aws

관리 설명서

Amazon Detective

Amazon Detective: 관리 설명서

Table of Contents

Amazon Detective란 무엇인가요?

Amazon Detective는 사용자가 보안 조사 결과 또는 의심스러운 활동의 근본 원인을 분석 및 조사하고 신속하게 식별하는 데 도움이 됩니다. Detective는 AWS 리소스에서 로그 데이터를 자동으로 수집합니다. 그런 다음 기계 학습, 통계 분석 및 그래프 이론을 사용하여 더 빠르고 효율적으로 보안 조사를 수행할 수 있도록 시각화를 생성합니다. Detective의 사전 구축된 데이터 집계, 요약 및 컨텍스트는 가능한 보안 문제의 특성과 범위를 신속하게 분석하고 확인하는 데 도움이 됩니다.

Detective를 사용하면 최대 1년 분량의 과거 이벤트 데이터에 액세스할 수 있습니다. 이 데이터는 선택한 기간 동안의 활동 유형 및 양의 변화를 보여주는 일련의 시각화를 통해 제공됩니다. Detective는 이러한 변경 사항을 GuardDuty 조사 결과와 연결합니다. Detective의 소스 데이터에 대한 자세한 내용은 동작 그래프에 사용된 소스 데이터 섹션을 참조하세요.

Detective는 어떻게 작동하나요?

Detective는 AWS CloudTrail 및 Amazon VPC 흐름 로그에서 로그인 시도, API 직접 호출 및 네트워크 트래픽과 같은 시간 기반 이벤트를 자동으로 추출합니다. 또한 GuardDDDDuty에서 탐지한 조사 결과를 수집합니다.

Detective는 이러한 이벤트를 기반으로 기계 학습과 시각화를 사용하여 리소스 동작과 시간 경과에 따른 리소스 동작 간의 상호 작용에 대한 통합된 대화형 보기를 생성합니다. 이 동작 그래프를 탐색하여 실패한 로그인 시도 또는 의심스러운 API 직접 호출과 같은 잠재적으로 악의적인 작업을 검사할 수 있습니다. 또한 이러한 작업이 AWS 계정 및 Amazon EC2 인스턴스와 같은 리소스에 미치는 영향을 확인할 수 있습니다. 다음과 같이 다양한 작업에 맞게 동작 그래프의 범위와 타임라인을 조정할 수 있습니다.

- 규범을 벗어나는 모든 활동을 신속하게 조사합니다.
- 보안 문제를 나타낼 수 있는 패턴을 식별합니다.
- 조사 결과의 영향을 받는 모든 리소스를 이해합니다.

Detective 맞춤형 시각화는 계정 정보의 기준을 제공하고 요약합니다. 이러한 조사 결과는 “이 역할을 위한 비정상적인 API 직접 호출입니까?” 또는 “이 인스턴스에서 트래픽이 급증할 것으로 예상됩니까?”와 같은 질문에 답하는 데 도움이 될 수 있습니다.

Detective를 사용하면 데이터를 구성하거나 자체 쿼리 및 알고리즘을 개발, 구성 또는 조정할 필요가 없습니다. 선결제 비용은 없으며 분석된 이벤트에 대해서만 비용을 지불합니다. 추가 소프트웨어를 배포하거나 구독할 다른 피드는 없습니다.

누가 Detective를 사용하나요?

계정이 Detective를 활성화하면 동작 그래프의 관리자 계정이 됩니다. 동작 그래프는 하나 이상의 AWS 계정에서 추출 및 분석된 데이터를 연결한 집합입니다. 관리자 계정은 멤버 계정을 초대하여 관리자 계정의 동작 그래프에 데이터를 제공합니다.

Detective는 또한 AWS Organizations와 통합되어 있습니다. 조직 관리 계정은 조직의 Detective 관리자 계정을 지정합니다. Detective 관리자 계정을 사용하면 조직 동작 그래프에서 조직 계정을 멤버 계정으로 사용할 수 있습니다.

Detective가 동작 그래프 계정의 소스 데이터를 사용하는 방법에 대한 자세한 내용은 동작 그래프에 사용된 소스 데이터 섹션을 참조하세요.

관리자 계정이 동작 그래프를 관리하는 방법에 대한 자세한 내용은 계정 관리 섹션을 참조하세요. 멤버 계정이 동작 그래프 초대와 멤버십을 관리하는 방법에 대한 자세한 내용은 the section called “멤버 계정의 경우: 초대 및 멤버십 관리” 섹션을 참조하세요.

관리자 계정은 동작 그래프에서 생성된 분석 및 시각화를 사용하여 AWS 리소스 및 GuardDuty 조사 결과를 조사합니다. Detective와 GuardDuty 및 AWS Security Hub의 통합을 사용하면 이러한 서비스에서 GuardDuty 조사 결과를 Detective 콘솔로 직접 피벗할 수 있습니다.

Detective 조사는 관련 AWS 리소스와 관련된 활동에 초점을 맞춥니다. Detective의 조사 프로세스에 대한 개요는 Detective 사용 설명서의 Amazon Detective를 조사에 사용하는 방법을 참조하세요.

Amazon Detective 용어 및 개념

다음은 Amazon Detective 및 해당 작동 방식을 이해하는 데 중요한 용어 및 개념입니다.

관리자 계정

동작 그래프를 소유하고 동작 그래프를 사용하여 조사하는 AWS 계정입니다.

관리자 계정은 멤버 계정을 초대하여 동작 그래프에 해당 데이터를 제공합니다. 자세한 내용은 the section called “동작 그래프에 멤버 계정 초대” 섹션을 참조하세요.

조직 동작 그래프의 경우 관리자 계정은 조직 관리 계정이 지정하는 Detective 관리자 계정입니다. 자세한 내용은 the section called “Detective 관리자 계정 지정” 섹션을 참조하세요. Detective 관리자 계정은 조직 동작 그래프에서 모든 조직 계정을 멤버 계정으로 활성화할 수 있습니다. 자세한 내용은 the section called “조직 멤버 계정 관리” 섹션을 참조하세요.

관리자 계정은 동작 그래프의 데이터 사용량을 확인하고 동작 그래프에서 멤버 계정을 제거할 수도 있습니다.

자율 시스템 조직(ASO)

자율 시스템을 할당받은 직함이 지정 조직입니다. 이 자율 시스템은 유사한 라우팅 로직 및 정책을 사용하는 이기종 네트워크 또는 네트워크 집합입니다.

동작 그래프

하나 이상의 AWS 계정와 연결된 수신 소스 데이터에서 생성된 연결된 데이터 세트입니다.

각 동작 그래프는 동일한 구조의 조사 결과, 엔터티 및 관계를 사용합니다.

위임된 관리자 계정(AWS Organizations)

조직에서 서비스의 위임된 관리자 계정은 조직의 서비스 사용을 관리할 수 있습니다.

Detective에서는 Detective 관리자 계정이 조직 관리 계정이 아닌 한 Detective 관리자 계정도 위임된 관리자 계정입니다. 조직 관리 계정은 위임된 관리자 계정일 수 없습니다.

Detective에서는 자체 위임이 허용됩니다. 조직 관리 계정은 자신의 계정을 Detective의 위임된 관리자로 위임할 수 있지만 이는 Detective의 범위에서만 등록되거나 기억되며 조직은 등록되지 않습니다.

Detective 관리자 계정

조직 관리 계정이 리전의 조직 동작 그래프에 대한 관리자 계정으로 지정한 계정입니다. 자세한 내용은 the section called “Detective 관리자 계정 지정” 섹션을 참조하세요.

Detective는 조직 관리 계정이 자신의 계정이 아닌 다른 계정을 선택할 것을 권장합니다.

계정이 조직 관리 계정이 아닌 경우 Detective 관리자 계정은 Organizations에서 Detective에 대한 위임된 관리자 계정이기도 합니다.

Detective 소스 데이터

다음 유형의 피드에서 처리되고 구조화된 버전의 정보입니다.

- AWS 서비스의 로그(예: AWS CloudTrail 로그 및 Amazon VPC 흐름 로그)
- GuardDuty 조사 결과

Detective는 Detective 소스 데이터를 사용하여 동작 그래프를 채웁니다. 또한 Detective는 해당 분석을 지원하기 위해 Detective 소스 데이터의 사본을 저장합니다.

엔터티

수집된 데이터에서 추출한 항목입니다.

각 엔터티에는 엔터티가 나타내는 객체 유형을 식별하는 유형이 있습니다. 엔터티 유형의 예로는 IP 주소, Amazon EC2 인스턴스, AWS 사용자 등이 있습니다.

엔티티는 관리하는 AWS 리소스이거나 해당 리소스와 상호 작용한 외부 IP 주소일 수 있습니다.

각 엔터티의 소스 데이터는 엔터티 속성을 채우는 데에도 사용됩니다. 속성 값은 소스 레코드에서 직접 추출하거나 여러 레코드에서 집계할 수 있습니다.

결과

Amazon GuardDuty에서 감지한 보안 문제입니다.

조사 결과 그룹

동일한 이벤트 또는 보안 문제와 관련이 있을 수 있는 조사 결과, 엔터티 및 증거 컬렉션입니다. Detective는 내장된 기계 학습 모델을 기반으로 조사 결과 그룹을 생성합니다.

Detective 증거

Detective는 지난 45일 이내에 수집된 동작 그래프의 데이터를 기반으로 조사 결과 그룹과 관련된 추가 증거를 식별합니다. 이 증거는 심각도 값이 정보용인 조사 결과로 제시됩니다. 증거는 조사 결과 그룹 내에서 볼 때 잠재적으로 의심스러울 수 있는 특이한 활동이나 알려지지 않은 동작을 강조

하는 지원 정보를 제공합니다. 조사 결과 범위 시간 내에서 새로 관찰된 지리적 위치 또는 API 직접 호출이 그 예가 될 수 있습니다. 현재 이러한 결과는 Detective에서만 볼 수 있으며 Security Hub로 전송되지 않습니다.

조사 결과 개요

조사 결과에 대한 요약 정보를 제공하는 단일 페이지입니다.

조사 결과 개요에는 조사 결과와 관련된 엔터티 목록이 포함되어 있습니다. 목록에서 엔티티의 프로필로 피벗할 수 있습니다.

조사 결과 개요에는 조사 결과 속성이 포함된 세부 정보 패널도 포함되어 있습니다.

대용량 엔터티

일정 기간 동안 많은 수의 다른 엔터티와 연결되거나 다른 엔터티에서 연결되어 있는 엔터티입니다. 예를 들어, EC2 인스턴스에는 수백만 개의 IP 주소에서의 연결이 있을 수 있습니다. 연결 수가 Detective에서 수용할 수 있는 임계값을 초과합니다.

현재 범위 시간에 대용량 시간 간격이 포함되어 있는 경우 Detective는 사용자에게 알립니다.

자세한 내용은 Amazon Detective 사용 설명서의 대용량 엔터티에 대한 세부 정보 보기를 참조하세요.

조사

의심스럽거나 흥미로운 활동을 분류하고, 범위를 결정하며, 근본 출처 또는 원인을 파악한 다음 진행 방법을 결정하는 프로세스입니다.

멤버 계정

동작 그래프에 데이터를 제공하도록 관리자 계정을 초대하는 AWS 계정입니다. 조직 동작 그래프에서 멤버 계정은 Detective 관리자 계정이 멤버 계정으로 활성화한 조직 계정일 수 있습니다.

초대를 받은 멤버 계정은 동작 그래프 초대에 응답하고 동작 그래프에서 해당 계정을 제거할 수 있습니다. 자세한 내용은 the section called “멤버 계정의 경우: 초대 및 멤버십 관리” 섹션을 참조하세요.

조직 계정은 조직 동작 그래프에서 멤버십을 변경할 수 없습니다.

또한 모든 멤버 계정은 자신이 데이터를 제공하는 동작 그래프에서 해당 계정의 사용 정보를 볼 수 있습니다.

동작 그래프에 다른 접근 권한은 없습니다.

조직 동작 그래프

Detective 관리자 계정이 소유하는 동작 그래프입니다. 조직 관리 계정은 Detective 관리자 계정을 지정합니다. 자세한 내용은 the section called “Detective 관리자 계정 지정” 섹션을 참조하세요.

조직 동작 그래프에서 Detective 관리자 계정은 조직 계정이 멤버 계정인지 여부를 제어합니다. 조직 계정은 조직 동작 그래프에서 자체적으로 제거할 수 없습니다.

Detective 관리자 계정은 조직 동작 그래프에 다른 계정을 초대할 수도 있습니다.

프로필

엔티티의 활동과 관련된 데이터 시각화 컬렉션을 제공하는 단일 페이지입니다.

조사 결과의 경우, 프로필을 통해 분석가는 해당 결과가 진정한 우려인지 아니면 거짓 긍정인지 판단할 수 있습니다.

프로필은 조사 결과에 대한 조사를 지원하거나 의심스러운 활동에 대한 일반적인 추적을 지원하는 정보를 제공합니다.

프로필 패널

프로필에 대한 단일 시각화입니다. 각 프로필 패널은 분석가의 조사에 도움이 되도록 특정 질문이나 질문에 답변하는 데 도움을 주기 위한 것입니다.

프로필 패널에는 키-값 페어, 테이블, 타임라인, 막대형 차트 또는 지리적 위치 차트가 포함될 수 있습니다.

관계

개별 엔터티 간에 발생하는 활동입니다. 관계는 수신되는 소스 데이터에서도 추출됩니다.

엔터티와 마찬가지로 관계에도 유형이 있으며, 이를 통해 관련된 엔터티의 유형과 연결 방향을 식별할 수 있습니다. 관계 유형의 예로는 Amazon EC2 인스턴스에 연결하는 IP 주소가 있습니다.

범위 시간

프로필에 표시되는 데이터의 범위를 지정하는 데 사용되는 기간입니다.

조사 결과의 기본 범위 시간은 의심스러운 활동이 처음 관찰된 시간과 마지막 시간을 반영합니다.

엔터티 프로필의 경우 기본 범위 시간은 이전 24시간입니다.

Amazon Detective 리전 및 할당량

Amazon Detective를 사용할 때는 이러한 할당량을 숙지합니다.

Detective 리전 및 엔드포인트

Detective를 사용할 수 있는 AWS 리전 목록을 보려면 Detective 서비스 엔드포인트를 참조하세요.

Detective 할당량

Detective에는 다음과 같은 할당량이 있으며 이는 구성할 수 없습니다.

리소스	Quota	설명
멤버 계정의 수	1,200	관리자 계정이 동작 그래프에 추가할 수 있는 멤버 계정의 수.
동작 그래프 데이터 볼륨 - 볼륨 경고	일일 9TB	동작 그래프 데이터 볼륨이 일일 9TB를 초과하는 경우 Detective는 동작 그래프가 최대 허용 볼륨에 가까워지고 있다는 경고를 표시합니다.
동작 그래프 데이터 볼륨 - 새로운 계정 없음	일일 10TB	동작 그래프 데이터 볼륨이 일일 10TB를 초과하는 경우 동작 그래프에 새 멤버 계정을 추가할 수 없습니다.
동작 그래프 데이터 볼륨 - 동작 그래프에 데이터 수집 중지	일일 15TB	동작 그래프 데이터 볼륨이 일일 15TB를 초과하는 경우 Detective는 동작 그래프에 대한 데이터 수집을 중지합니다. 일일 15TB는 일반적인 데이터 볼륨과 데이터 볼륨 급증을 모두 반영합니다. 데이터 수집을 다시 활성화하려면 AWS Support를 문의해야 합니다.

Internet Explorer 11은 지원되지 않음

Internet Explorer 11에서는 Detective를 사용할 수 없습니다.

Amazon Detective 설정

Amazon Detective를 활성화하면 Detective는 사용자 계정을 관리자 계정으로 사용하는 리전별 동작 그래프를 생성합니다. 처음에는 이 계정이 동작 그래프에 있는 유일한 계정입니다. 그러면 관리자 AWS 계정은 다른 계정을 초대하여 행동 그래프에 데이터를 제공할 수 있습니다. 계정 관리 섹션을 참조하십시오.

리전에서 Detective를 처음 활성화하면 동작 그래프에 대한 30일 무료 평가판도 시작됩니다. 계정에서 Detective를 비활성화했다가 다시 활성화하면 무료 평가판을 사용할 수 없습니다. 동작 그래프 무료 평가판에 대한 정보 섹션을 참조하십시오.

무료 평가판 사용 후에는 동작 그래프에 있는 각 계정에 기여한 데이터에 대한 요금이 청구됩니다. 관리자 계정은 사용량을 추적하고 전체 동작 그래프에 대한 일반적인 30일 기간의 총 예상 비용을 확인할 수 있습니다. 자세한 설명은 the section called “관리자 계정 사용량 및 비용” 섹션을 참조하세요. 멤버 계정은 자신이 속한 동작 그래프의 사용량과 예상 비용을 추적할 수 있습니다. 자세한 내용은 the section called “멤버 계정 사용량 추적” 단원을 참조하십시오.

목차

Amazon Detective 사전 요구 사항 및 권장 사항

Amazon Detective를 활성화하려면 AWS 계정가 있어야 합니다.

가입하여 다음을 수행하십시오. AWS 계정

계정이 없는 경우 다음 단계를 완료하여 계정을 만드세요. AWS 계정

가입하려면 AWS 계정

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.

   에 AWS 계정 가입하면 AWS 계정 루트 사용자a가 생성됩니다. 루트 사용자에게는 계정의 모든 AWS 서비스 및 리소스에 액세스하는 권한이 주어집니다. 보안 모범 사례는 관리자 사용자에게 관

리자 액세스 권한을 할당하고, 루트 사용자만 루트 사용자 액세스 권한이 필요한 태스크를 수행하는 것입니다.

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

관리 사용자 생성

등록한 AWS 계정 후에는 일상적인 작업에 루트 사용자를 사용하지 않도록 관리 사용자를 보호하고 AWS IAM Identity Center 활성화하고 생성하십시오 AWS 계정 루트 사용자.

보안을 유지하세요. AWS 계정 루트 사용자

1. 루트 사용자를 선택하고 AWS 계정 이메일 주소를 입력하여 계정 AWS Management Console소유자로 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 사용자 (콘솔) 에 대한 가상 MFA 디바이스 활성화를 참조하십시오.

관리자 사용자 생성

1. IAM Identity Center를 활성화합니다.

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

   를 ID 소스로 사용하는 방법에 대한 자습서는 사용 설명서의 기본값으로 IAM Identity Center 디렉터리 사용자 액세스 구성을 참조하십시오. IAM Identity Center 디렉터리 AWS IAM Identity Center

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 사용자를 사용하여 로그인하는 데 도움이 필요하면 사용 설명서의 AWS 액세스 포털에 로그인을 참조하십시오. AWS 로그인

다음과 같은 요구 사항 및 권장 사항을 숙지해야 합니다.

지원되는 버전 AWS Command Line Interface

를 사용하여 Detective 작업을 수행하는 AWS CLI 데 필요한 최소 버전은 1.16.303입니다.

및 를 기준으로 정렬하는 것이 좋습니다. GuardDuty AWS Security Hub

GuardDuty 및 AWS Security Hub 에 등록한 경우 해당 서비스의 관리자 계정을 사용하는 것이 좋습니다. 세 서비스 모두의 관리자 계정이 동일한 경우 다음 통합 지점이 원활하게 작동합니다.

- GuardDuty 또는 Security Hub에서 검색 결과에 대한 세부 정보를 볼 때 GuardDuty 검색 결과 세부 정보에서 Detective 검색 결과 프로필로 전환할 수 있습니다.
- Detective에서는 GuardDuty 결과를 조사할 때 해당 결과를 보관하는 옵션을 선택할 수 있습니다.

Security GuardDuty Hub와 관리자 계정이 다른 경우 자주 사용하는 서비스에 따라 관리자 계정을 정렬하는 것이 좋습니다.

- GuardDuty 더 자주 사용하는 경우 GuardDuty 관리자 계정을 사용하여 Detective를 활성화하십시오.

  를 AWS Organizations 사용하여 계정을 관리하는 경우 GuardDuty 관리자 계정을 조직의 Detective 관리자 계정으로 지정하십시오.
- Security Hub를 더 자주 사용하는 경우 Security Hub 관리자 계정을 사용하여 Detective를 활성화합니다.

  Organizations를 사용하여 계정을 관리하는 경우 Security Hub 관리자 계정을 조직의 Detective 관리자 계정으로 지정합니다..

모든 서비스에서 동일한 관리자 계정을 사용할 수 없는 경우 Detective를 활성화한 후 선택적으로 크로스 계정 역할을 만들 수 있습니다. 이 역할은 관리자 계정에 다른 계정에 대한 액세스 권한을 부여합니다.

IAM이 이러한 유형의 역할을 지원하는 방법에 대한 자세한 내용은 IAM 사용 설명서에서 소유하고 있는 다른 AWS 계정의 IAM 사용자에게 액세스 권한 제공을 참조하십시오.

필요한 Detective 권한 부여

Detective를 활성화하려면 먼저 IAM 보안 주체에 필요한 Detective 권한이 있는지 확인해야 합니다. 보안 주체는 이미 사용 중인 기존 사용자 또는 역할일 수도 있고, Detective에 사용할 새 사용자 또는 역할을 만들 수도 있습니다.

Amazon Web Services(AWS)에 가입 시 해당 계정은 Amazon Detective를 포함한 모든 AWS 서비스에 자동으로 가입됩니다. 그러나 Detective를 활성화하고 사용하려면 Amazon Detective 콘솔에 대한 액세스와 API 작업에 대한 액세스를 허용하는 권한을 설정해야 합니다. 사용자 또는 관리자는 AWS Identity and Access Management (IAM) 을 사용하여 `AmazonDetectiveFullAccess`관리형 정책을 IAM 보안 주체에 연결하여 모든 Detective 작업에 대한 액세스 권한을 부여함으로써 이 작업을 수행할 수 있습니다.

알림 빈도에 대한 권장 업데이트 GuardDuty CloudWatch

GuardDuty에서는 탐지기가 Amazon CloudWatch 알림 빈도로 구성되어 있어 후속 탐지 결과를 보고할 수 있습니다. 여기에는 Detective에 알림을 보내는 것도 포함됩니다.

기본 빈도는 6시간입니다. 즉, 조사 결과가 여러 번 반복되더라도 최대 6시간이 지나야 새로운 발생이 Detective에 반영됩니다.

Detective에서 이러한 업데이트를 수신하는 데 걸리는 시간을 줄이려면 GuardDuty 관리자 계정에서 감지기의 설정을 15분으로 변경하는 것이 좋습니다. 단, 구성을 변경해도 사용 비용에는 영향을 미치지 않습니다. GuardDuty

알림 빈도 설정에 대한 자세한 내용은 Amazon GuardDuty 사용 설명서의 Amazon CloudWatch Events를 통한 모니터링 GuardDuty 결과를 참조하십시오.

Amazon Detective 활성화

Detective를 활성화하면 Detective 관리자 계정을 지정하고 다른 계정을 멤버 계정으로 초대합니다. 예비 구성원 계정이 관리자 계정의 초대를 수락하면 Security Hub 관리자-구성원 관계가 성립됩니다. 자세한 내용은 계정 관리를 참조하십시오.

조직 동작 그래프에서 Detective 관리자 계정은 모든 조직 계정의 동작 그래프 멤버십을 관리합니다. Detective 관리자 계정을 관리하는 방법에 대한 자세한 내용은 조직의 Detective 관리자 계정 지정을 참조하십시오.

Detective 콘솔, Detective API 또는 AWS Command Line Interface에서 Detective를 활성화할 수 있습니다.

Detective는 각 리전에서 한 번만 활성화할 수 있습니다. 이미 해당 리전의 동작 그래프의 관리자 계정인 경우 해당 리전에서 Detective를 다시 활성화할 수 없습니다.

Detective 활성화(콘솔)

AWS Management Console에서 Amazon Detective를 활성화할 수 있습니다.

Detective 활성화(콘솔)

1. AWS Management Console에 로그인합니다. 그런 다음 https://console.aws.amazon.com/detective/에서 Detective 콘솔을 엽니다.
2. Get started를 선택합니다.
3. Amazon Detective 활성화 페이지에서 관리자 계정 정렬 (권장) 에는 관리자 계정을 Detective와 Amazon 및 간에 정렬하기 위한 권장 사항이 설명되어 있습니다. GuardDuty AWS Security Hub the section called “및 를 기준으로 정렬하는 것이 좋습니다. GuardDuty AWS Security Hub” 섹션을 참조하십시오.
4. IAM 정책 연결 버튼을 누르면 IAM 콘솔로 바로 이동하여 권장 정책을 엽니다. Detective에 사용하는 보안 주체에 권장 정책을 연결할 수 있습니다. IAM 콘솔에서 작업할 권한이 없는 경우 필수 권한 내에서 Amazon 리소스 이름(ARN) 정책을 복사하여 IAM 관리자에게 제공할 수 있습니다. 사용자를 대신하여 정책을 첨부할 수 있습니다.

   필수 IAM 정책이 적용되었는지 확인합니다.
5. 태그 추가 섹션에서는 동작 그래프에 태그를 추가할 수 있습니다.

   태그를 추가하려면 다음을 수행합니다.

   a. 새 태그 추가(Add new tag)를 선택합니다.
   b. 키에는 태그의 이름을 입력합니다.
   c. 값에는 태그 값을 입력합니다.

   태그를 제거하려면 태그의 제거 옵션을 선택합니다.
6. Amazon Detective 활성화를 선택합니다.
7. Detective를 활성화한 후 멤버 계정을 동작 그래프에 초대할 수 있습니다.

   계정 관리 페이지로 이동하려면 지금 멤버 추가를 선택합니다. 멤버 계정 초대에 대한 자세한 내용은 the section called “동작 그래프에 멤버 계정 초대” 섹션을 참조하세요.

디텍티브 활성화 (디텍티브 API,) AWS CLI

Detective API 또는 AWS Command Line Interface에서 Amazon Detective를 활성화할 수 있습니다.

Detective (Detective API) 를 활성화하려면 AWS CLI

- Detective API: `CreateGraph` 작업을 사용합니다.
- AWS CLI: 명령줄에서 `create-graph` 명령을 실행합니다.

```
aws detective create-graph --tags '{"tagName": "tagValue"}'
```

다음 명령은 Detective를 활성화하고 `Department` 태그의 값을 `Security`로 설정합니다.

```
aws detective create-graph --tags '{"Department": "Security"}'
```

지역 간 Detective 활성화 (Python 스크립트 켜짐) GitHub

Detective는 다음과 같은 작업을 GitHub 수행하는 오픈 소스 스크립트를 제공합니다.

- 지정된 리전 목록의 관리자 계정에 대해 Detective 활성화
- 제공된 멤버 계정 목록을 결과 동작 그래프에 추가
- 멤버 계정에 초대 이메일 전송
- 멤버 계정에 대한 초대 자동 수락

GitHub 스크립트 구성 및 사용 방법에 대한 자세한 내용은 을 참조하십시오. Amazon Detective Python 스크립트 사용

데이터가 추출되고 있는지 확인

Detective를 활성화하면 AWS 계정 데이터를 수집하여 행동 그래프로 추출하기 시작합니다.

초기 추출의 경우 일반적으로 2시간 이내에 행동 그래프에서 데이터를 사용할 수 있습니다.

Detective가 데이터를 추출하고 있는지 확인하는 한 가지 방법은 Detective 검색 페이지에서 예제 값을 찾는 것입니다.

검색 페이지에서 예제 값 확인

1. https://console.aws.amazon.com/detective/에서 Amazon Detective 콘솔을 엽니다.
2. 탐색 창에서 검색을 선택합니다.
3. 유형 선택 메뉴에서 항목 유형을 선택합니다.

   데이터의 예제에는 동작 그래프 데이터에 있는 선택한 유형의 식별자 샘플 세트가 포함되어 있습니다.

   예제 값을 보면 데이터가 수집되고 동작 그래프로 추출되고 있다는 것을 알 수 있습니다.

동작 그래프 무료 평가판에 대한 정보

Amazon Detective는 각 리전의 각 계정에 대해 30일 무료 평가판을 제공합니다. 계정의 무료 평가판은 다음 작업 중 하나가 처음 발생할 때 시작됩니다.

- 계정이 Detective를 수동으로 활성화하고 동작 그래프의 관리자 계정이 됩니다.
- 계정이 AWS Organizations에서 조직의 Detective 관리자 계정으로 지정되고 처음으로 Detective가 활성화되었습니다.
- Detective 관리자 계정을 지정하기 전에 이미 Detective를 활성화한 경우에는 새 30일 무료 평가판이 시작되지 않습니다.
- 계정이 동작 그래프에서 멤버 계정으로 가입하라는 초대를 수락하고 멤버 계정으로 활성화됩니다.
- 조직 계정이 Detective 관리자 계정에 의해 멤버 계정으로 활성화됩니다.

무료 평가판은 해당 시점부터 30일 동안 지속됩니다. 해당 기간 동안 처리된 데이터에 대해서는 계정에 요금이 청구되지 않습니다. 평가 기간이 끝나면 Detective는 동작 그래프에 기여한 데이터에 대해 계정에 요금을 청구하기 시작합니다. Detective 활동을 추적하고 사용량을 모니터링하고 예상 비용을 확인하는 방법에 대한 자세한 내용은 Amazon Detective에서의 활동 및 사용량 추적 섹션을 참조하세요. 요금에 대한 자세한 내용은 Detective 요금을 참조하세요.

해당 리전의 모든 동작 그래프에는 동일한 30일 기간이 사용됩니다. 예를 들어, 계정이 동작 그래프의 멤버 계정으로 활성화되어 있습니다. 그러면 30일 무료 평가판이 시작됩니다. 10일 후 해당 계정은 동일한 리전에서 두 번째 동작 그래프를 생성할 수 있습니다. 두 번째 동작 그래프의 경우 계정에 20일간의 무료 데이터가 제공됩니다.

무료 평가판은 여러 가지 이점을 제공합니다.

- 관리자 계정은 Detective의 기능을 탐색하여 그 가치를 확인할 수 있습니다.
- 관리자 및 멤버 계정은 Detective가 청구를 시작하기 전에 데이터 양과 예상 비용을 모니터링할 수 있습니다. the section called “관리자 계정 사용량 및 비용” 및 the section called “멤버 계정 사용량 추적”를 참조하세요.

선택적 데이터 소스에 대한 무료 평가판

또한 Detective는 선택적 데이터 소스에 대해 30일 무료 평가판을 제공합니다. 이 무료 평가판은 Detective가 처음 활성화되었을 때 핵심 Detective 데이터 소스에 제공되는 무료 평가판과는 별개입니다.

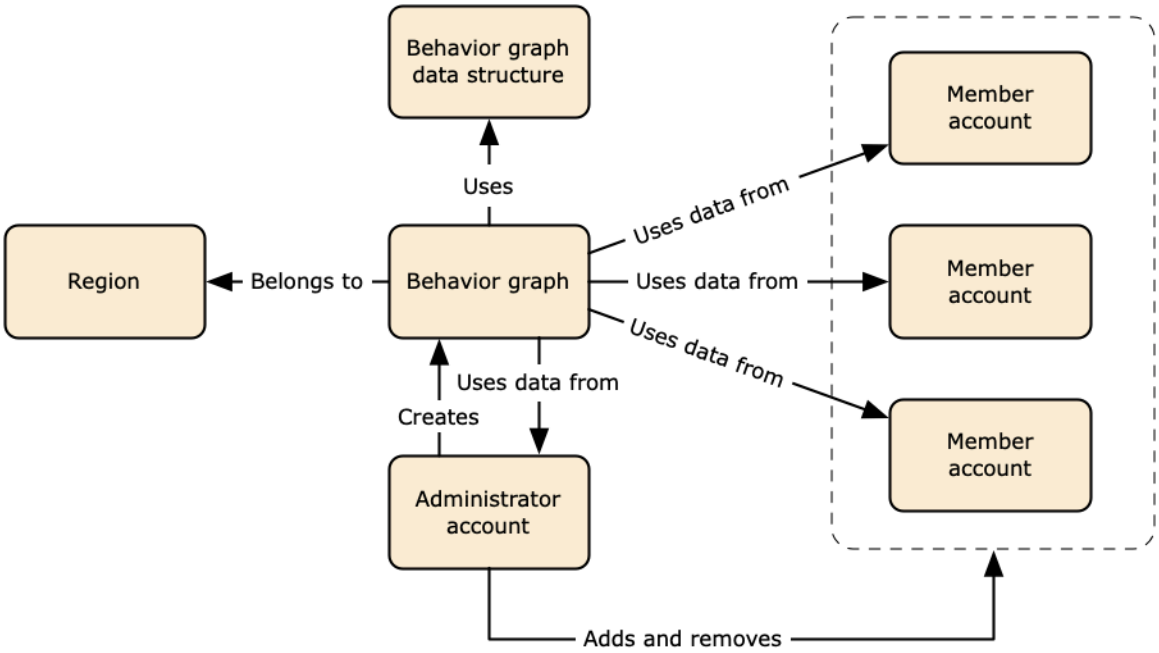
> **Note**
>
> 고객이 선택적 데이터 소스 패키지를 활성화한 후 7일 이내에 비활성화하면 Detective는 해당 데이터 소스 패키지가 다시 활성화되는 경우 해당 데이터 소스 패키지의 무료 평가판을 1회 자동 재설정합니다.

선택적 데이터 소스를 활성화 또는 비활성화하려면 Detective의 선택적 데이터 소스 유형 섹션을 참조하세요.

동작 그래프에 사용된 소스 데이터

Amazon Detective는 동작 그래프를 채우기 위해 동작 그래프 관리자 계정 및 멤버 계정의 소스 데이터를 사용합니다.

Detective를 사용하면 최대 1년 분량의 과거 이벤트 데이터에 액세스할 수 있습니다. 이 데이터는 선택한 기간 동안의 활동 유형 및 양의 변화를 보여주는 일련의 시각화를 통해 제공됩니다. Detective는 이러한 변경 사항을 GuardDuty 조사 결과와 연결합니다.



동작 그래프 데이터 구조에 대한 자세한 내용은 Detective 사용 설명서의 동작 그래프 데이터 구조 개요를 참조하세요.

Detective의 핵심 데이터 소스 유형

Detective는 다음과 같은 유형의 AWS 로그에서 데이터를 수집합니다.

- AWS CloudTrail 로그
- Amazon Virtual Private Cloud(VPC) 흐름 로그
- GuardDuty에 등록된 계정의 경우 Detective는 GuardDuty 조사 결과도 수집합니다.

Detective는 CloudTrail 및 VPC 흐름 로그의 독립적이고 중복된 스트림을 통해 CloudTrail 및 VPC 흐름 로그 이벤트를 사용합니다. 이러한 프로세스는 기존 CloudTrail 및 VPC 흐름 로그 구성에 영향을 주거

나 이를 사용하지 않습니다. 또한 이러한 서비스의 성능에 영향을 미치거나 비용을 증가시키지 않습니다.

Detective의 선택적 데이터 소스 유형

Detective는 Detective 핵심 패키지에서 제공되는 세 가지 데이터 소스 외에도 선택적 소스 패키지를 제공합니다(핵심 패키지에는 AWS CloudTrail 로그그, VPC 흐름 로그 및 GuardDuty 조사 결과가 포함됨). 동작 그래프의 선택적 데이터 소스 패키지는 언제든지 시작하거나 중지할 수 있습니다.

Detective는 리전별 모든 핵심 및 선택적 소스 패키지에 대해 30일 무료 평가판을 제공합니다.

> **Note**
>
> Detective는 각 데이터 소스 패키지에서 받은 모든 데이터를 최대 1년 동안 보관합니다.

현재 사용 가능한 선택적 소스 패키지는 다음과 같습니다.

- EKS 감사 로그

  이 선택적 데이터 소스 패키지를 사용하면 Detective가 사용자 환경의 EKS 클러스터에 대한 세부 정보를 수집하고 해당 데이터를 동작 그래프에 추가할 수 있습니다. 세부 정보는 Detective에 대한 Amazon EKS 감사 로그을 참조하십시오.
- AWS 보안 조사 결과

  이 선택적 데이터 소스 패키지를 사용하면 Detective가 Security Hub에서 데이터를 수집하여 동작 그래프에 추가할 수 있습니다. 세부 정보는 AWS 보안 조사 결과을 참조하십시오.

선택적 데이터 소스 시작 또는 중지:

1. https://console.aws.amazon.com/detective/에서 Detective 콘솔을 엽니다.
2. 탐색 창의 설정 아래에서 일반을 선택합니다.
3. 선택적 소스 패키지에서 업데이트를 선택합니다. 그런 다음 활성화하려는 데이터 소스를 선택하거나 이미 활성화된 데이터 소소의 확인란을 선택 취소하고 업데이트를 선택하여 활성화된 데이터 소스 패키지를 변경합니다.

> **Note**
>
> 선택적 데이터 소스를 중지했다가 다시 시작하면 일부 엔터티 프로필에 표시된 데이터에 차이가 있는 것을 확인할 수 있습니다. 이 차이는 콘솔 디스플레이에 표시되며 데이터 소스가 중지된 기간을 나타냅니다. 데이터 소스가 재시작되면 Detective는 데이터를 소급하여 수집하지 않습니다.

Detective에 대한 Amazon EKS 감사 로그

Amazon EKS 감사 로그는 Detective 행동 그래프에 추가할 수 있는 선택적 데이터 소스 패키지입니다. 콘솔의 설정 페이지 또는 Detective API를 통해 계정에서 사용 가능한 선택적 소스 패키지와 해당 상태를 볼 수 있습니다.

이 데이터 소스에 대해 30일 무료 평가판이 제공됩니다. 자세한 내용은 선택적 데이터 소스에 대한 무료 평가판 섹션을 참조하세요.

Amazon EKS 감사 로그를 활성화하면 Detective에서 Amazon EKS로 생성한 리소스에 대한 심층적인 정보를 동작 그래프에 추가할 수 있습니다. 이 데이터 소스는 EKS 클러스터, Kubernetes 포드, 컨테이너 이미지 및 Kubernetes 객제와 같은 엔터티 유형에 대해 제공된 정보를 개선합니다.

또한 Amazon GuardDuty에서 EKS 감사 로그를 데이터 소스로 활성화한 경우 GuardDuty에서 Kubernetes 조사 결과에 대한 세부 정보를 볼 수 있습니다. GuardDuty에서 이 데이터 소스를 활성화하는 방법에 대한 자세한 내용은 Amazon GuardDuty의 Kubernetes 보호를 참조하세요.

> **Note**
>
> 이 데이터 소스는 2022년 7월 26일 이후에 생성된 새 동작 그래프에 대해 기본적으로 활성화됩니다. 2022년 7월 26일 이전에 만든 동작 그래프의 경우 수동으로 활성화해야 합니다.

Amazon EKS 감사 로그를 선택적 데이터 소스로 추가 또는 제거:

1. https://console.aws.amazon.com/detective/에서 Detective 콘솔을 엽니다.
2. 탐색 창의 설정 아래에서 일반을 선택합니다.
3. 소스 패키지에서 EKS 감사 로그를 선택하여 이 데이터 소스를 활성화합니다. 이미 활성화되어 있는 경우 다시 선택하면 EKS 감사 로그가 동작 그래프에 수집되는 것을 중지할 수 있습니다.

AWS 보안 조사 결과

AWS 보안 조사 결과는 Detective 동작 그래프에 추가할 수 있는 선택적 데이터 소스 패키지입니다.

콘솔의 설정 페이지 또는 Detective API를 통해 계정에서 사용 가능한 선택적 소스 패키지와 해당 상태를 볼 수 있습니다.

이 데이터 소스에 대해 30일 무료 평가판이 제공됩니다. 자세한 내용은 선택적 데이터 소스에 대한 무료 평가판 섹션을 참조하세요.

AWS 보안 조사 결과를 활성화하면 Detective는 업스트림 서비스에서 Security Hub가 집계한 Security Hub의 조사 결과를 AWS Security Format(ASFF)이라는 표준 조사 결과 형식으로 사용할 수 있으므로 시간이 많이 걸리는 데이터 변환 작업이 필요하지 않습니다. 그러면 가장 중요한 제품에 우선 순위를 부여하기 위해 제품 전반에 걸쳐 수집된 결과를 상호 연관시킵니다.

AWS 보안 조사 결과를 선택적 데이터 소스로 추가 또는 제거:

> **Note**
>
> AWS 보안 조사 결과 데이터 소스는 2023년 5월 16일 이후에 생성된 새 동작 그래프에 대해 기본적으로 활성화됩니다. 2023년 5월 16일 이전에 만든 동작 그래프의 경우 수동으로 활성화해야 합니다.

1. https://console.aws.amazon.com/detective/에서 Detective 콘솔을 엽니다.
2. 탐색 창의 설정 아래에서 일반을 선택합니다.
3. 소스 패키지에서 AWS 보안 조사 결과를 선택하여 이 데이터 소스를 활성화합니다. 이미 활성화되어 있는 경우 다시 선택하면 AWS Security Finding Format(AWS ASFF) 조사 결과를 동작 그래프에 수집하는 것을 중지할 수 있습니다.

현재 지원되는 조사 결과

Detective는 Amazon 또는 AWS 소유의 서비스로부터 Security Hub에 있는 모든 ASFF 조사 결과를 수집합니다.

- 지원되는 서비스 통합 목록을 보려면 AWS Security Hub 사용 설명서의 사용 가능한 AWS 서비스 통합을 참조하세요.
- 지원되는 리소스 목록은 AWS Security Hub 사용 설명서의 리소스를 참조하세요.

- 규정 준수 상태가 FAILED로 설정되지 않은 AWS 서비스 검색 결과 및 크로스 리전 집계 활성화 조사 결과는 수집되지 않습니다.

Detective가 소스 데이터를 수집하고 저장하는 방법

Detective가 활성화되면 Detective는 동작 그래프 관리자 계정에서 소스 데이터를 수집하기 시작합니다. 멤버 계정이 동작 그래프에 추가되면 Detective는 해당 멤버 계정의 데이터도 사용하기 시작합니다.

Detective 소스 데이터는 원본 피드의 구조화된 버전과 처리된 버전으로 구성됩니다. Detective 분석을 지원하기 위해 Detective는 Detective 소스 데이터의 사본을 저장합니다.

Detective 수집 프로세스는 Detective 소스 데이터 스토어의 Amazon Simple Storage Service(S3) 버킷에 데이터를 제공합니다. 새 소스 데이터가 도착하면 다른 Detective 구성 요소가 데이터를 수집하여 추출 및 분석 프로세스를 시작합니다. 자세한 내용은 Detective 사용 설명서의 Detective가 소스 데이터를 사용하여 동작 그래프를 채우는 방법 참조하세요.

Detective가 동작 그래프의 데이터 볼륨 할당량을 적용하는 방법

Detective는 각 동작 그래프에서 허용하는 데이터의 볼륨에 대해 엄격한 할당량을 적용합니다. 데이터 볼륨은 Detective 동작 그래프에 유입되는 일일 데이터 양입니다.

Detective는 관리자 계정이 Detective를 활성화하고 멤버 계정이 동작 그래프에 제공하도록 초대를 수락할 때 이러한 할당량을 적용합니다.

- 관리자 계정의 데이터 볼륨이 하루 10TB를 초과하는 경우 관리자 계정에서 Detective를 활성화할 수 없습니다.
- 멤버 계정에서 추가된 데이터 볼륨으로 인해 동작 그래프가 하루 10TB를 초과하는 경우 멤버 계정을 활성화할 수 없습니다.

동작 그래프의 데이터 볼륨은 시간 경과에 따라 자연스럽게 증가할 수도 있습니다. Detective는 매일 동작 그래프 데이터 볼륨을 확인하여 할당량을 초과하지 않는지 확인합니다.

동작 그래프 데이터 볼륨이 할당량에 가까워지면 Detective는 콘솔에 경고 메시지를 표시합니다. 할당량을 초과하지 않도록 멤버 계정을 제거할 수 있습니다.

동작 그래프 데이터 용량이 하루 10TB를 초과하는 경우 동작 그래프에 새 멤버 계정을 추가할 수 없습니다.

동작 그래프 데이터 용량이 하루 15TB를 초과하는 경우 Detective는 동작 그래프에 대한 데이터 수집을 중단합니다. 일일 15TB 할당량은 일반적인 데이터 볼륨과 데이터 볼륨 급증을 모두 반영합니다. 이 할당량에 도달하면 동작 그래프에 새 데이터가 수집되지 않지만 기존 데이터는 제거되지 않습니다. 해당 과거 데이터를 조사에 계속 사용할 수 있습니다. 콘솔에 동작 그래프에 대한 데이터 수집이 일시 중단되었음을 알리는 메시지가 표시됩니다.

데이터 수집이 일시 중단된 경우 다시 활성화하려면 AWS Support 작업을 수행해야 합니다. 가능하면 AWS Support에 연락하기 전에 멤버 계정을 삭제하여 데이터 용량이 할당량 이하로 떨어지도록 합니다. 그러면 동작 그래프에 대한 데이터 수집을 다시 활성화하기가 더 쉬워집니다.

계정 관리

각 동작 그래프에는 하나 이상의 계정 데이터가 포함됩니다. 계정이 Detective를 활성화하면 해당 계정이 동작 그래프의 관리자 계정이 되고 동작 그래프에 사용할 멤버 계정을 선택합니다. 동작 그래프에는 최대 1,200개의 멤버 계정을 포함할 수 있습니다.

와 AWS Organizations 통합된 경우 조직 관리 계정이 조직의 Detective 관리자 계정을 지정합니다. 그러면 Detective 관리자 계정이 조직 동작 그래프의 관리자 계정이 됩니다. Detective 관리자 계정은 조직 동작 그래프에서 모든 조직 계정을 멤버 계정으로 활성화할 수 있습니다. 조직 계정은 조직 동작 그래프에서 자신을 제거할 수 없습니다.

관리자 계정은 동작 그래프에 조인하도록 계정을 초대할 수도 있습니다. 계정이 초대를 수락하면 Detective는 해당 계정을 멤버 계정으로 활성화합니다. 초대를 통해 추가된 멤버 계정은 동작 그래프에서 자신을 연결 해제할 수 있습니다.

계정이 멤버 계정으로 활성화되면 Detective는 멤버 계정의 데이터를 수집하고 해당 동작 그래프로 추출하기 시작합니다.

Detective는 각 동작 그래프에 기여한 데이터에 대해 각 계정에 요금을 부과합니다. 동작 그래프에서 각 계정의 데이터 양을 추적하는 방법에 대한 자세한 내용은 the section called “관리자 계정 사용량 및 비용” 섹션을 참조하세요.

내용

Detective의 계정 제한 및 권장 사항

Amazon Detective에서 계정을 관리할 때 다음 제한 사항에 유의합니다.

회원 계정 최대 수

Detective는 각 동작 그래프에서 최대 1,200개의 멤버 계정을 허용합니다.

계정 및 리전

AWS Organizations를 사용하여 계정을 관리하는 경우 조직 관리 계정을 조직의 Detective 관리자 계정으로 지정합니다. Detective 관리자 계정은 조직 동작 그래프의 관리자 계정이 됩니다.

Detective 관리자 계정은 모든 리전에서 동일해야 합니다. 조직 관리 계정은 각 리전에 있는 Detective 관리자 계정을 개별적으로 지정합니다. 또한 Detective 관리자 계정은 각 리전의 조직 동작 그래프와 멤버 계정을 개별적으로 관리합니다.

초대를 통해 생성된 멤버 계정의 경우 초대를 보낸 리전에서만 관리자-멤버 연결이 생성됩니다. 관리자 계정은 각 리전에서 Detective를 활성화해야 하며 각 리전마다 별도의 동작 그래프가 있어야 합니다. 그러면 관리자 계정이 각 계정을 해당 리전의 구성원 계정으로 연결하도록 초대합니다.

계정은 동일한 리전 내 여러 동작 그래프의 멤버 계정일 수 있습니다. 계정은 리전당 하나의 동작 그래프의 관리자 계정만 될 수 있습니다. 계정은 여러 리전의 관리자 계정일 수 있습니다.

Security Hub 및 GuardDuty와 관리자 계정 정렬

AWS Security Hub 및 Amazon GuardDuty와의 통합이 원활하게 작동하도록 하려면 이러한 모든 서비스에서 동일한 계정을 관리자 계정으로 사용하는 것이 좋습니다.

the section called “및 를 기준으로 정렬하는 것이 좋습니다. GuardDuty AWS Security Hub” 섹션을 참조하세요.

관리자 계정에 필요한 권한 부여

관리자 계정이 동작 그래프를 관리하는 데 필요한 권한을 갖도록 하려면 `AmazonDetectiveFullAccess` 관리형 정책을 IAM 보안 주체에 연결합니다.

Detective에 조직 업데이트 반영

조직의 변경 사항은 Detective에 즉시 반영되지 않습니다.

신규 및 제거된 조직 계정과 같은 대부분의 변경 사항은 Detective에 알림이 전송되는 데 최대 1시간이 걸릴 수 있습니다.

Organizations에서 지정된 Detective 관리자 계정을 변경하면 변경 내용을 전파하는 데 시간이 덜 걸립니다.

Organizations를 사용하여 동작 그래프 계정을 관리하도록 전환

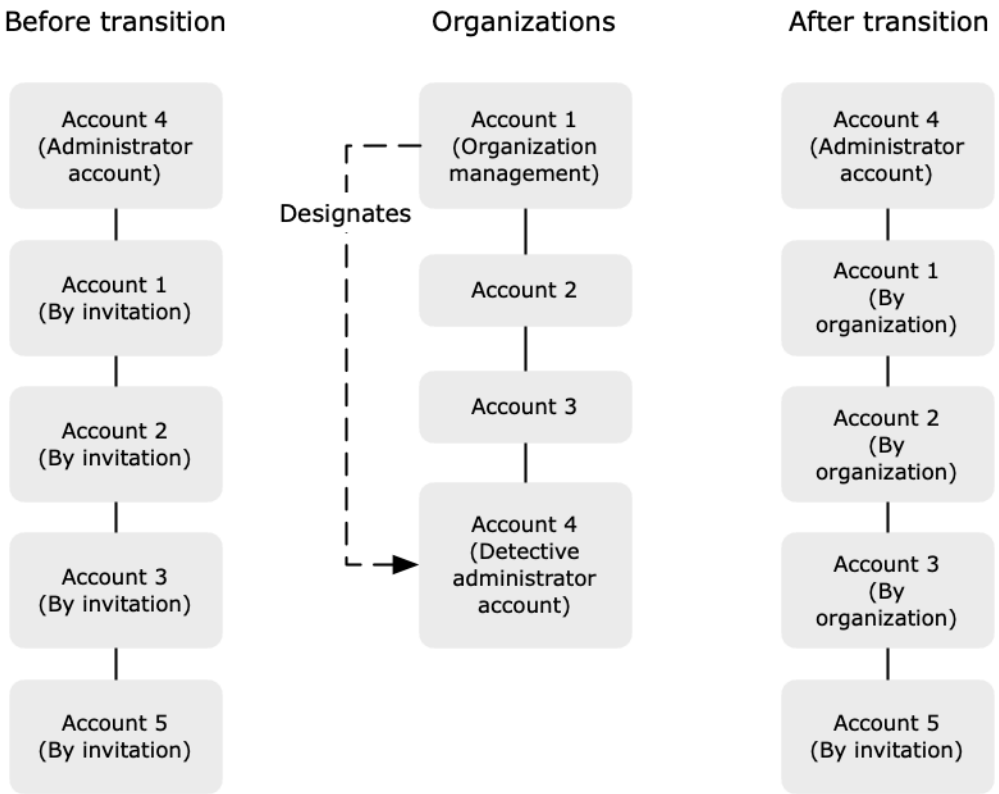
수동 초대를 수락한 멤버 계정이 표시된 기존 동작 그래프가 있을 수 있습니다. AWS Organizations에 등록한 경우 수동 초대 프로세스를 사용하는 대신 다음과 같은 단계를 통해 Organizations를 사용하여 구성원 계정을 활성화하고 관리하십시오.

1. 조직을 위해 Detective 관리자 계정을 지정합니다. 그러면 조직 동작 그래프가 생성됩니다.

   Detective 관리자 계정에 이미 동작 그래프가 있는 경우 해당 동작 그래프는 조직 동작 그래프가 됩니다.
2. 조직 동작 그래프에서 조직 계정을 멤버 계정으로 활성화합니다.

   조직 동작 그래프에 조직 계정인 기존 멤버 계정이 있는 경우 해당 계정은 자동으로 활성화됩니다.

다음 다이어그램은 전환 전의 동작 그래프 구조, Organizations의 구성, 전환 후의 동작 그래프 계정 구조에 대한 개요를 보여줍니다.



조직의 Detective 관리자 계정 지정

조직 관리 계정은 조직의 Detective 관리자 계정을 지정합니다. the section called “Detective 관리자 계정 지정” 섹션을 참조하세요.

전환을 더 단순하게 만들기 위해 Detective는 현재 관리자 계정을 조직의 Detective 관리자 계정으로 선택할 것을 권장합니다.

Organizations에 Detective에 대해 위임된 관리자 계정이 있는 경우 해당 계정 또는 조직 관리 계정을 Detective 관리자 계정으로 사용해야 합니다.

그렇지 않으면 조직 관리 계정이 아닌 Detective 관리자 계정을 처음 지정할 때 Detective는 Organizations를 호출하여 해당 계정을 Detective의 위임된 관리자 계정으로 설정합니다.

조직 계정을 구성원 계정으로 활성화합니다.

Detective 관리자 계정은 조직 동작 그래프의 관리자 계정입니다. Detective 관리자 계정은 조직 동작 그래프에서 멤버 계정으로 활성화할 조직 계정을 선택합니다. the section called “조직 멤버 계정 관리” 섹션을 참조하세요.

계정 페이지에서 Detective 관리자 계정은 조직의 모든 계정을 볼 수 있습니다.

Detective 관리자 계정이 이미 동작 그래프의 관리자 계정인 경우 해당 동작 그래프는 조직 동작 그래프가 됩니다. 동작 그래프에서 이미 멤버 계정이었던 조직 계정은 자동으로 멤버 계정으로 활성화됩니다. 다른 조직 계정의 상태는 멤버가 아님입니다.

조직 계정이 이전에 초대를 통한 구성원 계정이었더라도 조직 계정에는 조직을 통한 유형이 있습니다.

조직에 속하지 않는 멤버 계정의 유형은 초대별 계정입니다.

계정 관리 페이지에는 새 계정이 조직에 추가될 때 자동으로 활성화할 수 있는 새 조직 계정 자동 활성화 옵션도 제공합니다. the section called “새 조직 계정 자동 활성화” 섹션을 참조하세요. 이 옵션은 처음에는 꺼져 있습니다.

Detective 관리자 계정이 계정 관리 페이지를 처음 표시하면 모든 조직 계정 활성화 버튼이 포함된 메시지가 표시됩니다. 모든 조직 계정 활성화를 선택하면 Detective는 다음 작업을 수행합니다.

- 현재 조직 계정 전체를 멤버 계정으로 활성화합니다.
- 옵션을 켜면 새 조직 계정을 자동 활성화합니다.

멤버 계정 목록에는 모든 조직 계정 활성화 옵션도 있습니다.

계정에 사용할 수 있는 작업

관리자 및 구성원 계정은 다음과 같은 Detective 작업에 액세스할 수 있습니다. 테이블에서 값의 의미는 다음과 같습니다.

- 모두 - 이 계정은 동일한 Detective 관리자 계정에 속한 모든 계정에 대해 작업을 수행할 수 있습니다.
- 본인 - 이 계정은 자신의 계정에서만 작업을 수행할 수 있습니다.
- 대시(-) - 해당 계정에서 작업을 수행할 수 없습니다.

다음 테이블에는 관리자 및 멤버 계정의 기본 권한이 반영되어 있습니다. 사용자 지정 IAM 정책을 사용하여 Detective 특징 및 기능에 대한 액세스를 추가로 제한할 수 있습니다.

작업	관리자 계정(조직)	관리자 계정(초대)	멤버(조직)	멤버(초대)
계정 보기	모두	모두	본인(관리자 계정 보기)	본인(관리자 계정 보기)
멤버 계정 제거	모두 초대된 계정이 제거됨 조직 계정 연결 해제됨	모두	–	본인
선택적 데이터 소스 패키지 추가 또는 제거	모두(설정은 모든 멤버 계정에 적용됨)	모두(설정은 모든 멤버 계정에 적용됨)	–	–
Detective 비활성화	본인	본인	–	–
동작 그래프 데이터 보기	모두	모두	–	–

작업	관리자 계정(조직)	관리자 계정(초대)	멤버(조직)	멤버(초대)
선택적 데이터 소스 패키지 활성화 또는 비활성화	모두	모두	–	–

조직의 Detective 관리자 계정 지정

조직 동작 그래프에서 Detective 관리자 계정은 모든 조직 계정의 동작 그래프 멤버십을 관리합니다.

Detective 관리자 계정을 관리하는 방법

조직 관리 계정은 각 AWS 리전에서 조직의 Detective 관리자 계정을 지정합니다.

Detective 관리자 계정을 위임된 관리자 계정으로 설정

Detective 관리자 계정은 AWS Organizations에서 Detective에 대한 위임된 관리자 계정이 되기도 합니다. 단, 조직 관리 계정이 본인을 Detective 관리자 계정으로 지정한 경우는 예외입니다. 조직 관리 계정은 조직에서 위임된 관리자일 수 있습니다.

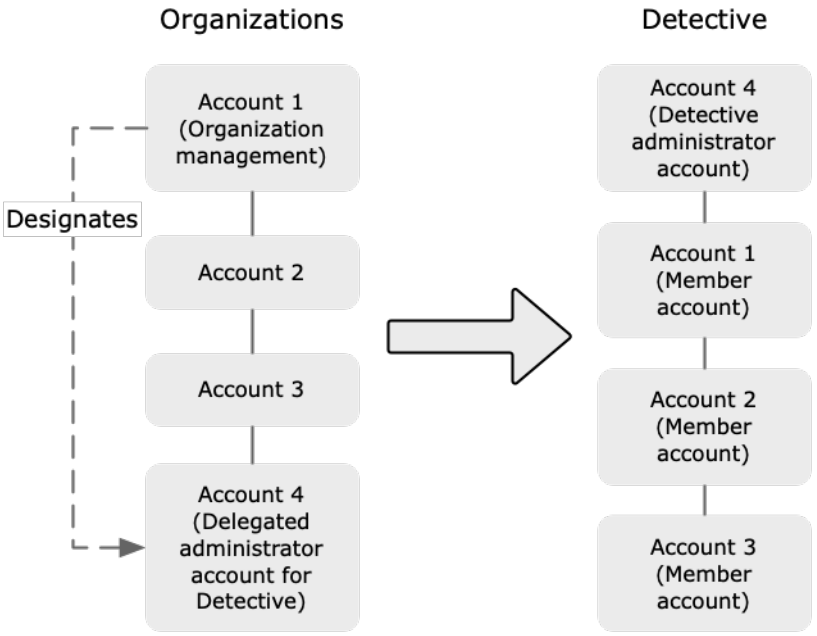
조직에 위임된 관리자 계정이 설정되면 조직 관리 계정은 위임된 관리자 계정 또는 자체 계정만 Detective 관리자 계정으로 선택할 수 있습니다. 모든 리전에 위임된 관리자 계정을 선택하는 것을 권장합니다.

조직 동작 그래프 생성 및 관리

조직 관리 계정이 Detective 관리자 계정을 선택하면 Detective는 해당 계정에 대한 새 동작 그래프를 생성합니다. 이 동작 그래프는 조직 동작 그래프입니다.

Detective 관리자 계정이 기존 동작 그래프의 관리자 계정인 경우 해당 동작 그래프는 조직 동작 그래프가 됩니다.

Detective 관리자 계정은 조직 동작 그래프에서 멤버 계정으로 활성화할 조직 계정을 선택합니다.



Detective 관리자 계정은 조직에 속하지 않는 계정으로 초대를 보낼 수도 있습니다. 자세한 정보는 the section called “조직 멤버 계정 관리” 및 the section called “초대된 계정 관리” 섹션을 참조하세요.

Detective 관리자 계정 지정

조직 관리자 계정은 리전의 현재 Detective 관리자 계정을 제거할 수 있습니다. Detective 관리자 계정을 제거하면 Detective는 현재 리전에서만 해당 계정을 제거합니다. Organizations의 위임된 관리자 계정은 변경되지 않습니다.

조직 관리 계정이 리전의 Detective 관리자 계정을 제거하면 Detective는 조직 동작 그래프를 삭제합니다. 제거된 Detective 관리자 계정에 대해 Detective가 비활성화됩니다.

Detective의 현재 위임된 관리자 계정을 제거하려면 Organizations API를 사용합니다. Organizations의 Detective에 대한 위임된 관리자 계정을 제거하면 Detective는 위임된 관리자 계정이 Detective 관리자 계정인 조직 동작 그래프를 모두 삭제합니다. 조직 관리 계정을 Detective 관리자 계정으로 사용하는 조직 동작 그래프는 영향을 받지 않습니다.

Detective 관리자 계정을 구성하는 데 필요한 권한

조직 관리 계정이 Detective 관리자 계정을 구성할 수 있도록 하기 위해 `AmazonDetectiveOrganizationsAccess` 관리형 정책을 AWS Identity and Access Management(IAM) 엔티티에 연결할 수 있습니다.

Detective 관리자 계정 지정(콘솔)

조직 관리 계정은 Detective 콘솔을 사용하여 Detective 관리자 계정을 지정합니다.

Detective 관리자 계정을 관리하기 위해 Detective를 활성화할 필요는 없습니다. Detective 관리자 계정은 Detective 활성화 페이지에서 관리할 수 있습니다.

Detective 관리자 계정 지정(Detective 활성화 페이지)

1. https://console.aws.amazon.com/detective/에서 Amazon Detective 콘솔을 엽니다.
2. 시작하기를 선택합니다.
3. 관리자 계정에 필요한 권한 패널에서 선택한 계정에 필요한 권한을 부여하여 해당 계정이 Detective의 모든 작업에 대한 전체 액세스 권한을 가진 Detective 관리자로 운영할 수 있도록 합니다. 관리자로 운영하려면 보안 주체에 `AmazonDetectiveFullAccess` 정책을 연결하는 것이 좋습니다.
4. IAM 콘솔에서 직접 권장 정책을 보려면 IAM에서 정책 연결을 선택합니다.
5. IAM 콘솔에서 권한이 있는지 여부에 따라 다음과 같이 진행합니다.
   - IAM 콘솔에서 운영할 권한이 있는 경우 Detective에 사용하는 보안 주체에 권장 정책을 연결합니다.
   - IAM 콘솔에서 작업할 수 있는 권한이 없는 경우 정책의 Amazon 리소스 이름(ARN)을 복사하여 IAM 관리자에게 제공합니다. 그러면 담당자가 사용자를 대신하여 정책을 연결할 수 있습니다.
6. Detective 관리자에서 Detective 관리자 계정을 선택합니다.

   사용 가능한 옵션은 Organizations의 Detective 관리자 계정을 위임했는지 여부에 따라 달라집니다.

   - Organizations의 Detective에 대한 위임된 관리자 계정이 없는 경우 계정의 계정 식별자를 입력하여 Detective 관리자 계정으로 지정합니다.

     수동 초대 프로세스의 기존 관리자 계정 및 동작 그래프가 있을 수 있습니다. 있는 경우 해당 계정을 Detective 관리자 계정으로 지정하는 것이 좋습니다.

     Amazon GuardDuty용 Organizations, AWS Security Hub 또는 Amazon Macie에 위임된 관리자 계정이 있는 경우 Detective는 해당 계정 중 하나를 선택하라는 메시지를 표시합니다. 다른 계정을 입력할 수도 있습니다.

- Organizations의 Detective에 대한 위임된 관리자 계정이 있는 경우 해당 계정 또는 사용자 계정을 선택하라는 메시지가 표시됩니다. 모든 리전에 위임된 관리자 계정을 선택하는 것을 권장합니다.

7. 위임(Delegate)을 선택합니다.

Detective를 활성화했거나 기존 동작 그래프의 멤버 계정인 경우 일반 페이지에서 Detective 관리자 계정을 지정할 수 있습니다.

Detective 관리자 계정 지정(일반 페이지)

1. https://console.aws.amazon.com/detective/에서 Amazon Detective 콘솔을 엽니다.
2. Detective 탐색 창의 설정 아래에서 일반을 선택합니다.
3. 관리형 정책 패널에서 Detective가 지원하는 모든 관리형 정책에 대해 자세히 알아볼 수 있습니다. Detective에서 사용자가 수행하기를 원하는 작업에 따라 계정에 필요한 권한을 부여할 수 있습니다. 관리자로 운영하려면 보안 주체에 `AmazonDetectiveFullAccess` 정책을 연결하는 것이 좋습니다.
4. IAM 콘솔에서 권한이 있는지 여부에 따라 다음과 같이 진행합니다.

   - IAM 콘솔에서 운영할 권한이 있는 경우 Detective에 사용하는 보안 주체에 권장 정책을 연결합니다.
   - IAM 콘솔에서 작업할 수 있는 권한이 없는 경우 정책의 Amazon 리소스 이름(ARN)을 복사하여 IAM 관리자에게 제공합니다. 그러면 담당자가 사용자를 대신하여 정책을 연결할 수 있습니다.

   사용 가능한 옵션은 Organizations의 Detective 관리자 계정을 위임했는지 여부에 따라 달라집니다.

   - Organizations의 Detective에 대한 위임된 관리자 계정이 없는 경우 계정의 계정 식별자를 입력하여 Detective 관리자 계정으로 지정합니다.

     수동 초대 프로세스의 기존 관리자 계정 및 동작 그래프가 있을 수 있습니다. 있는 경우 해당 계정을 Detective 관리자 계정으로 지정하는 것이 좋습니다.

     Amazon GuardDuty용 Organizations, AWS Security Hub 또는 Amazon Macie에 위임된 관리자 계정이 있는 경우 Detective는 해당 계정 중 하나를 선택하라는 메시지를 표시합니다. 다른 계정을 입력할 수도 있습니다.

- Organizations의 Detective에 대한 위임된 관리자 계정이 있는 경우 해당 계정 또는 사용자 계정을 선택하라는 메시지가 표시됩니다. 모든 리전에 위임된 관리자 계정을 선택하는 것을 권장합니다.

5. 위임(Delegate)을 선택합니다.

Detective 관리자 계정 지정(Detective API, AWS CLI)

Detective 관리자 계정을 지정하기 위해 API 직접 호출 또는 AWS Command Line Interface를 사용할 수 있습니다. 조직 관리 계정 보안 인증 정보를 사용해야 합니다.

조직에 Detective에 대한 위임된 관리자 계정이 이미 있는 경우 해당 계정 또는 사용자 계정을 선택해야 합니다. 위임된 관리자 계정을 선택하는 것이 좋습니다.

Detective 관리자 계정 지정(Detective API, AWS CLI)

- Detective API: `EnableOrganizationAdminAccount` 작업을 사용합니다. Detective 관리자 계정의 AWS 계정 식별자를 제공해야 합니다. 계정 식별자를 얻으려면 `ListOrganizationAdminAccounts` 작업을 사용합니다.
- AWS CLI: 명령줄에서 `enable-organization-admin-account` 명령을 실행합니다.

```
aws detective enable-organization-admin-account --account-id <admin account ID>
```

예

```
aws detective enable-organization-admin-account --account-id 777788889999
```

Detective 관리자 계정 제거(콘솔)

Detective 관리자 계정은 Detective 콘솔에서 제거할 수 있습니다.

Detective 관리자 계정을 제거하면 해당 계정에 대해 Detective가 비활성화되고 조직 동작 그래프가 삭제됩니다. Detective 관리자 계정은 현재 리전에서만 제거됩니다.

> **Important**
>
> Detective 관리자 계정을 제거해도 Organizations의 위임된 관리자 계정에는 영향을 미치지 않습니다.

Detective 관리자 계정을 제거(Detective 활성화 페이지)

1. https://console.aws.amazon.com/detective/에서 Amazon Detective 콘솔을 엽니다.
2. 시작하기를 선택합니다.
3. 위임된 관리자에서 Amazon Detective 비활성화를 선택합니다.
4. 확인 대화 상자에서 **disable**을 입력한 다음 Amazon Detective 비활성화를 선택합니다.

Detective 관리자 계정 제거(일반 페이지)

1. https://console.aws.amazon.com/detective/에서 Amazon Detective 콘솔을 엽니다.
2. Detective 탐색 창의 설정 아래에서 일반을 선택합니다.
3. 위임된 관리자에서 Amazon Detective 비활성화를 선택합니다.
4. 확인 대화 상자에서 **disable**을 입력한 다음 Amazon Detective 비활성화를 선택합니다.

Detective 관리자 계정 제거(Detective API, AWS CLI)

Detective 관리자 계정을 제거하기 위해 API 직접 호출 또는 AWS CLI를 사용할 수 있습니다. 조직 관리 계정 보안 인증 정보를 사용해야 합니다.

Detective 관리자 계정을 제거하면 해당 계정에 대해 Detective가 비활성화되고 조직 동작 그래프가 삭제됩니다.

> **Important**
>
> Detective 관리자 계정을 제거해도 Organizations의 위임된 관리자 계정에는 영향을 미치지 않습니다.

Detective 관리자 계정 제거(Detective API, AWS CLI)

- Detective API: `DisableOrganizationAdminAccount` 작업을 사용합니다.

  Detective API를 사용하여 Detective 관리자 계정을 제거하면 API 직접 호출 또는 명령이 실행된 리전에서만 해당 계정이 제거됩니다.
- AWS CLI: 명령줄에서 `disable-organization-admin-account` 명령을 실행합니다.

```
aws detective disable-organization-admin-account
```

위임된 관리자 계정 제거하기 (조직 API, AWS CLI)

Detective 관리자 계정을 제거해도 Organizations의 위임된 관리자 계정은 자동으로 제거되지 않습니다. Detective의 위임된 관리자 계정을 제거하기 위해 Organizations API를 사용할 수 있습니다.

위임된 관리자 계정을 제거하면 위임된 관리자 계정이 Detective 관리자 계정인 조직 동작 그래프가 모두 삭제됩니다. 또한 해당 리전의 계정에 대해 Detective를 비활성화합니다.

위임된 관리자 계정 제거(Organizations API, AWS CLI)

- 조직 API: `DeregisterDelegatedAdministrator` 작업을 사용합니다. Detective 관리자 계정의 계정 식별자 및 Detective의 서비스 보안 주체인 `detective.amazonaws.com`을 제공해야 합니다.
- AWS CLI: 명령줄에서 `deregister-delegated-administrator` 명령을 실행합니다.

```
aws organizations deregister-delegated-administrator --account-id <Detective
 administrator account ID> --service-principal <Detective service principal>
```

예

```
aws organizations deregister-delegated-administrator --account-id 777788889999 --
service-principal detective.amazonaws.com
```

계정 목록 보기

관리자 계정은 Detective 콘솔 또는 API를 사용하여 계정 목록을 볼 수 있습니다. 목록에는 다음을 포함할 수 있습니다.

- 동작 그래프에 조인하도록 관리자 계정이 초대한 계정. 이러한 계정에는 초대별 유형이 있습니다.
- 조직 동작 그래프의 경우 조직의 모든 계정. 이러한 계정에는 조직별 유형이 있습니다.

초대를 거부했거나 관리자 계정이 동작 그래프에서 제거한 초대된 멤버 계정은 결과에 포함되지 않습니다. 다음 상태의 계정만 포함됩니다.

확인 진행 중

초대된 계정의 경우 Detective는 초대를 보내기 전에 계정 이메일 주소를 확인합니다.

조직 계정의 경우 Detective는 해당 계정이 조직에 속하는지 확인합니다. Detective는 해당 계정을 활성화한 계정이 Detective 관리자 계정인지도 확인합니다.

확인 실패

확인 실패 초대가 전송되지 않았거나 조직 계정이 멤버으로 활성화되지 않았습니다.

초대됨

초대된 계정의 경우. 초대를 보냈지만 멤버 계정이 아직 응답하지 않았습니다.

멤버가 아님

조직 동작 그래프의 조직 계정의 경우. 조직 계정이 현재 멤버 계정이 아닙니다. 조직 동작 그래프에 데이터를 제공하지 않습니다.

활성화됨

초대된 계정의 경우 멤버 계정이 초대를 수락하고 동작 그래프에 데이터를 제공합니다.

조직 동작 그래프의 조직 계정의 경우 Detective 관리자 계정을 통해 해당 계정을 멤버 계정으로 활성화했습니다. 이 계정은 조직 동작 그래프에 데이터를 제공합니다.

활성화되지 않음

초대된 계정의 경우, 멤버 계정이 초대를 수락했지만 활성화할 수는 없습니다.

조직 동작 그래프에 있는 조직 계정의 경우 Detective 관리자 계정이 해당 계정을 활성화하려고 했지만 활성화할 수 없습니다.

초대된 계정의 경우 Detective는 회원 계정 수를 확인합니다. 동작 그래프의 최대 멤버 계정 수는 1,200개입니다. 행동 그래프에 이미 1,200개의 회원 계정이 있는 경우 새 계정을 활성화할 수 없습니다.

Detective는 데이터 볼륨이 Detective 할당량 내에 있는지 확인합니다. 동작 그래프에 입력되는 데이터의 볼륨은 Detective에서 허용하는 최대값보다 작아야 합니다. 현재 수집된 볼륨이 Behavior 그래프 데이터 볼륨의 일일 한도인 10TB를 초과하는 경우 Detective에서는 추가 회원 계정을 추가할 수 없습니다.

계정 목록 작성(콘솔)

를 AWS Management Console 사용하여 계정 목록을 보고 필터링할 수 있습니다.

계정 목록 표시(콘솔)

1. AWS Management Console에 로그인합니다. 그런 다음 https://console.aws.amazon.com/detective/에서 Detective 콘솔을 엽니다.
2. Detective 탐색 창에서 계정 관리를 선택합니다.

   멤버 계정 목록에는 다음 계정이 포함됩니다.

   - 사용자 계정
   - 동작 그래프에 데이터를 제공하도록 초대한 계정
   - 조직 동작 그래프의 모든 조직 계정

   각 계정의 경우 목록에는 다음 정보가 표시됩니다.

   - AWS 계정 식별자.
   - 조직 계정의 경우, 계정 이름.
   - 계정 유형(초대별 또는 조직별).
   - 초대된 계정의 경우, 계정 루트 사용자 이메일 주소.
   - 계정 상태.
   - 계정의 일일 데이터 볼륨. Detective는 멤버 계정으로 활성화되지 않은 계정의 데이터 볼륨을 검색할 수 없습니다.
   - 계정 상태가 마지막으로 업데이트된 날짜.

테이블 상단의 탭을 사용하여 멤버 계정 상태를 기준으로 목록을 필터링할 수 있습니다. 각 탭에는 일치하는 멤버 계정 수가 표시됩니다.

- 모든 멤버 계정을 보려면 모두를 선택합니다.
- 활성화됨 상태인 계정을 보려면 활성화됨을 선택합니다.
- 활성화됨 외 상태의 계정을 보려면 활성화되지 않음을 선택합니다.

멤버 계정 목록에 다른 필터를 추가할 수도 있습니다.

동작 그래프의 계정 목록에 필터 추가(콘솔)

1. 필터 상자를 선택합니다.

2. 목록에서 필터에 사용할 열을 선택합니다.
3. 지정된 열에 대해 필터에 사용할 값을 선택합니다.
4. 필터를 제거하려면 오른쪽 상단에 있는 x 아이콘을 선택합니다.
5. 목록을 최신 상태 정보로 업데이트하려면 오른쪽 상단에 있는 새로 고침 아이콘을 선택합니다.

회원 계정 등록하기 (Detective API,) AWS CLI

API 호출 또는 를 사용하여 행동 그래프에서 회원 계정 목록을 볼 수 있습니다. AWS Command Line Interface

요청에 사용할 동작 그래프의 ARN을 가져오려면 `ListGraphs` 작업을 사용합니다.

회원 계정 목록을 검색하려면 (Detective API,) AWS CLI

- Detective API: `ListMembers` 작업을 사용합니다. 의도한 동작 그래프를 식별하려면 동작 그래프 ARN을 지정합니다.

  단, 조직 동작 그래프의 경우 `ListMembers`는 멤버 계정으로 활성화하지 않았거나 동작 그래프에서 연결 해제한 조직 계정을 반환하지 않습니다.
- AWS CLI: 명령줄에서 `list-members` 명령을 실행합니다.

```
aws detective list-members --graph-arn <behavior graph ARN>
```

예제

```
aws detective list-members --graph-arn arn:aws:detective:us-
east-1:111122223333:graph:123412341234
```

동작 그래프에서 특정 멤버 계정에 대한 세부 정보 검색(Detective API, AWS CLI)

- Detective API: `GetMembers` 작업을 사용합니다. 동작 그래프 ARN과 멤버 계정의 계정 식별자 목록을 지정합니다.
- AWS CLI: 명령줄에서 `get-members` 명령을 실행합니다.

```
aws detective get-members --account-ids <member account IDs> --graph-arn <behavior
 graph ARN>
```

예제

```
aws detective get-members --account-ids 444455556666 123456789012 --graph-arn
 arn:aws:detective:us-east-1:111122223333:graph:123412341234
```

조직 계정을 멤버 계정으로 관리

조직 동작 그래프에서 Detective 관리자 계정은 멤버 계정으로 활성화할 조직 계정을 결정합니다.

새 조직 계정을 멤버 계정으로 자동 활성화하도록 Detective를 구성하거나 조직 계정을 수동으로 활성화하도록 Detective를 구성할 수 있습니다.

Detective 관리자 계정은 조직 동작 그래프에서 조직 계정 연결을 해제할 수도 있습니다.

내용

새 조직 계정을 멤버 계정으로 자동 활성화

Detective 관리자 계정은 조직 동작 그래프에서 새 조직 계정을 멤버 계정으로 자동 활성화화도록 Detective를 구성할 수 있습니다.

조직에 새 계정을 추가하면 해당 계정이 계정 관리 페이지의 목록에 추가됩니다. 조직 계정의 경우 유형은 조직별입니다.

기본적으로 새 조직 계정은 멤버 계정으로 활성화되지 않습니다. 해당 멤버의 상태는 멤버가 아님입니다.

조직 계정을 자동으로 활성화하도록 선택하면 Detective는 새 계정이 조직에 추가될 때 새 계정을 멤버 계정으로 활성화하기 시작합니다. Detective는 아직 활성화되지 않은 기존 조직 계정을 활성화하지 않습니다.

Detective는 행동 그래프의 최대 구성원 계정 수가 1,200개인 경우에만 조직 계정을 구성원 계정으로 활성화할 수 있습니다. 동작 그래프에 이미 1,200개의 멤버 계정이 있는 경우 새 계정을 활성화할 수 없습니다.

Detective는 데이터 볼륨이 Detective 할당량 내에 있는지 확인합니다. 동작 그래프에 입력되는 데이터의 볼륨은 Detective에서 허용하는 최대값보다 작아야 합니다. 현재 수집된 볼륨이 하루 한도인 10TB를 초과하는 경우 계정을 더 추가할 수 없으며 Detective는 추가 데이터 수집을 비활성화합니다.

새 조직 계정 자동 활성화(콘솔)

계정 관리 페이지의 새 조직 계정 자동 활성화 설정은 조직에 계정을 추가할 때 계정을 자동으로 활성화할지 여부를 결정합니다.

새 조직 계정을 멤버 계정으로 자동 활성화

1. https://console.aws.amazon.com/detective/에서 Amazon Detective 콘솔을 엽니다.
2. Detective 탐색 창에서 계정 관리를 선택합니다.
3. 새 조직 계정 자동 활성화 상태로 전환합니다.

새 조직 계정을 자동으로 활성화하기 (Detective API,) AWS CLI

관리자 계정은 Detective API 또는 AWS Command Line Interface를 사용하여 새 조직 계정을 멤버 계정으로 자동 활성화할지 여부를 결정할 수 있습니다.

구성을 보고 관리하려면 동작 그래프 ARN을 제공해야 합니다. ARN을 가져오려면 `ListGraphs` 작업을 사용합니다.

조직 계정 자동 활성화를 위한 현재 구성 보기

- Detective API: `DescribeOrganizationConfiguration` 작업을 사용합니다.

  응답에서 새 조직 계정이 자동 활성화되면 `AutoEnable`은 `true`입니다.
- AWS CLI: 명령줄에서 `describe-organization-configuration` 명령을 실행합니다.

```
aws detective describe-organization-configuration --graph-arn <behavior graph ARN>
```

예

```
aws detective describe-organization-configuration --graph-arn arn:aws:detective:us-east-1:111122223333:graph:123412341234
```

새 조직 계정 자동 활성화

- Detective API: UpdateOrganizationConfiguration 작업을 사용합니다. 새 조직 계정을 자동 활성화하려면 AutoEnable을 true로 설정합니다.
- AWS CLI: 명령줄에서 update-organization-configuration 명령을 실행합니다.

```
aws detective update-organization-configuration --graph-arn <behavior graph ARN> --
auto-enable | --no-auto-enable
```

예

```
aws detective update-organization-configuration --graph-arn arn:aws:detective:us-
east-1:111122223333:graph:123412341234 --auto-enable
```

조직 계정을 멤버 계정으로 활성화

자동으로 새 조직 계정을 자동으로 활성화하지 않는 경우 해당 계정을 수동으로 활성화할 수 있습니다. 또한 연결을 해제한 계정도 수동으로 활성화해야 합니다.

계정 활성화 여부 결정

조직 동작 그래프에 이미 최대 1,200개의 활성 계정이 있는 경우 조직 계정을 멤버 계정으로 활성화할 수 없습니다. 이 경우 조직 계정 상태는 멤버가 아님으로 유지됩니다. 계정은 동작 그래프에 데이터를 제공하지 않습니다.

멤버 계정을 활성화할 수 있게 되면 Detective는 자동으로 멤버 계정 상태를 활성화됨으로 변경합니다. 예를 들어 관리자 계정이 계정을 위한 공간을 확보하기 위해 다른 구성원 계정을 제거하면 구성원 계정 상태가 활성화됨으로 변경됩니다.

조직 계정을 멤버 계정으로 활성화(콘솔)

계정 관리 페이지에서 조직 계정을 멤버 계정으로 활성화할 수 있습니다.

조직 계정을 멤버 계정으로 활성화

1. https://console.aws.amazon.com/detective/에서 Amazon Detective 콘솔을 엽니다.
2. Detective 탐색 창에서 계정 관리를 선택합니다.
3. 현재 활성화되지 않은 계정 목록을 보려면 활성화되지 않음을 선택합니다.

4. 특정 조직 계정을 선택하거나 모든 조직 계정을 활성화할 수 있습니다.

   선택한 조직 계정 활성화

   a. 활성화하려는 각 조직 계정을 선택합니다.
   b. 계정 활성화를 선택합니다.

   모든 조직 계정을 활성화하려면 모든 조직 계정 활성화를 선택합니다.

조직 계정을 구성원 계정으로 활성화 (Detective API,) AWS CLI

Detective API 또는 를 사용하여 조직 행동 그래프에서 조직 계정을 구성원 계정으로 AWS Command Line Interface 활성화할 수 있습니다. 요청에 사용할 동작 그래프의 ARN을 가져오려면 `ListGraphs` 작업을 사용합니다.

조직 계정을 구성원 계정으로 활성화하려면 (Detective API,) AWS CLI

- Detective API: `CreateMembers` 작업을 사용합니다. 그래프 ARN을 제공해야 합니다.

  각 계정에 대해 계정 식별자를 지정합니다. 조직 동작 그래프의 조직 계정은 초대를 받지 않습니다. 이메일 주소 또는 기타 초대 정보는 제공할 필요가 없습니다.
- AWS CLI: 명령줄에서 `create-members` 명령을 실행합니다.

```
aws detective create-members --accounts AccountId=<AWS account ID> --graph-
arn <behavior graph ARN>
```

예

```
aws detective create-members --accounts AccountId=444455556666 AccountId=123456789012
 --graph-arn arn:aws:detective:us-east-1:111122223333:graph:123412341234
```

조직 계정을 멤버 계정과 연결 해제

조직 동작 그래프에서 조직 계정의 데이터 수집을 중지하기 위해 계정 연결을 해제할 수 있습니다. 해당 계정의 기존 데이터는 동작 그래프에 그대로 남아 있습니다.

조직 계정 연결을 해제하면 상태가 멤버가 아님으로 변경됩니다. Detective는 해당 계정의 데이터 수집을 중지하지만 계정은 목록에 남아 있습니다.

조직 계정 연결 해제(콘솔)

계정 관리 페이지에서 조직 계정을 멤버 계정 연결과 해제할 수 있습니다.

1. https://console.aws.amazon.com/detective/에서 Amazon Detective 콘솔을 엽니다.
2. Detective 탐색 창에서 계정 관리를 선택합니다.
3. 활성화된 계정 목록을 표시하려면 활성화됨을 선택합니다.
4. 연결을 해제할 각 계정의 확인란을 선택합니다.
5. 작업을 선택합니다. 그런 다음 계정 비활성화를 선택합니다.

   연결이 해제된 계정의 계정 상태가 멤버가 아님으로 변경됩니다.

조직 계정 연결 끊기 (Detective API,) AWS CLI

Detective API 또는 를 사용하여 행동 그래프에서 조직 계정을 구성원 계정과 AWS Command Line Interface 분리할 수 있습니다.

요청에 사용할 동작 그래프의 ARN을 가져오려면 `ListGraphs` 작업을 사용합니다.

조직 동작 그래프에서 조직 계정 연결 해제(Detective API, AWS CLI)

- Detective API: `DeleteMembers` 작업을 사용합니다. 연결을 해제할 멤버 계정의 그래프 ARN과 계정 식별자 목록을 지정합니다.
- AWS CLI: 명령줄에서 `delete-members` 명령을 실행합니다.

```
aws detective delete-members --account-ids <account ID list> --graph-arn <behavior
 graph ARN>
```

예

```
aws detective delete-members --account-ids 444455556666 123456789012 --graph-arn
 arn:aws:detective:us-east-1:111122223333:graph:123412341234
```

초대된 멤버 계정 관리

관리자 계정은 동작 그래프에서 계정을 멤버 계정으로 초대할 수 있습니다. 멤버 계정이 초대를 수락하고 활성화되면 Amazon Detective는 멤버 계정의 데이터를 수집하고 해당 동작 그래프로 추출하기 시작합니다.

조직 동작 그래프 이외의 동작 그래프의 경우 모든 멤버 계정은 초대된 계정입니다.

Detective 관리자 계정은 조직 계정이 아닌 계정을 조직 동작 그래프에 초대할 수도 있습니다.

관리자 계정의 동작 그래프에서 초대된 멤버 계정을 제거할 수 있습니다.

내용

동작 그래프에 멤버 계정 초대

관리자 계정은 계정을 초대하여 동작 그래프에 제공할 수 있습니다. 동작 그래프에는 최대 1,200개의 멤버 계정이 포함될 수 있습니다.

상위 수준에서 동작 그래프에 제공하도록 계정을 초대하는 프로세스는 다음과 같습니다.

1. 추가할 각 구성원 계정에 대해 관리자 계정은 AWS 계정 식별자와 루트 사용자 이메일 주소를 제공합니다.
2. Detective는 이메일 주소가 계정의 루트 사용자 이메일 주소인지 확인합니다. 계정 정보가 유효하면 Detective는 멤버 계정으로 초대를 보냅니다.

   Detective는 다음 지역의 회원 계정에 이 검증을 수행하거나 이메일 초대장을 보내지 않습니다.

   - AWS GovCloud (미국 동부) 지역
   - AWS GovCloud (미국 서부) 지역

   다른 지역의 경우 Detective API CreateMembers작업을 `DisableEmailNotification` 사용할 수 있습니다. 를 true로 설정하면 `DisableEmailNotification` Detective는 멤버 계정으로 초대를 보내지 않습니다. 중앙에서 관리되는 계정에 유용한 설정입니다.
3. 멤버 계정은 초대를 수락 또는 거부합니다.

관리자 계정이 초대 이메일을 보내지 않더라도 멤버 계정은 초대에 응답해야 합니다.

4. 멤버 계정이 초대를 수락하면 Detective는 멤버 계정의 데이터를 행동 그래프로 수집하기 시작합니다.
5. 멤버 계정을 활성화할 수 있게 되면 Detective는 자동으로 멤버 계정 상태를 활성화됨으로 변경합니다.

   예를 들어 관리자 계정이 계정을 위한 공간을 확보하기 위해 다른 구성원 계정을 제거하면 구성원 계정 상태가 활성화됨으로 변경됩니다.

   둘 이상의 계정이 활성화되지 않음 상태인 경우 Detective는 초대된 순서대로 계정을 활성화합니다. 활성화되지 않음 상태의 계정을 활성화할지 여부를 확인하는 프로세스가 1시간마다 실행됩니다.

   또한 관리자 계정은 자동 프로세스를 기다리지 않고 수동으로 계정을 활성화할 수 있습니다. 예를 들어 관리자 계정은 활성화할 계정을 선택하려고 할 수 있습니다. the section called “활성화되지 않은 멤버 계정 활성화” 섹션을 참조하십시오.

   참고로 Detective는 2021년 5월 12일부터 활성화되지 않음 상태의 계정을 자동으로 활성화하기 시작했습니다. 이전에 활성화되지 않음 상태의 계정은 자동으로 활성화되지 않습니다. 관리자 계정이 수동으로 활성화해야 합니다.

동작 그래프에 개별 계정 초대(콘솔)

동작 그래프에 데이터를 제공하도록 초대할 멤버 계정을 수동으로 지정할 수 있습니다.

초대할 멤버 계정 수동으로 선택(콘솔)

1. https://console.aws.amazon.com/detective/에서 Amazon Detective 콘솔을 엽니다.
2. Detective 탐색 창에서 계정 관리를 선택합니다.
3. 작업을 선택합니다. 그런 당므 계정 초대를 선택합니다.
4. 계정 추가에서 개별 계정 추가를 선택합니다.
5. 초대 목록에 멤버 계정을 추가하려면 다음 단계를 수행합니다.

   a. 계정 추가를 선택합니다.

   b. AWS 계정 ID에는 AWS 계정 ID를 입력합니다.

   c. 이메일 주소에 계정의 루트 사용자 이메일 주소를 입력합니다.
6. 목록에서 계정을 제거하려면 해당 계정에 대해 제거를 선택합니다.

7. 초대 이메일 개인화에서 초대 이메일에 포함할 사용자 지정 콘텐츠를 추가합니다.

   예를 들어 이 영역을 사용하여 연락처 정보를 제공할 수 있습니다. 또는 이를 사용하여 멤버 계정에 필요한 IAM 정책을 사용자 또는 역할에 연결해야 초대를 수락할 수 있음을 알릴 수 있습니다.
8. 멤버 계정 IAM 정책에는 멤버 계정에 필요한 IAM 정책 텍스트가 포함되어 있습니다. 이메일 초대에는 이 정책 텍스트가 포함되어 있습니다. 정책 텍스트를 복사하려면 복사를 선택합니다.
9. [Invite]를 선택합니다.

멤버 계정 목록을 동작 그래프에 초대(콘솔)

Detective 콘솔에서 동작 그래프에 초대할 멤버 계정 목록이 포함된 `.csv` 파일을 제공할 수 있습니다.

파일의 첫 번째 행은 헤더 행입니다. 그러면 각 계정이 별도의 행에 나열됩니다. 각 구성원 계정 항목에는 AWS 계정 ID와 계정의 루트 사용자 이메일 주소가 포함됩니다.

예제

```
Account ID,Email address
111122223333,srodriguez@example.com
444455556666,rroe@example.com
```

계정 상태가 확인 실패가 아닌 한 Detective는 파일을 처리할 때 이미 초대된 계정을 무시합니다. 이 상태는 계정에 제공된 이메일 주소가 계정의 루트 사용자 이메일 주소와 일치하지 않았음을 나타냅니다. 이 경우 Detective는 원래 초대장을 삭제하고 이메일 주소를 확인하고 초대장을 보내려고 다시 시도합니다.

이 옵션은 계정 목록을 생성하는 데 사용할 수 있는 템플릿도 제공합니다.

.csv 목록에서 멤버 계정 초대(콘솔)

1. https://console.aws.amazon.com/detective/에서 Amazon Detective 콘솔을 엽니다.
2. Detective 탐색 창에서 계정 관리를 선택합니다.
3. 작업을 선택합니다. 그런 당므 계정 초대를 선택합니다.
4. 계정 추가에서 .csv에서 추가를 선택합니다.
5. 작업할 템플릿 파일을 다운로드하려면 .csv 템플릿 다운로드를 선택합니다.
6. 계정 목록이 포함된 파일을 선택하려면 .csv 파일 선택을 선택합니다.
7. 멤버 계정 검토에서 Detective가 파일에서 찾은 멤버 계정 목록을 확인합니다.
8. 초대 이메일 개인화에서 초대 이메일에 포함할 사용자 지정 콘텐츠를 추가합니다.

예를 들어 연락처 정보를 제공하거나 멤버 계정에 필요한 IAM 정책을 상기시킬 수 있습니다.

9. 멤버 계정 IAM 정책에는 멤버 계정에 필요한 IAM 정책 텍스트가 포함되어 있습니다. 이메일 초대에는 이 정책 텍스트가 포함되어 있습니다. 정책 텍스트를 복사하려면 복사를 선택합니다.
10. [Invite]를 선택합니다.

행동 그래프에 회원 계정 초대 (Detective API,) AWS CLI

Detective API 또는 를 사용하여 회원 계정을 초대하여 행동 그래프에 데이터를 제공할 수 있습니다. AWS Command Line Interface 요청에 사용할 동작 그래프의 ARN을 가져오려면 `ListGraphs` 작업을 사용합니다.

회원 계정을 행동 그래프에 초대하려면 (Detective API,) AWS CLI

- Detective API: `CreateMembers` 작업을 사용합니다. 그래프 ARN을 제공해야 합니다. 각 계정에 대해 계정 식별자와 루트 사용자 이메일 주소를 지정합니다.

  멤버 계정에 초대 이메일을 보내지 않으려면 `DisableEmailNotification`을 true로 설정합니다. 기본적으로 `DisableEmailNotification`은 false입니다.

  초대 이메일을 보내는 경우 초대 이메일에 추가할 사용자 지정 텍스트를 선택적으로 제공할 수 있습니다.
- AWS CLI: 명령줄에서 `create-members` 명령을 실행합니다.

```
aws detective create-members --accounts AccountId=<AWS account ID>,EmailAddress=<root
 user email address> --graph-arn <behavior graph ARN> --message "<Custom message
 text>"
```

예

```
aws detective create-members --accounts
 AccountId=444455556666,EmailAddress=mmajor@example.com
 AccountId=123456789012,EmailAddress=jstiles@example.com --graph-arn
 arn:aws:detective:us-east-1:111122223333:graph:123412341234 --message "This is Paul
 Santos. I need to add your account to the data we use for security investigation in
 Amazon Detective. If you have any questions, contact me at psantos@example.com."
```

멤버 계정에 초대 이메일을 보내지 않도록 지정하려면 `--disable-email-notification`을 포함합니다.

```
aws detective create-members --accounts AccountId=<AWS account ID>,EmailAddress=<root
 user email address> --graph-arn <behavior graph ARN> --disable-email-notification
```

예

```
aws detective create-members --accounts
 AccountId=444455556666,EmailAddress=mmajor@example.com
 AccountId=123456789012,EmailAddress=jstiles@example.com --graph-arn
 arn:aws:detective:us-east-1:111122223333:graph:123412341234 --disable-email-
notification
```

지역 간 회원 계정 목록 추가 (Python 스크립트 사용 GitHub)

Detective는 다음과 같은 작업을 수행할 수 GitHub 있는 오픈 소스 스크립트를 제공합니다.

- 지정된 리전 목록 전반에서 관리자 계정의 동작 그래프에 지정된 멤버 계정 목록을 추가합니다.
- 관리자 계정의 리전에 동작 그래프가 없는 경우 스크립트는 또한 Detective를 활성화하고 해당 리전에 동작 그래프를 생성합니다.
- 멤버 계정에 초대 이메일을 전송합니다.
- 멤버 계정에 대한 초대를 자동으로 수락합니다.

GitHub 스크립트 구성 및 사용 방법에 대한 자세한 내용은 을 참조하십시오. Amazon Detective Python 스크립트 사용

활성화되지 않은 멤버 계정 활성화

멤버 계정이 초대를 수락하면 Amazon Detective는 멤버 계정 수를 확인합니다. 동작 그래프의 최대 멤버 계정 수는 1,200개입니다. 동작 그래프에 이미 1,200개의 멤버 계정이 있는 경우 새 계정을 활성화할 수 없습니다. Detective에서 멤버 계정을 활성화할 수 없는 경우 멤버 계정 상태를 활성화되지 않음으로 설정합니다.

활성화되지 않음 상태의 멤버 계정은 동작 그래프에 데이터를 제공하지 않습니다.

Detective는 동작 그래프가 계정을 수용할 수 있도록 계정을 자동으로 활성화합니다.

활성화되지 않음 상태의 멤버 계정을 수동으로 활성화할 수도 있습니다. 예를 들어 기존 멤버 계정을 제거하여 데이터 볼륨을 줄일 수 있습니다. 계정이 활성화되는 자동 프로세스를 기다리는 대신 활성화되지 않음 상태의 멤버 계정을 활성화해 볼 수 있습니다.

활성화되지 않은 멤버 계정 활성화

멤버 계정 목록에는 활성화되지 않음 상태의 멤버 계정을 선택하여 활성화할 수 있는 옵션이 포함되어 있습니다.

활성화되지 않은 멤버 계정 활성화

1. https://console.aws.amazon.com/detective/에서 Amazon Detective 콘솔을 엽니다.
2. Detective 탐색 창에서 계정 관리를 선택합니다.
3. 내 멤버 계정에서 활성화할 각 멤버 계정의 확인란을 선택합니다.

   활성화되지 않음 상태인 멤버 계정만 활성화할 수 있습니다.
4. 계정 활성화를 선택합니다.

Detective는 멤버 계정을 활성화할 수 있는지 여부를 결정합니다. 멤버 계정을 활성화할 수 있는 경우 상태가 활성화됨으로 변경됩니다.

활성화되지 않은 멤버 계정 활성화 (Detective API,) AWS CLI

API 호출 또는 를 사용하여 활성화되지 않은 단일 회원 계정을 AWS Command Line Interface 활성화할 수 있습니다. 요청에 사용할 동작 그래프의 ARN을 가져오려면 `ListGraphs` 작업을 사용합니다.

활성화되지 않은 멤버 계정 활성화

- Detective API: `StartMonitoringMember` API 작업을 사용합니다. 동작 그래프 ARN을 제공해야 합니다. 멤버 계정을 식별하려면 AWS 계정 식별자를 사용하십시오.
- AWS CLI: 명령줄에서 `start-monitoring-member` 명령을 실행합니다.

```
start-monitoring-member --graph-arn <behavior graph ARN> --account-id <AWS account
 ID>
```

예:

```
start-monitoring-member --graph-arn arn:aws:detective:us-
east-1:111122223333:graph:123412341234 --account-id 444455556666
```

동작 그래프에서 초대된 멤버 계정 제거

관리자 계정의 동작 그래프에서 멤버 계정을 언제든지 제거할 수 있습니다.

Detective는 AWS GovCloud (미국 동부) 및 AWS GovCloud (미국 서부 AWS) 지역을 제외하고 해지된 회원 계정을 자동으로 제거합니다.

초대된 멤버 계정이 동작 그래프에서 제거되면 다음과 같은 상황이 발생합니다.

- 멤버 계정이 내 멤버 계정에서 제거됩니다.
- Amazon Detective는 제거된 계정의 데이터 수집을 중단합니다.

Detective는 멤버 계정 전체의 데이터를 집계하는 동작 그래프에서 기존 데이터를 제거하지 않습니다.

동작 그래프에서 초대된 멤버 계정 제거(콘솔)

를 사용하여 행동 그래프에서 초대된 AWS Management Console 회원 계정을 제거할 수 있습니다.

멤버 계정 제거(콘솔)

1. https://console.aws.amazon.com/detective/에서 Amazon Detective 콘솔을 엽니다.
2. Detective 탐색 창에서 계정 관리를 선택합니다.
3. 계정 목록에서 제거할 각 멤버 계정의 확인란을 선택합니다.

   목록에서 자신의 계정은 제거할 수 없습니다.
4. 작업을 선택합니다. 그런 다음 계정 비활성화를 선택합니다.

행동 그래프에서 초대된 회원 계정 제거 (Detective API,) AWS CLI

Detective API 또는 를 사용하여 행동 그래프에서 AWS Command Line Interface 초대된 회원 계정을 제거할 수 있습니다. 요청에 사용할 동작 그래프의 ARN을 가져오려면 `ListGraphs` 작업을 사용합니다.

행동 그래프에서 초대된 회원 계정을 제거하려면 (Detective API,) AWS CLI

- Detective API: `DeleteMembers` 작업을 사용합니다. 그래프 ARN 및 제거할 멤버 계정의 계정 식별자 목록을 지정합니다.
- AWS CLI: 명령줄에서 `delete-members` 명령을 실행합니다.

```
aws detective delete-members --account-ids <account ID list> --graph-arn <behavior
 graph ARN>
```

예제

```
aws detective delete-members --account-ids 444455556666 123456789012 --graph-arn
 arn:aws:detective:us-east-1:111122223333:graph:123412341234
```

여러 지역에서 초대된 회원 계정 목록 제거 (Python 스크립트 사용 GitHub)

Detective는 오픈 소스 스크립트를 제공합니다. GitHub 이 스크립트를 사용하여 지정된 리전 목록에 대한 관리자 계정의 동작 그래프에서 지정된 멤버 계정 목록을 제거할 수 있습니다.

GitHub 스크립트 구성 및 사용 방법에 대한 자세한 내용은 을 참조하십시오. Amazon Detective Python 스크립트 사용

멤버 계정의 경우: 동작 그래프 초대 및 멤버십 관리

Amazon Detective는 기여하는 각 동작 그래프에 대해 수집된 데이터에 대해 각 멤버 계정에 요금을 부과합니다.

계정 관리 페이지에서는 멤버 계정이 자신이 속한 동작 그래프의 관리자 계정을 볼 수 있습니다.

동작 그래프에 초대된 멤버 계정은 초대를 보고 초대에 응답할 수 있습니다. 동작 그래프에서 계정을 제거할 수도 있습니다.

조직 동작 그래프의 경우 조직 계정은 해당 계정이 멤버 계정인지 여부를 제어할 수 없습니다. Detective 관리자 계정은 멤버 계정으로 활성화하거나 비활성화할 조직 계정을 선택합니다.

내용

- 멤버 계정의 필수 IAM 정책
- 동작 그래프 초대 목록 보기
- 동작 그래프 초대에 응답
- 동작 그래프에서 계정 제거

멤버 계정의 필수 IAM 정책

멤버 계정에서 초대를 보고 관리하려면 먼저 필수 IAM 정책을 보안 주체에 연결해야 합니다. 보안 주체는 기존 사용자 또는 역할일 수도 있고, Detective에 사용할 새 사용자 또는 역할을 만들 수도 있습니다.

관리자 계정에 IAM 관리자가 필수 정책을 연결하도록 하는 것이 가장 좋습니다.

멤버 계정 IAM 정책은 Amazon Detective에서의 멤버 계정 작업에 대한 액세스 권한을 부여합니다. 동작 그래프에 기여하라는 이메일 초대장에는 해당 IAM 정책의 텍스트가 포함되어 있습니다.

이 정책을 사용하려면 *<behavior graph ARN>*을 그래프 ARN으로 대체합니다.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "detective:AcceptInvitation",
        "detective:DisassociateMembership",
        "detective:RejectInvitation"
      ],
      "Resource": "<behavior graph ARN>"
    },
   {
    "Effect":"Allow",
    "Action":[
        "detective:BatchGetMembershipDatasources",
        "detective:GetFreeTrialEligibility",
        "detective:GetPricingInformation",
        "detective:GetUsageInformation",
        "detective:ListInvitations"
    ],
    "Resource":"*"
   }
 ]
}
```

단, 조직 동작 그래프의 조직 계정은 초대를 받지 않으므로 조직 동작 그래프에서 해당 계정을 분리할 수 없습니다. 다른 동작 그래프에 속하지 않는 경우에는 `ListInvitations` 권한만 있으면 됩니다. `ListInvitations`는 동작 그래프의 관리자 계정을 볼 수 있습니다. 초대를 관리하고 멤버십을 분리할 수 있는 권한은 초대를 통한 멤버십에만 적용됩니다.

동작 그래프 초대 목록 보기

Amazon Detective 콘솔, Detective API 또는 멤버 계정에서 행동 AWS Command Line Interface 그래프 초대를 볼 수 있습니다.

동작 그래프 초대 보기(콘솔)

에서 행동 그래프 초대를 볼 수 있습니다. AWS Management Console

동작 그래프 초대 보기(콘솔)

1. AWS Management Console에 로그인합니다. 그런 다음 https://console.aws.amazon.com/detective/에서 Detective 콘솔을 엽니다.
2. Detective 탐색 창에서 계정 관리를 선택합니다.

계정 관리 페이지의 내 관리자 계정에는 현재 리전에서 열려 있고 수락된 동작 그래프 초대가 포함되어 있습니다. 조직 계정의 경우 내 관리자 계정에는 조직 동작 그래프도 포함됩니다.

계정이 현재 무료 평가 기간 중이면 이 페이지에 무료 평가판 사용 기간이 남은 일수도 표시됩니다.

이 목록에는 거부한 초대, 탈퇴된 멤버십 또는 관리자 계정으로 제거된 멤버십이 포함되어 있지 않습니다.

각 초대에는 관리자 계정 번호, 초대를 수락한 날짜, 초대의 현재 상태가 표시됩니다.

- 응답하지 않은 초대의 경우 상태는 초대됨으로 표시됩니다.
- 수락한 초대의 상태는 활성화됨 또는 활성화되지 않음입니다.

  상태가 활성화됨 경우 계정이 동작 그래프에 데이터를 재공하는 것입니다.

  상태가 비활성화됨 경우 계정은 동작 그래프에 데이터를 제공하지 않습니다.

  사용자 계정으로 인해 행동 그래프가 Detective 할당량을 초과하지 않는 경우 Detective는 계정 상태를 Enabled로 업데이트합니다. 그렇지 않으면 상태가 활성화되지 않음으로 유지됩니다.

  동작 그래프가 계정의 데이터 볼륨을 수용할 수 있게 되면 Detective는 자동으로 해당 그래프를 활성화됨으로 업데이트합니다. 예를 들어 관리자 계정은 계정을 활성화하기 위해 다른 멤버 계정을 제거할 수 있습니다. 관리자 계정은 계정을 수동으로 활성화할 수도 있습니다.

동작 그래프 초대 보기(Detective API, AWS CLI)

Detective API 또는 AWS Command Line Interface에서 동작 그래프 초대를 나열할 수 있습니다.

동작 그래프에 대한 공개 및 수락된 초대의 목록 검색(Detective API, AWS CLI)

- Detective API: `ListInvitations` 작업을 사용합니다.
- AWS CLI: 명령줄에서 `list-invitations` 명령을 실행합니다.

```
aws detective list-invitations
```

동작 그래프 초대에 응답

초대를 수락하면 Detective가 회원 계정 수를 확인합니다. 동작 그래프의 최대 멤버 계정 수는 1,200개입니다. 동작 그래프에 이미 1,200개의 멤버 계정이 있는 경우 새 계정을 활성화할 수 없습니다.

초대를 수락하면 계정에서 Detective가 활성화됩니다. Detective는 데이터 볼륨이 Detective 할당량 내에 있는지 확인합니다. 동작 그래프에 입력되는 데이터의 볼륨은 Detective에서 허용하는 최대값보다 작아야 합니다. 현재 수집된 볼륨이 하루 한도인 10TB를 초과하는 경우 계정을 더 추가할 수 없으며 Detective는 추가 데이터 수집을 비활성화합니다. Detective 콘솔은 데이터 볼륨이 너무 커서 상태가 “사용 안 함”으로 남아 있음을 나타내는 알림을 표시합니다.

초대를 거부하면 초대 목록에서 제거되며 Detective는 동작 그래프에서 계정 데이터를 사용하지 않습니다.

동작 그래프 초대에 응답(콘솔)

를 사용하여 Detective 콘솔로 연결되는 링크가 포함된 이메일 초대에 응답할 수 있습니다. AWS Management Console 초대됨 상태인 초대에만 응답할 수 있습니다.

동작 그래프 초대에 응답(콘솔)

1. https://console.aws.amazon.com/detective/에서 Amazon Detective 콘솔을 엽니다.
2. Detective 탐색 창에서 계정 관리를 선택합니다.
3. 내 관리자 계정에서 초대를 수락하고 동작 그래프에 데이터를 제공하기 시작하려면 초대 수락을 선택합니다.

   초대를 거절하고 목록에서 제거하려면 거절을 선택합니다.

행동 그래프 초대에 대한 응답 (Detective API,) AWS CLI

Detective API 또는 AWS Command Line Interface에서 동작 그래프 초대에 응답할 수 있습니다.

행동 그래프 초대를 수락하려면 (Detective API,) AWS CLI

- Detective API: `AcceptInvitation` 작업을 사용합니다. 그래프 ARN을 지정해야 합니다.
- AWS CLI: 명령줄에서 `accept-invitation` 명령을 실행합니다.

```
aws detective accept-invitation --graph-arn <behavior graph ARN>
```

예제

```
aws detective accept-invitation --graph-arn arn:aws:detective:us-
east-1:111122223333:graph:123412341234
```

행동 그래프 초대를 거부하려면 (Detective API,) AWS CLI

- Detective API: `RejectInvitation` 작업을 사용합니다. 그래프 ARN을 지정해야 합니다.
- AWS CLI: 명령줄에서 `reject-invitation` 명령을 실행합니다.

```
aws detective reject-invitation --graph-arn <behavior graph ARN>
```

예제

```
aws detective reject-invitation --graph-arn arn:aws:detective:us-
east-1:111122223333:graph:123412341234
```

동작 그래프에서 계정 제거

초대를 수락한 후에는 언제든지 동작 그래프에서 계정을 제거할 수 있습니다. 동작 그래프에서 계정을 제거하면 Amazon Detective는 계정에서 동작 그래프로 데이터를 수집하는 것을 중지합니다. 기존 데이터는 동작 그래프에 그대로 남아 있습니다.

초대된 계정만 동작 그래프에서 계정을 제거할 수 있습니다. 조직 계정은 조직 동작 그래프에서 해당 계정을 제거할 수 없습니다.

동작 그래프에서 계정 제거(콘솔)

를 AWS Management Console 사용하여 행동 그래프에서 계정을 제거할 수 있습니다.

동작 그래프에서 계정 제거(콘솔)

1. https://console.aws.amazon.com/detective/에서 Amazon Detective 콘솔을 엽니다.
2. Detective 탐색 창에서 계정 관리를 선택합니다.
3. 내 관리자 계정에서 탈퇴하려는 동작 그래프에 대해 탈퇴를 선택합니다.

행동 그래프에서 계정 삭제하기 (Detective API,) AWS CLI

Detective API 또는 를 사용하여 행동 AWS Command Line Interface 그래프에서 계정을 제거할 수 있습니다.

행동 그래프에서 계정을 삭제하려면 (Detective API,) AWS CLI

- Detective API: `DisassociateMembership` 작업을 사용합니다. 그래프 ARN을 지정해야 합니다.
- AWS CLI: 명령줄에서 `disassociate-membership` 명령을 실행합니다.

```
aws detective disassociate-membership --graph-arn <behavior graph ARN>
```

예제

```
aws detective disassociate-membership --graph-arn arn:aws:detective:us-
east-1:111122223333:graph:123412341234
```

계정 활동이 동작 그래프에 미치는 영향

이러한 업은 Amazon Detective 데이터 및 액세스에 다음과 같은 영향을 미칩니다.

Detective 비활성화

관리자 계정이 Detective를 비활성화하면 다음과 같은 상황이 발생합니다.

- 동작 그래프가 삭제됩니다.
- Detective는 관리자 계정 및 해당 동작 그래프의 멤버 계정에서 데이터 수집을 중단합니다.

동작 그래프에서 멤버 계정이 제거됩니다.

멤버 계정이 동작 그래프에서 제거되면 Detective는 해당 계정의 데이터 수집을 중단합니다.

동작 그래프의 기존 데이터는 영향을 받지 않습니다.

초대된 계정의 경우 해당 계정이 내 멤버 계정 목록에서 제거됩니다.

조직 동작 그래프에서 조직 계정의 경우 계정 상태가 멤버 아님으로 변경됩니다.

멤버 계정이 조직을 떠남

멤버 계정이 조직을 떠나면 다음과 같은 상황이 발생합니다.

- 해당 계정이 조직 동작 그래프의 내 멤버 계정 목록에서 제거됩니다.
- Detective는 해당 계정의 데이터 수집을 중단합니다.

동작 그래프의 기존 데이터는 영향을 받지 않습니다.

AWS 계정이 일시 중지됨

AWS에서 관리자 계정이 일시 중지되면 해당 계정은 Detective에서 동작 그래프를 볼 수 있는 권한을 상실합니다. Detective는 동작 그래프에 데이터를 수집하는 것을 중단합니다.

AWS에서 멤버 계정이 일시 중지되면 Detective는 해당 계정에 대한 데이터 수집을 중단합니다.

90일이 지나면 계정이 해지되거나 다시 활성화됩니다. 관리자 계정이 다시 활성화되면 Detective 권한이 복원됩니다. Detective는 계정에서 데이터 수집을 재개합니다. 멤버 계정이 다시 활성화되면 Detective는 계정에서 데이터 수집을 재개합니다.

AWS 계정이 폐쇄됨

AWS 계정이 폐쇄되면 Detective는 다음과 같이 폐쇄에 응답합니다.

- 관리자 계정의 경우 Detective는 동작 그래프를 삭제합니다.
- 멤버 계정의 경우 Detective는 해당 계정을 동작 그래프에서 제거합니다.

AWS는 관리자 계정 해지 유효 날짜부터 90일 동안 계정에 대한 정책 데이터를 유지합니다. 90일의 기간이 종료되는 시점에 AWS는 계정의 모든 정책 데이터를 영구적으로 삭제합니다.

- 정책을 보관하면 결과를 90일 넘게 유지할 수 있습니다. 또한 EventBridge 규칙에 사용자 지정 작업을 사용하여 결과를 S3 버킷에 저장할 수 있습니다.
- AWS가 정책 데이터를 유지하는 한 해지된 계정을 다시 열 때 AWS가 계정을 서비스 관리자로 재할당하고 계정의 서비스 정책 데이터를 복구합니다.
- 자세한 내용은 계정 해지를 참조하세요.

Important

AWS GovCloud (US) 리전의 고객인 경우:

- 계정을 해지하기 전에 계정 리소스를 백업한 다음 삭제합니다. 계정을 해지한 뒤에는 더 이상 해당 계정에 액세스할 수 없습니다.

Amazon Detective에서의 활동 및 사용량 추적

Detective 활동을 추적하는 데 도움이 되도록 사용량 페이지에는 수집된 데이터의 양과 예상 비용이 표시됩니다.

- 관리자 계정의 경우 사용량 페이지에 전체 동작 그래프의 데이터 볼륨 및 예상 비용이 표시됩니다.
- 멤버 계정의 경우 사용량 페이지에는 멤버 계정이 제공하는 동작 그래프 전반에서 해당 계정의 데이터 양과 예상 비용이 표시됩니다.

Detective는 AWS CloudTrail 로깅도 지원합니다.

목차

동작 그래프의 사용량 및 비용 모니터링(관리자 계정)

Amazon Detective는 계정이 속한 각 동작 그래프에 사용된 데이터에 대해 각 계정에 요금을 청구합니다. Detective는 출처에 관계없이 모든 데이터에 대해 GB당 계층화된 고정 요금을 부과합니다.

관리자 계정의 경우 Detective 콘솔의 사용량 페이지를 통해 지난 30일 동안 데이터 소스별 또는 계정별로 수집된 데이터의 볼륨을 볼 수 있습니다. 또한 관리자 계정은 해당 계정 및 전체 동작 그래프에서 일반적인 30일 기간의 예상 비용을 확인할 수 있습니다.

Detective 사용량 정보 보기

1. AWS Management Console에 로그인합니다. 그런 다음 https://console.aws.amazon.com/detective/에서 Detective 콘솔을 엽니다.
2. Detective 탐색 창의 설정 아래에서 사용량을 선택합니다.
3. 탭을 선택하여 데이터 소스별 또는 계정별 사용량 보기 중에서 선택합니다.

각 계정에서 수집된 데이터의 볼륨양

멤버 계정별로 수집된 볼륨은 동작 그래프에 활성 계정을 나열합니다. 제거된 멤버 계정은 나열되지 않습니다.

각 계정에 대해 수집된 볼륨 목록은 다음 정보를 제공합니다.

- AWS 계정 식별자 및 루트 사용자 이메일 주소.
- 계정이 동작 그래프에 데이터를 제공하기 시작한 날짜.

  관리자 계정의 경우 이 날짜는 해당 계정이 Detective를 활성화한 날짜입니다.

  멤버 계정의 경우 이 날짜는 초대를 수락한 후 계정이 멤버 계정으로 활성화된 날짜입니다.
- 지난 30일 동안 계정에서 수집된 데이터의 볼륨. 합계에는 모든 소스 유형이 포함됩니다.
- 계정이 현재 무료 평가판 기간 중인지 여부. 현재 무료 평가 기간이 있는 계정의 경우 목록에 남은 일수가 표시됩니다.

  무료 평가판 기간 중인 계정이 없는 경우 무료 평가판 상태 열이 표시되지 않습니다.

동작 그래프의 예상 비용

이 계정의 예상 비용은 관리자 계정의 30일 데이터 예상 비용을 나타냅니다. 예상 비용은 관리자 계정의 일일 평균 볼륨을 기준으로 합니다.

> **Important**
>
> 이 금액은 예상 비용일 뿐입니다. 이는 일반적인 30일 기간의 관리자 계정 데이터에 대한 총 비용을 예상합니다. 이는 이전 30일간의 사용량을 기준으로 합니다. the section called “Detective가 예상 비용을 계산하는 방법” 섹션을 참조하세요.

동작 그래프의 예상 비용

모든 계정의 예상 비용에는 전체 동작 그래프에 대한 30일간의 데이터에 대한 총 예상 비용이 표시됩니다. 예상 비용은 각 계정의 일일 평균 볼륨을 기준으로 합니다.

> **Important**
>
> 이 금액은 예상 비용일 뿐입니다. 이는 일반적인 30일 기간 동안의 동작 그래프 데이터에 대한 총 비용을 예측합니다. 이는 이전 30일간의 사용량을 기준으로 합니다. 예상 비용에는 동작 그래프에서 삭제된 멤버 계정이 포함되지 않습니다. the section called “Detective가 예상 비용을 계산하는 방법” 섹션을 참조하세요.

소스 패키지에서 수집한 데이터의 볼륨

동작 그래프에 활성화된 다양한 소스 패키지에서 수집한 데이터 볼륨을 나열하여 보려면 소스 패키지별을 선택합니다.

모든 계정이 해당 계정에 대해 이 데이터를 볼 수 있습니다. 관리자 계정은 각 멤버의 소스 패키지별 사용량을 나열하는 추가 패널을 볼 수 있습니다. 제거된 멤버 계정은 나열되지 않습니다.

Detective 핵심

Detective 핵심 패널은 지난 30일 동안 Detective 핵심 소스(CloudTrail 로그, VPC 흐름 로그, GuardDuty 조사 결과)에서 수집된 데이터의 볼륨을 보여줍니다.

EKS 감사 로그

EKS 감사 로그 패널에는 지난 30일간 EKS 감사 로그 소스에서 수집된 데이터의 볼륨이 표시됩니다. 이 소스 패키지의 패널은 동작 그래프에 EKS 감사 로그가 활성화된 경우에만 사용할 수 있습니다.

동작 그래프 전반의 사용량 및 비용 모니터링(멤버 계정)

Amazon Detective는 계정이 속한 각 동작 그래프에 사용된 데이터에 대해 각 계정에 요금을 청구합니다. Detective는 출처에 관계없이 모든 데이터에 대해 GB당 계층화된 고정 요금을 부과합니다.

멤버 계정의 경우 사용량 페이지에는 해당 계정의 데이터 볼륨과 30일 예상 비용만 표시됩니다.

Detective 사용량 정보 보기

1. AWS Management Console에 로그인합니다. 그런 다음 https://console.aws.amazon.com/detective/에서 Detective 콘솔을 엽니다.
2. Detective 탐색 창의 설정 아래에서 사용량을 선택합니다.

각 동작 그래프의 수집 볼륨

이 계정의 수집 볼륨에는 멤버 계정이 제공한 동작 그래프가 나열됩니다. 여기에는 탈퇴된 멤버십 또는 관리자 계정으로 제거된 멤버십이 포함되어 있지 않습니다.

각 동작 그래프의 경우 목록에는 다음과 같은 정보가 포함되어 있습니다.

- 관리자의 계정의 계정 번호
- 지난 30일 동안 멤버 계정에서 수집된 데이터의 볼륨. 합계에는 모든 소스 유형이 포함됩니다.
- 멤버 계정이 동작 그래프에 활성화 날짜.

동작 그래프 전반의 예상 비용

이 계정의 예상 비용에는 해당 계정이 제공하는 모든 동작 그래프에서 해당 멤버 계정의 30일 데이터에 대한 예상 비용이 표시됩니다. 예상 비용은 멤버 계정의 일일 평균 볼륨을 기준으로 합니다.

> **Important**
>
> 이 금액은 예상 비용일 뿐입니다. 이는 일반적인 30일 기간의 관리자 계정 데이터에 대한 총 비용을 예상합니다. 이는 이전 30일간의 사용량을 기준으로 합니다. the section called “Detective가 예상 비용을 계산하는 방법”을(를) 참조하세요.

Amazon Detective가 예상 비용을 계산하는 방법

Detective는 사용량 페이지에 표시되는 예상 비용 값을 계산하기 위해 다음 작업을 수행합니다.

1. 동작 그래프에서 개별 계정의 예상 비용을 구하기 위해 Detective는 다음을 수행합니다.
   a. 일일 평균 볼륨을 계산합니다. 모든 활성 일수의 데이터 볼륨을 더한 다음 계정이 활성화된 기간(일)으로 나눕니다.

      계정을 활성화한 지 30일이 지난 경우 남은 일수는 30일입니다. 계정을 활성화한 지 30일이 지나지 않은 경우 남은 일수는 수락 날짜 이후입니다.

      예를 들어 계정이 12일 전에 활성화된 경우 Detective는 해당 12일 동안 수집된 볼륨을 더한 다음 이를 12로 나눕니다.
   b. 계정의 일일 평균에 30을 곱합니다. 이는 해당 계정의 30일 예상 사용량입니다.

c. 요금 모델을 사용하여 30일 예상 사용량에 대한 30일 예상 비용을 계산합니다.

2. 동작 그래프의 총 예상 비용을 구하기 위해 Detective는 다음을 수행합니다.
   a. 동작 그래프에 있는 모든 계정의 30일 예상 사용량을 합산합니다.
   b. 요금 모델을 사용하여 30일 총 예상 사용량에 대한 30일 예상 비용을 계산합니다.
3. 동작 그래프에서 멤버 계정의 총 예상 비용을 구하기 위해 Detective는 다음을 수행합니다.
   a. 모든 동작 그래프의 30일 예상 사용량을 합산합니다.
   b. 요금 모델을 사용하여 30일 총 예상 사용량에 대한 30일 예상 비용을 계산합니다.
4. 공유 Amazon VPC를 사용하는 경우, Detective는 모니터링 활동을 기반으로 예상 비용을 계산합니다. 본인의 환경에 해당하는 조사의 예상 비용을 검토하는 것이 좋습니다.
   a. Detective 멤버 계정에 공유 Amazon VPC가 있고 이 공유 VPC를 사용하는 다른 비 Detective 계정이 있는 경우 Detective는 해당 VPC에서 들어오는 모든 트래픽을 모니터링합니다. 사용량과 비용이 증가하고 Detective는 VPC 내의 모든 트래픽 흐름을 시각화합니다.
   b. 공유 Amazon VPC 내에 EC2 인스턴스가 있고 공유 소유자가 Detective 멤버가 아닌 경우, Detective는 VPC의 트래픽을 모니터링하지 않으므로 사용량과 비용이 감소합니다. VPC 내의 트래픽 흐름을 보려면 Amazon VPC 소유자를 Detective 그래프의 멤버로 추가해야 합니다.

AWS CloudTrail을 사용하여 Amazon Detective API 직접 호출 로깅

Detective는 Detective 에서 사용자, 역할, 또는 AWS 서비스가 수행한 작업에 대한 레코드를 제공하는 서비스인 AWS CloudTrail과 통합됩니다. CloudTrail은 Detective에 대한 모든 API 직접 호출을 이벤트로 캡처합니다. 캡처되는 호출에는 Detective 콘솔로부터의 호출과 Detective API 작업에 대한 코드 호출이 포함됩니다.

- 추적을 생성하면 Detective 이벤트를 포함한 CloudTrail 이벤트를 지속적으로 Amazon S3 버킷에 배포할 수 있습니다.
- 추적을 구성하지 않은 경우에도 CloudTrail 콘솔의 이벤트 기록에서 최신 이벤트를 볼 수 있습니다.

CloudTrail에서 수집한 정보를 사용하여 다음을 확인할 수 있습니다.

- Detective에 대한 요청
- 요청을 보낸 IP 주소
- 요청한 사람
- 요청한 시기

- 요청에 대한 추가 세부 정보

CloudTrail에 대한 자세한 내용은 AWS CloudTrail 사용 설명서를 참조하세요.

CloudTrail의 Detective 정보

CloudTrail은 계정 생성 시 AWS 계정에서 사용되도록 설정됩니다. Detective에서 활동이 발생하면 해당 활동이 이벤트 기록의 다른 AWS 서비스 이벤트와 함께 CloudTrail 이벤트에 기록됩니다. AWS 계정에서 최신 이벤트를 확인, 검색 및 다운로드할 수 있습니다. 자세한 내용은 CloudTrail 이벤트 기록을 사용하여 이벤트 보기를 참조하세요.

Detective에 대한 이벤트를 포함하여 AWS 계정에 이벤트를 지속적으로 기록하려면 추적을 생성합니다. CloudTrail은 추적을 사용하여 Amazon S3 버킷으로 로그 파일을 전송할 수 있습니다.

콘솔에서 추적을 생성하면 기본적으로 모든 AWS 리전에 추적이 적용됩니다. 추적은 AWS 파티션에 있는 모든 리전의 이벤트를 로깅하고 지정된 Amazon S3 버킷으로 로그 파일을 전송합니다. CloudTrail 로그에 수집된 이벤트 데이터를 좀 더 분석하고 작업하도록 다른 AWS 서비스를 구성할 수 있습니다.

자세한 내용은 다음을 참조하세요.

- 추적 생성 개요
- CloudTrail 지원 서비스 및 통합
- CloudTrail에 대한 Amazon SNS 알림 구성
- 여러 리전에서 CloudTrail 로그 파일 받기 및 여러 계정에서 CloudTrail 로그 파일 받기

CloudTrail은 모든 Detective 작업을 기록하며, 이는 Detective API참조에 문서화되어 있습니다.

예를 들어, `CreateMembers`, `AcceptInvitation` 및 `DeleteMembers` 작업에 대한 호출은 CloudTrail 로그 파일의 항목을 생성합니다.

모든 이벤트 및 로그 항목에는 요청을 생성한 사용자에 대한 정보가 들어 있습니다. 자격 증명 정보를 이용하면 다음을 쉽게 판단할 수 있습니다.

- 요청을 루트로 했는지 아니면 AWS Identity and Access Management(IAM) 사용자 자격 증명으로 했는지 여부
- 역할 또는 연합된 사용자에 대한 임시 보안 자격 증명을 사용하여 요청이 생성되었는지 여부
- 다른 AWS 서비스에서 요청했는지 여부

자세한 내용은 CloudTrail userIdentity 요소를 참조하세요.

Detective 로그 파일 항목 이해

추적이란 지정한 Amazon S3 버킷에 이벤트를 로그 파일로 입력할 수 있게 하는 구성입니다. CloudTrail 로그 파일에는 하나 이상의 로그 항목이 포함될 수 있습니다.

이벤트는 모든 소스의 단일 요청을 의미합니다. 이벤트에는 요청된 작업, 작업 날짜 및 시간, 요청 파라미터 등에 대한 정보가 포함되어 있습니다. CloudTrail 로그 파일은 퍼블릭 API 직접 호출의 주문 스택 기록이 아니므로 특정 순서로 표시되지 않습니다.

다음은 `AcceptInvitation` 작업을 보여주는 CloudTrail 로그 항목이 나타낸 예제입니다.


```
      {
            "EventId": "f2545ee3-170f-4340-8af4-a983c669ce37",
            "Username": "JaneRoe",
            "EventTime": 1571956406.0,
            "CloudTrailEvent": "{\"eventVersion\":\"1.05\",\"userIdentity\":
{\"type\":\"AssumedRole\",\"principalId\":\"AROAJZARKEP6WKJ5JHSUS:JaneRoe\",\"arn
\":\"arn:aws:sts::111122223333:assumed-role/1A4R5SKSPGG9V/JaneRoe\",\"accountId
\":\"111122223333\",\"accessKeyId\":\"AKIAIOSFODNN7EXAMPLE\",\"sessionContext\":
{\"attributes\":{\"mfaAuthenticated\":\"false\",\"creationDate\":\"2019-10-24T21:54:56Z
\"},\"sessionIssuer\":{\"type\":\"Role\",\"principalId\":\"AROAJZARKEP6WKJ5JHSUS
\",\"arn\":\"arn:aws:iam::111122223333:role/1A4R5SKSPGG9V\",\"accountId\":
\"111122223333\",\"userName\":\"JaneRoe\"}}},\"eventTime\":\"2019-10-24T22:33:26Z
\",\"eventSource\":\"detective.amazonaws.com\",\"eventName\":\"AcceptInvitation
\",\"awsRegion\":\"us-east-2\",\"sourceIPAddress\":\"192.0.2.123\",\"userAgent
\":\"aws /3 aws-sdk-java/1.11.648 Linux/4.14.133-97.112.amzn2.x86_64 OpenJDK_64-
Bit_Server_VM/25.201-b09 java/1.8.0_201 vendor/Oracle_Corporation exec-env/
AWS_Lambda_java8\",\"errorCode\":\"ValidationException\",\"requestParameters\":
{\"masterAccount\":\"111111111111\"},\"responseElements\":{\"message\":\"Invalid
 request body\"},\"requestID\":\"8437ff99-5ec4-4b1a-8353-173be984301f\",\"eventID\":
\"f2545ee3-170f-4340-8af4-a983c669ce37\",\"readOnly\":false,\"eventType\":\"AwsApiCall
\",\"recipientAccountId\":\"111122223333\"}",
            "EventName": "AcceptInvitation",
            "EventSource": "detective.amazonaws.com",
            "Resources": []
        },
```

동작 그래프의 태그 관리

동작 그래프에 태그를 할당할 수 있습니다. 그런 다음 IAM 정책의 태그 값을 사용하여 Detective의 동작 그래프 기능에 대한 액세스를 관리할 수 있습니다. the section called “Detective 동작 그래프 태그를 기반으로 한 권한 부여” 섹션을 참조하세요.

태그를 비용 보고 도구로 사용할 수도 있습니다. 예를 들어 보안과 관련된 비용을 추적하기 위해 Detective 동작 그래프, AWS Security Hub 허브 리소스 및 Amazon GuardDuty 탐지기에 동일한 태그를 할당할 수 있습니다. AWS Cost Explorer에서는 해당 태그를 검색하여 해당 리소스의 비용을 통합적으로 확인할 수 있습니다.

동작 그래프의 태그 보기(콘솔)

동작 그래프의 태그는 일반 페이지에서 관리할 수 있습니다.

동작 그래프에 할당된 태그 목록 보기

1. https://console.aws.amazon.com/detective/에서 Amazon Detective 콘솔을 엽니다.
2. 탐색 창의 [Settings] 아래에서 [General]을 선택합니다.

동작 그래프의 태그 목록 작성(Detective API, AWS CLI)

Detective API 또는 AWS Command Line Interface를 사용하여 동작 그래프의 태그 목록을 가져올 수 있습니다.

동작 그래프의 태그 목록 가져오기(Detective API, AWS CLI)

- Detective API: `ListTagsForResource` 작업을 사용합니다. 동작 그래프의 ARN을 제공해야 합니다.
- AWS CLI: 명령줄에서 `list-tags-for-resource` 명령을 실행합니다.

```
aws detective list-tags-for-resource --resource-arn <behavior graph ARN>
```

예

```
aws detective list-tags-for-resource --resource-arn arn:aws:detective:us-
east-1:111122223333:graph:123412341234
```

동작 그래프에 태그 추가(콘솔)

일반 페이지의 태그 목록에서 동작 그래프에 태그 값을 추가할 수 있습니다.

동작 그래프에 태그 추가

1. Add new tag(새 태그 추가가)를 선택합니다.
2. 키에는 태그의 이름을 입력합니다.
3. 값에는 태그 값을 입력합니다.

동작 그래프에 태그 추가(Detective API, AWS CLI)

Detective API 또는 AWS CLI를 사용하여 동작 그래프에 태그 값을 추가할 수 있습니다.

동작 그래프에 태그 추가(Detective API, AWS CLI)

- Detective API: `TagResource` 작업을 사용합니다. 동작 그래프 ARN과 추가할 태그 값을 제공합니다.
- AWS CLI: 명령줄에서 `tag-resource` 명령을 실행합니다.

```
aws-detective tag-resource --aws detective tag-resource --resource-arn <behavior
 graph ARN> --tags '{"TagName":"TagValue"}'
```

예

```
aws detective tag-resource --resource-arn arn:aws:detective:us-
east-1:111122223333:graph:123412341234 --tags '{"Department":"Finance"}'
```

동작 그래프에서 태그 제거(콘솔)

일반 페이지의 목록에서 태그를 제거하려면 해당 태그의 제거 옵션을 선택합니다.

동작 그래프에서 태그 제거(Detective API, AWS CLI)

Detective API 또는 AWS CLI를 사용하여 동작 그래프에서 태그 값을 제거할 수 있습니다.

동작 그래프에서 태그 제거(Detective API, AWS CLI)

- Detective API: `UntagResource` 작업을 사용합니다. 동작 그래프 ARN과 제거할 태그의 이름을 제공합니다.
- AWS CLI: 명령줄에서 `untag-resource` 명령을 실행합니다.

```
aws detective untag-resource --resource-arn <behavior graph ARN> --tag-keys "TagName"
```

예

```
aws detective untag-resource --resource-arn arn:aws:detective:us-
east-1:111122223333:graph:123412341234 --tag-keys "Department"
```

Amazon Detective의 보안

AWS에서는 클라우드 보안을 가장 중요하게 생각합니다. 여러분은 AWS 고객으로서 보안에 민감한 기관의 요구 사항을 충족하도록 구축된 데이터 센터 및 네트워크 아키텍처의 혜택을 누릴 수 있습니다.

보안은 AWS과 사용자의 공동 책임입니다. 공동 책임 모델은 이 사항을 클라우드 내 보안 및 클라우드의 보안으로 설명합니다.

- 클라우드의 보안 - AWS는 AWS클라우드에서 AWS서비스를 실행하는 인프라를 보호합니다.AWS는 또한 안전하게 사용할 수 있는 서비스를 제공합니다.

  서드 파티 감사원은 정기적으로 AWS규정 준수 프로그램의 일환으로 보안 효과를 테스트하고 검증합니다.

  Amazon Detective에 적용되는 규정 준수 프로그램에 대한 자세한 내용은 규정 준수 프로그램 제공 범위 내 AWS 서비스를 참조하세요.
- 클라우드 내 보안: 귀하의 책임은 귀하가 사용하는 AWS 서비스에 의해 결정됩니다. 또한 귀하는 귀사의 데이터의 민감도, 귀사의 요구 사항, 관련 법률 및 규정을 비롯한 기타 요소에 대해서도 책임이 있습니다.

이 설명서는 Detective 사용 시 공동 책임 모델을 적용하는 방법을 이해하는 데 도움이 됩니다. 다음 주제에서는 보안 및 규정 준수 목표를 충족하도록 Detective를 구성하는 방법을 보여줍니다. 또한 Detective 리소스를 모니터링하고 보호하는 데 도움이 되는 다른 AWS 서비스를 사용하는 방법을 알아봅니다.

내용

Amazon Detective의 데이터 보호

AWS 공동 책임 모델은 Amazon Detective의 데이터 보호에 적용됩니다. 이 모델이 설명하는 것처럼 AWS는 모든 AWS 클라우드를 실행하는 글로벌 인프라를 보호할 책임이 있습니다. 사용자는 인프라에서 호스팅되는 콘텐츠를 관리해야 합니다. 사용하는 AWS 서비스의 보안 구성과 관리 작업에 대한 책임도 사용자에게 있습니다. 데이터 프라이버시에 대한 자세한 내용은 Data Privacy FAQ(데이터 프라이버시 FAQ)를 참조하세요. 유럽의 데이터 보호에 대한 자세한 내용은 AWS 보안 블로그의 AWS Shared Responsibility Model and GDPR 블로그 게시물을 참조하세요.

데이터를 보호하려면 AWS 계정보안 인증 정보를 보호하고 AWS IAM Identity Center또는 AWS Identity and Access Management(IAM)를 통해 개별 사용자 계정을 설정하는 것이 좋습니다. 이렇게 하면 개별 사용자에게 자신의 직무를 충실히 이행하는 데 필요한 권한만 부여됩니다. 또한 다음과 같은 방법으로 데이터를 보호하는 것이 좋습니다.

- 각 계정에 멀티 팩터 인증 설정(MFA)을 사용하세요.
- SSL/TLS를 사용하여 AWS 리소스와 통신하세요. TLS 1.2는 필수이며 TLS 1.3를 권장합니다.
- AWS CloudTrail로 API 및 사용자 활동 로깅을 설정하세요.
- AWS 암호화 솔루션을 AWS 서비스 내의 모든 기본 보안 컨트롤과 함께 사용하세요.
- Amazon S3에 저장된 민감한 데이터를 검색하고 보호하는 데 도움이 되는 Amazon Macie와 같은 고급 관리형 보안 서비스를 사용하세요.
- 명령줄 인터페이스 또는 API를 통해 AWS에 액세스할 때 FIPS 140-2 인증 암호화 모듈이 필요한 경우 FIPS 엔드포인트를 사용하세요. 사용 가능한 FIPS 엔드포인트에 대한 자세한 내용은 FIPS(Federal Information Processing Standard) 140-2를 참조하세요.

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

Detective는 저장 및 전송 중인 모든 데이터를 암호화합니다.

내용

- Amazon Detective의 키 관리

Amazon Detective의 키 관리

Detective는 개인 식별이 가능한 고객 데이터를 저장하지 않기 때문에 AWS 관리형 키를 사용합니다.

이 유형의 KMS 키는 여러 계정에서 사용할 수 있습니다. AWS Key Management Service 개발자 안내서의 AWS 소유 키 설명을 참조하세요.

이 유형의 KMS 키는 1년마다(약 365일) 자동으로 순환됩니다. AWS Key Management Service 개발자 안내서의 키 순환 설명을 참조하세요.

Amazon Detective용 Identity and Access Management

AWS Identity and Access Management(IAM)은 관리자가 AWS 리소스에 대한 액세스를 안전하게 제어할 수 있도록 지원하는 AWS 서비스입니다. IAM 관리자는 누가 Detective 리소스를 사용하도록 인증되고(로그인됨) 권한이 부여되는지(권한 있음)를 제어합니다. IAM은 추가 비용 없이 사용할 수 있는 AWS 서비스입니다.

내용

고객

AWS Identity and Access Management(IAM)를 사용하는 방법은 Detective에서 수행하는 작업에 따라 달라집니다.

서비스 사용자 - Detective 서비스를 사용하여 작업을 수행하는 경우 필요한 보안 인증 정보 및 권한을 관리자가 제공합니다. 더 많은 Detective 기능을 사용하여 작업을 수행하게 되면 추가 권한이 필요할 수 있습니다. 액세스 권한 관리 방식을 이해하면 적절한 권한을 관리자에게 요청할 수 있습니다. Detective의 기능에 액세스할 수 없는 경우 Amazon Detective 자격 증명 및 액세스 문제 해결 섹션을 참조하세요.

서비스 관리자 - 회사에서 Detective 리소스를 책임지고 있는 경우 Detective에 대한 전체 액세스 권한을 가지고 있을 것입니다. 서비스 관리자는 서비스 사용자가 액세스해야 하는 Detective 기능과 리소스

를 결정합니다. 그런 다음, IAM 관리자에게 요청을 제출하여 서비스 사용자의 권한을 변경해야 합니다. 이 페이지의 정보를 검토하여 IAM의 기본 개념을 이해합니다. 회사가 Detective에서 IAM을 사용하는 방법에 대해 자세히 알아보려면 Amazon Detective가 IAM과 작동하는 방식 섹션을 참조하세요.

IAM 관리자 - IAM 관리자라면 Detective에 대한 액세스 권한 관리 정책 작성 방법을 자세히 알고 싶을 것입니다. IAM에서 사용할 수 있는 Detective 자격 증명 기반 정책 예제를 보려면 Amazon Detective 자격 증명 기반 정책 예제 섹션을 참조하세요.

자격 증명을 통한 인증

인증은 ID 보안 인증을 사용하여 AWS에 로그인하는 방식입니다. AWS 계정 루트 사용자 또는 IAM 사용자로 또는 IAM 역할을 수임하여 인증(AWS에 로그인)되어야 합니다.

자격 증명 소스를 통해 제공된 보안 인증 정보를 사용하여 페더레이션 ID로 AWS에 로그인할 수 있습니다. AWS IAM Identity Center (IAM Identity Center) 사용자, 회사의 Single Sign-On 인증, Google 또는 Facebook 보안 인증이 페더레이션형 ID의 예입니다. 페더레이션형 ID로 로그인할 때 관리자가 이전에 IAM 역할을 사용하여 ID 페더레이션을 설정했습니다. 연동을 사용하여 AWS에 액세스하면 간접적으로 역할을 수임합니다.

사용자 유형에 따라 AWS Management Console 또는AWS 액세스 포털에 로그인할 수 있습니다. AWS에 로그인하는 방법에 대한 자세한 내용은 AWS 로그인 사용 설명서의 AWS 계정에 로그인하는 방법을 참조하세요.

AWS에 프로그래밍 방식으로 액세스하는 경우, AWS는 보안 인증 정보를 사용하여 요청에 암호화 방식으로 서명할 수 있는 소프트웨어 개발 키트(SDK) 및 명령줄 인터페이스(CLI)를 제공합니다. AWS 도구를 사용하지 않는 경우 요청에 직접 서명해야 합니다. 권장 방법을 사용하여 요청에 직접 서명하는 방법에 대한 자세한 내용은 IAM 사용 설명서의 AWS API 요청에 서명을 참조하세요.

사용하는 인증 방법에 상관없이 추가 보안 정보를 제공해야 할 수도 있습니다. 예를 들어, AWS는 다중 인증(MFA)을 사용하여 계정의 보안을 강화하는 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

AWS 계정을 생성할 때는 해당 계정의 모든 AWS 서비스 및 리소스에 대한 완전한 액세스 권한이 있는 단일 로그인 자격 증명으로 시작합니다. 이 자격 증명은 AWS 계정루트 사용자라고 하며, 계정을 생성할 때 사용한 이메일 주소와 암호로 로그인하여 액세스합니다. 일상적인 태스크에는 루트 사용자를 가급적 사용하지 않는 것이 좋습니다. 루트 사용자 자격 증명을 보호하고 루트 사용자만 수행할 수 있는 태스크를 수행하는 데 사용합니다. 루트 사용자로 로그인해야 하는 전체 작업 목록은 IAM 사용 설명서의 루트 사용자 자격 증명이 필요한 태스크를 참조하세요.

IAM 사용자 및 그룹

IAM 사용자는 단일 개인 또는 애플리케이션에 대한 특정 권한을 가지고 있는 AWS 계정에 속하는 ID입니다. 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 자격 증명입니다. 사용자는 그룹으로 로그인할 수 없습니다. 그룹을 사용하여 여러 사용자의 권한을 한 번에 지정할 수 있습니다. 그룹을 사용하면 대규모 사용자 집합의 권한을 더 쉽게 관리할 수 있습니다. 예를 들어 IAMAdmins라는 그룹이 있고 이 그룹에 IAM 리소스를 관리할 권한을 부여할 수 있습니다.

사용자는 역할과 다릅니다. 사용자는 한 사람 또는 애플리케이션과 고유하게 연결되지만, 역할은 해당 역할이 필요한 사람이라면 누구나 수임할 수 있습니다. 사용자는 영구적인 장기 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 가지고 있는 AWS 계정 내의 ID입니다. IAM 사용자와 유사하지만, 특정 개인과 연결되지 않습니다. 역할 전환하여 AWS Management Console에서 IAM 역할을 임시로 수임할 수 있습니다. AWS CLI 또는 AWS API 태스크를 직접적으로 호출하거나 사용자 지정 URL을 사용하여 역할을 수임할 수 있습니다. 역할 사용 방법에 대한 자세한 정보는 IAM 사용 설명서의 IAM 역할 사용을 참조하세요.

보안 인증 정보가 있는 IAM 역할은 다음과 같은 상황에서 유용합니다.

- 연동 사용자 액세스 - 연동 자격 증명에 권한을 부여하려면 역할을 생성하고 해당 역할의 권한을 정의합니다. 연동 자격 증명이 인증되면 역할이 연결되고 역할에 정의된 권한이 부여됩니다. 페더레이션 역할에 대한 자세한 내용은 IAM 사용 설명서의 타사 자격 증명 공급자의 역할 생성을 참조하세요. IAM Identity Center를 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 태스크에 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 방법입

니다. 그러나 일부 AWS 서비스를 사용하면 정책을 리소스에 직접 연결할 수 있습니다(역할을 프록시로 사용하는 대신). 교차 계정 액세스를 위한 역할과 리소스 기반 정책의 차이점을 알아보려면 IAM 사용 설명서의 IAM 역할과 리소스 기반 정책의 차이 섹션을 참조하세요.

- 교차 서비스 액세스: 일부 AWS 서비스는 다른 AWS 서비스의 기능을 사용합니다. 예를 들어 서비스에서 직접적으로 호출하면 일반적으로 해당 서비스는 Amazon EC2에서 애플리케이션을 실행하거나 Amazon S3에 객체를 저장합니다. 서비스는 직접 호출하는 보안 주체의 권한을 사용하거나, 서비스 역할을 사용하거나, 또는 서비스 연결 역할을 사용하여 이 태스크를 수행할 수 있습니다.
  - 전달 액세스 세션(FAS) - IAM 사용자 또는 역할을 사용하여 AWS에서 작업을 수행하는 사람은 보안 주체로 간주됩니다. 일부 서비스를 사용하는 경우 다른 서비스에서 다른 작업을 시작하는 작업을 수행할 수 있습니다. FAS는 AWS 서비스를 직접 호출하는 보안 주체의 권한과 요청하는 AWS 서비스를 함께 사용하여 다운스트림 서비스에 대한 요청을 수행합니다. FAS 요청은 서비스에서 완료를 위해 다른 AWS 서비스 또는 리소스와의 상호 작용이 필요한 요청을 받은 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 수임하는 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 AWS 서비스에 연결된 서비스 역할의 한 유형입니다. 서비스는 사용자를 대신하여 작업을 수행하기 위해 역할을 수임할 수 있습니다. 서비스 연결 역할은 AWS 계정에 나타나고, 서비스가 소유합니다. IAM 관리자는 서비스 연결 역할의 권한을 볼 수 있지만 편집할 수는 없습니다.
- Amazon EC2에서 실행 중인 애플리케이션 – IAM 역할을 사용하여 EC2 인스턴스에서 실행되고 AWS CLI 또는 AWS API 요청을 수행하는 애플리케이션의 임시 보안 인증을 관리할 수 있습니다. 이는 EC2 인스턴스 내에 액세스 키를 저장할 때 권장되는 방법입니다. EC2 인스턴스에 AWS역할을 할당하고 해당 역할을 모든 애플리케이션에서 사용할 수 있도록 하려면 인스턴스에 연결된 인스턴스 프로파일을 생성합니다. 인스턴스 프로파일에는 역할이 포함되어 있으며 EC2 인스턴스에서 실행되는 프로그램이 임시 보안 인증을 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 사용하여 액세스 관리

정책을 생성하고 AWS 자격 증명 또는 리소스에 연결하여 AWS 내 액세스를 제어합니다. 정책은 ID 또는 리소스와 연결될 때 해당 권한을 정의하는 AWS의 개체입니다. AWS는 보안 주체(사용자, 루트 사

용자 또는 역할 세션)가 요청을 보낼 때 이러한 정책을 평가합니다. 정책에서 권한은 요청이 허용되는지 또는 거부되는지를 결정합니다. 대부분의 정책은 AWS에 JSON 설명서로서 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 있는 지를 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 정책이 있는 사용자는 AWS Management Console, AWS CLI또는 AWSAPI에서 역할 정보를 가져올 수 있습니다.

자격 증명 기반 정책

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.

ID 기반 정책은 인라인 정책 또는 관리형 정책으로 한층 더 분류할 수 있습니다. 인라인 정책은 단일 사용자, 그룹 또는 역할에 직접 포함됩니다. 관리형 정책은 AWS 계정에 속한 다수의 사용자, 그룹 및 역할에 독립적으로 추가할 수 있는 정책입니다. 관리형 정책에는 AWS관리형 정책과 고객 관리형 정책이 포함되어 있습니다. 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, 페더레이션 사용자 또는 AWS 서비스이(가) 포함될 수 있습니다.

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

액세스 제어 목록(ACL)

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

Amazon S3, AWS WAF 및 Amazon VPC는 ACL을 지원하는 대표적인 서비스입니다. ACL에 대해 자세히 알아보려면 Amazon Simple Storage Service 개발자 안내서의 ACL(액세스 제어 목록) 개요 섹션을 참조하세요.

기타 정책 유형

AWS은(는) 비교적 일반적이지 않은 추가 정책 유형을 지원합니다. 이러한 정책 유형은 더 일반적인 정책 유형에 따라 사용자에게 부여되는 최대 권한을 설정할 수 있습니다.

- 권한 경계 – 권한 경계는 ID 기반 정책에 따라 IAM 엔터티(IAM 사용자 또는 역할)에 부여할 수 있는 최대 권한을 설정하는 고급 기능입니다. 개체에 대한 권한 경계를 설정할 수 있습니다. 그 결과로 얻는 권한은 개체의 ID 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 AWS Organizations에서 조직 또는 조직 단위(OU)에 최대 권한을 지정하는 JSON 정책입니다. AWS Organizations는 기업이 소유하는 여러 개의 AWS 계정을 그룹화하고 중앙에서 관리하기 위한 서비스입니다. 조직에서 모든 기능을 활성화할 경우 서비스 제어 정책(SCP)을 임의의 또는 모든 계정에 적용할 수 있습니다. SCP는 각 AWS 계정 루트 사용자을(를) 비롯하여 멤버 계정의 엔터티에 대한 권한을 제한합니다. 조직 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 ID 기반 정책의 교차와 세션 정책입니다. 또한 권한을 리소스 기반 정책에서 가져올 수도 있습니다. 이러한 정책 중 하나에 포함된 명시적 거부는 허용을 재정의합니다. 자세한 정보는 IAM 사용 설명서의 세션 정책을 참조하세요.

여러 정책 유형

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

Amazon Detective가 IAM과 작동하는 방식

기본적으로 사용자 및 역할은 Amazon Detective 리소스를 생성하거나 수정할 수 있는 권한이 없습니다. 또한 AWS Management Console, AWS CLI또는 AWSAPI를 사용해 태스크를 수행할 수 없습니다. Detective 관리자는 필요한 지정된 리소스에서 특정 API 작업을 수행할 수 있는 IAM 사용자 및 역할 권한을 부여하는 AWS Identity and Access Management(IAM) 정책이 있어야 합니다. 그런 다음 관리자는 해당 권한이 필요한 보안 주체에 이러한 정책을 연결해야 합니다.

Detective는 IAM 자격 증명 기반 정책을 사용하여 다음 유형의 사용자 및 작업에 권한을 부여합니다.

- 관리자 계정 - 관리자 계정은 계정 데이터를 사용하는 동작 그래프의 소유자입니다. 관리자 계정은 멤버 계정을 초대하여 동작 그래프에 데이터를 제공할 수 있습니다. 또한 동작 그래프를 사용하여 해당 계정과 관련된 조사 결과 및 리소스를 분류하고 조사할 수 있습니다.

  관리자 계정이 아닌 사용자가 다양한 유형의 작업을 수행할 수 있도록 정책을 설정할 수 있습니다. 예를 들어 관리자 계정의 사용자는 멤버 계정을 관리할 권한만 가질 수 있습니다. 다른 사용자에게는 조사를 위해 동작 그래프를 사용할 권한만 있을 수 있습니다.
- 멤버 계정 - 멤버 계정은 동작 그래프에 데이터를 제공하도록 초대받은 계정입니다. 멤버 계정은 초대에 응답합니다. 초대를 수락한 후 멤버 계정은 동작 그래프에서 자신의 계정을 제거할 수 있습니다.

Detective 및 IAM을 기타 AWS 서비스 작업 방법을 개괄적으로 알아보려면 IAM 사용 설명서의 JSON 탭에서 정책 생성을 참조하세요.

Detective 자격 증명 기반 정책

IAM 자격 증명 기반 정책을 사용하면 허용되거나 거부되는 작업과 리소스는 물론, 작업이 허용되거나 거부되는 조건도 지정할 수 있습니다. Detective는 특정 작업, 리소스 및 조건 키를 지원합니다.

JSON 정책에서 사용하는 모든 요소에 대해 알고 싶은 경우 IAM 사용 설명서의 IAM JSON 정책 요소 참조를 참조하세요.

작업

관리자는 AWSJSON 정책을 사용하여 누가 무엇에 액세스할 수 있는지를 지정할 수 있습니다. 즉, 어떤 보안 주체가 어떤 리소스와 어떤 조건에서 작업을 수행할 수 있는 지를 지정할 수 있습니다.

JSON 정책의 `Action` 요소는 정책에서 액세스를 허용하거나 거부하는 데 사용할 수 있는 작업을 설명합니다. 일반적으로 정책 작업의 이름은 연결된 AWSAPI 작업의 이름과 동일합니다. 일치하는 API 작

업이 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 포함합니다.

정책 설명에는 `Action` 또는 `NotAction` 요소가 포함되어야 합니다. `Action` 요소는 정책에서 허용되는 작업을 나열합니다. `NotAction` 요소는 허용되지 않는 작업을 나열합니다.

Detective에 정의된 작업은 Detective를 사용하여 수행할 수 있는 작업을 반영합니다. Detective의 정책 작업에는 다음과 같은 접두사가 붙습니다: `detective:`.

예를 들어 `CreateMembers` API 작업으로 멤버 계정을 동작 그래프에 초대할 수 있는 권한을 부여하려면 해당 정책에 `detective:CreateMembers` 작업을 포함합니다.

단일 명령문에서 여러 작업을 지정하려면 다음과 같이 쉼표로 구분합니다. 예를 들어 멤버 계정의 경우 정책에는 초대 관리와 관련된 일련의 작업이 포함됩니다.

```
"Action": [
      "detective:ListInvitations",
      "detective:AcceptInvitation",
      "detective:RejectInvitation",
      "detective:DisassociateMembership
]
```

와일드카드(*)를 사용하여 여러 작업을 지정할 수도 있습니다. 예를 들어 동작 그래프에 사용되는 데이터를 관리하려면 Detective의 관리자 계정이 다음 작업을 수행할 수 있어야 합니다.

- 멤버 계정 목록 보기(`ListMembers`).
- 선택한 멤버 계정에 대한 정보 가져오기(`GetMembers`).
- 멤버 계정을 동작 그래프에 초대(`CreateMembers`).
- 동작 그래프에서 멤버 삭제(`DeleteMembers`).

이러한 작업을 별도로 나열하는 대신, `Members` 단어로 끝나는 모든 작업에 대한 액세스 권한을 부여할 수 있습니다. 이에 대한 정책에는 다음과 같은 작업이 포함될 수 있습니다.

```
"Action": "detective:*Members"
```

Detective 작업 목록을 보려면 서비스 권한 부여 참조의 Amazon Detective에서 정의한 작업을 참조하세요.

리소스

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

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

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

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

ARN 형식에 대한 자세한 내용은 Amazon 리소스 이름(ARNs) 및 AWS 서비스 네임스페이스를 참조하세요.

Detective의 경우 리소스 유형만 동작 그래프입니다. Detective의 동작 그래프 리소스에는 다음 ARN이 있습니다.

```
arn:aws:detective:${Region}:${AccountId}:graph:${GraphId}
```

예를 들어 동작 그래프는 다음과 같은 값을 가질 수 있습니다.

- 동작 그래프의 리전은 us-east-1입니다.
- 관리자의 계정 ID의 계정 ID는 111122223333입니다.
- 동작 그래프의 그래프 ID는 027c7c4610ea4aacaf0b883093cab899입니다.

Resource 문에서 이 동작 그래프를 식별하려면 다음 ARN을 사용합니다.

```
"Resource": "arn:aws:detective:us-
east-1:111122223333:graph:027c7c4610ea4aacaf0b883093cab899"
```

Resource 문에서 여러 리소스를 지정하려면 ARN을 쉼표로 구분합니다.

```
"Resource": [
      "resource1",
```

```
      "resource2"
]
```

예를 들어 둘 이상의 동작 그래프에서 동일한 AWS 계정을 멤버 계정으로 초대할 수 있습니다. 해당 멤버 계정의 정책에서 Resource 문에는 초대를 받은 동작 그래프가 나열되어 있습니다.

```
"Resource": [
      "arn:aws:detective:us-
east-1:111122223333:graph:027c7c4610ea4aacaf0b883093cab899",
      "arn:aws:detective:us-east-1:444455556666:graph:056d2a9521xi2bbluw1d164680eby416"
]
```

동작 그래프 생성, 동작 그래프 나열, 동작 그래프 초대 목록 작성과 같은 일부 Detective 작업은 특정 동작 그래프에서 수행되지 않습니다. 이러한 작업의 경우 Resource 문에 와일드카드(*)를 사용해야 합니다.

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

관리자 계정 작업의 경우 Detective는 요청하는 사용자가 영향을 받는 동작 그래프의 관리자 계정에 속하는지 항상 확인합니다. 멤버 계정 작업의 경우 Detective는 요청하는 사용자가 멤버 계정에 속하는지 항상 확인합니다. IAM 정책에서 동작 그래프에 대한 액세스 권한을 부여하더라도 사용자가 올바른 계정에 속하지 않으면 사용자는 작업을 수행할 수 없습니다.

특정 동작 그래프에서 수행되는 모든 작업에 대해 IAM 정책에는 그래프 ARN이 포함되어야 합니다. 그래프 ARN은 나중에 추가할 수 있습니다. 예를 들어, 계정이 처음으로 Detective를 활성화하면 초기 IAM 정책은 그래프 ARN의 와일드카드를 사용하여 모든 Detective 작업에 대한 액세스를 제공합니다. 이를 통해 사용자는 즉시 멤버 계정을 관리하고 동작 그래프에서 조사를 수행할 수 있습니다. 동작 그래프가 생성된 후 정책을 업데이트하여 그래프 ARN을 추가할 수 있습니다.

조건 키

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

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

한 문에서 여러 Condition 요소를 지정하거나 단일 Condition 요소에서 여러 키를 지정하는 경우 AWS는 논리적 AND 작업을 사용하여 평가합니다. 단일 조건 키의 여러 값을 지정하는 경우 AWS는 논

리적 OR 작업을 사용하여 조건을 평가합니다. 명문의 권한을 부여하기 전에 모든 조건을 충족해야 합니다.

조건을 지정할 때 자리표시자 변수를 사용할 수도 있습니다. 예를 들어, IAM 사용자에게 IAM 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.

AWS는 전역 조건 키와 서비스별 조건 키를 지원합니다. 모든 AWS 전역 조건 키를 보려면 IAM 사용 설명서의 AWS 전역 조건 컨텍스트 키 섹션을 참조하세요.

Detective는 자체 조건 키 집합을 정의하지 않습니다. 이는 일부 전역 조건 키를 사용하도록 지원합니다. 모든 AWS 전역 조건 키를 보려면 IAM 사용 설명서의 AWS 전역 조건 컨텍스트 키를 참조하세요.

조건 키를 사용할 수 있는 작업과 리소스를 알아보려면 Amazon Detective에서 정의한 작업을 참조하세요.

예제

Detective 자격 증명 기반 정책의 예를 보려면 Amazon Detective 자격 증명 기반 정책 예제 섹션을 참조하세요.

Detective 리소스 기반 정책(지원되지 않음)

Detective는 리소스 기반 정책을 지원하지 않습니다.

Detective 동작 그래프 태그를 기반으로 한 권한 부여

각 동작 그래프에 태그 값을 할당할 수 있습니다. 조건문에서 이러한 태그 값을 사용하여 동작 그래프에 대한 액세스를 관리할 수 있습니다.

태그 값의 조건문은 다음 형식을 사용합니다.

```
{"StringEquals"{"aws:ResourceTag/<tagName>": "<tagValue>"}}
```

예를 들어, `Department` 태그의 값이 `Finance`인 경우 다음 코드를 사용하여 작업을 허용하거나 거부할 수 있습니다.

```
{"StringEquals"{"aws:ResourceTag/Department": "Finance"}}
```

리소스 태그 값을 사용하는 정책의 예는 the section called “관리자 계정: 태그 값을 기반으로 액세스 제한” 섹션을 참조하세요.

Detective IAM 역할

IAM 역할은 특정 권한을 가지고 있는 AWS계정 내 엔터티입니다.

Detective에서 임시 보안 인증 정보 사용

임시 보안 인증을 사용하여 페더레이션을 통해 로그인하거나, IAM 역할을 맡거나, 크로스 계정 역할을 맡을 수 있습니다. AssumeRole 또는 GetFederationToken 같은 AWS STS API 작업을 호출하여 임시 보안 자격 증명을 가져옵니다.

Detective는 임시 보안 인증 정보 사용을 지원합니다.

서비스 연결 역할

서비스 연결 역할을 사용하면 AWS 서비스가 다른 서비스의 리소스에 액세스하여 사용자 대신 작업을 완료할 수 있습니다. 서비스 연결 역할은 IAM 계정에 나타나고 서비스가 소유합니다. IAM 관리자는 서비스 연결 역할의 권한을 볼 수 있지만 편집할 수 없습니다.

Detective 서비스 연결 역할을 생성 또는 관리하는 방법에 대한 자세한 내용은 the section called “서비스 연결 역할 사용” 섹션을 참조하세요.

서비스 역할(지원되지 않음)

이 기능을 사용하면 서비스가 사용자를 대신하여 서비스 역할을 수임할 수 있습니다. 이 역할을 사용하면 서비스가 다른 서비스의 리소스에 액세스해 사용자를 대신해 작업을 완료할 수 있습니다. 서비스 역할은 IAM 계정에 나타나고, 해당 계정이 소유합니다. 즉, IAM 관리자가 이 역할에 대한 권한을 변경할 수 있습니다. 그러나 권한을 변경하면 서비스의 기능이 손상될 수 있습니다.

Detective는 서비스 역할을 지원하지 않습니다.

Amazon Detective 자격 증명 기반 정책 예제

기본적으로 IAM 사용자 및 역할은 Detective 리소스를 생성하거나 수정할 수 있는 권한이 없습니다. 또한 AWS Management Console, AWS CLI또는 AWSAPI를 사용해 태스크를 수행할 수 없습니다.

IAM 관리자는 지정된 리소스에서 특정 API 작업을 수행할 수 있는 권한을 사용자와 역할에게 부여하는 IAM 정책을 생성해야 합니다. 그런 다음, 관리자는 해당 권한이 필요한 IAM 사용자 또는 그룹에 이러한 정책을 연결합니다.

이러한 예제 JSON 정책 문서를 사용하여 IAM ID 기반 정책을 생성하는 방법을 알아보려면 IAM 사용 설명서의 JSON 탭에서 정책 생성을 참조하세요.

주제

- 정책 모범 사례
- Detective 콘솔 사용
- 사용자가 자체 권한을 볼 수 있도록 허용
- 관리자 계정: 동작 그래프에서 멤버 계정 관리
- 관리자 계정: 조사를 위한 동작 그래프 사용
- 멤버 계정: 동작 그래프 초대 및 멤버십 관리
- 관리자 계정: 태그 값을 기반으로 액세스 제한

정책 모범 사례

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

- AWS 관리형 정책으로 시작하고 최소 권한을 향해 나아가기: 사용자 및 워크로드에 권한 부여를 시작하려면 많은 일반 사용 사례에 대한 권한을 부여하는 AWS 관리형 정책을 사용합니다. 관리형 정책은 AWS 계정에서 사용할 수 있습니다. 사용 사례에 고유한 AWS고객 관리형 정책을 정의하여 권한을 줄이는 것이 좋습니다. 자세한 정보는 IAM 사용 설명서의 AWS managed policies(관리형 정책) 또는 AWS managed policies for job functions(직무에 대한 관리형 정책) 섹션을 참조하세요.
- 최소 권한 적용: IAM 정책을 사용하여 권한을 설정하는 경우 태스크를 수행하는 데 필요한 권한만 부여합니다. 이렇게 하려면 최소 권한으로 알려진 특정 조건에서 특정 리소스에 대해 수행할 수 있는 작업을 정의합니다. IAM을 사용하여 권한을 적용하는 방법에 대한 자세한 정보는 IAM 사용 설명서의 IAM의 정책 및 권한을 참조하세요.
- IAM 정책의 조건을 사용하여 액세스 추가 제한: 정책에 조건을 추가하여 작업 및 리소스에 대한 액세스를 제한할 수 있습니다. 예를 들어 SSL을 사용하여 모든 요청을 전송해야 한다고 지정하는 정책 조건을 작성할 수 있습니다. 특정 AWS 서비스(예: AWS CloudFormation)을(를) 통해 사용되는 경우에만 서비스 작업에 대한 액세스 권한을 부여할 수도 있습니다. 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 IAM 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 작성하도록 돕습니다. 자세한 정보는 IAM 사용 설명서의 IAM Access Analyzer 정책 검증을 참조하세요.
- 다중 인증(MFA) 필요: AWS 계정 계정에 IAM 사용자 또는 루트 사용자가 필요한 시나리오가 있는 경우 추가 보안을 위해 MFA를 설정합니다. API 작업을 직접적으로 호출할 때 MFA가 필요하면 정

책에 MFA 조건을 추가합니다. 자세한 정보는 IAM 사용 설명서의 Configuring MFA-protected API access(MFA 보호 API 액세스 구성) 섹션을 참조하세요.

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

Detective 콘솔 사용

Amazon Detective 콘솔을 사용하려면 사용자 또는 역할이 API의 해당 작업과 일치하는 관련 작업에 액세스할 수 있어야 합니다.

Detective를 활성화하고 동작 그래프의 관리자 계정이 되려면 사용자 또는 역할에 `CreateGraph` 작업 권한을 부여해야 합니다.

Detective 콘솔을 사용하여 관리자 계정 작업을 수행하려면 사용자 또는 역할에 `ListGraphs` 작업에 대한 권한을 부여해야 합니다. 그러면 해당 계정이 관리자 계정인 동작 그래프를 검색할 수 있는 권한이 부여됩니다. 또한 특정 관리자 계정 작업을 수행할 수 있는 권한도 부여받아야 합니다.

가장 기본적인 관리자 계정 작업은 동작 그래프에서 멤버 계정 목록을 보고 동작 그래프를 사용하여 조사하는 것입니다.

- 동작 그래프에서 멤버 계정 목록을 보려면 보안 주체에게 해당 `ListMembers` 작업에 대한 권한을 부여해야 합니다.
- 동작 그래프에서 조사를 수행하려면 보안 주체에게 해당 `SearchGraph` 작업에 대한 권한을 부여해야 합니다.

Detective 콘솔을 사용하여 멤버 계정 작업을 수행하려면 사용자 또는 역할에 `ListInvitations` 작업 권한을 부여해야 합니다. 그러면 동작 그래프 초대를 볼 수 있는 권한이 부여됩니다. 그러면 특정 멤버 계정 작업에 대한 권한을 부여받을 수 있습니다.

사용자가 자체 권한을 볼 수 있도록 허용

이 예시는 IAM 사용자가 자신의 사용자 자격 증명에 연결된 인라인 및 관리형 정책을 볼 수 있도록 허용하는 정책을 생성하는 방법을 보여줍니다. 이 정책에는 콘솔에서 또는 AWS CLI나 AWS API를 사용하여 프로그래밍 방식으로 이 작업을 완료할 수 있는 권한이 포함됩니다.

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

```
            "Sid": "ViewOwnUserInfo",
            "Effect": "Allow",
            "Action": [
                "iam:GetUserPolicy",
                "iam:ListGroupsForUser",
                "iam:ListAttachedUserPolicies",
                "iam:ListUserPolicies",
                "iam:GetUser"
            ],
            "Resource": ["arn:aws:iam::*:user/${aws:username}"]
        },
        {
            "Sid": "NavigateInConsole",
            "Effect": "Allow",
            "Action": [
                "iam:GetGroupPolicy",
                "iam:GetPolicyVersion",
                "iam:GetPolicy",
                "iam:ListAttachedGroupPolicies",
                "iam:ListGroupPolicies",
                "iam:ListPolicyVersions",
                "iam:ListPolicies",
                "iam:ListUsers"
            ],
            "Resource": "*"
        }
    ]
}
```

관리자 계정: 동작 그래프에서 멤버 계정 관리

이 예제 정책은 동작 그래프에 사용되는 멤버 계정만 관리할 책임이 있는 관리자 계정 사용자를 대상으로 합니다. 또한 사용자가 사용 정보를 보고 Detective를 비활성화할 수 있도록 허용합니다. 이 정책은 조사를 위해 동작 그래프를 사용할 권한을 부여하지 않습니다.

```
{"Version":"2012-10-17",
  "Statement":[
   {
    "Effect":"Allow",
    "Action":
["detective:ListMembers","detective:CreateMembers","detective:DeleteMembers","detective:DeleteG
    "Resource":"arn:aws:detective:us-
east-1:111122223333:graph:027c7c4610ea4aacaf0b883093cab899"
```

```
  },
  {
    "Effect":"Allow",
    "Action":["detective:CreateGraph","detective:ListGraphs"],
    "Resource":"*"
  }
 ]
}
```

관리자 계정: 조사를 위한 동작 그래프 사용

이 예제 정책은 조사 목적으로만 동작 그래프를 사용하는 관리자 계정 사용자를 대상으로 합니다. 사용자는 동작 그래프에서 멤버 계정 목록을 보거나 편집할 수 없습니다.

```
{"Version":"2012-10-17",
  "Statement":[
   {
    "Effect":"Allow",
    "Action":["detective:SearchGraph"],
    "Resource":"arn:aws:detective:us-
east-1:111122223333:graph:027c7c4610ea4aacaf0b883093cab899"
   },
   {
    "Effect":"Allow",
    "Action":["detective:ListGraphs"],
    "Resource":"*"
  }
 ]
}
```

멤버 계정: 동작 그래프 초대 및 멤버십 관리

이 예제 정책은 멤버 계정에 속한 사용자를 대상으로 합니다. 이 예제에서 멤버 계정은 두 개의 동작 그래프에 속합니다. 이 정책은 초대에 응답하고 동작 그래프에서 멤버 계정을 제거할 권한을 부여합니다.

```
{"Version":"2012-10-17",
  "Statement":[
   {
    "Effect":"Allow",
   "Action":
["detective:AcceptInvitation","detective:RejectInvitation","detective:DisassociateMembership"],
   "Resource":[
```

```
       "arn:aws:detective:us-
east-1:111122223333:graph:027c7c4610ea4aacaf0b883093cab899",
       "arn:aws:detective:us-
east-1:444455556666:graph:056d2a9521xi2bbluw1d164680eby416"
    ]
  },
  {
    "Effect":"Allow",
    "Action":["detective:ListInvitations"],
    "Resource":"*"
  }
 ]
}
```

관리자 계정: 태그 값을 기반으로 액세스 제한

다음 정책은 사용자가 동작 그래프의 SecurityDomain 태그가 사용자의 SecurityDomain 태그와 일치하는지 여부를 조사하기 위해 동작 그래프를 사용할 수 있도록 허용합니다.

```
{
    "Version":"2012-10-17",
    "Statement":[ {
        "Effect":"Allow",
        "Action":["detective:SearchGraph"],
        "Resource":"arn:aws:detective:*:*:graph:*",
        "Condition": {
            "StringEquals"{
                "aws:ResourceTag/SecurityDomain": "aws:PrincipalTag/SecurityDomain"
            }
        }
    },
    {
        "Effect":"Allow",
        "Action":["detective:ListGraphs"],
        "Resource":"*"
    } ]
}
```

다음 정책은 동작 그래프의 SecurityDomain 태그 값이 Finance인 경우 사용자가 동작 그래프를 조사에 사용할 수 없도록 합니다.

```
{
```

```
    "Version":"2012-10-17",
    "Statement":[ {
        "Effect":"Deny",
        "Action":["detective:SearchGraph"],
        "Resource":"arn:aws:detective:*:*:graph:*",
        "Condition": {
            "StringEquals": {"aws:ResourceTag/SecurityDomain": "Finance"}
        }
    } ]
}
```

Amazon Detective 자격 증명 및 액세스 문제 해결

다음 정보를 사용하여 Detective 및 IAM에서 발생할 수 있는 공통적인 문제를 진단하고 수정할 수 있습니다. AWS Identity and Access Management(IAM) 작업 시 액세스 거부 문제 또는 이와 유사한 문제가 발생하면 IAM 사용자 안내서의 IAM 문제 해결 주제를 참조하세요.

Detective에서 작업을 수행할 권한이 없음

AWS Management Console에서 작업을 수행할 권한이 없다는 메시지가 나타나는 경우 관리자에게 문의하여 도움을 받아야 합니다. 관리자는 사용자 이름과 비밀번호를 제공한 사람입니다.

다음 예제 오류는 `mateojackson` IAM 사용자가 콘솔을 사용하여 동작 그래프의 멤버 계정이 되기 위한 초대를 수락하려고 하지만 `detective:AcceptInvitation` 권한이 없는 경우에 발생합니다.

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to
 perform: detective:AcceptInvitation on resource: arn:aws:detective:us-
east-1:444455556666:graph:567856785678
```

이 경우 Mateo는 `arn:aws:detective:us-east-1:444455556666:graph:567856785678`작업을 사용하여 `detective:AcceptInvitation`리소스에 액세스하도록 허용하는 정책을 업데이트하라고 관리자에게 요청합니다.

iam:PassRole을 수행하도록 인증되지 않음

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

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

다음 예제 오류는 marymajor라는 IAM 사용자가 콘솔을 사용하여 Detective에서 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:PassRole작업을 수행할 수 있도록 Mary의 정책을 업데이트해야 합니다.

도움이 필요한 경우 AWS 관리자에게 문의합니다. 관리자는 로그인 보안 인증을 제공한 사람입니다.

내 AWS 계정 외부의 사람이 내 Detective 리소스에 액세스하도록 허용하려고 함

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

자세히 알아보려면 다음을 참조하세요.

- Detective에서 이러한 기능을 지원하는지 여부를 알아보려면 Amazon Detective가 IAM과 작동하는 방식 섹션을 참조하세요.
- 소유하고 있는 AWS 계정의 리소스에 대한 액세스 권한을 제공하는 방법을 알아보려면 IAM 사용 설명서의 자신이 소유한 다른 AWS 계정의 IAM 사용자에 대한 액세스 권한 제공을 참조하세요.
- 리소스에 대한 액세스 권한을 타사 AWS 계정에게 제공하는 방법을 알아보려면 IAM 사용 설명서의 타사가 소유한 AWS 계정에 대한 액세스 제공을 참조하세요.
- ID 페더레이션을 통해 액세스 권한을 제공하는 방법을 알아보려면 IAM 사용 설명서의 외부에서 인증된 사용자에게 액세스 권한 제공(ID 페더레이션)을 참조하세요.
- 교차 계정 액세스를 위한 역할과 리소스 기반 정책 사용의 차이점을 알아보려면 IAM 사용 설명서의 IAM 역할과 리소스 기반 정책의 차이를 참조하세요.

Detective에 서비스 연결 역할 사용

Amazon Detective는 AWS Identity and Access Management(IAM) 서비스 연결 역할을 사용합니다. 서비스 연결 역할은 Detective에 직접 연결된 고유한 유형의 IAM 역할입니다. 서비스 연결 역할은 Detective에서 사전 정의하며 서비스에서 사용자 대신 다른 AWS 서비스를 호출하기 위해 필요한 모든 권한을 포함합니다.

서비스 연결 역할을 사용하면 필요한 권한을 수동으로 추가할 필요가 없으므로 Detective를 더 간편하게 설정할 수 있습니다. Detective에서 서비스 연결 역할의 권한을 정의하므로 다르게 정의되지 않은 한, Detective만 해당 역할을 수임할 수 있습니다. 정의된 권한에는 신뢰 정책과 권한 정책이 포함되며, 이 권한 정책은 다른 IAM 엔터티에 연결할 수 없습니다.

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

서비스 연결 역할을 지원하는 기타 서비스에 대한 자세한 내용은 IAM으로 작업하는 AWS 서비스를 참조하고 서비스 연결 역할 열에 예가 있는 서비스를 찾습니다. 해당 서비스에 대한 서비스 연결 역할 설명서를 보려면 [예(Yes)] 링크를 선택합니다.

Detective에 대한 서비스 연결 역할 권한

Detective는 AWSServiceRoleForDetective라는 서비스 연결 역할을 사용하며, 이를 통해 Detective가 사용자를 대신하여 AWS Organizations 정보에 액세스할 수 있습니다.

AWSServiceRoleForDetective 서비스 연결 역할은 역할을 수임하기 위해 다음 서비스를 신뢰합니다.

- `detective.amazonaws.com`

AWSServiceRoleForDetective 서비스 역할 연결 역할은 `AmazonDetectiveServiceLinkedRolePolicy`관리형 정책을 사용합니다.

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

Detective에 대한 서비스 연결 역할 생성

서비스 연결 역할은 수동으로 생성할 필요가 없습니다. AWS Management Console, AWS CLI 또는 AWS API에서 조직의 Detective 관리자 계정을 지정할 때 Detective는 서비스 연결 역할을 생성합니다.

이 서비스 연결 역할을 삭제한 다음 다시 생성해야 하는 경우 동일한 프로세스를 사용하여 계정에서 역할을 다시 생성할 수 있습니다. 조직의 Detective 관리자 계정을 지정할 때 Detective는 서비스 연결 역할을 다시 생성합니다.

Detective에 대한 서비스 연결 역할 편집

Detective는 AWSServiceRoleForDetective 서비스 연결 역할을 편집하도록 허용하지 않습니다. 서비스 연결 역할을 생성한 후에는 다양한 개체가 역할을 참조할 수 있기 때문에 역할 이름을 변경할 수 없습

니다. 하지만 IAM을 사용하여 역할의 설명을 편집할 수 있습니다. 자세한 내용은 IAM 사용 설명서의 서비스 연결 역할 편집을 참조하세요.

Detective에 대한 서비스 연결 역할 삭제

서비스 연결 역할이 필요한 기능 또는 서비스가 더 이상 필요 없는 경우에는 해당 역할을 삭제할 것을 권합니다. 따라서 적극적으로 모니터링하거나 유지하지 않는 미사용 개체가 없도록 합니다. 단, 서비스 연결 역할에 대한 리소스를 먼저 정리해야 수동으로 삭제할 수 있습니다.

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

AWSServiceRoleForDetective에서 사용하는 Detective 리소스 삭제

1. Detective 관리자 계정을 제거합니다. the section called “Detective 관리자 계정 지정” 섹션을 참조하세요.
2. Detective 관리자 계정을 지정한 각 리전에서 이 절차를 반복합니다.

IAM을 사용하여 수동으로 서비스 연결 역할 삭제

IAM 콘솔, AWS CLI 또는 AWS API를 사용하여 AWSServiceRoleForDetective 서비스 연결 역할을 삭제합니다. 자세한 내용은 IAM 사용 설명서의 서비스 연결 역할 삭제 섹션을 참조하세요.

Detective 서비스 연결 역할에 대해 지원되는 리전

Detective에서는 서비스를 사용할 수 있는 모든 리전에서 서비스 연결 역할 사용을 지원합니다. 자세한 내용은 AWS 리전 및 엔드포인트 단원을 참조하세요.

Amazon Detective의 AWS 관리형 정책

AWS 관리형 정책은 AWS에서 생성되고 관리되는 독립 실행형 정책입니다. AWS 관리형 정책은 사용자, 그룹 및 역할에 권한 할당을 시작할 수 있도록 많은 일반 사용 사례에 대한 권한을 제공하도록 설계되었습니다.

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

AWS 관리형 정책에서 정의한 권한은 변경할 수 없습니다. AWS에서 AWS 관리형 정책에 정의된 권한을 업데이트할 경우 정책이 연결되어 있는 모든 보안 주체 엔터티(사용자, 그룹 및 역할)에도 업데이트가 적용됩니다. 새로운 AWS 서비스를 시작하거나 새로운 API 작업을 기존 서비스에 이용하는 경우 AWS가 AWS 관리형 정책을 업데이트할 가능성이 높습니다.

자세한 내용은 IAM 사용 설명서의 AWS 관리형 정책을 참조하세요.

AWS 관리형 정책: AmazonDetectiveFullAccess

`AmazonDetectiveFullAccess` 정책을 IAM ID에 연결할 수 있습니다.

이 정책은 모든 Amazon Detective 작업에 대한 전체 액세스 권한을 허용하는 관리 권한을 보안 주체에게 부여합니다. 이 정책은 보안 주체가 해당 계정에 대해 Detective를 활성화하기 전에 보안 주체에게 연결할 수 있습니다. 또한 동작 그래프를 생성하고 관리하기 위해 Detective Python 스크립트를 실행하는 데 사용되는 역할에 연결되어야 합니다.

이러한 권한이 있는 보안 주체는 멤버 계정을 관리하고, 동작 그래프에 태그를 추가하고, Detective를 사용하여 조사할 수 있습니다. 또한 GuardDuty 조사 결과를 보관할 수도 있습니다. 이 정책은 Detective 콘솔에 AWS Organizations에 있는 계정의 계정 이름을 표시하는 데 필요한 권한을 제공합니다.

권한 세부 정보

이 정책에는 다음 권한이 포함되어 있습니다.

- `detective` – 보안 주체가 Detective 작업에 대한 모든 액세스 권한을 가질 수 있습니다.
- `organizations` – 보안 주체가 조직의 계정에 대한 AWS Organizations 정보를 검색할 수 있습니다. 계정이 조직에 속한 경우 이러한 권한을 통해 Detective 콘솔은 계정 번호 외에도 계정 이름을 표시할 수 있습니다.
- `guardduty` - 보안 주체가 Detective 내에서 GuardDuty 조사 결과를 가져오고 보관할 수 있습니다.
- `securityhub` - 보안 주체가 Detective 내에서 Security Hub 조사 결과를 가져올 수 있습니다.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "detective:*",
                "organizations:DescribeOrganization",
                "organizations:ListAccounts"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "guardduty:ArchiveFindings"
            ],
            "Resource": "arn:aws:guardduty:*:*:detector/*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "guardduty:GetFindings",
                "guardduty:ListDetectors"

            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                 "securityHub:GetFindings"
            ],
            "Resource": "*"
         }
    ]
}
```

AWS 관리형 정책: AmazonDetectiveMemberAccess

`AmazonDetectiveMemberAccess` 정책을 IAM 엔터티에 연결할 수 있습니다.

이 정책은 Amazon Detective에 대한 멤버 액세스 권한과 콘솔에 대한 범위 지정 액세스를 제공합니다.

이 정책을 통해 다음을 수행할 수 있습니다.

- Detective 그래프 멤버십 초대를 확인하고 해당 초대를 수락하거나 거부할 수 있습니다.
- 사용 페이지에서 Detective에서의 활동이 이 서비스 사용 비용에 어떻게 기여하는지 확인합니다.
- 그래프로 멤버십에서 탈퇴합니다.

이 정책은 Detective
콘솔에 대한 범위 지정 액세스를 허용하는 읽기 전용 권한을 부여합니다.

권한 세부 정보

이 정책에는 다음 권한이 포함되어 있습니다.

- `detective` - 멤버가 Detective에 액세스할 수 있습니다.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "detective:AcceptInvitation",
        "detective:BatchGetMembershipDatasources",
        "detective:DisassociateMembership",
        "detective:GetFreeTrialEligibility",
        "detective:GetPricingInformation",
        "detective:GetUsageInformation",
        "detective:ListInvitations",
        "detective:RejectInvitation"
      ],
      "Resource": "*"
    }
  ]
}
```

AWS 관리형 정책: AmazonDetectiveInvestigatorAccess

`AmazonDetectiveInvestigatorAccess` 정책을 IAM 엔터티에 연결할 수 있습니다.

이 정책은 Detective 서비스에 대한 조사자 액세스 권한과 콘솔 UI 종속성에 대한 범위 지정 액세스 권한을 제공합니다. 이 정책은 IAM 사용자 및 IAM 역할에 대해 Detective에서 Detective 조사를 활성화할 수 있는 권한을 부여합니다. 보안 지표에 대한 분석 및 통찰력을 제공하는 조사 보고서를 사용하여 조사 결과와 같은 손상 지표를 식별할 수 있습니다. 보고서는 Detective의 동작 분석 및 기계 학습을 사용하여 결정되는 심각도에 따라 순위가 매겨집니다. 보고서를 사용하여 리소스 문제 해결의 우선 순위를 정할 수 있습니다.

권한 세부 정보

이 정책에는 다음 권한이 포함되어 있습니다.

- `detective` - 보안 주체 조사자가 Detective 작업에 액세스하여 Detective 조사를 활성화하고 조사 결과 그룹 요약을 활성화할 수 있도록 합니다.
- `guardduty` - 보안 주체가 Detective 내에서 GuardDuty 조사 결과를 가져오고 보관할 수 있습니다.
- `securityhub` - 보안 주체가 Detective 내에서 Security Hub 조사 결과를 가져올 수 있습니다.
- `organizations` – 보안 주체가 AWS Organizations에서 조직의 계정에 대한 정보를 검색할 수 있습니다. 계정이 조직에 속하면 이러한 권한을 통해 Detective 콘솔은 계정 번호 외에도 계정 이름을 표시할 수 있습니다.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "DetectivePermissions",
      "Effect": "Allow",
      "Action": [
        "detective:BatchGetGraphMemberDatasources",
        "detective:BatchGetMembershipDatasources",
        "detective:DescribeOrganizationConfiguration",
        "detective:GetFreeTrialEligibility",
        "detective:GetGraphIngestState",
        "detective:GetMembers",
```

```
        "detective:GetPricingInformation",
        "detective:GetUsageInformation",
        "detective:ListDatasourcePackages",
        "detective:ListGraphs",
        "detective:ListHighDegreeEntities",
        "detective:ListInvitations",
        "detective:ListMembers",
        "detective:ListOrganizationAdminAccount",
        "detective:ListTagsForResource",
        "detective:SearchGraph",
        "detective:StartInvestigation",
        "detective:GetInvestigation",
        "detective:ListInvestigations",
        "detective:UpdateInvestigationState",
        "detective:ListIndicators",
        "detective:InvokeAssistant"
      ],
      "Resource": "*"
    },
    {
      "Sid": "OrganizationsPermissions",
      "Effect": "Allow",
      "Action": [
        "organizations:DescribeOrganization",
        "organizations:ListAccounts"
      ],
      "Resource": "*"
    },
    {
      "Sid": "GuardDutyPermissions",
      "Effect": "Allow",
      "Action": [
        "guardduty:ArchiveFindings",
        "guardduty:GetFindings",
        "guardduty:ListDetectors"
      ],
      "Resource": "*"
    },
    {
      "Sid": "SecurityHubPermissions",
      "Effect": "Allow",
      "Action": [
        "securityHub:GetFindings"
      ],
```

```
      "Resource": "*"
    }
  ]
}
```

AWS 관리형 정책: AmazonDetectiveOrganizationsAccess

`AmazonDetectiveOrganizationsAccess` 정책을 IAM 엔터티에 연결할 수 있습니다.

이 정책은 조직 내에서 Amazon Detective를 활성화하고 관리할 권한을 부여합니다. 조직 전체에서 Detective를 활성화하고 Detective의 위임된 관리자 계정을 결정할 수 있습니다.

권한 세부 정보

이 정책에는 다음 권한이 포함되어 있습니다.

- `detective` – 보안 주체가 Detective 작업에 대한 액세스 권한을 가질 수 있습니다.
- `iam` - Detective가 `EnableOrganizationAdminAccount`를 호출할 때 서비스 연결 역할이 생성되도록 지정합니다.
- `organizations` – 보안 주체가 AWS Organizations에서 조직의 계정에 대한 정보를 검색할 수 있습니다. 계정이 조직에 속하면 이러한 권한을 통해 Detective 콘솔은 계정 번호 외에도 계정 이름을 표시할 수 있습니다. AWS 서비스 통합을 활성화하고, 지정된 멤버 계정을 위임된 관리자로 등록 및 등록 취소할 수 있으며, 보안 주체가 Amazon Detective, Amazon GuardDuty, Amazon Macie, AWS Security Hub 등과 같은 다른 보안 서비스에서 위임된 관리자 계정을 검색할 수 있습니다.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "detective:DisableOrganizationAdminAccount",
        "detective:EnableOrganizationAdminAccount",
        "detective:ListOrganizationAdminAccount"
      ],
      "Resource": "*"
    },
    {
```

```
      "Effect": "Allow",
      "Action": [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "iam:AWSServiceName": "detective.amazonaws.com"
        }
      }
    },
    {
      "Effect": "Allow",
      "Action": [
        "organizations:EnableAWSServiceAccess",
        "organizations:RegisterDelegatedAdministrator",
        "organizations:DeregisterDelegatedAdministrator"
      ],
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "organizations:ServicePrincipal": [
            "detective.amazonaws.com"
          ]
        }
      }
    },
    {
      "Effect": "Allow",
      "Action": [
        "organizations:DescribeAccount",
        "organizations:DescribeOrganization",
        "organizations:ListAccounts"
      ],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": [
        "organizations:ListDelegatedAdministrators"
      ],
      "Resource": "*",
      "Condition": {
        "StringEquals": {
```

```
          "organizations:ServicePrincipal": [
            "detective.amazonaws.com",
            "guardduty.amazonaws.com",
            "macie.amazonaws.com",
            "securityhub.amazonaws.com"
          ]
        }
      }
    }
  ]
}
```

AWS 관리형 정책: AmazonDetectiveServiceLinkedRole

`AmazonDetectiveServiceLinkedRole` 정책을 IAM 엔터티에 연결할 수 없습니다. 이 정책은 Detective에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 자세한 내용은 the section called “서비스 연결 역할 사용” 섹션을 참조하세요.

이 정책은 서비스 연결 역할이 조직의 계정 정보를 검색할 수 있도록 하는 관리 권한을 부여합니다.

권한 세부 정보

이 정책에는 다음 권한이 포함되어 있습니다.

- `organizations` - 조직의 계정 정보를 검색합니다.

```
{
  "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
              "organizations:DescribeAccount",
              "organizations:ListAccounts"
            ],
            "Resource": "*"
        }
    ]
}
```

AWS 관리형 정책에 대한 Detective 업데이트

이 서비스가 이러한 변경 내용을 추적하기 시작한 이후부터 Detective의 AWS 관리형 정책 업데이트에 대한 세부 정보를 봅니다. 이 페이지의 변경 사항에 대한 자동 알림을 받으려면 문서 기록 페이지에서 RSS 피드를 구독하세요.

변경 사항	설명	날짜
AmazonDetectiveInvestigatorAccess - 기존 정책에 대한 업데이트	Detective 조사 및 조사 결과 그룹 요약 작업을 `AmazonDetectiveInvestigatorAccess` 정책에 추가했습니다. 이러한 작업을 통해 Detective 조사를 시작, 검색 및 업데이트하고 Detective 내에서 조사 결과 그룹 요약을 얻을 수 있습니다.	2023년 11월 26일
AmazonDetectiveFullAccess 및 AmazonDetectiveInvestigatorAccess - 기존 정책 업데이트	Detective는 `AmazonDetectiveFullAccess` 및 `AmazonDetectiveInvestigatorAccess` 정책에 Security Hub `GetFindings` 작업을 추가했습니다. 이러한 작업을 통해 Detective 내에서 Security Hub 조사 결과를 가져올 수 있습니다.	2023년 5월 16일
AmazonDetectiveOrganizationsAccess - 새 정책	Detective는 `AmazonDetectiveOrganizationsAccess` 정책을 추가했습니다. 이 정책은 조직 내에서 Detective를 활성화하고 관리할 권한을 부여합니다.	2023년 3월 2일

변경 사항	설명	날짜
AmazonDetectiveMemberAccess - 새 정책	Detective는 `AmazonDetectiveMemberAccess` 정책을 추가했습니다. 이 정책은 멤버에게 Detective에 대한 액세스 권한과 콘솔 UI 종속성에 대한 범위 지정 액세스 권한을 제공합니다.	2023년 1월 17일
AmazonDetectiveFullAccess - 기존 정책에 대한 업데이트	Detective는 GuardDuty `GetFindings` 작업을 `AmazonDetectiveFullAccess` 정책에 추가했습니다. 이러한 작업을 통해 Detective 내에서 GuardDuty 조사 결과를 가져올 수 있습니다.	2023년 1월 17일
AmazonDetectiveInvestigatorAccess - 새 정책	Detective는 `AmazonDetectiveInvestigatorAccess` 정책을 추가했습니다. 이 정책을 통해 보안 주체가 Detective에서 조사를 수행할 수 있습니다.	2023년 1월 17일
AmazonDetectiveServiceLinkedRole - 새 정책	Detective는 해당 서비스 연결 역할에 대한 새 정책을 추가했습니다. 이 정책은 서비스 연결 역할이 조직의 계정에 대한 정보를 검색할 수 있도록 허용합니다.	2021년 12월 16일
Detective가 변경 사항 추적하기 시작	Detective는 AWS 관리형 정책에 대한 변경 사항 추적을 시작했습니다.	2021년 5월 10일

Amazon Detective의 로깅 및 모니터링

Amazon Detective는 AWS CloudTrail과 통합되었습니다. CloudTrail은 Detective에 대한 모든 API 직접 호출을 이벤트로 캡처합니다.

Detective의 CloudTrail 로깅 사용에 대한 자세한 내용은 the section called “CloudTrail을 사용하여 Detective API 직접 호출 로깅” 섹션을 참조하세요.

Amazon Detective에 대한 규정 준수 확인

Amazon Detective는 AWS 보증 프로그램 적용 범위에 포함됩니다. 자세한 내용은 Health Information Trust Alliance Common Security Framework(HITRUST) CSF를 참조하세요.

특정 규정 준수 프로그램의 범위 내에 있는 AWS 서비스 목록은 규정 준수 프로그램 제공 범위 내 AWS 서비스를 참조하십시오. 일반적인 정보는 AWS 규정 준수 프로그램을 참조하세요.

AWS Artifact를 사용하여 타사 감사 보고서를 다운로드할 수 있습니다. 자세한 내용은 AWS Artifact에서 보고서 다운로드를 참조하십시오.

AWS는 규정 준수에 도움이 되도록 다음 리소스를 제공합니다.

- 보안 및 규정 준수 빠른 시작 안내서 – 이 배포 안내서에서는 아키텍처 고려 사항에 관해 설명하고 AWS에서 보안 및 규정 준수에 중점을 둔 기본 환경을 배포하기 위한 단계를 제공합니다.
- AWS Config 개발자 가이드의 규칙을 사용하여 리소스 평가 – AWS Config 서비스는 내부 사례, 산업 지침 및 규제에 대한 리소스 구성의 준수 상태를 평가합니다.
- AWS Security Hub - 이 AWS 서비스는 보안 산업 표준 및 모범 사례 규정 준수 여부를 확인하는 데 도움이 되도록 AWS 내 보안 상태를 종합적으로 보여줍니다.

Amazon Detective의 복원성

AWS 글로벌 인프라는 AWS 리전 및 가용 영역을 중심으로 구축됩니다. AWS 리전은 물리적으로 분리되고 격리된 다수의 가용 영역을 제공하며 이러한 가용 영역은 짧은 지연 시간, 높은 처리량 및 높은 중복성을 갖춘 네트워크에 연결되어 있습니다. 가용 영역을 사용하면 중단 없이 영역 간에 자동으로 장애 조치가 이루어지는 애플리케이션 및 데이터베이스를 설계하고 운영할 수 있습니다. 가용 영역은 기존의 단일 또는 다중 데이터 센터 인프라보다 가용성, 내결함성, 확장성이 뛰어납니다.

AWS 리전 및 가용 영역에 대한 자세한 내용은 AWS 글로벌 인프라를 참조하세요.

Detective는 AWS 글로벌 인프라 외에도 Amazon DynamoDB 및 Amazon Simple Storage Service(S3)에 내장된 복원성 또한 활용합니다.

Detective 아키텍처는 단일 가용 영역의 장애에도 탄력적입니다. 이러한 복원성은 Detective에 내장되어 있으며 구성이 필요하지 않습니다.

Amazon Detective의 인프라 보안

관리형 서비스인 Amazon Detective는 AWS 글로벌 네트워크 보안으로 보호됩니다. AWS 보안 서비스와 AWS의 인프라 보호 방법에 대한 자세한 내용은 AWS 클라우드 보안을 참조하세요. 인프라 보안에 대한 모범 사례를 사용하여 AWS 환경을 설계하려면 보안 원칙 AWS Well-Architected Framework의 인프라 보호를 참조하세요.

AWS에서 게시한 API 직접 호출을 사용하여 네트워크를 통해 액세스합니다. 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 보안 액세스 키를 사용하여 서명해야 합니다. 또는 AWS Security Token Service(AWS STS)를 사용하여 임시 보안 자격 증명을 생성하여 요청에 서명할 수 있습니다.

Amazon Detective의 보안 모범 사례

Detective는 자체 보안 정책을 개발하고 구현할 때 고려해야 할 여러 보안 기능을 제공합니다. 다음 모범 사례는 일반적인 지침이며 완벽한 보안 솔루션을 나타내지는 않습니다. 이러한 모범 사례는 환경에 적절하지 않거나 충분하지 않을 수 있으므로 참고용으로만 사용해 주세요.

Detective의 경우 보안 모범 사례는 동작 그래프에서의 계정 관리와 관련이 있습니다.

계정 관리자를 위한 모범 사례

멤버 계정을 동작 그래프에 초대할 때는 감독하는 계정만 초대합니다.

동작 그래프에 대한 액세스를 제한합니다. 동작 그래프에 액세스할 수 있는 사용자는 멤버 계정에 대한 모든 조사 결과를 볼 수 있습니다. 이러한 조사 결과로 인해 민감한 보안 정보가 노출될 수 있습니다.

멤버 계정의 모범 사례

동작 그래프에 대한 초대를 받으면 초대의 출처를 확인해야 합니다.

초대를 보낸 관리자 계정의 AWS 계정 식별자를 확인합니다. 계정이 누구의 소유인지 알고 있는지, 초대 계정에 보안 데이터를 모니터링할 정당한 이유가 있는지 확인합니다.

Amazon Detective 비활성화

동작 그래프의 관리자 계정은 Detective 콘솔, Detective API 또는 AWS Command Line Interface에서 Amazon Detective를 비활성화할 수 있습니다. Detective를 비활성화하면 동작 그래프 및 관련 Detective 데이터가 삭제됩니다.

동작 그래프를 삭제한 후에는 복원할 수 없습니다.

목차

Detective 비활성화(콘솔)

AWS Management Console에서 Amazon Detective를 비활성화할 수 있습니다.

Detective 비활성화(콘솔)

1. https://console.aws.amazon.com/detective/에서 Amazon Detective 콘솔을 엽니다.
2. Detective 탐색 창의 설정 아래에서 일반을 선택합니다.
3. 일반 페이지의 Detective 비활성화화에서 Detective 비활성화를 선택합니다.
4. 확인 메시지가 나타나면 **`disable`**을 입력합니다.
5. Detective 비활성화를 선택합니다.

Detective 비활성화(Detective API, AWS CLI)

Detective API 또는 AWS Command Line Interface에서 Amazon Detective를 비활성화할 수 있습니다. 요청에 사용할 동작 그래프의 ARN을 가져오려면 `ListGraphs` 작업을 사용합니다.

Detective 비활성화(Detective API, AWS CLI)

- Detective API: `DeleteGraph` 작업을 사용합니다. 그래프 ARN을 제공해야 합니다.
- AWS CLI: 명령줄에서 `delete-graph` 명령을 실행합니다.

```
aws detective delete-graph --graph-arn <graph ARN>
```

예제:

```
aws detective delete-graph --graph-arn arn:aws:detective:us-
east-1:111122223333:graph:123412341234
```

리전 간 Detective 비활성화(GitHub의 Python 스크립트)

Detective는 GitHub에서 오픈 소스 스크립트를 제공하여 지정된 리전 목록의 관리자 계정에 대해 Detective를 비활성화할 수 있습니다.

GitHub 스크립트를 구성하고 사용하는 방법에 대한 자세한 내용은 Amazon Detective Python 스크립트 사용 섹션을 참조하세요.

Amazon Detective Python 스크립트 사용

Amazon Detective는 GitHub 리포지토리 amazon-detective-multiaccount-scripts에서 오픈 소스 Python 스크립트 세트를 제공합니다. 스크립트에는 Python 3이 필요합니다.

이를 사용하여 다음 작업을 수행할 수 있습니다.

- 여러 리전의 관리자 계정에 대해 Detective를 활성화합니다.

  Detective를 활성화하면 동작 그래프에 태그 값을 할당할 수 있습니다.
- 리전별 관리자 계정의 동작 그래프에 멤버 계정을 추가합니다.
- 선택적으로 멤버 계정에 초대 이메일을 보낼 수 있습니다. 초대 이메일을 보내지 않도록 요청을 구성할 수도 있습니다.
- 관리자 계정의 리전별 동작 그래프에서 멤버 계정을 제거합니다.
- 여러 리전의 관리자 계정에 대해 Detective를 비활성화합니다. 관리자 계정이 Detective를 비활성화하면 각 리전의 관리자 계정 동작 그래프가 비활성화됩니다.

`enableDetective.py` 스크립트 개요

`enableDetective.py` 스크립트는 다음 작업을 수행합니다.

1. 지정된 각 리전의 관리자 계정에 Detective가 아직 활성화되어 있지 않은 경우, 해당 리전의 관리자 계정에 대해 Detective를 활성화합니다.

   스크립트를 사용하여 Detective를 활성화하면 동작 그래프에 태그 값을 할당할 수 있습니다.
2. 선택적으로 관리자 계정에서 각 동작 그래프의 지정된 멤버 계정으로 초대를 보냅니다.

   초대 이메일 메시지는 기본 메시지 콘텐츠를 사용하며 사용자 지정할 수 없습니다.

   초대 이메일을 보내지 않도록 요청을 구성할 수도 있습니다.
3. 멤버 계정에 대한 초대를 자동으로 수락합니다.

   스크립트가 초대를 자동으로 수락하므로 멤버 계정은 이러한 메시지를 무시할 수 있습니다.

   초대가 자동으로 수락된다는 사실을 멤버 계정에 직접 문의하여 알리는 것이 좋습니다.

disableDetective.py 스크립트 개요

disableDetective.py 스크립트는 지정된 리전의 관리자 계정 동작 그래프에서 지정된 멤버 계정을 삭제합니다.

또한 지정된 리전의 관리자 계정에 대해 Detective를 비활성화하는 옵션도 제공합니다.

스트립트에 필요한 권한

스크립트에는 관리자 계정과 추가 또는 제거한 모든 멤버 계정의 기존 AWS 역할이 필요합니다.

> **Note**
>
> 역할 이름은 모든 계정에서 동일해야 합니다.

IAM 정책에서 권장하는 모범 사례는 범위가 가장 적은 역할을 사용하는 것입니다. 그래프 생성, 멤버 생성, 그래프에 멤버 추가 등의 스크립트 워크플로를 실행하려면 다음과 같은 권한이 필요합니다.

- detective:CreateGraph
- detective:CreateMembers
- detective:DeleteGraph
- detective:DeleteMembers
- detective:ListGraphs
- detective:ListMembers
- detective:AcceptInvitation

역할 신뢰 관계

역할 신뢰 관계를 통해 인스턴스 또는 로컬 보안 인증 정보가 역할을 맡을 수 있어야 합니다.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::<ACCOUNTID>:user/<USERNAME>"
```

```
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

필수 권한이 포함된 공통 역할이 없는 경우 각 멤버 계정에서 최소한 해당 권한을 가진 역할을 만들어야 합니다. 또한 관리자 계정에서 역할을 만들어야 합니다.

역할을 생성하는 경우 다음을 수행해야 합니다.

- 모든 계정에서 동일한 역할 이름을 사용합니다.
- 위의 필수 권한을 추가하거나(권장) AmazonDetectiveFullAccess 관리형 정책을 선택합니다.
- 위에서 설명한 대로 역할 신뢰 관계 블록을 추가합니다.

이 프로세스를 자동화하기 위해 `EnableDetective.yaml` AWS CloudFormation 템플릿을 사용할 수 있습니다. 템플릿은 글로벌 리소스만 생성하므로 모든 리전에서 실행할 수 있습니다.

Python 스크립트를 위한 실행 환경 설정

EC2 인스턴스 또는 로컬 시스템에서 스크립트를 실행할 수 있습니다.

EC2 인스턴스 시작 및 구성

스크립트를 실행하는 한 가지 옵션은 EC2 인스턴스에서 스크립트를 실행하는 것입니다.

EC2 인스턴스 시작 및 구성

1. 관리자 계정에서 EC2 인스턴스를 시작합니다. EC2 인스턴스 시작 방법에 대한 세부 정보는 Linux 용 Amazon EC2 사용 설명서의 Amazon EC2 Linux 인스턴스 시작하기를 참조하세요.
2. 인스턴스가 관리자 계정 `AssumeRole` 내에서 호출할 수 있도록 허용하는 권한이 있는 IAM 역할을 인스턴스에 연결합니다.

   `EnableDetective.yaml` AWS CloudFormation템플릿을 사용한 경우 `EnableDetective` 이름이 지정된 프로필이 있는 인스턴스 역할이 생성됩니다.

   또는 인스턴스 역할 생성에 대한 자세한 내용은 EC2 콘솔을 사용하여 기존 EC2 인스턴스에 IAM 역할을 쉽게 교체 또는 연결 블로그 게시물을 참조하세요.
3. 필수 소프트웨어 설치:

- APT: `sudo apt-get -y install python3-pip python3 git`
- RPM: `sudo yum -y install python3-pip python3 git`
- Boto(최소 버전 1.15): `sudo pip install boto3`

4. 리포지토리를 EC2 인스턴스에 복제합니다.

```
git clone https://github.com/aws-samples/amazon-detective-multiaccount-scripts.git
```

스크립트를 실행하도록 로컬 시스템 구성

로컬 시스템에서 스크립트를 실행할 수도 있습니다.

스크립트를 실행하도록 로컬 시스템 구성

1. `AssumeRole` 호출 권한이 있는 관리자 계정의 로컬 시스템 보안 인증 정보를 설정했는지 확인합니다.
2. 필수 소프트웨어 설치:

   - Python 3
   - Boto(최소 버전 1.15)
   - GitHub 스크립트

플랫폼	설치 지침
Windows	1. Python 3(https://www.python.org/downloads/windows/)을 설치합니다. 2. 명령 프롬프트를 엽니다. 3. Boto를 설치하려면 `pip install boto3`을 실행합니다. 4. GitHub(https://github.com/aws-samples/amazon-detective-multiaccount-scripts)에서 스크립트 소스 코드를 다운로드합니다.
Mac	1. Python 3(https://www.python.org/downloads/mac-osx/)을 설치합니다. 2. 명령 프롬프트를 엽니다.

플랫폼	설치 지침
	3. Boto를 설치하려면 `pip install boto3`을 실행합니다. 4. GitHub(https://github.com/aws-samples/amazon-detective-multiaccount-scripts)에서 스크립트 소스 코드를 다운로드합니다.
Linux	1. Python 3를 설치하려면 다음 중 하나를 실행합니다. • `sudo apt-get -y install install python3-pip python3 git` • `sudo yum install git python` 2. Boto를 설치하려면 `sudo pip install boto3`을 실행합니다. 3. https://github.com/aws-samples/amazon-detective-multiaccount-scripts에서 스크립트 소스 코드를 복제합니다.

추가 또는 제거할 멤버 계정 `.csv` 목록 생성

동작 그래프에 추가하거나 동작 그래프에서 제거할 멤버 계정을 식별하려면 계정 목록이 포함된 `.csv` 파일을 제공합니다.

각 계정을 별도의 줄에 나열합니다. 각 멤버 계정 항목에는 AWS 계정 ID와 계정의 루트 사용자 이메일 주소가 포함됩니다.

다음 예를 참조하세요.

```
111122223333,srodriguez@example.com
444455556666,rroe@example.com
```

`enableDetective.py` 실행

EC2 인스턴스 또는 로컬 시스템에서 `enableDetective.py` 스크립트를 실행할 수 있습니다.

`enableDetective.py`를 실행하려면

1. `.csv` 파일을 EC2 인스턴스 또는 로컬 시스템의 `amazon-detective-multiaccount-scripts` 디렉터리에 복사합니다.

2. 디렉터리를 amazon-detective-multiaccount-scripts로 변경합니다.
3. enableDetective.py스크립트 실행.

```
enableDetective.py --master_account administratorAccountID --assume_role roleName
 --input_file inputFileName --tags tagValueList --enabled_regions regionList  --
disable_email
```

스크립트를 실행할 때 다음 값을 바꿉니다.

administratorAccountID

관리자의 계정의 AWS 계정 ID.

roleName

관리자 계정 및 각 멤버 계정에서 맡을 AWS 역할의 이름.

inputFileName

관리자 계정의 동작 그래프에 추가할 멤버 계정 목록이 들어 있는 .csv 파일 이름.

tagValueList

(선택 사항) 새 동작 그래프에 할당할 쉼표로 구분된 태그 값 목록.

각 태그 값의 형식은 *key*=*value*입니다. 예:

```
--tags Department=Finance,Geo=Americas
```

regionList

(선택 사항) 관리자 계정의 동작 그래프에 멤버 계정을 추가할 리전의 쉼표로 구분된 목록입니다. 예:

```
--enabled_regions us-east-1,us-east-2,us-west-2
```

관리자 계정의 경우 리전에서 Detective를 아직 활성화하지 않았을 수 있습니다. 이 경우 스크립트는 Detective를 활성화하고 관리자 계정을 위한 새 동작 그래프를 생성합니다.

리전 목록을 제공하지 않는 경우 스크립트는 Detective가 지원하는 모든 리전에서 작동합니다.

--disable_email

(선택 사항) 포함된 경우 Detective는 멤버 계정에 초대 이메일을 보내지 않습니다.

disableDetective.py 실행

EC2 인스턴스 또는 로컬 시스템에서 disableDetective.py 스크립트를 실행할 수 있습니다.

disableDetective.py를 실행하려면

1. .csv 파일을 amazon-detective-multiaccount-scripts 디렉터리로 복사합니다.
2. .csv 파일을 사용하여 지정된 리전 목록에 대한 관리자 계정의 동작 그래프에서 나열된 멤버 계정을 삭제하려면 다음과 같이 disableDetective.py 스크립트를 실행합니다.

```
disabledetective.py --master_account administratorAccountID --assume_role roleName
 --input_file inputFileName --disabled_regions regionList
```

3. 모든 리전의 관리자 계정에 대해 Detective를 비활성화하려면 --delete-master 플래그를 사용하여 disableDetective.py 스크립트를 실행합니다.

```
disabledetective.py --master_account administratorAccountID --assume_role roleName
 --input_file inputFileName --disabled_regions regionList --delete_master
```

스크립트를 실행할 때 다음 값을 바꿉니다.

administratorAccountID

관리자의 계정의 AWS 계정 ID.

roleName

관리자 계정 및 각 멤버 계정에서 맡을 AWS 역할의 이름.

inputFileName

관리자 계정의 동작 그래프에서 제거할 멤버 계정 목록이 들어 있는 .csv 파일 이름.

Detective를 비활성화한 경우에도 .csv 파일을 제공해야 합니다.

regionList

(선택 사항) 다음 중 하나를 수행할 수 있는 쉼표로 구분된 리전 목록입니다.

- 관리자 계정의 동작 그래프에서 멤버 계정을 제거합니다.
- --delete-master 플래그가 포함된 경우 Detective를 비활성화합니다.

예:

```
--disabled_regions us-east-1,us-east-2,us-west-2
```

리전 목록을 제공하지 않는 경우 스크립트는 Detective가 지원하는 모든 리전에서 작동합니다.

Detective 관리 가이드에 대한 문서 기록

다음 테이블에서는 Detective의 최신 릴리스가 발표된 이후 이 설명서에서 변경된 중요 사항에 대해 설명합니다. 이 설명서에 대한 업데이트 알림을 받으려면 RSS 피드를 구독하면 됩니다.

- 최신 설명서 업데이트: 2024년 2월 2일

변경 사항	설명	날짜
Amazon GuardDuty 멤버십 요구 사항 제거	더 이상 GuardDuty 고객이 아니어도 Amazon Detective를 활성화할 수 있습니다. Detective를 GuardDuty 활성화하기 전에 48시간 동안 계정에서 활성화해야 한다는 요구 사항이 제거되었습니다.	2024년 2월 2일
Detective가 공유 VPC의 흐름 트래픽을 읽는 방식의 변경 사항	공유 Amazon VPC를 사용하는 경우, Detective에서 모니터링하는 트래픽의 변화를 확인할 수 있습니다. 전체 VPC 흐름량에 대한 활동 세부 정보의 변경 사항을 검토하여 적용 범위에 미치는 잠재적 영향을 이해하고, Detective에서 예상 비용을 계산하는 방법을 검토하여 서비스 비용에 어떤 영향을 미칠 수 있는지 이해하는 것이 좋습니다.	2023년 12월 20일
보안 장에 관리형 정책 정보 추가	Detective 조사 및 조사 결과 그룹 요약 작업을 `AmazonDetectiveInvestigatorAccess` 정책에 추가했습니다.	2023년 11월 26일

Amazon Detective 엔드포인트 및 할당량	이제 이스라엘(텔아비브) 리전에서 Detective를 사용할 수 있습니다.	2023년 8월 25일
AWS 보안 탐지 결과를 새로운 선택적 데이터 소스 패키지로 추가했습니다.	Detective는 이제 AWS 보안 탐지 결과를 선택적 데이터 소스 패키지로 제공합니다. 이 선택적 데이터 소스 패키지를 사용하면 Detective가 Security Hub에서 데이터를 수집하여 동작 그래프에 추가할 수 있습니다.	2023년 5월 16일
Detective 콘솔에 새 콘솔 패널이 추가되어 사용자가 특정 사용 사례에 적합한 AWS 관리형 정책을 선택할 수 있도록 지원합니다.	Detective는 안전한 관리형 정책을 제공합니다. 필요한 권한을 선택합니다.	2023년 4월 3일
보안 장에 관리형 정책 정보 추가	Detective는 이제 정책을 통한 검색 결과 GuardDuty 가져오기 작업을 지원합니다. AmazonDetectiveFullAccess 이제 보안 장에서는 Detective의 다음과 같은 새로운 관리형 정책에 대한 세부 정보를 제공합니다: 및. AmazonDetectiveMemberAccess AmazonDetectiveInvestigatorAccess	2023년 1월 17일
데이터 보존 추가	Detective를 사용하면 최대 1년 분량의 과거 이벤트 데이터에 액세스할 수 있습니다.	2022년 12월 20일

조사 결과 그룹과 관련된 용어 추가	이제 Detective는 관련 조사 결과를 단일 디스플레이로 연결하는 조사 결과 그룹을 지원하여 사용자 환경의 잠재적 악의적 활동을 조사할 수 있습니다. 조사 결과 그룹 프로필에서 엔터티 프로필 및 해당 그룹과 관련된 조사 결과 개요로 피벗할 수 있습니다.	2022년 8월 3일
새 선택적 데이터 소스 추가	이제 Detective는 EKS 감사 로그를 선택적 데이터 소스 패키지로 지원합니다. 관리자 계정은 기존 동작 그래프에 이 새 데이터 소스를 활성화할 수 있습니다. 이 날짜 이후에 생성된 그래프에는 이 데이터 소스가 기본적으로 활성화됩니다. 관리자는 언제든지 이 데이터 소스를 수동으로 비활성화할 수 있습니다.	2022년 7월 26일
Detective를 위한 새 서비스 연결 역할 및 관리형 정책	이제 Detective에는 서비스 연결 역할 `AWSServiceRoleForDetective` 가 있습니다. 서비스 연결 역할을 통해 사용자를 대신하여 Organizations 데이터에 액세스할 수 있습니다. 역할은 새 `AmazonDetectiveServiceLinkedRolePolicy` 관리형 정책을 사용합니다.	2021년 12월 16일

다음과 통합이 추가되었습니다. AWS Organizations	이제 Detective는 Organizations와 통합됩니다. 조직 관리 계정은 조직의 Detective 관리자 계정을 지정합니다. Detective 관리자 계정은 조직의 모든 계정을 볼 수 있고, 조직 동작 그래프에서 해당 계정을 멤버 계정으로 활성화할 수 있습니다.	2021년 12월 16일
동작 그래프 데이터 볼륨 할당량 값 추가	동작 그래프의 데이터 볼륨 할당량이 증가되었습니다. Detective는 일일 3.24TB에서 경고를 보냅니다. 일일 3.6TB에서는 새 계정을 추가할 수 없습니다. Detective는 일일 4.5TB에서 동작 그래프에 데이터를 더 이상 수집하지 않습니다.	2021년 6월 10일
Python 스크립트 옵션에 태그 값 추가	이제 Detective Python script `enableDetective.py` 을 사용하여 Detective를 활성화하면 동작 그래프에 태그 값을 할당할 수 있습니다.	2021년 5월 19일

데이터 볼륨 검사를 통과한 멤버 계정을 자동으로 활성화하는 기능 추가	멤버 계정이 초대를 수락하면 Detective에서 해당 데이터로 인해 동작 그래프 데이터 볼륨이 할당량을 초과하지 않는지 확인할 때까지 멤버 계정의 상태는 수락(활성화되지 않음)으로 표시됩니다. 데이터 볼륨에 문제가 없는 경우 Detective는 자동으로 상태를 수락(활성화)으로 변경합니다. 참고로 현재 수락(활성화되지 않음) 상태인 기존 멤버 계정은 자동으로 활성화할 수 없습니다.	2021년 5월 12일
보안 장에 관리형 정책 정보 추가	보안 장의 새 섹션에서 Detective의 관리형 정책에 대한 세부 정보를 제공합니다. Detective는 현재 단일 관리형 정책 `AmazonDetectiveFullAccess` 를 제공합니다.	2021년 5월 10일
멤버 계정 목록의 데이터 볼륨 값 변경	이제 계정 관리 페이지에서 멤버 계정 목록에 각 멤버 계정의 일일 데이터 볼륨이 표시됩니다. 이전에는 목록에 볼륨이 허용된 전체 볼륨의 백분율로 표시되었습니다.	2021년 4월 29일
멤버 계정 관리 옵션 수정	계정 관리 메뉴를 작업 메뉴로 대체했습니다. 개별 계정을 추가하는 옵션과 .csv 파일에서 계정을 추가하는 옵션을 결합했습니다. 계정 관리에서 계정 활성화를 작업 옆의 별도 옵션으로 이동했습니다.	2021년 4월 5일

동작 그래프 태그 및 태그 기반 권한 부여 추가	Detective를 활성화하면 동작 그래프에 태그를 추가할 수 있습니다. 일반 페이지에서 동작 그래프에 대한 태그를 관리할 수 있습니다. Detective는 태그 값을 기반으로 한 권한 부여도 지원합니다.	2021년 3월 31일
AWS GovCloud (US) 지역에 대한 차이점 추가	이제 지역에서 Detective를 사용할 수 있습니다. AWS GovCloud (US) AWS GovCloud (미국 동부) 및 AWS GovCloud (미국 서부) 에서는 Detective가 회원 계정에 초대 이메일을 보내지 않습니다. 또한 Detective는 AWS에서 종료된 멤버 계정을 자동으로 제거하지 않습니다.	2021년 3월 24일
멤버 계정 상태를 기준으로 멤버 계정 목록을 필터링하는 탭 추가	이제 멤버 계정 목록에 멤버 계정 상태를 기준으로 목록을 필터링하는 데 사용할 수 있는 탭이 표시됩니다. 수락(활성화됨) 상태인 멤버 계정 또는 수락(활성화됨) 이외의 상태인 멤버 계정을 모두 볼 수 있습니다.	2021년 3월 16일
초대 이메일을 억제하는 Python 스크립트에 옵션 추가	이제 Detective `enableDetective.py` 스크립트에서 `--disable_email` 옵션을 제공합니다. 해당 옵션을 포함하면 Detective는 멤버 계정에 초대 이메일을 보내지 않습니다.	2021년 2월 26일

“마스터 계정”이 “관리자 계정”으로 변경	‘마스터 계정’이라는 용어가 ‘관리자 계정’으로 변경되었습니다. Detective 콘솔 및 API에서도 이 용어가 변경되었습니다.	2021년 2월 25일
멤버 계정으로 초대 이메일을 보내지 않도록 API 옵션 추가	Detective API를 사용하여 멤버 계정을 추가할 때 관리자 계정은 멤버 계정에 초대 이메일을 보내지 않도록 선택할 수 있습니다.	2021년 2월 25일
멤버 계정 할당량이 1,200개로 증가	이제 마스터 계정은 최대 1,200개의 멤버 계정을 동작 그래프에 초대할 수 있습니다. 이전에는 할당량이 1,000이었습니다.	2020년 12월 11일
동작 그래프 데이터 볼륨 할당량 값 추가	동작 그래프 데이터 볼륨 할당량에 대한 정보를 업데이트하여 특정 할당량 값을 추가했습니다.	2020년 12월 11일
이제 멤버 계정에서 사용량 및 예상 비용 확인	이제 멤버 계정은 자신의 사용 정보를 볼 수 있습니다. 멤버 계정의 경우 사용량 페이지에는 멤버 계정이 기여한 각 동작 그래프에 수집된 데이터의 양이 표시됩니다. 멤버 계정은 30일 예상 비용도 확인할 수 있습니다.	2020년 5월 26일
이제 무료 평가판이 동작 그래프가 아닌 계정별로 제공	이제 각 계정 Amazon Detective는 각 리전 내에서 별도의 무료 평가판을 받게 됩니다. 무료 평가판은 계정이 Detective를 활성화하거나 계정이 멤버 계정으로 처음 활성화될 때 시작됩니다.	2020년 5월 26일

새로운 오픈 소스 Python 스크립트 GitHub	의 새 amazon-detective-multiaccount-scripts리포지토리는 지역 간 행동 그래프를 관리하는 데 사용할 수 있는 오픈 소스 Python 스크립트를 GitHub 제공합니다. Detective를 활성화하고, 멤버 계정을 추가하고, 멤버 계정을 제거하고, Detective를 비활성화할 수 있습니다.	2020년 1월 21일
Amazon Detective 소개	Detective는 기계 학습과 특수 목적의 시각화를 사용하여 Amazon Web Services(AWS) 워크로드 전반의 보안 문제를 분석하고 조사할 수 있도록 지원합니다.	2019년 12월 2일

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