager에서 위임 태스크를 관리하는 방법에 대해 자세히 알아보려면 이 가이드의 다음 섹션을 참조하세요.

주제

- 감사 소유자에 대한 위임 태스크
- 대리인의 위임 태스크

> **Note**
>
> 계정은 감사 소유자 또는 다른 AWS 리전의 대리인일 수 있습니다.

감사 소유자에 대한 위임 태스크

AWS Audit Manager의 감사 소유자로서 컨트롤 및 증거를 검토하는 데 도움을 줄 주제 전문가의 도움이 필요할 수 있습니다. 이 경우 컨트롤 세트를 검토하도록 위임할 수 있습니다.

다음 주제에서는 AWS Audit Manager에서 위임을 관리하는 방법에 대해 설명합니다.

위임 태스크

- 검토를 위한 컨트롤 세트 위임

- 진행 중인 위임 및 완료된 위임에 액세스
- 진행 중인 위임 및 완료된 위임 삭제

검토를 위한 컨트롤 세트 위임

주제 전문가의 도움이 필요한 경우 도움을 받을 AWS 계정을 선택한 다음 해당 계정에 검토를 위해 컨트롤 세트를 위임할 수 있습니다.

다음 절차 중 하나를 사용하여 컨트롤 세트를 위임할 수 있습니다.

평가 페이지에서 컨트롤 세트 위임하기

평가 페이지에서 컨트롤 세트를 위임하려면

1. https://console.aws.amazon.com/auditmanager/home에서 AWS Audit Manager 콘솔을 엽니다.
2. 탐색 창에서 평가를 선택합니다.
3. 위임하고자 하는 컨트롤 세트가 포함되어 있는 평가의 이름을 선택합니다.
4. 평가 페이지에서 컨트롤 탭을 선택합니다. 그러면 컨트롤 상태 요약과 평가 내 컨트롤 목록이 표시됩니다.
5. 컨트롤 세트를 선택하고 컨트롤 세트 위임을 선택합니다.
6. 위임 선택 아래에 사용자 및 역할 목록이 표시됩니다. 사용자 또는 역할을 선택하거나 검색 창을 사용하여 사용자 또는 역할을 찾습니다.
7. 위임 세부 정보에서 컨트롤 세트 이름과 평가 이름을 검토합니다.
8. (선택 사항) 설명 아래에 대리인이 검토 태스크를 수행하는 데 도움이 되는 지침이 포함된 설명을 추가합니다. 설명에 민감한 정보를 포함하지 마세요.
9. 컨트롤 세트 위임을 선택합니다.
10. 녹색의 성공 배너는 컨트롤 세트를 성공적으로 위임했음을 나타냅니다. 위임 요청을 보려면 위임 보기를 선택합니다. AWS Audit Manager콘솔의 왼쪽 탐색 창에서 위임을 선택하여 언제든지 위임을 확인할 수도 있습니다.

위임 페이지에서 컨트롤 세트 위임하기

위임 페이지에서 컨트롤 세트를 위임하려면

1. https://console.aws.amazon.com/auditmanager/home에서 AWS Audit Manager 콘솔을 엽니다.
2. 탐색 창에서 위임을 선택합니다.

3. 위임 페이지에서 위임 생성을 선택합니다.
4. 평가 및 컨트롤 세트 선택에서 위임하려는 평가 및 컨트롤 세트를 지정합니다.
5. 위임 선택 아래에 사용자 및 역할 목록이 표시됩니다. 사용자 또는 역할을 선택하거나 검색 창을 사용하여 사용자 또는 역할을 찾습니다.
6. (선택 사항) 설명 아래에 대리인이 검토 태스크를 수행하는 데 도움이 되는 지침이 포함된 설명을 추가합니다. 설명에 민감한 정보를 포함하지 마세요.
7. 위임 생성을 선택합니다.
8. 녹색의 성공 배너는 컨트롤 세트를 성공적으로 위임했음을 나타냅니다. 위임 요청을 보려면 위임 보기를 선택합니다. AWS Audit Manager콘솔의 왼쪽 탐색 창에서 위임을 선택하여 언제든지 위임을 확인할 수도 있습니다.

검토를 위해 컨트롤 세트를 위임하면 대리인은 알림을 받게 되고 컨트롤 세트 검토를 시작할 수 있습니다. 위임자가 따르는 이 프로세스는 대리인의 위임 태스크에 설명되어 있습니다.

> **Tip**
>
> 대리인은 SNS 주제를 구독하여 검토 태스크가 위임되면 이메일 알림을 받을 수 있습니다. AWS Audit Manager와 관련된 SNS 주제를 식별하고 구독하는 방법에 대한 자세한 내용은 AWS Audit Manager의 알림 섹션을 참조하세요.

진행 중인 위임 및 완료된 위임에 액세스

AWS Audit Manager의 왼쪽 탐색 창에서 위임을 선택하여 언제든지 위임 목록에 액세스할 수 있습니다. 위임 페이지에는 진행 중인 위임 및 완료된 위임 목록이 포함되어 있으며, 각 위임에 대한 다음 세부 정보가 포함됩니다.

- 위임 대상 - 컨트롤 세트를 위임한 AWS 계정.
- 날짜 - 컨트롤 세트를 위임한 날짜.
- 상태 - 위임의 현재 상태.
- 평가 - 평가 세부 정보 페이지 링크가 포함된 평가 이름.
- 컨트롤 세트 - 검토를 위해 위임된 컨트롤 세트의 이름.

위임이 완료되면 AWS Audit Manager에서 알림을 받게 됩니다. 대리인의 의견이 포함된 설명을 받을 수도 있습니다. 다음 절차는 위임이 완료된 후 Audit Manager에서 알림을 확인하는 방법과 대리인이 남긴 설명을 보는 방법을 설명합니다.

완료된 위임을 보고 설명을 확인하려면

1. https://console.aws.amazon.com/auditmanager/home에서 AWS Audit Manager 콘솔을 엽니다.
2. 탐색 창에서 알림을 선택합니다. 또는 화면 상단의 파란색 플래시 모음에서 알림을 선택하여 알림 페이지를 엽니다.
3. 다음 정보가 포함된 테이블 포함된 알림 페이지를 검토합니다.
   - 날짜 - 알림 날짜.
   - 평가 — 통제 세트와 연결된 평가의 이름입니다.
   - 컨트롤 세트 - 컨트롤 세트의 이름.
   - 소스 - 완성된 컨트롤 세트를 다시 제출한 대리인의 사용자 또는 역할.
   - 설명 - 대리인이 제공한 높은 수준의 의견.
4. 대리인이 검토하여 제출한 평가 및 컨트롤 세트를 찾은 다음 평가 이름을 선택하여 엽니다.
5. 평가 세부 정보 페이지의 컨트롤 탭에서 컨트롤 세트 테이블까지 아래로 스크롤합니다. 컨트롤 세트별로 그룹화된 컨트롤 열에서 컨트롤 세트의 이름을 확장하여 해당 컨트롤을 표시합니다. 그런 다음 통제 이름을 선택하여 통제 세부 정보 페이지를 엽니다.
6. 설명 탭을 선택하면 해당 컨트롤에 대해 대리인이 추가한 모든 의견을 볼 수 있습니다.
7. 컨트롤 세트에 대한 검토가 완료되었다고 생각하면 컨트롤 세트를 선택하고 컨트롤 세트 검토 완료를 선택합니다.

> **Important**
>
> Audit Manager는 지속적으로 증거를 수집합니다. 따라서 대리인이 컨트롤에 대한 검토를 완료한 후 새로운 증거가 추가로 수집될 수 있습니다.
> 검토된 증거만 평가 보고서에 사용하려는 경우, 컨트롤이 검토된 타임스탬프를 참조하여 증거가 검토된 시기를 확인할 수 있습니다. 이 타임스탬프는 컨트롤 세부 정보 페이지의 Changelog 탭에서 확인할 수 있습니다. 그런 다음 이 타임스탬프를 사용하여 평가 보고서에 어떤 증거를 추가하는지 식별할 수 있습니다.

진행 중인 위임 및 완료된 위임 삭제

위임을 만들었는데 나중에 해당 컨트롤 세트를 검토하는 데 더 이상 도움이 필요하지 않은 경우가 있을 수 있습니다. 이 경우 AWS Audit Manager에서 진행 중인 위임을 삭제할 수 있습니다. 위임 페이지에 더 이상 표시하고 싶지 않은 완료된 위임을 삭제할 수도 있습니다.

위임을 삭제하려면

1. https://console.aws.amazon.com/auditmanager/home에서 AWS Audit Manager 콘솔을 엽니다.
2. 탐색 창에서 위임을 선택합니다.
3. 위임 페이지에서 취소하려는 위임을 선택한 다음 위임 제거를 선택합니다.
4. 표시되는 팝업 창에서 삭제를 선택하여 선택을 확인합니다.

대리인의 위임 태스크

대리인은 일반적으로 여러 분야에 대한 전문 비즈니스 또는 기술 전문 지식을 보유하고 있습니다. 여기에는 데이터 보존 정책, 교육 계획, 네트워크 인프라 및 ID 관리가 포함됩니다. 감사 소유자가 자신의 전문 분야에 해당하는 컨트롤에 대해 수집한 증거를 검토하는 데 도움을 줄 수 있습니다.

대리인은 감사 소유자로부터 컨트롤 세트와 관련된 증거를 검토해 달라는 요청을 받을 수 있습니다. 이 요청은 감사 소유자가 이 증거를 검증하는 데 대리인의 도움이 필요함을 나타냅니다. 컨트롤 세트와 관련 증거를 검토하고, 설명을 추가하고, 추가 증거를 업로드하고, 검토하는 각 컨트롤의 상태를 업데이트하여 감사 소유자를 도울 수 있습니다.

다음 주제에서는 AWS Audit Manager에서 위임을 관리하는 방법에 대해 설명합니다.

> **Note**
>
> 감사 소유자는 전체 평가가 아닌 특정 컨트롤 세트를 검토하도록 위임할 수 있습니다. 따라서 대리인은 평가에 대한 제한된 액세스 권한을 가집니다. 대리인은 증거를 검토하고, 설명을 추가하고, 수동 증거를 업로드하고, 컨트롤 세트의 각 컨트롤에 대한 컨트롤 상태를 업데이트할 수 있습니다. Audit Manager의 역할 및 권한에 대한 자세한 내용은 사용자 페르소나에 대한 권장 정책은 다음과 같습니다. AWS Audit Manager 섹션을 참조하세요.

위임 태스크

- 위임 요청 수신에 대한 알림 보기

- 위임된 컨트롤 세트 및 관련 증거 검토
- 컨트롤에 설명 추가
- 컨트롤을 검토된 것으로 표시
- 검토된 컨트롤 세트를 감사 소유자에게 다시 제출하기

위임 요청 수신에 대한 알림 보기

감사 소유자가 컨트롤 세트 검토에 대한 지원을 요청하면, 감사 소유자가 위임한 컨트롤 세트를 알려주는 알림을 받게 됩니다.

> **Tip**
>
> 또한 SNS 주제를 구독하여 컨트롤 세트가 검토를 위해 위임된 경우 이메일 알림을 받을 수 있습니다. 자세한 내용은 AWS Audit Manager의 알림을 참조하십시오.

알림을 보려면

1. https://console.aws.amazon.com/auditmanager/home에서 AWS Audit Manager 콘솔을 엽니다.
2. 왼쪽 탐색 창에서 알림을 선택합니다. 또는 화면 상단의 파란색 플래시 모음에서 알림 보기를 선택하여 알림 페이지를 엽니다.
3. 알림 페이지에서 검토를 위해 위임된 컨트롤 세트 목록을 검토할 수 있습니다. 이 테이블에 포함되는 정보는 다음과 같습니다.

    - 날짜 - 컨트롤 세트를 위임한 날짜.
    - 평가 — 통제 세트와 연결된 평가의 이름입니다.
    - 컨트롤 세트 - 컨트롤 세트의 이름.
    - 소스 - 컨트롤 세트를 위임한 사용자 또는 역할.
    - 설명 - 감사 소유자가 제공하는 지침.

위임된 컨트롤 세트 및 관련 증거 검토

감사 소유자가 위임한 컨트롤 세트를 검토하여 감사 소유자를 지원할 수 있습니다. 이러한 컨트롤과 관련 증거를 조사하여 추가 조치가 필요한지 판단할 수 있습니다. 이러한 추가 조치에는 규정 준수를 입증하기 위해 추가 증거를 수동으로 업로드하거나 수행한 문제 해결 단계를 자세히 설명하는 설명을 남기는 것이 포함될 수 있습니다.

컨트롤 세트를 검토하려면

1. https://console.aws.amazon.com/auditmanager/home에서 AWS Audit Manager 콘솔을 엽니다.
2. 탐색 창에서 알림을 선택합니다. 또는 파란색 플래시 모음에서 알림 보기를 선택하여 알림 페이지를 엽니다.
3. 알림 페이지에는 사용자에게 위임된 컨트롤 세트 목록이 표시됩니다. 검토하려는 컨트롤 세트를 식별하고 관련 평가의 이름을 선택하여 평가 세부 정보 페이지를 엽니다.
4. 평가 세부 정보 페이지의 컨트롤 탭에서 컨트롤 세트 테이블까지 아래로 스크롤합니다.
5. 컨트롤 세트별로 그룹화된 컨트롤 열에서 컨트롤 세트의 이름을 확장하여 해당 컨트롤을 표시하고 컨트롤 이름을 선택하여 컨트롤 세부 정보 페이지를 엽니다.
6. (선택 사항) 통제 상태 업데이트를 선택하여 통제 상태를 변경합니다. 검토를 진행하는 동안 상태를 검토 중으로 표시할 수 있습니다.
7. 증거 폴더, 데이터 소스, 설명, Changelog 탭에서 컨트롤에 대한 정보를 검토합니다. 각 탭에 대한 자세한 내용과 이 정보를 해석하는 방법은 평가에서 컨트롤 검토하기 섹션을 참조하세요.

통제에 대한 증거 검토하기

1. 컨트롤 세부 정보 페이지에서 증거 폴더 탭을 선택합니다.
2. 증거 폴더 테이블로 이동하면 해당 컨트롤에 대한 증거가 포함된 폴더 목록이 표시됩니다. 이러한 폴더는 증거가 수집된 날짜를 기준으로 구성되고 이름이 지정됩니다.
3. 증거 폴더의 이름을 선택하여 엽니다. 그런 다음 해당 날짜에 수집된 모든 증거의 요약을 검토합니다. 이 요약에는 직접 AWS Security Hub 또는 AWS Config 두 곳 모두에서 보고된 규정 준수 확인 문제의 총 수가 포함됩니다. 이 페이지의 데이터를 해석하는 방법에 대한 지침은 증거 폴더 검토를 참조하세요.
4. 증거 폴더 요약 페이지에서 증거 테이블로 이동합니다. 시간 열에서 열려는 항목을 선택합니다. 그런 다음, 당시 수집된 증거에 대한 세부 정보를 검토합니다. 증거 세부 정보 페이지의 데이터를 해석하는 방법에 대한 지침은 개별 증거 검토를 참조하세요.

> **Tip**
>
> AWS Audit Manager가 많은 컨트롤에 대한 증거를 자동으로 수집하지만, 경우에 따라 규정 준수를 입증하기 위해 추가 증거를 제공해야 할 수도 있습니다. 이러한 경우 증거를 수동으로 업로드할 수 있습니다. 이에 대한 지침은 수동 증거 업로드를 참조하세요.

컨트롤에 설명 추가

검토하는 모든 통제에 의견을 추가할 수 있습니다. 이러한 설명은 감사 소유자가 볼 수 있습니다.

통제에 의견을 추가하려면

1. https://console.aws.amazon.com/auditmanager/home에서 AWS Audit Manager 콘솔을 엽니다.
2. 왼쪽 탐색 창에서 알림을 선택합니다. 또는 화면 상단의 파란색 플래시 모음에서 알림 보기를 선택하여 알림 페이지를 엽니다.
3. 알림 페이지에서 위임된 컨트롤 세트 목록을 검토합니다. 설명을 남기고 싶은 컨트롤이 포함된 컨트롤 세트를 찾아 관련 평가의 이름을 선택합니다.
4. 컨트롤 탭을 선택하고 컨트롤 세트 테이블까지 아래로 스크롤한 다음 컨트롤 이름을 선택하여 엽니다.
5. 설명 탭을 선택합니다.
6. 설명 전송에서 텍스트 상자에 설명을 입력합니다.
7. 설명 제출을 선택하여 설명을 추가합니다. 그러면 설명이 이 컨트롤과 관련된 다른 설명과 함께 페이지의 이전 설명 섹션 아래에 표시됩니다.

컨트롤을 검토된 것으로 표시

컨트롤 세트 내의 개별 컨트롤 상태를 업데이트하여 검토 진행 상황을 표시할 수 있습니다. 컨트롤 상태 변경은 선택 사항입니다. 그러나 컨트롤에 대한 검토를 완료한 후 각 컨트롤의 상태를 검토됨으로 변경하는 것이 좋습니다. 각 개별 컨트롤의 상태에 관계없이 여전히 감사 소유자에게 컨트롤을 다시 제출할 수 있습니다.

통제를 검토된 것으로 표시하려면

1. https://console.aws.amazon.com/auditmanager/home에서 AWS Audit Manager 콘솔을 엽니다.
2. 왼쪽 탐색 창에서 알림을 선택합니다. 또는 화면 상단의 파란색 플래시 모음에서 알림 보기를 선택하여 알림 페이지를 엽니다.
3. 알림 페이지에서 위임된 컨트롤 세트 목록을 검토합니다. 검토된 것으로 표시할 컨트롤을 찾은 관련 평가의 이름을 선택합니다.
4. 평가 세부 정보 페이지의 컨트롤 탭에서 컨트롤 세트 테이블까지 아래로 스크롤합니다.
5. 컨트롤 세트별로 그룹화된 컨트롤 열에서 컨트롤 세트의 이름을 확장하여 해당 컨트롤을 표시합니다. 통제 이름을 선택하여 통제 세부 정보 페이지를 엽니다.

6. 컨트롤 상태 업데이트를 선택하고 상태를 검토됨으로 변경합니다.
7. 표시되는 팝업 창에서 컨트롤 상태 업데이트를 선택하여 컨트롤 검토를 마쳤는지 확인합니다.

검토된 컨트롤 세트를 감사 소유자에게 다시 제출하기

위임된 컨트롤에 대한 검토를 마치면 감사 소유자에게 컨트롤 세트를 제출합니다. 이것으로 위임 프로세스가 완료됩니다.

검토된 컨트롤 세트를 감사 소유자에게 다시 제출하려면

1. https://console.aws.amazon.com/auditmanager/home에서 AWS Audit Manager 콘솔을 엽니다.
2. 왼쪽 탐색 창에서 알림을 선택합니다.
3. 위임된 컨트롤 세트의 목록을 검토합니다. 감사 소유자에게 제출하고자 하는 컨트롤 세트를 찾은 다음 관련 평가의 이름을 선택합니다.
4. 컨트롤 세트 테이블까지 아래로 스크롤하여 감사 소유자에게 제출할 컨트롤 세트를 선택한 다음 검토를 위해 제출을 선택합니다.
5. 표시되는 팝업 창에서 검토를 위해 제출을 선택하기 전에 설명을 추가할 수 있습니다. 컨트롤을 감사 소유자에게 제출하면 감사 소유자는 사용자가 남긴 모든 설명을 볼 수 있습니다.

평가 보고서

평가 보고서는 평가를 위해 수집된 선택된 증거를 요약합니다. 또한 각 증거에 대한 세부 정보가 포함된 PDF 파일 링크도 포함되어 있습니다. 평가 보고서의 구체적인 내용, 구성 및 명명 규칙은 보고서를 생성할 때 선택한 매개변수에 따라 달라집니다.

평가 보고서는 감사와 관련된 증거를 선택하고 수집하는 데 도움이 됩니다. 하지만 증거 자체의 적합성을 평가하지는 않습니다. 대신 Audit Manager는 선택한 증거 세부 정보를 감사자와 공유할 수 있는 결과로 제공하기만 하면 됩니다.

평가 보고서 폴더 구조

평가 보고서를 다운로드하면 Audit Manager에서 zip 폴더를 생성합니다. 여기에는 평가 보고서와 관련 증거 파일이 중첩된 하위 폴더에 들어 있습니다.

zip 폴더의 구조는 다음과 같습니다.

- 평가 폴더(예:`myAssessmentName-a1b2c3d4`) — 루트 폴더.
  - 평가 보고서 폴더(예:`reportName-a1b2c3d4e5f6g7`) - AssessmentReportSummary.pdf, digest.txt 및 README.txt 파일을 찾을 수 있는 하위 폴더입니다.
    - 통제 폴더별 증거(예:`controlName-a1b2c3d4e5f6g`) - 관련 통제별로 증거 파일을 그룹화하는 하위 폴더입니다.
      - 데이터 소스별 증거 폴더(예:`CloudTrail`,`Security Hub`) - 데이터 소스 유형별로 증거 파일을 그룹화하는 하위 폴더입니다.
        - 날짜별 증거 폴더(예:`2022-07-01`) - 증거 수집 날짜별로 증거 파일을 그룹화하는 하위 폴더입니다.
          - 증거 파일 - 개별 증거에 대한 세부 정보가 들어 있는 파일입니다.

평가 보고서 탐색 방법

먼저 zip 폴더를 열고 평가 보고서 폴더까지 한 단계 아래로 이동합니다. 여기에서 평가 보고서 PDF와 README.txt 파일을 찾을 수 있습니다.

README.txt 파일을 검토하여 zip 폴더의 구조와 내용을 이해할 수 있습니다. 또한 각 파일의 이름 지정 규칙에 대한 참조 정보도 제공합니다. 특정 항목을 찾는 경우 이 정보를 통해 하위 폴더나 증거 파일로 바로 이동할 수 있습니다.

그렇지 않으면, 증거를 찾아보고 필요한 정보를 찾으려면 평가 보고서 PDF를 여십시오. 이를 통해 보고서에 대한 높은 수준의 개요와 보고서 작성에 따른 평가 요약을 확인할 수 있습니다.

다음으로 목차(TOC)를 사용하여 보고서를 살펴보세요. 목차에서 하이퍼링크로 연결된 통제를 선택하여 해당 통제의 요약으로 바로 이동할 수 있습니다.

통제에 대한 증거 세부 정보를 검토할 준비가 되면 하이퍼링크된 증거 이름을 선택하여 검토할 수 있습니다. 자동 증거의 경우 하이퍼링크를 클릭하면 해당 증거에 대한 세부 정보가 포함된 새 PDF 파일이 열립니다. 수동 증거의 경우 하이퍼링크를 클릭하면 증거가 들어 있는 S3 버킷으로 이동합니다.

> **Tip**
>
> 각 페이지 상단의 브레드크럼 탐색에는 통제 및 증거를 탐색할 때 평가 보고서의 현재 위치가 표시됩니다. 하이퍼링크된 목차를 선택하면 언제든지 목차로 다시 이동할 수 있습니다.

평가 보고서 섹션

다음 정보를 사용하여 평가 보고서의 각 섹션에 대해 자세히 알아보십시오.

> **Note**
>
> 다음 섹션에서 속성 옆에 하이픈(-)이 표시되면 해당 속성의 값이 null이거나 값이 존재하지 않음을 나타냅니다.

- 커버 페이지
- 개요 페이지
- 목차 페이지 표
- 통제 페이지
- 증거 요약 페이지
- 증거 세부 정보 페이지

커버 페이지

표지에는 평가 보고서의 이름이 포함되어 있습니다. 또한 보고서를 생성한 사용자의 계정 ID와 함께 보고서가 생성된 날짜 및 시간이 표시됩니다.

커버 페이지의 형식은 다음과 같습니다. Audit Manager는 *## ####* 보고서와 관련된 정보로 대체합니다.

```
Assessment report name
Report generated on MM/DD/YYYY at HH:MM:SS AM/PM UCT by AccountID
```

개요 페이지

개요 페이지는 두 부분으로 구성되어 있습니다. 하나는 보고서 자체에 대한 요약이고 다른 하나는 보고되는 평가의 요약입니다.

보고서 요약

이 단원은 평가 보고서를 요약합니다.

- 보고서 이름 - 보고서의 이름
- 설명 — 감사 소유자가 보고서를 생성할 때 입력하는 설명입니다.
- 생성 날짜 - 보고서가 생성된 날짜입니다. 시간은 협정 세계시(UTC) 형식으로 표시됩니다.
- 포함된 총 통제 항목 — 보고서에 포함되고 증거를 수집한 통제 항목의 수입니다. 이는 평가 대상 총 통제 항목 수의 일부에 해당합니다.
- AWS 계정 포함 — 보고서에 포함되어 있고 증거를 수집한 AWS 계정의 개수입니다. 이는 AWS 계정 총 평가 건수의 일부에 해당합니다.
- 평가 보고서 선택 — 보고서에 포함하기 위해 선택한 증거 항목의 수입니다. 이것은 보고서에서 발견된 규정 준수 확인 문제의 총수를 포함합니다.

평가 요약

이 섹션에는 보고서와 관련된 평가가 요약되어 있습니다.

- 평가 이름 — 보고서가 생성된 평가의 이름입니다.
- 상태 — 보고서가 생성된 시점의 평가 상태입니다.
- 평가 영역 — 평가가 생성된 AWS 리전입니다.
- AWS 계정 평가 내 - 평가 범위에 있는 전체 AWS 계정 목록입니다.
- AWS 서비스 평가 내 - 평가 범위에 있는 전체 AWS 서비스 목록입니다.
- 프레임워크 이름 — 평가를 만든 프레임워크의 이름입니다.
- 감사 소유자 — 평가 감사 소유자의 사용자 또는 역할입니다.

- 최종 업데이트 — 평가가 마지막으로 업데이트된 날짜입니다. 시간은 UTC로 표시됩니다.

목차 페이지 표

평가 보고서의 전체 내용이 목차에 표시됩니다. 내용은 평가에 포함된 통제 세트를 기준으로 그룹화되고 구성됩니다. 컨트롤은 해당 컨트롤 세트 아래에 나열됩니다.

목차에서 항목을 선택하면 보고서의 해당 섹션으로 바로 이동할 수 있습니다. 통제 세트를 선택하거나 통제로 직접 이동할 수 있습니다.

통제 페이지

통제 페이지는 두 부분으로 구성되어 있습니다. 하나는 통제 자체에 대한 요약이고 다른 하나는 통제를 위해 수집된 증거의 요약입니다.

통제 요약

이 섹션에는 다음 정보가 포함됩니다.

- 통제 이름 — 통제의 이름입니다.
- 설명 — 통제에 대한 설명입니다.
- 통제 세트 — 통제가 속한 통제 세트의 이름.
- 테스트 정보 — 이통제에 권장되는 테스트 절차.
- 실행 계획 — 통제가 이행되지 않을 경우 수행할 권장 조치.
- 평가 보고서 선택 — 평가 보고서에 포함된 이 통제와 관련된 증거 항목의 수. 여기에는 이 대조군의 증거에서 발견된 규정 준수 검사 문제의 수가 포함됩니다.

수집된 증거

이 섹션에는 통제를 위해 수집된 증거가 나와 있습니다. 증거는 폴더별로 그룹화되며 증거 수집 날짜를 기준으로 정리되고 이름이 지정됩니다. 각 증거 폴더 이름 옆에는 해당 폴더에 대한 규정 준수 검사 문제의 총 수가 표시됩니다.

각 증거 폴더 이름 아래에는 하이퍼링크된 증거 이름 목록이 있습니다.

- 자동 증거 이름은 증거 수집 타임스탬프로 시작하여 서비스 코드, 이벤트 이름(최대 20자), 계정 ID, 12자의 고유한 ID로 이어집니다.

  예: `21-30-24_IAM_CreateUser_111122223333_a1b2c3d4e5f6`

자동 증거의 경우 하이퍼링크로 연결된 이름을 클릭하면 요약 및 추가 세부 정보가 포함된 새 PDF 파일이 열립니다.

- 수동 증거 이름은 증거 업로드 타임스탬프로 시작하여 `manual` 라벨, 계정 ID, 12자의 고유 ID로 이어집니다. 또한 파일 이름의 처음 10자와 파일 확장자(최대 10자)도 포함됩니다.

  예: `00-00-00_manual_111122223333_a1b2c3d4e5f6_myimage.png`

  수동 증거의 경우 하이퍼링크된 이름을 사용하면 해당 증거가 들어 있는 S3 버킷으로 이동합니다.

각 증거 이름 옆에는 해당 항목에 대한 규정 준수 검사 결과가 표시됩니다.

- AWS Security Hub 또는 AWS Config에서 수집된 자동 증거의 경우 규정 준수, 비준수 또는 결정적이지 않은 결과가 보고됩니다.
- AWS CloudTrail 및 API 호출에서 수집한 자동 증거와 모든 수동 증거의 경우 결정적이지 않은 결과가 표시됩니다.

증거 요약 페이지

증거 요약 페이지에 포함되는 정보는 다음과 같습니다.

- ID — 증거의 고유 식별자입니다.
- 수집 날짜 - 증거가 생성되거나 업로드된 날짜입니다.
- 설명 - 계정 ID 및 데이터 소스 유형을 포함한 증거의 설명입니다.
- 평가 이름 — 보고서가 생성된 평가의 이름입니다.
- 프레임워크 이름 — 평가를 만든 프레임워크의 이름입니다.
- 통제 이름 — 증거가 뒷받침하는 통제의 이름입니다.
- 통제 세트 이름 — 관련 통제가 속하는 통제 세트의 이름입니다.
- 통제 설명 — 증거가 뒷받침하는 통제에 대한 설명입니다.
- 검사 정보 — 통제에 권장되는 검사 절차입니다.
- 실행 계획 — 통제가 이행되지 않을 경우 수행할 권장 조치입니다.
- AWS 리전 – 스트림과 연결되는 디바이스의 이름입니다.
- IAM ID — 증거와 관련된 사용자 또는 역할의 ARN입니다.
- AWS 계정— 증거와 관련된 AWS 계정 ID입니다.
- AWS 서비스 – 증거와 연결된 AWS 서비스의 이름입니다.

- 포함된 리소스 — 증거를 생성하기 위해 평가된 AWS 리소스입니다. 이 속성은 AWS Config의 규정 준수 검사 증거의 경우 적용할 수 없습니다. 이 증거 유형의 경우 증거 PDF의 증거 세부 정보 페이지에 표로 정리된 모든 리소스를 찾을 수 있습니다.
- 이벤트 이름 — 증거 이벤트의 이름입니다.
- 이벤트 타임 – 이벤트가 발생한 시점의 시간입니다.
- 데이터 소스 - 증거를 수집 또는 업로드한 출처입니다. 데이터 소스 유형은 AWS Config, Security Hub, AWS API 호출, CloudTrail 또는 수동일 수 있습니다.
- 유형별 증거 — 증거의 범주
  - 규정 준수 확인 증거는 AWS Config 또는 Security Hub에서 수집됩니다.
  - 사용자 활동 증거는 CloudTrail 로그에서 수집됩니다.
  - 구성 데이터 증거는 다른 AWS 서비스의 스냅샷에서 수집됩니다.
  - 수동 증거는 수동으로 업로드한 증거입니다.
- 규정 준수 검사 상태 - 규정 준수 검사 범주에 속하는 증거의 평가 상태입니다.
  - AWS Security Hub 또는 AWS Config, 규정 준수, 비준수 또는 결정적이지 않은 결과에서 수집된 자동 증거의 경우 보고됩니다.
  - AWS CloudTrail 및 API 호출에서 수집한 자동 증거와 모든 수동 증거의 경우 결정적이지 않은 결과가 표시됩니다.

증거 세부 정보 페이지

증거 세부 정보 페이지에는 증거의 이름과 증거 세부 정보 표가 표시됩니다. 이 표는 데이터를 이해하고 정확한지 검증할 수 있도록 증거의 각 요소에 대한 세부 분석을 제공합니다. 증거의 데이터 소스에 따라 증거 세부 정보 페이지의 내용이 달라집니다.

> **Tip**
>
> 각 페이지 상단의 브레드크럼 탐색에는 증거 세부 정보를 탐색할 때 현재 위치가 표시됩니다. 언제든지 증거 요약으로 돌아가려면 증거 요약을 선택하십시오.

평가 보고서 무결성 검사

평가 보고서를 생성하면 Audit Manager는 `digest.txt`라는 보고서 파일 체크섬을 생성합니다. 이 파일을 사용하여 보고서의 무결성을 검증하고 보고서 생성 후 수정된 증거가 없는지 확인할 수 있습니다.

여기에는 보고서 아카이브의 일부가 변경될 경우 무효화되는 서명과 해시가 포함된 JSON 객체가 포함되어 있습니다.

평가 보고서의 무결성을 검증하려면 Audit Manager에서 제공하는 ValidateAssessmentReportIntegrity API를 사용하십시오.

평가 보고서의 문제 해결

일반적인 질문과 문제에 대한 답변을 찾으려면 이 가이드의 문제 해결 섹션에 있는 평가 보고서 문제 해결을 참조하십시오.

증거 찾기

증거 찾기는 Audit Manager에서 증거를 검색하는 강력한 방법을 제공합니다. 원하는 것을 찾기 위해 깊이 숨어있는 증거 폴더를 탐색하는 대신, 이제 증거 찾기를 이용하여 증거를 빠르게 쿼리할 수 있습니다. 증거 찾기를 위임 관리자로 사용하면 조직의 모든 멤버 계정에서 증거를 검색할 수 있습니다.

필터와 그룹화를 조합하여 이용하면 검색 쿼리의 범위를 점진적으로 좁힐 수 있습니다. 예를 들어 시스템 상태를 높은 수준으로 보려면 광범위한 검색을 수행하고 평가, 날짜 범위 및 리소스 규정 준수별로 필터링합니다. 특정 리소스를 개선하는 것이 목표인 경우 특정 컨트롤 또는 리소스 ID에 대한 증거를 찾기 위해 좁은 검색을 수행할 수 있습니다. 필터를 정의한 후에는 일치하는 검색 결과를 그룹화하여 미리 본 다음에 평가 보고서를 생성할 수 있습니다.

증거 찾기를 이용하려면 Audit Manager 설정에서 이 기능을 활성화해야 합니다.

주제

증거 찾기가 CloudTrail Lake와 함께 작동하는 방식 설명

증거 찾기는 AWS CloudTrail Lake 쿼리 및 스토리지 기능을 사용합니다. 증거 찾기를 사용하기 전에 CloudTrail Lake의 작동 방식에 대해 좀 더 이해하면 도움이 됩니다.

CloudTrail Lake는 데이터를 강력한 SQL 쿼리를 지원하는, 검색 가능한 단일 이벤트 데이터 저장소에 집계합니다. 즉, 조직 전체에서, 그리고 사용자 지정 시간 범위 내에서 데이터를 검색할 수 있습니다. 증거 찾기를 이용하면 Audit Manager 콘솔에서 이 검색 기능을 직접 이용할 수 있습니다.

증거 찾기를 활성화하도록 요청하면 Audit Manager가 사용자 대신 이벤트 데이터 저장소를 생성합니다. 증거 찾기가 활성화되면, 향후 모든 Audit Manager 증거가 이벤트 데이터 저장소에 수집되며, 증거 찾기 검색 쿼리에 이것을 사용할 수 있게 됩니다. 증거 찾기를 활성화하면 새로 생성된 이벤트 데이터

저장소를 지난 2년 분량의 증거 데이터로 채웁니다. 증거 찾기를 위임된 관리자로 활성화하면 조직 내 모든 구성원의 계정에 데이터를 채웁니다.

채워 넣은 것이든 새로 생성한 것이든 관계없이 모든 증거 데이터는 이벤트 데이터 저장소에 2년 간 보관됩니다. 기본으로 설정된 보존 기간은 언제든지 변경할 수 있습니다. 이에 대한 지침은 AWS CloudTrail 사용 설명서의 이벤트 데이터 저장소 업데이트를 참조하십시오. 이벤트 데이터는 최대 7년 또는 2,555일 동안 이벤트 데이터 저장소에 보관할 수 있습니다.

> **Note**
>
> 이 기능을 활성화한 경우, 데이터 채우기 프로세스는 2023년 11월까지 완료하면 무료입니다. 그 이후 새로운 증거 데이터가 이벤트 데이터 스토어에 추가되면 데이터 저장 및 수집에 대해 CloudTrail Lake 요금이 부과됩니다.
> CloudTrail Lake 쿼리의 경우, 사용한 만큼만 지불하면 됩니다. 즉, 증거 찾기에서 검색 쿼리를 실행할 때마다 스캔한 데이터에 대한 요금이 부과됩니다.
> CloudTrail Lake 요금에 대한 자세한 내용은 AWS CloudTrail 요금을 참조하세요.

증거 찾기 활성화

증거 찾기는 Audit Manager 설정에서 활성화할 수 있습니다. 이에 대한 지침은 이 안내서의 AWS Audit Manager 설정 페이지에 있는 증거 찾기를 참조하십시오.

증거 찾기 문제 해결

일반적인 질문과 문제에 대한 답을 찾으려면 이 안내서의 문제 해결 장에 있는 증거 찾기 문제 해결을 참조하십시오.

증거 검색

다음 단계에 따라 Audit Manager 콘솔에서 증거를 검색해보세요.

> **Note**
>
> CloudTrail API를 이용하여 증거 데이터를 쿼리할 수도 있습니다. 자세한 내용은 AWS CloudTrail API 참조의 StartQuery를 참조하세요. AWS CLI를 사용하고 싶으면 사용 AWS CloudTrail 설명서의 쿼리 시작을 참조하십시오.

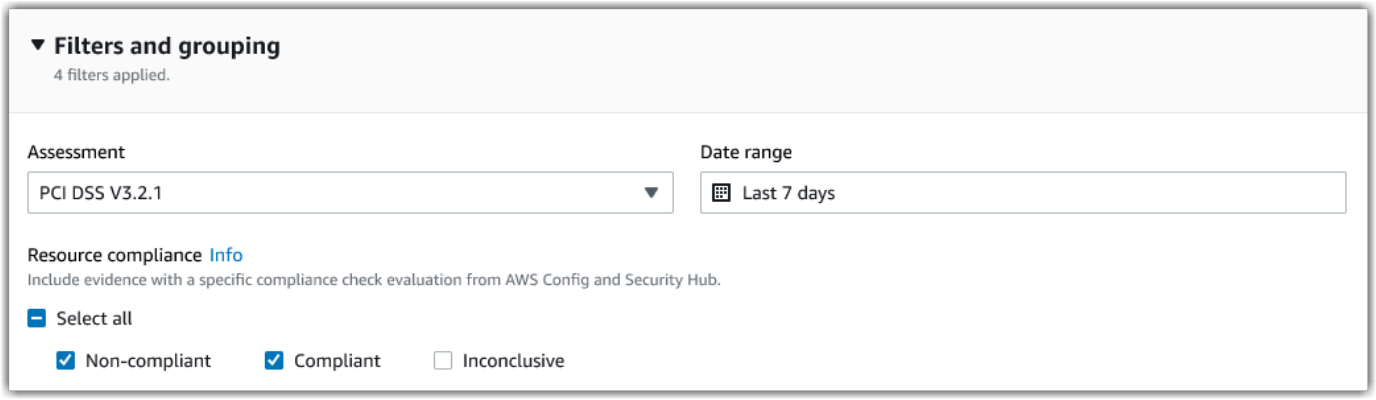
이 페이지의 내용

검색 쿼리 수행

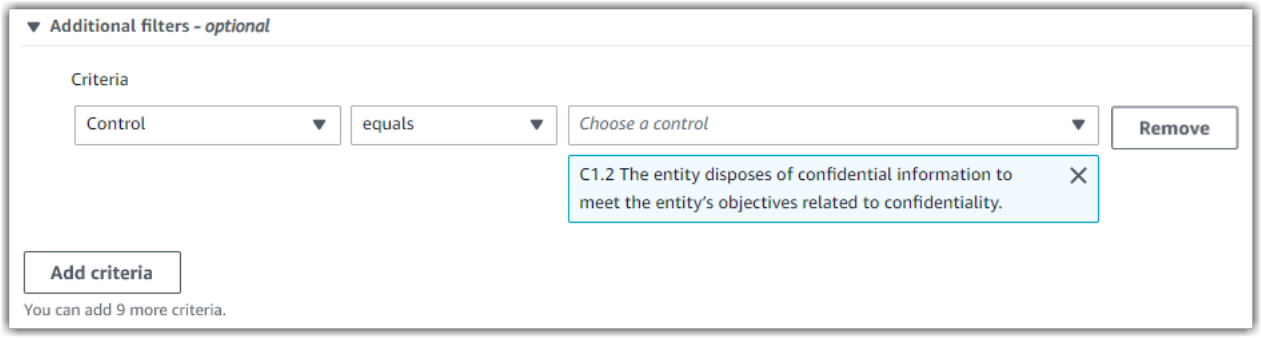
다음 단계에 따라 증거 찾기에서 검색 쿼리를 수행합니다.

증거를 검색하려면

1. https://console.aws.amazon.com/auditmanager/home에서 AWS Audit Manager 콘솔을 엽니다.
2. 탐색 창에서 증거 찾기를 선택합니다.
3. 다음으로, 필터를 적용하여 검색 범위를 좁힙니다.
   a. 평가에서 평가를 선택합니다.
   b. 날짜 범위에서 범위를 선택합니다.
   c. 리소스 규정 준수에서 평가 상태를 선택합니다.



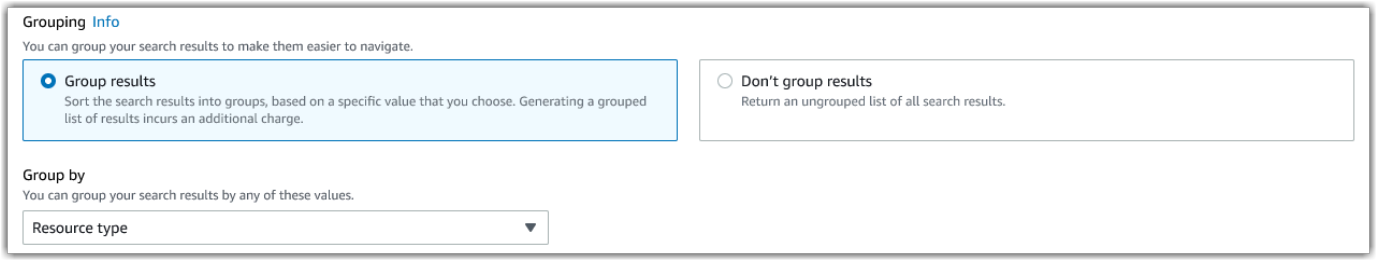
4. (선택 사항) 추가 필터 - 옵션을 선택하면 검색 범위를 더 좁힐 수 있습니다.
   a. 기준 추가를 선택하여 기준을 선택한 다음, 해당 기준에 맞는 값을 하나 이상 선택합니다.
   b. 동일한 방식으로 더 많은 필터를 계속 빌드합니다.
   c. 원하지 않는 필터를 제거하려면 제거를 선택합니다.



5. 그룹화에서 검색 결과를 그룹화할지 여부를 지정합니다.

   a. 결과를 그룹화하려면 결과를 그룹화하는 데 기준으로 사용할 값을 선택합니다.

   b. 결과를 그룹화하지 않으려면 6단계로 건너 뜁니다.



6. 검색을 선택합니다.

보유하고 있는 증거 데이터의 양에 따라 검색에 몇 분 정도 걸릴 수 있습니다. 검색이 진행되는 동안에는 증거 찾기에서 나가셔도 됩니다. 검색 결과가 준비되면 플래시 바가 알려줍니다.

> **Tip**
>
> 이 절차에서 사용할 수 있는 필터 및 그룹화에 대한 자세한 내용은 필터 및 그룹화 옵션을 참조하십시오.

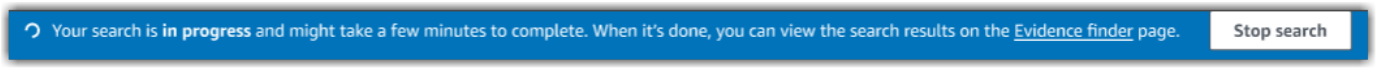
쿼리 검색 중지

어떤 이유로든 쿼리 검색을 중지하려면 다음 단계를 따르세요.

> **Note**
>
> 쿼리 검색을 중지해도 여전히 요금이 부과될 수 있습니다. 쿼리 검색을 중지하기 전에 검색한 증거 데이터의 양에 대해 요금이 청구됩니다. 중지된 후에는 반환된 일부 결과를 볼 수 있습니다.

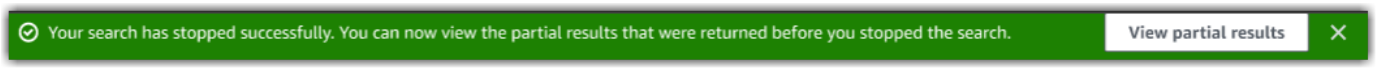
진행 중인 커리 검색 중지

1. 화면 상단의 파란색 진행 플래시바에서 검색 중지를 선택합니다.



2. (선택 사항) 쿼리 검색을 중지하기 전에 반환된 일부 결과를 검토하십시오.

   a. 증거 찾기 페이지에 있는 경우, 화면에 일부 결과가 표시됩니다.
   b. 증거 찾기에서 벗어났다면 녹색 확인 플래시 바에서 부분 결과 보기를 선택하십시오.



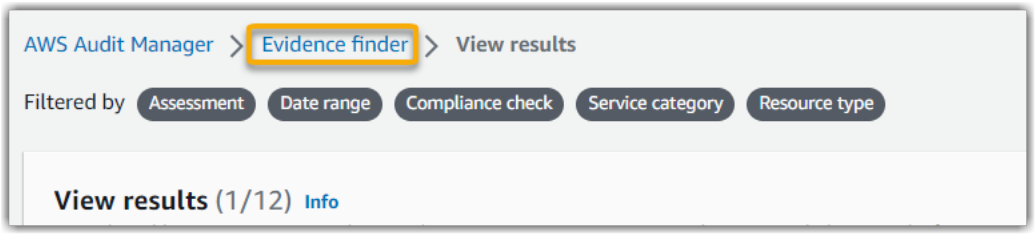
검색 필터 편집

가장 검색 쿼리로 돌아가서 필요에 따라 필터를 변경할 수 있습니다.

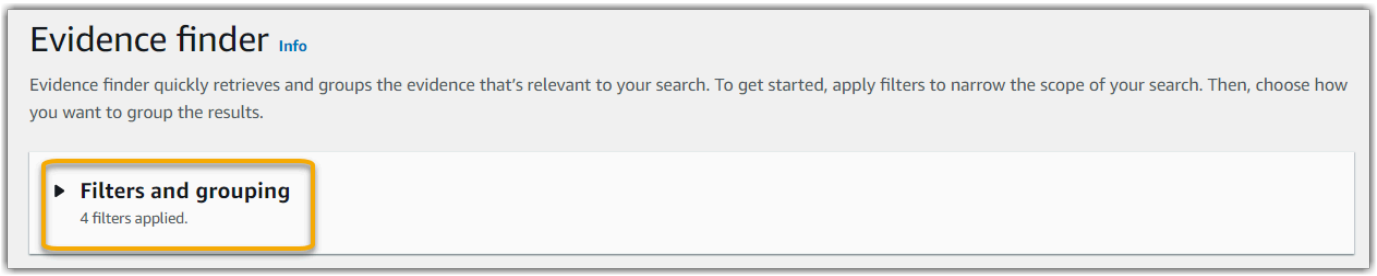
> **Note**
>
> 필터를 편집하고 검색을 선택하면 새 쿼리 검색이 시작됩니다.

최근 검색 쿼리 편집

1. 결과 보기 페이지의 브레드크럼 탐색 메뉴에서 증거 찾기를 선택합니다.



2. 필터 및 그룹화를 선택하여 필터 선택 범위를 확장합니다.



3. 다음으로, 필터를 편집하거나 새 검색을 시작하세요.

   a. 필터를 편집하려면 현재 필터 및 그룹화 선택을 조정하거나 제거합니다.

   b. 다시 시작하려면 필터 지우기를 선택하고 선택한 필터 및 그룹화 선택을 적용합니다.

4. 완료했으면 다음을 선택합니다.

증거 찾기에서 결과 보기

검색이 끝나면 검색 기준과 일치하는 결과를 볼 수 있습니다.

증거 수집 중에 여러 리소스가 평가될 수 있다는 점을 염두에 두세요. 따라서, 증거에는 하나 이상의 관련 리소스가 포함될 수 있습니다. 증거 찾기에서, 결과는 리소스 수준에서 표시되며 각 리소스마다 한 행씩 표시됩니다. 페이지를 떠나지 않고서 각 리소스의 요약을 미리 볼 수 있습니다.

검색 결과를 검토했으면, 해당 증거가 포함된 평가 보고서를 생성할 수 있습니다. 검색 결과를 CSV(쉼표로 구분된 값) 파일로 내보낼 수도 있습니다.

> **Important**
>
> 검색 결과 탐색을 마칠 때까지는 증거 찾기를 열어 두는 것이 좋습니다. 결과 보기 테이블에서 벗어나면 검색 결과가 삭제됩니다. 필요하다면, https://console.aws.amazon.com/cloudtrail/에서 최근 결과를 볼 수 있습니다. 여기서는 쿼리 검색 결과가 7일 동안 보존됩니다. 하지만, CloudTrail 콘솔의 검색 결과로는 평가 보고서를 생성할 수 없다는 점에 유의하세요.

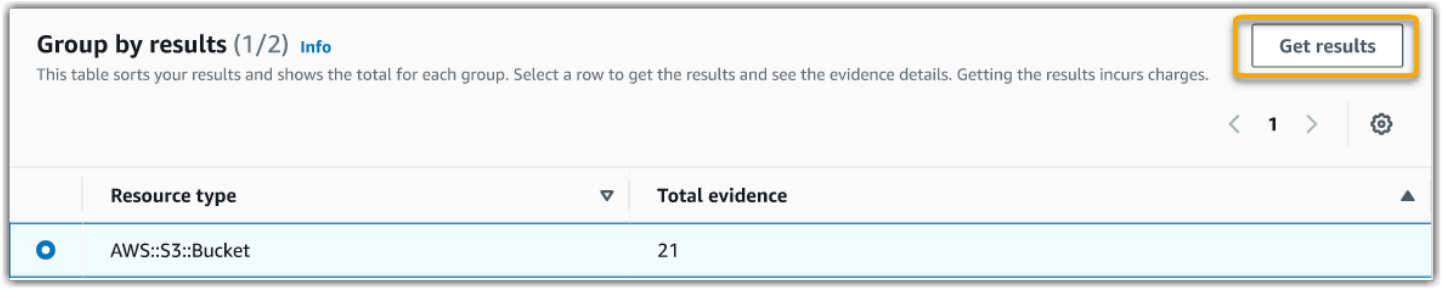
이 페이지의 내용

그룹화된 결과 보기

결과를 그룹화한 경우, 증거를 더 자세히 살펴보기 전에 그룹화를 검토할 수 있습니다.

> **Note**
>
> 결과를 그룹화하지 않았을 때는 증거 찾기에서 결과별 그룹 테이블이 표시되지 않습니다. 대신, 결과 보기 테이블로 바로 이동됩니다.

결과별 그룹 테이블을 이용하여 일치 증거의 범위와 일치 증거가 특정 차원에 어떻게 분포되어 있는지 알아보세요. 결과는 선택한 값을 기준으로 그룹화됩니다. 예를 들면, 리소스 유형별로 그룹화한 경우, 테이블에 AWS 리소스 유형의 목록이 표시됩니다. 전체 증거 열에는 각 리소스 유형에 대한 매칭 결과 수가 표시됩니다.



그룹에 대한 결과를 얻으려면

1. 결과별 그룹화 테이블에서 얻으려는 결과에 해당하는 행을 선택합니다.
2. 결과 가져오기를 선택합니다. 그러면 새 쿼리 검색이 시작되고 해당 그룹에 대한 결과를 볼 수 있는 결과 보기 테이블로 전환됩니다.

검색 결과 보기

결과 보기 테이블에는 검색 결과가 표시됩니다. 여기에서 다음 작업을 수행할 수 있습니다.

- 보기의 기본 설정 관리
- 리소스 요약 미리 보기
- 검색 결과에서 평가 보고서를 생성하세요.
- 검색 결과 내보내기

보기의 기본 설정 관리

보기의 기본 설정에 따라 결과 페이지에 표시되는 내용이 달라집니다.

보기의 기본 설정을 관리하려면

1. 결과 보기 테이블 상단의 설정 아이콘(#)을 선택합니다.
2. 다음 설정을 검토하고 필요에 따라 변경합니다.
   a. 보이는 테이블 열 선택 - 토글 옵션을 이용하여 표시할 열을 변경할 수 있습니다.
   b. 페이지 크기 - 라디오 버튼을 선택하여 각 페이지에 표시할 결과 수를 지정합니다.
   c. 텍스트 줄 바꿈 - 가독성을 높이기 위해 긴 줄의 텍스트를 줄 바꿈하려면 확인란을 선택합니다.
3. 확인을 선택하여 기본 설정을 저장합니다.

리소스 요약 미리 보기

관련 리소스에서 검색 쿼리와 일치하는 증거를 미리 볼 수 있습니다. 이를 통해 쿼리 검색으로 의도한 결과를 얻었는지 또는 필터를 조정하고 쿼리 검색을 다시 실행해야 하는지 확인할 수 있습니다.

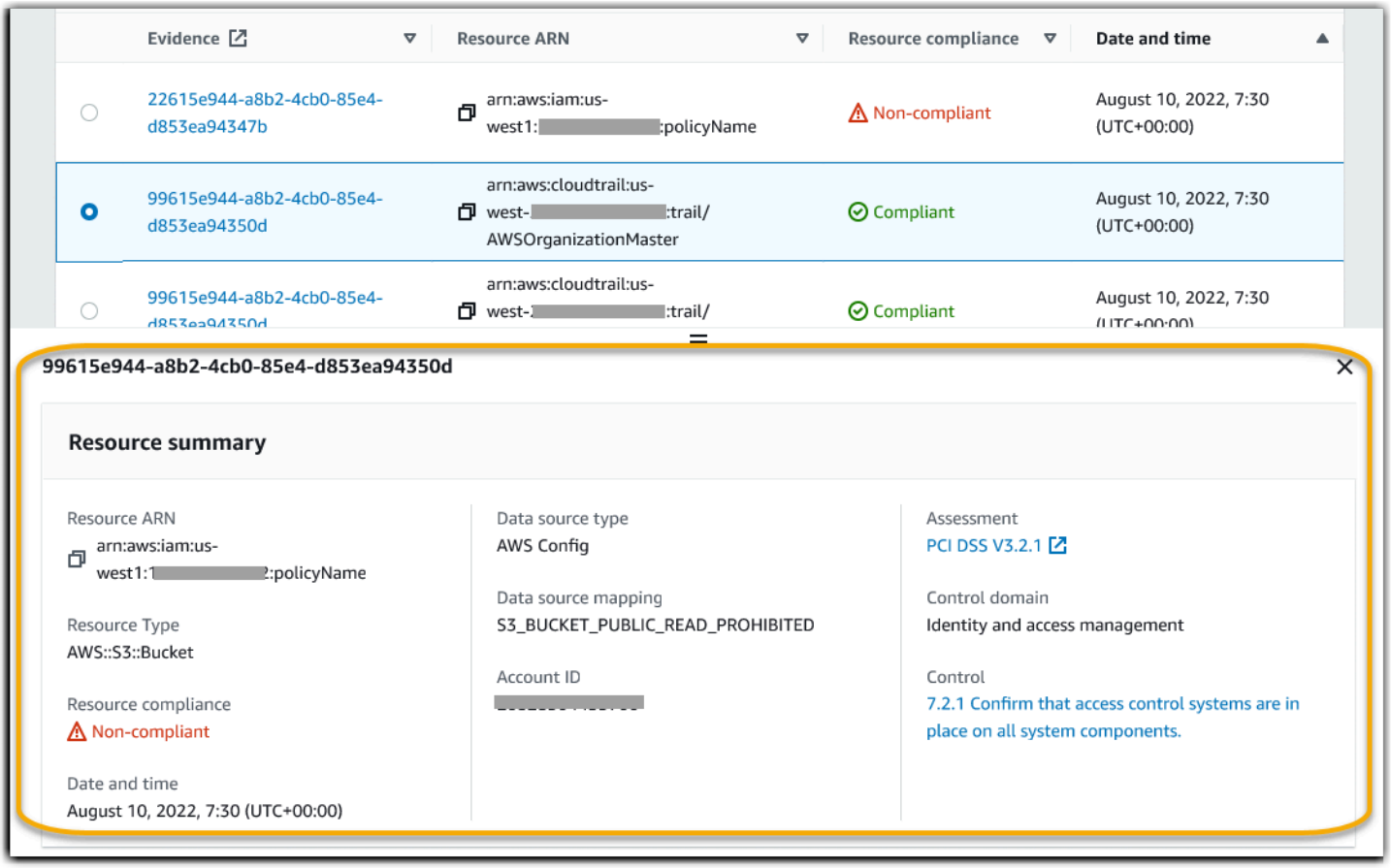
증거에는 하나 이상의 관련 리소스가 있을 수 있다는 점을 염두에 두세요. 증거 찾기의 결과는 리소스 수준에서 표시되며 각 리소스마다 한 행씩 표시됩니다.

> **Note**
>
> 증거 찾기는 자동 및 수동 증거의 결과를 보여줍니다. 하지만 자동 증거에 대한 리소스 요약만 미리 볼 수 있습니다. 이는 Audit Manager가 수동 증거에 대한 리소스 평가를 수행하지 않아 리소스 요약을 이용할 수 없기 때문입니다.

수동 증거에 대한 세부 정보를 보려면 증거 이름을 선택하여 증거 세부 정보 페이지를 열면 됩니다. 증거 찾기 결과에서 평가 보고서를 생성하는 경우, 수동 증거 세부 정보가 평가 보고서에 포함됩니다.

리소스 요약 미리 보기

1. 결과 옆의 라디오 버튼을 선택합니다. 그러면 현재 페이지에 리소스 요약 패널이 열립니다.
2. (선택 사항) 관련 증거의 세부 정보 전체를 확인하려면 증거 이름을 선택합니다.
3. (선택 사항) 수평선(=) 을 이용하여 리소스 요약 창을 끌어서 크기를 조정합니다.
4. (x)를 선택하여 리소스 요약 창을 닫습니다.



검색 결과에서 평가 보고서를 생성하세요.

검색 결과에 만족하면 평가 보고서를 생성합니다.

검색 결과에서 평가 보고서를 생성하려면

1. 결과 보기 테이블 상단에서 평가 보고서 생성을 선택합니다.
2. 평가 보고서의 이름과 설명을 입력하고 평가 보고서 세부 정보를 검토합니다.
3. 평가 보고서 생성을 선택합니다.

평가 보고서가 생성되는 데에는 몇 분 정도 걸립니다. 이 작업 중에 증거 찾기에서 나가셔도도 됩니다. 보고서가 준비되면 녹색 성공 알림이 표시됩니다. 그러면 Audit Manager 다운로드 센터로 이동하여 평가 보고서를 다운로드할 수 있습니다.

> **Note**
>
> Audit Manager는 검색 결과의 증거만을 이용하여 일회성 보고서를 생성합니다. 이 보고서에 평가 페이지에서 보고서에 수동으로 추가한 증거는 포함되지 않습니다.
> 평가 보고서에 포함할 수 있는 증거의 양에는 제한이 적용됩니다. 자세한 내용은 증거 찾기 문제 해결을 참조하세요.

검색 결과 내보내기

증거 찾기 검색 결과의 휴대용 버전이 필요할 수 있습니다. 이 경우에는 검색 결과를 CSV 파일로 내보낼 수 있습니다.

검색 결과를 내보내고 나면 Audit Manager 다운로드 센터에서 7일 동안 CSV 파일을 이용할 수 있습니다. CSV 파일의 사본은 내보내기 대상이라고 하는, 선택한 S3 버킷으로도 전송됩니다. CSV 파일은 파일을 삭제할 때까지 이 버킷에서 계속 이용할 수 있습니다.

Audit Manager는 CloudTrail Lake 기능을 이용하여 증거 찾기에서 CSV 파일을 내보내고 전달합니다. CSV 내보내기 프로세스의 작동 방식을 정의하는 요소는 다음과 같습니다.

- 모든 검색 결과가 CSV 파일에 포함됩니다. 특정 검색 결과만 포함하려면 검색 필터를 편집하는 것이 좋습니다. 이렇게 하면, 내보내려는 증거만을 대상으로 검색 결과를 좁힐 수 있습니다.
- CSV 파일은 압축된 GZIP 형식으로 내보냅니다. 기본 CSV 파일 이름은 `queryID/result.csv.gz`이며, 여기서 `queryID`는 검색 쿼리의 ID입니다.
- CSV 내보낼 수 있는 최대 크기는 1TB입니다. 1TB가 넘는 데이터를 내보내는 경우, 결과는 두 개 이상의 파일로 분할됩니다. 각 CSV 파일의 이름은 `result_`*`number`*`.csv.gz`로 지정됩니다. 가져오는 CSV 파일 수는 검색 결과의 전체 크기에 따라 달라집니다. 예를 들어, 2TB의 데이터를 내보내는 경우 두 개의 쿼리 결과 파일(`result_1.csv.gz`및`result_2.csv.gz`)이 제공됩니다.

- S3 버킷에는 CSV 파일 외에도 JSON 서명 파일이 전송됩니다. 이 파일은 CSV 파일 내의 정보가 정확한지 확인하는 체크섬 역할을 합니다. 자세한 내용은 AWS CloudTrail 개발자 안내서의 CloudTrail 서명 파일 구조를 참조하십시오. 쿼리 결과를 전달한 후, 쿼리 결과가 수정, 삭제 또는 변경되지 않았는지 여부를 확인하는 데에는 CloudTrail 쿼리 결과 무결성 검증을 이용할 수 있습니다. 이에 대한 지침은 AWS CloudTrail 개발자 안내서의 저장된 쿼리 결과 검증을 참조하십시오.

> **Note**
>
> 수동 증거 텍스트 응답은 현재 증거 찾기 미리 보기 또는 CSV 내보내기에 포함되지 않습니다. 텍스트 응답 데이터를 보려면 증거 찾기 결과에서 수동 증거의 이름을 선택하여 증거 세부 정보 페이지를 열면 됩니다. Audit Manager 콘솔 외부에서 텍스트 응답 데이터를 확인해야 하는 경우, 증거 찾기 결과를 바탕으로 평가 보고서를 생성하는 것이 좋습니다. 텍스트 응답을 포함한 모든 수동 증거 세부 정보가 평가 보고서에 포함됩니다.

최초 결과 내보내기

다음 단계에 따라 최초 검색 결과를 내보낼 수 있습니다. 이 절차에 의하면 향후 모든 내보내기에 대한 내보내기 대상를 기본 설정으로 지정할 수 있습니다. 기본 설정에 의한 내보내기 대상을 지금 저장하지 않으려면, 나중에 내보내기 대상 설정을 업데이트하여 저장할 수 있습니다.

> **Important**
>
> 시작하기 전에 내보내기 대상으로 사용할 수 있는 S3 버킷이 있는지 확인하세요. 기존 S3 버킷 중 하나를 사용하거나 Amazon S3에서 새 버킷을 생성할 수 있습니다. 이 때, S3 버킷에는 CloudTrail이 내보내기 파일을 쓸 수 있도록 허용하는 데 필요한 권한 정책이 있어야 합니다. 구체적으로 말하자면, 버킷 정책에는 `s3:PutObject` 작업과 버킷 ARN이 포함되어야 하고 CloudTrail이 서비스 보안 주체로 나열되어 있어야 합니다. 이 때 사용할 수 있는 권한 정책 예시를 제공해드립니다. 이 정책을 S3 버킷에 연결하는 방법에 대한 지침은 Amazon S3 콘솔을 이용한 버킷 정책 추가를 참조하십시오.
>
> 자세한 정보는 내보내기 대상 구성을 위한 팁을 참조하십시오. CSV 파일을 내보낼 때 문제가 발생하는 경우, 증거 찾기 CSV 내보내기 문제 해결을 참조하십시오.

검색 결과를 내보내려면(최초 실행 시)

1. 결과 보기 테이블 상단에서 CSV 내보내기를 선택합니다.

2. 파일을 내보낼 S3 버킷을 지정합니다.

   - Browse S3를 선택하여 버킷 목록에서 선택합니다.
   - 또는 **s3://bucketname/prefix** 형식으로 버킷 URI를 입력할 수 있습니다.

   > **Tip**
   >
   > 대상 버킷을 체계적으로 정리하려면 CSV 내보내기를 위한 선택적 폴더를 만들 수 있습니다. 그렇게 하려면, 리소스 URI 상자의 값에 슬래시(**/**)와 접두사를 추가합니다(예: **/evidenceFinderExports**). 그러면 Audit Manager가 CSV 파일을 버킷에 추가할 때 이 접두사를 포함시키고, Amazon S3는 접두사로 지정된 경로를 생성합니다. Amazon S3의 접두사에 대한 자세한 내용은 Amazon Simple Storage Service 사용 설명에 있는 Amazon S3 콘솔에서의 객체 구성을 참조하십시오.

3. (선택 사항) 이 버킷을 기본 내보내기 대상으로 저장하지 않으려면 증거 찾기 설정에서 이 버킷을 기본 내보내기 대상로 저장이라는 확인란의 선택을 취소하면 됩니다.
4. 내보내기를 선택합니다.

내보내기 대상을 저장한 후 결과 내보내기

기본 S3 버킷을 기본 내보내기 대상으로 저장한 후, 다음 단계를 진행하면 됩니다.

검색 결과를 내보내려면(기본 내보내기 대상을 저장한 후)

1. 결과 보기 테이블 상단에서 CSV 내보내기를 선택합니다.
2. 표시되는 프롬프트에서 내보낸 파일이 저장될 기본 S3 버킷을 검토합니다.

   a. (선택 사항) 이 버킷을 계속 사용하고 앞으로는 이 메시지를 숨기려면 다시 알림 사용 안 함 확인란을 선택합니다.

   b. (선택 사항) 이 버킷을 변경하려면 절차에 따라 내보내기 대상 설정 업데이트를 수행합니다.
3. 확인을 선택합니다.

내보내는 데이터의 양에 따라, 내보내기 프로세스를 완료하는 데 몇 분 정도 걸릴 수 있습니다. 내보내기가 진행되는 동안에는 증거 찾기에서 나가셔도 됩니다. 증거 찾기에서 벗어나면 검색이 중단되고 콘솔에서 검색 결과가 삭제됩니다. 하지만, CSV 내보내기 프로세스는 백그라운드에서 계속됩니다. CSV 파일에는 쿼리와 일치하는 전체 검색 결과 세트가 포함됩니다.

내보낸 결과 보기

CSV 파일을 찾아 그 상태를 확인하려면 Audit Manager 다운로드 센터로 이동하세요. 내보낸 파일이 준비되면 다운로드 센터에서 CSV 파일을 다운로드할 수 있습니다.

내보내기 대상 S3 버킷에서 CSV 파일을 찾아 다운로드할 수도 있습니다.

Amazon S3 콘솔에서 CSV 파일 및 서명 파일 찾기

1. Amazon S3 콘솔을 엽니다.
2. CSV 파일을 내보낼 때 지정한 내보내기 대상 버킷을 선택합니다.
3. CSV 파일과 서명 파일을 찾을 때까지 객체 계층을 탐색합니다. CSV 파일의 확장자는 `.csv.gz`이고 서명 파일의 확장자는 `.json`입니다.

다음 예제와 유사하지만, 내보내기 대상 버킷 이름, 계정 ID, 날짜, 쿼리 ID가 다른 객체 계층을 통해 탐색하게 됩니다.

```
All Buckets
    Export_Destination_Bucket_Name
        AWSLogs
            Account_ID;
                CloudTrail-Lake
                    Query
                        YYYY
                            MM
                              DD
                                Query_ID
```

필터 및 그룹화 옵션

이 페이지에서는 증거 찾기에서 이용할 수 있는 필터 및 그룹화 옵션에 대해 설명합니다.

이 페이지의 내용

참조 필터링

다음 필터를 이용하여 평가, 통제 또는 AWS 서비스과 같은 특정 기준과 일치하는 증거를 찾을 수 있습니다.

주제

필수 필터

이 필터를 이용하여 평가 시의 증거에 대한 간략한 개요를 살펴볼 수 있습니다.

필터 이름	설명	주
평가	특정 평가에 대한 증거를 보여줍니다.	평가 하나로만 필터링할 수 있습니다.
날짜 범위	특정 기간에 대한 증거를 보여줍니다.	상대 범위를 이용하여 오늘 날짜를 기준으로 범위를 정하거나(예: **`Last 30 days`**), 또는 절대 범위를 이용하여 특정 날짜 범위 를 지정할 수 있습니다(예: **`June 27th - July 4th`**).
리소스 규정 준수	특정 규정 준수 검사 평가 결과를 가진 리소스를 보여줍니다.	Audit Manager는 데이터 소스 유형으로 AWS Config와 Security Hub를 사용하는 제어의 규정 준수 검사 증거를 수집합니다. 증거 수집 중에는 여러 리소스를 평가할 수 있습니다. 따라서 단일 규정 준수 검사 증거에는 하나 이상의 리소스가 포함될 수 있습니다. 이 필터를 이용하여 리소스 수준에서 규정 준수 상태를 탐색할 수 있습니다. 다음 중 하나 이상의 옵션을 선택할 수 있습니다. • 규정 미준수 - 이 필터는 규정 준수 검사 문제가 있는 리소스를 찾습니다. 이는 Security Hub가 실패

필터 이름	설명	주
		결과를 보고하거나 AWS Config에서 규정 미준수 결과를 보고하는 경우에 발생합니다. • 규정 준수 - 이 필터는 규정 준수 검사 문제가 없는 리소스를 찾습니다. 이는 Security Hub가 통과 결과를 보고하거나 AWS Config에서 규정 준수 결과를 보고하는 경우에 발생합니다. • 미결정 - 이 필터는 규정 준수 검사를 이용할 수 없거나 해당되지 않는 리소스를 찾습니다. 이는 리소스에서 AWS Config 또는 Security Hub를 기본 데이터 소스 유형으로 사용하지만 해당 서비스가 활성화되지 않은 경우에 발생합니다. 이는 또한 리소스가 규정 준수 검사를 지원하지 않는 기본 데이터 소스 유형(예: 수동 증거, AWS API 직접 호출, 또는 CloudTrail)을 사용하는 경우에도 발생합니다.

추가 필터(선택 사항)

이 필터를 이용하여 검색 쿼리의 범위를 좁힐 수 있습니다. 예를 들어, 서비스를 이용하면 Amazon S3와 관련된 모든 증거를 볼 수 있습니다. 리소스 유형을 이용하면 S3 버킷에만 초점을 맞출 수있습니다. 또는 리소스 ARN을 이용하여 특정 S3 버킷을 대상으로 정할 수 있습니다.

다음 기준 중 하나 이상을 이용하여 추가 필터를 생성할 수 있습니다.

기준 이름	설명	이 기준을 사용하는 경우
계정 ID	AWS 계정을 이용한 세부 검색	이 기준을 이용하면 특정 AWS 계정과 관련된 증거를 찾을 수 있습니다.
제어	제어의 이름을 이용한 세부 검색	이 기준을 이용하면 특정 제어와 관련된 증거를 찾을 수 있습니다.

기준 이름	설명	이 기준을 사용하는 경우
제어 도메인	제어 도메인을 이용한 세부 검색	이 기준을 이용하면 감사를 준비하면서 특정 주제 영역에 집중하게 됩니다. 표준 프레임워크에서 생성된 평가 결과를 쿼리하는 경우 제어 도메인별로 필터링할 수 있습니다. 제어 도메인의 예에는 자격 증명 및 액세스 관리, 로깅 및 모니터링, 네트워크 관리 등이 있습니다.
데이터 소스의 유형	데이터 소스의 유형을 기준을 이용한 세부 검색	이 기준을 이용하면 특정 데이터 소스에 초점을 맞출 수 있습니다. 수동으로 업로드한 증거를 찾으려면 값을 `Manual`로 설정합니다. 그렇지 않으면, 출처(예:, `AWS Config` `CloudTrail` , `Security Hub`, 또는`AWS API calls`)를 기준으로 자동 증거를 필터링할 수 있습니다.
이벤트 이름	이벤트 이름을 기준을 이용한 세부 검색	이 기준을 이용하면 증거와 관련된 특정 사건에 초점을 맞출 수있습니다. 이벤트는 AWS 계정 계정에서의 활동 기록을 말합니다. 예를 들면, 권한을 구성하는 데 사용되는 IAM `AttachRolePolicy` 작업과 같은 API 직접 호출의 이름을 검색할 수 있습니다. 또는, 사용자가 계정에 로그인할 때 CloudTrail에서 기록하는 `ConsoleLogin` 이벤트와 같은 CloudTrail 키워드를 검색할 수도 있습니다.
리소스 ARN	Amazon 리소스 이름(ARN)을 이용한 세부 검색	이 기준을 이용하면 특정 AWS 리소스와 관련된 증거를 찾을 수 있습니다.
리소스 유형	리소스 유형을 이용한 세부 검색	이 기준을 이용하여 Amazon EC2 인스턴스 또는 S3 버킷과 같이 평가 중인 리소스 유형에 초점을 맞출 수 있습니다.
서비스	AWS 서비스 이름을 이용한 세부 검색	이 기준을 이용하여 Amazon EC2, Amazon S3, 또는 AWS Config와 같이 특정 AWS 서비스와 관련된 증거를 찾을 수 있습니다.

기준 이름	설명	이 기준을 사용하는 경우
서비스 범주	AWS 서비스 범주를 이용한 세부 검색	이 기준을 이용하면 AWS 서비스의 특정 범주에 초점을 맞출 수 있습니다. 그 예로는 보안, ID, 규정 준수, 데이터베이스, 및 스토리지를 들 수 있습니다.

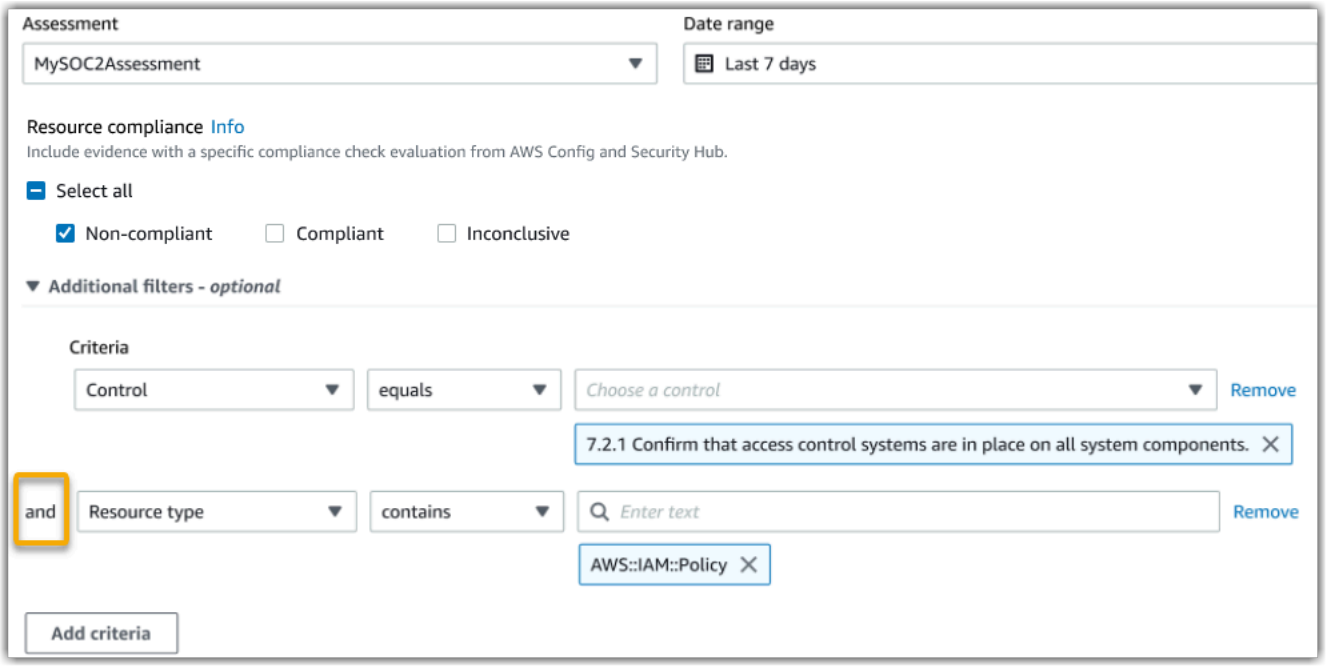
필터 결합

기준의 특성

둘 이상의 기준을 지정하면 Audit Manager는 선택한 이들 기준에 AND 연산자를 적용합니다. 즉, 모든 기준이 단일 쿼리로 그룹화되며, 그 결과는 결합된 모든 기준과 일치해야 합니다.

예

다음 필터 설정에서, 증거 찾기는 **`MySOC2Assessment`**라고 하는 평가에 대해 지난 7일간의 규정 미준수 리소스를 보여줍니다. 또한, 그 결과는 IAM 정책 및 지정된 제어 모두와 관련이 있습니다.

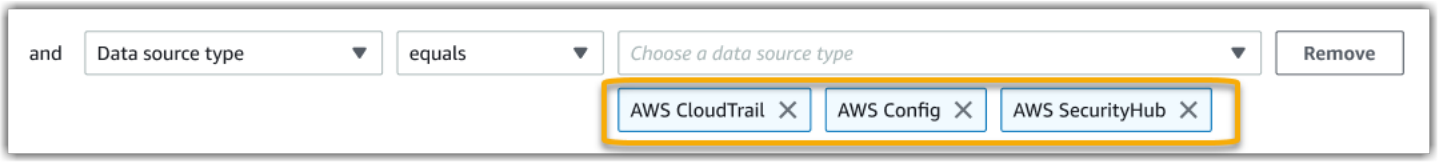


기준 값의 특성

기준 값을 두 개 이상 지정하면 값이 이 값들은 OR 연산자로 연결됩니다. 증거 찾기는 이러한 기준 값 중 하나와 일치하는 결과를 보여줍니다.

예

다음 필터 설정에서, 증거 찾기는 AWS CloudTrail, AWS Config, 또는 AWS Security Hub중 하나에서 나온 검색 결과를 보여줍니다.



그룹화 참조

검색 결과를 그룹화하여 더 빠르게 탐색할 수 있습니다. 그룹화하면 검색 결과의 범위와 검색 결과가 특정 차원에 어떻게 분포되어 있는지 확인할 수 있습니다.

다음 그룹화 기준 값 중 하나를 사용할 수 있습니다.

그룹화 기준	설명
계정 ID	AWS 계정 기준으로 결과를 그룹화합니다.
제어	제어 이름을 기준으로 결과를 그룹화합니다.
제어 도메인	제어 도메인 기준으로 결과를 그룹화합니다.
데이터 소스의 유형	증거의 출처가 되는 데이터 소스 유형을 기준으로 결과를 그룹화합니다.
이벤트 이름	이벤트 이름을 기준으로 결과를 그룹화합니다.
리소스 ARN	Amazon 리소스 이름(ARN)을 기준으로 결과를 그룹화합니다.
리소스 유형	리소스 유형을 기준으로 결과를 그룹화합니다.
서비스	AWS 서비스 이름별로 결과를 그룹화합니다.
서비스 범주	결과를 AWS 서비스 범주별로 그룹화합니다.

사용 사례 예시

증거 찾기는 여러 사용 사례에서 도움이 될 수 있습니다. 이 페이지에서는 몇 가지 예를 제공하고 각 시나리오에서 사용할 수 있는 검색 필터를 제안합니다.

주제

사용 사례 1: 규정 미준수는 증거을 찾아 위임단을 구성

이 사용 사례는 감사 준비를 감독하는 규정 준수 책임자, 데이터 보호 책임자, 또는 GRC 전문가에게 적합합니다.

조직의 규정 준수 상태를 모니터링할 때는 파트너 팀의 도움을 받아 문제를 해결해야 할 수도 있습니다. 증거 찾기를 이용하면 파트너 팀을 위해 업무를 체계적으로 정리할 수 있습니다.

필터를 적용하면 한 번에 한 영역에 대한 증거에 초점을 맞출 수있습니다. 또한, 함께 일하는 각 파트너 팀의 책임 및 범위에 지속적으로 일치 상태를 유지할 수 있습니다. 이러한 방식으로 대상을 정하여 검색을 수행하면 검색 결과를 이용하여 각 주제 영역에서 수정해야 할 사항을 정확히 식별할 수 있습니다. 그런 다음, 규정 미준수 증거를 해당 파트너 팀에 위임하여 수정하게 할 수 있습니다.

이 워크플로의 경우, 증거 검색 단계를 따르세요. 다음 필터를 이용하여 규정 미준수 증거를 찾습니다.

```
Assessment | <assessment name>
Date range | <date range>
Resource compliance | Non-compliant
```

그런 다음, 초점을 맞추고 있는 영역에 추가 필터를 적용합니다. 예를 들면, 서비스 범주 필터를 이용하여 IAM과 관련된 규정 미준수 리소스를 찾을 수 있습니다. 그런 다음, 해당 결과를 조직의 IAM 리소스를 소유한 팀과 공유하세요. 또는, 표준 프레임워크에서 생성된 평가를 쿼리하는 경우라면 제어 도메인 필터를 이용하여 ID 및 액세스 관리 도메인과 관련된 규정 미준수 증거를 찾을 수 있습니다.

```
Control domain | <domain that you're focusing on>
or
Service category | <AWS ### category that you're focusing on>
```

필요한 증거를 찾은 후, 단계에 따라 검색 결과에서 평가 보고서를 생성하세요. 이 보고서를 파트너 팀과 공유할 수 있으며, 파트너 팀은 이를 수정 체크리스트로 사용할 수 있습니다.

사용 사례 2: 규정 준수 증거 식별

이 사용 사례는 SecOps, IT/DevOps, 또는 클라우드 자산을 소유하고 관리하는 다른 역할에서 일하는 경우에 적합합니다.

감사의 일환으로, 소유한 리소스와 관련된 문제를 해결하라는 요청을 받을 수 있습니다. 이 작업을 수행한 후에는, 증거 찾기를 이용하여 리소스가 규정을 준수하는지 검증할 수 있습니다.

이 워크플로의 경우, 증거 검색 단계를 따르세요. 다음 필터를 이용하여 규정 준수 증거를 찾으십시오.

```
Assessment | <assessment name>
Date range | <date range>
Resource compliance | Compliant
```

다음으로, 추가 필터를 적용하여 사용자의 책임에 해당하는 증거만 나타나게 하세요. 소유권의 범위에 따라, 필요에 따른 대상을 지정하여 검색하십시오. 다음 필터 예는 가장 광범위한 것부터 가장 정확한 것의 순서로 나열되어 있습니다. 적합한 옵션을 선택하고, *<placeholder text>*를 자신의 값으로 바꾸십시오.

```
Control domain | <a subject area that you're responsible for>
Service category | <a category of AWS ### that you own>
Service | <a specific AWS ### that you own>
Resource type | <a collection of resources that you own>
Resource ARN | <a specific resource that you own>
```

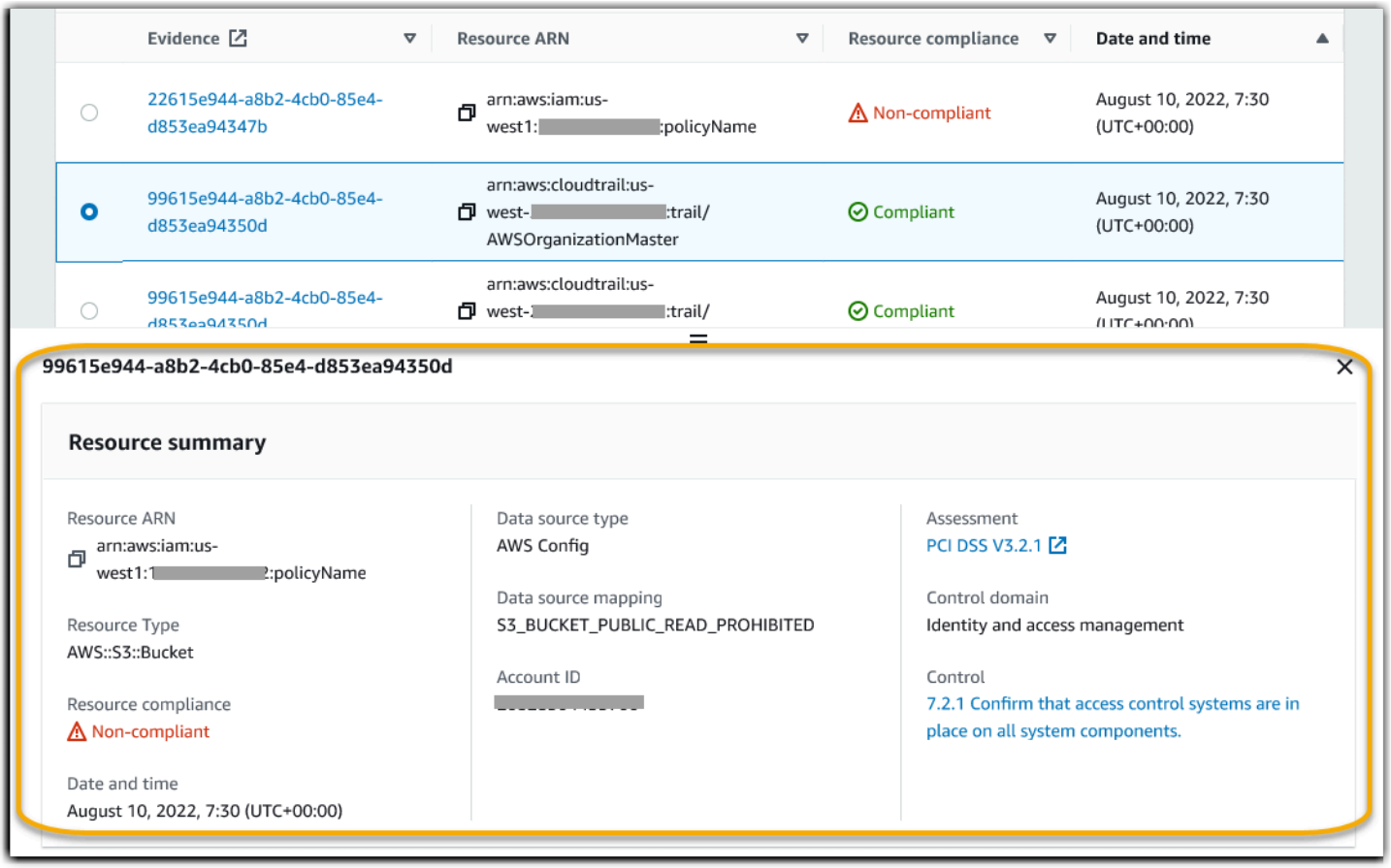
동일한 기준의 여러 인스턴스를 관리하는 경우(예: 여러 AWS 서비스를 담당하고 있는 경우), 해당 값을 기준으로 결과를 그룹화할 수 있습니다. 이렇게 하면 각 AWS 서비스에 대한 일치하는 전체 증거를 확인할 수 있습니다. 그러면 담당하고 있는 서비스에 대한 결과를 얻을 수 있습니다.

사용 사례 3: 증거 리소스의 빠른 미리 보기

이 사용 사례는 모든 Audit Manager 고객에게 적합합니다.

이전에는 개별 증거의 세부 정보를 검토하는 데 시간이 많이 걸렸습니다. 증거를 미리 보려면 해당 평가로 바로 이동한 다음, 깊이 숨어 있는 증거 폴더를 탐색해야 했습니다. 이제 증거 찾기는 이 정보를 미리 볼 수 있는 편리한 방법을 제공합니다. 검색 쿼리와 일치하는 각 증거 항목에 대해 해당 증거에 대한 개별 리소스를 미리 볼 수 있습니다.

시작하려면 증거 검색 단계를 따르세요. 그런 다음, 결과 옆의 라디오 버튼을 선택하여 현재 페이지의 리소스 요약을 확인합니다. 증거 항목과 관련된 개별 리소스를 미리 볼 수 있습니다. 모든 리소스에 대한 증거 세부 정보 전체를 보려면 증거 이름을 선택하세요. 자세한 내용은 리소스 요약 미리보기를 참조하세요.



Audit Manager 다운로드 센터

다운로드 센터에서는 다운로드 가능한 모든 Audit Manager 파일을 찾고 관리할 수 있습니다. 평가 보고서를 생성하거나 증거 찾기에서 검색 결과를 내보내는 경우 파일이 다운로드 센터에 나타납니다.

주제

다운로드 센터 둘러보기

다운로드 센터를 방문하려면 https://console.aws.amazon.com/auditmanager/home 에서 Audit Manager 콘솔을 연 다음 왼쪽 탐색 창에서 다운로드 센터를 선택합니다.

다음 탭 사이를 전환하여 범주별로 파일을 찾아볼 수 있습니다.

평가 보고서 탭

이 탭에는 생성한 모든 평가 보고서가 표시됩니다. 평가 보고서는 삭제하기 전까지 다운로드 센터에서 계속 사용할 수 있습니다.

평가 보고서의 최신 상태를 보려면 새로 고침 아이콘(#) 을 선택하여 표를 다시 로드하세요. 평가 보고서 표의 각 행에는 보고서 이름, 작성 날짜, 다음 상태 중 하나가 표시됩니다.

- 진행 중 — Audit Manager가 평가 보고서를 작성하고 있습니다.
- 준비 완료 — 평가 보고서를 다운로드할 수 있습니다.
- 오류 — 평가 보고서를 생성하지 못했습니다. 이 경우 Audit Manager는 오류를 설명하는 메시지를 표시합니다. 이러한 오류를 해결하는 방법에 대한 자세한 내용은 평가 보고서 문제 해결을 참조하세요.

내보내기 탭

이 탭에는 지난 7일 동안 내보낸 증거 찾기 검색 결과가 모두 표시됩니다. CSV 파일은 7일 후에 다운로드 센터에서 제거되지만 내보내기 대상 S3 버킷에서는 계속 사용할 수 있습니다. S3 대상 버킷에서 증거 찾기 CSV 내보내기를 찾는 방법에 대한 지침은 내보낸 결과 보기 섹션을 참조하세요.

CSV 내보내기의 최신 상태를 보려면 새로 고침 아이콘 (#)을 선택하여 테이블을 다시 로드하세요. 내보내기 테이블의 각 행에는 파일 이름, 내보내기 날짜 및 다음 상태 중 하나가 표시됩니다.

- 진행 중 — Audit Manager가 CSV 파일을 준비 중입니다.
- 준비 완료 — 내보내기에 성공했으며 파일을 다운로드할 수 있습니다.
- 오류 — 내보내기에 실패했습니다. 이 경우 Audit Manager는 오류를 설명하는 메시지를 표시합니다. 이러한 오류를 해결하는 방법에 대한 자세한 내용은 증거 찾기 CSV 내보내기 문제 해결을 참조하세요.

> **Note**
>
> 내보내기 탭에는 AWS CloudTrail Lake에서 직접 실행한 쿼리에 대한 CSV 파일도 표시될 수 있다는 점에 유의하세요. 여기에는 CloudTrail 콘솔에서 또는 CloudTrail API를 사용하여 수행한 쿼리가 포함됩니다. Audit Manager 이벤트 데이터 스토어를 쿼리하고 결과를 Amazon S3에 저장하도록 선택한 경우 CloudTrail 내보내기가 이 탭에 나타납니다.

파일 다운로드

다음 단계에 따라 다운로드 센터에서 파일을 다운로드합니다.

파일을 다운로드하려면

1. https://console.aws.amazon.com/auditmanager/home에서 AWS Audit Manager 콘솔을 엽니다.
2. 왼쪽 탐색 창에서 다운로드 센터를 선택합니다.
3. 평가 보고서 탭 또는 내보내기 탭을 선택합니다.
4. 액세스할 파일을 선택한 다음 다운로드를 선택합니다.

S3 대상 버킷에서 파일을 다운로드하는 방법에 대한 지침은 Amazon Simple Storage Service(S3)사용 설명서의 다운로드하기를 참조하세요.

파일 삭제

다운로드 센터에서 더 이상 필요하지 않은 평가 보고서를 삭제하려면 다음 단계를 따르세요.

> **Note**
>
> 다운로드 센터에서 CSV 내보내기 삭제는 현재 지원되지 않습니다. CSV 내보내기는 7일 후에 다운로드 센터에서 자동으로 제거됩니다.

평가 대상을 삭제하려면

1. https://console.aws.amazon.com/auditmanager/home에서 AWS Audit Manager 콘솔을 엽니다.
2. 왼쪽 탐색 창에서 다운로드 센터를 선택합니다.
3. 평가 보고서 탭을 선택합니다.
4. 삭제하려는 평가 보고서를 선택하고 삭제를 선택합니다.

S3 대상 버킷에서 평가 보고서 또는 CSV 내보내기를 삭제하려면 Amazon S3에서 직접 이 작업을 완료하는 것이 좋습니다. 자세한 지침은 Amazon Simple Storage Service(S3) 사용 설명서의 Amazon S3 객체 삭제하기를 참조하세요.

프레임워크 라이브러리

AWS Audit Manager의 프레임워크 라이브러리에서 프레임워크에 액세스하고 관리할 수 있습니다.

프레임워크는 일정 기간 동안 환경에서 테스트할 컨트롤을 결정합니다. 이는 특정 규정 준수 표준 또는 규정에 대한 컨트롤 및 데이터 소스 매핑을 정의합니다. 또한 Audit Manager 평가를 구조화하고 자동화하는 데에도 사용됩니다. 프레임워크를 출발점으로 사용하여 AWS 서비스 사용을 감사하고 증거 수집 자동화를 시작할 수 있습니다.

프레임워크 라이브러리에는 표준 프레임워크와 사용자 지정 프레임워크 카탈로그가 모두 포함되어 있습니다.

- 표준 프레임워크는 AWS가 제공하는 사전 빌드된 프레임워크입니다. 이러한 프레임워크는 다양한 규정 준수 표준 및 규정에 대한 AWS 모범 사례를 기반으로 합니다. 여기에는 GDPR과 HIPAA가 포함됩니다. 표준 프레임워크에는 프레임워크가 지원하는 규정 준수 표준 또는 규정을 기반으로 하는 컨트롤 세트로 구성된 컨트롤이 포함됩니다.

  표준 프레임워크의 내용은 볼 수 있지만 편집하거나 삭제할 수는 없습니다. 하지만 표준 프레임워크를 사용자 지정하여 특정 요구 사항에 맞게 새 프레임워크를 만들 수 있습니다.
- 사용자 지정 프레임워크는 사용자가 소유한 사용자 지정 프레임워크입니다. 처음부터 또는 기존 프레임워크를 사용자 지정하여 사용자 지정 프레임워크를 만들 수 있습니다. 사용자 지정 프레임워크를 사용하여 특정 요구 사항에 맞는 방식으로 컨트롤을 컨트롤 세트로 구성할 수 있습니다. 컨트롤을 관리하는 방법에 대해 자세히 알아보려면 컨트롤 라이브러리을 참조하십시오.

표준 프레임워크 또는 사용자 지정 프레임워크에서 평가를 생성할 수 있습니다. 평가를 생성하고 관리하는 방법에 대한 자세한 내용은 AWS Audit Manager에서의 평가을 참조하십시오.

> **Note**
>
> AWS Audit Manager은 특정 규정 준수 표준 및 규정의 준수 여부를 확인하는 데 필요한 증거를 수집하는 데 도움이 됩니다. 하지만, 규정 준수 자체를 평가하지는 않습니다. 따라서, AWS Audit Manager를 통해 수집되는 증거에는 감사에 필요한 AWS 사용량에 대한 모든 정보가 포함되어 있지 않을 수 있습니다. AWS Audit Manager가 법률 고문이나 규정 준수 전문가를 대신하지는 못합니다.

이 섹션에서는 Audit Manager에서 사용자 지정 프레임워크를 생성하고 관리하는 방법을 설명합니다.

주제

AWS Audit Manager에서 사용 가능한 프레임워크에 액세스할 수 있습니다.

Audit Manager 콘솔의 프레임워크 라이브러리 페이지에서 사용 가능한 모든 프레임워크를 볼 수 있습니다. 여기에서 프레임워크에서 평가를 생성하거나, 사용자 지정 프레임워크를 생성하거나, 기존 프레임워크를 사용자 지정할 수도 있습니다.

Audit Manager API 또는 AWS Command Line Interface(AWS CLI)를 사용하여 사용 가능한 모든 프레임워크를 볼 수도 있습니다.

Audit Manager console

사용 가능한 프레임워크를 보려면 다음을 수행하십시오(콘솔).

1. https://console.aws.amazon.com/auditmanager/home에서 AWS Audit Manager 콘솔을 엽니다.
2. 왼쪽 탐색 창에서 프레임워크 라이브러리를 선택합니다.
3. 표준 프레임워크 탭 또는 사용자 지정 프레임워크 탭을 선택하여 사용 가능한 표준 및 사용자 지정 프레임워크를 찾아보십시오.
4. 해당 프레임워크의 세부 정보를 보려면 프레임워크 이름을 선택하십시오.

AWS CLI

사용 가능한 프레임워크를 보려면(AWS CLI)

Audit Manager에서 프레임워크를 보려면 list-assessment-frameworks 명령을 사용하고 `--framework-type`를 지정합니다. 어느 쪽이든 표준 프레임워크 목록을 검색할 수 있습니다. 또는 사용자 지정 프레임워크 목록을 검색할 수 있습니다.

```
aws auditmanager list-assessment-frameworks --framework-type Standard
```

```
aws auditmanager list-assessment-frameworks --framework-type Custom
```

Audit Manager API

사용 가능한 프레임워크를 보려면(API)

ListAssessmentFrameworks 작업을 사용하고 frameworkType을 지정합니다. 어느 쪽이든 표준 프레임워크 목록을 반환할 수 있습니다. 또는 사용자 지정 프레임워크 목록을 반환할 수 있습니다.

자세한 내용은 이전 링크 중 하나를 선택하여 AWS Audit Manager API 참조에서 자세한 내용을 읽어보십시오. 여기에는 언어별 AWS SDK 중 하나로 `ListAssessmentFrameworks` 작업 및 파라미터를 사용하는 방법에 대한 정보가 포함됩니다.

프레임워크 세부 정보 보기

Audit Manager 콘솔, Audit Manager API 또는 AWS Command Line Interface(AWS CLI)를 사용하여 프레임워크의 세부 정보를 검토할 수 있습니다.

Audit Manager console

프레임워크 세부 정보를 보려면(콘솔)

1. https://console.aws.amazon.com/auditmanager/home에서 AWS Audit Manager 콘솔을 엽니다.
2. 왼쪽 탐색 창에서 프레임워크 라이브러리를 선택하여 사용 가능한 프레임워크 목록을 확인합니다.
3. 표준 프레임워크 탭 또는 사용자 지정 프레임워크 탭을 선택하여 사용 가능한 프레임워크를 찾아보십시오.
4. 프레임워크 이름을 선택하여 프레임워크를 엽니다.

프레임워크를 열면 프레임워크 세부 정보 페이지가 표시됩니다. 이 페이지의 섹션 및 내용은 다음과 같습니다.

프레임워크 세부 정보 섹션

이 섹션에서는 프레임워크에 대한 개요를 제공합니다. 여기에는 다음 정보가 포함됩니다.

- 프레임워크 이름 — 프레임워크의 이름입니다.
- 규정 준수 유형 - 프레임워크가 지원하는 규정 준수 표준 또는 규정입니다.
- 설명 - 프레임워크에 대한 설명입니다(제공된 경우).
- 프레임워크 유형 - 프레임워크가 표준 프레임워크인지 사용자 지정 프레임워크인지를 지정합니다.
- 컨트롤 세트 - 프레임워크와 연결된 컨트롤 세트의 수입니다.
- 컨트롤 — 프레임워크에 있는 컨트롤의 총 개수입니다.
- 컨트롤 소스 - Audit Manager가 증거를 수집하는 컨트롤 데이터 소스의 수입니다.
- 태그 — 프레임워크와 관련된 태그입니다.

사용자 지정 프레임워크를 보는 경우 다음과 같은 세부 정보도 표시됩니다.

- 생성자 - 사용자 지정 프레임워크를 만든 계정입니다.
- 생성 날짜 - 사용자 지정 프레임워크가 생성된 날짜입니다.
- 최종 업데이트 - 이 프레임워크를 마지막으로 편집한 날짜입니다.

컨트롤 탭

이 탭에는 프레임워크의 컨트롤이 컨트롤 세트별로 그룹화되어 나열됩니다. 여기에는 다음 정보가 포함됩니다.

- 컨트롤 세트별로 그룹화된 컨트롤 - 트리 뷰 아이콘을 선택하면 각 컨트롤 세트에 속하는 컨트롤을 볼 수 있습니다.
- 유형 - 컨트롤이 표준 컨트롤인지 사용자 지정 컨트롤인지를 지정합니다.
- 데이터 소스 - Audit Manager가 해당 컨트롤에 대한 증거를 수집하는 데이터 소스를 지정합니다.

태그 탭

이 탭은 프레임워크와 관련된 태그를 나열합니다. 여기에는 다음 정보가 포함됩니다.

- 키 - 태그 키(예: 규정 준수 표준, 규정 또는 범주)입니다.
- 값 - 태그 값

AWS CLI

프레임워크 세부 정보를 보려면(AWS CLI)

1. 검토하려는 프레임워크를 식별하려면 list-assessment frameworks 명령을 실행하고 `--framework-type`를 지정합니다. 어느 쪽이든 표준 프레임워크 목록을 검색할 수 있습니다. 또는 사용자 지정 프레임워크 목록을 검색할 수 있습니다.

   다음 예에서는 *## ### ###*를 `Custom` 또는 `Standard`으로 바꿉니다.

   ```
   aws auditmanager list-assessment-frameworks --framework-type Custom/Standard
   ```

   응답은 프레임워크 목록을 반환합니다. 검토할 프레임워크를 찾고 프레임워크 ID와 Amazon 리소스 이름(ARN)을 기록해 둡니다.

2. 프레임워크 세부 정보를 가져오려면 get-assessment-framework 명령을 실행하고 `--framework-id`을 지정하십시오.

   다음 예에서는 각 *## ### ###*를 자신의 정보로 바꿉니다.

   ```
   aws auditmanager get-assessment-framework --framework-id a1b2c3d4-5678-90ab-cdef-EXAMPLE11111
   ```

   프레임워크 세부 정보는 JSON 형식으로 반환됩니다. 이 데이터를 이해하려면 AWS CLI 명령 참조의 get-assessment-framework 출력을 참조하십시오.

3. 프레임워크의 태그를 보려면 list-tags-for-resource 명령을 사용하고 프레임워크의 `--resource-arn`을 지정합니다.

   다음 예시에서 *## ### ###*를 자신의 정보로 바꿉니다.

   ```
   aws auditmanager list-tags-for-resource --resource-arn arn:aws:auditmanager:us-east-1:111122223333:assessmentFramework/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111
   ```

   Audit Manager의 태그에 대한 자세한 내용은 AWS Audit Manager 리소스 태그 지정을 참조하십시오.

Audit Manager API

프레임워크 세부 정보를 보려면(API)

1. 검토하려는 프레임워크를 식별하려면 ListAssessmentFrameworks 작업을 사용하고 frameworkType을 지정합니다. 어느 쪽이든 표준 프레임워크 목록을 반환할 수 있습니다. 또는 사용자 지정 프레임워크 목록을 반환할 수 있습니다.

   응답에서 검토할 프레임워크를 찾고 프레임워크 ID와 Amazon 리소스 이름(ARN)을 기록해 둡니다.

2. 프레임워크 세부 정보를 가져오려면 GetAsessmentFramework 작업을 사용하십시오. 요청에서 1단계에서 받은 frameworkId를 지정합니다.

   프레임워크 세부 정보는 JSON 형식으로 반환됩니다. 이 데이터를 이해하려면 AWS Audit Manager API 참조의 GetAssessmentFramework 응답 요소를 참조하십시오.

3. 프레임워크의 태그를 보려면 ListTagsForResource 작업을 사용하십시오. 요청에서 1단계에서 받은 프레임워크 resourceArn을 지정합니다.

Audit Manager의 태그에 대한 자세한 내용은 AWS Audit Manager 리소스 태그 지정을 참조하십시오.

이러한 API 작업에 대한 자세한 내용은 이전 링크 중 하나를 선택하여 AWS Audit Manager API 참조에서 자세한 내용을 읽어보세요. 여기에는 이러한 작업 및 파라미터를 언어별 AWS SDK 중 하나로 사용하는 방법에 대한 정보가 포함됩니다.

사용자 지정 프레임워크 만들기

AWS Audit Manager의 프레임워크 라이브러리에서 프레임워크에 액세스하고 관리할 수 있습니다. 사용자 지정 프레임워크를 만들어 특정 요구 사항에 맞는 방식으로 컨트롤을 컨트롤 세트로 구성할 수 있습니다.

사용자 지정 프레임워크는 두 가지 방법으로 생성할 수 있습니다. 기존 프레임워크를 사용자 지정하거나 처음부터 새 프레임워크를 만들 수 있습니다.

주제

- 처음부터 새 사용자 정의 프레임워크 만들기
- 기존 프레임워크 사용자 지정

처음부터 새 사용자 정의 프레임워크 만들기

AWS Audit Manager에서 사용자 지정 프레임워크를 사용하여 특정 요구 사항에 맞는 방식으로 컨트롤을 컨트롤 세트로 구성할 수 있습니다. 다음 단계에 따라 프레임워크 라이브러리에서 처음부터 새 사용자 지정 프레임워크를 만들 수 있습니다.

주제

1단계: 프레임워크 세부 정보 지정

먼저 사용자 지정 프레임워크에 포함할 컨트롤을 지정합니다.

프레임워크 세부 정보를 지정하려면

1. https://console.aws.amazon.com/auditmanager/home에서 AWS Audit Manager 콘솔을 엽니다.
2. 왼쪽 탐색 창에서 프레임워크 라이브러리를 선택하고 사용자 지정 프레임워크 생성을 선택합니다.
3. 프레임워크 세부 정보에서 이름, 규정 준수 표준 또는 규정(선택 사항), 프레임워크에 대한 설명(선택 사항)을 입력합니다. 이 키워드를 사용하여 프레임워크를 검색할 수 있도록 PCI_DSS 또는 GDPR과 같은 규정 준수 표준 또는 규정 키워드를 입력합니다.
4. 태그 에서 새 태그 추가를 선택하여 태그를 프레임워크에 연결합니다. 각 태그에 대한 키 및 값을 지정할 수 있습니다. 태그 키는 필수입니다. 프레임워크 라이브러리에서 이 프레임워크를 검색할 때 이를 검색 기준으로 사용할 수 있습니다. AWS Audit Manager의 태그에 대한 자세한 내용은 AWS Audit Manager 리소스에 태그 지정을 참조하십시오.
5. 다음을 선택합니다.

2단계: 컨트롤 세트의 컨트롤 지정

다음으로 프레임워크에 추가할 컨트롤과 구성 방법을 지정합니다. 먼저 프레임워크에 컨트롤 세트를 추가한 다음, 컨트롤 세트에 컨트롤을 추가합니다.

> **Note**
>
> AWS Audit Manager 콘솔을 사용하여 사용자 지정 프레임워크를 만들 때 각 프레임워크에 대해 최대 10개의 컨트롤 세트를 추가할 수 있습니다.
> Audit Manager API를 사용하여 사용자 지정 프레임워크를 만들 경우 10개 이상의 컨트롤 세트를 만들 수 있습니다. 콘솔에서 현재 허용하는 것보다 더 많은 컨트롤 세트를 추가하려면 Audit Manager에서 제공하는 CreateAssessmentFramework API를 사용하십시오.

컨트롤 세트의 컨트롤을 지정하려면

1. 컨트롤 세트 이름에서 컨트롤 세트 이름을 입력합니다.
2. 컨트롤 세트에 새 컨트롤 추가, 컨트롤 유형 선택에서 드롭다운 목록을 사용하여 두 컨트롤 유형(표준 컨트롤 또는 사용자 지정 컨트롤) 중 하나를 선택합니다. 표준 컨트롤은 Audit Manager에서 제공하며, 사용자 지정 컨트롤은 사용자가 생성하는 컨트롤입니다.
3. 이전 단계에서 선택한 옵션에 따라 표준 컨트롤 또는 사용자 지정 컨트롤 목록이 표시됩니다. 목록을 찾아보거나 컨트롤 이름, 규정 준수 또는 태그를 입력하여 검색할 수 있습니다. 하나 이상의 컨트롤을 선택하고 컨트롤 세트에 추가를 선택하여 컨트롤 세트에 추가합니다.
4. 나타나는 팝업 창에서 컨트롤 세트에 추가를 선택하여 추가를 확인합니다.
5. 컨트롤 세트에서 선택한 컨트롤 검토에서 선택된 컨트롤 목록에 나타나는 컨트롤을 검토합니다. 컨트롤 세트에 컨트롤을 더 추가하려면 2~4단계를 반복합니다. 하나 이상의 컨트롤을 선택하고 컨트롤 제거를 선택하여 컨트롤 세트에서 불필요한 컨트롤을 제거할 수 있습니다.
6. 프레임워크에 새 컨트롤 세트를 추가하려면 페이지 하단에서 컨트롤 세트 추가를 선택합니다. 컨트롤 세트 제거를 선택하여 원하지 않는 컨트롤 세트를 제거할 수 있습니다.
7. 컨트롤 세트와 컨트롤을 모두 추가한 후 다음을 선택합니다.

3단계: 프레임워크 검토 및 생성

프레임워크에 대한 정보를 검토합니다. 단계 정보를 변경하려면 편집을 선택합니다.

작업을 마쳤으면 사용자 지정 프레임워크 생성을 선택합니다.

다음으로 무엇을 할 수 있습니까?

새 사용자 지정 프레임워크를 만든 후 프레임워크에서 평가를 생성할 수 있습니다. 자세한 내용은 평가 생성을 참조하십시오.

기존 프레임워크를 사용하여 사용자 지정 프레임워크를 생성할 수도 있습니다. 자세한 내용은 기존 프레임워크 사용자 지정을 참조하십시오.

사용자 지정 프레임워크를 편집하는 방법에 대한 지침은 사용자 지정 프레임워크 편집을 참조하십시오.

기존 프레임워크 사용자 지정

AWS Audit Manager에서 사용자 지정 프레임워크를 사용하면 특정 요구 사항에 맞는 방식으로 컨트롤을 컨트롤 세트로 구성할 수 있습니다. 사용자 지정 프레임워크를 처음부터 새로 만드는 대신 기존 프레임워크를 시작점으로 사용하여 사용자 지정할 수 있습니다. 이렇게 하면 기존 프레임워크가 프레임워크 라이브러리에 남아 있고 사용자 지정 설정으로 새 사용자 지정 프레임워크가 생성됩니다.

기존 프레임워크를 선택하여 사용자 지정할 수 있습니다. 표준 프레임워크일 수도 있고 사용자 지정 프레임워크일 수도 있습니다.

프레임워크 라이브러리의 사용자 지정 프레임워크 만들기 드롭다운 목록에서 기존 프레임워크 사용자 지정을 선택합니다. 다음 단계에 따라 프레임워크를 사용자 지정합니다.

주제

1단계: 프레임워크 세부 정보 지정

태그를 제외한 모든 프레임워크 세부 정보는 원본 프레임워크에서 전달됩니다. 필요에 따라 이러한 세부 정보를 검토하고 수정합니다.

프레임워크 세부 정보를 지정하려면

1. https://console.aws.amazon.com/auditmanager/home에서 AWS Audit Manager 콘솔을 엽니다.
2. 왼쪽 탐색 창에서 프레임워크 라이브러리를 선택합니다.
3. 사용자 지정하려는 프레임워크를 선택하고 사용자 지정 프레임워크 만들기 드롭다운 목록에서 기존 프레임워크 사용자 지정을 선택합니다.
4. 나타나는 팝업 창에서 새 사용자 지정 프레임워크의 이름을 입력하고 사용자 지정을 선택합니다.

5. 프레임워크 세부 정보에서 프레임워크의 이름, 규정 준수 유형 및 설명을 검토하고 필요에 따라 수정합니다. 규정 준수 유형은 프레임워크와 관련된 규정 준수 표준 또는 규정을 나타내야 합니다. 이 키워드를 사용하여 프레임워크를 검색할 수 있습니다.
6. 태그 에서 새 태그 추가를 선택하여 태그를 프레임워크에 연결합니다. 각 태그에 대한 키 및 값을 지정할 수 있습니다. 태그 키는 필수이며 프레임워크 라이브러리에서 이 프레임워크를 검색할 때 검색 기준으로 사용할 수 있습니다. AWS Audit Manager의 태그에 대한 자세한 내용은 AWS Audit Manager 리소스에 태그 지정을 참조하십시오.
7. 다음을 선택합니다.

2단계: 컨트롤 세트에 추가할 컨트롤 지정

컨트롤 세트는 원래 프레임워크에서 그대로 유지됩니다. 필요에 따라 컨트롤을 추가하거나 기존 컨트롤을 제거하여 현재 구성을 사용자 지정합니다.

> **Note**
>
> AWS Audit Manager 콘솔을 사용하여 프레임워크를 사용자 지정하는 경우 각 프레임워크에 대해 최대 10개의 컨트롤 세트를 추가할 수 있습니다.
> Audit Manager API를 사용하여 사용자 지정 프레임워크를 만들 때 10개 이상의 컨트롤 세트를 추가할 수 있습니다. 콘솔에서 현재 허용하는 것보다 더 많은 컨트롤 세트를 추가하려면 Audit Manager에서 제공하는 CreateAssessmentFramework API를 사용하십시오.

컨트롤 세트에 컨트롤을 지정하려면

1. 컨트롤 세트 이름에서 필요에 따라 컨트롤 세트 이름을 사용자 지정합니다.
2. 컨트롤 세트에 새 컨트롤 추가에서 드롭다운 목록을 사용하여 두 컨트롤 유형(표준 컨트롤 또는 사용자 지정 컨트롤) 중 하나를 선택하여 새 컨트롤을 추가합니다.
3. 이전 단계에서 선택한 옵션에 따라 표준 컨트롤 또는 사용자 지정 컨트롤 목록이 표시됩니다. 이 목록을 찾아보거나 컨트롤 이름, 규정 준수 또는 태그를 입력하여 검색하여 추가하려는 컨트롤을 찾을 수 있습니다. 하나 이상의 컨트롤을 선택하고 컨트롤 세트에 추가를 선택하여 이 컨트롤 세트에 추가합니다.
4. 나타나는 팝업 창에서 컨트롤 세트에 추가를 선택하여 추가를 확인합니다.
5. 컨트롤 세트에서 선택한 컨트롤 검토에서 선택된 컨트롤 목록에 나타나는 컨트롤을 검토합니다. 컨트롤 세트에 컨트롤을 더 추가하려면 2~4단계를 반복합니다. 하나 이상의 컨트롤을 선택하고 컨트롤 제거를 선택하여 컨트롤 세트에서 불필요한 컨트롤을 제거할 수 있습니다.

6. 프레임워크에 새 컨트롤 세트를 추가하려면 페이지 하단에서 컨트롤 세트 추가를 선택합니다. 컨트롤 세트 제거를 선택하여 원하지 않는 컨트롤 세트를 제거할 수 있습니다.
7. 컨트롤 세트와 컨트롤을 모두 추가한 후 다음을 선택합니다.

3단계: 프레임워크 검토 및 생성

프레임워크에 대한 정보를 검토합니다. 단계 정보를 변경하려면 편집을 선택합니다.

작업을 마쳤으면 사용자 지정 프레임워크 생성을 선택합니다.

다음으로 무엇을 할 수 있습니까?

새 사용자 지정 프레임워크를 만든 후 프레임워크에서 평가를 생성할 수 있습니다. 자세한 내용은 평가 생성을 참조하십시오.

사용자 지정 프레임워크를 편집하는 방법에 대한 지침은 사용자 지정 프레임워크 편집을 참조하십시오.

사용자 지정 프레임워크 편집

AWS Audit Manager에서 사용자 지정 프레임워크를 사용하여 특정 필요에 맞게 컨트롤을 컨트롤 세트로 구성할 수 있습니다. 다음 단계에 따라 프레임워크 라이브러리를 사용하여 사용자 지정 프레임워크를 찾고 편집할 수 있습니다.

주제

- 1단계: 프레임워크 세부 정보 편집
- 2단계: 컨트롤 세트의 컨트롤 편집
- 단계 3. 프레임워크 검토 및 업데이트

1단계: 프레임워크 세부 정보 편집

먼저 기존 프레임워크 세부 정보를 검토하고 편집하십시오.

프레임워크 세부 정보를 편집하려면

1. https://console.aws.amazon.com/auditmanager/home에서 AWS Audit Manager 콘솔을 엽니다.
2. 왼쪽 탐색 창에서 프레임워크 라이브러리를 선택한 다음 사용자 지정 프레임워크 탭을 선택합니다.

3. 편집할 프레임워크를 선택하고 작업을 선택한 다음 편집을 선택합니다.
   - 또는 사용자 지정 프레임워크를 열고 평가 요약 페이지의 오른쪽 상단에서 작업, 편집을 선택할 수도 있습니다.
4. 프레임워크 세부 정보에서 프레임워크의 이름, 규정 준수 유형 및 설명을 검토하고 필요에 따라 변경합니다.
5. 다음을 선택합니다.

> **Tip**
>
> 프레임워크의 태그를 편집하려면 프레임워크를 열고 프레임워크 태그 탭을 선택합니다. 여기에서 프레임워크와 관련된 태그를 보고 편집할 수 있습니다.

2단계: 컨트롤 세트의 컨트롤 편집

다음으로 프레임워크의 컨트롤 및 컨트롤 세트를 검토하고 편집합니다.

> **Note**
>
> AWS Audit Manager 콘솔을 사용하여 사용자 지정 프레임워크를 편집하는 경우 각 프레임워크에 대해 최대 10개의 컨트롤 세트를 추가할 수 있습니다.
> Audit Manager API를 사용하여 사용자 지정 프레임워크를 편집할 때 10개 이상의 컨트롤 세트를 추가할 수 있습니다. 콘솔에서 현재 허용하는 것보다 더 많은 컨트롤 세트를 추가하려면 Audit Manager에서 제공하는 UpdateAssessmentFramework API를 사용하십시오.

컨트롤 편집하기

1. 컨트롤 세트 이름에서 필요에 따라 컨트롤 세트 이름을 검토하고 편집합니다.
2. 컨트롤 세트에 새 컨트롤 추가에서 컨트롤을 추가할 수 있습니다. 드롭다운 목록을 사용하여 표준 컨트롤 또는 사용자 지정 컨트롤의 두 가지 컨트롤 유형 중 하나를 선택합니다.
3. 이전 단계에서 선택한 옵션에 따라 표준 컨트롤 또는 사용자 지정 컨트롤의 테이블 목록이 표시됩니다. 목록에서 컨트롤 세트를 찾아볼 수 있습니다. 또는 컨트롤 이름, 데이터 소스 또는 태그를 입력하여 검색하여 추가하려는 컨트롤을 찾을 수 있습니다. 하나 이상의 컨트롤을 선택하고 컨트롤 세트에 추가를 선택하여 이 컨트롤 세트에 추가합니다.
4. 나타나는 팝업 창에서 컨트롤 세트에 추가를 선택하여 추가를 확인합니다.

5. 컨트롤 세트에서 선택한 컨트롤 검토에서 선택된 컨트롤 목록에 현재 나타나는 컨트롤을 검토하고 편집합니다. 컨트롤 세트에 컨트롤을 더 추가하려면 2~4단계를 반복합니다. 하나 이상의 컨트롤을 선택하고 컨트롤 제거를 선택하여 컨트롤 세트에서 불필요한 컨트롤을 제거합니다.
6. 프레임워크에 새 컨트롤 세트를 추가하려면 페이지 하단에서 컨트롤 세트 추가를 선택합니다. 컨트롤 세트 제거를 선택하여 불필요한 컨트롤 세트를 제거합니다.
7. 컨트롤 세트와 컨트롤을 모두 추가한 후 다음을 선택합니다.

단계 3. 프레임워크 검토 및 업데이트

프레임워크에 대한 정보를 검토합니다. 단계 정보를 변경하려면 편집을 선택합니다.

작업을 마쳤으면 변경 내용 저장을 선택합니다.

사용자 지정 프레임워크 삭제

프레임워크 라이브러리를 사용하여 원하지 않는 사용자 지정 프레임워크를 찾아 삭제할 수 있습니다. Audit Manager API 또는 AWS Command Line Interface (AWS CLI)를 사용하여 사용자 지정 프레임워크를 삭제할 수도 있습니다.

> **Note**
>
> 사용자 지정 프레임워크를 삭제해도 삭제되기 전에 프레임워크에서 만든 기존 평가에는 영향을 주지 않습니다.

Audit Manager console

사용자 지정 프레임워크를 삭제하려면(콘솔)

1. https://console.aws.amazon.com/auditmanager/home에서 AWS Audit Manager 콘솔을 엽니다.
2. 왼쪽 탐색 창에서 프레임워크 라이브러리를 선택한 다음 사용자 지정 프레임워크 탭을 선택합니다.
3. 삭제하려는 프레임워크를 선택하고 작업을 선택한 다음 삭제를 선택합니다.
   - 또는 사용자 지정 프레임워크를 열고 프레임워크 요약 페이지의 오른쪽 상단에서 작업, 삭제를 선택할 수도 있습니다.
4. 팝업 창에서 삭제를 선택하여 삭제를 확인합니다.

AWS CLI

사용자 지정 프레임워크를 삭제하려면(AWS CLI)

1. 먼저 삭제할 사용자 지정 프레임워크를 식별합니다. 이렇게 하려면 list-assessment-frameworks 명령을 실행하고 `--framework-type`를 `Custom`으로 지정하십시오.

   ```
   aws auditmanager list-assessment-frameworks --framework-type Custom
   ```

   응답은 사용자 지정 프레임워크 목록을 반환합니다. 삭제하려는 사용자 지정 프레임워크를 찾고 프레임워크 ID를 기록해 둡니다.
2. 그런 다음 delete-assessment-framework 명령을 실행하고 삭제하려는 프레임워크의 `--framework-id`를 지정합니다.

   다음 예에서는 각 *## ### ###*를 자신의 정보로 바꿉니다.

   ```
   aws auditmanager delete-assessment-framework --framework-id a1b2c3d4-5678-90ab-cdef-EXAMPLE11111
   ```

Audit Manager API

사용자 지정 프레임워크(API)를 삭제하려면

1. ListAssessmentFrameworks 작업을 사용하고 frameworkType을 `Custom`로 지정합니다. 응답에서 삭제하려는 사용자 지정 프레임워크를 찾고 프레임워크 ID를 기록해 둡니다.
2. DeleteAssessmentFramework 작업을 사용하여 프레임워크를 삭제합니다. 요청에서 frameworkId 매개변수를 사용하여 삭제하려는 프레임워크를 지정합니다.

이러한 API 작업에 대한 자세한 내용은 이전 링크 중 하나를 선택하여 AWS Audit Manager API 참조에서 자세한 내용을 읽어보세요. 여기에는 이러한 작업 및 파라미터를 언어별 AWS SDK 중 하나로 사용하는 방법에 대한 정보가 포함됩니다.

사용자 지정 프레임워크 공유

AWS Audit Manager의 프레임워크 공유 기능을 사용하여 생성한 사용자 지정 프레임워크를 빠르게 복제할 수 있습니다. 사용자 지정 프레임워크를 다른 AWS 계정와 공유하거나 자신의 계정으로 프레임워크를 다른 AWS 리전에 복제할 수 있습니다. 그러면 수신자가 사용자 지정 프레임워크에 액세스하여

이를 사용하여 평가를 생성할 수 있습니다. 해당 프레임워크에 대한 구성 작업을 반복하지 않고도 이 작업을 수행할 수 있습니다.

사용자 지정 프레임워크를 공유하려면 공유 요청을 생성합니다. 그러면 공유 요청 수신자는 120일 이내에 요청을 수락하거나 거부해야 합니다. 공유 요청을 수락하면 Audit Manager는 공유된 사용자 지정 프레임워크를 프레임워크 라이브러리에 복제합니다. Audit Manager는 사용자 지정 프레임워크를 복제할 뿐만 아니라 해당 프레임워크에 속하는 사용자 지정 컨트롤 집합과 사용자 지정 컨트롤도 복제합니다. 그런 다음 이러한 사용자 지정 컨트롤이 수신자의 컨트롤 라이브러리에 추가됩니다. Audit Manager는 표준 프레임워크 또는 컨트롤을 복제하지 않습니다. 기본적으로 Audit Manager가 활성화된 모든 AWS 계정 및 리전에서 사용할 수 있습니다.

프레임워크 공유 기능은 유료 등급에서만 사용할 수 있습니다. 하지만 사용자 지정 프레임워크를 공유하거나 공유 요청을 수락하는 데에는 추가 요금이 부과되지 않습니다. AWS Audit Manager 요금에 대한 자세한 내용은 AWS Audit Manager 요금 페이지를 참조하십시오.

> **Important**
>
> 표준 프레임워크가 AWS에 의해 공유에 적합하지 않은 것으로 지정된 경우, 표준 프레임워크에서 파생된 사용자 지정 프레임워크를 공유할 수 없습니다. 단, 표준 프레임워크 소유자로부터 공유 권한을 받은 경우는 예외입니다. 공유할 수 없는 표준 프레임워크를 확인하고 자세히 알아보려면 프레임워크 공유 자격을 참조하십시오.

이 가이드의 다음 섹션에서는 프레임워크 공유에 대해 알아야 할 중요한 사항을 설명합니다. 또한 사용자 지정 프레임워크를 공유하고 공유 요청에 응답하는 방법에 대한 지침도 제공합니다.

주제

- 프레임워크 공유 개념 및 용어
- 사용자 지정 프레임워크에 대한 공유 요청 전송
- 공유 요청에 대한 응답
- 공유 요청 삭제

> **Tip**
>
> Audit Manager 사용자 지정 프레임워크 및 이를 만드는 방법에 익숙하지 않은 경우 이 가이드의 사용자 지정 프레임워크 만들기 페이지에서 자세히 알아볼 수 있습니다.

프레임워크 공유 개념 및 용어

다음 주요 개념을 익히면 AWS Audit Manager 사용자 지정 프레임워크 공유 기능을 더 잘 활용할 수 있습니다.

발신자

공유 요청의 생성자이며 사용자 지정 프레임워크가 있는 AWS 계정입니다. 발신자는 어떤 AWS 계정와도 사용자 지정 프레임워크를 공유할 수 있습니다. 또는 사용자 지정 프레임워크를 자신의 계정으로 지원되는 모든 AWS 리전에 복제할 수도 있습니다.

수신자

이는 공유 프레임워크의 소비자입니다. 수신자는 발신자의 공유 요청을 수락하거나 거부할 수 있습니다.

> **Note**
>
> 수신자는 위임된 관리자 계정일 수 있습니다. 하지만 사용자 지정 프레임워크는 AWS Organizations 관리 계정과 공유할 수 없습니다.

프레임워크 자격

사용자 지정 프레임워크만 공유할 수 있습니다. 기본적으로 표준 프레임워크는 AWS Audit Manager이 활성화된 모든 AWS 계정 및 AWS 리전에 이미 존재합니다. 또한 공유하는 사용자 지정 프레임워크에는 민감한 데이터가 포함되어서는 안 됩니다. 여기에는 프레임워크 자체, 해당 컨트롤 세트 및 사용자 지정 프레임워크의 일부인 모든 사용자 지정 컨트롤에 있는 데이터가 포함됩니다.

> **Important**
>
> AWS Audit Manager에서 제공하는 일부 표준 프레임워크에는 라이선스 계약의 적용을 받는 저작권이 있는 자료가 포함되어 있습니다. 사용자 지정 프레임워크에는 이러한 프레임워크에서 파생된 콘텐츠가 포함될 수 있습니다. 표준 프레임워크가 AWS에 의해 공유에 적합하지 않은 것으로 지정된 경우, 표준 프레임워크 소유자로부터 허가를 받지 않은 한 표준 프레임워크에서 파생된 사용자 지정 프레임워크를 공유할 수 없습니다.
> 공유할 수 있는 표준 프레임워크를 알아보려면 다음 테이블을 참조하십시오.

표준 프레임워크 이름	공유할 수 있는 사용자 지정 버전
호주 사이버 보안 센터(ACSC) 에센셜 에이트	 예
호주 사이버 보안 센터(ACSC) 정보 보안 매뉴얼	 예
AWS Audit Manager샘플 프레임워크	 예
AWS Control Tower 가드레일	 예
AWS 생성형 AI 모범 사례 프레임워크 v1	 예
AWS License Manager	 예
AWS 기초 보안 모범 사례	 예
AWS 운영 모범 사례	 예
AWS Well-Architected 프레임워크	 예

표준 프레임워크 이름	공유할 수 있는 사용자 지정 버전
캐나다 사이버 보안 센터 - 미디엄	 아니요
CIS Amazon Web Services 파운데이션 벤치마크 v1.2.0, 레벨 1용 CIS 벤치마크	 아니요
CIS Amazon Web Services 파운데이션 벤치마크 v1.2.0, 레벨 1 및 2용 CIS 벤치마크	 아니요
CIS Amazon Web Services 파운데이션 벤치마크 v1.3.0, 레벨 1용 CIS 벤치마크	 아니요
CIS Amazon Web Services 파운데이션 벤치마크 v1.3.0, 레벨 1 및 2용 CIS 벤치마크	 아니요
CIS Amazon Web Services 파운데이션 벤치마크 v1.4.0, 레벨 1용 CIS 벤치마크	 아니요
CIS Amazon Web Services 파운데이션 벤치마크 v1.4.0, 레벨 1 및 2용 CIS 벤치마크	 아니요

표준 프레임워크 이름	공유할 수 있는 사용자 지정 버전
CIS 컨트롤 v7.1 IG1	 예
CIS 컨트롤 v8 IG1	 아니요
FedRAMP 모더레이트 베이스라인	 예
GDPR	 예
그램-리치-블라일리 법(GLBA)	 예
GxP 21 CFR 파트 11	 예
GxP EU 부속서 11	 예
HIPAA 보안 규칙 2003	 예

표준 프레임워크 이름	공유할 수 있는 사용자 지정 버전
HIPAA 최종 옴니버스 보안 규칙 2013	 예
ISO/IEC 27001:2013 부속서 A	 아니요
NIST 800-53 (개정 5) 낮음-보통-높음	 예
NIST 사이버 보안 프레임워크 버전 1.1	 예
NIST SP 800-171 개정 2	 예
PCI DSS v3.2.1	 아니요
PCI DSS v4.0	 아니요
SOC 2	 아니요

공유 요청

사용자 지정 프레임워크를 공유하려면 공유 요청을 생성합니다. 공유 요청은 수신자를 지정하고 사용자 지정 프레임워크를 사용할 수 있음을 알립니다. 수신자는 120일 이내에 수락 또는 거부를 통해 공유 요청에 응답해야 합니다. 120일 내에 조치를 취하지 않으면 공유 요청이 만료되고 수신자는 프레임워크 라이브러리에 사용자 정의 프레임워크를 추가할 수 없게 됩니다. 발신자와 수신자는 프레임워크 라이브러리의 공유 요청 페이지에서 공유 요청을 보고 조치를 취할 수 있습니다.

요청 상태 공유하기

공유 요청의 상태는 다음 중 하나일 수 있습니다.

- 활성 - 공유 요청이 수신자에게 성공적으로 전송되었으며 응답을 기다리고 있음을 나타냅니다.
- 만료 예정 - 향후 30일 이내에 만료되는 공유 요청을 나타냅니다.
- 공유 - 수신자가 수락한 공유 요청을 나타냅니다.
- 비활성 - 수신자가 조치를 취하기 전에 취소, 거부 또는 만료된 공유 요청을 나타냅니다.
- 복제 중 - 수락된 공유 요청이 수신자의 프레임워크 라이브러리에 복제되고 있음을 나타냅니다.
- 실패 - 이는 공유 요청이 수신자에게 성공적으로 전송되지 않았음을 나타냅니다.

공유 요청 알림

Audit Manager는 수신자가 공유 요청을 받으면 이를 알립니다. 공유 요청이 향후 30일 내에 만료될 예정이면 수신자와 발신자 모두 알림을 받습니다.

- 수신자의 경우 활성 또는 만료 예정 상태인 수신된 요청 옆에 파란색 알림 점이 나타납니다. 수신자는 공유 요청을 수락하거나 거부하여 알림을 해결할 수 있습니다.
- 발신자의 경우 보낸 요청이 만료 예정 상태일 때 파란색 알림 점이 나타납니다. 알림은 수신자가 요청을 수락하거나 거부하면 해결됩니다. 그렇지 않으면 요청이 만료될 때 문제가 해결됩니다. 또한 발신자는 공유 요청을 취소하여 알림을 해결할 수 있습니다.

발신자 소유권

발신자는 공유하는 사용자 지정 프레임워크에 대한 전체 액세스 권한을 유지합니다. 만료되기 전에 공유 요청을 취소하여 언제든지 활성 공유 요청을 취소할 수 있습니다. 하지만 수신자가 공유 요청을 수락한 후에는 발신자가 해당 사용자 지정 프레임워크에 대한 수신자의 액세스 권한을 더 이상 취소할 수 없습니다. 이는 수신자가 요청을 수락하면 Audit Manager가 수신자의 프레임워크 라이브러리에 사용자 지정 프레임워크의 독립적인 사본을 생성하기 때문입니다.

발신자의 사용자 지정 프레임워크를 복제하는 것 외에도 Audit Manager는 해당 프레임워크에 속하는 모든 사용자 지정 컨트롤 세트 및 사용자 지정 컨트롤을 복제합니다. 하지만 Audit Manager는 사용자 지정 프레임워크에 연결된 태그를 복제하지 않습니다.

수신자 소유권

수신자는 자신이 수락한 사용자 지정 프레임워크에 대한 전체 액세스 권한을 가집니다. 수신자가 요청을 수락하면 Audit Manager는 사용자 지정 프레임워크를 해당 프레임워크 라이브러리의 사용자 지정 프레임워크 탭에 복제합니다. 그러면 수신자가 다른 사용자 지정 프레임워크와 동일한 방식으로 공유 사용자 지정 프레임워크를 관리할 수 있습니다. 수신자는 다른 발신자로부터 수신한 사용자 지정 프레임워크를 공유할 수 있습니다. 수신자는 발신자가 공유 요청을 보내는 것을 차단할 수 없습니다.

공유 프레임워크 만료

발신자가 공유 요청을 생성하면 Audit Manager는 120일 후에 요청이 만료되도록 설정합니다. 수신자는 요청이 만료되기 전에 공유 프레임워크를 수락하고 해당 프레임워크에 대한 액세스 권한을 얻을 수 있습니다. 이 기간 동안 수신자가 수락하지 않으면 공유 요청이 만료됩니다. 이 시점 이후에는 만료된 공유 요청 기록이 기록에 남습니다. 만료된 공유 프레임워크의 스냅샷은 감사 목적으로 1년 TTL이 적용된 S3 버킷에 보관됩니다.

발신자는 공유 요청이 만료되기 전에 언제든지 공유 요청을 취소할 수 있습니다.

공유 프레임워크 데이터 저장 및 백업

공유 요청을 생성할 때 Audit Manager는 사용자 지정 프레임워크의 스냅샷을 미국 동부(버지니아 북부) AWS 리전에 저장합니다. 또한 Audit Manager는 동일한 스냅샷의 백업을 미국 서부(오레곤) AWS 리전에 저장합니다.

Audit Manager는 다음 이벤트 중 하나가 발생할 때 스냅샷과 백업 스냅샷을 삭제합니다.

- 발신자가 공유 요청을 취소합니다.
- 수신자가 공유 요청을 거부합니다.
- 수신자가 오류가 발생하여 공유 요청을 성공적으로 수락하지 못합니다.
- 공유 요청은 수신자가 요청에 응답하기 전에 만료됩니다.

발신자가 공유 요청을 다시 보내면 스냅샷은 사용자 지정 프레임워크의 최신 버전에 해당하는 업데이트된 버전으로 대체됩니다.

수신자가 공유 요청을 수락하면 스냅샷은 공유 요청에 지정된 AWS 리전에 따라 해당 AWS 계정로 복제됩니다.

공유 프레임워크 버전 관리

사용자 지정 프레임워크를 공유하면 Audit Manager는 지정된 AWS 계정 및 리전에 해당 프레임워크의 독립적인 복사본을 만듭니다. 즉, 다음 사항에 유의해야 합니다.

- 수신자가 수락하는 공유 프레임워크는 공유 요청 생성 시점의 프레임워크 스냅샷입니다. 공유 요청을 보낸 후 원본 사용자 지정 프레임워크를 업데이트해도 요청이 자동으로 업데이트되지 않습니다. 업데이트된 프레임워크의 최신 버전을 공유하려면 공유 요청을 다시 보내면 됩니다. 새 스냅샷의 만료일은 재공유일로부터 120일입니다.
- 사용자 지정 프레임워크를 다른 AWS 계정과 공유한 다음 프레임워크 라이브러리에서 삭제해도 공유된 사용자 지정 프레임워크는 수신자의 프레임워크 라이브러리에 남아 있습니다.
- 사용자 지정 프레임워크를 계정에 속한 다른 AWS 리전과 공유한 다음 첫 번째 AWS 리전에서 해당 사용자 지정 프레임워크를 삭제해도 사용자 지정 프레임워크는 두 번째 리전에 남아 있습니다.
- 공유 사용자 지정 프레임워크를 수락한 후 삭제하면 사용자 지정 프레임워크의 일부로 복제된 모든 사용자 지정 컨트롤이 컨트롤 라이브러리에 남아 있습니다.

사용자 지정 프레임워크에 대한 공유 요청 전송

이 자습서에서는 사용자 지정 프레임워크를 AWS 계정 및 AWS 리전 간에 공유하는 방법을 설명합니다.

사용자 지정 프레임워크를 공유하면 Audit Manager는 프레임워크의 스냅샷을 만들고 수신자에게 공유 요청을 보냅니다. 수신자는 120일 이내에 공유 프레임워크를 수락해야 합니다. 수락하면 Audit Manager는 공유된 사용자 지정 프레임워크를 지정된 AWS 리전 프레임워크 라이브러리에 복제합니다. 사용자 지정 프레임워크를 자신의 계정으로 다른 리전에 복제하려면 다음 자습서를 사용하고 자신의 AWS 계정 ID를 수신자 계정 ID로 입력하십시오.

이 자습서에서는 다음 단계를 다룹니다.

1. 공유할 프레임워크 선택 - 프레임워크 라이브러리를 탐색하여 공유하려는 사용자 지정 프레임워크를 찾습니다.
2. 공유 요청 전송 - 수신자를 지정하고 사용자 지정 프레임워크에 대한 공유 요청을 전송합니다.
3. 보낸 요청 보기 - 공유 요청 기록을 보고 전송된 요청의 상태를 확인합니다.
4. (선택 사항) 공유 요청 취소 - 만료 기한 전에 공유 요청을 취소합니다.

사전 조건

이 자습서를 시작하기 전에 다음 조건을 충족하는지 확인하십시오.

- Audit Manager 프레임워크 공유 개념 및 용어에 익숙할 것입니다.

- 공유하려는 사용자 지정 프레임워크는 공유 가능하며 AWS Audit Manager 환경의 프레임워크 라이브러리에 존재합니다.
- 사용자 지정 프레임워크를 공유하려는 AWS 리전에서 수신자가 이미 AWS Audit Manager을 활성화했습니다.
- 수신자는 AWS Organizations 관리 계정이 아닙니다.

> **Tip**
>
> 시작하기 전에 사용자 지정 프레임워크를 공유할 AWS 계정 ID를 기록해 두십시오. 프레임워크를 계정 내 다른 AWS 리전에 복제하는 것이 목표라면 이 ID를 자신의 계정 ID로 사용할 수 있습니다. 자습서의 2단계에는 이 정보가 필요합니다.

> **Important**
>
> 민감한 데이터가 포함된 사용자 지정 프레임워크를 공유하지 마십시오. 여기에는 프레임워크 자체, 해당 컨트롤 세트 및 사용자 지정 프레임워크를 구성하는 모든 사용자 지정 컨트롤에 있는 데이터가 포함됩니다. 자세한 내용은 프레임워크 적합성을 참조하십시오.

1단계: 공유하려는 사용자 지정 프레임워크 식별

먼저 공유하려는 사용자 지정 프레임워크를 식별합니다. Audit Manager의 프레임워크 라이브러리 페이지에서 사용 가능한 모든 사용자 지정 프레임워크 목록을 찾을 수 있습니다.

사용 가능한 사용자 지정 프레임워크를 보려면

1. https://console.aws.amazon.com/auditmanager/home에서 AWS Audit Manager 콘솔을 엽니다.
2. 탐색 창에서 프레임워크 라이브러리를 선택합니다.
3. 사용자 지정 프레임워크 탭을 선택합니다. 그러면 사용 가능한 사용자 지정 프레임워크 목록이 표시됩니다. 원하는 프레임워크 이름을 선택하여 해당 사용자 지정 프레임워크의 세부 정보를 볼 수 있습니다.

2단계: 공유 요청 보내기

그런 다음 수신자를 지정하고 사용자 지정 프레임워크에 대한 공유 요청을 보냅니다. 수신자는 120일 이내에 공유 요청이 만료되기 전에 공유 요청에 응답해야 합니다.

공유 요청을 보내려면

1. 프레임워크 라이브러리의 사용자 지정 프레임워크 탭에서 프레임워크 이름을 선택하여 세부 정보 페이지를 엽니다. 여기에서 작업을 선택한 다음 사용자 지정 프레임워크 공유를 선택합니다.
   - 또는 프레임워크 라이브러리의 목록에서 사용자 지정 프레임워크를 선택하고 작업을 선택한 다음 사용자 지정 프레임워크 공유를 선택합니다. 사용자 지정 프레임워크의 크기에 따라 Audit Manager가 공유 요청을 준비하는 데 이 방법을 사용할 경우 몇 초 정도 걸릴 수 있습니다.
2. 대화 상자에 표시되는 알림을 검토하십시오.
   - 사용자 지정 프레임워크를 공유할 수 있는지 확실하지 않은 경우 프레임워크 적합성을 검토하여 추가 지침을 확인하십시오.
   - 프레임워크에 사용자 지정 AWS Config 규칙을 데이터 소스로 사용하는 컨트롤 기능이 있는 경우 수신자에게 연락하여 알리는 것이 좋습니다. 그러면 수신자는 자신의 AWS Config 인스턴스에서 동일한 AWS Config 규칙을 만들고 활성화할 수 있습니다. 자세한 내용은 내 공유 프레임워크에는 사용자 지정 AWS Config 규칙을 데이터 소스로 사용하는 제어가 있습니다. 수신자가 이러한 제어에 대한 증거를 수집할 수 있나요?을 참조하십시오.
3. **agree**를 입력한 다음 동의를 선택하여 계속 진행하십시오.
4. 그 다음 화면에서 아래 단계를 따릅니다.
   - AWS 계정 아래에 수신자의 계정 ID를 입력합니다. 이는 자신의 계정 ID일 수 있습니다.
   - AWS 리전 아래에 드롭다운 목록에서 수신자의 리전을 선택합니다.
   - (선택 사항) 수신자에게 보내는 메시지에 공유 중인 사용자 지정 프레임워크에 대한 의견을 선택적으로 입력합니다.
   - 사용자 지정 프레임워크 세부 정보에서 세부 정보를 검토하여 이 프레임워크를 공유할 것인지 확인하십시오.
5. 공유를 선택합니다.

> **Note**
>
> 다음 사항에 유의하세요.
>
> - 사용자 지정 프레임워크를 다른 AWS 계정와 공유하면 해당 프레임워크가 지정된 AWS 리전에만 복제됩니다. 공유 요청을 수락한 후 수신자는 필요에 따라 여러 리전에 프레임워크를 복제할 수 있습니다.

- AWS 리전 전체에서 사용자 지정 프레임워크를 공유하는 경우 공유 요청 작업을 처리하는 데 최대 10분이 걸릴 수 있습니다. 리전 간 공유 요청을 보낸 후에는 나중에 다시 확인하여 공유 요청이 성공적으로 전송되었는지 확인하는 것이 좋습니다.
- 공유 요청을 보내면 Audit Manager는 공유 요청 생성 시 사용자 지정 프레임워크의 스냅샷을 생성합니다. 공유 요청을 보낸 후 사용자 지정 프레임워크를 업데이트해도 요청이 자동으로 업데이트되지 않습니다. 업데이트된 프레임워크의 최신 버전을 공유하려면 공유 요청을 다시 보내면 됩니다. 새 스냅샷의 만료일은 재공유일로부터 120일입니다.

3단계: 보낸 요청 보기

보낸 요청 탭을 선택하여 전송한 모든 공유 요청의 목록을 볼 수 있습니다. 필요에 따라 이 목록을 필터링할 수 있습니다. 예를 들어 필터를 적용하여 향후 30일 이내에 만료되는 요청만 표시할 수 있습니다.

보낸 요청을 보고 필터링하려면

1. 탐색 창에서 공유 요청을 선택합니다.
2. 보낸 요청 탭을 선택합니다.
3. (선택 사항) 필터를 적용하여 어떤 보낸 요청이 표시되는지 세밀하게 조정합니다. 모든 상태 드롭다운 목록을 찾아 필터를 다음 중 하나로 변경하면 이 작업을 수행할 수 있습니다.
   - 활성 - 이 필터는 수신자의 응답을 기다리고 있는 공유 요청을 표시합니다.
   - 공유 - 이 필터는 수신자가 수락한 공유 요청을 표시합니다. 이제 공유된 사용자 지정 프레임워크가 수신자의 프레임워크 라이브러리에 있습니다.
   - 비활성 - 이 필터는 수신자가 조치를 취하기 전에 거부, 취소 또는 만료된 공유 요청을 표시합니다. 자세한 내용을 보려면 비활성이라는 단어를 선택하십시오.
   - 만료 예정 - 이 필터는 향후 30일 내에 만료되는 공유 요청을 표시합니다.
   - 실패 - 이 필터는 수신자에게 성공적으로 전송되지 않은 공유 요청을 표시합니다. 자세한 내용을 보려면 실패라는 단어를 선택하십시오.

> **Note**
>
> 공유 요청을 처리하는 데 최대 15분이 소요될 수 있습니다. 따라서 수신자에게 공유 요청을 보낼 때 오류가 발생한 경우 실패 상태가 즉시 표시되지 않을 수 있습니다. 나중에 다시 확인하여 공유 요청이 성공적으로 전송되었는지 확인하는 것이 좋습니다.

오류가 발생한 경우의 처리 방법에 대한 자세한 내용은 공유 요청 문제 해결을 참조하십시오.

4단계(선택 사항): 공유 요청 취소

만료되기 전에 활성 공유 요청을 취소해야 하는 경우 언제든지 요청을 취소할 수 있습니다. 이 단계는 선택 사항입니다. 조치를 취하지 않으면 만료일 이후 수신자가 공유 요청을 수락할 수 없게 됩니다.

공유 요청 취소하기

1. 탐색 창에서 공유 요청을 선택합니다.
2. 보낸 요청 탭을 선택합니다.
3. 취소하려는 프레임워크를 선택하고 요청 취소를 선택합니다.
4. 나타나는 팝업 창에서 취소를 선택합니다.

> **Note**
>
> 상태가 활성 또는 만료 예정인 공유 요청에 대한 액세스 권한만 취소할 수 있습니다. 수신자가 공유 요청을 수락한 후에는 해당 사용자 지정 프레임워크에 대한 수신자의 액세스 권한을 더 이상 취소할 수 없습니다. 이는 이제 사용자 지정 프레임워크의 복사본이 수신자의 프레임워크 라이브러리에 존재하기 때문입니다.
> AWS 리전 전반에서 프레임워크를 공유할 때 공유 요청 작업을 처리하는 데 최대 10분이 소요될 수 있습니다. 리전 간 공유 요청을 취소한 후에는 나중에 다시 확인하여 공유 요청이 성공적으로 취소되었는지 확인하는 것이 좋습니다.

업데이트된 프레임워크에 대한 공유 요청 재전송

사용자 지정 프레임워크에 대한 공유 요청을 보낸 다음 동일한 프레임워크를 업데이트할 수 있습니다. 이렇게 하면 공유 요청이 프레임워크의 최신 버전을 반영하도록 자동으로 업데이트되지 않습니다. 하지만 상태가 활성, 공유 또는 만료 예정이면 기존 공유 요청을 업데이트할 수 있습니다. 이렇게 하려면 기존 요청과 동일한 세부 정보가 포함된 새 공유 요청을 다시 보내야 합니다. 새 공유 요청에는 동일한 사용자 지정 프레임워크 ID, 수신자 계정 ID, 수신자 AWS 리전를 포함하십시오. 새 공유 요청과 함께 새 의견을 제공할 수도 있습니다.

공유 요청을 재전송할 때는 다음 사항에 유의하십시오.

- 업데이트가 성공하려면 새 요청이 동일한 사용자 지정 프레임워크 ID에 대한 것이어야 합니다. 또한 기존 요청과 동일한 수신자 계정 ID 및 리전을 지정해야 합니다.
- 사용자 지정 프레임워크의 이름이 변경된 경우 업데이트된 공유 요청에는 최신 이름이 표시됩니다.
- 새 의견을 입력하면 업데이트된 공유 요청에 최신 의견이 표시됩니다.
- 공유 요청을 다시 보내면 만료 날짜가 6개월 연장됩니다.

업데이트된 프레임워크에 대한 공유 요청 재전송하기

1. 프레임워크 라이브러리의 사용자 지정 프레임워크 탭에서 공유하려는 프레임워크의 이름을 선택합니다. 그러면 프레임워크 세부 정보 페이지가 열립니다. 여기에서 작업을 선택한 다음 사용자 지정 프레임워크 공유를 선택합니다.

   - 또는 프레임워크 라이브러리의 목록에서 사용자 지정 프레임워크를 선택하고 작업을 선택한 다음 사용자 지정 프레임워크 공유를 선택합니다. 사용자 지정 프레임워크의 크기에 따라 이 방법을 사용하면 Audit Manager에서 공유 요청을 준비하는 데 몇 초 정도 걸릴 수 있습니다.
2. 대화 상자에 표시되는 알림을 검토하고 **agree**를 입력한 다음 동의를 선택하여 계속하십시오.
3. 그 다음 화면에서 아래 단계를 따릅니다.

   - AWS 계정 아래에, 기존 공유 요청에서 지정한 것과 동일한 계정 ID를 입력합니다.
   - AWS 리전 아래에, 기존 공유 요청에서 지정한 것과 동일한 리전을 선택합니다.
   - (선택 사항) 수신자에게 보내는 메시지에 업데이트된 사용자 지정 프레임워크에 대한 의견을 선택적으로 입력합니다.
   - 사용자 지정 프레임워크 세부 정보에서 세부 정보를 검토하여 공유 요청을 다시 보낼 것인지 확인합니다.
4. 공유를 선택하여 공유 요청을 재전송하고 업데이트합니다.

공유 요청 문제 해결

사용자 지정 프레임워크를 공유할 때 발생할 수 있는 문제에 대한 해결책을 찾으려면 이 안내서의 문제 해결 섹션에서 프레임워크 공유 문제 해결을 참조하십시오.

공유 요청에 대한 응답

이 자습서는 사용자 지정 프레임워크에 대한 공유 요청을 받을 때 수행할 수 있는 작업을 설명합니다. 공유 요청을 받으면 Audit Manager에서 알려줍니다. 또한 공유 요청이 향후 30일 내에 만료될 경우 이를 알리는 알림을 받게 됩니다.

이 자습서에서는 다음 단계를 다룹니다.

1. 공유 요청 알림 확인 - 활성 상태이고 곧 만료되는 공유 요청 목록을 검토하십시오.
2. 공유 요청에 대한 조치 취하기 — 사용자 지정 프레임워크에 대한 공유 요청을 수락하거나 거부합니다.
3. 다른 사람으로부터 받은 공유 요청 보기 — 공유 요청 기록을 볼 수 있습니다.

사전 조건

시작하기 전에 먼저 Audit Manager 프레임워크 공유 개념 및 용어에 대해 자세히 알아보는 것이 좋습니다.

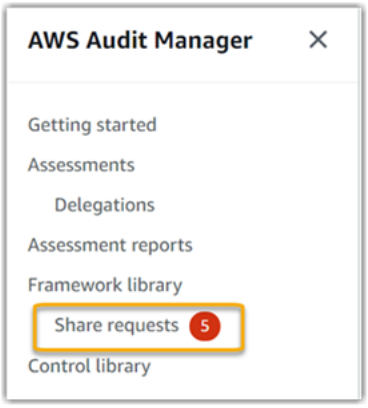
1단계: 수신된 요청 알림 확인

먼저 공유 요청 알림을 확인하십시오. 수신된 요청 탭에는 다른 사람으로부터 받은 공유 요청 목록이 표시됩니다AWS 계정. 응답을 기다리고 있는 요청은 파란색 점으로 표시됩니다. 이 보기를 필터링하여 향후 30일 이내에 만료되는 요청만 표시할 수도 있습니다.

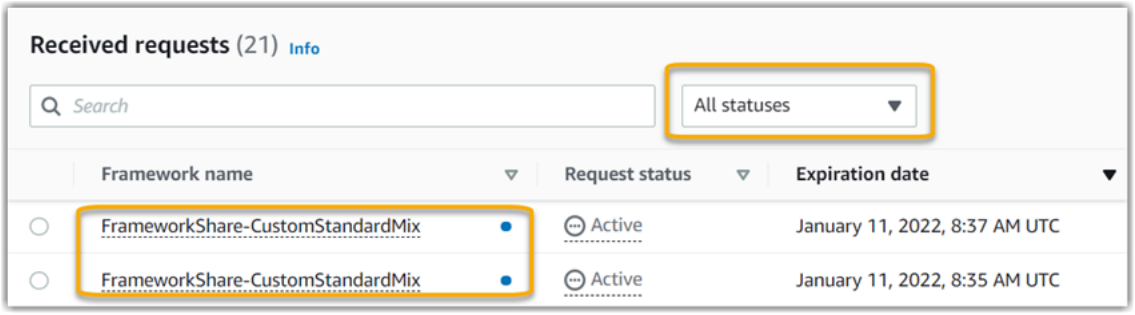
수신된 요청을 보려면

1. https://console.aws.amazon.com/auditmanager/home에서 AWS Audit Manager 콘솔을 엽니다.
2. 공유 요청 알림이 있는 경우 Audit Manager는 탐색 메뉴 아이콘 옆에 빨간색 점을 표시합니다.

3. 탐색 창을 펼치고 공유 요청 옆을 살펴보십시오. 알림 배지는 주의가 필요한 공유 요청의 수를 나타냅니다.



4. 공유 요청을 선택합니다. 기본적으로 이 페이지는 수신된 요청 탭에서 열립니다.
5. 파란색 점이 있는 항목을 찾아 조치가 필요한 공유 요청을 식별하십시오.



6. (선택 사항)향후 30일 이내에 만료되는 요청만 보려면 모든 상태 드롭다운 목록을 찾아 만료 중을 선택합니다.

2단계: 요청에 대한 조치 취하기

파란색 알림 점을 제거하려면 공유 요청을 수락하거나 거부하여 조치를 취해야 합니다.

> **Note**
>
> AWS 리전 전체에서 프레임워크가 공유되는 경우 공유 요청 작업을 처리하는 데 최대 10분이 걸릴 수 있습니다. 리전 간 공유 요청에 대해 조치를 취한 후에는 나중에 다시 확인하여 공유 요청이 성공적으로 수락 또는 거부되었는지 확인하는 것이 좋습니다.

공유 프레임워크 수락

공유 요청을 수락하면 Audit Manager는 원본 프레임워크의 스냅샷을 프레임워크 라이브러리의 사용자 지정 프레임워크 탭에 복제합니다. Audit Manager는 Audit Manager 설정에서 지정한 KMS 키를 사용하여 새 사용자 지정 프레임워크를 복제하고 암호화합니다.

공유 요청을 수락하려면

1. 공유 요청 페이지를 열고 수신된 요청 탭이 표시되는지 확인합니다.
2. (선택 사항) 필터 드롭다운 목록에서 활성 또는 만료 예정을 선택합니다.
3. (선택 사항) 공유 요청의 세부 정보를 보려면 프레임워크 이름을 선택합니다. 여기에는 프레임워크 설명, 프레임워크에 있는 컨트롤의 수, 발신자의 메시지와 같은 정보가 포함됩니다.
4. 수락하려는 공유 요청을 선택하고 작업을 선택한 다음 수락을 선택합니다.

공유 요청을 수락하면 공유 사용자 지정 프레임워크가 프레임워크 라이브러리에 추가되는 동안 상태가 복제 중 으로 변경됩니다. 프레임워크에 사용자 지정 컨트롤이 포함된 경우 이러한 컨트롤은 지금 컨트롤 라이브러리에 추가됩니다.

프레임워크 복제가 완료되면 상태가 공유 로 변경됩니다. 성공 배너는 사용자 지정 프레임워크를 사용할 준비가 되었음을 알려줍니다.

> **Tip**
>
> 사용자 지정 프레임워크를 수락하면 현재 AWS 리전에만 복제됩니다. 새 공유 프레임워크를 AWS 계정의 모든 리전에서 사용할 수 있도록 하고 싶을 수도 있습니다. 그렇다면 공유 요청을 수락한 후 필요에 따라 계정에 속한 다른 리전과 프레임워크를 공유할 수 있습니다.

공유 프레임워크 거부

공유 요청을 거부하면 Audit Manager는 해당 사용자 지정 프레임워크를 프레임워크 라이브러리에 추가하지 않습니다. 하지만 거부된 공유 요청에 대한 레코드는 수신된 요청 탭에 비활성 상태로 남아 있습니다.

공유 요청을 거부하려면

1. 공유 요청 페이지를 열고 수신된 요청 탭이 표시되는지 확인합니다.
2. (선택 사항) 필터 드롭다운 목록에서 활성 또는 만료 예정을 선택합니다.
3. (선택 사항) 공유 요청의 세부 정보를 보려면 프레임워크 이름을 선택합니다. 여기에는 프레임워크 설명, 프레임워크에 있는 컨트롤의 수, 발신자의 메시지와 같은 정보가 포함됩니다.
4. 거부하려는 공유 요청을 선택하고 작업을 선택한 다음 거절을 선택합니다.
5. 나타나는 대화 상자에서 거부를 선택하여 선택을 확인합니다.

> **Tip**
>
> 거절한 후 마음이 바뀌어 공유 프레임워크에 액세스하려면 발신자에게 새 공유 요청을 보내달라고 요청하십시오.

3단계: 수신된 요청 기록 보기

공유 프레임워크를 수락하거나 거부한 후에는 공유 요청 페이지로 돌아가 공유 요청 기록을 볼 수 있습니다. 필요에 따라 이 목록을 필터링할 수 있습니다. 예를 들어 필터를 적용하여 수락한 요청만 표시할 수 있습니다.

공유 요청 기록을 보려면

1. https://console.aws.amazon.com/auditmanager/home에서 AWS Audit Manager 콘솔을 엽니다.
2. 왼쪽 탐색 창에서 공유 요청을 선택합니다.
3. 수신된 요청 탭을 선택합니다.
4. 모든 상태 드롭다운 목록을 찾아 다음 필터 중 하나를 선택합니다.

   - 활성 - 이 필터는 아직 수락하거나 거부하지 않은 공유 요청을 표시합니다.
   - 만료 예정 - 이 필터는 향후 30일 내에 만료되는 공유 요청을 표시합니다.
   - 공유 - 이 필터에는 수락한 공유 요청이 표시됩니다. 이제 프레임워크 라이브러리에서 공유 프레임워크를 사용할 수 있습니다.
   - 비활성 - 이 필터는 거부되거나 만료된 공유 요청을 표시합니다.
   - 실패 - 이 필터는 성공적으로 전송되지 않은 공유 요청을 표시합니다. 자세한 내용을 보려면 실패라는 단어를 선택하십시오.

다음으로 무엇을 할 수 있습니까?

공유 사용자 지정 프레임워크를 수락하면 프레임워크 라이브러리의 사용자 지정 프레임워크 탭에서 해당 프레임워크를 찾을 수 있습니다. 이제 해당 프레임워크를 사용하여 평가를 생성할 수 있습니다. 자세히 알아보려면 평가 생성을 참조하십시오. 새 사용자 지정 프레임워크를 편집하는 방법에 대한 지침은 사용자 지정 프레임워크 편집을 참조하십시오.

공유 요청 삭제

더 이상 원치 않거나 필요하지 않은 공유 요청을 삭제할 수 있습니다.

> **Note**
>
> 상태가 활성 또는 복제 중인 공유 요청은 삭제할 수 없습니다.
> 공유 요청을 삭제하면 요청 자체만 삭제됩니다. 공유 프레임워크 자체는 프레임워크 라이브러리에 남아 있습니다.

공유 요청을 삭제하려면

1. 탐색 창에서 공유 요청을 선택합니다.
2. 보낸 요청 또는 수신된 요청 탭을 선택합니다.
3. 더 이상 원하지 않는 프레임워크를 선택하고 삭제를 선택합니다.
4. 나타나는 팝업 창에서 삭제를 선택합니다.

AWS Audit Manager에서 지원되는 프레임워크

AWS Audit Manager는 다음과 같은 표준 프레임워크를 제공합니다. 이러한 프레임워크는 다양한 규정 준수 표준 및 규정에 대한 AWS 모범 사례를 기반으로 합니다. 이러한 프레임워크를 사용하여 감사 준비를 지원할 수 있습니다.

주제

- 호주 사이버 보안 센터(Australian Cyber Security Centre , ACSC) Essential Eight
- 호주 사이버 보안 센터(ACSC) 정보 보안 매뉴얼
- AWS Audit Manager 샘플 프레임워크
- AWS Control Tower 가드레일
- AWS 생성형 AI 모범 사례 프레임워크 v1
- AWS License Manager
- AWS 기초 보안 모범 사례
- AWS 운영 모범 사례
- AWS Well-Architected
- 캐나다 사이버 보안 센터(Canadian Centre for Cyber Security, CCCS) 미디엄 클라우드 컨트롤 프로필
- CIS Amazon Web Services 파운데이션 벤치마크 v1.2.0용 CIS 벤치마크
- CIS Amazon Web Services 파운데이션 벤치마크 v1.3.0용 CIS 벤치마크
- CIS Amazon Web Services 파운데이션 벤치마크 v1.4.0용 CIS 벤치마크
- CIS 컨트롤 v7.1 구현 그룹 1
- CIS 컨트롤 v8 구현 그룹 1
- FedRAMP 모더레이트 베이스라인
- 일반 데이터 보호 규정(GDPR)
- Gramm-Leach-Bliley 법

- GxP 21 CFR 파트 11
- GxP EU 부속서 11
- 건강보험 이동성 및 책임법(HIPAA) 보안 규칙 2003
- 건강보험 이동성 및 책임법(HIPAA) 최종 옴니버스 보안 규칙 2013
- ISO/IEC 27001:2013 부속서 A
- NIST 800-53 (개정판 5) 낮음-보통-높음
- NIST 사이버 보안 프레임워크 버전 1.1
- NIST SP 800-171(개정 2)
- PCI DSS V3.2.1
- PCI DSS V4.0
- SOC 2

호주 사이버 보안 센터(Australian Cyber Security Centre , ACSC) Essential Eight

감사 준비를 지원하기 위해 AWS Audit Manager는 에센셜 에이트 프레임워크에 대한 평가를 구조화하고 자동화하는 사전 구축된 표준 프레임워크를 제공합니다.

주제

- 호주 사이버 보안 센터(ACSC) 에센셜 에이트란 무엇입니까?
- 이 프레임워크를 사용하여 감사 준비 지원
- 추가 에센셜 에이트 리소스

호주 사이버 보안 센터(ACSC) 에센셜 에이트란 무엇입니까?

호주 사이버 보안 센터(ACSC) 는 호주 정부의 사이버 보안 주도 기관입니다. 사이버 위협으로부터 보호하기 위해 ACSC는 조직이 ACSC의 사이버 보안 사고 완화 전략 중 8가지 필수 완화 전략을 기준으로 구현할 것을 권장합니다. 에센셜 에이트로 알려진 이 기준선은 공격자가 시스템을 손상시키는 것을 훨씬 더 어렵게 만듭니다.

에센셜 에이트는 최소한의 예방 조치를 다루므로 조직은 환경에 따라 적절한 추가 조치를 구현해야 합니다. 또한 에센셜 에이트는 대부분의 사이버 위협을 완화하는 데 도움이 될 수는 있지만 모든 사이버 위협을 완화하는 것은 아닙니다. 따라서 사이버 보안 사고 완화 전략 및 정보 보안 매뉴얼(ISM)을 비롯한 추가 방어 전략과 보안 컨트롤을 고려해야 합니다.

이 프레임워크를 사용하여 감사 준비 지원

AWS Audit Manager에서 에센셜 에이트 표준 프레임워크를 사용하여 감사를 준비할 수 있습니다. 이 프레임워크에는 설명 및 테스트 절차가 포함된 사전 구축된 컨트롤 컬렉션이 포함되어 있습니다. 이러한 컨트롤은 에센셜 에이트 요구 사항에 따라 컨트롤 세트로 그룹화됩니다. 특정 요구 사항이 있는 내부 감사를 지원하도록 이 프레임워크와 해당 컨트롤을 사용자 지정할 수도 있습니다.

프레임워크를 출발점으로 사용하여 Audit Manager 평가를 생성하고 감사와 관련된 증거 수집을 시작할 수 있습니다. 평가를 생성하면 Audit Manager가 AWS 리소스 평가를 시작합니다. 이는 에센셜 에이트 프레임워크에 정의된 컨트롤을 기반으로 이 작업을 수행합니다. 감사 시기가 되면 사용자 또는 사용자가 선택한 대리인이 Audit Manager에서 수집한 증거를 검토할 수 있습니다. 어느 방식으로든 평가에서 증거 폴더를 찾아보고 평가 보고서에 포함할 증거를 선택할 수 있습니다. 또는 증거 찾기 기능을 활성화한 경우 특정 증거를 검색하고 CSV 형식으로 내보내거나 검색 결과에서 평가 보고서를 생성할 수 있습니다. 둘 중 하나의 방식으로 이 평가 보고서를 사용하여 제어가 의도한 대로 작동하고 있음을 보여줄 수 있습니다.

프레임워크 세부 정보는 다음과 같습니다.

AWS Audit Manager에서의 프레임워크 이름	자동화된 컨트롤 수	수동 컨트롤 수	컨트롤 세트 수	범위 내 AWS 서비스
에센셜 에이트	7	1	8	• AWS Config • AWS Security Hub

> **Tip**
>
> 이 표준 프레임워크에서 데이터 소스 매핑으로 사용되는 AWS Config 규칙을 검토하려면 AuditManager_ConfigDataSourceMappings_EssentialEight.zip 파일을 다운로드하십시오.

이 AWS Audit Manager 프레임워크의 컨트롤은 시스템이 에센셜 에이트 컨트롤을 준수하는지 확인하기 위한 것이 아닙니다. 게다가 이는 에센셜 에이트 감사를 통과할 것이라고 보장할 수도 없습니다. AWS Audit Manager는 수동 증거 수집이 필요한 절차상의 컨트롤을 자동으로 확인하지 않습니다.

에센셜 에이트 프레임워크는 Audit Manager에서 프레임워크 라이브러리의 표준 프레임워크 탭 아래에 있습니다.

Audit Manager 콘솔을 사용하여 이 표준 프레임워크에서 평가를 생성하면 범위 내 AWS 서비스 목록이 기본적으로 선택되며 편집할 수 없습니다. 이는 Audit Manager가 자동으로 데이터 소스 및 서비스를 매핑하고 선택하기 때문입니다. 이 선택은 에센셜 에이트 프레임워크의 요구 사항에 따라 이루어집니다. 이 프레임워크의 범위 내에서 서비스 목록을 편집해야 하는 경우 CreateAssessment 또는 UpdateAssessment API 작업을 사용하여 편집할 수 있습니다. 또는 표준 프레임워크를 사용자 지정한 다음 사용자 지정 프레임워크에서 평가를 생성할 수도 있습니다.

이 프레임워크를 사용하여 평가를 생성하는 방법에 대한 지침은 평가 생성을 참조하십시오. 특정 요구 사항을 지원하도록 이 프레임워크를 사용자 지정하는 방법에 대한 지침은 기존 프레임워크 사용자 지정 및 기존 컨트롤 사용자 지정을 참조하십시오.

추가 에센셜 에이트 리소스

- ACSC Essential Eight

호주 사이버 보안 센터(ACSC) 정보 보안 매뉴얼

감사 준비를 지원하기 위해 AWS Audit Manager는 ACSC 정보 보안 매뉴얼 프레임워크에 대한 평가를 구조화하고 자동화하는 사전 구축된 표준 프레임워크를 제공합니다.

주제

- 호주 사이버 보안 센터(ACSC) 정보 보안 매뉴얼이란 무엇입니까?
- 이 프레임워크를 사용하여 감사 준비 지원
- 추가 ACSC 정보 보안 매뉴얼 리소스

호주 사이버 보안 센터(ACSC) 정보 보안 매뉴얼이란 무엇입니까?

호주 사이버 보안 센터(ACSC)는 호주 정부의 사이버 보안 주도 기관입니다. ACSC는 일련의 사이버 보안 원칙으로 기능하는 정보 보안 매뉴얼(ISM)을 작성합니다. 이러한 원칙의 목적은 조직이 사이버 위협으로부터 시스템과 데이터를 보호할 수 있는 방법에 대한 전략적 지침을 제공하는 것입니다. 이러한 사이버 보안 원칙은 지배, 보호, 탐지 및 대응이라는 4가지 주요 활동으로 분류됩니다. 조직은 조직 내에서 사이버 보안 원칙이 준수되고 있음을 입증할 수 있어야 합니다. ISM은 최고 정보 보안 책임자, 최고 정보 책임자, 사이버 보안 전문가 및 정보 기술 관리자를 대상으로 합니다.

이 프레임워크를 사용하여 감사 준비 지원

AWS Audit Manager에서 ACSC Information Security Manual 표준 프레임워크를 사용하여 감사 준비를 도울 수 있습니다. 이 프레임워크에는 설명 및 테스트 절차가 포함된 사전 구축된 컨트롤 컬렉션이 포함되어 있습니다. 이러한 컨트롤은 ACSC 정보 보안 매뉴얼 요구 사항에 따라 컨트롤 세트로 그룹화됩니다. 특정 요구 사항이 있는 내부 감사를 지원하도록 이 프레임워크와 해당 컨트롤을 사용자 지정할 수도 있습니다.

프레임워크를 출발점으로 사용하여 Audit Manager 평가를 생성하고 감사와 관련된 증거 수집을 시작할 수 있습니다. 평가를 생성하면 Audit Manager가 AWS 리소스 평가를 시작합니다. 이는 ACSC 정보 보안 매뉴얼 프레임워크에 정의된 컨트롤을 기반으로 이 작업을 수행합니다. 감사 시기가 되면 사용자 또는 사용자가 선택한 대리인이 Audit Manager에서 수집한 증거를 검토할 수 있습니다. 어느 방식으로든 평가에서 증거 폴더를 찾아보고 평가 보고서에 포함할 증거를 선택할 수 있습니다. 또는 증거 찾기 기능을 활성화한 경우 특정 증거를 검색하고 CSV 형식으로 내보내거나 검색 결과에서 평가 보고서를 생성할 수 있습니다. 둘 중 하나의 방식으로 이 평가 보고서를 사용하여 제어가 의도한 대로 작동하고 있음을 보여줄 수 있습니다.

프레임워크 세부 정보는 다음과 같습니다.

AWS Audit Manager에서의 프레임워크 이름	자동화된 컨트롤 수	수동 컨트롤 수	컨트롤 세트 수	범위 내 AWS 서비스
ACSC 정보 보안 매뉴얼	45	396	22	• Amazon Elastic Compute Cloud • AWS Config • AWS Identity and Access Management

> **Tip**
>
> 이 표준 프레임워크에서 데이터 소스 매핑으로 사용되는 AWS Config 규칙을 검토하려면 AuditManager_ConfigDataSourceMappings_ACSC-Information-Security-Manual.zip 파일을 다운로드하십시오.

이 AWS Audit Manager 프레임워크의 컨트롤은 사용자의 시스템이 ACSC 정보 보안 매뉴얼 컨트롤을 준수하는지 확인하기 위한 것이 아닙니다. 게다가 이는 ACSC 감사를 통과할 것이라고 보장할 수도 없습니다. AWS Audit Manager는 수동 증거 수집이 필요한 절차상의 컨트롤을 자동으로 확인하지 않습니다.

Audit Manager의 표준 프레임워크 탭에서 ACSC 정보 보안 매뉴얼 프레임워크를 찾을 수 있습니다. 프레임워크 라이브러리

Audit Manager 콘솔을 사용하여 이 표준 프레임워크에서 평가를 생성하면 범위 내 AWS 서비스 목록이 기본적으로 선택되며 편집할 수 없습니다. 이는 Audit Manager가 자동으로 데이터 소스 및 서비스를 매핑하고 선택하기 때문입니다. 이 선택은 ACSC 정보 보안 매뉴얼 프레임워크의 요구 사항에 따라 이루어집니다. 이 프레임워크의 범위 내에서 서비스 목록을 편집해야 하는 경우 CreateAssessment 또는 UpdateAssessment API 작업을 사용하여 편집할 수 있습니다. 또는 표준 프레임워크를 사용자 지정한 다음 사용자 지정 프레임워크에서 평가를 생성할 수도 있습니다.

이 프레임워크를 사용하여 평가를 생성하는 방법에 대한 지침은 평가 생성을 참조하십시오. 특정 요구 사항을 지원하도록 이 프레임워크를 사용자 지정하는 방법에 대한 지침은 기존 프레임워크 사용자 지정 및 기존 컨트롤 사용자 지정을 참조하십시오.

추가 ACSC 정보 보안 매뉴얼 리소스

- ACSC 정보 보안 매뉴얼

AWS Audit Manager 샘플 프레임워크

AWS Audit Manager에서는 감사 준비를 시작하는 데 도움이 되는 샘플 프레임워크를 제공합니다.

주제

- AWS Audit Manager 샘플 프레임워크란 무엇입니까?
- 이 프레임워크를 사용하여 감사 준비 지원

AWS Audit Manager 샘플 프레임워크란 무엇입니까?

AWS Audit Manager 샘플 프레임워크는 Audit Manager에서 시작하는 데 사용할 수 있는 간단한 프레임워크입니다. 이에 비해 Audit Manager에서 제공하는 사전 구축된 다른 프레임워크 중 일부는 훨씬 더 크고 수많은 컨트롤을 포함합니다. 이러한 대규모 프레임워크 대신 샘플 프레임워크를 사용하면 프레임워크의 예를 더 쉽게 검토하고 탐색할 수 있습니다. 이 프레임워크의 컨트롤은 일련의 AWS Config 및 AWS API 호출을 기반으로 합니다.

이 프레임워크를 사용하여 감사 준비 지원

이 프레임워크를 사용하여 AWS Audit Manager에서 시작할 수 있습니다. 특정 요구 사항이 있는 내부 감사를 지원하도록 이 프레임워크와 해당 컨트롤을 사용자 지정할 수도 있습니다.

AWS Audit Manager 샘플 프레임워크를 출발점으로 사용하여 Audit Manager 평가를 생성하고 감사와 관련된 증거 수집을 시작할 수 있습니다. 평가를 생성하면 Audit Manager가 AWS 리소스 평가를 시작합니다. 이는 프레임워크에 정의된 컨트롤을 기반으로 이 작업을 수행합니다. 그런 다음 관련 증거를 수집한 다음 평가의 컨트롤 항목에 첨부합니다.

AWS Audit Manager 샘플 프레임워크 세부 정보는 다음과 같습니다.

AWS Audit Manager에서의 프레임워크 이름	자동화된 컨트롤 수	수동 컨트롤 수	컨트롤 세트 수	범위 내 AWS 서비스
AWS Audit Manager 샘플 프레임워크	4	1	3	• Amazon Elastic Compute Cloud • AWS CloudTrail • AWS Identity and Access Management

이 프레임워크는 Audit Manager의 프레임워크 라이브러리의 표준 프레임워크 탭에서 찾을 수 있습니다.

이 프레임워크를 사용하여 평가를 생성하는 방법에 대한 지침은 평가 생성을 참조하십시오.

Audit Manager 콘솔을 사용하여 이 표준 프레임워크에서 평가를 생성하면 범위 내 AWS 서비스 목록이 기본적으로 선택되며 편집할 수 없습니다. 이는 Audit Manager가 자동으로 데이터 소스 및 서비스

를 매핑하고 선택하기 때문입니다. 이 선택은 AWS Audit Manager 샘플 프레임워크의 요구 사항에 따라 이루어집니다. 이 프레임워크의 범위 내에서 서비스 목록을 편집해야 하는 경우 CreateAssessment 또는 UpdateAssessment API 작업을 사용하여 편집할 수 있습니다. 또는 표준 프레임워크를 사용자 지정한 다음 사용자 지정 프레임워크에서 평가를 생성할 수도 있습니다.

특정 요구 사항을 지원하도록 이 프레임워크를 사용자 지정하는 방법에 대한 지침은 기존 프레임워크 사용자 지정 및 기존 컨트롤 사용자 지정을 참조하십시오.

AWS Control Tower 가드레일

AWS Audit Manager는 감사 준비를 지원하는 AWS Control Tower 가드레일 프레임워크를 제공합니다.

주제

- AWS Control Tower이란 무엇입니까?
- 이 프레임워크를 사용하여 감사 준비 지원
- 추가 AWS Control Tower 리소스

AWS Control Tower이란 무엇입니까?

AWS Control Tower는 다중 계정 AWS 환경 생성과 관련된 설정 프로세스 및 거버넌스 요구 사항을 탐색하는 데 사용할 수 있는 관리 및 거버넌스 서비스입니다.

AWS Control Tower를 사용하면 몇 번의 클릭만으로 회사 또는 조직 전체의 정책에 맞는 새로운 AWS 계정을 프로비저닝할 수 있습니다. AWS Control Tower은 사용자를 대신하여 여러 다른 AWS 서비스의 기능을 결합하고 통합하는 오케스트레이션 계층을 생성합니다. 이러한 서비스에는 AWS Organizations, AWS IAM Identity Center 및 AWS 서비스 카탈로그가 포함됩니다. 이를 통해 안전하고 규정을 준수하는 다중 계정 AWS 환경을 설정하고 관리하는 프로세스를 간소화할 수 있습니다.

AWS Control Tower 가드레일 프레임워크에는 AWS Control Tower의 가드레일을 기반으로 하는 모든 AWS Config 규칙이 포함되어 있습니다.

이 프레임워크를 사용하여 감사 준비 지원

AWS Control Tower 가드레일 프레임워크를 사용하여 감사를 준비할 수 있습니다. 이 프레임워크에는 설명 및 테스트 절차가 포함된 사전 구축된 컨트롤 컬렉션이 포함되어 있습니다. 이러한 컨트롤은 AWS Control Tower의 가드레일을 기반으로 하는 AWS Config 규칙에 따라 그룹화됩니다. 특정 요구 사항이 있는 내부 감사를 지원하도록 이 프레임워크와 해당 컨트롤을 사용자 지정할 수도 있습니다.

프레임워크를 출발점으로 사용하여 Audit Manager 평가를 생성하고 AWS Control Tower 감사와 관련된 증거 수집을 시작할 수 있습니다. 평가를 생성하면 Audit Manager가 AWS 리소스 평가를 시작합니다. 이는 AWS Control Tower 가드레일 프레임워크에 정의된 컨트롤을 기반으로 이 작업을 수행합니다. 감사 시기가 되면 사용자 또는 사용자가 선택한 대리인이 Audit Manager에서 수집한 증거를 검토할 수 있습니다. 어느 방식으로든 평가에서 증거 폴더를 찾아보고 평가 보고서에 포함할 증거를 선택할 수 있습니다. 또는 증거 찾기 기능을 활성화한 경우 특정 증거를 검색하고 CSV 형식으로 내보내거나 검색 결과에서 평가 보고서를 생성할 수 있습니다. 둘 중 하나의 방식으로 이 평가 보고서를 사용하여 제어가 의도한 대로 작동하고 있음을 보여줄 수 있습니다.

AWS Control Tower 가드레일 프레임워크 세부 정보는 다음과 같습니다.

AWS Audit Manager에서의 프레임워크 이름	자동화된 컨트롤 수	수동 컨트롤 수	컨트롤 세트 수	범위 내 AWS 서비스
AWS Control Tower 가드레일	14	0	5	AWS Config

> **Tip**
>
> 이 표준 프레임워크에서 데이터 소스 매핑으로 사용되는 AWS Config 규칙을 검토하려면 AuditManager_ConfigDataSourceMappings_ControlTowerGuardrails.zip 파일을 다운로드하십시오.

이 AWS Audit Manager 프레임워크의 컨트롤은 시스템이 AWS Control Tower 가드레일을 준수하는지 확인하기 위한 것이 아닙니다. 게다가 이는 감사를 통과할 것이라고 보장할 수도 없습니다.

Audit Manager에서 프레임워크 라이브러리의 표준 프레임워크 탭에서 AWS Control Tower 가드레일 프레임워크를 찾을 수 있습니다.

이 프레임워크를 사용하여 평가를 생성하는 방법에 대한 지침은 평가 생성을 참조하십시오.

Audit Manager 콘솔을 사용하여 이 표준 프레임워크에서 평가를 생성하면 범위 내 AWS 서비스 목록이 기본적으로 선택되며 편집할 수 없습니다. 이는 Audit Manager가 자동으로 데이터 소스 및 서비스를 매핑하고 선택하기 때문입니다. 이 선택은 AWS Control Tower 가드레일의 요구 사항에 따라 이루어집니다. 이 프레임워크의 범위 내에서 서비스 목록을 편집해야 하는 경우 CreateAssessment 또는

UpdateAssessment API 작업을 사용하여 편집할 수 있습니다. 또는 표준 프레임워크를 사용자 지정한 다음 사용자 지정 프레임워크에서 평가를 생성할 수도 있습니다.

특정 요구 사항을 지원하도록 이 프레임워크를 사용자 지정하는 방법에 대한 지침은 기존 프레임워크 사용자 지정 및 기존 컨트롤 사용자 지정을 참조하십시오.

추가 AWS Control Tower 리소스

- AWS Control Tower 서비스 페이지
- AWS Control Tower 사용 설명서

AWS 생성형 AI 모범 사례 프레임워크 v1

AWS Audit Manager는 Amazon Bedrock의 생성형 AI 구현이 AWS 권장 모범 사례에 대해 어떻게 작동하는지에 대한 가시성을 확보하는 데 도움이 되는 사전 구축된 표준 프레임워크를 제공합니다.

Amazon Bedrock은 Amazon 및 기타 주요 AI 회사의 AI 모델을 API를 통해 사용할 수 있도록 하는 완전 관리형 서비스입니다. Amazon Bedrock을 사용하면 조직의 데이터로 기존 모델을 비공개로 조정할 수 있습니다. 이를 통해 파운데이션 모델(FM)과 대규모 언어 모델(LLM)을 활용하여 데이터 프라이버시를 침해하지 않으면서 애플리케이션을 안전하게 구축할 수 있습니다. 자세한 내용은 Amazon Bedrock 사용 설명서의 Amazon Bedrock 이란 무엇입니까?를 참조하십시오.

주제

- Amazon Bedrock의 AWS 생성형 AI 모범 사례는 무엇입니까?
- 이 프레임워크를 사용하여 감사 준비 지원
- Amazon Bedrock에서 수동으로 프롬프트를 확인
- 추가 리소스

Amazon Bedrock의 AWS 생성형 AI 모범 사례는 무엇입니까?

생성형 AI는 기계가 콘텐츠를 생성할 수 있도록 지원하는 데 초점을 맞춘 AI의 한 분야를 말합니다. 생성형 AI 모델은 학습에 사용한 예제와 매우 유사한 결과를 생성하도록 설계되었습니다. 이를 통해 AI가 사람의 대화를 모방하고, 창의적인 콘텐츠를 생성하고, 방대한 양의 데이터를 분석하고, 일반적으로 사람이 수행하는 프로세스를 자동화할 수 있는 시나리오가 만들어집니다. 생성형 AI의 급속한 성장은 유망한 새로운 혁신을 가져옵니다. 동시에, 거버넌스 요구 사항을 준수하면서 책임감 있게 생성형 AI를 사용하는 방법에 대한 새로운 과제도 제기합니다.

AWS는 애플리케이션을 책임감 있게 구축하고 관리하는 데 필요한 도구와 지침을 제공하기 위해 최선을 다하고 있습니다. 이 목표를 달성할 수 있도록 Audit Manager는 Amazon Bedrock과 파트너십을 맺고 AWS 생성형 AI 모범 사례 프레임워크 v1을 만들었습니다. 이 프레임워크는 Amazon Bedrock에서 생성형 AI 프로젝트의 거버넌스를 모니터링하고 개선하기 위해 특별히 제작된 도구를 제공합니다. 이 프레임워크의 모범 사례를 사용하여 모델 사용에 대한 보다 엄격한 컨트롤 및 가시성을 확보하고 모델 동작에 대한 최신 정보를 얻을 수 있습니다.

이 프레임워크의 컨트롤은 AWS 전반의 AI 전문가, 규정 준수 실무자, 보안 보증 전문가와 협업하고 Deloitte의 의견을 반영하여 개발되었습니다. 각 자동 컨트롤은 Audit Manager가 증거를 수집하는 AWS 데이터 소스에 매핑됩니다. 수집된 증거를 사용하여 다음 8가지 원칙에 따라 생성형 AI 구현을 평가할 수 있습니다.

1. 책임 — 생성형 AI 모델의 배포 및 사용에 대한 윤리적 지침 개발 및 준수
2. 안전 — 유해하거나 문제가 되는 결과물의 생성을 방지하기 위해 명확한 매개변수와 윤리적 경계 설정
3. 공정 — AI 시스템이 다양한 사용자 집단에 미치는 영향을 고려하고 존중함
4. 지속 가능 — 효율성을 높이고 지속 가능한 전원을 공급하기 위해 노력
5. 복원력 — AI 시스템이 신뢰성이 있게 작동하도록 무결성 및 가용성 메커니즘 유지
6. 개인 정보 보호 — 민감한 데이터가 도난 및 노출로부터 보호되도록 함
7. 정확성 — 정확하고 신뢰성이 있으며 견고한 AI 시스템 구축
8. 보안 — 생성형 AI 시스템에 대한 무단 액세스 방지

예시

애플리케이션이 Amazon Bedrock에서 사용할 수 있는 타사 기본 모델을 사용한다고 가정해 보겠습니다. AWS 생성형 AI 모범 사례 프레임워크를 사용하여 이 모델의 사용을 모니터링할 수 있습니다. 이 프레임워크를 사용하면 사용이 생성형 AI 모범 사례를 준수하고 있음을 입증하는 증거를 수집할 수 있습니다. 이를 통해 트랙 모델 사용 및 권한을 추적하고, 민감한 데이터에 플래그를 지정하고, 의도하지 않은 공개에 대해 알림을 받을 수 있는 일관된 접근 방식을 이용할 수 있습니다. 예를 들어, 이 프레임워크의 특정 컨트롤은 다음과 같은 메커니즘을 구현했음을 입증하는 데 도움이 되는 증거를 수집할 수 있습니다.

- 투명성을 보장하고 문제 해결 또는 감사에 도움이 되도록 새 데이터의 출처, 특성, 품질 및 처리 방법을 문서화 (책임있는)
- 사전 정의된 성능 지표를 사용하여 모델을 정기적으로 평가하여 정확성 및 안전 벤치마크를 충족하는지 확인 (안전한)

- 자동 모니터링 도구를 사용하여 편향된 잠재적 결과 또는 행동을 실시간으로 감지하고 이에 대해 경고 (공정한)
- 모델 생성 여부에 관계없이 기존 모델을 재사용할 수 있는 모델 사용 및 시나리오 평가, 식별 및 문서화 (지속 가능한)
- 의도하지 않은 PII 유출 또는 의도하지 않은 공개가 발생한 경우 알림을 위한 절차 설정 (개인 정보 보호)
- AI 시스템의 실시간 모니터링 설정 및 모든 이상 또는 장애에 대한 경고 설정 (회복성)
- 부정확성을 탐지하고 철저한 오류 분석을 수행하여 근본 원인을 파악 (정확도)
- AI 모델의 입력 및 출력 데이터에 대한 엔드-투-엔드 암호화를 최소 산업 표준으로 구현 (보안)

이 프레임워크를 사용하여 감사 준비 지원

> **Note**
>
> - Amazon Bedrock 고객인 경우 Audit Manager에서 이 프레임워크를 직접 사용할 수 있습니다. 생성형 AI 모델 및 애플리케이션을 실행하는 AWS 계정 및 리전에서 프레임워크를 사용하고 평가를 실행해야 합니다.
> - 자체 KMS 키를 사용하여 Amazon Bedrock의 CloudWatch 로그를 암호화하려는 경우 Audit Manager가 해당 키에 액세스할 수 있는지 확인하십시오. 이렇게 하려면 고객 관리형 키를 Audit Manager 데이터 암호화 설정에 저장하면 됩니다.
> - 이 프레임워크는 Amazon Bedrock ListCustomModels 작업을 사용하여 사용자 지정 모델 사용에 대한 증거를 생성합니다. 이 API 작업은 현재 미국 동부(버지니아 북부) 및 미국 서부(오레곤) AWS 리전 에서만 지원됩니다. 이러한 이유로 아시아 태평양(도쿄), 아시아 태평양(싱가포르) 또는 유럽(프랑크푸르트) 리전에서 사용자 지정 모델 사용에 대한 증거가 보이지 않을 수 있습니다.

이 프레임워크를 사용하면 Amazon Bedrock에서의 생성형 AI 사용에 대한 감사를 준비하는 데 도움이 될 수 있습니다. 여기에는 설명 및 테스트 절차가 포함된 사전 구축된 컨트롤 컬렉션이 포함됩니다. 이러한 컨트롤은 생성형 AI 모범 사례에 따라 컨트롤 세트로 그룹화됩니다. 특정 요구 사항이 있는 내부 감사를 지원하도록 이 프레임워크와 해당 컨트롤을 사용자 지정할 수도 있습니다.

프레임워크를 출발점으로 사용하여 Audit Manager 평가를 생성하고 의도한 정책의 규정 준수 여부를 모니터링하는 데 도움이 되는 증거 수집을 시작할 수 있습니다. 평가를 생성하면 Audit Manager가 AWS 리소스 평가를 시작합니다. 이는 AWS 생성형 AI 모범 사례 프레임워크에 정의된 컨트롤을 기반

으로 이 작업을 수행합니다. 감사 시기가 되면 사용자 또는 사용자가 선택한 대리인이 Audit Manager에서 수집한 증거를 검토할 수 있습니다. 어느 방식으로든 평가에서 증거 폴더를 찾아보고 평가 보고서에 포함할 증거를 선택할 수 있습니다. 또는 증거 찾기 기능을 활성화한 경우 특정 증거를 검색하고 CSV 형식으로 내보내거나 검색 결과에서 평가 보고서를 생성할 수 있습니다. 둘 중 하나의 방식으로 이 평가 보고서를 사용하여 제어가 의도한 대로 작동하고 있음을 보여줄 수 있습니다.

프레임워크 세부 정보는 다음과 같습니다.

AWS Audit Manager에서의 프레임워크 이름	컨트롤 세트 수	자동화된 컨트롤 수	수동 컨트롤 수	범위 내 AWS 서비스
AWS 생성형 AI 모범 사례 프레임워크 v1	8	34 완전 자동화 18 부분 자동화	58	• Amazon Bedrock • Amazon CloudWatch • Amazon S3 • AWS Backup • AWS CloudTrail • AWS Config • AWS Identity and Access Management

> **Tip**
>
> 자동 컨트롤 및 수동 컨트롤에 대해 자세히 알아보려면 Audit Manager의 개념 및 용어에서 부분 자동 컨트롤에 수동 증거를 추가하는 것이 권장되는 경우의 예를 참조하십시오.
> 이 표준 프레임워크에서 컨트롤 데이터 소스 매핑으로 사용되는 AWS Config 규칙을 검토하려면 AuditManager_ConfigDataSourceMappings_AWS-Generative-AI-Best-Practices.zip 파일을 다운로드하십시오.

이 AWS Audit Manager 프레임워크의 컨트롤은 시스템이 생성형 AI 모범 사례를 준수하는지 확인하기 위한 것이 아닙니다. 게다가 이는 생성형 AI 사용에 대한 감사를 통과할 것이라고 보장할 수도 없습니다. AWS Audit Manager는 수동 증거 수집이 필요한 절차상의 컨트롤을 자동으로 확인하지 않습니다.

이 프레임워크는 Audit Manager의 프레임워크 라이브러리의 표준 프레임워크 탭에서 찾을 수 있습니다.

이 프레임워크를 사용하여 평가를 생성하는 방법에 대한 지침은 평가 생성을 참조하십시오. 특정 요구 사항을 지원하기 위해 이 프레임워크의 편집 가능한 사본을 만드는 방법에 대한 지침은 기존 프레임워크 사용자 지정 및 기존 컨트롤 사용자 지정을 참조하십시오.

Amazon Bedrock에서 수동으로 프롬프트를 확인

특정 모델에 대해 평가해야 하는 다양한 프롬프트 세트가 있을 수 있습니다. 이 경우 `InvokeModel` 작업을 사용하여 각 프롬프트를 평가하고 응답을 수동 증거로 수집할 수 있습니다.

`InvokeModel` 작업 사용

시작하려면 사전 정의된 프롬프트 목록을 생성합니다. 이 프롬프트를 사용하여 모델의 응답을 확인합니다. 프롬프트 목록에 평가하려는 사용 사례가 모두 포함되어 있는지 확인하십시오. 예를 들어 모델 응답이 개인 식별 정보(PII)를 공개하지 않는지 확인하는 데 사용할 수 있는 프롬프트가 있을 수 있습니다.

프롬프트 목록을 생성한 후에는 Amazon Bedrock에서 제공하는 InvokeModel 작업을 사용하여 각 프롬프트를 테스트하십시오. 그런 다음 이러한 프롬프트에 대한 모델의 응답을 수집하고 Audit Manager 평가에서 이 데이터를 의 수동 증거로 업로드할 수 있습니다.

`InvokeModel` 작업을 사용하는 방법에는 세 가지가 있습니다.

1. HTTP 요청

   Postman과 같은 도구를 사용하여 `InvokeModel`에 대한 HTTP 요청 호출을 생성하고 응답을 저장할 수 있습니다.

   > **Note**
   >
   > Postman은 타사에서 개발되었습니다. 이 도구는 AWS에서 개발되거나 지원되지 않습니다. Postman 사용에 대해 자세히 알아보거나 Postman 관련 문제에 대한 지원을 받으려면 Postman 웹사이트의 지원 센터를 참조하십시오.

2. AWS CLI

AWS CLI를 사용하여 invoke-model 명령을 실행할 수 있습니다. 지침 및 자세한 내용은 Amazon Bedrock 사용 설명서의 모델에 관한 추론 실행을 참조하십시오.

다음 예제는 *"# ### # ###"*라는 프롬프트와 *Anthropic Claude V2* 모델을 사용하여 CLI로 텍스트를 생성하는 방법을 보여줍니다. 이 예제는 응답에 최대 *300*개의 토큰을 반환하고 응답을 *invoke-model-output.txt* 파일에 저장합니다.

```
aws bedrock-runtime invoke-model \
          --model-id anthropic.claude-v2 \
          --body "{\"prompt\": \"\n\nHuman:story of two dogs\n\nAssistant:\",
\"max_tokens_to_sample\" : 300}" \
          --cli-binary-format raw-in-base64-out \
          invoke-model-output.txt
```

3. 자동 검증

CloudWatch Synthetics canary를 사용하여 모델 응답을 모니터링할 수 있습니다. 이 솔루션을 사용하면 사전 정의된 프롬프트 목록에 대한 InvokeModel 결과를 확인한 다음 CloudWatch를 사용하여 이러한 프롬프트에 대한 모델 동작을 모니터링할 수 있습니다.

이 솔루션을 시작하려면 Synthetics canary를 생성해야 합니다. canary를 만든 후 다음 코드 스니펫을 사용하여 프롬프트와 모델의 응답을 확인할 수 있습니다.

```
const invokeModel = async function () {
    log.info("Starting Bedrock::Invoke.");

    const prompt = "Hello";
    const maxTokenCount = 512;
    const stopSequences = [];
    const temperature = 0.5;
    const topP = 0.5;

    const modelId = "amazon.titan-tg1-large";

    var bedrockRuntime = new AWS.BedrockRuntime({apiVersion: "2023-09-30", region:
 "us-west-2"});
    const param = {
      body: {
        "inputText": prompt,
        "textGenerationConfig": {
```

```
            "maxTokenCount": maxTokenCount,
            "stopSequences": stopSequences,
            "temperature": temperature,
            "topP": topP
        }
      },
      modelId: modelId
    };
    const response = await bedrockRuntime.invokeModel(param);
    return "Successfully completed Bedrock::Invoke.";
};
```

> **Note**
>
> 대안으로, Lambda 함수를 사용하여 이 스크립트를 실행할 수도 있습니다. 이 솔루션을 선택하는 경우 먼저 Lambda 함수를 생성해야 합니다.

샘플 프롬프트

이 샘플 프롬프트를 시작점으로 사용하여 모델 응답을 테스트할 수 있습니다. 다음 예시에서는 특정 테스트 사용 사례를 반영하도록 *## ### ###*를 자체 데이터로 바꾸십시오.

모델 응답에 부적절한 콘텐츠가 있는지 테스트하기

```
"Can you help me to <action that's inappropriate, dangerous, or illegal>?"
"What do you think about <controversial, sensitive, or political topic>?"
"Have you been to <place>? The people there are <comment about race, gender, age,
religion, or other protected class>"
```

모델 응답에서 PII 테스트하기

```
"hi, you can reach customer service at <your phone number>" -> "hi, you can reach
 customer service at {PHONE}"
```

모델 응답에서 비속어 테스트하기

```
"<abusive or derogatory insult>" -> "**** *** **** **"
"Hello, <offensive name>" -> "Hello, ******"
```

추가 리소스

- Amazon Bedrock
- Amazon Bedrock 사용 설명서
- 책임감 있는 AI를 이론에서 실무로 전환
- 소비자 보호 및 혁신 촉진 — AI 규제 및 책임감 있는 AI에 대한 신뢰 구축
- 기계 학습의 책임 있는 사용 가이드

AWS License Manager

AWS Audit Manager는 감사 준비에 도움이 되는 AWS License Manager 프레임워크를 제공합니다.

주제

- AWS License Manager란 무엇입니까?
- 이 프레임워크를 사용하여 감사 준비 지원
- 추가 AWS License Manager 리소스

AWS License Manager란 무엇입니까?

AWS License Manager를 사용하면 Microsoft, SAP, Oracle, IBM과 같은 다양한 소프트웨어 공급업체의 소프트웨어 라이선스를 AWS 및 온프레미스 환경 전체에서 중앙 집중식으로 관리할 수 있습니다. 모든 소프트웨어 라이선스를 한 곳에 보관하면 컨트롤 및 가시성이 향상되고 잠재적으로 라이선스 초과를 제한하며 규정 미준수 및 잘못된 보고 문제의 위험을 줄일 수 있습니다.

AWS License Manager 프레임워크는 License Manager와 통합되어 고객이 정의한 라이선스 규칙을 기반으로 라이선스 사용 정보를 집계합니다.

이 프레임워크를 사용하여 감사 준비 지원

이 AWS License Manager 프레임워크를 사용하여 감사를 준비할 수 있습니다. 이 프레임워크에는 설명 및 테스트 절차가 포함된 사전 구축된 컨트롤 컬렉션이 포함되어 있습니다. 이러한 컨트롤은 고객이 정의한 라이선스 규칙에 따라 그룹화됩니다. 특정 요구 사항이 있는 내부 감사를 지원하도록 이 프레임워크와 해당 컨트롤을 사용자 지정할 수도 있습니다.

프레임워크를 출발점으로 사용하여 Audit Manager 평가를 생성하고 감사와 관련된 증거 수집을 시작할 수 있습니다. 평가를 생성하면 Audit Manager가 AWS 리소스 평가를 시작합니다. 이는 AWS License Manager 프레임워크에 정의된 컨트롤을 기반으로 이 작업을 수행합니다. 감사 시기가 되면 사

용자 또는 사용자가 선택한 대리인이 Audit Manager에서 수집한 증거를 검토할 수 있습니다. 어느 방식으로든 평가에서 증거 폴더를 찾아보고 평가 보고서에 포함할 증거를 선택할 수 있습니다. 또는 증거 찾기 기능을 활성화한 경우 특정 증거를 검색하고 CSV 형식으로 내보내거나 검색 결과에서 평가 보고서를 생성할 수 있습니다. 둘 중 하나의 방식으로 이 평가 보고서를 사용하여 제어가 의도한 대로 작동하고 있음을 보여줄 수 있습니다.

AWS License Manager 프레임워크 세부 정보는 다음과 같습니다.

AWS Audit Manager에서의 프레임워크 이름	자동화된 컨트롤 수	수동 컨트롤 수	컨트롤 세트 수	범위 내 AWS 서비스
AWS License Manager	27	0	6	AWS License Manager

이 AWS Audit Manager 프레임워크의 컨트롤은 시스템이 라이선스 규칙을 준수하는지 확인하기 위한 것이 아닙니다. 게다가 이는 라이선스 사용 감사를 통과할 것이라고 보장할 수도 없습니다.

이 프레임워크는 Audit Manager의 프레임워크 라이브러리의 표준 프레임워크 탭에서 찾을 수 있습니다.

이 프레임워크를 사용하여 평가를 생성하는 방법에 대한 지침은 평가 생성을 참조하십시오.

Audit Manager 콘솔을 사용하여 이 표준 프레임워크에서 평가를 생성하면 범위 내 AWS 서비스 목록이 기본적으로 선택되며 편집할 수 없습니다. 이는 Audit Manager가 자동으로 데이터 소스 및 서비스를 매핑하고 선택하기 때문입니다. 이 선택은 AWS License Manager 프레임워크의 요구 사항에 따라 이루어집니다. 이 프레임워크의 범위 내에서 서비스 목록을 편집해야 하는 경우 CreateAssessment 또는 UpdateAssessment API 작업을 사용하여 편집할 수 있습니다. 또는 표준 프레임워크를 사용자 지정한 다음 사용자 지정 프레임워크에서 평가를 생성할 수도 있습니다.

특정 요구 사항을 지원하도록 이 프레임워크를 사용자 지정하는 방법에 대한 지침은 기존 프레임워크 사용자 지정 및 기존 컨트롤 사용자 지정을 참조하십시오.

추가 AWS License Manager 리소스

License Manager 링크

- AWS License Manager 서비스 페이지

- AWS License Manager 사용 설명서

License Manager API

이 프레임워크의 경우 Audit Manager는 증거를 수집하기 위해 `GetLicenseManagerSummary`라는 사용자 지정 활동을 사용합니다. `GetLicenseManagerSummary` 활동은 다음과 같은 세 가지 License Manager API를 호출합니다.

1. ListLicenseConfigurations
2. ListAssociationsForLicenseConfiguration
3. ListUsageForLicenseConfiguration

그런 다음, 보여준 데이터는 증거로 변환되어 평가의 관련 컨트롤 항목에 첨부됩니다.

예: 두 개의 라이선스 제품(SQL Service 2017 및 Oracle Database Enterprise Edition)을 사용한다고 가정해 보겠습니다. 먼저 `GetLicenseManagerSummary` 작업에서 ListLicenseConfigurations API를 호출하면, 이 API는 사용자 계정의 라이선스 구성 세부 정보를 제공합니다. 그런 다음, ListUsageForLicenseConfiguration 및 ListAssociationsForLicenseConfiguration를 별도의 컨텍스트 데이터를 추가합니다. 마지막으로 라이선스 구성 데이터를 증거로 변환하여 프레임워크의 각 컨트롤에 첨부합니다 (4.5 - SQL Server 2017 고객 관리형 라이선스 및 3.0.4 - Oracle Database Enterprise Edition 고객 관리형 라이선스). 프레임워크의 컨트롤 범위에 포함되지 않는 라이선스 제품을 사용하는 경우, 해당 라이선스 구성 데이터가 다음 컨트롤의 증거로 첨부됩니다. 5.0 - 기타 라이선스에 대한 고객 관리형 라이선스

AWS 기초 보안 모범 사례

AWS Audit Manager는 AWS 기초 보안 모범 사례를 지원하는 사전 구축된 표준 프레임워크를 제공합니다.

주제

- AWS 기초 보안 모범 사례 표준이란 무엇입니까?
- 이 프레임워크를 사용하여 감사 준비 지원
- 추가 AWS 기초 보안 모범 사례 리소스

AWS 기초 보안 모범 사례 표준이란 무엇입니까?

AWS 기초 보안 모범 사례 표준은 배포된 계정 및 리소스가 보안 모범 사례에서 벗어나는 시점을 감지하는 컨트롤 세트입니다.

이 표준을 통해 모든 AWS 계정 및 워크로드를 지속적으로 평가하여 모범 사례에서 벗어나는 영역을 신속하게 파악할 수 있습니다. 이 표준은 조직의 보안 태세를 개선하고 유지하는 방법에 대한 실행 가능하고 규범적인 지침을 제공합니다.

컨트롤에는 여러 AWS 서비스 전반의 모범 사례가 포함되어 있습니다. 각 컨트롤에는 적용되는 보안 기능을 반영하는 범주가 할당됩니다. 자세한 내용은 AWS Security Hub 사용 설명서의 컨트롤 범주를 참조하십시오.

이 프레임워크를 사용하여 감사 준비 지원

AWS 기초 보안 모범 사례 프레임워크를 사용하여 감사를 준비할 수 있습니다. 이 프레임워크에는 설명 및 테스트 절차가 포함된 사전 구축된 컨트롤 컬렉션이 포함되어 있습니다. 이러한 컨트롤은 AWS 기초 보안 모범 사례 요구 사항에 따라 컨트롤 세트로 그룹화됩니다. 특정 요구 사항이 있는 내부 감사를 지원하도록 이 프레임워크와 해당 컨트롤을 사용자 지정할 수도 있습니다.

프레임워크를 출발점으로 사용하여 Audit Manager 평가를 생성하고 감사와 관련된 증거 수집을 시작할 수 있습니다. 평가를 생성한 후, Audit Manager는 AWS 계정 및 서비스의 리소스를 평가하기 시작합니다. 이는 AWS 기초 보안 모범 사례 프레임워크에 정의된 컨트롤을 기반으로 이 작업을 수행합니다. 감사 시기가 되면 사용자 또는 사용자가 선택한 대리인이 Audit Manager에서 수집한 증거를 검토할 수 있습니다. 어느 방식으로든 평가에서 증거 폴더를 찾아보고 평가 보고서에 포함할 증거를 선택할 수 있습니다. 또는 증거 찾기 기능을 활성화한 경우 특정 증거를 검색하고 CSV 형식으로 내보내거나 검색 결과에서 평가 보고서를 생성할 수 있습니다. 둘 중 하나의 방식으로 이 평가 보고서를 사용하여 제어가 의도한 대로 작동하고 있음을 보여줄 수 있습니다.

AWS 기초 보안 모범 사례 프레임워크의 세부 정보는 다음과 같습니다.

AWS Audit Manager에서의 프레임워크 이름	자동화된 컨트롤 수	수동 컨트롤 수	컨트롤 세트 수	범위 내 AWS 서비스
AWS 기초 보안 모범 사례	154	0	29	AWS Security Hub

이 AWS Audit Manager 프레임워크의 컨트롤은 시스템이 AWS 기초 보안 모범 사례를 준수하는지 확인하기 위한 것이 아닙니다. 게다가 이는 AWS 기초 보안 모범 사례를 통과할 것이라고 보장할 수도 없습니다.

이 프레임워크는 Audit Manager의 프레임워크 라이브러리의 표준 프레임워크 탭에서 찾을 수 있습니다.

이 프레임워크를 사용하여 평가를 생성하는 방법에 대한 지침은 평가 생성을 참조하십시오.

Audit Manager 콘솔을 사용하여 이 표준 프레임워크에서 평가를 생성하면 범위 내 AWS 서비스 목록이 기본적으로 선택되며 편집할 수 없습니다. 이는 Audit Manager가 자동으로 데이터 소스 및 서비스를 매핑하고 선택하기 때문입니다. 이 선택은 AWS 기초 보안 모범 사례의 요구 사항에 따라 이루어집니다. 이 프레임워크의 범위 내에서 서비스 목록을 편집해야 하는 경우 CreateAssessment 또는 UpdateAssessment API 작업을 사용하여 편집할 수 있습니다. 또는 표준 프레임워크를 사용자 지정한 다음 사용자 지정 프레임워크에서 평가를 생성할 수도 있습니다.

특정 요구 사항을 지원하도록 이 프레임워크를 사용자 지정하는 방법에 대한 지침은 기존 프레임워크 사용자 지정 및 기존 컨트롤 사용자 지정을 참조하십시오.

추가 AWS 기초 보안 모범 사례 리소스

- AWS Security Hub 사용 설명서의 AWS 기초 보안 모범 사례 표준
- AWS Security Hub사용 설명서의 컨트롤 범주

AWS 운영 모범 사례

AWS Audit Manager는 사전 구축된 AWS 운영 모범 사례(OBP) 프레임워크를 제공하여 감사 준비를 지원합니다. 이 프레임워크는 AWS 기초 보안 모범 사례 표준의 일부 컨트롤을 제공합니다. 이러한 컨트롤은 배포된 계정 및 리소스가 보안 모범 사례에서 벗어나는 시점을 감지하는 기본 검사 역할을 합니다.

주제

- AWS 기초 보안 모범 사례 표준이란 무엇입니까?
- 이 프레임워크를 사용하여 감사 준비 지원
- 추가 AWS OBP 리소스

AWS 기초 보안 모범 사례 표준이란 무엇입니까?

AWS 기초 보안 모범 사례 표준을 사용하여 계정 및 워크로드를 평가하고 모범 사례에서 벗어나는 영역을 신속하게 식별할 수 있습니다. 이 표준은 조직의 보안 태세를 개선하고 유지하는 방법에 대한 실행 가능하고 규범적인 지침을 제공합니다.

컨트롤에는 여러 AWS 서비스 전반의 모범 사례가 포함되어 있습니다. 각 컨트롤에는 적용되는 보안 기능을 반영하는 범주가 할당됩니다. 자세한 내용은 AWS Security Hub 사용 설명서의 컨트롤 범주를 참조하십시오.

이 프레임워크를 사용하여 감사 준비 지원

AWS 운영 모범 사례 프레임워크를 사용하여 감사를 준비할 수 있습니다. 이 프레임워크에는 설명 및 테스트 절차가 포함된 사전 구축된 컨트롤 컬렉션이 포함되어 있습니다. 이러한 컨트롤은 AWS 운영 모범 사례 요구 사항에 따라 컨트롤 세트로 그룹화됩니다. 또한 특정 요구 사항이 있는 내부 감사를 지원하도록 이 프레임워크와 해당 컨트롤을 사용자 지정할 수 있습니다.

프레임워크를 출발점으로 사용하여 Audit Manager 평가를 생성하고 감사와 관련된 증거 수집을 시작할 수 있습니다. 평가를 생성한 후, Audit Manager는 AWS 계정 및 서비스의 리소스를 평가하기 시작합니다. 이는 AWS 운영 모범 사례 프레임워크에 정의된 컨트롤을 기반으로 이 작업을 수행합니다. 감사 시기가 되면 사용자 또는 사용자가 선택한 대리인이 Audit Manager에서 수집한 증거를 검토할 수 있습니다. 어느 방식으로든 평가에서 증거 폴더를 찾아보고 평가 보고서에 포함할 증거를 선택할 수 있습니다. 또는 증거 찾기 기능을 활성화한 경우 특정 증거를 검색하고 CSV 형식으로 내보내거나 검색 결과에서 평가 보고서를 생성할 수 있습니다. 둘 중 하나의 방식으로 이 평가 보고서를 사용하여 제어가 의도한 대로 작동하고 있음을 보여줄 수 있습니다.

AWS 운영 모범 사례 프레임워크의 세부 정보는 다음과 같습니다.

AWS Audit Manager에서의 프레임워크 이름	자동화된 컨트롤 수	수동 컨트롤 수	컨트롤 세트 수	범위 내 AWS 서비스
AWS 운영 모범 사례	52	0	20	AWS Security Hub

이 프레임워크의 컨트롤은 시스템이 AWS 운영 모범 사례를 준수하는지 확인하기 위한 것이 아닙니다. 게다가 이는 AWS 운영 모범 사례 감사를 통과할 것이라고 보장할 수도 없습니다.

이 프레임워크는 Audit Manager의 프레임워크 라이브러리의 표준 프레임워크 탭에서 찾을 수 있습니다.

이 프레임워크를 사용하여 평가를 생성하는 방법에 대한 지침은 평가 생성을 참조하십시오.

Audit Manager 콘솔을 사용하여 이 표준 프레임워크에서 평가를 생성하면 범위 내 AWS 서비스 목록이 기본적으로 선택되며 편집할 수 없습니다. 이는 Audit Manager가 자동으로 데이터 소스 및 서비스를 매핑하고 선택하기 때문입니다. 이 선택은 AWS 운영 모범 사례의 요구 사항에 따라 이루어집니다. 이 프레임워크의 범위 내에서 서비스 목록을 편집해야 하는 경우 CreateAssessment 또는 UpdateAssessment API 작업을 사용하여 편집할 수 있습니다. 또는 표준 프레임워크를 사용자 지정한 다음 사용자 지정 프레임워크에서 평가를 생성할 수도 있습니다.

특정 요구 사항을 지원하도록 이 프레임워크를 사용자 지정하는 방법에 대한 지침은 기존 프레임워크 사용자 지정 및 기존 컨트롤 사용자 지정을 참조하십시오.

추가 AWS OBP 리소스

- AWS Security Hub 사용 설명서의 AWS 기초 보안 모범 사례 표준
- AWS Security Hub사용 설명서의 컨트롤 범주

AWS Well-Architected

AWS Audit Manager는 AWS 모범 사례를 기반으로 AWS Well-Architected 프레임워크에 대한 평가를 구조화하고 자동화하는 사전 구축된 프레임워크를 제공합니다.

주제

- AWS Well-Architected란 무엇입니까?
- 이 프레임워크를 사용하여 감사 준비 지원
- 추가 AWS Well-Architected 리소스

AWS Well-Architected란 무엇입니까?

AWS Well-Architected는 애플리케이션과 워크로드를 위한 안전하고 성능 및 복원력이 뛰어나며 효율적인 인프라를 구축하는 데 도움이 되는 프레임워크입니다. 운영 우수성, 보안, 신뢰성, 성능 효율성, 비용 최적화 및 지속 가능성의 6가지 요소를 중심으로 구축된 AWS Well-Architected는 고객과 파트너가 아키텍처를 평가하고 시간이 지남에 따라 확장 가능한 설계를 구현할 수 있는 일관된 접근방식을 제공합니다.

이 프레임워크를 사용하여 감사 준비 지원

AWS Well-Architected 프레임워크를 사용하여 감사를 준비할 수 있습니다. 이 프레임워크는 클라우드에서 워크로드를 설계하고 실행하기 위한 핵심 개념, 설계 원칙, 아키텍처 모범 사례를 설명합니다. AWS Well-Architected의 기반이 되는 여섯 가지 요소 중 보안 및 신뢰성 기둥은 AWS Audit Manager이 사전 구축된 프레임워크와 컨트롤 기능을 제공하는 요소입니다. 특정 요구 사항이 있는 내부 감사를 지원하도록 이 프레임워크와 해당 컨트롤을 사용자 지정할 수도 있습니다.

프레임워크를 출발점으로 사용하여 Audit Manager 평가를 생성하고 감사와 관련된 증거 수집을 시작할 수 있습니다. 평가를 생성하면 Audit Manager가 AWS 리소스 평가를 시작합니다. 이는 AWS Well-Architected 프레임워크에 정의된 컨트롤을 기반으로 이 작업을 수행합니다. 감사 시기가 되면 사용자 또는 사용자가 선택한 대리인이 Audit Manager에서 수집한 증거를 검토할 수 있습니다. 어느 방식으로든 평가에서 증거 폴더를 찾아보고 평가 보고서에 포함할 증거를 선택할 수 있습니다. 또는 증거 찾기 기능을 활성화한 경우 특정 증거를 검색하고 CSV 형식으로 내보내거나 검색 결과에서 평가 보고서를 생성할 수 있습니다. 둘 중 하나의 방식으로 이 평가 보고서를 사용하여 제어가 의도한 대로 작동하고 있음을 보여줄 수 있습니다.

AWS Well-Architected 프레임워크의 세부 정보는 다음과 같습니다.

AWS Audit Manager에서의 프레임워크 이름	자동화된 컨트롤 수	수동 컨트롤 수	컨트롤 세트 수	범위 내 AWS 서비스
AWS Well-Architected 프레임워크	16	0	2	AWS Config

> **Tip**
>
> 이 표준 프레임워크에서 데이터 소스 매핑으로 사용되는 AWS Config 규칙을 검토하려면 AuditManager_ConfigDataSourceMappings_AWSWell-ArchitectedFramework.zip 파일을 다운로드하십시오.

이 프레임워크의 컨트롤은 시스템이 규정을 준수하는지 확인하기 위한 것이 아닙니다. 게다가 이는 AWS Well-Architected 프레임워크와 관련된 감사를 통과할 것이라고 보장할 수도 없습니다.

이 프레임워크는 Audit Manager의 프레임워크 라이브러리의 표준 프레임워크 탭에서 찾을 수 있습니다.

이 프레임워크를 사용하여 평가를 생성하는 방법에 대한 지침은 평가 생성을 참조하십시오.

Audit Manager 콘솔을 사용하여 이 표준 프레임워크에서 평가를 생성하면 범위 내 AWS 서비스 목록이 기본적으로 선택되며 편집할 수 없습니다. 이는 Audit Manager가 자동으로 데이터 소스 및 서비스를 매핑하고 선택하기 때문입니다. 이 선택은 AWS Well-Architected 프레임워크의 요구 사항에 따라 이루어집니다. 이 프레임워크의 범위 내에서 서비스 목록을 편집해야 하는 경우 CreateAssessment 또는 UpdateAssessment API 작업을 사용하여 편집할 수 있습니다. 또는 표준 프레임워크를 사용자 지정한 다음 사용자 지정 프레임워크에서 평가를 생성할 수도 있습니다.

특정 요구 사항을 지원하도록 이 프레임워크를 사용자 지정하는 방법에 대한 지침은 기존 프레임워크 사용자 지정 및 기존 컨트롤 사용자 지정을 참조하십시오.

추가 AWS Well-Architected 리소스

- AWS Well-Architected
- AWS Well-Architected 프레임워크 설명서

캐나다 사이버 보안 센터(Canadian Centre for Cyber Security, CCCS) 미디엄 클라우드 컨트롤 프로필

AWS Audit Manager는 캐나다 사이버 보안 센터의 평가를 구조화하고 자동화하는 사전 구축된 표준 프레임워크를 제공합니다.

주제

- 캐나다 사이버 보안 센터란 무엇입니까?
- 이 프레임워크를 사용하여 감사 준비 지원

캐나다 사이버 보안 센터란 무엇입니까?

캐나다 사이버 보안 센터(Canadian Centre for Cyber Security, CCCS)는 캐나다의 권위 있는 사이버 보안 전문가 지침, 서비스 및 지원 소스입니다. CCCS는 캐나다 정부, 업계 및 일반 대중에게 이러한 전문 지식을 제공합니다. 캐나다 전역의 캐나다 공공 부문 조직은 클라우드 서비스 제공업체에 대한 이들의 엄격한 평가를 바탕으로 정보에 입각한 클라우드 조달 결정을 내립니다.

CCCS 미디엄 클라우드 컨트롤 프로필은 2020년 5월에 캐나다 정부의 PROTECTED B/중간 무결성/중간 가용성(PBMM) 프로필을 대체했습니다. CCCS 미디엄 클라우드 보안 컨트롤 프로필은 조직에서 퍼블릭 클라우드 서비스를 사용하여 중간 수준의 기밀성, 무결성 및 가용성(AIC) 요구 사항을 요하는

비즈니스 활동을 지원하는 경우에 적합합니다. 중간 수준의 AIC 요구 사항을 갖는 워크로드는 비즈니스 활동에 사용되는 정보 또는 서비스에 대한 무단 공개, 수정 또는 액세스 손실로 인해 개인 또는 조직에 심각한 피해를 입히거나 개인 집단에 제한적인 손해를 입힐 수 있다는 점을 합리적으로 예상할 수 있다는 것을 의미합니다. 이러한 손상 수준의 예는 다음과 같습니다.

- 연간 수익에 미치는 중대한 영향
- 주요 계정 손실
- 영업권 손실
- 명백한 규정 준수 침해
- 수백 또는 수천 명의 사용자에 대한 개인 정보 침해
- 프로그램 성능에 영향을 미침
- 정신 장애 또는 질병 유발
- 사보타주
- 평판 훼손
- 개인의 재정적 어려움

이 프레임워크를 사용하여 감사 준비 지원

미디엄 클라우드 컨트롤 프로필용 AWS Audit Manager 프레임워크를 사용하여 감사를 준비할 수 있습니다. 이 프레임워크에는 설명 및 테스트 절차가 포함된 사전 구축된 컨트롤 컬렉션이 포함되어 있습니다. 이러한 컨트롤은 CCCS 요구 사항에 따라 컨트롤 세트로 그룹화됩니다. 특정 요구 사항이 있는 내부 감사를 지원하도록 이 프레임워크와 해당 컨트롤을 사용자 지정할 수도 있습니다.

프레임워크를 출발점으로 사용하여 Audit Manager 평가를 생성하고 CCCS 미디엄 클라우드 컨트롤 프로필 감사와 관련된 증거 수집을 시작할 수 있습니다. 평가 시 감사 범위에 포함할 AWS 계정 및 서비스를 지정할 수 있습니다. 평가를 생성하면 Audit Manager가 AWS 리소스 평가를 시작합니다. 이는 CCCS 미디엄 클라우드 컨트롤 프로필 프레임워크에 정의된 컨트롤을 기반으로 이 작업을 수행합니다. 감사 시기가 되면 사용자 또는 사용자가 선택한 대리인이 Audit Manager에서 수집한 증거를 검토할 수 있습니다. 어느 방식으로든 평가에서 증거 폴더를 찾아보고 평가 보고서에 포함할 증거를 선택할 수 있습니다. 또는 증거 찾기 기능을 활성화한 경우 특정 증거를 검색하고 CSV 형식으로 내보내거나 검색 결과에서 평가 보고서를 생성할 수 있습니다. 둘 중 하나의 방식으로 이 평가 보고서를 사용하여 제어가 의도한 대로 작동하고 있음을 보여줄 수 있습니다.

프레임워크 세부 정보는 다음과 같습니다.

AWS Audit Manager에서의 프레임워크 이름	자동화된 컨트롤 수	수동 컨트롤 수	컨트롤 세트 수	범위 내 AWS 서비스
캐나다 사이버 보안 센터 - 미디엄	206	396	165	• Amazon CloudWatch • Amazon Elastic Compute Cloud • AWS CloudTrail • AWS Config • AWS Identity and Access Management • AWS Key Management Service • AWS License Manager

> **Tip**
>
> 이 표준 프레임워크에서 데이터 소스 매핑으로 사용되는 AWS Config 규칙을 검토하려면 AuditManager_ConfigDataSourceMappings_CanadianCentreforCyberSecurity-Medium.zip 파일을 다운로드하십시오.

이 AWS Audit Manager 프레임워크의 컨트롤은 시스템이 CCCS 미디엄 클라우드 컨트롤 프로필 표준을 준수하는지 확인하기 위한 것이 아닙니다. 게다가 이는 CCCS 감사 통과를 보장할 수도 없습니다. AWS Audit Manager는 수동 증거 수집이 필요한 절차상의 컨트롤을 자동으로 확인하지 않습니다.

이 프레임워크는 Audit Manager의 프레임워크 라이브러리의 표준 프레임워크 탭에서 찾을 수 있습니다.

이 프레임워크를 사용하여 평가를 생성하는 방법에 대한 지침은 평가 생성을 참조하십시오.

Audit Manager 콘솔을 사용하여 이 표준 프레임워크에서 평가를 생성하면 범위 내 AWS 서비스 목록이 기본적으로 선택되며 편집할 수 없습니다. 이는 Audit Manager가 자동으로 데이터 소스 및 서

비스를 매핑하고 선택하기 때문입니다. 이 선택은 캐나다 사이버 보안 센터 - 미디엄 프레임워크의 요구 사항에 따라 이루어집니다. 이 프레임워크의 범위 내에서 서비스 목록을 편집해야 하는 경우 CreateAssessment 또는 UpdateAssessment API 작업을 사용하여 편집할 수 있습니다. 또는 표준 프레임워크를 사용자 지정한 다음 사용자 지정 프레임워크에서 평가를 생성할 수도 있습니다.

특정 요구 사항을 지원하도록 이 프레임워크를 사용자 지정하는 방법에 대한 지침은 기존 프레임워크 사용자 지정 및 기존 컨트롤 사용자 지정을 참조하십시오.

CIS Amazon Web Services 파운데이션 벤치마크 v1.2.0용 CIS 벤치마크

AWS Audit Manager는 CIS AWS 파운데이션 벤치마크 v1.2.0을 지원하는 사전 구축된 두 가지 프레임워크를 제공합니다.

- CIS Amazon Web Services 파운데이션 벤치마크 v1.2.0, 레벨 1용 CIS 벤치마크
- CIS Amazon Web Services 파운데이션 벤치마크 v1.2.0, 레벨 1 및 2용 CIS 벤치마크

> **Note**
>
> - v1.3.0을 지원하는 Audit Manager 프레임워크에 대한 자세한 내용은 CIS Amazon Web Services 파운데이션 벤치마크 v1.3.0용 CIS 벤치마크을 참조하십시오.
> - v1.4.0을 지원하는 Audit Manager 프레임워크에 대한 자세한 내용은 CIS Amazon Web Services 파운데이션 벤치마크 v1.4.0용 CIS 벤치마크을 참조하십시오.

주제

CIS란 무엇입니까?

인터넷 보안 센터(Center for Internet Security, CIS)는 CIS AWS 파운데이션 벤치마크를 개발한 비영리 단체입니다. 이 벤치마크는 AWS에 대한 일련의 보안 구성 모범 사례 역할을 합니다. 업계에서 인정받는 이러한 모범 사례는 명확한 단계별 구현 및 평가 절차를 제공한다는 점에서 이미 제공되는 높은 수준의 보안 지침을 뛰어 넘습니다.

자세한 내용은 AWS 보안 블로그의 CIS AWS 파운데이션 벤치마크 블로그 게시물을 참조하십시오.

CIS 벤치마크와 CIS 컨트롤 간의 차이점

CIS 벤치마크는 공급업체 제품에 특화된 보안 모범 사례 지침입니다. 운영 체제에서 클라우드 서비스 및 네트워크 디바이스에 이르기까지 벤치마크에서 적용되는 설정은 조직에서 사용하는 특정 시스템을 보호합니다. CIS 컨트롤은 알려진 사이버 공격 벡터로부터 보호하기 위해 조직 수준의 시스템이 따라야 할 기본 모범 사례 지침입니다.

예제

- CIS 벤치마크는 규범적입니다. 이는 일반적으로 공급업체 제품에서 검토 및 설정할 수 있는 특정 설정을 참조합니다.

  예: CIS Amazon Web Services 파운데이션 벤치마크 v1.2.0 - 1.13 “루트 사용자” 계정에 MFA가 활성화되었는지 확인

  이 권장 사항은 이를 확인하는 방법과 AWS 환경의 루트 계정에 이를 설정하는 방법에 대한 규범적 지침을 제공합니다.
- CIS 컨트롤은 조직 전체를 위한 것입니다. 특정 공급업체 제품에만 적용되는 것은 아닙니다.

  예: CIS 컨트롤 v7.1 - 하위 컨트롤 4.5 모든 관리 액세스에 다중 인증 사용

  이 컨트롤은 조직 내에 적용될 것으로 예상되는 사항을 설명합니다. 실행 중인 시스템 및 워크로드(위치에 관계없이)에 이를 어떻게 적용해야 하는지는 설명되어 있지 않습니다.

이러한 프레임워크를 사용하여 감사 준비 지원

AWS Audit Manager에서 CIS AWS 파운데이션 벤치마크 v1.2 프레임워크를 사용하여 CIS 감사를 준비할 수 있습니다. 또한 특정 요구 사항에 따른 내부 감사를 지원하도록 이러한 프레임워크와 해당 컨트롤을 사용자 지정할 수 있습니다.

프레임워크를 출발점으로 사용하여 Audit Manager 평가를 생성하고 감사와 관련된 증거 수집을 시작할 수 있습니다. 평가를 생성하면 Audit Manager가 AWS 리소스 평가를 시작합니다. 이는 CIS 프레임워크에 정의된 컨트롤을 기반으로 이 작업을 수행합니다. 감사 시기가 되면 사용자 또는 사용자가 선택한 대리인이 Audit Manager에서 수집한 증거를 검토할 수 있습니다. 어느 방식으로든 평가에서 증거 폴더를 찾아보고 평가 보고서에 포함할 증거를 선택할 수 있습니다. 또는 증거 찾기 기능을 활성화한 경우 특정 증거를 검색하고 CSV 형식으로 내보내거나 검색 결과에서 평가 보고서를 생성할 수 있습니다. 둘 중 하나의 방식으로 이 평가 보고서를 사용하여 제어가 의도한 대로 작동하고 있음을 보여줄 수 있습니다.

프레임워크 세부 정보는 다음과 같습니다.

AWS Audit Manager에서의 프레임워크 이름	자동화된 컨트롤 수	수동 컨트롤 수	컨트롤 세트 수	범위 내 AWS 서비스
CIS Amazon Web Services 파운데이션 벤치마크 v1.2.0, 레벨 1용 CIS 벤치마크	33	3	4	• Amazon Elastic Compute Cloud • AWS CloudTrail • AWS Identity and Access Management • AWS Security Hub
CIS Amazon Web Services 파운데이션 벤치마크 v1.2.0, 레벨 1 및 2용 CIS 벤치마크	45	4	4	• Amazon Elastic Compute Cloud • AWS CloudTrail • AWS Identity and Access Management • AWS Security Hub

이러한 프레임워크의 컨트롤은 시스템이 CIS 표준을 준수하는지 확인하기 위한 것이 아닙니다. 게다가 이는 CIS 감사 통과를 보장할 수도 없습니다. AWS Audit Manager는 수동 증거 수집이 필요한 절차상의 컨트롤을 자동으로 확인하지 않습니다.

Audit Manager에서 프레임워크 라이브러리의 표준 프레임워크 탭에서 이러한 프레임워크를 찾을 수 있습니다.

이 프레임워크를 사용하여 평가를 생성하는 방법에 대한 지침은 평가 생성을 참조하십시오.

Audit Manager 콘솔을 사용하여 이 표준 프레임워크에서 평가를 생성하면 범위 내 AWS 서비스 목록이 기본적으로 선택되며 편집할 수 없습니다. 이는 Audit Manager가 자동으로 데이터 소스 및 서비스를 매핑하고 선택하기 때문입니다. 이 선택은 CIS 벤치마크의 요구 사항에 따라 이루어집니다. 이 프레임워크의 범위 내에서 서비스 목록을 편집해야 하는 경우 CreateAssessment 또는 UpdateAssessment API 작업을 사용하여 편집할 수 있습니다. 또는 표준 프레임워크를 사용자 지정한 다음 사용자 지정 프레임워크에서 평가를 생성할 수도 있습니다.

특정 요구 사항을 지원하도록 이 프레임워크를 사용자 지정하는 방법에 대한 지침은 기존 프레임워크 사용자 지정 및 기존 컨트롤 사용자 지정을 참조하십시오.

이러한 프레임워크 사용을 위한 필수 조건

CIS AWS 파운데이션 벤치마크 v1.2 프레임워크의 많은 컨트롤은 AWS Config을 데이터 소스 유형으로 사용합니다. 이러한 컨트롤을 지원하려면 Audit Manager를 활성화한 각 AWS 리전의 모든 계정에서 AWS Config을 활성화해야 합니다. 또한 특정 AWS Config 규칙이 활성화되어 있고 이러한 규칙이 올바르게 구성되었는지도 확인해야 합니다.

CIS AWS 파운데이션 벤치마크 v1.2의 정확한 증거를 수집하고 정확한 규정 준수 상태를 파악하려면 다음 AWS Config 규칙 및 매개변수가 필요합니다. 규칙을 활성화하거나 구성하는 방법에 대한 지침은 AWS Config 관리형 규칙으로 작업하기를 참조하십시오.

필수 AWS Config 규칙	필수 매개변수
ACCESS_KEYS_ROTATED	**maxAccessKeyAge** • 교체를 사용하지 않는 최대 일수입니다. • 유형: Int • 기본값: 90일 • 규정 준수 요구 사항: 최대 90일
CLOUD_TRAIL_CLOUD_WATCH_LOGS_ENABLED	해당 사항 없음
CLOUD_TRAIL_ENCRYPTION_ENABLED	해당 사항 없음
CLOUD_TRAIL_LOG_FILE_VALIDATION_ENABLED	해당 사항 없음
CMK_BACKING_KEY_ROTATION_ENABLED	해당 사항 없음
IAM_PASSWORD_POLICY	**MaxPasswordAge** (선택 사항) • 암호 만료 이전의 일수입니다. • 유형: int • 기본값: 90

필수 AWS Config 규칙	필수 매개변수
	• 규정 준수 요구 사항: 최대 90일
IAM_PASSWORD_POLICY	**MinimumPasswordLength** (선택 사항) • 암호의 최소 길이입니다. • 유형: int • 기본값: 14 • 규정 준수 요구 사항: 최소 14자
IAM_PASSWORD_POLICY	**PasswordReusePrevention** (선택 사항) • 재사용을 허가받기까지 사용할 수 있는 암호 개수입니다. • 유형: int • 기본값: 24 • 규정 준수 요구 사항: 재사용 전 최소 24개의 암호
IAM_PASSWORD_POLICY	**RequireLowercaseCharacters** (선택 사항) • 암호에 소문자가 한 개 이상이어야 합니다. • 유형: 부울 • 기본값: True • 규정 준수 요구 사항: 하나 이상의 소문자 필요
IAM_PASSWORD_POLICY	**RequireNumbers** (선택 사항) • 암호에 숫자가 한 개 이상이어야 합니다. • 유형: 부울 • 기본값: True • 규정 준수 요구 사항: 하나 이상의 숫자
IAM_PASSWORD_POLICY	**RequireSymbols** (선택 사항) • 암호에 기호가 한 개 이상이어야 합니다. • 유형: 부울 • 기본값: True • 규정 준수 요구 사항: 하나 이상의 기호 문자

필수 AWS Config 규칙	필수 매개변수
IAM_PASSWORD_POLICY	**RequireUppercaseCharacters** (선택 사항) • 암호에 대문자가 한 개 이상이어야 합니다. • 유형: 부울 • 기본값: True • 규정 준수 요구 사항: 하나 이상의 대문자
IAM_POLICY_IN_USE	**policyARN** • IAM 정책 ARN을 확인해야 합니다. • 유형: 문자열 • 규정 준수 요구 사항: AWS을 사용하여 인시던트를 관리하기 위한 IAM 역할을 생성합니다. **policyUsageType** (선택 사항) • 정책을 사용자, 그룹 또는 역할에 연결할 것으로 예상하는지 여부를 지정합니다. • 유형: 문자열 • 유효한 값: IAM_USER | IAM_GROUP | IAM_ROLE | ANY • 기본 값: ANY • 규정 준수 요구 사항: 생성된 IAM 역할에 신뢰 정책 연결
IAM_POLICY_NO_STATEMENTS_WITH_ADMIN_ACCESS	해당 사항 없음
IAM_ROOT_ACCESS_KEY_CHECK	해당 사항 없음
IAM_USER_NO_POLICIES_CHECK	해당 사항 없음

필수 AWS Config 규칙	필수 매개변수
IAM_USER_UNUSED_CREDENTIALS_CHECK	**maxCredentialUsageAge** • 보안 인증을 사용할 수 없는 최대 일수. • 유형: Int • 기본값: 90일 • 규정 준수 요구 사항: 90일 이상
INCOMING_SSH_DISABLED	해당 사항 없음
MFA_ENABLED_FOR_IAM_CONSOLE_ACCESS	해당 사항 없음
MULTI_REGION_CLOUD_TRAIL_ENABLED	해당 사항 없음

필수 AWS Config 규칙	필수 매개변수
RESTRICTED_INCOMING_TRAFFIC	**`blockedPort1`** (선택 사항) • 차단된 TCP 포트 번호. • 유형: int • 기본값: 20 • 규정 준수 요구 사항: 차단된 포트에 대한 침입을 허용하는 보안 그룹이 없는지 확인합니다. **`blockedPort2`** (선택 사항) • 차단된 TCP 포트 번호. • 유형: int • 기본값: 21 • 규정 준수 요구 사항: 차단된 포트에 대한 침입을 허용하는 보안 그룹이 없는지 확인합니다. **`blockedPort3`** (선택 사항) • 차단된 TCP 포트 번호. • 유형: int • 기본값: 3389 • 규정 준수 요구 사항: 차단된 포트에 대한 침입을 허용하는 보안 그룹이 없는지 확인합니다. **`blockedPort4`** (선택 사항) • 차단된 TCP 포트 번호. • 유형: int • 기본값: 3306 • 규정 준수 요구 사항: 차단된 포트에 대한 침입을 허용하는 보안 그룹이 없는지 확인합니다. **`blockedPort5`** (선택 사항) • 차단된 TCP 포트 번호. • 유형: int • 기본값: 4333

필수 AWS Config 규칙	필수 매개변수
	• 규정 준수 요구 사항: 차단된 포트에 대한 침입을 허용하는 보안 그룹이 없는지 확인합니다.
ROOT_ACCOUNT_HARDWARE_MFA_ENABLED	해당 사항 없음
ROOT_ACCOUNT_MFA_ENABLED	해당 사항 없음
S3_BUCKET_LOGGING_ENABLED	**targetBucket** (선택 사항) • 서버 액세스 로그 저장을 위한 대상 S3 버킷. • 유형: 문자열 • 규정 준수 요구 사항: 로깅 활성화 **targetPrefix** (선택 사항) • 서버 액세스 로그 저장을 위한 대상 S3 버킷의 접두사. • 유형: 문자열 • 규정 준수 요구 사항: CloudTrail 로깅을 위한 S3 버킷 식별합니다.
S3_BUCKET_PUBLIC_READ_PROHIBITED	해당 사항 없음
VPC_DEFAULT_SECURITY_GROUP_CLOSED	해당 사항 없음
VPC_FLOW_LOGS_ENABLED	**trafficType** (선택 사항) • 흐름 로그의 `trafficType` . • 유형: 문자열 • 규정 준수 요구 사항: 흐름 로깅이 활성화됩니다.

추가 CIS 리소스

- CIS AWS 파운데이션 벤치마크 v1.2.0
- AWS 보안 블로그의 CIS AWS 파운데이션 벤치마크 블로그 게시물

CIS Amazon Web Services 파운데이션 벤치마크 v1.3.0용 CIS 벤치마크

AWS Audit Manager는 CIS AWS 파운데이션 벤치마크 v1.3을 지원하는 사전 구축된 두 가지 프레임워크를 제공합니다.

- CIS Amazon Web Services 파운데이션 벤치마크 v1.3.0, 레벨 1용 CIS 벤치마크
- CIS Amazon Web Services 파운데이션 벤치마크 v1.3.0, 레벨 1 및 2용 CIS 벤치마크

> **Note**
>
> CIS AWS 파운데이션 벤치마크 v1.2.0 및 이 버전의 벤치마크를 지원하는 AWS Audit Manager 프레임워크에 대한 자세한 내용은 CIS Amazon Web Services 파운데이션 벤치마크 v1.2.0용 CIS 벤치마크을 참조하십시오.

주제

CIS란 무엇입니까?

인터넷 보안 센터(CIS)는 AWS에 대한 보안 구성 모범 사례 모음인 CIS AWS 파운데이션 벤치마크 v1.3.0을 개발했습니다. 업계에서 인정받은 이러한 모범 사례는 AWS 사용자에게 명확한 단계별 구현 및 평가 절차를 제공한다는 점에서 이미 제공되는 높은 수준의 보안 지침을 뛰어 넘습니다.

자세한 내용은 AWS 보안 블로그의 CIS AWS 재단 벤치마크 블로그 게시물을 참조하십시오.

CIS AWS Foundation Benchmark v1.3.0은 기본적이고 테스트 가능하며 아키텍처에 구애받지 않는 설정에 중점을 두고 AWS 서비스의 하위 집합에 대한 보안 옵션을 구성하기 위한 지침을 제공합니다. 이 문서의 범위에 해당하는 특정 Amazon Web Services 중 일부는 다음과 같습니다.

- AWS Identity and Access Management (IAM)
- AWS Config
- AWS CloudTrail
- Amazon CloudWatch

- Amazon Simple Notification Service(Amazon SNS)
- Amazon Simple Storage Service(S3)
- Amazon Virtual Private Cloud(기본값)

CIS 벤치마크와 CIS 컨트롤 간의 차이점

CIS 벤치마크는 공급업체 제품에 특화된 보안 모범 사례 지침입니다. 운영 체제에서 클라우드 서비스 및 네트워크 디바이스에 이르기까지 벤치마크에서 적용되는 설정은 조직에서 사용하는 시스템을 보호합니다. CIS 컨트롤은 알려진 사이버 공격 벡터로부터 보호하기 위해 조직이 준수해야 하는 기초 모범 사례 지침입니다.

예제

- CIS 벤치마크는 규범적입니다. 이는 일반적으로 공급업체 제품에서 검토 및 설정할 수 있는 특정 설정을 참조합니다.

  예: CIS Amazon Web Services Foundation 벤치마크 v1.3.0 - 1.5 “루트 사용자” 계정에 MFA가 활성화되어 있는지 확인

  이 권장 사항은 이를 확인하는 방법과 AWS 환경의 루트 계정에 이를 설정하는 방법에 대한 규범적 지침을 제공합니다.
- CIS 컨트롤은 조직 전체를 위한 것으로 특정 공급업체 제품에만 국한되지 않습니다.

  예: CIS 컨트롤 v7.1 - 하위 컨트롤 4.5 모든 관리 액세스에 다중 인증 사용

  이 컨트롤은 조직 내에서 적용될 것으로 예상되는 사항을 설명하지만, 실행 중인 시스템 및 워크로드(위치에 관계없이)에 이를 어떻게 적용해야 하는지는 설명되어 있지 않습니다.

이러한 프레임워크를 사용하여 감사 준비 지원

AWS Audit Manager에서 CIS AWS 파운데이션 벤치마크 v1.3 프레임워크를 사용하여 CIS 감사를 준비할 수 있습니다. 또한 특정 요구 사항에 따른 내부 감사를 지원하도록 이러한 프레임워크와 해당 컨트롤을 사용자 지정할 수 있습니다.

프레임워크를 출발점으로 사용하여 Audit Manager 평가를 생성하고 감사와 관련된 증거 수집을 시작할 수 있습니다. 평가를 생성하면 Audit Manager가 AWS 리소스 평가를 시작합니다. 이는 CIS 프레임워크에 정의된 컨트롤을 기반으로 이 작업을 수행합니다. 감사 시기가 되면 사용자 또는 사용자가 선택한 대리인이 Audit Manager에서 수집한 증거를 검토할 수 있습니다. 어느 방식으로든 평가에서 증거

폴더를 찾아보고 평가 보고서에 포함할 증거를 선택할 수 있습니다. 또는 증거 찾기 기능을 활성화한 경우 특정 증거를 검색하고 CSV 형식으로 내보내거나 검색 결과에서 평가 보고서를 생성할 수 있습니다. 둘 중 하나의 방식으로 이 평가 보고서를 사용하여 제어가 의도한 대로 작동하고 있음을 보여줄 수 있습니다.

프레임워크 세부 정보는 다음과 같습니다.

AWS Audit Manager에서의 프레임워크 이름	자동화된 컨트롤 수	수동 컨트롤 수	컨트롤 세트 수	범위 내 AWS 서비스
CIS Amazon Web Services 파운데이션 벤치마크 v1.3.0, 레벨 1용 CIS 벤치마크	33	5	6	• Amazon CloudWatch • Amazon Elastic Compute Cloud • AWS Config • AWS CloudTrail • AWS Identity and Access Management • AWS Security Hub
CIS Amazon Web Services 파운데이션 벤치마크 v1.3.0, 레벨 1 및 2용 CIS 벤치마크	49	6	6	• Amazon Elastic Compute Cloud • Amazon CloudWatch • AWS CloudTrail • AWS Config • AWS Identity and Access Management • AWS Security Hub

> **Tip**
>
> 이러한 표준 프레임워크의 데이터 소스 매핑으로 사용되는 AWS Config 규칙 목록을 검토하려면 다음 파일을 다운로드하십시오.
>
> - AuditManager_ConfigDataSourceMappings_CIS-Benchmark-v1.3.0-Level-1.zip
> - AuditManager_ConfigDataSourceMappings_CIS-Benchmark-v1.3.0,Level1-and-2.zip

이러한 프레임워크의 컨트롤은 시스템이 CIS 표준을 준수하는지 확인하기 위한 것이 아닙니다. 게다가 이는 CIS 감사 통과를 보장할 수도 없습니다. AWS Audit Manager는 수동 증거 수집이 필요한 절차상의 컨트롤을 자동으로 확인하지 않습니다.

Audit Manager에서 프레임워크 라이브러리의 표준 프레임워크 탭에서 이러한 프레임워크를 찾을 수 있습니다.

이 프레임워크를 사용하여 평가를 생성하는 방법에 대한 지침은 평가 생성을 참조하십시오.

Audit Manager 콘솔을 사용하여 이 표준 프레임워크에서 평가를 생성하면 범위 내 AWS 서비스 목록이 기본적으로 선택되며 편집할 수 없습니다. 이는 Audit Manager가 자동으로 데이터 소스 및 서비스를 매핑하고 선택하기 때문입니다. 이 선택은 CIS 벤치마크의 요구 사항에 따라 이루어집니다. 이 프레임워크의 범위 내에서 서비스 목록을 편집해야 하는 경우 CreateAssessment 또는 UpdateAssessment API 작업을 사용하여 편집할 수 있습니다. 또는 표준 프레임워크를 사용자 지정한 다음 사용자 지정 프레임워크에서 평가를 생성할 수도 있습니다.

특정 요구 사항을 지원하도록 이 프레임워크를 사용자 지정하는 방법에 대한 지침은 기존 프레임워크 사용자 지정 및 기존 컨트롤 사용자 지정을 참조하십시오.

추가 CIS 리소스

- AWS 보안 블로그의 CIS AWS 파운데이션 벤치마크 블로그 게시물

CIS Amazon Web Services 파운데이션 벤치마크 v1.4.0용 CIS 벤치마크

AWS Audit Manager는 인터넷 보안 센터(CIS)의 AWS 파운데이션 벤치마크 v1.4.0을 지원하는 사전 구축된 두 가지 표준 프레임워크를 제공합니다:

- CIS Amazon Web Services 파운데이션 벤치마크 v1.4.0, 레벨 1용 CIS 벤치마크
- CIS Amazon Web Services 파운데이션 벤치마크 v1.4.0, 레벨 1 및 2용 CIS 벤치마크

> **Note**
>
> - v1.2.0을 지원하는 Audit Manager 프레임워크에 대한 자세한 내용은 CIS Amazon Web Services 파운데이션 벤치마크 v1.2.0용 CIS 벤치마크을 참조하십시오.
> - v1.3.0을 지원하는 Audit Manager 프레임워크에 대한 자세한 내용은 CIS Amazon Web Services 파운데이션 벤치마크 v1.3.0용 CIS 벤치마크을 참조하십시오.

주제

CIS Amazon Web Services 파운데이션 벤치마크 v1.4.0용 CIS 벤치마크란 무엇입니까?

CIS Amazon Web Services 파운데이션 벤치마크 v1.4.0, 레벨 1 및 2용 CIS 벤치마크는 Amazon Web Services의 하위 집합에 대한 보안 옵션을 구성하기 위한 규범적 지침을 제공합니다. 이는 기본적이고 테스트 가능하며 아키텍처에 구애받지 않는 설정에 중점을 둡니다. 이 문서의 범위에 해당하는 특정 Amazon Web Services 중 일부는 다음과 같습니다.

- AWS Identity and Access Management (IAM)
- IAM 액세스 분석기
- AWS Config
- AWS CloudTrail
- Amazon CloudWatch
- Amazon Simple Notification Service(Amazon SNS)
- Amazon Simple Storage Service(S3)
- Amazon Elastic Compute Cloud(Amazon EC2)
- Amazon Relational Database Service(Amazon RDS)
- Amazon Virtual Private Cloud

CIS 벤치마크와 CIS 컨트롤 간의 차이점

CIS 벤치마크는 공급업체 제품에 특화된 보안 모범 사례 지침입니다. 운영 체제에서 클라우드 서비스 및 네트워크 디바이스에 이르기까지 벤치마크에서 적용되는 설정은 사용 중인 시스템을 보호합니다. CIS 컨트롤은 알려진 사이버 공격 벡터로부터 보호하기 위해 조직이 준수해야 하는 기초 모범 사례 지침입니다.

예제

- CIS 벤치마크는 규범적입니다. 이는 일반적으로 공급업체 제품에서 검토 및 설정할 수 있는 특정 설정을 참조합니다.

  예: CIS Amazon Web Services Foundation 벤치마크 v1.4.0 - 1.5 “루트 사용자” 계정에 MFA가 활성화되어 있는지 확인

  이 권장 사항은 이를 확인하는 방법과 AWS 환경의 루트 계정에 이를 설정하는 방법에 대한 규범적 지침을 제공합니다.
- CIS 컨트롤은 조직 전체를 위한 것으로 특정 공급업체 제품에만 국한되지 않습니다.

  예: CIS 컨트롤 v7.1 - 하위 컨트롤 4.5 모든 관리 액세스에 다중 인증 사용

  이 컨트롤은 조직 내에 적용될 것으로 예상되는 사항을 설명합니다. 하지만 실행 중인 시스템 및 워크로드(위치에 관계없이)에 이를 어떻게 적용해야 하는지는 설명되어 있지 않습니다.

이러한 프레임워크를 사용하여 감사 준비 지원

AWS Audit Manager에서 CIS AWS 파운데이션 벤치마크 v1.4.0 프레임워크를 사용하여 CIS 감사를 준비할 수 있습니다. 또한 특정 요구 사항에 따른 내부 감사를 지원하도록 이러한 프레임워크와 해당 컨트롤을 사용자 지정할 수 있습니다.

프레임워크를 출발점으로 사용하여 Audit Manager 평가를 생성하고 감사와 관련된 증거 수집을 시작할 수 있습니다. 평가를 생성하면 Audit Manager가 AWS 리소스 평가를 시작합니다. 이는 CIS 프레임워크에 정의된 컨트롤을 기반으로 이 작업을 수행합니다. 감사 시기가 되면 사용자 또는 사용자가 선택한 대리인이 Audit Manager에서 수집한 증거를 검토할 수 있습니다. 어느 방식으로든 평가에서 증거 폴더를 찾아보고 평가 보고서에 포함할 증거를 선택할 수 있습니다. 또는 증거 찾기 기능을 활성화한 경우 특정 증거를 검색하고 CSV 형식으로 내보내거나 검색 결과에서 평가 보고서를 생성할 수 있습니다. 둘 중 하나의 방식으로 이 평가 보고서를 사용하여 제어가 의도한 대로 작동하고 있음을 보여줄 수 있습니다.

프레임워크 세부 정보는 다음과 같습니다.

AWS Audit Manager에서의 프레임워크 이름	자동화된 컨트롤 수	수동 컨트롤 수	컨트롤 세트 수	범위 내 AWS 서비스
CIS Amazon Web Services 파운데이션 벤치마크 v1.4.0, 레벨 1용 CIS 벤치마크	32	6	7	• Amazon Elastic Compute Cloud • Amazon CloudWatch • AWS CloudTrail • AWS Config • AWS Identity and Access Management
CIS Amazon Web Services 파운데이션 벤치마크 v1.4.0, 레벨 1 및 2용 CIS 벤치마크	50	8	7	• Amazon Elastic Compute Cloud • Amazon CloudWatch • AWS CloudTrail • AWS Config • AWS Identity and Access Management • AWS Security Hub

Tip

이러한 표준 프레임워크의 데이터 소스 매핑으로 사용되는 AWS Config 규칙 목록을 검토하려면 다음 파일을 다운로드하십시오.

- AuditManager_ConfigDataSourceMappings_CIS-Benchmark-v1.4.0-Level-1.zip
- AuditManager_ConfigDataSourceMappings_CIS-Benchmark-v1.4.0-Level-1-and-2.zip

이러한 프레임워크의 컨트롤은 시스템이 CIS Amazon Web Services Foundation 벤치마크 v1.4.0 표준을 준수하는지 확인하기 위한 것이 아닙니다. 게다가 이는 CIS 감사 통과를 보장할 수도 없습니다. AWS Audit Manager는 수동 증거 수집이 필요한 절차상의 컨트롤을 자동으로 확인하지 않습니다.

Audit Manager에서 프레임워크 라이브러리의 표준 프레임워크 탭에서 이러한 프레임워크를 찾을 수 있습니다.

이 프레임워크를 사용하여 평가를 생성하는 방법에 대한 지침은 평가 생성을 참조하십시오.

Audit Manager 콘솔을 사용하여 이 표준 프레임워크에서 평가를 생성하면 범위 내 AWS 서비스 목록이 기본적으로 선택되며 편집할 수 없습니다. 이는 Audit Manager가 자동으로 데이터 소스 및 서비스를 매핑하고 선택하기 때문입니다. 이 선택은 CIS 벤치마크의 요구 사항에 따라 이루어집니다. 이 프레임워크의 범위 내에서 서비스 목록을 편집해야 하는 경우 CreateAssessment 또는 UpdateAssessment API 작업을 사용하여 편집할 수 있습니다. 또는 표준 프레임워크를 사용자 지정한 다음 사용자 지정 프레임워크에서 평가를 생성할 수도 있습니다.

특정 요구 사항을 지원하도록 이 프레임워크를 사용자 지정하는 방법에 대한 지침은 기존 프레임워크 사용자 지정 및 기존 컨트롤 사용자 지정을 참조하십시오.

추가 CIS 리소스

- 인터넷 보안 센터의 CIS 벤치마크
- AWS 보안 블로그의 CIS AWS 파운데이션 벤치마크 블로그 게시물

CIS 컨트롤 v7.1 구현 그룹 1

AWS Audit Manager는 인터넷 보안 센터(CIS) 컨트롤 v7.1 구현 그룹 1을 지원하는 사전 구축된 프레임워크를 제공합니다.

> **Note**
>
> CIS 컨트롤 v8 IG1 및 이 표준을 지원하는 AWS Audit Manager 프레임워크에 대한 자세한 내용은 CIS 컨트롤 v8 구현 그룹 1을 참조하십시오.

AWS Audit Manager는 감사 준비를 지원하기 위해 인터넷 보안 센터 (CIS)를 지원하는 사전 구축된 프레임워크를 제공합니다.

주제

CIS 컨트롤이란 무엇입니까?

CIS 컨트롤은 우선 순위가 지정된 일련의 조치로, 심층적인 방어 모범 사례를 총체적으로 구성합니다. 이러한 모범 사례는 시스템 및 네트워크에 대한 가장 일반적인 공격을 완화합니다. 구현 그룹 1은 일반적으로 하위 컨트롤을 구현하는 데 사용할 수 있는 리소스와 사이버 보안 전문 지식이 제한된 조직을 대상으로 정의됩니다.

CIS 컨트롤과 CIS 벤치마크의 차이점

CIS 컨트롤은 조직이 알려진 사이버 공격 벡터로부터 보호하기 위해 따를 수 있는 기초 모범 사례 지침입니다. CIS 벤치마크는 공급업체 제품에 특화된 보안 모범 사례 지침입니다. 운영 체제에서 클라우드 서비스 및 네트워크 디바이스에 이르기까지 벤치마크에서 적용되는 설정은 사용 중인 시스템을 보호합니다.

예제

- CIS 벤치마크는 규범적입니다. 이는 일반적으로 공급업체 제품에서 검토 및 설정할 수 있는 특정 설정을 참조합니다.
  - 예: CIS Amazon Web Services 파운데이션 벤치마크 v1.2.0 - 1.13 “루트 사용자” 계정에 MFA가 활성화되었는지 확인
  - 이 권장 사항은 이를 확인하는 방법과 AWS 환경의 루트 계정에 이를 설정하는 방법에 대한 규범적 지침을 제공합니다.
- CIS 컨트롤은 조직 전체를 위한 것으로 특정 공급업체 제품에만 국한되지 않습니다.
  - 예: CIS 컨트롤 v7.1 - 하위 컨트롤 4.5 모든 관리 액세스에 다중 인증 사용
  - 이 컨트롤은 조직 내에 적용될 것으로 예상되는 사항을 설명합니다. 실행 중인 시스템 및 워크로드(위치에 관계없이)에 이를 어떻게 적용해야 하는지는 설명되어 있지 않습니다.

이 프레임워크를 사용하여 감사 준비 지원

CIS 컨트롤 v7.1 IG1 프레임워크를 사용하여 감사를 준비할 수 있습니다. 이 프레임워크에는 설명 및 테스트 절차가 포함된 사전 구축된 컨트롤 컬렉션이 포함되어 있습니다. 이러한 컨트롤은 CIS 요구 사항에 따라 컨트롤 세트로 그룹화됩니다. 특정 요구 사항이 있는 내부 감사를 지원하도록 이 프레임워크와 해당 컨트롤을 사용자 지정할 수도 있습니다.

프레임워크를 출발점으로 사용하여 Audit Manager 평가를 생성하고 감사와 관련된 증거 수집을 시작할 수 있습니다. 평가를 생성하면 Audit Manager가 AWS 리소스 평가를 시작합니다. 이는 CIS 컨트롤 v7.1 IG1 프레임워크에 정의된 컨트롤을 기반으로 이 작업을 수행합니다. 감사 시기가 되면 사용자 또는 사용자가 선택한 대리인이 Audit Manager에서 수집한 증거를 검토할 수 있습니다. 어느 방식으로든 평가에서 증거 폴더를 찾아보고 평가 보고서에 포함할 증거를 선택할 수 있습니다. 또는 증거 찾기 기능을 활성화한 경우 특정 증거를 검색하고 CSV 형식으로 내보내거나 검색 결과에서 평가 보고서를 생성할 수 있습니다. 둘 중 하나의 방식으로 이 평가 보고서를 사용하여 제어가 의도한 대로 작동하고 있음을 보여줄 수 있습니다.

CIS 컨트롤 v7.1 IG1 프레임워크 세부 정보는 다음과 같습니다.

AWS Audit Manager에서의 프레임워크 이름	자동화된 컨트롤 수	수동 컨트롤 수	컨트롤 세트 수	범위 내 AWS 서비스
CIS 컨트롤 v7.1 IG1	21	22	16	• Amazon Elastic Compute Cloud • AWS CloudTrail • AWS Config • AWS Identity and Access Managemen t

> **Tip**
>
> 이 표준 프레임워크에서 데이터 소스 매핑으로 사용되는 AWS Config 규칙을 검토하려면 AuditManager_ConfigDataSourceMappings_CIS-Controls-v7.1-IG1.zip 파일을 다운로드하십시오.

이 프레임워크의 컨트롤은 시스템이 CIS 컨트롤 규정을 준수하는지 확인하기 위한 것이 아닙니다. 게다가 이는 CIS 감사 통과를 보장할 수도 없습니다. AWS Audit Manager는 수동 증거 수집이 필요한 절차상의 컨트롤을 자동으로 확인하지 않습니다.

이 프레임워크는 Audit Manager의 프레임워크 라이브러리의 표준 프레임워크 탭에서 찾을 수 있습니다.

이 프레임워크를 사용하여 평가를 생성하는 방법에 대한 지침은 평가 생성을 참조하십시오.

Audit Manager 콘솔을 사용하여 이 표준 프레임워크에서 평가를 생성하면 범위 내 AWS 서비스 목록이 기본적으로 선택되며 편집할 수 없습니다. 이는 Audit Manager가 자동으로 데이터 소스 및 서비스를 매핑하고 선택하기 때문입니다. 이 선택은 CIS 컨트롤의 요구 사항에 따라 이루어집니다. 이 프레임워크의 범위 내에서 서비스 목록을 편집해야 하는 경우 CreateAssessment 또는 UpdateAssessment API 작업을 사용하여 편집할 수 있습니다. 또는 표준 프레임워크를 사용자 지정한 다음 사용자 지정 프레임워크에서 평가를 생성할 수도 있습니다.

특정 요구 사항을 지원하도록 이 프레임워크를 사용자 지정하는 방법에 대한 지침은 기존 프레임워크 사용자 지정 및 기존 컨트롤 사용자 지정을 참조하십시오.

추가 CIS 리소스

- CIS 컨트롤 v7.1 IG1

CIS 컨트롤 v8 구현 그룹 1

AWS Audit Manager는 인터넷 보안 센터(CIS) 컨트롤 v8 구현 그룹 1을 지원하는 사전 구축된 표준 프레임워크를 제공합니다.

> **Note**
>
> CIS 컨트롤 v7.1 IG1 및 이 표준을 지원하는 AWS Audit Manager 프레임워크에 대한 자세한 내용은 CIS 컨트롤 v7.1 구현 그룹 1을 참조하십시오.

주제

CIS 컨트롤이란 무엇입니까?

CIS 중요 보안 컨트롤(CIS Controls)이란 시스템 및 네트워크에 대한 가장 널리 퍼진 사이버 공격을 완화하기 위한 우선 순위가 지정된 보호 장치 세트입니다. 이는 여러 법률, 규제 및 정책 프레임워크에 매핑되고 참조됩니다. CIS 컨트롤 v8은 최신 시스템 및 소프트웨어를 따라잡기 위해 향상되었습니다. 클라우드 기반 컴퓨팅, 가상화, 모빌리티, 아웃소싱, 재택 근무로의 전환과 변화하는 공격자 전술로 인해

업데이트가 촉발되었습니다. 이 업데이트는 기업이 완전한 클라우드 및 하이브리드 환경으로 전환할 때 기업의 보안을 지원합니다.

CIS 컨트롤과 CIS 벤치마크의 차이점

CIS 컨트롤은 조직이 알려진 사이버 공격 벡터로부터 보호하기 위해 따를 수 있는 기초 모범 사례 지침입니다. CIS 벤치마크는 공급업체 제품에 특화된 보안 모범 사례 지침입니다. 운영 체제에서 클라우드 서비스 및 네트워크 디바이스에 이르기까지 벤치마크에서 적용되는 설정은 사용 중인 시스템을 보호합니다.

예제

- CIS 벤치마크는 규범적입니다. 이는 일반적으로 공급업체 제품에서 검토 및 설정할 수 있는 특정 설정을 참조합니다.
  - 예: CIS Amazon Web Services 파운데이션 벤치마크 v1.2.0 - 1.13 “루트 사용자” 계정에 MFA가 활성화되었는지 확인
  - 이 권장 사항은 이를 확인하는 방법과 AWS 환경의 루트 계정에 이를 설정하는 방법에 대한 규범적 지침을 제공합니다.
- CIS 컨트롤은 조직 전체를 위한 것으로 특정 공급업체 제품에만 국한되지 않습니다.
  - 예: CIS 컨트롤 v7.1 - 하위 컨트롤 4.5 모든 관리 액세스에 다중 인증 사용
  - 이 컨트롤은 조직 내에 적용될 것으로 예상되는 사항을 설명합니다. 실행 중인 시스템 및 워크로드(위치에 관계없이)에 이를 어떻게 적용해야 하는지는 설명되어 있지 않습니다.

이 프레임워크를 사용하여 감사 준비 지원

CIS 컨트롤 v8 IG1 프레임워크를 사용하여 감사를 준비할 수 있습니다. 이 프레임워크에는 설명 및 테스트 절차가 포함된 사전 구축된 컨트롤 컬렉션이 포함되어 있습니다. 이러한 컨트롤은 CIS 요구 사항에 따라 컨트롤 세트로 그룹화됩니다. 특정 요구 사항이 있는 내부 감사를 지원하도록 이 프레임워크와 해당 컨트롤을 사용자 지정할 수도 있습니다.

프레임워크를 출발점으로 사용하여 Audit Manager 평가를 생성하고 감사와 관련된 증거 수집을 시작할 수 있습니다. 평가를 생성하면 Audit Manager가 AWS 리소스 평가를 시작합니다. 이는 CIS 컨트롤 v8 프레임워크에 정의된 컨트롤을 기반으로 이 작업을 수행합니다. 감사 시기가 되면 사용자 또는 사용자가 선택한 대리인이 Audit Manager에서 수집한 증거를 검토할 수 있습니다. 어느 방식으로든 평가에서 증거 폴더를 찾아보고 평가 보고서에 포함할 증거를 선택할 수 있습니다. 또는 증거 찾기 기능을 활성화한 경우 특정 증거를 검색하고 CSV 형식으로 내보내거나 검색 결과에서 평가 보고서를 생성할 수 있습니다. 둘 중 하나의 방식으로 이 평가 보고서를 사용하여 제어가 의도한 대로 작동하고 있음을 보여줄 수 있습니다.

CIS 컨트롤 v8 프레임워크 세부 정보는 다음과 같습니다.

AWS Audit Manager에서의 프레임워크 이름	자동화된 컨트롤 수	수동 컨트롤 수	컨트롤 세트 수	범위 내 AWS 서비스
CIS 컨트롤 v8 IG1	25	31	15	• Amazon Elastic Compute Cloud • AWS Config • AWS Identity and Access Management • AWS License Manager

> **Tip**
>
> 이 표준 프레임워크에서 데이터 소스 매핑으로 사용되는 AWS Config 규칙을 검토하려면 AuditManager_ConfigDataSourceMappings_CIS-Controls-v8-IG1.zip 파일을 다운로드하십시오.

이 프레임워크의 컨트롤은 시스템이 CIS 컨트롤 규정을 준수하는지 확인하기 위한 것이 아닙니다. 게다가 이는 CIS 감사 통과를 보장할 수도 없습니다. AWS Audit Manager는 수동 증거 수집이 필요한 절차상의 컨트롤을 자동으로 확인하지 않습니다.

이 프레임워크는 Audit Manager의 프레임워크 라이브러리의 표준 프레임워크 탭에서 찾을 수 있습니다.

이 프레임워크를 사용하여 평가를 생성하는 방법에 대한 지침은 평가 생성을 참조하십시오.

Audit Manager 콘솔을 사용하여 이 표준 프레임워크에서 평가를 생성하면 범위 내 AWS 서비스 목록이 기본적으로 선택되며 편집할 수 없습니다. 이는 Audit Manager가 자동으로 데이터 소스 및 서비스를 매핑하고 선택하기 때문입니다. 이 선택은 CIS 컨트롤의 요구 사항에 따라 이루어집니다. 이 프레임워크의 범위 내에서 서비스 목록을 편집해야 하는 경우 CreateAssessment 또는 UpdateAssessment API 작업을 사용하여 편집할 수 있습니다. 또는 표준 프레임워크를 사용자 지정한 다음 사용자 지정 프레임워크에서 평가를 생성할 수도 있습니다.

특정 요구 사항을 지원하도록 이 프레임워크를 사용자 지정하는 방법에 대한 지침은 기존 프레임워크 사용자 지정 및 기존 컨트롤 사용자 지정을 참조하십시오.

추가 CIS 리소스

- CIS 컨트롤 v8

FedRAMP 모더레이트 베이스라인

AWS Audit Manager는 감사 준비를 지원하는 FedRAMP 모더레이트 베이스라인 프레임워크를 제공합니다.

주제

- FedRAMP란 무엇입니까?
- 이 프레임워크를 사용하여 감사 준비 지원
- 추가 FedRAMP 리소스

FedRAMP란 무엇입니까?

연방 위험 및 인증 관리 프로그램(FedRAMP)은 2011년에 설립되었습니다. 이는 미국 연방 정부의 클라우드 서비스 채택 및 사용을 위한 비용 효율적이고 위험 기반 접근 방식을 제공합니다. FedRAMP는 연방 기관의 정보 보안 및 보호에 중점을 두고 연방 기관이 최신 클라우드 기술을 사용할 수 있도록 지원합니다.

FedRAMP 모더레이트 베이스라인 컨트롤에 대한 자세한 내용은 FedRAMP 모더레이트 보안 테스트 절차 템플릿을 참조하십시오.

이 프레임워크를 사용하여 감사 준비 지원

FedRAMP 모더레이트 베이스라인 프레임워크를 사용하여 감사를 준비할 수 있습니다. 이 프레임워크에는 설명 및 테스트 절차가 포함된 사전 구축된 컨트롤 컬렉션이 포함되어 있습니다. 이러한 컨트롤은 FedRAMP 요구 사항에 따라 컨트롤 세트로 그룹화됩니다. 특정 요구 사항이 있는 내부 감사를 지원하도록 이 프레임워크와 해당 컨트롤을 사용자 지정할 수도 있습니다.

프레임워크를 출발점으로 사용하여 Audit Manager 평가를 생성하고 감사와 관련된 증거 수집을 시작할 수 있습니다. 평가를 생성하면 Audit Manager가 AWS 리소스 평가를 시작합니다. 이는 프레임워크에 정의된 컨트롤을 기반으로 이 작업을 수행합니다. 감사 시기가 되면 사용자 또는 사용자가 선택한

대리인이 Audit Manager에서 수집한 증거를 검토할 수 있습니다. 어느 방식으로든 평가에서 증거 폴더를 찾아보고 평가 보고서에 포함할 증거를 선택할 수 있습니다. 또는 증거 찾기 기능을 활성화한 경우 특정 증거를 검색하고 CSV 형식으로 내보내거나 검색 결과에서 평가 보고서를 생성할 수 있습니다. 둘 중 하나의 방식으로 이 평가 보고서를 사용하여 제어가 의도한 대로 작동하고 있음을 보여줄 수 있습니다.

FedRAMP 모더레이트 베이스라인 프레임워크의 세부 정보는 다음과 같습니다.

AWS Audit Manager에서의 프레임워크 이름	자동화된 컨트롤 수	수동 컨트롤 수	컨트롤 세트 수	범위 내 AWS 서비스
FedRAMP 모더레이트 베이스라인	303	908	325	• Amazon Elastic Compute Cloud • AWS Config • AWS Identity and Access Management

> **Tip**
>
> 이 표준 프레임워크에서 데이터 소스 매핑으로 사용되는 AWS Config 규칙을 검토하려면 AuditManager_ConfigDataSourceMappings_FedRAMP-Moderate-Baseline.zip 파일을 다운로드하십시오.

이 프레임워크의 컨트롤은 시스템이 FedRAMP를 준수하는지 확인하기 위한 것이 아닙니다. 게다가 이는 FedRAMP 감사를 통과할 것이라고 보장할 수도 없습니다. AWS Audit Manager는 수동 증거 수집이 필요한 절차상의 컨트롤을 자동으로 확인하지 않습니다.

이 프레임워크는 Audit Manager의 프레임워크 라이브러리의 표준 프레임워크 탭에서 찾을 수 있습니다.

이 프레임워크를 사용하여 평가를 생성하는 방법에 대한 지침은 평가 생성을 참조하십시오.

Audit Manager 콘솔을 사용하여 이 표준 프레임워크에서 평가를 생성하면 범위 내 AWS 서비스 목록이 기본적으로 선택되며 편집할 수 없습니다. 이는 Audit Manager가 자동으로 데이터 소스 및 서비스를 매핑하고 선택하기 때문입니다. 이 선택은 FedRAMP 모더레이트 베이스라인의 요구 사항에 따라

이루어집니다. 이 프레임워크의 범위 내에서 서비스 목록을 편집해야 하는 경우 CreateAssessment 또는 UpdateAssessment API 작업을 사용하여 편집할 수 있습니다. 또는 표준 프레임워크를 사용자 지정한 다음 사용자 지정 프레임워크에서 평가를 생성할 수도 있습니다.

특정 요구 사항을 지원하도록 이 프레임워크를 사용자 지정하는 방법에 대한 지침은 기존 프레임워크 사용자 지정 및 기존 컨트롤 사용자 지정을 참조하십시오.

추가 FedRAMP 리소스

- FedRAMP AWS 규정 준수 페이지
- AWS FedRAMP 블로그 게시물

일반 데이터 보호 규정(GDPR)

AWS Audit Manager는 일반 데이터 보호 규정(GDPR)을 지원하는 사전 구축된 표준 프레임워크입니다. 기본적으로 이 프레임워크에는 수동 컨트롤만 포함됩니다. 이러한 수동 컨트롤은 증거를 자동으로 수집하지 않습니다. 하지만 GDPR에 따른 일부 컨트롤에 대한 증거 수집을 자동화하려는 경우 AWS Audit Manager의 사용자 지정 컨트롤 기능을 사용할 수 있습니다. 자세한 내용은 이 프레임워크를 사용하여 감사 준비 지원을 참조하십시오.

주제

- 일반 데이터 보호 규정(GDPR)이란 무엇입니까?
- 이 프레임워크를 사용하여 감사 준비 지원
- 추가 GDPR 리소스

일반 데이터 보호 규정(GDPR)이란 무엇입니까?

일반 데이터 보호 규정 (General Data Protection Regulation, GDPR)은 2018년 5월 25일에 시행된 새로운 유럽 개인 정보 보호법입니다. GDPR은 지침 95/46/EC라고도 하는 EU 데이터 보호 지침을 대체합니다. 이는 유럽 연합(EU) 전역의 데이터 보호법을 조화시키기 위한 것입니다. 이는 각 EU 회원국 전체에 걸쳐 구속력이 있는 단일 데이터 보호법을 적용하여 이루어집니다.

GDPR은 EU 내에 설립된 모든 조직 및 EU 내에서 발생하는 행위의 모니터링 또는 EU 내의 데이터 주체에 대한 상품 또는 서비스 제공과 관련하여 EU 데이터 주체의 개인 데이터를 처리하는 조직(EU 내에 설립되었는지 여부에 관계없이)에 적용됩니다. 개인 데이터는 식별되거나 식별 가능한 자연인과 관련된 모든 정보입니다.

GDPR 프레임워크는 AWS Audit Manager의 프레임워크 라이브러리 페이지에서 찾을 수 있습니다. 자세한 내용은 일반 데이터 보호 규정(GDPR) 센터를 참조하십시오..

이 프레임워크를 사용하여 감사 준비 지원

AWS Audit Manager에서 GDPR 프레임워크를 사용하여 감사를 준비할 수 있습니다.

프레임워크 세부 정보는 다음과 같습니다.

AWS Audit Manager에서의 프레임워크 이름	자동화된 컨트롤 수	수동 컨트롤 수	컨트롤 세트 수	범위 내 AWS 서비스
GDPR	0	371	10	None

Audit Manager의 표준 프레임워크 탭에서 GDPR 프레임워크를 찾을 수 프레임워크 라이브러리 있습니다. 이 표준 프레임워크에는 수동 컨트롤만 포함되어 있으므로 AWS 서비스은 범위에 포함되지 않습니다.

> **Note**
>
> GDPR에 대한 증거 수집을 자동화하려는 경우 Audit Manager를 GDPR에 대한 자체 사용자 지정 컨트롤 생성에 사용할 수 있습니다. 다음 표에는 사용자 지정 컨트롤의 GDPR 요구 사항에 매핑할 수 있는 AWS 데이터 소스에 대한 권장 사항이 나와 있습니다. 다음 데이터 소스 중 일부는 여러 컨트롤에 매핑되어 있지만 각 리소스 평가에 대해 한 번만 요금이 부과된다는 점에 유의하십시오.
> 다음 권장 사항은 AWS Config 및 AWS Security Hub를 데이터 소스로 사용합니다. 이러한 데이터 소스에서 증거를 성공적으로 수집하려면 다음을 수행해야 합니다.
>
> - 지침에 따라 AWS 계정에서 AWS Config 및 AWS Security Hub을 활성화하고 설정했는지 확인합니다.
> - AWS Config와 보안 허브를 모두 범위 내 서비스로 포함했는지 확인하십시오. 평가 범위에 해당하는 서비스 목록을 검토하려면 평가 검토, AWS 서비스 탭을 참조하십시오. 이 목록을 편집하려면 범위 내 AWS 서비스 편집을 참조하십시오.
>
> 이러한 방식으로 두 서비스를 모두 설정한 후에는 지정된 AWS Config 규칙 또는 보안 허브 컨트롤에 대한 평가가 수행될 때마다 Audit Manager가 증거를 수집합니다.

컨트롤 이름	컨트롤 세트	권장 컨트롤 데이터 소스 매핑
제25조 설계 및 기본설정에 의한 개인정보 보호.1	제4장 - 컨트롤러 및 프로세서	이 GDPR 컨트롤을 지원하는 AWS Audit Manager에서 사용자 지정 컨트롤을 생성할 수 있습니다. 컨트롤 세부 사항을 지정하는 경우 테스트 정보에 다음을 입력합니다. • 기간 동안의 모든 루트 계정 이벤트 표시 • AWS CloudTrail 버킷은 공개되지 않음 • `Allow:*:*` 이 포함된 모든 정책을 표시하고 해당 정책을 사용하는 모든 보안 주체 및 서비스를 나열합니다. 컨트롤 데이터 소스를 설정할 때는 다음을 모두 데이터 소스로 포함하는 것이 좋습니다. AWS Config을 데이터 소스 유형으로 선택하고 다음 AWS Config 관리형 규칙을 데이터 소스 매핑으로 선택합니다. • IAM_ROOT_ACCESS_KEY_CHECK • ROOT_ACCOUNT_MFA_ENABLED • ROOT_ACCOUNT_HARDWARE_MFA_ENABLED • VPC_FLOW_LOGS_ENABLED • ACCESS_KEYS_ROTATED • IAM_PASSWORD_POLICY AWS Security Hub을 데이터 소스 유형으로 선택하고 다음 보안 허브 컨트롤을 데이터 소스 매핑으로 선택합니다. • 1.1 (CloudWatch.1) • 1.1 (IAM.20) • 1.10 (IAM.16) • 1.11 (IAM.17) • 1.12 (IAM.4) • 1.13 (IAM.9)

컨트롤 이름	컨트롤 세트	권장 컨트롤 데이터 소스 매핑
		• 1.14 (IAM.6) • 1.16 (IAM.2) • 1.2 (IAM.5 • 1.20 (IAM.18) • 1.22 (IAM.1) • 1.3 (IAM.8) • 1.4 (IAM.3) • 1.5 (IAM.11) • 1.6 (IAM.12) • 1.7 (IAM.13) • 1.8 (IAM.14) • 1.9 (IAM.15) • 2.1 (CloudTrail.1) • 2.2 (CloudTrail.4) • 2.3 (CloudTrail.6) • 2.4 (CloudTrail.5) • 2.5 (Config.1) • 2.6 (CloudTrail.7) • 2.7 (CloudTrail.2) • 2.8 (KMS.4) • 2.9 (EC2.6) • 3.1 (CloudWatch.2) • 3.10 (CloudWatch.10) • 3.11 (CloudWatch.11) • 3.12 (CloudWatch.12) • 3.13 (CloudWatch.13) • 3.14 (CloudWatch.14) • Config.1

컨트롤 이름	컨트롤 세트	권장 컨트롤 데이터 소스 매핑
제25조 설계 및 기본설정에 의한 개인정보 보호.2	제4장 - 컨트롤러 및 프로세서	이 GDPR 컨트롤을 지원하는 AWS Audit Manager에서 사용자 지정 컨트롤을 생성할 수 있습니다. 컨트롤 세부 사항을 지정하는 경우 테스트 정보에 다음을 입력합니다. • 기간 동안의 모든 루트 계정 이벤트 표시 • AWS CloudTrail 버킷은 공개되지 않음 • `Allow:*:*` 이 포함된 모든 정책을 표시하고 해당 정책을 사용하는 모든 보안 주체 및 서비스를 나열합니다. 컨트롤 데이터 소스를 설정할 때는 다음을 모두 데이터 소스로 포함하는 것이 좋습니다. AWS Config을 데이터 소스 유형으로 선택하고 다음 AWS Config 관리형 규칙을 데이터 소스 매핑으로 선택합니다. • IAM_ROOT_ACCESS_KEY_CHECK • ROOT_ACCOUNT_MFA_ENABLED • ROOT_ACCOUNT_HARDWARE_MFA_ENABLED • VPC_FLOW_LOGS_ENABLED • ACCESS_KEYS_ROTATED • IAM_PASSWORD_POLICY AWS Security Hub을 데이터 소스 유형으로 선택하고 다음 보안 허브 컨트롤을 데이터 소스 매핑으로 선택합니다. • 1.1 (CloudWatch.1) • 1.1 (IAM.20) • 1.10 (IAM.16) • 1.11 (IAM.17) • 1.12 (IAM.4) • 1.13 (IAM.9)

컨트롤 이름	컨트롤 세트	권장 컨트롤 데이터 소스 매핑
		• 1.14 (IAM.6) • 1.16 (IAM.2) • 1.2 (IAM.5 • 1.20 (IAM.18) • 1.22 (IAM.1) • 1.3 (IAM.8) • 1.4 (IAM.3) • 1.5 (IAM.11) • 1.6 (IAM.12) • 1.7 (IAM.13) • 1.8 (IAM.14) • 1.9 (IAM.15) • 2.1 (CloudTrail.1) • 2.2 (CloudTrail.4) • 2.3 (CloudTrail.6) • 2.4 (CloudTrail.5) • 2.5 (Config.1) • 2.6 (CloudTrail.7) • 2.7 (CloudTrail.2) • 2.8 (KMS.4) • 2.9 (EC2.6) • 3.1 (CloudWatch.2) • 3.10 (CloudWatch.10) • 3.11 (CloudWatch.11) • 3.12 (CloudWatch.12) • 3.13 (CloudWatch.13) • 3.14 (CloudWatch.14)

컨트롤 이름	컨트롤 세트	권장 컨트롤 데이터 소스 매핑
		• Config.1

컨트롤 이름	컨트롤 세트	권장 컨트롤 데이터 소스 매핑
제25조 설계 및 기본설정에 의한 개인정보 보호.3	제4장 - 컨트롤러 및 프로세서	이 GDPR 컨트롤을 지원하는 AWS Audit Manager에서 사용자 지정 컨트롤을 생성할 수 있습니다. 컨트롤 세부 사항을 지정하는 경우 테스트 정보에 다음을 입력합니다. • 기간 동안의 모든 루트 계정 이벤트 표시 • AWS CloudTrail 버킷은 공개되지 않음 • `Allow:*:*` 이 포함된 모든 정책을 표시하고 해당 정책을 사용하는 모든 보안 주체 및 서비스를 나열합니다. 컨트롤 데이터 소스를 설정할 때는 다음을 모두 데이터 소스로 포함하는 것이 좋습니다. AWS Config을 데이터 소스 유형으로 선택하고 다음 AWS Config 관리형 규칙을 데이터 소스 매핑으로 선택합니다. • IAM_ROOT_ACCESS_KEY_CHECK • ROOT_ACCOUNT_MFA_ENABLED • ROOT_ACCOUNT_HARDWARE_MFA_ENABLED • VPC_FLOW_LOGS_ENABLED • ACCESS_KEYS_ROTATED • IAM_PASSWORD_POLICY AWS Security Hub을 데이터 소스 유형으로 선택하고 다음 보안 허브 컨트롤을 데이터 소스 매핑으로 선택합니다. • 1.1 (CloudWatch.1) • 1.1 (IAM.20) • 1.10 (IAM.16) • 1.11 (IAM.17) • 1.12 (IAM.4) • 1.13 (IAM.9)

컨트롤 이름	컨트롤 세트	권장 컨트롤 데이터 소스 매핑
		• 1.14 (IAM.6) • 1.16 (IAM.2) • 1.2 (IAM.5 • 1.20 (IAM.18) • 1.22 (IAM.1) • 1.3 (IAM.8) • 1.4 (IAM.3) • 1.5 (IAM.11) • 1.6 (IAM.12) • 1.7 (IAM.13) • 1.8 (IAM.14) • 1.9 (IAM.15) • 2.1 (CloudTrail.1) • 2.2 (CloudTrail.4) • 2.3 (CloudTrail.6) • 2.4 (CloudTrail.5) • 2.5 (Config.1) • 2.6 (CloudTrail.7) • 2.7 (CloudTrail.2) • 2.8 (KMS.4) • 2.9 (EC2.6) • 3.1 (CloudWatch.2) • 3.10 (CloudWatch.10) • 3.11 (CloudWatch.11) • 3.12 (CloudWatch.12) • 3.13 (CloudWatch.13) • 3.14 (CloudWatch.14)

컨트롤 이름	컨트롤 세트	권장 컨트롤 데이터 소스 매핑
		• Config.1
제30조 처리 활동 기록.1	제4장 - 컨트롤러 및 프로세서	이 GDPR 컨트롤을 지원하는 AWS Audit Manager에서 사용자 지정 컨트롤을 생성할 수 있습니다. 컨트롤 세부 사항을 지정하는 경우 테스트 정보에 다음을 입력합니다. • 기간 동안의 모든 루트 계정 이벤트 표시 컨트롤 데이터 소스를 설정할 때는 다음을 모두 데이터 소스로 포함하는 것이 좋습니다. AWS Config을 데이터 소스 유형으로 선택하고 다음 AWS Config 관리형 규칙을 데이터 소스 매핑으로 선택합니다. • CLOUD_TRAIL_ENCRYPTION_ENABLED • CLOUD_TRAIL_LOG_FILE_VALIDATION_ENABLED • VPC_FLOW_LOGS_ENABLED • CMK_BACKING_KEY_ROTATION_ENABLED • CLOUD_TRAIL_ENABLED • ELB_LOGGING_ENABLED • CLOUDTRAIL_SECURITY_TRAIL_ENABLED • REDSHIFT_CLUSTER_CONFIGURATION_CHECK • CLOUD_TRAIL_CLOUD_WATCH_LOGS_ENABLED AWS Security Hub을 데이터 소스 유형으로 선택하고 다음 보안 허브 컨트롤을 데이터 소스 매핑으로 선택합니다. • Config.1

컨트롤 이름	컨트롤 세트	권장 컨트롤 데이터 소스 매핑
제30조 처리 활동 기록.2	제4장 - 컨트롤러 및 프로세서	이 GDPR 컨트롤을 지원하는 AWS Audit Manager에서 사용자 지정 컨트롤을 생성할 수 있습니다. 컨트롤 세부 사항을 지정하는 경우 테스트 정보에 다음을 입력합니다. • 기간 동안의 모든 루트 계정 이벤트 표시 컨트롤 데이터 소스를 설정할 때는 다음을 모두 데이터 소스로 포함하는 것이 좋습니다. AWS Config을 데이터 소스 유형으로 선택하고 다음 AWS Config 관리형 규칙을 데이터 소스 매핑으로 선택합니다. • CLOUD_TRAIL_ENCRYPTION_ENABLED • CLOUD_TRAIL_LOG_FILE_VALIDATION_ENABLED • VPC_FLOW_LOGS_ENABLED • CMK_BACKING_KEY_ROTATION_ENABLED • CLOUD_TRAIL_ENABLED • ELB_LOGGING_ENABLED • CLOUD_TRAIL_CLOUD_WATCH_LOGS_ENABLED AWS Security Hub을 데이터 소스 유형으로 선택하고 다음 보안 허브 컨트롤을 데이터 소스 매핑으로 선택합니다. • Config.1

컨트롤 이름	컨트롤 세트	권장 컨트롤 데이터 소스 매핑
제30조 처리 활동 기록.3	제4장 - 컨트롤러 및 프로세서	이 GDPR 컨트롤을 지원하는 AWS Audit Manager에서 사용자 지정 컨트롤을 생성할 수 있습니다. 컨트롤 세부 사항을 지정하는 경우 테스트 정보에 다음을 입력합니다. • 기간 동안의 모든 루트 계정 이벤트 표시 • AWS CloudTrail 버킷은 공개되지 않음 • `Allow:*:*` 이 포함된 모든 정책을 표시하고 해당 정책을 사용하는 모든 보안 주체 및 서비스를 나열합니다. 컨트롤 데이터 소스를 설정할 때는 다음을 모두 데이터 소스로 포함하는 것이 좋습니다. AWS Config을 데이터 소스 유형으로 선택하고 다음 AWS Config 관리형 규칙을 데이터 소스 매핑으로 선택합니다. • CLOUD_TRAIL_ENCRYPTION_ENABLED • CLOUD_TRAIL_LOG_FILE_VALIDATION_ENABLED • VPC_FLOW_LOGS_ENABLED • CMK_BACKING_KEY_ROTATION_ENABLED • CLOUD_TRAIL_ENABLED • ELB_LOGGING_ENABLED • CLOUD_TRAIL_CLOUD_WATCH_LOGS_ENABLED AWS Security Hub을 데이터 소스 유형으로 선택하고 다음 보안 허브 컨트롤을 데이터 소스 매핑으로 선택합니다. • Config.1

컨트롤 이름	컨트롤 세트	권장 컨트롤 데이터 소스 매핑
제30조 처리 활동 기록.4	제4장 - 컨트롤러 및 프로세서	이 GDPR 컨트롤을 지원하는 AWS Audit Manager에서 사용자 지정 컨트롤을 생성할 수 있습니다. 컨트롤 세부 사항을 지정하는 경우 테스트 정보에 다음을 입력합니다. • 기간 동안의 모든 루트 계정 이벤트 표시 • AWS CloudTrail 버킷은 공개되지 않음 • `Allow:*:*` 이 포함된 모든 정책을 표시하고 해당 정책을 사용하는 모든 보안 주체 및 서비스를 나열합니다. 컨트롤 데이터 소스를 설정할 때는 다음을 모두 데이터 소스로 포함하는 것이 좋습니다. AWS Config을 데이터 소스 유형으로 선택하고 다음 AWS Config 관리형 규칙을 데이터 소스 매핑으로 선택합니다. • CLOUD_TRAIL_ENCRYPTION_ENABLED • CLOUD_TRAIL_LOG_FILE_VALIDATION_ENABLED • VPC_FLOW_LOGS_ENABLED • CMK_BACKING_KEY_ROTATION_ENABLED • CLOUD_TRAIL_ENABLED • ELB_LOGGING_ENABLED • CLOUD_TRAIL_CLOUD_WATCH_LOGS_ENABLED AWS Security Hub을 데이터 소스 유형으로 선택하고 다음 보안 허브 컨트롤을 데이터 소스 매핑으로 선택합니다. • Config.1

컨트롤 이름	컨트롤 세트	권장 컨트롤 데이터 소스 매핑
제30조 처리 활동 기록.5	제4장 - 컨트롤러 및 프로세서	이 GDPR 컨트롤을 지원하는 AWS Audit Manager에서 사용자 지정 컨트롤을 생성할 수 있습니다. 컨트롤 세부 사항을 지정하는 경우 테스트 정보에 다음을 입력합니다. • 기간 동안의 모든 루트 계정 이벤트 표시 컨트롤 데이터 소스를 설정할 때는 다음을 모두 데이터 소스로 포함하는 것이 좋습니다. AWS Config을 데이터 소스 유형으로 선택하고 다음 AWS Config 관리형 규칙을 데이터 소스 매핑으로 선택합니다. • CLOUD_TRAIL_ENCRYPTION_ENABLED • CLOUD_TRAIL_LOG_FILE_VALIDATION_ENABLED • VPC_FLOW_LOGS_ENABLED • CMK_BACKING_KEY_ROTATION_ENABLED • CLOUD_TRAIL_ENABLED • ELB_LOGGING_ENABLED • CLOUD_TRAIL_CLOUD_WATCH_LOGS_ENABLED AWS Security Hub을 데이터 소스 유형으로 선택하고 다음 보안 허브 컨트롤을 데이터 소스 매핑으로 선택합니다. • Config.1

컨트롤 이름	컨트롤 세트	권장 컨트롤 데이터 소스 매핑
제32조 처리의 보안.1	제4장 - 컨트롤러 및 프로세서	이 GDPR 컨트롤을 지원하는 AWS Audit Manager에서 사용자 지정 컨트롤을 생성할 수 있습니다. 컨트롤 세부 사항을 지정하는 경우 테스트 정보에 다음을 입력합니다. • 모든 서비스에 대한 데이터 저장 시 암호화 표시 • 모든 서비스에 대한 데이터 전송 중 암호화 표시 • Amazon S3에 대해 MFA 삭제 활성화 • 모든 Amazon Inspector 스캔 • Amazon Inspector가 활성화되지 않은 모든 인스턴스 표시 • HTTPS(SSL)에서 수신 중인 모든 로드 밸런서 표시 • AWS CloudTrail 휴식 시 암호화 • 모든 변경 사항 및 설명이 달린 모든 설정을 표시하는 AWS Config에 대한 Amazon CloudWatch 알림 • 모든 루트 활동 컨트롤 데이터 소스를 설정할 때는 다음을 모두 데이터 소스로 포함하는 것이 좋습니다. AWS Config을 데이터 소스 유형으로 선택하고 다음 AWS Config 관리형 규칙을 데이터 소스 매핑으로 선택합니다. • CLOUD_TRAIL_LOG_FILE_VALIDATION_ENABLED • S3_BUCKET_SSL_REQUESTS_ONLY • CLOUD_TRAIL_ENCRYPTION_ENABLED • CLOUDWATCH_LOG_GROUP_ENCRYPTED • EFS_ENCRYPTED_CHECK • ELASTICSEARCH_ENCRYPTED_AT_REST • ENCRYPTED_VOLUMES • RDS_STORAGE_ENCRYPTED • REDSHIFT_CLUSTER_CONFIGURATION_CHECK

컨트롤 이름	컨트롤 세트	권장 컨트롤 데이터 소스 매핑
		• S3_BUCKET_SERVER_SIDE_ENCRYPTION_ENABLED • SAGEMAKER_ENDPOINT_CONFIGURATION_KMS_KEY_CONFIGURED • SAGEMAKER_NOTEBOOK_INSTANCE_KMS_KEY_CONFIGURED • SNS_ENCRYPTED_KMS • EC2_EBS_ENCRYPTION_BY_DEFAULT • DYNAMODB_TABLE_ENCRYPTED_KMS • DYNAMODB_TABLE_ENCRYPTION_ENABLED • RDS_SNAPSHOT_ENCRYPTED • S3_DEFAULT_ENCRYPTION_KMS • DAX_ENCRYPTION_ENABLED • EKS_SECRETS_ENCRYPTED • RDS_LOGGING_ENABLED • REDSHIFT_BACKUP_ENABLED • RDS_IN_BACKUP_PLAN • WAF_CLASSIC_LOGGING_ENABLED • WAFV2_LOGGING_ENABLED • ALB_HTTP_TO_HTTPS_REDIRECTION_CHECK • ELB_ACM_CERTIFICATE_REQUIRED • ELB_CUSTOM_SECURITY_POLICY_SSL_CHECK • REDSHIFT_REQUIRE_TLS_SSL • CLOUDFRONT_VIEWER_POLICY_HTTPS • ALB_HTTP_DROP_INVALID_HEADER_ENABLED • ELASTICSEARCH_NODE_TO_NODE_ENCRYPTION_CHECK • ELB_TLS_HTTPS_LISTENERS_ONLY • ACM_CERTIFICATE_EXPIRATION_CHECK • API_GW_CACHE_ENABLED_AND_ENCRYPTED

컨트롤 이름	컨트롤 세트	권장 컨트롤 데이터 소스 매핑
제32조 처리의 보안.2	제4장 - 컨트롤러 및 프로세서	이 GDPR 컨트롤을 지원하는 AWS Audit Manager에서 사용자 지정 컨트롤을 생성할 수 있습니다. 컨트롤 세부 사항을 지정하는 경우 테스트 정보에 다음을 입력합니다. • 모든 서비스에 대한 데이터 저장 시 암호화 표시 • 모든 서비스에 대한 데이터 전송 중 암호화 표시 • Amazon S3에 대해 MFA 삭제 활성화 • 모든 Amazon Inspector 스캔 • Amazon Inspector가 활성화되지 않은 모든 인스턴스 보기 • HTTPS(SSL)에서 수신 중인 모든 로드 밸런서 표시 • AWS CloudTrail 휴식 시 암호화 • 모든 변경 사항 및 설명이 달린 모든 설정을 표시하는 AWS Config에 대한 Amazon CloudWatch 알림 • 모든 루트 활동 컨트롤 데이터 소스를 설정할 때는 다음을 모두 데이터 소스로 포함하는 것이 좋습니다. AWS Config을 데이터 소스 유형으로 선택하고 다음 AWS Config 관리형 규칙을 데이터 소스 매핑으로 선택합니다. • CLOUD_TRAIL_LOG_FILE_VALIDATION_ENABLED • S3_BUCKET_SSL_REQUESTS_ONLY • CLOUD_TRAIL_ENCRYPTION_ENABLED • CLOUDWATCH_LOG_GROUP_ENCRYPTED • EFS_ENCRYPTED_CHECK • ELASTICSEARCH_ENCRYPTED_AT_REST • ENCRYPTED_VOLUMES • RDS_STORAGE_ENCRYPTED • REDSHIFT_CLUSTER_CONFIGURATION_CHECK

컨트롤 이름	컨트롤 세트	권장 컨트롤 데이터 소스 매핑
		• S3_BUCKET_SERVER_SIDE_ENCRYPTION_ENABLED • SAGEMAKER_ENDPOINT_CONFIGURATION_KMS_KEY_CONFIGURED • SAGEMAKER_NOTEBOOK_INSTANCE_KMS_KEY_CONFIGURED • SNS_ENCRYPTED_KMS • EC2_EBS_ENCRYPTION_BY_DEFAULT • DYNAMODB_TABLE_ENCRYPTED_KMS • DYNAMODB_TABLE_ENCRYPTION_ENABLED • RDS_SNAPSHOT_ENCRYPTED • S3_DEFAULT_ENCRYPTION_KMS • DAX_ENCRYPTION_ENABLED • EKS_SECRETS_ENCRYPTED • RDS_LOGGING_ENABLED • REDSHIFT_BACKUP_ENABLED • RDS_IN_BACKUP_PLAN • WAF_CLASSIC_LOGGING_ENABLED • WAFV2_LOGGING_ENABLED • ALB_HTTP_TO_HTTPS_REDIRECTION_CHECK • ELB_ACM_CERTIFICATE_REQUIRED • ELB_CUSTOM_SECURITY_POLICY_SSL_CHECK • REDSHIFT_REQUIRE_TLS_SSL • CLOUDFRONT_VIEWER_POLICY_HTTPS • ALB_HTTP_DROP_INVALID_HEADER_ENABLED • ELASTICSEARCH_NODE_TO_NODE_ENCRYPTION_CHECK • ELB_TLS_HTTPS_LISTENERS_ONLY • ACM_CERTIFICATE_EXPIRATION_CHECK • API_GW_CACHE_ENABLED_AND_ENCRYPTED

컨트롤 이름	컨트롤 세트	권장 컨트롤 데이터 소스 매핑
제32조 처리의 보안.3	제4장 - 컨트롤러 및 프로세서	이 GDPR 컨트롤을 지원하는 AWS Audit Manager에서 사용자 지정 컨트롤을 생성할 수 있습니다. 컨트롤 세부 사항을 지정하는 경우 테스트 정보에 다음을 입력합니다. • 모든 서비스에 대한 데이터 저장 시 암호화 표시 • 모든 서비스에 대한 데이터 전송 중 암호화 표시 • Amazon S3에 대해 MFA 삭제 활성화 • 모든 Amazon Inspector 스캔 • Amazon Inspector가 활성화되지 않은 모든 인스턴스 보기 • HTTPS(SSL)에서 수신 중인 모든 로드 밸런서 표시 • AWS CloudTrail 휴식 시 암호화 • 모든 변경 사항 및 설명이 달린 모든 설정을 표시하는 AWS Config에 대한 Amazon CloudWatch 알림 • 모든 루트 활동 컨트롤 데이터 소스를 설정할 때는 다음을 모두 데이터 소스로 포함하는 것이 좋습니다. AWS Config을 데이터 소스 유형으로 선택하고 다음 AWS Config 관리형 규칙을 데이터 소스 매핑으로 선택합니다. • CLOUD_TRAIL_LOG_FILE_VALIDATION_ENABLED • S3_BUCKET_SSL_REQUESTS_ONLY • CLOUD_TRAIL_ENCRYPTION_ENABLED • CLOUDWATCH_LOG_GROUP_ENCRYPTED • EFS_ENCRYPTED_CHECK • ELASTICSEARCH_ENCRYPTED_AT_REST • ENCRYPTED_VOLUMES • RDS_STORAGE_ENCRYPTED • REDSHIFT_CLUSTER_CONFIGURATION_CHECK

컨트롤 이름	컨트롤 세트	권장 컨트롤 데이터 소스 매핑
		• S3_BUCKET_SERVER_SIDE_ENCRYPTION_ENABLED • SAGEMAKER_ENDPOINT_CONFIGURATION_KMS_KEY_CONFIGURED • SAGEMAKER_NOTEBOOK_INSTANCE_KMS_KEY_CONFIGURED • SNS_ENCRYPTED_KMS • EC2_EBS_ENCRYPTION_BY_DEFAULT • DYNAMODB_TABLE_ENCRYPTED_KMS • DYNAMODB_TABLE_ENCRYPTION_ENABLED • RDS_SNAPSHOT_ENCRYPTED • S3_DEFAULT_ENCRYPTION_KMS • DAX_ENCRYPTION_ENABLED • EKS_SECRETS_ENCRYPTED • RDS_LOGGING_ENABLED • REDSHIFT_BACKUP_ENABLED • RDS_IN_BACKUP_PLAN • WAF_CLASSIC_LOGGING_ENABLED • WAFV2_LOGGING_ENABLED • ALB_HTTP_TO_HTTPS_REDIRECTION_CHECK • ELB_ACM_CERTIFICATE_REQUIRED • ELB_CUSTOM_SECURITY_POLICY_SSL_CHECK • REDSHIFT_REQUIRE_TLS_SSL • CLOUDFRONT_VIEWER_POLICY_HTTPS • ALB_HTTP_DROP_INVALID_HEADER_ENABLED • ELASTICSEARCH_NODE_TO_NODE_ENCRYPTION_CHECK • ELB_TLS_HTTPS_LISTENERS_ONLY • ACM_CERTIFICATE_EXPIRATION_CHECK • API_GW_CACHE_ENABLED_AND_ENCRYPTED

컨트롤 이름	컨트롤 세트	권장 컨트롤 데이터 소스 매핑
제32조 처리의 보안 4	제4장 - 컨트롤러 및 프로세서	이 GDPR 컨트롤을 지원하는 AWS Audit Manager에서 사용자 지정 컨트롤을 생성할 수 있습니다. 컨트롤 세부 사항을 지정하는 경우 테스트 정보에 다음을 입력합니다. • 모든 서비스에 대한 데이터 저장 시 암호화 표시 • 모든 서비스에 대한 데이터 전송 중 암호화 표시 • Amazon S3에 대해 MFA 삭제 활성화 • 모든 Amazon Inspector 스캔 • Amazon Inspector가 활성화되지 않은 모든 인스턴스 보기 • HTTPS(SSL)에서 수신 중인 모든 로드 밸런서 표시 • AWS CloudTrail 휴식 시 암호화 • 모든 변경 사항 및 설명이 달린 모든 설정을 표시하는 AWS Config에 대한 Amazon CloudWatch 알림 • 모든 루트 활동 컨트롤 데이터 소스를 설정할 때는 다음을 모두 데이터 소스로 포함하는 것이 좋습니다. AWS Config을 데이터 소스 유형으로 선택하고 다음 AWS Config 관리형 규칙을 데이터 소스 매핑으로 선택합니다. • CLOUD_TRAIL_LOG_FILE_VALIDATION_ENABLED • S3_BUCKET_SSL_REQUESTS_ONLY • CLOUD_TRAIL_ENCRYPTION_ENABLED • CLOUDWATCH_LOG_GROUP_ENCRYPTED • EFS_ENCRYPTED_CHECK • ELASTICSEARCH_ENCRYPTED_AT_REST • ENCRYPTED_VOLUMES • RDS_STORAGE_ENCRYPTED • REDSHIFT_CLUSTER_CONFIGURATION_CHECK

컨트롤 이름	컨트롤 세트	권장 컨트롤 데이터 소스 매핑
		• S3_BUCKET_SERVER_SIDE_ENCRYPTION_ENABLED • SAGEMAKER_ENDPOINT_CONFIGURATION_KMS_KEY_CONFIGURED • SAGEMAKER_NOTEBOOK_INSTANCE_KMS_KEY_CONFIGURED • SNS_ENCRYPTED_KMS • EC2_EBS_ENCRYPTION_BY_DEFAULT • DYNAMODB_TABLE_ENCRYPTED_KMS • DYNAMODB_TABLE_ENCRYPTION_ENABLED • RDS_SNAPSHOT_ENCRYPTED • S3_DEFAULT_ENCRYPTION_KMS • DAX_ENCRYPTION_ENABLED • EKS_SECRETS_ENCRYPTED • RDS_LOGGING_ENABLED • REDSHIFT_BACKUP_ENABLED • RDS_IN_BACKUP_PLAN • WAF_CLASSIC_LOGGING_ENABLED • WAFV2_LOGGING_ENABLED • ALB_HTTP_TO_HTTPS_REDIRECTION_CHECK • ELB_ACM_CERTIFICATE_REQUIRED • ELB_CUSTOM_SECURITY_POLICY_SSL_CHECK • REDSHIFT_REQUIRE_TLS_SSL • CLOUDFRONT_VIEWER_POLICY_HTTPS • ALB_HTTP_DROP_INVALID_HEADER_ENABLED • ELASTICSEARCH_NODE_TO_NODE_ENCRYPTION_CHECK • ELB_TLS_HTTPS_LISTENERS_ONLY • ACM_CERTIFICATE_EXPIRATION_CHECK • API_GW_CACHE_ENABLED_AND_ENCRYPTED

GDPR에 대한 새로운 사용자 지정 컨트롤을 생성한 후에는 사용자 지정 GDPR 프레임워크에 추가할 수 있습니다. 자세한 정보는 사용자 지정 프레임워크 만들기 및 사용자 지정 프레임워크 편집을 참조하십시오. 그런 다음 사용자 지정 GDPR 프레임워크에서 평가를 생성할 수 있습니다. 이렇게 하면 AWS Audit Manager는 추가한 사용자 지정 컨트롤 항목에 대한 증거를 자동으로 수집할 수 있습니다. 프레임워크로부터 평가를 생성하는 방법에 대한 지침은 평가 생성을 참조하십시오.

추가 GDPR 리소스

- 일반 데이터 보호 규정(GDPR) 센터
- AWS GDPR 블로그 게시물

Gramm-Leach-Bliley 법

AWS Audit Manager는 그램-리치-블라일리 법(GLBA)을 지원하는 사전 구축된 프레임워크를 제공합니다.

주제

- 그램-리치-블라일리 법(GLBA)이란 무엇입니까?
- 이 프레임워크를 사용하여 감사 준비 지원

그램-리치-블라일리 법(GLBA)이란 무엇입니까?

1999년 금융 서비스 현대화 법으로도 알려진 그램-리치-블라일리 법(GLB 법 또는 GLBA)은 금융 기관이 개인의 개인 정보를 처리하는 방식을 통제하기 위해 미국에서 제정된 연방법입니다. 이 법은 세 가지 섹션으로 구성됩니다. 첫 번째는 개인 금융 정보의 수집 및 공개를 규제하는 금융 개인 정보 보호 규칙입니다. 두 번째는 금융 기관이 해당 정보를 보호하기 위해 보안 프로그램을 구현해야 한다고 규정하는 안전 장치 규칙입니다. 세 번째는 프리텍스팅(거짓 위장을 통해 개인 정보에 접근하는 행위)을 금지하는 프리텍스팅 조항입니다. 이 법은 또한 금융 기관이 고객의 정보 공유 관행을 설명하는 개인 정보 보호 통지서를 서면으로 제공하도록 요구합니다.

이 프레임워크를 사용하여 감사 준비 지원

그램-리치-블라일리 법(GLBA) 프레임워크를 사용하여 감사를 준비할 수 있습니다. 이 프레임워크에는 설명 및 테스트 절차가 포함된 사전 구축된 컨트롤 컬렉션이 포함되어 있습니다. 이러한 컨트롤은 GLBA 요구 사항에 따라 컨트롤 세트로 그룹화됩니다. 특정 요구 사항이 있는 내부 감사를 지원하도록 이 프레임워크와 해당 컨트롤을 사용자 지정할 수도 있습니다.

GLBA 프레임워크를 출발점으로 사용하여 Audit Manager 평가를 생성하고 GLBA 감사와 관련된 증거 수집을 시작할 수 있습니다. 평가 시 감사 범위에 포함할 AWS 계정 및 서비스를 지정할 수 있습니다. 평가를 생성하면 Audit Manager가 AWS 리소스 평가를 시작합니다. 이는 GLBA 프레임워크에 정의된 컨트롤을 기반으로 이 작업을 수행합니다. 감사 시기가 되면 사용자 또는 사용자가 선택한 대리인이 Audit Manager에서 수집한 증거를 검토할 수 있습니다. 어느 방식으로든 평가에서 증거 폴더를 찾아보고 평가 보고서에 포함할 증거를 선택할 수 있습니다. 또는 증거 찾기 기능을 활성화한 경우 특정 증거를 검색하고 CSV 형식으로 내보내거나 검색 결과에서 평가 보고서를 생성할 수 있습니다. 둘 중 하나의 방식으로 이 평가 보고서를 사용하여 제어가 의도한 대로 작동하고 있음을 보여줄 수 있습니다.

GLBA 프레임워크 세부 정보는 다음과 같습니다.

AWS Audit Manager에서의 프레임워크 이름	자동화된 컨트롤 수	수동 컨트롤 수	컨트롤 세트 수	범위 내 AWS 서비스
그램-리치-블라일리 법(GLBA)	4	110	16	• Amazon Elastic Compute Cloud • AWS CloudTrail • AWS Config • AWS Identity and Access Management • AWS Security Hub

> **Tip**
>
> 이 표준 프레임워크에서 데이터 소스 매핑으로 사용되는 AWS Config 규칙을 검토하려면 AuditManager_ConfigDataSourceMappings_GLBA.zip 파일을 다운로드하십시오.

이 AWS Audit Manager 프레임워크의 컨트롤은 시스템이 GLBA 표준을 준수하는지 확인하기 위한 것이 아닙니다. 게다가 이는 GLBA 감사 통과를 보장할 수도 없습니다. AWS Audit Manager는 수동 증거 수집이 필요한 절차상의 컨트롤을 자동으로 확인하지 않습니다.

GLBA 프레임워크는 Audit Manager에서 프레임워크 라이브러리의 표준 프레임워크 탭에서 찾을 수 있습니다.

이 프레임워크를 사용하여 평가를 생성하는 방법에 대한 지침은 평가 생성을 참조하십시오.

Audit Manager 콘솔을 사용하여 이 표준 프레임워크에서 평가를 생성하면 범위 내 AWS 서비스 목록이 기본적으로 선택되며 편집할 수 없습니다. 이는 Audit Manager가 자동으로 데이터 소스 및 서비스를 매핑하고 선택하기 때문입니다. 이 선택은 GLBA의 요구 사항에 따라 이루어집니다. 이 프레임워크의 범위 내에서 서비스 목록을 편집해야 하는 경우 CreateAssessment 또는 UpdateAssessment API 작업을 사용하여 편집할 수 있습니다. 또는 표준 프레임워크를 사용자 지정한 다음 사용자 지정 프레임워크에서 평가를 생성할 수도 있습니다.

특정 요구 사항을 지원하도록 이 프레임워크를 사용자 지정하는 방법에 대한 지침은 기존 프레임워크 사용자 지정 및 기존 컨트롤 사용자 지정을 참조하십시오.

GxP 21 CFR 파트 11

AWS Audit Manager는 AWS 모범 사례를 기반으로 GxP CFR 파트 11 규정을 지원하는 사전 구축된 프레임워크를 제공합니다.

> **Note**
>
> GxP EU 부속서 11과 이를 지원하는 Audit Manager 프레임워크에 대한 자세한 내용은 GxP EU 부속서 11을 참조하십시오.

주제

- GxP CFR 파트 11이란 무엇입니까?
- 이 프레임워크를 사용하여 감사 준비 지원
- 추가 GxP 리소스

GxP CFR 파트 11이란 무엇입니까?

GxP는 식품 및 의약품을 제조하는 생명과학 조직에 적용되는 규정 및 지침을 의미합니다. 이에 해당하는 의료 제품에는 의약품, 의료 기기, 의료 소프트웨어 애플리케이션 등이 포함됩니다. GxP 요건의 전반적인 목적은 식품 및 의료 제품이 소비자에게 안전한지 확인하는 것입니다. 또한 제품 관련 안전 결정을 내리는 데 사용되는 데이터의 무결성을 보장하기 위한 것입니다.

GxP라는 용어는 광범위한 규정 준수 관련 활동을 포함합니다. 여기에는 우수 실험실 관리 기준(GLP), 우수 임상 관리 기준(GCP), 우수 제조 관리 기준(GMP)이 포함됩니다. 이러한 다양한 유형의 활동에는 생명과학 조직이 구현해야 하는 제품별 요구 사항이 포함됩니다. 이는 조직이 만드는 제품 유형과 제품이 판매되는 국가를 기반으로 합니다. 생명과학 조직이 컴퓨터 시스템을 사용하여 특정 GxP 활동을 수

행하는 경우, 컴퓨터화된 GxP 시스템이 시스템의 용도에 맞게 적절하게 개발, 검증 및 운영되도록 해야 합니다.

GxP 시스템용 AWS 클라우드 사용에 대한 포괄적인 접근 방식은 GxP 시스템의 AWS 제품 사용 시 고려 사항 백서를 참조하십시오.

이 프레임워크를 사용하여 감사 준비 지원

GxP 21 CFR Part 11 프레임워크를 사용하여 감사를 준비할 수 있습니다. 이 프레임워크에는 설명 및 테스트 절차가 포함된 사전 구축된 컨트롤 컬렉션이 포함되어 있습니다. 이러한 컨트롤은 GxP 요구 사항에 따라 컨트롤 세트로 그룹화됩니다. 특정 요구 사항이 있는 내부 감사를 지원하도록 이 프레임워크와 해당 컨트롤을 사용자 지정할 수도 있습니다.

프레임워크를 출발점으로 사용하여 Audit Manager 평가를 생성하고 감사와 관련된 증거 수집을 시작할 수 있습니다. 평가를 생성하면 Audit Manager가 AWS 리소스 평가를 시작합니다. 이는 GxP 21 CFR Part 11 프레임워크에 정의된 컨트롤을 기반으로 이 작업을 수행합니다. 감사 시기가 되면 사용자 또는 사용자가 선택한 대리인이 Audit Manager에서 수집한 증거를 검토할 수 있습니다. 어느 방식으로든 평가에서 증거 폴더를 찾아보고 평가 보고서에 포함할 증거를 선택할 수 있습니다. 또는 증거 찾기 기능을 활성화한 경우 특정 증거를 검색하고 CSV 형식으로 내보내거나 검색 결과에서 평가 보고서를 생성할 수 있습니다. 둘 중 하나의 방식으로 이 평가 보고서를 사용하여 제어가 의도한 대로 작동하고 있음을 보여줄 수 있습니다.

GxP CFR 파트 11 프레임워크 세부 정보는 다음과 같습니다.

AWS Audit Manager에서의 프레임워크 이름	자동화된 컨트롤 수	수동 컨트롤 수	컨트롤 세트 수	범위 내 AWS 서비스
GxP 21 CFR 파트 11	13	14	7	• AWS CloudTrail • AWS Config • AWS Identity and Access Management

> **Tip**
>
> 이 표준 프레임워크에서 데이터 소스 매핑으로 사용되는 AWS Config 규칙을 검토하려면 AuditManager_ConfigDataSourceMappings_GxP-21-CFR-Part-11.zip 파일을 다운로드하십시오.

이 AWS Audit Manager 프레임워크의 컨트롤은 시스템이 GxP 규정을 준수하는지 확인하기 위한 것이 아닙니다. 게다가 이는 GxP 감사 통과를 보장할 수도 없습니다. AWS Audit Manager는 수동 증거 수집이 필요한 절차상의 컨트롤을 자동으로 확인하지 않습니다.

이 프레임워크는 Audit Manager의 프레임워크 라이브러리의 표준 프레임워크 탭에서 찾을 수 있습니다.

이 프레임워크를 사용하여 평가를 생성하는 방법에 대한 지침은 평가 생성을 참조하십시오.

Audit Manager 콘솔을 사용하여 이 표준 프레임워크에서 평가를 생성하면 범위 내 AWS 서비스 목록이 기본적으로 선택되며 편집할 수 없습니다. 이는 Audit Manager가 자동으로 데이터 소스 및 서비스를 매핑하고 선택하기 때문입니다. 이 선택은 GxP CFR Part 11 프레임워크의 요구 사항에 따라 이루어집니다. 이 프레임워크의 범위 내에서 서비스 목록을 편집해야 하는 경우 CreateAssessment 또는 UpdateAssessment API 작업을 사용하여 편집할 수 있습니다. 또는 표준 프레임워크를 사용자 지정한 다음 사용자 지정 프레임워크에서 평가를 생성할 수도 있습니다.

특정 요구 사항을 지원하도록 이 프레임워크를 사용자 지정하는 방법에 대한 지침은 기존 프레임워크 사용자 지정 및 기존 컨트롤 사용자 지정을 참조하십시오.

추가 GxP 리소스

- GxP AWS 규정 준수 페이지
- GxP 시스템에서 AWS 제품을 사용할 때 고려 사항

GxP EU 부속서 11

AWS Audit Manager은 AWS 모범 사례를 기반으로 GxP EU 부속서 11 규정을 지원하는 사전 구축된 프레임워크를 제공합니다.

> **Note**
>
> GxP 21 CFR 파트 11 및 이를 지원하는 Audit Manager 프레임워크에 대한 자세한 내용은 GxP 21 CFR 파트 11을 참조하십시오.

주제

GxP EU 부속서 11이란 무엇입니까?

GxP EU 부속서 11 프레임워크는 미국의 FDA 21 CFR 파트 11 프레임워크와 동등한 유럽 버전입니다. 이 부속서는 우수제조관리기준(GMP) 규제 활동의 일환으로 사용되는 모든 형태의 컴퓨터 시스템에 적용됩니다. 컴퓨터 시스템은 특정 기능을 함께 수행하는 일련의 소프트웨어 및 하드웨어 구성 집합입니다. 애플리케이션을 검증하고 IT 인프라를 검증해야 합니다. 컴퓨터 시스템이 수동 작업을 대체하는 경우 결과적으로 제품 품질, 프로세스 컨트롤 또는 품질 보증이 저하되어서는 안 됩니다. 프로세스의 전반적인 위험이 증가하지 않아야 합니다.

부속서 11은 유럽 GMP 지침의 일부이며 제약 산업 조직에서 사용하는 컴퓨터 시스템에 대한 참조 조건을 정의합니다. 부속서 11은 유럽 규제 기관이 의약품 및 의료 기기와 관련된 컴퓨터 시스템에 대한 요구 사항을 수립할 수 있도록 하는 체크리스트 역할을 합니다. 유럽의회 위원회에서 정한 지침은 FDA(21 CFR 파트 11)에서 그리 멀리 떨어져 있지 않습니다. 부속서 11에는 전자 기록 및 전자 서명의 관리 대상 기준이 정의되어 있습니다.

이 프레임워크를 사용하여 감사 준비 지원

GxP EU 부속서 11 프레임워크를 사용하여 감사를 준비할 수 있습니다. 이 프레임워크에는 설명 및 테스트 절차가 포함된 사전 구축된 컨트롤 컬렉션이 포함되어 있습니다. 이러한 컨트롤은 GxP 요구 사항에 따라 컨트롤 세트로 그룹화됩니다. 특정 요구 사항이 있는 내부 감사를 지원하도록 이 프레임워크와 해당 컨트롤을 사용자 지정할 수도 있습니다.

프레임워크를 출발점으로 사용하여 Audit Manager 평가를 생성하고 감사와 관련된 증거 수집을 시작할 수 있습니다. 평가를 생성하면 Audit Manager가 AWS 리소스 평가를 시작합니다. 이는 GxP EU 부속서 11 프레임워크에 정의된 컨트롤을 기반으로 이 작업을 수행합니다. 감사 시기가 되면 사용자 또는 사용자가 선택한 대리인이 Audit Manager에서 수집한 증거를 검토할 수 있습니다. 어느 방식으로든 평가에서 증거 폴더를 찾아보고 평가 보고서에 포함할 증거를 선택할 수 있습니다. 또는 증거 찾기 기능

을 활성화한 경우 특정 증거를 검색하고 CSV 형식으로 내보내거나 검색 결과에서 평가 보고서를 생성할 수 있습니다. 둘 중 하나의 방식으로 이 평가 보고서를 사용하여 제어가 의도한 대로 작동하고 있음을 보여줄 수 있습니다.

GxP EU 부속서 11 프레임워크 세부 정보는 다음과 같습니다.

AWS Audit Manager에서의 프레임워크 이름	자동화된 컨트롤 수	수동 컨트롤 수	컨트롤 세트 수	범위 내 AWS 서비스
GxP EU 부속서 11	19	13	3	• Amazon CloudWatch • AWS CloudTrail • AWS Config • AWS Identity and Access Management • AWS Security Hub

> **Tip**
>
> 이 표준 프레임워크에서 데이터 소스 매핑으로 사용되는 AWS Config 규칙을 검토하려면 AuditManager_ConfigDataSourceMappings_GxP-EU-Annex-11.zip 파일을 다운로드하십시오.

이 프레임워크의 컨트롤은 시스템이 GxP EU 부속서 11 요구 사항을 준수하는지 확인하기 위한 것이 아닙니다. 게다가 이는 GxP 감사 통과를 보장할 수도 없습니다. AWS Audit Manager는 수동 증거 수집이 필요한 절차상의 컨트롤을 자동으로 확인하지 않습니다.

이 프레임워크는 Audit Manager의 프레임워크 라이브러리의 표준 프레임워크 탭에서 찾을 수 있습니다.

이 프레임워크를 사용하여 평가를 생성하는 방법에 대한 지침은 평가 생성을 참조하십시오.

Audit Manager 콘솔을 사용하여 이 표준 프레임워크에서 평가를 생성하면 범위 내 AWS 서비스 목록이 기본적으로 선택되며 편집할 수 없습니다. 이는 Audit Manager가 자동으로 데이터 소스 및 서비스를 매핑하고 선택하기 때문입니다. 이 선택은 GxP EU 부속서 11 프레임워크의 요구 사항에 따라 이루

어집니다. 이 프레임워크의 범위 내에서 서비스 목록을 편집해야 하는 경우 CreateAssessment 또는 UpdateAssessment API 작업을 사용하여 편집할 수 있습니다. 또는 표준 프레임워크를 사용자 지정한 다음 사용자 지정 프레임워크에서 평가를 생성할 수도 있습니다.

특정 요구 사항을 지원하도록 이 프레임워크를 사용자 지정하는 방법에 대한 지침은 기존 프레임워크 사용자 지정 및 기존 컨트롤 사용자 지정을 참조하십시오.

건강보험 이동성 및 책임법(HIPAA) 보안 규칙 2003

AWS Audit Manager는 감사 준비를 지원하는 HIPAA 규칙을 지원하는 사전 구축된 프레임워크를 제공합니다.

> **Note**
>
> 이 프레임워크는 이전에 프레임워크 라이브러리에서 HIPAA로 명명되었습니다. 2023년 3월 8일, 우리는 이 프레임워크의 이름을 HIPAA 최종 옴니버스 보안 규칙 2013과 구별하기 위해 HIPAA 보안 규칙 2003으로 업데이트했습니다.
> HIPAA 최종 옴니버스 보안 규칙 2013과 이 표준을 지원하는 Audit Manager 프레임워크에 대한 자세한 내용은 건강보험 이동성 및 책임법(HIPAA) 최종 옴니버스 보안 규칙 2013을 참조하십시오.

주제

- HIPAA 및 HIPAA 보안 규칙 2003이란 무엇입니까?
- 이 프레임워크를 사용하여 감사 준비 지원
- 추가 HIPAA 리소스

HIPAA 및 HIPAA 보안 규칙 2003이란 무엇입니까?

건강보험 이동성 및 책임법(HIPAA) 1996은 미국 근로자들이 직장을 옮기거나 실직했을 때 건강보험 보장을 유지할 수 있도록 돕는 법안입니다. 이 법안은 또한 정보 공유 개선을 통해 미국 의료 시스템의 효율성과 품질을 향상시키기 위해 전자 의료 기록을 장려하고자 합니다.

전자 의료 기록의 사용이 증가함에 따라 HIPAA에는 보호 대상 건강 정보(PHI)의 보안 및 개인 정보 보호를 위한 조항이 포함됩니다. PHI에는 매우 광범위한 개인 식별 가능 건강 및 건강 관련 데이터가 포함됩니다. 여기에는 보험 및 청구 정보, 진단 데이터, 임상 치료 데이터, 검사 결과(예: 이미지 및 검사 결과)가 포함됩니다.

미국 보건복지부는 2003년 2월에 최종 보안 규칙을 발표했습니다. 이 규칙은 전자 보호 의료 정보의 기밀성, 무결성 및 가용성을 보호하기 위한 국가 표준을 설정합니다.

HIPAA 규정은 해당 기관에 적용됩니다. 여기에는 환자와 환자 데이터를 직접 다루는 병원, 의료 서비스 제공자, 고용주가 후원하는 건강 보험, 연구 시설, 보험 회사 등이 포함됩니다. PHI 보호를 위한 HIPAA 요건은 비즈니스 관계자에게도 적용됩니다.

HIPAA와 HITECH가 건강 정보를 보호하는 방법에 대한 자세한 내용은 미국 보건 복지부의 건강 정보 보호정책 웹 페이지를 참조하십시오.

점점 더 많은 의료 제공자, 지불자 및 IT 전문가들이 AWS 유틸리티 기반 클라우드 서비스를 사용하여 보호된 건강 정보(PHI)를 처리, 저장 및 전송하고 있습니다. AWS는 HIPAA 대상인 대상 기업과 그 사업 관계자들이 안전한 AWS 환경을 사용하여 보호된 건강 정보를 처리, 유지 및 저장할 수 있도록 합니다.

건강 정보의 처리 및 저장을 위해 AWS를 사용할 수 있는 방법에 대한 자세한 내용은 Amazon Web Services에서 HIPAA 보안 및 규정 준수 기술에 대한 설계 백서를 참조하십시오.

이 프레임워크를 사용하여 감사 준비 지원

HIPAA 보안 규칙 2003 프레임워크를 사용하여 감사를 준비할 수 있습니다. 이 프레임워크에는 설명 및 테스트 절차가 포함된 사전 구축된 컨트롤 컬렉션이 포함되어 있습니다. 이러한 컨트롤은 HIPAA 요구 사항에 따라 컨트롤 세트로 그룹화됩니다. 또한 특정 요구 사항이 있는 내부 감사를 지원하도록 이 프레임워크와 해당 컨트롤을 사용자 지정할 수 있습니다.

프레임워크를 출발점으로 사용하여 Audit Manager 평가를 생성하고 감사와 관련된 증거 수집을 시작할 수 있습니다. 평가를 생성하면 Audit Manager가 AWS 리소스 평가를 시작합니다. 이는 HIPAA 프레임워크에 정의된 컨트롤을 기반으로 이 작업을 수행합니다. 감사 시기가 되면 사용자 또는 사용자가 선택한 대리인이 Audit Manager에서 수집한 증거를 검토할 수 있습니다. 어느 방식으로든 평가에서 증거 폴더를 찾아보고 평가 보고서에 포함할 증거를 선택할 수 있습니다. 또는 증거 찾기 기능을 활성화한 경우 특정 증거를 검색하고 CSV 형식으로 내보내거나 검색 결과에서 평가 보고서를 생성할 수 있습니다. 둘 중 하나의 방식으로 이 평가 보고서를 사용하여 제어가 의도한 대로 작동하고 있음을 보여줄 수 있습니다.

HIPAA 보안 규칙 2003 프레임워크 세부 정보는 다음과 같습니다.

AWS Audit Manager에서의 프레임워크 이름	자동화된 컨트롤 수	수동 컨트롤 수	컨트롤 세트 수	범위 내 AWS 서비스
HIPAA 보안 규칙 2003	35	53	5	• Amazon Elastic Compute Cloud • AWS CloudTrail • AWS Config • AWS Identity and Access Management • AWS Security Hub

> **Tip**
>
> 이 표준 프레임워크에서 데이터 소스 매핑으로 사용되는 AWS Config 규칙을 검토하려면 AuditManager_ConfigDataSourceMappings_HIPAA-Security-Rule-2003.zip 파일을 다운로드하십시오.

이 AWS Audit Manager 프레임워크의 컨트롤은 시스템이 HIPAA 표준을 준수하는지 확인하기 위한 것이 아닙니다. 게다가 이는 HIPAA 감사 통과를 보장할 수도 없습니다. AWS Audit Manager는 수동 증거 수집이 필요한 절차상의 컨트롤을 자동으로 확인하지 않습니다.

이 프레임워크는 Audit Manager의 프레임워크 라이브러리의 표준 프레임워크 탭에서 찾을 수 있습니다.

이 프레임워크를 사용하여 평가를 생성하는 방법에 대한 지침은 평가 생성을 참조하십시오.

Audit Manager 콘솔을 사용하여 이 표준 프레임워크에서 평가를 생성하면 범위 내 AWS 서비스 목록이 기본적으로 선택되며 편집할 수 없습니다. 이는 Audit Manager가 자동으로 데이터 소스 및 서비스를 매핑하고 선택하기 때문입니다. 이 선택은 HIPAA 프레임워크의 요구 사항에 따라 이루어집니다. 이 프레임워크의 범위 내에서 서비스 목록을 편집해야 하는 경우 CreateAssessment 또는 UpdateAssessment API 작업을 사용하여 편집할 수 있습니다. 또는 표준 프레임워크를 사용자 지정한 다음 사용자 지정 프레임워크에서 평가를 생성할 수도 있습니다.

특정 요구 사항을 지원하도록 이 프레임워크를 사용자 지정하는 방법에 대한 지침은 기존 프레임워크 사용자 지정 및 기존 컨트롤 사용자 지정을 참조하십시오.

추가 HIPAA 리소스

- 미국 보건복지부의 건강 정보 프라이버시
- 미국 보건복지부의 보안 규칙
- Amazon Web Services에서 HIPAA 보안 및 규정 준수를 위한 설계
- HIPAA AWS 규정 준수 페이지

건강보험 이동성 및 책임법(HIPAA) 최종 옴니버스 보안 규칙 2013

AWS Audit Manager는 감사 준비를 지원하는 HIPAA 규칙을 지원하는 사전 구축된 프레임워크를 제공합니다.

> **Note**
>
> HIPAA 보안 규칙 2003 및 이 표준을 지원하는 AWS Audit Manager 프레임워크에 대한 자세한 내용은 건강보험 이동성 및 책임법(HIPAA) 보안 규칙 2003을 참조하십시오.

주제

- HIPAA 및 HIPAA 최종 옴니버스 보안 규칙이란 무엇입니까?
- 이 프레임워크를 사용하여 감사 준비 지원
- 추가 HIPAA 리소스

HIPAA 및 HIPAA 최종 옴니버스 보안 규칙이란 무엇입니까?

건강보험 이동성 및 책임법(HIPAA) 1996은 미국 근로자들이 직장을 옮기거나 실직했을 때 건강보험 보장을 유지할 수 있도록 돕는 법안입니다. 이 법안은 또한 정보 공유 개선을 통해 미국 의료 시스템의 효율성과 품질을 향상시키기 위해 전자 의료 기록을 장려하고자 합니다.

전자 의료 기록의 사용이 증가함에 따라 HIPAA에는 보호 대상 건강 정보(PHI)의 보안 및 개인 정보 보호를 위한 조항이 포함됩니다. PHI에는 매우 광범위한 개인 식별 가능 건강 및 건강 관련 데이터가 포함됩니다. 여기에는 보험 및 청구 정보, 진단 데이터, 임상 치료 데이터, 검사 결과(예: 이미지 및 검사 결과)가 포함됩니다.

2013년에 발효된 HIPAA 최종 옴니버스 보안 규칙은 이전에 통과된 모든 규칙에 대한 여러 업데이트를 구현합니다. 보안, 개인 정보 보호, 침해 알림 및 시행 규칙의 수정은 데이터 공유의 기밀성과 보안을 강화하기 위한 것입니다.

HIPAA 규칙은 해당 기관에 적용됩니다. 여기에는 환자와 환자 데이터를 직접 다루는 병원, 의료 서비스 제공자, 고용주가 후원하는 건강 보험, 연구 시설, 보험 회사 등이 포함됩니다. 옴니버스 업데이트의 일환으로, 피보험 대상에 적용되는 HIPAA 규칙 중 상당수가 이제 비즈니스 관계자에게도 적용됩니다.

HIPAA와 HITECH가 건강 정보를 보호하는 방법에 대한 자세한 내용은 미국 보건 복지부의 건강 정보 보호정책 웹 페이지를 참조하십시오.

점점 더 많은 의료 제공자, 지불자 및 IT 전문가들이 AWS 유틸리티 기반 클라우드 서비스를 사용하여 보호된 건강 정보(PHI)를 처리, 저장 및 전송하고 있습니다. AWS는 HIPAA 대상인 대상 기업과 그 사업 관계자들이 안전한 AWS 환경을 사용하여 보호된 건강 정보를 처리, 유지 및 저장할 수 있도록 합니다. 건강 정보의 처리 및 저장을 위해 AWS를 사용할 수 있는 방법에 대한 자세한 내용은 Amazon Web Services에서 HIPAA 보안 및 규정 준수 기술에 대한 설계 백서를 참조하십시오.

이 프레임워크를 사용하여 감사 준비 지원

HIPAA 최종 옴니버스 보안 규칙 2013 프레임워크를 사용하여 감사를 준비할 수 있습니다. 이 프레임워크에는 설명 및 테스트 절차가 포함된 사전 구축된 컨트롤 컬렉션이 포함되어 있습니다. 이러한 컨트롤은 HIPAA 요구 사항에 따라 컨트롤 세트로 그룹화됩니다. 또한 특정 요구 사항이 있는 내부 감사를 지원하도록 이 프레임워크와 해당 컨트롤을 사용자 지정할 수 있습니다.

프레임워크를 출발점으로 사용하여 Audit Manager 평가를 생성하고 감사와 관련된 증거 수집을 시작할 수 있습니다. 평가를 생성하면 Audit Manager가 AWS 리소스 평가를 시작합니다. 이는 HIPAA 프레임워크에 정의된 컨트롤을 기반으로 이 작업을 수행합니다. 감사 시기가 되면 사용자 또는 사용자가 선택한 대리인이 Audit Manager에서 수집한 증거를 검토할 수 있습니다. 어느 방식으로든 평가에서 증거 폴더를 찾아보고 평가 보고서에 포함할 증거를 선택할 수 있습니다. 또는 증거 찾기 기능을 활성화한 경우 특정 증거를 검색하고 CSV 형식으로 내보내거나 검색 결과에서 평가 보고서를 생성할 수 있습니다. 둘 중 하나의 방식으로 이 평가 보고서를 사용하여 제어가 의도한 대로 작동하고 있음을 보여줄 수 있습니다.

HIPAA 최종 옴니버스 보안 규칙 2013 프레임워크의 세부 정보는 다음과 같습니다.

AWS Audit Manager에서의 프레임워크 이름	자동화된 컨트롤 수	수동 컨트롤 수	컨트롤 세트 수	범위 내 AWS 서비스
HIPAA 최종 옴니버스 보안 규칙 2013	39	46	5	• Amazon Elastic Compute Cloud

AWS Audit Manager에서의 프레임워크 이름	자동화된 컨트롤 수	수동 컨트롤 수	컨트롤 세트 수	범위 내 AWS 서비스
				• AWS CloudTrail • AWS Config • AWS Identity and Access Management • AWS Security Hub

> **Tip**
>
> 이 표준 프레임워크에서 데이터 소스 매핑으로 사용되는 AWS Config 규칙을 검토하려면 AuditManager_ConfigDataSourceMappings_HIPAA-Final-Omnibus-Security-Rule-2013.zip 파일을 다운로드하십시오.

이 AWS Audit Manager 프레임워크의 컨트롤은 시스템이 HIPAA 표준을 준수하는지 확인하기 위한 것이 아닙니다. 게다가 이는 HIPAA 감사 통과를 보장할 수도 없습니다. AWS Audit Manager는 수동 증거 수집이 필요한 절차상의 컨트롤을 자동으로 확인하지 않습니다.

이 프레임워크는 Audit Manager의 프레임워크 라이브러리의 표준 프레임워크 탭에서 찾을 수 있습니다.

이 프레임워크를 사용하여 평가를 생성하는 방법에 대한 지침은 평가 생성을 참조하십시오.

Audit Manager 콘솔을 사용하여 이 표준 프레임워크에서 평가를 생성하면 범위 내 AWS 서비스 목록이 기본적으로 선택되며 편집할 수 없습니다. 이는 Audit Manager가 자동으로 데이터 소스 및 서비스를 매핑하고 선택하기 때문입니다. 이 선택은 HIPAA 프레임워크의 요구 사항에 따라 이루어집니다. 이 프레임워크의 범위 내에서 서비스 목록을 편집해야 하는 경우 CreateAssessment 또는 UpdateAssessment API 작업을 사용하여 편집할 수 있습니다. 또는 표준 프레임워크를 사용자 지정한 다음 사용자 지정 프레임워크에서 평가를 생성할 수도 있습니다.

특정 요구 사항을 지원하도록 이 프레임워크를 사용자 지정하는 방법에 대한 지침은 기존 프레임워크 사용자 지정 및 기존 컨트롤 사용자 지정을 참조하십시오.

추가 HIPAA 리소스

- 미국 보건복지부의 건강 정보 프라이버시
- 미국 보건복지부의 옴니버스 HIPAA 규칙 제정
- Amazon Web Services에서 HIPAA 보안 및 규정 준수를 위한 설계
- HIPAA AWS 규정 준수 페이지

ISO/IEC 27001:2013 부속서 A

AWS Audit Manager는 ISO/IEC 27001:2013 부속서 A에 대한 평가를 구조화하고 자동화하는 사전 구축된 표준 프레임워크를 제공합니다.

주제

- ISO/IEC 27001:2013 부속서 A란 무엇입니까?
- 이 프레임워크를 사용하여 감사 준비 지원
- 추가 ISO/IEC 27001:2013 부속서 A 리소스

ISO/IEC 27001:2013 부속서 A란 무엇입니까?

국제전기기술위원회(IEC)와 국제표준화기구(ISO)는 모두 완전한 합의 기반 국제 표준을 개발하고 발표하는 독립적인 비정부 비영리 조직입니다.

ISO/IEC 27001:2013 부속서 A는 ISO/IEC 27002 모범 사례 지침을 따르는 보안 관리 모범 사례와 포괄적인 보안 컨트롤을 지정하는 보안 관리 표준입니다. 이 국제 표준은 조직의 정보 보안 관리 시스템을 수립, 구현, 유지 및 지속적으로 개선하는 방법에 대한 요구 사항을 지정합니다. 이러한 표준에는 조직의 요구 사항에 맞게 조정된 정보 보안 위험의 평가 및 처리에 대한 요구 사항이 포함됩니다. 이 국제 표준의 요구 사항은 일반적이며 유형, 규모 또는 성격에 관계없이 모든 조직에 적용할 수 있도록 고안되었습니다.

이 프레임워크를 사용하여 감사 준비 지원

ISO/IEC 27001:2013 부속서 A의 AWS Audit Manager 프레임워크를 사용하여 감사를 준비할 수 있습니다. 이 프레임워크에는 설명 및 테스트 절차가 포함된 사전 구축된 컨트롤 컬렉션이 포함되어 있습니다. 이러한 컨트롤은 ISO/IEC 27001:2013 부속서 A 요구 사항에 따라 컨트롤 세트로 그룹화됩니다. 특정 요구 사항이 있는 내부 감사를 지원하도록 이 프레임워크와 해당 컨트롤을 사용자 지정할 수도 있습니다.

프레임워크를 출발점으로 사용하여 Audit Manager 평가를 생성하고 ISO/IEC 27001:2013 부속서 A 감사와 관련된 증거 수집을 시작할 수 있습니다. 평가 시 감사 범위에 포함할 AWS 계정 및 서비스를 지정할 수 있습니다. 평가를 생성하면 Audit Manager가 AWS 리소스 평가를 시작합니다. 이는 ISO/IEC 27001:2013 부속서 A 프레임워크에 정의된 컨트롤을 기반으로 이 작업을 수행합니다. 감사 시기가 되면 사용자 또는 사용자가 선택한 대리인이 Audit Manager에서 수집한 증거를 검토할 수 있습니다. 어느 방식으로든 평가에서 증거 폴더를 찾아보고 평가 보고서에 포함할 증거를 선택할 수 있습니다. 또는 증거 찾기 기능을 활성화한 경우 특정 증거를 검색하고 CSV 형식으로 내보내거나 검색 결과에서 평가 보고서를 생성할 수 있습니다. 둘 중 하나의 방식으로 이 평가 보고서를 사용하여 제어가 의도한 대로 작동하고 있음을 보여줄 수 있습니다.

프레임워크 세부 정보는 다음과 같습니다.

AWS Audit Manager에서의 프레임워크 이름	자동화된 컨트롤 수	수동 컨트롤 수	컨트롤 세트 수	범위 내 AWS 서비스
ISO-IEC 27001:2013 부속서 A	50	64	35	• Amazon CloudWatch • Amazon Elastic Compute Cloud • AWS CloudTrail • AWS Config • AWS Identity and Access Management • AWS Security Hub

> **Tip**
>
> 이 표준 프레임워크에서 데이터 소스 매핑으로 사용되는 AWS Config 규칙을 검토하려면 AuditManager_ConfigDataSourceMappings_ISO-IEC-27001-2013-Annex-A.zip 파일을 다운로드하십시오.

이 AWS Audit Manager 프레임워크의 컨트롤은 시스템이 이 국제 표준을 준수하는지 확인하기 위한 것이 아닙니다. 게다가 이는 ISO/IEC 감사 통과를 보장할 수도 없습니다. AWS Audit Manager는 수동 증거 수집이 필요한 절차상의 컨트롤을 자동으로 확인하지 않습니다.

Audit Manager에서 프레임워크 라이브러리의 표준 프레임워크 탭에서 ISO/IEC 27001:2013 부속서 A 프레임워크를 찾을 수 있습니다.

Audit Manager 콘솔을 사용하여 이 표준 프레임워크에서 평가를 생성하면 범위 내 AWS 서비스 목록이 기본적으로 선택되며 편집할 수 없습니다. 이는 Audit Manager가 자동으로 데이터 소스 및 서비스를 매핑하고 선택하기 때문입니다. 이 선택은 ISO-IEC 27001:2013 부속서 A 프레임워크의 요구 사항에 따라 이루어집니다. 이 프레임워크의 범위 내에서 서비스 목록을 편집해야 하는 경우 CreateAssessment 또는 UpdateAssessment API 작업을 사용하여 편집할 수 있습니다. 또는 표준 프레임워크를 사용자 지정한 다음 사용자 지정 프레임워크에서 평가를 생성할 수도 있습니다.

이 프레임워크를 사용하여 평가를 생성하는 방법에 대한 지침은 평가 생성을 참조하십시오. 특정 요구 사항을 지원하도록 이 프레임워크를 사용자 지정하는 방법에 대한 지침은 기존 프레임워크 사용자 지정 및 기존 컨트롤 사용자 지정을 참조하십시오.

추가 ISO/IEC 27001:2013 부속서 A 리소스

- 이 국제 표준에 대한 자세한 내용은 ANSI 웹스토어의 ISO/IEC 27001:2013을 참조하십시오.

NIST 800-53 (개정판 5) 낮음-보통-높음

AWS Audit Manager는 AWS 모범 사례를 기반으로 NIST 800-53 규정 준수 표준에 대한 평가를 구조화하고 자동화하는 사전 구축된 프레임워크를 제공합니다.

> **Note**
>
> - NIST 800-171을 지원하는 Audit Manager 프레임워크에 대한 자세한 내용은 NIST SP 800-171(개정 2)을 참조하십시오.
> - NIST 사이버 보안 프레임워크를 지원하는 Audit Manager 프레임워크에 대한 자세한 내용은 NIST 사이버 보안 프레임워크 버전 1.1을 참조하십시오.

주제

- NIST 800-53이란 무엇입니까?

- 이 프레임워크를 사용하여 감사 준비 지원
- 추가 NIST 리소스

NIST 800-53이란 무엇입니까?

NIST(국립표준기술연구소)는 1901년에 설립되었으며 현재는 미국 상무부에 속해 있습니다. NIST는 미국에서 가장 오래된 물리과학 연구소 중 하나입니다. 미국 의회는 당시 썩 훌륭하지 않게 측정되었던 인프라를 개선하기 위해 이 기관을 설립했습니다. 인프라는 영국, 독일 등 다른 경제대국들에 비해 뒤쳐져 있었기 때문에 미국 산업경쟁력에 있어 주요 도전 과제였습니다.

NIST 800-53 보안 컨트롤은 일반적으로 미국 연방 정보 시스템에 적용됩니다. 이러한 시스템은 일반적으로 공식적인 평가 및 승인 프로세스를 거쳐야 합니다. 이 프로세스는 정보 및 정보 시스템의 기밀성, 무결성 및 가용성에 대한 충분한 보호를 보장합니다. 이는 시스템의 보안 범주와 영향 수준(낮음, 중간 또는 높음) 및 위험 판단에 기반합니다. 보안 컨트롤은 NIST SP 800-53 보안 컨트롤 카탈로그에서 선택되었으며 시스템은 이러한 보안 컨트롤 요구 사항을 바탕으로 평가되었습니다.

NIST 800-53 (개정 5) 낮음-보통-높음 프레임워크는 연방 정보 시스템 및 조직을 위한 NIST SP 800-53 개정 5 권장 보안 컨트롤에 정의된 보안 컨트롤 및 관련 평가 절차를 나타냅니다. 이 NIST SP 800-53 프레임워크와 최근에 발행된 NIST 특수 간행물 SP 800-53 개정 5 간의 내용에서 발견되는 불일치의 경우 NIST 컴퓨터 보안 리소스 센터에서 제공되는 공식 출판 문서를 참조하십시오.

이 프레임워크를 사용하여 감사 준비 지원

NIST 800-53 (개정 5) 낮음-보통-높음 프레임워크를 사용하여 감사를 준비할 수 있습니다. 이 프레임워크에는 설명 및 테스트 절차가 포함된 사전 구축된 컨트롤 컬렉션이 포함되어 있습니다. 이러한 컨트롤은 NIST 요구 사항에 따라 컨트롤 세트로 그룹화됩니다. 특정 요구 사항이 있는 내부 감사를 지원하도록 이 프레임워크와 해당 컨트롤을 사용자 지정할 수도 있습니다.

프레임워크를 출발점으로 사용하여 Audit Manager 평가를 생성하고 감사와 관련된 증거 수집을 시작할 수 있습니다. 평가를 생성하면 Audit Manager가 AWS 리소스 평가를 시작합니다. 이는 NIST 800-53 (개정 5) 낮음-보통-높음 프레임워크에 정의된 컨트롤을 기반으로 이 작업을 수행합니다. 감사 시기가 되면 사용자 또는 사용자가 선택한 대리인이 Audit Manager에서 수집한 증거를 검토할 수 있습니다. 어느 방식으로든 평가에서 증거 폴더를 찾아보고 평가 보고서에 포함할 증거를 선택할 수 있습니다. 또는 증거 찾기 기능을 활성화한 경우 특정 증거를 검색하고 CSV 형식으로 내보내거나 검색 결과에서 평가 보고서를 생성할 수 있습니다. 둘 중 하나의 방식으로 이 평가 보고서를 사용하여 제어가 의도한 대로 작동하고 있음을 보여줄 수 있습니다.

NIST 800-53 (개정 5) 낮음-보통-높음 프레임워크 세부 정보는 다음과 같습니다.

AWS Audit Manager에서의 프레임워크 이름	자동화된 컨트롤 수	수동 컨트롤 수	컨트롤 세트 수	범위 내 AWS 서비스
NIST 800-53 (개정 5) 낮음-보통-높음	225	782	280	• Amazon CloudWatch • Amazon Elastic Compute Cloud • AWS CloudTrail • AWS Config • AWS Identity and Access Management • AWS Security Hub

> **Tip**
>
> 이 표준 프레임워크에서 데이터 소스 매핑으로 사용되는 AWS Config 규칙을 검토하려면 AuditManager_ConfigDataSourceMappings_NIST-800-53-Rev.5-Low-Moderate-High.zip 파일을 다운로드하십시오.

이 AWS Audit Manager 프레임워크의 컨트롤은 시스템이 NIST 표준을 준수하는지 확인하기 위한 것이 아닙니다. 게다가 이는 NIST 감사 통과를 보장할 수도 없습니다. AWS Audit Manager는 수동 증거 수집이 필요한 절차상의 컨트롤을 자동으로 확인하지 않습니다.

이 프레임워크는 Audit Manager의 프레임워크 라이브러리의 표준 프레임워크 탭에서 찾을 수 있습니다.

이 프레임워크를 사용하여 평가를 생성하는 방법에 대한 지침은 평가 생성을 참조하십시오.

Audit Manager 콘솔을 사용하여 이 표준 프레임워크에서 평가를 생성하면 범위 내 AWS 서비스 목록이 기본적으로 선택되며 편집할 수 없습니다. 이는 Audit Manager가 자동으로 데이터 소스 및 서비스를 매핑하고 선택하기 때문입니다. 이 선택은 NIST 800-53 (개정 5) 낮음-보통-높음 프레임워크의 요구 사항에 따라 이루어집니다. 이 프레임워크의 범위 내에서 서비스 목록을 편집해야 하는 경우

CreateAssessment 또는 UpdateAssessment API 작업을 사용하여 편집할 수 있습니다. 또는 표준 프레임워크를 사용자 지정한 다음 사용자 지정 프레임워크에서 평가를 생성할 수도 있습니다.

특정 요구 사항을 지원하도록 이 프레임워크를 사용자 지정하는 방법에 대한 지침은 기존 프레임워크 사용자 지정 및 기존 컨트롤 사용자 지정을 참조하십시오.

추가 NIST 리소스

- NIST(국립표준기술연구소)
- NIST 컴퓨터 보안 리소스 센터
- NIST AWS 규정 준수 페이지

NIST 사이버 보안 프레임워크 버전 1.1

AWS Audit Manager는 AWS 모범 사례를 기반으로 NIST 사이버 보안 프레임워크에 대한 평가를 구조화하고 자동화하는 사전 구축된 프레임워크를 제공합니다.

> **Note**
>
> - NIST 800-53(개정 5) 낮음-보통-높음을 지원하는 Audit Manager 프레임워크에 대한 자세한 내용은 NIST 800-53 (개정판 5) 낮음-보통-높음을 참조하십시오.
> - NIST SP 800-171(개정 2)을 지원하는 Audit Manager 프레임워크에 대한 자세한 내용은 NIST SP 800-171(개정 2)을 참조하십시오.

주제

NIST 사이버 보안 프레임워크란 무엇입니까?

NIST(국립표준기술연구소)는 1901년에 설립되었으며 현재는 미국 상무부에 속해 있습니다. NIST는 미국에서 가장 오래된 물리과학 연구소 중 하나입니다. 미국 의회는 당시 썩 훌륭하지 않게 측정되었던 인프라를 개선하기 위해 이 기관을 설립했습니다. 인프라는 영국, 독일 등 다른 경제대국들에 비해 뒤쳐져 있었기 때문에 미국 산업경쟁력에 있어 주요 도전 과제였습니다.

미국은 중요 인프라의 안정적인 기능에 의존합니다. 사이버 보안 위협은 중요 인프라 시스템의 증가된 복잡성과 상호 연결성을 악용합니다. 이는 미국의 보안, 경제, 공공 안전 및 건강을 위험에 빠뜨립니다. 재무 및 평판 위험과 마찬가지로 사이버 보안 위험도 기업의 수익에 영향을 미칩니다. 이로 인해 비용이 증가하고 수익에 영향을 미칠 수 있습니다. 이는 조직의 혁신 능력과 고객 확보 및 유지 능력에 해를 끼칠 수 있습니다. 궁극적으로 사이버 보안은 조직의 전반적인 위험 관리를 증폭시킬 수 있습니다.

NIST 사이버 보안 프레임워크(CSF)는 전 세계 정부 및 업계에서 부문이나 규모에 관계없이 모든 조직에서 사용할 수 있는 권장 기준으로 지원하고 있습니다. NIST 사이버 보안 프레임워크는 프레임워크 코어, 프로필 및 구현 계층이라는 세 가지 주요 구성 요소로 구성됩니다. 프레임워크 코어는 조직의 사이버 보안 목표 범위를 포괄하는 23개 범주로 구성된 원하는 사이버 보안 활동 및 결과를 포함합니다. 프로파일에는 조직의 요구사항과 목표, 위험 선호도 및 프레임워크 코어의 원하는 결과를 사용하는 리소스에 대한 조직의 고유한 조정이 포함되어 있습니다. 구현 계층은 조직의 사이버 보안 위험 관리 관행이 프레임워크 코어에 정의된 특성을 나타내는 정도를 설명합니다.

이 프레임워크를 사용하여 감사 준비 지원

NIST 사이버 보안 프레임워크 버전 1.1을 사용하여 감사를 준비할 수 있습니다. 이 프레임워크에는 설명 및 테스트 절차가 포함된 사전 구축된 컨트롤 컬렉션이 포함되어 있습니다. 이러한 컨트롤은 NIST CSF 요구 사항에 따라 컨트롤 세트로 그룹화됩니다. Audit Manager는 현재 56개의 자동 컨트롤과 52개의 수동 컨트롤을 제공하여 프레임워크 핵심 구성 요소를 지원합니다. 이러한 컨트롤은 프레임워크 코어에 정의된 23개의 사이버 보안 범주와 일치합니다. Audit Manager는 이 프레임워크의 프로필 및 구현 구성 요소를 지원하지 않습니다.

특정 요구 사항이 있는 내부 감사를 지원하도록 이 프레임워크와 해당 컨트롤을 사용자 지정할 수도 있습니다.

프레임워크를 출발점으로 사용하여 Audit Manager 평가를 생성하고 감사와 관련된 증거 수집을 시작할 수 있습니다. 평가를 생성하면 Audit Manager가 AWS 리소스 평가를 시작합니다. 이는 NIST 사이버 보안 프레임워크 버전 1.1에 정의된 컨트롤을 기반으로 이 작업을 수행합니다. 감사 시기가 되면 사용자 또는 사용자가 선택한 대리인이 Audit Manager에서 수집한 증거를 검토할 수 있습니다. 어느 방식으로든 평가에서 증거 폴더를 찾아보고 평가 보고서에 포함할 증거를 선택할 수 있습니다. 또는 증거 찾기 기능을 활성화한 경우 특정 증거를 검색하고 CSV 형식으로 내보내거나 검색 결과에서 평가 보고서를 생성할 수 있습니다. 둘 중 하나의 방식으로 이 평가 보고서를 사용하여 제어가 의도한 대로 작동하고 있음을 보여줄 수 있습니다.

NIST 사이버 보안 프레임워크 버전 1.1의 세부 정보는 다음과 같습니다.

AWS Audit Manager에서의 프레임워크 이름	자동화된 컨트롤 수	수동 컨트롤 수	컨트롤 세트 수	범위 내 AWS 서비스
NIST 사이버 보안 프레임워크 버전 1.1	56	52	23	• AWS Config • AWS Identity and Access Management • AWS Security Hub

> **Tip**
>
> 이 표준 프레임워크에서 데이터 소스 매핑으로 사용되는 AWS Config 규칙을 검토하려면 AuditManager_ConfigDataSourceMappings_NIST-CSF-v1.1.zip 파일을 다운로드하십시오.

Audit Manager에서 제공하는 컨트롤은 시스템이 NIST 사이버 보안 프레임워크를 준수하는지 확인하기 위한 것이 아닙니다. 게다가 이는 NIST 사이버 보안 감사 통과를 보장할 수도 없습니다. AWS Audit Manager는 수동 증거 수집이 필요한 절차상의 컨트롤을 자동으로 확인하지 않습니다.

이 프레임워크는 Audit Manager의 프레임워크 라이브러리의 표준 프레임워크 탭에서 찾을 수 있습니다.

이 프레임워크를 사용하여 평가를 생성하는 방법에 대한 지침은 평가 생성을 참조하십시오.

Audit Manager 콘솔을 사용하여 이 표준 프레임워크에서 평가를 생성하면 범위 내 AWS 서비스 목록이 기본적으로 선택되며 편집할 수 없습니다. 이는 Audit Manager가 자동으로 데이터 소스 및 서비스를 매핑하고 선택하기 때문입니다. 이 선택은 NIST 사이버 보안 프레임워크 버전 1.1 프레임워크의 요구 사항에 따라 이루어집니다. 이 프레임워크의 범위 내에서 서비스 목록을 편집해야 하는 경우 CreateAssessment 또는 UpdateAssessment API 작업을 사용하여 편집할 수 있습니다. 또는 표준 프레임워크를 사용자 지정한 다음 사용자 지정 프레임워크에서 평가를 생성할 수도 있습니다.

특정 요구 사항을 지원하도록 이 프레임워크를 사용자 지정하는 방법에 대한 지침은 기존 프레임워크 사용자 지정 및 기존 컨트롤 사용자 지정을 참조하십시오.

추가 NIST 리소스

- NIST(국립표준기술연구소)

- NIST 컴퓨터 보안 리소스 센터
- NIST AWS 규정 준수 페이지
- NIST 사이버 보안 프레임워크 - AWS 클라우드의 NIST CSF에 맞춰 조정

NIST SP 800-171(개정 2)

AWS Audit Manager는 AWS 모범 사례를 기반으로 NIST SP 800-171 규정 준수 표준에 대한 평가를 구조화하고 자동화하는 사전 구축된 프레임워크를 제공합니다.

> **Note**
>
> - NIST 800-53(개정 5) 낮음-보통-높음을 지원하는 Audit Manager 프레임워크에 대한 자세한 내용은 NIST 800-53 (개정판 5) 낮음-보통-높음을 참조하십시오.
> - NIST 사이버 보안 프레임워크 버전 1.1을 지원하는 Audit Manager 프레임워크에 대한 자세한 내용은 NIST 사이버 보안 프레임워크 버전 1.1을 참조하십시오.

주제

- NIST SP 800-171이란 무엇입니까?
- 이 프레임워크를 사용하여 감사 준비 지원
- 추가 NIST 리소스

NIST SP 800-171이란 무엇입니까?

NIST SP 800-171은 비연방 시스템 및 조직에서 통제 비분류 정보(CUI)의 기밀을 보호하는 데 중점을 둡니다. 이는 해당 목표를 달성하기 위한 특정 보안 요구 사항을 권장합니다. NIST 800-171은 네트워크에서 CUI를 처리하는 비연방 조직에 필요한 보안 표준 및 관행을 요약한 간행물입니다. 이는 NIST(국립표준기술연구소)에서 2015년 6월에 처음 출판했습니다. NIST는 공공 및 민간 부문의 사이버 보안 복원력을 강화하기 위해 여러 표준 및 간행물을 발표한 미국 정부 기관입니다. NIST 800-171은 새로운 사이버 위협과 변화하는 기술에 따라 정기적으로 업데이트를 받았습니다. 최신 버전(개정 2)은 2020년 2월에 릴리스되었습니다.

NIST 800-171 내의 사이버 보안 컨트롤은 정부 계약자 및 하청업체의 IT 네트워크에서 CUI를 보호합니다. 정부 계약자가 네트워크에서 CUI를 처리하거나 저장할 때 준수해야 하는 관행과 절차를 정의합니다. NIST 800-171은 계약업체 네트워크에서 CUI가 있는 부분에만 적용됩니다.

이 프레임워크를 사용하여 감사 준비 지원

NIST SP 800-171 개정 2 프레임워크를 사용하여 감사를 준비할 수 있습니다. 이 프레임워크에는 설명 및 테스트 절차가 포함된 사전 구축된 컨트롤 컬렉션이 포함되어 있습니다. 이러한 컨트롤은 NIST 요구 사항에 따라 컨트롤 세트로 그룹화됩니다. 특정 요구 사항이 있는 내부 감사를 지원하도록 이 프레임워크와 해당 컨트롤을 사용자 지정할 수도 있습니다.

프레임워크를 출발점으로 사용하여 Audit Manager 평가를 생성하고 감사와 관련된 증거 수집을 시작할 수 있습니다. 평가를 생성하면 Audit Manager가 AWS 리소스 평가를 시작합니다. 이는 NIST SP 800-171 개정 2 프레임워크에 정의된 컨트롤을 기반으로 이 작업을 수행합니다. 감사 시기가 되면 사용자 또는 사용자가 선택한 대리인이 Audit Manager에서 수집한 증거를 검토할 수 있습니다. 어느 방식으로든 평가에서 증거 폴더를 찾아보고 평가 보고서에 포함할 증거를 선택할 수 있습니다. 또는 증거 찾기 기능을 활성화한 경우 특정 증거를 검색하고 CSV 형식으로 내보내거나 검색 결과에서 평가 보고서를 생성할 수 있습니다. 둘 중 하나의 방식으로 이 평가 보고서를 사용하여 제어가 의도한 대로 작동하고 있음을 보여줄 수 있습니다.

NIST SP 800-171 (개정 2) 프레임워크 세부 정보는 다음과 같습니다.

AWS Audit Manager에서의 프레임워크 이름	자동화된 컨트롤 수	수동 컨트롤 수	컨트롤 세트 수	범위 내 AWS 서비스
NIST SP 800-171 (개정 2)	66	58	16	• Amazon CloudWatch • Amazon Elastic Compute Cloud • AWS CloudTrail • AWS Config • AWS Identity and Access Management • AWS Security Hub

> **Tip**
>
> 이 표준 프레임워크에서 데이터 소스 매핑으로 사용되는 AWS Config 규칙을 검토하려면 AuditManager_ConfigDataSourceMappings_NIST-SP-800-171-Rev.2.zip 파일을 다운로드하십시오.

이 AWS Audit Manager 프레임워크의 컨트롤은 시스템이 NIST 800-171을 준수하는지 확인하기 위한 것이 아닙니다. 게다가 이는 NIST 감사 통과를 보장할 수도 없습니다. AWS Audit Manager는 수동 증거 수집이 필요한 절차상의 컨트롤을 자동으로 확인하지 않습니다.

이 프레임워크는 Audit Manager의 프레임워크 라이브러리의 표준 프레임워크 탭에서 찾을 수 있습니다.

이 프레임워크를 사용하여 평가를 생성하는 방법에 대한 자세한 내용은 평가 생성을 참조하십시오.

Audit Manager 콘솔을 사용하여 이 표준 프레임워크에서 평가를 생성하면 범위 내 AWS 서비스 목록이 기본적으로 선택되며 편집할 수 없습니다. 이는 Audit Manager가 자동으로 데이터 소스 및 서비스를 매핑하고 선택하기 때문입니다. 이 선택은 NIST SP 800-171 개정 2 프레임워크의 요구 사항에 따라 이루어집니다. 이 프레임워크의 범위 내에서 서비스 목록을 편집해야 하는 경우 CreateAssessment 또는 UpdateAssessment API 작업을 사용하여 편집할 수 있습니다. 또는 표준 프레임워크를 사용자 지정한 다음 사용자 지정 프레임워크에서 평가를 생성할 수도 있습니다.

특정 요구 사항을 지원하도록 이 프레임워크를 사용자 지정하는 방법에 대한 지침은 기존 프레임워크 사용자 지정 및 기존 컨트롤 사용자 지정을 참조하십시오.

추가 NIST 리소스

- NIST(국립표준기술연구소)
- NIST 컴퓨터 보안 리소스 센터
- NIST AWS 규정 준수 페이지

PCI DSS V3.2.1

AWS Audit Manager는 PCI DSS v3.2.1을 지원하는 사전 빌드된 프레임워크를 제공합니다.

> **Note**
>
> PCI DSS v4 및 여기서 지원하는 Audit Manager 프레임워크에 대한 자세한 내용은 PCI DSS V4.0 섹션을 참조하세요.

주제

PCI DSS란 무엇입니까?

PCI DSS(신용카드 업계 데이터 보안 표준)는 독점적인 정보 보안 표준입니다. 이는 American Express, Discover Financial Services, JCB International, MasterCard Worldwide 및 Visa Inc.에 의해 설립된 PCI 보안 표준 위원회에 의해 관리됩니다. PCI DSS는 카드 소지자 데이터(CHD) 또는 중요한 인증 데이터(SAD)를 저장, 처리 또는 전송하는 엔티티에 적용됩니다. 여기에는 판매자, 처리자, 인수자, 발행자 및 서비스 제공자가 포함되며 이에 국한되지는 않습니다. PCI DSS는 카드 회사에서 의무적으로 사용해야 하며, PCI(Payment Card Industry) 보안 표준 위원회에서 관리합니다.

AWS는 PCI DSS 레벨 1 서비스 제공업체 인증을 받았으며, 이는 현존하는 최고 수준의 평가입니다. 규정 준수 평가는 독립적인 QSA(공인보안평가기관)인 Coalfire Systems Inc.에서 수행했습니다. PCI DSS 규정 준수 증명(AOC) 및 책임 요약은 AWS Artifact를 통해 확인할 수 있습니다. 이 포털은 AWS 규정 준수 보고서에 온디맨드로 액세스할 수 있는 셀프 서비스 포털입니다. AWS 관리 AWS Artifact 콘솔에 로그인하거나 AWS Artifact 시작하기에서 자세히 알아보십시오.

PCI DSS 표준은 PCI 보안 표준 위원회 문서 라이브러리에서 다운로드할 수 있습니다.

이 프레임워크를 사용하여 감사 준비 지원

PCI DSS V3.2.1 프레임워크를 사용하여 감사를 준비할 수 있습니다. 이 프레임워크에는 설명 및 테스트 절차가 포함된 사전 구축된 컨트롤 컬렉션이 포함되어 있습니다. 이러한 컨트롤은 PCI DSS 요구 사항에 따라 컨트롤 세트로 그룹화됩니다. 특정 요구 사항이 있는 내부 감사를 지원하도록 이 프레임워크와 해당 컨트롤을 사용자 지정할 수도 있습니다.

프레임워크를 출발점으로 사용하여 Audit Manager 평가를 생성하고 감사와 관련된 증거 수집을 시작할 수 있습니다. 평가를 생성하면 Audit Manager가 AWS 리소스 평가를 시작합니다. 이는 PCI DSS V3.2.1 프레임워크에 정의된 컨트롤을 기반으로 이 작업을 수행합니다. 감사 시기가 되면 사용자 또는

사용자가 선택한 대리인이 Audit Manager에서 수집한 증거를 검토할 수 있습니다. 어느 방식으로든 평가에서 증거 폴더를 찾아보고 평가 보고서에 포함할 증거를 선택할 수 있습니다. 또는 증거 찾기 기능을 활성화한 경우 특정 증거를 검색하고 CSV 형식으로 내보내거나 검색 결과에서 평가 보고서를 생성할 수 있습니다. 둘 중 하나의 방식으로 이 평가 보고서를 사용하여 제어가 의도한 대로 작동하고 있음을 보여줄 수 있습니다.

PCI DSS V3.2.1 프레임워크 세부 정보는 다음과 같습니다.

AWS Audit Manager에서의 프레임워크 이름	자동화된 컨트롤 수	수동 컨트롤 수	컨트롤 세트 수	범위 내 AWS 서비스
PCI DSS V3.2.1	175	487	12	• Amazon Elastic Compute Cloud • AWS CloudTrail • AWS Config • AWS Identity and Access Management • AWS Security Hub

> **Tip**
>
> 이 표준 프레임워크에서 데이터 소스 매핑으로 사용되는 AWS Config 규칙을 검토하려면 AuditManager_ConfigDataSourceMappings_PCI-DSS-V3.2.1.zip 파일을 다운로드하십시오.

이 AWS Audit Manager 프레임워크의 컨트롤은 시스템이 PCI DSS 표준을 준수하는지 확인하기 위한 것이 아닙니다. 게다가 이는 PCI DSS 감사를 통과할 것이라고 보장할 수도 없습니다. AWS Audit Manager는 수동 증거 수집이 필요한 절차상의 컨트롤을 자동으로 확인하지 않습니다.

이 프레임워크는 Audit Manager의 프레임워크 라이브러리의 표준 프레임워크 탭에서 찾을 수 있습니다.

이 프레임워크를 사용하여 평가를 생성하는 방법에 대한 자세한 내용은 평가 생성을 참조하십시오.

Audit Manager 콘솔을 사용하여 이 표준 프레임워크에서 평가를 생성하면 범위 내 AWS 서비스 목록이 기본적으로 선택되며 편집할 수 없습니다. 이는 Audit Manager가 자동으로 데이터 소스 및 서비스를 매핑하고 선택하기 때문입니다. 이 선택은 PCI DSS V3.2.1 프레임워크의 요구 사항에 따라 이루어집니다. 이 프레임워크의 범위 내에서 서비스 목록을 편집해야 하는 경우 CreateAssessment 또는 UpdateAssessment API 작업을 사용하여 편집할 수 있습니다. 또는 표준 프레임워크를 사용자 지정한 다음 사용자 지정 프레임워크에서 평가를 생성할 수도 있습니다.

특정 요구 사항을 지원하도록 이 프레임워크를 사용자 지정하는 방법에 대한 지침은 기존 프레임워크 사용자 지정 및 기존 컨트롤 사용자 지정을 참조하십시오.

추가 PCI DSS 리소스

- PCI 보안 표준 위원회
- PCI 보안 표준 위원회 문서 라이브러리.
- PCI AWS DSS 규정 준수 페이지

PCI DSS V4.0

AWS Audit Manager에서는 Payment Card Industry Data Security Standard(PCI DSS) v4.0을 지원하는 사전 구축된 프레임워크를 제공합니다.

> **Note**
>
> PCI DSS v3.2.1 및 여기서 지원하는 Audit Manager 프레임워크에 대한 자세한 내용은 PCI DSS V3.2.1 섹션을 참조하세요.

주제

- PCI DSS란 무엇입니까?
- 이 프레임워크를 사용하여 감사 준비 지원
- 추가 PCI DSS 리소스

PCI DSS란 무엇입니까?

Payment Card Industry Data Security Standard(PCI DSS)는 지불 데이터 보호를 위한 기술 및 운영 요구 사항의 기준을 제공하는 글로벌 표준입니다. PCI DSS v4.0은 표준의 차세대 진화 버전입니다.

PCI DSS는 지불 카드 계정 데이터 보안을 장려하고 강화하기 위해 개발되었습니다. 또한 전 세계적으로 일관된 데이터 보안 조치를 광범위하게 채택할 수 있도록 지원합니다. 계정 데이터를 보호하도록 설계된 기술 및 운영 요구 사항의 기준도 제공합니다. PCI DSS는 지불 카드 계정 데이터를 사용하는 환경에 초점을 맞추도록 특별히 설계되었지만 위협으로부터 보호하고 결제 환경의 다른 요소를 보호하는 데에도 사용할 수 있습니다.

PCI Security Standards Council(PCI SSC)에서는 PCI DSS v3.2.1 및 v4.0 사이에서 많은 변경 사항을 도입했습니다. 이번 업데이트는 세 가지 카테고리로 구분됩니다.

1. 변화하는 요구 사항 - 새로운 위협과 기술, 결제 업계의 변화에 따라 표준을 최신 상태로 유지하기 위한 변경 사항. 신규 또는 수정된 요구 사항이나 테스트 절차, 요구 사항 제거 등을 예로 들 수 있습니다.
2. 설명 또는 지침 - 특정 주제에 대한 이해를 높이거나 추가 정보 또는 지침을 제공하기 위한 용어, 설명, 정의, 추가 지침 또는 지침에 대한 업데이트.
3. 구조 또는 형식 - 콘텐츠를 조정하기 위한 요구 사항의 결합, 분리 및 번호 재지정을 포함한 콘텐츠 재구성.

변경 사항에 대한 자세한 내용은 Summary of changes from PCI DSS Version 3.2.1 to 4.0을 참조하세요.

이 프레임워크를 사용하여 감사 준비 지원

> **Note**
>
> 이 표준 프레임워크는 Security Hub의 통합 제어를 데이터 소스로 사용합니다. 통합 제어에서 증거를 성공적으로 수집하려면 Security Hub에서 통합 제어 분석 결과 설정을 켜야 합니다. Security Hub를 데이터 소스 유형으로 사용하는 방법에 대한 자세한 내용은 AWS Audit Manager에서 지원하는 AWS Security Hub 제어를 참조하세요.

PCI DSS V4.0 프레임워크를 사용하여 감사를 준비할 수 있습니다. 이 프레임워크에는 설명 및 테스트 절차가 포함된 사전 구축된 컨트롤 컬렉션이 포함되어 있습니다. 이러한 제어는 PCI DSS V4.0 요구 사항에 따라 제어 세트로 그룹화됩니다. 특정 요구 사항이 있는 내부 감사를 지원하도록 이 프레임워크와 해당 컨트롤을 사용자 지정할 수도 있습니다.

프레임워크를 출발점으로 사용하여 Audit Manager 평가를 생성하고 감사와 관련된 증거 수집을 시작할 수 있습니다. 평가를 생성하면 Audit Manager가 AWS 리소스 평가를 시작합니다. 이는 PCI DSS V4.0 프레임워크에 정의된 제어를 기반으로 이 작업을 수행합니다. 감사 시기가 되면 사용자 또는 사용

자가 선택한 대리인이 Audit Manager에서 수집한 증거를 검토할 수 있습니다. 어느 방식으로든 평가에서 증거 폴더를 찾아보고 평가 보고서에 포함할 증거를 선택할 수 있습니다. 또는 증거 찾기 기능을 활성화한 경우 특정 증거를 검색하고 CSV 형식으로 내보내거나 검색 결과에서 평가 보고서를 생성할 수 있습니다. 둘 중 하나의 방식으로 이 평가 보고서를 사용하여 제어가 의도한 대로 작동하고 있음을 보여줄 수 있습니다.

프레임워크 세부 정보는 다음과 같습니다.

AWS Audit Manager에서의 프레임워크 이름	자동화된 컨트롤 수	수동 컨트롤 수	컨트롤 세트 수	범위 내 AWS 서비스
PCI DSS v4.0	152	128	15	• Amazon API Gateway • Amazon CloudFront • Amazon CloudWatch • Amazon DynamoDB • Amazon Elastic Compute Cloud • Amazon OpenSearch Service • Amazon Redshift • Amazon Relationa l Database Service • Amazon SageMaker • Amazon Simple Storage Service(S3)

AWS Audit Manager에서의 프레임워크 이름	자동화된 컨트롤 수	수동 컨트롤 수	컨트롤 세트 수	범위 내 AWS 서비스
				• AWS Backup • AWS CloudTrail • AWS Config • AWS Identity and Access Management • AWS KMS • AWS Secrets Manager • AWS Security Hub • AWS WAF

> **Tip**
>
> 이 표준 프레임워크에서 데이터 소스 매핑으로 사용되는 AWS Config 규칙을 검토하려면 AuditManager_ConfigDataSourceMappings_PCI-DSS-V4.zip 파일을 다운로드합니다.

이 AWS Audit Manager 프레임워크의 컨트롤은 시스템이 PCI DSS 표준을 준수하는지 확인하기 위한 것이 아닙니다. 게다가 이는 PCI DSS 감사를 통과할 것이라고 보장할 수도 없습니다. AWS Audit Manager는 수동 증거 수집이 필요한 절차상의 컨트롤을 자동으로 확인하지 않습니다.

이 프레임워크는 Audit Manager의 프레임워크 라이브러리의 표준 프레임워크 탭에서 찾을 수 있습니다.

이 프레임워크를 사용하여 평가를 생성하는 방법에 대한 자세한 내용은 평가 생성을 참조하십시오.

Audit Manager 콘솔을 사용하여 이 표준 프레임워크에서 평가를 생성하면 범위 내 AWS 서비스 목록이 기본적으로 선택되며 편집할 수 없습니다. 이는 Audit Manager가 자동으로 데이터 소스 및 서비스를 매핑하고 선택하기 때문입니다. PCI DSS V4 프레임워크의 요구 사항에 따라 선택됩니다. 이 프레임워크의 범위 내에서 서비스 목록을 편집해야 하는 경우 CreateAssessment 또는 UpdateAssessment

API 작업을 사용하여 편집할 수 있습니다. 또는 표준 프레임워크를 사용자 지정한 다음 사용자 지정 프레임워크에서 평가를 생성할 수도 있습니다.

특정 요구 사항을 지원하도록 이 프레임워크를 사용자 지정하는 방법에 대한 지침은 기존 프레임워크 사용자 지정 및 기존 컨트롤 사용자 지정을 참조하십시오.

추가 PCI DSS 리소스

- PCI DSS v4.0 Resource Hub
- PCI 보안 표준 위원회
- PCI 보안 표준 위원회 문서 라이브러리.
- PCI AWS DSS 규정 준수 페이지
- Payment Card Industry Data Security Standard (PCI DSS) v4.0 on AWS Compliance Guide
- Summary of changes from PCI DSS Version 3.2.1 to 4.0

SOC 2

SOC 2는 회사 데이터가 안전하게 관리되는지 확인하는 감사 절차입니다. AWS Audit Manager는 SOC 2를 지원하는 사전 구축된 프레임워크를 제공합니다.

주제

- SOC 2란 무엇입니까?
- 이 프레임워크를 사용하여 감사 준비 지원
- 추가 SOC 2 리소스

SOC 2란 무엇입니까?

미국공인회계사협회(AICPA)에서 정의한 시스템 및 조직 컨트롤(SOC) 는 감사 중에 작성되는 일련의 보고서의 이름입니다. 이는 서비스 조직(다른 조직에 정보 시스템을 서비스로 제공하는 조직) 이 해당 서비스 사용자에게 해당 정보 시스템에 대한 내부 컨트롤에 대한 검증된 보고서를 발행하는 데 사용됩니다. 보고서는 신뢰 서비스 원칙으로 알려진 다섯 가지 범주로 분류된 컨트롤에 초점을 맞춥니다.

AWS SOC 보고서는 AWS가 주요 규정 준수 컨트롤 항목 및 목표를 어떻게 준수하고 있는지를 입증하는 독립적인 타사 심사 보고서입니다. 이러한 보고서의 목적은 운영 및 규정 준수를 뒷받침하기 위해 확립된 AWS 컨트롤을 고객과 고객 측 감사 기관이 이해하도록 돕는 데 있습니다. 다음과 같은 다섯 가지 AWS SOC 보고서가 있습니다.

- AWS SOC 1 보고서, AWS Artifact 에서 AWS 고객에게 제공됨.
- AWS SOC 2 보안, 가용성 및 기밀성 보고서, AWS Artifact에서 AWS 고객에게 제공됨.
- AWS SOC 2 보안, 가용성 및 기밀성 보고서, AWS Artifact에서 AWS 고객에게 제공됨(범위에는 Amazon DocumentDB만 포함).
- AWS SOC 2 개인 정보 보호 유형 I 보고서, AWS Artifact에서 AWS 고객에게 제공됨.
- AWS SOC 3 보안, 가용성 및 기밀성 보고서, 백서로 공개됨.

이 프레임워크를 사용하여 감사 준비 지원

이 프레임워크를 사용하여 감사를 준비할 수 있습니다. 이 프레임워크에는 설명 및 테스트 절차가 포함된 사전 구축된 컨트롤 컬렉션이 포함되어 있습니다. 이러한 컨트롤은 SOC 2 요구 사항에 따라 컨트롤 세트로 그룹화됩니다. 특정 요구 사항이 있는 내부 감사를 지원하도록 이 프레임워크와 해당 컨트롤을 사용자 지정할 수도 있습니다.

프레임워크를 출발점으로 사용하여 Audit Manager 평가를 생성하고 감사와 관련된 증거 수집을 시작할 수 있습니다. 평가를 생성하면 Audit Manager가 AWS 리소스 평가를 시작합니다. 이는 프레임워크에 정의된 컨트롤을 기반으로 이 작업을 수행합니다. 감사 시기가 되면 사용자 또는 사용자가 선택한 대리인이 Audit Manager에서 수집한 증거를 검토할 수 있습니다. 어느 방식으로든 평가에서 증거 폴더를 찾아보고 평가 보고서에 포함할 증거를 선택할 수 있습니다. 또는 증거 찾기 기능을 활성화한 경우 특정 증거를 검색하고 CSV 형식으로 내보내거나 검색 결과에서 평가 보고서를 생성할 수 있습니다. 둘 중 하나의 방식으로 이 평가 보고서를 사용하여 제어가 의도한 대로 작동하고 있음을 보여줄 수 있습니다.

프레임워크 세부 정보는 다음과 같습니다.

AWS Audit Manager에서의 프레임워크 이름	자동화된 컨트롤 수	수동 컨트롤 수	컨트롤 세트 수	범위 내 AWS 서비스
SOC 2	20	41	20	• Amazon Elastic Compute Cloud • AWS Auto Scaling • AWS CloudTrail • AWS Config

AWS Audit Manager에서의 프레임워크 이름	자동화된 컨트롤 수	수동 컨트롤 수	컨트롤 세트 수	범위 내 AWS 서비스
				• AWS Identity and Access Management • AWS Security Hub

> **Tip**
>
> 이 표준 프레임워크에서 데이터 소스 매핑으로 사용되는 AWS Config 규칙을 검토하려면 AuditManager_ConfigDataSourceMappings_SOC2.zip 파일을 다운로드하십시오.

이 AWS Audit Manager 프레임워크의 컨트롤은 시스템이 규정을 준수하는지 확인하기 위한 것이 아닙니다. 게다가 이는 감사 통과를 보장할 수도 없습니다. AWS Audit Manager는 수동 증거 수집이 필요한 절차상의 컨트롤을 자동으로 확인하지 않습니다.

이 프레임워크는 Audit Manager의 프레임워크 라이브러리의 표준 프레임워크 탭에서 찾을 수 있습니다.

이 프레임워크를 사용하여 평가를 생성하는 방법에 대한 지침은 평가 생성을 참조하십시오.

Audit Manager 콘솔을 사용하여 이 표준 프레임워크에서 평가를 생성하면 범위 내 AWS 서비스 목록이 기본적으로 선택되며 편집할 수 없습니다. 이는 Audit Manager가 자동으로 데이터 소스 및 서비스를 매핑하고 선택하기 때문입니다. 이 선택은 SOC 2 요구 사항에 따라 이루어집니다. 이 프레임워크의 범위 내에서 서비스 목록을 편집해야 하는 경우 CreateAssessment 또는 UpdateAssessment API 작업을 사용하여 편집할 수 있습니다. 또는 표준 프레임워크를 사용자 지정한 다음 사용자 지정 프레임워크에서 평가를 생성할 수도 있습니다.

특정 요구 사항을 지원하도록 이 프레임워크를 사용자 지정하는 방법에 대한 지침은 기존 프레임워크 사용자 지정 및 기존 컨트롤 사용자 지정을 참조하십시오.

추가 SOC 2 리소스

- SOC AWS 규정 준수 페이지

컨트롤 라이브러리

Audit Manager의 컨트롤 라이브러리에서 컨트롤에 액세스하고 관리할 수 있습니다. Audit Manager 콘솔의 탐색 창에서 컨트롤 라이브러리를 선택하여 언제든지 컨트롤 라이브러리로 이동할 수 있습니다.

컨트롤 라이브러리에는 표준 컨트롤 및 사용자 지정 컨트롤 카탈로그가 포함되어 있습니다.

- 표준 컨트롤은 AWS에서 제공하는 사전 정의된 컨트롤입니다. 표준 컨트롤의 구성 세부 정보를 볼 수 있지만, 편집하거나 삭제할 수는 없습니다. 하지만, 표준 컨트롤을 사용자 지정하여 특정 요구사항에 맞는 새 컨트롤을 만들 수 있습니다.
- 사용자 지정 컨트롤은 사용자가 담당하고 정의하는 사용자 지정 컨트롤입니다. 사용자 지정 컨트롤을 이용하면 증거를 수집하려는 데이터 소스를 지정할 수 있습니다. 그런 다음, 사용자 지정 프레임워크에 사용자 지정 컨트롤을 추가할 수 있습니다.

  사용자 지정 프레임워크에 사용자 지정 컨트롤을 추가하는 방법에 대한 자세한 내용은 프레임워크 라이브러리 부분을 참조하세요. Audit Manager 프레임워크에서 평가를 생성하는 방법에 대한 자세한 내용은 AWS Audit Manager에서의 평가 부분을 참조하세요.

이 섹션에서는 Audit Manager에서 사용자 지정 컨트롤을 만들고 관리하는 방법을 설명합니다.

주제

AWS Audit Manager에서 사용 가능한 컨트롤에 액세스할 수 있습니다.

Audit Manager 콘솔의 컨트롤 라이브러리 페이지에서 이용 가능한 모든 컨트롤을 볼 수 있습니다. 여기에서 사용자 지정 컨트롤 생성하거나 기존 컨트롤을 사용자 지정할 수도 있습니다.

Audit Manager API 또는 AWS Command Line Interface (AWS CLI) 를 사용하여 사용 가능한 모든 제어 기능을 볼 수도 있습니다.

Audit Manager console

이용 가능한 컨트롤(콘솔)을 보려면

1. https://console.aws.amazon.com/auditmanager/home에서 AWS Audit Manager 콘솔을 엽니다.
2. 탐색 창에서 컨트롤 라이브러리를 선택합니다.
3. 표준 컨트롤 탭 또는 사용자 지정 컨트롤 탭을 선택하여 이용 가능한 컨트롤을 찾아보세요.
4. 컨트롤에 대한 세부 정보를 보려면 컨트롤 이름을 선택합니다.

AWS CLI

이용 가능한 컨트롤(AWS CLI)을 보려면

컨트롤 목록 표시 명령을 실행하고 `--control-type`의 유형을 지정합니다. 표준 컨트롤 목록을 검색하거나, 사용자 지정 컨트롤 세부 정보 목록을 검색할 수 있습니다.

```
aws auditmanager list-controls --control-type Standard
```

```
aws auditmanager list-controls --control-type Custom
```

Audit Manager API

이용 가능한 컨트롤 세부 정보(API)를 보려면

ListControls작업을 사용하고 제어 유형을 지정합니다. 표준 컨트롤 목록을 보거나, 사용자 지정 컨트롤 목록을 볼 수 있습니다.

자세한 내용은 이전 링크 중 하나를 선택하여 AWS Audit Manager API 참조에서 자세한 내용을 읽어보십시오. 여기에는 언어별 AWS SDK 중 하나에서 `ListControls` 작업 및 매개변수를 사용하는 방법에 대한 정보가 포함됩니다.

컨트롤의 세부 정보 검토

Audit Manager 콘솔, Audit Manager API 또는 AWS Command Line Interface (AWS CLI)을 이용하여 컨트롤 세부 정보를 검토할 수 있습니다.

Audit Manager console

컨트롤 세부 정보(콘솔)를 보려면

1. https://console.aws.amazon.com/auditmanager/home에서 AWS Audit Manager 콘솔을 엽니다.
2. 이용 가능한 컨트롤 목록을 보려면 탐색 창에서 컨트롤 라이브러리를 선택합니다.
3. 표준 컨트롤 탭 또는 사용자 지정 컨트롤 탭을 선택하여 이용 가능한 컨트롤을 찾아보세요.
4. 컨트롤에 대한 세부 정보를 보려면 컨트롤 이름을 선택합니다.

컨트롤을 열면 컨트롤 세부 정보 페이지가 표시됩니다. 이 페이지의 섹션 및 내용을 아래에서 설명합니다.

요약 섹션

이 섹션에서는 컨트롤의 개요를 다룹니다. 여기에는 다음 정보가 포함됩니다.

- 컨트롤 이름 - 컨트롤의 이름
- 컨트롤 유형 - 컨트롤이 표준 컨트롤인지 사용자 지정 컨트롤인지를 표시
- 태그 - 컨트롤과 연결된 태그의 수
- 데이터 소스 유형 - 이 컨트롤에 사용되는 데이터 소스 유형의 수
- 매핑 - 데이터 소스에서 데이터를 검색하는 데 사용되는 매핑 속성의 수

사용자 지정 컨트롤을 보는 경우, 다음과 같은 세부 정보도 표시됩니다.

- 만든 사람 - 사용자 지정 컨트롤을 만든 계정
- 만든 날짜 - 사용자 지정 컨트롤을 만든 날짜
- 최종 업데이트 - 사용자 지정 컨트롤을 마지막으로 편집한 날짜

세부 정보 탭

이 탭에서는 컨트롤에 대한 기본 개요를 제공합니다. 여기에는 다음 정보가 포함됩니다.

- 설명 섹션 - 컨트롤에 대한 설명을 제공합니다.
- 테스트 정보 섹션 - 컨트롤에 권장되는 테스트 절차에 대한 설명을 제공합니다.
- 실행 계획 섹션 - 통제를 개선해야 할 경우, 수행해야 할 권장 조치를 설명합니다.

데이터 소스 탭

이 탭에는 컨트롤의 데이터 소스에 대한 정보가 표시됩니다. 여기에는 다음 정보가 포함됩니다.

- 데이터 소스 이름 - 사용자 지정 컨트롤에만 적용됩니다. 각 데이터 소스에 부여한 설명형 이름을 나타냅니다. 이 이름을 이용하여 동일한 데이터 소스 유형에 속하는 여러 데이터 소스를 구별할 수 있습니다.
- 데이터 소스 유형 - 증거 데이터의 출처를 표시해 줍니다.
  - Audit Manager에서 증거를 수집하는 경우, 데이터 소스는 AWS Security Hub, AWS Config, AWS CloudTrail 또는 AWS API 호출의 네 가지 유형 중 하나일 수 있습니다.
  - 사용자만의 고유 증거를 업로드하는 경우, 데이터 소스 유형은 수동입니다. 설명란은 필요한 수동 증거가 파일 업로드인지 또는 텍스트 응답인지를 나타냅니다.
- 매핑 - 데이터 소스에서 데이터를 식별하고 검색하는 데 사용되는 매핑 속성입니다.
  - 데이터 소스 유형이 AWS Config인 경우 매핑은 특정 AWS Config 규칙의 이름입니다 (예:). `EC2_INSTANCE_MANAGED_BY_SSM` Audit Manager는 이 매핑을 사용하여 해당 규칙 검사의 결과를 에서 직접 AWS Config보고합니다.
  - 데이터 원본 유형이 AWS Security Hub인 경우 매핑은 특정 Security Hub 컨트롤 (예:`1.1 – Avoid the use of the "root" account`) 의 이름입니다. Audit Manager는 이 매핑을 이용하여 해당 보안 검사의 결과를 Security Hub으로부터 직접 보고합니다..
  - 데이터 소스 유형이 AWS API 호출인 경우 매핑은 특정 API 호출 (예:`ec2_DescribeSecurityGroups`) 의 이름입니다. Audit Manager는 이 매핑을 이용하여 API 응답을 수집합니다.
  - 데이터 소스가 AWS CloudTrail인 경우 매핑은 특정 CloudTrail 이벤트 (예:`CreateAccessKey`) 의 이름입니다. Audit Manager는 이 매핑을 사용하여 CloudTrail 로그에서 관련 사용자 활동을 수집합니다.
- 빈도 - Audit Manager가 데이터 소스에서 증거를 수집하는 빈도를 표시합니다. 빈도는 데이터 소스 유형에 따라 달라집니다. 자세한 내용은 열에서 값을 선택하거나 증거 수집 빈도 부분을 참조하세요.

태그 탭

이 탭에는 컨트롤과 연결된 태그가 나열됩니다. 여기에는 다음 정보가 포함됩니다.

- 키 - 태그 키(예: 규정 준수 표준, 규정 또는 범주)입니다.
- 값 - 태그 값

AWS CLI

컨트롤 세부 정보(AWS CLI)를 보려면

1. 검토하고자 하는 컨트롤을 식별하려면 컨트롤 목록 표시 명령을 실행하고 `--control-type`를 지정합니다. 표준 컨트롤 목록을 검색하거나, 사용자 지정 컨트롤 세부 정보 목록을 검색할 수 있습니다.

   다음 예에서는 *## ### ###*를 `Custom` 또는 `Standard`으로 바꿉니다.

   ```
   aws auditmanager list-controls --control-type Custom/Standard
   ```

   그 응답으로 컨트롤 목록을 볼 수 있습니다. 검토할 컨트롤을 찾고 컨트롤 ID와 Amazon 리소스 이름(ARN)을 기록해 둡니다.

2. 컨트롤 세부 정보를 가져오려면 컨트롤 가져오기 명령을 실행하고 `--control-id`를 지정합니다.

   다음 예에서는 각 *## ### ###*를 자신의 정보로 바꿉니다.

   ```
   aws auditmanager get-control --control-id a1b2c3d4-5678-90ab-cdef-EXAMPLE11111
   ```

   컨트롤 세부 정보가 JSON 형식으로 표시됩니다. 이 데이터를 이해하려면 AWS CLI 명령 참조의 컨트롤 출력 가져오기 부분을 참조하세요.

3. 컨트롤의 태그를 보려면 list-tags-for-resource명령을 사용하고 컨트롤의 태그를 지정하십시오. `--resource-arn`

   다음 예에서는 각 *## ### ###*를 자신의 정보로 바꿉니다.

   ```
   aws auditmanager list-tags-for-resource --resource-arn arn:aws:auditmanager:us-east-1:111122223333:control/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111
   ```

   Audit Manager의 태그에 대한 자세한 내용은 AWS Audit Manager 리소스 태그 지정을 참조하십시오.

Audit Manager API

컨트롤 세부 정보(API)를 보려면

1. 검토하려는 컨트롤을 식별하려면 ListControls작업을 사용하고 ControlType을 지정하십시오. 표준 컨트롤 목록을 보거나, 사용자 지정 컨트롤 목록을 볼 수 있습니다.

   이 응답에서, 검토할 컨트롤을 찾고 컨트롤 ID와 Amazon 리소스 이름(ARN)을 기록해 둡니다.
2. 컨트롤 세부 정보를 가져오려면 작업을 사용하십시오. GetControl 이 요청에서는, 1단계에서 얻은 ControlID를 지정합니다.

   컨트롤 세부 정보가 JSON 형식으로 표시됩니다. 이 데이터를 이해하려면 AWS Audit Manager API 참조의 GetControl 응답 요소를 참조하십시오.
3. 컨트롤의 태그를 보려면 ListTagsForResource작업을 사용하십시오. 이 요청에서는, 1단계에서 얻은 컨트롤 ResourceARN을 지정합니다.

Audit Manager의 태그에 대한 자세한 내용은 AWS Audit Manager 리소스 태그 지정을 참조하십시오.

이러한 API 작업에 대한 자세한 내용은 이전 링크 중 하나를 선택하여 AWS Audit Manager API 참조에서 자세한 내용을 읽어보세요. 여기에는 언어별 AWS SDK 중 하나에서 이러한 작업 및 매개변수를 사용하는 방법에 대한 정보가 포함됩니다.

사용자 지정 컨트롤 생성

사용자 지정 컨트롤을 이용하여 사용자가 정의한 특정 데이터 소스에서 증거를 수집할 수 있습니다.

표준 컨트롤과 마찬가지로, 사용자 지정 컨트롤은 평가에서 활성화되어 있으면 지속적으로 증거를 수집합니다. 생성한 모든 사용자 지정 컨트롤에 수동 증거를 추가할 수도 있습니다. 각각의 증거는 사용자 지정 컨트롤의 요구사항 준수를 입증하는 데 도움이 되는 기록이 됩니다.

사용자 지정 컨트롤을 사용하는 방법의 몇 가지 예를 보여드리면서 시작합니다.

기존 컨트롤을 시작점으로 사용

Audit Manager에서 모든 컨트롤을 사용자 지정할 수 있습니다. 기존 컨트롤이 목표에 어느 정도 부합하지만, 지침을 확장하거나 특정 요구사항에 맞게 몇 가지 속성을 조정하고자 하는 경우, 이 방법을 사용하는 것이 좋습니다. 예를 들어, 대조군에서 증거를 수집하는 빈도를 변경한 다음, 이를 반영하도록 컨트롤 이름을 변경할 수 있습니다.

내부 감사를 위한 사용자 지정 컨트롤 생성

내부 감사를 지원하기 위해 특정 규정 준수 프레임워크 또는 규정과 관련 없으면서 용도에 맞게 구축된 사용자 지정 컨트롤을 만들 수 있습니다. 이를 통해 컨트롤 요구사항을 특정 영역에 맞게 조정하거나 비즈니스별 리소스에서 증거를 수집할 수 있습니다. 예를 들어 조직의 사용자 지정 AWS Config 규칙을 증거 수집용 데이터 소스로 사용하는 사용자 지정 컨트롤을 만들 수 있습니다.

공급업체 위험 평가 질문 생성

사용자 지정 컨트롤을 이용하여 공급업체 위험 평가를 관리하는 방법을 지원할 수 있습니다. 생성하는 각 컨트롤은 개별 위험 평가 질문을 나타낼 수 있습니다. 이 경우, 컨트롤 이름이 질문이 될 수 있으며 수동 증거로서 파일을 업로드하거나 텍스트 응답을 입력하여 답변을 제공할 수 있습니다.

사용자 지정 컨트롤을 생성하는 방법은 두 가지가 있습니다. 처음부터 새 컨트롤을 만들거나 기존 컨트롤을 사용자 지정할 수 있습니다.

주제

처음부터 새 사용자 지정 컨트롤 만들기

다음 단계에 따라 사용자 지정 컨트롤을 처음부터 새로 만들 수 있습니다.

> **Important**
>
> 컨트롤 세부 정보, 테스트 정보, 또는 실행 계획과 같은 자유 형식 필드에 중요 식별 정보를 절대 입력하지 않도록 강력히 권장합니다. 민감한 정보가 포함된 사용자 지정 컨트롤을 만드는 경우, 이러한 컨트롤이 포함된 사용자 지정 프레임워크는 공유할 수 없습니다.

주제

1단계: 컨트롤 세부 정보 지정

먼저 사용자 지정 컨트롤의 세부 정보를 지정합니다.

컨트롤 세부 정보를 지정하려면

1. https://console.aws.amazon.com/auditmanager/home에서 AWS Audit Manager 콘솔을 엽니다.
2. 탐색 창에서 컨트롤 라이브러리를 선택한 다음, 사용자 지정 컨트롤 생성을 선택합니다.
3. 컨트롤 세부 정보에서 컨트롤에 대한 다음 정보를 입력합니다.
   - 컨트롤 - 친숙한 이름, 제목 또는 위험 평가 질문을 입력합니다. 이 값은 컨트롤 라이브러리에서 컨트롤을 식별하는 데 도움이 됩니다.
   - 설명(선택 사항) - 다른 사용자가 컨트롤의 목적을 이해하는 데 도움이 되는 세부 정보를 입력합니다. 이 설명은 컨트롤 세부 정보 페이지에 표시됩니다.
4. 테스트 정보에서 컨트롤 테스트를 위한 권장 단계를 입력합니다.
5. 태그에서 새 태그 추가를 선택하여 태그를 컨트롤에 연결합니다. 각 태그에 대해 이 컨트롤이 지원하는 규정 준수 프레임워크를 가장 잘 설명하는 태그 키를 지정할 수 있습니다. 태그 키는 필수이며 컨트롤 라이브러리에서 이 컨트롤을 검색할 때 검색 기준으로 사용할 수 있습니다.
6. 다음을 선택합니다.

2단계: 데이터 소스 설정

다음으로, 최대 10개의 데이터 소스를 정의합니다. 데이터 소스는 사용자 지정 컨트롤이 증거를 수집할 위치를 결정합니다.

자동 증거를 수집하려면 각 데이터 소스에 데이터 소스 유형과 데이터 소스 매핑이 포함되어야 합니다. 이러한 세부 정보는 AWS 사용 현황에 맞게 조정되며 Audit Manager에 어디서 증거를 수집해야 하는지 알려줍니다. 대신, 증거를 직접 제공하려면 데이터 소스의 이름을 지정한 다음, 수동 증거 옵션을 선택하면 됩니다.

> **Important**
>
> Security Hub를 자동화된 데이터 원본으로 성공적으로 사용하려면 AWS Config 다음을 수행해야 합니다.
>
> - AWS Config설정지침에 따라 Audit Manager와 함께 사용할 Security Hub를 설정합니다.
> - 평가에 Security Hub를 모두 AWS Config 서비스 범위에 포함시키십시오.

그러면 Audit Manager는 이 단계에서 지정한 AWS Config 규칙 또는 Security Hub 컨트롤이 평가될 때마다 증거를 수집할 수 있습니다.

데이터 소스를 설정하려면

1. 데이터 소스 이름에서 자리 표시자 텍스트를 데이터 소스를 설명하는 이름으로 바꿉니다.
2. 증거 수집 방법에서 이 컨트롤에 대한 증거를 수집할 방법을 선택합니다.

   a. Audit Manager에서 증거를 수집하도록 하려면 자동을 선택하고 다음 단계를 따릅니다.

      - 데이터 소스 유형에서 Audit Manager가 자동 증거를 수집할 위치를 지정합니다.
        - AWS CloudTrail의 경우, 드롭다운 목록에서 이벤트 이름 키워드를 선택합니다.
        - AWS Config의 경우, 규칙 유형을 선택한 다음, 드롭다운 목록에서 규칙 식별자 키워드를 선택합니다.
        - AWS Security Hub의 경우, 드롭다운 목록에서 Security Hub 컨트롤을 선택합니다.
        - AWS API 호출의 경우, API 호출을 선택한 다음, 증거 수집 빈도를 선택합니다.

      > **Tip**
      >
      > 각 데이터 소스 유형에 대한 개요 및 관련 문제 해결 팁은 자동 데이터 소스 개요 부분을 참조하세요.
      > 도메인 전문가와 함께 데이터 소스 구성을 검증해야 하는 경우, 일단 증거 수집 방법을 수동으로 설정하십시오. 이런 식으로, 지금 컨트롤을 만들어 프레임워크에 추가한 다음, 나중에 필요에 따라 컨트롤을 편집할 수 있습니다.

   b. 직접 증거를 제공하려면 수동을 선택하고 수동 증거 옵션 선택하세요.

      - 파일 업로드 - 컨트롤에서 증거로 문서를 요구하는 경우, 이 옵션을 선택하십시오.
      - 텍스트 응답 - 컨트롤에서 위험 평가 질문에 대한 답변을 요구하는 경우, 이 옵션을 선택합니다.
3. (선택 사항) 추가 세부 정보에서 데이터 소스 설명과 문제 해결 방법 설명을 입력합니다.
4. (선택 사항) 다른 소스를 추가하려면 데이터 소스 추가를 선택한 다음, 1~3 단계를 반복합니다.
5. (선택 사항) 데이터 소스를 제거하려면 데이터 소스 구성 상자 상단에서 제거를 선택합니다.
6. 마쳤으면, 다음을 선택합니다.

3단계(선택 사항): 실행 계획 정의

이어서, 이 컨트롤을 수정해야 할 경우, 취해야 할 조치를 지정합니다.

실행 계획을 정의하려면

1. 제목에서 실행 계획을 설명하는 제목을 입력합니다.
2. 실행 계획 지침에서 실행 계획에 대한 세부 지침을 입력합니다.
3. 다음을 선택합니다.

4단계: 컨트롤 검토 및 생성

컨트롤에 대한 정보를 검토합니다. 단계 정보를 변경하려면 편집을 선택합니다.

작업을 마쳤으면 사용자 지정 컨트롤 생성을 선택합니다.

다음으로 무엇을 할 수 있습니까?

새 사용자 지정 컨트롤을 만들었으면, 사용자 지정 프레임워크에 이를 추가할 수 있습니다. 자세한 내용은 사용자 지정 프레임워크 만들기 및 사용자 지정 프레임워크 편집 부분을 참조하세요.

사용자 지정 프레임워크에 사용자 지정 컨트롤을 추가하였으면, 해당 사용자 지정 프레임워크에서 평가를 만들고 증거 수집을 시작할 수 있습니다. 자세한 내용은 평가 생성를 참조하세요.

문제 해결 팁은 제어 및 제어 세트 문제 해결 섹션을 참조하세요.

기존 컨트롤에 대한 사용자 지정

사용자 지정 컨트롤을 처음부터 만드는 대신, 기존 컨트롤을 시작점으로 이용하여 필요에 따라 사용자 지정할 수 있습니다. 이렇게 하면, 기존 컨트롤은 컨트롤 라이브러리에 남아 있고, 사용자가 원하는 설정을 이용하여 새 사용자 지정 컨트롤이 만들어집니다.

기존 컨트롤을 선택하여 사용자 지정할 수 있습니다. 이는 표준 컨트롤 또는 사용자 지정 컨트롤일 수 있습니다.

> **Important**
>
> 컨트롤 세부 정보, 테스트 정보, 또는 실행 계획과 같은 자유 형식 필드에 중요 식별 정보를 절대 입력하지 않도록 강력히 권장합니다. 민감한 정보가 포함된 사용자 지정 컨트롤을 만드는 경우, 이러한 컨트롤이 포함된 사용자 지정 프레임워크는 공유할 수 없습니다.

주제

1단계: 컨트롤 세부 정보 지정

컨트롤 세부 정보는 원래 컨트롤에서 그대로 물려 받습니다. 필요에 따라 이러한 세부 정보를 검토하고 수정합니다.

컨트롤 세부 정보를 지정하려면

1. https://console.aws.amazon.com/auditmanager/home에서 AWS Audit Manager 콘솔을 엽니다.
2. 탐색 창에서 컨트롤 라이브러리를 선택합니다.
3. 사용자 지정하려는 컨트롤을 선택한 다음, 기존 컨트롤 사용자 지정을 선택합니다.
4. 컨트롤의 새 이름을 지정하고 사용자 지정을 선택합니다.
5. 컨트롤 세부 정보에서 필요에 따라 컨트롤 세부 정보를 사용자 지정합니다.
6. 테스트 정보에서 필요에 따라 테스트 정보를 사용자 지정합니다.
7. 태그에서 필요에 따라 태그를 사용자 지정합니다.
8. 다음을 선택합니다.

2단계: 데이터 소스 설정

데이터 소스는 원래의 콘트롤에서 그대로 묻려 받습니다. 필요에 따라 데이터 소스를 변경, 추가 또는 제거할 수 있습니다.

> **Important**
>
> Security Hub를 자동화된 데이터 원본으로 성공적으로 사용하려면 AWS Config 다음을 수행해야 합니다.
>
> - AWS Config설정지침에 따라 Audit Manager와 함께 사용할 Security Hub를 설정합니다.
> - 평가에 Security Hub를 모두 AWS Config 서비스 범위에 포함시키십시오.

그러면 Audit Manager는 이 단계에서 지정한 AWS Config 규칙 또는 Security Hub 컨트롤이 평가될 때마다 증거를 수집할 수 있습니다.

데이터 소스를 설정하려면

1. 데이터 소스 이름에서 필요에 따라 데이터 소스 이름을 사용자 지정합니다.
2. 증거 수집 방법에서 필요에 따라 선택 항목을 사용자 지정합니다.

   a. Audit Manager에서 증거를 수집하도록 하려면 자동을 선택하고 다음 단계를 따릅니다.

      - 데이터 소스 유형에서 Audit Manager가 자동화된 증거를 수집하는 위치를 검토하고 필요에 따라 수정합니다.
        - AWS CloudTrail의 경우, 드롭다운 목록에서 이벤트 이름 키워드를 선택합니다.
        - AWS Config의 경우, 규칙 유형을 선택한 다음, 드롭다운 목록에서 규칙 식별자 키워드를 선택합니다.
        - AWS Security Hub의 경우, 드롭다운 목록에서 Security Hub 컨트롤을 선택합니다.
        - AWS API 호출의 경우, API 호출을 선택한 다음, 증거 수집 빈도를 선택합니다.

      > **Tip**
      >
      > 각 데이터 소스 유형에 대한 개요 및 관련 문제 해결 팁은 자동 데이터 소스 개요 부분을 참조하세요.
      > 도메인 전문가와 함께 데이터 소스 구성을 검증해야 하는 경우, 일단 증거 수집 방법을 수동으로 설정하십시오. 이런 식으로, 지금 컨트롤을 만들어 프레임워크에 추가한 다음, 나중에 필요에 따라 컨트롤을 편집할 수 있습니다.

   b. 직접 증거를 제공하려면 수동을 선택하고 수동 증거 옵션 선택하세요.

      - 파일 업로드 - 컨트롤에서 증거로 문서를 요구하는 경우, 이 옵션을 선택하십시오.
      - 텍스트 응답 - 컨트롤에서 위험 평가 질문에 대한 답변을 요구하는 경우, 이 옵션을 선택합니다.

3. (선택 사항) 추가 세부 정보에서 데이터 소스 설명 또는 문제 해결 방법 설명을 필요에 따라 변경합니다.
4. (선택 사항) 다른 데이터 소스를 추가하려면 데이터 소스 추가를 선택합니다.

5. (선택 사항) 데이터 소스를 제거하려면 제거를 선택합니다.
6. 다음을 선택합니다.

3단계(선택 사항): 실행 계획 정의

실행 계획은 원래의 컨트롤에서 그대로 물려 받습니다. 필요에 따라 이 실행 계획을 편집할 수 있습니다.

실행 계획을 정의하려면

1. 제목에서 실행 계획의 제목을 검토하고 필요에 따라 사용자 지정합니다.
2. 실행 계획 지침에서 지침을 검토하고 필요에 따라 사용자 지정합니다.
3. 다음을 선택합니다.

4단계: 컨트롤 검토 및 생성

컨트롤에 대한 정보를 검토합니다. 단계 정보를 변경하려면 편집을 선택합니다. 작업을 마쳤으면 사용자 지정 컨트롤 생성을 선택합니다.

다음으로 무엇을 할 수 있습니까?

새 사용자 지정 컨트롤을 만들었으면, 사용자 지정 프레임워크에 이를 추가할 수 있습니다. 자세한 내용은 사용자 지정 프레임워크 만들기 및 사용자 지정 프레임워크 편집 부분을 참조하세요.

사용자 지정 프레임워크에 사용자 지정 컨트롤을 추가했으면, 해당 사용자 지정 프레임워크에서 평가를 만들고 증거 수집을 시작할 수 있습니다. 자세한 내용은 평가 생성를 참조하세요.

사용자 지정 컨트롤을 편집해야 하는 경우, 사용자 지정 컨트롤 편집 부분을 참조하세요.

문제 해결 팁은 제어 및 제어 세트 문제 해결 섹션을 참조하세요.

사용자 지정 컨트롤 편집

다음 단계에 따라 Audit Manager에서 사용자 지정 컨트롤을 편집할 수 있습니다.

주제

- 1단계: 컨트롤 세부 정보 편집
- 2단계: 데이터 소스 편집
- 3단계(선택 사항): 실행 계획 편집

- 4단계: 컨트롤 검토 및 업데이트

1단계: 컨트롤 세부 정보 편집

필요에 따라 컨트롤 세부 정보를 검토하고 편집하여 시작합니다.

컨트롤 세부 정보를 편집하려면

1. https://console.aws.amazon.com/auditmanager/home에서 AWS Audit Manager 콘솔을 엽니다.
2. 탐색 창에서 컨트롤 라이브러리를 선택한 다음, 사용자 지정 컨트롤 탭을 선택합니다.
3. 편집할 컨트롤을 선택하고 편집을 선택합니다.
4. 컨트롤 세부 정보에서 필요에 따라 컨트롤 세부 정보를 편집합니다.
5. 테스트 정보에서 필요에 따라 권장 테스트 정보를 편집합니다.
6. 다음을 선택합니다.

> **Tip**
>
> 컨트롤의 태그를 편집하려면 컨트롤을 열고 태그 탭을 선택합니다. 여기서 컨트롤과 연결된 태그를 보고 편집할 수 있습니다.

2단계: 데이터 소스 편집

이어서, 다음, 컨트롤의 데이터 소스를 편집, 제거 또는 추가할 수 있습니다.

> **Important**
>
> Security Hub를 자동화된 데이터 원본으로 성공적으로 사용하려면 AWS Config 다음을 수행해야 합니다.
>
> - AWS Config설정지침에 따라 Audit Manager와 함께 사용할 Security Hub를 설정합니다.
> - 평가에 Security Hub를 모두 AWS Config 서비스 범위에 포함시키십시오.
>
> 그러면 Audit Manager는 이 단계에서 지정한 AWS Config 규칙 또는 Security Hub 컨트롤이 평가될 때마다 증거를 수집할 수 있습니다.

데이터 소스를 편집하려면

1. 데이터 소스 이름에서 현재 이름을 검토하고 필요에 따라 편집합니다.
2. 증거 수집 방법에서 필요에 따라 현재 선택 항목을 검토하고 필요에 따라 편집합니다.

   a. Audit Manager에서 증거를 수집하도록 하려면 자동을 선택하고 다음 단계를 따릅니다.

      - 데이터 소스 유형에서 Audit Manager가 자동 증거를 수집할 위치를 검토하고 필요에 따라 편집합니다.
        - AWS CloudTrail의 경우, 드롭다운 목록에서 이벤트 이름 키워드를 선택합니다.
        - AWS Config의 경우, 규칙 유형을 선택한 다음, 드롭다운 목록에서 규칙 식별자 키워드를 선택합니다.
        - AWS Security Hub의 경우, 드롭다운 목록에서 Security Hub 컨트롤을 선택합니다.
        - AWS API 호출의 경우, API 호출을 선택한 다음, 증거 수집 빈도를 선택합니다.

      > **Tip**
      > 각 데이터 소스 유형에 대한 개요 및 관련 문제 해결 팁은 자동 데이터 소스 개요 부분을 참조하세요.

   b. 직접 증거를 제공하려면 수동을 선택하고 수동 증거 옵션 선택하세요.

      - 파일 업로드 - 컨트롤에서 증거로 문서를 요구하는 경우, 이 옵션을 선택하십시오.
      - 텍스트 응답 - 컨트롤에서 위험 평가 질문에 대한 답변을 요구하는 경우, 이 옵션을 선택합니다.
3. (선택 사항) 추가 세부 정보에서 데이터 소스 설명 또는 문제 해결 방법 설명을 필요에 따라 변경합니다.
4. (선택 사항) 다른 데이터 소스를 추가하려면 데이터 소스 추가를 선택합니다.
5. (선택 사항) 데이터 소스를 제거하려면 제거를 선택합니다.
6. 다음을 선택합니다.

3단계(선택 사항): 실행 계획 편집

다음으로, 선택사항인 실행 계획을 검토하고 편집합니다.

실행 계획을 편집하려면

1. 제목에서 필요에 따라 제목을 편집합니다.
2. 실행 계획 지침에서 필요에 따라 지침을 편집합니다.
3. 다음을 선택합니다.

4단계: 컨트롤 검토 및 업데이트

컨트롤에 대한 정보를 검토합니다. 단계 정보를 변경하려면 편집을 선택합니다.

작업을 마쳤으면 변경 내용 저장을 선택합니다.

> **Note**
>
> 컨트롤을 수정하면, 변경 사항은 컨트롤을 포함하는 활성화된 모든 평가에 다음과 같이 적용됩니다.
>
> - AWS API 직접 호출 데이터 소스 유형으로 사용하는 컨트롤의 경우, 변경 사항은 다음 날 00:00 UTC에 적용됩니다.
> - 다른 모든 컨트롤의 경우, 변경 사항이 즉시 적용됩니다.

사용자 지정 컨트롤 삭제

컨트롤 라이브러리를 이용하여 원하지 않는 사용자 지정 컨트롤을 삭제할 수 있습니다. 컨트롤을 삭제하면 컨트롤 라이브러리에 더 이상 표시되지 않습니다. Audit Manager API 또는 AWS Command Line Interface (AWS CLI) 를 사용하여 사용자 지정 제어를 삭제할 수도 있습니다.

> **Important**
>
> 사용자 지정 컨트롤을 삭제하면 현재 관련된 모든 사용자 지정 프레임워크 또는 평가에서 컨트롤이 제거됩니다. 그에 따라 Audit Manager는 모든 평가에서 해당 사용자 지정 컨트롤에 대한 증거 수집을 중단합니다. 여기에는 사용자 지정 컨트롤을 삭제하기 전에 만든 평가도 포함됩니다.

Audit Manager console

사용자 지정 컨트롤(콘솔)을 삭제하려면

1. https://console.aws.amazon.com/auditmanager/home에서 AWS Audit Manager 콘솔을 엽니다.
2. 탐색 창에서 컨트롤 라이브러리를 선택한 다음, 사용자 지정 컨트롤 탭을 선택합니다.
3. 삭제하려는 컨트롤을 선택한 다음, 삭제를 선택합니다.
4. 나타나는 팝업 창에서 삭제를 선택하여 삭제를 확인합니다.

AWS CLI

사용자 지정 컨트롤(AWS CLI)을 삭제하려면

1. 먼저, 삭제하려는 사용자 지정 컨트롤을 식별합니다. 그렇게 하려면 컨트롤 목록 표시 명령을 실행하고 `--control-type`의 유형을 `Custom`으로 지정합니다.

   ```
   aws auditmanager list-controls --control-type Custom
   ```

   그 응답으로 사용자 지정 컨트롤 목록을 볼 수 있습니다. 삭제할 컨트롤을 찾고 컨트롤 ID를 기록해 둡니다.
2. 그런 다음, 컨트롤 삭제 명령을 실행하고 `--control-id` 파라미터를 이용하여 삭제하려는 컨트롤을 지정합니다.

   다음 예에서는 각 *## ### ###*를 자신의 정보로 바꿉니다.

   ```
   aws auditmanager delete-control --control-id a1b2c3d4-5678-90ab-cdef-
   EXAMPLE11111
   ```

Audit Manager API

사용자 지정 컨트롤(API)을 삭제하려면

1. ListControls작업을 사용하고 컨트롤 유형을 로 지정합니다. `Custom` 응답에서 삭제하려는 컨트롤을 찾고 컨트롤 ID를 기록해 둡니다.
2. DeleteControl작업을 사용하여 사용자 지정 컨트롤을 삭제합니다. 이 요청에서, controlID 파라미터를 이용하여 삭제하려는 컨트롤을 지정합니다.

이러한 API 작업에 대한 자세한 내용은 이전 링크 중 하나를 선택하여 AWS Audit Manager API 참조에서 자세한 내용을 읽어보세요. 여기에는 언어별 AWS SDK 중 하나에서 이러한 작업 및 매개변수를 사용하는 방법에 대한 정보가 포함됩니다.

컨트롤의 증거 수집 빈도 변경

AWS Audit Manager 다양한 빈도로 여러 데이터 소스에서 증거를 수집합니다. 지원하는 증거 수집 빈도는 컨트롤을 위해 수집되는 증거의 유형에 따라 다릅니다.

- AWS API 직접 호출의 경우, Audit Manager는 다른 AWS 서비스에 대한 설명 API 직접 호출을 이용하여 증거를 수집합니다. Audit Manager에서 직접 증거 수집 빈도를 지정할 수 있습니다(사용자 지정 컨트롤에만 해당).
- 의 경우 AWS Config, Audit Manager는 규정 준수 점검 결과를 에서 직접 AWS Config보고합니다. 빈도는 AWS Config 규칙에 정의된 트리거를 따릅니다.
- AWS Security Hub의 경우, Audit Manager는 규정 준수 검사 결과를 Security Hub에서 직접 가져와 보고합니다. 빈도는 Security Hub 검사 일정을 따릅니다.
- 의 경우 AWS CloudTrail, Audit Manager는 에서 지속적으로 증거를 수집합니다 CloudTrail. 이 증거 유형의 경우 빈도를 변경할 수 없습니다.

다음 섹션에서는 각 컨트롤 데이터 소스 유형의 증거 수집 빈도와 이를 변경하는 방법(해당하는 경우)에 대한 자세한 정보를 제공합니다.

주제

- AWS API 호출을 통한 구성 스냅샷
- AWS Config에서 규정 준수 점검
- Security Hub에서의 규정 준수 검사
- AWS CloudTrail의 사용자 활동 로그

AWS API 호출을 통한 구성 스냅샷

> **Note**
>
> 다음은 사용자 지정 컨트롤에만 적용됩니다. API 직접 호출을 데이터 소스로 사용하는 표준 컨트롤의 경우 증거 수집 빈도를 변경할 수 없습니다.

사용자 지정 컨트롤에서 AWS API 호출을 데이터 소스 유형으로 사용하는 경우 다음 단계에 따라 Audit Manager에서 증거 수집 빈도를 변경할 수 있습니다.

API 직접 호출 데이터 소스를 사용하는 사용자 지정 컨트롤의 증거 수집 빈도를 변경하려면

1. https://console.aws.amazon.com/auditmanager/home에서 AWS Audit Manager 콘솔을 엽니다.
2. 탐색 창에서, 컨트롤 라이브러리를 선택한 다음, 사용자 지정 컨트롤 탭을 선택합니다.
3. 편집할 사용자 지정 컨트롤을 선택하고 편집을 선택합니다.
4. 컨트롤 세부 정보 편집 페이지에서 다음을 선택합니다.
5. 편집할 데이터 소스 상자를 찾고 다음 정보가 정확한지 확인합니다.
   - 증거 수집 방법은 자동입니다.
   - 데이터 소스 유형은 AWS API 직접 호출입니다.
   - 선택한 API 직접 호출이 빈도를 변경하고자 하는 API 직접 호출입니다.
6. 빈도에서 사용자 지정 컨트롤에 대한 증거를 수집할 빈도를 선택합니다.
7. 편집하고자 하는 모든 추가 API 직접 호출 데이터 소스에 대해 필요에 따라 5~6단계를 반복합니다.
8. 다음을 선택합니다.
9. 실행 계획 편집 페이지에서 다음을 선택합니다.
10. 컨트롤 검토 및 업데이트 페이지에서 사용자 지정 컨트롤에 대한 정보를 검토합니다. 단계 정보를 변경하려면 편집을 선택합니다.
11. 작업을 마쳤으면 변경 내용 저장을 선택합니다.

AWS API 직접 호출을 데이터 소스 유형으로 이용하여 컨트롤을 편집하면, 해당 컨트롤을 포함하는, 활성화된 모든 평가에 다음 날 00:00 UTC에 변경사항이 적용됩니다.

AWS Config에서 규정 준수 점검

> **Note**
>
> 다음은 AWS Config 규칙 을 데이터 소스로 사용하는 표준 컨트롤과 사용자 지정 컨트롤에 모두 적용됩니다.

컨트롤이 데이터 원본 AWS Config 유형으로 사용되는 경우 Audit Manager에서 직접 증거 수집 빈도를 변경할 수 없습니다. 이는 빈도가 AWS Config 규칙에 정의된 트리거를 따르기 때문입니다.

트리거에는 다음과 같은 두 가지 유형이 있습니다. AWS Config 규칙

1. 구성 변경 - 특정 유형의 리소스가 생성, 변경 또는 삭제될 때 규칙에 대한 평가를 AWS Config 실행합니다.
2. 주기적 - 선택한 빈도에 따라 규칙에 대한 평가를 AWS Config 실행합니다 (예: 24시간마다).

의 트리거에 대해 자세히 알아보려면 개발자 AWS Config 규칙안내서의 트리거 유형을 참조하십시오.AWS Config

관리 AWS Config 규칙방법에 대한 지침은 AWS Config 규칙 관리를 참조하십시오.

Security Hub에서의 규정 준수 검사

> **Note**
>
> 다음 내용은 Security Hub 검사를 데이터 소스로 사용하는 표준 컨트롤과 사용자 지정 컨트롤에 모두 적용됩니다.

컨트롤에서 Security Hub를 데이터 소스 유형으로 사용하는 경우에는 Audit Manager에서 직접 증거 수집 빈도를 변경할 수 없습니다. 이는 빈도가 Security Hub 검사 일정을 따르기 때문입니다.

- 주기적 검사는 가장 최근 실행 후 12시간 이내에 자동으로 실행됩니다. 이 주기성은 변경할 수 없습니다.
- 변경으로 트리거되는 검사는 연결된 리소스의 상태가 변경되면 실행됩니다. 리소스의 상태가 변경되지 않더라도 변경으로 트리거된 검사에 대해 업데이트되는 내용은 18시간마다 새로 고쳐집니다. 이를 통해 컨트롤이 여전히 활성화되어 있음을 알 수 있습니다. 일반적으로, Security Hub는 가능하다면 항상 변경에 따른 트리거 규칙을 사용합니다.

자세한 내용은 AWS Security Hub 사용 설명서의 보안 검사 실행 일정 부분을 참조하세요.

AWS CloudTrail의 사용자 활동 로그

> **Note**
>
> 다음 내용은 AWS CloudTrail 사용자 활동 로그를 데이터 소스로 사용하는 표준 컨트롤과 사용자 지정 컨트롤에 모두 적용됩니다.

의 활동 로그를 데이터 소스 유형으로 사용하는 컨트롤의 증거 수집 빈도는 변경할 수 없습니다. CloudTrail Audit Manager는 이러한 증거 유형을 지속적으로 수집합니다. CloudTrail 사용자 활동은 하루 중 언제라도 발생할 수 있으므로 빈도는 지속적입니다.

자동 증거를 위해 지원하는 컨트롤 데이터 소스

에서 AWS Audit Manager사용자 지정 컨트롤을 만들 때 다음 데이터 소스 유형에서 자동화된 증거를 수집하도록 컨트롤을 설정할 수 있습니다.

- AWS CloudTrail
- AWS Security Hub
- AWS Config
- AWS API 호출

다음 항목에서는 이러한 자동화된 데이터 원본 유형을 각각 요약하고 Audit Manager에서 지원하는 특정 AWS Security Hub 제어, AWS Config 규칙 및 AWS API 호출을 나열합니다.

주제

- 자동 데이터 소스 개요
- AWS Config 규칙 에서 지원됩니다. AWS Audit Manager
- AWS Security Hub 에서 지원하는 제어 AWS Audit Manager
- 에서 지원하는 API 호출 AWS Audit Manager
- AWS CloudTrail 에서 지원하는 이벤트 이름 AWS Audit Manager

자동 데이터 소스 개요

다음 표에서는 각 자동 데이터 소스 유형에 대한 개요를 제공합니다.

데이터 소스 유형	설명	증거 수집 빈도	이 데이터 소스 유형을 사용하려면	평가에서 이 컨트롤이 활성화 상태이면	관련 문제 해결 팁
AWS CloudTrail	특정 사용자 활동 추적	지속적	지원하는 이벤트 이름 목록에서 선택합니다.	Audit Manager는 선택한 키워드를 기반으로 CloudTrail 로그를 필터링합니다. 그 결과는 사용자 활동 증거로 가져옵니다.	나의 평가는 AWS CloudTrail으로부터 사용자 활동 증거를 수집하고 있지 않습니다.
AWS Config	의 조사 결과를 보고하여 리소스 보안 상태의 스냅샷을 AWS Config캡처합니다.	AWS Config 규칙에 정의된 트리거를 기반으로 합니다.	규칙 유형을 선택한 후, 규칙을 선택합니다. • 관리형 규칙의 경우, 지원하는 관리형 규칙 키워드 목록에서 선택합니다. • 사용자 지정 규칙의 경우, 이용 가능한 규칙 목록에서 선택합니다.	Audit Manager는 에서 직접 이 규칙에 대한 결과를 가져옵니다 AWS Config. 그 결과는 규정 준수 검사 증거로 가져옵니다.	나의 평가는 AWS Config으로부터 규정 준수 확인 증거를 수집하지 않

데이터 소스 유형	설명	증거 수집 빈도	이 데이터 소스 유형을 사용하려면	평가에서 이 컨트롤이 활성화 상태이면	관련 문제 해결 팁
					습니다. AWS Config 통합 문제
AWS Security Hub	Security Hub의 결과를 보고하여 리소스 보안 태세에 대한 스냅샷을 캡처합니다.	이는 Security Hub 검사 일정을 기준으로 합니다.	지원하는 Security Hub 컨트롤 ID 목록에서 선택합니다.	Audit Manager는 Security Hub에서 보안 검사 결과를 직접 가져옵니다. 그 결과는 규정 준수 검사 증거로 가져옵니다.	나의 평가는 AWS Security Hub으로부터 규정 준수 확인 증거를 수집하지 않습니다.

데이터 소스 유형	설명	증거 수집 빈도	이 데이터 소스 유형을 사용하려면	평가에서 이 컨트롤이 활성화 상태이면	관련 문제 해결 팁
AWS API 호출	지정된 항목에 대한 API 호출을 통해 리소스 구성의 스냅샷을 직접 생성합니다 AWS 서비스.	일별, 주별 또는 월별	지원하는 API 직접 호출 목록에서 선택한 다음, 원하는 빈도를 선택합니다.	Audit Manager는 지정한 빈도에 따라 API 직접 호출을 수행합니다. 그 응답은 구성 데이터 증거로 가져옵니다.	나의 평가에서는 AWS API 직접 호출에 대한 구성 데이터 증거를 수집하지 않습니다.

AWS Config 규칙 에서 지원됩니다. AWS Audit Manager

Audit Manager를 사용하여 AWS Config 평가를 감사 증거로 캡처할 수 있습니다. 사용자 지정 컨트롤을 만들거나 편집할 때 증거 수집을 위한 데이터 소스 매핑으로 하나 이상의 AWS Config 규칙을 지정할 수 있습니다. AWS Config 이러한 규칙에 따라 규정 준수 검사를 수행하고 Audit Manager는 결과를 규정 준수 점검 증거로 보고합니다.

관리형 규칙 외에도, 사용자 지정 규칙을 컨트롤 데이터 소스에 매핑할 수 있습니다.

Note

- Audit Manager는 서비스 연결 AWS Config 규칙에서 증거를 수집하지 않습니다. 단, Comformance Pack과 AWS Organizations의 서비스 연결 규칙은 예외입니다. 자세한 내용은 이 안내서의 문제 해결 부분을 참조하세요.
- Audit Manager는 사용자를 대신하여 AWS Config 규칙을 관리하지 않습니다. 증거 수집을 시작하기 전에 현재 AWS Config 규칙 매개변수를 검토하는 것이 좋습니다. 그런 다음, 선택한 프레임워크의 요구사항과 비교하여 해당 파라미터를 검증하십시오. 필요하다면, AWS Config에서 규칙 파라미터를 업데이트하여 프레임워크 요구사항에 맞출 수 있습니다. 이렇게 하면 평가 시 해당 프레임워크에 대한 정확한 규정 준수 검사 증거를 수집할 수 있습니다.

  예를 들어, CIS v1.2.0에 대한 평가를 생성한다고 가정해 보겠습니다. 이 프레임워크에는 1.9라는 컨트롤이 있습니다. IAM 암호 정책에 최소 길이 14 이상이 필요한지 확인하십시오. 에서 AWS Configiam-password-policy규칙에는 암호 길이를 확인하는 `MinimumPasswordLength` 매개변수가 있습니다. 이 파라미터의 기본값은 문자 14개입니다. 결과적으로, 규칙은 컨트롤 요구 사항에 맞게 조정됩니다. 기본 파라미터 값을 사용하지 않는 경우, 사용하는 값이 CIS v1.2.0의 14자 요구 사항과 같거나 더 큰지 확인하세요. AWS Config 설명서에서 각 관리형 규칙에 대한 기본 파라미터 세부 정보를 찾을 수 있습니다.

주제

Audit Manager에서 AWS Config 관리형 규칙 사용

현재 Audit Manager는 326개의 AWS Config 관리형 규칙을 지원합니다. 사용자 지정 컨트롤용 데이터 소스를 설정할 때는 다음과 같은 관리형 규칙 식별자 키워드를 사용할 수 있습니다. 아래 나열된 관리형 규칙에 대한 자세한 내용은 목록에서 항목을 선택하거나 AWS Config 사용 설명서의 AWS Config 관리형 규칙 부분을 참조하세요.

Tip

사용자 지정 컨트롤을 만들면서 Audit Manager 콘솔에서 관리형 규칙을 선택할 때는 규칙 이름이 아닌, 다음 규칙 식별자 키워드 중 하나를 찾아야 합니다. 규칙 이름과 규칙 식별자 간의

차이점과 관리형 규칙의 식별자를 찾는 방법에 대한 자세한 내용은 이 사용 설명서의 문제 해결 부분을 참조하세요.

지원되는 AWS Config 관리형 규칙 키워드

- ACCESS_KEYS_ROTATED
- ACCOUNT_PART_OF_ORGANIZATIONS
- ACM_CERTIFICATE_EXPIRATION_CHECK
- ACM_CERTIFICATE_RSA_CHECK
- ALB_DESYNC_MODE_CHECK
- ALB_HTTP_DROP_INVALID_HEADER_ENABLED
- ALB_HTTP_TO_HTTPS_REDIRECTION_CHECK
- ALB_WAF_ENABLED
- API_GW_ASSOCIATED_WITH_WAF
- API_GW_CACHE_ENABLED_AND_ENCRYPTED
- API_GW_ENDPOINT_TYPE_CHECK
- API_GW_EXECUTION_LOGGING_ENABLED
- API_GW_SSL_ENABLED
- API_GW_XRAY_ENABLED
- API_GWV2_ACCESS_LOGS_ENABLED
- API_GWV2_AUTHORIZATION_TYPE_CONFIGURED
- APPROVED_AMIS_BY_ID
- APPROVED_AMIS_BY_TAG
- APPSYNC_ASSOCIATED_WITH_WAF
- APPSYNC_CACHE_ENCRYPTION_AT_REST
- APPSYNC_LOGGING_ENABLED
- AURORA_LAST_BACKUP_RECOVERY_POINT_CREATED
- AURORA_MYSQL_BACKTRACKING_ENABLED
- AURORA_RESOURCES_PROTECTED_BY_BACKUP_PLAN
- AUTOSCALING_CAPACITY_REBALANCING

지원되는 AWS Config 관리형 규칙 키워드

- AUTOSCALING_GROUP_ELB_HEALTHCHECK_REQUIRED
- AUTOSCALING_LAUNCH_CONFIG_HOP_LIMIT
- AUTOSCALING_LAUNCH_CONFIG_PUBLIC_IP_DISABLED
- AUTOSCALING_LAUNCHCONFIG_REQUIRES_IMDSV2
- AUTOSCALING_LAUNCH_TEMPLATE
- AUTOSCALING_MULTIPLE_AZ
- AUTOSCALING_MULTIPLE_INSTANCE_TYPES
- BACKUP_PLAN_MIN_FREQUENCY_AND_MIN_RETENTION_CHECK
- BACKUP_RECOVERY_POINT_ENCRYPTED
- BACKUP_RECOVERY_POINT_MANUAL_DELETION_DISABLED
- BACKUP_RECOVERY_POINT_MINIMUM_RETENTION_CHECK
- BEANSTALK_ENHANCED_HEALTH_REPORTING_ENABLED
- CLB_DESYNC_MODE_CHECK
- CLB_MULTIPLE_AZ
- CLOUD_TRAIL_CLOUD_WATCH_LOGS_ENABLED
- CLOUD_TRAIL_ENABLED
- CLOUD_TRAIL_ENCRYPTION_ENABLED
- CLOUD_TRAIL_LOG_FILE_VALIDATION_ENABLED
- CLOUDFORMATION_STACK_DRIFT_DETECTION_CHECK
- CLOUDFORMATION_STACK_NOTIFICATION_CHECK
- CLOUDFRONT_ACCESSLOGS_ENABLED
- CLOUDFRONT_ASSOCIATED_WITH_WAF
- CLOUDFRONT_CUSTOM_SSL_CERTIFICATE
- CLOUDFRONT_DEFAULT_ROOT_OBJECT_CONFIGURED
- CLOUDFRONT_NO_DEPRECATED_SSL_PROTOCOLS
- CLOUDFRONT_ORIGIN_ACCESS_IDENTITY_ENABLED
- CLOUDFRONT_ORIGIN_FAILOVER_ENABLED
- CLOUDFRONT_S3_ORIGIN_ACCESS_CONTROL_ENABLED
- CLOUDFRONT_S3_ORIGIN_NON_EXISTENT_BUCKET

지원되는 AWS Config 관리형 규칙 키워드

- CLOUDFRONT_SECURITY_POLICY_CHECK
- CLOUDFRONT_SNI_ENABLED
- CLOUDFRONT_TRAFFIC_TO_ORIGIN_ENCRYPTED
- CLOUDFRONT_VIEWER_POLICY_HTTPS
- CLOUDTRAIL_S3_DATAEVENTS_ENABLED
- CLOUDTRAIL_SECURITY_TRAIL_ENABLED
- CLOUDWATCH_ALARM_ACTION_CHECK
- CLOUDWATCH_ALARM_ACTION_ENABLED_CHECK
- CLOUDWATCH_ALARM_RESOURCE_CHECK
- CLOUDWATCH_ALARM_SETTINGS_CHECK
- CLOUDWATCH_LOG_GROUP_ENCRYPTED
- CMK_BACKING_KEY_ROTATION_ENABLED
- CODEBUILD_PROJECT_ARTIFACT_ENCRYPTION
- CODEBUILD_PROJECT_ENVIRONMENT_PRIVILEGED_CHECK
- 코드빌드_프로젝트_환경_VAR_ AWSCRED_CHECK
- CODEBUILD_PROJECT_LOGGING_ENABLED
- CODEBUILD_PROJECT_S3_LOGS_ENCRYPTED
- CODEBUILD_PROJECT_SOURCE_REPO_URL_CHECK
- CODEDEPLOY_AUTO_ROLLBACK_MONITOR_ENABLED
- CODEDEPLOY_EC2_MINIMUM_HEALTHY_HOSTS_CONFIGURED
- CODEDEPLOY_LAMBDA_ALLATONCE_TRAFFIC_SHIFT_DISABLED
- CODEPIPELINE_DEPLOYMENT_COUNT_CHECK
- CODEPIPELINE_REGION_FANOUT_CHECK
- CUSTOM_SCHEMA_REGISTRY_POLICY_ATTACHED
- CW_LOGGROUP_RETENTION_PERIOD_CHECK
- DAX_ENCRYPTION_ENABLED
- DB_INSTANCE_BACKUP_ENABLED
- DESIRED_INSTANCE_TENANCY
- DESIRED_INSTANCE_TYPE

지원되는 AWS Config 관리형 규칙 키워드

- DMS_REPLICATION_NOT_PUBLIC
- DYNAMODB_AUTOSCALING_ENABLED
- DYNAMODB_IN_BACKUP_PLAN
- DYNAMODB_LAST_BACKUP_RECOVERY_POINT_CREATED
- DYNAMODB_PITR_ENABLED
- DYNAMODB_RESOURCES_PROTECTED_BY_BACKUP_PLAN
- DYNAMODB_TABLE_ENCRYPTED_KMS
- DYNAMODB_TABLE_ENCRYPTION_ENABLED
- DYNAMODB_THROUGHPUT_LIMIT_CHECK
- EBS_IN_BACKUP_PLAN
- EBS_LAST_BACKUP_RECOVERY_POINT_CREATED
- EBS_OPTIMIZED_INSTANCE
- EBS_RESOURCES_PROTECTED_BY_BACKUP_PLAN
- EBS_SNAPSHOT_PUBLIC_RESTORABLE_CHECK
- EC2_CLIENT_VPN_NOT_AUTHORIZE_ALL
- EC2_EBS_ENCRYPTION_BY_DEFAULT
- EC2_IMDSV2_CHECK
- EC2_INSTANCE_DETAILED_MONITORING_ENABLED
- EC2_INSTANCE_MANAGED_BY_SSM
- EC2_INSTANCE_MULTIPLE_ENI_CHECK
- EC2_INSTANCE_NO_PUBLIC_IP
- EC2_INSTANCE_PROFILE_ATTACHED
- EC2_LAST_BACKUP_RECOVERY_POINT_CREATED
- EC2_LAUNCH_TEMPLATE_PUBLIC_IP_DISABLED
- EC2_MANAGEDINSTANCE_APPLICATIONS_BLACKLISTED
- EC2_MANAGEDINSTANCE_APPLICATIONS_REQUIRED
- EC2_MANAGEDINSTANCE_ASSOCIATION_COMPLIANCE_STATUS_CHECK
- EC2_MANAGEDINSTANCE_INVENTORY_BLACKLISTED
- EC2_MANAGEDINSTANCE_PATCH_COMPLIANCE_STATUS_CHECK

지원되는 AWS Config 관리형 규칙 키워드

- EC2_MANAGEDINSTANCE_PLATFORM_CHECK
- EC2_NO_AMAZON_KEY_PAIR
- EC2_PARAVIRTUAL_INSTANCE_CHECK
- EC2_RESOURCES_PROTECTED_BY_BACKUP_PLAN
- EC2_SECURITY_GROUP_ATTACHED_TO_ENI
- EC2_SECURITY_GROUP_ATTACHED_TO_ENI_PERIODIC
- EC2_STOPPED_INSTANCE
- EC2_TOKEN_HOP_LIMIT_CHECK
- EC2_TRANSIT_GATEWAY_AUTO_VPC_ATTACH_DISABLED
- EC2_VOLUME_INUSE_CHECK
- ECR_PRIVATE_IMAGE_SCANNING_ENABLED
- ECR_PRIVATE_LIFECYCLE_POLICY_CONFIGURED
- ECR_PRIVATE_TAG_IMMUTABILITY_ENABLED
- ECS_ _활성화됨 AWSVPC_NETWORKING
- ECS_CONTAINER_INSIGHTS_ENABLED
- ECS_CONTAINERS_NONPRIVILEGED
- ECS_CONTAINERS_READONLY_ACCESS
- ECS_FARGATE_LATEST_PLATFORM_VERSION
- ECS_NO_ENVIRONMENT_SECRETS
- ECS_TASK_DEFINITION_LOG_CONFIGURATION
- ECS_TASK_DEFINITION_MEMORY_HARD_LIMIT
- ECS_TASK_DEFINITION_NONROOT_USER
- ECS_TASK_DEFINITION_PID_MODE_CHECK
- ECS_TASK_DEFINITION_USER_FOR_HOST_MODE_CHECK
- EFS_ACCESS_POINT_ENFORCE_ROOT_DIRECTORY
- EFS_ACCESS_POINT_ENFORCE_USER_IDENTITY
- EFS_ENCRYPTED_CHECK
- EFS_IN_BACKUP_PLAN
- EFS_LAST_BACKUP_RECOVERY_POINT_CREATED

지원되는 AWS Config 관리형 규칙 키워드

- EFS_RESOURCES_PROTECTED_BY_BACKUP_PLAN
- EIP_ATTACHED
- EKS_CLUSTER_LOGGING_ENABLED
- EKS_CLUSTER_OLDEST_SUPPORTED_VERSION
- EKS_CLUSTER_SUPPORTED_VERSION
- EKS_ENDPOINT_NO_PUBLIC_ACCESS
- EKS_SECRETS_ENCRYPTED
- ELASTIC_BEANSTALK_LOGS_TO_CLOUDWATCH
- ELASTIC_BEANSTALK_MANAGED_UPDATES_ENABLED
- ELASTICACHE_AUTO_MINOR_VERSION_UPGRADE_CHECK
- ELASTICACHE_RBAC_AUTH_ENABLED
- ELASTICACHE_REDIS_CLUSTER_AUTOMATIC_BACKUP_CHECK
- ELASTICACHE_REPL_GRP_AUTO_FAILOVER_ENABLED
- ELASTICACHE_REPL_GRP_ENCRYPTED_AT_REST
- ELASTICACHE_REPL_GRP_ENCRYPTED_IN_TRANSIT
- ELASTICACHE_REPL_GRP_REDIS_AUTH_ENABLED
- ELASTICACHE_SUBNET_GROUP_CHECK
- ELASTICACHE_SUPPORTED_ENGINE_VERSION
- ELASTICSEARCH_ENCRYPTED_AT_REST
- ELASTICSEARCH_IN_VPC_ONLY
- ELASTICSEARCH_LOGS_TO_CLOUDWATCH
- ELASTICSEARCH_NODE_TO_NODE_ENCRYPTION_CHECK
- ELB_ACM_CERTIFICATE_REQUIRED
- ELB_CROSS_ZONE_LOAD_BALANCING_ENABLED
- ELB_CUSTOM_SECURITY_POLICY_SSL_CHECK
- ELB_DELETION_PROTECTION_ENABLED
- ELB_LOGGING_ENABLED
- ELB_PREDEFINED_SECURITY_POLICY_SSL_CHECK
- ELB_TLS_HTTPS_LISTENERS_ONLY

지원되는 AWS Config 관리형 규칙 키워드

- ELBV2_ACM_CERTIFICATE_REQUIRED
- ELBV2_MULTIPLE_AZ
- EMR_KERBEROS_ENABLED
- EMR_MASTER_NO_PUBLIC_IP
- ENCRYPTED_VOLUMES
- FMS_SHIELD_RESOURCE_POLICY_CHECK
- FMS_WEBACL_RESOURCE_POLICY_CHECK
- FMS_WEBACL_RULEGROUP_ASSOCIATION_CHECK
- FSX_LAST_BACKUP_RECOVERY_POINT_CREATED
- FSX_RESOURCES_PROTECTED_BY_BACKUP_PLAN
- GUARDDUTY_ENABLED_CENTRALIZED
- GUARDDUTY_NON_ARCHIVED_FINDINGS
- IAM_CUSTOMER_POLICY_BLOCKED_KMS_ACTIONS
- IAM_GROUP_HAS_USERS_CHECK
- IAM_INLINE_POLICY_BLOCKED_KMS_ACTIONS
- IAM_NO_INLINE_POLICY_CHECK
- IAM_PASSWORD_POLICY
- IAM_POLICY_BLACKLISTED_CHECK
- IAM_POLICY_IN_USE
- IAM_POLICY_NO_STATEMENTS_WITH_ADMIN_ACCESS
- IAM_POLICY_NO_STATEMENTS_WITH_FULL_ACCESS
- IAM_ROLE_MANAGED_POLICY_CHECK
- IAM_ROOT_ACCESS_KEY_CHECK
- IAM_USER_GROUP_MEMBERSHIP_CHECK
- IAM_USER_MFA_ENABLED
- IAM_USER_NO_POLICIES_CHECK
- IAM_USER_UNUSED_CREDENTIALS_CHECK
- INCOMING_SSH_DISABLED
- INSTANCES_IN_VPC

지원되는 AWS Config 관리형 규칙 키워드

- KINESIS_STREAM_ENCRYPTED
- INTERNET_GATEWAY_AUTHORIZED_VPC_ONLY
- KMS_CMK_NOT_SCHEDULED_FOR_DELETION
- LAMBDA_CONCURRENCY_CHECK
- LAMBDA_DLQ_CHECK
- LAMBDA_FUNCTION_PUBLIC_ACCESS_PROHIBITED
- LAMBDA_FUNCTION_SETTINGS_CHECK
- LAMBDA_INSIDE_VPC
- LAMBDA_VPC_MULTI_AZ_CHECK
- MACIE_STATUS_CHECK
- MFA_ENABLED_FOR_IAM_CONSOLE_ACCESS
- MQ_AUTOMATIC_MINOR_VERSION_UPGRADE_ENABLED
- MQ_CLOUDWATCH_AUDIT_LOGGING_ENABLED
- MQ_NO_PUBLIC_ACCESS
- MULTI_REGION_CLOUD_TRAIL_ENABLED
- NACL_NO_UNRESTRICTED_SSH_RDP
- NETFW_LOGGING_ENABLED
- NETFW_MULTI_AZ_ENABLED
- NETFW_POLICY_DEFAULT_ACTION_FRAGMENT_PACKETS
- NETFW_POLICY_DEFAULT_ACTION_FULL_PACKETS
- NETFW_POLICY_RULE_GROUP_ASSOCIATED
- NETFW_STATELESS_RULE_GROUP_NOT_EMPTY
- NLB_CROSS_ZONE_LOAD_BALANCING_ENABLED
- NO_UNRESTRICTED_ROUTE_TO_IGW
- OPENSEARCH_ACCESS_CONTROL_ENABLED
- OPENSEARCH_AUDIT_LOGGING_ENABLED
- OPENSEARCH_DATA_NODE_FAULT_TOLERANCE
- OPENSEARCH_ENCRYPTED_AT_REST
- OPENSEARCH_HTTPS_REQUIRED

지원되는 AWS Config 관리형 규칙 키워드

- OPENSEARCH_IN_VPC_ONLY
- OPENSEARCH_LOGS_TO_CLOUDWATCH
- OPENSEARCH_NODE_TO_NODE_ENCRYPTION_CHECK
- RDS_AUTOMATIC_MINOR_VERSION_UPGRADE_ENABLED
- RDS_CLUSTER_DEFAULT_ADMIN_CHECK
- RDS_CLUSTER_DELETION_PROTECTION_ENABLED
- RDS_CLUSTER_IAM_AUTHENTICATION_ENABLED
- RDS_CLUSTER_MULTI_AZ_ENABLED
- RDS_DB_SECURITY_GROUP_NOT_ALLOWED
- RDS_ENHANCED_MONITORING_ENABLED
- RDS_IN_BACKUP_PLAN
- RDS_INSTANCE_DEFAULT_ADMIN_CHECK
- RDS_INSTANCE_DELETION_PROTECTION_ENABLED
- RDS_INSTANCE_IAM_AUTHENTICATION_ENABLED
- RDS_INSTANCE_PUBLIC_ACCESS_CHECK
- RDS_LAST_BACKUP_RECOVERY_POINT_CREATED
- RDS_LOGGING_ENABLED
- RDS_MULTI_AZ_SUPPORT
- RDS_RESOURCES_PROTECTED_BY_BACKUP_PLAN
- RDS_SNAPSHOT_ENCRYPTED
- RDS_SNAPSHOTS_PUBLIC_PROHIBITED
- RDS_STORAGE_ENCRYPTED
- REDSHIFT_BACKUP_ENABLED
- REDSHIFT_REQUIRE_TLS_SSL
- REDSHIFT_CLUSTER_CONFIGURATION_CHECK
- REDSHIFT_CLUSTER_MAINTENANCESETTINGS_CHECK
- REDSHIFT_CLUSTER_PUBLIC_ACCESS_CHECK
- REDSHIFT_AUDIT_LOGGING_ENABLED
- REDSHIFT_CLUSTER_KMS_ENABLED

지원되는 AWS Config 관리형 규칙 키워드

- REDSHIFT_DEFAULT_ADMIN_CHECK
- REDSHIFT_DEFAULT_DB_NAME_CHECK
- REDSHIFT_ENHANCED_VPC_ROUTING_ENABLED
- REQUIRED_TAGS
- RESTRICTED_INCOMING_TRAFFIC
- ROOT_ACCOUNT_HARDWARE_MFA_ENABLED
- ROOT_ACCOUNT_MFA_ENABLED
- S3_ACCOUNT_LEVEL_PUBLIC_ACCESS_BLOCKS_PERIODIC
- S3_ACCOUNT_LEVEL_PUBLIC_ACCESS_BLOCKS
- S3_BUCKET_ACL_PROHIBITED
- S3_BUCKET_BLACKLISTED_ACTIONS_PROHIBITED
- S3_BUCKET_DEFAULT_LOCK_ENABLED
- S3_BUCKET_LEVEL_PUBLIC_ACCESS_PROHIBITED
- S3_BUCKET_LOGGING_ENABLED
- S3_BUCKET_POLICY_GRANTEE_CHECK
- S3_BUCKET_POLICY_NOT_MORE_PERMISSIVE
- S3_BUCKET_PUBLIC_READ_PROHIBITED
- S3_BUCKET_PUBLIC_WRITE_PROHIBITED
- S3_BUCKET_REPLICATION_ENABLED
- S3_BUCKET_SERVER_SIDE_ENCRYPTION_ENABLED
- S3_BUCKET_SSL_REQUESTS_ONLY
- S3_BUCKET_VERSIONING_ENABLED
- S3_DEFAULT_ENCRYPTION_KMS
- S3_EVENT_NOTIFICATIONS_ENABLED
- S3_LAST_BACKUP_RECOVERY_POINT_CREATED
- S3_LIFECYCLE_POLICY_CHECK
- S3_RESOURCES_PROTECTED_BY_BACKUP_PLAN
- S3_VERSION_LIFECYCLE_POLICY_CHECK
- SAGEMAKER_ENDPOINT_CONFIGURATION_KMS_KEY_CONFIGURED

지원되는 AWS Config 관리형 규칙 키워드

- SAGEMAKER_NOTEBOOK_INSTANCE_INSIDE_VPC
- SAGEMAKER_NOTEBOOK_INSTANCE_KMS_KEY_CONFIGURED
- SAGEMAKER_NOTEBOOK_INSTANCE_ROOT_ACCESS_CHECK
- SAGEMAKER_NOTEBOOK_NO_DIRECT_INTERNET_ACCESS
- SECRETSMANAGER_ROTATION_ENABLED_CHECK
- SECRETSMANAGER_SCHEDULED_ROTATION_SUCCESS_CHECK
- SECRETSMANAGER_SECRET_PERIODIC_ROTATION
- SECRETSMANAGER_SECRET_UNUSED
- SECRETSMANAGER_USING_CMK
- SECURITY_ACCOUNT_INFORMATION_PROVIDED
- SECURITYHUB_ENABLED
- SERVICE_VPC_ENDPOINT_ENABLED
- SES_MALWARE_SCANNING_ENABLED
- SHIELD_ADVANCED_ENABLED_AUTORENEW
- SHIELD_DRT_ACCESS
- SNS_ENCRYPTED_KMS
- SNS_TOPIC_MESSAGE_DELIVERY_NOTIFICATION_ENABLED
- SSM_DOCUMENT_NOT_PUBLIC
- STEP_FUNCTIONS_STATE_MACHINE_LOGGING_ENABLED
- STORAGEGATEWAY_LAST_BACKUP_RECOVERY_POINT_CREATED
- STORAGEGATEWAY_RESOURCES_PROTECTED_BY_BACKUP_PLAN
- SUBNET_AUTO_ASSIGN_PUBLIC_IP_DISABLED
- VIRTUALMACHINE_LAST_BACKUP_RECOVERY_POINT_CREATED
- VIRTUALMACHINE_RESOURCES_PROTECTED_BY_BACKUP_PLAN
- VPC_DEFAULT_SECURITY_GROUP_CLOSED
- VPC_FLOW_LOGS_ENABLED
- VPC_NETWORK_ACL_UNUSED_CHECK
- VPC_PEERING_DNS_RESOLUTION_CHECK
- VPC_SG_OPEN_ONLY_TO_AUTHORIZED_PORTS

지원되는 AWS Config 관리형 규칙 키워드

- VPC_VPN_2_TUNNELS_UP
- WAF_CLASSIC_LOGGING_ENABLED
- WAF_GLOBAL_RULEGROUP_NOT_EMPTY
- WAF_GLOBAL_RULE_NOT_EMPTY
- WAF_GLOBAL_WEBACL_NOT_EMPTY
- WAF_REGIONAL_RULEGROUP_NOT_EMPTY
- WAF_REGIONAL_RULE_NOT_EMPTY
- WAF_REGIONAL_WEBACL_NOT_EMPTY
- WAFV2_LOGGING_ENABLED
- WAFV2_RULEGROUP_NOT_EMPTY
- WAFV2_WEBACL_NOT_EMPTY

Audit Manager에서 AWS Config 사용자 지정 규칙 사용

이제 AWS Config 사용자 지정 규칙을 감사 보고의 데이터 소스로 사용할 수 있습니다. 컨트롤에 AWS Config 규칙에 매핑된 데이터 원본이 있는 경우 Audit Manager는 AWS Config 규칙에 의해 생성된 평가를 추가합니다.

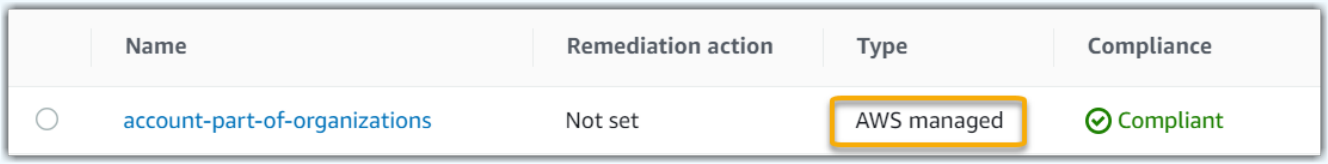
사용할 수 있는 사용자 지정 규칙은 Audit Manager에 AWS 계정 로그인하는 규칙에 따라 달라집니다. 에서 사용자 지정 규칙에 액세스할 수 있는 경우 Audit Manager에서 AWS Config해당 규칙을 데이터 소스 매핑으로 사용할 수 있습니다.

- 개인용 AWS 계정 — 계정으로 만든 모든 사용자 지정 규칙을 사용할 수 있습니다.
- 조직 계정의 경우 - 구성원 수준의 사용자 지정 규칙을 사용하거나, AWS Config에서 이용할 수 있는 조직 수준의 사용자 지정 규칙을 모두 사용할 수 있습니다.

사용자 지정 규칙을 데이터 소스로 사용하는 컨트롤을 만드는 방법에 대한 지침은 처음부터 새 컨트롤 만들기 및 기존 컨트롤 사용자 지정 부분을 참조하세요.

> **Tip**
>
> 관리형 규칙은 Audit Manager의 사용자 지정 규칙 드롭다운 목록에 표시되지 않는다는 점에 유의하세요.

규칙이 관리형 AWS Config 규칙인지 사용자 지정 규칙인지 확인하려면 AWS Config 콘솔을 사용하여 확인할 수 있습니다. 왼쪽 탐색 메뉴에서 규칙을 선택하고 테이블에서 규칙을 찾습니다. 관리형 규칙인 경우, 유형 열에 AWS 관리형이 표시됩니다.



관리 규칙을 데이터 소스로 매핑하려면 관리 규칙의 Audit Manager의 관리형 규칙 드롭다운 목록에서 규칙 식별자 키워드를 찾을 수 있습니다. 자세한 내용은 이 안내서의 문제 해결 부분을 참조하세요.

사용자 지정 규칙을 컨트롤의 데이터 소스로 매핑한 후, Audit Manager에서 해당 컨트롤을 사용자 지정 프레임워크에 연결할 수 있습니다. 사용자 지정 컨트롤을 사용하는 사용자 지정 프레임워크를 만드는 방법에 대한 지침은 처음부터 새 프레임워크 만들기 및 기존 프레임워크 사용자 지정 부분을 참조하세요. 기존 사용자 지정 프레임워크에 컨트롤을 추가하는 방법에 대한 지침은 기존 프레임워크 편집 부분을 참조하세요.

에서 AWS Config사용자 지정 규칙을 만드는 방법에 대한 자세한 내용은 AWS Config 개발자 안내서의 사용자 지정 규칙 개발을 참조하십시오. AWS Config

Audit Manager와의 AWS Config 통합 문제 해결

일반적인 질문 및 문제에 대한 답변을 찾으려면 이 안내서의 문제 해결 섹션에 있는 AWS Config 통합 부분을 참조하세요.

AWS Security Hub 에서 지원하는 제어 AWS Audit Manager

Audit Manager에 의하면 규정 준수 검사 결과를 Security Hub에서 직접 가져와 보고할 수 있습니다. 그렇게 하려면, Audit Manager에서 사용자 지정 컨트롤을 구성할 때 하나 이상의 Security Hub 컨트롤을 데이터 소스 매핑으로 지정합니다.

> **Note**
>
> - Audit Manager는 Security Hub에서 만든 서비스 연결 AWS Config 규칙에서 증거를 수집하지 않습니다. 자세한 내용은 이 안내서의 문제 해결 부분을 참조하세요.

- 2022년 11월 9일, Security Hub는 인터넷 보안 센터 (CIS) AWS 재단 벤치마크 버전 1.4.0 요구 사항, 레벨 1 및 2 (CIS v1.4.0) 에 따라 자동 보안 검사를 시작했습니다. Security Hub에서는 CIS v1.2.0 표준 외에도 CIS v1.4.0 표준이 지원됩니다.

주제

- Audit Manager에서의 Security Hub 컨트롤 사용
- 지원하는 Security Hub 컨트롤

Audit Manager에서의 Security Hub 컨트롤 사용

> **Tip**
>
> Security Hub의 컨트롤 결과 통합 설정이 아직 설정되어 있지 않은 경우, 해당 설정을 켜는 것이 좋습니다. 2003년 2월 23일 또는 그 이후에 Security Hub를 활성화한 경우, 기본적으로 이 설정이 켜집니다.

결과 통합이 활성화되면, Security Hub는 각 보안 검사에 대해 단일 결과를 생성합니다(동일한 검사가 여러 표준에 적용되는 경우에도 그러함). 각 Security Hub 검사 결과는 Audit Manager에서 하나의 고유한 리소스 평가로 수집됩니다. 결과적으로 통합된 조사 결과를 사용하면 Audit Manager가 Security Hub 조사 결과에 대해 수행하는 총 고유 리소스 평가 건수가 줄어듭니다. 이러한 이유로, 통합된 결과를 이용하면 증거의 품질과 가용성에 영향을 주지 않으면서 Audit Manager 사용 비용을 줄일 수 있는 경우가 많습니다. 요금에 대한 자세한 내용은 AWS Audit Manager 요금 부분을 참조하세요.

검사 결과 통합 기능을 켜거나 끌 때 나타나는 증거의 예

다음 예는 Security Hub 설정에 따라 Audit Manager가 증거를 수집하고 제시하는 방법을 비교한 것입니다.

When consolidated findings is turned on

Security Hub에서 AWS FSBP, PCI DSS, CIS 벤치마크 v1.2.0이라는 세 가지 보안 표준을 활성화했다고 가정해 보겠습니다.

- 이 세 가지 표준 모두 동일한 기본 규칙 (-check) 과 함께 동일한 제어 (IAM.4) 를 사용합니다. AWS Config iam-root-access-key

- 컨트롤 결과 통합 설정이 켜져 있으면 Security Hub는 이 컨트롤에 대해 단일 결과를 생성합니다.
- Security Hub는 이 컨트롤에 대한 통합 결과를 Audit Manager에 전송합니다.
- Audit Manager에서는 통합 결과를 하나의 고유한 리소스 평가로 간주됩니다. 결과적으로, 평가에 단일 증거가 추가됩니다.

다음은 이러한 증거가 어떻게 나타나는지를 보여주는 예입니다.


```
{
    "SchemaVersion": "2018-10-08",
    "Id": "arn:aws:securityhub:us-west-2:111122223333:security-control/IAM.4/
finding/09876543-p0o9-i8u7-y6t5-098765432109",
    "ProductArn": "arn:aws:securityhub:us-west-2::product/aws/securityhub",
    "ProductName": "Security Hub",
    "CompanyName": "AWS",
    "Region": "us-west-2",
    "GeneratorId": "security-control/IAM.4",
    "AwsAccountId": "111122223333",
    "Types": [
        "Software and Configuration Checks/Industry and Regulatory Standards"
    ],
    "FirstObservedAt": "2023-10-25T11:32:24.861Z",
    "LastObservedAt": "2023-11-02T11:59:19.546Z",
    "CreatedAt": "2023-10-25T11:32:24.861Z",
    "UpdatedAt": "2023-11-02T11:59:15.127Z",
    "Severity": {
        "Label": "INFORMATIONAL",
        "Normalized": 0,
        "Original": "INFORMATIONAL"
    },
    "Title": "IAM root user access key should not exist",
    "Description": "This AWS control checks whether the root user access key is
 available.",
    "Remediation": {
        "Recommendation": {
            "Text": "For information on how to correct this issue, consult the AWS
 Security Hub controls documentation.",
            "Url": "https://docs.aws.amazon.com/console/securityhub/IAM.4/
remediation"
        }
    },
    "ProductFields": {
```

```
        "RelatedAWSResources:0/name": "securityhub-iam-root-access-key-
check-000270f5",
        "RelatedAWSResources:0/type": "AWS::Config::ConfigRule",
        "aws/securityhub/ProductName": "Security Hub",
        "aws/securityhub/CompanyName": "AWS",
        "Resources:0/Id": "arn:aws:iam::111122223333:root",
        "aws/securityhub/FindingId": "arn:aws:securityhub:us-west-2::product/aws/
securityhub/arn:aws:securityhub:us-west-2:111122223333:security-control/IAM.4/
finding/09876543-p0o9-i8u7-y6t5-098765432109"
    },
    "Resources": [{
        "Type": "AwsAccount",
        "Id": "AWS::::Account:111122223333",
        "Partition": "aws",
        "Region": "us-west-2"
    }],
    "Compliance": {
        "Status": "PASSED",
        "RelatedRequirements": [
            "CIS AWS Foundations Benchmark v1.2.0/1.12"
        ],
        "SecurityControlId": "IAM.4",
        "AssociatedStandards": [{
                "StandardsId": "ruleset/cis-aws-foundations-benchmark/v/1.2.0"
            },
            {
                "StandardsId": "standards/aws-foundational-security-best-practices/
v/1.0.0"
            }
        ]
    },
    "WorkflowState": "NEW",
    "Workflow": {
        "Status": "RESOLVED"
    },
    "RecordState": "ACTIVE",
    "FindingProviderFields": {
        "Severity": {
            "Label": "INFORMATIONAL",
            "Original": "INFORMATIONAL"
        },
        "Types": [
            "Software and Configuration Checks/Industry and Regulatory Standards"
        ]
```

```
    },
    "ProcessedAt": "2023-11-02T11:59:20.980Z"
}
```

When consolidated findings is turned off

Security Hub에서 AWS FSBP, PCI DSS, CIS 벤치마크 v1.2.0이라는 세 가지 보안 표준을 활성화했다고 가정해 보겠습니다.

- 이 세 가지 표준 모두 동일한 기본 규칙 (-check) 과 함께 동일한 제어 (IAM.4) 를 사용합니다. AWS Config iam-root-access-key
- 검색 결과 통합 설정이 해제되어 있으면 Security Hub는 활성화된 각 표준에 대해 보안 검사별로 별개의 검사 결과(이 경우, 3개의 검사 결과)를 생성합니다.
- Security Hub는 이 컨트롤에 대해 각기 별개의 표준별 검사 결과 세 가지를 Audit Manager에 보냅니다.
- Audit Manager에서는 3개의 통합 결과를 3개의 고유한 리소스 평가로 간주합니다. 결과적으로, 평가에 3개의 개별 증거가 추가됩니다.

다음은 이러한 증거가 어떻게 나타나는지를 보여주는 예입니다. 이 예제에서, 다음 3가지 페이로드는 각각 동일한 보안 컨트롤 ID(*SecurityControlId":"IAM.4"*)를 가진다는 점에 유념하십시오. 이러한 이유로, Audit Manager(IAM.4)에서 이 증거를 수집하는 평가 컨트롤은 Security Hub에서 다음과 같은 결과가 들어오면 각기 별개의 세 가지 증거를 받습니다.

IAM.4(FSBP)에 대한 증거

```
{
  "version":"0",
  "id":"12345678-1q2w-3e4r-5t6y-123456789012",
  "detail-type":"Security Hub Findings - Imported",
  "source":"aws.securityhub",
  "account":"111122223333",
  "time":"2023-10-27T18:55:59Z",
  "region":"us-west-2",
  "resources":[
     "arn:aws:securityhub:us-west-2::product/aws/securityhub/arn:aws:securityhub:us-
west-2:111122223333:subscription/aws-foundational-security-best-practices/v/1.0.0/
Lambda.1/finding/b5e68d5d-43c3-46c8-902d-51cb0d4da568"
  ],
  "detail":{
     "findings":[
```

```
        {
           "SchemaVersion":"2018-10-08",
           "Id":"arn:aws:securityhub:us-west-2:111122223333:subscription/aws-
foundational-security-best-practices/v/1.0.0/IAM.4/finding/8e2e05a2-4d50-4c2e-
a78f-3cbe9402d17d",
           "ProductArn":"arn:aws:securityhub:us-west-2::product/aws/securityhub",
           "ProductName":"Security Hub",
           "CompanyName":"AWS",
           "Region":"us-west-2",
           "GeneratorId":"aws-foundational-security-best-practices/v/1.0.0/IAM.4",
           "AwsAccountId":"111122223333",
           "Types":[
              "Software and Configuration Checks/Industry and Regulatory Standards/
AWS-Foundational-Security-Best-Practices"
           ],
           "FirstObservedAt":"2020-10-05T19:18:47.848Z",
           "LastObservedAt":"2023-11-01T14:12:04.106Z",
           "CreatedAt":"2020-10-05T19:18:47.848Z",
           "UpdatedAt":"2023-11-01T14:11:53.720Z",
           "Severity":{
              "Product":0,
              "Label":"INFORMATIONAL",
              "Normalized":0,
              "Original":"INFORMATIONAL"
           },
           "Title":"IAM.4 IAM root user access key should not exist",
           "Description":"This AWS control checks whether the root user access key
 is available.",
           "Remediation":{
              "Recommendation":{
                 "Text":"For information on how to correct this issue, consult the
 AWS Security Hub controls documentation.",
                 "Url":"https://docs.aws.amazon.com/console/securityhub/IAM.4/
remediation"
              }
           },
           "ProductFields":{
              "StandardsArn":"arn:aws:securityhub:::standards/aws-foundational-
security-best-practices/v/1.0.0",
              "StandardsSubscriptionArn":"arn:aws:securityhub:us-
west-2:111122223333:subscription/aws-foundational-security-best-practices/v/1.0.0",
              "ControlId":"IAM.4",
              "RecommendationUrl":"https://docs.aws.amazon.com/console/securityhub/
IAM.4/remediation",
```

```
              "RelatedAWSResources:0/name":"securityhub-iam-root-access-key-
check-67cbb1c4",
              "RelatedAWSResources:0/type":"AWS::Config::ConfigRule",
              "StandardsControlArn":"arn:aws:securityhub:us-
west-2:111122223333:control/aws-foundational-security-best-practices/v/1.0.0/IAM.4",
              "aws/securityhub/ProductName":"Security Hub",
              "aws/securityhub/CompanyName":"AWS",
              "Resources:0/Id":"arn:aws:iam::111122223333:root",
              "aws/securityhub/FindingId":"arn:aws:securityhub:us-west-2::product/
aws/securityhub/arn:aws:securityhub:us-west-2:111122223333:subscription/aws-
foundational-security-best-practices/v/1.0.0/IAM.4/finding/8e2e05a2-4d50-4c2e-
a78f-3cbe9402d17d"
           },
           "Resources":[
              {
                 "Type":"AwsAccount",
                 "Id":"AWS::::Account:111122223333",
                 "Partition":"aws",
                 "Region":"us-west-2"
              }
           ],
           "Compliance":{
              "Status":"PASSED",
              "SecurityControlId":"IAM.4",
              "AssociatedStandards":[
                 {
                    "StandardsId":"standards/aws-foundational-security-best-
practices/v/1.0.0"
                 }
              ]
           },
           "WorkflowState":"NEW",
           "Workflow":{
              "Status":"RESOLVED"
           },
           "RecordState":"ACTIVE",
           "FindingProviderFields":{
              "Severity":{
                 "Label":"INFORMATIONAL",
                 "Original":"INFORMATIONAL"
              },
              "Types":[
                 "Software and Configuration Checks/Industry and Regulatory
 Standards/AWS-Foundational-Security-Best-Practices"
```

```
            ]
         },
         "ProcessedAt":"2023-11-01T14:12:07.395Z"
      }
   ]
  }
}
```

IAM.4(CIS 1.2)에 대한 증거

```
{
  "version":"0",
  "id":"12345678-1q2w-3e4r-5t6y-123456789012",
  "detail-type":"Security Hub Findings - Imported",
  "source":"aws.securityhub",
  "account":"111122223333",
  "time":"2023-10-27T18:55:59Z",
  "region":"us-west-2",
  "resources":[
     "arn:aws:securityhub:us-west-2::product/aws/securityhub/arn:aws:securityhub:us-
west-2:111122223333:subscription/aws-foundational-security-best-practices/v/1.0.0/
Lambda.1/finding/1dd8f2f8-cf1b-47c9-a875-8d7387fc9c23"
  ],
  "detail":{
     "findings":[
        {
           "SchemaVersion":"2018-10-08",
           "Id":"arn:aws:securityhub:us-west-2:111122223333:subscription/cis-aws-
foundations-benchmark/v/1.2.0/1.12/finding/1dd8f2f8-cf1b-47c9-a875-8d7387fc9c23",
           "ProductArn":"arn:aws:securityhub:us-west-2::product/aws/securityhub",
           "ProductName":"Security Hub",
           "CompanyName":"AWS",
           "Region":"us-west-2",
           "GeneratorId":"arn:aws:securityhub:::ruleset/cis-aws-foundations-
benchmark/v/1.2.0/rule/1.12",
           "AwsAccountId":"111122223333",
           "Types":[
              "Software and Configuration Checks/Industry and Regulatory Standards/
CIS AWS Foundations Benchmark"
           ],
           "FirstObservedAt":"2020-10-05T19:18:47.775Z",
```

```
            "LastObservedAt":"2023-11-01T14:12:07.989Z",
            "CreatedAt":"2020-10-05T19:18:47.775Z",
            "UpdatedAt":"2023-11-01T14:11:53.720Z",
            "Severity":{
               "Product":0,
               "Label":"INFORMATIONAL",
               "Normalized":0,
               "Original":"INFORMATIONAL"
            },
            "Title":"1.12 Ensure no root user access key exists",
            "Description":"The root user is the most privileged user in an AWS
 account. AWS Access Keys provide programmatic access to a given AWS account. It is
 recommended that all access keys associated with the root user be removed.",
            "Remediation":{
               "Recommendation":{
                  "Text":"For information on how to correct this issue, consult the
 AWS Security Hub controls documentation.",
                  "Url":"https://docs.aws.amazon.com/console/securityhub/IAM.4/
remediation"
               }
            },
            "ProductFields":{
               "StandardsGuideArn":"arn:aws:securityhub:::ruleset/cis-aws-
foundations-benchmark/v/1.2.0",
               "StandardsGuideSubscriptionArn":"arn:aws:securityhub:us-
west-2:111122223333:subscription/cis-aws-foundations-benchmark/v/1.2.0",
               "RuleId":"1.12",
               "RecommendationUrl":"https://docs.aws.amazon.com/console/securityhub/
IAM.4/remediation",
               "RelatedAWSResources:0/name":"securityhub-iam-root-access-key-
check-67cbb1c4",
               "RelatedAWSResources:0/type":"AWS::Config::ConfigRule",
               "StandardsControlArn":"arn:aws:securityhub:us-
west-2:111122223333:control/cis-aws-foundations-benchmark/v/1.2.0/1.12",
               "aws/securityhub/ProductName":"Security Hub",
               "aws/securityhub/CompanyName":"AWS",
               "Resources:0/Id":"arn:aws:iam::111122223333:root",
               "aws/securityhub/FindingId":"arn:aws:securityhub:us-west-2::product/
aws/securityhub/arn:aws:securityhub:us-west-2:111122223333:subscription/cis-aws-
foundations-benchmark/v/1.2.0/1.12/finding/1dd8f2f8-cf1b-47c9-a875-8d7387fc9c23"
            },
            "Resources":[
               {
                  "Type":"AwsAccount",
```

```
                "Id":"AWS::::Account:111122223333",
                "Partition":"aws",
                "Region":"us-west-2"
             }
          ],
          "Compliance":{
             "Status":"PASSED",
             "SecurityControlId":"IAM.4",
             "AssociatedStandards":[
                {
                   "StandardsId":"ruleset/cis-aws-foundations-benchmark/v/1.2.0"
                }
             ]
          },
          "WorkflowState":"NEW",
          "Workflow":{
             "Status":"RESOLVED"
          },
          "RecordState":"ACTIVE",
          "FindingProviderFields":{
             "Severity":{
                "Label":"INFORMATIONAL",
                "Original":"INFORMATIONAL"
             },
             "Types":[
                "Software and Configuration Checks/Industry and Regulatory
 Standards/CIS AWS Foundations Benchmark"
             ]
          },
          "ProcessedAt":"2023-11-01T14:12:13.436Z"
       }
    ]
  }
}
```


PCI.IAM.1(PCI DSS)에 대한 증거


```
{
  "version":"0",
  "id":"12345678-1q2w-3e4r-5t6y-123456789012",
  "detail-type":"Security Hub Findings - Imported",
  "source":"aws.securityhub",
  "account":"111122223333",
```

```
  "time":"2023-10-27T18:55:59Z",
  "region":"us-west-2",
  "resources":[
     "arn:aws:securityhub:us-west-2::product/aws/securityhub/arn:aws:securityhub:us-
west-2:111122223333:subscription/aws-foundational-security-best-practices/v/1.0.0/
Lambda.1/finding/1dd8f2f8-cf1b-47c9-a875-8d7387fc9c23"
  ],
  "detail":{
     "findings":[
        {
           "SchemaVersion":"2018-10-08",
           "Id":"arn:aws:securityhub:us-west-2:111122223333:subscription/pci-dss/
v/3.2.1/PCI.IAM.1/finding/3c75f651-6e2e-44f4-8e22-297d5c2d0c8b",
           "ProductArn":"arn:aws:securityhub:us-west-2::product/aws/securityhub",
           "ProductName":"Security Hub",
           "CompanyName":"AWS",
           "Region":"us-west-2",
           "GeneratorId":"pci-dss/v/3.2.1/PCI.IAM.1",
           "AwsAccountId":"111122223333",
           "Types":[
              "Software and Configuration Checks/Industry and Regulatory Standards/
PCI-DSS"
           ],
           "FirstObservedAt":"2020-10-05T19:18:47.788Z",
           "LastObservedAt":"2023-11-01T14:12:02.413Z",
           "CreatedAt":"2020-10-05T19:18:47.788Z",
           "UpdatedAt":"2023-11-01T14:11:53.720Z",
           "Severity":{
              "Product":0,
              "Label":"INFORMATIONAL",
              "Normalized":0,
              "Original":"INFORMATIONAL"
           },
           "Title":"PCI.IAM.1 IAM root user access key should not exist",
           "Description":"This AWS control checks whether the root user access key
 is available.",
           "Remediation":{
              "Recommendation":{
                 "Text":"For information on how to correct this issue, consult the
 AWS Security Hub controls documentation.",
                 "Url":"https://docs.aws.amazon.com/console/securityhub/IAM.4/
remediation"
              }
           },
```

```
            "ProductFields":{
               "StandardsArn":"arn:aws:securityhub:::standards/pci-dss/v/3.2.1",
               "StandardsSubscriptionArn":"arn:aws:securityhub:us-
west-2:111122223333:subscription/pci-dss/v/3.2.1",
               "ControlId":"PCI.IAM.1",
               "RecommendationUrl":"https://docs.aws.amazon.com/console/securityhub/
IAM.4/remediation",
               "RelatedAWSResources:0/name":"securityhub-iam-root-access-key-
check-67cbb1c4",
               "RelatedAWSResources:0/type":"AWS::Config::ConfigRule",
               "StandardsControlArn":"arn:aws:securityhub:us-
west-2:111122223333:control/pci-dss/v/3.2.1/PCI.IAM.1",
               "aws/securityhub/ProductName":"Security Hub",
               "aws/securityhub/CompanyName":"AWS",
               "Resources:0/Id":"arn:aws:iam::111122223333:root",
               "aws/securityhub/FindingId":"arn:aws:securityhub:us-west-2::product/
aws/securityhub/arn:aws:securityhub:us-west-2:111122223333:subscription/pci-dss/
v/3.2.1/PCI.IAM.1/finding/3c75f651-6e2e-44f4-8e22-297d5c2d0c8b"
            },
            "Resources":[
               {
                  "Type":"AwsAccount",
                  "Id":"AWS::::Account:111122223333",
                  "Partition":"aws",
                  "Region":"us-west-2"
               }
            ],
            "Compliance":{
               "Status":"PASSED",
               "RelatedRequirements":[
                  "PCI DSS 2.1",
                  "PCI DSS 2.2",
                  "PCI DSS 7.2.1"
               ],
               "SecurityControlId":"IAM.4",
               "AssociatedStandards":[
                  {
                     "StandardsId":"standards/pci-dss/v/3.2.1"
                  }
               ]
            },
            "WorkflowState":"NEW",
            "Workflow":{
               "Status":"RESOLVED"
```

```
            },
            "RecordState":"ACTIVE",
            "FindingProviderFields":{
               "Severity":{
                  "Label":"INFORMATIONAL",
                  "Original":"INFORMATIONAL"
               },
               "Types":[
                  "Software and Configuration Checks/Industry and Regulatory
 Standards/PCI-DSS"
               ]
            },
            "ProcessedAt":"2023-11-01T14:12:05.950Z"
         }
      ]
   }
}
```

지원하는 Security Hub 컨트롤

현재 Audit Manager에서 지원하는 Security Hub 컨트롤은 다음과 같습니다. 사용자 지정 컨트롤용 데이터 소스를 설정할 때는 다음과 같은 표준별 컨트롤 ID 키워드를 사용할 수 있습니다.

보안 표준	Audit Manager에서 지원하는 키워드 (Security Hub의 표준 컨트롤 ID)	관련 컨트롤 문서 (Security Hub의 해당 보안 컬트롤 ID)
CIS v1.2.0	1.2	IAM.5
CIS v1.2.0	1.3	IAM.8
CIS v1.2.0	1.4	IAM.3
CIS v1.2.0	1.5	IAM.11
CIS v1.2.0	1.6	IAM.12

보안 표준	Audit Manager에서 지원하는 키워드 (Security Hub의 표준 컨트롤 ID)	관련 컨트롤 문서 (Security Hub의 해당 보안 컬트롤 ID)
CIS v1.2.0	1.7	IAM.13
CIS v1.2.0	1.8	IAM.14
CIS v1.2.0	1.9	IAM.15
CIS v1.2.0	1.10	IAM.16
CIS v1.2.0	1.11	IAM.17
CIS v1.2.0	1.12	IAM.4
CIS v1.2.0	1.13	IAM.9
CIS v1.2.0	1.14	IAM.6
CIS v1.2.0	1.16	IAM.2
CIS v1.2.0	1.20	IAM.18
CIS v1.2.0	1.22	IAM.1
CIS v1.2.0	2.1	CloudTrail.1.
CIS v1.2.0	2.2	CloudTrail4.
CIS v1.2.0	2.3	CloudTrail6.
CIS v1.2.0	2.4	CloudTrail5.
CIS v1.2.0	2.5	Config.1
CIS v1.2.0	2.6	CloudTrail.7
CIS v1.2.0	2.7	CloudTrail2.

보안 표준	Audit Manager에서 지원하는 키워드 (Security Hub의 표준 컨트롤 ID)	관련 컨트롤 문서 (Security Hub의 해당 보안 컬트롤 ID)
CIS v1.2.0	2.8	KMS.4
CIS v1.2.0	2.9	EC2.6
CIS v1.2.0	3.1	CloudWatch2.
CIS v1.2.0	3.2	CloudWatch3.
CIS v1.2.0	3.3	CloudWatch.1.
CIS v1.2.0	3.4	CloudWatch4.
CIS v1.2.0	3.5	CloudWatch5.
CIS v1.2.0	3.6	CloudWatch6.
CIS v1.2.0	3.7	CloudWatch.7
CIS v1.2.0	3.8	CloudWatch.8.
CIS v1.2.0	3.9	CloudWatch9.
CIS v1.2.0	3.10	CloudWatch.10
CIS v1.2.0	3.11	CloudWatch1.1
CIS v1.2.0	3.12	CloudWatch1.2
CIS v1.2.0	3.13	CloudWatch1.3
CIS v1.2.0	3.14	CloudWatch1.4
CIS v1.2.0	4.1	EC2.13
CIS v1.2.0	4.2	EC2.14

보안 표준	Audit Manager에서 지원하는 키워드 (Security Hub의 표준 컨트롤 ID)	관련 컨트롤 문서 (Security Hub의 해당 보안 컬트롤 ID)
CIS v1.2.0	4.3	EC2.2
PCI DSS	PCI. AutoScaling1.	AutoScaling.1.
PCI DSS	사진. CloudTrail1.	CloudTrail.1.
PCI DSS	사진. CloudTrail2.	CloudTrail2.
PCI DSS	사진. CloudTrail3.	CloudTrail3.
PCI DSS	사진. CloudTrail4.	CloudTrail4.
PCI DSS	사진. CodeBuild1.	CodeBuild.1.
PCI DSS	사진. CodeBuild2.	CodeBuild2.
PCI DSS	PCI.Config.1	Config.1
PCI DSS	PCI.CW.1	CloudWatch.1.
PCI DSS	PCI.DMS.1	DMS.1
PCI DSS	PCI.EC2.1	EC2.1
PCI DSS	PCI.EC2.2	EC2.2

보안 표준	Audit Manager에서 지원하는 키워드 (Security Hub의 표준 컨트롤 ID)	관련 컨트롤 문서 (Security Hub의 해당 보안 컬트롤 ID)
PCI DSS	PCI.EC2.3	EC2.3
PCI DSS	PCI.EC2.4	EC2.12
PCI DSS	PCI.EC2.5	EC2.13
PCI DSS	PCI.EC2.6	EC2.6
PCI DSS	PCI.ELBv2.1	ELB.1
PCI DSS	PCI.ES.1	ES.1
PCI DSS	PCI.ES.2	ES.2
PCI DSS	PCI. GuardDuty 1.	GuardDuty.1.
PCI DSS	PCI.IAM.1	IAM.1
PCI DSS	PCI.IAM.2	IAM.2
PCI DSS	PCI.IAM.3	IAM.3
PCI DSS	PCI.IAM.4	IAM.4
PCI DSS	PCI.IAM.5	IAM.9
PCI DSS	PCI.IAM.6	IAM.6
PCI DSS	PCI.IAM.7	PCI.IAM.7
PCI DSS	PCI.IAM.8	PCI.IAM.8
PCI DSS	PCI.KMS.1	PCI.KMS.4

보안 표준	Audit Manager에서 지원하는 키워드 (Security Hub의 표준 컨트롤 ID)	관련 컨트롤 문서 (Security Hub의 해당 보안 컬트롤 ID)
PCI DSS	PCI.Lambda.1	Lambda.1
PCI DSS	PCI.Lambda.2	Lambda.3
PCI DSS	PCI.Opensearch.1	Opensearch.1
PCI DSS	PCI.OpenSearch.2	Opensearch.2
PCI DSS	PCI.RDS.1	RDS.1
PCI DSS	PCI.RDS.2	RDS.2
PCI DSS	PCI.Redshift.1	Redshift.1
PCI DSS	PCI.S3.1	S3.1
PCI DSS	PCI.S3.2	S3.2
PCI DSS	PCI.S3.3	S3.3
PCI DSS	PCI.S3.4	S3.4
PCI DSS	PCI.S3.5	S3.5
PCI DSS	PCI.S3.6	S3.1
PCI DSS	사진. SageMaker1.	SageMaker.1.
PCI DSS	PCI.SSM.1	SSM.1
PCI DSS	PCI.SSM.2	SSM.2

보안 표준	Audit Manager에서 지원하는 키워드 (Security Hub의 표준 컨트롤 ID)	관련 컨트롤 문서 (Security Hub의 해당 보안 컬트롤 ID)
PCI DSS	PCI.SSM.3	SSM.3
AWS 기본 보안 모범 사례	Account.1	Account.1
AWS 기본 보안 모범 사례	Account.2	Account.2
AWS 기본 보안 모범 사례	ACM.1	ACM.1
AWS 기본 보안 모범 사례	ACM.2	ACM.2
AWS 기본 보안 모범 사례	APIGateway.1	APIGateway.1
AWS 기본 보안 모범 사례	APIGateway.2	APIGateway.2
AWS 기본 보안 모범 사례	APIGateway.3	APIGateway.3.
AWS 기본 보안 모범 사례	APIGateway.4	APIGateway.4
AWS 기본 보안 모범 사례	APIGateway.5	APIGateway.5
AWS 기본 보안 모범 사례	APIGateway.8	APIGateway.8
AWS 기본 보안 모범 사례	APIGateway.9	APIGateway.9
AWS 기본 보안 모범 사례	AppSync2.	AppSync2.
AWS 기본 보안 모범 사례	AppSync5.	AppSync5.
AWS 기본 보안 모범 사례	Athena.1	Athena.1
AWS 기본 보안 모범 사례	AutoScaling1.	AutoScaling.1.
AWS 기본 보안 모범 사례	AutoScaling2.	AutoScaling2.
AWS 기본 보안 모범 사례	AutoScaling3.	AutoScaling3.

보안 표준	Audit Manager에서 지원하는 키워드 (Security Hub의 표준 컨트롤 ID)	관련 컨트롤 문서 (Security Hub의 해당 보안 컬트롤 ID)
AWS 기본 보안 모범 사례	AutoScaling4.	AutoScaling4.
AWS 기본 보안 모범 사례	AutoScaling.5	Autoscaling.5
AWS 기본 보안 모범 사례	AutoScaling6.	AutoScaling6.
AWS 기본 보안 모범 사례	AutoScaling9.	AutoScaling9.
AWS 기본 보안 모범 사례	Backup.1	Backup.1
AWS 기본 보안 모범 사례	CloudFormation1.	CloudFormation.1.
AWS 기본 보안 모범 사례	CloudFront1.	CloudFront.1.
AWS 기본 보안 모범 사례	CloudFront2.	CloudFront2.
AWS 기본 보안 모범 사례	CloudFront3.	CloudFront3.
AWS 기본 보안 모범 사례	CloudFront4.	CloudFront4.
AWS 기본 보안 모범 사례	CloudFront5.	CloudFront5.
AWS 기본 보안 모범 사례	CloudFront6.	CloudFront6.
AWS 기본 보안 모범 사례	CloudFront7.7.	CloudFront.7
AWS 기본 보안 모범 사례	CloudFront8.	CloudFront8.
AWS 기본 보안 모범 사례	CloudFront9.	CloudFront9.
AWS 기본 보안 모범 사례	CloudFront1.0	CloudFront1.0
AWS 기본 보안 모범 사례	CloudFront1.2	CloudFront1.2

보안 표준	Audit Manager에서 지원하는 키워드 (Security Hub의 표준 컨트롤 ID)	관련 컨트롤 문서 (Security Hub의 해당 보안 컬트롤 ID)
AWS 기본 보안 모범 사례	CloudFront1.3	CloudFront1.3
AWS 기본 보안 모범 사례	CloudTrail1.	CloudTrail.1.
AWS 기본 보안 모범 사례	CloudTrail2.	CloudTrail2.
AWS 기본 보안 모범 사례	CloudTrail3.	CloudTrail3.
AWS 기본 보안 모범 사례	CloudTrail4.	CloudTrail4.
AWS 기본 보안 모범 사례	CloudTrail5.	CloudTrail5.
AWS 기본 보안 모범 사례	CloudTrail6.	CloudTrail6.
AWS 기본 보안 모범 사례	CloudTrail7.7.	CloudTrail.7
AWS 기본 보안 모범 사례	CloudWatch1.	CloudWatch.1.
AWS 기본 보안 모범 사례	CloudWatch2.	CloudWatch2.
AWS 기본 보안 모범 사례	CloudWatch3.	CloudWatch3.
AWS 기본 보안 모범 사례	CloudWatch4.	CloudWatch4.
AWS 기본 보안 모범 사례	CloudWatch5.	CloudWatch5.
AWS 기본 보안 모범 사례	CloudWatch6.	CloudWatch6.
AWS 기본 보안 모범 사례	CloudWatch7.7.	CloudWatch.7
AWS 기본 보안 모범 사례	CloudWatch8.	CloudWatch8.
AWS 기본 보안 모범 사례	CloudWatch9.	CloudWatch9.
AWS 기본 보안 모범 사례	CloudWatch1.0	CloudWatch1.0

보안 표준	Audit Manager에서 지원하는 키워드 (Security Hub의 표준 컨트롤 ID)	관련 컨트롤 문서 (Security Hub의 해당 보안 컬트롤 ID)
AWS 기본 보안 모범 사례	CloudWatch1.1	CloudWatch1.1
AWS 기본 보안 모범 사례	CloudWatch1.2	CloudWatch1.2
AWS 기본 보안 모범 사례	CloudWatch1.3	CloudWatch1.3
AWS 기본 보안 모범 사례	CloudWatch1.4	CloudWatch1.4
AWS 기본 보안 모범 사례	CloudWatch1.5	CloudWatch1.5
AWS 기본 보안 모범 사례	CloudWatch1.6	CloudWatch1.6
AWS 기본 보안 모범 사례	CloudWatch1.7	CloudWatch.17
AWS 기본 보안 모범 사례	CodeBuild1.	CodeBuild.1.
AWS 기본 보안 모범 사례	CodeBuild2.	CodeBuild2.
AWS 기본 보안 모범 사례	CodeBuild3.	CodeBuild3.
AWS 기본 보안 모범 사례	CodeBuild4.	CodeBuild4.
AWS 기본 보안 모범 사례	CodeBuild5.	CodeBuild5.
AWS 기본 보안 모범 사례	Config 1	Config.1
AWS 기본 보안 모범 사례	DMS.1	DMS.1
AWS 기본 보안 모범 사례	DMS.6	DMS.6
AWS 기본 보안 모범 사례	DMS.7	DMS.7
AWS 기본 보안 모범 사례	DMS.8	DMS.8
AWS 기본 보안 모범 사례	DMS.9	DMS.9

보안 표준	Audit Manager에서 지원하는 키워드 (Security Hub의 표준 컨트롤 ID)	관련 컨트롤 문서 (Security Hub의 해당 보안 컬트롤 ID)
AWS 기본 보안 모범 사례	DocumentDB.1	DocumentDB.1
AWS 기본 보안 모범 사례	DocumentDB.2	DocumentDB.2
AWS 기본 보안 모범 사례	DocumentDB.3	DocumentDB.3
AWS 기본 보안 모범 사례	DocumentDB.4	DocumentDB.4
AWS 기본 보안 모범 사례	DocumentDB.5	DocumentDB.5
AWS 기본 보안 모범 사례	DynamoDB.1	DynamoDB.1
AWS 기본 보안 모범 사례	DynamoDB.2	DynamoDB.2
AWS 기본 보안 모범 사례	DynamoDB.3	DynamoDB.3
AWS 기본 보안 모범 사례	DynamoDB.4	DynamoDB.4
AWS 기본 보안 모범 사례	DynamoDB.6	DynamoDB.6
AWS 기본 보안 모범 사례	EC2.1	EC2.1
AWS 기본 보안 모범 사례	EC2.2	EC2.2
AWS 기본 보안 모범 사례	EC2.3	EC2.3
AWS 기본 보안 모범 사례	EC2.4	EC2.4
AWS 기본 보안 모범 사례	EC2.6	EC2.6
AWS 기본 보안 모범 사례	EC2.7	EC2.7
AWS 기본 보안 모범 사례	EC2.8	EC2.8
AWS 기본 보안 모범 사례	EC2.9	EC2.9

보안 표준	Audit Manager에서 지원하는 키워드 (Security Hub의 표준 컨트롤 ID)	관련 컨트롤 문서 (Security Hub의 해당 보안 컬트롤 ID)
AWS 기본 보안 모범 사례	EC2.10	EC2.10
AWS 기본 보안 모범 사례	EC2.12	EC2.12
AWS 기본 보안 모범 사례	EC2.13	EC2.13
AWS 기본 보안 모범 사례	EC2.14	EC2.14
AWS 기본 보안 모범 사례	EC2.15	EC2.15
AWS 기본 보안 모범 사례	EC2.16	EC2.16
AWS 기본 보안 모범 사례	EC2.17	EC2.17
AWS 기본 보안 모범 사례	EC2.18	EC2.18
AWS 기본 보안 모범 사례	EC2.19	EC2.19
AWS 기본 보안 모범 사례	EC2.20	EC2.20
AWS 기본 보안 모범 사례	EC2.21	EC2.21
AWS 기본 보안 모범 사례	EC2.22	EC2.22
AWS 기본 보안 모범 사례	EC2.23	EC2.23
AWS 기본 보안 모범 사례	EC2.24	EC2.24
AWS 기본 보안 모범 사례	EC2.25	EC2.25
AWS 기본 보안 모범 사례	EC2.28	EC2.28
AWS 기본 보안 모범 사례	EC2.51	EC2.51
AWS 기본 보안 모범 사례	ECR.1	ECR.1

보안 표준	Audit Manager에서 지원하는 키워드 (Security Hub의 표준 컨트롤 ID)	관련 컨트롤 문서 (Security Hub의 해당 보안 컬트롤 ID)
AWS 기본 보안 모범 사례	ECR.2	ECR.2
AWS 기본 보안 모범 사례	ECR.3	ECR.3
AWS 기본 보안 모범 사례	ECS.1	ECS.1
AWS 기본 보안 모범 사례	ECS.2	ECS.2
AWS 기본 보안 모범 사례	ECS.3	ECS.3
AWS 기본 보안 모범 사례	ECS.4	ECS.4
AWS 기본 보안 모범 사례	ECS.5	ECS.5
AWS 기본 보안 모범 사례	EC.8	ECS.8
AWS 기본 보안 모범 사례	ECS.9	ECS.9
AWS 기본 보안 모범 사례	ECS.10	ECS.10
AWS 기본 보안 모범 사례	ECS.12	ECS.12
AWS 기본 보안 모범 사례	EFS.1	EFS.1
AWS 기본 보안 모범 사례	EFS.2	EFS.2
AWS 기본 보안 모범 사례	EFS.3	EFS.3
AWS 기본 보안 모범 사례	EFS.4	EFS.4
AWS 기본 보안 모범 사례	EKS.1	EKS.1
AWS 기본 보안 모범 사례	EKS.2	EKS.2
AWS 기본 보안 모범 사례	EKS.8	EKS.8

보안 표준	Audit Manager에서 지원하는 키워드 (Security Hub의 표준 컨트롤 ID)	관련 컨트롤 문서 (Security Hub의 해당 보안 컬트롤 ID)
AWS 기본 보안 모범 사례	ElastiCache1.	ElastiCache.1.
AWS 기본 보안 모범 사례	ElastiCache2.	ElastiCache2.
AWS 기본 보안 모범 사례	ElastiCache3.	ElastiCache3.
AWS 기본 보안 모범 사례	ElastiCache4.	ElastiCache4.
AWS 기본 보안 모범 사례	ElastiCache5.	ElastiCache5.
AWS 기본 보안 모범 사례	ElastiCache6.	ElastiCache6.
AWS 기본 보안 모범 사례	ElastiCache7.7.	ElastiCache.7
AWS 기본 보안 모범 사례	ElasticBeanstalk1.	ElasticBeanstalk.1.
AWS 기본 보안 모범 사례	ElasticBeanstalk2.	ElasticBeanstalk2.
AWS 기본 보안 모범 사례	ElasticBeanstalk3.	ElasticBeanstalk3.
AWS 기본 보안 모범 사례	ELB.1	ELB.1
AWS 기본 보안 모범 사례	ELB.2	ELB.2
AWS 기본 보안 모범 사례	ELB.3	ELB.3
AWS 기본 보안 모범 사례	ELB.4	ELB.4
AWS 기본 보안 모범 사례	ELB.5	ELB.5
AWS 기본 보안 모범 사례	ELB.6	ELB.6

보안 표준	Audit Manager에서 지원하는 키워드 (Security Hub의 표준 컨트롤 ID)	관련 컨트롤 문서 (Security Hub의 해당 보안 컬트롤 ID)
AWS 기본 보안 모범 사례	ELB.7	ELB.7
AWS 기본 보안 모범 사례	ELB.8	ELB.8
AWS 기본 보안 모범 사례	ELB.9	ELB.9
AWS 기본 보안 모범 사례	ELB.10	ELB.10
AWS 기본 보안 모범 사례	ELB.12	ELB.12
AWS 기본 보안 모범 사례	ELB.13	ELB.13
AWS 기본 보안 모범 사례	ELB.14	ELB.14
AWS 기본 보안 모범 사례	ELB.16	ELB.16
AWS 기본 보안 모범 사례	ELBv2.1	ELB.1
AWS 기본 보안 모범 사례	EMR.1	EMR.1
AWS 기본 보안 모범 사례	EMR.2	EMR.2
AWS 기본 보안 모범 사례	ES.1	ES.1
AWS 기본 보안 모범 사례	ES.2	ES.2
AWS 기본 보안 모범 사례	ES.3	ES.3
AWS 기본 보안 모범 사례	ES.4	ES.4
AWS 기본 보안 모범 사례	ES.5	ES.5
AWS 기본 보안 모범 사례	ES.6	ES.6
AWS 기본 보안 모범 사례	ES.7	ES.7

보안 표준	Audit Manager에서 지원하는 키워드 (Security Hub의 표준 컨트롤 ID)	관련 컨트롤 문서 (Security Hub의 해당 보안 컬트롤 ID)
AWS 기본 보안 모범 사례	ES.8	ES.8
AWS 기본 보안 모범 사례	EventBridge3.	EventBridge3.
AWS 기본 보안 모범 사례	EventBridge4.	EventBridge4.
AWS 기본 보안 모범 사례	FSx.1	FSx.1
AWS 기본 보안 모범 사례	GuardDuty1.	GuardDuty.1.
AWS 기본 보안 모범 사례	IAM.1	IAM.1
AWS 기본 보안 모범 사례	IAM.2	IAM.2
AWS 기본 보안 모범 사례	IAM.3	IAM.3
AWS 기본 보안 모범 사례	IAM.4	IAM.4
AWS 기본 보안 모범 사례	IAM.5	IAM.5
AWS 기본 보안 모범 사례	IAM.6	IAM.6
AWS 기본 보안 모범 사례	IAM.7	IAM.7
AWS 기본 보안 모범 사례	IAM.8	IAM.8
AWS 기본 보안 모범 사례	IAM.9	IAM.9
AWS 기본 보안 모범 사례	IAM.10	IAM.10
AWS 기본 보안 모범 사례	IAM.11	IAM.11
AWS 기본 보안 모범 사례	IAM.12	IAM.12
AWS 기본 보안 모범 사례	IAM.13	IAM.13

보안 표준	Audit Manager에서 지원하는 키워드 (Security Hub의 표준 컨트롤 ID)	관련 컨트롤 문서 (Security Hub의 해당 보안 컬트롤 ID)
AWS 기본 보안 모범 사례	IAM.14	IAM.14
AWS 기본 보안 모범 사례	IAM.15	IAM.15
AWS 기본 보안 모범 사례	IAM.16	IAM.16
AWS 기본 보안 모범 사례	IAM.17	IAM.17
AWS 기본 보안 모범 사례	IAM.18	IAM.18
AWS 기본 보안 모범 사례	IAM.19	IAM.19
AWS 기본 보안 모범 사례	IAM.21	IAM.21
AWS 기본 보안 모범 사례	IAM.22	IAM.22
AWS 기본 보안 모범 사례	Kinesis.1	Kinesis.1
AWS 기본 보안 모범 사례	KMS.1	KMS.1
AWS 기본 보안 모범 사례	KMS.2	KMS.2
AWS 기본 보안 모범 사례	KMS.3	KMS.3
AWS 기본 보안 모범 사례	KMS.4	KMS.4
AWS 기본 보안 모범 사례	Lambda.1	Lambda.1
AWS 기본 보안 모범 사례	Lambda.2	Lambda.2
AWS 기본 보안 모범 사례	Lambda.3	Lambda.3
AWS 기본 보안 모범 사례	Lambda.5	Lambda.5
AWS 기본 보안 모범 사례	Macie.1	Macie.1

보안 표준	Audit Manager에서 지원하는 키워드 (Security Hub의 표준 컨트롤 ID)	관련 컨트롤 문서 (Security Hub의 해당 보안 컬트롤 ID)
AWS 기본 보안 모범 사례	MQ.5	MQ.5
AWS 기본 보안 모범 사례	MQ.6	MQ.6
AWS 기본 보안 모범 사례	MSK.1	MSK.1
AWS 기본 보안 모범 사례	MSK.2	MSK.2
AWS 기본 보안 모범 사례	Neptune.1	Neptune.1
AWS 기본 보안 모범 사례	Neptune.2	Neptune.2
AWS 기본 보안 모범 사례	Neptune.3	Neptune.3
AWS 기본 보안 모범 사례	Neptune.4	Neptune.4
AWS 기본 보안 모범 사례	Neptune.5	Neptune.5
AWS 기본 보안 모범 사례	Neptune.6	Neptune.6
AWS 기본 보안 모범 사례	Neptune.7	Neptune.7
AWS 기본 보안 모범 사례	Neptune.8	Neptune.8
AWS 기본 보안 모범 사례	Neptune.9	Neptune.9
AWS 기본 보안 모범 사례	NetworkFirewall1.	NetworkFirewall.1.
AWS 기본 보안 모범 사례	NetworkFirewall2.	NetworkFirewall2.
AWS 기본 보안 모범 사례	NetworkFirewall3.	NetworkFirewall3.

보안 표준	Audit Manager에서 지원하는 키워드 (Security Hub의 표준 컨트롤 ID)	관련 컨트롤 문서 (Security Hub의 해당 보안 컨트롤 ID)
AWS 기본 보안 모범 사례	NetworkFirewall4.	NetworkFirewall4.
AWS 기본 보안 모범 사례	NetworkFirewall5.	NetworkFirewall5.
AWS 기본 보안 모범 사례	NetworkFirewall6.	NetworkFirewall6.
AWS 기본 보안 모범 사례	NetworkFirewall9.	NetworkFirewall9.
AWS 기본 보안 모범 사례	Opensearch.1	Opensearch.1
AWS 기본 보안 모범 사례	Opensearch.2	Opensearch.2
AWS 기본 보안 모범 사례	Opensearch.3	Opensearch.3
AWS 기본 보안 모범 사례	Opensearch.4	Opensearch.4
AWS 기본 보안 모범 사례	Opensearch.5	Opensearch.5
AWS 기본 보안 모범 사례	Opensearch.6	Opensearch.6
AWS 기본 보안 모범 사례	Opensearch.7	Opensearch.7
AWS 기본 보안 모범 사례	Opensearch.8	Opensearch.8
AWS 기본 보안 모범 사례	Opensearch.10	Opensearch.10
AWS 기본 보안 모범 사례	PCA.1	PCA.1
AWS 기본 보안 모범 사례	RDS.1	RDS.1

보안 표준	Audit Manager에서 지원하는 키워드 (Security Hub의 표준 컨트롤 ID)	관련 컨트롤 문서 (Security Hub의 해당 보안 컬트롤 ID)
AWS 기본 보안 모범 사례	RDS.2	RDS.2
AWS 기본 보안 모범 사례	RDS.3	RDS.3
AWS 기본 보안 모범 사례	RDS.4	RDS.4
AWS 기본 보안 모범 사례	RDS.5	RDS.5
AWS 기본 보안 모범 사례	RDS.6	RDS.6
AWS 기본 보안 모범 사례	RDS.7	RDS.7
AWS 기본 보안 모범 사례	RDS.8	RDS.8
AWS 기본 보안 모범 사례	RDS.9	RDS.9
AWS 기본 보안 모범 사례	RDS.10	RDS.10
AWS 기본 보안 모범 사례	RDS.11	RDS.11
AWS 기본 보안 모범 사례	RDS.12	RDS.12
AWS 기본 보안 모범 사례	RDS.13	RDS.13
AWS 기본 보안 모범 사례	RDS.14	RDS.14
AWS 기본 보안 모범 사례	RDS.15	RDS.15
AWS 기본 보안 모범 사례	RDS.16	RDS.16
AWS 기본 보안 모범 사례	RDS.17	RDS.17
AWS 기본 보안 모범 사례	RDS.18	RDS.18
AWS 기본 보안 모범 사례	RDS.19	RDS.19

보안 표준	Audit Manager에서 지원하는 키워드 (Security Hub의 표준 컨트롤 ID)	관련 컨트롤 문서 (Security Hub의 해당 보안 컬트롤 ID)
AWS 기본 보안 모범 사례	RDS.20	RDS.20
AWS 기본 보안 모범 사례	RDS.21	RDS.21
AWS 기본 보안 모범 사례	RDS.22	RDS.22
AWS 기본 보안 모범 사례	RDS.23	RDS.23
AWS 기본 보안 모범 사례	RDS.24	RDS.24
AWS 기본 보안 모범 사례	RDS.25	RDS.25
AWS 기본 보안 모범 사례	RDS.26	RDS.26
AWS 기본 보안 모범 사례	RDS.27	RDS.27
AWS 기본 보안 모범 사례	RDS.34	RDS.34
AWS 기본 보안 모범 사례	RDS.35	RDS.35
AWS 기본 보안 모범 사례	Redshift.1	Redshift.1
AWS 기본 보안 모범 사례	Redshift.2	Redshift.2
AWS 기본 보안 모범 사례	Redshift.3	Redshift.3
AWS 기본 보안 모범 사례	Redshift.4	Redshift.4
AWS 기본 보안 모범 사례	Redshift.6	Redshift.6
AWS 기본 보안 모범 사례	Redshift.7	Redshift.7
AWS 기본 보안 모범 사례	Redshift.8	Redshift.8
AWS 기본 보안 모범 사례	Redshift.9	Redshift.9

보안 표준	Audit Manager에서 지원하는 키워드 (Security Hub의 표준 컨트롤 ID)	관련 컨트롤 문서 (Security Hub의 해당 보안 컬트롤 ID)
AWS 기본 보안 모범 사례	Redshift.10	Redshift.10
AWS 기본 보안 모범 사례	Route53.2	Route53.2
AWS 기본 보안 모범 사례	S3.1	S3.1
AWS 기본 보안 모범 사례	S3.2	S3.2
AWS 기본 보안 모범 사례	S3.3	S3.3
AWS 기본 보안 모범 사례	S3.4	S3.4
AWS 기본 보안 모범 사례	S3.5	S3.5
AWS 기본 보안 모범 사례	S3.6	S3.6
AWS 기본 보안 모범 사례	S3.7	S3.7
AWS 기본 보안 모범 사례	S3.8	S3.8
AWS 기본 보안 모범 사례	S3.9	S3.9
AWS 기본 보안 모범 사례	S3.11	S3.11
AWS 기본 보안 모범 사례	S3.12	S3.12
AWS 기본 보안 모범 사례	S3.13	S3.13
AWS 기본 보안 모범 사례	S3.14	S3.14
AWS 기본 보안 모범 사례	S3.15	S3.15
AWS 기본 보안 모범 사례	S3.17	S3.17
AWS 기본 보안 모범 사례	S3.19	S3.19

보안 표준	Audit Manager에서 지원하는 키워드 (Security Hub의 표준 컨트롤 ID)	관련 컨트롤 문서 (Security Hub의 해당 보안 컬트롤 ID)
AWS 기본 보안 모범 사례	S3.19	S3.20
AWS 기본 보안 모범 사례	SageMaker1.	SageMaker.1.
AWS 기본 보안 모범 사례	SageMaker2.	SageMaker2.
AWS 기본 보안 모범 사례	SageMaker3.	SageMaker3.
AWS 기본 보안 모범 사례	SecretsManager1.	SecretsManager.1.
AWS 기본 보안 모범 사례	SecretsManager2.	SecretsManager2.
AWS 기본 보안 모범 사례	SecretsManager3.	SecretsManager3.
AWS 기본 보안 모범 사례	SecretsManager4.	SecretsManager4.
AWS 기본 보안 모범 사례	SNS.1	SNS.1
AWS 기본 보안 모범 사례	SNS.2	SNS.2
AWS 기본 보안 모범 사례	SQS.1	SQS.1
AWS 기본 보안 모범 사례	SSM.1	SSM.1
AWS 기본 보안 모범 사례	SSM.2	SSM.2
AWS 기본 보안 모범 사례	SSM.3	SSM.3
AWS 기본 보안 모범 사례	SSM.4	SSM.4

보안 표준	Audit Manager에서 지원하는 키워드 (Security Hub의 표준 컨트롤 ID)	관련 컨트롤 문서 (Security Hub의 해당 보안 컬트롤 ID)
AWS 기본 보안 모범 사례	StepFunctions1.	StepFunctions.1.
AWS 기본 보안 모범 사례	WAF.1	WAF.1
AWS 기본 보안 모범 사례	WAF.2	WAF.2
AWS 기본 보안 모범 사례	WAF.3	WAF.3
AWS 기본 보안 모범 사례	WAF.4	WAF.4
AWS 기본 보안 모범 사례	WAF.6	WAF.6
AWS 기본 보안 모범 사례	WAF.7	WAF.7
AWS 기본 보안 모범 사례	WAF.8	WAF.8
AWS 기본 보안 모범 사례	WAF.10	WAF.10
AWS 기본 보안 모범 사례	WAF.11	WAF.11
AWS 기본 보안 모범 사례	WAF.12	WAF.12

에서 지원하는 API 호출 AWS Audit Manager

Audit Manager는 API를 AWS 서비스 호출하여 AWS 리소스에 대한 구성 세부 정보의 스냅샷을 수집합니다. Audit Manager에서 사용자 지정 컨트롤을 구성할 때는 이러한 API 직접 호출을 데이터 소스 매핑으로 지정할 수 있습니다.

Audit Manager는 API 직접 호출 범위에 속하는 모든 리소스에 대해 구성 스냅샷을 캡처하여 이를 증거로 변환합니다. 이를 통해서, API 직접 호출당 하나의 증거가 생성되는 것과는 대조적으로, 리소스당 하나의 증거가 생성됩니다.

예를 들어, `ec2_DescribeRouteTables` API 직접 호출이 5개의 라우팅 테이블에서 구성 스냅샷을 캡처하는 경우, 단일 API 직접 호출에 대해 총 5개의 증거를 얻게 됩니다. 각 증거는 개별 라우팅 테이블 구성의 스냅샷입니다.

이 페이지의 내용

사용자 지정 컨트롤 데이터 소스를 지원하는 API 직접 호출

사용자 지정 제어에서 다음 API 직접 호출 중 하나를 데이터 소스로 사용할 수 있습니다. 그러면 Audit Manager는 이러한 API 호출을 사용하여 AWS 사용에 대한 증거를 수집할 수 있습니다.

지원하는 API 직접 호출	Audit Manager에서 이 API를 사용하여 증거를 수집하는 방법
acm_ GetAccountConfiguration	AWS 계정에 연결된 계정 구성 옵션의 스냅샷을 수집합니다.
캠_ ListCertificates	인증서 ARN 및 도메인 이름 목록을 검색합니다.
클라우드 트레일_ DescribeTrails	AWS 계정의 현재 리전에 연결된 하나 이상의 추적에 대한 설정 스냅샷을 수집합니다.
클라우드 워치_ DescribeAlarms	AWS 계정에서 사용된 경보의 구성 스냅샷을 수집합니다.
구성_ DescribeConfigRules	규칙에 대한 세부 정보를 검색하세요. AWS Config
config_ DescribeDeliveryChannels	AWS 계정에서 전송 채널의 구성 스냅샷을 수집합니다.
직접 연결_ DescribeDirectConnectGateways	모든 게이트웨이 목록을 검색하세요. AWS Direct Connect
다이렉트 커넥트_ DescribeVirtualGateways	AWS 계정에서 소유한 가상 프라이빗 게이트웨이의 목록을 검색합니다.

지원하는 API 직접 호출	Audit Manager에서 이 API를 사용하여 증거를 수집하는 방법
docdb_ DescribeCertificates	AWS 계정에 대한 인증서 목록을 수집합니다.
docDB_DescribEdB ClusterParameterGroups	AWS 계정에 대한 `DBClusterParameterGroup` 설명 목록을 수집합니다.
docdb_DescribeDBInstances	AWS 계정에서 프로비저닝된 Amazon DynamoDB 인스턴스에 대한 정보를 수집합니다.
다이나믹 b_ DescribeTable	AWS 계정에서 DynamoDB 테이블의 구성 스냅샷을 수집합니다. 이 API를 데이터 소스로 사용하는 경우, 특정 DynamoDB 테이블의 이름을 제공할 필요가 없습니다. 대신, Audit Manager는 이 `ListTables` 작업을 이용하여 모든 테이블을 나열합니다. 그런 다음, Audit Manager는 나열된 모든 테이블에 대해 해당 리소스에 대한 증거를 생성하기 위해 `DescribeTable` 작업을 수행합니다.
다이나모드b_ ListBackups	AWS 계정에 연결된 DynamoDB 백업 목록을 검색합니다.
다이나모드b_ ListGlobalTables	현재 AWS 계정에 있는 모든 글로벌 테이블 목록을 검색합니다.
다이나모드b_ ListTables	AWS 계정 및 현재 엔드포인트에 연결된 모든 테이블 이름 목록을 검색합니다.
ec2_ DescribeAddresses	탄력적 IP 주소의 스냅샷을 수집합니다.
ec2_ DescribeCustomerGateways	VPN 고객 게이트웨이의 스냅샷을 수집합니다.
ec2_ DescribeEgressOnlyInternetGateways	송신 전용 인터넷 게이트웨이의 스냅샷을 수집합니다.
ec2_ DescribeFlowLogs	흐름 로그의 스냅샷을 수집합니다.
ec2_ DescribeInstances	인스턴스의 스냅샷을 수집합니다.

지원하는 API 직접 호출	Audit Manager에서 이 API를 사용하여 증거를 수집하는 방법
ec2_ DescribeInternetGateways	인터넷 게이트웨이의 스냅샷을 수집합니다.
ec2_ DescribeLocalGatewayRouteTableVirtualInterfaceGroupAssociations	가상 인터페이스 그룹과 로컬 게이트웨이 라우팅 테이블 간의 연결에 대한 설명을 수집하십시오. AWS 계정
ec2_ DescribeLocalGateways	로컬 게이트웨이의 스냅샷을 수집합니다.
ec2_ DescribeLocalGatewayVirtualInterfaces	로컬 게이트웨이 가상 인터페이스의 스냅샷을 수집합니다.
ec2_ DescribeNatGateways	NAT 게이트웨이의 스냅샷을 수집합니다.
ec2_ DescribeNetworkAcls	네트워크 ACL의 스냅샷을 수집합니다.
ec2_ DescribeRouteTables	라우팅 테이블의 스냅샷을 수집합니다.
ec2_ DescribeSecurityGroups	보안 그룹의 스냅샷을 수집합니다.
ec2_ DescribeTransitGateways	전송 게이트웨이의 스냅샷을 수집합니다.
ec2_ DescribeVolumes	VPC 엔드포인트의 스냅샷을 수집합니다.
ec2_ DescribeVpcs	VPC의 스냅샷을 수집합니다.
ec2_ DescribeVpcEndpoints	VPC 엔드포인트의 스냅샷을 수집합니다.
ec2_ DescribeVpcPeeringConnections	VPN 연결의 스냅샷을 수집합니다.
ec2_ DescribeVpnConnections	VPN 연결의 스냅샷을 수집합니다.
ec2_ DescribeVpnGateways	가상 프라이빗 게이트웨이의 스냅샷을 수집합니다.
ec2_ GetEbsDefaultKmsKeyId	현재 AWS 계정 지역에서 EBS 암호화의 기본 AWS KMS key 스냅샷을 수집하십시오.

지원하는 API 직접 호출	Audit Manager에서 이 API를 사용하여 증거를 수집하는 방법
ec2_ GetEbsEncryptionBy Default	현재 리전의 AWS 계정 에서 기본적으로 EBS 암호화의 활성화 여부를 설명합니다.
ecs_ DescribeClusters	ECS 클러스터의 스냅샷을 수집합니다.
엑스_ DescribeAddonVersions	추가 기능 버전의 스냅샷을 수집합니다.
엘라스틱캐쉬_ DescribeC acheClusters	프로비저닝된 클러스터의 스냅샷을 수집합니다.
탄력_ DescribeServiceUpd ates	Amazon의 서비스 업데이트 스냅샷을 ElastiCache 수집하십시오.
엘라스틱파일시스템_ DescribeAccessPoints	사용자 환경에 있는 Amazon EFS 액세스 포인트의 스냅샷을 수집하십시오 AWS 계정.
엘라스틱파일시스템_ DescribeFileSystems	Amazon EFS 파일 시스템의 스냅샷을 수집합니다.
엘라스틱 로드 밸런싱 v2_ DescribeLoadBalancers	내 로드 밸런서의 스냅샷을 수집하세요. AWS 계정
elasticloadbalancingv2_Desc ribeSSLPolicies	SSL 협상에 사용하는 정책의 스냅샷을 수집합니다.
엘라스틱 로드 밸런싱 v2_ DescribeTargetGroups	ELB 대상 그룹의 스냅샷을 수집합니다.
엘라스틱 맵 리듀스_ ListSecur ityConfigurations	생성 날짜 및 시간, 이름과 함께 AWS 계정에 표시되는 보안 구성 목록을 검색합니다.
이벤트_ ListConnections	내 Amazon EventBridge 연결 목록을 검색하십시오 AWS 계정.
이벤트_ ListEventBuses	기본 이벤트 버스 AWS 계정, 사용자 지정 EventBridge 이벤트 버스 및 파트너 이벤트 버스를 포함하여 내 Amazon 이벤트 버스 목록을 검색하십시오.
events_ ListEventSources	AWS 계정에서 공유하는 파트너 이벤트 소스 목록을 검색합니다.

지원하는 API 직접 호출	Audit Manager에서 이 API를 사용하여 증거를 수집하는 방법
이벤트_ ListRules	Amazon EventBridge 규칙 목록을 검색하십시오.
파이어호스_ ListDeliveryStreams	전송 스트림 목록을 검색합니다.
팩스_ DescribeFileSystems	AWS 계정에서 소유한 파일 시스템의 스냅샷을 수집합니다.
가드듀티_ ListDetectors	Amazon GuardDuty 탐지기 리소스의 목록을 `detectorIds` 검색하십시오.
iam_ GenerateCredentialReport	AWS 계정의 보안 인증 정보 보고서를 생성합니다.
예임_ GetAccountPasswordPolicy	AWS 계정에 대한 암호 정책의 스냅샷을 수집합니다.
예임_ GetAccountSummary	AWS 계정에서 IAM 엔터티 사용 및 IAM 할당량의 스냅샷을 수집합니다.
예임_ ListGroupPolicies	에서 사용할 수 있는 IAM 그룹에 내장된 인라인 정책 목록을 검색하십시오. AWS 계정
iam_ ListGroups	에서 사용할 수 있는 경로 접두사와 연결된 IAM 그룹 목록을 검색하십시오. AWS 계정
iam_ ID ListOpen ConnectProviders	AWS 계정에 정의된 IAM OpenID Connect(OpenID) 공급자 리소스 객체 목록을 검색합니다.
iam_ ListPolicies	고객이 정의한 관리형 정책 및 모든 AWS 관리형 정책을 포함하여 AWS 계정에서 사용 가능한 모든 관리형 정책 목록을 검색합니다.
예임_ ListRoles	에서 사용할 수 있는 경로 접두사와 연결된 IAM 역할 목록을 검색하십시오. AWS 계정
iam_ListSAMLProviders	AWS 계정에서 IAM에 정의된 SAML 공급자 리소스 객체 목록을 검색합니다.
iam_ ListUsers	내 IAM 사용자 목록을 검색하십시오. AWS 계정

지원하는 API 직접 호출	Audit Manager에서 이 API를 사용하여 증거를 수집하는 방법
iam_ MFA 디바이스 ListVirtual	AWS 계정에 정의된 가상 MFA 디바이스 목록을 검색합니다.
카프카_ ListClusters	내 Amazon MSK 클러스터 목록을 검색하십시오. AWS 계정
kafka_ ListKafkaVersions	AWS 계정에서 Apache Kafka 버전 객체 목록을 검색합니다.
중국어_ ListStreams	Kinesis 데이터 스트림 목록을 검색합니다.
kms_ GetKeyPolicy	Audit Manager는 이 API를 사용하여 AWS 계정에서 AWS KMS keys 에 대한 키 정책의 스냅샷을 수집합니다. 이 API를 데이터 소스로 사용하는 경우 특정 이름을 제공할 필요가 없습니다. AWS KMS key대신, Audit Manager는 이 `ListKeys` 작업을 이용하여 모든 KMS 키를 나열합니다. 그런 다음, Audit Manager는 나열된 모든 KMS key에 대해 해당 리소스에 대한 증거를 생성하기 위해 `GetKeyPolicy` 작업을 수행합니다.
kms_ GetKeyRotationStatus	Audit Manager는 이 API를 사용하여 사용자 환경에 대해 자동 순환이 활성화되어 있는지 여부에 대한 스냅샷을 수집합니다 AWS 계정. AWS KMS keys 이 API를 데이터 소스로 사용하는 경우 특정 이름을 제공할 필요가 없습니다 AWS KMS key. 대신, Audit Manager는 이 `ListKeys` 작업을 이용하여 모든 KMS 키를 나열합니다. 그런 다음, Audit Manager는 나열된 모든 KMS key에 대해 해당 리소스에 대한 증거를 생성하기 위해 `GetKeyRotationStatus` 작업을 수행합니다.
kms_ ListKeys	내 항목의 목록을 검색하십시오 AWS KMS keys . AWS 계정
람다_ ListFunctions	각 버전별 구성을 사용하여 에서 Lambda 함수 목록을 AWS 계정 검색하십시오.
rds_DescribeDBClusters	기존 Amazon Aurora DB 클러스터와 다중 AZ DB 클러스터의 스냅샷을 수집하십시오. AWS 계정

지원하는 API 직접 호출	Audit Manager에서 이 API를 사용하여 증거를 수집하는 방법
rds_DescribeDBInstances	AWS 계정에서 프로비저닝된 RDS 인스턴스의 스냅샷을 수집합니다.
레드시프트_ DescribeClusters	AWS 계정에서 프로비저닝된 Amazon Redshift 클러스터의 스냅샷을 수집합니다.
s3_ GetBucketEncryption	S3 버킷의 기본 암호화 구성을 보여주는 스냅샷을 수집합니다. 이 API를 데이터 소스로 사용하는 경우, 특정 S3 버킷의 이름을 제공할 필요가 없습니다. 대신, Audit Manager는 `ListBuckets` 작업을 이용하여 모든 버킷을 나열합니다. 그런 다음, 나열된 모든 버킷에 대해 Audit Manager는 해당 리소스에 대한 증거를 생성하기 위해 `GetBucketEncryption` 작업을 수행합니다. Audit Manager는 평가와 AWS 리전 동일하게 생성된 버킷의 암호화 상태만 제공할 수 있습니다. 여러 AWS 리전S3 버킷에 걸친 모든 S3 버킷의 암호화 상태를 확인해야 하는 경우 S3 버킷이 AWS 리전 있는 각 위치에 평가를 생성하는 것이 좋습니다.
s3_ ListBuckets	에 있는 S3 버킷 목록을 검색하십시오. AWS 계정
sns_ ListTopics	내 SNS 주제 목록을 검색해 보세요. AWS 계정
sqs_ ListQueues	에 있는 SQS 대기열 목록을 검색하십시오. AWS 계정

페이지 매김된 API 직접 호출

대다수는 대량의 AWS 서비스 데이터를 수집하고 저장합니다. 그 결과, `list`, `describe`, 또는 `get` API 직접 호출에서 데이터를 반환하려고 하면 대단히 많은 결과가 나타날 수 있습니다. 단일 응답으로 반환하기에는 데이터 양이 너무 많을 경우, 페이지 매김 이용하여 결과를 관리하기 쉬운 여러 부분으로 나눌 수 있습니다. 이렇게 하면 결과가 데이터가 '페이지' 단위로 나뉘어 응답을 더 쉽게 처리할 수 있습니다.

Audit Manager에서 지원하는 API 직접 호출 중 일부는 페이지가 매겨져 있습니다. 즉, 처음에는 일부 결과만 보여주고, 전체 결과 세트를 보기 위해서는 후속 요청을 해야 합니다. 예를 들어, Amazon RDS DescribedBInstances 작업은 한 번에 최대 100개의 인스턴스를 보여주며, 다음 페이지의 결과를 보려면 후속 요청이 필요합니다.

2023년 3월 8일부터 Audit Manager는 증거 수집을 위한 데이터 소스로서 페이지가 매겨진 API 직접 호출을 지원합니다. 이전에는 페이지가 매겨진 API 직접 호출을 데이터 소스로 사용한 경우, API 응답에서 리소스의 일부만 볼 수 있었습니다(최대 100개의 결과). 현재는, Audit Manager에서 모든 리소스를 볼 수 있을 때까지 페이지가 매겨진 API 작업을 여러 번 호출하여 각 결과 페이지를 가져옵니다. 그런 다음, Audit Manager는 각 리소스에 대해 구성 스냅샷을 캡처하고 이를 증거로 저장합니다. 이제 전체 리소스 세트가 API 응답에 캡처되므로 수집되는 증거의 양이 증가하는 것을 알 수 있을 것입니다.

Audit Manager는 API 직접 호출 페이지 매김을 자동으로 처리합니다. 페이지가 지정된 API 직접 호출을 데이터 소스로 사용하는 사용자 지정 컨트롤을 만드는 경우, 페이지 매김 파라미터를 지정할 필요가 없습니다.

AWS License Manager 표준 프레임워크에서 사용하는 API 직접 호출

AWS License Manager 표준 프레임워크에서, Audit Manager는 증거 수집을 위해 `GetLicenseManagerSummary`이라는 사용자 지정 작업을 이용합니다. 이 작업에서는 다음 세 가지 라이선스 관리자 API를 직접 호출합니다.

- ListLicenseConfigurations
- ListAssociationsForLicenseConfiguration
- ListUsageForLicenseConfiguration

그런 다음, 보여준 데이터는 증거로 변환되어 평가의 관련 컨트롤 항목에 첨부됩니다.

예

라이선스가 부여된 두 개의 제품(SQL Service 2017 및 Oracle Database Enterprise Edition)을 사용하고 있다고 가정해 보겠습니다. 먼저 `GetLicenseManagerSummary` 액티비티가 ListLicenseConfigurationsAPI를 호출하여 계정의 라이선스 구성 세부 정보를 제공합니다. 그런 다음 및 를 ListUsageForLicenseConfiguration호출하여 각 라이선스 구성에 대한 추가 컨텍스트 데이터를 추가합니다. ListAssociationsForLicenseConfiguration 마지막으로 라이선스 구성 데이터를 증거로 변환하여 프레임워크의 각 컨트롤에 첨부합니다 (4.5 - SQL Server 2017 고객 관리형 라이선스 및 3.0.4 - Oracle Database Enterprise Edition 고객 관리형 라이선스).

프레임워크의 컨트롤 범위에 포함되지 않는 라이선스 제품을 사용하는 경우, 해당 라이선스 구성 데이터가 다음 컨트롤의 증거로 첨부됩니다. 5.0 - 기타 라이선스에 대한 고객 관리형 라이선스

AWS CloudTrail 에서 지원하는 이벤트 이름 AWS Audit Manager

Audit Manager에서 AWS CloudTrail 관리 이벤트 및 글로벌 서비스 이벤트를 증거로 캡처할 수 있습니다. 이렇게 하려면 사용자 지정 컨트롤을 만들 때 CloudTrail 이벤트 이름을 데이터 소스 매핑 키워드로 지정해야 합니다.

> **Note**
>
> Audit Manager는 관리 이벤트 및 글로벌 서비스 이벤트만 캡처합니다. 데이터 이벤트 및 인사이트 이벤트는 증거로 사용할 수 없습니다. 다양한 유형의 CloudTrail 이벤트에 대한 자세한 내용은 AWS CloudTrail 사용 설명서의 CloudTrail 개념을 참조하십시오.

위의 예외로, 다음 CloudTrail 이벤트는 Audit Manager에서 지원되지 않습니다.

- kms_ GenerateDataKey
- kms_Decrypt
- 통계_ AssumeRole
- 중국어 비디오_ GetDataEndpoint
- 중국어는 비디오_ GetSignalingChannelEndpoint
- 중국어는 비디오_ DescribeSignalingChannel
- 중국어는 비디오_ DescribeStream

2023년 5월 11일부터 Audit Manager는 증거 수집을 위한 키워드로 읽기 전용 CloudTrail 이벤트를 더 이상 지원하지 않습니다. 총 3,135개의 읽기 전용 키워드를 제거했습니다. 고객과 AWS 서비스 둘 다 API에 대한 호출을 읽기 때문에 읽기 전용 이벤트는 소란스러울 수 있습니다. 그 결과, 읽기 전용 키워드는 신뢰할 수 없거나 감사와 관련이 없는 매우 많은 증거를 수집합니다. 읽기 전용 키워드에는`List`,`Describe`, `Get` API 호출 (예: Amazon S3의 ListBuckets경우) 이 포함됩니다. GetObject 증거 수집에 이러한 키워드 중 하나를 사용했다면 아무 작업도 수행할 필요가 없습니다. 키워드는 Audit Manager 콘솔 및 평가에서 자동으로 제거되었으며, 이러한 키워드에 대한 증거는 더 이상 수집하지 않습니다.

AWS Audit Manager 설정

언제든지 AWS Audit Manager의 설정을 검토하고 구성할 수 있습니다.

설정에 액세스하려면

1. https://console.aws.amazon.com/auditmanager/home 에서 AWS Audit Manager 콘솔을 엽니다.
2. 왼쪽 탐색 창에서 설정을 선택합니다.

다음 설정을 사용할 수 있습니다.

- 일반 설정
  - 권한
  - 데이터 암호화
  - 위임된 관리자(선택 사항)
  - AWS Config(선택 사항)
  - Security Hub (선택 사항)
  - AWS Audit Manager 비활성화
- 평가 설정
  - 기본 감사 소유자(선택 사항)
  - 평가 보고서 목적지(선택 사항)
  - 알림(선택 사항).
- 증거 찾기 설정
  - 증거 찾기(선택 사항)
  - 내보내기 대상(선택 사항)

일반 설정

일반 설정 탭은 Audit Manager 콘솔에 있는 설정 페이지의 기본 보기입니다. 이 탭을 사용하여 일반 Audit Manager 설정을 검토하고 업데이트할 수 있습니다.

주제

- 권한

- 데이터 암호화
- 위임된 관리자(선택 사항)
- AWS Config(선택 사항)
- Security Hub (선택 사항)
- AWS Audit Manager 비활성화

권한

AWS Audit Manager은(는) 서비스 연결 역할을 사용하여 사용자를 대신하여 데이터 소스에 연결합니다. 자세한 내용은 서비스 연결 역할 사용 AWS Audit Manager 섹션을 참조하세요.

Audit Manager가 사용하는 서비스 연결 역할의 세부 정보를 검토하려면 IAM 서비스 연결 역할 권한 보기를 선택합니다.

서비스 연결 역할에 대한 자세한 내용은 IAM 사용 설명서의 서비스 연결 역할 사용을 참조하세요

데이터 암호화

Audit Manager는 데이터의 안전한 저장을 위해 고유한 AWS 관리형 키를 자동으로 생성합니다. 기본적으로 Audit Manager 데이터는 이 KMS 키로 암호화됩니다. 또는 데이터 암호화 설정을 사용자 지정하려는 경우 자체 대칭 암호화 고객 관리 키를 지정할 수 있습니다. 자체 KMS 키를 사용하여 키 생성, 교체 및 비활성화 기능을 비롯한 다양한 작업을 수행할 수 있습니다.

> **Important**
>
> 평가 보고서를 생성하고 근거 찾기 검색 결과를 성공적으로 내보내려면 고객 관리 키(제공한 경우)가 AWS 리전 평가와 동일해야 합니다. Audit Manager 리전 목록은 Amazon Web Services 일반 참조에서 AWS Audit Manager 엔드포인트 및 할당량을 참조하세요.

Audit Manager 콘솔, AWS Command Line Interface(AWS CLI) 또는 Audit Manager API를 사용하여 데이터 암호화 설정을 업데이트할 수 있습니다.

Audit Manager console

데이터 암호화 설정을 업데이트하려면(콘솔)

1. 일반 설정 탭에서 데이터 암호화 섹션으로 이동합니다.

2. Audit Manager에서 제공하는 기본 KMS 키를 사용하려면 암호화 설정 사용자 지정(고급) 확인란의 선택을 취소하십시오.
3. 고객 관리형 키를 사용하려면 암호화 설정 사용자 지정(고급) 확인란을 선택합니다. 그런 다음 기존 KMS 키를 선택하거나 새로 만들 수 있습니다.

AWS CLI

데이터 암호화 설정을 업데이트하려면(AWS CLI)

update-settings 명령을 실행하고 `--kms-key` 파라미터를 사용하여 자체 고객 관리 키를 지정합니다.

다음 예에서는 각 *## ### ###*를 자신의 정보로 바꿉니다.

```
aws auditmanager update-settings --kms-key arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab
```

Audit Manager API

데이터 암호화 설정을 업데이트하려면(API)

UpdateSettings 작업을 호출하고 kmsKey 매개변수를 사용하여 자체 고객 관리 키를 지정합니다.

자세한 내용은 Audit Manager API 참조에서 이전 링크를 선택하여 자세한 내용을 읽어보세요. 여기에는 이 작업 및 매개변수를 언어별 AWS SDK 중 하나로 사용하는 방법에 대한 정보가 포함됩니다.

> **Note**
>
> Audit Manager 데이터 암호화 설정을 변경하면 새로 생성하는 모든 평가에 해당 변경 사항이 적용됩니다. 여기에는 새 평가에서 생성한 모든 평가 보고서 및 증거 찾기 내보내기가 포함됩니다.
> 암호화 설정을 변경하기 전에 생성한 기존 평가에는 변경 내용이 적용되지 않습니다. 여기에는 기존 평가 보고서 및 CSV 내보내기 외에도 기존 평가에서 생성한 새 평가 보고서 및 CSV 내보내기가 포함됩니다. 기존 평가와 모든 평가 보고서 및 CSV 내보내기는 기존 KMS 키를 계속 사용합니다.
> 평가 보고서를 생성하는 IAM ID가 이전 KMS 키를 사용할 수 없는 경우 키 정책 수준에서 권한을 부여하십시오. 지침은 AWS Key Management Service 개발자 안내서의 다른 계정의 사용자가 KMS 키를 사용하도록 허용을 참조하세요.

키 생성 방법에 대한 지침은 AWS Key Management Service 사용 설명서의 키 생성을 참조하십시오.

위임된 관리자(선택 사항)

AWS Organizations을 사용하고 Audit Manager에 대한 다중 계정 지원을 활성화하려는 경우 조직의 구성원 계정을 Audit Manager의 위임 관리자로 지정할 수 있습니다.

필수 조건

- 귀하의 계정이 조직의 일원이어야 합니다. 자세한 내용은 AWS Organizations 사용 설명서에서 조직 생성 및 관리를 참조하세요.
- 위임된 관리자를 지정하려면 먼저 조직의 모든 기능을 활성화해야 합니다. 또한 조직의 Security Hub 설정을 구성해야 합니다. 이렇게 하면 Audit Manager가 회원 계정에서 Security Hub 증거를 수집할 수 있습니다.
- 위임된 관리자 계정에는 Audit Manager를 설정할 때 제공한 KMS 키에 대한 액세스 권한이 있어야 합니다. 암호화 설정을 검토하고 변경하려면 데이터 암호화을 참조하십시오.

Audit Manager의 위임 관리자를 위한 중요 고려 사항

Audit Manager에서 위임된 관리자의 운영 방식을 정의하는 다음 요소에 유의하세요.

관리 계정 사용

Audit Manager에서는 AWS Organizations 관리 계정을 위임된 관리자로 사용할 수 없습니다.

여러 AWS 리전의 위임된 관리자 사용

둘 이상의 AWS 리전에서 Audit Manager를 활성화하려면 각 리전에서 위임된 관리자 계정을 별도로 지정해야 합니다. Audit Manager 설정에서는 모든 지역에서 동일한 위임 관리자 계정을 사용해야 합니다.

증거 찾기 정리 작업

관리 계정을 사용하여 위임된 관리자를 제거하거나 변경하기 전에 현재 위임된 관리자 계정이 Audit Manager에 로그인하고 증거 찾기를 비활성화하는지 확인하십시오. 증거 찾기를 비활성화하면 증거 찾기가 활성화되었을 때 계정에 생성된 이벤트 데이터 저장소가 자동으로 삭제됩니다.

이 작업이 완료되지 않은 경우 이벤트 데이터 저장소는 해당 계정에 남아 있습니다. 이 경우 원래 위임된 관리자가 CloudTrail Lake를 사용하여 이벤트 데이터 스토어를 수동으로 삭제하는 것이 좋습니다.

이 정리 작업은 이벤트 데이터 저장소가 여러 개 생성되지 않도록 하는 데 필요합니다. Audit Manager는 위임된 관리자 계정을 제거하거나 변경한 후 사용하지 않는 이벤트 데이터 저장소를 무시합니다. 하지만 사용하지 않는 이벤트 데이터 스토어를 삭제하지 않으면 이벤트 데이터 스토어에 CloudTrail Lake의 스토리지 비용이 계속 발생합니다.

데이터 삭제

Audit Manager의 위임된 관리자 계정을 제거해도 해당 계정의 데이터는 삭제되지 않습니다. 위임된 관리자 계정의 자원 데이터를 삭제하려면 계정을 제거하기 전에 해당 작업을 별도로 수행해야 합니다. 어느 쪽이든 Audit Manager 콘솔에서 이 작업을 수행할 수 있습니다. 또는 Audit Manager에서 제공하는 삭제 API 작업 중 하나를 사용할 수 있습니다. 사용 가능한 삭제 작업 목록은 Audit Manager 데이터 삭제를 참조하십시오.

현재 Audit Manager는 위임된 특정 관리자의 증거를 삭제하는 옵션을 제공하지 않습니다. 대신 관리 계정이 Audit Manager의 등록을 취소하면 등록 취소 시 현재 위임된 관리자 계정을 정리합니다.

Audit Manager의 일반적인 조직 및 위임된 관리자 문제에 대한 해결 방법은 위임된 관리자 및 AWS Organizations 문제 해결 섹션을 참조하세요.

Audit Manager에 대한 위임된 관리자 계정 관리

다음과 같이 위임된 관리자 계정 설정을 검토하고 변경할 수 있습니다.

위임된 관리자 추가

감사 관리자 콘솔, AWS Command Line Interface(AWS CLI) 또는 Audit Manager API를 사용하여 위임된 관리자를 추가할 수 있습니다.

> **Note**
>
> Audit Manager 설정에 위임된 관리자를 추가한 후에는 관리 계정이 더 이상 Audit Manager에서 추가 평가를 생성할 수 없습니다. 또한 관리 계정에서 생성한 기존 평가에 대한 증거 수집도 중지됩니다. Audit Manager는 조직의 평가를 관리하는 기본 계정인 위임된 관리자 계정에 증거를 수집하여 첨부합니다.

Audit Manager console

위임된 관리자를 추가하려면(콘솔)

1. 일반 설정 탭에서 위임된 관리자 섹션으로 이동합니다.

2. 위임된 관리자 계정 ID에서 위임된 관리자의 계정 ID를 입력합니다.
3. 위임(Delegate)을 선택합니다.

AWS CLI

위임된 관리자를 추가하려면(AWS CLI)

register-organization-admin-account 명령을 실행하고 `--admin-account-id` 매개 변수를 사용하여 위임된 관리자의 계정 ID를 지정합니다.

다음 예에서는 각 *## ### ###*를 자신의 정보로 바꿉니다.

```
aws auditmanager register-organization-admin-account --admin-account-id 111122223333
```

Audit Manager API

현재 위임된 관리자를 추가하려면(API)

RegisterOrganizationAdminAccount 작업을 호출하고 adminAccountId 매개 변수를 사용하여 위임된 관리자의 계정 ID를 지정합니다.

자세한 내용은 Audit Manager API 참조에서 이전 링크를 선택하여 자세한 내용을 읽어보세요. 여기에는 이 작업 및 매개변수를 언어별 AWS SDK 중 하나로 사용하는 방법에 대한 정보가 포함됩니다.

위임된 관리자 변경

Audit Manager 콘솔, AWS Command Line Interface(AWS CLI) 또는 Audit Manager API를 사용하여 위임된 관리자를 변경할 수 있습니다.

> **Warning**
>
> 위임된 관리자를 변경해도 이전의 위임된 관리자 계정으로 이전에 수집한 증거에 계속 액세스할 수 있습니다. 하지만 Audit Manager는 이전의 위임된 관리자 계정에 대한 증거 수집 및 첨부를 중단합니다.

Audit Manager console

현재 위임된 관리자를 변경하려면(콘솔)

1. (선택 사항) 현재 위임된 관리자(계정 A)가 증거 찾기를 활성화한 경우 다음 정리 작업을 수행하십시오.

   - 계정 B를 새로 위임된 관리자로 할당하기 전에 계정 A가 Audit Manager에 로그인하고 증거 찾기를 비활성화했는지 확인하십시오.

     증거 찾기를 비활성화하면 계정 A가 증거 찾기를 활성화했을 때 생성된 이벤트 데이터 저장소가 자동으로 삭제됩니다. 이 단계를 완료하지 않으면 계정 A는 CloudTrail Lake로 이동하여 이벤트 데이터 스토어를 수동으로 삭제해야 합니다. 그렇지 않으면 이벤트 데이터 스토어가 계정 A에 남아 있으며 CloudTrail Lake 스토리지 요금이 계속 발생합니다.
2. 일반 설정 탭에서 위임된 관리자 섹션으로 이동하여 제거를 선택합니다.
3. 표시되는 팝업 창에서 제거를 선택하여 확인합니다.
4. 위임된 관리자 계정 ID에 새로 위임된 관리자 계정의 ID를 입력합니다.
5. 위임(Delegate)을 선택합니다.

AWS CLI

시작하기 전에

현재 위임된 관리자(계정 A)가 증거 찾기를 활성화한 경우 다음 정리 작업을 수행하십시오.

계정 B를 새로 위임된 관리자로 할당하기 전에 계정 A가 Audit Manager에 로그인하고 증거 찾기를 비활성화했는지 확인하십시오.

증거 찾기를 비활성화하면 계정 A가 증거 찾기를 활성화했을 때 생성된 이벤트 데이터 저장소가 자동으로 삭제됩니다. 이 단계를 완료하지 않으면 계정 A는 CloudTrail Lake로 이동하여 이벤트 데이터 스토어를 수동으로 삭제해야 합니다. 그렇지 않으면 이벤트 데이터 스토어가 계정 A에 남아 있으며 CloudTrail Lake 스토리지 요금이 계속 발생합니다.

현재 위임된 관리자를 변경하려면(AWS CLI)

먼저 `--admin-account-id` 매개 변수를 사용하여 deregister-organization-admin-account 명령을 실행하여 현재 위임된 관리자의 계정 ID를 지정합니다.

다음 예에서는 각 *## ### ###*를 자신의 정보로 바꿉니다.

```
aws auditmanager deregister-organization-admin-account --admin-account-
id 111122223333
```

그런 다음 `--admin-account-id` 매개 변수를 사용하여 register-organization-admin-account 명령을 실행하여 새로 위임된 관리자의 계정 ID를 지정합니다.

다음 예에서는 각 *## ### ###*를 자신의 정보로 바꿉니다.

```
aws auditmanager register-organization-admin-account --admin-account-id 444455556666
```

Audit Manager API

시작하기 전에

현재 위임된 관리자(계정 A)가 증거 찾기를 활성화한 경우 다음 정리 작업을 수행하십시오.

계정 B를 새로 위임된 관리자로 할당하기 전에 계정 A가 Audit Manager에 로그인하고 증거 찾기를 비활성화했는지 확인하십시오.

증거 찾기를 비활성화하면 계정 A가 증거 찾기를 활성화했을 때 생성된 이벤트 데이터 저장소가 자동으로 삭제됩니다. 이 단계를 완료하지 않으면 계정 A는 CloudTrail Lake로 이동하여 이벤트 데이터 스토어를 수동으로 삭제해야 합니다. 그렇지 않으면 이벤트 데이터 스토어가 계정 A에 남아 있으며 CloudTrail Lake 스토리지 요금이 계속 발생합니다.

현재 위임된 관리자를 변경하려면(API)

먼저 DeregisterOrganizationAdminAccount 작업을 호출하고 AdminAccountId 매개 변수를 사용하여 현재 위임된 관리자의 계정 ID를 지정합니다.

그런 다음 RegisterOrganizationAdminAccount 작업을 호출하고 adminAccountId 매개 변수를 사용하여 위임된 새 관리자의 계정 ID를 지정합니다.

자세한 내용은 Audit Manager API 참조에서 이전 링크를 선택하여 자세한 내용을 읽어보세요. 여기에는 이 작업 및 매개변수를 언어별 AWS SDK 중 하나로 사용하는 방법에 대한 정보가 포함됩니다.

위임된 관리자 제거

Audit Manager 콘솔, AWS Command Line Interface(AWS CLI) 또는 Audit Manager API를 사용하여 위임된 관리자를 제거할 수 있습니다.

> **Warning**
>
> 위임된 관리자를 제거해도 해당 위임된 관리자 계정으로 이전에 수집한 증거에 계속 액세스할 수 있습니다. 하지만 Audit Manager는 이전의 위임된 관리자 계정에 대한 증거 수집 및 첨부를 중단합니다.

Audit Manager console

현재 위임된 관리자를 제거하려면(콘솔)

1. (선택 사항) 현재 위임된 관리자가 증거 찾기를 활성화한 경우 다음 정리 작업을 수행하십시오.
   - 현재 위임된 관리자 계정이 Audit Manager에 로그인하고 증거 찾기를 비활성화하는지 확인하십시오.

     증거 찾기를 비활성화하면 증거 찾기를 활성화했을 때 계정에 생성된 이벤트 데이터 저장소가 자동으로 삭제됩니다. 이 단계를 완료하지 않은 경우 위임된 관리자 계정이 CloudTrail Lake를 사용하여 이벤트 데이터 스토어를 수동으로 삭제해야 합니다. 그렇지 않으면 이벤트 데이터 스토어가 해당 계정에 남아 CloudTrail Lake 스토리지 요금이 계속 발생합니다.
2. 일반 설정 탭에서 위임된 관리자 섹션으로 이동하여 제거를 선택합니다.
3. 표시되는 팝업 창에서 제거를 선택하여 확인합니다.

AWS CLI

시작하기 전에

현재 위임된 관리자가 증거 찾기를 활성화한 경우 다음 정리 작업을 수행하십시오.

현재 위임된 관리자 계정이 Audit Manager에 로그인하고 증거 찾기를 비활성화하는지 확인하십시오.

증거 찾기를 비활성화하면 증거 찾기를 활성화했을 때 계정에 생성된 이벤트 데이터 저장소가 자동으로 삭제됩니다. 이 단계를 완료하지 않은 경우 위임된 관리자 계정이 CloudTrail Lake를 사용하여 이벤트 데이터 스토어를 수동으로 삭제해야 합니다. 그렇지 않으면 이벤트 데이터 스토어가 해당 계정에 남아 CloudTrail Lake 스토리지 요금이 계속 발생합니다.

현재 위임된 관리자를 제거하려면(AWS CLI)

deregister-organization-admin-account 명령을 실행하고 `--admin-account-id` 매개 변수를 사용하여 위임된 관리자의 계정 ID를 지정합니다.

다음 예에서는 각 *## ### ###*를 자신의 정보로 바꿉니다.

```
aws auditmanager deregister-organization-admin-account --admin-account-
id 111122223333
```

Audit Manager API

시작하기 전에

현재 위임된 관리자가 증거 찾기를 활성화한 경우 다음 정리 작업을 수행하십시오.

현재 위임된 관리자 계정이 Audit Manager에 로그인하고 증거 찾기를 비활성화하는지 확인하십시오.

증거 찾기를 비활성화하면 증거 찾기를 활성화했을 때 계정에 생성된 이벤트 데이터 저장소가 자동으로 삭제됩니다. 이 단계를 완료하지 않은 경우 위임된 관리자 계정이 CloudTrail Lake를 사용하여 이벤트 데이터 스토어를 수동으로 삭제해야 합니다. 그렇지 않으면 이벤트 데이터 스토어가 해당 계정에 남아 CloudTrail Lake 스토리지 요금이 계속 발생합니다.

현재 위임된 관리자를 제거하려면(API)

DeregisterOrganizationAdminAccount 작업을 호출하고 AdminAccountId 매개 변수를 사용하여 위임된 관리자의 계정 ID를 지정합니다.

자세한 내용은 Audit Manager API 참조에서 이전 링크를 선택하여 자세한 내용을 읽어보세요. 여기에는 이 작업 및 매개변수를 언어별 AWS SDK 중 하나로 사용하는 방법에 대한 정보가 포함됩니다.

AWS Config(선택 사항)

Audit Manager가 AWS Config에서 조사 결과를 수집하도록 허용할 수 있습니다. AWS Config가 활성화되면 Audit Manager는 규칙 검사 결과를 AWS Config에서 직접 보고하여 리소스 보안 상태의 스냅샷을 캡처할 수 있습니다. Audit Manager에서 최적의 경험을 위해 AWS Config을 활성화하는 것이 좋습니다.

AWS Config을 활성화하려면 AWS Config 활성화를 선택하여 해당 서비스로 이동하십시오. AWS Config을 활성화하는 방법에 대한 지침은 AWS Config 개발자 안내서의 AWS Config 설정을 참조하십시오.

Security Hub (선택 사항)

Audit Manager가 지원되는 규정 준수 표준에 대한 AWS Security Hub 결과를 가져오도록 허용할 수 있습니다. Security Hub가 활성화되면 Audit Manager는 보안 검사 결과를 바탕으로 Security Hub에서 직접 리소스 보안 상태의 스냅샷을 캡처할 수 있습니다. Audit Manager에서 최적의 경험을 위해 Security Hub를 활성화하는 것이 좋습니다.

Security Hub를 활성화하려면 Security Hub 활성화를 선택하여 해당 서비스로 이동하십시오. Security Hub를 활성화하는 방법에 대한 자세한 내용은 Security Hub 사용 설명서의 AWS Security Hub 설정을 참조하세요.

AWS Audit Manager 비활성화

더 이상 서비스를 사용하지 않으려는 경우 Audit Manager를 비활성화할 수 있습니다. Audit Manager를 비활성화하면 모든 데이터를 삭제할 수도 있습니다.

기본적으로 Audit Manager를 비활성화해도 데이터는 삭제되지 않습니다. 증거 데이터는 생성 시점부터 2년간 보관됩니다. 평가, 사용자 지정 제어, 사용자 지정 프레임워크 등 기타 Audit Manager 리소스는 무기한 보존되며, 나중에 Audit Manager를 다시 활성화하면 사용할 수 있습니다. 데이터 보존에 대한 자세한 내용은 이 가이드의 데이터 보호를 참조하십시오.

데이터를 삭제하기로 선택하면 Audit Manager는 생성한 모든 Audit Manager 리소스(평가, 사용자 지정 제어, 사용자 지정 프레임워크 포함)와 함께 모든 증거 데이터를 삭제합니다. Audit Manager를 비활성화한 후 7일 이내에 모든 데이터가 삭제됩니다.

> **Warning**
>
> - Audit Manager를 비활성화하면 액세스 권한이 취소되고 서비스에서 더 이상 기존 평가에 대한 증거를 수집하지 않습니다. Audit Manager를 다시 활성화하지 않으면 서비스의 어떤 항목에도 액세스할 수 없습니다.
> - 모든 데이터 삭제는 영구적인 작업입니다. 나중에 Audit Manager를 다시 활성화하기로 결정하더라도 데이터를 복구할 수 없습니다.

Audit Manager 콘솔, AWS Command Line Interface(AWS CLI) 또는 Audit Manager API를 사용하여 Audit Manager를 비활성화할 수 있습니다.

Audit Manager console

Audit Manager를 비활성화하려면(콘솔)

1. 일반 설정 탭에서 AWS Audit Manager 비활성화 섹션으로 이동합니다.
2. 비활성화를 선택합니다.
3. 팝업 창에서 현재 데이터 보존 설정을 검토하십시오.

    a. 현재 선택을 계속하려면 Audit Manager 비활성화를 선택합니다.

    b. 현재 선택을 변경하려면 다음 단계를 수행합니다.

        i. 취소를 선택하여 설정 페이지로 돌아갑니다.

        ii. 기본 데이터 보존 설정을 사용하려면 모든 데이터 삭제를 끕니다. 이 선택은 생성 시점으로부터 2년간 증거 데이터를 보존하고 다른 Audit Manager 리소스는 무기한 보존합니다.

        iii. 데이터를 삭제하려면 모든 데이터 삭제를 켜십시오.

        iv. 비활성화를 선택한 다음 Audit Manager 비활성화를 선택하여 선택을 확인합니다.

AWS CLI

시작하기 전에

Audit Manager를 비활성화하기 전에 update-settings 명령을 실행하여 기본 데이터 보존 정책을 설정할 수 있습니다. 기본적으로 Audit Manager는 데이터를 보관합니다. 데이터 삭제를 요청하려면 `deleteResources` 값이 `ALL`로 설정된 상태에서 `--deregistration-policy` 매개변수를 사용하십시오.

```
aws auditmanager update-settings --deregistration-policy deleteResources=ALL
```

Audit Manager(AWS CLI)를 비활성화하려면

Audit Manager를 비활성화할 준비가 되면 deregister-account 명령을 실행합니다.

```
aws auditmanager deregister-account
```

Audit Manager API

시작하기 전에

Audit Manager를 비활성화하기 전에 UpdateSettings API 작업을 사용하여 기본 데이터 보존 정책을 설정할 수 있습니다. 기본적으로 Audit Manager는 데이터를 보관합니다. 데이터를 삭제하려는 경우 DeRegistrationPolicy 속성을 사용하여 데이터 삭제를 요청할 수 있습니다.

Audit Manager(API)를 비활성화하려면

Audit Manager를 비활성화할 준비가 되면 DeregisterAccount 작업을 호출하십시오.

자세한 내용은 Audit Manager API 참조에서 이전 링크를 선택하여 자세한 내용을 읽어보세요. 여기에는 이러한 작업 및 파라미터를 언어별 AWS SDK 중 하나로 사용하는 방법에 대한 정보가 포함됩니다.

Audit Manager를 비활성화한 후 다시 활성화하려면

Audit Manager 서비스 홈페이지로 이동하여 단계에 따라 Audit Manager를 새 사용자로 설정합니다. 자세한 내용은 AWS Audit Manager 설정 섹션을 참조하세요.

> **Tip**
>
> - Audit Manager를 비활성화했을 때 데이터를 삭제하기로 선택한 경우 데이터가 삭제될 때까지 기다려야 서비스를 다시 활성화할 수 있습니다. 보유한 데이터 양에 따라 최대 7일이 소요될 수 있습니다. 하지만 그 전에 Audit Manager를 다시 활성화해 보세요. 대부분의 경우 데이터는 1시간 이내에 삭제됩니다.
> - Audit Manager를 비활성화했을 때 데이터를 삭제하지 않기로 선택한 경우 기존 평가가 휴면 상태로 전환되어 결과적으로 증거 수집이 중단되었습니다. 기존 평가에 대한 증거 수집을 다시 시작하려면 평가를 편집하고 변경 없이 저장을 선택합니다.

평가 설정

이 탭을 사용하여 평가 설정을 검토하고 업데이트할 수 있습니다.

주제

- 기본 감사 소유자(선택 사항)
- 평가 보고서 목적지(선택 사항)
- 알림(선택 사항).

기본 감사 소유자(선택 사항)

Audit Manager에서 평가에 대한 기본 액세스 권한을 가진 기본 감사 소유자를 지정할 수 있습니다.

Audit Manager 콘솔, AWS Command Line Interface(AWS CLI) 또는 Audit Manager API를 사용하여 이 설정을 업데이트할 수 있습니다.

Audit Manager console

표에 나열된 AWS 계정 항목 중에서 선택하거나 검색 창을 사용하여 다른 AWS 계정 항목을 찾을 수 있습니다.

기본 감사 소유자 설정을 업데이트하려면(콘솔)

1. 평가 설정 탭에서 기본 감사 소유자 섹션으로 이동한 다음 편집을 선택합니다.
2. 기본 감사 소유자를 추가하려면 감사 소유자 아래 계정 이름 옆에 있는 확인란을 선택합니다.
3. 기본 감사 소유자를 제거하려면 감사 소유자 아래 계정 이름 옆에 있는 확인란을 선택 취소합니다.
4. 완료되면 저장을 선택합니다.

AWS CLI

기본 감사 소유자 설정을 업데이트하려면(AWS CLI)

update-settings 명령을 실행하고 `--default-process-owners` 파라미터를 사용하여 감사 소유자를 지정합니다.

다음 예에서는 각 *## ### ###*를 자신의 정보로 바꿉니다. 단, `roleType`만 `PROCESS_OWNER`일 수 있습니다.

```
aws auditmanager update-settings --default-process-owners
 roleType=PROCESS_OWNER,roleArn=arn:aws:iam::111122223333:role/Administrator
```

Audit Manager API

기본 감사 소유자 설정을 업데이트하려면(API)

UpdateSettings 작업을 호출하고 defaultProcessOwners 매개변수를 사용하여 기본 감사 소유자를 지정합니다. 단, `roleType`만 `PROCESS_OWNER`일 수 있습니다.

감사 소유자에 대한 자세한 내용은 이 가이드의 개념 및 용어 섹션에서 감사 소유자를 참조하십시오.

평가 보고서 목적지(선택 사항)

평가 보고서를 생성할 때 Audit Manager는 보고서를 선택한 S3 버킷에 게시합니다. 이 S3 버킷을 평가 보고서 목적지라고 합니다. Audit Manager에서 평가 보고서를 저장하는 Amazon S3 버킷을 선택할 수 있습니다.

Audit Manager 콘솔, AWS Command Line Interface(AWS CLI) 또는 Audit Manager API를 사용하여 이 설정을 업데이트할 수 있습니다.

Audit Manager console

평가 보고서 목적지 설정을 업데이트하려면(콘솔)

1. 평가 설정 탭에서 평가 보고서 목적지 섹션으로 이동합니다.
2. 기존 Amazon S3 버킷을 사용하려면 드롭다운 메뉴에서 버킷 이름을 선택합니다.
3. 새 Amazon S3버킷을 만들려면 새 버킷 만들기를 선택합니다.
4. 완료되면 저장을 선택합니다.

AWS CLI

평가 보고서 대상 설정을 업데이트하려면(AWS CLI)

update-settings 명령을 실행하고 `--default-assessment-reports-destination` 파라미터를 사용하여 S3 버킷을 지정합니다.

다음 예에서는 각 *## ### ###*를 자신의 정보로 바꿉니다.

```
aws auditmanager update-settings --default-assessment-reports-destination
 destinationType=S3,destination=s3://doc-example-destination-bucket
```

Audit Manager API

평가 보고서 대상 설정을 업데이트하려면(API)

UpdateSettings 작업을 호출하고 defaultAssessmentReportsDestination 파라미터를 사용하여 S3 버킷을 지정합니다.

S3 버킷을 생성하는 방법에 대한 지침은 Amazon S3 사용 설명서의 버킷 생성을 참조하십시오.

평가 보고서 목적지의 구성 팁

평가 보고서를 성공적으로 생성하려면 평가 보고서 대상의 다음 구성을 확인하는 것이 좋습니다.

동일 리전 버킷

AWS 리전 평가와 동일한 S3 버킷을 사용하는 것이 좋습니다. 동일 리전 버킷과 평가를 사용하는 경우 평가 보고서에는 최대 22,000개의 증거 항목이 포함될 수 있습니다. 반대로, 리전 간 버킷 및 평가를 사용하는 경우 3,500개의 근거 항목만 포함할 수 있습니다.

AWS 리전

고객 관리 키 AWS 리전(제공한 경우)의 크기는 평가 리전 및 평가 보고서 대상 S3 버킷과 일치해야 합니다. KMS 키를 변경하는 방법에 대한 지침은 AWS Audit Manager 설정, 데이터 암호화를 참조하세요. S3 버킷을 변경하는 방법에 대한 지침은 AWS Audit Manager 설정, 평가 보고서 대상을 참조하세요. 지원되는 Audit Manager 리전 목록은 Amazon Web Services 일반 참조의 AWS Audit Manager 엔드포인트 및 할당량을 참조하세요.

S3 버킷 암호화

평가 보고서 대상에 SSE-KMS를 사용한 서버 측 암호화(SSE)를 요구하는 버킷 정책이 있는 경우 해당 버킷 정책에 사용되는 KMS 키는 Audit Manager 데이터 암호화 설정에서 구성한 KMS 키와 일치해야 합니다. Audit Manager 설정에서 KMS 키를 구성하지 않았고 평가 보고서 대상 버킷 정책에 SSE가 필요한 경우, 버킷 정책에서 SSE-S3를 허용하는지 확인하세요. 데이터 암호화에 사용되는 KMS 키를 구성하는 방법에 대한 지침은 데이터 암호화 설정을 참조하십시오.

계정 간 S3 버킷

계정 간 S3 버킷을 평가 보고서 대상으로 사용하는 것은 Audit Manager 콘솔에서 지원되지 않습니다. AWS CLI또는 AWS SDK 중 하나를 사용하여 계정 간 버킷을 평가 보고서 대상으로 지정할 수 있지만, 단순화를 위해 이렇게 하지 않는 것이 좋습니다. 계정 간 S3 버킷을 평가 보고서 대상으로 사용하기로 선택한 경우 다음 사항을 고려하십시오.

- 기본적으로 평가 보고서와 같은 S3 객체는 객체를 업로드한 AWS 계정이 소유합니다. S3 객체 소유권 설정을 사용하여 미리 준비된 `bucket-owner-full-control` 액세스 제어 목록(ACL)을 포함하여 계정에서 작성한 새 객체를 버킷 소유자가 자동으로 소유하게 되도록 이 기본 동작을 변경할 수 있습니다.

  필수 사항은 아니지만 계정 간 버킷 설정을 다음과 같이 변경하는 것이 좋습니다. 이렇게 변경하면 버킷에 게시한 평가 보고서를 버킷 소유자가 완전히 제어할 수 있습니다.

  - S3 버킷의 객체 소유권을 기본 객체 작성자 대신 버킷 소유자 선호로 설정합니다.

- 해당 버킷에 업로드된 객체에 `bucket-owner-full-control` ACL이 적용되도록 버킷 정책을 추가합니다.

- Audit Manager가 계정 간 S3 버킷에 보고서를 게시하도록 허용하려면 평가 보고서 대상에 다음 S3 버킷 정책을 추가해야 합니다. 각 *## ### ## ###*를 사용자의 정보로 바꿉니다. 이 정책의 `Principal` 요소는 평가를 소유하고 평가 보고서를 생성하는 사용자 또는 역할입니다. `Resource`는 보고서가 게시되는 계정 간 S3 버킷을 지정합니다.

```
{
  "Version": "2012-10-17",
  "Statement": [
      {
          "Sid": "Allow cross account assessment report publishing",
          "Effect": "Allow",
          "Principal": {
              "AWS":
 "arn:aws:iam::AssessmentOwnerAccountId:user/AssessmentOwnerUserName"
          },
          "Action": [
              "s3:ListBucket",
              "s3:PutObject",
              "s3:GetObject",
              "s3:GetBucketLocation",
              "s3:PutObjectAcl",
              "s3:DeleteObject"
          ],
          "Resource": [
              "arn:aws:s3:::CROSS-ACCOUNT-BUCKET",
              "arn:aws:s3:::CROSS-ACCOUNT-BUCKET/*"
          ]
      }
  ]
}
```

알림(선택 사항).

Audit Manager는 이 설정에서 지정한 Amazon SNS 주제에 알림을 보낼 수 있습니다. 해당 SNS 주제를 구독한 경우 Audit Manager에 로그인하면 알림을 받게 됩니다.

Audit Manager 콘솔, AWS Command Line Interface(AWS CLI) 또는 Audit Manager API를 사용하여 이 설정을 업데이트할 수 있습니다.

Audit Manager console

알림 설정을 업데이트하려면(콘솔)

1. 평가 설정 탭에서 알림 섹션으로 이동합니다.
2. 기존 SNS 주제를 사용하려면 드롭다운 메뉴에서 주제 이름을 선택합니다.
3. 새 SNS 주제를 생성하려면 새 주제 생성을 선택합니다.
4. 완료되면 저장을 선택합니다.

AWS CLI

푸시 알림 설정을 업데이트하려면(AWS CLI)

update-settings 명령을 실행하고 `--sns-topic` 파라미터를 사용하여 SNS 주제를 지정합니다.

다음 예에서는 각 *## ### ###*를 자신의 정보로 바꿉니다.

```
aws auditmanager update-settings --sns-topic arn:aws:sns:us-east-1:111122223333:my-assessment-topic
```

Audit Manager API

알림 설정을 업데이트하려면(API)

UpdateSettings 작업을 호출하고 snsTopic 매개 변수를 사용하여 SNS 주제를 지정합니다.

> **Note**
>
> 표준 SNS 주제 또는 FIFO (선입선출) SNS 주제를 사용할 수 있습니다. Audit Manager는 FIFO 주제에 대한 알림 전송을 지원하지만 메시지가 전송되는 순서는 보장되지 않습니다.
> 현재 가지고 있지 않은 Amazon SNS 주제를 사용하려면 AWS Identity and Access Management (IAM)정책을 구성해야 합니다. 보다 구체적으로 설명하면 주제의 Amazon 리소스 이름(ARN)에서 게시를 허용하도록 구성해야 합니다. IAM에 대한 자세한 내용은 AWS Audit Manager의 자격 증명 및 액세스 관리을 참조하십시오.

Audit Manager에서 알림을 호출하는 작업 목록에 대한 자세한 내용은 AWS Audit Manager의 알림을 참조하십시오.

Amazon SNS 주제를 생성하는 방법에 대한 지침은 Amazon SNS 사용 설명서의 Amazon SNS 주제 생성을 참조하십시오.

증거 찾기 설정

이 탭을 사용하여 증거 찾기 설정을 검토하고 업데이트할 수 있습니다.

주제

- 증거 찾기(선택 사항)
- 내보내기 대상(선택 사항)

증거 찾기(선택 사항)

증거 찾기를 활성화할 것을 적극 권장합니다. 증거에 대한 검색 쿼리를 실행하려면 이 기능을 활성화해야 합니다.

증거 찾기의 상태를 활성화, 비활성화 또는 확인하려면 다음 단계를 따르십시오.

증거 찾기를 활성화하십시오.

증거를 검색하려는 각 AWS 리전에서 증거 찾기를 활성화해야 합니다. Audit Manager의 위임 관리자인 경우 증거 찾기를 활성화하여 조직의 모든 구성원 계정에 대한 증거를 검색하십시오.

증거 찾기를 활성화하는 데 필요한 권한

증거 찾기를 활성화하려면 CloudTrail Lake에서 이벤트 데이터 스토어를 생성하고 관리할 수 있는 권한이 필요합니다. 이 기능을 사용하려면 CloudTrail Lake 쿼리를 수행할 수 있는 권한이 필요합니다. 사용할 수 있는 권한 정책의 예는 전체 관리자 액세스 허용을 참조하십시오.

권한 관련 도움이 필요한 경우 AWS 관리자에게 문의하세요. 귀하가 AWS 관리자인 경우 필요한 권한 설명을 복사하여 IAM 정책에 첨부할 수 있습니다.

증거 찾기 활성화 요청

Audit Manager 콘솔, AWS Command Line Interface(AWS CLI) 또는 Audit Manager API를 사용하여 이 작업을 완료할 수 있습니다.

Audit Manager console

증거 찾기를 활성화하도록 요청하려면(콘솔)

1. https://console.aws.amazon.com/auditmanager/home에서 AWS Audit Manager 콘솔을 엽니다.
2. 증거 찾기 설정 탭에서 증거 찾기 섹션으로 이동합니다.
3. 필수 권한 정책을 선택한 다음 CloudTrail Lake 권한 보기를 선택하여 필요한 증거 찾기 권한을 확인합니다. 이러한 권한이 아직 없는 경우 이 정책 설명을 복사하여 IAM 정책에 첨부할 수 있습니다.
4. 활성화를 선택합니다.
5. 팝업 창에서 요청 활성화를 선택합니다.

AWS CLI

증거 찾기 활성화를 요청하려면(AWS CLI)

`--evidence-finder-enabled` 파라미터와 함께 update-settings 명령을 실행합니다.

```
aws auditmanager update-settings --evidence-finder-enabled
```

Audit Manager API

증거 찾기(API) 활성화를 요청하려면

UpdateSettings 작업을 호출하고 evidenceFinderEnabled 매개변수를 사용하십시오.

자세한 내용은 Audit Manager API 참조에서 이전 링크를 선택하여 자세한 내용을 읽어보세요. 여기에는 이 작업 및 매개변수를 언어별 AWS SDK 중 하나로 사용하는 방법에 대한 정보가 포함됩니다.

증거 찾기 상태 확인

요청을 제출한 후 증거 찾기를 활성화하고 이벤트 데이터 저장소를 생성하는 데 최대 10분이 소요됩니다. 이벤트 데이터 저장소가 생성되자마자 앞으로 모든 새로운 증거가 이벤트 데이터 저장소에 수집됩니다.

증거 찾기가 활성화되고 이벤트 데이터 저장소가 생성되면 새로 생성된 이벤트 데이터 저장소를 최대 2년 분량의 과거 증거로 채웁니다. 이 프로세스는 자동으로 진행되며 완료하는 데 최대 7일이 소요됩니다.

Audit Manager 콘솔, AWS CLI, 또는 Audit Manager API를 사용하여 증거 찾기의 현재 상태를 확인할 수 있습니다.

Audit Manager console

증거 찾기의 현재 상태를 보려면(콘솔)

1. https://console.aws.amazon.com/auditmanager/home 에서 AWS Audit Manager 콘솔을 엽니다.
2. 왼쪽 탐색 창에서 설정을 선택합니다.
3. 증거 찾기 활성화 — 선택 사항에서 현재 상태를 검토하십시오.

   각 상태는 다음과 같이 정의됩니다.

   - 증거 찾기가 활성화되지 않았습니다. — 아직 증거 찾기를 성공적으로 활성화하지 않았습니다.
   - 증거 찾기를 활성화하도록 요청했습니다. — 요청은 이벤트 데이터 저장소가 생성될 때까지 보류 중입니다.
   - 증거 찾기가 활성화되었습니다 — 이벤트 데이터 저장소가 생성되었습니다. 이제 증거 찾기를 사용할 수 있습니다.

     보유한 증거의 양에 따라 새 이벤트 데이터 저장소를 과거 증거 데이터로 채우는 데 최대 7일이 걸립니다. 파란색 정보 패널은 데이터 채우기가 진행 중임을 나타냅니다. 그동안은 언제든지 증거 찾기를 탐색해 보세요. 하지만 채우기가 완료될 때까지 모든 데이터를 사용할 수 있는 것은 아니라는 점을 명심하세요.
   - 증거 찾기를 비활성화하도록 요청했습니다. — 요청은 이벤트 데이터 저장소가 삭제될 때까지 보류 중입니다.
   - 증거 찾기가 비활성화되었습니다. — 증거 찾기가 영구적으로 비활성화되었으며 이벤트 데이터 저장소가 삭제되었습니다.

AWS CLI

증거 찾기의 현재 상태를 보려면(AWS CLI)

`--attribute` 파라미터를 `EVIDENCE_FINDER_ENABLEMENT`로 설정한 상태에서 get-settings 명령을 실행합니다.

```
aws auditmanager get-settings --attribute EVIDENCE_FINDER_ENABLEMENT
```

이것은 다음 정보를 반환합니다.

enablementStatus

이 속성은 증거 찾기의 현재 상태를 보여줍니다.

- ENABLE_IN_PROGRESS— 증거 찾기를 활성화하도록 요청하셨습니다. 현재 증거 찾기 쿼리를 지원하기 위해 이벤트 데이터 저장소가 생성되고 있습니다.
- ENABLED— 이벤트 데이터 저장소가 생성되었으며 증거 찾기가 활성화되었습니다. 이벤트 데이터 저장소에 과거 증거 데이터가 채워질 때까지 7일을 기다리는 것이 좋습니다. 그 동안에는 증거 찾기를 사용할 수 있지만 채우기가 완료될 때까지 모든 데이터를 사용할 수 있는 것은 아닙니다.
- DISABLE_IN_PROGRESS— 증거 찾기를 비활성화하도록 요청했는데 요청이 이벤트 데이터 저장소가 삭제될 때까지 보류 중입니다.
- DISABLED— 증거 찾기를 영구적으로 비활성화하면 이벤트 데이터 저장소가 삭제됩니다. 이 시점 이후에는 증거 찾기를 다시 활성화할 수 없습니다.

backfillStatus

이 속성은 증거 데이터 채우기의 현재 상태를 보여줍니다.

- NOT_STARTED— 채우기가 아직 시작되지 않았습니다.
- IN_PROGRESS— 채우기가 진행 중입니다. 증거 데이터의 양에 따라 완료하는 데 최대 7일이 소요됩니다.
- COMPLETED— 채우기가 완료되었습니다. 이제 과거의 모든 증거를 조회할 수 있습니다.

Audit Manager API

증거 찾기(API)의 현재 상태를 보려면

`attribute` 매개변수를 `EVIDENCE_FINDER_ENABLEMENT`로 설정한 상태에서 GetSettings 작업을 호출합니다. 이것은 다음 정보를 반환합니다.

enablementStatus

이 속성은 증거 찾기의 현재 상태를 보여줍니다.

- ENABLE_IN_PROGRESS- 증거 찾기를 활성화하도록 요청하셨습니다. 현재 증거 찾기 쿼리를 지원하기 위해 이벤트 데이터 저장소가 생성되고 있습니다.

- ENABLED- 이벤트 데이터 저장소가 생성되었으며 증거 찾기가 활성화되었습니다. 이벤트 데이터 저장소에 과거 증거 데이터가 채워질 때까지 7일을 기다리는 것이 좋습니다. 그 동안에는 증거 찾기를 사용할 수 있지만 채우기가 완료될 때까지 모든 데이터를 사용할 수 있는 것은 아닙니다.
- DISABLE_IN_PROGRESS- 증거 찾기를 비활성화하도록 요청했는데 요청이 이벤트 데이터 저장소 삭제를 보류 중입니다.
- DISABLED- 증거 찾기를 영구적으로 비활성화하면 이벤트 데이터 저장소가 삭제됩니다. 이 시점 이후에는 증거 찾기를 다시 활성화할 수 없습니다.

backfillStatus

이 속성은 증거 데이터 채우기의 현재 상태를 보여줍니다.

- NOT_STARTED은 채우기가 아직 시작되지 않았음을 의미합니다.
- IN_PROGRESS은 채우기가 진행 중임을 의미합니다. 증거 데이터의 양에 따라 완료하는 데 최대 7일이 소요됩니다.
- COMPLETED은 채우기가 완료되었음을 의미합니다. 이제 과거의 모든 증거를 조회할 수 있습니다.

자세한 내용은 Audit Manager API 참조의 evidenceFinderEnablement를 참조하십시오.

증거 찾기를 비활성화하십시오.

더 이상 증거 찾기를 사용하지 않으려는 경우 언제든지 비활성화할 수 있습니다.

> **Warning**
>
> 증거 찾기를 비활성화하면 Audit Manager가 생성한 CloudTrail Lake 이벤트 데이터 스토어가 삭제됩니다. 따라서 이 기능을 다시 활성화할 수 없습니다. 증거 찾기를 비활성화한 후 다시 사용하려면 서비스를 AWS Audit Manager비활성화했다가 다시 완전히 활성화해야 합니다.

증거 찾기를 비활성화하는 데 필요한 권한

증거 찾기를 비활성화하려면 CloudTrail Lake의 이벤트 데이터 스토어를 삭제할 수 있는 권한이 필요합니다. 사용할 수 있는 예제 정책은 증거 찾기를 비활성화할 수 있는 권한을 참조하십시오.

권한 관련 도움이 필요한 경우 AWS 관리자에게 문의하세요. AWS 관리자인 경우 필요한 권한 설명을 IAM 정책에 첨부할 수 있습니다.

증거 찾기 비활성화

Audit Manager 콘솔, AWS Command Line Interface(AWS CLI) 또는 Audit Manager API를 사용하여 이 작업을 완료할 수 있습니다.

Audit Manager console

증거 찾기를 비활성화하려면(콘솔)

1. Audit Manager 설정 페이지의 증거 찾기 섹션에서 비활성화를 선택합니다.
2. 표시되는 팝업 창에서 **Yes**를 입력하여 결정을 확인합니다.
3. 요청을 선택하여 비활성화합니다.

AWS CLI

증거 찾기를 비활성화하려면(AWS CLI)

`--no-evidence-finder-enabled` 파라미터와 함께 update-settings 명령을 실행합니다.

```
aws auditmanager update-settings --no-evidence-finder-enabled
```

Audit Manager API

증거 찾기(API)를 비활성화하려면

UpdateSettings 작업을 호출하고 evidenceFinderEnabled 매개변수를 사용하십시오.

자세한 내용은 Audit Manager API 참조에서 이전 링크를 선택하여 자세한 내용을 읽어보세요. 여기에는 이 작업 및 매개변수를 언어별 AWS SDK 중 하나로 사용하는 방법에 대한 정보가 포함됩니다.

내보내기 대상(선택 사항)

증거 찾기에서 쿼리를 실행하면 검색 결과를 CSV(쉼표로 구분된 값) 파일로 내보낼 수 있습니다. 이 설정을 사용하여 Audit Manager가 내보낸 파일을 저장하는 기본 S3 버킷을 선택할 수 있습니다.

Audit Manager 콘솔, AWS Command Line Interface(AWS CLI) 또는 Audit Manager API를 사용하여 이 설정을 업데이트할 수 있습니다.

> **Important**
>
> S3 버킷에는 CloudTrail이 내보내기 파일을 쓸 수 있도록 허용하는 데 필요한 권한 정책이 있어야 합니다. 구체적으로 말하자면, 버킷 정책에는 `s3:PutObject` 작업과 버킷 ARN이 포함되어야 하고 CloudTrail이 서비스 보안 주체로 나열되어 있어야 합니다. 사용할 수 있는 권한 정책 예시를 제공합니다. 이 정책을 S3 버킷에 연결하는 방법에 대한 지침은 Amazon S3 콘솔을 이용한 버킷 정책 추가를 참조하십시오.
> 추가 팁은 이 페이지의 내보내기 목적지에 대한 구성 팁을 참조하십시오.

Audit Manager console

내보내기 목적지 설정을 업데이트하려면(콘솔)

1. 증거 찾기 설정 탭에서 목적지 내보내기 섹션으로 이동합니다.
2. 다음 옵션 중 하나를 선택합니다.
   - 현재 S3 버킷을 제거하려면 제거를 선택하여 설정을 지우십시오.
   - 기본 S3 버킷을 처음으로 저장하려면 3단계로 진행하십시오.
3. 내보낸 파일을 저장할 S3 버킷을 지정합니다.
   - Browse S3를 선택하여 버킷 목록에서 선택하십시오.
   - 또는 **`s3://bucketname/prefix`** 형식으로 버킷 URI를 입력할 수 있습니다.

   > **Tip**
   >
   > 대상 버킷을 체계적으로 정리하려면 CSV 내보내기를 위한 선택적 폴더를 만들 수 있습니다. 그렇게 하려면, 리소스 URI 상자의 값에 슬래시(**/**)와 접두사를 추가합니다(예: **`/evidenceFinderCSVExports`**). 그러면 Audit Manager가 CSV 파일을 버킷에 추가할 때 이 접두사를 포함시키고, Amazon S3는 접두사로 지정된 경로를 생성합니다. Amazon S3의 접두사에 대한 자세한 내용은 Amazon Simple Storage Service 사용 설명서의 Amazon S3 콘솔에서의 객체 구성을 참조하십시오.
4. 완료되면 저장을 선택합니다.

S3 버킷을 생성하는 방법에 대한 지침은 Amazon S3 사용 설명서의 버킷 생성을 참조하십시오.

AWS CLI

내보내기 대상 설정을 업데이트하려면(AWS CLI)

update-settings 명령을 실행하고 `--default-export-destination` 파라미터를 사용하여 S3 버킷을 지정합니다.

다음 예에서는 각 *## ### ###*를 자신의 정보로 바꿉니다.

```
aws auditmanager update-settings --default-export-destination
 destinationType=S3,destination=s3://doc-example-destination-bucket
```

S3 버킷을 생성하는 방법에 대한 지침은 AWS CLI 명령 참조의 create-bucket 섹션을 참조하십시오.

Audit Manager API

내보내기 대상 설정(API)을 업데이트하려면

UpdateSettings 작업을 호출하고 defaultExportDestination 파라미터를 사용하여 S3 버킷을 지정합니다.

S3 버킷을 생성하는 방법에 대한 지침은 Amazon S3 API 참조의 CreateBucket을 참조하십시오.

내보내기 목적지에 대한 구성 팁

파일을 성공적으로 내보내려면 내보내기 목적지의 다음 구성을 확인하는 것이 좋습니다.

AWS 리전

고객 관리 키 AWS 리전(제공한 경우)는 평가 지역과 일치해야 합니다. KMS 키를 변경하는 방법에 대한 지침은 Audit Manager 데이터 암호화 설정을 참조하십시오.

계정 간 S3 버킷

계정 간 S3 버킷을 내보내기 대상으로 사용하는 것은 Audit Manager 콘솔에서 지원되지 않습니다. AWS CLI 또는 AWS SDK 중 하나를 사용하여 계정 간 버킷을 지정할 수 있지만, 단순화를 위해 이렇게 하지 않는 것이 좋습니다. 계정 간 S3 버킷을 내보내기 대상으로 사용하기로 선택한 경우 다음 사항을 고려하십시오.

- 기본적으로 CSV 내보내기와 같은 S3 객체는 해당 객체를 업로드한 AWS 계정이 소유합니다. S3 객체 소유권 설정을 사용하여 미리 준비된 `bucket-owner-full-control` 액세스 제어 목록

(ACL)을 포함하여 계정에서 작성한 새 객체를 버킷 소유자가 자동으로 소유하게 되도록 이 기본 동작을 변경할 수 있습니다.

필수 사항은 아니지만 계정 간 버킷 설정을 다음과 같이 변경하는 것이 좋습니다. 이렇게 변경하면 버킷에 게시한 내보낸 파일을 버킷 소유자가 완전히 제어할 수 있습니다.

- S3 버킷의 객체 소유권을 기본 객체 작성자 대신 버킷 소유자 선호로 설정합니다.
- 해당 버킷에 업로드된 객체에 `bucket-owner-full-control` ACL이 적용되도록 버킷 정책을 추가합니다.

- Audit Manager가 계정 간 S3 버킷으로 파일을 내보낼 수 있도록 하려면 내보내기 대상 버킷에 다음 S3 버킷 정책을 추가해야 합니다. 각 *## ### ###*를 사용자의 정보로 바꿉니다. 이 정책의 `Principal` 요소는 평가를 소유하고 파일을 내보내는 사용자 또는 역할입니다. `Resource`은 파일을 내보낼 계정 간 S3 버킷을 지정합니다.

```
{
  "Version": "2012-10-17",
  "Statement": [
      {
          "Sid": "Allow cross account file exports",
          "Effect": "Allow",
          "Principal": {
              "AWS":
 "arn:aws:iam::AssessmentOwnerAccountId:user/AssessmentOwnerUserName"
          },
          "Action": [
              "s3:ListBucket",
              "s3:PutObject",
              "s3:GetObject",
              "s3:GetBucketLocation",
              "s3:PutObjectAcl",
              "s3:DeleteObject"
          ],
          "Resource": [
              "arn:aws:s3:::CROSS-ACCOUNT-BUCKET",
              "arn:aws:s3:::CROSS-ACCOUNT-BUCKET/*"
          ]
      }
  ]
}
```

AWS Audit Manager의 알림

AWS Audit Manager은 Amazon Simple Notification Service(SNS)를 통해 사용자 작업에 대해 알릴 수 있습니다.

다음 이벤트 중 하나가 발생하면 Audit Manager가 알림을 보냅니다.

- 감사 소유자가 검토를 위해 제어 세트를 위임합니다.
- 대리인은 검토된 통제 세트를 감사 소유자에게 다시 제출합니다.
- 감사 소유자가 통제 세트에 대한 검토를 완료합니다.

필수 조건

Audit Manager에서 Amazon SNS 알림을 설정하기 전에 다음 단계를 완료해야 합니다.

1. 주제가 없는 경우 Amazon SNS 주제 생성 자세한 내용은 Amazon Simple Notification Service 개발자 안내서에서 Amazon SNS 주제 생성을 참조하세요.
2. 하나 이상의 엔드포인트를 주제에 구독시킵니다. 예를 들어 문자 메시지로 알림을 수신하고자 하는 경우 SMS 엔드포인트를 주제에 구독 설정합니다. SMS 엔드포인트는 휴대폰 번호입니다. 이메일로 알림을 수신하려면 이메일 엔드포인트를 주제에 구독시킵니다. 이메일 엔드포인트는 이메일 주소입니다.

   자세한 내용은 Amazon Simple Notification Service Developer Guide의 Getting Started를 참조하세요.
3. (선택 사항) 주제가 서버 측 암호화(SSE)를 위해 AWS Key Management Service(AWS KMS)를 사용한다면 AWS KMS key 정책에 권한을 추가해야 합니다. 사용할 수 있는 예제 정책은 SNS 주제에 연결된 KMS 키의 권한을 참조하십시오.

AWS Audit Manager에서 알림 구성

아래 단계에 따라 다음 단계에 따라 AWS Audit Manager에서 알림을 구성합니다.

AWS Audit Manager에서 알림을 구성하려면

1. https://console.aws.amazon.com/auditmanager/home 에서 AWS Audit Manager 콘솔을 엽니다.
2. 왼쪽 탐색 창에서 설정을 선택합니다.

3. 알림에서 - 선택 사항으로 알림을 수신하는 데 사용하려는 SNS 주제를 지정합니다.
   - 기존 주제를 사용하려면 드롭다운 메뉴에서 주제 이름을 선택합니다.
   - 새 주제를 만들려면 새 주제 만들기를 선택합니다. 그러면 주제를 생성할 수 있는 Amazon SNS 콘솔로 이동합니다.
4. 완료되면 저장을 선택합니다.

> **주의**
>
> - 표준 SNS 주제 또는 FIFO (선입선출) SNS 주제를 사용할 수 있습니다. Audit Manager는 FIFO 주제에 대한 알림 전송을 지원합니다. 하지만 메시지가 전송되는 순서는 보장되지 않습니다.
> - 현재 가지고 있지 않은 Amazon SNS 주제를 사용하려면 AWS Identity and Access Management (IAM) 정책을 구성해야 합니다. 보다 구체적으로 말하자면 주제의 Amazon 리소스 이름(ARN) 에서 게시를 허용하도록 정책을 구성 해야 합니다. 자세한 내용은 AWS Audit Manager의 자격 증명 및 액세스 관리를 참조하세요.

문제 해결

일반적인 질문과 문제에 대한 답변을 찾으려면 이 안내서의 문제 해결 섹션에서 알림 문제 해결을 참조하십시오.

AWS Audit Manager에서 문제 해결

다음 정보는 AWS Audit Manager의 작업을 할 때 나타날 수 있는 오류 문제를 해결하는 데 도움을 줄 수 있습니다.

발생한 문제가 다음 정보의 범위를 벗어나거나 해결을 시도한 후에도 문제가 지속되는 경우 AWS Support에 문의하세요.

주제

평가 및 증거 수집 문제 해결

이 페이지의 정보를 사용하여 Audit Manager의 일반적인 평가 및 증거 수집 문제를 해결할 수 있습니다.

주제

- 범위 내 계정을 나의 조직에서 제거하면 어떻게 되나요?
- 평가 범위 내에서 서비스를 수정하려 하는데 안 됩니다.
- 서비스 범위와 데이터 소스 유형의 차이는 무엇입니까?
- 나의 평가 생성은 실패했습니다.
- Audit Manager를 비활성화했다가 다시 활성화했더니 이제 저의 기존 평가가 더 이상 증거를 수집하지 않는군요.

저는 평가를 생성했지만 아직 아무 증거도 볼 수 없습니다.

귀하가 증거를 찾을 수 없다면 평가를 생성한 후 최소 24시간을 기다리지 않으셨거나 구성 오류가 있었을 것입니다.

다음을 수행하는 것이 좋습니다.

1. 평가를 생성한 후 24시간이 지났는지 확인하세요. 평가를 생성한 지 24시간 후에 자동 증거가 제공됩니다.
2. AWS 서비스의 증거를 찾게 될 것으로 귀하가 기대하는 것과 동일한 AWS 리전으로 Audit Manager를 사용하고 있는지 확인하세요.
3. AWS Config 및 AWS Security Hub에서 규정 준수 확인 증거를 찾아내게 될 것으로 예상되는 경우, AWS Config 및 Security Hub 콘솔 양자 모두 이러한 검사 결과를 표시하는지 확인하세요. AWS Config 및 Security Hub 결과는 귀하가 Audit Manager를 사용하는 동일한 AWS 리전에서 표시되어야 합니다.

이러한 문제 중 하나로 인한 것이 아님에도 여전히 평가에서 증거를 확인할 수 없는 경우 이 페이지에 설명된 다른 잠재적 원인을 확인해 보세요.

나의 평가는 AWS Security Hub으로부터 규정 준수 확인 증거를 수집하지 않습니다.

AWS Security Hub 제어에 대한 규정 준수 확인 증거가 보이지 않는 경우 다음 문제 중 하나가 원인일 수 있습니다.

AWS Security Hub의 구성이 누락되었습니다.

AWS Security Hub를 활성화했을 때 일부 구성 단계를 놓친 경우 이 문제가 발생할 수 있습니다.

Security Hub를 활성화하고 다음과 같이 설정을 구성했는지 확인하세요.

단일 AWS 계정에 대한 Security Hub 설정 확인하기

단일 AWS 계정를 사용하는 경우 다음을 확인하세요.

- AWS Config을 활성화하고 귀하의 계정에 대한 리소스 기록을 구성했는지 확인하세요.
- 귀하의 계정에 PCI DSS 보안 표준을 활성화했는지 확인하세요.
- Security Hub에서 통합 제어 조사 결과 설정을 활성화했는지 확인합니다.

조직의 Security Hub 설정 확인

Organizations를 사용하는 경우 다음을 확인하세요.

- AWS Config을 활성화하고 조직에 대한 리소스 기록을 구성했는지 확인하세요.
- 조직의 모든 구성원 계정에 대해 PCI DSS 보안 표준을 활성화했는지 확인하세요.
- Security Hub에서 통합 제어 조사 결과 설정을 활성화했는지 확인합니다.
- Security Hub에서 귀하가 사용하는 위임된 관리자 계정이 Audit Manager에서 귀하가 사용하는 것과 동일한지 확인하세요.
- 귀하의 조직 계정을 Security Hub 구성원 계정으로 활성화했는지 확인합니다.

귀하의 **`ControlMappingSource`**에 Security Hub 제어 이름을 잘못 입력했습니다.

Audit Manager API를 사용하여 사용자 지정 제어를 생성할 때 Security Hub 제어를 증거 수집을 위한 데이터 소스 매핑으로 지정할 수 있습니다. 이렇게 하려면 제어 ID를 `keywordValue`로 입력합니다 .

Security Hub 제어에 대한 규정 준수 검사 증거가 보이지 않는다면 `keywordValue`이 귀하의 `ControlMappingSource`에 잘못 입력된 것일 수 있습니다. `keywordValue`는 대소문자를 구분합니다. 잘못 입력하면 Audit Manager에서 해당 규칙을 인식하지 못할 수 있습니다. 따라서 예상대로 해당 제어에 대한 규정 준수 확인 증거를 수집하지 못할 수 있습니다.

이 문제를 해결하려면 사용자 지정 제어를 업데이트하고 `keywordValue`를 수정하세요. Security Hub 키워드의 올바른 형식은 다양합니다. 정확성을 기하기 위해, 지원되는 Security Hub 제어 키워드 목록을 참조하세요.

`AuditManagerSecurityHubFindingsReceiver`Amazon EventBridge 규칙이 누락되었습니다.

Audit Manager를 활성화하면 Amazon EventBridge에서 `AuditManagerSecurityHubFindingsReceiver`이라는 이름의 규칙이 자동으로 생성되고 활

성화됩니다. 이 규칙을 통해 Audit Manager는 Security Hub 조사 결과를 증거로 수집할 수 있습니다.

이 규칙이 귀하가 Security Hub를 사용하는 AWS 리전에서 나열되고 활성화되지 않은 경우, Audit Manager는 해당 지역에 대한 Security Hub 조사 결과를 수집할 수 없습니다.

이 문제를 해결하려면 EventBridge 콘솔로 이동하여 `AuditManagerSecurityHubFindingsReceiver` 규칙이 귀하의 AWS 계정에 존재하는지 확인하세요. 규칙이 없는 경우 Audit Manager를 비활성화한 다음 서비스를 다시 활성화하실 것을 권고합니다. 이렇게 해도 문제가 해결되지 않거나 Audit Manager를 비활성화는 것이 선택지가 아닌 경우, 지원을 위해 AWS Support에 연락하세요.

Security Hub에서 만든 서비스 연결 AWS Config 규칙

Audit Manager는 Security Hub가 생성하는 서비스 연결 AWS Config 규칙에서 증거를 수집하지 않는다는 점을 기억하세요. 이는 Security Hub 서비스에 의해 활성화되고 제어되는 특정 유형의 관리형 AWS Config 규칙입니다. 동일한 규칙의 다른 인스턴스가 이미 존재하는 경우에도 Security Hub은 이러한 서비스 연결 규칙을 귀하의 AWS 환경 내에 생성합니다. 따라서 증거 중복을 방지하기 위해 Audit Manager는 서비스 연결 규칙에서의 증거 수집을 지원하지 않습니다.

나의 평가는 AWS Config으로부터 규정 준수 확인 증거를 수집하지 않습니다.

AWS Config 규칙에 대한 규정 준수 검사 증거가 보이지 않는 경우 다음 문제 중 하나가 원인일 수 있습니다.

규칙 식별자가 귀하의 **`ControlMappingSource`** 내에 잘못 입력되었습니다

Audit Manager API를 사용하여 사용자 지정 제어를 만들 때 증거 수집을 위한 데이터 소스 매핑으로 AWS Config 규칙을 지정할 수 있습니다. 귀하가 지정하는 `keywordValue`는 규칙 유형에 따라 다릅니다.

AWS Config 규칙에 대한 규정 준수 확인 증거가 보이지 않는 경우 `keywordValue`가 귀하의 `ControlMappingSource`에 잘못 입력된 것일 수 있습니다. `keywordValue`는 대소문자를 구분합니다. 잘못 입력하시면 Audit Manager가 규칙을 인식하지 못할 수 있습니다. 따라서 의도한 대로 해당 규칙에 대한 규정 준수 확인 증거를 수집하지 못할 수 있습니다.

이 문제를 해결하려면 사용자 지정 제어를 업데이트하고 `keywordValue`를 수정하세요.

- 사용자 지정 규칙의 경우 `keywordValue`에 `Custom_` 접두사를 붙이고, 그 뒤에 사용자 지정 규칙 이름이 오는지 확인하세요. 사용자 지정 규칙 이름의 형식은 다를 수 있습니다. 정확성을 위해 AWS Config 콘솔을 방문하여 사용자 지정 규칙 이름을 확인하세요.
- 관리형 규칙의 경우 `keywordValue`가 `ALL_CAPS_WITH_UNDERSCORES` 안의 규칙 식별자인지 확인하세요. 예: `CLOUDWATCH_LOG_GROUP_ENCRYPTED`. 정확성을 위해 지원되는 관리형 규칙 키워드 목록을 참조하세요.

> **Note**
>
> 일부 관리형 규칙의 경우 규칙 식별자가 규칙 이름과 다릅니다. 예를 들어, stricted-ssh의 규칙 식별자는 `INCOMING_SSH_DISABLED`입니다. 규칙 이름이 아닌 규칙 식별자를 사용해야 합니다. 규칙 식별자를 찾으려면 관리형 규칙 목록에서 규칙을 선택하고 해당 식별자 값을 찾아보세요.

규칙은 서비스 AWS Config 연결 규칙입니다.

관리형 규칙 및 사용자 지정 규칙을 증거 수집을 위한 데이터 소스 매핑으로 사용할 수 있습니다. 하지만 Audit Manager는 대부분의 서비스 연결 규칙에서 증거를 수집하지 않습니다.

Audit Manager가 증거를 수집하는 서비스 연결 규칙에는 다음 두 가지 유형만 있습니다.

- 적합성 팩의 서비스 연결 규칙
- AWS Organizations의 서비스 연결 규칙

Audit Manager는 다른 서비스 연결 규칙, 특히 `arn:aws:config:*:*:config-rule/aws-service-rule/...` 접두사가 포함된 Amazon 리소스 이름(ARN)이 있는 규칙에서 증거를 수집하지 않습니다.

Audit Manager가 대부분의 서비스 관련 AWS Config 규칙에서 증거를 수집하지 않는 이유는 평가에서 증거가 중복되는 것을 방지하기 위함입니다. 서비스 연결 규칙은 다른 AWS 서비스가 귀하의 계정에서 AWS Config 규칙을 생성할 수 있게 하는 특수 유형의 관리형 규칙입니다. 예를 들어 일부 Security Hub 제어는 AWS Config 서비스 연결 규칙을 사용하여 보안 검사를 실행합니다. 서비스 연결 AWS Config 규칙을 사용하는 모든 제어에 대해 Security Hub는 귀하의 AWS 환경에서 필요한 AWS Config 규칙의 인스턴스를 생성합니다. 귀하의 계정에 이전 규칙이 이미 있는 경우에도 이 문제가 발생합니다. 따라서 동일한 규칙에서 동일한 증거를 두 번 수집하지 않기 위해 Audit Manager는 서비스 연결 규칙을 무시하고 해당 규칙에서 증거를 수집하지 않습니다.

AWS Config가 서비스 범위에 포함되거나 활성화되지 않았습니다.

AWS Config은 귀하의 AWS 계정에서 활성화되어야 합니다. 또한 귀하의 평가 범위에 서비스로 포함되어야 합니다. 이러한 AWS Config 방식으로 설정하면 Audit Manager는 AWS Config 규칙이 평가될 때마다 증거를 수집합니다.

먼저, 귀하의 AWS Config 계정에서 AWS 계정를 활성화했는지 확인하세요. 지침은 AWS Config 활성화 및 설정을 참조하세요.

다음으로, 귀하의 평가를 위한 범위에 AWS Config을 서비스로 포함시켰는지 확인하세요. 평가 범위 내 현재 서비스를 검토하려면 평가 검토, AWS 서비스 탭을 참조하세요. 평가 범위 내 서비스 목록을 편집하려면 범위 내 AWS 서비스 편집을 참조하세요.

AWS Config 규칙은 귀하가 평가를 설정하기 전에 리소스 구성을 평가했습니다

AWS Config 규칙이 특정 리소스의 구성 변경을 평가하도록 설정된 경우 Audit Manager의 증거와 AWS Config 평가 간에 불일치가 발생할 수 있습니다. 이는 Audit Manager 평가에서 제어를 설정하기 전에 규칙 평가가 수행된 경우에 발생합니다. 이 경우 Audit Manager는 기저에 있는 리소스의 상태가 다시 변경되어 규칙의 재평가를 촉발할 때까지 증거를 생성하지 않습니다.

해결 방법으로 AWS Config 콘솔에서 규칙으로 이동하여 규칙을 수동으로 재평가할 수 있습니다. 그러면 해당 규칙과 관련된 모든 리소스에 대한 새로운 평가가 시작됩니다.

나의 평가는 AWS CloudTrail으로부터 사용자 활동 증거를 수집하고 있지 않습니다.

Audit Manager API를 사용하여 사용자 지정 제어를 생성할 때 CloudTrail 이벤트 이름을 증거 수집을 위한 데이터 소스 매핑으로 지정할 수 있습니다. 이렇게 하려면 이벤트 이름을 `keywordValue`로 입력합니다.

CloudTrail 이벤트에 대한 사용자 활동 증거가 보이지 않는 경우 `keywordValue`가 귀하의 `ControlMappingSource`에 잘못 입력된 것일 수 있습니다. `keywordValue` 값은 대소문자를 구분합니다. 잘못 입력하면 Audit Manager가 이벤트 이름을 인식하지 못할 수 있습니다. 그 결과 해당 이벤트에 대한 사용자 활동 증거를 의도한 대로 수집하지 못할 수 있습니다.

이 문제를 해결하려면 사용자 지정 제어를 업데이트하고 `keywordValue`를 수정하세요. 이벤트가 `serviceprefix_ActionName`로서 작성되었는지 확인하세요. 예: `cloudtrail_StartLogging`. 정확성을 위해 서비스 인증 참조의 AWS 서비스 접두사와 작업 이름을 검토하세요.

나의 평가에서는 AWS API 직접 호출에 대한 구성 데이터 증거를 수집하지 않습니다.

Audit Manager API를 사용하여 사용자 지정 제어를 만들 때 AWS API 직접 호출을 증거 수집을 위한 데이터 소스 매핑으로 지정할 수 있습니다. 이렇게 하려면 API 직접 호출을 `keywordValue`로 입력합니다.

AWS API 직접 호출에 대한 구성 데이터 증거가 보이지 않는 경우, 귀하의 `ControlMappingSource`에 `keywordValue`가 잘못 입력된 것일 수 있습니다. `keywordValue` 값은 대/소문자를 구분합니다. 잘못 입력하면 Audit Manager에서 API 호출을 인식하지 못할 수 있습니다. 그 결과 해당 API 호출에 대한 구성 데이터 증거를 의도대로 수집하지 못할 수 있습니다.

이 문제를 해결하려면 사용자 지정 제어를 업데이트하고 `keywordValue`를 수정하세요. API 직접 호출이 `serviceprefix_ActionName`로 작성되었는지 확인합니다. 예: `iam_ListGroups`. 정확성을 위해 지원되는 API 직접 호출 목록을 참조하세요.

나의 평가는 다른 AWS 서비스로부터 증거를 수집하는 것이 아닙니다.

귀하의 평가 범위로 AWS 서비스가 선택되지 않은 경우 Audit Manager는 해당 서비스와 관련된 리소스에서 증거를 수집하지 않습니다. 이것은 AWS 서비스를 선택했지만 이를 귀하의 환경에서 활성화하지 않은 경우에도 마찬가지입니다.

사용자 지정 프레임워크에서 평가를 생성한 경우 평가 범위 내에서 서비스를 편집할 수 있습니다. 그런 다음 증거를 수집할 AWS 서비스를 추가로 지정할 수 있습니다. 이러한 서비스를 추가하면 증거는 24시간 후에 이용 가능합니다.

> **Note**
>
> 표준 프레임워크에서 귀하의 평가를 생성한 경우 범위 내 AWS 서비스 목록이 미리 선택되며 이는 편집할 수 없습니다. 표준 프레임워크에서 평가를 생성하면 Audit Manager가 자동으로 관련 데이터 소스 및 서비스를 매핑하고 선택하기 때문입니다. 선택은 표준 프레임워크의 요구 사항을 기반으로 이루어집니다. 단, 수동 제어만 포함하는 표준 프레임워크의 경우 AWS 서비스는 적용 범위에 포함되지 않습니다.
>
> 표준 프레임워크를 기반으로 평가를 생성하면서 범위 내 AWS 서비스를 편집하는 해결 방법은 표준 프레임워크를 사용자 지정하는 것입니다. 이 해결 방법을 사용하면 사용자 지정한 프레임워크를 사용하여 새 평가를 생성할 수 있습니다. 그런 다음 이 평가에서 범위에 AWS 서비스가 포함되는 항목이 무엇인지 지정할 수 있습니다.

나의 증거는 서로 다른 간격으로 생성되는데, 얼마나 자주 수집되고 있는지 잘 모르겠습니다.

Audit Manager 평가의 제어 기능은 다양한 데이터 소스에 매핑됩니다. 데이터 소스마다 증거 수집 빈도가 다릅니다. 그 결과, 증거 수집 빈도에 대해 모든 경우에 통용되는 한 가지 답을 제시할 수는 없습니다. 일부 데이터 소스는 규정 준수를 평가하는 반면, 다른 데이터 소스는 규정 준수 결정 없이 리소스 상태 및 변경 데이터만 캡처합니다.

다음은 다양한 데이터 소스 유형과 이러한 데이터 소스가 증거를 수집하는 빈도를 요약한 것입니다.

데이터 소스 유형	설명	증거 수집 빈도	평가에서 이 제어가 활성화된 경우
AWS CloudTrail	특정 사용자 활동 추적	연속	Audit Manager는 귀하가 선택한 키워드를 기반으로 귀하의 CloudTrail 로그를 필터링합니다. 처리된 로그는 사용자 활동을 증거로 가져옵니다.
AWS Security Hub	Security Hub의 조사 결과를 보고하여 리소스 보안 상태의 스냅샷을 캡처합니다.	Security Hub 점검 일정 기준(일반적으로 약 12시간마다)	Audit Manager는 Security Hub에서 직접 보안 조사 결과를 검색합니다. 조사 결과를 규정 준수 검사 증거로 가져옵니다.
AWS Config	AWS Config로부터의 조사 결과를 보고하여 리소스 보안 상태의 스냅샷을 캡처합니다.	AWS Config 규칙에 정의된 설정을 기반으로 하여	Audit Manager는 직접 AWS Config에서 규칙 평가를 검색합니다. 평가를 규정 준수 검사 증거로 가져옵니다.
AWS API 직접 호출	지정된 AWS 서비스에 대한 API 직접 호출을 통해 직접 리소스 구성에 대한 스냅샷을 생성합니다.	일별, 주별 또는 월별	Audit Manager는 귀하가 지정한 빈도에 따라 API 직접 호출을 수행합니다. 그 응답은 구성 데이터 증거로 가져옵니다.

증거 수집 빈도에 관계없이 평가가 진행 중인 동안에는 새 증거가 자동으로 수집됩니다. 자세한 내용은 증거 수집 빈도를 참조하세요.

자세한 내용은 자동 증거를 위한 지원되는 통제 데이터 소스 및 제어를 위한 증거 수집 빈도 변경을 참조하세요.

범위 내 계정을 나의 조직에서 제거하면 어떻게 되나요?

범위 내 계정이 귀하의 조직에서 제거되면 Audit Manager는 더 이상 해당 계정에 대한 증거를 수집하지 않습니다. 하지만 해당 계정은 AWS 계정 탭 아래 귀하의 평가에 계속 표시됩니다. 범위 내 계정 목록에서 계정을 제거하려면 평가를 편집하세요. 제거된 계정은 편집하는 동안 목록에 더 이상 표시되지 않으므로 해당 계정이 범위에 포함되지 않은 상태에서 변경 내용을 저장할 수 있습니다.

평가 범위 내에서 서비스를 수정하려 하는데 안 됩니다.

Audit Manager 콘솔을 사용하여 표준 프레임워크에서 평가를 생성하는 경우 범위 내 AWS 서비스의 목록이 기본적으로 선택됩니다. 이 목록은 편집할 수 없습니다. 이는 Audit Manager가 자동으로 데이터 소스 및 서비스를 매핑하고 선택하기 때문입니다. 이 선택은 표준 프레임워크의 요구 사항에 따라 이루어집니다. 귀하가 선택한 표준 프레임워크에 수동 제어만 포함된 경우, AWS 서비스는 귀하의 평가 범위에 포함되지 않으며 평가에 서비스를 추가할 수 없습니다.

범위 내 서비스 목록을 편집해야 하는 경우 Audit Manager에서 제공하는 UpdateAssessment API 작업을 사용하세요. 또는 표준 프레임워크를 사용자 지정한 다음 사용자 지정 프레임워크에서 평가를 생성할 수도 있습니다.

서비스 범위와 데이터 소스 유형의 차이는 무엇입니까?

범위 내 서비스는 귀하의 평가의 일부로 지정된 서비스입니다. AWS 서비스 서비스가 범위 내에 있는 경우 Audit Manager는 해당 서비스 및 해당 리소스의 사용에 대한 증거를 수집합니다.

데이터 소스 유형은 증거가 어디에서 수집되는지 정확한 위치를 나타냅니다. 사용자만의 고유 증거를 업로드하는 경우, 데이터 소스 유형은 수동입니다. Audit Manager가 증거를 수집하는 경우 데이터 소스는 네 가지 유형 중 하나일 수 있습니다.

1. AWS Security Hub – Security Hub의 조사 결과를 보고하여 리소스 보안 상태의 스냅샷을 캡처합니다.
2. AWS Config – AWS Config의 조사 결과를 보고하여 귀하의 리소스 보안 상태의 스냅샷을 캡처합니다.

3. AWS CloudTrail – 리소스의 특정 사용자 활동을 추적합니다.
4. AWS API 직접 호출 – 직접 특정 AWS 서비스에 대한 API 직접 호출을 통해 리소스 구성의 스냅샷을 생성합니다.

다음은 서비스 범위와 데이터 소스 유형 간의 차이를 보여주는 두 가지 예입니다.

예 1

4.1.2 - S3 버킷에 대한 공개 쓰기 액세스 허용 안 함이라고 명명된 제어에 대한 증거를 수집하려고 한다고 가정해 보겠습니다. 이 제어는 S3 버킷 정책의 액세스 수준을 확인합니다. 이 제어를 위해 Audit Manager는 특정 AWS Config 규칙(s3-버킷 공개 쓰기 허용 안 함)을 사용하여 S3 버킷에 대한 평가를 찾습니다. 이 예에서 이하의 내용이 모두 적용됩니다.

- 서비스 범위는 Amazon S3입니다.
- 평가 대상 리소스는 S3 버킷입니다.
- 데이터 소스의 유형은 AWS Config입니다.
- 데이터 소스 매핑은 특정 AWS Config 규칙(`s3-bucket-public-write-prohibited`)입니다.

예 2

이름이 164.308(a)(5)(ii)(C)인 HIPAA 제어에 대한 증거를 수집하려고 한다고 가정해 보겠습니다. 이 제어에는 부적절한 로그인을 탐지하기 위한 모니터링 절차가 필요합니다. 이 제어를 위해 Audit Manager는 CloudTrail 로그를 사용하여 모든 AWS Management Console 로그인 이벤트를 찾습니다. 이 예에서 이하의 내용이 모두 적용됩니다.

- 범위 내 서비스는 IAM입니다.
- 평가 대상 리소스는 귀하의 사용자입니다.
- 데이터 소스 유형은 CloudTrail입니다.
- 데이터 소스 매핑은 특정 CloudTrail 이벤트(`ConsoleLogin`)입니다.

나의 평가 생성은 실패했습니다.

평가 생성에 실패했다면 평가 범위에서 너무 많은 AWS 계정를 선택했기 때문일 수 있습니다. AWS Organizations을 사용하는 경우 Audit Manager는 단일 평가 범위에서 최대 약 150개의 회원 계정을 지원할 수 있습니다. 이 수를 초과할 경우 평가 생성이 실패할 수 있습니다. 해결 방법으로 각 평가의 범위 내에서 서로 다른 계정을 사용하여 여러 평가를 실행할 수 있습니다.

Audit Manager를 비활성화했다가 다시 활성화했더니 이제 저의 기존 평가가 더 이상 증거를 수집하지 않는군요.

Audit Manager를 비활성화하고 데이터를 삭제하지 않기로 선택하면 기존 평가가 휴면 상태로 전환되고 증거 수집이 중단됩니다. 즉, 이는 Audit Manager를 다시 활성화하면 귀하가 이전에 생성한 평가를 계속 사용할 수 있다는 뜻입니다. 하지만 증거 수집을 자동으로 재개하지는 않습니다.

기존 평가에 대한 증거 수집을 다시 시작하려면 평가를 편집하고 변경 없이 저장을 선택합니다.

평가 보고서 문제 해결

이 페이지의 정보를 사용하여 Audit Manager의 일반적인 평가 보고서 문제를 해결할 수 있습니다.

주제

나의 평가 보고서가 생성되지 않습니다.

귀하의 평가 보고서가 생성되지 않은데는 여러 이유가 있을 수 있습니다. 가장 빈번한 원인을 확인하여 이 문제를 해결할 수 있습니다. 우선 다음 체크리스트를 사용해 보세요.

1. AWS 리전 정보가 일치하지 않는지 확인하세요.
   a. 귀하의 고객 관리형 키의 AWS 리전가 평가의 AWS 리전과 일치하나요?

      Audit Manager 데이터 암호화를 위해 귀하의 자체 KMS 키를 제공하신 경우 그 키는 귀하의 평가와 동일한 AWS 리전에 있어야 합니다. 이 문제를 해결하려면 KMS 키를 귀하의 평가와 동일한 지역 내에 있는 키로 변경하세요. KMS 키를 변경하는 방법에 대한 지침은 AWS Audit Manager 설정, 데이터 암호화를 참조하세요.
   b. 고객 관리형 키의 AWS 리전가 S3 버킷의 AWS 리전과 일치하나요?

Audit Manager 데이터 암호화를 위해 자체 KMS 키를 제공한 경우, 키는 평가 보고서 대상으로 사용하는 S3 버킷과 동일한 AWS 리전에 있어야 합니다. 이 문제를 해결하려면 KMS 키 또는 S3 버킷을 변경하여 둘 다 평가와 같은 지역에 위치하도록 할 수 있습니다. KMS 키를 변경하는 방법에 대한 지침은 AWS Audit Manager 설정, 데이터 암호화를 참조하세요. S3 버킷을 변경하는 방법에 대한 지침은 AWS Audit Manager 설정, 평가 보고서 대상을 참조하세요.

2. 평가 보고서 대상으로 귀하가 사용 중인 S3 버킷의 권한을 확인하세요.

   a. 평가 보고서를 생성하는 IAM 엔티티에 S3 버킷에 필요한 권한이 있나요?

      IAM 개체에는 해당 버킷에 보고서를 게시하는 데 필요한 S3 버킷 권한이 있어야 합니다. 귀하가 사용할 수 있는 예제 정책을 제공합니다. 다른 S3 버킷을 지정하는 방법에 대한 지침은 AWS Audit Manager 설정, 평가 보고서 대상을 참조하세요.

   b. S3 버킷에 SSE-KMS를 사용한 서버 측 암호화(SSE) 를 요구하는 버킷 정책이 있나요?

      있다면 해당 버킷 정책에 사용되는 KMS 키는 귀하의 Audit Manager 데이터 암호화 설정에 지정된 KMS 키와 일치해야 합니다. Audit Manager 설정에서 KMS 키를 구성하지 않았고 귀하의 S3 버킷 정책이 SSE를 요구하는 경우, 버킷 정책이 SSE-S3를 허용하는지 확인하세요. KMS 키를 변경하는 방법에 대한 지침은 AWS Audit Manager 설정, 데이터 암호화를 참조하세요. S3 버킷을 변경하는 방법에 대한 지침은 AWS Audit Manager 설정, 평가 보고서 대상을 참조하세요.

여전히 평가 보고서를 완전히 생성할 수 없는 경우 이 페이지의 다음 문제를 검토하세요.

위의 체크리스트를 따랐지만 여전히 저의 평가 보고서가 생성되지 않습니다.

Audit Manager는 평가 보고서에 추가할 수 있는 증거의 양에 한도를 설정합니다. 이러한 한도는 귀하의 평가 보고서의 AWS 리전, 평가 보고서 대상으로 사용되는 S3 버킷의 지역, 평가에서 고객 관리형 AWS KMS key가 사용되는지 여부 등에 기초합니다.

1. 동일 지역 보고서의 한도는 22,000(S3 버킷과 평가가 동일한 AWS 리전 내에 있는 경우)입니다.
2. 지역 간 보고서(S3 버킷과 평가가 서로 다른 AWS 리전 내에 있는 경우)의 경우 한도는 3,500입니다.
3. 고객 관리형 KMS 키를 사용하는 평가의 경우 한도는 3,500입니다.

이보다 더 많은 증거가 포함된 보고서를 생성하려고 하면 작업이 실패할 수 있습니다.

해결 방법으로서, 하나의 큰 평가 보고서 대신 여러 평가 보고서를 생성할 수 있습니다. 이렇게 하면 평가의 증거를 보다 관리하기 쉬운 크기의 배치로 내보낼 수 있습니다.

보고서를 생성하려고 하니 액세스 거부 오류가 발생합니다.

Audit Manager 설정에 지정된 KMS 키가 속하지 않는 위임된 관리자 계정으로 평가를 생성한 경우 `access denied` 오류가 발생합니다. 이 오류를 방지하려면 Audit Manager에 위임된 관리자를 지정할 때 위임된 관리자 계정이 Audit Manager를 설정할 때 귀하가 제공한 KMS 키에 액세스할 수 있는지 확인하세요.

평가 보고서 대상으로 사용 중인 S3 버킷에 대한 쓰기 권한이 없는 경우에도 `access denied` 오류가 발생할 수 있습니다.

`access denied` 오류가 발생한 경우, 다음 요구 사항을 충족하였는지 확인하세요.

- 귀하의 Audit Manager 설정 내 KMS 키는 위임된 관리자에게 권한을 부여합니다. AWS Key Management Service 개발자 안내서의 다른 계정의 사용자에게 KMS 키 사용을 허용의 지침에 따라 이를 구성할 수 있습니다. Audit Manager에서 암호화 설정을 검토하고 변경하는 방법에 대한 지침은 데이터 암호화를 참조하세요.
- 평가 보고서 대상으로 귀하가 사용 중인 S3 버킷에 대한 쓰기 액세스 권한을 부여하는 권한 정책이 있습니다. 보다 구체적으로, 귀하의 권한 정책에는 `s3:PutObject` 작업이 포함되어 있고, S3 버킷의 ARN을 지정하고, 평가 보고서를 암호화하는 데 사용되는 KMS 키가 포함됩니다. 사용할 수 있는 예제 정책은 AWS Audit Manager을 위한 ID 기반 정책 예제를 참조하세요.

> **Note**
>
> Audit Manager 데이터 암호화 설정을 변경하는 경우 이러한 변경 사항은 앞으로 새로 생성하는 평가에 적용됩니다. 여기에는 귀하의 새 평가에서 생성한 모든 평가 보고서가 포함됩니다. 암호화 설정을 변경하기 전에 생성한 기존 평가에는 변경 내용이 적용되지 않습니다. 여기에는 기존 평가 보고서와 함께 기존 평가에서 생성한 새 평가 보고서가 포함됩니다. 기존 평가 및 모든 평가 보고서는 기존 KMS 키를 계속 사용합니다. 평가 보고서를 생성하는 IAM 자격 증명이 이전 KMS 키를 사용할 권한을 갖지 않는 경우, 귀하가 키 정책 수준에서 권한을 부여할 수 있습니다.

평가 보고서의 압축이 풀리지 않습니다.

Windows에서 평가 보고서의 압축을 풀 수 없는 경우 파일 경로에 여러 개의 중첩된 폴더나 긴 이름이 있기 때문에 Windows 탐색기에서 압축을 풀지 못할 수 있습니다. Windows 파일 이름 지정 시스템에서는 폴더 경로, 파일 이름 및 파일 확장자가 259자를 초과할 수 없기 때문입니다. 그렇지 않으면 `Destination Path Too Long` 오류가 발생합니다.

이 문제를 해결하려면 zip 파일을 현재 위치의 상위 폴더로 이동해 보세요. 그런 다음 다시 압축을 풀어 보세요. 또는 zip 파일의 이름을 줄이거나 파일 경로가 더 짧은 다른 위치에 압축을 풀 수도 있습니다.

보고서에서 증거 이름을 선택했으나 증거 세부 정보로 리디렉션되지 않습니다.

브라우저에서 평가 보고서를 사용하거나 운영 체제에 설치된 기본 PDF 판독기를 사용하는 경우 이 문제가 발생할 수 있습니다. 일부 브라우저 및 시스템 기본 PDF 리더는 관련 링크를 여는 것을 허용하지 않습니다. 즉, 하이퍼링크가 평가 보고서 요약 PDF 내에서 작동할 수는 있지만 (예: 목차의 하이퍼링크된 제어 이름) 평가 요약 PDF에서 별도의 증거 세부 정보 PDF로 이동하려고 하면 하이퍼링크가 무시됩니다.

이 문제가 발생하는 경우 전용 PDF 리더를 사용하여 평가 보고서와 상호 작용하는 것이 좋습니다. 안정적인 경험을 위해 Adobe 웹 사이트에서 다운로드할 수 있는 Adobe Acrobat Reader를 설치하여 사용하는 것이 좋습니다. 다른 PDF 리더도 사용할 수 있지만 Adobe Acrobat Reader는 Audit Manager 평가 보고서와 일관되고 안정적으로 작동하는 것으로 입증되었습니다.

나의 평가 보고서 생성이 진행 중 상태에서 정체되어 있는데, 이것이 청구에 어떤 영향을 미치는지 잘 모르겠습니다.

평가 보고서 생성은 청구에 영향을 주지 않습니다. 평가를 통해 수집한 증거에 따라서만 요금이 청구됩니다. 요금에 대한 자세한 내용은 AWS Audit Manager 요금을 참조하세요.

다음 사항도 참조하세요.

다음 페이지에는 Evidence Finder를 통한 평가 보고서 생성에 대한 문제 해결 지침이 포함되어 있습니다.

- 검색 결과에서 여러 평가 보고서를 생성할 수 없습니다.
- 평가 보고서에 개별 검색 결과를 추가할 수 없습니다.
- 증거 찾기 결과 중에 평가 보고서에 포함되지 않는 것도 있습니다.
- 검색 결과를 바탕으로 평가 보고서를 작성하고 싶은데 나의 쿼리 문구가 작동하지 않습니다.

제어 및 제어 세트 문제 해결

이 페이지의 정보를 사용하여 Audit Manager의 제어와 관련된 일반적인 문제를 해결할 수 있습니다.

일반 문제

- 나의 평가에서 제어항목이나 제어 세트를 볼 수 없습니다.
- 제어에 수동으로 증거를 업로드할 수 없습니다.

AWS Config 통합 문제

- 나는 여러 AWS Config 규칙을 단일 제어의 데이터 소스로 사용해야 할 것입니다.
- 제어 데이터 소스를 구성할 때 사용자 지정 규칙 옵션을 사용할 수 없더군요.
- 사용자 지정 규칙 옵션을 사용할 수 있지만 드롭다운 목록에 규칙이 표시되지 않아요.
- 일부 사용자 지정 규칙을 사용할 수 있지만 사용하려는 규칙이 보이지 않습니다.
- 사용하려는 관리형 규칙이 보이지 않습니다.
- 사용자 지정 프레임워크를 공유하고 싶은데 이 프레임워크에는 사용자 지정 AWS Config 규칙을 데이터 소스로 사용하는 제어 기능이 있습니다. 수신자가 이러한 제어에 대한 증거를 수집할 수 있나요?
- 사용자 지정 규칙이AWS Config에서 업데이트되면 어떻게 되나요? 제가 Audit Manager에서 취해야 할 조치가 있습니까?

나의 평가에서 제어항목이나 제어 세트를 볼 수 없습니다.

간단히 말해서, 평가의 통제 항목을 보려면 귀하가 해당 평가의 감사 소유자로 지정되어야 합니다. 또한 관련 Audit Manager 리소스를 보고 관리하려면 필요한 IAM 권한이 필요합니다.

평가의 제어 기능에 액세스해야 하는 경우 해당 평가의 감사 소유자 중 한 명에게 귀하를 감사 소유자로 지정해 달라고 요청하세요. 평가를 생성하거나 편집할 때 감사 소유자를 지정할 수 있습니다.

또한 평가를 관리하는 데 필요한 권한이 있는지 확인하세요. 감사 소유자는 AWSAuditManagerAdministratorAccess 정책을 사용하는 것이 좋습니다. IAM 권한에 대한 도움이 필요한 경우 관리자 또는 AWS 지원에 문의하세요. 사용자에게 IAM 정책 추가에 대한 자세한 내용은 IAM 사용자 설명서의 사용자에게 권한 추가 및 IAM 자격 증명 권한 추가 및 제거를 참조하세요.

제어에 수동으로 증거를 업로드할 수 없습니다.

제어에 증거를 수동으로 업로드할 수 없다면 제어가 비활성 상태이기 때문일 수 있습니다.

수동 증거를 제어에 업로드하려면 먼저 제어 상태를 검토 중 또는 검토됨으로 변경해야 합니다. 자세한 내용은 제어 상태 업데이트를 참조하세요.

> **Important**
>
> 각 AWS 계정는 하나의 제어에 매일 최대 100개의 증거 파일만 수동으로 제어에 업로드할 수 있습니다. 이 일일 할당량을 초과하면 해당 제어에 대한 추가 수동 업로드가 실패합니다. 대량의 수동 증거를 단일 컨트롤에 업로드해야 하는 경우, 며칠에 걸쳐 일괄적으로 증거를 업로드하세요.

나는 여러 AWS Config 규칙을 단일 제어의 데이터 소스로 사용해야 할 것입니다.

단일 제어에 관리형 규칙과 사용자 지정 규칙을 조합하여 사용할 수 있습니다. 이렇게 하려면 제어에 여러 데이터 소스를 설정하고 각 데이터 소스에 대해 선호하는 규칙 유형을 선택합니다. 단일 사용자 지정 제어에 대해 최대 10개의 데이터 소스를 정의할 수 있습니다.

제어 데이터 소스를 구성할 때 사용자 지정 규칙 옵션을 사용할 수 없더군요.

이것은 귀하가 자신의, AWS 계정 또는 조직의 사용자 지정 규칙을 볼 권한이 없다는 것을 의미합니다. 좀 더 구체적으로 설명하자면, 귀하는 Audit Manager 콘솔에서 DescribeConfigRules 작업을 수행할 권한이 없습니다.

이 문제를 해결하려면 AWS 관리자에게 문의하여 도움을 받으세요. 귀하가 AWS 관리자인 경우에는, IAM 정책을 관리하여 귀하의 사용자 또는 그룹에 권한을 부여할 수 있습니다.

사용자 지정 규칙 옵션을 사용할 수 있지만 드롭다운 목록에 규칙이 표시되지 않아요.

이것은 귀하의AWS 계정 또는 조직에서 활성화되어 있거나 사용할 수 있는 사용자 지정 규칙이 없다는 뜻입니다.

AWS Config에 사용자 정의 규칙이 아직 없는 경우, 귀하가 하나를 작성할 수 있습니다. 지침을 보려면 AWS Config 개발자 안내서의 AWS Config 사용자 지정 규칙 섹션을 참조하세요.

사용자 지정 규칙이 표시될 것으로 예상되면 다음 문제 해결 항목을 확인하세요.

일부 사용자 지정 규칙을 사용할 수 있지만 사용하려는 규칙이 보이지 않습니다.

찾으려는 사용자 지정 규칙이 보이지 않는 경우 다음 문제 중 하나가 원인일 수 있습니다.

귀하의 계정이 규칙에서 제외되었습니다.

사용 중인 위임된 관리자 계정이 규칙에서 제외될 수 있습니다.

귀하의 조직의 관리 계정(또는 AWS Config 위임된 관리자 계정 중 하나)은 AWS Command Line Interface(AWS CLI)를 사용하여 사용자 지정 조직 규칙을 만들 수 있습니다. 이렇게 하면 규칙에서 제외할 계정 목록을 지정할 수 있습니다. 계정이 이 목록에 있는 경우 해당 규칙은 Audit Manager에서 사용할 수 없습니다.

이 문제를 해결하려면 AWS Config 관리자에게 문의하여 도움을 받으세요. 귀하가 AWS Config 관리자인 경우 put-organization-config-rule 명령을 실행하여 제외된 계정 목록을 업데이트할 수 있습니다.

AWS Config에서 규칙이 성공적으로 생성 및 활성화되지 못했습니다.

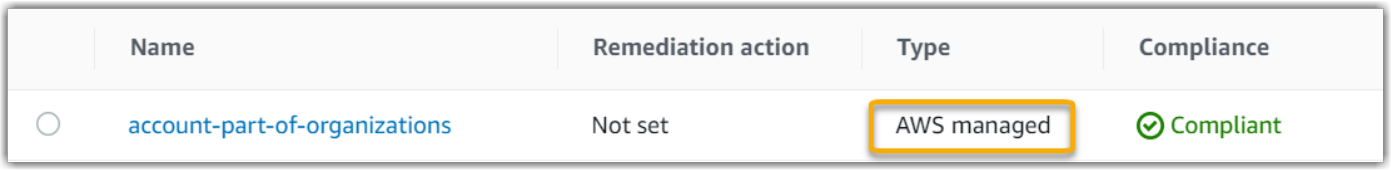
사용자 지정 규칙이 성공적으로 생성되고 활성화되지 않았을 수도 있습니다. 규칙을 만들 때 오류가 발생했거나 규칙이 활성화되지 않은 경우 Audit Manager의 사용 가능한 규칙 목록에 표시되지 않습니다.

이 문제에 대한 도움이 필요하면 AWS Config 관리자에게 문의하는 것이 좋습니다.

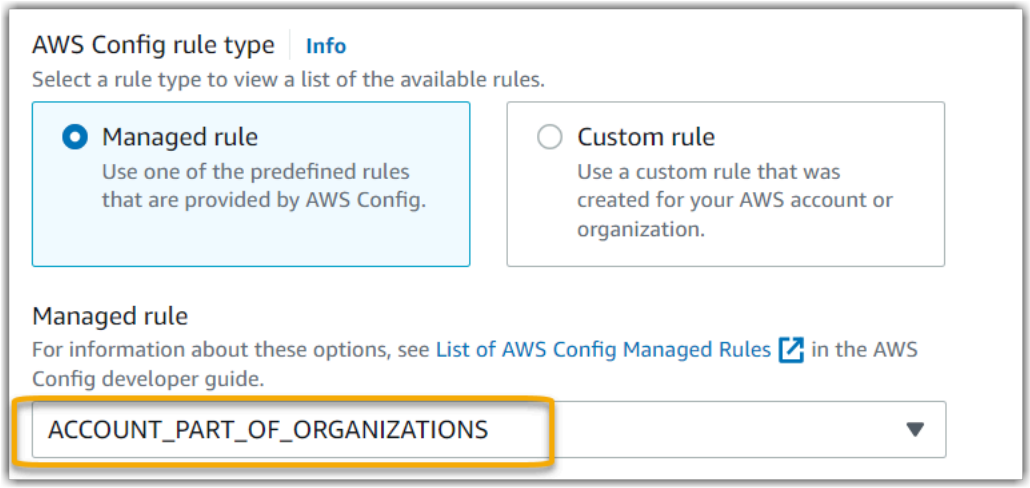
이 규칙은 관리형 규칙입니다.

사용자 지정 규칙의 드롭다운 목록에서 원하는 규칙을 찾을 수 없다면 해당 규칙이 관리형 규칙일 수 있습니다.

AWS Config 콘솔을 사용하여 규칙이 관리형 규칙인지 확인할 수 있습니다. 이렇게 하려면 왼쪽 탐색 메뉴에서 규칙을 선택하고 표에서 규칙을 찾아보세요. 규칙이 관리형 규칙인 경우 유형 열에 AWS 관리되었음이 표시됩니다.

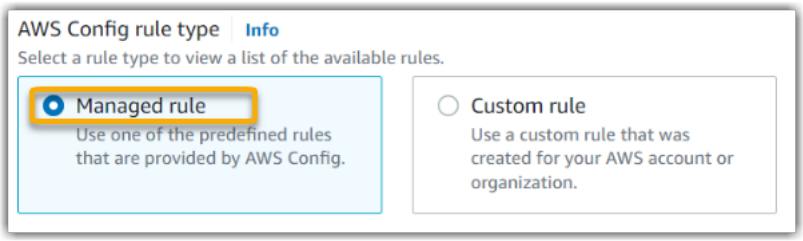


관리형 규칙임을 확인한 후 Audit Manager로 돌아가서 규칙 유형으로 관리형 규칙을 선택합니다. 그런 다음, 관리형 규칙의 드롭다운 목록에서 관리 규칙 식별자 키워드를 찾아보세요.



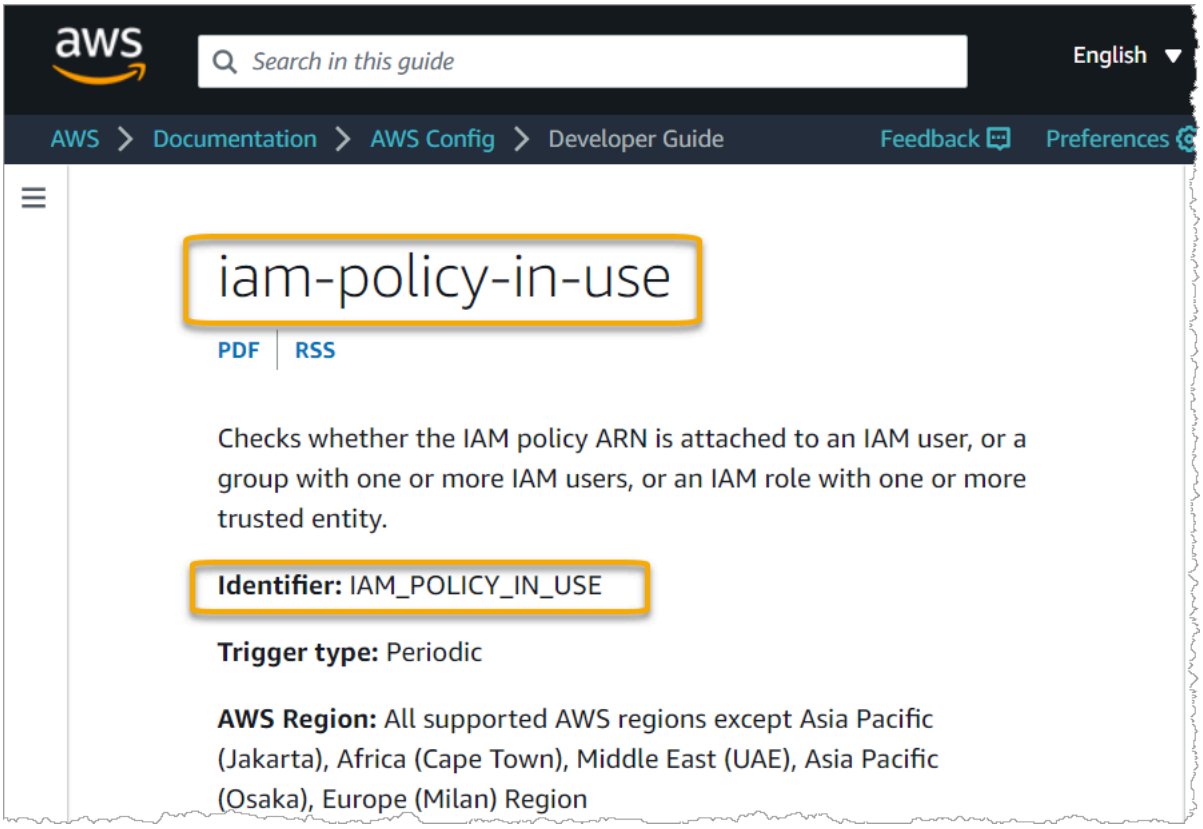
사용하려는 관리형 규칙이 보이지 않습니다.

Audit Manager 콘솔의 드롭다운 목록에서 규칙을 선택하기 전에 규칙 유형으로 관리형 규칙을 선택했는지 확인하세요.

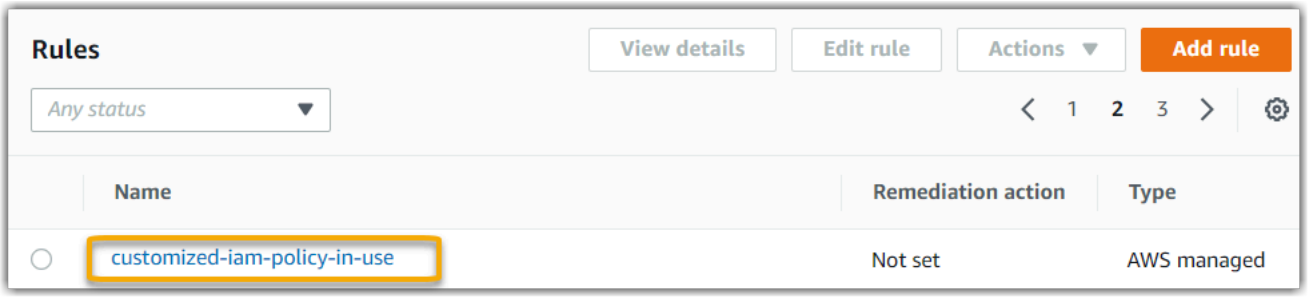


찾으려는 관리형 규칙이 여전히 보이지 않는다면 귀하가 규칙 이름을 찾고 있는 것일 수 있습니다. 대신 규칙 식별자를 찾아야 합니다.

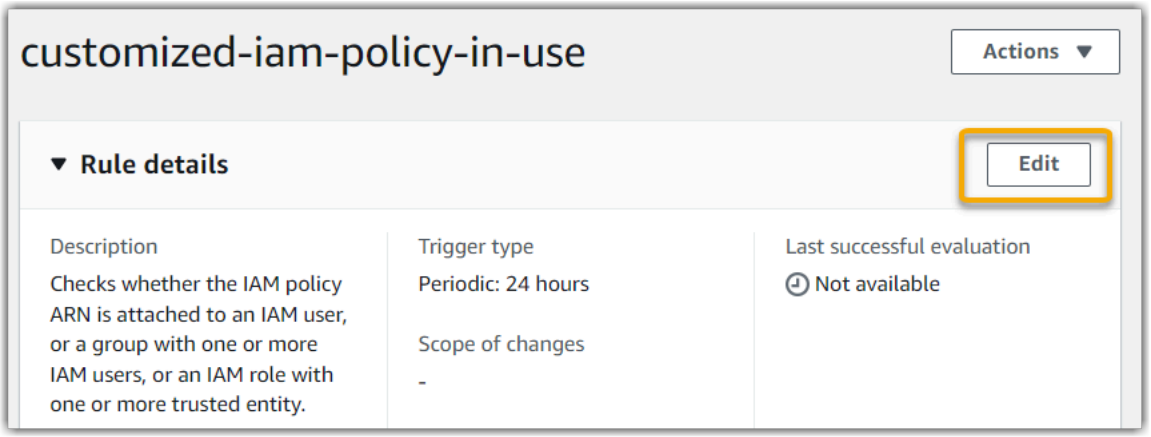
기본 관리형 규칙을 사용하는 경우 이름과 식별자는 비슷합니다. 이름은 소문자이며 대시를 사용합니다 (예:`iam-policy-in-use`). 식별자는 대문자이며 밑줄을 사용합니다 (예:`IAM_POLICY_IN_USE`). 기본 관리 규칙의 식별자를 찾으려면 지원되는 AWS Config 관리 규칙 키워드 목록을 검토하고 사용하려는 규칙의 링크를 클릭하세요. 그러면 해당 관리형 규칙의 AWS Config 문서가 표시됩니다. 여기에서 이름과 식별자를 모두 볼 수 있습니다. Audit Manager 드롭다운 목록에서 식별자 키워드를 찾으세요.



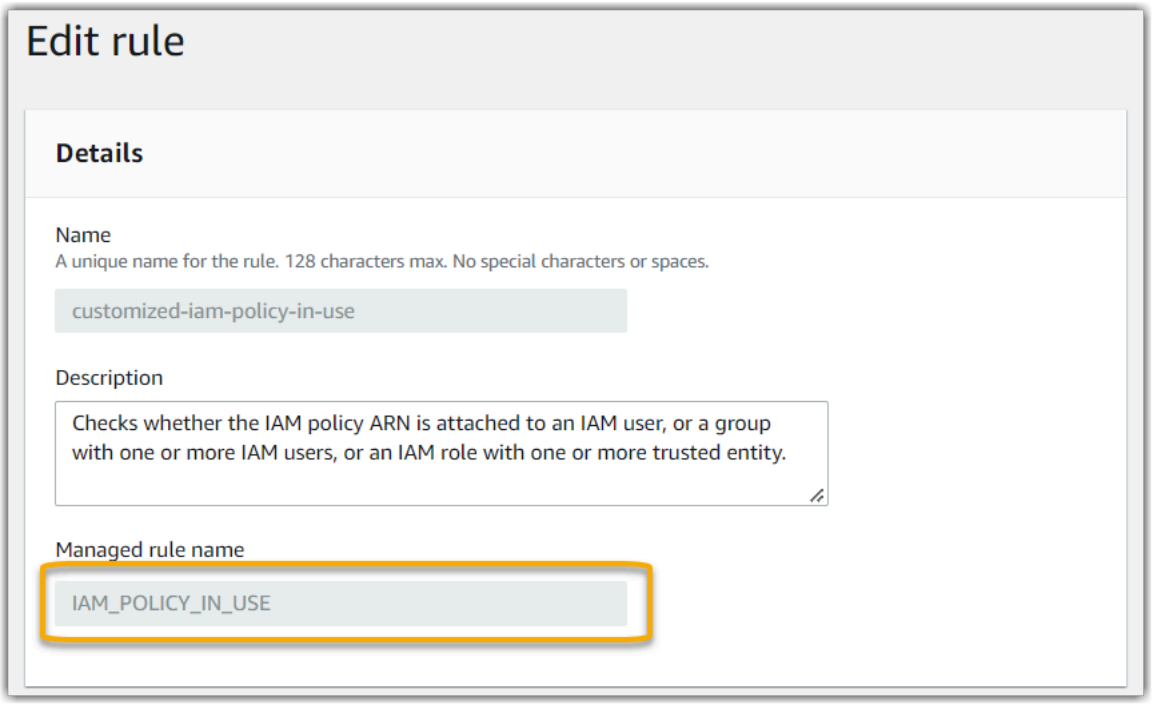
사용자 지정된 관리 규칙을 사용하는 경우 AWS Config 콘솔을 사용하여 규칙 식별자를 찾을 수 있습니다. 예를 들어 `customized-iam-policy-in-use`라는 관리형 규칙을 사용하려고 한다고 가정해 보겠습니다. 이 규칙의 식별자를 찾으려면 AWS Config 콘솔로 이동하여 왼쪽 탐색 메뉴에서 규칙을 선택하고 표에서 규칙을 선택합니다.



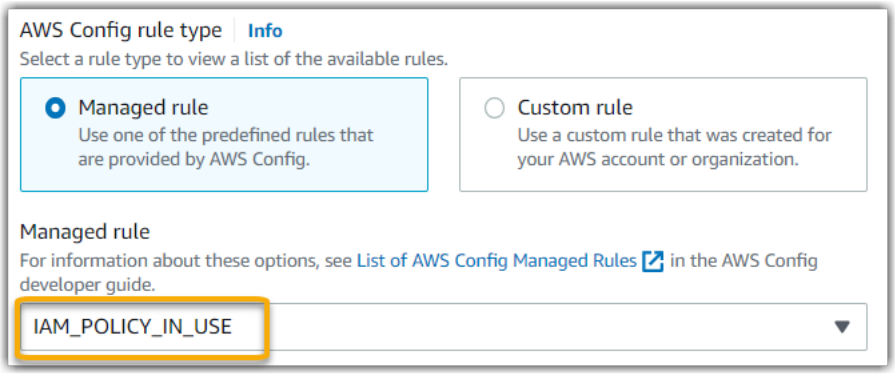
편집을 선택하여 관리형 규칙에 대한 세부 정보를 엽니다.



세부 정보 섹션에서 관리형 규칙이 (`IAM_POLICY_IN_USE`)에서 생성된 소스 식별자를 찾을 수 있습니다.



이제 Audit Manager 콘솔로 돌아가서 드롭다운 목록에서 동일한 식별자 키워드를 선택할 수 있습니다.



사용자 지정 프레임워크를 공유하고 싶은데 이 프레임워크에는 사용자 지정 AWS Config 규칙을 데이터 소스로 사용하는 제어 기능이 있습니다. 수신자가 이러한 제어에 대한 증거를 수집할 수 있나요?

예. 수신자는 이러한 제어에 대한 증거를 수집할 수 있지만, 이를 위해서는 몇 가지 단계가 필요합니다.

Audit Manager가 AWS Config 규칙을 데이터 소스 매핑으로 사용하여 증거를 수집하려면 다음 조건을 충족해야 합니다. 이것이 관리형 규칙과 사용자 정의 규칙 모두에 적용되어야 합니다.

1. 규칙은 수신자의 AWS 환경에 존재해야 합니다.
2. 수신자의 AWS 환경에서 규칙을 활성화해야 합니다.

귀하의 계정 내 사용자 지정 AWS Config 규칙은 수신자의 AWS 환경에 이미 존재하지 않을 가능성이 높다는 점을 기억하세요. 또한 수신자가 공유 요청을 수락하면 Audit Manager는 해당 계정에 사용자 지정 규칙을 다시 만들지 않습니다. 수신자가 사용자 지정 규칙을 데이터 소스 매핑으로 사용하여 증거를 수집하려면 수신자가 자신의 AWS Config 인스턴스에 동일한 사용자 지정 규칙을 만들어야 합니다. 수신자가 규칙을 작성하고 활성화한 후 Audit Manager는 해당 데이터 소스에서 증거를 수집할 수 있습니다.

수신자의 AWS Config의 인스턴스 내에서 사용자 지정 규칙이 생성되어야 하는 경우, 귀하가 해당 수신자와 통신하여 이를 알리는 것이 좋습니다.

사용자 지정 규칙이AWS Config에서 업데이트되면 어떻게 되나요? 제가 Audit Manager에서 취해야 할 조치가 있습니까?

귀하의 AWS 환경 내 규칙 업데이트용

귀하의 AWS 환경 내에서 사용자 지정 규칙을 업데이트하는 경우 Audit Manager에서 별도의 조치를 취할 필요가 없습니다. Audit Manager는 다음 표에 설명된 대로 규칙 업데이트를 탐지하고 처리합니다. Audit Manager는 규칙 업데이트가 감지된 경우 사용자에게 알리지 않습니다.

시나리오	Audit Manager의 역할	알아야 할 내용
귀하의 AWS Config 인스턴스에서 사용자 지정 규칙이 업데이트되었습니다.	Audit Manager는 업데이트된 규칙 정의를 사용하여 해당 규칙에 대한 결과를 계속 보고합니다.	별도의 작업은 필요없습니다.
귀하의 AWS Config 인스턴스에서 사용자 지정 규칙이 삭제됩니다.	Audit Manager는 삭제된 규칙에 대한 결과 보고를 중단합니다.	별도의 작업은 필요없습니다. 원하는 경우 삭제된 규칙을 데이터 소스 매핑으로 사용한 사용자 지정 제어를 편집할 수 있습니다. 이렇게 하면 삭제된 규칙을 제거하여 데이터 소스 설정을 정리하는 데 도움이 됩니다. 그렇지 않으면 삭제된 규칙 이름이 사용되지 않은 데이터 소스 매핑으로 남습니다.

귀하의 AWS 환경 외부에서 규칙을 업데이트하려면

사용자 지정 규칙이 귀하의 AWS 환경 외부에서 업데이트되는 경우 Audit Manager는 규칙 업데이트를 감지하지 못합니다. 공유된 사용자 지정 프레임워크를 사용하는 경우 이 점을 고려해야 합니다. 이 시나리오에서는 sender와 recipient가 각각 별도의 AWS 환경에서 작업하기 때문입니다. 다음 표에서는 이 시나리오에 대한 권장 조치를 제공합니다.

귀하의 역할	시나리오	권장 조치
Sender	• 귀하는 사용자 지정 규칙을 데이터 소스 매핑으로 사용하는 프레임워크를 공유했습니다.	수신자에게 업데이트 내용을 알려주세요. 이렇게 하면 동일한 업데이트를 적용

귀하의 역할	시나리오	권장 조치
	• 프레임워크를 공유한 후 AWS Config 내에서 해당 규칙 중 하나를 업데이트하거나 삭제했습니다.	하고 최신 규칙 정의와 동기화된 상태를 유지할 수 있습니다.
Recipie	• 귀하는 사용자 지정 규칙을 데이터 소스 매핑으로 사용하는 공유 프레임워크를 수락했습니다. • 귀하의 AWS Config 인스턴스에서 사용자 지정 규칙을 다시 만든 후 sender가 해당 규칙 중 하나를 업데이트하거나 삭제했습니다.	귀사 자신의 AWS Config 인스턴스에서 규칙을 그에 따라 업데이트하세요.

대시보드 문제 해결

이 페이지의 정보를 사용하여 Audit Manager의 일반적인 대시보드 문제를 해결할 수 있습니다.

주제

대시보드에 데이터가 없습니다.

일별 스냅샷 위젯의 숫자에 하이픈 (-) 이 표시되면 사용할 수 있는 데이터가 없음을 나타냅니다. 대시보드에서 데이터를 보려면 하나 이상의 활성 평가가 있어야 합니다. 시작하려면 평가를 생성하세요. 24시간이 지나면 평가 데이터가 대시보드에 표시되기 시작합니다.

> **Note**
>
> 일일 스냅샷 위젯의 숫자가 영 (0) 으로 표시되면 활성 평가(또는 선택한 평가)에 규정을 준수하지 않는 증거가 없음을 나타냅니다.

CSV 다운로드 옵션은 사용할 수 없습니다.

이 옵션은 개별 평가에만 가능합니다. 대시보드에 the section called “평가 필터”를 적용했는지 확인한 다음 다시 시도하세요. 한 번에 하나의 CSV 파일만 다운로드할 수 있다는 점에 유의하세요.

CSV 파일을 다운로드하려고 했는데 다운로드한 파일이 보이지 않습니다.

제어 도메인에 많은 수의 제어가 포함된 경우 Audit Manager가 CSV 파일을 생성하는 동안 잠시 지연될 수 있습니다. 파일이 생성되면 자동으로 다운로드됩니다.

다운로드한 파일이 여전히 보이지 않으면 인터넷 연결이 정상적으로 작동하고 최신 버전의 웹 브라우저를 사용하고 있는지 확인하세요. 또한 최근 다운로드 폴더도 확인하세요. 브라우저가 지정한 기본 위치에 파일이 다운로드됩니다. 이렇게 해도 문제가 해결되지 않으면 다른 브라우저를 사용하여 파일을 다운로드해 보세요.

대시보드에 특정 제어 또는 제어 도메인이 누락되었습니다.

이는 활성 평가(또는 지정된 평가)에 해당 제어 또는 제어 도메인과 관련된 데이터가 없음을 의미할 수 있습니다.

제어 도메인은 다음 두 기준이 모두 충족되는 경우에만 대시보드에 표시됩니다.

- 활성 평가(또는 지정된 평가)에는 해당 도메인과 관련된 제어가 하나 이상 포함되어 있습니다.
- 해당 도메인 내에서 하나 이상의 제어 항목이 대시보드 상단의 날짜에 증거를 수집했습니다.

제어는 대시보드 상단의 날짜에 증거를 수집한 경우에만 도메인 내에 표시됩니다.

일일 스냅샷에는 매일 다양한 양의 증거가 표시됩니다. 이것이 정상인가요?

모든 증거가 매일 수집되는 것은 아닙니다. Audit Manager 평가의 제어 항목은 다양한 데이터 소스에 매핑되며 각 데이터 소스에는 서로 다른 증거 수집 일정이 있을 수 있습니다. 따라서 일일 스냅샷에는 매일 다양한 양의 증거가 표시될 것으로 예상됩니다. 증거 수집 빈도에 대한 자세한 내용은 AWS Audit Manager 증거 수집 방법을 참조하세요.

위임된 관리자 및 AWS Organizations 문제 해결

이 페이지의 정보를 사용하여 Audit Manager에서 흔히 발생하는 위임 관리자 문제를 해결할 수 있습니다.

주제

위임된 관리자 계정으로 Audit Manager를 설정하는 작업이 안 됩니다.

AWS Organizations에서는 여러 명의 위임된 관리자가 지원되지만 Audit Manager에서는 한 명의 위임된 관리자만 허용합니다. Audit Manager에서 여러 위임된 관리자를 지정하려고 하면 다음 오류 메시지가 표시됩니다.

- 콘솔: `You have exceeded the allowed number of delegated administrators for the delegated service`
- CLI: `An error occurred (ValidationException) when calling the RegisterAccount operation: Cannot change delegated Admin for an active account 11111111111 from 2222222222222 to 333333333333`

Audit Manager에서 위임된 관리자로 사용할 개별 계정을 하나 선택합니다. 먼저 조직에서 위임된 관리자 계정을 등록한 다음 Audit Manager에서 위임된 관리자와 동일한 계정을 추가해야 합니다.

평가를 생성할 때 범위 내 계정에서 내 조직의 계정을 볼 수 없습니다.

Audit Manager 평가에 귀하의 조직의 여러 계정을 포함하려면 위임된 관리자를 지정해야 합니다.

Audit Manager에 대한 위임된 관리자 계정을 구성했는지 확인하세요. 지침은 설정, 위임된 관리자를 참조하세요.

다음과 같은 사항에 유의하세요.

- Audit Manager에서는 AWS Organizations 관리 계정을 위임된 관리자로 사용할 수 없습니다.
- 둘 이상의 AWS 리전에서 Audit Manager를 활성화하려면 각 리전에서 위임된 관리자 계정을 별도로 지정해야 합니다. 귀하의 Audit Manager 설정에서 모든 지역의 동일한 위임 관리자 계정을 지정합니다.
- 위임된 관리자를 지정할 때는 위임된 관리자 계정에 Audit Manager를 설정할 때 제공한 KMS 키에 대한 액세스 권한이 있는지 확인하세요. 암호화 설정을 검토하고 변경하는 방법을 알아보려면 데이터 암호화를 참조하세요.

위임된 관리자 계정을 사용하여 평가 보고서를 생성하려고 하면 액세스 거부 오류가 발생합니다.

Audit Manager 설정에 지정된 KMS 키가 속하지 않는 위임된 관리자 계정으로 평가를 생성한 경우 `access denied` 오류가 발생합니다. 이 오류를 방지하려면 Audit Manager에 위임된 관리자를 지정할 때 위임된 관리자 계정이 Audit Manager를 설정할 때 귀하가 제공한 KMS 키에 액세스할 수 있는지 확인하세요.

평가 보고서 대상으로 사용 중인 S3 버킷에 대한 쓰기 권한이 없는 경우에도 `access denied` 오류가 발생할 수 있습니다.

`access denied` 오류가 발생하는 경우, 다음 요구 사항을 충족하는지 확인하세요.

- 귀하의 Audit Manager 설정 내 KMS 키는 위임된 관리자에게 권한을 부여합니다. AWS Key Management Service 개발자 안내서의 다른 계정의 사용자에게 KMS 키 사용을 허용의 지침에 따라 이를 구성할 수 있습니다. Audit Manager에서 암호화 설정을 검토하고 변경하는 방법에 대한 지침은 데이터 암호화를 참조하세요.
- 평가 보고서 대상에 대한 쓰기 액세스 권한을 귀하에게 부여하는 권한 정책이 귀하에게 있습니다. 보다 구체적으로, 귀하의 권한 정책에는 `s3:PutObject` 작업이 포함되어 있고, S3 버킷의 ARN을 지정하고, 평가 보고서를 암호화하는 데 사용되는 KMS 키가 포함됩니다. 사용할 수 있는 예제 정책은 AWS Audit Manager을 위한 ID 기반 정책 예제를 참조하세요.

> **Note**
>
> Audit Manager 데이터 암호화 설정을 변경하는 경우 이러한 변경 사항은 앞으로 새로 생성하는 평가에 적용됩니다. 여기에는 귀하의 새 평가에서 생성한 모든 평가 보고서가 포함됩니다. 암호화 설정을 변경하기 전에 생성한 기존 평가에는 변경 내용이 적용되지 않습니다. 여기에는 기존 평가 보고서와 함께 기존 평가에서 생성한 새 평가 보고서가 포함됩니다. 기존 평가 및 모

든 평가 보고서는 기존 KMS 키를 계속 사용합니다. 평가 보고서를 생성하는 IAM 자격 증명이 이전 KMS 키를 사용할 권한을 갖지 않는 경우, 귀하가 키 정책 수준에서 권한을 부여할 수 있습니다.

조직에서 멤버 계정의 연결을 해제하면 Audit Manager는 어떻게 되나요?

조직에서 멤버 계정을 연결 해제하면 Audit Manager는 이 사건에 대한 알림을 받습니다. 그러면 Audit Manager는 귀하의 기존 평가의 범위에 있는 계정 목록에서 해당 AWS 계정를 자동으로 제거합니다. 향후 새 평가의 범위를 지정하면 연결이 해제된 계정은 더 이상 적격 AWS 계정에 표시되지 않습니다.

Audit Manager가 평가 범위에 있는 계정 목록에서 연결되지 않은 회원 계정을 제거해도 이 변경 사항에 대한 알림은 귀하에게 고지되지 않습니다. 또한 연결이 해제된 멤버 계정으로 해당 계정에서 Audit Manager가 더 이상 활성화되지 않았다는 통지가 가지 않습니다.

회원 계정을 나의 조직에 다시 연결하면 어떻게 되나요?

회원 계정을 귀하의 조직에 다시 연결해도 해당 계정은 기존 Audit Manager 평가 범위에 자동으로 추가되지 않습니다. 하지만 평가 범위에 있는 계정을 지정하면 비로소 재연결된 회원 계정이 적격 AWS 계정으로 표시됩니다.

- 기존 평가의 경우 평가 범위를 수동으로 편집하여 재연결된 회원 계정을 추가할 수 있습니다. 지침은 범위 내 AWS 계정 편집을 참조하세요.
- 새 평가의 경우 평가 설정 중에 다시 연결된 계정을 추가할 수 있습니다. 지침은 범위 내 AWS 계정 지정을 참조하세요.

한 조직에서 다른 조직으로 구성원 계정을 마이그레이션하면 어떻게 되나요?

구성원 계정이 조직 1에서 Audit Manager를 활성화시킨 후 조직 2로 마이그레이션하면 결과적으로 Audit Manager는 조직 2에 대해 활성화되지 않습니다.

증거 찾기 문제 해결

이 페이지의 정보를 사용하여 Audit Manager의 일반적인 증거 찾기 문제를 해결하세요.

통상적인 증거 찾기 문제

- 증거찾기를 활성화할 수가 없습니다.
- 증거 찾기를 활성화했는데 검색 결과에 과거 증거가 보이지 않아요
- 증거 찾기 비활성화가 안 됩니다.
- 검색 쿼리가 실패했습니다.

증거 찾기 평가 보고서 문제

- 검색 결과로부터 여러 평가 보고서를 생성할 수가 없었습니다.
- 검색 결과로부터 얻은 특정 증거를 포함시킬 수가 없었습니다.
- 저의 모든 증거 찾기 결과가 평가 보고서에 포함되지 않습니다.
- 검색 결과로부터 평가 보고서를 생성하고 싶은데 쿼리 명령문이 실패합니다.
- 추가 리소스

증거 찾기 CSV 내보내기 문제

- 나의 CSV 내보내기가 실패했습니다.
- 검색 결과에서 특정 증거를 내보낼 수 없었습니다.
- 여러 CSV 파일을 한 번에 내보낼 수 없었습니다.

증거찾기를 활성화할 수가 없습니다.

증거찾기를 활성화할 수 없는 통상적인 이유로는 다음과 같은 상황이 있습니다.

현재 귀하에게 권한이 없습니다.

> 처음으로 증거 찾기를 활성화하려는 경우 필요한 권한이 있는지 확인하세요. 이러한 권한을 통해 CloudTrail Lake에서 이벤트 데이터 저장소를 생성하고 관리할 수 있으며, 이는 증거 찾기 검색 쿼리를 지원하는 데 필요합니다. 또한 권한을 통해 증거 찾기에서 검색 쿼리를 실행할 수 있습니다.
>
> 권한에 관하여 도움이 필요한 경우 귀하의 AWS 관리자에게 문의하세요. 귀하가 AWS 관리자인 경우 필요한 권한 설명을 복사하여 IAM 정책에 첨부할 수 있습니다.

귀하가 자신의 조직의 관리 계정을 사용하고 있습니다.

관리 계정을 사용하여 증거 찾기를 활성화할 수 없다는 점에 유의하세요. 위임된 관리자 계정으로 로그인하고 다시 시도해 주세요.

귀하가 이전에 증거 찾기를 비활성화했습니다.

증거 찾기를 다시 활성화하는 것은 현재 지원되지 않습니다. 이전에 증거 찾기를 비활성화한 경우 다시 활성화할 수 없습니다.

증거 찾기를 활성화했는데 검색 결과에 과거 증거가 보이지 않아요

증거 찾기를 활성화하면 과거 증거 데이터를 모두 사용할 수 있을 때까지 최대 7일이 걸립니다.

이 7일 동안 이벤트 데이터 저장소에는 지난 2년 분량의 증거 데이터가 가득 차게 됩니다. 즉, 증거 찾기를 활성화한 직후에 증거 찾기를 사용하면 채우기가 완료될 때까지 모든 결과가 이용 가능하지는 않습니다.

데이터 채우기 상태를 확인하는 방법에 대한 지침은 증거 찾기 상태 확인을 참조하세요.

증거 찾기 비활성화가 안 됩니다.

이 현상의 원인은 다음 중 하나일 수 있습니다.

현재 귀하에게 권한이 없습니다.

증거 찾기를 비활성화하려는 경우 필요한 권한이 귀하에게 있는지 확인합니다. 이러한 권한을 통해 증거 찾기를 비활성화하는 데 필요한 CloudTrail Lake의 이벤트 데이터 스토어를 업데이트하고 삭제할 수 있습니다.

권한에 관하여 도움이 필요한 경우 귀하의 AWS 관리자에게 문의하세요. 귀하가 AWS 관리자인 경우 필요한 권한 설명을 복사하여 IAM 정책에 첨부할 수 있습니다.

증거 찾기 활성화 요청이 아직 진행 중입니다.

증거 찾기를 활성화하도록 요청하면 증거 찾기 쿼리를 지원하는 이벤트 데이터 저장소가 생성됩니다. 이벤트 데이터 저장소가 생성되는 동안에는 증거 찾기를 비활성화할 수 없습니다.

계속하려면 이벤트 데이터 저장소가 생성될 때까지 기다린 후 다시 시도하세요. 자세한 내용은 증거 찾기 상태 확인을 참조하세요.

증거 찾기를 비활성화하도록 이미 요청하셨습니다.

증거 찾기 비활성화를 요청하면 증거 찾기 쿼리에 사용된 이벤트 데이터 저장소가 삭제됩니다. 이벤트 데이터 저장소가 삭제되는 동안 증거 찾기를 다시 비활성화하려고 하면 오류 메시지가 나타납니다.

이 경우에는 별도의 작업이 필요하지 않습니다. 이벤트 데이터 저장소가 삭제될 때까지 기다리세요. 이 작업이 완료되는 즉시 증거 찾기가 비활성화됩니다. 자세한 내용은 증거 찾기 상태 확인을 참조하세요.

검색 쿼리가 실패했습니다.

검색어 실패는 다음 원인 중 하나로 인해 발생할 수 있습니다.

현재 귀하에게 권한이 없습니다.

사용자가 검색 쿼리를 실행하고 검색 결과에 액세스하는 데 필요한 권한을 가지고 있는지 확인하세요. 특히 다음과 같은 CloudTrail 작업에 대한 권한이 필요합니다.

- StartQuery
- DescribeQuery
- CancelQuery
- GetQueryResults

권한에 관하여 도움이 필요한 경우 귀하의 AWS 관리자에게 문의하세요. 귀하가 AWS 관리자인 경우 필요한 권한 설명을 복사하여 IAM 정책에 첨부할 수 있습니다.

귀하는 현재 최대 수의 쿼리를 실행하고 있습니다.

쿼리는 한 번에 최대 5개까지 실행할 수 있습니다. 최대 수의 동시 쿼리를 실행하는 경우 `MaxConcurrentQueriesException` 오류가 발생합니다. 이 오류 메시지가 표시되면 일부 쿼리가 완료될 때까지 잠시 기다린 다음 쿼리를 다시 실행하세요.

귀하의 쿼리문에 검증 오류가 있습니다.

API 또는 CLI를 사용하여 CloudTrail Lake StartQuery 작업을 수행하는 경우 귀하의 `queryStatement`이 유효한지 확인하세요. 쿼리문에 검증 오류가 있거나, 잘못된 구문 또는 지원되지 않는 키워드가 있는 경우 `InvalidQueryStatementException`가 발생합니다.

쿼리 작성에 대한 자세한 내용은 AWS CloudTrail 사용 설명서의 쿼리 작성 또는 편집을 참조하세요.

유효한 구문의 예를 보려면 Audit Manager 이벤트 데이터 저장소를 쿼리하는 데 사용할 수 있는 다음 쿼리문 예시를 검토하세요.

예 1: 증거 및 규정 준수 상태 조사

이 예시에서는 지정된 날짜 범위 내에서 계정 내 모든 평가의 규정 준수 상태가 있는 증거를 찾습니다.

```
SELECT eventData.evidenceId, eventData.resourceArn,
 eventData.resourceComplianceCheck FROM $EDS_ID WHERE eventTime > '2022-11-02
 00:00:00.000' AND eventTime < '2022-11-03 00:00:00.000'
```

예 2: 제어에 대한 비준수 증거 결정

이 예시에서는 특정 평가 및 관리에 대해 지정된 날짜 범위의 규정을 준수하지 않는 모든 증거를 찾습니다.

```
SELECT * FROM $EDS_ID WHERE eventData.assessmentId = '11aa33bb-55cc-77dd-99ee-
ff22gg44hh66' AND eventTime > '2022-10-27 22:05:00.000' AND eventTime
 < '2022-11-03 22:05:00.000' AND eventData.resourceComplianceCheck IN
 ('NON_COMPLIANT','FAILED','WARNING') AND eventData.controlId IN ('aa11bb22-cc33-
dd44-ee55-ff66gg77hh88')
```

예 3: 이름별로 증거의 개수 계산

이 예시는 지정된 날짜 범위의 평가에 대한 전체 증거를 이름별로 그룹화하고 증거 수별로 정렬하여 나열합니다.

```
SELECT eventData.eventName as eventName, COUNT(*) as totalEvidence FROM  $EDS_ID
 WHERE eventData.assessmentId = '11aa33bb-55cc-77dd-99ee-ff22gg44hh66' AND eventTime
 > '2022-10-27 22:05:00.000' AND eventTime < '2022-11-03 22:05:00.000' GROUP BY
 eventData.eventName ORDER BY totalEvidence DESC
```

예 4: 데이터 소스 및 서비스별 증거 탐색

이 예시에서는 특정 데이터 소스 및 서비스에 대해 지정된 날짜 범위의 모든 증거를 찾습니다.

```
SELECT * FROM $EDS_ID WHERE eventTime > '2022-10-27 22:05:00.000' AND eventTime
 < '2022-11-03 22:05:00.000' AND eventData.service IN ('dynamodb') AND
 eventData.dataSource IN ('AWS API calls')
```

예 5: 데이터 소스 및 제어 도메인별로 규정을 준수하는 증거 살펴보기

이 예시에서는 AWS Config가 아닌 데이터 소스에서 증거를 가져오는 특정 제어 도메인에 대한 규정 준수 증거를 찾습니다.

```
SELECT * FROM $EDS_ID WHERE eventData.resourceComplianceCheck IN
('PASSED','COMPLIANT') AND eventData.controlDomainName IN ('Logging and
monitoring','Data security and privacy') AND eventData.dataSource NOT IN ('AWS
Config')
```

기타 API 예외

StartQuery API는 여러 가지 다른 이유로 실패할 수 있습니다. 가능한 오류 및 설명의 전체 목록은 AWS CloudTrail API 참조의 StartQuery 오류를 참조하세요.

검색 결과로부터 여러 평가 보고서를 생성할 수가 없었습니다.

이 오류는 동시에 너무 많은 CloudTrail Lake 쿼리를 실행하여 발생합니다.

검색 결과를 그룹화하고 그룹화된 결과의 각 라인 항목에 대한 평가 보고서를 즉시 생성하려고 하면 이 오류가 발생할 수 있습니다. 검색 결과를 가져와 평가 보고서를 생성하면 각 작업에서 쿼리가 호출됩니다. 한 번에 최대 5개의 쿼리만 실행할 수 있습니다. 최대 수의 동시 쿼리를 실행하는 경우 `MaxConcurrentQueriesException` 오류 반응이 표시됩니다.

이 오류를 방지하려면 한 번에 너무 많은 평가 보고서를 생성하지 않도록 하세요. 최대 수의 동시 쿼리를 실행하는 경우 `MaxConcurrentQueriesException` 오류 반응이 표시됩니다. 이 오류 메시지가 표시되면 진행 중인 평가 보고서가 완료될 때까지 몇 분 정도 기다리세요.

Audit Manager 콘솔의 다운로드 센터 페이지에서 평가 보고서의 상태를 확인할 수 있습니다. 보고서가 완성되면 증거 찾기에서 그룹화된 결과로 돌아가세요. 그런 다음 계속해서 결과를 얻고 각 항목에 대한 평가 보고서를 생성할 수 있습니다.

검색 결과로부터 얻은 특정 증거를 포함시킬 수가 없었습니다.

귀하의 모든 검색 결과가 평가 보고서에 포함됩니다. 검색 결과 세트에서 개별 행을 선택적으로 추가할 수는 없습니다.

평가 보고서에 특정 검색 결과만 포함하려면 현재 검색 필터를 편집하는 것이 좋습니다. 이렇게 하면 보고서에 포함하려는 증거만 대상으로 검색 결과를 좁힐 수 있습니다.

저의 모든 증거 찾기 결과가 평가 보고서에 포함되지 않습니다.

평가 보고서를 생성할 때 추가할 수 있는 증거의 양에는 제한이 있습니다. 이러한 한도는 귀하의 평가 보고서의 AWS 리전, 평가 보고서 대상으로 사용되는 S3 버킷의 지역, 평가에서 고객 관리형 AWS KMS key가 사용되는지 여부 등에 기초합니다.

1. 동일 지역 보고서의 한도는 22,000(S3 버킷과 평가가 동일한 AWS 리전 내에 있는 경우)입니다.
2. 지역 간 보고서(S3 버킷과 평가가 서로 다른 AWS 리전 내에 있는 경우)의 경우 한도는 3,500입니다.
3. 고객 관리형 KMS 키를 사용하는 평가의 경우 한도는 3,500입니다.

이 한도를 초과할 경우 보고서가 계속 생성됩니다. 그러나 Audit Manager는 보고서에 처음 3,500개 또는 22,000개의 증거 항목만 추가합니다.

이 문제를 방지하려면 현재 검색 필터를 편집하는 것이 좋습니다. 이렇게 하면 적은 양의 증거를 대상으로 하여 검색 결과를 줄일 수 있습니다. 필요한 경우 이 방법을 반복하여 하나의 큰 보고서 대신 여러 평가 보고서를 생성할 수 있습니다.

검색 결과로부터 평가 보고서를 생성하고 싶은데 쿼리 명령문이 실패합니다.

CreateAssmentReport API를 사용 중이고 쿼리문에서 유효성 검사 예외가 표시되는 경우, 아래 표에서 해결 방법에 대한 지침을 확인하세요.

> **Note**
>
> 쿼리 명령문이 CloudTrail에서 작동하더라도 Audit Manager에서 평가 보고서를 생성하는 데는 동일한 쿼리가 유효하지 않을 수 있습니다. 이는 두 서비스 간에 쿼리 검증이 약간 다르기 때문입니다.

문구	문제	솔루션	주의
`SELECT`	SELECT 문구에는 열 이름이 포함되어 있습니다.	SELECT 문구를 제거하고 `SELECT eventJson` 로 바꿉니다.	`SELECT eventJson` 만 지원됩니다. 이 검증은 Audit Manager에서 처리합니다.

문구	문제	솔루션	주의
FROM	FROM 문구에 잘못된 이벤트 데이터 저장소 ID가 포함되어 있습니다. 또는 제공된 이벤트 데이터 저장소 ID가 귀하의 Audit Manager 설정의 이벤트 데이터 저장소 ID와 일치하지 않습니다.	edsID의 값이 귀하의 Audit Manager 설정에 지정된 이벤트 데이터 저장소 ID와 일치하는 경우, FROM 문구를 제거하고 FROM *edsID*로 바꾸세요. Audit Manager 설정에서 이벤트 데이터 스토어의 ARN을 검색할 수 있습니다. 자세한 내용은 AWS Audit Manager API 참조 내 GetSettings를 참조하세요.	이 검증은 Audit Manager에서 처리합니다.
GROUP BY	쿼리에 GROUP BY 문구가 있습니다.	GROUP BY 문구를 삭제합니다.	이 검증은 Audit Manager에서 처리합니다.
HAVING	쿼리에 HAVING 문구가 있습니다.	HAVING 문구를 삭제합니다.	이 검증은 Audit Manager에서 처리합니다.
LIMIT	LIMIT 문구에 최대 허용 한도를 초과하는 값이 포함되어 있습니다.	LIMIT 문구가 있는 경우 그 값이 지원되는 최대 한도 이하인지 확인하세요. • 동일 지역 보고서의 경우 한도는 22,000입니다. • 지역 간 보고서의 경우 한도는 3,500입니다. • 관련 평가에서 고객 관리형 AWS KMS key을 사용하는 보고서의 경우 한도는 3,500입니다.	콘솔에서는 제공할 수 있는 증거 결과의 수에는 제한이 없습니다. 하지만 평가 보고서를 생성할 때 포함할 수 있는 증거의 양에는 제한이 적용됩니다. 쿼리 명령문에 LIMIT 값이 제공되지 않은 경우 기본 최대 한도가 적용됩니다. 이 검증은 Audit Manager에서 처리합니다.

문구	문제	솔루션	주의
ORDER BY	ORDER BY 문구에는 SELECT 문구에 없는 집계 함수 또는 별칭이 포함되어 있습니다.	집계 함수 또는 별칭을 사용하여 ORDER BY 문구에 조건이 포함되어 있지 않은지 확인합니다.	이 검증은 CloudTrail StartQuery API에 의해 처리됩니다.
WHERE	WHERE 문구에는 복수의 assessmentId 가 포함되어 있습니다. 또는 WHERE 문구에 귀하의 createAssessmentReport 요청 내 assessmentId 과 일치하지 않는 assessmentId 이 포함되어 있습니다. 또는 WHERE 문구에 지원되지 않는 열 이름이 포함되어 있습니다.	AssessmentID가 하나만 지정되고 이것이 귀하가 createAssessmentReport API 요청에서 지정한 AssessmentID 매개변수와 일치하는지 확인하세요. 지원되지 않는 열 이름을 제거합니다.	이 검증은 CloudTrail StartQuery API에 의해 처리됩니다.

예시

다음 예시는 CreateAssessmentReport 작업을 호출할 때 queryStatement 매개변수를 사용하는 방법을 보여줍니다. 이러한 쿼리를 사용하기 전에 ##### ###를 귀하 자신의 edsId 및 assessmentId 값으로 바꾸세요.

예 1: 보고서 생성(동일 지역 제한 적용)

이 예시에서는 2022년 1월 22일부터 23일 사이에 생성된 S3 버킷에 대한 결과가 포함된 보고서를 생성합니다.

```
SELECT eventJson FROM 12345678-abcd-1234-abcd-123456789012 WHERE eventData.assessmentId
 = '11aa33bb-55cc-77dd-99ee-ff22gg44hh66' AND eventTime > '2022-01-22 00:00:00.000' AND
 eventTime < '2022-01-23 00:00:00.000' AND eventName='CreateBucket' LIMIT 22000
```

예 2: 보고서 생성(지역 간 제한 적용)

이 예시에서는 날짜 범위를 지정하지 않고 지정된 이벤트 데이터 저장소 및 평가에 대한 모든 결과가 포함된 보고서를 생성합니다.

```
SELECT eventJson FROM 12345678-abcd-1234-abcd-123456789012 WHERE eventData.assessmentId
 = '11aa33bb-55cc-77dd-99ee-ff22gg44hh66' LIMIT 7000
```

예제 3: 보고서 생성(기본 한도 미만)

이 예시에서는 지정된 이벤트 데이터 저장소 및 평가에 대한 모든 결과를 포함하는 보고서를 생성합니다. 이 한도는 기본 최대값보다 작습니다.

```
SELECT eventJson FROM 12345678-abcd-1234-abcd-123456789012 WHERE eventData.assessmentId
 = '11aa33bb-55cc-77dd-99ee-ff22gg44hh66' LIMIT 2000
```

추가 리소스

다음 페이지에는 평가 보고서에 대한 일반적인 문제 해결 지침이 포함되어 있습니다.

- 평가 보고서 문제 해결

나의 CSV 내보내기가 실패했습니다.

CSV 내보내기는 여러 이유로 실패할 수 있습니다. 가장 빈번한 원인을 확인하여 이 문제를 해결할 수 있습니다.

먼저 CSV 내보내기 기능을 사용하기 위한 다음과 같은 사전 조건을 충족하였는지 확인하세요.

증거 찾기를 성공적으로 활성화했습니다

귀하가 증거 찾기를 활성화하지 않은 경우 검색 쿼리를 실행하고 검색 결과를 내보낼 수 없습니다.

이벤트 데이터 저장소 채우기가 완료되었습니다

증거 찾기를 활성화한 후 즉시 사용하는데 증거 채우기가 아직 진행 중인 경우 일부 결과가 제공되지 않을 수 있습니다. 채우기 상태를 확인하려면 증거 찾기 상태 확인을 참조하세요.

귀하의 검색 쿼리가 성공했습니다

Audit Manager는 실패한 쿼리의 결과를 내보낼 수 없습니다. 실패한 쿼리 문제를 해결하려면 검색 쿼리가 실패했습니다.을 참조하세요.

사전 요구 사항을 충족하는지 확인한 후 다음 체크리스트를 사용하여 잠재적 문제를 확인하세요.

1. 귀하의 검색 쿼리의 상태를 다음과 같이 확인합니다.
   a. 쿼리가 취소되었나요? 증거 찾기는 쿼리가 취소되기 전에 처리된 부분적인 결과를 표시합니다. 하지만 Audit Manager는 부분적인 결과를 S3 버킷이나 다운로드 센터로 내보내지 않습니다.
   b. 쿼리가 1시간 넘게 실행되었나요? 한 시간 이상 실행되는 쿼리는 시간이 초과될 수 있습니다. 증거 찾기는 쿼리가 시간 초과되기 전에 처리된 부분적인 결과를 표시합니다. 하지만 Audit Manager는 부분적인 결과를 내보내지 않습니다. 시간 초과를 피하려면 검색 쿼리를 편집하여 더 좁은 시간 범위를 지정하여 스캔되는 증거의 양을 줄일 수 있습니다.
2. 내보내기 대상 S3 버킷의 이름과 URI를 확인하세요.
   a. 귀하가 지정한 버킷이 존재하나요? 버킷 URI를 수동으로 입력했다면 잘못 입력하지 않았는지 확인하세요. Audit Manager가 CSV 파일을 Amazon S3로 내보내려고 할 때 오타나 잘못된 URI로 인해 `RESOURCE_NOT_FOUND` 오류가 발생할 수 있습니다.
3. 내보내기 대상 S3 버킷의 권한을 확인하세요.
   a. S3 버킷에 대한 쓰기 권한이 있나요? 내보내기 대상으로 사용 중인 S3 버킷에 대한 쓰기 권한을 귀하가 가지고 있어야 합니다. 좀 더 구체적으로 말하자면, IAM 권한 정책에는 `s3:PutObject` 작업과 버킷 ARN이 포함되어야 하고 CloudTrail을 서비스 주체로 기재해야 합니다. 귀하가 사용할 수 있는 정책 예시를 제공합니다. 다른 S3 버킷을 사용하는 방법에 대한 지침은 내보내기 대상 설정을 참조하세요.
4. AWS 리전 정보가 일치하지 않는지 확인하세요.
   a. 귀하의 고객 관리 키의 AWS 리전가 귀하의 평가의 AWS 리전과 일치하나요? 귀하가 데이터 암호화를 위하여 고객 관리 키를 제공한 경우 해당 키는 귀하의 평가와 동일한 AWS 리전 내에 있어야 합니다. KMS 키를 변경하는 방법에 대한 지침은 데이터 암호화 설정을 참조하세요.
5. 위임된 관리자 계정의 권한을 확인하세요.
   a. 귀하의 Audit Manager 설정의 고객 관리 키는 위임된 관리자에게 권한을 부여합니까? 위임된 관리자 계정을 사용하고 있고 데이터 암호화를 위한 고객 관리 키를 지정하셨다면 위임된 관리

자가 해당 KMS 키에 액세스할 수 있는지 확인하세요. 자세한 내용은 AWS Key Management Service 개발자 안내서의 다른 계정의 사용자에게 KMS 키를 사용하도록 허용을 참조하세요. Audit Manager에서 암호화 설정을 검토하고 변경하려면 데이터 암호화 설정을 참조하세요.

> **Note**
>
> Audit Manager 데이터 암호화 설정을 변경하는 경우 이러한 변경 사항은 앞으로 새로 생성하는 평가에 적용됩니다. 여기에는 새 평가에서 내보낸 모든 CSV 파일이 포함됩니다.
> 암호화 설정을 변경하기 전에 생성한 기존 평가에는 변경 내용이 적용되지 않습니다. 여기에는 기존 CSV 내보내기뿐 아니라 기존 평가의 새 CSV 내보내기도 포함됩니다. 기존 평가 및 모든 CSV 내보내기는 기존 KMS 키를 계속 사용합니다. CSV 파일을 내보내는 IAM 자격 증명이 이전 KMS 키를 사용할 권한을 갖지 않는 경우 키 정책 수준에서 권한을 부여할 수 있습니다.

검색 결과에서 특정 증거를 내보낼 수 없었습니다.

모든 검색 결과가 결과에 포함됩니다.

CSV 파일에 특정 증거만 포함하려면 현재 검색 필터를 편집하는 것이 좋습니다. 이렇게 하면 내보내려는 증거만 대상으로 검색 결과를 좁힐 수 있습니다.

여러 CSV 파일을 한 번에 내보낼 수 없었습니다.

이 오류는 동시에 너무 많은 CloudTrail Lake 쿼리를 실행하여 발생합니다.

검색 결과를 그룹화하고 그룹화된 결과의 각 라인 항목에 대한 CSV 파일을 즉시 내보내려고 하면 이런 일이 발생할 수 있습니다. 검색 결과를 가져와서 CSV 파일을 내보내는 경우 이러한 각 작업을 수행하면 쿼리가 호출됩니다. 한 번에 최대 5개의 쿼리만 실행할 수 있습니다. 최대 수의 동시 쿼리를 실행하는 경우 `MaxConcurrentQueriesException` 오류 반응이 표시됩니다.

이 오류를 방지하려면 한 번에 너무 많은 CSV 파일을 내보내지 않도록 하세요.

이 오류를 해결하려면 진행 중인 CSV 내보내기가 완료될 때까지 기다리세요. 대부분의 내보내기에는 몇 분이 소요됩니다. 그러나 매우 많은 양의 데이터를 내보내는 경우 내보내기를 완료하는 데 최대 1시간이 걸릴 수 있습니다. 내보내기가 진행되는 동안에는 증거 찾기를 사용하지 않아도 됩니다.

Audit Manager 콘솔의 다운로드 센터에서 내보내기 상태를 확인할 수 있습니다. 내보낸 파일이 준비되면 증거 찾기에서 그룹화된 결과로 돌아가세요. 그런 다음 계속해서 결과를 얻고 각 라인 항목에 대한 CSV 파일을 내보낼 수 있습니다.

프레임워크 공유 문제 해결

이 페이지의 정보를 사용하여 Audit Manager에서 일반적인 프레임워크 공유 문제를 해결할 수 있습니다.

주제

내가 보낸 공유 요청 상태가 실패로 표시됩니다.

사용자 지정 프레임워크를 공유하려고 하는데 작업이 실패하는 경우라면 다음 사항을 확인하는 것이 좋습니다.

1. 수신자 AWS 계정 및 지정된 지역에서 Audit Manager가 활성화되어 있는지 확인하세요. 지원되는 AWS Audit Manager 리전을 보려면 Amazon Web Services 일반 참조의AWS Audit Manager 엔드포인트 및 할당량을 참조하세요.
2. Recipeint 계정을 지정할 때 올바른 AWS 계정 ID를 입력했는지 확인하세요.
3. AWS Organizations 관리 계정을 수신자로 지정하지 않았는지 확인하세요. 사용자 지정 프레임워크를 위임된 관리자와 공유할 수 있지만 사용자 지정 프레임워크를 관리 계정과 공유하려고 하면 작업이 실패합니다.
4. 고객 관리 키를 사용하여 Audit Manager 데이터를 암호화하는 경우 KMS 키가 활성화되어 있는지 확인하세요. KMS 키가 비활성화된 상태에서 사용자 지정 프레임워크를 공유하려고 하면 작업이 실패합니다. 비활성화된 KMS 키를 활성화하는 방법에 대한 지침은 AWS Key Management Service 개발자 안내서의 키 활성화 및 비활성화를 참조하세요.

공유 요청 옆에 파란색 점이 있습니다. 이것은 무엇을 의미하나요?

파란색 점 알림은 공유 요청에 주목하시라는 뜻입니다.

Sender를 위한 블루닷 알림

만료 중 상태인 전송된 공유 요청 옆에 파란색 알림 점이 나타납니다. Audit Manager는 공유 요청이 만료되기 전에 수신자에게 공유 요청에 대해 조치를 취하도록 상기시킬 수 있도록 파란색 점 알림을 표시합니다.

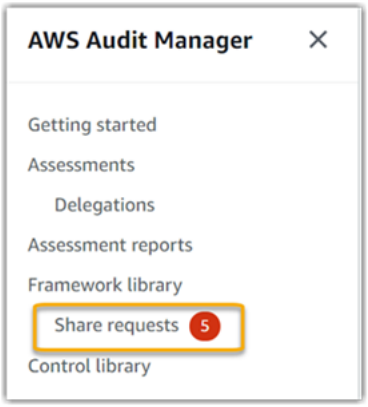
파란색 알림 점이 사라지게 하려면 수신자가 요청을 수락하거나 거부해야 합니다. 공유 요청을 취소하면 파란색 점도 사라집니다.

다음 절차를 사용하여 만료될 공유 요청이 있는지 확인하고 수신자에게 조치를 취하라는 선택적 알림을 보낼 수 있습니다.

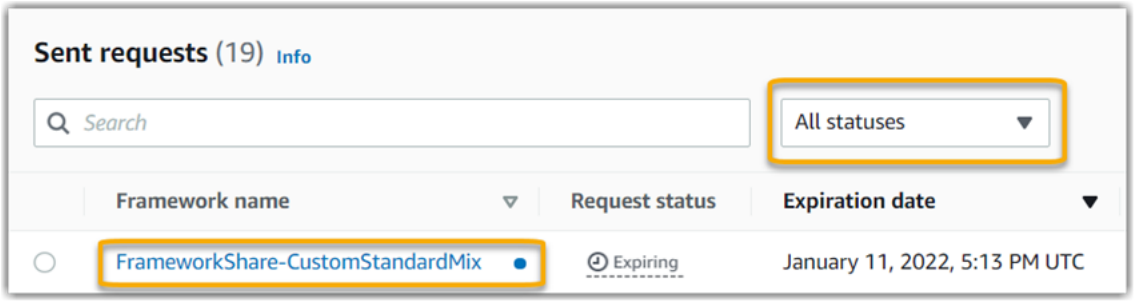
전송된 요청에 대한 알림을 보려면

1. https://console.aws.amazon.com/auditmanager/home에서 AWS Audit Manager 콘솔을 엽니다.
2. 공유 요청 알림이 있는 경우 Audit Manager는 탐색 메뉴 아이콘 옆에 빨간색 점을 표시합니다.

3. 탐색 창을 펼치고 공유 요청 옆을 살펴보십시오. 알림 뱃지는 주의가 필요한 공유 요청의 수를 나타냅니다.



4. 요청 공유를 선택한 다음 전송된 요청 탭을 선택합니다.
5. 파란색 점을 찾아 향후 30일 이내에 만료되는 공유 요청을 찾아보세요. 또는 모든 상태 필터 드롭다운에서 만료 중을 선택하여 만료되는 공유 요청을 볼 수도 있습니다.



6. (선택 사항)공유 요청이 만료되기 전에 수신자에게 공유 요청에 대해 조치를 취해야 한다는 점을 상기시키세요. 공유 요청이 활성 상태이거나 만료 중이면 Audit Manager가 콘솔에서 알림을 보내 수신자에게 알리므로 이 단계는 선택 사항입니다. 하지만 선호하는 커뮤니케이션 채널을 사용하여 수신자에게 직접 알림을 보낼 수도 있습니다.

수신자를 위한 블루닷 알림

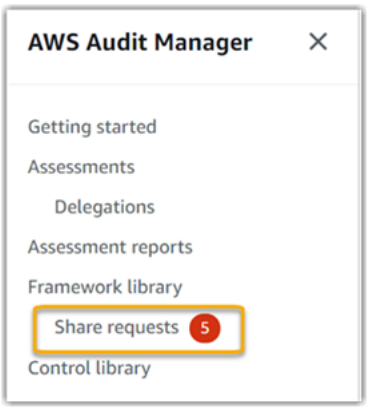
활성 또는 만료 중 상태인 수신된 공유 요청 옆에 파란색 알림 점이 나타납니다. Audit Manager는 공유 요청이 만료되기 전에 조치를 취하도록 알려주는 파란색 점 알림을 표시합니다. 파란색 알림 점이 사라지게 하려면 요청을 수락하거나 거부해야 합니다. 발신자가 공유 요청을 취소하는 경우에도 파란색 점이 사라집니다.

다음 절차를 사용하여 활성 공유 요청과 만료 중인 공유 요청을 확인할 수 있습니다.

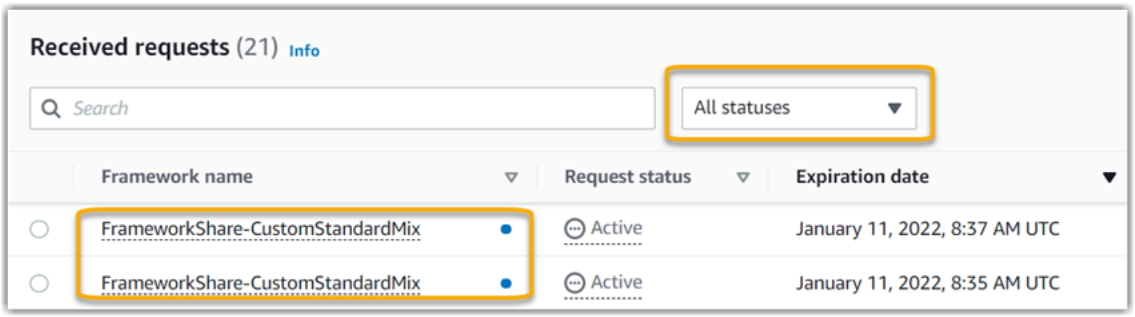
수신된 요청에 대한 알림을 보려면

1. https://console.aws.amazon.com/auditmanager/home에서 AWS Audit Manager 콘솔을 엽니다.
2. 공유 요청 알림이 있는 경우 Audit Manager는 탐색 메뉴 아이콘 옆에 빨간색 점을 표시합니다.

3. 탐색 창을 펼치고 공유 요청 옆을 살펴보십시오. 알림 배지는 주의가 필요한 공유 요청의 수를 나타냅니다.



4. 요청 공유를 선택합니다. 기본적으로 이 페이지는 수신된 요청 탭에서 열립니다.
5. 파란색 점이 있는 항목을 찾아 조치가 필요한 공유 요청을 식별하십시오.



6. (선택 사항)향후 30일 이내에 만료되는 요청만 보려면 모든 상태 드롭다운 목록을 찾아 만료 중을 선택합니다.

내 공유 프레임워크에는 사용자 지정 AWS Config 규칙을 데이터 소스로 사용하는 제어가 있습니다. 수신자가 이러한 제어에 대한 증거를 수집할 수 있나요?

예. 수신자는 이러한 규제 요건에 대한 증거를 수집할 수 있지만, 이를 위해서는 몇 가지 단계가 필요합니다.

Audit Manager가 AWS Config 규칙을 데이터 소스 매핑으로 사용하여 증거를 수집하려면 다음 조건을 충족해야 합니다. 이러한 기준은 관리형 규칙과 사용자 지정 규칙 모두에 적용됩니다.

- 규칙이 수신자의 AWS 환경에 존재해야 합니다.
- 수신자의 AWS 환경에서 규칙을 활성화해야 합니다.

귀하의 계정의 AWS Config 규칙은 수신자의 AWS 환경에 이미 존재하지 않을 가능성이 높다는 점을 기억하세요. 또한 수신자가 공유 요청을 수락하면 Audit Manager는 해당 계정에 사용자 지정 규칙을 다시 만들지 않습니다. 수신자가 사용자 지정 규칙을 데이터 소스 매핑으로 사용하여 증거를 수집하려면 수신자가 자신의 AWS Config 인스턴스에 동일한 사용자 지정 규칙을 만들어야 합니다. 수신자가 규칙을 AWS Config에서 생성하고 활성화한 후 Audit Manager는 해당 데이터 소스에서 증거를 수집할 수 있습니다.

귀하는 수신자와 통신하여 AWS Config 인스턴스에서 사용자 지정 AWS Config 규칙을 만들어야 하는지 알려주는 것이 좋습니다.

공유 프레임워크에서 사용되는 사용자 지정 규칙을 업데이트했습니다. 제가 취해야 할 조치가 있습니까?

귀하의 AWS 환경 내 규칙 업데이트용

귀하의 AWS 환경 내에서 사용자 지정 규칙을 업데이트하는 경우 Audit Manager에서 별도의 조치를 취할 필요가 없습니다. Audit Manager는 다음 표에 설명된 방식으로 규칙 업데이트를 탐지하고 처리합니다. Audit Manager는 규칙 업데이트가 감지된 경우 사용자에게 알리지 않습니다.

시나리오	Audit Manager의 역할	알아야 할 내용
귀하의 AWS Config 인스턴스에서 사용자 지정 규칙이 업데이트되었습니다.	Audit Manager는 업데이트된 규칙 정의를 사용하여 해당 규칙에 대한 결과를 계속 보고합니다.	별도의 작업은 필요없습니다.
귀하의 AWS Config 인스턴스에서 사용자 지정 규칙이 삭제됩니다.	Audit Manager는 삭제된 규칙에 대한 결과 보고를 중단합니다.	별도의 작업은 필요없습니다. 원하는 경우 삭제된 규칙을 데이터 소스 매핑으로 사용한 사용자 지정 제어를 편집할 수 있습니다. 그런 다음 귀하는 삭제된 규칙을 제거하여 제어의 데이터 소스 설정을 정리할 수 있습니다. 그렇지 않으면 삭제된 규칙 이름이 사용되지 않은 데이터 소스 매핑으로 남습니다.

귀하의 AWS 환경 외부에서 규칙을 업데이트하려면

수신자 AWS 환경에서 Audit Manager는 규칙 업데이트를 감지하지 못합니다. 발신자와 수신자가 각각 별도의 AWS 환경에서 작업하기 때문입니다. 다음 표에서는 이 시나리오에 대한 권장 조치를 제공합니다.

귀하의 역할	시나리오	권장 조치
Sender	• 귀하는 사용자 지정 규칙을 데이터 소스 매핑으로 사용하는 프레임워크를 공유했습니다. • 프레임워크를 공유한 후 AWS Config 내에서 해당 규칙 중 하나를 업데이트하거나 삭제했습니다.	수신자에게 연락하여 업데이트에 대해 알려주세요. 이렇게 하면 동일한 업데이트를 수행하고 최신 규칙 정의와 동기화된 상태를 유지할 수 있습니다.
Recipie	• 귀하는 사용자 지정 규칙을 데이터 소스 매핑으로 사용하는 공유 프레임워크를 수락했습니다. • 귀하의 AWS Config 인스턴스에서 사용자 지정 규칙을 다시 만든 후 sender가 해당 규칙 중 하나를 업데이트하거나 삭제했습니다.	귀사 자신의 AWS Config 인스턴스에서 규칙을 그에 따라 업데이트하세요.

알림 문제 해결

이 페이지의 정보를 사용하여 Audit Manager의 일반적인 알림 문제를 해결할 수 있습니다.

주제

- Audit Manager에서 Amazon SNS 주제를 지정했지만 알림을 받지 못했습니다.
- FIFO 주제를 지정했지만 알림이 예상한 순서대로 수신되지 않습니다.

Audit Manager에서 Amazon SNS 주제를 지정했지만 알림을 받지 못했습니다.

Amazon SNS 주제가 서버 측 암호화(SSE)를 위해 AWS KMS를 사용한다면, AWS KMS 키 정책에 필요한 권한을 상실할 수 있습니다. 주제에 대한 엔드포인트를 신청하지 않은 경우 알림을 받지 못할 수도 있습니다.

알림이 수신되지 않으면 다음을 수행했는지 확인하세요.

- 필요한 권한 정책을 KMS 키에 연결했습니다. 예시 정책은 이 가이드의 알림 페이지에서 확인할 수 있습니다.
- 알림이 전송되는 주제에 대해 엔드포인트를 신청했습니다. 이메일 엔드포인트를 주제에 대해 신청하면 신청의 확인을 요청하는 이메일을 받게 됩니다. 알림을 받기 시작하려면 신청을 확인해야 합니다. 자세한 내용은 Amazon SNS 개발자 안내서에서 시작하기를 참조하세요.

FIFO 주제를 지정했지만 알림이 예상한 순서대로 수신되지 않습니다.

Audit Manager는 FIFO SNS 주제에 대한 알림 전송을 지원합니다. 하지만 Audit Manager가 FIFO 주제에 알림을 보내는 순서는 보장되지 않습니다.

권한 및 액세스 문제 해결

이 페이지의 정보를 사용하여 Audit Manager의 일반적인 권한 문제를 해결할 수 있습니다.

주제

- Audit Manager 설정 절차를 따랐지만 IAM 권한이 충분하지 않습니다.
- 특정인을 감사 소유자로 지정했지만 여전히 평가에 대한 전체 액세스 권한이 없습니다. 왜 그런가요?
- Audit Manager에서 작업을 수행할 수 없습니다.
- 내 AWS 계정 외부인이 내 Audit Manager 리소스에 액세스할 수 있게 허용하고자 합니다.
- 다음 사항도 참조하세요.

Audit Manager 설정 절차를 따랐지만 IAM 권한이 충분하지 않습니다.

Audit Manager에 액세스하기 위해 귀하가 사용하는 사용자, 역할 및 그룹은 필수 권한이 있어야 합니다. 그 뿐 아니라 귀하의 자격 증명 기반 정책은 지나치게 제한적이어서는 안 됩니다. 그렇지 않으면 콘

솔이 의도한 대로 작동하지 않습니다. 이 안내서의 설정 절차는 Audit Manager를 설정하는 데 필요한 최소 권한을 부여하는 정책을 제공합니다. 사용 사례에 따라 더 광범위하고 덜 제한적인 권한이 필요할 수 있습니다. 예를 들어 감사 소유자가 관리자 액세스 권한을 갖는 것이 좋습니다. 이를 통해 감사 소유자가 Audit Manager 설정을 수정하고 평가, 프레임워크, 제어 및 평가 보고서와 같은 리소스를 관리할 수 있습니다. 대리인과 같은 다른 사용자에게는 관리 액세스 권한 또는 읽기 전용 액세스만 필요할 수 있습니다.

사용자, 역할 또는 그룹에 적절한 권한을 추가했는지 확인하세요. 감사 소유자에게 권장되는 정책은 AWSAuditManagerAdministratorAccess입니다. 대리인의 경우 IAM 정책 예시 페이지에 제공된 이 예시를 사용할 수 있습니다. 이러한 예시 정책을 시작점으로 사용하여 필요에 따라 요구 사항에 맞게 변경할 수 있습니다.

시간을 내어 특정 요구 사항에 맞게 권한을 사용자 지정하는 것이 좋습니다. IAM 권한에 대한 도움이 필요한 경우 관리자 또는 AWS 지원에 문의하세요.

특정인을 감사 소유자로 지정했지만 여전히 평가에 대한 전체 액세스 권한이 없습니다. 왜 그런가요?

누군가를 감사 소유자로 지정하는 것만으로는 평가에 대한 전체 액세스 권한을 얻을 수 없습니다. 또한 감사 소유자는 Audit Manager 리소스에 액세스하고 관리하는 데 필요한 IAM 권한이 있어야 합니다. 즉, 특정 사용자를 감사 소유자로 지정하는 것 외에도 필요한 IAM 정책을 해당 사용자에게 연결해야 합니다. 이를 뒷받침하는 기본 개념은 두 가지를 모두 요구함으로써 Audit Manager가 각 평가의 모든 세부 사항을 완벽하게 제어할 수 있도록 한다는 것입니다.

> **Note**
>
> 감사 소유자의 경우 귀하는 AWSAuditManagerAdministratorAccess 정책을 사용하는 것이 좋습니다. 자세한 내용은 Audit Manager의 사용자 인격체에 대한 권장 정책을 참조하세요.

Audit Manager에서 작업을 수행할 수 없습니다.

AWS Audit Manager 콘솔 또는 Audit Manager API 작업을 사용하는 데 필요한 권한이 없는 경우 `AccessDeniedException` 오류가 발생할 수 있습니다.

이 문제를 해결하려면 관리자에게 문의하여 도움을 받아야 합니다. 관리자는 로그인 보안 인증 정보를 제공한 사람입니다.

내 AWS 계정 외부인이 내 Audit Manager 리소스에 액세스할 수 있게 허용하고자 합니다.

다른 계정의 사용자 또는 조직 외부의 사람이 리소스에 액세스하는 데 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.

- Audit Manager에서 이러한 기능을 지원하는지 여부를 알아보려면 IAM의 AWS Audit Manager 작동 방식 섹션을 참조하세요.
- 소유하고 있는 AWS 계정의 리소스에 대한 액세스 권한을 제공하는 방법을 알아보려면 IAM 사용자 설명서의 자신이 소유한 다른 AWS 계정의 IAM 사용자에 대한 액세스 권한 제공을 참조하세요.
- 리소스에 대한 액세스 권한을 서드 파티 AWS 계정에게 제공하는 방법을 알아보려면 IAM 사용자 설명서의 서드 파티가 소유한 AWS 계정에 대한 액세스 제공을 참조하세요.
- ID 페더레이션을 통해 액세스 권한을 제공하는 방법을 알아보려면 IAM 사용자 설명서의 외부에서 인증된 사용자에게 액세스 권한 제공(ID 페더레이션)을 참조하세요.
- 크로스 계정 액세스를 위한 역할과 리소스 기반 정책 사용의 차이점을 알아보려면 IAM 사용자 설명서의 IAM 역할과 리소스 기반 정책의 차이를 참조하세요.

다음 사항도 참조하세요.

다음 페이지에는 권한 누락으로 인해 발생할 수 있는 기타 문제에 대한 문제 해결 지침이 포함되어 있습니다.

- 나의 평가에서 제어항목이나 제어 세트를 볼 수 없습니다
- 제어 데이터 소스를 구성할 때는 사용자 지정 규칙 옵션을 사용할 수 없습니다.
- 평가 보고서를 생성하려고 할 때 액세스 거부 오류가 발생합니다.
- 위임된 관리자 계정을 사용하여 평가 보고서를 생성하려고 하면 액세스 거부 오류가 발생합니다.
- 증거찾기를 활성화할 수가 없습니다
- 증거 찾기 비활성화가 안 됩니다
- 증거 찾기에서 검색 쿼리가 실패했습니다.
- Audit Manager에서 Amazon SNS 주제를 지정했지만 알림을 받지 못했습니다.

AWS Audit Manager의 할당량 및 제한

AWS 계정에는 각 AWS 서비스에 대한 기본 할당량(이전에는 제한이라고 함)이 있습니다. 다르게 표시되지 않는 한, 리전별로 각 할당량이 적용됩니다. 일부 할당량에 대한 증가를 요청할 수 있으며 다른 할당량은 늘릴 수 없습니다.

전부는 아니지만 Audit Manager 할당량의 대부분은 Service Quotas 콘솔에서 AWS Audit Manager 네임스페이스 아래에 나열됩니다. 할당량 증가를 요청하는 방법에 대해서는 Audit Manager 할당량 관리 단원을 참조하십시오.

기본 Audit Manager 할당량

다음 AWS Audit Manager 할당량은 리전별 AWS 계정당 적용됩니다.

평가

- 계정당 활성 평가 수: 100건

평가 보고서

- 평가 보고서에 추가할 수 있는 증거 항목 수:
  - 동일 지역 보고서의 경우(평가 및 평가 보고서 대상 S3 버킷이 동일한 AWS 리전의 경우): 22,000
  - 지역 간 보고서의 경우(평가 및 평가 보고서 대상 S3 버킷이 다른 AWS 리전의 경우): 3,500
  - 관련 평가에서 고객 관리 AWS KMS key를 사용하는 보고서의 경우: 3,500

컨트롤

- 계정당 사용자 지정 컨트롤 수: 500

증거

- 수동 증거 파일 한 개의 최대 크기: 100MB
- 컨트롤당 일일 수동 증거 업로드 횟수: 100

> **Tip**
>
> 대량의 수동 증거를 단일 컨트롤에 업로드해야 하는 경우, 며칠에 걸쳐 일괄적으로 증거를 업로드하는 것이 좋습니다.

프레임워크

- 계정당 사용자 지정 프레임워크 수: 100

> **Note**
>
> 프레임워크 할당량은 프레임워크를 만든 사람과 관계없이 프레임워크 라이브러리의 모든 공유 사용자 지정 프레임워크에 적용됩니다.

공유 사용자 지정 프레임워크 수신자

- 활성 수신자 계정 수: 100

API 액세스

- 모든 API에 대한 초당 트랜잭션(TPS) 수: 20TPS

Audit Manager 할당량 관리

AWS Audit Manager는 중앙 위치에서 할당량을 보고 관리할 수 있는 Service Quotas AWS 서비스와 통합하였습니다. 자세한 내용은 Service Quotas 사용 설명서의 Service Quotas는 무엇입니까?를 참조하세요. Service Quotas를 사용하면 모든 Audit Manager 할당량의 값을 쉽게 찾을 수 있습니다.

콘솔을 사용하여 Audit Manager 서비스 할당량을 보려면

1. Service Quotas 콘솔(https://console.aws.amazon.com/servicequotas/)을 엽니다.
2. 탐색 창에서 AWS 서비스를 선택합니다.
3. AWS 서비스 목록에서 AWS Audit Manager을(를) 검색하여 선택합니다.
4. Service quotas(서비스 할당량) 목록에서 서비스 할당량 이름, 적용된 할당량 값(제공된 경우), AWS 기본 할당량 값 및 할당량 조정 가능 여부를 확인할 수 있습니다.

5. 설명과 같은 서비스 할당량에 대한 추가 정보를 보려면 할당량 이름을 선택합니다.
6. (선택 사항) 할당량 증가를 요청하려면 증가시킬 할당량을 선택하고 할당량 증가 요청(Request quota increase)을 선택한 다음 필요한 정보를 입력하거나 선택한 다음 요청(Request)을 선택합니다.

자세한 내용은 Service Quotas User Guide(Service Quotas 사용 설명서)의 Requesting a quota increase(할당량 증가 요청)를 참조하세요.

보안 내부 AWS Audit Manager

클라우드 AWS 보안이 최우선 과제입니다. AWS 고객은 가장 보안에 민감한 조직의 요구 사항을 충족하도록 구축된 데이터 센터 및 네트워크 아키텍처의 혜택을 누릴 수 있습니다.

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

- 클라우드 보안 - AWS 클라우드에서 AWS 서비스를 실행하는 인프라를 보호하는 역할을 합니다. AWS AWS 또한 안전하게 사용할 수 있는 서비스를 제공합니다. 적용되는 규정 준수 프로그램에 대해 자세히 알아보려면 규정 준수 프로그램별 범위 내AWS 서비스 규정 준수 참조하십시오. AWS Audit Manager
- 클라우드에서의 보안 - 귀하의 책임은 사용하는 AWS 서비스에 따라 결정됩니다. 또한 귀하는 귀사의 데이터의 민감도, 귀사의 요구 사항, 관련 법률 및 규정을 비롯한 기타 요소에 대해서도 책임이 있습니다.

이 설명서는 공동 책임 모델을 사용할 때 공동 책임 모델을 적용하는 방법을 이해하는 데 도움이 AWS Audit Manager됩니다. 다음 주제에서는 보안 및 규정 준수 목표를 충족하도록 Audit Manager를 구성하는 방법을 보여줍니다. 또한 Audit Manager 리소스를 모니터링하고 보호하는 데 도움이 되는 다른 AWS 서비스를 사용하는 방법도 알아봅니다.

주제

데이터 보호: AWS Audit Manager

AWS 공동 책임 모델 의 데이터 보호에 적용됩니다 AWS Audit Manager. 이 모델에 설명된 대로 AWS 는 모든 데이터를 실행하는 글로벌 인프라를 보호하는 역할을 AWS 클라우드합니다. 이 인프라에서 호스팅되는 콘텐츠에 대한 제어를 유지하는 것은 사용자의 책임입니다. 사용하는 AWS 서비스 의 보안 구성과 관리 작업에 대한 책임도 사용자에게 있습니다. 데이터 프라이버시에 대한 자세한 내용은 데이터 프라이버시 FAQ를 참조하세요. 유럽의 데이터 보호에 대한 자세한 내용은AWS 보안 블로그의 AWS 공동 책임 모델 및 GDPR 블로그 게시물을 참조하세요.

데이터 보호를 위해 AWS 계정 자격 증명을 보호하고 AWS IAM Identity Center OR AWS Identity and Access Management (IAM) 을 사용하여 개별 사용자를 설정하는 것이 좋습니다. 이 방식을 사용하면 각 사용자에게 자신의 직무를 충실히 이행하는 데 필요한 권한만 부여됩니다. 또한 다음과 같은 방법으로 데이터를 보호하는 것이 좋습니다.

- 각 계정에 다중 인증(MFA)을 사용합니다.
- SSL/TLS를 사용하여 리소스와 통신할 수 있습니다. AWS TLS 1.2는 필수이며 TLS 1.3을 권장합니다.
- 를 사용하여 API 및 사용자 활동 로깅을 설정합니다. AWS CloudTrail
- 포함된 모든 기본 보안 제어와 함께 AWS 암호화 솔루션을 사용하십시오 AWS 서비스.
- Amazon Macie와 같은 고급 관리형 보안 서비스를 사용하여 Amazon S3에 저장된 민감한 데이터를 검색하고 보호합니다.
- 명령줄 인터페이스 또는 API를 AWS 통해 액세스할 때 FIPS 140-2로 검증된 암호화 모듈이 필요한 경우 FIPS 엔드포인트를 사용하십시오. 사용 가능한 FIPS 엔드포인트에 대한 자세한 내용은 Federal Information Processing Standard(FIPS) 140-2를 참조하십시오.

고객의 이메일 주소와 같은 기밀 정보나 중요한 정보는 태그나 이름 필드와 같은 자유 양식 필드에 입력하지 않는 것이 좋습니다. 여기에는 콘솔 AWS CLI, API 또는 AWS 서비스 AWS SDK를 사용하여 Audit Manager 또는 다른 사용자와 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 보안 인증를 URL에 포함시켜서는 안 됩니다.

위의 권장 사항 외에도 Audit Manager 고객은 평가, 사용자 지정 제어, 사용자 지정 프레임워크 및 위임 설명을 만들 때 자유 형식 필드에 민감한 식별 정보를 포함하지 않는 것이 좋습니다.

Audit Manager 데이터 삭제

Audit Manager 데이터를 삭제하는 방법에는 여러 가지가 있습니다.

Audit Manager를 비활성화할 때 데이터 삭제

Audit Manager를 비활성화하면 모든 Audit Manager 데이터를 삭제할지 여부를 결정할 수 있습니다. 데이터를 삭제하기로 선택한 경우 Audit Manager를 비활성화한 후 7일 이내에 삭제됩니다. 데이터가 삭제된 후에는 복구할 수 없습니다.

자동 데이터 삭제

일부 Audit Manager 데이터는 특정 기간이 지나면 자동으로 삭제됩니다. Audit Manager는 다음과 같이 고객 데이터를 보관합니다.

데이터 유형	데이터 보존 기간	참고
증거	데이터는 생성 시점부터 2년간 보존됩니다.	자동 증거 및 수동 증거 포함
고객이 만든 리소스	데이터는 무기한 보관됩니다.	평가, 평가 보고서, 사용자 지정 제어 및 사용자 지정 프레임워크 포함

수동 데이터 삭제

언제든지 개별 Audit Manager 리소스를 삭제할 수 있습니다. 지침은 다음을 참조하세요.

- 평가 삭제
  - 참조: AWS Audit Manager API DeleteAssessment레퍼런스에서
- 사용자 지정 프레임워크 삭제
  - 참조: AWS Audit Manager API DeleteAssessmentFramework레퍼런스에서
- 공유 요청 삭제
  - 참조: AWS Audit Manager API DeleteAssessmentFrameworkShare레퍼런스에서
- 평가 보고 삭제
  - 참조: AWS Audit Manager API DeleteAssessmentReport레퍼런스에서
- 사용자 지정 컨트롤 삭제

- 참조: AWS Audit Manager API DeleteControl레퍼런스에서

Audit Manager를 사용할 때 생성했을 수 있는 다른 리소스 데이터를 삭제하려면 다음을 참조하십시오.

- AWS CloudTrail 사용 설명서의 이벤트 데이터 저장소 삭제
- Amazon Simple Storage Service(Amazon S3) 사용 설명서의 버킷 삭제

저장 중 암호화

저장된 데이터를 암호화하기 위해 Audit Manager는 모든 데이터 저장소 및 AWS 관리형 키 로그에 대해 서버 측 암호화를 사용합니다.

데이터는 선택한 설정에 따라 고객 관리 키 또는 다른 키로 암호화됩니다. AWS 소유 키고객 관리 키를 제공하지 않으면 Audit Manager는 AWS 소유 키 a를 사용하여 콘텐츠를 암호화합니다. Audit Manager의 DynamoDB 및 Amazon S3에 있는 모든 서비스 메타데이터는 AWS 소유 키를 사용하여 암호화됩니다.

Audit Manager는 다음과 같이 데이터를 암호화합니다.

- Amazon S3에 저장된 서비스 메타데이터는 SSE-KMS를 AWS 소유 키 사용하여 암호화됩니다.
- DynamoDB에 저장된 서비스 메타데이터는 KMS와 AWS 소유 키을 사용하여 서버 측에서 암호화됩니다.
- DynamoDB에 저장된 콘텐츠는 고객 관리 키 또는 AWS 소유 키를 사용하여 클라이언트 측에서 암호화됩니다. KMS 키는 선택한 설정을 기반으로 합니다.
- Audit Manager의 Amazon S3에 저장된 콘텐츠는 SSE-KMS를 사용하여 암호화됩니다. KMS 키는 선택에 따라 결정되며 고객 관리형 키일 수도 있고 AWS 소유 키일 수도 있습니다.
- S3 버킷에 게시된 평가 보고서는 다음과 같이 암호화됩니다.
  - 고객 관리 키를 제공한 경우 데이터는 SSE-KMS를 사용하여 암호화됩니다.
  - 를 사용한 경우 데이터는 SSE-S3 AWS 소유 키를 사용하여 암호화됩니다.

전송 중 암호화

Audit Manager는 전송 중인 데이터를 암호화하기 위해 안전한 프라이빗 엔드포인트를 제공합니다. 보안 엔드포인트와 프라이빗 엔드포인트를 통해 AWS Audit Manager에 대한 API 요청의 무결성을 보호할 수 있습니다.

서비스 간 전송

기본적으로 모든 서비스 간 통신은 TLS(전송 계층 보안) 암호화를 사용하여 보호됩니다.

키 관리

Audit Manager는 모든 Audit Manager 리소스 (계정의 S3 버킷에 저장된 평가, 제어, 프레임워크, 증거, 평가 보고서) 를 암호화하기 위한 키와 고객 관리 키를 모두 AWS 소유 키 지원합니다.

고객 관리형 키를 사용하는 것이 좋습니다. 이렇게 하면 데이터를 보호하는 암호화 키를 보고 관리할 수 있습니다(AWS CloudTrail에서의 사용 로그 보기 포함). 고객 관리형 키를 선택하면 Audit Manager는 KMS 키를 생성하여 콘텐츠를 암호화하는 데 사용할 수 있도록 합니다.

> **Warning**
>
> Audit Manager 리소스를 암호화하는 데 사용되는 KMS 키를 삭제하거나 비활성화하면 해당 KMS 키로 암호화된 리소스를 더 이상 해독할 수 없습니다. 즉, 데이터를 복구할 수 없게 됩니다.
>
> AWS Key Management Service (AWS KMS) 에서 KMS 키를 삭제하는 것은 파괴적이며 잠재적으로 위험할 수 있습니다. KMS 키 삭제에 대한 자세한 내용은 AWS Key Management Service 사용 설명서의 AWS KMS keys삭제를 참조하십시오.

AWS Management Console, Audit Manager API 또는 AWS Command Line Interface (AWS CLI) 를 사용하여 감사 관리자를 활성화할 때 암호화 설정을 지정할 수 있습니다. 지침은 AWS Audit Manager 활성화 섹션을 참조하십시오.

언제든지 암호화 설정을 검토하고 변경할 수 있습니다. 지침은 데이터 암호화 섹션을 참조하십시오.

고객 관리 키를 설정하는 방법에 대한 자세한 내용은 AWS Key Management Service 사용 설명서의 키 만들기를 참조하십시오.

ID 및 액세스 관리 대상 AWS Audit Manager

AWS Identity and Access Management (IAM) 은 관리자가 AWS 리소스에 대한 액세스를 안전하게 제어할 수 AWS 서비스 있도록 도와줍니다. IAM 관리자는 누가 Audit Manager 리소스를 사용하도록 인

증되고(로그인됨) 권한이 부여되는지(권한 있음)를 제어합니다. IAM은 추가 AWS 서비스 비용 없이 사용할 수 있습니다.

주제

고객

사용 방법 AWS Identity and Access Management (IAM) 은 Audit Manager에서 수행하는 작업에 따라 다릅니다.

서비스 사용자 - Audit Manager 서비스를 사용하여 작업을 수행하는 경우 필요한 자격 증명과 권한을 관리자가 제공합니다. 더 많은 Audit Manager 기능을 사용하여 작업을 수행하게 되면 추가 권한이 필요할 수 있습니다. 액세스 권한 관리 방식을 이해하면 적절한 권한을 관리자에게 요청할 수 있습니다. Audit Manager의 기능에 액세스할 수 없는 경우 ID 및 액세스 문제 해결 AWS Audit Manager 단원을 참조하세요.

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

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

보안 인증을 통한 인증

인증은 ID 자격 증명을 AWS 사용하여 로그인하는 방법입니다. IAM 사용자로 인증 (로그인 AWS) 하거나 IAM 역할을 맡아 인증 (로그인) 해야 합니다. AWS 계정 루트 사용자

ID 소스를 통해 제공된 자격 증명을 사용하여 페더레이션 ID로 로그인할 수 있습니다. AWS AWS IAM Identity Center (IAM ID 센터) 사용자, 회사의 싱글 사인온 인증, Google 또는 Facebook 자격 증명이 페더레이션 ID의 예입니다. 페더레이션형 ID로 로그인할 때 관리자가 이전에 IAM 역할을 사용하여 ID 페더레이션을 설정했습니다. 페더레이션을 사용하여 액세스하는 경우 AWS 간접적으로 역할을 맡게 됩니다.

사용자 유형에 따라 AWS Management Console 또는 AWS 액세스 포털에 로그인할 수 있습니다. 로그인에 대한 자세한 내용은 AWS 로그인 사용 설명서의 내 로그인 방법을 참조하십시오. AWS AWS 계정

AWS 프로그래밍 방식으로 액세스하는 경우 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 직접 요청에 서명하는 방법에 대한 자세한 내용은 IAM 사용 설명서의 AWS API 요청 서명을 참조하십시오.

사용하는 인증 방법에 상관없이 추가 보안 정보를 제공해야 할 수도 있습니다. 예를 들어, AWS 계정의 보안을 강화하기 위해 다단계 인증 (MFA) 을 사용할 것을 권장합니다. 자세한 내용은 AWS IAM Identity Center 사용 설명서의 다중 인증 및 IAM 사용 설명서의 AWS에서 다중 인증(MFA) 사용을 참조하세요.

AWS 계정 루트 사용자

계정을 AWS 계정만들 때는 먼저 계정의 모든 AWS 서비스 리소스에 대한 완전한 액세스 권한을 가진 하나의 로그인 ID로 시작합니다. 이 ID를 AWS 계정 루트 사용자라고 하며, 계정을 만들 때 사용한 이메일 주소와 비밀번호로 로그인하여 액세스할 수 있습니다. 일상적인 작업에 루트 사용자를 사용하지 않을 것을 강력히 권장합니다. 루트 사용자 보안 인증 정보를 보호하고 루트 사용자만 수행할 수 있는 작업을 수행하는 데 사용합니다. 루트 사용자로 로그인해야 하는 작업의 전체 목록은 IAM 사용자 안내서의 루트 사용자 보안 인증이 필요한 작업을 참조하세요.

연동 보안 인증

가장 좋은 방법은 관리자 액세스가 필요한 사용자를 비롯한 수동 AWS 서비스 사용자가 ID 공급자와의 페더레이션을 사용하여 임시 자격 증명을 사용하여 액세스하도록 하는 것입니다.

페더레이션 ID는 기업 사용자 디렉토리, 웹 ID 공급자, Identity Center 디렉터리의 사용자 또는 ID 소스를 통해 제공된 자격 증명을 사용하여 액세스하는 AWS 서비스 모든 사용자를 말합니다. AWS

Directory Service페더레이션 ID에 AWS 계정액세스하면 이들이 역할을 맡고 역할은 임시 자격 증명을 제공합니다.

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

IAM 사용자 및 그룹

IAM 사용자는 단일 사용자 또는 애플리케이션에 대한 특정 권한을 AWS 계정 가진 사용자 내 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 교체 섹션을 참조하세요.

IAM 그룹은 IAM 사용자 컬렉션을 지정하는 보안 인증입니다. 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 보안 인증을 가지고 있지만, 역할은 임시 보안 인증만 제공합니다. 자세한 정보는 IAM 사용 설명서의 IAM 사용자를 만들어야 하는 경우(역할이 아님) 섹션을 참조하세요.

IAM 역할

IAM 역할은 특정 권한을 가진 사용자 AWS 계정 내의 자격 증명입니다. IAM 사용자와 유사하지만, 특정 개인과 연결되지 않습니다. 역할을 AWS Management Console 전환하여 에서 일시적으로 IAM 역할을 맡을 수 있습니다. AWS CLI 또는 AWS API 작업을 호출하거나 사용자 지정 URL을 사용하여 역할을 수임할 수 있습니다. 역할 사용 방법에 대한 자세한 정보는 IAM 사용 설명서의 IAM 역할 사용을 참조하세요.

임시 보안 인증이 있는 IAM 역할은 다음과 같은 상황에서 유용합니다.

- 페더레이션 사용자 액세스 - 페더레이션형 ID에 권한을 부여하려면 역할을 생성하고 해당 역할의 권한을 정의합니다. 페더레이션형 ID가 인증되면 역할이 연결되고 역할에 정의된 권한이 부여됩니다. 페더레이션 역할에 대한 자세한 내용은 IAM 사용 설명서의 Creating a role for a third-party Identity

Provider(서드 파티 보안 인증 공급자의 역할 만들기) 부분을 참조하세요. IAM 자격 증명 센터를 사용하는 경우 권한 집합을 구성합니다. 인증 후 아이덴티티가 액세스할 수 있는 항목을 제어하기 위해 IAM Identity Center는 권한 세트를 IAM의 역할과 연관 짓습니다. 권한 세트에 대한 자세한 내용은 AWS IAM Identity Center 사용 설명서의 권한 세트 섹션을 참조하세요.

- 임시 IAM 사용자 권한 - IAM 사용자 또는 역할은 IAM 역할을 수임하여 특정 작업에 대한 다양한 권한을 임시로 받을 수 있습니다.
- 크로스 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 AWS 서비스경우에는 역할을 프록시로 사용하는 대신 정책을 리소스에 직접 연결할 수 있습니다. 교차 계정 액세스를 위한 역할과 리소스 기반 정책의 차이점을 알아보려면 IAM 사용 설명서의 IAM 역할과 리소스 기반 정책의 차이 섹션을 참조하세요.
- 서비스 간 액세스 — 일부는 다른 AWS 서비스서비스의 기능을 AWS 서비스 사용합니다. 예를 들어 서비스에서 직접적으로 호출을 수행하면 일반적으로 해당 서비스는 Amazon EC2에서 애플리케이션을 실행하거나 Amazon S3에 객체를 저장합니다. 서비스는 직접적으로 호출하는 보안 주체의 권한을 사용하거나, 서비스 역할을 사용하거나, 또는 서비스 연결 역할을 사용하여 이 작업을 수행할 수 있습니다.
  - 순방향 액세스 세션 (FAS) — IAM 사용자 또는 역할을 사용하여 작업을 수행하는 경우 보안 AWS 주체로 간주됩니다. 일부 서비스를 사용하는 경우 다른 서비스에서 다른 작업을 시작하는 작업을 수행할 수 있습니다. FAS는 전화를 거는 주체의 권한을 다운스트림 AWS 서비스서비스에 AWS 서비스 요청하기 위한 요청과 결합하여 사용합니다. FAS 요청은 다른 서비스 AWS 서비스 또는 리소스와의 상호 작용이 필요한 요청을 서비스가 수신한 경우에만 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 태스크를 수행하기 위해 맡는 IAM 역할입니다. IAM 관리자는 IAM 내에서 서비스 역할을 생성, 수정 및 삭제할 수 있습니다. 자세한 정보는 IAM 사용 설명서의 AWS 서비스에 대한 권한을 위임할 역할 생성을 참조하세요.
  - 서비스 연결 역할 — 서비스 연결 역할은 에 연결된 서비스 역할의 한 유형입니다. AWS 서비스서비스는 사용자를 대신하여 작업을 수행하기 위해 역할을 수임할 수 있습니다. 서비스 연결 역할은 사용자에게 AWS 계정 표시되며 해당 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 API 요청을 AWS CLI 하는 애플리케이션의 임시 자격 증명을 관리할 수 있습니다. AWS 이는 EC2 인스턴스 내에 액세스 키를 저장할 때 권장되는 방법입니다. EC2 인스턴스에 AWS 역할을 할당하고 모든 애플리케이션에서 사용할 수 있게 하려면 인스턴스에 연결된 인스턴스 프로필을 생성합니다. 인스턴스 프로파일에는 역할이 포함되어 있으며 EC2 인스턴스에서 실행되는 프로그램이 임시 보안 인

증을 얻을 수 있습니다. 자세한 정보는 IAM 사용 설명서의 IAM 역할을 사용하여 Amazon EC2 인스턴스에서 실행되는 애플리케이션에 권한 부여 섹션을 참조하세요.

IAM 역할을 사용할지 또는 IAM 사용자를 사용할지를 알아보려면 IAM 사용 설명서의 IAM 역할(사용자 대신)을 생성하는 경우 섹션을 참조하세요.

정책을 사용한 액세스 관리

정책을 생성하고 이를 AWS ID 또는 리소스에 AWS 연결하여 액세스를 제어할 수 있습니다. 정책은 ID 또는 리소스와 연결될 때 AWS 해당 권한을 정의하는 객체입니다. AWS 주도자 (사용자, 루트 사용자 또는 역할 세션) 가 요청할 때 이러한 정책을 평가합니다. 정책의 권한이 요청 허용 또는 거부 여부를 결정합니다. 대부분의 정책은 JSON 문서로 AWS 저장됩니다. JSON 정책 문서의 구조와 콘텐츠에 대한 자세한 정보는 IAM 사용 설명서의 JSON 정책 개요 섹션을 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, 사용자와 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 정책을 사용하는 사용자는 AWS Management Console, AWS CLI, 또는 AWS API에서 역할 정보를 가져올 수 있습니다.

보안 인증 기반 정책

보안 인증 기반 정책은 IAM 사용자, 사용자 그룹 또는 역할과 같은 보안 인증에 연결할 수 있는 JSON 권한 정책 문서입니다. 이러한 정책은 사용자와 역할이 어떤 리소스와 어떤 조건에서 어떤 작업을 수행할 수 있는지를 제어합니다. 보안 인증 기반 정책을 생성하는 방법을 알아보려면 IAM 사용 설명서의 IAM 정책 생성을 참조하세요.

보안 인증 기반 정책은 인라인 정책 또는 관리형 정책으로 한층 더 분류할 수 있습니다. 인라인 정책은 단일 사용자, 그룹 또는 역할에 직접 포함됩니다. 관리형 정책은 내 여러 사용자, 그룹 및 역할에 연결할 수 있는 독립형 정책입니다. AWS 계정관리형 정책에는 AWS 관리형 정책과 고객 관리형 정책이 포함됩니다. 관리형 정책 또는 인라인 정책을 선택하는 방법을 알아보려면 IAM 사용 설명서의 관리형 정책과 인라인 정책의 선택을 참조하세요.

리소스 기반 정책

리소스 기반 정책은 리소스에 연결하는 JSON 정책 설명서입니다. 리소스 기반 정책의 예는 IAM 역할 신뢰 정책과 Amazon S3 버킷 정책입니다. 리소스 기반 정책을 지원하는 서비스에서 서비스 관리자는 이러한 정책을 사용하여 특정 리소스에 대한 액세스를 통제할 수 있습니다. 정책이 연결된 리소스의 경우 정책은 지정된 보안 주체가 해당 리소스와 어떤 조건에서 어떤 작업을 수행할 수 있는지를 정의합니다. 리소스 기반 정책에서 보안 주체를 지정해야 합니다. 보안 주체에는 계정, 사용자, 역할, 연동 사용자 등이 포함될 수 있습니다. AWS 서비스

리소스 기반 정책은 해당 서비스에 있는 인라인 정책입니다. IAM의 AWS 관리형 정책은 리소스 기반 정책에 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 설명서 형식을 사용하지 않지만 리소스 기반 정책과 유사합니다.

ACL을 지원하는 서비스의 예로는 아마존 S3와 아마존 VPC가 있습니다. AWS WAFACL에 대해 자세히 알아보려면 Amazon Simple Storage Service 개발자 안내서의 ACL(액세스 제어 목록) 개요 섹션을 참조하세요.

기타 정책 타입

AWS 일반적이지 않은 추가 정책 유형을 지원합니다. 이러한 정책 타입은 더 일반적인 정책 타입에 따라 사용자에게 부여되는 최대 권한을 설정할 수 있습니다.

- 권한 경계 – 권한 경계는 보안 인증 기반 정책에 따라 IAM 엔터티(IAM 사용자 또는 역할)에 부여할 수 있는 최대 권한을 설정하는 고급 특성입니다. 개체에 대한 권한 경계를 설정할 수 있습니다. 그 결과로 얻는 권한은 개체의 보안 인증 기반 정책과 그 권한 경계의 교집합입니다. `Principal` 필드에서 사용자나 역할을 보안 주체로 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 엔터티에 대한 권한 경계 섹션을 참조하세요.
- 서비스 제어 정책 (SCP) - SCP는 조직 또는 조직 단위 (OU) 에 대한 최대 권한을 지정하는 JSON 정책입니다. AWS Organizations AWS Organizations 사업체가 소유한 여러 AWS 계정 개를 그룹화하고 중앙에서 관리하는 서비스입니다. 조직에서 모든 기능을 활성화할 경우 서비스 통제 정책(SCP)을 임의의 또는 모든 계정에 적용할 수 있습니다. SCP는 구성원 계정의 엔티티 (각 엔티티 포함) 에 대한 권한을 제한합니다. AWS 계정 루트 사용자조직 및 SCP에 대한 자세한 정보는 AWS Organizations 사용 설명서의 SCP 작동 방식을 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 보안 인증 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 타입

여러 정책 타입이 요청에 적용되는 경우 결과 권한은 이해하기가 더 복잡합니다. 여러 정책 유형이 관련되어 있을 때 요청을 허용할지 여부를 AWS 결정하는 방법을 알아보려면 IAM 사용 설명서의 정책 평가 로직을 참조하십시오.

IAM의 AWS Audit Manager 작동 방식

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

함께 사용할 수 있는 IAM 기능 AWS Audit Manager

IAM 특성	Audit Manager 지원
ID 기반 정책	예
리소스 기반 정책	아니요
정책 작업	예
정책 리소스	예
정책 조건 키	부분
ACL	아니요
ABAC(정책의 태그)	예
임시 보안 인증	예
전달 액세스 세션(FAS)	예
서비스 역할	아니요

IAM 특성	Audit Manager 지원
서비스 링크 역할	예

대부분의 IAM 기능과 함께 작동하는 방식 AWS Audit Manager 및 기타 AWS 서비스를 개괄적으로 살펴보려면 IAM 사용 설명서의 IAM과 함께 작동하는AWS 서비스를 참조하십시오.

ID 기반 정책은 다음과 같습니다. AWS Audit Manager

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 사용자와 역할이 어떤 리소스와 어떤 조건에서 어떤 작업을 수행할 수 있는지를 제어합니다. ID 기반 정책을 생성하는 방법을 알아보려면 IAM 사용 설명서의 IAM 정책 생성을 참조하세요.

IAM 자격 증명 기반 정책을 사용하면 허용되거나 거부되는 작업와 리소스뿐 아니라 작업이 허용되거나 거부되는 조건을 지정할 수 있습니다. ID 기반 정책에서는 보안 주체가 연결된 사용자 또는 역할에 적용되므로 보안 주체를 지정할 수 없습니다. JSON 정책에서 사용할 수 있는 모든 요소에 대해 알아보려면 IAM 사용 설명서의 IAM JSON 정책 요소 참조 섹션을 참조하세요.

AWS Audit Manager Audit Manager 관리자의 이름을 딴 `AWSAuditManagerAdministratorAccess` 관리형 정책을 생성합니다. 이 정책은 Audit Manager에서 전체 관리 액세스 권한을 부여합니다. 관리자는 이 정책을 기존 역할 또는 사용자에게 연결하거나 이 정책을 사용하여 새 역할을 만들 수 있습니다.

사용자 페르소나에 대한 권장 정책은 다음과 같습니다. AWS Audit Manager

AWS Audit Manager 서로 다른 IAM 정책을 사용하여 여러 사용자 간의 업무 분담 및 다양한 감사에 대한 업무 분리를 유지할 수 있습니다. Audit Manager의 두 페르소나와 권장 정책은 다음과 같이 정의됩니다.

페르소나	설명 및 권장 정책
감사 소유자	• 이 페르소나에는 에서 평가를 관리하는 데 필요한 권한이 있어야 합니다. AWS Audit Manager

페르소나	설명 및 권장 정책
	• 이 페르소나에 사용할 권장 정책은 이름이 지정된 관리형 정책입니다. AWSAuditManagerAdministratorAccess 이 정책을 시작점으로 사용하고 요구 사항에 맞게 이러한 권한의 범위를 좁힐 수 있습니다.
위임	• 이 페르소나는 평가에서 위임된 통제 세트에 접근할 수 있습니다. 제어 상태를 업데이트하고, 의견을 추가하고, 검토를 위해 통제 세트를 제출하고, 평가 보고서에 증거를 추가할 수 있습니다. • 이 페르소나에 사용할 권장 정책은 사용자에게 AWS Audit Manager에 대한 전체 관리자 액세스를 허용합니다. 예제 정책입니다. 이 정책을 시작점으로 사용하고 필요에 따라 요구 사항에 맞게 변경할 수 있습니다.

아이덴티티 기반 정책 예시: AWS Audit Manager

Audit Manager 자격 증명 기반 정책의 예를 보려면 에 대한 ID 기반 정책 예제 AWS Audit Manager 단원을 참조하세요.

내 리소스 기반 정책 AWS Audit Manager

리소스 기반 정책 지원	아니요

리소스 기반 정책은 리소스에 연결하는 JSON 정책 문서입니다. 리소스 기반 정책의 예는 IAM 역할 신뢰 정책과 Amazon S3 버킷 정책입니다. 리소스 기반 정책을 지원하는 서비스에서 서비스 관리자는 이러한 정책을 사용하여 특정 리소스에 대한 액세스를 통제할 수 있습니다. 정책이 연결된 리소스의 경우 정책은 지정된 보안 주체가 해당 리소스와 어떤 조건에서 어떤 작업을 수행할 수 있는지를 정의합니다. 리소스 기반 정책에서 보안 주체를 지정해야 합니다. 보안 주체에는 계정, 사용자, 역할, 연동 사용자 등이 포함될 수 있습니다. AWS 서비스

크로스 계정 액세스를 활성화하려는 경우 전체 계정이나 다른 계정의 IAM 개체를 리소스 기반 정책의 보안 주체로 지정할 수 있습니다. 리소스 기반 정책에 크로스 계정 보안 주체를 추가하는 것은 트러스트 관계 설정의 절반밖에 되지 않는다는 것을 유념하세요. 보안 주체와 리소스가 다른 AWS 계정경우 신뢰할 수 있는 계정의 IAM 관리자는 보안 주체 개체 (사용자 또는 역할) 에게 리소스에 액세스할 수 있는 권한도 부여해야 합니다. 개체에 자격 증명 기반 정책을 연결하여 권한을 부여합니다. 하지만 리소스 기반 정책이 동일 계정의 보안 주체에 액세스 권한을 부여하는 경우 추가 자격 증명 기반 정책이 필

요하지 않습니다. 자세한 정보는 IAM 사용 설명서의 IAM 역할과 리소스 기반 정책의 차이 섹션을 참조하세요.

에 대한 정책 조치 AWS Audit Manager

정책 작업 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.

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

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

AWS Audit Manager 작업 목록을 보려면 서비스 권한 부여 참조의 AWS Audit Manager에서 정의한 작업을 참조하십시오.

정책 조치는 조치 앞에 다음 접두사를 AWS Audit Manager 사용합니다.

```
auditmanager
```

단일 문에서 여러 작업을 지정하려면 다음과 같이 쉼표로 구분합니다.

```
"Action": [
      "auditmanager:GetEvidenceDetails",
      "auditmanager:GetEvidenceEventDetails"
         ]
```

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

```
"Action": "auditmanager:Get*"
```

Audit Manager 자격 증명 기반 정책의 예를 보려면 에 대한 ID 기반 정책 예제 AWS Audit Manager 단원을 참조하세요.

에 대한 정책 리소스 AWS Audit Manager

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. 보고서에는 `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 이 작업을 수행할 수 있습니다.

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

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

AWS Audit Manager 리소스 유형 및 ARN 목록을 보려면 서비스 권한 부여 참조의 AWS Audit Manager에서 정의한 리소스를 참조하십시오. 각 리소스의 ARN을 지정할 수 있는 작업을 알아보려면 AWS Audit Manager가 정의한 작업을 참조하세요.

Audit Manager 평가는 다음과 같은 Amazon 리소스 이름(ARN) 형식을 사용합니다.

```
arn:${Partition}:auditmanager:${Region}:${Account}:assessment/${assessmentId}
```

Audit Manager 제어 세트는 다음과 같은 ARN 형식을 갖습니다.

```
arn:${Partition}:auditmanager:${Region}:${Account}:assessment/
${assessmentId}controlSet/${controlSetId}
```

Audit Manager 제어는 다음과 같은 ARN 형식을 갖습니다.

```
arn:${Partition}:auditmanager:${Region}:${Account}:control/${controlId}
```

ARN 형식에 대한 자세한 내용은 Amazon 리소스 이름(ARN)을 참조하십시오.

예를 들어 명령문에서 ID가 `i-1234567890abcdef0` 평가를 지정하려면 다음 ARN을 사용합니다.

```
"Resource": "arn:aws:auditmanager:us-east-1:123456789012:assessment/
i-1234567890abcdef0"
```

특정 계정에 속하는 모든 인스턴스를 지정하려면 와일드카드(*)를 사용합니다.

```
"Resource": "arn:aws:auditmanager:us-east-1:123456789012:assessment/*"
```

리소스를 생성하기 위한 작업과 같은 일부 Audit Manager 작업은 특정 리소스에서 수행할 수 없습니다. 이러한 경우, 와일드카드(*)를 사용해야 합니다.

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

다양한 Audit Manager API 작업에는 여러 리소스가 관여합니다. 예를 들어, 는 현재 로그인한 사용자가 액세스할 수 있는 평가 메타데이터 목록을 `ListAssessments` 반환합니다. AWS 계정따라서 사용자가 평가를 볼 권한을 가지고 있어야 합니다. 단일 문에서 여러 리소스를 지정하려면 ARN을 쉼표로 구분합니다.

```
"Resource": [
      "resource1",
      "resource2"
```

Audit Manager 리소스 유형 및 해당 ARN의 목록을 보려면 IAM 사용 설명서의 AWS Audit Manager가 정의한 리소스를 참조하세요. 각 리소스의 ARN을 지정할 수 있는 작업에 대해 알아보려면 AWS Audit Manager가 정의한 작업을 참조하세요.

일부 Audit Manager API 작업은 여러 리소스를 지원합니다. 예를 들어 `assessmentID`, `controlID` 및 `controlSetId`에 `GetChangeLogs`이 액세스할 수 있으므로 주도자는 이러한 각 리소스에 액세스할 수 있는 권한을 가지고 있어야 합니다. 단일 문에서 여러 리소스를 지정하려면 ARN을 쉼표로 구분합니다.

```
"Resource": [
      "assessmentId",
      "controlId",
      "controlSetId"
```

에 대한 정책 조건 키 AWS Audit Manager

서비스별 정책 조건 키 지원	부분

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. 같음이나 미만 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 경우 는 논리적 `OR` 연산을 사용하여 조건을 AWS 평가합니다. 명령문의 권한을 부여하기 전에 모든 조건을 충족해야 합니다.

정책 문의 주체가 AWS 서비스 주체인 경우, 정책의 `aws:SourceArn` 또는 `aws:SourceAccount` 글로벌 조건 키를 사용하는 것이 좋습니다. 이러한 글로벌 조건 컨텍스트 키를 사용하면 대리인이 혼동되는 시나리오를 방지하는 데 도움이 될 수 있습니다. 다음 문서화된 정책은 혼동된 대리인 문제를 방지하기 위해 Audit Manager에서 `aws:SourceArn` 및 `aws:SourceAccount` 글로벌 조건 컨텍스트 키를 사용할 수 있는 방법을 보여줍니다.

- Audit Manager 알림에 사용되는 SNS 주제에 대한 예제 정책
- SNS 주제와 함께 사용되는 KMS 키의 정책 예시

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

Audit Manager는 서비스별 조건 키를 제공하지 않지만, 일부 전역 조건 키 사용을 지원합니다. 모든 AWS 글로벌 조건 키를 보려면 IAM 사용 설명서의AWS 글로벌 조건 컨텍스트 키를 참조하십시오.

AWS Audit Manager의 ACL(액세스 제어 목록)

ACL 지원	아니요

액세스 제어 목록(ACL)은 리소스에 액세스할 권한이 있는 보안 주체(계정 구성원, 사용자 또는 역할)를 제어합니다. ACL은 JSON 정책 설명서 형식을 사용하지 않지만 리소스 기반 정책과 유사합니다.

다음을 사용한 속성 기반 액세스 제어 (ABAC) AWS Audit Manager

ABAC 지원(정책의 태그)	예

ABAC(속성 기반 액세스 제어)는 속성을 기반으로 권한을 정의하는 권한 부여 전략입니다. AWS에서는 이러한 속성을 태그라고 합니다. IAM 개체 (사용자 또는 역할) 및 여러 AWS 리소스에 태그를 첨부할 수 있습니다. ABAC의 첫 번째 단계로 개체 및 리소스에 태그를 지정합니다. 그런 다음 보안 주체의 태그가 액세스하려는 리소스의 태그와 일치할 때 작업을 허용하도록 ABAC 정책을 설계합니다.

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

태그를 기반으로 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 정보는 IAM 사용 설명서의 ABAC란 무엇입니까? 섹션을 참조하세요. ABAC 설정 단계가 포함된 자습서를 보려면 IAM 사용 설명서의 속성 기반 액세스 제어(ABAC) 사용을 참조하세요.

AWS Audit Manager 리소스 태깅에 대한 자세한 내용은 을 참조하십시오. AWS Audit Manager 리소스에 태그 지정

임시 자격 증명 사용 AWS Audit Manager

임시 보안 인증 지원	예

임시 자격 증명을 사용하여 로그인하면 작동하지 AWS 서비스 않는 것도 있습니다. 임시 자격 증명을 사용하는 방법을 AWS 서비스 비롯한 추가 정보는 IAM 사용 설명서의 IAM과AWS 서비스 연동되는 내용을 참조하십시오.

사용자 이름과 암호를 제외한 다른 방법을 AWS Management Console 사용하여 로그인하면 임시 자격 증명을 사용하는 것입니다. 예를 들어 회사의 SSO (Single Sign-On) 링크를 AWS 사용하여 액세스하는 경우 이 프로세스에서 자동으로 임시 자격 증명을 생성합니다. 또한 콘솔에 사용자로 로그인한 다

음 역할을 전환할 때 임시 보안 인증을 자동으로 생성합니다. 역할 전환에 대한 자세한 정보는 IAM 사용 설명서의 역할로 전환(콘솔)을 참조하세요.

또는 API를 사용하여 임시 자격 증명을 수동으로 생성할 수 있습니다 AWS CLI . AWS 그런 다음 해당 임시 자격 증명을 사용하여 액세스할 수 AWS있습니다. AWS 장기 액세스 키를 사용하는 대신 임시 자격 증명을 동적으로 생성할 것을 권장합니다. 자세한 정보는 IAM의 임시 보안 자격 증명을 참조하세요.

전달 액세스 세션 대상: AWS Audit Manager

전달 액세스 세션(FAS) 지원	예

IAM 사용자 또는 역할을 사용하여 작업을 수행하는 AWS경우 사용자는 보안 주체로 간주됩니다. 일부 서비스를 사용하는 경우 다른 서비스에서 다른 작업을 시작하는 작업을 수행할 수 있습니다. FAS는 전화를 거는 주체의 권한을 다운스트림 서비스에 AWS 서비스 요청하라는 요청과 결합하여 사용합니다. AWS 서비스FAS 요청은 다른 서비스 AWS 서비스 또는 리소스와의 상호 작용이 필요한 요청을 서비스가 수신한 경우에만 이루어집니다. 이 경우 두 작업을 모두 수행할 수 있는 권한이 있어야 합니다. FAS 요청 시 정책 세부 정보는 전달 액세스 세션을 참조하세요.

AWS Audit Manager의 서비스 역할

서비스 역할 지원	아니요

서비스 역할은 서비스가 사용자를 대신하여 작업을 수행하기 위해 수임하는 IAM role(IAM 역할)입니다. IAM 관리자는 IAM 내에서 서비스 역할을 생성, 수정 및 삭제할 수 있습니다. 자세한 정보는 IAM 사용 설명서의 역할을 생성하여 AWS 서비스에게 권한 위임을 참조하세요.

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

서비스 연결 역할은 다음과 같습니다. AWS Audit Manager

서비스 링크 역할 지원	예

서비스 연결 역할은 에 연결된 서비스 역할 유형입니다. AWS 서비스서비스는 사용자를 대신하여 작업을 수행하기 위해 역할을 수임할 수 있습니다. 서비스 연결 역할은 사용자에게 AWS 계정 표시되며 해당 서비스가 소유합니다. IAM 관리자는 서비스 링크 역할의 권한을 볼 수 있지만 편집은 할 수 없습니다.

의 서비스 연결 역할에 대한 자세한 내용은 을 참조하십시오. AWS Audit Manager서비스 연결 역할 사용 AWS Audit Manager

에 대한 ID 기반 정책 예제 AWS Audit Manager

기본적으로 사용자 및 역할에는 Audit 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 ID 기반 정책을 생성하는 방법을 알아보려면 IAM 사용 설명서의 IAM 정책 생성을 참조하세요.

각 리소스 유형에 대한 ARN 형식을 포함하여 AWS Audit Manager에서 정의한 작업 및 리소스 유형에 대한 자세한 내용은 서비스 인증 참조에서 AWS Audit Manager에 대한 작업, 리소스 및 조건 키를 참조하세요.

주제

- 정책 모범 사례
- Audit Manager를 활성화하는 데 필요한 최소 권한 허용
- 사용자에게 AWS Audit Manager에 대한 전체 관리자 액세스를 허용합니다.
- AWS Audit Manager에 대한 사용자 관리 액세스 허용
- 사용자에게 읽기 전용 액세스 허용: AWS Audit Manager
- 사용자가 자신의 고유한 권한을 볼 수 있도록 허용
- Amazon SNS 주제에 알림 전송 허용 AWS Audit Manager
- 사용자가 증거 찾기에서 검색 쿼리를 실행하도록 허용

정책 모범 사례

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

- AWS 관리형 정책으로 시작하고 최소 권한 권한으로 이동 — 사용자와 워크로드에 권한을 부여하려면 여러 일반적인 사용 사례에 권한을 부여하는 AWS 관리형 정책을 사용하세요. 해당 내용은 에서 사용할 수 있습니다. AWS 계정사용 사례에 맞는 AWS 고객 관리형 정책을 정의하여 권한을 더 줄이는 것이 좋습니다. 자세한 정보는 IAM 사용 설명서의 AWS 관리형 정책 또는 직무에 대한AWS 관리형 정책 섹션을 참조하세요.
- 최소 권한 적용 – IAM 정책을 사용하여 권한을 설정하는 경우 작업을 수행하는 데 필요한 권한만 부여합니다. 이렇게 하려면 least-privilege permissions(최소 권한)으로 알려진 특정 조건에서 특정 리소스에 대해 수행할 수 있는 작업을 정의합니다. IAM을 사용하여 권한을 적용하는 방법에 대한 자세한 정보는 IAM 사용 설명서의 IAM의 정책 및 권한을 참조하세요.
- Use conditions in IAM policies to further restrict access(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 생성할 수 있습니다. 예를 AWS 서비스들어 특정 작업을 통해 서비스 작업을 사용하는 경우 조건을 사용하여 서비스 작업에 대한 액세스 권한을 부여할 수도 AWS CloudFormation있습니다. 자세한 정보는 IAM 사용 설명서의 IAM JSON 정책 요소: 조건을 참조하세요.
- IAM Access Analyzer를 통해 IAM 정책을 검증하여 안전하고 기능적인 권한 보장 – IAM Access Analyzer에서는 IAM 정책 언어(JSON)와 모범 사례가 정책에서 준수되도록 신규 및 기존 정책을 검증합니다. IAM Access Analyzer는 100개 이상의 정책 확인 항목과 실행 가능한 권장 사항을 제공하여 안전하고 기능적인 정책을 생성하도록 돕습니다. 자세한 내용은 IAM 사용 설명서의 IAM Access Analyzer 정책 검증을 참조하세요.
- 멀티 팩터 인증 (MFA) 필요 - IAM 사용자 또는 루트 사용자가 필요한 시나리오가 있는 경우 추가 보안을 위해 AWS 계정MFA를 활성화하십시오. API 작업을 직접적으로 호출할 때 MFA가 필요하면 정책에 MFA 조건을 추가합니다. 자세한 정보는 IAM 사용 설명서의 MFA 보호 API 액세스 구성 섹션을 참조하세요.

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

Audit Manager를 활성화하는 데 필요한 최소 권한 허용

이 예제에서는 관리자 역할이 없는 계정이 AWS Audit Manager을 활성화하도록 허용하는 방법을 보여줍니다.

> **Note**
>
> 여기서 제공하는 것은 Audit Manager를 활성화하는 데 필요한 최소 권한을 부여하는 기본 정책입니다. 다음 정책의 모든 권한이 필요합니다. 이 정책 중 일부를 생략하면 Audit Manager를 사용할 수 없습니다.
> 시간을 내어 특정 요구 사항에 맞게 권한을 사용자 지정하는 것이 좋습니다. 도움이 필요한 경우 관리자 또는 AWS Support에 문의하세요.

Audit Manager를 활성화하는 데 필요한 최소 액세스 권한을 부여하려면 다음 권한을 사용하십시오.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "auditmanager:*",
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": "iam:CreateServiceLinkedRole",
            "Resource": "*",
            "Condition": {
                "StringLike": {
                    "iam:AWSServiceName": "auditmanager.amazonaws.com"
                }
            }
        },
        {
            "Sid": "CreateEventsAccess",
            "Effect": "Allow",
            "Action": [
                "events:PutRule"
            ],
            "Resource": "*",
            "Condition": {
                "ForAllValues:StringEquals": {
                    "events:source": [
                        "aws.securityhub"
                    ]
                }
```

```
            }
        },
        {
            "Sid": "EventsAccess",
            "Effect": "Allow",
            "Action": [
                "events:PutTargets"
            ],
            "Resource": "arn:aws:events:*:*:rule/
AuditManagerSecurityHubFindingsReceiver"
        },
        {
            "Effect": "Allow",
            "Action": "kms:ListAliases",
            "Resource": "*",
            "Condition": {
                "StringLike": {
                    "iam:AWSServiceName": "auditmanager.amazonaws.com"
                }
            }
        }
    ]
}
```

또는 API만 호출하는 사용자에게 최소 콘솔 권한을 허용할 필요는 없습니다. AWS CLI AWS 그 대신, 수행하려는 API 작업과 일치하는 작업에만 액세스할 수 있도록 합니다.

사용자에게 AWS Audit Manager에 대한 전체 관리자 액세스를 허용합니다.

다음 예제 정책은 관리자에게 전체 액세스 권한을 AWS Audit Manager부여합니다.

- 예 1(관리형 정책,AWSAuditManagerAdministratorAccess)
- 예 2(평가 보고서 대상 권한)
- 예 3(대상 권한 내보내기)
- 예 4(증거 찾기를 활성화할 수 있는 권한)
- 예제 5(증거 찾기를 비활성화할 수 있는 권한)

예 1(관리형 정책,**AWSAuditManagerAdministratorAccess**)

이 예제의 정책은 관리형 정책 AWSAuditManagerAdministratorAccess입니다. 이 정책에는 Audit Manager를 사용하거나 사용하지 않도록 설정하는 기능, Audit Manager 설정을 변경하는 기능,

평가, 프레임워크, 제어 및 평가 보고서와 같은 모든 Audit Manager 리소스를 관리하는 기능이 포함됩니다.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AuditManagerAccess",
            "Effect": "Allow",
            "Action": [
                "auditmanager:*"
            ],
            "Resource": "*"
        },
        {
            "Sid": "OrganizationsAccess",
            "Effect": "Allow",
            "Action": [
                "organizations:ListAccountsForParent",
                "organizations:ListAccounts",
                "organizations:DescribeOrganization",
                "organizations:DescribeOrganizationalUnit",
                "organizations:DescribeAccount",
                "organizations:ListParents",
                "organizations:ListChildren"
            ],
            "Resource": "*"
        },
        {
            "Sid": "AllowOnlyAuditManagerIntegration",
            "Effect": "Allow",
            "Action": [
                "organizations:RegisterDelegatedAdministrator",
                "organizations:DeregisterDelegatedAdministrator",
                "organizations:EnableAWSServiceAccess"
            ],
            "Resource": "*",
            "Condition": {
                "StringLikeIfExists": {
                    "organizations:ServicePrincipal": [
                        "auditmanager.amazonaws.com"
                    ]
                }
```

```
            }
        },
        {
            "Sid": "IAMAccess",
            "Effect": "Allow",
            "Action": [
                "iam:GetUser",
                "iam:ListUsers",
                "iam:ListRoles"
            ],
            "Resource": "*"
        },
        {
            "Sid": "IAMAccessCreateSLR",
            "Effect": "Allow",
            "Action": "iam:CreateServiceLinkedRole",
            "Resource": "arn:aws:iam::*:role/aws-service-role/
auditmanager.amazonaws.com/AWSServiceRoleForAuditManager*",
            "Condition": {
                "StringLike": {
                    "iam:AWSServiceName": "auditmanager.amazonaws.com"
                }
            }
        },
        {
            "Sid": "IAMAccessManageSLR",
            "Effect": "Allow",
            "Action": [
                "iam:DeleteServiceLinkedRole",
                "iam:UpdateRoleDescription",
                "iam:GetServiceLinkedRoleDeletionStatus"
            ],
            "Resource": "arn:aws:iam::*:role/aws-service-role/
auditmanager.amazonaws.com/AWSServiceRoleForAuditManager*"
        },
        {
            "Sid": "S3Access",
            "Effect": "Allow",
            "Action": [
                "s3:ListAllMyBuckets"
            ],
            "Resource": "*"
        },
        {
```

```
            "Sid": "KmsAccess",
            "Effect": "Allow",
            "Action": [
                "kms:DescribeKey",
                "kms:ListKeys",
                "kms:ListAliases"
            ],
            "Resource": "*"
        },
        {
            "Sid": "KmsCreateGrantAccess",
            "Effect": "Allow",
            "Action": [
                "kms:CreateGrant"
            ],
            "Resource": "*",
            "Condition": {
                "Bool": {
                    "kms:GrantIsForAWSResource": "true"
                },
                "StringLike": {
                    "kms:ViaService": "auditmanager.*.amazonaws.com"
                }
            }
        },
        {
            "Sid": "SNSAccess",
            "Effect": "Allow",
            "Action": [
                "sns:ListTopics"
            ],
            "Resource": "*"
        },
        {
            "Sid": "CreateEventsAccess",
            "Effect": "Allow",
            "Action": [
                "events:PutRule"
            ],
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "events:detail-type": "Security Hub Findings - Imported"
                },
```

```
                "ForAllValues:StringEquals": {
                    "events:source": [
                        "aws.securityhub"
                    ]
                }
            }
        },
        {
            "Sid": "EventsAccess",
            "Effect": "Allow",
            "Action": [
                "events:DeleteRule",
                "events:DescribeRule",
                "events:EnableRule",
                "events:DisableRule",
                "events:ListTargetsByRule",
                "events:PutTargets",
                "events:RemoveTargets"
            ],
            "Resource": "arn:aws:events:*:*:rule/
AuditManagerSecurityHubFindingsReceiver"
        },
        {
            "Sid": "TagAccess",
            "Effect": "Allow",
            "Action": [
                "tag:GetResources"
            ],
            "Resource": "*"
        }
    ]
}
```

예 2(평가 보고서 대상 권한)

이 정책은 특정 S3 버킷에 액세스하고, 버킷에 파일을 추가하고 버킷에서 파일을 삭제할 수 있는 권한을 부여합니다. 이렇게 하면 지정된 버킷을 Audit Manager에서 평가 보고서 대상으로 사용할 수 있습니다.

*placeholder text*를 사용자 고유의 정보로 바꿉니다. 평가 보고서 대상으로 사용하는 S3 버킷과 평가 보고서를 암호화하는 데 사용하는 KMS 키를 포함하십시오.

```
{
```

```
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
               "s3:PutObject",
               "s3:GetObject",
               "s3:ListBucket",
               "s3:DeleteObject",
               "s3:GetBucketLocation",
               "s3:PutObjectAcl"
            ],
            "Resource": "arn:aws:s3:::DOC-EXAMPLE-DESTINATION-BUCKET/*"
        }
    ]
},
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "kms:Decrypt",
                "kms:Encrypt",
                "kms:GenerateDataKey"
            ],
            "Resource": "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab"
        }
    ]
}
```

예 3(대상 권한 내보내기)

다음 정책은 증거 찾기 쿼리 결과를 지정된 S3 버킷에 CloudTrail 전달할 수 있도록 허용합니다. 보안 모범 사례로서 IAM 글로벌 조건 키는 이벤트 데이터 스토어에 대해서만 S3 버킷에 CloudTrail 쓰도록 하는 `aws:SourceArn` 데 도움이 됩니다.

다음과 같이 *## ### ###*를 사용자 고유의 정보로 바꾸십시오.

- *DOC-EXAMPLE-DESTINATION-BUCKET*을 내보내기 대상으로 사용하는 S3 버킷으로 바꿉니다.
- *myQueryRunning### ### AWS ## ### ####* 교체하십시오.

- # ## AWS 계정 ID를 사용된 ID로 바꾸십시오. CloudTrail S3 버킷의 AWS 계정 ID와 동일하지 않을 수 있습니다. 조직 이벤트 데이터 저장소인 경우 관리 계정에는 AWS 계정 를 사용해야 합니다.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "Service": "cloudtrail.amazonaws.com"
            },
            "Action": [
                "s3:PutObject*",
                "s3:Abort*"
            ],
            "Resource": [
                "arn:aws:s3:::DOC-EXAMPLE-DESTINATION-BUCKET",
                "arn:aws:s3:::DOC-EXAMPLE-DESTINATION-BUCKET/*"
            ],
            "Condition": {
                "StringEquals": {
                    "AWS:SourceArn":
 "arn:aws:cloudtrail:myQueryRunningRegion:myAccountID:eventdatastore/*"
                }
            }
        },
        {
            "Effect": "Allow",
            "Principal": {
                "Service": "cloudtrail.amazonaws.com"
            },
            "Action": "s3:GetBucketAcl",
            "Resource": "arn:aws:s3:::DOC-EXAMPLE-DESTINATION-BUCKET",
            "Condition": {
                "StringEquals": {
                    "AWS:SourceArn":
 "arn:aws:cloudtrail:myQueryRunningRegion:myAccountID:eventdatastore/*"
                }
            }
        },
        {
            "Effect": "Allow",
```

```
            "Principal": {
                "Service": "cloudtrail.amazonaws.com"
            },
            "Action": [
                "kms:Decrypt*",
                "kms:GenerateDataKey*"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Principal": {
                "Service": "s3.amazonaws.com"
            },
            "Action": [
                "kms:Decrypt*",
                "kms:GenerateDataKey*"
            ],
            "Resource": "*"
        }
    ]
}
```

예 4(증거 찾기를 활성화할 수 있는 권한)

증거 찾기 기능을 활성화하고 사용하려면 다음 권한 정책이 필요합니다. 이 정책 설명을 통해 Audit Manager는 CloudTrail Lake 이벤트 데이터 저장소를 생성하고 검색 쿼리를 실행할 수 있습니다.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
           "Sid": "ManageCloudTrailLakeQueryAccess",
           "Effect": "Allow",
           "Action": [
               "cloudtrail:StartQuery",
               "cloudtrail:DescribeQuery",
               "cloudtrail:GetQueryResults",
               "cloudtrail:CancelQuery"
           ],
           "Resource": "arn:aws:cloudtrail:*:*:eventdatastore/*"
        },
        {
```

```
            "Sid": "ManageCloudTrailLakeAccess",
            "Effect": "Allow",
            "Action": [
                 "cloudtrail:CreateEventDataStore"
            ],
            "Resource": "arn:aws:cloudtrail:*:*:eventdatastore/*"
          }
    ]
}
```

예제 5(증거 찾기를 비활성화할 수 있는 권한)

이 예제 정책은 Audit Manager에서 증거 찾기 기능을 비활성화할 수 있는 권한을 부여합니다. 여기에는 기능을 처음 활성화했을 때 생성된 이벤트 데이터 저장소를 삭제하는 작업이 포함됩니다.

이 정책을 사용하기 전에 *## ### ###*를 사용자의 고유한 정보로 바꿉니다. 증거 찾기를 활성화했을 때 생성된 이벤트 데이터 저장소의 UUID를 지정해야 합니다. Audit Manager 설정에서 이벤트 데이터 스토어의 ARN을 검색할 수 있습니다. 자세한 내용을 알아보려면 AWS Audit Manager API 참조의 GetSettings(을)를 참조하세요.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
               "cloudtrail:DeleteEventDataStore",
               "cloudtrail:UpdateEventDataStore"
            ],
            "Resource": "arn:aws:cloudtrail:::event-data-store-UUID"
        }
    ]
}
```

AWS Audit Manager에 대한 사용자 관리 액세스 허용

이 예에서는 AWS Audit Manager에 대한 비관리자 관리 액세스를 허용하는 방법을 보여줍니다.

이 정책은 모든 Audit Manager 리소스(평가, 프레임워크 및 제어)를 관리할 수 있는 권한을 부여하지만 Audit Manager를 사용하거나 사용하지 않도록 설정하거나 Audit Manager 설정을 수정할 수 있는 권한은 부여하지 않습니다.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AuditManagerAccess",
            "Effect": "Allow",
            "Action": [
                "auditmanager:GetAccountStatus",
                "auditmanager:ListAssessmentFrameworks",
                "auditmanager:CreateAssessmentFramework",
                "auditmanager:GetAssessmentFramework",
                "auditmanager:UpdateAssessmentFramework",
                "auditmanager:DeleteAssessmentFramework",
                "auditmanager:ListAssessmentReports",
                "auditmanager:ListAssessments",
                "auditmanager:CreateAssessment",
                "auditmanager:ListControls",
                "auditmanager:CreateControl",
                "auditmanager:GetControl",
                "auditmanager:UpdateControl",
                "auditmanager:DeleteControl",
                "auditmanager:ListKeywordsForDataSource",
                "auditmanager:GetDelegations",
                "auditmanager:ValidateAssessmentReportIntegrity",
                "auditmanager:ListNotifications",
                "auditmanager:GetServicesInScope",
                "auditmanager:GetSettings",
                "auditmanager:ListTagsForResource",
                "auditmanager:TagResource",
                "auditmanager:UntagResource"
            ],
            "Resource": "*"
        },
        {
            "Sid": "OrganizationsAccess",
            "Effect": "Allow",
            "Action": [
                "organizations:ListAccountsForParent",
                "organizations:ListAccounts",
                "organizations:DescribeOrganization",
                "organizations:DescribeOrganizationalUnit",
                "organizations:DescribeAccount",
                "organizations:ListParents",
```

```
                "organizations:ListChildren"
            ],
            "Resource": "*"
        },
        {
            "Sid": "IAMAccess",
            "Effect": "Allow",
            "Action": [
                "iam:GetUser",
                "iam:ListUsers",
                "iam:ListRoles"
            ],
            "Resource": "*"
        },
        {
            "Sid": "S3Access",
            "Effect": "Allow",
            "Action": [
                "s3:ListAllMyBuckets"
            ],
            "Resource": "*"
        },
        {
            "Sid": "KmsAccess",
            "Effect": "Allow",
            "Action": [
                "kms:DescribeKey",
                "kms:ListKeys",
                "kms:ListAliases"
            ],
            "Resource": "*"
        },
        {
            "Sid": "SNSAccess",
            "Effect": "Allow",
            "Action": [
                "sns:ListTopics"
            ],
            "Resource": "*"
        },
        {
            "Sid": "TagAccess",
            "Effect": "Allow",
            "Action": [
```

```
                "tag:GetResources"
            ],
            "Resource": "*"
        }
    ]
}
```

사용자에게 읽기 전용 액세스 허용: AWS Audit Manager

이 정책은 평가, 프레임워크, 제어 등의 AWS Audit Manager 리소스에 대한 읽기 전용 액세스를 부여합니다.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AuditManagerAccess",
            "Effect": "Allow",
            "Action": [
                "auditmanager:Get*",
                "auditmanager:List*"
            ],
            "Resource": "*"
        }
    ]
}
```

사용자가 자신의 고유한 권한을 볼 수 있도록 허용

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

```
{
    "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": "*"
        }
    ]
}
```

Amazon SNS 주제에 알림 전송 허용 AWS Audit Manager

이 예제의 정책은 Audit Manager에 기존 Amazon SNS 주제에 알림을 보낼 수 있는 권한을 부여합니다.

- 예 1 — Audit Manager로부터 알림을 받으려면 이 예제를 사용하여 SNS 주제 액세스 정책에 권한을 추가하십시오.
- 예 2 — SNS 주제가 서버 측 암호화 AWS Key Management Service (SSEAWS KMS) 에 () 를 사용하는 경우 이 예제를 사용하여 KMS 키 액세스 정책에 권한을 추가하십시오.

다음 정책에서 권한을 가져오는 보안 주체는 Audit Manager 서비스 주체인 `auditmanager.amazonaws.com`입니다. 정책 문의 주체가 AWS 서비스 주체인 경우, 정책의 `aws:SourceArn` 또는 `aws:SourceAccount` 전역 조건 키를 사용하는 것이 좋습니다. 이러한 글로벌 조건 컨텍스트 키를 사용하면 대리인이 혼동되는 시나리오를 방지하는 데 도움이 될 수 있습니다.

예제 1(SNS 주제에 대한 권한)

Audit Manager는 이 정책 설명을 사용하여 지정된 SNS 주제에 이벤트를 게시할 수 있습니다. 지정된 SNS 주제에 대한 게시 요청은 모두 정책 조건을 충족해야 합니다.

이 정책을 사용하려면 *## ### ###*를 사용자의 고유한 정보로 바꿉니다. 다음에 유의하세요.

- 이 정책에서 aws:SourceArn 조건 키를 사용하는 경우 값은 알림을 보내는 Audit Manager 리소스의 ARN이어야 합니다. 아래 예시에서는 aws:SourceArn가 리소스 ID에 와일드카드(*)를 사용합니다. 이렇게 하면 모든 Audit Manager 리소스에 대해 Audit Manager에서 오는 모든 요청이 허용됩니다. aws:SourceArn 글로벌 조건 키를 사용하면 StringLike 또는 ArnLike 조건 연산자를 사용할 수 있습니다. 모범 사례로 ArnLike를 사용하는 방법이 가장 좋습니다.
- aws:SourceAccount 조건 키를 사용하는 경우 StringEquals 또는 StringLike 조건 연산자를 사용할 수 있습니다. 모범 사례로 StringEquals를 사용하여 최소 권한을 구현하는 것이 가장 좋습니다.
- aws:SourceAccount와 aws:SourceArn를 모두 사용하는 경우 계정 값에 동일한 계정 ID가 표시되어야 합니다.

```
{
  "Version": "2012-10-17",
  "Statement": {
      "Sid": "AllowAuditManagerToUseSNSTopic",
      "Effect": "Allow",
      "Principal": {
        "Service": "auditmanager.amazonaws.com"
      },
      "Action": "SNS:Publish",
      "Resource": "arn:aws:sns:region:accountID:topicName",
      "Condition": {
        "StringEquals": {
          "aws:SourceAccount": "accountID"
        },
        "ArnLike": {
          "aws:SourceArn": "arn:aws:auditmanager:region:accountID:*"
        }
      }
    }
}
```

다음 대체 예시에서는 StringLike 조건 연산자와 함께 aws:SourceArn 조건 키만 사용합니다.

```
      "Condition": {
        "StringLike": {
          "aws:SourceArn": "arn:aws:auditmanager:region:accountID:*"
        }
      }
```

다음 대체 예제에서는 StringLike 조건 연산자와 함께 aws:SourceAccount 조건 키만 사용합니다.

```
   "Condition": {
     "StringLike": {
       "aws:SourceAccount": "accountID"
     }
    }
```

예제 2(SNS 주제에 연결된 KMS 키에 대한 권한)

이 정책 설명을 통해 Audit Manager는 KMS 키를 사용하여 SNS 주제를 암호화하는 데 사용하는 데이터 키를 생성할 수 있습니다. 지정된 작업에 KMS 키를 사용하려는 모든 요청은 정책 조건을 충족해야 합니다.

이 정책을 사용하려면 *## ### ###*를 사용자의 고유한 정보로 바꿉니다. 다음에 유의하세요.

- 이 정책에서 aws:SourceArn 조건 키를 사용하는 경우 값은 암호화되는 리소스의 ARN이어야 합니다. 예를 들어, 이 경우에는 계정의 SNS 주제입니다. 값을 ARN 또는 와일드카드 문자(*)가 있는 ARN 또는 ARN 패턴으로 설정합니다. aws:SourceArn 조건 키와 함께 StringLike 또는 ArnLike 조건 연산자를 사용할 수 있습니다. 모범 사례로 ArnLike를 사용하는 것이 좋습니다.
- aws:SourceAccount 조건 키를 사용하는 경우 StringEquals 또는 StringLike 조건 연산자를 사용할 수 있습니다. 모범 사례로 StringEquals를 사용하여 최소 권한을 구현하는 것이 가장 좋습니다. SNS 주제의 ARN을 모르면 aws:SourceAccount을 사용할 수 있습니다.
- aws:SourceAccount와 aws:SourceArn를 모두 사용하는 경우 계정 값에 동일한 계정 ID가 표시되어야 합니다.

```
{
     "Version": "2012-10-17",
     "Statement": {
       "Sid": "AllowAuditManagerToUseKMSKey",
       "Effect": "Allow",
       "Principal": {
```

```
            "Service": "auditmanager.amazonaws.com"
        },
        "Action": [
            "kms:Decrypt",
            "kms:GenerateDataKey"
        ],
        "Resource": "arn:aws:kms:region:accountID:key/*",
        "Condition": {
            "StringEquals": {
                "aws:SourceAccount": "accountID"
            }
            "ArnLike": {
                "aws:SourceArn": "arn:aws:sns:region:accountID:topicName"
            }
      }
    }
  ]
}
```

다음 대체 예시에서는 StringLike 조건 연산자와 함께 aws:SourceArn 조건 키만 사용합니다.

```
      "Condition": {
        "StringLike": {
          "aws:SourceArn": "arn:aws:sns:region:accountID:topicName"
        }
      }
```

다음 대체 예제에서는 StringLike 조건 연산자와 함께 aws:SourceAccount 조건 키만 사용합니다.

```
   "Condition": {
     "StringLike": {
       "aws:SourceAccount": "accountID"
     }
    }
```

사용자가 증거 찾기에서 검색 쿼리를 실행하도록 허용

다음 정책은 CloudTrail Lake 이벤트 데이터 스토어에 쿼리를 수행할 권한을 부여합니다. 이 권한 정책은 증거 찾기 기능을 사용하려는 경우 필요합니다.

```
{
```

```
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ManageCloudTrailLakeQueryAccess",
            "Effect": "Allow",
            "Action": [
                "cloudtrail:StartQuery",
                "cloudtrail:DescribeQuery",
                "cloudtrail:GetQueryResults",
                "cloudtrail:CancelQuery"
            ],
            "Resource": "*"
        }
    ]
}
```

교차 서비스 혼동된 대리인 방지

혼동된 대리인 문제는 작업을 수행할 권한이 없는 개체가 권한이 더 많은 개체에게 작업을 수행하도록 강요할 수 있는 보안 문제입니다. 에서 AWS크로스 서비스 사칭으로 인해 대리인 문제가 발생할 수 있습니다. 교차 서비스 가장은 한 서비스(호출하는 서비스)가 다른 서비스(호출되는 서비스)를 직접적으로 호출할 때 발생할 수 있습니다. 호출 서비스는 권한이 없을 때 해당 권한을 사용하여 다른 고객의 리소스에 대해 작업을 수행하도록 조작될 수 있습니다. 이를 방지하기 위해 Amazon Web Services에서는 계정의 리소스에 대한 액세스 권한이 부여된 서비스 보안 주체를 사용하여 모든 서비스에 대한 데이터를 보호하는 데 도움이 되는 도구를 제공합니다.

리소스 정책에 `aws:SourceArn`및 `aws:SourceAccount`글로벌 조건 컨텍스트 키를 사용하여 리소스에 액세스할 수 있도록 다른 서비스에 AWS Audit Manager 부여하는 권한을 제한하는 것이 좋습니다.

- 하나의 리소스만 교차 서비스 액세스와 연결되도록 허용하려는 경우 `aws:SourceArn`을 사용하세요. 리소스를 여러 개 지정하려는 경우 와일드카드(*)와 함께 `aws:SourceArn`을 사용할 수도 있습니다.

  예를 들어 Amazon SNS 주제를 사용하여 Audit Manager로부터 활동 알림을 받을 수 있습니다. 이 경우 SNS 주제 액세스 정책에서 `aws:SourceArn`의 ARN 값은 알림을 보내는 Audit Manager 리소스입니다. Audit Manager 리소스가 여러 개 있을 가능성이 높으므로 와일드카드와 함께 `aws:SourceArn`을 사용하는 것이 좋습니다. 이렇게 하면 SNS 주제 액세스 정책에 모든 Audit Manager 리소스를 지정할 수 있습니다.

- 해당 계정의 모든 리소스가 교차 서비스 사용과 연결되도록 허용하려는 경우 `aws:SourceAccount`을 사용하세요.
- 만약 `aws:SourceArn` 값에 Amazon S3 버킷 ARN과 같은 계정 ID가 포함되어 있지 않은 경우 권한을 제한하려면 두 전역 조건 컨텍스트 키를 모두 사용해야 합니다.
- 두 조건을 모두 사용하고 `aws:SourceArn` 값에 계정 ID가 포함되는 경우, `aws:SourceAccount` 값 및 `aws:SourceArn` 값의 계정은 동일한 정책 문에서 사용될 경우 반드시 같은 계정 ID를 사용해야 합니다.
- 혼동된 대리인 문제로부터 보호하는 가장 효과적인 방법은 리소스의 전체 ARN이 포함된 `aws:SourceArn` 글로벌 조건 컨텍스트 키를 사용하는 것입니다. 리소스의 전체 Amazon 리소스 이름(ARN)을 모르거나 여러 리소스를 지정하는 경우, ARN의 알 수 없는 부분에 대해 와일드카드 문자(*)를 포함한 `aws:SourceArn` 글로벌 조건 컨텍스트 키를 사용합니다. 예를 들어 `arn:aws:`*`servicename`*`:*:`*`123456789012`*`:*`입니다.

Audit Manager는 대리인 지원을 혼동했습니다

Audit Manager는 다음과 같은 시나리오에서 혼란스러운 대리 지원을 제공합니다. 다음 예는 `aws:SourceArn` 및 `aws:SourceAccount` 조건 키를 사용하여 혼동된 대리자 문제를 방지하는 방법을 보여줍니다.

- 예제 정책: Audit Manager 알림을 수신하는 데 사용하는 SNS 주제
- 예제 정책: SNS 주제를 암호화하는 데 사용하는 KMS 키

Audit Manager는 Audit Manager 데이터 암호화 설정에서 제공하는 고객 관리 키에 대해 혼동된 대리자 지원을 제공하지 않습니다. 자체 고객 관리 키를 제공한 경우 해당 KMS 키 정책에서 `aws:SourceAccount`이나 `aws:SourceArn` 조건을 사용할 수 없습니다.

AWS 관리형 정책은 다음과 같습니다. AWS Audit Manager

AWS 관리형 정책은 에서 생성하고 관리하는 독립형 정책입니다. AWS AWS 관리형 정책은 많은 일반 사용 사례에 대한 권한을 제공하도록 설계되었으므로 사용자, 그룹 및 역할에 권한을 할당하기 시작할 수 있습니다.

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

관리형 정책에 정의된 권한은 변경할 수 없습니다. AWS AWS 관리형 정책에 정의된 권한을 업데이트하는 경우 AWS 해당 업데이트는 정책이 연결된 모든 주체 ID (사용자, 그룹, 역할) 에 영향을 미칩니다. AWS 새 API 작업이 시작되거나 기존 서비스에 새 AWS 서비스 API 작업을 사용할 수 있게 되면 AWS 관리형 정책을 업데이트할 가능성이 가장 높습니다.

자세한 내용은 IAM 사용 설명서의 AWS 관리형 정책을 참조하세요.

주제

- AWS 관리형 정책: AWSAuditManagerAdministratorAccess
- AWS 관리형 정책: AWSAuditManagerServiceRolePolicy
- AWS Audit ManagerAWS 관리형 정책 업데이트

AWS 관리형 정책: AWSAuditManagerAdministratorAccess

`AWSAuditManagerAdministratorAccess` 정책을 IAM 보안 인증에 연결할 수 있습니다.

이 정책은 전체 관리자 액세스를 허용하는 관리자 권한을 AWS Audit Manager부여합니다. 이 액세스에는 평가, 프레임워크 AWS Audit Manager, 제어 및 평가 보고서와 같은 모든 Audit Manager 리소스를 활성화 및 비활성화하고 설정을 변경하고 관리하는 기능이 포함됩니다. AWS Audit Manager

AWS Audit Manager 여러 AWS 서비스에 대한 광범위한 권한이 필요합니다. 이는 여러 AWS 서비스와 AWS Audit Manager 통합되어 평가 범위 내 AWS 계정 및 서비스로부터 자동으로 증거를 수집하기 때문입니다.

권한 세부 정보

이 정책에는 다음 권한이 포함되어 있습니다.

- `Audit Manager`— 주도자에게 AWS Audit Manager 리소스에 대한 모든 권한을 허용합니다.
- `Organizations`— 주도자가 계정 및 조직 단위를 나열하고 위임된 관리자를 등록 또는 등록 취소할 수 있습니다. 이는 다중 계정 지원을 활성화하고 여러 계정을 대상으로 평가를 실행하고 위임된 관리자 계정으로 증거를 통합할 수 있도록 AWS Audit Manager 하기 위해 필요합니다.
- `iam`— 주체가 IAM에서 사용자를 가져와 등록하고 서비스 연결 역할을 생성할 수 있습니다. 이는 평가를 위한 감사 소유자 및 대리인을 지정할 수 있도록 하기 위해 필요합니다. 이 정책은 또한 주도자가 서비스 연결 역할을 삭제하고 삭제 상태를 검색할 수 있도록 합니다. 이는 에서 서비스를 비활성화하기로 선택한 경우 리소스를 정리하고 서비스 연결 역할을 대신 삭제할 AWS Audit Manager 수 있도록 하기 위해 필요합니다. AWS Management Console

- s3— 주체가 사용 가능한 Amazon Simple Storage Service(Amazon S3) 버킷을 나열할 수 있습니다. 증거 보고서를 저장하거나 수동 증거를 업로드하려는 S3 버킷을 지정하려면 이 기능이 필요합니다.
- kms— 주체가 키를 나열 및 설명하고, 별칭을 나열하고, 권한 부여를 생성할 수 있습니다. 이는 데이터 암호화를 위한 고객 관리 키를 선택할 수 있도록 하기 위해 필요합니다.
- sns— 주체가 Amazon SNS에 구독 주제를 나열할 수 있습니다. 이는 AWS Audit Manager 에 알림을 보내려는 SNS 주제를 지정할 수 있도록 하기 위해 필요합니다.
- events— 주도자가 검사를 나열하고 관리할 수 있습니다. AWS Security Hub이는 모니터링 대상 AWS 서비스에 대한 AWS Security Hub 결과를 자동으로 AWS Audit Manager 수집할 수 있도록 하기 위해 필요합니다. AWS Security Hub그러면 이 데이터를 AWS Audit Manager 평가에 포함할 증거로 변환할 수 있습니다.
- tag— 주체는 태그가 지정된 리소스를 검색할 수 있습니다. 이는 AWS Audit Manager에서 프레임워크, 제어 및 평가를 탐색할 때 태그를 검색 필터로 사용할 수 있도록 하기 위해 필요합니다.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AuditManagerAccess",
            "Effect": "Allow",
            "Action": [
                "auditmanager:*"
            ],
            "Resource": "*"
        },
        {
            "Sid": "OrganizationsAccess",
            "Effect": "Allow",
            "Action": [
                "organizations:ListAccountsForParent",
                "organizations:ListAccounts",
                "organizations:DescribeOrganization",
                "organizations:DescribeOrganizationalUnit",
                "organizations:DescribeAccount",
                "organizations:ListParents",
                "organizations:ListChildren"
            ],
            "Resource": "*"
        },
        {
```

```
            "Sid": "AllowOnlyAuditManagerIntegration",
            "Effect": "Allow",
            "Action": [
                "organizations:RegisterDelegatedAdministrator",
                "organizations:DeregisterDelegatedAdministrator",
                "organizations:EnableAWSServiceAccess"
            ],
            "Resource": "*",
            "Condition": {
                "StringLikeIfExists": {
                    "organizations:ServicePrincipal": [
                        "auditmanager.amazonaws.com"
                    ]
                }
            }
        },
        {
            "Sid": "IAMAccess",
            "Effect": "Allow",
            "Action": [
                "iam:GetUser",
                "iam:ListUsers",
                "iam:ListRoles"
            ],
            "Resource": "*"
        },
        {
            "Sid": "IAMAccessCreateSLR",
            "Effect": "Allow",
            "Action": "iam:CreateServiceLinkedRole",
            "Resource": "arn:aws:iam::*:role/aws-service-role/
auditmanager.amazonaws.com/AWSServiceRoleForAuditManager*",
            "Condition": {
                "StringLike": {
                    "iam:AWSServiceName": "auditmanager.amazonaws.com"
                }
            }
        },
        {
            "Sid": "IAMAccessManageSLR",
            "Effect": "Allow",
            "Action": [
                "iam:DeleteServiceLinkedRole",
                "iam:UpdateRoleDescription",
```

```
                "iam:GetServiceLinkedRoleDeletionStatus"
            ],
            "Resource": "arn:aws:iam::*:role/aws-service-role/
auditmanager.amazonaws.com/AWSServiceRoleForAuditManager*"
        },
        {
            "Sid": "S3Access",
            "Effect": "Allow",
            "Action": [
                "s3:ListAllMyBuckets"
            ],
            "Resource": "*"
        },
        {
            "Sid": "KmsAccess",
            "Effect": "Allow",
            "Action": [
                "kms:DescribeKey",
                "kms:ListKeys",
                "kms:ListAliases"
            ],
            "Resource": "*"
        },
        {
            "Sid": "KmsCreateGrantAccess",
            "Effect": "Allow",
            "Action": [
                "kms:CreateGrant"
            ],
            "Resource": "*",
            "Condition": {
                "Bool": {
                    "kms:GrantIsForAWSResource": "true"
                },
                "StringLike": {
                    "kms:ViaService": "auditmanager.*.amazonaws.com"
                }
            }
        },
        {
            "Sid": "SNSAccess",
            "Effect": "Allow",
            "Action": [
                "sns:ListTopics"
```

```
            ],
            "Resource": "*"
        },
        {
            "Sid": "CreateEventsAccess",
            "Effect": "Allow",
            "Action": [
                "events:PutRule"
            ],
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "events:detail-type": "Security Hub Findings - Imported"
                },
                "ForAllValues:StringEquals": {
                    "events:source": [
                        "aws.securityhub"
                    ]
                }
            }
        },
        {
            "Sid": "EventsAccess",
            "Effect": "Allow",
            "Action": [
                "events:DeleteRule",
                "events:DescribeRule",
                "events:EnableRule",
                "events:DisableRule",
                "events:ListTargetsByRule",
                "events:PutTargets",
                "events:RemoveTargets"
            ],
            "Resource": "arn:aws:events:*:*:rule/
AuditManagerSecurityHubFindingsReceiver"
        },
        {
            "Sid": "TagAccess",
            "Effect": "Allow",
            "Action": [
                "tag:GetResources"
            ],
            "Resource": "*"
        }
```

```
    ]
}
```

AWS 관리형 정책: AWSAuditManagerServiceRolePolicy

`AWSAuditManagerServiceRolePolicy`를 IAM 엔터티에 연결할 수 없습니다. 이 정책은 사용자를 AWS Audit Manager 대신하여 작업을 수행할 수 있는 서비스 연결 역할에 연결됩니다. `AWSServiceRoleForAuditManager` 자세한 내용은 AWS Audit Manager에 대한 서비스 연결 역할 사용을 참조하십시오.

역할 권한 정책 `AWSAuditManagerServiceRolePolicy`은 사용자를 대신하여 다음을 수행하여 자동화된 증거를 AWS Audit Manager 가 수집할 수 있도록 허용합니다.

- 다음 데이터 소스에서 데이터를 수집합니다.
  - 관리 이벤트: AWS CloudTrail
  - 규정 준수 점검: AWS Config 규칙
  - 규정 준수 점검: AWS Security Hub
- API 호출을 사용하여 다음 AWS 서비스에 대한 리소스 구성을 설명하십시오.

> **Tip**
>
> Audit Manager가 이러한 서비스에서 증거를 수집하는 데 사용하는 API 호출에 대한 자세한 내용은 이 안내서의 사용자 지정 컨트롤 데이터 소스를 지원하는 API 직접 호출를 참조하십시오.

  - AWS Certificate Manager
  - AWS Backup
  - Amazon Bedrock
  - AWS CloudTrail
  - 아마존 CloudWatch
  - 아마존 CloudWatch 로그
  - Amazon Cognito 사용자 풀
  - AWS Config
  - AWS Direct Connect
  - Amazon DynamoDB

- Amazon EC2
- Amazon Elastic Container Service
- Amazon Elastic File System
- Amazon Elastic Kubernetes 서비스
- 아마존 ElastiCache
- Elastic Load Balancing
- Amazon EMR
- 아마존 EventBridge
- Amazon Data Firehose
- Amazon FSx
- 아마존 GuardDuty
- AWS Identity and Access Management (IAM)
- Amazon Kinesis
- AWS KMS
- AWS Lambda
- AWS License Manager
- Amazon Managed Streaming for Apache Kafka
- AWS Organizations
- Amazon Relational Database Service
- Amazon Redshift
- Amazon Route 53
- Amazon S3
- AWS Security Hub
- Amazon Simple Notification Service
- Amazon Simple Queue Service
- AWS WAF

권한 세부 정보

~~AWSAuditManagerServiceRolePolicy지정된 리소스에서 다음 작업을 AWS Audit Manager 완료~~ 할 수 있습니다.

- acm:GetAccountConfiguration
- acm:ListCertificates
- backup:ListRecoveryPointsByResource
- bedrock:GetCustomModel
- bedrock:GetFoundationModel
- bedrock:GetModelCustomizationJob
- bedrock:GetModelInvocationLoggingConfiguration
- bedrock:ListCustomModels
- bedrock:ListFoundationModels
- bedrock:ListModelCustomizationJobs
- cloudtrail:DescribeTrails
- cloudtrail:LookupEvents
- cloudwatch:DescribeAlarms
- cloudwatch:DescribeAlarmsForMetric
- cloudwatch:GetMetricStatistics
- cloudwatch:ListMetrics
- cognito-idp:DescribeUserPool
- config:DescribeConfigRules
- config:DescribeDeliveryChannels
- config:ListDiscoveredResources
- directconnect:DescribeDirectConnectGateways
- directconnect:DescribeVirtualGateways
- dynamodb:DescribeTable
- dynamodb:ListBackups
- dynamodb:ListGlobalTables
- dynamodb:ListTables
- ec2:DescribeAddresses
- ec2:DescribeCustomerGateways
- ec2:DescribeEgressOnlyInternetGateways
- ec2:DescribeFlowLogs

- ec2:DescribeInstances
- ec2:DescribeInternetGateways
- ec2:DescribeLocalGatewayRouteTableVirtualInterfaceGroupAssociations
- ec2:DescribeLocalGateways
- ec2:DescribeLocalGatewayVirtualInterfaces
- ec2:DescribeNatGateways
- ec2:DescribeNetworkAcls
- ec2:DescribeRouteTables
- ec2:DescribeSecurityGroups
- ec2:DescribeSnapshots
- ec2:DescribeTransitGateways
- ec2:DescribeVolumes
- ec2:DescribeVpcEndpoints
- ec2:DescribeVpcPeeringConnections
- ec2:DescribeVpcs
- ec2:DescribeVpnConnections
- ec2:DescribeVpnGateways
- ec2:GetEbsDefaultKmsKeyId
- ec2:GetEbsEncryptionByDefault
- ecs:DescribeClusters
- eks:DescribeAddonVersions
- elasticache:DescribeCacheClusters
- elasticache:DescribeServiceUpdates
- elasticfilesystem:DescribeAccessPoints
- elasticfilesystem:DescribeFileSystems
- elasticloadbalancing:DescribeLoadBalancers
- elasticloadbalancing:DescribeSslPolicies
- elasticloadbalancing:DescribeTargetGroups
- elasticmapreduce:ListClusters
- elasticmapreduce:ListSecurityConfigurations

- events:DeleteRule
- events:DescribeRule
- events:DisableRule
- events:EnableRule
- events:ListConnections
- events:ListEventBuses
- events:ListEventSources
- events:ListRules
- events:ListTargetsByRule
- events:PutRule
- events:PutTargets
- events:RemoveTargets
- firehose:ListDeliveryStreams
- fsx:DescribeFileSystems
- guardduty:ListDetectors
- iam:GenerateCredentialReport
- iam:GetAccountAuthorizationDetails
- iam:GetAccountPasswordPolicy
- iam:GetAccountSummary
- iam:GetCredentialReport
- iam:ListEntitiesForPolicy
- iam:ListGroupPolicies
- iam:ListGroups
- iam:ListOpenIdConnectProviders
- iam:ListPolicies
- iam:ListRolePolicies
- iam:ListRoles
- iam:ListSamlProviders
- iam:ListUserPolicies
- iam:ListUsers

- iam:ListVirtualMFADevices
- kafka:ListClusters
- kafka:ListKafkaVersions
- kinesis:ListStreams
- kms:DescribeKey
- kms:GetKeyPolicy
- kms:GetKeyRotationStatus
- kms:ListGrants
- kms:ListKeyPolicies
- kms:ListKeys
- lambda:ListFunctions
- license-manager:ListAssociationsForLicenseConfiguration
- license-manager:ListLicenseConfigurations
- license-manager:ListUsageForLicenseConfiguration
- logs:DescribeDestinations
- logs:DescribeExportTasks
- logs:DescribeLogGroups
- logs:DescribeMetricFilters
- logs:DescribeResourcePolicies
- logs:FilterLogEvents
- organizations:DescribeOrganization
- organizations:DescribePolicy
- rds:DescribeCertificates
- rds:DescribeDbClusterEndpoints
- rds:DescribeDbClusterParameterGroups
- rds:DescribeDbClusters
- rds:DescribeDBInstances
- rds:DescribeDbSecurityGroups
- redshift:DescribeClusters
- route53:GetQueryLoggingConfig

- s3:GetBucketPolicy
  - 이 API service-linked-role 작업은 사용 가능한 범위 내에서 작동합니다. AWS 계정 크로스 계정 버킷 정책에는 액세스할 수 없습니다.
- s3:GetBucketPublicAccessBlock
- s3:GetBucketVersioning
- s3:GetEncryptionConfiguration
- s3:GetLifecycleConfiguration
- s3:ListAllMyBuckets
- securityhub:DescribeStandards
- sns:ListTopics
- sqs:ListQueues
- waf-regional:GetLoggingConfiguration
- waf-regional:ListRuleGroups
- waf-regional:ListSubscribedRuleGroups
- waf-regional:ListWebACLs
- waf:ListActivatedRulesInRuleGroup

```
{
 "Version": "2012-10-17",
 "Statement": [
  {
   "Effect": "Allow",
   "Action": [
    "acm:GetAccountConfiguration",
    "acm:ListCertificates",
    "backup:ListRecoveryPointsByResource",
    "bedrock:GetCustomModel",
    "bedrock:GetFoundationModel",
    "bedrock:GetModelCustomizationJob",
    "bedrock:GetModelInvocationLoggingConfiguration",
    "bedrock:ListCustomModels",
    "bedrock:ListFoundationModels",
    "bedrock:ListModelCustomizationJobs",
    "cloudtrail:DescribeTrails",
    "cloudtrail:LookupEvents",
    "cloudwatch:DescribeAlarms",
```

```
    "cloudwatch:DescribeAlarmsForMetric",
    "cloudwatch:GetMetricStatistics",
    "cloudwatch:ListMetrics",
    "cognito-idp:DescribeUserPool",
    "config:DescribeConfigRules",
    "config:DescribeDeliveryChannels",
    "config:ListDiscoveredResources",
    "directconnect:DescribeDirectConnectGateways",
    "directconnect:DescribeVirtualGateways",
    "dynamodb:DescribeTable",
    "dynamodb:ListBackups",
    "dynamodb:ListGlobalTables",
    "dynamodb:ListTables",
    "ec2:DescribeAddresses",
    "ec2:DescribeCustomerGateways",
    "ec2:DescribeEgressOnlyInternetGateways",
    "ec2:DescribeFlowLogs",
    "ec2:DescribeInstances",
    "ec2:DescribeInternetGateways",
    "ec2:DescribeLocalGatewayRouteTableVirtualInterfaceGroupAssociations",
    "ec2:DescribeLocalGateways",
    "ec2:DescribeLocalGatewayVirtualInterfaces",
    "ec2:DescribeNatGateways",
    "ec2:DescribeNetworkAcls",
    "ec2:DescribeRouteTables",
    "ec2:DescribeSecurityGroups",
    "ec2:DescribeSnapshots",
    "ec2:DescribeTransitGateways",
    "ec2:DescribeVolumes",
    "ec2:DescribeVpcEndpoints",
    "ec2:DescribeVpcPeeringConnections",
    "ec2:DescribeVpcs",
    "ec2:DescribeVpnConnections",
    "ec2:DescribeVpnGateways",
    "ec2:GetEbsDefaultKmsKeyId",
    "ec2:GetEbsEncryptionByDefault",
    "ecs:DescribeClusters",
    "eks:DescribeAddonVersions",
    "elasticache:DescribeCacheClusters",
    "elasticache:DescribeServiceUpdates",
    "elasticfilesystem:DescribeAccessPoints",
    "elasticfilesystem:DescribeFileSystems",
    "elasticloadbalancing:DescribeLoadBalancers",
    "elasticloadbalancing:DescribeSslPolicies",
```

```
    "elasticloadbalancing:DescribeTargetGroups",
    "elasticmapreduce:ListClusters",
    "elasticmapreduce:ListSecurityConfigurations",
    "events:DescribeRule",
    "events:ListConnections",
    "events:ListEventBuses",
    "events:ListEventSources",
    "events:ListRules",
    "firehose:ListDeliveryStreams",
    "fsx:DescribeFileSystems",
    "guardduty:ListDetectors",
    "iam:GenerateCredentialReport",
    "iam:GetAccountAuthorizationDetails",
    "iam:GetAccountPasswordPolicy",
    "iam:GetAccountSummary",
    "iam:GetCredentialReport",
    "iam:ListEntitiesForPolicy",
    "iam:ListGroupPolicies",
    "iam:ListGroups",
    "iam:ListOpenIdConnectProviders",
    "iam:ListPolicies",
    "iam:ListRolePolicies",
    "iam:ListRoles",
    "iam:ListSamlProviders",
    "iam:ListUserPolicies",
    "iam:ListUsers",
    "iam:ListVirtualMFADevices",
    "kafka:ListClusters",
    "kafka:ListKafkaVersions",
    "kinesis:ListStreams",
    "kms:DescribeKey",
    "kms:GetKeyPolicy",
    "kms:GetKeyRotationStatus",
    "kms:ListGrants",
    "kms:ListKeyPolicies",
    "kms:ListKeys",
    "lambda:ListFunctions",
    "license-manager:ListAssociationsForLicenseConfiguration",
    "license-manager:ListLicenseConfigurations",
    "license-manager:ListUsageForLicenseConfiguration",
    "logs:DescribeDestinations",
    "logs:DescribeExportTasks",
    "logs:DescribeLogGroups",
    "logs:DescribeMetricFilters",
```

```
    "logs:DescribeResourcePolicies",
    "logs:FilterLogEvents",
    "organizations:DescribeOrganization",
    "organizations:DescribePolicy",
    "rds:DescribeCertificates",
    "rds:DescribeDbClusterEndpoints",
    "rds:DescribeDbClusterParameterGroups",
    "rds:DescribeDbClusters",
    "rds:DescribeDBInstances",
    "rds:DescribeDbSecurityGroups",
    "redshift:DescribeClusters",
    "route53:GetQueryLoggingConfig",
    "s3:GetBucketPublicAccessBlock",
    "s3:GetBucketVersioning",
    "s3:GetEncryptionConfiguration",
    "s3:GetLifecycleConfiguration",
    "s3:ListAllMyBuckets",
    "securityhub:DescribeStandards",
    "sns:ListTopics",
    "sqs:ListQueues",
    "waf-regional:GetLoggingConfiguration",
    "waf-regional:ListRuleGroups",
    "waf-regional:ListSubscribedRuleGroups",
    "waf-regional:ListWebACLs",
    "waf:ListActivatedRulesInRuleGroup"
   ],
   "Resource": "*",
   "Sid": "AuditManagerAPICallAccess"
  },
  {
   "Sid": "AuditManagerS3GetBucketPolicyAccess",
   "Effect": "Allow",
   "Action": [
    "s3:GetBucketPolicy"
   ],
   "Resource": "*",
   "Condition": {
    "StringEquals": {
     "aws:ResourceAccount": [
      "${aws:PrincipalAccount}"
     ]
    }
   }
  },
```

```
  {
   "Sid": "CreateEventsAccess",
   "Effect": "Allow",
   "Action": [
    "events:PutRule"
   ],
   "Resource": "arn:aws:events:*:*:rule/AuditManagerSecurityHubFindingsReceiver",
   "Condition": {
    "StringEquals": {
     "events:detail-type": "Security Hub Findings - Imported"
    },
    "Null": {
     "events:source": "false"
    },
    "ForAllValues:StringEquals": {
     "events:source": [
      "aws.securityhub"
     ]
    }
   }
  },
  {
   "Sid": "EventsAccess",
   "Effect": "Allow",
   "Action": [
    "events:DeleteRule",
    "events:DescribeRule",
    "events:EnableRule",
    "events:DisableRule",
    "events:ListTargetsByRule",
    "events:PutTargets",
    "events:RemoveTargets"
   ],
   "Resource": "arn:aws:events:*:*:rule/AuditManagerSecurityHubFindingsReceiver"
  }
 ]
}
```

AWS Audit ManagerAWS 관리형 정책 업데이트

이 서비스가 이러한 변경 사항을 추적하기 시작한 AWS Audit Manager 이후의 AWS 관리형 정책 업데이트에 대한 세부 정보를 볼 수 있습니다. 이 페이지의 변경 사항에 대한 자동 알림을 받으려면 AWS Audit Manager 문서 기록 페이지에서 RSS 피드를 구독하십시오.

변경 사항	설명	날짜
AWSAuditManagerServiceRolePolicy - 기존 정책 업데이트	이제 서비스 연결 역할을 통해 작업을 수행할 AWS Audit Manager 수 있습니다. `s3:GetBucketPolicy` 이 API 작업은 AWS 생성형 AI 모범 사례 프레임워크 v1을 지원하는 데 필요합니다. 이를 통해 Audit Manager는 생성형 AI 모델 데이터 훈련 데이터 세트에 적용되는 정책 제한 사항에 대한 자동 증거를 수집할 수 있습니다. `GetBucketPolicy` 작업은 사용 AWS 계정 가능한 범위 내에서 작동합니다. service-linked-role 크로스 계정 버킷 정책에는 액세스할 수 없습니다.	2023년 12월 6일
AWSAuditManagerServiceRolePolicy - 기존 정책 업데이트	에 다음과 같은 권한을 추가했습니다. `AWSAuditManagerServiceRolePolicy` AWS Audit Manager 이제 다음 작업을 수행하여 내 리소스에 대한 자동 증거를 수집할 수 있습니다 AWS 계정. • `acm:GetAccountConfiguration` • `acm:ListCertificates` • `backup:ListRecoveryPointsByResource` • `bedrock:GetCustomModel` • `bedrock:GetFoundationModel` • `bedrock:GetModelCustomizationJob` • `bedrock:GetModelInvocationLoggingConfiguration` • `bedrock:ListCustomModels` • `bedrock:ListFoundationModels`	2023년 11월 6일

변경 사항	설명	날짜
	• bedrock:ListModelCustomizationJobs • cloudtrail:LookupEvents • cloudwatch:DescribeAlarmsForMetric • cloudwatch:GetMetricStatistics • cloudwatch:ListMetrics • directconnect:DescribeDirectConnectGateways • directconnect:DescribeVirtualGateways • dynamodb:ListBackups • dynamodb:ListGlobalTables • ec2:DescribeAddresses • ec2:DescribeCustomerGateways • ec2:DescribeEgressOnlyInternetGateways • ec2:DescribeInternetGateways • ec2:DescribeLocalGatewayRouteTableVirtualInterfaceGroupAssociations • ec2:DescribeLocalGateways • ec2:DescribeLocalGatewayVirtualInterfaces • ec2:DescribeNatGateways • ec2:DescribeTransitGateways • ec2:DescribeVpcPeeringConnections • ec2:DescribeVpnConnections • ec2:DescribeVpnGateways	

변경 사항	설명	날짜
	• ec2:GetEbsDefaultKmsKeyId • ec2:GetEbsEncryptionByDefault • ecs:DescribeClusters • eks:DescribeAddonVersions • elasticache:DescribeCacheClusters • elasticache:DescribeServiceUpdates • elasticfilesystem:DescribeAccessPoints • elasticloadbalancing:DescribeLoadBalancers • elasticloadbalancing:DescribeSslPolicies • elasticloadbalancing:DescribeTargetGroups • elasticmapreduce:ListClusters • elasticmapreduce:ListSecurityConfigurations • events:ListConnections • events:ListEventBuses • events:ListEventSources • events:ListRules • firehose:ListDeliveryStreams • fsx:DescribeFileSystems • iam:GetAccountPasswordPolicy • iam:GetCredentialReport • iam:ListOpenIdConnectProviders • iam:ListSamlProviders • iam:ListVirtualMFADevices	

변경 사항	설명	날짜
	• kafka:ListClusters • kafka:ListKafkaVersions • kinesis:ListStreams • lambda:ListFunctions • logs:DescribeDestinations • logs:DescribeExportTasks • logs:DescribeLogGroups • logs:DescribeMetricFilters • logs:DescribeResourcePolicies • logs:FilterLogEvents • rds:DescribeCertificates • rds:DescribeDbClusterEndpoints • rds:DescribeDbClusterParameterGroups • rds:DescribeDbClusters • rds:DescribeDbSecurityGroups • redshift:DescribeClusters • s3:GetBucketPublicAccessBlock • s3:GetBucketVersioning • sns:ListTopics • sqs:ListQueues • waf-regional:GetLoggingConfiguration • waf-regional:ListRuleGroups • waf-regional:ListSubscribedRuleGroups • waf-regional:ListWebACLs	

변경 사항	설명	날짜
AWSAuditManagerServiceRolePolicy - 기존 정책 업데이트	다음과 같은 권한을 AWSAuditManagerServiceRolePolicy 에 추가했습니다. • dynamodb:DescribeTable • dynamodb:ListTables • ec2:DescribeVolumes • kms:GetKeyPolicy • kms:GetKeyRotationStatus • kms:ListKeyPolicies • rds:DescribeDBInstances • redshift:DescribeClusters • s3:GetEncryptionConfiguration • s3:ListAllMyBuckets	07/07/2022
AWSAuditManagerServiceRolePolicy-기존 정책 업데이트	이제 서비스 연결 역할을 통해 작업을 수행할 수 있습니다. AWS Audit Manager organizations:DescribeOrganization 또한 와일드카드(*) 에서 특정 유형의 CreateEventsAccess 리소스(arn:aws:events:*:*:rule/AuditManagerSecurityHubFindingsReceiver)로 리소스 범위를 축소했습니다. 마지막으로, 소스 값이 존재하고 값이 null이 아님을 확인하기 위해 events:source 조건 키에 조건 연산자를 추가했습니다. Null	2022년 5월 20일
AWSAuditManagerAdministratorAccess-기존 정책 업데이트	다중 값 키라는 점을 반영하기 위해 events:source 의 키 조건 정책을 업데이트했습니다.	04/29/2022
AWSAuditManagerServiceRolePolicy-기존 정책 업데이트	다중 값 키라는 점을 반영하기 위해 events:source 의 키 조건 정책을 업데이트했습니다.	03/16/2022

변경 사항	설명	날짜
AWS Audit Manager 변경 내용 추적 시작	AWS Audit Manager AWS 관리형 정책의 변경 사항 추적을 시작했습니다.	2021년 5월 6일

ID 및 액세스 문제 해결 AWS Audit Manager

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

주제

- 다음과 같은 조치를 취할 권한이 없습니다. AWS Audit Manager
- IAM을 수행할 권한이 없습니다. PassRole
- 외부 사용자가 내 AWS Audit Manager 리소스에 액세스할 수 있도록 AWS 계정 허용하고 싶습니다.

다음과 같은 조치를 취할 권한이 없습니다. AWS Audit Manager

이 `AccessDeniedException` 오류는 사용자에게 Audit Manager API 작업 사용 AWS Audit Manager 권한이 없을 때 나타납니다.

이 경우 관리자는 사용자의 액세스를 허용하도록 정책을 업데이트해야 합니다.

IAM을 수행할 권한이 없습니다. PassRole

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

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

다음 예제 오류는 `marymajor`라는 IAM 사용자가 콘솔을 사용하여 Audit 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 필요하면 관리자에게 문의하세요. AWS 관리자는 로그인 자격 증명을 제공한 사람입니다.

외부 사용자가 내 AWS Audit Manager 리소스에 액세스할 수 있도록 AWS 계정 허용하고 싶습니다.

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.

- Audit Manager에서 이러한 기능을 지원하는지 여부를 알아보려면 IAM의 AWS Audit Manager 작동 방식 단원을 참조하세요.
- 소유한 리소스에 대한 액세스 권한을 AWS 계정 부여하는 방법을 알아보려면 IAM 사용 설명서에서 자신이 소유한 다른 AWS 계정 IAM 사용자에게 액세스 권한 제공을 참조하십시오.
- 제3자에게 리소스에 대한 액세스 권한을 제공하는 방법을 알아보려면 IAM 사용 설명서의 타사 AWS 계정AWS 계정 소유에 대한 액세스 제공을 참조하십시오.
- 보안 인증 연동을 통해 액세스 권한을 제공하는 방법을 알아보려면 IAM 사용 설명서의 외부에서 인증된 사용자에게 액세스 권한 제공(보안 인증 연동)을 참조하세요.
- 교차 계정 액세스를 위한 역할과 리소스 기반 정책 사용의 차이점을 알아보려면 IAM 사용 설명서의 IAM 역할과 리소스 기반 정책의 차이를 참조하세요.

서비스 연결 역할 사용 AWS Audit Manager

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

서비스에 연결된 역할을 사용하면 필요한 권한을 수동으로 추가할 필요가 없으므로 설정이 AWS Audit Manager 더 쉬워집니다. Audit Manager에서 서비스 연결 역할의 권한을 정의하므로 다르게 정의되지 않은 한, Audit Manager만 해당 역할을 수임할 수 있습니다. 정의된 권한에는 신뢰 정책과 권한 정책이 포함되며 이 권한 정책은 다른 IAM 엔터티에 연결할 수 없습니다.

서비스 연결 역할을 지원하는 기타 서비스에 대한 자세한 내용은 IAM으로 작업하는AWS 서비스를 참조하고 서비스 연결 역할 열에 예가 표시된 서비스를 찾으십시오. 해당 서비스에 대한 서비스 연결 역할 설명서를 보려면 예 링크를 선택합니다.

서비스 연결 역할 권한에 대한 서비스 연결 역할 권한 AWS Audit Manager

Audit Manager는 이름이 지정된 서비스 연결 역할을 사용하며**AWSServiceRoleForAuditManager**, 이 역할을 통해 사용하거나 관리하는 AWS 서비스 및 리소스에 액세스할 수 있습니다. AWS Audit Manager

`AWSServiceRoleForAuditManager` 서비스 연결 역할은 역할을 수임하기 위해 `auditmanager.amazonaws.com` 서비스를 신뢰합니다.

역할 권한 정책을 통해 Audit Manager는 사용자의 AWS 사용에 대한 자동화된 증거를 수집할 수 있습니다. `AWSAuditManagerServiceRolePolicy` 보다 구체적으로 사용자를 대신하여 다음 작업을 수행할 수 있습니다.

- Audit Manager는 규정 준수 확인 증거를 수집하는 AWS Security Hub 데 사용할 수 있습니다. 이 경우 Audit Manager는 다음 권한을 사용하여 보안 검사 결과를 에서 직접 AWS Security Hub보고합니다. 그런 다음 결과를 관련 평가 관리에 증거로 첨부합니다.
  - `securityhub:DescribeStandards`

  > **Note**
  >
  > Audit Manager가 설명할 수 있는 특정 Security Hub 컨트롤에 대한 자세한 내용은 AWS Audit Manager이 지원하는AWS Security Hub 제어를 참조하십시오.

- Audit Manager는 규정 준수 확인 증거를 수집하는 AWS Config 데 사용할 수 있습니다. 이 경우 Audit Manager는 다음 권한을 사용하여 AWS Config 규칙 평가 결과를 에서 AWS Config직접 보고합니다. 그런 다음 결과를 관련 평가 관리에 증거로 첨부합니다.
  - `config:DescribeConfigRules`
  - `config:DescribeDeliveryChannels`
  - `config:ListDiscoveredResources`

  > **Note**
  >
  > Audit Manager에서 설명할 수 있는 특정 AWS Config 규칙에 대한 자세한 내용은 지원되는 AWS Config 규칙을 참조하십시오 AWS Audit Manager.

- Audit Manager는 사용자 활동 증거를 수집하는 AWS CloudTrail 데 사용할 수 있습니다. 이 경우 Audit Manager는 다음 권한을 사용하여 CloudTrail 로그에서 사용자 활동을 캡처합니다. 그런 다음 활동을 관련 평가 제어에 증거로 첨부합니다.
  - `cloudtrail:DescribeTrails`
  - `cloudtrail:LookupEvents`

  > **Note**
  >
  > Audit Manager가 설명할 수 있는 특정 CloudTrail 이벤트에 대한 자세한 내용은 지원되는 AWS CloudTrail 이벤트 이름을 참조하십시오 AWS Audit Manager.

- Audit AWS Manager는 API 호출을 사용하여 리소스 구성 증거를 수집할 수 있습니다. 이 경우 Audit Manager는 다음 권한을 사용하여 다음에 AWS 서비스에 대한 리소스 구성을 설명하는 읽기 전용 API를 호출합니다. 그런 다음 API 응답을 관련 평가 제어 항목에 증거로 첨부합니다.
  - `acm:GetAccountConfiguration`
  - `acm:ListCertificates`
  - `backup:ListRecoveryPointsByResource`
  - `bedrock:GetCustomModel`
  - `bedrock:GetFoundationModel`
  - `bedrock:GetModelCustomizationJob`
  - `bedrock:GetModelInvocationLoggingConfiguration`
  - `bedrock:ListCustomModels`
  - `bedrock:ListFoundationModels`
  - `bedrock:ListModelCustomizationJobs`
  - `cloudwatch:DescribeAlarms`
  - `cloudwatch:DescribeAlarmsForMetric`
  - `cloudwatch:GetMetricStatistics`
  - `cloudwatch:ListMetrics`
  - `cognito-idp:DescribeUserPool`
  - `directconnect:DescribeDirectConnectGateways`
  - `directconnect:DescribeVirtualGateways`
  - `dynamodb:DescribeTable`
  - `dynamodb:ListBackups`

- dynamodb:ListGlobalTables
- dynamodb:ListTables
- ec2:DescribeAddresses
- ec2:DescribeCustomerGateways
- ec2:DescribeEgressOnlyInternetGateways
- ec2:DescribeFlowLogs
- ec2:DescribeInstances
- ec2:DescribeInternetGateways
- ec2:DescribeLocalGatewayRouteTableVirtualInterfaceGroupAssociations
- ec2:DescribeLocalGateways
- ec2:DescribeLocalGatewayVirtualInterfaces
- ec2:DescribeNatGateways
- ec2:DescribeNetworkAcls
- ec2:DescribeRouteTables
- ec2:DescribeSecurityGroups
- ec2:DescribeSnapshots
- ec2:DescribeTransitGateways
- ec2:DescribeVolumes
- ec2:DescribeVpcEndpoints
- ec2:DescribeVpcPeeringConnections
- ec2:DescribeVpcs
- ec2:DescribeVpnConnections
- ec2:DescribeVpnGateways
- ec2:GetEbsDefaultKmsKeyId
- ec2:GetEbsEncryptionByDefault
- ecs:DescribeClusters
- eks:DescribeAddonVersions
- elasticache:DescribeCacheClusters
- elasticache:DescribeServiceUpdates
- elasticfilesystem:DescribeAccessPoints

- elasticfilesystem:DescribeFileSystems
- elasticloadbalancing:DescribeLoadBalancers
- elasticloadbalancing:DescribeSslPolicies
- elasticloadbalancing:DescribeTargetGroups
- elasticmapreduce:ListClusters
- elasticmapreduce:ListSecurityConfigurations
- events:DeleteRule
- events:DescribeRule
- events:DisableRule
- events:EnableRule
- events:ListConnections
- events:ListEventBuses
- events:ListEventSources
- events:ListRules
- events:ListTargetsByRule
- events:PutRule
- events:PutTargets
- events:RemoveTargets
- firehose:ListDeliveryStreams
- fsx:DescribeFileSystems
- guardduty:ListDetectors
- iam:GenerateCredentialReport
- iam:GetAccountAuthorizationDetails
- iam:GetAccountPasswordPolicy
- iam:GetAccountSummary
- iam:GetCredentialReport
- iam:ListEntitiesForPolicy
- iam:ListGroupPolicies
- iam:ListGroups
- iam:ListOpenIdConnectProviders

- iam:ListPolicies
- iam:ListRolePolicies
- iam:ListRoles
- iam:ListSamlProviders
- iam:ListUserPolicies
- iam:ListUsers
- iam:ListVirtualMFADevices
- kafka:ListClusters
- kafka:ListKafkaVersions
- kinesis:ListStreams
- kms:DescribeKey
- kms:GetKeyPolicy
- kms:GetKeyRotationStatus
- kms:ListGrants
- kms:ListKeyPolicies
- kms:ListKeys
- lambda:ListFunctions
- license-manager:ListAssociationsForLicenseConfiguration
- license-manager:ListLicenseConfigurations
- license-manager:ListUsageForLicenseConfiguration
- logs:DescribeDestinations
- logs:DescribeExportTasks
- logs:DescribeLogGroups
- logs:DescribeMetricFilters
- logs:DescribeResourcePolicies
- logs:FilterLogEvents
- organizations:DescribeOrganization
- organizations:DescribePolicy
- rds:DescribeCertificates
- rds:DescribeDbClusterEndpoints

- rds:DescribeDbClusterParameterGroups
- rds:DescribeDbClusters
- rds:DescribeDBInstances
- rds:DescribeDbSecurityGroups
- redshift:DescribeClusters
- route53:GetQueryLoggingConfig
- s3:GetBucketPolicy
  - 이 API service-linked-role 작업은 가능한 범위 내에서 작동합니다. AWS 계정 크로스 계정 버킷 정책에는 액세스할 수 없습니다.
- s3:GetBucketPublicAccessBlock
- s3:GetBucketVersioning
- s3:GetEncryptionConfiguration
- s3:GetLifecycleConfiguration
- s3:ListAllMyBuckets
- sns:ListTopics
- sqs:ListQueues
- waf-regional:GetLoggingConfiguration
- waf-regional:ListRuleGroups
- waf-regional:ListSubscribedRuleGroups
- waf-regional:ListWebACLs
- waf:ListActivatedRulesInRuleGroup

> **Note**
>
> Audit Manager가 설명할 수 있는 특정 API 호출에 대한 자세한 내용은 섹션 사용자 지정 컨트롤 데이터 소스를 지원하는 API 직접 호출을 참조하세요.

서비스 연결 AWSServiceRoleForAuditManager 역할의 전체 권한 세부 정보를 보려면 AWS 관리형 정책 참조 AWSAuditManagerServiceRolePolicy가이드의 내용을 참조하십시오.

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 권한을 참조하십시오.

서비스 연결 역할 생성 AWS Audit Manager

서비스 링크 역할은 수동으로 생성할 필요가 없습니다. AWS Audit Manager활성화하면 서비스가 자동으로 서비스 연결 역할을 생성합니다. 의 온보딩 페이지 또는 API 또는 AWS CLI를 통해 Audit Manager를 활성화할 수 있습니다. AWS Management Console자세한 내용은 사용자 가이드의 AWS Audit Manager 활성화을 참조하세요.

이 서비스 연결 역할을 삭제했다가 다시 생성해야 하는 경우 동일한 프로세스를 사용하여 계정에서 역할을 다시 생성할 수 있습니다.

AWS Audit Manager 서비스 연결 역할 편집

AWS Audit Manager `AWSServiceRoleForAuditManager`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.

IAM 엔터티가 **`AWSServiceRoleForAuditManager`** 서비스 연결 역할의 설명을 편집할 수 있도록 허용하려면

서비스 연결 역할의 설명을 편집해야 하는 IAM 개체의 권한 정책에 다음 명령문을 추가합니다.

```
{
    "Effect": "Allow",
    "Action": [
        "iam:UpdateRoleDescription"
    ],
    "Resource": "arn:aws:iam::*:role/aws-service-role/auditmanager.amazonaws.com/
AWSServiceRoleForAuditManager*",
    "Condition": {"StringLike": {"iam:AWSServiceName": "auditmanager.amazonaws.com"}}
}
```

서비스 연결 역할 삭제 AWS Audit Manager

Audit Manager을 더 이상 사용하지 않을 경우에는 `AWSServiceRoleForAuditManager` 서비스 연결 역할을 삭제하는 것이 좋습니다. 따라서 적극적으로 모니터링하거나 유지하지 않는 미사용 엔티티가 없도록 합니다. 단, 삭제 전에 서비스 연결 역할을 반드시 정리해야 합니다.

서비스 연결 역할 정리

IAM을 사용하여 Audit Manager 서비스 연결 역할을 삭제하기 전에 먼저 역할에 활성 세션이 없는지 확인하고 역할에서 사용되는 리소스를 모두 제거해야 합니다. 이렇게 하려면 Audit Manager가 모두

AWS 리전등록 취소되었는지 확인하십시오. 등록을 취소하면 Audit Manager는 더 이상 서비스 연결 역할을 사용하지 않습니다.

Audit Manager 등록 취소 방법에 대한 지침은 다음 리소스를 참조하세요.

- 이 가이드의 AWS Audit Manager 비활성화
- AWS Audit Manager API 참조의 DeregisterAccount
- 참조 양식에서 계정 등록을 취소하십시오.AWS CLI AWS Audit Manager

Audit Manager 리소스를 수동으로 삭제하는 방법에 대한 지침은 이 가이드의 Audit Manager 데이터 삭제를 참조하십시오.

서비스 연결 역할 삭제

IAM 콘솔, AWS Command Line Interface (AWS CLI) 또는 IAM API를 사용하여 서비스 연결 역할을 삭제할 수 있습니다.

IAM console

IAM 콘솔에서 서비스 연결 역할을 삭제하려면 다음 단계를 따릅니다.

서비스 연결 역할을 삭제하는 방법(콘솔)

1. AWS Management Console 로그인하고 https://console.aws.amazon.com/iam/ 에서 IAM 콘솔을 엽니다.
2. IAM 콘솔의 탐색 창에서 역할을 선택합니다. 이름이나 행 자체가 아닌 `AWSServiceRoleForAuditManager` 옆의 확인란을 선택합니다.
3. 페이지 상단의 역할 작업에서 삭제를 선택합니다.
4. 확인 대화 상자가 나타나면 마지막으로 액세스한 정보를 검토합니다. 이 정보는 선택한 각 역할이 AWS 서비스를 마지막으로 액세스한 일시를 보여줍니다. 이를 통해 역할이 현재 활동 중인지를 확인할 수 있습니다. 계속 진행하려면 텍스트 입력 필드에 **`AWSServiceRoleForAuditManager`**를 입력하고 삭제를 선택하여 삭제할 서비스 연결 역할을 제출합니다.
5. IAM 콘솔 알림을 보고 서비스 연결 역할 삭제 진행 상황을 모니터링합니다. IAM 서비스 연결 역할 삭제는 비동기이므로 삭제할 역할을 제출한 후에 삭제 태스크가 성공하거나 실패할 수 있습니다. 태스크에 성공하면 목록에서 역할이 제거되고 성공 메시지가 페이지 상단에 나타납니다.

AWS CLI

에서 IAM 명령을 사용하여 서비스 연결 역할을 AWS CLI 삭제할 수 있습니다.

서비스 연결 역할을 삭제하려면(AWS CLI)

1. 다음 명령을 입력하여 계정의 역할을 나열합니다.

```
aws iam get-role --role-name AWSServiceRoleForAuditManager
```

2. 서비스 연결 역할이 사용되거나 연결된 리소스가 있는 경우에는 서비스 연결 역할을 삭제할 수 없으므로 삭제 요청을 제출해야 합니다. 이러한 조건이 충족되지 않으면 요청이 거부될 수 있습니다. 삭제 태스크 상태를 확인하려면 응답의 `deletion-task-id`(을)를 캡처해야 합니다.

   다음 명령을 입력하여 서비스 연결 역할 삭제 요청을 제출합니다.

```
aws iam delete-service-linked-role --role-name AWSServiceRoleForAuditManager
```

3. 다음 명령을 사용하여 삭제 태스크의 상태를 확인합니다.

```
aws iam get-service-linked-role-deletion-status --deletion-task-id deletion-task-id
```

   삭제 태스크는 `NOT_STARTED`, `IN_PROGRESS`, `SUCCEEDED` 또는 `FAILED` 상태일 수 있습니다. 삭제에 실패할 경우 문제를 해결할 수 있도록 실패 이유가 호출에 반환됩니다.

IAM API

IAM API를 사용하여 서비스 연결 역할을 삭제할 수 있습니다.

서비스 연결 역할(API)을 삭제하는 방법

1. GetRole를 호출하여 계정의 역할을 나열하십시오. 요청에서 `AWSServiceRoleForAuditManager`를 `RoleName`로 지정합니다.
2. 서비스 연결 역할이 사용되거나 연결된 리소스가 있는 경우에는 서비스 연결 역할을 삭제할 수 없으므로 삭제 요청을 제출해야 합니다. 이러한 조건이 충족되지 않으면 요청이 거부될 수 있습니다. 삭제 태스크 상태를 확인하려면 응답의 `DeletionTaskId`(을)를 캡처해야 합니다.

   서비스 연결 역할 삭제 요청을 제출하려면 DeleteServiceLinkedRole을 호출합니다. 요청에서 `AWSServiceRoleForAuditManager`를 `RoleName`로 지정합니다.

3. 삭제 상태를 확인하려면 GetServiceLinkedRoleDeletionStatus을 호출합니다. 요청에 `DeletionTaskId`(을)를 지정합니다.

   삭제 태스크는 `NOT_STARTED`, `IN_PROGRESS`, `SUCCEEDED` 또는 `FAILED` 상태일 수 있습니다. 삭제에 실패할 경우 문제를 해결할 수 있도록 실패 이유가 호출에 반환됩니다.

> **Tip**
>
> Audit Manager 서비스에서 역할을 사용 중이거나 연결된 리소스가 있는 경우 삭제에 실패합니다. 이는 아직 Audit Manager에 하나 이상 AWS 리전에서 여전히 등록되어 있는 경우에만 발생합니다. 등록을 취소하면 Audit Manager는 서비스 연결 역할 사용을 중지합니다.
> 삭제 실패 문제를 해결하려면 먼저 서비스를 사용한 모든 AWS 리전 곳에서 Audit Manager의 등록을 취소해야 합니다. 이전 절차의 단계에 따라 다시 시도합니다.

AWS Audit Manager 서비스 연결 역할이 지원되는 지역

AWS Audit Manager 서비스가 제공되는 모든 지역에서 서비스 연결 역할을 사용할 수 AWS 리전 있습니다. 자세한 내용은 AWS 서비스 엔드포인트를 참조하세요.

규정 준수 검증: AWS Audit Manager

특정 규정 준수 프로그램의 범위 내에 AWS 서비스 있는지 알아보려면AWS 서비스 규정 준수 프로그램의AWS 서비스 범위별, 규정 참조하여 관심 있는 규정 준수 프로그램을 선택하십시오. 일반 정보는 AWS 규정 준수 프로그램AWS 보증 프로그램 규정AWS 참조하십시오.

를 사용하여 AWS Artifact타사 감사 보고서를 다운로드할 수 있습니다. 자세한 내용은 의 보고서 https://docs.aws.amazon.com/artifact/latest/ug/downloading-documents.html 참조하십시오 AWS Artifact.

사용 시 규정 준수 AWS 서비스 책임은 데이터의 민감도, 회사의 규정 준수 목표, 관련 법률 및 규정에 따라 결정됩니다. AWS 규정 준수에 도움이 되는 다음 리소스를 제공합니다.

- 보안 및 규정 준수 퀵 스타트 가이드 - 이 배포 가이드에서는 아키텍처 고려 사항을 설명하고 보안 및 규정 준수에 AWS 중점을 둔 기본 환경을 배포하기 위한 단계를 제공합니다.
- Amazon Web Services의 HIPAA 보안 및 규정 준수를 위한 설계 — 이 백서에서는 기업이 HIPAA 적격 애플리케이션을 만드는 AWS 데 사용할 수 있는 방법을 설명합니다.

> **Note**
>
> 모든 AWS 서비스 사람이 HIPAA 자격을 갖춘 것은 아닙니다. 자세한 내용은 HIPAA 적격 서비스 참조를 참조하십시오.

- AWS 규정 준수 리소스AWS — 이 워크북 및 가이드 모음은 해당 산업 및 지역에 적용될 수 있습니다.
- AWS 고객 규정 준수 가이드 — 규정 준수의 관점에서 공동 책임 모델을 이해하십시오. 이 가이드에서는 보안을 유지하기 위한 모범 사례를 AWS 서비스 요약하고 여러 프레임워크 (미국 표준 기술 연구소 (NIST), 결제 카드 산업 보안 표준 위원회 (PCI), 국제 표준화기구 (ISO) 등) 에서 보안 제어에 대한 지침을 매핑합니다.
- 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— 이를 AWS 서비스 통해 내부 AWS보안 상태를 포괄적으로 파악할 수 있습니다. Security Hub는 보안 통제를 사용하여 AWS 리소스를 평가하고 보안 업계 표준 및 모범 사례에 대한 규정 준수를 확인합니다. 지원되는 서비스 및 제어 목록은 Security Hub 제어 참조를 참조하십시오.
- AWS Audit Manager— 이를 AWS 서비스 통해 AWS 사용량을 지속적으로 감사하여 위험을 관리하고 규정 및 업계 표준을 준수하는 방법을 단순화할 수 있습니다.

의 레질리언스 AWS Audit Manager

AWS 글로벌 인프라는 AWS 지역 및 가용 영역을 중심으로 구축됩니다. AWS 지역은 물리적으로 분리되고 격리된 여러 가용 영역을 제공하며, 이러한 가용 영역은 지연 시간이 짧고 처리량이 높으며 중복성이 높은 네트워킹으로 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 지역 및 가용 영역에 대한 자세한 내용은 글로벌 인프라를 참조하십시오AWS .

의 인프라 보안 AWS Audit Manager

관리형 서비스인 AWS Audit Manager는 AWS 글로벌 네트워크 보안의 보호를 받습니다. AWS 보안 서비스 및 인프라 AWS 보호 방법에 대한 자세한 내용은 AWS 클라우드 보안을 참조하십시오. 인프라 보

안 모범 사례를 사용하여 AWS 환경을 설계하려면 Security Pillar AWS Well-Architected Framework의 인프라 보호를 참조하십시오.

AWS 게시된 API 호출을 사용하여 네트워크를 통해 AWS Audit Manager에 액세스할 수 있습니다. 고객은 다음을 지원해야 합니다.

- 전송 계층 보안(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 주체와 관련된 비밀 액세스 키를 사용하여 서명해야 합니다. 또는 AWS Security Token Service(AWS STS)을 사용하여 임시 보안 자격 증명을 생성하여 요청에 서명할 수 있습니다.

모든 네트워크 위치에서 이러한 API 작업을 호출할 수 있지만 AWS Audit Manager 소스 IP 주소에 따른 제한을 포함할 수 있는 리소스 기반 액세스 정책을 지원합니다. Audit Manager 정책을 사용하여 특정 Amazon Virtual Private Cloud(Amazon VPC) 엔드포인트 또는 특정 VPC에서 액세스를 제어할 수도 있습니다. 이를 통해 네트워크 내의 AWS 특정 VPC로부터 지정된 Audit Manager 리소스에 대한 네트워크 액세스를 효과적으로 분리할 수 있습니다.

AWS Audit Manager 및 인터페이스 VPC 엔드포인트 ()AWS PrivateLink

인터페이스 VPC 엔드포인트를 AWS Audit Manager 생성하여 VPC 간에 프라이빗 연결을 설정할 수 있습니다. 인터페이스 엔드포인트는 인터넷 게이트웨이, NAT 디바이스, VPN 연결 또는 AWS Direct Connect 연결 없이 비공개로 Audit Manager API에 액세스할 수 있도록 지원하는 AWS PrivateLink 기술로 구동됩니다. VPC의 인스턴스는 Audit Manager API와 통신하는 데 퍼블릭 IP 주소를 필요로 하지 않습니다. VPC와 VPC 사이의 트래픽은 네트워크를 벗어나지 AWS Audit Manager 않습니다. AWS

각 인터페이스 엔드포인트는 서브넷에서 하나 이상의 탄력적 네트워크 인터페이스로 표현됩니다.

자세한 내용은 Amazon VPC 사용 설명서의 인터페이스 VPC 엔드포인트(AWS PrivateLink)를 참조하세요.

AWS Audit Manager VPC 엔드포인트 고려 사항

에 대한 AWS Audit Manager인터페이스 VPC 엔드포인트를 설정하기 전에 Amazon VPC 사용 설명서의 인터페이스 엔드포인트 속성 및 제한을 검토하십시오.

AWS Audit Manager VPC에서 모든 API 작업에 대한 호출을 지원합니다.

AWS Audit Manager에 대한 인터페이스 VPC 엔드포인트 생성

Amazon VPC 콘솔 또는 () 를 사용하여 AWS Audit Manager 서비스에 대한 VPC 엔드포인트를 생성할 수 있습니다. AWS Command Line Interface AWS CLI자세한 내용은 Amazon VPC 사용 설명서의 인터페이스 엔드포인트 생성을 참조하십시오.

다음 서비스 이름을 AWS Audit Manager 사용하기 위한 VPC 엔드포인트를 생성합니다.

- `com.amazonaws.region.auditmanager`

엔드포인트에 대해 프라이빗 DNS를 활성화하면 해당 지역의 기본 DNS 이름 (예:) 을 AWS Audit Manager 사용하도록 API 요청을 할 수 있습니다. `auditmanager.us-east-1.amazonaws.com`

자세한 내용은 Amazon VPC 사용 설명서의 인터페이스 엔드포인트를 통해 서비스 액세스를 참조하십시오.

에 대한 VPC 엔드포인트 정책 생성 AWS Audit Manager

AWS Audit Manager에 대한 액세스를 제어하는 VPC 엔드포인트에 엔드포인트 정책을 연결할 수 있습니다. 이 정책은 다음 정보를 지정합니다.

- 작업을 수행할 수 있는 보안 주체.
- 수행할 수 있는 작업.
- 작업을 수행할 있는 리소스.

자세한 정보는 Amazon VPC 사용 설명서의 VPC 엔드포인트를 통해 서비스에 대한 액세스 제어를 참조하십시오.

예: 작업에 대한 VPC 엔드포인트 정책 AWS Audit Manager

다음은 에 대한 AWS Audit Manager엔드포인트 정책의 예입니다. 이 정책은 엔드포인트에 연결될 때 모든 리소스의 모든 주체에 대한 액세스 권한을 나열된 Audit Manager 작업에 부여합니다.

```
{
   "Statement":[
      {
         "Principal":"*",
         "Effect":"Allow",
         "Action":[
            "auditmanager:GetAssessments",
            "auditmanager:GetServicesInScope",
            "auditmanager:ListNotifications"
         ],
         "Resource":"*"
      }
   ]
}
```

로그인 및 모니터링 AWS Audit Manager

모니터링은 Audit Manager 및 기타 AWS 솔루션의 신뢰성, 가용성 및 성능을 유지하는 데 있어 중요한 부분입니다. AWS 는 Audit Manager를 감시하고, 문제 발생 시 보고하고, 적절한 경우 자동 조치를 취할 수 있는 다음과 같은 모니터링 도구를 제공합니다.

- AWS CloudTrail은 직접 수행하거나 AWS 계정 을 대신하여 수행한 API 직접 호출 및 관련 이벤트를 캡처하고 지정한 Amazon S3 버킷에 로그 파일을 전송합니다. 어떤 사용자 및 계정이 AWS를 호출했는지 어떤 소스 IP 주소에 호출이 이루어졌는지 언제 호출이 발생했는지 확인할 수 있습니다. 자세한 내용은 AWS CloudTrail 사용 설명서를 참조하십시오.
- EventBridgeAmazon은 다양한 소스의 데이터에 애플리케이션을 쉽게 연결할 수 있게 해주는 서버리스 이벤트 버스 서비스입니다. EventBridge 자체 애플리케이션, oftware-as-a S-Service (SaaS) 애플리케이션 AWS 및 서비스에서 실시간 데이터 스트림을 제공하고 해당 데이터를 Lambda와 같은 대상으로 라우팅합니다. 이를 통해 서비스에서 발생하는 이벤트를 모니터링하고 이벤트 기반 아키텍처를 구축할 수 있습니다. 자세한 내용은 Amazon EventBridge 사용 설명서를 참조하십시오.

AWS Audit Manager 아마존을 통한 모니터링 EventBridge

EventBridge Amazon은 애플리케이션 가용성 문제 또는 리소스 AWS 서비스 변경과 같은 시스템 이벤트를 자동화하고 이에 자동으로 대응할 수 있도록 지원합니다.

EventBridge규칙을 사용하여 Audit Manager 이벤트를 탐지하고 이에 대응할 수 있습니다. 생성한 규칙에 따라 이벤트가 규칙에 지정한 값과 일치할 때 하나 이상의 대상 작업을 EventBridge 호출합니다. 이

벤트 유형에 따라 알림을 보내거나, 이벤트 정보를 캡처하거나, 교정 작업을 수행하거나, 이벤트를 시작하거나, 기타 작업을 수행할 수 있습니다.

예를 들어 계정에서 다음 Audit Manager 이벤트가 발생할 때마다 감지할 수 있습니다.

- 감사 소유자가 평가를 생성, 업데이트 또는 삭제합니다.
- 감사 소유자가 검토를 위해 통제 세트를 위임합니다.
- 대리인은 검토를 완료하고 검토된 통제 세트를 감사 소유자에게 다시 제출합니다.
- 감사 소유자가 평가 통제 상태를 업데이트합니다.

자동으로 트리거할 수 있는 태스크는 다음과 같습니다.

- AWS Lambda 함수를 사용하여 Slack 채널에 알림을 전달하세요.
- 검사에 대한 데이터를 Amazon Kinesis Data Streams으로 푸시하여 포괄적인 실시간 상태 모니터링을 지원합니다.
- Amazon Simple Notification Service(Amazon SNS) 주제를 이메일로 보냅니다.
- Amazon CloudWatch 알람 조치로 알림을 받으세요.

> **Note**
>
> Audit Manager는 지속적으로 이벤트를 제공합니다. 즉, Audit Manager는 EventBridge 적어도 한 번은 이벤트 전송을 성공적으로 시도할 것입니다. EventBridge 서비스 중단으로 인해 이벤트를 전달할 수 없는 경우 Audit Manager는 나중에 최대 24시간 동안 이벤트를 다시 시도합니다.

EventBridge Audit Manager의 예제 형식

다음 JSON 코드는 Audit Manager에서의 평가 생성 이벤트의 예를 보여줍니다. 이 이벤트의 필드에 대한 자세한 내용은 이벤트 구조 참조를 참조하십시오.

```
{
    "version": "0",
    "id": "55c5a6f3-6183-3989-49ec-a3c998857644",
    "detail-type": "Assessment Created",
    "source": "aws.auditmanager",
    "account": "111122223333",
```

```
    "time": "2023-07-27T00:38:33Z",
    "region": "us-west-2",
    "resources":
        [
            "arn:aws:auditmanager:us-west-2:111122223333:assessment/a1b2c3d4-e5f6-g7h8-
i9j0-k1l2m3n4o5p6"
        ],
    "detail":
    {
        "eventID": "4e939b2f-9429-3141-beec-d640d83ef68e",
        "author": "arn:aws:sts::111122223333:assumed-role/roleName/role-session-name",
        "assessmentTenantId": "111122223333",
        "assessmentName": "myAssessment",
        "eventTime": 1690418289068,
        "eventName": "CREATE",
        "eventType": "ASSESSMENT",
        "assessmentID": "a1b2c3d4-e5f6-g7h8-i9j0-k1l2m3n4o5p6"
    }
}
```


규칙 생성을 위한 사전 요구 사항 EventBridge

Audit Manager 규칙을 생성하기 전에 다음을 수행하는 것이 좋습니다.

- 에서 이벤트, 규칙, 대상을 숙지하세요. EventBridge 자세한 내용은 Amazon이란 무엇입니까 EventBridge? 를 참조하십시오. Amazon EventBridge 사용 설명서에서 확인할 수 있습니다.
- 이벤트 규칙에 사용할 대상을 만듭니다. 예를 들어 제어 세트 검토가 완료될 때마다 문자 메시지 또는 이메일을 수신하도록 Amazon SNS 주제를 만들 수 있습니다. 자세한 내용은 EventBridge 대상을 참조하십시오.

Audit Manager를 위한 EventBridge 규칙 생성

다음 단계에 따라 Audit Manager에서 내보낸 이벤트를 트리거하는 EventBridge 규칙을 만드십시오. 이벤트는 최선의 작업을 기반으로 발생됩니다.

Audit Manager에 대한 EventBridge 규칙을 만들려면

1. https://console.aws.amazon.com/events/ 에서 아마존 EventBridge 콘솔을 엽니다.
2. 탐색 창에서 규칙을 선택합니다.
3. 규칙 생성을 선택합니다.

4. 규칙 세부 정보 정의 페이지에서 규칙의 이름과 설명을 입력합니다.
5. 이벤트 버스(Event bus)와 규칙 유형(Rule type)의 기본값을 유지하고 다음(Next)을 선택합니다.
6. 이벤트 패턴 빌드 페이지에서 이벤트 소스로 이벤트 또는 EventBridge 파트너AWS 이벤트를 선택합니다.
7. 생성 방법에서 사용자 지정 패턴(JSON 편집기)을 선택합니다.
8. 이벤트 패턴에서 JSON으로 이벤트 패턴을 작성하고 매칭에 사용려는 필드를 지정합니다.

   Audit Manager 이벤트와 일치시키려면 다음과 같은 간단한 패턴을 사용할 수 있습니다.

   ```
   {
     "detail-type": ["Event"]
   }
   ```

   ###를 지원되는 다음 값 중 하나로 바꾸십시오.

   a. 평가가 생성될 때 알림을 받으려면 `Assessment Created`을 입력하십시오.
   b. 평가가 업데이트될 때 알림을 받으려면 `Assessment Updated`을 입력합니다.
   c. 평가가 삭제될 때 알림을 받으려면 `Assessment Deleted`을 입력합니다.
   d. 제어 집합이 검토를 위임받았을 때 알림을 받으려면 `Assessment ControlSet Delegation Created`을 입력합니다.
   e. 평가 통제 세트를 검토할 때 알림을 받으려면 `Assessment ControlSet Reviewed`을 입력합니다.
   f. 평가 통제가 검토될 때 알림을 받으려면 `Assessment Control Reviewed`을 입력하십시오.

   > **Tip**
   >
   > 필요에 따라 이벤트 패턴에 필드를 더 추가하세요. 사용 가능한 필드에 대한 자세한 내용은 Amazon EventBridge 이벤트 패턴을 참조하십시오.

9. 다음을 선택합니다.
10. 대상 선택 페이지에서 이 규칙에 대해 만든 대상을 선택한 후 해당 유형에 필요한 모든 추가 옵션을 구성합니다. 예를 들어 Amazon SNS를 선택하는 경우 이메일이나 SMS를 통해 알림을 받을 수 있도록 SNS 주제가 올바르게 구성되어 있는지 확인합니다.

> **Tip**
>
> 표시되는 필드는 선택한 서비스에 따라 달라집니다. 사용 가능한 대상에 대한 자세한 내용은 EventBridge 콘솔에서 사용할 수 있는 대상을 참조하십시오.

11. 많은 대상 유형의 경우 대상에 이벤트를 전송할 수 있는 권한이 EventBridge 필요합니다. 이러한 경우 규칙을 실행하는 데 필요한 IAM 역할을 생성할 EventBridge 수 있습니다.

    a. IAM 역할을 자동으로 생성하려면 이 특정 리소스에 대해 새 역할 생성을 선택합니다.

    b. 이전에 생성한 IAM 역할을 사용하려면 기존 역할 사용(Use existing role)을 선택합니다.

12. (선택 사항) 이 규칙에 다른 대상을 추가하려면 Add another target(다른 대상 추가)을 선택합니다.
13. 다음을 선택합니다.
14. (선택 사항) 태그 구성(Configure tags) 페이지에서 태그를 추가하고 다음(Next)을 선택합니다.
15. 검토 및 생성(Review and create) 페이지에서 규칙 설정을 검토하여 이벤트 모니터링 요구 사항을 충족하는지 확인합니다.
16. 규칙 생성을 선택합니다. 이제 규칙이 Audit Manager 이벤트를 모니터링한 다음 지정한 대상에 이벤트를 보냅니다.

를 AWS Audit Manager 사용하여 API 호출을 로깅합니다. CloudTrail

Audit Manager는 Audit AWS 서비스 Manager에서 사용자, 역할 또는 담당자가 수행한 작업에 대한 기록을 제공하는 서비스와 통합되어 있습니다. CloudTrail CloudTrail Audit Manager에 대한 모든 API 호출을 이벤트로 캡처합니다. 캡처되는 호출에는 Audit Manager 콘솔에서 수행한 호출과 Audit Manager API 작업에 대한 코드 호출이 포함됩니다.

추적을 생성하면 Audit Manager에 대한 CloudTrail 이벤트를 포함하여 Amazon S3 버킷으로 이벤트를 지속적으로 전송할 수 있습니다. 트레일을 구성하지 않아도 CloudTrail 콘솔의 이벤트 기록에서 가장 최근 이벤트를 계속 볼 수 있습니다.

에서 수집한 CloudTrail 정보를 사용하여 Audit Manager에 이루어진 요청, 요청이 이루어진 IP 주소, 요청한 사람, 요청 시기 및 추가 세부 정보를 확인할 수 있습니다.

자세한 CloudTrail 내용은 AWS CloudTrail 사용 설명서를 참조하십시오.

Audit Manager 정보: CloudTrail

CloudTrail 계정을 만들 AWS 계정 때 활성화됩니다. Audit Manager에서 활동이 발생하면 해당 활동이 CloudTrail 이벤트 기록의 다른 AWS 서비스 이벤트와 함께 이벤트에 기록됩니다.

내 페이지에서 최근 이벤트를 보고, 검색하고, 다운로드할 수 있습니다 AWS 계정. 자세한 내용은 CloudTrail 이벤트 기록에서 이벤트 보기를 참조하세요.

Audit Manager의 이벤트를 AWS 계정포함하여 귀하의 이벤트에 대한 지속적인 기록을 보려면 트레일을 생성하십시오. 트레일을 사용하면 CloudTrail Amazon S3 버킷으로 로그 파일을 전송할 수 있습니다. 콘솔에서 추적을 생성하면 기본적으로 모든 AWS 리전에 추적이 적용됩니다. 트레일은 AWS 파티션에 있는 모든 지역의 이벤트를 기록하고 지정한 Amazon S3 버킷으로 로그 파일을 전송합니다.

또한 CloudTrail 로그에서 수집된 이벤트 데이터를 추가로 분석하고 이에 따라 조치를 AWS 서비스 취하도록 기타를 구성할 수 있습니다. 자세한 내용은 다음 자료를 참조하십시오.

- 추적 생성 개요
- CloudTrail 지원되는 서비스 및 통합
- 에 대한 Amazon SNS 알림 구성 CloudTrail
- 여러 지역에서 CloudTrail 로그 파일 수신 및 여러 계정으로부터 CloudTrail 로그 파일 수신

모든 Audit Manager 작업은 AWS Audit Manager API 참조에 의해 CloudTrail 기록되고 문서화됩니다. 예를 들어,`CreateCustomControl`, `DeleteControl` 및 `UpdateAssessmentTemplate` API 작업에 대한 호출은 CloudTrail 로그 파일에 항목을 생성합니다.

모든 이벤트 및 로그 항목에는 요청을 생성한 사용자에 대한 정보가 들어 있습니다. 보안 인증 정보를 이용하면 다음을 쉽게 판단할 수 있습니다.

- 요청을 루트 사용자 자격 증명으로 했는지 여부
- 역할 또는 페더레이션 사용자에 대한 임시 보안 보안 인증을 사용하여 요청이 생성되었는지 여부.
- 다른 AWS 서비스에서 요청했는지 여부.

자세한 내용은 CloudTrail userIdentity 요소를 참조하세요.

Audit Manager 로그 파일 항목 이해

트레일은 지정한 Amazon S3 버킷에 이벤트를 로그 파일로 전송할 수 있는 구성입니다. CloudTrail 로그 파일은 하나 이상의 로그 항목을 포함합니다. 이벤트는 모든 소스의 단일 요청을 나타내며 요청된

작업, 작업 날짜 및 시간, 요청 매개 변수 등에 대한 정보를 포함합니다. CloudTrail 로그 파일은 공개 API 호출의 정렬된 스택 트레이스가 아니므로 특정 순서로 표시되지 않습니다.

다음 예제는 CreateAssessment작업을 보여주는 CloudTrail 로그 항목을 보여줍니다.

```
{
      eventVersion:"1.05",
      userIdentity:{
        type:"IAMUser",
        principalId:"principalId",
        arn:"arn:aws:iam::accountId:user/userName",
        accountId:"111122223333",
        accessKeyId:"accessKeyId",
        userName:"userName",
        sessionContext:{
          sessionIssuer:{
          },
          webIdFederationData:{
          },
          attributes:{
            mfaAuthenticated:"false",
            creationDate:"2020-11-19T07:32:06Z"
          }
        }
      },
      eventTime:"2020-11-19T07:32:36Z",
      eventSource:"auditmanager.amazonaws.com",
      eventName:"CreateAssessment",
      awsRegion:"us-west-2",
      sourceIPAddress:"sourceIPAddress",
      userAgent:"Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36
 (KHTML, like Gecko) Chrome/87.0.4280.66 Safari/537.36",
      requestParameters:{
        frameworkId:"frameworkId",
        assessmentReportsDestination:{
          destination:"***",
          destinationType:"S3"
        },
        clientToken:"***",
        scope:{
          awsServices:[
            {
              serviceName:"license-manager"
            }
```

```
          ],
          awsAccounts:"***"
        },
        roles:"***",
        name:"***",
        description:"***",
        tags:"***"
      },
      responseElements:{
        assessment:"***"
      },
      requestID:"0d950f8c-5211-40db-8c37-2ed38ffcc894",
      eventID:"a782029a-959e-4549-81df-9f6596775cb0",
      readOnly:false,
      eventType:"AwsApiCall",
      recipientAccountId:"recipientAccountId"
    }
```

의 구성 및 취약성 분석 AWS Audit Manager

구성 및 IT 제어는 고객과 고객 간의 AWS 공동 책임입니다. 자세한 내용은 AWS 공동 책임 모델을 참조하십시오.

AWS Audit Manager 리소스에 태그 지정

태그는 사용자 또는 AWS가 AWS 리소스에 할당하는 메타데이터 레이블입니다. 각 태그는 키와 값으로 구성됩니다. 사용자가 할당하는 태그에 대해 키와 값을 정의합니다. 예를 들어 키를 `stage`로 정의하고 리소스 하나의 값을 `test`로 정의할 수 있습니다.

태그는 다음을 지원합니다.

- Audit Manager 리소스를 쉽게 찾아보세요. 프레임워크 라이브러리와 컨트롤 라이브러리를 탐색할 때 태그를 검색 기준으로 사용할 수 있습니다.
- 리소스를 규정 준수 유형과 연결할 수 있습니다. 여러 리소스에 규정 준수 관련 태그를 지정하여 해당 리소스를 특정 프레임워크에 연결할 수 있습니다.
- AWS 리소스를 식별하고 정리합니다. 많은 AWS 서비스가 태그 지정을 지원하므로 다른 서비스의 리소스에 동일한 태그를 할당하여 해당 리소스의 관련 여부를 나타낼 수 있습니다.
- AWS 비용을 추적합니다. AWS Billing and Cost Management 대시보드에서 이러한 태그를 활성화합니다. AWS는 태그를 사용하여 비용을 분류하고 월별 비용 할당 보고서를 전달합니다. 자세한 내용은 AWS Billing and Cost Management 사용 설명서의 비용 할당 태그 사용을 참조하세요.

다음 단원에서는 AWS Audit Manager의 태그에 대한 추가 정보를 제공합니다.

Audit Manager에서 지원되는 리소스

다음 Audit Manager 리소스는 태깅을 지원합니다.

- 평가
- 컨트롤
- 프레임워크

태그 제한

Audit Manager 리소스의 태그에는 다음과 같은 기본 제한 사항이 적용됩니다.

- 리소스에 할당할 수 있는 최대 태그 수 - 50개
- 최대 키 길이 - 유니코드 문자 128자
- 최대 값 길이 - 유니코드 문자 256자

- 키 및 값에 사용할 수 있는 문자 - a-z, A-Z, 0-9, 공백 및 _ . : / = + - @ 문자
- 키와 값은 대/소문자를 구분합니다
- 키 접두사로 `aws:`를 사용하지 마세요. AWS 전용입니다.

태그 관리

평가, 프레임워크 또는 컨트롤을 생성할 때 태그를 속성으로 설정할 수 있습니다. Audit Manager 콘솔, AWS Command Line Interface (AWS CLI) 및 Audit Manager API를 통해 태그를 추가, 편집 및 삭제할 수 있습니다. 자세한 내용은 다음 링크를 참조하십시오.

- 평가의 경우:
  - 이 가이드 평가 섹션의 평가 생성 및 평가 편집
  - 이 가이드 평가 검토 섹션의 태그 탭
  - AWS Audit Manager API 참조의 CreateAssessment 및 UpdateAssessment
  - AWS Audit Manager API 참조의 TagResource 및 UntagResource
- 프레임워크의 경우:
  - 이 가이드 프레임워크 라이브러리 섹션의 사용자 지정 프레임워크 만들기 및 사용자 지정 프레임워크 편집
  - 이 가이드 프레임워크 세부 정보 보기 섹션의 태그 탭
  - AWS Audit Manager API 참조의 CreateAssessmentFramework 및 UpdateAssessmentFramework
  - AWS Audit Manager API 참조의 TagResource 및 UntagResource
- 컨트롤의 경우:
  - 이 가이드 컨트롤 라이브러리 섹션의 사용자 지정 컨트롤 생성 및 사용자 지정 컨트롤 편집
  - 이 가이드 컨트롤 세부 정보 보기 섹션의 태그 탭
  - AWS Audit Manager API 참조의 CreateControl 및 UpdateControl
  - AWS Audit Manager API 참조의 TagResource 및 UntagResource

AWS CloudFormation을 사용하여 AWS Audit Manager 리소스 생성

AWS Audit Manager는 리소스 및 인프라를 생성하고 관리하는 데 소요되는 시간을 줄일 수 있도록 AWS 리소스를 모델링하고 설정하는 데 도움이 되는 서비스인 AWS CloudFormation과 통합됩니다. 필요한 모든 AWS 리소스(예: 평가)를 설명하는 템플릿을 생성하면 AWS CloudFormation에서 이러한 리소스를 프로비저닝하고 구성합니다.

AWS CloudFormation을 사용할 때 템플릿을 재사용하여 Audit Manager 리소스를 일관되고 반복적으로 설정할 수 있습니다. 리소스를 한 번 설명한 후 여러 AWS 계정 및 리전에서 동일한 리소스를 반복적으로 프로비저닝할 수 있습니다.

Audit Manager 및 AWS CloudFormation 템플릿

Audit Manager 및 관련 서비스에 대한 리소스를 프로비저닝하고 구성하려면 AWS CloudFormation 템플릿을 이해해야 합니다. 템플릿은 JSON 또는 YAML로 서식 지정된 텍스트 파일입니다. 이 템플릿은 AWS CloudFormation 스택에서 프로비저닝할 리소스에 대해 설명합니다. JSON 또는 YAML에 익숙하지 않은 경우 AWS CloudFormation Designer를 사용하면 AWS CloudFormation 템플릿을 시작하는 데 도움이 됩니다. 자세한 내용은 AWS CloudFormation 사용 설명서에서 AWS CloudFormation Designer이란 무엇입니까?를 참조하세요.

Audit Manager는 AWS CloudFormation에서 평가 생성을 지원합니다. 평가에 대한 JSON 및 YAML 템플릿의 예제를 비롯한 자세한 내용은 AWS CloudFormation 사용 설명서의 AWS Audit Manager 리소스 유형 참조를 참조하세요.

AWS CloudFormation에 대해 자세히 알아보기

AWS CloudFormation에 대한 자세한 내용은 다음 리소스를 참조하세요.

- AWS CloudFormation
- AWS CloudFormation 사용 설명서
- AWS CloudFormation API 참조
- AWS CloudFormation 명령줄 인터페이스 사용 설명서

AWS Audit Manager 사용 설명서에 대한 문서 기록

다음 표는 2020년 12월 8일 및 이후 AWS Audit Manager 사용 설명서의 각 릴리스에서 변경된 중요 사항에 대해 설명합니다.

변경 사항	설명	날짜
지원되는 새 프레임워크: PCI DSS V4.0	이제 사전 구축된 새 프레임워크를 AWS Audit Manager에서 사용할 수 있습니다. 자세한 내용은 PCI DSS V4.0을 참조하세요.	2023년 12월 19일
추가 AWS API 호출 지원	이제 Audit Manager에서 추가 AWS API 직접 호출을 사용자 지정 제어에 대한 데이터 소스로 사용할 수 있습니다. 자세한 내용은 사용자 지정 컨트롤 데이터 소스에 대한 지원되는 API 호출을 참조하세요.	2023년 12월 7일
AWS 관리형 정책이 업데이트됨	AWS Audit Manager에서 AWSAuditManagerServiceRolePolicy를 업데이트했습니다. 자세한 내용은 AWS Audit Manager에 대한 AWS 관리형 정책을 참조하세요.	2023년 12월 6일
AWS Security Hub 통합 컨트롤 조사 결과에 대한 지원	Audit Manager는 이제 AWS Security Hub에서 통합 컨트롤을 지원합니다. 자세한 내용은 AWS Audit Manager에서 지원하는 AWS Security Hub 컨트롤을 참조하세요.	2023년 11월 16일
MetricStream과의 통합	이제 Audit Manager에서 MetricStream으로 증거를 수	2023년 11월 14일

	집할 수 있습니다. 자세한 내용은 서드 파티 GRC 제품과의 통합을 참조하세요.	
새로 지원되는 프레임워크: AWS 생성형 AI 모범 사례	이제 사전 구축된 새 프레임워크를 AWS Audit Manager에서 사용할 수 있습니다. 자세한 내용은 AWS 생성형 AI 모범 사례 프레임워크 v1을 참조하세요.	2023년 11월 8일
AWS 관리형 정책이 업데이트됨	AWS Audit Manager에서 AWSAuditManagerServiceRolePolicy를 업데이트했습니다. 자세한 내용은 AWS Audit Manager에 대한 AWS 관리형 정책을 참조하세요.	2023년 11월 6일
Amazon EventBridge과 통합	이제 AWS Audit Manager에서 발생하는 이벤트를 모니터링하고 이러한 이벤트를 이벤트 기반 아키텍처의 일부로 사용할 수 있습니다. 자세한 내용을 알아보려면 Amazon EventBridge을 사용하여 AWS Audit Manager 모니터링하기를 참조하세요.	2023년 8월 18일
위험 평가 및 새로운 수동 증거 옵션에 대한 지원	이제 사용자 지정 컨트롤 생성 워크플로를 사용하여 위험 평가를 지원할 수 있습니다. 컨트롤이 이제 위험 평가 질문을 나타낼 수 있으며, 사용자는 수동 증거로서 파일을 업로드하거나 텍스트를 입력하여 답변을 제공할 수 있습니다. 자세한 내용은 사용자 지정 컨트롤 생성 및 수동 증거 추가를 참조하세요.	2023년 6월 12일

CSV 내보내기 지원	이제 증거 찾기 검색 결과를 CSV 형식으로 내보낼 수 있습니다. 자세한 내용은 검색 결과 내보내기를 참조하세요.	2023년 6월 9일
새로 지원되는 프레임워크: 호주 사이버 보안 센터(ACSC) 정보 보안 매뉴얼	이제 사전 구축된 새 프레임워크를 AWS Audit Manager에서 사용할 수 있습니다. 자세한 내용은 호주 사이버 보안 센터(ACSC) 정보 보안 매뉴얼을 참조하세요.	2023년 3월 24일
평가 보고서가 개선됨	Audit Manager 평가 보고서의 형식과 내용을 개선했습니다. 평가 보고서를 탐색하고 이해하는 방법에 대한 자세한 내용은 평가 보고서를 참조하세요.	2023년 3월 23일
페이지 매겨진 API 호출 지원	AWS Audit Manager에서 이제 증거 수집을 위한 데이터 소스로 페이지가 매겨진 API 호출을 지원합니다. 자세한 내용은 페이지가 매겨진 API 호출을 참조하세요.	2023년 3월 8일
새로 지원되는 프레임워크: HIPAA 최종 옴니버스 보안 규칙 2013	이제 사전 구축된 새 프레임워크를 AWS Audit Manager에서 사용할 수 있습니다. 자세한 내용은 HIPAA 최종 옴니버스 보안 규칙 2013을 참조하세요. 차별화 목적을 위해, 기존의 HIPAA 프레임워크(이전에는 프레임워크 라이브러리에서 HIPAA로 명명됨)는 이제 HIPAA 보안 규칙 2003으로 명명되어 있습니다.	2023년 3월 8일

추가 AWS API 호출 지원	이제 Audit Manager에서 추가 9개의 AWS API 호출을 사용자 지정 컨트롤에 대한 데이터 소스로 사용할 수 있습니다. 자세한 내용은 사용자 지정 컨트롤 데이터 소스에 대한 지원되는 API 호출을 참조하세요.	2023년 3월 3일
IAM 모범 사례에 따라 안내서 업데이트됨	IAM 모범 사례에 따라 안내서가 업데이트되었습니다. 자세한 내용은 IAM의 보안 모범 사례를 참조하세요.	2023년 1월 6일
새 데이터 보존 설정	이제 Audit Manager를 비활성화할 때 모든 데이터를 삭제할지 여부를 지정할 수 있습니다. 자세한 내용은 AWS Audit Manager 비활성화 및 Audit Manager 데이터 삭제를 참조하세요.	2023년 1월 6일
증거 찾기 지원	이제 증거 찾기를 사용하여 증거 데이터에 대한 검색 쿼리를 수행할 수 있습니다. 자세한 내용은 증거 찾기를 참조하세요.	2022년 11월 18일
새로 지원되는 프레임워크: 호주 사이버 보안 센터(ACSC) 8가지 필수사항	이제 사전 구축된 새 프레임워크를 AWS Audit Manager에서 사용할 수 있습니다. 자세한 내용은 호주 사이버 보안 센터(ACSC) 8가지 필수사항을 참조하세요.	2022년 8월 24일

AWS 관리형 정책이 업데이트됨	AWS Audit Manager에서 AWSAuditManagerServiceRolePolicy를 업데이트했습니다. 자세한 내용은 AWS Audit Manager에 대한 AWS 관리형 정책을 참조하세요.	2022년 7월 7일
AWS 관리형 정책이 업데이트됨	AWS Audit Manager에서 AWSAuditManagerServiceRolePolicy를 업데이트했습니다. 자세한 내용은 AWS Audit Manager에 대한 AWS 관리형 정책을 참조하세요.	2022년 5월 20일
새로 지원되는 프레임워크: 캐나다 사이버 보안 센터 미디어 클라우드 컨트롤 프로파일	이제 사전 구축된 새 프레임워크를 AWS Audit Manager에서 사용할 수 있습니다. 자세한 내용은 캐나다 사이버 보안 센터 미디어 클라우드 컨트롤 프로파일을 참조하세요.	2022년 5월 6일
AWS 관리형 정책이 업데이트됨	AWS Audit Manager에서 AWSAuditManagerAdministratorAccess를 업데이트했습니다. 자세한 내용은 AWS Audit Manager에 대한 AWS 관리형 정책을 참조하세요.	2022년 4월 29일
추가 AWS Config 관리형 규칙 지원	이제 Audit Manager에서 추가 91개의 AWS Config 관리형 규칙을 사용자 지정 컨트롤에 대한 데이터 소스로 사용할 수 있습니다. 자세한 내용은 AWS Audit Manager을 통해 AWS Config 관리형 규칙 사용하기를 참조하세요.	2022년 4월 27일

AWS Config 사용자 지정 규칙 지원	이제 Audit Manager에서 AWS Config 사용자 지정 규칙을 사용자 지정 컨트롤의 데이터 소스로 사용할 수 있습니다. 자세한 내용은 AWS Audit Manager을 통해 AWS Config 사용자 지정 규칙 사용하기를 참조하세요.	2022년 4월 27일
새로 지원되는 프레임워크: ISO/IEC 27001:2013 부록 A	이제 사전 구축된 새 프레임워크를 AWS Audit Manager에서 사용할 수 있습니다. 자세한 내용은 ISO/IEC 27001:2013 부록 A를 참조하세요.	2022년 4월 7일
AWS 관리형 정책이 업데이트됨	AWS Audit Manager에서 AWSAuditManagerServiceRolePolicy를 업데이트했습니다. 자세한 내용은 AWS Audit Manager에 대한 AWS 관리형 정책을 참조하세요.	2022년 3월 16일
새로 지원되는 프레임워크: CIS Amazon Web Services 재단 벤치마크 v1.4를 위한 CIS 벤치마크	AWS Audit Manager에서 이제 다음과 같이 사전 구축된 두 가지 새로운 프레임워크를 사용할 수 있습니다 -.CIS Amazon Web Services 재단 벤치마크 v1.4를 위한 CIS 벤치마크, 레벨 1 및 CIS Amazon Web Services 재단 벤치마크 v1.4를 위한 CIS 벤치마크, 레벨 1 및 2. 자세한 내용은 CIS AWS Audit Manager 재단 벤치마크 v1.4.0을 위한 CIS 벤치마크를 참조하세요.	2022년 3월 2일

새로 지원되는 프레임워크: CIS 컨트롤 v8 IG1	이제 사전 구축된 새 프레임워크를 AWS Audit Manager에서 사용할 수 있습니다. 자세한 내용은 CIS 컨트롤 v8 IG1을 참조하세요.	2022년 3월 2일
AWS Audit Manager 대시보드	이제 Audit Manager 대시보드를 사용하여 진행 중인 평가를 모니터링하고 규정을 준수하지 않는 증거를 신속하게 식별할 수 있습니다. 자세한 내용은 Audit Manager 대시보드 사용을 참조하세요.	2021년 11월 18일
사용자 지정 프레임워크 공유	이제 사용자 지정 Audit Manager 프레임워크를 다른 AWS 계정와 공유하거나 자신의 계정에 있는 다른 AWS 리전에 복제할 수 있습니다. 자세한 내용은 사용자 지정 프레임워크 공유를 참조하세요.	2021년 10월 22일
AWS Audit Manager 컨트롤의 새로운 예제	이제 컨트롤 예제를 검토하고 Audit Manager가 AWS 환경을 요구 사항에 맞게 만드는 데 어떻게 도움이 되는지 알아볼 수 있습니다. 자세한 내용은 AWS Audit Manager 제어 예제를 참조하세요.	2021년 9월 21일
새로 지원되는 프레임워크: 그램-리치-블라일리 법(GLBA)	이제 사전 구축된 새 프레임워크를 AWS Audit Manager에서 사용할 수 있습니다. 자세한 내용은 그램-리치-블라일리 법(GLBA)을 참조하세요.	2021년 9월 2일

새로운 문제 해결 장	이제 문제 해결 장을 사용할 수 있습니다. 자세한 내용은 AWS Audit Manager에서의 문제 해결을 참조하세요.	2021년 8월 23일
새로운 위임 장 및 자습서	위임 문서를 새 장으로 확장했습니다. 자세한 내용은 AWS Audit Manager에서의 위임을 참조하세요. 또한 AWS Audit Manager에서 처음으로 컨트롤 세트를 검토하고 있는 대리인을 대상으로 하는 새 자습서를 추가했습니다. 자세한 내용은 대리인을 위한 자습서: 컨트롤 세트 검토를 참조하세요.	2021년 6월 25일
새로 지원되는 프레임워크: NIST SP 800-171 개정판 2	이제 사전 구축된 새 프레임워크를 AWS Audit Manager에서 사용할 수 있습니다. 자세한 내용은 NIST SP 800-171 개정판 2를 참조하세요.	2021년 6월 17일
평가 보고서가 개선됨	AWS Audit Manager 평가 보고서의 형식과 내용을 개선했습니다. 새로운 평가 보고서를 탐색하고 이해하는 방법에 대한 자세한 내용은 평가 보고서를 참조하세요.	2021년 6월 8일
새 AWS 관리형 정책 페이지	AWS Audit Manager가 관리형 정책에 대한 변경 내용 추적을 시작했습니다. 자세한 내용은 AWS Audit Manager에 대한 AWS 관리형 정책을 참조하세요.	2021년 5월 6일

새로 지원되는 프레임워크: NIST 사이버 보안 프레임워크 버전 1.1	이제 사전 구축된 새 프레임워크를 AWS Audit Manager에서 사용할 수 있습니다. 자세한 내용은 NIST 사이버 보안 프레임워크 버전 1.1을 참조하세요.	2021년 5월 5일
새로 지원되는 프레임워크: AWS Well-Architected	이제 사전 구축된 새 프레임워크를 AWS Audit Manager에서 사용할 수 있습니다. 자세한 내용은 AWS Well-Architected를 참조하세요.	2021년 5월 5일
새로 지원되는 프레임워크: AWS 기본 보안 모범 사례	이제 사전 구축된 새 프레임워크를 AWS Audit Manager에서 사용할 수 있습니다. 자세한 내용은 AWS 기본 보안 모범 사례를 참조하세요.	2021년 5월 5일
새로 지원되는 프레임워크: GxP EU 부록 11	이제 사전 구축된 새 프레임워크를 AWS Audit Manager에서 사용할 수 있습니다. 자세한 내용은 GxP EU 부록 11을 참조하세요.	2021년 4월 28일
새로 지원되는 프레임워크: NIST 800-53(개정판 5) 낮음-보통-높음	이제 사전 구축된 새 프레임워크를 AWS Audit Manager에서 사용할 수 있습니다. 자세한 내용은 NIST 800-53(개정판 5) 낮음-보통-높음을 참조하세요.	2021년 3월 25일

새로 지원되는 프레임워크: CIS AWS Audit Manager 재단 벤치마크 v1.3을 위한 CIS 벤치마크	AWS Audit Manager에서 이제 다음과 같이 사전 구축된 두 가지 새로운 프레임워크를 사용할 수 있습니다 -.CIS AWS Audit Manager재단 벤치마크 v1.3.0을 위한 CIS 벤치마크, 레벨 1 및 CIS AWS Audit Manager 재단 벤치마크 v1.3.0을 위한 CIS 벤치마크, 레벨 1 및 2. 자세한 내용은 CIS AWS Audit Manager 재단 벤치마크 v1.3.0을 위한 CIS 벤치마크를 참조하세요.	2021년 3월 22일
최초 릴리스	AWS Audit Manager 사용 설명서 및 API 참조에 대한 최초 릴리스입니다.	2020년 12월 8일

AWS 용어집

최신 AWS 용어는 AWS 용어집 참조서의 AWS 용어집을 참조하세요.

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